Az igazságügyi informatikai szakértő a büntetőeljárásban

– doktori értekezés –

Máté István Zsolt
2017

Pécsi Tudományegyetem
Állam és Jogtudományi Kar
Doktori Iskola

Az igazságügyi informatikai szakértő a büntetőeljárásban

– doktori értekezés –

Máté István Zsolt
2017

Témavezető
dr. habil. Nagy Zoltán András (2016-2017)
Balog Zsolt György (2013-2015)

„Az igazságügyi szakértő feladata, hogy a hatóság kirendelése vagy megbízás alapján, a tudomány és a műszaki fejlődés eredményeinek felhasználásával készített szakvéleménnyel, a függetlenség és pártatlanság követelményének megtartásával döntse el a szakkérdést, és segítse a tényállás megállapítását."[1]

[1] 2016. évi XXIX. törvény az igazságügyi szakértőkről 3. § (1)

Tartalomjegyzék

1 Bevezetés

A szakértői munka minden esetben tudományközi tevékenységet takar, melynek rögzített pontja a jogtudomány, változó pontja pedig az a szakterület, melyen a szakértő bizonyítandó tény megállapításához vagy megítéléséhez szükséges különleges szakértelmét alkalmazza.[2]

Azok a tudományterületek, melyek csupán felületesen ágyazódtak be a mindennapokba különösen érzékenyek a bizonyítandó tények szempontjából, tekintettel arra, hogy a tudományterület eredményeit nagyságrendekkel többen használják, alkalmazzák a gyakorlatban, mint ahányan képesek megítélni az egyes kapcsolódó események összefüggéseit. Ilyen tudományterület az alig több mint fél évszázados múltra visszatekintő informatika is.

Az informatika és a jogtudomány kapcsolata – nevezetesen a számítógépes bűncselekmény megjelenése – sem tekinthet hosszú múltra vissza:

> „A bűnügyi informatikai szakterülete még mindig gyerekcipőben jár, nagy szükség van az irányok és definíciók meghatározására. A szakterületen belüli specializáció területén a tanúsítás és tananyagfejlesztés még mindig megkérdőjelezhető.
>
> Folyamatosan szükség van az egyes részterületek szabványosítására, módszertanok létrehozására, melyek lehetővé teszik az egységességet és irányt mutatnak."[3]

Az egyik elsők között feljegyzett eset 1966-ban Mineapolisban történt, melynek során számítógépes programot használtak fel egy gazdasági bűncselekményhez.[4]

A fenti idézet keletkezéséig – 1966 és 2005 között – eltelt közel negyven esztendő alatt még az informatikai területen vezető szerepet betöltő észak-amerikai térség szereplői sem válaszoltak meg minden alapvető kérdést a Digital Forensic Science, magyarul a bűnügyi informatika tudományterületén.

---

[2] 1998. évi XIX. törvény a büntetőeljárásról (Be.) 99. §

[3] BRINSON, Ashley –ROBINSON, Abigail – ROGERS, Marcus: A cyber forensics ontology: Creating a new approach to studying cyber forensics. in digital investigation 3S (2006) S37 – S43, Amsterdam, 2006., a szerző fordítása

[4] JOHNSON, Thomas A. (editor): Forensic Computer Crime Investigation. Boca Raton, FL, USA, 2005. CRC Press.

2 A kutatás tárgya, célja és módszere

2.1 A problémafelvetés aktualitása

Amikor az 1960-as évek elején a köztudatba került a globális falu gondolata[5] még kevesen gondolták, hogy harminc esztendő múltán az emberi környezet digitalizálódása formájában fog megvalósulni (internet, mobiltelefónia stb.). Még kevesebben voltak azok, akik a következményeket előre látták volna, különösen azt, hogy a globális falu lakói milyen mennyiségben hagynak majd maguk után digitális nyomokat, mely alapján tevékenységük utólagosan nyomon követhetővé, felderíthetővé válik. Az, hogy a digitalizálódás megváltoztatta-e az emberi gondolkodást, még vitatják, de az kétségtelennek látszik, hogy a jelenségre minden tudományterületnek – így a jogtudománynak is – meg kell keresnie és meg kell adnia a saját válaszait.

A téma átfogó áttekintése már megkezdődött, gondoljunk akár az információs társadalomban megjelenő bűnözés átfogó vizsgálatára[6], akár az ennél szűkebb információbiztonság, adatbiztonság területét feldolgozó tanulmányokra[7]. Az információtechnológia azonban megjelenik azon bűncselekmények esetében is, melyek nem irányulnak közvetlenül információs rendszer ellen, illetve nem az ilyen rendszerek felhasználásával követik el. Ezen cselekmények során az információs rendszerek, illetve az informatikai eszközök – gondoljunk rájuk most a lehető legtágabb értelemben – „csupán" a nyomhordozó[8] szerepkörben jelennek meg, közvetlen, vagy közvetett információkat hordozva a cselekménnyel, vagy annak elkövetőjével kapcsolatban. Ez a feltétel a gyakorlatban csaknem valamennyi bűncselekmény típus esetén megállja a helyét, azaz bármely bűnügy nyomozása során találhatunk olyan informatikai eszközt, mely adatokat szolgáltathat az eljáráshoz. Mivel ez a terület – a hagyományos bűncselekmények során keletkező digitális nyomok vizsgálata – kevéssé került mindezidáig a kutatói érdeklődés fókuszába, jelen tanulmány hiánypótló lehet.

A jogalkalmazókon – ügyvédek, nyomozók, ügyészek, bírák – kívül a kutatás az igazságügyi informatikai szakértőnek is adhat új szempontokat munkájuk egységesítése területén.

---

[5] MCLUHAN, Marshall: The Gutenberg Galaxy. Routledge & Kegan Paul, London, 1962. p. 31.

[6] SZATHMÁRY Zoltán dr.: Bűnözés az információs társadalomban. Budapest, 2012. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskolája „Informatikai és Kommunikációs Jog" Program.

[7] SZÁDECZKY Tamás: Szabályozott biztonság. Az informatikai biztonság szabályozásának elmélete, gyakorlata és az alkalmazás megkönnyítésére felállított módszertan. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, 2011. Pécs.

[8] TREMMEL Flórián – FENYVESI Csaba: Kriminalisztika tankönyv és atlasz. Budapest-Pécs, 2002. Dialóg Campus. p. 29.

Magyarországon napjainkban alig több mint másfélszáz[9] igazságügyi informatikai szakértő (természetes személy) dolgozik. E szakértői közösség 2013 áprilisában tartotta második országos konferenciáját, ahol több előadó – közöttük jelen sorok szerzője is – megfogalmazta az egységes módszertan kialakítása iránti igényt.

Napjainkban ugyanis a szakértők saját ügyeik megoldásánál egyénenként munkálják ki azokat az eljárásokat, melyeket követnek a bizonyítás során. A közös követelményrendszer, s nem egyszer a tudományos megalapozottság hiánya hibás, vagy támadható következtetésre vezetik az igazságügyi informatikai szakértőket.

A helyzet tarthatatlanság nem csupán az új szakértői törvény elfogadásában mutatkozik, mutatkozott meg, hanem az igazságügyi informatikai szakértők saját szakmai kezdeményezései is ebbe az irányba mutatnak.

2.2 Hipotézis

A Digital Forensic Science, mint a jog segédtudománya – melynek letéteményesei az igazságügyi informatikai szakértők – elsősorban informatikai és kriminalisztikai megközelítést alkalmaz. Ez a kettős nézőpont a műszaki és társadalomtudományi területek között megfigyelhető hagyományos távolságtartás miatt csökkentik az informatikai vonatkozásokat is tartalmazó büntetőeljárások hatékonyságát, megbízhatóságát és hitelességét. A területek közti távolság minimalizálása a Digital Forensic Science tudományterület magyarországi beágyazottságának megteremtése és elmélyítése révén valósulhat meg, melynek érdekében szükséges megvizsgálni a következőket:

1. Az igazságügyi informatikai szakértői vizsgálatokat mely bűncselekmény típusok esetén veszik igénybe a jogalkalmazók?
2. Az egyes bűncselekmény típusok esetén a vizsgálat mire irányul (szoftverek, hardverek, rendszerek stb.)?
3. A leggyakoribb bűncselekmény típusok legjellemzőbb szakértői vizsgálati irányaira vonatkozóan léteznek-e nemzetközi szabványok, ajánlások?

[9] Az adatgyűjtés lezárásakor (2016. január 8.) az Igazságügyi Minisztérium által vezetett szakértői névjegyzék szerint 156 fő természetes személy rendelkezett valamely informatikai kompetenciával

A kérdésekkel kapcsolatos munkahipotézis szerint:

1. Az igazságügyi informatikai szakértői vizsgálatok az egyes bűncselekmény típusok vonatkozásában nem egyenletesen oszlik meg, azok közül néhány terület kiemelkedik (az előfordulási gyakoriság, az elkövetési érték szempontjából), melyek tudományos vizsgálata növelheti a szakértői bizonyítás hatékonyságát.
2. A bűncselekmény típusok és a szakértői vizsgálat iránya (tárgya) között szoros korreláció áll fenn, melynek vizsgálata megalapozhatja a kriminál taktikai döntéseket a büntetőeljárás nyomozási szakaszában.
3. A leggyakoribb bűncselekmény típusok és legjellemzőbb vizsgálati területekre (tárgyakra) vonatkozóan már kialakultak a nemzetközi szabványok és ajánlások, melyek honosítása növelheti a szakértői vizsgálatok megbízhatóságát és hitelességét.

2.3 A feldolgozás módszere

2.3.1 A vizsgálati terület lehatárolása

A kutatás fókuszában a büntetőeljárás során végzett igazságügyi informatikai szakértői tevékenység áll. Így nem kerül szó a polgári, közigazgatási eljárásokban történő részvételről, melyek több vonatkozásban eltérést mutatnak a vizsgált ügykörhöz képest. Hasonló szűkítés alá esik a magánmegbízások[10] köre, melynek egy része ugyan kapcsolódhat büntetőeljáráshoz is (pótmagánvád, fellebbezés stb.) de ez kívül esik a kutatás célterületén: nagyobb részt a büntetőeljárás nyomozási és kisebb részt a bírósági szakaszán.

A kutatás nem terjed ki az igazságügyi informatikai szakértőkre is hatást gyakorló szervezeti módosulásokra (Magyar Igazságügyi Szakértői Kamara tervezett, illetve a tanulmány írásának idején már megvalósult átalakítására), valamint az igazságügyi szakértői tevékenységről szóló 2005. évi XLVII. törvény (Szaktv.[2005]) módosítására sem[11]. Ez utóbbit annyiban veszi figyelembe a kutatás, amennyiben az a szakmai protokollokat érinti és amennyiben kutatás lezárásakor hatályos állapotú.

2.3.2 A kutatás adatforrásai

A kutatás a magyarországi büntetőeljárás vizsgálatán alapszik, annak gyakorlatát elemezi, így adatforrása nem lehet más, mint a szerző saját igazságügyi informatikai szakértői nyilvántartása, az abban szereplő 342 ügy[12] adatai. A kutató által teljes részletességgel ismert alapanyagból a vizsgálati terület lehatárolásánál írt szempontok szerint összesen 282 ügy felelt meg a kritériumoknak, ezek anonimizált módon történő felhasználása (Szaktv.[2005] 12. § (3) / Szaktv.[2016] 40. § (3) szerint) történik meg a tanulmányban.

[10] Ezt a 2016. évi XXIX. törvény 52. §-a – korábbi jogszabálytól eltérően –részletesen szabályozza

[11] 2016. június 15-én lépett hatályban az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény

[12] Az elemzés lezárásakori ügyszám

A kutatás – forrásaiból és jellegéből adódóan – erősen támaszkodik a szakértői vizsgálatok során kinyert és a büntetőeljárásokban felhasznált digitális bizonyítékokra. Ebből adódóan a digitális bizonyítékok, ontológiai vizsgálata, klasszifikálása és feldolgozási módjaik meghatározása a kutatás alapvető elemeiként jelennek meg.

A tapasztalati tényeken alapuló részt a nemzetközi szakirodalom áttekintése, valamint a Digital Forensic Science területén működő nemzetközi szervezetek ajánlásainak és a Nemzetközi Szabványügyi Szervezet (International Organization for Standardization) által elfogadott szabványok részletes elemzése egészíti ki. A nemzetközi szakirodalomból elsősorban a legnagyobb számban előforduló angol nyelvű, kisebb részben pedig az orosz nyelven megjelenő tanulmányok feldolgozása történik meg.

2.3.3 A kutatás módszerei

Az eltérő jellegű források más és más feldolgozási módszert kívánnak meg. Az empirikus adatok feldolgozása elsősorban statisztikai módszerekkel történik, melyet kiegészít az ügyek nem informatikai vonatkozású tényeit és körülményeit értékelő kvalitatív módszerek. A kettős megközelítés indokoltságát alátámasztja a vizsgálat korábbiakban már említett kettős (műszaki és társadalomtudományi) nézőpontja, illetve a műszaki tartalmak, tények mögött esetlegesen meghúzódó jelenségek feltárásának lehetősége. Az elemzés felvázolt módja lehetőséget ad arra, hogy a kutató kapcsolatot keressen a vizsgálatok műszaki-informatikai vonatkozásai és a vizsgálatban érintett személyek (tipikusan terhelt) viselkedési módjai, szokásai között, ezzel új eszközt adva a jogalkalmazók, elsősorban a nyomozók kezébe.

3 Az igazságügyi szakértői tevékenység jogszabályi keretei

Az igazságügyi informatikai szakértői munka jogszabályi kereteinek megismerése nélkül a szakmai és módszertani felvetések nehezen értelmezhetők. E keretek felvázolása az első feladatok közé tartozik, ugyanakkor a túlzóan részletes ismertetést a kutatás irányultságán kívül – nem jogtörténeti, vagy jogelméleti, hanem empirikus alapú joggyakorlatot vizsgáló, módszertani következtetések levonására irányuló vizsgálatról van szó – gátolja az igazságügyi szakértői tevékenységről szóló 2005. évi XLVII. törvény 2016 év első negyedévére tervezett[13] nagymértékű átalakítása is[14].

A fenti okok miatt a jogszabályi keretek alapvető – feltételezhetően nem változó – jellemzői kerülnek bemutatásra.

3.1 Szakétői törvény(ek)

Magyarországon az igazságügyi szakértői tevékenység jogszabályi alapját a Szaktv.[2005] / Szaktv.[2016] alapozza meg[15], mely a – a mottóban már idézett – első szakaszában meghatározza a szakértők alapvető feladatát: „... segítse a tényállás megállapítását, a szakkérdés eldöntését.”.[16] A Szaktv.[2016] szerint pedig: „…döntse el a szakkérdést, és segítse a tényállás megállapítását.”[17]

E szabályozás rögzíti a szakértőkkel kapcsolatos alapvető körülményeket:

- az igazságügyi szakértővé válás szabályait és szakterület változtással kapcsolatos teendőket,
- a szakértői névjegyzékkel kapcsolatos követelményeket és hatásköröket,
- a szakértők jogait és kötelezettségeit,
- a szakértők kirendelésével összefüggő tartalmi és eljárási körülményeket,
- a szakértői vélemény tartalmi és formai összetevőinek meghatározását,
- a szakértők képzésével kapcsolatos teendőket,
- a szakértői munka ellenőrzésének részleteit,
- a gazdasági társaságként történő szakértői munka kereteit,
- az igazságügyi szakértői intézmények létesítési és működési körülményeit,
- a szakértő munkáját segítő személyek (szakértőjelölt, szakkonzultáns, segédszemélyzet) alkalmazásának feltételeit, valamint
- a szakértői módszertani levéllel kapcsolatos határköröket és tennivalókat.

[13] A Kormány 2016. évi tavaszi törvényalkotási programja. TÖRVF-Á/2/2015. Melléklet, 16. tétel. Online: http://www.parlament.hu/documents/10181/87979/Tvalk_program_2016 _tavasz.pdf/a1eac7dd-8247-413a-bada-0311579775f8, hozzáférés: 2016. február 8.

[14] A jogszabálytervezet 2016. január 12-én került társadalmi vitára

[15] A kézirat lezárásakor hatályban lévő 2016. évi XXIX. törvénnyel azonos módon

[16] Szaktv.[2005] 1. § (1)

[17] Szaktv.[2016] 3. § (1)

A törvény egyes részletszabályokat alacsonyabb szintű jogszabály – elsődlegesen az igazságügyért felelős miniszter rendeletének, illetve egyes kérdések esetén a kormány rendeletének – hatáskörébe utalja. Így az igazságügyi szakértői szakterületekről, valamint az azokhoz kapcsolódó képesítési és egyéb szakmai feltételekről a 9/2006. (II. 27.) IM rendelet szól részletesen, míg az igazságügyi szakértői működés egyes részletszabályait a 31/2008. (XII. 31.) IRM rendelet határozza meg.

Az informatikai szakterülettel kapcsolatos releváns szabályok közül kiemelendő a Kormány 282/2007. (X. 26.) sz. rendelete, melyben lehetővé teszi[18], hogy az informatikai szakkérdések vizsgálatában a feljogosított szerven (Bűnügyi Szakértői és Kutatóintézet[19]) kívül egyéni szakértők is adhassanak szakértői véleményt.

3.2 A szakterületeket szabályozó miniszteri rendelet

A szakterületek elkülönítése Szaktv.[2005] 3. § (1) / Szaktv.[2016] 5. § (5) bekezdésében foglalt felhatalmazás alapján a 9/2006. (II. 27.) IM rendeletben történik meg. A rendelet az informatika vonatkozásában a következő szakterületeket[20] határozza meg:

- informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver)
- informatikai biztonság
- informatikai rendszerek tervezése, szervezése
- stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység
- számítástechnikai adatbázis, adatstruktúrák
- szoftverek

E szabályozás megszünteti a korábbi szakterület megnevezéseket, melynek emlékét a mai napig őrzik az Igazságügyi Minisztérium által vezetett szakértői névjegyzék[21] kereső kifejezései (részletesen lásd: 14.1 Informatikai szakterületek (2006 előtt)).

[18] 282/2007. (X. 26.) Korm. rendelet a szakterületek ágazati követelményeiért felelős szervek kijelöléséről, valamint a meghatározott szakkérdésekben kizárólagosan eljáró és egyes szakterületeken szakvéleményt adó szervekről. 5. §, valamint a 4. sz. melléklet Szakvélemény adására feljogosított szervek. 1. h) pontja.

[19] Jogutódja a nemzeti Szakértői és Kutató Központ

[20] 9/2006. (II. 27.) IM rendelet 6. sz. melléklet A) Igazságügyi szakértői szakterületek és az azokhoz kapcsolódó képesítési feltételek az informatikai területeken

[21] Igazságügyi Szakértői Névjegyzék. Online: https://szakertok.im.gov.hu/Shared/SelectSzakteruletView, hozzáférés: 2016. január 9. [a hivatkozás átirányításra került a https://inyr.im. gov.hu/szakertok címre, hozzáférés: 2016.09.17]

A 2017 áprilisi állapot szerint az informatikai és hírközlési szakterületen az alábbi megoszlás mutatkozott a fő szakterület vonatkozásában az Igazságügyi Minisztérium nyilvántartása alapján:

1. táblázat - Informatikai és hírközlési szakterült szakértőinek szakterületi megoszlása

Fő szakterület megnevezése	Fő
elektromágneses összeférhetőség (EMC)	1
elektronikus hírközléssel összefüggő méréstechnika	5
informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver)	67
informatikai biztonság	27
informatikai rendszerek tervezése, szervezése	23
műsorszolgáltatással összefüggő elektronikus hírközlési tevékenység	3
stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység	5
számítástechnikai adatbázis, adatstruktúrák	2
szoftverek	12
vezeték nélküli elektronikus hírközlés	2
vezetékes elektronikus hírközlés	6
Összesen	**153**

Az informatikai és hírközlési szakterületen ugyanezen időszakban a szakértők területi megoszlása a következő volt az Igazságügyi Minisztérium nyilvántartása alapján

2. táblázat - Informatikai és hírközlési szakterület szakértőinek területi megoszlása

Terület	Fő
Bács-Kiskun	7
Baranya	10
Békés	6
Borsod-Abaúj-Zemplén	7
Budapest	40
Csongrád	8
Fejér	7
Győr-Moson-Sopron	9
Hajdú-Bihar	9
Heves	5

Terület	Fő
Jász-Nagykun-Szolnok	2
Nógrád	1
Pest megye	15
Somogy	6
Szabolcs-Szatmár-Bereg	4
Tolna	1
Vas	4
Veszprém	6
Zala	6
Összesen	**153**

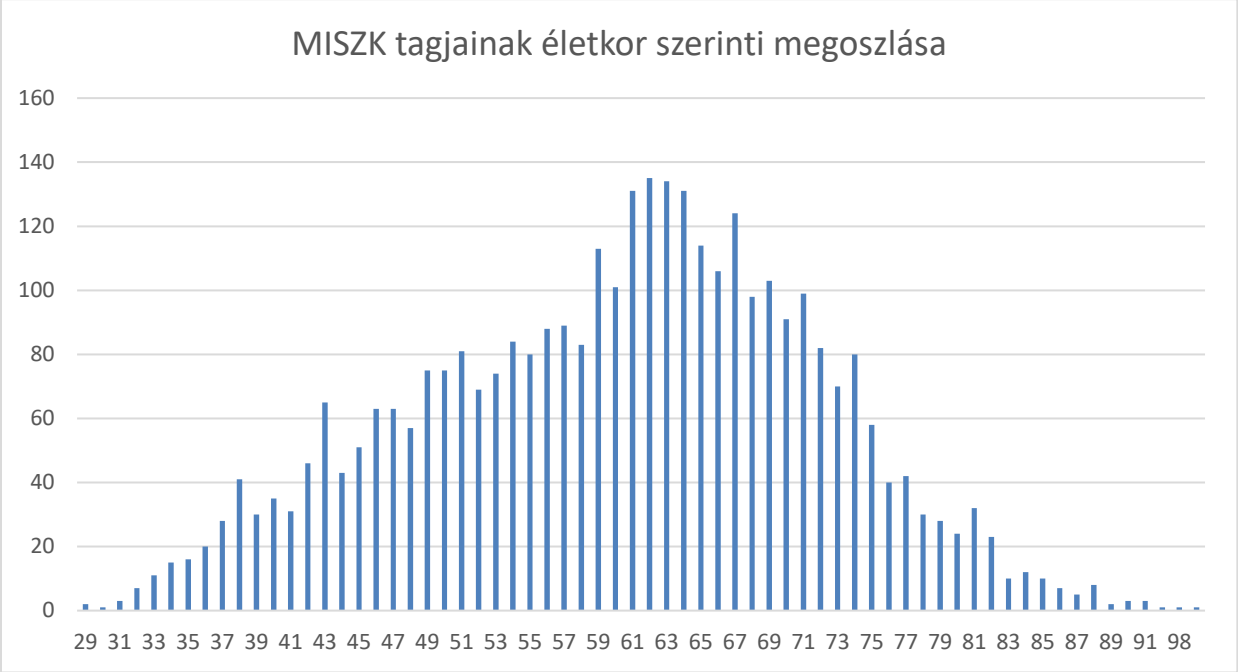
Az egyes informatikai szakterületekre vonatkozó képesítési követelmények az alábbi tizenöt – felsőfokú oktatásban megszerezhető – szakképesítést írják elő (a függelékben 14.2 pontjában bemutatott formában):

- informatikai szakirányon végzett okleveles gazdaság-informatikus
- mérnök-informatikus
- okleveles alkalmazott matematikus
- okleveles fizikus
- okleveles gazdaságmatematikai elemző szakos közgazdász
- okleveles informatika szakos tanár
- okleveles matematikus
- okleveles mérnök-informatikus
- okleveles programtervező matematikus
- okleveles rendszerinformatikus
- okleveles villamosmérnök
- programozó matematikus
- számítástechnika szakos tanár
- villamosmérnök

A fenti követelmények mellett az aktuális helyzet értékeléséhez néhány statisztikai adatsort érdemes figyelembe venni az informatikai és hírközlési szakterület igazságügyi szakértőire vonatkozóan:

Átlagéletkor:	52 év
Lefiatalabb szakértő	33 éves
Legidősebb szakértő	84 éves
65 év feletti szakértők	23 fő
60 – 65 év közötti szakértők	24 fő
55 – 60 év közötti szakértők	16 fő
50 – 55 év közötti szakértők	20 fő
45 - 50 év közötti szakértők	19 fő
40 – 45 év közötti szakértők	28 fő
35 – 40 év közötti szakértők	19 fő
30 – 35 év közötti szakértők	4 fő

Amennyiben az informatikai és hírközlési szakterület igazságügyi szakértőire vonatkozó életkori adatsort összevetjük a Magyar Igazságügyi Szakértői Kamara valamennyi tagjára (3 478 fő) vonatkozó korfa (lásd az alábbi diagramot) adataival, akkor meg állapíthatjuk, hogy az átlaghoz képest kedvezőbb helyzetben van a szakterület (életkor tekintetében), ugyanakkor megfigyelhető a fiatal szakértők hiánya is, mely valamennyi szakterületen jelentkezik.



1. ábra - MISZK tagjainak életkor szerinti megoszlása (2017.04.10-i állapot szerint)

A fenti adatsorok még akkor is figyelem felkeltőek, ha a végzettségre és a gyakorlati időre vonatkozó követelmények alapján nyilvánvaló, hogy 30 éves kor alatt lényegében nem szerezhető szakértői jogosultság.

3.3 A szakértői vélemény formai és tartalmi követelményei

Az igazságügyi szakértői tevékenység további alapvető eleme a szakértői vélemény, illetve annak tartalmi és formai meghatározása. E követelmények formai részét a Szaktv.[2005] a következők szerint tartalmazta:

> „(3) A szakvélemény magában foglalja a kirendelő hatóság által feltett kérdések megválaszolását, továbbá a feltett kérdésekkel összefüggő más szükséges megállapítások közlését.
>
> (4) Az igazságügyi szakértő az írásbeli szakvéleményt aláírásával köteles ellátni, és köteles azon feltüntetni a nyilvántartási számát. A szakvéleményt az igazságügyi szakértő ellátja bélyegzőjével is. A bélyegző feltünteti az igazságügyi szakértő nevét, az igazságügyi szakértői igazolványában meghatározott szakterületét és a nyilvántartási számát. A bélyegzőn az állami címer nem használható.
>
> (5) Az igazságügyi szakértő az elektronikus kézbesítés útján benyújtott szakvéleményben köteles nevét és nyilvántartási számát feltüntetni, és azt elektronikus úton, a külön jogszabályban meghatározott biztonságos elektronikus kézbesítési szolgáltatás útján kézbesíteni.”[22]

Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény 47. §-ában foglalkozik a szakvélemény tartalmi elemeivel a következők szerint:

> „(4) A szakvéleménynek tartalmaznia kell
>
> a) a leletet,
> b) a vizsgálat módszerének rövid ismertetését,
> c) a szakmai ténymegállapításokat,
> d) a szakértő véleményét,
> e) ha az ügyben korábban vizsgálat lefolytatására került sor és a kirendelés erre kiterjed, a korábbi vizsgálatra vonatkozó adatok és megállapítások értékelését,
> f) a módszertani levélre történő utalást, illetve a módszertani levélben foglaltaktól történő eltérés esetén ennek indokait és
> g) az arra való utalást, hogy az igazságügyi szakértő mely szakterületen jogosult szakvéleményt adni, illetve, hogy az igazságügyi szakértő vagy más személy eseti szakértőként járt el.”

[22] Szaktv.[2005] 16. § (3) – (5)

Megfigyelhető, hogy a felsorolás csaknem szó szerinti egyezést mutat a 31/2008. (XII. 31.) IRM rendelet 10. §-val (lásd alább), ami arra utal, hogy a szabályozást a jogalkotó a jogszabályi hierarchia magasabb szintjére emelve nyomatékosította:

> „10. § (1) A szakvéleménynek tartalmaznia kell:
>
> a) a vizsgálat tárgyára, a vizsgálati eljárásokra és eszközökre, a vizsgálat tárgyában bekövetkezett változásokra vonatkozó adatokat (lelet),
> b) a vizsgálat módszerének rövid ismertetését,
> c) a szakmai megállapítások összefoglalását (szakmai ténymegállapítás),
> d) a szakmai ténymegállapításokból levont következtetéseket, ennek keretében a feltett kérdésekre adott válaszokat (vélemény).
>
> (2) Ha az ügyben korábban vizsgálat lefolytatására került sor - ide nem értve a szakértői vizsgálatot -, a szakértőnek a szakvéleményben értékelnie kell annak adatait és megállapításait is."[23]

A korábbiaktól eltérően a törvényjavaslat (majd a hatályba lépett törvény) a szakvélemény két releváns komponensének meghatározását is tartalmazza az alábbiak szerint:

> „8. lelet: a szakvélemény részét képező tartalmi egység, amely a vizsgálat tárgyára, a vizsgálati eljárásokra és eszközökre, valamint a vizsgálat tárgyában bekövetkezett változásokra vonatkozó adatok összességét tartalmazza,
>
> …
>
> 11. szakmai állásfoglalás: a szakvélemény részét képező tartalmi egység, amely a szakmai ténymegállapításokból levont következtetéseket, ennek keretében a feltett kérdésekre adott válaszokat tartalmazza,"[24]

Azonosan a Szaktv.[2016] végleges szövegével:

> „12. *lelet*: a szakvélemény részét képező tartalmi egység, amely a vizsgálat tárgyára, a vizsgálati eljárásokra és eszközökre, valamint a vizsgálat tárgyában bekövetkezett változásokra vonatkozó adatok összességét tartalmazza"

Tartalmilag azonosan, de eltérő megnevezéssel, szakmai állásfoglalás helyett a szakértő véleményeként:

> „15. *a szakértő véleménye:* a szakvélemény részét képező tartalmi egység, amely a szakmai ténymegállapításokból levont következtetéseket, ennek keretében a feltett kérdésekre adott válaszokat tartalmazza,"

[23] 31/2008. (XII. 31.) IRM rendelet 10. §

[24] Szaktv. 2016. évi módosítása törvényjavaslat, 2. § 8 és 11. [Forrás: miszk.hu, 2016.01.13]

A Szaktv.2016 hatályba lépés előtti módosítására vonatkozó előterjesztés – jelen kutatás szempontjából releváns – vitatott tartalmai elemei a következők[25]:

A szakértő feladatára vonatkozóan

> „A tervezet 3. § (1) bekezdését pontosítani javasoljuk, a szakértőnek a szakkérdés eldöntését nem segítenie kell, hanem a szakkérdésben állást kell foglalnia, a rendelkezésére álló tények, körülmények alapján, szakmai módszerek és eszközök segítségével más – releváns – tényeket kell megállapítania."[26]

A Szaktv.2016 végleges szövege szerint:

> „Az igazságügyi szakértő feladata, hogy a hatóság kirendelése vagy megbízás alapján, a tudomány és a műszaki fejlődés eredményeinek felhasználásával készített szakvéleménnyel, a függetlenség és pártatlanság követelményének megtartásával **döntse el a szakkérdést**, és segítse a tényállás megállapítását."

A törvény a kamarai javaslathoz képest is nyomatékosítva, aktív szerepet ruház a szakértőre, egyben tevékenységének pontos célját – tényállás megállapítása – is rögzíti.

A szakértői véleményre vonatkozóan

> „A 2. § értelmező rendelkezései a szakvélemény tekintetében álláspontunk szerint hiányosak és ezt a 20. alcím rendelkezései sem orvosolják. A 2. § 8. pontjában a tervezetben a leletet, 11. pontjában pedig a szakmai állásfoglalást, mint a szakvélemény részeit írja körül.
>
> Emellett foglalkozni kellene a szakvélemény többi fontos részével is, mint pl.: a vizsgálattal (amelyben tételesen felsorolásra kerülnek azok az adatok, ismérvek, mérési eredmények, sajátosságok stb. és mindezek illusztrációi, amelyek a vélemény kialakítását megalapozzák), és az értékeléssel (amely a vizsgálati eredményekből kialakuló vélemény milyenségét magyarázza. Javasolt a vélemény rész önálló megnevezése is, kérdésekre tömören válaszoló része, amely a szakvéleménynek a kirendelő végzésben feltett kérdésekre tömören válaszoló része."[27]

A Szaktv.2016 végleges szövege a kamarai javaslatnak megfelelően alakult.

---

[25] A Pécsi Igazságügyi Szakértői Kamara honlapjának fórum rovatában lefolytatott szakmai vita anyagai alapján. Forrás: http://miszk.hu/system/files/piszk_elnokseg_velemenye_a_szakertoi _torveny_tervezett_mod....pdf

[26] A Magyar Igazságügyi Szakértői Kamara véleménye az igazságügyi szakértőkről szóló törvény tervezetével kapcsolatban. p.7. Forrás: http://miszk.hu/system/files/a_miszk_ velemenye _az_igazsagugyi_szakertokrol_szolo_torvenyterevezetrol.pdf

[27] MISZK véleménye im. p. 9.

3.4 A módszertani levél, mint a szakértői működés zsinórmértéke

Sem a törvényjavaslat, sem a Kamarák által megfogalmazott észrevételek nem tartalmaznak konkrét javaslatot a módszertani levelekre vonatkozóan[28]. A részletes szabályozás nem is e jogszabályi szint feladata lenne, ugyanakkor a módszertani levél tartalmi elemeinek, a szakértői véleményéhez hasonló definiálása fontos üzenet lehetett volna a létrehozásukért felelős Magyar Igazságügyi Kamara új szervezetének.

A törvényjavaslat szövege a módszertani levél segítő, standardizáló funkciójáról a számonkérés, felelősségre vonhatóság irányába helyezi át a hangsúlyt (lásd például a szakértők értékelésére vonatkozó részt):

> „(2) Az értékelést megalapozó vizsgálatnak – a jogerősen befejezett ügyek alapján – fel kell tárnia az igazságügyi szakértő gyakorlatát, különös tekintettel az alkalmazott gyakorlatnak az érintett szakterület által támasztott elméleti tételeknek való megfelelését, valamint az adott szakterületen kiadott módszertani leveleknek történő megfelelését."[29]

A jogszabály tervezethez képest a végleges normaszöveg jóval részletesebben szól a területről, ha lehet még jobban nyomatékosítja a felelősség kérdését az alábbiak szerint:

> „(3) Az értékelést megalapozó vizsgálatnak - alapvetően a jogerősen befejezett ügyek alapján - fel kell tárnia az igazságügyi szakértő gyakorlatát, különös tekintettel arra, hogy
>
> a) a szakvélemény előkészítése, elkészítése, valamint előterjesztése a vonatkozó jogszabályoknak megfelelt-e,
>
> b) az igazságügyi szakértő a jogszabályok és a hatóság által előírt határidőket és az ügyviteli, valamint adatkezelési szabályokat megtartotta-e,
>
> c) az igazságügyi szakértő a hatóság által feltett kérdések közül valamenynyi kérdésben véleményt nyilvánított-e,
>
> d) az igazságügyi szakértő a hatóságokkal megfelelően együttműködött-e, a jogszabályban előírt kötelező bejelentési kötelezettségeinek eleget tett-e,
>
> e) a szakvélemény megszerkesztése a jogszabályoknak és a releváns szakmai gyakorlatnak megfelelően, a hatóságok és a Kamara által elvárt megfelelő szakmai színvonalon történt-e,

[28] A Szaktv. 2016. évi módosítása törvényjavaslat, X. fejezetében a módszertani levél létrehozásának adminisztratív körülményeit szabályozza csupán.

[29] Szaktv. 2016. évi módosítása törvényjavaslat, 8. § 2) [Forrás: miszk.hu, 2016.01.13]

f) az igazságügyi szakértő a rá vonatkozó továbbképzési követelményeknek eleget tett-e, valamint azok eredményeit a szakmai tevékenységébe megfelelően integrálta-e,

g) az igazságügyi szakértő munkája során segédszemélyzet, szakkonzultáns, illetve szakértőjelölt közreműködését igénybe vette-e és

h) az igazságügyi szakértőre vonatkozó jogszabályi előírásoknak, kamarai és egyéb szakmai szabályzatoknak az adott szakterületen kiadott szakértői módszertani leveleknek (a továbbiakban: módszertani levél) az igazságügyi szakértő eljárása megfelelt-e.[30]

3.5 A büntetőeljárásról szóló törvény főbb szakértői vonatkozásai

A jogszabályi keretek áttekintésénél a második kiemelendő terület a – jelen kutatás tárgyát képező – büntetőeljárásban történő szakértői működés szabályainak számba vétele. Ennek elsődleges forrása a büntetőeljárásról szóló 1998. évi XIX. törvény (Be.).

A jogszabály szakértők alkalmazására vonatkozó szövege összecseng a tanulmány mottójával:

> „Ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges, szakértőt kell alkalmazni."[31]

Az igazságügyi szakértők büntetőeljárásban történő alkalmazásával összefüggésben az alábbiakat szabályozza a törvény:

- a szakértő kizárásának körülményeit,
- a szakértői vizsgálat egyes tartalmi elemeit,
- a szakértő eljárása során történő közreműködési kötelezettséget,
- a szakértői vélemény előterjesztésének módját,
- a szakértő (egyéni és párhuzamos) meghallgatásának körülményeit,
- újabb szakértő igénybe vételének módját, valamint
- a szakértői kötelezettség megszegésének szankcionálását.

A fentiekben kiemelt, a szakértőkre közvetlenül vonatkozó szabályozások kívül említést érdemel még az egyes bizonyítási eszközökre és az egyes eljárási szakaszokban történő részvétel módjára vonatkozó szabályok, melyek értékeléssel együtt történő bemutatására a későbbiekben kerül sor.

Összességében megállapítható, hogy az igazságügyi szakértői tevékenységet szabályozó harminckét hatályos jogszabály[32] (részletesen lásd a függelék 14.3 sz. pontjában) megszabja a szakértői tevékenység célját, szakterületeit, a tevékenységgel kapcsolatos

[30] Szaktv. 2016 17. § (3)

[31] 1998. évi XIX. törvény a büntetőeljárásról (Be.) 99. § (1)

[32] Utolsó ellenőrzés 2016.09.25.

szakmai követelményeket, illetve a szakértői működés körülményeinek tartalmi és formai kereteit.

4 A Digital Forensic Science eredete és tartalma

Az informatika – különösen a jogtudománnyal összevetve – fiatal tudomány, a részterületekre történő szétválására, a szakemberek specializálódására az utóbbi évtizedben került jórészt sor. Az informatikai alapokon nyugvó bűnügyi informatikai tudomány, a Digital Forensic Science ontológiai megközelítése[33] és a klasszifikációja is csupán az elmúlt néhány évben vált témává a tudományterület művelői között, a következőkben e folyamat bemutatásra kerül sor.

4.1 A tudományterület kialakulása

A bíróság előtti bizonyíték bemutatás – vagyis a forenzikus tudományok gyakorlati alkalmazása – jó néhány évszázados múltra tekinthet vissza (lásd a 14.4 számú függelékben), e történet utolsó évtizedeiben minden bizonnyal a Digital/Computer Forensics volt (van) a meghatározó tényező.

Ha a Digital Forensic Sciene helyét keressük, viszonyítási alapként szükségünk van a törvényszéki tudomány meghatározására is:

> A kriminalisztika a bizonyítékok bíróság előtt történő bemutatásának folyamata, mely tudományos ismereteket használ a bizonyítékok összegyűjtésénél, elemzésénél és bemutatásánál. [34]

Egy újonnan formálódó tudományterület (Digital Forensic Science) első feladatai közé tartozik az öndefiníció. Ez a mozzanat nem csupán a kutatott téma elkülönítését igényli, de az annak azonosítására szolgáló elnevezés megadása is feladata. A Digital Forensic Science az informatika és a jogtudomány határán helyezkedik el:

> Azokat a tudományos módszereket és eljárásokat foglalja magába, melyek a jogi eljárásokat látják el hiteles információval azon esetekben, ahol digitális adat és/vagy – a kifejezés tágabb értelmében vett – a számítógép rendszer is az ügy részét képezi[35].

[33] BRINSON et al. im.

[34] NOLAN, Richard - O'SULLIVAN, Colin - BRANSON, Jake - WAITS, Cal: First Responders Guide To Computer Forensics Pittsburg 2005. Carnegie Mellon Software Engeneering Institute. p. 3.

[35] MÁTÉ István Zsolt: Digital Forensic Science: szabványosítási törekvések régen és ma. Budapest, Budapesti Igazságügyi Szakértői Kamara, 2013. p. 1.

A munkadefiníciónak tekintendő meghatározás jelzi, hogy az alkalmazott tudományok területén, a bűnügyi tudományok[36] egy részterületeként kell keresnünk a Digital Forensic Science helyét. A terület elnevezése még koránt sem egységes, találkozhatunk a Cyber Forensics, Cyber Crime, Computer Forensics, Computer-related Crime elnevezésekkel az angolszász nyelvterületen. Orosz és német nyelvterületen szintén használatos Digital Forensic Science kifejezés tükörfordítása: цифровая криминалистика, illetve a digitale Forensik, habár az orosz szakirodalom és jogi szaknyelv használja a судебная компьютерно-техническая экспертиза[37] kifejezést is.

A magyar nyelvben egyelőre nem honosodott meg a szakterület azonosítására szolgáló kifejezés. Ha szó szerinti fordítás helyett a szakterület kriminalisztikával rokon vonásait és a digitális környezetre utaló már meghonosodott kifejezést használjuk, akkor a bűnügyi informatika kifejezés látszik helyénvalónak.

A szakterület meghatározása területén a 2001-ben megalakult Digital Forensics Research Workshop szervezet a fentinél részletesebb definíciót alakított ki első kongresszusán a New York állambeli (USA) Utica-ban az alábbiak szerint:

> "Digital Forensic Science
>
> A bevált tudományos módszerek használata a digitális forrásból származó bizonyítékok megőrzése, összegyűjtése, ellenőrzése, azonosítása, elemzése, értelmezése dokumentálása és bemutatása területén, a bűncselekményeknek bizonyult események rekonstrukciójának megkönnyítése, vagy támogatása céljából, vagy támogatva a felkészülést a jogosulatlan tevékenységek feltárása céljából, melyek zavart okozhatnak a megtervezett műveletekben. [38]

Amint az megfigyelhető a definíció munkaterület lehatárolása helyett részletes módszertani összefoglalást ad a tudományterületre vonatkozóan. A több mint ötven kutató által kialakított álláspont kiterjesztette a meghatározás hatókörét a tárgyalótermeken kívülre, azt az üzenetet hordozva, hogy tudományterület nem azonos a számítógépes biztonság, vagy védelem területével:

> „A Bűnügyi Informatika nem tartozik az adatvédelem szakterületéhez." [39]

---

[36] FENYVESI Csaba: A kriminalisztika mint tudományág és mint egyetemi tantárgy. In Magyar Tudomány 2003/2 online 2003. Magyar Tudományos Akadémia, Online: http://epa.oszk.hu/ 00700/00775/ 00051/2003_02_04.html, hozzáférés: 2013.03.30

[37] Российский Федеральный Центр Судебной Экспертизы при Министерстве юстиции Российской Федерации - Компьютерно-техническая экспертиза. online: http://www. sudexpert.ru/possib/comp.php, hozzáférés: 2016. január 10.

[38] PALMER, Gary et al.: A Road Map for Digital Forensic Research. First Digital Forensic Research Workshop. Utica, NY, USA, 2001. p. 16.

[39] PALMER et. al. im. p. 16.

4.2 A Digital Forensic Science hatóköre

A meghatározásokat összeállító munkacsoport felvázolta azokat a kereteket (egy lineáris folyamatként), melyek bűnügyi informatikai munkafolyamatok főbb elemeit tartalmazták, azzal a megjegyzéssel, hogy az egyes tartalmi elemek hierarchia viszonyai (kategória/alkategória) még változhatnak:

3. táblázat - A bűnügyi informatika vizsgálati eljárásai[40]

Azonosítás Identification	**Megőrzés** Preservation	**Összegyűjtés** Collection	**Vizsgálat** Examination	**Elemzés** Analysis	**Bemutatás** Presentation	**Döntés** Decision
Az eset észlelése [Event/Crime Detection]	Ügykezelés [Case Management]	Megőrzés Preservation	Megőrzés Preservation	Megőrzés Preservation	Iratok Documentation	
Ügy indítás [Resolve Signature]	Képalkotó eljárások [Imaging Technologies]	Jóváhagyott eljárások Approved Methods	Nyomon követhetőség Traceability	Nyomon követhetőség Traceability	Szakértői vélemény Expert Testimony	
Típus azonosítás [Profile Detection]	Felügyeleti lánc [Chain of Custody]	Jóváhagyott szoftverek Approved Software	Megbízhatóság ellenőrzési technikák Validation Techniques	Statisztikai Statistical	Körülmények tisztázása Clarification	
Rendellenesség érzékelése Anomalous Detection	Időszinkron [Time Synch.]	Jóváhagyott hardverek Approved Hardware	Szűrési technikák Filtering Techniques	Protocols	Hatástanulmány Mission Impact Statement	
Panaszkezelés Complaints		Jogi felhatalmazás Legal Authority	Mintázat keresés Pattern Matching	Adatbányászat Data Mining	Ajánlott ellenintézkedés Recommended Countermeasure	
Rendszer felügyelet System Monitoring		Veszteségmentes tömörítés Lossless Compression	Rejtett adatok felkutatása Hidden Data Discovery	Időbeli összefüggések Timeline	Statisztikai értelmezés Statistical Interpretation	
Tényelemzés Audit Analysis		Mintavételezés Sampling	Rejtett adatok kinyerése Hidden Data Extraction	Összefüggések, Kapcsolatok Link		
Egyéb Etc.		Adat egyszerűsítés Data Reduction		Térbeli összefüggések Spacial		
		Helyreállítási technikák Recovery Techniques				

[40] PALMER et. al. im. p. 17. Table 2.

A munkafolyamat egyes elkülönített szakaszai és azok részfolyamatai a gyakorlatban – bemutatott lineáris szerkezettől eltérően – több szálon párhozamosan is megvalósíthatók (részletesen lád később), ugyanakkor a sorfolytonos szerkezet a bűnügyi informatika módszertani leírásának gerinceként is funkcionálhat, alapot adva az igazságügyi informatikai szakértői módszertani levél (lásd előbb: 28. jegyzet, p.23) kidolgozásához.

A konferencia eredményeként létrejött egy szakmai műhely és fórum, mely a terület kutatói és a gyakorlati szakemberi együttműködése révén tudásbázist[41] és fórumot is teremtett[42].

4.3 A Digital Forensic Science alkalmazási területei

Amint az előzőekben bemutatott definícióból és az elnevezésekből is kitűnik, a bűnügyi informatika megközelíthető, mint a jogtudomány segédtudománya, mely a bizonyítékok hiteles összegyűjtését, azok elemzését és bemutatását végzi. A felsorolt három mozzanat mindegyike több tudományterület együttműködését, eredményeinek párhuzamos használatát igényli. Míg a bizonyítékok összegyűjtése és elemzése informatikai alapú, jogtudomány által támasztott követelményeket is figyelembe vevő művelet, addig az eredmények bemutatása elsősorban kommunikációtudományi megközelítést igényel az informatikai és jogi követelmények szem előtt tartása mellett.

Mindezeket a tevékenységeket a magyarországi gyakorlatban az igazságügyi szakértő végzi a korábban már idézett Szaktv.2005 / Szaktv.2016 felhatalmazása alapján. Csaknem azonos szavakkal fogalmaz az Amerikai Egyesült Államok igazságügyi szakértőkre (expert witness) vonatkozó, az igazságügyi szakértő vallomása című szabályozása:

„A tanú, aki szakértői minősítéssel, tudással, készséggel, tapasztalattal, jártassággal vagy végzettséggel rendelkezik, tanúskodhat szakértői vélemény formájában vagy egyéb módon, ha

a. a szakértőnek tudományos, technikai vagy egyéb speciális tudása segíti a ténymegállapítást a bizonyítékok megismerése, vagy a tények megértése révén, vagy a felmerült tény meghatározása által;
b. a vallomásnak elegendő tényen, vagy adaton kell alapulnia;
c. a vallomás, mint megbízható alapelvek és módszerek eredménye és
d. a szakértő ezeket megbízható módon használja fel a tényállás megállapításához.” [43]

[41] Lásd a DFRWS archívumát: http://www.dfrws.org/archives.shtml

[42] A szervezet éves konferenciái 2014 évtől az Egyesült Államokon kívül már az Európai Unióban is megrendezésre kerülnek (2014 Amsterdam, 2015 Dublin, 2016 Lausanne)

[43] Federal Rules of Evidence Rule 702. online: https://www.law.cornell.edu/rules/fre/rule_ 702, hozzáférés: 2016 január 10.

Az előzményekből következik, hogy az igazságügyi informatikai szakértő – mint a Digital Forensic Science gyakorlati alkalmazója – részéről nélkülözhetetlen a valódi multidiszciplináris / interdiszciplináris gondolkodás, melyben saját tapasztalatain kívül segíthetik a szakterületi felosztás rendszere, a módszertani és eljárási szabványok és a jó gyakorlatok rögzítése egyaránt.

4.4 A Digital Forensic Science szakterületi felosztása Magyarországon

A szakértő elsődleges tájékozódási pontja a szakterületek elkülönítése, annak rögzítése, hogy mely szakkérdésekben nyilatkozhat érvényesen. Ezt a kérdést a jogszabályi környezet határozza meg, mely a magyarországi gyakorlatban a tételes felsorolás módszerével élve a korábbiakban már idézett 9/2006. (II. 27.) IM rendelet 6. sz. mellékletében a következő szakterületeket különíti el:

1. informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver)
2. informatikai biztonság
3. informatikai rendszerek tervezése, szervezése
4. stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység
5. számítástechnikai adatbázis, adatstruktúrák
6. szoftverek

Megfigyelhető, hogy a felsorolás különböző típusú tartalmakat határoz meg vizsgálati célobjektumként, melyek között helyenként átfedések is tapasztalhatók (pl. szoftver és számítástechnikai adatbázis, informatikai berendezések és stúdiótechnika). Egyes vizsgálandó tartalmak, területek hiányoznak a felsorolásból: okostelefonok (Smart Phone), felhőalkalmazások (Cloud Computing) és így tovább. A taxatív felsorolás – jellegéből adódóan – sohasem tartalmazhatja teljes körűen a vizsgálat alá vonható szakterületeket, ami a szakértői vizsgálatok érvényességét is megkérdőjelezheti (pl. kompetencia túllépés).

Hasonló problémával találkozhatunk az általános szakterület-kijelölés esetén, amikor a technológiai szempont kerül előtérbe a hagyományos hardver és szoftver vizsgálati terület felosztás alapján[44]. Az eszközök és programok többrétegű osztályozása nem tér ki az irányelvek és tevékenységek vizsgálatára, így az előző példához hasonlóan a vizsgálandó tartalom egy része kívül marad a szakértő hatáskörén, vagy az illetékességi hatáskörök tisztázatlansága okán az eljárásokban támadhatóvá válik a szakértői vélemény. A szakterületi felosztásnál is megfigyelhető az egységes irányelv hiánya. Míg a Large Scale Digital Devices (nagy léptékű eszközök) és Small Scale Digital Devices (kis léptékű eszközök) kategóriánál a méret jellemzőt veszi alapul a felosztás

[44] BRINSON et al., 2006. p.38.

szerzője, addig a további kategóriáknál a funkcionalitás – Computers (számítógépek), Storage Devices (tároló eszközök) – vagy éppen a besorolhatatlanság – Obscure Devices (bizonytalan besorolású eszközök) – lesz az osztályozás alapja.

Belátható az előzőek alapján, hogy taxatív felsorolás és az általános kategóriákban történő szakterület kijelölés egyaránt felvet érvényességi problémákat.

4.5 A Digital Forensic Science kriminalisztikai megközelítése

Amennyiben a számítógépes bűnözést kriminalisztikai oldalról vizsgáljuk, úgy elsődlegesen három jelentős terület elkülönítését tehetjük meg:

1. **Számítógép központú bűnözés (computer centred crime)**
   A típus jellemzője, hogy célpontként a számítógépes rendszer, hálózat, adattároló, vagy egyéb eszköz jelenik meg (pl. kereskedelmi weboldal tartalmának módosítása). Ez tekinthető egy új bűncselekmény típusnak is, mely új eszközrendszert használ (ti. a számítógépet).
2. **Számítógéppel segített bűnözés (computer assisted crime)**
   Ebben az esetben a számítógépet, mint eszközt használja az elkövető a cselekmény során, mely „segíti" a tevékenységét, de nem feltétlenül szükséges hozzá (pl. gyermekpornográfia). Itt hagyományos bűncselekményekről beszélhetünk, új módszerek alkalmazása mellett.
3. **Járulékos számítógépes bűnözés (incidental computer crime)**
   Itt a számítógépes rendszer a bűncselekmény szempontjából mellékes a bűncselekmény szempontjából, lényegében egy hagyományos eszköz kiváltását jelenti (pl. könyvelés számítógéppel, papír alapú dokumentáció helyett).[45]

A bemutatott felosztás nem a megvizsgálandó eszközök jellemzői alapján különíti el a vizsgálat tárgyát, hanem a bűncselekményben betöltött szerepe szerint.

Ez a megközelítés lehetővé teszi az egyes területek közötti megoszlás vizsgálatát az esetszámok alapján, a cselekménytípusoknál alkalmazandó eljárások, módszertanok jellemzőinek megkülönböztetését, illetve az elkövetési értékek és a cselekményszám alapján a veszélyesség mértékének megállapítását is.

E körülmények szakszerű megállapításához természetesen egy reprezentatív mintán alapuló, országos területi kiterjedésű vizsgálat szolgáltathatna alapanyagot, melynek forrása az igazságügyi informatikai szakértő ügynyilvántartása, a nyomozó hatóságok által rögzített bűnügyi adatok, illetve a bíróságokon meghozott ítéletek statisztikai összesítő adatbázisa lehetne.

---

[45] HUEBNER, Ewa –BEM, Derek – BEM, Oscar: 'Computer Forensics – Past, Present And Future' Sydney 2007. University of Western Sydney, online: http://www.securimetric.org/library /software/ Computer_ Forensics _Past_ Present_Future.pdf, p.3., hozzáférés: 2013.03.16

Jelen tanulmány – erőforrások hiányában – csak arra vállalkozhat, hogy szakértői nézőpontból nyújtson egy nem országos lefedettségű, nem reprezentatív mintán alapuló képet, mely várhatóan az egyes felosztási területek közötti arányok megállapítására alkalmas lesz.

5 Empirikus kutatás – a szakterületi felosztás validálása

5.1 A kutatás forrásadatai

A kriminalisztikai alapú szakterületi felosztás megfelelőségét vizsgáló kutatás forrása a szakértői ügynyilvántartás volt, mely jogszabályban előírt adatok[46] mellett (lásd arab számmal jelölve) a statisztikai feldolgozást elősegítő további adatok (lásd kisbetűvel jelölve) is szerepeltek:

Ügynyilvántartás kötelező adatai

1. Társszakértő neve
2. Társszakértő ügyszáma
3. Kirendelő szerv vagy megbízó megnevezése
4. Kirendelésről szóló határozat vagy megbízás ügyszáma
5. Kirendelés tárgya
6. Az ügy érkezésének időpontja
7. Az ügy érkezésének módja
8. Szakvélemény elküldésének időpontja
9. Szakvélemény elküldésének módja
10. Szakértői díj összege
11. Szakértői díj megfizetésének időpontja
12. Irattárba helyezés időpontja

Ügynyilvántartás kiegészítő adatai

a. Előadó
b. Jogszabály hely szakasz
c. Jogszabály hely - minősítés
d. Jogszabály hely szakasz - megnevezés
e. Jogszabály hely - minősítés - megnevezés
f. Cselekmény típusa (bűntett/vétség)
g. Gyanúsított
h. Eset típusa [büntető, polgári, közigazgatási, hatósági, magán]
i. Ügy(szak) típusa [nyomozati, bírói, közjegyző, közigazgatási, hatósági, magán]

[46] Szaktv.[2005] 3. sz. melléklet

j. Eszköz / dolog
k. Vizsgálat iránya

Az ügynyilvántartás tartalmi elemeinek köre a Szaktv.[2016]-ban a következőkre változott:

1. az ügy száma, együttes vagy egyesített szakvélemény esetén a társszakértő megnevezésével és ügyszámával együtt,

2. a kirendelő szerv vagy megbízó megnevezése,

3. a kirendelésről szóló határozat vagy megbízás ügyszáma és tárgya,

4. az ügy érkezésének időpontja (év, hónap, nap megjelölésével) és módja,

5. társaság, igazságügyi szakértői intézmény vagy igazságügyi szakértői testület kirendelése esetén a szakvélemény adására kijelölt igazságügyi szakértő vagy eseti bizottság tagjainak neve,

6. az ügyben részt vevő szakértőjelölt neve,

7. a kirendelés elfogadása esetén:

7.1. a letétbe helyezett szakértői díj összege,

7.2. a szakértői díj megállapításának módja,

7.3. a szakvélemény kirendelő szerv vagy megbízó részére történő elküldésének időpontja (év, hónap, nap megjelölésével) és módja,

7.4. a jogerős díjmegállapító határozatban megjelölt szakértői díj összege és megfizetésének időpontja,

8. kiegészítő adatkérés esetén:

8.1. a kiegészítő adatkérés időpontja,

8.2. a kiegészítő adatok megküldésének időpontja,

9. a kirendelés alóli felmentés vagy kizárás esetén:

9.1. annak indoka,

9.2. a felmentésről vagy kizárásról szóló határozat érkezésének időpontja (év, hónap, nap megjelölésével),

10. a kirendelő szervtől vagy megbízótól kapott iratok visszaküldésének időpontja,

11. az irattárba helyezés időpontja.[47]

[47] Szaktv.2016 2. sz. melléklet

Amint az jól látható az alapadatok tekintetében bővülés figyelhető meg: a szakértői gazdasági társaság, szakértői intézmény vagy eseti bizottság esetén a kijelölt szakértő neve vonatkozásában, az ügyben részt vevő szakértőjelölt neve vonatkozásában, illetve a kiegészítő adatkérés, a kizárás és felmentés, valamint az iratok visszaküldésének tekintetében.

Ez a bővített adatkör a kriminalisztikai osztályozás megvalósítására nem volt hatással, tekintettel az előíró jogszabály hatályba lépésére.

5.2 Kriminalisztikai osztályozás

Az empirikus kutatás megválaszolandó kérdése: a kriminalisztikai osztályozás önmagában alkalmas-e a szakterületek kiegyensúlyozott szétválasztására? A kutató előzetes feltételezése szerint a kriminalisztikai megközelítésben a járulékos számítógépes bűnözés döntő súlyt képvisel, mely a felosztás önálló használatát kérdésessé teszi.

A szakértői nyilvántartás a vizsgálat adatainak összesítésekor 348 ügyet tartalmazott. A h.) mezőben rögzített eset típus alapján 292 ügy bizonyult büntető ügynek (az összes ügy 83,9%-a).

Az igazságügyi informatikai szakértő igénybevétele a büntetőeljárás egyes szakaszaiban a következő volt

Nyomozási szakasz	269 eset	92,0%
Vádemelési szakasz	0 eset	0 %
Bírósági szakasz	23 eset	7,9%

Az adatokból megállapítható, hogy az igazságügyi informatikai szakértői vizsgálat döntően a büntetőeljárás nyomozási szakaszára összpontosul és csupán néhány esetben, kiegészítő bizonyítékok beszerzése, vagy egy-egy szakkérdés vizsgálata marad a bírósági szakaszra.

A részletes elemzéshez a szakértői ügynyilvántartásban szereplő nyers adatokat a kirendelő szervezet szerinti csoportokba soroltam. Az egyes csoportokba a szervezettípus és a szervezeti hierarchiában elfoglalt hely alapján kerültek a szervezeti egységek.

4. táblázat - Szerveztek közötti ügymegoszlás a nyomozási szakaszban

Szervezet	Darabszám	Arány
RENDŐRSÉG	88	32,7%
NEMZETI ADÓ- ÉS VÁMHIVATAL	181	67,3%
ÖSSZESEN	**269**	

5.2.1 Nyomozási szakasz adatsorai és értékelésük

A nyomozási szakaszban összesen kilenc szervezeti kódot alakítottam ki, melyekben a Rendőrség és Nemzeti Adó-és Vámhivatal (korábban Vám- és Pénzügyőrség) szervezeti egységei szerepelnek területi és hierarchia szerinti bontásban:

5. táblázat - Szervezeti kódok

Szervezeti kód	A csoport jellemzője
BRFK_KERÜLET	Budapesti Rendőr-főkapitányság Kerületi Rendőrkapitányságai
BRFK_KGBEF	Budapesti Rendőr-főkapitányság Korrupciós és Gazdasági Bűnözés Elleni Főosztálya
MEGYE_RFK	Megyei Rendőr-főkapitányságok
NAV_DdRBI	Nemzeti Adó- és Vámhivatal Dél-dunántúli Regionális Bűnügyi Igazgatósága (korábban: Vám- és Pénzügyőrség Dél-dunántúli Regionális Nyomozó Hivatala)
NAV_KmRBI	Nemzeti Adó- és Vámhivatal Közép-magyarországi Regionális Bűnügyi Igazgatósága (korábban: Vám- és Pénzügyőrség Közép-magyarországi Regionális Nyomozó Hivatala)
NAV_KNyF	Nemzeti Adó- és Vámhivatal Bűnügyi Főigazgatóság Központi Nyomozó Főosztály (korábban: Vám- és Pénzügyőrség Központi Bűnüldözési Parancsnoksága)
NNI_NBEF	Készenléti Rendőrség Nemzeti Nyomozó Iroda Nemzetközi Bűnözés Elleni Főosztály
VÁROS_RK	Városi rendőrkapitányságok
VÁROS_RK_ŐRS	Városi rendőrkapitányságok rendőrőrsei

A cselekmények kirendelő szervezetenkénti megoszlásának adatait a következő táblázat tartalmazza részletesen:

6. táblázat - 14.7 Cselekménytípusok kirendelő szervezetenkénti megoszlása a nyomozási szakaszban (2007-2016) [48]

CSELEKMÉNYTÍPUSOK - NYOMOZÁSI SZAKASZ	DB	MIND/ DB	NY/DB	
BRFK_KERÜLET	**2**	**0,7%**	**0,7%**	
A vagyon elleni bűncselekmények	2			100,0%
BRFK_KGBEF	**3**	**1,0%**	**1,1%**	
A vagyon elleni bűncselekmények	1			33,3%
Pénzmosás	2			66,7%
MEGYE_RFK	**1**	**0,3%**	**0,4%**	
A vagyon elleni bűncselekmények	1			100,0%
NAV_DdRBI	**11**	**3,8%**	**4,1%**	
A költségvetést károsító bűncselekmények	5			45,5%
A szellemi tulajdonjog elleni bűncselekmények	2			18,2%
A vagyon elleni bűncselekmények	3			27,3%
Gazdálkodási kötelességeket és a gazdálkodás rendjét sértő bűncselekmények	1			9,1%
NAV_KmRBI	**20**	**6,8%**	**7,4%**	
A költségvetést károsító bűncselekmények	4			20,0%
A pénzügyi bűncselekmények	***8***			***40,0%***
A szellemi tulajdonjog elleni bűncselekmények	1			5,0%
A vagyon elleni bűncselekmények	5			25,0%
Gazdálkodási kötelességeket és a gazdálkodás rendjét sértő bűncselekmények	2			10,0%
NAV_KNyF	**150**	**51,4%**	**55,8%**	
A gazdálkodás rendjét sértő bűncselekmények	1			0,7%
A költségvetést károsító bűncselekmények	11			7,3%
A közbiztonság elleni bűncselekmények	1			0,7%
A közegészség elleni bűncselekmények	2			1,3%
A pénzügyi bűncselekmények	***120***			***80,0%***
A vagyon elleni bűncselekmények	15			10,0%
NNI_NBEF	**1**	**0,3%**	**0,4%**	
A korrupciós bűncselekmények	1			100,0%
VÁROS_RK	**76**	**26,0%**	**28,3%**	
A hivatalos személy elleni bűncselekmények	2			2,6%
A közbizalom elleni bűncselekmények	4			5,3%
A közegészség elleni bűncselekmények	12			15,8%
A köznyugalom elleni bűncselekmények	2			2,6%

[48] Forrás: Máté István Zsolt igazságügyi informatikai szakértő (007760) - szakértői ügynyilvántartás

CSELEKMÉNYTÍPUSOK - NYOMOZÁSI SZAKASZ	DB	MIND/ DB	NY/DB	
A nemi erkölcs elleni bűncselekmények	18			23,7%
A pénz- és bélyeghamisítás	1			1,3%
A szabadság és az emberi méltóság elleni bűncselekmények	6			7,9%
A vagyon elleni bűncselekmények	28			36,8%
Az egészséget veszélyeztető bűncselekmények	1			1,3%
Az élet, a testi épség és az egészség elleni bűncselekmények	1			1,3%
Gazdálkodási kötelességeket és a gazdálkodás rendjét sértő bűncselekmények	1			1,3%
VÁROS_RK_ŐRS	**5**	**1,7%**	**1,9%**	
A szabadság és az emberi méltóság elleni bűncselekmények	1			20,0%
A vagyon elleni bűncselekmények	4			80,0%

ÖSSZESEN nyomozási szakasz	**269**
MINDÖSSZESEN nyomozási és bírósági szakasz	**292**

Az összes cselekmény közül két bűncselekmény típus emelkedik ki jelentős mértékben, a pénzügyi bűncselekmények[49] (47,6% - 128 db), valamint a vagyon elleni bűncselekmények[50] (21,9% - 59 db). A további cselekménytípusok 10% alatti mértékben képviseltetik magukat:

7. táblázat - Cselekménytípusok a nyomozási szakaszban

CSELEKMÉNYTÍPUS	DB	ARÁNY
A vagyon elleni bűncselekmények	**59**	**21,9%**
Pénzmosás	2	0,7%
A költségvetést károsító bűncselekmények	**20**	**7,4%**
A szellemi tulajdonjog elleni bűncselekmények	3	1,1%
Gazdálkodási kötelességeket és a gazdálkodás rendjét sértő bűncselekmények	**4**	**1,5%**
A pénzügyi bűncselekmények	128	47,6%
A gazdálkodás rendjét sértő bűncselekmények	1	0,4%

[49] az 1978. évi IV. törvény szerint szerinti besorolás

[50] az 1978. évi IV. törvény szerint szerinti besorolás

CSELEKMÉNYTÍPUS	DB	ARÁNY
A közbiztonság elleni bűncselekmények	1	0,4%
A közegészség elleni bűncselekmények	14	5,2%
A korrupciós bűncselekmények	1	0,4%
A hivatalos személy elleni bűncselekmények	2	0,7%
A közbizalom elleni bűncselekmények	4	1,5%
A köznyugalom elleni bűncselekmények	2	0,7%
A nemi erkölcs elleni bűncselekmények	18	6,7%
A pénz- és bélyeghamisítás	1	0,4%
A szabadság és az emberi méltóság elleni bűncselekmények	7	2,6%
Az egészséget veszélyeztető bűncselekmények	1	0,4%
Az élet, a testi épség és az egészség elleni bűncselekmények	1	0,4%
ÖSSZESEN	**269**	

A pénzügyi bűncselekmények 100%-át a hatáskörből adódóan a Nemzeti Adó- és Vámhivatal bűnügyi szakterületéhez tartozó országos és területi szervei nyomozták. A vagyon elleni bűncselekmények esetén a Rendőrség különböző szervezeti egységei az ügyek 61%-át, míg a Nemzeti Adó- és Vámhivatal bűnügyi szervezeti egységei az ügyek 39%-át nyomozták.

Mivel a vizsgált időszakban került sor a Büntető Törvénykönyv módosítására, így a vizsgálat kitér a két jogszabály különbségein alapuló összevetésre is:

8. táblázat - 1978. évi IV. törvény szerinti besorolású ügytípusok a nyomozási szakaszban

NYOMOZÁSI SZAKASZ	DB	MIND/DB	ÖSSZ/DB	ARÁNY
A hivatalos személy elleni bűncselekmények	**2**	0,7%	0,9%	
hivatalos személy elleni erőszak	1			50,0%
személy elleni erőszak	1			50,0%
A közbizalom elleni bűncselekmények	**4**	1,7%	1,7%	
közokirat hamisítás	1			25,0%
magánokirat-hamisítás	3			75,0%
A közbiztonság elleni bűncselekmények	**1**	0,4%	0,4%	
visszaélés haditechnikai termékkel és szolgáltatással illetőleg kettős felhasználású termékkel	1			100,0%
A közegészség elleni bűncselekmények	**14**	6,0%	6,0%	
kábítószerrel visszaélés	10			71,4%
visszaélés kábítószerrel	4			28,6%

NYOMOZÁSI SZAKASZ	DB	MIND/DB	ÖSSZ/DB	ARÁNY
A köznyugalom elleni bűncselekmények	**2**	0,9%	0,9%	
garázdaság	1			50,0%
önbíráskodás	1			50,0%
A nemi erkölcs elleni bűncselekmények	**18**	7,7%	7,7%	
erőszakos közösülés	1			5,6%
megrontás	1			5,6%
pornográf felvétellel visszaélés	1			5,6%
szemérem elleni erőszak	2			11,1%
szeméremsértés	1			5,6%
tiltott pornográf felvétellel visszaélés	12			66,7%
A pénz- és bélyeghamisítás	**1**	0,4%	0,4%	
pénzhamisítás	1			100,0%
A pénzügyi bűncselekmények	**128**	54,7%	54,7%	
adócsalás	113			
adócsalás, pénzmosás, közokirat hamisítás	1			
csempészet	5			
költségvetési csalás	7			
nemzetközi jogsegély (adócsalás)	1			
visszaélés jövedékkel	1			
A szabadság és az emberi méltóság elleni bűncselekmények	**7**	3,0%	3,0%	
adattal visszaélés	2			
kényszerítés	2			
magántitok jogosulatlan megsértése	1			
zaklatás	2			
A vagyon elleni bűncselekmények	**52**	22,2%	22,2%	
csalás	17			32,7%
hűtlen kezelés	3			5,8%
lopás	4			7,7%
orgazdaság	1			1,9%
rablás	1			1,9%
rongálás	1			1,9%
sikkasztás	4			7,7%
szerzői joghoz kapcsolódó jogok megsértése	1			1,9%
szerzői vagy szerzői joghoz kapcsolódó jogok megsértése	9			17,3%
szerzői vagy szerzői joghoz kapcsolódó jogok megsértése, szerzői vagy szerzői joghoz kapcsolódó jogok védelmét biztosító műszaki intézkedés kijátszás	1			1,9%

NYOMOZÁSI SZAKASZ	DB	MIND/DB	ÖSSZ/DB	ARÁNY
szerzői vagy szerzői joghoz kapcsolódó jogok megsértése, szerzői, vagy szerzői jogokhoz kapcsolódó jogok védelmet biztosító műszaki intézkedés kijátszása	1			1,9%
szerzői vagy szerzői joghoz kapcsolódó jogok megsértése; szerzői vagy szerzői jogokhoz kapcsolódó jogok védelmét biztosító műszaki intézkedés kijátszása	1			1,9%
szerzői vagy szerzői joghoz kapcsolódó jogok védelmét biztosító műszaki intézkedés kijátszása	8			15,4%
Az élet, a testi épség és az egészség elleni bűncselekmények	**1**	0,4%	0,4%	
súlyos testi sértés	1			100,0%
Gazdálkodási kötelességeket és a gazdálkodás rendjét sértő bűncselekmények	**4**	1,7%	1,7%	
csődbűncselekmény	2			50,0%
számítástechnikai rendszer és adatok elleni bűntett	1			25,0%
számvitel rendjének megsértése szerzői joghoz kapcsolódó jogok megsértése	1			25,0%
ÖSSZESEN	**234**			
MINDÖSSZESEN	**269**			

9. táblázat - 2012. évi C. törvény szerinti besorolású ügytípusok a nyomozási szakaszban

	DB	MIND/DB	ÖSSZ/DB	ARÁNY
A gazdálkodás rendjét sértő bűncselekmények	**1**	0,4%	2,9%	
csődbűncselekmény	1			100,0%
A korrupciós bűncselekmények	**1**	0,4%	2,9%	
befolyással üzérkedés	1			100,0%
A költségvetést károsító bűncselekmények	**20**	7,4%	57,1%	
költségvetési csalás	20			100,0%
A szellemi tulajdonjog elleni bűncselekmények	**3**	1,1%	8,6%	
szerzői vagy szerzői joghoz kapcsolódó jogok megsértése	2			66,7%
szerzői, vagy szerzői joghoz kapcsolódó jogok megsértése	1			33,3%
A vagyon elleni bűncselekmények	**7**	2,6%	20,0%	

	DB	MIND/DB	ÖSSZ/DB	ARÁNY
csalás	4			57,1%
orgazdaság	3			42,9%
Az egészséget veszélyeztető bűncselekmények	**1**	0,4%	2,9%	
kábítószer-kereskedelem	1			100,0%
Pénzmosás	**2**	0,7%	5,7%	
pénzmosás	2			100,0%
ÖSSZESEN	**35**			
MINDÖSSZESEN	**269**			

Az adatokból jól látható, hogy mindkét esetben a gazdasági, illetve a vagyon elleni bűncselekmények teszik ki az esetek túlnyomó többségét.

Nem csupán a két vezető ügytípus, de a teljes statisztikai kép azt mutatja, hogy a szakértői támogatást igénylő ügyek csaknem száz százaléka a járulékos számítógépes bűnözés kategóriájába esik, mely csoport esetén a számítógépes rendszer a definíció szerint „lényegében egy hagyományos eszköz kiváltását jelenti".

Számítógép központú bűnözéssel (computer centred crime) kapcsolatba hozható eset, mindössze egy volt a 269 ügy között (számítástechnikai rendszer és adatok elleni bűntett), míg a számítógéppel segített bűnözés (computer assisted crime) csoportjába sorolható esetek közé sorolható 37 ügy, melyek többsége a szerzői, vagy szerzői jogokhoz kapcsolódó jogok megsértésére vonatkozott (24), illetve pornográf felvétellel visszaélés bűntettével volt kapcsolatos (13).

5.2.2 Bírósági szakasz adatsorai és értékelésük

A bírósági szakaszra vonatkozóan mindössze két szervezeti kódot alakítottam ki, melyekben a bírósági hierarchia szintek jelentek meg a következők szerint:

10. táblázat - Szervezeti kódokhoz tartozó kirendelő szervezetek a bírósági szakaszban

Szervezeti kód	A csoport jellemzője
TÖRVÉNYSZÉK	Törvényszékek (korábban Megyei Bíróságok)
JÁRÁSBÍRÓSÁG	Járásbíróságok és Budapesti Kerületi Bíróságok (korábban Városi Bíróságok)

A bírósági szakaszban lezajlott igazságügyi informatikai szakértői közreműködés az előzőhöz képest jelentősen alacsonyabb ügyszámot képvisel az összesen 23 esettel.

A cselekmények kirendelő szervezetenkénti megoszlásának adatait a következő táblázat tartalmazza részletesen:

11. táblázat - Cselekménytípusok kirendelő szervezetenkénti megoszlása a bírósági szakaszban[51]

CSELEKMÉNYTÍPUSOK - BÍRÓSÁGI SZAKASZ	DB	MIND/DB	B/DB
JÁRÁSBÍRÓSÁG	**17**	**5,8%**	
A közbiztonság elleni bűncselekmények	1		5,9%
A köznyugalom elleni bűncselekmények	1		5,9%
A nemi erkölcs elleni bűncselekmények	1		5,9%
A szabadság és az emberi méltóság elleni bűncselekmények	4		23,5%
A vagyon elleni bűncselekmények	7		41,2%
A vagyon elleni erőszakos bűncselekmények	1		5,9%
Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények	1		5,9%
Gazdálkodási kötelességeket és a gazdálkodás rendjét sértő bűncselekmények	1		5,9%
TÖRVÉNYSZÉK	**6**	**2,1%**	
A pénzügyi bűncselekmények	1		16,7%
A vagyon elleni bűncselekmények	3		50,0%
Az élet, a testi épség és az egészség elleni bűncselekmények	1		16,7%
Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények	1		16,7%
ÖSSZESEN bírósági szakasz	**23**		
MINDÖSSZESEN nyomozási és bírósági szakasz	**292**		

Az egyes csoportokba és a konkrét jogszabályhelyhez kapcsolódó adatok kis száma miatt ez az adatsor nem értékelhető:

12. táblázat - 1978. évi IV. törvény szerinti besorolású ügytípusok a bírósági szakaszban

BÍRÓSÁGI SZAKASZ	DB	MIND/DB	ÖSSZ/DB	ARÁNY
A nemi erkölcs elleni bűncselekmények	**1**	4,3%	6,7%	
tiltott pornográf felvétellel visszaélés	1			100,0%
A pénzügyi bűncselekmények	**1**	4,3%	6,7%	
adócsalás	1			100,0%
A szabadság és az emberi méltóság elleni bűncselekmények	**4**	17,4%	26,7%	
kényszerítés	1			25,0%
rágalmazás	1			25,0%

[51] Forrás: Máté István Zsolt igazságügyi informatikai szakértő (007760) - szakértői ügynyilvántartás

BÍRÓSÁGI SZAKASZ	DB	MIND/DB	ÖSSZ/DB	ARÁNY
személyes adattal visszaélés	2			50,0%
A vagyon elleni bűncselekmények	**7**	30,4%	46,7%	
lopás	1			14,3%
rablás	2			28,6%
sikkasztás	1			14,3%
szerzői joghoz kapcsolódó jogok megsértése	1			14,3%
szerzői vagy szerzői joghoz kapcsolódó jogok védelmét biztosító műszaki intézkedés kijátszása	2			28,6%
Az élet, a testi épség és az egészség elleni bűncselekmények	**1**	4,3%	6,7%	
emberölés	1			100,0%
Gazdálkodási kötelességeket és a gazdálkodás rendjét sértő bűncselekmények	**1**	4,3%	6,7%	
számítástechnikai rendszer és adatok elleni bűntett	1			100,0%
ÖSSZESEN	**15**			
MINDÖSSZESEN	**23**			

13. táblázat - 2012. évi C. törvény szerinti besorolású ügytípusok a bírósági szakaszban

BÍRÓSÁGI SZAKASZ	DB	MIND/DB	ÖSSZ/DB	ARÁNY
A közbiztonság elleni bűncselekmények	**1**	4,3%	14,3%	
hűtlen kezelés	1			100,0%
A vagyon elleni bűncselekmények	**3**	13,0%	42,9%	
csalás	1			33,3%
információs rendszer felhasználásával elkövetett csalás	1			33,3%
sikkasztás	1			33,3%
A vagyon elleni erőszakos bűncselekmények	**1**	4,3%	14,3%	
önbíráskodás	1			100,0%
Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények	**2**	8,7%	28,6%	
becsületsértés	1			50,0%
rágalmazás	1			50,0%
ÖSSZESEN	**7**			
MINDÖSSZESEN	**23**			

Mindenesetre itt is megfigyelhető a járulékos számítógépes bűnözés kategóriájába eső cselekmények jelentős túlsúlya.

Összefoglalva megállapítható, hogy a kriminalisztikai megközelítés szerinti elkülönítési kategóriák a Digital Forensic Science esetében a gyakorlat által nem igazolhatók, tekintettel arra, hogy az egyes kategóriák között nagyságrendinek tűnő ügyszámbeli különbségek mutatkoztak az empirikus vizsgálat során. Ugyanakkor nem szabad elfelejteni azt a tényt, mi szerint a kutatás alapanyag nem mutatott sem területi, sem kirendelő hatóság szerinti reprezentativitást sem.

A kapott eredmények megerősítése, vagy cáfolata az igazságügyi informatikai szakértők ügynyilvántartásának feldolgozásával, vagy a Szaktv.[2016] szerinti statisztikai adatszolgáltatás tartalmi elemzésével adható meg. Mivel minként esetben jelentős munkabefeketetésre lenne szükség, mely teher – adatkezelési okokból – nem vehető le az adott szakértő válláról, az eredmények validálására más forrást kell majd keresni a jövőben.

5.3 Empirikus adatok kritikai értékelése

Amint arra már több ízben történt utalás, a kutatás alapadatai sem területi, sem kirendelő szervezet szerint nem reprezentatívak. E szempontot egészíti ki a kutatás lezárását követően keletkezett adatsor, mely a Magyar Igazságügyi Szakértői Kamarához –

a 13/2016. IM rendelet[52] 4. § alapján – beérkezett befizetéseket mutatja. Ezek közül kiemelkedik a Nemzeti Szakértői és Kutató Központ (mely Bűnügyi Szakértői és Kutató Intézet és az Igazságügyi Szakértői és Kutató Intézetek összevonásával jött létre 2017 januárjában) befizetése, mely 2017 első negyedévében kevéssel több, mint 9 millió forintot tett ki. A 9 000 ügynél valamivel nagyobb esetszámból, valamint a kirendelők megoszlásából világossá vált, hogy a Rendőrség jelentősen nagyobb volument képvisel az informatikai vonatkozású büntetőügyek nyomozási szakaszában, mint az a kutatás adataiból következett.

5.4 Technológiai osztályozás adatsorai és értékelésük

A kriminalisztikai megközelítés vizsgálata mellett a hagyományos technológiai alapú osztályozás gyakorlati ellenőrzésére is szükség van, tekintettel arra, hogy a hatályos szakterületi felosztás részben ezen a szisztémán alapul.

A kutató előzetes feltételezése szerint a technológiai megközelítés a kriminalisztikaihoz hasonló jelentős egyenlőtlenségeket fog mutatni az egyes vizsgálati tárgyak között, mely megkérdőjelezi az osztályozási rendszer önálló alkalmazhatóságát.

A feldolgozott és elemzett adatok forrása azonos a kriminalisztikai szempontú vizsgálati rész forrásaival, így azok egyenként és összességükben is elemezhetők. A vizsgálathoz az érintett ügyekben készített igazságügyi informatikai szakértői véleményekből – a vizsgálat tárgya rész adatait felhasználva – kigyűjtöttem az egyes ügyekben vizsgált eszközöket oly módon, hogy azokat az alábbiakban bemutatott osztályokba soroltam be.

14. táblázat - Besorolási osztályok a technológiai alapú empirikus vizsgálatnál

1.	PC	személyi számítógép
2.	Mac	Apple asztali számítógép
3.	Szerver	kiszolgáló számítógép
4.	Laptop	hordozható számítógép
5.	MacBook	Apple hordozható számítógép
6.	Tablet	táblagép
7.	iPad	Apple táblagép
8.	HDD	merevlemez, külső egyedi adattár
9.	SAN/NAS	hálózati adattár,
10.	Flash tár	memóriakártya, pendrive
11.	Optikai lemez	CD, DVD, mini Disk
12.	Okostelefon vagy PDA	kéziszámítógép és smartphone
13.	iPhone	Apple okostelefon

[52] az igazságügyi szakértők statisztikai adatszolgáltatásáról, a kamarai költségátalány bevallásának és megfizetésének szabályairól, valamint az igazságügyi szakértő által vezetett adattovábbítási nyilvántartásról

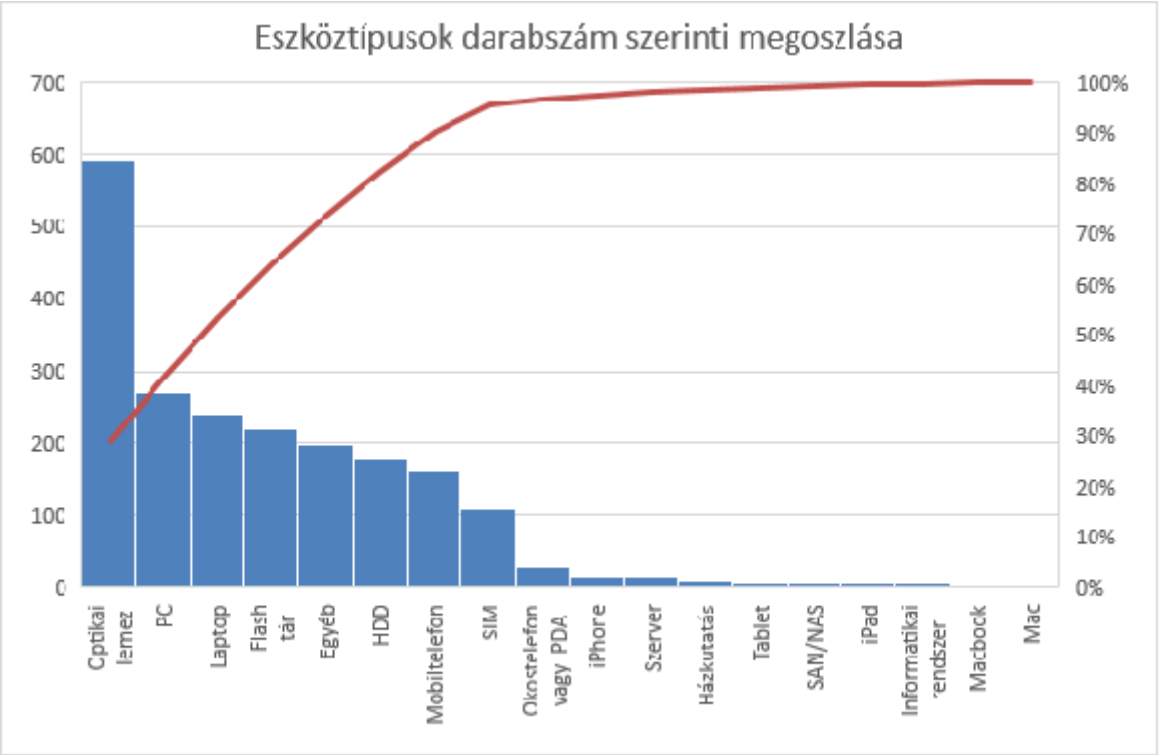
14.	Mobiltelefon	feature phone (hagyományos mobiltelefon)
15.	SIM	subscriber identity module
16.	Informatikai rendszer	számítógépes programrendszer
17.	Házkutatás	helyszíni vizsgálat
18.	Egyéb	digitális fényképezőgép, videokamera, diktafon, DVR készülék, nyomtatós etc.

A vizsgálat folytatásában ügyenként rögzítettem a vizsgált eszközöket vagy rendszereket. Az összesített adatokat a következő táblázatban mutatom be:

15. táblázat - Technológiai alapú empirikus vizsgálat nyers adatsora

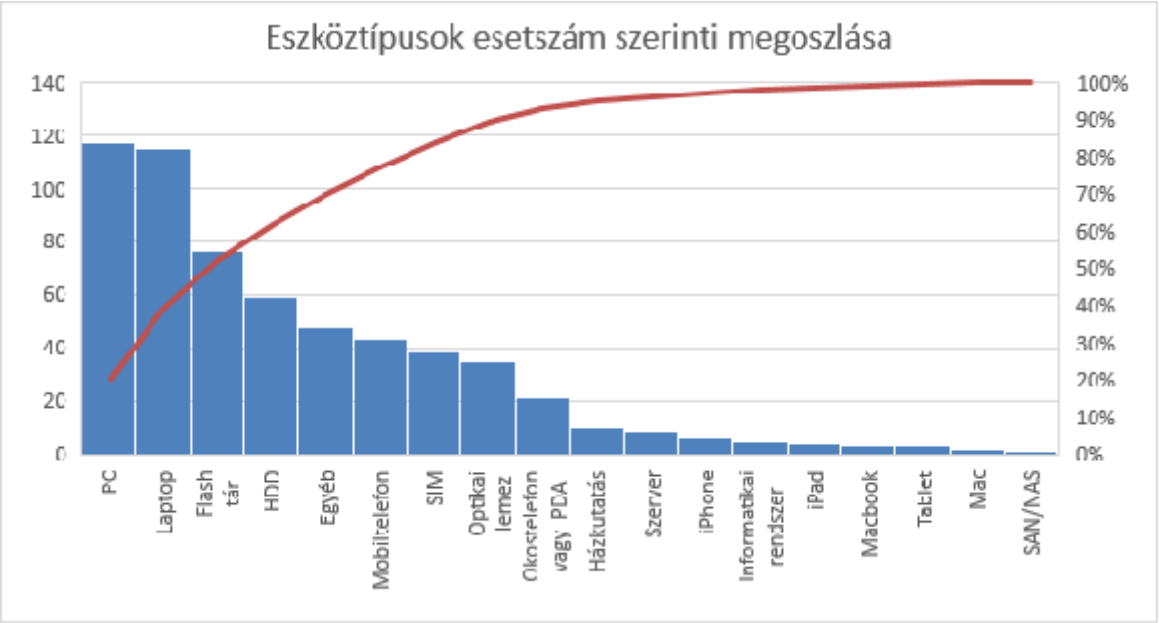
Adatosztály	Eszközök száma	Ügyek száma
PC	271	117
Mac	2	2
Szerver	14	8
Laptop	242	115
MacBook	4	3
Tablet	6	3
iPad	5	4
HDD	179	59
SAN/NAS	6	1
Flash tár	221	76
Optikai lemez	592	35
Okostelefon vagy PDA	30	21
iPhone	16	6
Mobiltelefon	161	43
SIM	108	38
Informatikai rendszer	5	5
Házkutatás	10	10
Egyéb	198	48

Az adatokból jól látszik, hogy mennyiségi megközelítésben (lásd a következő diagramot) az optikai lemezek (CD, DVD) vizsgálata a legnagyobb tömegű (összesen 592 db), melyet a személyi számítógép (271 db) és a hordozható számítógép (242 db) kategória követ.



2. ábra - Eszköztípusok darabszám szerinti megoszlása

A képet árnyalja az esetszám szerinti összesítés – lásd a következő diagramot –, ami megmutatja, hogy valójában a személyi számítógép, a hordozható számítógép, a flash tárak és a merevlemezek az ügyekben leggyakrabban szereplő eszközök.



3. ábra - Eszköztípusok esetszám szerinti megoszlása

Az optikai lemezek előtérbe kerülését a szerzői és szomszédos jogok megsértése ügytípus egy esete (226 db optikai lemez vizsgálata egyetlen ügyben) okozta, mely torzító hatást az ügyenkénti eszközmennyiség vizsgálat kiszűrt.

Az adatsorok arra utalnak, hogy a szakértő vizsgálatok a gyakorlatban adattárak tartalmi vizsgálatára vonatkoznak és csak kevéssé vagy egyáltalán nem jelenik meg ettől eltérő (pl. számítógépes rendszer elleni támadás) nézőpont.

A fentiekből egyenesen következik, hogy az alábbi táblázatban látható felosztási javaslatot a gyakorlat nem igazolja, helyette a tárolóeszközök és az egyéb eszközök kategóriák felállítása látszik indokoltnak. Árnyalva az előző megállapítást kijelenthető, hogy bármilyen technológia alapú felosztás esetén a tárolóeszközök vizsgálatának kell a legnagyobb hangsúlyt kapnia, ami megjelenthet a vizsgálati módszertan meghatározása és rögzítése formájában.

16. táblázat - Technológiai szemléletű szakterület felosztás BRINSON és szerzőtársai nyomán[53]

Software	Analysys Tool (elemző eszközök)	Proprietary Open Source	(szabadalmazott) (nyílt forráskódú)
	Operating Systems (operációs rendszerek)	Proprietary Open Source	(szabadalmazott) (nyílt forráskódú)
	File Systems (fájlrendszerek)	Windows Unix/Linux Mac	
Hardware	Large Scale Digital Devices (nagy léptékű eszközök)	Grids Clusters	(elosztott számítógéprendszerek) (számítógép fürtök)
	Small Scale Digital Devices (kis léptékű eszközök)	Cell Phones PDAs SSDD Software	(mobiltelefonok) (kéziszámítógépek / okostelefonok) (kiléptékű eszközök szoftverei)
	Computers (számítógépek)	Desktops Laptops Servers Tablets	(asztali számítógépek) (hordozható számítógépek) (kiszolgáló számítógépek) (táblaszámítógépek)
	Storage Devices (tárolóeszközök)	Thumb drive Digital Music Players External Hard Drives	(elektronikus tárak) (digitális zenelejátszók) (külső merevlemezek)
	Obscure Devices (bizonytalan besorolású eszközök)	Gaming Devices Recording Devices	(játék eszközök) (rögzítő eszközök)

Amennyiben a fenti adatokat az idő dimenziójában vizsgáljuk (lásd a következő táblázatban), egyértelmű, hogy valamennyi tároló típusú eszköz (PC, laptop, HDD, Flash

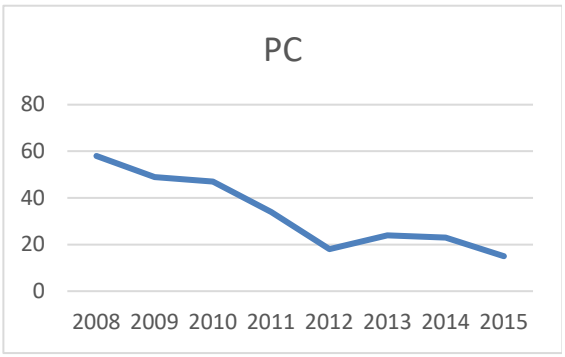
[53] BRINSON et al., 2006. p.38.

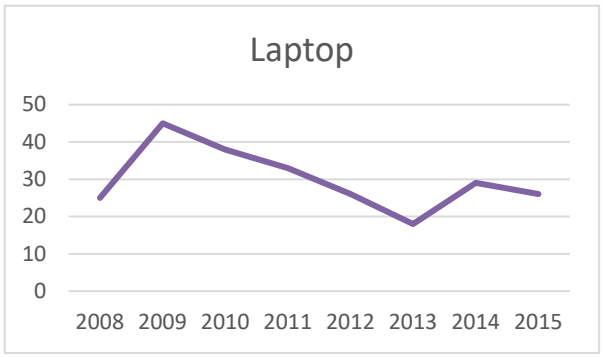
tár)) esetén mennyiségi csökkenésről beszélhetünk, ugyanakkor nem látszik pontosan az új súlypont, talán az egyéb eszköztípusok és a mobiltelefonok növekedése jelölhető meg lehetséges új irányként.

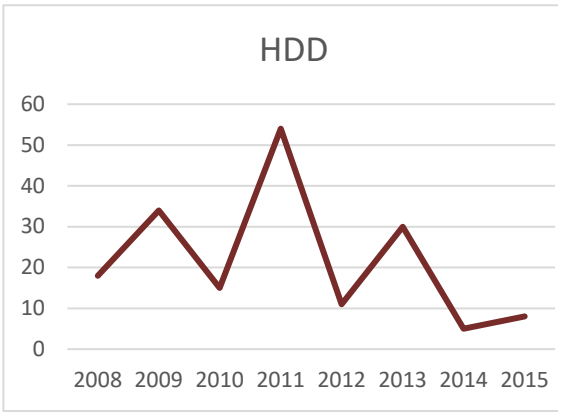
17. táblázat – Vizsgált eszköztípusok időbeli alakulása

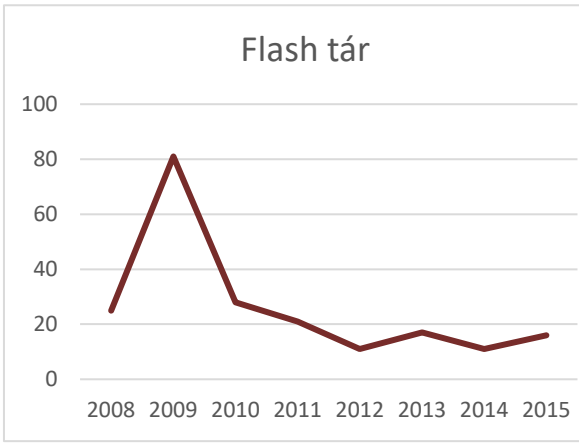
	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	Összesen
PC	0	58	49	47	34	18	24	23	15	3	271
Mac	0	0	0	0	1	0	1	0	0	0	2
Szerver	0	0	0	3	10	0	0	1	0	0	14
Laptop	0	25	45	38	33	26	18	29	26	2	242
MacBook	0	1	1	2	0	0	0	0	0	0	4
Tablet	0	1	0	0	0	0	0	0	5	0	6
iPad	0	0	0	0	0	0	2	1	0	2	5
HDD	0	18	34	15	54	11	30	5	8	4	179
SAN/NAS	0	0	0	6	0	0	0	0	0	0	6
Flash tár	0	25	81	28	21	11	17	11	16	11	221
Optikai lemez	0	61	113	344	22	20	14	10	0	8	592
Okostelefon vagy PDA	0	6	5	3	4	5	7	0	0	0	30
iPhone	0	0	2	0	0	1	3	0	10	0	16
Mobiltelefon	0	2	37	8	24	11	0	25	54	0	161
SIM	0	5	38	14	22	16	4	1	8	0	108
Informatikai rendszer	0	0	0	0	1	0	2	0	2	0	5
Házkutatás	0	0	0	3	4	0	2	0	0	1	10
Egyéb	1	3	14	30	8	32	7	94	8	1	198
Összesen	1	205	419	541	238	151	131	200	152	32	

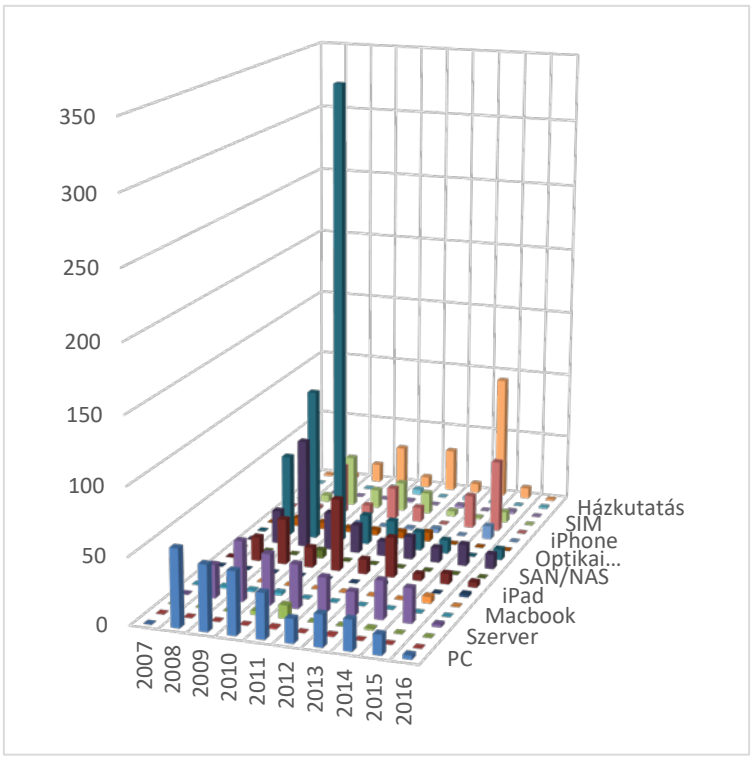
18. táblázat - Vizsgált eszköztípusok mennyiségi változásának alakulása











1. diagram - Vizsgált eszköztípusok mennyiségi változásának alakulása

A tényszerű adatok mellet figyelembe véve a szakértő személyes benyomásait, illetve a statisztikai feldolgozásba be nem került 2016 évi adatokat, elmondható, hogy az online tartalmak, felhőszolgáltatások (pl. Gmail fiókok) vizsgálata gyakorivá vált, sőt megjelentek a virtuális térben (pl. Second Life) végzett szakértői vizsgálatok is (részletesen lásd később). A kibontakozni látszó változás és annak iránya a 2016. évi szakértői vizsgálatok adatainak feldolgozását követően számszerűsíthető, igazolható vagy cáfolható.

5.5 Az empirikus kutatás eredményei

A kutatás során feltárt összefüggések szerint mind a technológiai alapú, mind a kriminalisztikai megközelítés tartalmaz egyensúlytalanságot, nevezetesen az egyes szakterületek, illetve eszköztípusok között túlsúly állapítható meg, mely kérdésessé teszi az osztályozási módszer megfelelőségét.

A képet tovább árnyalja az a tény, miszerint a kutatás nem reprezentatív mintán alapult, egy szakértő ügynyilvántartásából származnak az adatok, így az eredmény inkább csak a tendenciákra vonatkozóan szolgáltathat adatokat.

Mindezeket figyelembe véve határozottan kijelenthető, hogy kiemelt figyelmet kell fordítani a járulékos számítógépes bűnözés (incidental computer crime) irányába, vagyis azokra az esetekre kell fókuszálni, ahol mintegy mellékes szerep jut az informatika rendszernek, adott esetben, mint a digitális nyomok közegének. Ebben a közegben jelennek meg a technológiai megközelítés szerinti hardver és szoftver eszközök, melyek hordozói és egyben létrehozói is a digitális nyomnak, mely később digitális bizonyítékká válhat a büntetőeljárás folyamán. A digitális bizonyítékok változásának dinamikája indukálja az igazságügyi informatikai szakértői szakterületek rugalmas újraértelmezését, mely folyamatban helye van a komplex, interdiszciplináris / multidiszciplináris megközelítésnek is.

A jelenlegi és a közeljövőben hatályossá váló jogszabályi keretek (ti. kompetenciakörök) mellett ki kell alakítani a gyakorlat tapasztalatai alapján rugalmasan kezelhető keretet is, mely a módszertanok frissítésével, a hangsúlyok időről-időre történő áthelyezésével dinamikusan tud reagálni az egyes cselekménytípusokra, adott esetben elébe menni azoknak.

5.6 A kutatás eredményeinek kritikai megközelítése

A kutatási eredményekből egyértelműen kitűnik, hogy a magyarországi bűnügyi informatikai vizsgálatok fókuszában a különféle fizikai adattárolókról történő információ (digitális bizonyíték) kinyerése áll. Ezek a digitális bizonyítékok túlnyomó többsége a járulékos számítógépes bűnözés (incidental computer crime) körébe esik. Helyénvalónak látszik, ha ez a gyakorlat által alátámasztott tény a Digital Forensic Science vizsgálati terület meghatározásánál is megjelenne. A cél ebben az esetben nem egy újabb (adott esetben a szerző nevével fémjelzett) osztályozási forma bevezetése, hanem a bűnügyi informatikai vizsgálati profiljának megtisztítása a járulékos, esetenként önállóként is megjeleníthető területektől.

Ebben az értelemben a vizsgálat terét két nagy részre oszthatjuk fel, egyrészt a dinamikus jellegzetességeket mutató esemény központú, másrészt a statikus jellegű adat központú területre. Az esemény központú területen leginkább az azonnali beavatkozást igénylő, az eseménykezeléssel összefüggő beavatkozást értjük, míg a statikus terület egy adott cselekmény következményeinek feltárást végzi a digitális bizonyítékok megszerzése által. Jól látható, hogy a dinamikus rész az informatikai biztonság (ha jobban tetszik védelem), míg a statikus rész a tényleges bűnügyi informatika (szakértői munka) fogalmakkal írható le.

A fentiekből adódóan Digital Forensic Science alapvető vizsgálati területe a digitális bizonyítékra koncentráló igazságügyi informatikai szakértői munka, így a tudományterülettel kapcsolatos kutatásnak is elsősorban a digitális bizonyítékkal végzett szakértői tevékenységre kell koncentrálnia.

5.7 A bűnügyi informatika helye a büntetőeljárásban

Az ontológiai, osztályozási és profil tisztítási szempontok mellett a bűnügyi informatika helyének azonosítása is alapkérdés. A tudományterület a magyarországi büntetőeljárások során a nyomozási és a bírósági szakaszban egyaránt megjelenhet (amint azt az empirikus kutatás is alátámasztotta), ugyanakkor nem hagyhatjuk figyelmen kívül azt a tényt, hogy az eljárás első szakaszában jelentősen nagyobb mértékű a bűnügyi informatika és ezáltal az igazságügyi informatikai szakértők jelenléte. Míg a nyomozás során az alapvető cél a bizonyítékok azonosítása, összegyűjtése és vizsgálata, addig a bírósági szakaszban gyakran kiegészítő, újraértékelő szerep jut az informatikai szakértőnek, s csak ritkán kerül sor új tartalom vizsgálatára.

Tisztán kell látni, hogy mindkét szakaszban segédtudományként kerül alkalmazásra a bűnügyi informatika, segítenie kell a szakkérdés eldöntését, vagy más megközelítésben a szakkérdésben állást kell foglalnia, de semmiképpen nem kell, nem szabad döntenie. A magyarországi gyakorlatban nem ritkán fordul elő – akár a nyomozási, akár a bírósági szakaszban – jogkérdés feltétele a szakértő részére, a kirendelő határozatban, vagy végzésben. A szakértői törvény tervezett módosítása a 45. § (5) bekezdésében egyértelműen fogalmaz: „A szakvéleményben jogkérdésben nem lehet állást foglalni.”, mely a végleges jogszabályszövegben így hangzik a 47.§ (6) szerint: „A szakvéleményben jogkérdésben - ha jogszabály eltérően nem rendelkezik - nem lehet állást foglalni.”.

Összegezve a bűnügyi informatikának és művelőinek a szakkérdésekkel kapcsolatos tények megállapításával kell foglalkozniuk, se többel, se kevesebbel.

6 Az igazságügyi informatikai szakértői módszertanok

Az igazságügyi informatikai szakértői tevékenység tartalmi elemeit a szakértői módszertan vagy módszertanok határozzák meg. Kialakulásuk a hagyományos kriminalisztikai módszerekhez kötődik, létrejöttük pedig a 21. század első éveire tehető, amikor a korábbiakban már idézett Digital Forensics Research Workshop során kidolgozták, illetve megtárgyalták az első módszertanok részleteit.

6.1 Az informatikai szakértői módszertanok fejlődése

6.1.1 Lee's Model of Scientific Crime Scene Investigation

Lee modellje (2001) alapvetően a bűnügyi helyszínek tudományos vizsgálatát állítja a középpontba, általános megközelítést ad, nem specifikálja azt a Digital Forensic Science szakterületek egyikére sem, így a módszertanok történetében kiinduló pontként tekinthetjük.

Alapvető lépései a következők:

- **Recognition –** a potenciális bizonyítékként felhasználható tételek vagy mintázatok felismerése
- **Identification** of the various types of evidence – a bizonyíték típusok azonosítása
- **Individualization –** személyhez, vagy eseményhez egyedileg kötődő bizonyítékok azonosítása
- **Reconstruction –** az előzmények feltárása a bizonyítékokból

A Lee és társai által összeállított modell az ismertetett lépéseket logikai fák (döntési pontok elágazásai) mentén értékeli ez által segítve a nyomozati munkát, annak konkrét tárgyától függetlenül. Az eljárás a vizsgálat rendszerességére és módszerességére helyezi a hangsúlyt, mely Digital Forensic Science területeken is jól alkalmazhatók. Az elemzők hátrányként említik a kizárólagos kriminalisztikai megközelítést, ezáltal a más kutatók számára történő információátadás hiányát[54].

Megfigyelhető, hogy a kriminalisztikai megközelítés szerinti négy alapmozzanat visszsza-visszatér az új módszertanokban is, s ez okból mindenképpen vizsgálandó, hogy ez a kiindulási pont nem tartalmaz-e alapvető hiányosságot, hibát, mely a Digital Forensic Science területén történő alkalmazását gátolhatja, vagy hibás eredményre vezetheti alkalmazóit.

[54] CIARDHUÁIN, Séamus Ó.: An Extended Model of Cybercrime Investigations. in Inter-national Journal of Digital Evidence. Summer 2004, Volume 3, Issue 1, p.2. online, 2004. ijde.org online: www.ijde.org, hozzáférés: 2013.03.16

6.1.2 Casey digitális bizonyíték vizsgálati modellje

Az általános kriminalisztikai megközelítéssel közel azonos időben (2000) Eoghan CASEY is közzé tette a digitális bizonyítékok vizsgálatára vonatkozó modelljének vázlatát, mely:

- **Recognition** a bizonyítékként felhasználható eszközök és/vagy tartalmak felismerése
- **Preservation –** a bizonyíték megőrzése
  - ~ collection a bizonyítékok összegyűjtése
  - ~ documentation a tevékenység dokumentálása
- **Classification** a bizonyítékok osztályozása
  - ~ comparison a bizonyítékok összehasonlítása
  - ~ individualization a bizonyíték személyhez kötése
- **Reconstruction** a tények felépítése a bizonyítékokból

Ezt a modellt Caesy a későbbiekben (2004) tovább finomította, erről részletesen a módszertanok terminológiai összehasonlításánál lesz szó.

6.1.3 Digital Forensics Research Workshop módszertan

Továbbra is a 21. század első éveiben járunk, amikor a frissen megalakult (2001) Digital Forensics Research Workshop szervezet első konferenciáján tárgyalta és kialakította a saját vizsgálati eljárásmodelljét, melyben az alábbi műveleteket azonosította[55]:

Identification	a digitális bizonyíték azonosítása
Preservation	a digitális bizonyíték megőrzése, megóvása
Collection	a digitális bizonyíték összegyűjtése
Examination	a digitális bizonyíték vizsgálata
Analysis	a digitális bizonyíték elemzése
Presentation	a digitális bizonyíték bemutatása
Decision	döntés a digitális bizonyíték alapján

A későbbiekben a Digital Forensics kutatói ezt a modellt bővítették, egészítették ki saját preferenciáik alapján, de lényegében valamennyi későbbi modellben visszaköszön a 2001-es alapvetés.

[55] PALMER, Gary et al.: A Road Map for Digital Forensic Research. First Digital Forensic Research Workshop. Utica, NY, USA, 2001. p.17.

6.1.4 Ciardhuáin kiterjesztett eljárásmodellje

A Limerick Institute of Technology Információtechnológiai Tanszéke tanárának javaslatát (2004) a korábban felvázolt modellekkel összevetve megfigyelhető, hogy egyrészt nem lineárisan egymásra épülő tevékenységekről van szó (bár ezen a módon is értelmezhető a módszer), hanem többszöri visszacsatolási és ismétlési lehetőségeket is megenged az eljárás (vesd össze a Digital Forensics Research Workshop modellel), másrészt az egyes lépések jelentős kommunikációs aktivitást és együttműködést igényelnek a résztvevőktől (vesd össze Lee és társai modelljével):

„1. Awareness	a vizsgálat szükségességének felismerése
2. Authorisation	jogosultság, felhatalmazás megszerzése a vizsgálathoz
3. Planning	tervezés a belső (pl. ügyrend) és külső (pl. jogi környezet) információk alapján
4. Notification	értesítés, tájékoztatás a vizsgálatról (kriminál-taktikai szempontok figyelembevétele mellett)
5. Search for and identify evidence	a bizonyítékok felkutatása és azonosítása
6. Collection of evidence	a bizonyítékok összegyűjtése konzerválásra és elemzésre alkalmas módon a jogszabályi előírások betartása mellett
7. Transport of evidence	a bizonyíték(ok) szállítása az érvényesség (validity) megőrzése mellett, beleértve a számítógépes hálózatokon történő továbbítást és a fizikai szállítást egyaránt
8. Storage of evidence	a bizonyíték(ok) tárolása oly módon, hogy annak integritása ne sérülhessen
9. Examination of evidence	a bizonyíték(ok) vizsgálata a rendelkezésre álló technikai eljárások és eszközök felhasználásával a bizonyítékok integritásának megőrzése mellett
10. Hypothesis	feltevés megalkotása a bizonyítékok vizsgálata során feltárt tények alapján
11. Presentation of hypothesis	a feltevés bemutatása
12. Proof/Defence of hypothesis	a feltevés bizonyítása vagy védelme

13. Dissemination of information	a vizsgálatból származó módszertani, műveleti eredmények információinak továbbadása terjesztése a szervezeten belül, illetve a társszervezetek irányába”[56]

A modell visszacsatolási és kommunikációs aspektusai lehetővé teszik, hogy azt akár képzési, továbbképzési célokra is alkalmazzák a jogalkalmazók különböző csoportjai számára (nyomozó, ügyészek, bírák etc.) részére.

6.2 A szakértői módszertanok szabvánnyá válása

Az előzőekben bemutatott vizsgálati modellek által javasolt meghatározások, módszerek és eljárások egységesítésének törekvésén alapuló szabványosítás elérte az információ technológián alapuló biztonsági technikák, röviden információbiztonság területét (Information technology — Security techniques) is. A 21. század első éveiben jelentek meg az írásos formában is rögzített szabványok, melyek később az ISO 27000-es szabványcsalád elemeit adták.

Itt érdemes rövid kitérőt tenni és néhány szót szólni a szabványosítás jelentőségéről általánosságban.

> *„A szabványok figyelmen kívül hagyása súlyos gazdasági és jogi következménnyel járhat mivel a szabványok – az Európai Unió műszaki jogalkotásának egyik legfontosabb alapelve szerint – a jogszabályokban meghatározott alapvető követelmények teljesítéséhez kínálnak önkéntesen alkalmazható megoldásokat. Ezek figyelembevétele esetében – ugyancsak európai uniós, de már jogkövetési alapelv szerint – vélelmezni kell a jogszabálynak való megfelelőséget és ezt tilos vizsgálattal ellenőrizni.*
>
> *Az önkéntes szabványok, akár van, akár nincs kapcsolatuk a jogszabályokkal közmegegyezéssel születnek. Kidolgozásukban – érdekeik, érdekérvényesítési igényük szerint – a gazdasági minden szereplője és a jogalkotók is részt vehetnek. Tartalmuk azokat a kiadásukkor ismert műszaki követelményeket, technológiákat, vizsgálati/ellenőrzési módszereket, tehát a technika mai állását tükrözik vissza, amelyek a közmegegyezésben részt vevők számára (esetenként kompromisszumok árán) elfogadottak.*
>
> *A szabványok általános és ismételten alkalmazható eljárásokat és műszaki megoldásokat adnak, amelyeket közmegegyezéssel fogadtak el, és optimális megoldást kínálnak a különböző érdekelt felek számára. Érvényes szabvány szerinti termék, szolgáltatás esetén feltételezhető, hogy az azt alkalmazó, a műszaki fejlődés elfogadott színvonalának megfelelően, kellő gondossággal járt el.”*[57]

[56] CIARDHUÁIN, Séamus Ó. i.m. p. 5.

[57] Magyar Szabványügyi Testület: TÉVHITEK ÉS TÉNYEK szabványok, nemzeti szabványosítás, Magyar Szabványügyi Testület, http://mszt.hu/web/guest/tevhitek-es-tenyek, hozzáférés: 2015.07.12.

A biztonságtechnikai szabványcsalád digitális bizonyítékokkal kapcsolatos követelményeket rögzítő első tagja a 27037-es jelzetű Irányelvek a digitális bizonyítékok azonosítása, összegyűjtése, kinyerése és megőrzése tárgyában című szabvány.

A biztonságtechnikai szabványcsalád digitális bizonyítékokkal kapcsolatos nyomozati eljárásokat rögzítő tagja a 27041-es jelzetű Útmutató a bűncselekmények nyomozati eljárása megfelelőségének és alkalmasságának biztosítása tárgyában című szabvány.

A biztonságtechnikai szabványcsalád digitális bizonyítékok elemzésével és értelmezésével kapcsolatos tagja a 27042-es jelzetű Irányelvek a digitális bizonyíték elemzése és értelmezése tárgyában című szabvány.

Míg a szabványcsalád digitális környezetben bekövetkezett bűncselekmények vizsgálatával kapcsolatos tagja a 27043-es jelzetű A bűncselekmények kivizsgálásának alapelvei és folyamatai című szabvány.

A következőkben a szabványcsalád felsorolt elemeit tekintjük át, kiemelve az igazságügyi informatikai szakértői munkára vonatkozó részeket.

6.2.1 ISO/IEC 27037:2012(E) - Irányelvek a digitális bizonyítékok azonosítása, összegyűjtése, kinyerése és megőrzése tárgyában

A szabvány hatálya (1. Scope) a digitális bizonyítékok kezelésére terjed ki, mely magában foglalja a bizonyíték azonosítását (identification), összegyűjtését (collection), kinyerését (acquisition) és megőrzését (preservation)[58].

A hatókört leíró felsorolás tételesen tartalmazza a mobiltelefon készüléket és a PDA-t (Personal Digital Assistants), mellyel lefedi a teljes hagyományos mobiltelefon (feature phone) és okostelefon (smartphone) vertikumot. A szabvány hatóköre a tételesen felsoroltak között nem szereplő egyéb rendszerekre is vonatkozik, melyet a szöveg a nem teljes körű (not exhaustive) felsorolásra utalva egyértelműsít.

A szabványok bevezető részében határozzák meg azokat a fogalmi kereteket, melyekre a szabványban ismertetésre kerülő tevékenységek (módszerek és eljárások) épülnek.

A szabvány szövegében a meghatározások szoros abc sorrendben követik egymást, a következőkben a fogalmak logikai kapcsolataik szerint kerülnek bemutatásra a szerző magyarázataival kiegészítve:

[58] ISO/IEC 27037 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence. International Organization for Standardization. Geneva, 2012. p.1.

A szabvány által tárgyalt tartalmak a következők:

- A digitális bizonyítékokkal kapcsolatos fogalmak és eljárások áttekintése [5.]
- A digitális bizonyítékok azonosításának, összegyűjtésének, megszerzésének és megőrzésének legfontosabb elemei [6.]
- Az azonosítás, összegyűjtés, megszerzés és megőrzés esetei [7.]

6.2.1.1 Alapfogalmak és magyarázatuk

Digitális eszköz. Digitális adatok feldolgozására vagy tárolására használt elektronikus berendezés. *[3.4 – digital device]*

> Ide tartoznak a számítógép rendszerek (egészükben és egyes komponensenként, az asztali és hordozható számítógépek, a táblagépek (tablet), az okos és hagyományos (feature) telefonok, a mágneses és/vagy optikai és elektronikus tárak)

Digitális tárolóeszköz. Olyan eszköz, melyre digitális adatok rögzíthetők.

[3.9 – digital storage medium]

> A digitális eszközök részhalmaza, mely tipikusan a mágneses (szalag, merevlemez, hajlékony lemez), optikai (CD, DVD, Blu-ray), magneto-optikai (MO lemez), vagy elektronikus (SSD, memóriakártya, pendrive) formájában jelenik meg.

Digitális bizonyíték. Binárisan tárolt, vagy továbbított információ vagy adat, amelyre bizonyítékként lehet hivatkozni. *[3.5 – digital evidence]*

> Digitális bizonyíték lehet bármely olyan digitális eszköz, melyen adat található, ebből adódóan a digitális bizonyítékok lényegében tárolóeszközök, vagy tárat tartalmazó digitális eszközök.

Digitális bizonyíték másolata. A digitális bizonyíték másolata, mely abból a célból készült, hogy biztosítsa a bizonyíték megbízhatóságát, beleértve magát a digitális bizonyítékot és az ellenőrzés módszerét is. *[3.6]*

> A digitális bizonyíték másolata az előzőekből következően egy digitális adat, mely az eredeti adathordozóról egy nagy biztonságú tárolást és megváltoztathatatlanságot is biztosító tárolóra készül. Beszélhetünk bitazonos és tartalmi másolatról is. Az első esetben a másolat tartalmazza az eredeti tárolókörnyezet valamennyi adatát (így a korábban törölt adatok töredékei is elérhetők), míg a tartami másolat fájl szinten tartalmazza az eredeti adatot.

Bizonyíték őrzési helye. Olyan környezet, vagy helyszín, ahol a megszerzett, vagy összegyűjtött bizonyítékok biztonságosan tárolhatók.

[3.10 – evidence preservation facility]

Megjegyzés: A bizonyítékok őrzési helye nem lehet kitéve mágneses mezőknek, pornak, rezgéseknek, nedvességnek vagy más környezeti hatásoknak (beleértve szélsőséges hőmérséklet vagy páratartalom értékeket), amelyek károsíthatják a lehetséges bizonyítékokat a létesítményen belül.

A bizonyítékok őrzési helye a magyarországi gyakorlatban a nyomozási szakaszban a nyomozó hatóság bűnjelraktára, míg a bírósági szakaszban az eljáró bíróság irattára. Mindkét esetre jellemző, hogy a helyiségek eredetileg nem digitális bizonyítékok (digitális eszközök) őrzésére, tárolására lettek kialakítva, hanem tipikusan iratok befogadására. Ebből adódóan a por és hőmérséklet terhelés nem optimális.

A mágneses mezők hatását a tárolórendszerek tipikus megoldása (ti. fémpolcos tárolás) érdemben nem tudja befolyásolni. Ez a követelmény csak teljesen zárt mágnesezhető falú dobozban (passzív árnyékolás) történő elhelyezéssel valósítható meg[59], mely az eszközök méretének változatossága okán nehezen kivitelezhető. A szabvány meghatározásában nem szereplő elektromos mezők elleni védelem az utóbbi időben különösen fontossá vált a szilárdtest tárak (SSD) elektronikus adattárolása okán. Bár az elektromos mezők esetén a passzív árnyékolás (sűrű fémhálóval történő körbevétel - Faraday-kalitka) megvalósítható, s ezt részben teljesíti is a tárlóhelyiségek vasbeton szerkezete és a tároló polcok anyaga.

Minezek ismeretében elmondható, hogy a digitális bizonyítékok tárolásának magyarországi gyakorlata nem körülírt, az alapvető követelmények tekintetében is hiányosságok mutatkoznak, ebből adódóan a vonatkozó szabályozás kiadása, de még inkább a feltételek megteremtése kiemelkedő fontosságú.

[59] CSOHÁNY Tibor: Aktív mágneses árnyékolás. TDK dolgozat, Budapesti Műszaki és Gazdaságtudományi Egyetem, Budapest, 2003. p. 4.

Periféria. A digitális eszközhöz kapcsolt berendezés, mely bővíti az eszköz funkcionalitását. *[3.14 – peripheral]*

A digitális eszköz valamely része, kiegészítő komponense, mely legtöbbször bontható csatlakozással kapcsolódik a számítógéprendszer központi eleméhez.

A régmúltbeli gyakorlat szerint a számítógépes rendszer valamennyi perifériáját lefoglalta a nyomozó hatóság (beleértve a monitorokat és billentyűzeteket is). Napjainkban ez a gyakorlat megszűnt. Ez részben az informatikai írástudás terjedésének is köszönhető, ugyanakkor veszélyeket is rejthet magában, tekintettel arra, hogy a digitális eszközök formagazdagsága miatt nehezebbé vált az egyes eszköztípusok azonosítása. A monitorok korábban jól megkülönböztethető perifériák voltak, azonban az All-in-one számítógépek megjelenésével (pl. iMac, AIO PC) ez megváltozott, a kijelző és számítógép egybeépítése révén.

A körülmények változásához történő alkalmazkodást a nyomozóhatóságok munkatársainak gyakorlati – bűnügyi informatikai – képzése valósíthatja meg.

Lefoglalt tárterület. A digitális tárolóeszközökön (beleértve az operatív memóriát is) adatok (beleértve a metadatokat is) tárolására használatba vett tárterület.

[3.2 – allocated space]

Az adott számítógépen alkalmazott operációs rendszer által használt tárterület, melyen az adatok (digitális bizonyítékok) leggyakrabban közvetlenül hozzáférhetőek. A lefoglalt tárterület adatairól közvetlen, tartalmi másolat és bitazonos másolat is készíthető.

Le nem foglalt tárterület. A digitális tárolóeszközökön (beleértve az operatív memóriát is) az operációs rendszer által tárolásra ki nem jelölt tárterület, mely (egyébként) adatok (beleértve a metadatokat is) tárolására használható.

[3.23 – unallocated space]

Az adott számítógépen alkalmazott operációs rendszer által nem használt tárterület, melyen azonban a korábbi használatból adódóan tartalmazhat fájltöredékeket, melyek közvetlenül ugyan nem hozzáférhetőek, de szakértői szoftverek (data carving[60]) segítségével összefüggő adatállományokká alakíthatók vissza. A le nem foglalt tárterületről bitazonos másolat készíthető, melynek feldolgozásával az adatok helyreállíthatók.

[60] fájlok helyreállítása adatdarabok összeillesztése révén

Változékony adat. Olyan adatok, amelyek különösen hajlamosak a megváltozásra, könnyen módosítható adat. *[3.26 – volatile data]*

A helyszíni vizsgálatok előkészítése során játszik kiemelkedő szerepet a változékony adatok azonosítása és begyűjtésükre vonatkozó taktika meghatározása. Ez az adattípus többnyire számítógépes hálózatok elosztó eszközeinek (pl. útvonalválasztó, számítógépes kapcsoló) adatait jelenti, de lehetnek a számítógépek memóriájában (operatív tár) lévő információk vagy az elektronikus pénztárca hozzáférési adati is.

Hasító függvény érték. Hasítófüggvény eredményeként létrejövő számsorozat. *[3.11 – hash value]*

A hasító vagy hash függvény definíció szerint „A hash függvény egy üzenetet feldolgozva kimenetként egy hash kódot állít elő. Pontosabban a hash függvény egy tetszőleges hosszúságú bitfolyamból véges hosszúságú bitsorozatot állít elő."[61] Ez magyarul azt jelenti, hogy a tetszőleges digitális tartalomból (pl. fénykép, video, dokumentum, program stb.) képezhető egy meghatározott hosszúságú (meghatározott darabszámú számjegyből álló) kód, mely egyedileg azonosítja az eredeti fájlt. Ha az eredeti fájlban egy bitnyi adat (az információ legkisebb egysége) is megváltozik, a hash kód értéke is megváltozik. Ebből adódóan amennyiben kér állomány (pl. program forráskód) hash kódja azonos, úgy azok bitről-bitre megegyeznek, tehát tartalmuk teljes egészében azonos.

A hasító függvények jelentős szerepet kapnak a házkutatások során mentett adatok változatlanságának igazolásában, amikor a mentést követően a lefoglalást szenvedő megkapja a mentett adatokról készített hash kódot, vagy kódokat, melyek segítségével a későbbiekben ellenőrizheti az ügyében felhasznált adatok változatlanságát.

Rendszeridő. Az operációs rendszer által használt, a (számítógép) rendszer órája által előállított idő, mely nem azonos az operációs rendszer által számított idővel. *[3.20 – system time]*

A rendszeridő vizsgálata, illetve rögzítése a helyszíni vizsgálatok során válik nélkülözhetetlenné, különösen abban az esetben, ha egy adott esemény időbeliségének igazolására is sor kerül. A rendszeridő mellet ilyen esetekben nélkülözhetetlen az időbélyeggel hitelesített referenciaidő rögzítése is.

[61] MENEZES, Alfred J., –VAN OORSCHOt, Paul C. and VANSTONE, Paul C.: Handbook of Applied Cryptography, CRC Press, 1997. p. 321.

A laboratóriumi vizsgálatok esetén a rendszeridő lekérdezésekor az adott számítógépes rendszer adathordozóit le kell választani (adat és elektromos tápellátást egyaránt), hogy az adathordozó tartalma a részvizsgálat során ne változzon meg.

Időbélyeg. Olyan időértéket tartalmazó paraméter, mely egy adott időpont viszonyát jelzi egy referencia időhöz (pl. a koordinált világidőhöz) képest.

[3.22 – timestamp]

Az időbélyegzés szolgáltatójának meghatározása szerint: „Egy elektronikus dokumentumhoz hozzárendelt vagy azzal logikailag összekapcsolt adat, amely segítségével igazolható, hogy a dokumentum változatlan az időbélyeg elhelyezésének időpontjában létező állapothoz képest.

Egy időbélyeg jellemzően az aláírói dokumentum lenyomatát és az időbélyegzés szolgáltató hiteles és pontos órája szerinti időpontot tartalmazza, amelyeket együttesen az időbélyegzés szolgáltató aláírt, ezáltal biztosítva ezek összetartozását. Ennek révén később és harmadik fél előtt is bizonyítható, hogy a dokumentum az adott formában az adott időpontban létezett."[62]

6.2.1.2 Alapelvek és alkalmazásuk

Megbízhatóság. Következetesen tervezett viselkedés és eredmény jellemzője.
[3.16 – reliability]

Az igazságügyi informatikai szakértői tevékenység során a vizsgálati eljárások egyik fő jellemzője a megbízhatóság. Ez az alapelv biztosítja azt, hogy a szakértői vizsgálat eredménye felhasználható legyen a büntetőeljárásban. Eszközei a hasító függvények által létrejövő lenyomatfájlok, az időbélyegek, a validált szakértői hardverek és szoftverek alkalmazása.

Megismételhetőség. Annak az eljárásnak a jellemzője, amely azonos tesztelési környezetben (azonos számítógép, merevlemez, működési mód stb.) azonos eredményt ad. *[3.17 – repeatability]*

Az igazságügyi informatikai szakértői vizsgálatot oly módon kell dokumentálni, hogy az alapján egy szakképzett és gyakorlott digitális bizonyíték specialista ugyanolyan eredményt érjen el minden különösebb útmutatás, vagy értelmezés nélkül is. Ez a követelmény megjelenik a Szaktv.[2016] 47. § (4) b)-ben is, ahol a szakértői vélemény kötelező részeként kerül megnevezésre a vizsgálat módszerének ismertetése.

[62] Forrás: https://e-szigno.hu/tudasbazis/fogalmak.html#idobelyeg

Reprodukálhatóság. Annak az eljárásnak a jellemzője, amely különböző tesztelési környezetben (különböző számítógép, merevlemez, működési mód stb.) azonos eredményt ad. *[3.18 – reproducibility]*

A reprodukálhatóság biztosítja az adott tény bizonyíthatóságát vagy cáfolhatóságát. Az alapelv a vizsgált ügy dokumentálása során az esetleírásnál kap szerepet – függően az adott ügy körülményeitől – egy műveletsor következményeinek eseménysorát bemutató logikai vázlat esetén.

Példaként említhető az internetes bankkártyás vásárlások során a bankkártya adatok automatikus mentésének kérdése (11/2015 szakértő ügyszám), mely az internetes bankkártyás tranzakció folyamatát kellett különböző szoftver környezetekre vonatkozóan bemutatni (reprodukálni).

Rongálódás. Az a cselekedet, vagy olyan változtatásnak a lehetővé tétele, melynek révén a lehetséges digitális bizonyíték bizonyító ereje csökken. *[3.19 – spoliation]*

A digitális bizonyíték tartalmának megváltozása az igazságügyi informatikai szakértői tevékenység során elkerülendő. A rongálódás leggyakrabban a vizsgált adathordozó részbeni tartalmi módosulását jelenti, mely leggyakrabban nem érinti a releváns tartalmakat, ugyanakkor – a nem megfelelő kezelés révén – csökkentheti a digitális bizonyíték bizonyító erejét.

A módosulás elkerülésére különféle hardveres és szoftveres megoldások állnak a szakértők rendelkezésére, mint az írásvédő eszközökön keresztül történő tároló vizsgálat, duplikátorral készített bitazonos másolaton történő vizsgálat, okostelefonok szoftveresen írásvédett kommunikációs csatornán keresztüli vizsgálata, valamint azok az eljárásrendek, amelyek kiküszöbölik a véletlenszerű eszköz bekapcsolást (pl. akkumulátorok eltávolítása a telefonkészülékekből).

Néhány esetben azonban elkerülhetetlen a rongálódás, vagy annak enyhébb változata az adatmódosulás. Ilyen például az online, vagy bekapcsolt rendszerek vizsgálata, vagy a digitális eszközből eltávolíthatatlan tárolók elemzése. Ilyenkor a vizsgálat részletes dokumentálásával lehet a megváltozott paramétert és adatcsoportok pontos tartalmát és a változás okát meghatározni.

Az esetek elenyésző kisebbségében szükség lehet a digitális eszköz roncsolásos vizsgálatára is. Ilyen lehet a telefonkészülékek memóriaáramköreinek kiforrasztása és speciális kiolvasó készülékkel történő vizsgálata.

Ennek során akár a titkosított adatok is kinyerhetők, viszont az eszköz eredeti fizikai állapota jellemzően már nem állítható vissza. Ilyen esetben a kirendelő hatóság előzetes engedélye alapján a roncsolásos vizsgálat részletes dokumentálása mellett végezhető el a vizsgálat.

Illetéktelen hozzáférés. Szándékos cselekedet, vagy a digitális bizonyíték megváltoztatásnak a lehetővé tétele (azaz szándékos vagy tervezett rongálás).

[3.21 – tampering]

Az alapelv kapcsolódik a bizonyíték őrzési helye esetében támasztott követelmények teljesüléséhez, részben pedig a szakértői vizsgálatnál alkalmazott módszerek kiválasztásához. Ezeken kívül a digitális bizonyíték dokumentált mozgatása és a mozgatás során a felügyeleti lánc (chain of custody) fenntartása akadályozhatja meg az illetéktelen hozzáférést.

6.2.1.3 Eljárások és megvalósításuk

Azonosítás. Az a folyamat – beleértve a keresést is – amely során felismerik és dokumentálják a lehetséges digitális bizonyítékokat.

[3.12 – identification]

Az eljárás a házkutatás során jelenik meg legelemibb formájában, amikor változatos környezetben nagy mennyiségű digitális eszköz között kell felismerni a potenciális digitális bizonyítékokat tartalmazó tárgyakat, vagy rendszer komponenseket. A részletes dokumentálás első lépéseként a tárgyat, vagy rendszer komponenst meg kell jelölni oly módon, hogy az a továbbiakban egyedileg azonosítható legyen. Komplex azonosítóként alkalmazható az ügyszám – helyszín azonosító – eszköz sorszám kódminta, melyet az eszköz rövid leírása egészíthet ki.

Az azonosítási eljárás képzett és gyakorlott szakember közreműködését igényli, különösen komplex számítógépes környezetben.

Adatok megszerzése. Az adatok meghatározott köréről készített másolat létrehozásának folyamata. *[3.1 – acquisition]*

Az eljárás a helyszíni és laboratóriumi vizsgálatok során egyaránt alkalmazott alapvető szakértői munkamozzanat. Ennek során az igazságügyi informatikai szakértő duplikátorok, vagy írásvédők használata mellett teljes, vagy részleges másolatot készít az adott adathordozó tartalmáról a megfelelő szakértői szoftver (lemezkép készítő – imager alkalmazás) használatával. A keletkező szabványos formátumú lemezkép fájlok (pl. AFF, AFF4, Encase, RAW stb.) alkalmasak további részletes vizsgálatra,

a tartalmi másolatok eredetiségét az adatok megszerzését követően generált hash kóddal lehet biztosítani.

Összegyűjtés. A potenciális digitális bizonyítékot tartalmazó fizikai tárgyak összegyűjtésének folyamata. *[3.3 – collection]*

A házkutatás, vagy helyszíni vizsgálat alapvető eljárása. Az azonosítási eljárást követően kell lefolytatni, végrehajtása megelőzheti az adatok megszerzését (laboratóriumi vizsgálat), de követheti is azt (helyszíni adatmentés). Az összegyűjtés során különös figyelmet kell fordítani a potenciális digitális bizonyíték rongálódásának (módosulásának) elkerülésére. Ez lehet akár fizikai sérülés, akár az adatterületet érintő felülírás, törlés vagy más módosító művelet.

Az összegyűjtés fontos mozzanata az eszköz biztonságos csomagolása, mely egyrészt lehetővé teszi az azonosítást, másrészt megakadályozza az illetéktelen hozzáférést. Ez utóbbit oly módon, hogy a csomagolóanyag megbontása (sérülése) nélkül nem lehet hozzáférni a potenciális digitális bizonyítékot tartalmazó tárgyhoz.

A hazai gyakorlatban – sajnálatos módon – nem fordítódik kellő figyelem erre az eljárásra, így kerülhet több eszköz azonos bűnjeltasakba (vagy más csomagoló rendszerbe) mindössze darabszám megjelöléssel. Ez a hibás gyakorlat lehetetlenné teszi a felügyeleti lánc (chain of custody) megbízható dokumentálását és fenntartását, miáltal a beszerzett digitális bizonyítékok felhasználhatósága sérül, vagy megszűnik.

Megőrzés. Az a folyamat melynek során megvédik és fenntartják a lehetséges digitális bizonyíték eredeti állapotát. *[3.15 – preservation]*

Ahogy arról korábban már szó került a digitális bizonyítékok tárolása, a megfelelő elhelyezés és környezet biztosítása a digitális bizonyíték felhasználhatóságát és ismételt értékelhetőségét jelentősen befolyásoló tényező. A fizikai feltételek mellett hasonló fontosságot kell tulajdonítani a megőrzést, mozgatást, nyilvántartást végző személyzet megfelelőségének is. A jelenlegi gyakorlat szerint a bűnjelek – így a digitális bizonyítékok – kezelésével megbízott munkatársak inkább irattárosi tevékenységet végeznek, mintsem szakszerű digitális eszköz kezelést. Ebből adódóan előfordulhat a digitális bizonyítékot tartalmazó adathordozók fizikai sérülése (tipikusan külső merevlemezek esetén), mely a bizonyíték értékelését ismételt ellenőrzését lehetetlenné teheti.

A fentiekben írtak elkerülése érdekében fontos a digitális bizonyítékokkal kapcsolatba kerülő munkatársak megfelelő, folyamatos képzése és a megszerzett ismeretek és készségek időszakos gyakorlatorientált ellenőrzése.

Érvényesítés. Annak megerősítése objektív bizonyítékok révén, hogy a rendeltetésszerű használat, vagy alkalmazás követelményei teljesültek egy adott dologra vonatkozóan. *[3.24 – validation]*

Az eljárás lehetővé teszi az igazságügyi informatikai szakértői vizsgálatok során alkalmazott módszerek és eszközök működésének ellenőrzését. A validált módszerek és eszközök (beleértve a hardver és szoftver eszközöket egyaránt) bekerülhetnek a módszertani levelekbe, mint ajánlott, vagy ellenőrzött segédeszközök.

Felülvizsgálati funkció. Két adat egyezőségének ellenőrzésére szolgáló funkció.

[3.25 – verification function]

Az adatok egyezőségének ellenőrzését leggyakrabban a hash függvénynyel létrehozott digitális lenyomattal (számsorozat) ellenőrizhetjük. A két adat bitről-bitre azonos, ha a belőlük képzett hash kódok megegyeznek. Ezzel a funkcióval történik a lemezképfájlok és a helyszíni vizsgálatok során mentett tartalmak azonosítása, illetve változatlanságuk biztosítása, ellenőrizhetővé tételük révén.

Lemezkép fájl készítés. Digitális tárolókról készített bitazonos másolat készítés folyamata. A bitazonos másolatot fizikai másolatnak is nevezik. *[3.13 – imaging]*

Az igazságügyi informatikai szakértői vizsgálat alapművelete, melynek során a teljes fizikai adathordozóról, annak egy logikailag elkülönített részéről (partíció), vagy tartalmi részéről (könyvtár, mappa) egy fájlba történik az adatok átmásolása. A lemezkép fájl (image fájl) további vizsgálatok tárgya lehet, ilyen esetben az eredeti adathordozó visszaadható a bűnjelkezelőnek, aki gondoskodik a digitális eszköz megfelelő hosszútávú tárolásáról, vagy visszaadásáról a tulajdonosnak.

6.2.1.4 Személyek és tevékenységük

Digitális bizonyítékok helyszíni vizsgálója. Az a személy, aki képzettséggel és jogosultsággal rendelkezik arra vonatkozóan, hogy egy esemény helyszínén elsőként elvégezze a digitális bizonyítékok összegyűjtését és beszerzését.

[3.7 – Digital Evidence First Responder, DEFR]

> A magyarországi gyakorlatban az egyes nyomozó hatóságok rendelkeznek saját személyzettel, melynek tagjai olyan szakképzettséggel és gyakorlattal rendelkeznek, mely a helyszíni vizsgálatok során jelentkező valamennyi helyzet és körülmény kezelésére alkalmassá teszi őket. A büntetőeljárás nyomozási szakaszában az ügyek időbeli és térbeli elhelyezkedése gyakran nem teszi lehetővé a nyomozó hatóság részére a saját felkészül munkatársak bevonását, ebben az esetben történik meg a szaktanácsadó, vagy szakértő bevonása a vizsgálatba. Ez esetben az intézkedésre vonatkozó jogosultság egy része az eljárásvezetőnél marad, aki a szaktanácsadó, vagy szakértő munkáját koordinálja, szakkérdésekben a szaktanácsadó, vagy szakértő tesz javaslatot a döntésre.

Digitális bizonyíték szakértő. Az a személy, aki képes elvégezni a digitális bizonyítékok helyszíni szakértőjének feladatát, ezen felül olyan specifikus tudással és készségekkel rendelkezik, melyek révén széleskörűen kezelni tudja a felmerülő műszaki problémákat. *[3.8 – Digital Evidence Specialist, DES]*[63]

> A hazai gyakorlatban ezt a funkciót az igazságügyi informatikai szakértők látják el, akik leggyakrabban laboratóriumi vizsgálatok során nyerik ki a digitális bizonyítékokat a különféle hordozó eszközökből.

6.2.2 ISO/IEC 27041:2015(E) – Útmutató a bűncselekmények nyomozati eljárása megfelelőségének és alkalmasságának biztosítása tárgyában

A nyomozati eljárásokról szóló szabvány – jelen tanulmány szempontjából – kiemelendő eleme a munkafolyamatok (Process Class) és tevékenységek (Activity) viszonyrendszerének bemutatása a vonatkozó szabványok megnevezésével (lásd az 14.6 sz. függelékben található ábrát). A bevezető részben megtalálható meghatározások jegyzéke e szabványnál már nem alapfogalmakból, hanem a munkafolyamatok során megvalósuló tevékenységek és az ott használt eszközöket, eljárásokat, definíciókat tartalmazza. 2015. évi megjelenése okán már támaszkodik a korábbiakban létrehozott szabványokra és az azokban szereplő definíciókra egyaránt. A szabvány a következő területeket fedi le:

– Általános fejlesztési és bevezetési modell [5.3]

[63] Az ISO/IEC 27037 szabványból idézett szövegrészek a szerző fordításai.

- Adatgyűjtés és elemzés követelményei [5.5]
- Munkafolyamat tervezés [5.6]
- Munkafolyamat megvalósítás [5.7]
- Munkafolyamat ellenőrzés [5.8]
- Munkafolyamat jóváhagyás [5.9]
- Ellenőrzés [5.10]
- Bevezetés [5.11]

Amint az kitűnik a fenti felsorolásból a szabvány a vizsgálat munkafolyamatainak körülményeinek szabályozását, s ez által a vizsgálati eredmény hitelességének biztosítását írja le. Ezzel mintegy elméleti keretbe foglalja a szakértői vizsgálat gyakorlati lépéseit, melyek a következőként bemutatandó szabványban kerülnek kibontásra. A szabványban alkalmazott alapfogalmakat a következőkben mutatom be logikai kapcsolataik szerint (az eredetiben szereplő abc sorrend helyett):

6.2.2.1 Alapfogalmak és magyarázatuk

Módszer. Egy műveletet határoz meg, mely képes adatot előállítani, vagy egy meghatározott bemenetből létrehozni azt. *[3.11 – method]*

> Az igazságügyi informatikai szakértői vizsgálat során az adott eszközre, eszközrendszerre (pl. tároló, számítógépes hálózat), tartalomra (pl. elektronikus levelezés, titkosított adat), vagy egyéb szakkérdésre (szoftver értékének meghatározása) vonatkozó információszerzési, vagy adatmeghatározási eljárás leírása. A módszertani levelek nagyobb egysége, mely a főbb vizsgálati típusokra vonatkozóan meghatározza a követendő eljárásokat, egyfajta ajánlásként, vagy követendő protokollként. A módszer rövid leírása a szakértői vélemény kötelező tartalmi eleme (Szaktv.[2016] 47. § (4) b) szerint).

Folyamat. Egy adott módszer (3.11) gyakorlati végrehajtása. *[3.12 – process]*

> A módszer gyakorlati alkalmazása során az igazságügyi informatikai szakértőnek figyelembe kell vennie az eszköz, adat, vagy szakkérdés egyedi jellemzőit, melyre vonatkozóan a módszer nem ad útmutatást.
>
> Ilyen folyamat lehet egy merevlemez tartalmáról készített bitazonos másolat is, mely esetében az egyedi jellemző a tároló csatolófelülete lehet, melyhez illeszkedően kell kiválasztani a duplikátor, vagy írásvédő eszköz adapterét.
>
> A folyamatok leírása – a módszerek gyakorlati megvalósításának útmutatójaként – a módszertani levelek fontos elemei lehetnek.

Elemi (folyamat). Csak egy funkciót ellátó tevékenység. *[3.1 - atomic]*

Megjegyzés 1: Egy eszközről történő, valamennyi létező fájl visszaállítására vonatkozó módszer (3.11) lehet elemi tevékenység, ha kizárólag a fájlrendszer metaadatinak használatára támaszkodik. Az összes törölt fájl helyreállítására vonatkozó módszer nem valószínű, hogy elemi folyamat, mivel ebben az esetben szükség lesz további módszerekre, amelyek azonosítják és kibontják az adott fájlszerkezetet az eszközön tárolt adatokból, mely alapján megsimerhető a fájlok tartalma (pl. .jpg, .png, .odt, .XML, stb.).

Eszköz. A folyamat (3.12) során alkalmazott szoftver, hardver, vagy beágyazott program. *[3.17 – tool]*

Ilyen eszközök lehetnek forensic duplikátorok (lásd 252. oldal), a lemezképfájl készítő hardver eszközök, az imagerek (lásd 253. oldal), a tartalmi másolatok és lemezkép fájlok készítésére egyaránt alkalmazott írásvédő eszközök, a forensic bridge-ek (lásd 254. oldal), valamint a hardver eszközöket kezelő mager szoftverek, mint az AccessData FTK Imager (lásd a 255. oldalon).

Követelmények. Nyilatkozat, mely értelmezi, vagy kifejezi a szükségleteket, valamint a hozzá kapcsolódó korlátozásokat és feltételeket. *[3.14 – requirements]*

Megjegyzés 1: A követelményeknek különböző szintjei és a szükségletekre vonatkozó magas szintű kifejezési módjai vannak (pl. szoftver komponens követelmények). [forrás: ISO/IEC IEEE 29148:2011, 4.1.17]

A követelmények tekintetében beszélhetünk funkcionális követelményekről, melyek leírják az elvégzendő feladatokat, a bemeneti és kimeneti adatok jellemzőit. Ide tartozik továbbá a teljesítményre vonatkozó követelmény (pl. adatátviteli sebesség egy duplikátor esetében), a csatolófelületekre (interface) vonatkozó leírás (ilyen lehet egy forensic bridge csatlakozófelületeinek típusa és száma, vagy a szoftver kezelőfelületének jellemzői), de ide sorolható be a helyi jog és adminisztratív követelményeknek történő megfelelés is.

A másik megközelítés a nem funkcionális követelmények pedig a minőséggel, a rendszer hordozhatóságával (fizikai és logikai) és megbízhatóságával kapcsolatos előírások lehetnek.

Eredeti feljegyzés. Az intézkedéseket és döntéseket tartalmazó írásos feljegyzés, mely készülhet az intézkedéssel azonos időben, vagy amint az lehetséges. *[3.5 – contemporaneous notes, forrás: ISO/IEC 27042:2015, 3.4]*

Az eredeti feljegyzéseknek különösen a házkutatások során van jelentős szerepe. Elkészítésük nem csak a nyomozók részéről történik meg (ami a

jegyzőkönyv alapjául szolgál), hanem az igazságügyi informatikai szakértő részéről is kívánatos elkészíteni. A szakértő ugyanis más szempontokat emelhet ki, melyek a későbbiekben leírandó jegyzőkönyvek szempontjából nem fontosak.

A szakértői jegyzetek készülhetnek hagyományos írásos módon, vagy digitális képrögzítés révén. Ez utóbbi esetben, amennyiben nem mozgóképes felvétel készül hangalámondással, úgy mindenképpen szükséges a szöveges kiegészítés.

Az eredeti feljegyzés tartalma lehet egy élő (online) rendszer vizsgálata során a bejelentkezett felhasználó azonosítója, a kapcsolódó távoli gépek adatai, de ugyanúgy a számítógépek és eszközök fizikai elhelyezkedése, a hagyományos nyomozati módszerekkel feltárt jelszavak és hozzáférési adatok.

Érvényesítési készlet. Objektív tesztek sorozata világosan meghatározott célokkal, be és kimenő adatokkal, melyek közvetlenül kapcsolódnak a folyamat (3.12) megegyezés szerinti követelményeihez (3.14) az érvényesítés (3.18) alatt.

[3.19 - validation set]

Az adott módszer vagy eszköz helyes működésének ellenőrzésére szolgáló adat és eszközrendszer, mely ellenőrzött körülmények között már a korábbiakban adatokat szolgáltatott. Ezek a referencia adatok lesznek az éppen validált eszközre, vagy módszerre vonatkozó kontroll adatok, melyek hitelesítik a vizsgált dolgok megfelelő működését.

Felülvizsgálati funkció. Két adat egyezőségének ellenőrzésére szolgáló funkció. *[3.21 – verification function, forrás: ISO/IEC 27037:2012, 3.25, módosítva – megjegyzés eltávolítva]*

Részletesen lásd az ISO/IEC 27037:2012(E) szabványnál a 3.25 ponthoz fűzött megjegyzéseket.

Munkautasítás. Részletes leírása annak, hogy miként kell elvégezni és rögzíteni a folyamatot (3.12).

[3.23 – work instruction, forrás: ISO/TR 10013:2001, 3.1, módosítva- többes szám egyes számra cserélve, a feladat megváltoztatása folyamatra]

A munkautasítás a módszertani levél részeként az adott módszer folyamatainak és elemi folyamatainak végrehajtási rendjét tartalmazza. A leírásnak alkalmasnak kell lennie arra, hogy általa teljesüljön a megismételhetőség alapelve, vagyis egy szakképzett és gyakorlott digitális bizo-

nyíték specialista ugyanolyan eredményt érjen el minden különösebb útmutatás vagy értelmezés nélkül is, mint ami a munkautasításban szerepel.

6.2.2.2 Eljárások és megvalósításuk

Megerősítés. Objektív bizonyíték hivatalos ellenőrzése arra vonatkozóan, hogy egy folyamat megfelelő (vagy továbbra is alkalmas) a meghatározott célra.

[3.4 – confirmation]

A módszertani levélben rögzítendő eljárások és folyamatok időszakos felülvizsgálata szükséges, elsősorban a technológiai változásoknak történő megfelelés érdekében (melyet a Szaktv.[2016] is követelményként támaszt). Az ellenőrzés joga és felelőssége a Magyar Igazságügyi Szakértői Kamara Informatikai és Hírközlési Szakmai Tagozatáé, mely összefogja a szakterületen működő valamennyi igazságügyi informatikai szakértő szakmai munkáját.

Az ellenőrzést az adott módszertani levél célterületére fókuszáló munkacsoportnak kell elvégeznie oly módon, hogy az ellenőrzés módszerei, tartalma és eredménye átlátható módon jelenjen meg a szakterület szakértői és szakértői véleményeket felhasználó szervezet irányába egyaránt.

Érvényesítés. Annak megerősítése (3.4) objektív bizonyítékok révén, hogy a rendeltetésszerű használat, vagy alkalmazás követelményei (3.14) teljesültek egy adott dologra vonatkozóan. *[3.18 – validation]*

Megjegyzés 1: Érvényesítést hajtanak végre a folyamaton (3.12) annak érdekében, hogy az megfeleljen a célnak, vagyis annak biztosítására, hogy a folyamat a várt eredményekkel, ellentmondás mentesen, megismételhetően és reprodukálható módon valósuljon meg.

[forrás: ISO/IEC 27004:2009, 3.17, módosítva – az 1. sz. megjegyzéssel kiegészült]

Részletesen lásd az ISO/IEC 27037:2012(E) szabványnál a 3.24 ponthoz fűzött megjegyzéseket.

Felülvizsgálat. Annak megerősítésé (3.4) objektív bizonyítékok által, hogy a meghatározott követelmények teljesültek. *[3.20 – verification]*

Megjegyzés 1: Az ellenőrzés csupán arra nyújt biztosítékot, hogy a termék megfelel a vonatkozó előírásoknak.

[forrás: ISO/IEC 27004:2009, 3.18, módosítva – az eredeti megjegyzés eltávolítva, 1. sz. megjegyzés hozzáadva]

A megerősítési eljárás részfolyamata, melynek során a módszertanok és eszközök időszakos felülvizsgálatát végző munkacsoport az adott dolog jellemzőit összeveti az aktuális módszertani levélben szereplő követelményekkel.

Követelményelemzés. Az a folyamat (3.12), amelyen keresztül elérhető a követelmények (3.14) megértése és rangsorolása. *[3.15 – requirements analysis]*

A megerősítési eljárás részfolyamat, melynek során a megerősítést végző munkacsoport újra tárgyalja az egyes módszerekhez és eszközökhöz kapcsolódó követelményeket és azok fontosságát az igazságügyi informatikai szakértői munkában. Ennek során egyes folyamatok vagy eszközök a fontossági rangsorban előrébb, vagy hátrább sorolható. A fontossági sorrend módosításának alátámasztására célszerű az adott területre vonatkozó kutatás elvégzése (pl. mely cselekménytípusok, eszköztípusok kerültek előtérbe az adott időszak bűnügyi statisztikái szerint).

Követelmények rögzítése. Az a folyamat (3.12), amelyen keresztül a követelmények (3.14) feltárása, felülvizsgálata, tagolása és dokumentálása megtörténik.

[3.16 – requirements capture]

A megerősítési eljárás részfolyamat, melynek során a követelményelemzés révén kialakított változások bekerülnek az új módszertani előírásba.

Vizsgálat. Azoknak az eljárásoknak a sorozata, mely alkalmazható a releváns lehetséges digitális bizonyítékok azonosítására és megkeresésére egy vagy több forrásból. *[3.6 – examination, forrás: ISO/IEC 27042:2015, 3.7]*

A vizsgálat a módszertani levélben foglalt módszerek és folyamatok gyakorlati megvalósítása abból a célból, hogy a digitális eszközről kinyerhető legyen a digitális bizonyíték. A vizsgálat tényszerű leírása, dokumentálása a megismételhetőség és reprodukálhatóság követelménye mellett lehetővé teszi az eljárás utólagos azonosítását és adott időszakra vonatkozó érvényességének megítélését is.

Nyomozás. Vizsgálati műveletek alkalmazása (3.6), elemzés és értelmezés az esemény megértése érdekében. *[3.7 – investigation, forrás: ISO/IEC 27042:2015, 3.10]*

A büntetőeljárásnak azt a mozzanatát, melynek során a nyomozó és az igazságügyi informatikai szakértő a digitális bizonyítékok értékelése vonatkozásában együttműködik.

A jelenlegi hazai gyakorlatban jelentős tere van annak a – jelen sorok szerzője szerint helytelen – gyakorlatnak, mely szerint az igazságügyi informatikai szakértő szerepe befejeződik a digitális bizonyítékok kinyerésével és semmiféle további teendője nincs a nyomozás során.

Ez a szűken értelmezett szakértői szerepvállalás jelentősen befolyásolhatja a nyomozás irányát és tartalmát, tekintettel arra a körülményre, hogy az informatikai szakkérdések megértése és azok beépítése a nyomozástaktikába és stratégiába gyakran meghaladja a nyomozók képességeit.

Amíg a nyomozók digitális írástudásban nem érik el a digitális bizonyítékok helyszíni vizsgálója (Digital Evidence First Responder, DEFR -részletesen lásd az előbbiekben) szintet, addig az igazságügyi informatikai szakértő szaktudásával kell – a vonatkozó jogi szabályozás betartása mellett – segíteni a nyomozó hatóság munkáját.

Kétségtelen, hogy a fentiekben írt szerepkör részben érinti és/vagy átfedést is mutat a nyomozó és a szakértő tevékenysége között, ezért az együttműködés formai és tartalmi körülményeinek szabályozására mindenképpen szükség van. Ennek legkézenfekvőbb dokumentuma és egyben szabályozó eszköze az együttműködésre vonatkozó módszertani levél lehet, melynek megalkotásában az illetékes Szakmai Tagozat mellett a nyomozó hatóságok képviselőinek is szerepet kell vállalniuk.

Feketedobozos teszt. Vizsgálati eljárás, mely ismert bemeneti adatok feldolgozásának eredményét hasonlítja össze a tervezett kimenettel, melyek megfelelnek a folyamat követelményeinek. *[3.2 – black box testing]*

A szoftverfejlesztésből ismert tesztelési eljárás, melynek során a vizsgálati módszer tartalmi értékelésére nem kerül sor, csupán a bemeneti adatokból következő eredmény megfelelőségét vizsgálják az értékelők. A tesztelés része lehet az érvényesítés folyamatának (részletesen lásd az előzőekben).

Fehérdoboz teszt. Vizsgálat, mely magába foglalja a végrehajtás részleteinek ellenőrzését. *[3.22 – white box testing]*

A szoftverfejlesztésből ismert tesztelési eljárás, melynek során a vizsgálati módszer részletes tartalmi értékelésére is sor kerül, vagyis az elemi folyamatok szintjén történik megfelelőség vizsgálat. A tesztelés része lehet az érvényesítés folyamatának (részletesen lásd az előzőekben).

6.2.2.3 Személyek, szervezetek és tevékenységük

Ügyfél. Személy, vagy szervezet, melynek a nevében a vizsgálatot el kell végezni. *[3.3 - client, forrás: ISO/IEC 27042:2015, 3.2]*

A büntetőeljárás nyomozási szakasza során az ügyfél – az igazságügyi informatikai szakértő nézőpontjából – tipikusan a nyomozó hatóság munkatársa, leggyakrabban a nyomozó, vagy az ügy előadója, közvetett módon az eljárást felügyelő ügyész. A büntetőeljárás bírósági szakaszában az ügyfél szinte kizárólag az ügyben eljáró bíró, vagy a bírói tanács vezetője lehet.

Nyomozás vezető. Az a személy, aki a nyomozást stratégiai szinten irányítja. *[3.8 - investigative lead, forrás: ISO/IEC 27042:2015, 3.11]*

A nyomozás vezetővel a büntetőeljárás nyomozási szakaszában a házkutatások, helyszíni vizsgálatok előkészítése során találkozik az igazságügyi informatikai szakértő. Ekkor lehetőség nyílik az informatikai műszaki szempontok egyeztetése a nyomozástaktikai és stratégiai szempontokkal. A nyomozásvezető a helyszínen tartózkodó eljárásvezetővel történő kapcsolattartás révén tud közvetlenül beavatkozni a folyamatokba, de általános esetben előzetes stratégiai döntésekben van szerepe.

Nyomozó. A nyomozócsoport (3.9) tagja, beleértve a nyomozásvezetőt is (3.8). *[3.10 – investigator, forrás: ISO/IEC 27042:2015, 3.13]*

A nyomozó a büntetőeljárás nyomozási szakaszában kerül kapcsolatba az igazságügyi informatikai szakértővel, mint a helyszíni vizsgálaton részt vevő eljárásvezető, vagy mint az eljárásban részt vevő munkatárs. Nem helyszíni vizsgálat esetén az ügy előadójaként a digitális bizonyítékok közvetlen értékelését végzi, vagy az értékelési feladattal megbízott szervezeti egység által szolgáltatott kész eredményt használja fel. Munkája során közvetlen kapcsolatban áll az igazságügyi informatikai szakértővel, együttműködésük jelentősen meghatározza az eljárás minőségét és eredményességét.

A nyomozónak a digitális bizonyítékok értékeléséhez és azok megfelelő szintű felhasználásához a digitális bizonyítékok helyszíni vizsgálója (Digital Evidence First Responder, DEFR -részletesen lásd az előbbiekben) felkészültségi szintjéhez közelítő ismeretekkel és készségekkel kell rendelkeznie. Hasonló ismeretek és készségek várhatók el a nyomozást felügyelő ügyésztől is, akinek többek között a digitális bizonyítékok alapján kell döntenie a vádemelésről.

Nyomozócsoport. A vizsgálat lefolytatásában közvetlenül részt vevő valamennyi személyt magában foglaló csoport.

[3.9 – investigative team, forrás: ISO/IEC 27042:2015, 3.12]

Az igazságügyi informatikai szakértő a nyomozócsoport tagjaival leggyakrabban a házkutatások és helyszíni vizsgálatok során kerülnek kapcsolatba. A házkutatás előkészítése során, különösen, ha több helyszínen több szakértő részvételével történik a vizsgálat kiemelkedő fontosságú követelmény a nyomozó csoport tagjaival történő szoros együttműködés, legyen az a potenciális digitális bizonyítékok azonosítása, a digitális eszközök csomagolása, az eljárás folyamatainak dokumentálása, vagy éppen a helyszínek közötti mozgás előkészítése és megvalósítása, beleértve a megkülönböztető jelzéssel ellátott járművel történő szakértői kiszállás eseteit is (több helyszín esetén a szakértő azonnali beavatkozást igénylő esetben a nyomozás vezető döntése alapján).

Gyártó. Egy eszköz (3.17) létrehozója, vagy szolgáltatója, beleértve bárkit, aki módosítja, vagy testre szabja az eszközt. *[3.13 – producer]*

Megjegyzés 1: A gyártó az a személy vagy szervezet, mely felelős az eszköz létrehozásáért, fenntartásáért vagy testre szabásáért.

Megjegyzés 2: Biztosítja a parancsfájlokat az eszköz általános funkcióinak automatizálásához vagy testre szabásához.

Az igazságügyi informatikai szakértők által használt hardver és szoftver eszközök fejlesztését és gyártását speciális kör végzi. A legjelentősebb gyártók a következők:

AccessData	computer forensic sofware
Guidance Software Inc.	computer forensic sofware
Paraben	computer forensic sofware / hardvare
Belkasoft	computer forensic sofware
CRU, Inc.	computer forensic sofware/ hardware
GetData	computer forensic sofware
Cellebrite	mobil device forensic hardware
Compelson	mobil device forensic software
Oxygen Software	mobil device forensic sotware

Az érvényesítési eljárás során (részletesen lásd az előzőekben) a vonatkozó szabványok szerint tanúsított gyártók termékeire vonatkozóan a tanúsítványok helyettesíthetik az egyes termékek egyedi vizsgálatát.

6.2.3 ISO/IEC 27042:2015(E) - Irányelvek a digitális bizonyíték elemzése és értelmezése tárgyában

A digitális bizonyítékok elemzéséről és értelmezéséről szóló segédlet az alapját képezi a már megszerzett digitális bizonyítékok feldolgozásának, mely folyamat az igazságügyi informatikai szakértők tevékenységének fókuszában áll. Ennek keretében a szabvány a következő alapvető témaköröket fogja át:

- Vizsgálat [mint folyamat]
- Elemzés [mint folyamat]
- Elemzési modellek [mint módszertan]
- Értelmezés [mint folyamat]
- Jelentés készítés [mint folyamat]
- Szaktudás [mint tulajdonság]
- Jártasság [mint tulajdonság]

A felsorolt tevékenységek az események vizsgálatával kapcsolatos tevékenységek utolsó harmadában foglalnak helyet:

6.2.3.1 Alapfogalmak és magyarázatuk

Lehetséges digitális bizonyíték. Binárisan tárolt, vagy továbbított információk, vagy adatok, amelyekkel kapcsolatosan az elemzés során még nem határozták meg, hogy a vizsgálat szempontjából fontosak-e.

[3.15 – potential digital evidence]

> *Megjegyzés 1: Az elemzési folyamat határozza meg, hogy melyik lehetséges digitális bizonyíték (válik) digitális bizonyíték(ká). (3.5)*
>
> Az igazságügy informatikai szakértői vizsgálat kezdeti fázisában valamennyi vizsgálat alá vont eszköz, adat vagy dolog potenciális digitális bizonyítéknak számítható. A digitális bizonyítékká válás a szakértő általi elemzés és a vizsgálat szempontjából történő fontosság meghatározását követően történhet meg. Az esetek egy részében ez a mozzanat nem a szakértői vizsgálat során, hanem azt követően a nyomozó, vagy az erre feljogosított szervezeti egység általi értékelést követően következik be.
>
> Amennyiben az igazságügyi informatikai szakértő rendelkezésére bocsátja a nyomozó hatóság (a nyomozás vezetőjének döntése alapján) a relevanciára vonatkozó kritériumokat, úgy a szakértő azt nagyobb hatékonysággal (pl. automatizált módon) tudja érvényesíteni a potenciális digitális bizonyítékokra vonatkozóan.

Digitális bizonyíték. Binárisan tárolt vagy továbbított információ vagy adat, mely meghatározásra került az elemzés során, mint a vizsgálat szempontjából fontos adat. *[3.5 – digital evidence, forrás: [SOURCE: ISO/IEC 27037:2012, 3.5, módosítás – 1. sz. és 2. sz. megjegyzés hozzáadása, a meghatározás módosítása a vizsgálat alatti eseményektől vagy egyéb más nem fontos adatoktól való megkülönböztetés érdekében]*

> *Megjegyzés 1: Ezt nem szabad összekeverni a jogszerű digitális bizonyítékkal (3.14), vagy a lehetséges digitális bizonyítékkal.*
>
> *Megjegyzés 2: Lásd „A digitális bizonyíték állapotának változásai" ábrát (eredetiben Figure 2)*
>
> Digitális bizonyíték lehet bármely olyan digitális eszköz, melyen adat található, ebből adódóan a digitális bizonyítékok lényegében tárolóeszközök, vagy tárat tartalmazó digitális eszközök.

Jogszerű digitális bizonyíték. Digitális bizonyítékok (3.5), amelyek bírósági eljárás során elfogadásra kerültek. *[3.14 – legal digital evidence]*

> *Megjegyzés 1: Lásd „A digitális bizonyíték állapotának változásai" ábrát (eredetiben Figure 2)*
>
> A magyar jogrendben ezt a követelményt a büntetőeljárásról szóló 1998. évi XIX. törvény tartalmazza az alábbiak szerint:
>
> „77. § (1) A bizonyítási eszközök felderítése, összegyűjtése, biztosítása és felhasználása során e törvény rendelkezései szerint kell eljárni. Jogszabály elrendelheti a bizonyítási cselekmények teljesítésének, a bizonyítási eszközök megvizsgálásának és rögzítésének, valamint a bizonyítási eljárások lefolytatásának meghatározott módját."

Alkalmasság. A szaktudás és képességek alkalmazása a tervezett eredmények elérése érdekében. *[3.3 – competence, forrás: ISO/IEC 17021:2011, 3.7]*

> Az alkalmasság az igazságügyi informatikai szakértő, valamint a büntetőeljárásban a digitális bizonyítékkal kapcsolatosan munkát végző személyek (köztük a digitális bizonyítékok helyszíni vizsgálója, digitális bizonyíték szakértő, a nyomozó, a bűnjelek kezelője stb.) alapvető tulajdonsága, melyet időszakosan mérni, vizsgálni kell. Ezt a tulajdonságot olyan alakszerű tények igazolhatják, mint képesítés, tudományos fokozat, teszt eredmények, tanúsítványok, munkatapasztalat, részvétel tréningeken, konferenciákon.

Eredeti feljegyzés. Az intézkedéseket és döntéseket tartalmazó írásos feljegyzés, mely készülhet az intézkedéssel azonos időben, vagy amint az lehetséges. *[3.4 - contemporaneous notes]*

Részletesen lásd a ISO/IEC 27037:2012(E) szabványnál.

Jártasság. A nyomozócsoport azon képességét jelenti, mely révén képes más nyomozócsoportokkal egyenértékű eredményeket produkálni azonos forrásból származó lehetséges digitális bizonyítékok alapján. *[3.16 - proficiency]*

Megjegyzés 1: Sok jogrendszerben szükséges kézírásos eredeti feljegyzés készítésére nem törölhető, szabotázsjelző jegyzettömbbe, segítendő a vonatkozó tartalmak letagadhatatlanságát és elfogadhatóságát.

A jártasság az alkalmasságnak azon aspektusa, amikor a nyomozóhatóság munkatársainak csoportja, vagy adott esetben a helyszíni vizsgálat során közreműködő igazságügyi szakértők csoportja tesz tanúbizonyságot arról, hogy a módszertani elvek és folyamatok alkalmazásával képes azonos eredményt szolgáltatni azonos forrású digitális bizonyítékok elemzése értékelése alapján.

Megismételhetőség. Annak az eljárásnak a jellemzője, amely azonos tesztelési környezetben azonos eredményt ad.

[3.17 – repeatability, forrás: ISO/IEC 27037:2012, 3.17]

Megjegyzés 1: Az azonos tesztkörnyezet azonos számítógépet, merevlemezt, működési módot stb. jelent.

Részletesen lásd a ISO/IEC 27037:2012(E) szabványnál.

Reprodukálhatóság. Annak az eljárásnak a jellemzője, amely különböző tesztelési környezetben (különböző számítógép, merevlemez, működési mód stb.) azonos eredményt ad. *[3.18 – reproducibility, forrás: ISO/IEC 27037:2012, 3.18]*

Megjegyzés 1: Az eltérő tesztkörnyezet eltérő számítógépet, merevlemezt, működési módot stb. jelent.

Részletesen lásd a ISO/IEC 27037:2012(E) szabványnál.

Rongálódás. Az a cselekedet, vagy olyan változtatásnak a lehetővé tétele, melynek révén a lehetséges digitális bizonyíték bizonyító ereje csökken.

[3.19 – spoliation, forrás: ISO/IEC 27037:2012, 3.19]

Részletesen lásd a ISO/IEC 27037:2012(E) szabványnál.

Felülvizsgálati funkció. Két adat egyezőségének ellenőrzésére szolgáló funkció.

[3.21 – verification function, forrás: ISO/IEC 27037:2012, 3.25, módosítva – megjegyzés eltávolítva]

Részletesen lásd a ISO/IEC 27037:2012(E) szabványnál.

Munkautasítás. Részletes leírása annak, hogy miként kell elvégezni és rögzíteni a folyamatot (3.12).

[3.23 - work instruction, forrás: ISO/TR 10013:2001, 3.1, módosítva- többes szám egyes számra cserélve, a feladat megváltoztatása folyamatra]

Részletesen lásd a ISO/IEC 27041:2015(E) szabványnál.

6.2.3.2 Eljárások és alkalmazásuk

Nyomozás. Vizsgálatok alkalmazása, elemzések és értelmezések az esemény megértését elősegítendő. *[3.10 - investigation]*

Részletesen lásd a ISO/IEC 27041:2015(E) szabványnál.

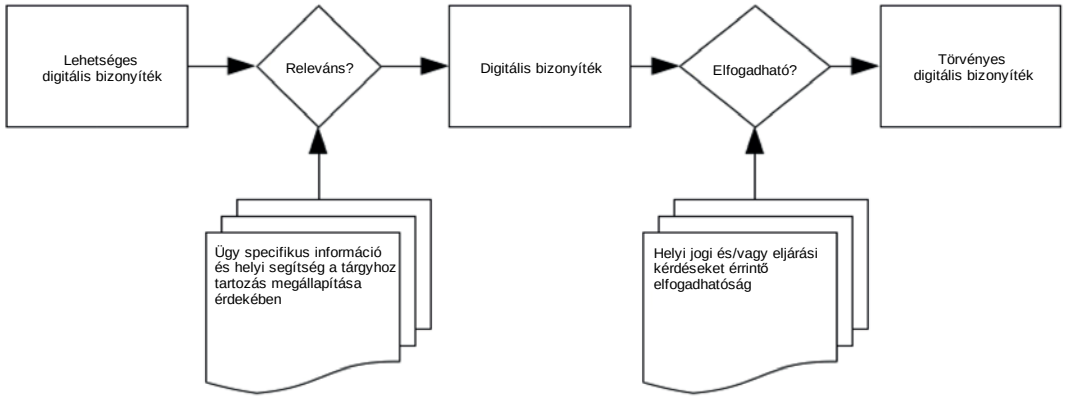
Vizsgálat. Azoknak az eljárásoknak a sorozata, mely alkalmazható a releváns lehetséges digitális bizonyítékok azonosítására és megkeresésére egy vagy több forrásból. *[3.7 - examination]*

Részletesen lásd a ISO/IEC 27041:2015(E) szabványnál.

Elemzés. A lehetséges digitális bizonyíték (3.15) értékelése, annak érdekében, hogy felmérjék annak a vizsgálatban való fontosságát. *[3.1 - analysis]*

Megjegyzés 1: A lehetséges digitális bizonyítékok (3.15), melyről megállapítást nyer, hogy fontos, digitális bizonyítékká (3.5) válik.

Megjegyzés 2: Lásd a következő ábrát (eredetiben Figure 2)



4. ábra - A digitális bizonyíték állapotának változásai (Figure 2)[64]

Az elemzést végezheti az igazságügyi informatikai szakértő (a megadott szempontok alapján, akár automatizált formában nagy mennyiségű potenciális digitális bizonyítékra vonatkozóan), végezheti a nyomozó, ha megfelelő jártassággal (részletesen lásd előbb) rendelkezik, illetve végezheti a digitális bizonyítékok helyszíni vizsgálója, vagy a digitális bizonyíték szakértő, aki megfelelő tanúsítással rendelkezik, vagy az ezzel megbízott szervezeti egység a nyomozó hatóságnál.

Utánzás (emuláció). Pontosan lekövetni, vagy azonos módon teljesíteni egy másik alkalmazás, vagy környezet körülményeit.

[3.6 – emulate]

Azokban az esetekben, amikor a digitális bizonyíték egy informatikai rendszer működésének rekonstruálását követeli meg, úgy a környezetet (legyen az akár hardver, akár szoftver környezet) megfelelően validált emulációs környezetben is meg lehet valósítani. Ebben az esetben előzetesen rögzíteni kell az eredeti rendszerkörnyezet valamennyi lényeges elemét, majd az emulált környezetben meg kell ezeket feleltetni az ottani környezeti tényezőkkel. Az emulált környezet részletes dokumentálása által a reprodukálhatóság követelményének (részletesen lásd a ISO/IEC 27037:2012(E) szabványnál) teljesülnie kell.

Értelmezés. A magyarázat összefoglalása meghatározott kereteken belül, a vizsgálatot alkotó elemzés során felhasznált bizonyítékok halmazából származó tényszerű információk alapján. *[3.9 - interpretation]*

[64] ISO/IEC 27042:2015(E) p. 3.

Az értelmezés a bűntetőeljárás nyomozási és bírósági szakaszában is megjelenő folyamat. Elvégzése jellemzően nem az igazságügyi informatikai szakértő feladata, ugyanakkor jelentősen segíteni, támogatni tudja az értelmezést a kellően részletes szakértői vélemény készítése által. Ez esetben a szakértői véleménynek nem csupán a vizsgálati eredményt kell tartalmaznia, hanem valamennyi olyan körülményt, mely befolyásolhatja a digitális bizonyítékok értékelését, legyen az akár a vizsgálati módszer, a vizsgálat során feltárt, de az ügyhöz közvetlenül nem kapcsolódó körülmény, vagy más adat.

Bizonyíték összezavarás. Egy művelet elvégzésének hatása a lehetséges digitális bizonyítékra vonatkozóan, melynek következtében a digitális bizonyíték eltűnik, vagy összezavarodik valamilyen módon. *[3.8 - evidence obfuscation]*

Megjegyzés 1: Ez lehet szándékos, vagy véletlen művelet következménye, mely a digitális bizonyítékok károsodásához is vezethet.

A rongálódás egy speciális esete, amikor a digitális bizonyíték tartalma megváltozik. Tipikus előfordulási esete az adott informatikai rendszer bekapcsolása során jön létre, amikor a rendszerek indítási folyamataival kapcsolatos adatmozgás megváltoztatja az eredeti tartalmat. Hasonló módosulás jön létre akkor is, ha a vizsgálat során az adathordozók nem írásvédő eszközön keresztül kapcsolódnak a vizsgálathoz használt szakértői számítógéphez, ilyenkor adat visszaírás történhet.

A bizonyíték módosulása elkerülhető a módszertani előírások betartásával, melyekben a vizsgálat hardver és szoftver környezetén kívül az egyes módszerek megvalósításának folyamatai elemi lépések szintjén vannak megfogalmazva.

Érvényesítés. Annak megerősítése objektív bizonyítékok révén, hogy a rendeltetésszerű használat, vagy alkalmazás követelményei teljesültek egy adott dologra vonatkozóan. *[3.20 – validation, forrás: ISO/IEC 27004:2009, 3.17]*

Részletesen lásd az ISO/IEC 27037:2012(E) szabványnál.

Igazolás. Annak megerősítése objektív bizonyítékok révén, hogy a meghatározott követelmények teljesülnek. *[3.21 – verification, forrás: ISO/IEC 27004:2009, 3.18, módosítva – eredeti jegyzet eltávolítva, 1. sz. megjegyzés hozzáadva]*

Megjegyzés 1: Az ellenőrzés csupán arra nyújt biztosítékot, hogy a termék megfelel a vonatkozó előírásoknak.

Akár módszerekre, folyamatokra, elemi folyamat lépésekre, eszközökre alkalmazható eljárás. Amennyiben tanúsító szervezet által kibocsátott igazolás tanúsítja a megfelelőséget, úgy azt az adott tanúsítási időszakon belül ismételten vizsgálni nem szükséges.

6.2.3.3 Személyek, szervezetek és tevékenységük

Ügyfél. Személy, vagy szervezet, melynek a nevében a vizsgálatot el kell végezni. *[3.2 - client]*

Részletesen lásd a ISO/IEC 27041:2015(E) szabvány értékelésénél.

Nyomozás vezető. Az a személy, aki a nyomozást stratégiai szinten irányítja

[3.11 – investigative lead]

Részletesen lásd a ISO/IEC 27041:2015(E) szabvány értékelésénél.

Nyomozócsoport. A vizsgálat lefolytatásában közvetlenül részt vevő valamennyi személyt magában foglaló csoport. *[3.12 – investigative team]*

Részletesen lásd a ISO/IEC 27041:2015(E) szabvány értékelésénél.

Nyomozó. A nyomozócsoport tagja, beleértve a nyomozásvezetőt is (3.11).

[3.13 – investigator]

Részletesen lásd a ISO/IEC 27041:2015(E) szabvány értékelésénél.

6.2.4 ISO/IEC 27043:2015(E) - A bűncselekmények kivizsgálásának alapelvei és folyamatai

Az események (digital incident) kivizsgálásának folyamatait tárgyalja a 27043 jelzetű szabvány, mely ebből adódóan a teljes vizsgálati folyamatot lefedi az alábbi fő szempontok szerint:

- Digitális vizsgálati folyamatok
- Felkészülési szakasz folyamatai
- Előkészítési szakasz folyamatai
- Kinyerési szakasz folyamatai
- Vizsgálati szakasz folyamatai
- Párhuzamosan végezhető folyamatok

A szabványban leírt tevékenységek és képességek az események vizsgálatával kapcsolatos tevékenységek utolsó harmadában foglalnak helyet:

6.2.4.1 Alapfogalmak és magyarázatuk

Biztonsági esemény. Az információbiztonság megsértése, vagy azzal kapcsolatos egyszeri, vagy sorozatos nem kívánt, vagy nem várt esemény, legyen az büntetőjogi vonatkozású, avagy nem, de nagy valószínűséggel veszélyeztetné az ügymenetet, vagy fenyegetné az informatikai biztonságot. *[3.8 – incident]*

> A büntetőeljárás során az igazságügyi informatikai szakértő a Szaktv.[2016] alapján kezeli az ügyben felmerülő adatokat. Azok átadását, vagy az azokkal kapcsolatos tájékoztatás nyújtásának körülményeit a kirendelő határozat vagy végzés szabályozza.

Folyamat. Azoknak a tevékenységeknek a köre, melyeknek egy közös végső céljuk van, melyet meghatározott időkeretben kell megvalósítani. *[3.14 – process]*

> *Megjegyzés 1: Lásd még az ISO/IEC 27000 és ISO 9000 szabványok hasonló folyamat meghatározását.*
>
> *Megjegyzés 2: A „folyamat" e szabványban használt jelentése magasabb absztrakciós szintű tartalomra utal, mint az ISO/IEC 27041 szabványban definiált „folyamat" fogalom.*
>
> Részletesen lásd az ISO/IEC 27041:2015(E) szabványnál.

Lehetséges digitális bizonyíték. Binárisan tárolt, vagy továbbított információk, vagy adatok, amelyekkel kapcsolatosan az elemzés során még nem határozták meg, hogy a vizsgálat szempontjából fontosak-e.

[3.12 – potential digital evidence, forrás: ISO/IEC 27042: – , 3.15, módosítva – a meghatározás hozzáigazítva a „vizsgálat és elemzés" absztrakt folyamat helyett csak az elemzéshez; az 1. sz. és 2. sz. megjegyzést a meghatározás nem tartalmazza]

> Az igazságügy informatikai szakértői vizsgálat kezdeti fázisában valamennyi vizsgálat alá vont eszköz, adat vagy dolog potenciális digitális bizonyítéknak számítható. A digitális bizonyítékká válás a szakértő általi elemzés és a vizsgálat szempontjából történő fontosság meghatározását követően történhet meg.

Digitális bizonyíték. Binárisan tárolt, vagy továbbított információ vagy adat, amelyre bizonyítékként lehet hivatkozni.

[3.5 – digital evidence, forrás: ISO/IEC 27037:2012, 3.5]

> Részletesen lásd az ISO/IEC 27042:2015(e) szabványnál.

Tevékenység. Egy folyamat összetartozó feladatai.

[3.2 – activity, forrás: ISO/IEC 12207:2008, 4.3]

> A folyamat elemi egységeiből (részletesen lásd az ISO/IEC 27041:2015(E) szabványnál az elemi folyamat leírását) összeálló résztevékenység, melynek során a módszer valamely gyakorlati lépésének nagyobb részlete valósul meg.

Változékony adat. Olyan adatok, amelyek különösen hajlamosak a megváltozásra, a könnyű módosíthatóság által.

[3.18 – volatile data, forrás: ISO/IEC 27037:2012, 3.26, módosítva – beillesztve az "által" szó az eredeti meghatározásba]

> Részletesen lásd az ISO/IEC 27037:2012(E) szabványnál.

6.2.4.2 *Eljárások és megvalósításuk*

Digitális vizsgálat. Tudományosan megalapozott, bevált módszerek alkalmazása a digitális forrásból származó bizonyítékok azonosítása, összegyűjtése, szállítása, tárolása, elemzése, értelmezése, bemutatása, megosztása, visszavétele és/vagy megsemmisítése területén, a megfelelő engedélyeket megszerezve, az összes tevékenységet megfelelően dokumentálva, a fizikai tárgyak vizsgálatával együttműködve, megőrizve a digitális bizonyítékot és fenntartva a felügyeleti láncot. Mindezt azzal a céllal megtéve, hogy megkönnyítse, vagy előmozdítsa a digitális vizsgálatot igénylő események rekonstruálását, akár büntetőjogi jellegűek azok, akár nem. *[3.6 – digital investigation]*

> A digitális vizsgálat a módszertani levélben foglalt módszerek és folyamatok gyakorlati megvalósítása abból a célból, hogy a digitális eszközről kinyerhető legyen a digitális bizonyíték. A vizsgálat tényszerű leírása, dokumentálása a megismételhetőség és reprodukálhatóság követelménye mellett lehetővé teszi az eljárás utólagos azonosítását és adott időszakra vonatkozó érvényességének megítélését is.

Nyomozás. Vizsgálatok alkalmazása, elemzések és értelmezések az esemény megértését elősegítendő. *[3.10 – investigation, forrás: ISO/IEC 27042: – , 3.10]*

> Részletesen lásd a SO/IEC 27041:2015(E) szabványnál.

Adatok megszerzése. Az adatok meghatározott köréről készített másolat létrehozásának folyamata. *[3.1 – acquisition, forrás: ISO/IEC 27037:2012, 3.1]*

> *Megjegyzés 1: Az adatok megszerzésének eredménye a lehetséges digitális bizonyíték másolata.*
>
> Részletesen lásd a ISO/IEC 27037:2012(E) szabványnál.

Azonosítás. Az a folyamat – beleértve a keresést is – amely során felismerik és dokumentálják a lehetséges digitális bizonyítékokat.
[3.7 – identification, forrás: ISO/IEC 27037:2012, 3.12]

> Részletesen lásd a ISO/IEC 27037:2012(E) szabványnál.

Összegyűjtés. A potenciális digitális bizonyítékot tartalmazó fizikai tárgyak összegyűjtésének folyamata. *[3.3 – collection, forrás: ISO/IEC 27037:2012, 3.3]*

> Részletesen lásd a ISO/IEC 27037:2012(E) szabványnál.

Elemzés. A lehetséges digitális bizonyíték (3.15) értékelése, annak érdekében, hogy felmérjék annak a vizsgálatban való fontosságát.
[3.3 – analysis, forrás: ISO/IEC 27042: – , 3.1]

> Részletesen lásd az ISO/IEC 27042:2015(E) szabványnál

Megjegyzés 1: A lehetséges digitális bizonyítékok, melyről megállapítást nyer, hogy fontos, digitális bizonyítékká válik.

Megjegyzés 2: Lásd a következő ábrát (eredetiben Figure 2)

Részletesen lásd a ISO/IEC 27042:2015(E) szabványnál.

Értelmezés. A magyarázat összefoglalása meghatározott kereteken belül, a vizsgálatot alkotó elemzés során felhasznált bizonyítékok halmazából származó tényszerű információk alapján.*[3.9 – interpretation, forrás: ISO/IEC 27042: – , 3.9]*

Részletesen lásd a ISO/IEC 27042:2015(E) szabványnál.

Módszer. Egy művelet meghatározása, amely használható adatszolgáltatásra, vagy információ kinyerésre egy adott bemeneti adatból.

[3.11 – method, forrás. ISO/IEC 27041: – , 3.11]

Megjegyzés 1: Ideális esetben a módszer elemi rész (azaz egynél több funkciót nem hajt végre) annak érdekében, hogy elősegítse a módszerek és eljárások újra hasznosítását és csökkentsék a folyamatok validálásához szükséges munka mennyiségét.

Részletesen lásd a ISO/IEC 27041:2015(E) szabványnál.

Megőrzés. Az a folyamat, melynek során megvédik és fenntartják a lehetséges digitális bizonyíték és a digitális bizonyíték eredeti állapotát.

[3.13 – preservation, forrás: ISO/IEC 27037:2012, 3.15, módosítva — hozzáadva az "és a digitális bizonyíték" szövegrész]

Részletesen lásd az ISO/IEC 27037:2012(E) szabványnál.

Készenlét. Az esemény bekövetkezte előtti folyamat, melynek során felkészülés történik a digitális vizsgálatra. *[3.15 – readiness]*

A készenlét a nyomozócsoportra és az igazságügyi informatikai szakértőre egyaránt értelmezhető állapot. Ennek során a felkészülés nem csupán egy passzív állapotot jelent, hanem az ismeretek és készségek folyamatos fejlesztése által egy aktív folyamatot, mely lehetővé teszi az adott esemény bekövetkezése esetén az adekvát válasz megadását.

Érvényesítés. Annak megerősítése objektív bizonyítékok révén, hogy a rendeltetésszerű használat, vagy alkalmazás követelményei teljesültek egy adott dologra vonatkozóan. *[3.16 – validation, forrás: ISO/IEC 27004:2009, 3.17]*

Részletesen lásd az ISO/IEC 27037:2012(E) szabványnál.

Igazolás. Annak megerősítése objektív bizonyítékok révén, hogy a meghatározott követelmények teljesülnek.

Megjegyzés 1: Az ellenőrzés csupán arra nyújt biztosítékot, hogy a termék megfelel a vonatkozó előírásoknak.

[3.17 – verification, forrás: ISO/IEC 27041:—, 3.20]

Részletesen lásd az ISO/IEC 27042:2015(E) szabványnál.

Összefoglalásként megállapítható, hogy az informatikai szakterületet érintő igazságügyi szakértői tevékenység módszertanára és alapfogalmaira vonatkozó széleskörű, nemzetközi szabványokban is rögzített példák állnak rendelkezésre. Ebből adódóan lehetőség nyílik a magyarországi viszony felmérésére és a szabványokban foglaltakkal történő összevetésére. Figyelemmel a hazai jogrendszer sajátosságaira, a szabványkövetelmények adaptációja is megvalósítható.

Ugyanakkor fontos szempont az is, hogy az így létrejövő tartalom, ne egy szűk körben értelmezhető szövegként kerüljön a jogalkalmazókhoz, hanem a mindennapi gyakorlatban is alkalmazható, valós eseteken keresztüli konkrét példák bemutatását is tartalmazó kézikönyvként.

Jelen tanulmány következő része ennek a feltételnek kíván megfelelni akkor, amikor a büntetőeljárást igazságügyi informatikai szakértői szempontból végig követve, a felvázolt szabványok és nemzetközi, valamint hazai példák felhasználásával a bírák, ügyészek, ügyvédek, nyomozók, s a téma iránt érdeklődők részére útmutatót ad az igazságügyi informatikai szakértői tevékenység minőségi és tartalmai alapkövetelményeiről.

7 Az igazságügyi informatikai szakértői vizsgálat tárgya és típusai

Az igazságügyi informatikai szakértők gyakorlati tevékenységét a vonatkozó jogszabályokon kívül a szakértői módszertani levél szabályozza, illetve ez utóbbi útmutatást nyújt a szakértőnek „a szakértői tevékenység egységes és magas színvonalú ellátása érdekében”[65-66]. Sajnálatos módon a korábbi időszakban a Magyar Igazságügyi Szakértői Kamara informatika szakterületre vonatkozó módszertani levelet nem adott ki, így az egységes gyakorlat követelményét megalapozó iránymutatás nem került a szakértők elé.

A MISZK Informatikai és Hírközlési Szakmai Tagozatának[67] 2017. február 18-án történt megalakulását – pontosabban első ülését, hiszen a Szakmai Tagozatok a törvény erejénél fogva jöttek létre[68] – követően megalakították a Módszertani Munkacsoportot, melynek feladata a szakmai módszertanokra vonatkozó tevékenység összefogása és az informatikai szakterület módszertani levelének kidolgozása.

A módszertani levelet megalapozó, illetve annak szerves részét képező információk és eljárások a következőkben olvashatók.

7.1 A digitális bizonyíték

Ahogy azt az előzőekben láthattuk, a szakértői módszertanok, s ez által az igazságügyi informatikai szakértői vizsgálatok gyújtópontjában a digitális bizonyíték áll. A digitális bizonyíték felismerésének, megóvásának, összegyűjtésének és vizsgálatának gyakorlata csak azt követően tárgyalható, miután tisztáztuk a fogalmi kereteket.

7.1.1 Bizonyíték fogalma a magyar jogban

A büntetőeljárásról szóló 1998. évi XIX. törvény a bizonyítás általános szabályai között határozza meg a bizonyítás eszközeit. Ezek között szerepel – a 75.§ (4)-ben – a jelen vizsgálódásban részletesen elemzendő tárgyi bizonyítási eszköz. A tárgyi bizonyítási eszközről a jogszabály 115.§ (1) és (2) bekezdése a következőket rögzíti:

> „***115. §*** *(1) Tárgyi bizonyítási eszköz minden olyan tárgy (dolog), amely a bizonyítandó tény bizonyítására alkalmas, így különösen az, amely a bűncselekmény elkövetésének vagy a bűncselekmény elkövetésével összefüggésben az elkövető nyomait hordozza, vagy a bűncselekmény elkövetése útján jött létre, amelyet a bűncselekmény elkövetéséhez eszközül használtak, vagy amelyre a bűncselekményt elkövették.*

[65] 2005. évi XLVII. törvény 30/A §

[66] 2016. évi XXIX. törvény 89. § (1)

[67] A tanulmány szerzőjét a szakértők az Informatikai és Hírközlési Szakmai tagozat elnökének választották

[68] Szaktv. 84. § (1)

(2) E törvény alkalmazásában tárgyi bizonyítási eszköz az irat, a rajz és minden olyan tárgy, amely műszaki, vegyi vagy más eljárással adatokat rögzít. Ahol e törvény iratról rendelkezik, ezen az adatot rögzítő tárgyat is érteni kell."

Amint az megfigyelhető a szöveg nem utal közvetlenül a digitális tartalomra, ugyanakkor az a tárgy, mely „… műszaki, vegyi vagy más eljárással adatokat rögzít." a digitális bizonyíték közvetett fogalom meghatározása lehet. Ebben az esetben a hangsúly az adatrögzítésen van, annak módja, pl. az, hogy digitális, vagy analóg technológiával történik-e, másodlagos.

A jogszabály ugyanakkor a 149.§ (1) bekezdésében nevesíti a „számítástechnikai rendszer"-t, bár annak tartalmát nem definiálja. A szövegösszefüggésből a számítástechnikai rendszer adattárolási funkcionalitása emelkedik ki, mely visszautal a tárgyi bizonyítási eszköznél írtakra: az adatok rögzítése vagy rögzítettsége a döntő motívum ezen bizonyítéktípus esetén.

Mindezeket kiegészítendő, meg kell jegyeznünk, hogy a „…a büntetőeljárásban csak az adatforrás, méghozzá a törvényes adatforrás és az adat, mégpedig a büntetőjogilag releváns tényre vonatkozó adat együtt képez bizonyítékot."[69]

Összegezve elmondható, hogy a magyar szabályozás önállóan nem definiálja a digitális bizonyítékot, ugyanakkor a keretek tágra szabása mellett biztos tám***pontként emeli ki az adatrögzítés mozzanatát, külön megemlítve a számítástech***nikai rendszert, mint adatrögzítési aktus eszközét.

Jelen tanulmány szerkesztésének utolsó fázisában került benyújtásra – 2017. február 14-én – T/13972 számon az Országgyűlésnek a büntetőeljárásról szóló törvényjavaslat az igazságügyi miniszter által. Az iromány a 165. §-ban sorolja fel a bizonytás eszközei az alábbiak szerint:

„A bizonyítás eszközei

165. § A bizonyítás eszközei:

a) a tanúvallomás,

b) a terhelt vallomása,

c) a szakvélemény,

d) a pártfogó felügyelői vélemény,

e) a tárgyi bizonyítási eszköz, ideértve az iratot és az okiratot is, és

[69] Tremmel Flórián: Bizonyítékok a büntetőeljárásban. Dialóg Campus. Budapest, 2012. – (Kivonat a Kriminalisztikai Szakirányú Továbbképzési Szak (KSzT) hallgatói részére.),
online: www.herke.hu/kszt/tf.doc, hozzáférés: 2013.11.02.

f) az elektronikus adat."[70]

Az f) nevesített elektronikus adatról szóló részletes útmutatás 205. §-ban található az alábbiak szerint:

„Az elektronikus adat

205. § (1) Elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.

(2) Ahol e törvény tárgyi bizonyítási eszközt említ, azon e törvény eltérő rendelkezése hiányában az elektronikus adatot is érteni kell."[71]

7.1.2 Nemzetközi kitekintés – digitális bizonyítékok helyzete a nagyvilágban

A digitális bizonyíték (digital evidence, digitaler Beweis, цифровых доказательств) fogalmának meghatározásakor elsőként a tudományterület szülőhazájának – Amerikai Egyesült Államok – szabályozását, illetve a tudomány művelőinek véleményét érdemes áttekinteni.

Amerikai Egyesült Államok

A bizonyítékokra vonatkozó szövetségi szabályozás (Federal Rules of Evidence) a magyar jogszabályhoz hasonlóan általános kereteket fogalmaz meg:

„101. szabály, hatókör, meghatározások

...

(6) egy hivatkozás bármilyen írásos anyagra, vagy más hordozóra, beleértve az elektronikusan tárolt információt is." [72]

Megfigyelhető, hogy az adatrögzítés mozzanata kap kiemelt szerepet bármilyen közvetítő eszközön (csatornán) is kerül az tárolásra. A szöveg ugyan utal az elektronikus tárolási formára, de a digitális bizonyíték kifejezés nem fordul elő sem a meghatározásoknál, sem a jogszabály szövegében.

A jogszabályokon kívül rendelkezésünkre áll a digitális bizonyítékokkal foglalkozó amerikai tudományos társaság (Scientific Working Group on Digital Evidence) szabványosító munkájának eredménye, mely az 1998-as megalakulástól kezdődően évről

[70] Magyarország Kormánya: T/13972. számú törvényjavaslat a büntetőeljárásról. 2017.02.14 .Budapest, online: http://www.parlament.hu/irom40/13972/13972.pdf, p.68.

[71] T/13972. számú törvényjavaslat a büntetőeljárásról. im. p. 81.

[72] Federal Rules of Evidence. Cornell University Law School, 2011. online: http://www.law.cornell.edu/ rules/ fre, hozzáférés: 2013.09.13.

évre válaszokat keres (és talál is) a digitális bizonyítékokkal kapcsolatos kérdésekre. Az SWGDE definíciója[73] szerint:

> ***Digitális bizonyíték***
> *Bizonyító erejű információk, melyeket bináris formában tároltak, vagy továbbítottak. (SWGDE)*

Amint az látható, a hangsúly a szakértői definícióban a bináris formában történő tárolásra kerül, leszűkítve a fókuszt a puszta adatra, s az adathordozót, bárminemű is legyen azt elhagyja a meghatározásból. Mivel a digitális adat más módon viselkedik, mint a legtöbb tárgyi bizonyíték (pl. többszörözhető minőségromlás nélkül) további meghatározásokat kell tennünk az eredetiség, a duplikátum és a másolat tekintetében. Az SWGDE szervezet válaszai a következők:

> ***Eredeti digitális bizonyíték***
> *Fizikai tárgyak és azok az adatok, melyek kapcsolatban álltak ezen tárgyakkal a lefoglalás idején.*
>
> ***Többszörözött digitális bizonyíték***
> *Pontos digitális reprodukciója valamennyi adatnak, melyet az eredeti fizikai tárgy tartalmazott.*
>
> ***Másolat***
> *Pontos – az eredeti fizikai tárgytól független – reprodukciója az adat objektumokban tárolt információknak.*

A gyakorlatban az eredetei digitális bizonyíték legtöbbször kézzel megfogható valós tárgyként jelenik meg, melyet a nyomozó hatóság lefoglal, vagy más korlátozó intézkedéssel eredeti állapotában őriz meg. Másrészt ezen tárgyak elhelyezkedhetnek földrajzi értelemben szétszórtan – mint például a felhő (cloud) szolgáltatások esetén –, amikor is a fizikai tárgy, vagy tárgyi bizonyítási eszköz eredeti értelmében nem azonosítható. Ez a jelenség a digitális adat azon tulajdonságán alapul, hogy az információtartalom kisebb adategységekből összefűzhető a technológia által[74].

A duplikátum és a másolat a digitális bizonyíték eredetiségének kérdését érintik, tekintettel arra, hogy a digitális adat minőségi (tartalmi) módosulás nélkül többszörözhető, miközben az eredeti példány „sértetlen" marad. A kétfajta többszörözés a gya-

[73] Scientific Working Groups on Digital Evidence and Imaging Technology: SWGDE and SWGIT Digital & Multimedia Evidence Glossary. version: 2.7, SWGDE/SWGIT, 2013. online: https://www.swgde.org/ documents, hozzáférés: 2013.11.02.

[74] Ugyanez játszódik le a hagyományos merevlemezes tárolás esetén is, amikor az adat az adattároló korong felületének egymástól távoli részein tárolódik le, s azok „összeolvasása" szoftveres eljárással történik.

korlatban a bitről bitre történő másolatot (ez a duplikátum) és az eszköz-független másolatot (tartalmi másolat) jelenti. A megkülönböztetés okát ismét a tárolási technológia rejti: a bitről bitre történő másolatból az eredeti eszközön rögzített és arról törölt adatok (bizonyos feltételek fennállása esetén) helyreállíthatók, míg az eszköz-független másolat esetében ez nem tehető meg.

Amint megfigyelhető, a szakértői definíciók a digitális adat (digitális bizonyíték) későbbi felhasználásával kapcsolatos körülmények figyelembe vétele mellett jöttek létre, így támogatva a szakértői vizsgálati eljárások kidolgozását és szabványosítását.

A meghatározásokon túl az amerikai szakirodalom felhívja a figyelmet digitális bizonyítékok két jellegzetességére, melyet Ehogan CASEY osztály és egyéni jellegzetességnek (class characteristics, individual characteristics) nevez[75]. Míg az osztály jellemzők az információk egy vagy több csoportját azonosítják (például egy cipőlenyomat esetén a méret), addig az egyedi jellemzők (például a cipőlenyomat egyedi hibái) az egyénre vonatkozó információkat teszik hozzáférhetővé. A digitális bizonyítékok elemzése során e két karakterisztika egybevetése és közös értékelése vezet az adott ügy szempontjából releváns információ kinyeréséhez.

A fentiek értelmezéséhez egy példával élve: ha a szakértő egy Word dokumentumot talál, mely olyan időszakra vonatkozik, amikor a szoftver adott változata még nem jelent meg, megállapíthatja a dokumentum kétségességét[76]. Más megközelítéssel az osztálytulajdonság lehet egy adott operációs rendszerhez történő kötődése az adatnak (szoftver, karakterkészlet vagy egyéb jellemző által), az egyedi jellemzőként pedig az IP cím, SIM azonosító, IMEI azonosító stb. sorolható fel.

A bemutatott kétféle megközelítés (SWGDE vs. Ehogan CASEY) tekintetében némi koherencia zavar érzékelhető. Míg az SWGDE szervezet adatorientált szemléletmódot alkalmaz, addig CASEY tágabb megközelítéssel rendszer szinten (adat és hordozója) kezeli a digitális bizonyíték fogalmát. Erre utal a digitális bizonyítékok CASEY féle csoportosítása[77], amikor HENSELER 'Computer crime and computer forensics' című írásából idézve három bizonyíték csoportot határoz meg, úgy mint:

> Számítógép rendszerek (Open computer systems)
> Ide tartoznak a kiszolgáló gépek (server), az asztali gépek (desktop) és a hordozható számítógépek (laptop) és azok tartozékai.
>
> Kommunikációs rendszerek (Communication systems)
> Ide tartoznak a hagyományos (vezetékes) telefon rendszerek, a vezeték nélküli (wireless) telekommunikációs rendszerek, az Internet és a számítógépes hálózatok.

[75] CASEY, Ehogan: Digital Evidence and Computer Crime. Elsevier. Amsterdam, 2011. p.17.
[76] CASEY im. p.18.
[77] CASEY im. pp.7-8.

Beágyazott számítógépes rendszerek (Embedded computer systems)
Ide tartoznak a mobil eszközök, smart card megoldások és minden tágabb értelemben vett számítógépet tartalmazó eszköz (digitális fényképezőgép, GPS, mobiltelefon, videofelvevő stb.).

Ez a megközelítés a gyakorlati tapasztalatokhoz jobban közelít a SWGDE szervezet definíciójával összevetve. Ugyanakkor érdemes a világ más tájain honos szabályozást is áttekinteni, mielőtt összegző javaslatot adnánk a digitális bizonyíték értelmezésével kapcsolatosan.

Az indiai szempont

Tejas D. KARIJA azonos című összefoglalója szerint[78] az indiai parlament a 2000. évben fogadta el az információtechnológia szabályozását (Information Technology Act), mely megalapozta a digitális bizonyítékok elfogadását az indiai jogrendszerben. A változás oly módon ment végbe, hogy 19. sz. végéről származó indiai szabályozást (Penal Code, 1860; Evidence Act, 1872; Banker's Book Evidence Act, 1891) kiegészítették az elektronikus rekord fogalmával (electronic records – section 3(a), Evidence Act). E szerint a bizonyíték két féle lehet: szóbeli és dokumentum jellegű, ez utóbbi pedig lehet elektronikus rögzítésű.

A változtatás jórészt az elektronikus kereskedelem UNCITRAL (United Nations Commission on International Trade Law) által javasolt modelljén (Model Law on Electronic Commerce – 1996) alapult, ugyanakkor hatása átfogóbb: az elektronikus közlönyök, elektronikus szerződések, digitális aláírások, elektronikus üzenetek bizonyítékként történő elfogadhatóságának körében a jogszabály előírja a bírónak bizonyos (az előbbiekben felsorolt) bizonyíték típusok kötelező figyelembe vételét, mint kivételt az általános szabály alól (nincs bírói mérlegelés!).

A szabályozás változását követően akár a számítógépes rendszerek merevlemezeinek elemzése (State of Punjab v. Amritsar Beverages Ltd., 2006), akár a CD-re rögzített hangfelvétel értékelése (Jagjit Singh v. State of Haryana, 2006) lehet példa arra, hogy a bíróságok pozitívan fogadták és alkalmazzák a digitális bizonyítékokra vonatkozó lehetőségeket, mely Karija szerint azt is jelzi, hogy India megpróbál lépést tartani e téren is a világgal.

[78] KARIJA, Tejas D.: Digital Evidence: An Indian Perspective. in Digital Evidence and Electronic Signature Law Review. Vol. 5. Pario Communication Ltd., Biggleswade, UK, 2008. pp. 214.

Közép-európai megközelítés

A nemzetközi kitekintés zárásaként – előre utalva az írást lezáró esettanulmányra – a szomszédos Románia szabályozásának a gyakorlati vonatkozásait tekintjük át. Tehetjük ezt annál is inkább, mert Bogdan MANOLEA beszámolója alapján[79] sok tekintetben azonos gondokkal küzd a romániai igazságszolgáltatás, mint a magyarországi.

Románia elfogadta és jogrendszerébe emelte a Cybercrime Convention (Council of Europe - ETS No. 185 - Convention on Cybercrime, Budapest, 23.XI.2001) ajánlásait (számítógépes bűncselekmény definiálása stb.). Ugyanez a szabályozás a digitális bizonyítékok (úgymint számítógépen tárolt adatok) utáni kutatás és lefoglalás jogát az ügyész és a bíró részére biztosította, míg az adatforgalom valós idejű gyűjtése kizárólag a bíró döntése alapján valósulhat meg. MANOLEA szerint ugyanakkor sem a bírói, sem az ügyészi szervezet nem rendelkezik azokkal a kompetenciákkal, amelyek a digitális bizonyítékok értékeléséhez szükségesek. A helyzetet súlyosbítja az a tény, hogy a romániai szakértői lista – ahonnan büntető eljárások során a szakértőket kötelezően ki kell jelölni – régi, elavult, illetve kevés szakértő található benne, aki a digitális bizonyítékokkal foglalkozna. A megfelelő szakértő megtalálása esetenként hat hónappal is hosszabbá teheti az eljárást.

A digitális bizonyítékokat is felsorakoztató büntető ügyekben, különösen a Romániában nagy mértékben jelen lévő adathalászat (phishing) esetén a bírák a szakértői válaszok komplexitása miatt nehezen tudnak különbséget tenni aközött, hogy az elkövető egy informatikai zseni, aki megérdemli a második esélyt, vagy egy veszélyes hacker[80].

7.1.3 Digitális bizonyítékok a hazai gyakorlatban

A magyarországi helyzet több tényezőjében hasonló a romániai viszonyokhoz. Egyrészt a digitális bizonyítékokkal foglalkozó szakértők kirendelése hazánkban is – általános szabályként – lista alapján történik (a szakértők létszáma ugyanakkor jóval kedvezőbb képet mutat: 162[81] szakértő rendelkezik informatikai kompetenciákkal). A valós összevetéshez (nem csupán a romániai példát tekintve) tekintsük át a digitális bizonyíték keletkezésének és megszerzésének folyamatát, ezúttal az igazságügyi informatikai szakértő nézőpontjából.

Digitális nyomok a hétköznapi élet csaknem minden pillanatában keletkeznek az emberekről. Ez akkor válik digitális bizonyítékká, amikor a nyomozó hatóság, vagy az erre feljogosított szervezet, többnyire a büntetőeljárás keretei között nyomozást indít.

---

[79] MANOLEA, Bogdan: The digital economy • where is the evidence? Theoretical and practical problems in understanding dlgital evidence in Romania. International Conference on Digital evidence. London, 26-27. June 2008., Conference Book pp. 227-228.

[80] MANOLEA. im. p.229.

[81] A Magyar Igazságügyi Szakértői Kamara Informatikai és Hírközlési Szakmai tagozatának nyilvántartása szerint (2017.02.18-i állapot), a kézirat lezárásakor 152 fő

Általános esetben az első eljárási cselekmény, ahol a digitális bizonyíték és a szakértő (esetenként együtt) megjelenhet, az a házkutatás.

Ha a házkutatást végző szerv számít digitális bizonyítékok felbukkanására, előzetesen szaktanácsadóként felkéri a szakértőt (leggyakrabban az igazságügyi szakértői listáról) a közreműködésre. Saját szakértői gyakorlatom azt mutatja, hogy a szakértővel közösen folytatott házkutatás és a digitális bizonyítékok szakértő általi kezelése csupán az esetek kis részében történik meg. Leggyakrabban a házkutatást végző szerv munkatársainak kell a későbbi vizsgálat szempontjából kulcsfontosságú tevékenységeket elvégezni (lásd: CIARDHUÁIN modelljét a 55. oldalon).

A szakértő a modell 5. pontjában szereplő bizonyíték felkutatása és azonosítása (Search for and identify evidence) résztől tud(na) hathatósan bekapcsolódni a vizsgálatba. Ez által elkerülhetővé válnának azok az esetek, amikor információkat nem tartalmazó készülékeket (pénzintézeti bejelentkező tokentől a monitorig és a billentyűzetig), vagy segédberendezéseket foglalnak le, illetve az is, hogy bizonyos nem speciális kialakítású eszközök (pl. Storage Area Network / Network Attached Storage, ipari jellegű számítógépek) nem kerülnek vizsgálat alá.

A digitális bizonyítékok elemzése tárgykörében a vizsgálati eljárási szabványok hiánya nehezíti a szakértők munkáját, s ugyanez a körülmény teszi az egyes vizsgálatokat nehezen összehasonlíthatóvá a kirendelő hatóságok és a bíróságok részére. A digitális bizonyítékokon alapuló szakértői vélemények gyakran próbára teszik már a nyomozó hatóság munkatársait is: az egyes hordozó médiumok megtekintése (Blu Ray lemez olvasása szinte sehol nem megoldott, a merevlemezek digitális duplikátumainak elemzéséhez szükséges írásvédő eszközök gyakran hiányoznak) és azok értelmezése (informatikai kompetenciák) a nyomozók fiatalabb generációjánál sem minden esetben készség szintű. Ez utóbbi körülmény a bírói testületre is jellemző, ezért a szakértőknek nagyobb gondot kell fordítaniuk a bizonyítékok bemutatására. Végül az egyes esetek tanulságainak a szakértői gyakorlatba történő visszaforgatása (CIARDHUÁIN modell 13. pont, Dissemination of information) rendszerszerűen nem történik meg.

7.1.4 A digitális bizonyítékok felhasználásának jövője

A digitális bizonyítékok megjelenése a büntetőeljárásban maga után vonta a definíciók és eljárási szabályok létrejöttét. Ezek országonként eltérőek lehetnek, hol általánosabb, hol pedig részletesebb szabályozással találkozhatunk. A digitális bizonyítékok kezelésének és értelmezésének problémái azonban sok hasonlóságot is mutatnak (vö. Románia és Magyarország példája), ami a kérdések nemzetközi együttműködés keretében történő megoldása irányába mutat. Hasonló megoldásra vár az eljárás módszertani szabványok kérdése, ahol a területen előrébb tartó országok (USA) megoldásainak ésszerű átvétele lehet a megoldás. A digitális bizonyítékok a büntetőeljárásban csak akkor válhatnak valóban teljes értékű bizonyítási eszközzé, ha az eljárás valamennyi szereplője rendelkezik a szerepéhez mérten megfelelő szintű kompetenciával a digitális írástudás területén.

8 Eszközök – módszerek – elemzés

8.1 A technológia hatása

Ahogy már többször utaltunk rá, a társadalomtudományok a 20. század közepétől intenzíven érdeklődnek a technológiának a társadalomra gyakorolt hatása iránt. Ez állt Harold INNIS és Marshall MCLUHAN munkásságának fókuszában, amikor az emberi gondolkodás technológia általi módosulását vizsgálták. Bár a hatás mibenléte még nem tisztázott részletesen, az mindenképpen megállapítható, hogy a technológia, pontosabban az elektronikus és/vagy digitális eszközök, szolgáltatások használata mélyen beépült a mindennapok szövetébe.

Ez a hatás akkor is nyilvánvaló, amikor a büntetőeljárás nyomozási szakaszában a vizsgálatot végző nyomozók – a cselekmény típusától szinte teljesen függetlenül – elektronikus/digitális nyomokra bukkannak, melyek felhasználása, értelmezése révén eljuthatnak az adott ügy megoldásához. Ez egyben új kihívást jelent, új készségek, képességek kifejlesztését igényli, s nem utolsó sorban olyan eljárások alkalmazását is, melyek az elektronikus / digitális nyomokat bizonyítékként történő felhasználásra alkalmassá tegyék.

8.2 A bűnjeltől a digitális bizonyítékig

A büntetőeljárás során a nyomozó hatóság munkáját – a szakértői törvény (Szaktv.2005 / Szaktv.2016) felhatalmazása alapján – az igazságügyi informatikai szakértő segíti, ha tényállás megállapításához szakkérdés eldöntése szükséges. A szakértő az eljárás során szaktanácsadóként is megjelenhet – a büntetőeljárásról szóló 1998. évi XIX. törvény 182.§ alapján – a bizonyítási eszközök felkutatásának támogatása céljából.

Az előzőek alapján az igazságügyi informatikai szakértő az elektronikus / digitális bizonyítékok felkutatása, azonosítása során jut szerephez, jellemzően a házkutatások alkalmával. A lefoglalás szabályairól szóló 11/2003. (V.8.) IM-BM-PM együttes rendelet alapján a nyomozó hatóság lefoglalja azt a dolgot „...amely az eljárás során a bizonyítás eszközéül szolgál...". A „dolog" kiválasztásában nyújt elsőként segítséget a szakértő, különösen azért, mert a releváns eszköz, nyom azonosítása komplex környezetben nem egyszerű feladat[82]. A jogszabály imént idézett részében definiált bűnjel válik majd a bizonyítás során legtöbbször tárgyi bizonyítási eszközzé, bizonyítékká.

8.3 A digitális bizonyítékok kezelésének alapelvei

Amint arra már utaltunk, a bizonyítékokkal kapcsolatos szakértői munka a digitális bizonyítékok felkutatásával és azonosításával kezdődhet el. A definíciók szerint a

[82] CIARDHUÁIN, Séamus Ó.: An Extended Model of Cybercrime Investigations. in International Journal of Digital Evidence. ijde.org, online, 2004. p.6

szakértőnek bináris adatokat kell keresnie egy tárolón, vagy bináris adatok átvitelének folyamatát (*stored or transmitted in binary form*) kell megfigyelnie, rögzítenie. Bár mindkét esetben az adatra fókuszálunk, alapesetben annak tárgyi megjelenését – a tároló, vagy átviteli eszközt – is keressük.

A következőkben Séamus Ó. CIARDHUÁIN kiterjesztett vizsgálati modelljének[83] szakértői munka szempontjából releváns részei alapján vesszük sorra az elvégzendő tevékenységeket:

8.3.1 Felkutatás és azonosítás

A binárisan tárolt, vagy továbbított adatok nagy változatosságot mutató eszközön jelenhetnek meg. Ha csak a szélsőségeket tekintjük ugyanúgy digitális bizonyítékot képezhet egy körömnyi méretű micro SD kártya, mint egy kiszolgáló gép (server). Ezek nem csak megjelenésükben, de egyéb jellemzőikben is eltérnek egymástól, így számos csoportosítási megközelítésre adnak módot.

Eogan CASEY javaslata[84] szerint a következő típusokat különíthetjük el egymástól:

- *Open computer systems*, melybe beletartoznak az asztali, vagy hordozható számítógépek, kiszolgáló gépek;
- *Communication systems*, melyek közé sorolhatók a telefonrendszerek, vezeték nélküli telekommunikáció, Internet, hálózatok;
- *Embedded computer systems*, mely jellemzően mobil eszközök, memóriakártyák, kép- és hangeszközök formájában jelenik meg.

CASEY az egyes bizonyíték típusokból az osztály és egyéni jellemzők (class and individual characteristics) alapján von le következtetéseket, melyet a cipőtalp lenyomat példájával magyaráz, ahol a cipőtalp lenyomat mérete az osztályjellemző, míg a talpfelület egyedi mintázata, sérülései révén létrejövő lenyomat az egyéni jellemző[85].

BRINSON és társai a hagyományos informatikai megközelítéshez hasonlóan osztályozzák a cybercrime technológiai oldalát. A hardver oldalon:

- *Nagy mérettartományba eső eszközök, mint számítógépes hálózatok, fürtök (Large Scale Digital Device* - Grids, Clusters);
- *Kis mérettartományba eső eszközök, mint mobiltelefonok, kéziszámítógépek (Small Scale Digital Device* – Cell Phones, PDAs);
- *Számítógépek, mint asztali számítógépek, laptopok, kiszolgáló gépek és táblaszámítógépek (Computers* – Desktops, Laptops, Servers, Tablets);
- *Tároló eszközök, mint elektronikus tárak, digitális zene lejátszók, külső merevlemezek (Storage Devices* - Thumb Drive, Digital Music Player, External Hard Drives);

[83] CIARDHUÁIN im. pp.6-7.

[84] CASEY, Ehogan: Digital Evidence and Computer Crime. Elsevier. Amsterdam, 2011. pp.7-8.

[85] CASEY im. p.653.

– *Bizonytalan besorolású eszközök, mint játék gépek, felvevő eszközök (Obscure Devices* - Gaming Devices, Recording Devices);

A gyakorlat szempontjából egyik megközelítés sem ad kézzelfogható előnyt a szakértő, vagy a nyomozóhatóság munkatársa részére.

Ha visszatérve a definíciókhoz, figyelemmel a gyakorlati szempontokra próbáljuk tagolni az eszközöket, akkor beszélhetünk az online és az offline eszközökről. Az online eszköz más eszközökkel kapcsolatban áll, a kapcsolat által az aktuális adattartalom módosulhat, míg az offline eszközök nem állnak más eszközökkel kapcsolatban, adattartalmuk statikus.

E csoportosításnak közvetlen hatása van az eszköz felkutatására és azonosítására, mégpedig annak a műveleti sorrendnek a formájában, melyet akár változékonysági rendnek (Order of Volatility) is nevezhetünk. Ez a sorrend Matthew BRAID szerint a következő is lehet[86]:

1. Registers and Cache – processzor regiszter és gyorsítótár tartalmak	6. Main Memory – operatív tár tartalma
2. Routing Tables – számítógépes hálózati útvonalválasztó útvonaltáblája	7. Temporary File Systems – ideiglenes fájlrendszer tartalma
3. Arp Cache – címfeloldási protokoll gyorsítótára (az IP címek és a fizikai címek megfeleltető táblázata)	8. Secondary Memory – másodlagos memória tartalma
4. Process Table – feladat végrehajtási tábla	9. Router Configuration – útvonalválasztó eszközök beállításai
5. Kernel Statistics and Modules – operációs rendszer rendszermag-statisztika és rendszermag-modulok tartalma	10. Network Topology – számítógépes hálózati összekötetés-rendszer

Braid azt javasolja, hogy a bizonyítékok felkutatási és azonosítási sorrendje az aktuális helyszínre, vagy esetre vonatkozó egyedi változékonysági sorrenden alapuljon. A kritikus gépek vagy rendszerek kerüljenek a sor elejére, míg a kevéssé változékony ezáltal kevéssé kritikus eszközök pedig a végére.

A gyakorlatban tipikus eset a kiszolgáló gép, asztali gép, laptop, külső merevlemez, pendrive, DVD, memóriakártya eszközcsoport lefoglalása. Ezek közül a legkritikusabb (legváltozékonyabb) rendszer a kiszolgáló gép (server), mely a legtöbb digitális bizonyítékot tartalmazhatja, ugyanakkor távoli hozzáféréssel (LAN, Wifi, mobil háló-

[86] BRAID, Matthew: Collecting Electronic Evidence After a System Compromise. AusCERT, Brisbane, 2001. p.6.

zat stb.) manipulálható a tartalma (vesd össze: pénzdíjas szoftver letöltés infrastruktúrája). A felkutatás és azonosítás első számú objektuma ezért a kiszolgáló gép, megjegyezve, hogy komplex hálózati környezetben pszeudo-hálózatok, vagy hálózati szegmensek is előfordulhatnak. A láncolat másik végén egyértelműen a megváltoztathatatlan adathordozók (pl. CD-R, DVD-R stb.) állnak, melyek megkeresése és azonosítása a vizsgálat későbbi szakaszában sem okozhat problémát.

A tipikus eljárás az előzőek szerint, hogy minden online eszközt offline eszközzé kell alakítani (amennyiben ezt a felhatalmazás lehetővé teszi), oly módon, hely megszüntetjük az eszközök közötti kapcsolatokat[87], majd a vizsgálat folytatását immár az offline eszközön végezzük. Amennyiben a kapcsolatok – a rendszer jellege miatt – nem szakíthatók meg, úgy rögzítenünk kell a vizsgálatkori állapotot.

Ennél a lépésnél szükséges az eszközök nyomozó hatóság és/vagy szakértő általi dokumentált azonosítása, ami jellemzően a bűnjelcímkék használatával történik meg a lefoglalás szabályairól szóló rendelet 7.§ (3)-(4) bekezdése alapján. Ezek a nyomdai úton előállított, viszonylag kisméretű és kevés írási felülettel rendelkező karton lapok esetenként nem praktikusak a későbbi pontos azonosításra. Ezen javíthat a bizonyíték sorszámának (jól olvasható) nagyméretű feltüntetése el nem távolítható módon, illetve a lefoglalás helyszínének hasonló megadása. Azok a kísérletek, melyek „fekete PC", vagy „azonosító nélküli számítógép" megnevezéssel próbálják leírni az eszközt, komolyan akadályozhatják a későbbi bizonyítékként történő felhasználást. Azonosító hiányában a nyomozó hatóság munkatársa, vagy a házkutatáson részt vevő szakértő is alkalmazhat (kell, hogy alkalmazzon) egyedi azonosító jelzést.

8.3.2 Bizonyítékok összegyűjtése

A megjelölt eszközök összegyűjtése során a vizsgálatban résztvevő valamennyi munkatársnak ügyelnie kell az eredeti állapot megőrzésére. E tevékenység mottója a "Preserve everything but change nothing" (őrizz meg mindent, ne változtass semmin) lehet. Ennek a követelmények a biztosítása érdekében e műveletnél kell a későbbi beavatkozást megakadályozni, illetve itt kell elindítani azt a dokumentációs folyamatot, amely felügyeleti lánc (Chain of Custody) formájában végigvonul a bizonyítékok kezelésének teljes életútján, mely alapján végig követhető marad, hogy mely időszakban hol, kinek a felügyelet alatt volt a bizonyíték, történt-e változás annak állapotában. Ez utóbbit a bizonyíték megfelelő csomagolás biztosíthatja. A lefoglalás szabályairól szóló rendelet 7.§-a rendelkezik a bűnjel (későbbi bizonyíték) csomagolásáról, s két lényeges követelményt támaszt:

> *A bűnjelet olyan módon kell becsomagolni és megőrizni, hogy annak tartalma illetéktelen személy előtt rejtve maradjon*

[87] BRAID im. p.9.

A csomagolásra olyan eszközt, anyagot kell alkalmazni, mely a bűnjelet megóvja a károsodástól, s egyúttal azt is megakadályozza, hogy mérgezést, fertőzést … okozzon."

A gyakorlatban a *„... a tartalma illetéktelen személy előtt rejtve maradjon."* kitétel miatt a bűnjelek részben, vagy teljes egészükben átlátszatlan anyagú csomagolásba kerülnek, ugyanakkor az *„...olyan anyagot vagy tárgyat használ,"* szövegrész nem korlátozza a csomagolásra használandó anyag fajtáját. A digitális bizonyítékká váló bűnjel esetén a *„...a károsodástól megóvja..."* követelményből fakadóan a szabványos kapcsolódási pontokhoz történő hozzáférés korlátozását is meg kell valósítani.

Az esetek jelentős részben a csomagolandó bűnjel asztali számítógép, vagy ennél kisebb eszköz formájában kerül a nyomozó hatóság munkatársa és/vagy a szakértő elé. A számítógépek esetén a szemeteszsák + széles ragasztószalag megoldás a legelterjedtebb, mellette az eszköz előlapjának és hátlapjának A/4 méretű másolópapírral történő lefedése és körcímkével történő rögzítése (a lefoglalást szenvedő aláírásával ellátva) tekinthető megszokott módszernek. Mindkét megoldás teljesíti a jogszabályi követelményeket, bár az utóbbi a hosszas tárolás következtében fizikailag oly mértékben megváltozhat (ragasztó felület elenged), hogy a beavatkozástól védő felület leesik.

A jogszabály alkotók és/vagy a jogalkalmazók figyelmét mindenképpen érdemes felhívni arra a körülményre, amely a digitális bizonyítékká váló bűnjeleket megkülönbözteti az egyéb tárgyi bizonyítási eszközöktől és okirati bizonyítéktól, mégpedig az a körülmény, hogy a bizonyíték – jellegéből adódóan – közvetlenül akkor sem figyelhető meg, ha átlátszó csomagolásban is van. Ugyanis a binárisan tárolt adat – ahogy azt a korábbi definíciókból megismerhettük – közvetítő eszköz (pl. számítógép) nélkül nem érzékelhető. Ebből adódóan az a jogértelmezés, mely szerint az a bűnjel, mely digitális bizonyítékot tartalmaz(hat) az azonosíthatóság érdekében átlátszó csomagolással is ellátható, nincs ellentétben a jogszabályi követelményekkel, ugyanakkor jelentősen egyszerűsítheti a nyomozó, a szakértő és a bűnjel kezelőjének a munkáját.

A számítógépnél kisebb méretű eszközök (pl. laptop, tablet, mobil telefon stb.) esetén a csomagolás egyrészt egyszerűbb, másrészt rejtett problémát okozhat. Ennek a veszélye különösen akkor áll fenn, ha az eszköz nem teljes egészében csomagoljuk be, ami a hordozható számítógépek (laptop, notebook, netbook, tablet) esetén tipikus. A csomagolás gyakran csak a vélt hozzáférési pontokat (elektromos csatlakozás, USB, LAN stb. csatlakozók) takarják el és az eszköz hátlapján (alján) található, a tárolóeszközt burkoló felület rögzítő csavarjait szabadon hagyják. Ez esetben a tároló és annak tartalma hozzáférhető marad, így kétségessé válhat a későbbi bizonyítékként történő felhasználás. Ugyanezt a következményt vonja maga után az eleve sérült anyagokkal történő csomagolás.

A kisméretű eszközök előtalálása még a vizsgálat alá vont személy együttműködése esetén sem egyszerű. A tipikus eszköztárolási helyek (pl. személyes, aktuális adatok

1- 1,5 méteres távolságon belül) azonosításához szakértői, vagy szaktanácsadói segítségre lehet szükség, illetve a helyszíni vizsgálatban résztvevő állomány tagjait megfelelő szintű továbbképzéssel fel lehet készíteni, mely Nelson és szerzőtársai szerint akár a következő is lehet[88]:

> *1. szint:* a digitális bizonyíték megszerzése és lefoglalása, ez rendszerint a rendőr járőr (street police officer) feladata
>
> *2 szint:* high-tech vizsgálatok irányítása, a számítógépes szakkifejezések ismerete, mit lehet és mit nem lehet kinyerni a digitális bizonyítékokból, ez rendszerint a nyomozók (detective) feladat
>
> *3. szint:* digitális bizonyítékok kinyerése, adat helyreállítás, számítógépes hálózati bűnfelderítés, internetes csalások vizsgálata

8.3.3 Bizonyítékok szállítása

A felkutatást és azonosítást, valamint a bizonyítékok összegyűjtését követően kerülhet sor – valamennyi lépés szigorú dokumentálása mellett (Chain of Custody) – a bizonyítékok elszállítására (házkutatás helyszínéről a bűnjel raktárba). A szállítandó bűnjelek csomagolása ennél a lépésnél sérülhet meg a bűnjelek csomagolása, illetve a kis méretű eszközök fokozottan veszélyeztetettek. A szállítás esetén a digitális bizonyítékot tartalmazó bűnjeleket érdemes gyűjtő csomagolásba helyezni, ez különösen a hordozható számítógépnél kisebb mérettartományba eső eszközökre érvényes. A szállítást megelőzően és azt követően (pl. bűnjelraktárba történő átadás) a tételes azonosítás szükséges.

A szállítás tipikus útvonala a házkutatás helyszíne és a nyomozó hatóság bűnjel raktára közötti mozgatás, illetve a bűnjel raktár és szakértői telephely közötti szállítás. Ez utóbbi esetben a szakértő tételes átvételt és a csomagolás sértetlenségének ellenőrzését már az átvétel helyszínén (nyomozó hatóság bűnjel raktára/irodahelyisége) el kell, hogy végezze. A dokumentálásra alkalmas bármely digitális fényképezőgép, mely képes 3-5 megapixel, vagy ennél nagyobb felbontású felvételek készítésére. A gyakorlatban csak a sérült csomagolás digitális rögzítése történik meg általában, de az átadás – átvétel teljes képi dokumentálása sem hibás megközelítés. Ezzel a mozzanattal biztosíthatja a szakértő, hogy a felügyeleti láncban betöltött szerepét megfelelően dokumentálja. Az itt tapasztalt eltéréseket (pl. csomagolás sérülése, vagy az eszköz sérülése) a későbbiekben a szakértői véleményben (ami szintén bizonyítékként értékelendő) is rögzíteni kell.

Nem esett eddig szó a hordozható eszközök akkumulátorról történő tápellátásának kérdéséről. A szállítás kapcsán azért kell erről megemlékezni, mert a tápellátás alatt

[88] NELSON, Bill – PHILLIPS, Amelia – ENFINGER, Frank – STEUART, Chris: Computer Forensics and Investigations. Thomson Course Technology, Boston, MA, USA, 2004. p.12.

álló eszközök (pl. alvó üzemmódban lévő hordozható számítógép) növelheti a szakértői szállítás kockázatát. A szállítás közben magára hagyott (szigorúan tilos!) gépkocsi csomagtartójában készenléti üzemmódban működő eszközök hőkamerás, vagy LAN szkenneres módszerrel felderíthetők (két ismert elkövetési magatartás) és az eszközök ez által illetéktelen kezekbe kerülhetnek. A mobiltelefonok és kézi számítógépek esetén az akkumulátoros tápellátás lehetővé teszi a tartalom esetleges módosulását, ami elkerülendő. A szállítást megelőzően, még a csomagolási fázis előtt célszerű az alvó, vagy készenléti üzemmódok megszüntetése, illetve az akkumulátorok eltávolítása a mobiltelefon készülékekből és PDA-kból.

8.3.4 Bizonyítékok tárolása

A tápellátási probléma a tárolási fázisban is fennáll. Amennyiben elmulasztottuk a csomagolás előtt „áramtalanítani" a mobil eszközt, úgy megfelelő dokumentálás mellett ez később is megtehető, bár ez esetben kétségessé válhat a bizonyíték eredeti állapotban tartása. Ugyanakkor a bűnjel raktában megszólaló mobiltelefon készülék (bejövő hívás) egyéb problémát is okozhat.

A szakértőnél történő tároláskor az egyes eszközökből kiszerelt alkatrészek, tipikusan tárolóeszközök azonosítása és nyomon követése okozhat problémát, különösen párhuzamosan futó ügyek esetén. Az egyes tárolóeszközök azonosítására az eltávolítható átlátszó ragasztószalagon történő jelölés alkalmas módszer. Az eszköz valamennyi azonosítója: ügyszám, helyszín, tétel szám, eszköz megnevezése, kiszerelt eszköz sorszáma, vagy pozíciója (több beépített tároló esetén) felkerülhet a szalagra. Az elemzés végeztével a visszaszerelést közvetlenül megelőzően a ragasztószalag nyom nélkül eltávolítható a tárolóeszköz felületéről.

A bizonyítékok szakértő általi tárolása során is meg kell felelni a jogszabály által támasztott követelményeknek a sértetlenség és változatlanul hagyás vonatkozásában is.

8.3.5 Bizonyítékok vizsgálata

A bizonyítékok szakértői vizsgálata önmegában is jelentős mozzanata a büntetőeljárásnak és azon belül a bizonyítékok kezelésének. Terjedelmi okokból csak címszószerűen tudjuk ismertetni azon követelményeket, melyek erre a szakaszra vonatkoznak.

A szakértői vizsgálat néhány fontos alapelve[89]:

- Az eredeti digitális bizonyíték minimális használata,
- A változások számontartása,
- A bizonyítás szabályainak betartása,
- A saját tudás határainak át nem lépése (a szakértő részéről sem).

[89] BRAID im. p.5

A szakértői vizsgálat lezárultával a szakértő mind a bűnjeleket, mind az azokból kinyert digitális bizonyítékokat átadja a kirendelő részére. Az elemző munka során létrejött és a szakértői számítógépen megtalálható digitális bizonyítékok sorsáról egyértelmű rendelkezés, állásfoglalás nem ismeretes.

A magyarországi igazságügyi informatikai szakértők között két megközelítés terjedt el és működik jelenleg is: az első szerint a munka végeztével a szakértő minden hozzá került digitális tartalmat véglegesen töröl a számítógépéről és egyéb adathordozóiról, egyedül a szakértői vélemény dokumentum állományát tartja meg saját archívumában a vizsgálattal összefüggésben. A másik megközelítésben (jelen sorok szerzője ezt támogatja) a szakértő a mentett digitális bizonyítékokat a szakértői archívumában megőrzi.

Az utóbbi megoldás számos kérdést vet fel. A megőrzés költségeit ki fedezi, a mentett tartalmakat mely időtartamig őrizze meg a szakértő és még sorolhatnánk. Ugyanakkor a gyakorlat azt mutatja, hogy nem ritkán kér a nyomozó hatóság hiteles másolatokat a szakértői véleményhez csatolt digitális mellékletekből néhány hónap és ritkábban akár 3-4 év múltán is. A kérdés megnyugtató megválaszolására az érintett szervezetek és szereplők szakmai egyeztetés és akár jogi eszközökkel történő szabályozására is szükség lehet.

8.4 Szakértői eszközök és alkalmazásuk

Az igazságügyi informatikai szakértői munka módszertani alapvetései az igazságügyi szakértői tevékenységről szóló 2005. évi XLVII. törvény (Szaktv.[2005]) első szakaszából eképpen vezethetők le:

„1. § (1) Az igazságügyi szakértő feladata, hogy a bíróság, a közjegyző, az ügyészség, a rendőrség és a jogszabályban meghatározott más hatóság (a továbbiakban együtt: hatóság) kirendelése, vagy megbízás alapján, a tudomány és a műszaki fejlődés eredményeinek felhasználásával készített szakvéleménnyel segítse a tényállás megállapítását, a szakkérdés eldöntését."

Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény (Szaktv.[2016]) esetén a hangsúly módosul az alábbiak szerint:

„3. § (1) Az igazságügyi szakértő feladata, hogy a hatóság kirendelése vagy megbízás alapján, a tudomány és a műszaki fejlődés eredményeinek felhasználásával készített szakvéleménnyel, a függetlenség és pártatlanság követelményének megtartásával **döntse el a szakkérdést**, és segítse a tényállás megállapítását."

A Szaktv.[2005]-ben – azonosan a Szaktv.[2016] 3. § (3)-vel – második szakasz a feladat elvégzésének módját is meghatározza:

„(2) Az igazságügyi szakértő a tevékenységét e törvény és más jogszabályok rendelkezései, valamint a tevékenységére irányadó szakmai szabályok megtartásával, legjobb tudása szerint köteles végezni."

Kiemelve a lényeget: szakkérdést kell eldönteni, a tudomány (benne a műszaki tudomány) eredményei alapján, az irányadó szakmai szabályok szerint. E fejezetben az irányadó szakmai szabályokat vizsgáljuk meg részletesen.

E szabályok forrása alapesetben lehet nemzeti, vagy nemzetközi szakmai szervezet által kiadott ajánlás (módszertani levél), illetve az ezek nyomán létrejött nemzeti, és/vagy nemzetközi szabvány. A hazai ajánlással még adós a Magyar Igazságügyi Szakértői Kamara az egyes szakterületek módszertani leveleivel (melynek kiadására az igazságügyi szakértői kamaráról szóló 1995. évi CXIV. törvény kötelezi, illetve hatalmazza fel), így nemzetközi szervezetek ajánlásait tudjuk csak áttekinteni. A 2001-ben megalakult Digital Forensics Research Workshop szervezet által kialakított vizsgálati eljárásmodell az alábbi műveleteket azonosította a szakértői munkában[90]:

Identification – azonosítás

Preservation – megóvás

Collection – összegyűjtés

[90] PALMER et. al. im. p. 17.

Examination – vizsgálat

Analysis – elemzés

Presentation – bemutatás

Decision – döntés

A későbbiekben a Digital Forensic kutatói ezt a modellt, bővítették, egészítették ki saját preferenciáik alapján, de lényegében valamennyi későbbi modellben visszaköszön a 2001-es alapvetés. Ez érvényes a Digital Forensic területen megszületett első nemzetközi szabványra az ISO 27037-re is, mely következőképpen foglalja össze az alapfeladatokat:

8.4.1 Általános alapelvek

A lehetséges digitális bizonyítékokat a következő alapelvek alapján kell kezelni:

- Minimalizálni kell a hozzáférést
- Minden változás dokumentálása és indoklása
- A bizonyíték kezelési szabályok betartása
- A kompetenciakörön belüli tevékenység

Azonosítás

A keresést, az azonosítást és a dokumentációt a következőképpen kell elvégezni a lehetséges digitális bizonyíték esetén:

- Fontossági sorrend meghatározása a bizonyítékok összegyűjtésekor, mely a bizonyíték változékonyságát (volatility) veszi figyelembe
- Károkozás minimalizálása,
- Rejtett digitális bizonyítékok azonosítása

Összegyűjtés

Az összegyűjtés egy olyan folyamat, mely során azokat az eszközöket, amelyek digitális bizonyítékokat tartalmazhatnak eltávolítják eredeti helyükről, majd azokat egy laboratóriumban, ellenőrzött környezetben vetik alá elemzésnek és adatkinyerésnek.

Kinyerés

Az a folyamat, melynek során másolat készül a lehetséges digitális bizonyítékról

Megőrzés

A megőrzés a lehetséges digitális bizonyítékok integritásának megőrzése. A lehetséges digitális bizonyítékot, vagy eszközt meg kell védeni az illetéktelen beavatkozástól vagy rongálódástól.[91]

Az általános alapelvek megvalósításakor a szakértő elsőként a szakterületi illetékességét vizsgálja meg, azaz jogosult-e szakértői véleményt adni az érintett területre vonatkozóan. Ezt a szakterületi besorolás és a vizsgálat alá vont tartalom összevetésével teheti meg. Nézzünk néhány konkrét példát:

19. táblázat – kompetencia körök ellenőrzése

Feladat	Kompetenciakör	Szakértői ügyszám
videofelvétel vizsgálata	stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység	1/2007
blogbejegyzés létrehozójának megállapítása	informatikai biztonság	4/2010
számítógépes rendszer vizsgálata	informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver)	13/2013

A bizonyítékok kezelésére vonatkozóan Magyarországon a 11/2003. (V. 8.) IM-BM-PM együttes rendelet tartalmaz előírásokat, melyek informatikai rendszerekre vonatkozóan nem tartalmaznak specifikus utalásokat, így a betartásáért felelős nyomozók nem ritkán megsértik a minimális hozzáférés követelményét. Ennek elkerülésére a nyomozó hatóság alkalmazhat szaktanácsadót vagy szakértőt a házkutatások és lefoglalások alkalmával.

A potenciális digitális bizonyítékok azonosítása (Identification) során az elsődleges követelmény a bizonyítékok változékonysági sorrendjének (Order of Volatility) felmérésre, mely a bizonyítékok megkeresésének és azonosításának sorrendjét is meghatározza. Ez a gyakorlatban azt jelenti, hogy a leggyorsabban megváltozó tartalom azonosítása és mentése az elsődleges: ilyen lehet egy számítógép operatív memóriájának (figyelem, ez nem a merevlemez vagy egyéb tartós tár) a tartalma a számítógépes hálózat aktív eszközeinek (pl. útvonalválasztó, híd, kapcsoló) memóriatartalma. Hasonlóképpen szakértői feladat a rejtett digitális bizonyítékok azonosítása, mely lehet egy kis méretű tárolóegység, vagy a számítógépes hálózaton keresztül elérhető helyi/távoli felhő szolgáltatás, de akár egy rejtett megfigyelő kamera adatainak továbbítását végző hálózati eszköz is. Ezek felismerése és a károkozás nélküli (Minimize the

[91] ISO/IEC 27037:2012(E), a szerző fordítása

damage to the potential digital evidence) bevonása a bizonyítékok körébe jelentősen befolyásolja a későbbi felhasználhatóságot. Mindezek felmérése és elvégzése szakértői feladat, de csak abban az esetben kerülhet rá sor (a hazai gyakorlat példái alapján), ha a kérdéses ügy súlya, vagy összetettsége okán a nyomozó hatóság már a lefoglalás időszakában bevonja a szakértőt a vizsgálatba.

A bizonyítékok összegyűjtésénél (Collection) érkezünk el ahhoz a lépéshez, ahol a szakértői eszközhasználat (hardver és szoftver) megjelenhet. Ez különösen azoknál az eseteknél történhet meg, ahol a vizsgálandó és a bizonyítékot feltételezhetően tartalmazó eszköz nem foglalható le, és/vagy nem a házkutatás helyszínén található. Ilyen lehet egy webes szolgáltatás kiszolgáló gépe fizikai helyének megállapítása a számítógépes hálózati kapcsolatok helyszíni elemzésével (szakértői ügyszám: 25/2013.). Amennyiben az eszköz elmozdítható, úgy a biztonságos, szakszerű és dokumentált (Chain of Custody) leállítást követően kerülhet csak sor a műveletre, mely biztosítja, hogy a bizonyítékként felhasználandó eszköz és tartalom állandó és dokumentált felügyelet alatt álljon a büntetőeljárás teljes ideje alatt.

Az adatok kinyerésére (Aquisition) optimális esetben szakértői laboratóriumban, ellenőrzött környezetben kerül sor, de megfelelő előkészítést követően – amikor a nyomozóhatóság és a szakértő előzetesen részt vesz a művelet tervezésében – a helyszínen is megvalósítható közel azonos minőségben. Az adatkinyerés helyszínen történő lefolytatásának kulcsmomentuma az idő, melyre vonatkozóan a tervezéskor kell figyelmet fordítani (az időtervezést az eszközöknél részletezzük).

A kinyert adatok megőrzése és előkészítése a bemutatásra legalább olyan fontosságú tevékenység, mint maga az azonosítás, az összegyűjtés, vagy a kinyerés. A megőrzött digitális bizonyítékok kerülnek ugyanis a nyomozási szakaszban az ügy előadójához, akinek a megkapott adatokat értelmeznie kell, azokból következtetéseket kell tudni levonnia. Mindez nem valósulhat meg anélkül, hogy a szakértő megfelelő formátumú, megfelelő tároló médiumon adja át az adatokat, melyek integritása, hitelessége nem változhat az eljárás folyamán.

Figyelembe véve a magyarországi adottságokat, kijelenthetjük, hogy ez a szakasz az egyik legnehezebben teljesíthető valamennyi közül. A nyomozó hatóság az adathordozók és adatformátumok tekintetében is többszörös hátrányban vannak az elvárható informatikai írástudással összevetve, a felszereltséget, készségeket és tudást tekintve egyaránt. Ez azt jelenti, hogy egyes adathordozók fogadása (pl. Blu-ray lemez) nem megoldott, mert nincs olvasó eszköz, a nagy tömegű adatokat tároló merevelemezek biztonságos olvasása megfelelő mennyiségű írásvédő eszköz (részleteket lásd később) nélkül nem lehetséges, a nyomozók informatikai felkészültsége nem megfelelő a digitális bizonyítékok értékeléséhez.

Mindezen körülmények a teljes fenti módszertan szerinti folyamat eredményét kérdőjelezhetik meg, s mint ilyen azonnali hathatós beavatkozást igényel a fentiekben kiemelt pontokon a rendszer döntéshozóitól.

8.4.2 Eszközrendszer

Az előbbiekben tárgyalt módszertani részletek egyes lépéseinél alkalmazott eszközrendszer két alapvető komponensből, szoftverből és hardverből áll. Míg az összegyűjtésnél és a kinyerésnél a hardver elemekre helyeződik a hangsúly, úgy a megőrzési, elemzési és bemutatási szakaszokban a szoftverek kerülnek előtérbe.

A felhasználható hardverek magját az ún. kivonuló készletek képezik, melyek az elnevezésükből adódóan a helyszíni vizsgálatok céljaira is alkalmasak, de természetesen használhatók a laboratóriumi munka során is. Ezek a készletek több különféle célú hardverből tevődnek össze: duplikátorokból, írásvédőkből, meghajtó adapterekből, kábelekből és kábel adapterekből, tápegységekből és az ezeket működtető, illetve szolgáltatásaikat felhasználó szoftverekből. Tekintsük át az egyes komponenseket részletesen:

Forensic duplicator

A forenzikus másolat készítő a tartós tárak hiteles, bitről-bitre történő lemásolását lehetővé tevő eszköz. A hitelesség azt jelenti, hogy az elkészített másolatokról digitális ellenőrzőszámot készít a rendszer pl. MD5 vagy SHA-1 HASH algoritmus szerint, mely biztosítja, hogy a másolatban történő egy bitnyi változás is felderíthetővé válik, tekintettel arra, hogy egy bit módosulása is az újból legenerált ellenőrző szám változását okozza. A bitről-bitre történő másolás fontossága akkor nyeri el értelmét, ha tudjuk, hogy a számítógépes rendszerekből történő adattörlés elsődlegesen ún. logikai törlést jelent, vagyis az adat fizikailag nem törlődik, csak az általa elfoglalt tárterület jelzése válik felülírható státuszúvá. A bitről-bitre történő másolás esetén a későbbiekben (pl. laboratóriumi vizsgálat során) lehetőség van a törölt adatok helyreállítására (szoftveres eljárás) is. Az eszközök jellemző tulajdonsága az egy időben készíthető másolatok száma: 1:1, 1:2, esetleg 1:3; a vizsgálandó eszköz felőli interfészek típusai: USB3/PATA, SATA; az adatátvitel sebessége, mely akár 15 GB/perc is lehet a gyártó specifikációja szerint[92] tömörített formában MD5 and SHA-1 hash kódok generálása mellett. Ez utóbbi fontos szerepet játszik a korábban már említett időfelhasználás tervezésekor, mely a helyszíni vizsgálat időszükségletét méri fel az előzetesen beszerezhető, vagy becsült adatok alapján. Megjegyzendő, hogy a művelet szoftveresen is megvalósítható, ehhez számítógép és ún. klónozó szoftver szükséges, e megoldás időszükséglete jelentősen nagyobb. mint a hardveres megoldásé.

[92] https://www.guidancesoftware.com/tableau/hardware/td2u

A duplikátorok további jellemzője a tisztítási (wiping) funkció, mely a másolat céljaira használt lemezek újrahasznosítását lehetővé tevő folyamat. Ennek során a lemez felületének többszörös fizikai újraírása törénik meg, akár 25 GB/perc sebességgel (a gyártó specifikációja szerint). Ez a művelet jelentősen igénybe veheti a tároló mechanikáját, tekintettel arra, hogy a rendszert nem folyamatos, tartós írásra méretezték általában. A tisztítás során ajánlott gondoskodni a rendszer fokozott hűtéséről.

Forensic bridges

Az írásvédő eszközök a különféle csatlakozófelületű tartós tárak (tipikusan HDD, SSD) vizsgálatára alkalmasak. A készülékek hardveresen akadályozzák meg a vizsgált eszközre történő adatírást, így a digitális bizonyíték törlését, módosulását, végső soron hitelvesztését. A duplikátorokhoz hasonlóan többfajta bemeneti és kimeneti csatolófelülettel (interface) is rendelkeznek, használatukhoz azonban (a duplikátoroktól eltérően) számítógép is szükséges, mely tényezőből adódóan nagyobb időigényű az eszközzel végzett tevékenység. A tipikusan laboratóriumi vizsgálatokra alkalmas készülékek a szakértői számítógépek irányába nagy sebességű USB3, vagy eSATA felületet biztosítanak, míg a vizsgált eszközök PATA/SATA/SAS, vagy Firewire, illetve USB csatlakozó és adapter felhasználásával szinte bármilyen adatkapcsolati felületű eszközök lehetnek. A szakértői számítógépekbe beépített írásvédők közvetlenül a számítógép adatcsatornáira kapcsolódva nagyobb sebességet képesek elérni.

Ezek az eszközök a nyomozó hatóságok munkájában is megjelennek, különösen az utóbbi néhány évben, amikor az ügyek egy részében rendkívül nagy mennyiségű (terrabájt nagyságrendbe eső: ~ 200 db hagyományos DVD kapacitása) adat kerül átadásra a szakértőtől a nyomozóhatóság felé, s ennek a nagy mennyiségű adatnak a legcélszerűbb tároló médiuma a merevlemez. Az adatok vizsgálata a nyomozói oldalról csak úgy történhet meg, hogy a bizonyítékok közben nem változhatnak meg, így az írásvédők használatának a közeljövőben növekvő szerepe lesz a nyomozói oldalon is.

Az írásvédelem is megoldható szoftveres úton, ekkor azonban biztosítani (igazolni-ellenőrizni) kell az alkalmazott módszer, vagy szoftver 100%-os írásblokkoló képességét.

Adapters

A szakértő által vizsgált eszközök széles spektruma azt igényli, hogy a szakértő hasonló változatosságú eszközparkot üzemeltessen. Ennek egyik legköltséghatékonyabb megvalósítása az adapterek használata. Ezek olyan adatátviteli felület és tápellátás csatlakozó felület átalakítók, melyek lehetővé teszik, hogy a speciális eszközök pl. 1,8” PATA felületű laptop merevlemez is (írásvédelmi eszközön keresztül) a szakértői számítógéphez kapcsolható legyen.

Forensic szoftverek

A forenzikus szoftverek széles skálája és a terjedelmi korlátok miatt a következőkben csak a főbb kategóriákat fogjuk áttekinteni. Ezek közül elsőként emelendő ki az ún. ügykezelő komplex rendszerek, melyek a szakértői oldal teljes körű támogatását végzik az adatkinyeréstől az ügy releváns adatainak osztályozásán keresztül egészen a dokumentálásig. Az ügykezelő rendszerek a korábbiakban bemutatott hardver eszközökkel szoros integritásban képesek a különféle eszközökről (tablet, smart phone, tároló eszközök stb.) kinyerni az adatokat, azokat szabványos formátumban tárolni és jelentések formájában bemutatni.

E komplex rendszerek egyes képességei önálló szoftverek formájában is megjelennek, melyek közül a legfontosabbak a következők:

Imager	adatakinyerés valamely tartós tárról
Data Recovery	adat helyreállítás (törölt adatok visszaállítása)
Emai Recovery/Converter	e-mail adatbázisok helyreállítása, a tárolt levelek kinyerése
Mobil Forensic	smart phone és hagyományos mobil készülékek adatainak mentése, helyreállítása
Password Tools	jelszó feltörő alkalmazások

A felsoroltakon kívül számos részterület szerinti szoftvert sorolhatnánk fel, s mint ilyen, valamennyi a szakértői eszközrendszer részét képezi.

Amint az érzékelhető az igazságügyi informatikai szakértői eszköztár rendkívül komplex úgy hardver, mint szoftver vonatkozásban, s emellett tartalmilag alkalmasnak kell lennie a módszertani részben felsorolt követelmények teljesítésére. Ez nem könnyű feladat, tekintettel arra, hogy az eszközök jelentős része az Európai Unión kívüli területről származik, s beszerzésük jelentős költségekkel jár.

Az igazságügyi informatikai szakértői tevékenység módszertani és eszközrendszerbeli hátterének rendezése aktuális feladat nem csak a szakértők, de a rendszer paramétereit meghatározó döntéshozók számára is. Míg a szakértői oldalnak a módszertani szabványok átvételével, annak a hazai gyakorlatban történő meghonosításával kell foglalkoznia:

- szabványok beszerzése (Magyar Igazságügyi Szakértői Kamara Informatikai és Hírközlési Szakmai Tagozata) és honosítása,
- szakmai továbbképzések,

addig a döntéshozói oldalnak megoldást kell találnia a szakértői életpályát érintő kérdésekre, nevezetesen:

- az igazságügyi informatikai szakértők anyagi hátterének rendezése (szakértői díjak mértéke)
- a szakértői eszközpark (hardver, szoftver) állandó színvonalon tartásának támogatás (law enforcement kedvezmények igénybevételében történő támogatás)
- a szakértői munka eredményét felhasználó szervezetek műszaki és készségbeli felkészítése a digitális bizonyítékok elemzésére és értékelésre

E legfontosabb kihívások és az arra adandó (fentiekben javasolt) válaszok döntően befolyásolják a büntetőeljárásban keletkező igazságügyi informatikai szakértői vélemények minőségének és felhasználhatóságának alakulását mind a szakértők, mint a nyomozó hatóságok oldaláról.

8.5 A digitális bizonyítékok elemzése

A digitális bizonyítékok kinyerését követően a szakértő átadja a bizonyítékokat a nyomozó hatóság munkatársainak, akik elemzik, értékelik és felhasználják munkájuk során. A digitális bizonyítékok elemzéséhez megfelelő informatikai ismeretre van szükség, mely a nyomozó hatóság munkatársainál gyakran nem áll rendelkezésre. Az igazságügyi informatikai szakértő a büntetőeljárás egyetlen olyan szereplője, aki képes és jogosult segíteni ezen a helyzeten. Az írásban esettanulmányokon keresztül kerül bemutatásra az elemzés folyamata, melynek során az igazságügyi informatikai szakértő és a nyomozó hatóság képviselője szorosan együttműködik. Látni fogjuk az együttműködés kereteit és határait, illetve a szerző javaslatot tesz a bemutatott helyzet kezelésére is.

8.5.1 Bizonyíték elemzés - egyéni, vagy csapamunka?

A bizonyítékok elemzése és előzetes értékelése a büntetőeljárás nyomozási szakaszában az ügyész és a nyomozást végző hatóság munkatársainak elsődleges feladata és egyben kötelezettsége is. Az informatikai rendszereket is érintő cselekmények esetén megjelenő új típusú, digitális bizonyítékok azonban a korábbiaktól eltérő elsősorban műszaki és mérnöki tudományokat érintő kihívásokat jelentenek a nyomozók számára. Jelen tanulmányban arra keresem a választ, hogy egyedül marad-e ebben a folyamatban a nyomozást végző (nyomozó, ügyész stb.), kaphat-e segítséget, azt milyen formában és kitől?

A digitális bizonyítékok szakértői előkészítése, elemzése

A digitális bizonyítékok kinyerésének és feldolgozásának általános esetében az igazságügyi informatikai szakértő a nyomozóhatóság által lefoglalt eszközöket (tipikusan számítógépek) vizsgálja saját laboratóriumában, esetleg házkutatás alkalmával a helyszínen.

A digitális tartalmak rögzítésének kiválasztása nem „csupán" szakértői, de nyomozástaktikai feladat is. A lehetőségek széles köréből választhat a kirendelő: a tartalom duplikálása történjen forenzikus másolatként, vagy teljes tartalmi másolat, fájltípusokra történő szűrést követő tartalmi másolat, kulcsszavas keresés eredményének másolata, hogy csak a leggyakoribbakat említsük. A gyakorlat azt mutatja, hogy a bizonyítékok megszerzésének e mozzanata gyakran a nyomozást végző szervezetben kialakult hagyományok alapján történik, nem kötődik az ügy specifikus körülményeihez.

Példa: egy adott eljárás kiterjesztésére irányuló nyomozati cselekmény során nem szükséges az adathordozók azonnali teljes körű duplikálása, megfelelő eljárás a releváns fájltípusokon (többnyire dokumentumok, táblázatok, adatbázisok) belüli kulcsszavas keresés helyszíni eredményeinek azonnali kiértékelése és a releváns adatokat tartalmazó adathordozók lefoglalása a későbbi vizsgálat céljaira.

Amennyiben törölt adatok kinyerésére is szükség van, úgy indokolt lehet a helyszíni, vagy laboratóriumi duplikálás (hétköznapi kifejezéssel klónozás), mely révén a későbbi adat helyreállítás is lehetséges.

Mivel a bemutatott két megoldás eltérő eszköz és időszükségletű, elengedhetetlen, hogy a nyomozó hatóság munkatársai tisztában legyenek az egyes műveletek tartalmi jelentésével és erőforrás igényével. Egy helyszíni vizsgálat (házkutatás) előtt például a művelet vezetőjének döntést kell hoznia a következő kérdésekben:

- rendelkezésre állnak-e a helyszíni vizsgálathoz szükséges fizikai és személyi feltételei, illetve ezek pótolhatók-e
  - adatmentéshez szükséges tárolókapacitás,
  - hiteles mentést támogató eszközök (forensic bridge, duplicator stb.),
  - számítógépes hálózat felderítésének hardver és szoftver komponensei,
  - szakértői csoport létszáma.
- a vizsgálat (akár helyszíni, akár laboratóriumi) érint-e az eljárást elszenvedőn kívül más természetes vagy jogi személyt,
  - a helyszíni vizsgálatból/lefoglalásból eredő szolgáltatás leállás, vagy lassulás következményei,

~ harmadik személy vagy szervezet adatainak ideiglenes elérhetetlensége (pl. könyvelő irodákban történő vizsgálat esetén)[93]

Összefoglalva tehát, az előkészítés különösen a digitális bizonyítékok mennyiségét és az utófeldolgozás mértékét is meghatározza, ezáltal közvetlenül kihat a bűnügyi költségekre is.

Ez utóbbi tényező jól megérthető a helyszíni duplikálás és a laboratóriumi célzott elemzés összevetésével. A jelenlegi tárolókapacitások egy-egy számítógép esetén megközelítik vagy túllépik a terrabájtos (TB) nagyságrendet (ez kb. 220 db DVD lemez tárkapacitásának felel meg). A forenzikus duplikátor eszközök adatátviteli sebessége 15 GB percenként, melyből 70 perc/TB ideális duplikálási sebesség kalkulálható. Több eszköz és élő rendszer esetén ez a megoldás jelentős időigényű, illetve a rendszer leállítása nélkül nem végezhető el.

A laboratóriumi célzott elemzés során a szakértői munkaidő egy része kiváltható gépidővel, amikor a szakértő személyes jelenléte nélkül is lefolytatható a fájltípusra történő szűrés (kigyűjtés), a szűrt adatok másolása, majd a kulcsszavas keresés a fájlok tartalmában.

A digitális bizonyítékok néhány típusa az előzőektől eltérően további szakértői munkát, elő feldolgozást igényel. Ezek közül kiemelendők az elektronikus levelezés adatbázisai (Outlook .PST, Outlook Express .DBX, Thunderbird, webes levelező rendszerek: Gmail, Freemail stb.), melyek közvetlenül nem, csak szakértői előkészítést követően vizsgálhatók. A szakértő ekkor nem csupán kinyeri, esetleg törölt állapotból visszaállítja az egyes elektronikus levelek tartalmát, de hozzá kapcsolódó csatolmányt is rendelkezésre bocsátja, többnyire időrendi sorrendben. Amennyiben rendelkezésre állnak kereső kifejezések (pl. természetes vagy jogi személyek nevei, elnevezései), akkor ez a művelet is az előkészítés körébe tartozhat.

Hasonló tevékenységet végez a szakértő a könyvelési adatbázisok esetén, amikor az adatokat a kérdéses program eredeti nyomatformátumában kell a nyomozó hatóság rendelkezésére bocsátani, tekintettel arra, hogy a könyvszakértői, vagy egyéb gazdasági tárgyú vizsgálatokat végző munkatársai, illetve szakértők ilyen adatokból tudnak dolgozni.

Itt érkeztünk el ahhoz a mozzanathoz, mely a jelen tanulmány elkészítését indukálta: nevezetesen a digitális bizonyítékok elemezhetők-e a nyomozó hatóság munkatársai által önállóan az igazságügyi informatikai szakértő közreműködése (támogatása) nélkül. A lehetséges választ a tanulmány záró fejezetében olvashatjuk.

[93] MÁTÉ István Zsolt: A házkutatás – az igazságügyi informatikai szakértő a büntetőeljárásban In. Tavaszi Szél 2014 Konferencia konferenciakötet, Debrecen, Debreceni Egyetem, 2014.

8.5.2 A nyomozó hatóság és a szakértő együttműködése

A digitális bizonyítékok nyomozó hatóság munkatársai által történő elemzése néhány alapvető tényezőtől függ: egyrészt a vizsgálatot végző munkatárs informatikai kompetenciáitól, a rendelkezésre álló informatikai felszereléstől (minőségi, tartalmi és használhatósági szempontok), illetve nem utolsó sorban a vizsgálandó digitális bizonyíték mennyiségétől (értsd: tárolókapacitás).

A legkönnyebben az utolsó szempont közelíthető meg: a nyomozó hatóság számára rendelkezésére álló vizsgálati idő alatt az esetenként (nagyobb ügyekben) 1-10 TB kapacitást is elérő digitális bizonyítékok elemzésére nincs elegendő idő.

Ezt a körülményt súlyosbítja a technikai felszereltségre vonatkozó adat: a digitális bizonyítékokkal kapcsolatba kerülő előadók számítógépe gyakran nem alkalmas műszakilag a feladat elvégzésére, nem rendelkeznek megfelelő kiegészítő eszközökkel (merevlemez elemzéshez szükséges írásvédő stb.), illetve a számítógép használatot korlátozó biztonsági intézkedések (helyi és hálózati házirendek) gyakran kizárják a digitális tartalommal történő munkavégzést.

Végül, de nem utolsó sorban az elemzést végző nyomozók, előadók informatikai készségei és ismerete gyakran nem elegendő még a tartalmak megkülönböztetéséhez sem, azok elemzéséhez, esetleg összetettebb (pl. adatbányászati) művelet elvégzésére pedig egyáltalán nem.

A bemutatott tények következménye: az igazságügyi informatikai szakértői munkával kinyert és feldolgozott tartalom nem hasznosul a büntetőeljárásban az akadályozó körülmények miatt. Ez a korábban már említett gazdasági (bűnügyi költségek) vonatkozásban azt jelenti, hogy a befektetett pénz (pl. szakértői munkadíj) nem térül meg az eljárás sikerességének formájában.

Amennyiben figyelembe vesszük azt a tényt, miszerint a digitális bizonyítékok számos ügytípusban, egyre nagyobb mértékben jelennek meg a büntetőeljárásban, nem késlekedhetünk a válaszok megkeresésével és megadásával.

Több megoldás is elképzelhető, ezek közül a két végpont bemutatására koncentrálunk: a nyomozó hatóság munkatársait alapos szakmai képzésnek kell alávetni és a rendelkezésre álló technikát az aktuális legmagasabb szintre kell hozni (ez rendkívül költségigényes és valószínűleg személyi ellenállásba is ütközik az állomány részéről). A megoldás másik módja szerint az igazságügyi informatikai szakértők tudását és eszközrendszerét felhasználva szervezési, ha szükséges eljárásrendbeli módosításokkal bevonni őket az elemzési munkába (kevésbé költséges, de nagyobb szervezés igényű, szükséges a szakértők eszközrendszerének állandó frissítése).

A felvetett probléma időszerűsége nem lehet kétséges, ha a növekvő mennyiségű digitális bizonyítékokat és az egyre komplexebbé váló ügyeket tekintjük. Az elkövetési értékek növekedésével párhuzamosan egyre fontosabbá válik, hogy a bűnüldözés ne

csak eredményes, hanem költséghatékony is legyen. E két kiemelt szempontot ajánlja a szerző – akár vitaindítóként is – azok figyelmébe, akik a büntetőeljárás szereplőjeként, vagy a jogszabályi környezet előkészítőjeként megoldásokat keresnek a jelen és a közeljövő kihívásaira.

Az előzőek mellett a bevezetőben feltett kérdésre is megadható a válasz, mely egyértelmű és határozott: az igazságügyi informatikai szakértők a nyomozást végzők jogszabályokban is feljogosított segítői, akik a szakvélemény adáson túlmenően is képesek segíteni a hatóságok tényfeltáró munkáját, akár tanácsadással, akár az egyes ügytípusokra vonatkozó szakmai ismeretek képzés során történő átadásával. Mindezek megvalósításához természetesen nélkülözhetetlen a nyomozó hatóságok vezetőinek egyetértése és támogatása is, melynek megszerzéséhez – a lehetőségek bemutatása révén – remélhetően jelen tanulmány is hozzájárul.

9 Az igazságügyi informatikai szakértői munka ügytípusai

9.1 A házkutatás, mint a szakértői munka esszenciája

A számítástechnikai rendszerek házkutatás során történő átvizsgálásának feladatát a magyarországi gyakorlatban az igazságügyi informatikai szakértők végzik a Be. és más jogszabályok felhatalmazása alapján, leggyakrabban a nyomozó hatóság kirendelése szerint. Munkájuk sikerét – figyelembe véve az ügyek növekvő komplexitását és az ügyekben szereplő eszközök növekvő mennyiségét – a megfelelő előkészítés és koordináció alapozhatja meg.

A büntetőeljárásról szóló 1998. évi XIX. törvény (Be.) 149. §-a (a jármű mellett) nevesíti a számítástechnikai rendszert, mint a házkutatás során átvizsgálandó dolgot. Ez a kiemelés mindkét esetben (jármű és számítástechnikai rendszer) arra utal, hogy elterjedtségük és valószínűsíthető érintettségük a többi tárgyhoz, dologhoz képest jelentős, s ezért a házkutatás kiemelt objektumaiként tekinthetők.

Ezen objektumok vizsgálatához a Be. megfogalmazásában „… a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges…”, ezért igazságügyi informatikai szakértők segítik a nyomozó hatóság munkáját.

A házkutatás során – előzetes feltevésünk szerint – a büntetőeljárásban megszokott gyakorlathoz képest szorosabban működnek együtt a résztvevők (kiemelten a nyomozó hatóság munkatársai és a szakértők) az eljárási cselekmény előkészítése és lefolytatása során egyaránt. Ez a közös munka igényli a legalapvetőbb tények és feladatok tisztázását, valamint olyan eljárási szabályok és módszerek kialakítását, amelyek a kriminalisztikai és informatikai szempontokat megfelelő szinten összehangolják.

9.1.1 A házkutatás előkészítése

A büntetőeljárás nyomozási szakaszában az ügyészség és a nyomozó hatóság a bűncselekmény elkövetőjének kézre kerítése érdekében végzi az egyes nyomozati cselekményeket. Ezek közül a házkutatás általában jól elkülöníthető mind térben, mind időben a többi cselekménytől, tartalmi elemei az egyszerűtől a komplexig terjedő skálán számos értéket felvehetnek. Terjedelmi okokból most három típusra korlátozzuk, pontosabban koncentráljuk a lehetséges változatokat, melyek a következők:

Egyszerű: egy helyszín, egy szakértő, 2-3 nyomozó, <10 eszköz,

Átlagos: több helyszín, egy szakértő, 5-10 nyomozó, >10 eszköz,

Komplex: több helyszín, több szakértő, >100 nyomozó, >>10 eszköz.

Az egyes típusok közötti határok gyakran elmosódnak, a fő jellegzetességek (kevésbé karakteresen) feltűnhetnek valamennyi változatban. A tipizálás e körülményektől függetlenül lehetővé teszi a nyomozati és szakértői munka tervezhetőségét, s ez által növeli az eredményességet is.

Közös jellemzők

A házkutatással kapcsolatos két legalapvetőbb információ a helyszín és az időpont. Ennek ellenére az esetek döntő többségében ezt a két adatot nem osztja meg a nyomozóhatóság munkatársa a szakértővel, amikor előzetesen egyezteti a helyszíni vizsgálaton történő részvételt. A nyomozástaktikai indokokat szem előtt tartva a szakértőnek támpontot nyújthat a következő körülmények előzetes tisztázása:

- földrajzi elhelyezkedés település, vagy járás pontossággal megadva,
- a helyszín jellegének megadása figyelemmel az infrastruktúrára (pl. áramellátás),
- az eszközök várható típusának és mennyiségének megadása,
- a művelet elsődleges céljának specifikálása[94], mely lehet:
    - logikai kutatás, például dokumentumok célzott megtalálása, adatbázis mentése, levelezés átvizsgálás, szoftver jogszerű használatának feltárása stb.),
    - fizikai kutatás, adathordozók, hardver komponensek megtalálása, illetve
    - kettős célú (logikai és fizikai) kutatás.

A felsorolt paraméterek ismertében a szakértő (elsősorban korábbi tapasztalatai alapján) meg tudja becsülni az eljárási cselekmény eszköz és szakember igényét.

Egyszerű helyszín

Az egy helyszínen egy szakértő munkáját igénylő feladatok gyakran kimerülnek az informatikai eszközök szakszerű lefoglalásának támogatásában, ami nem jelent mást, mint:

- az eszközök szakszerű leválasztása az elektromos és adatátviteli hálózatokról,
- a releváns eszköztípusok kiválasztása (vö. monitor vs. all-in-one PC)
- nem tipikus eszközök azonosítása (banki token vs. pendrive, netPC vs. router stb.)
- az eszközök szakszerű lezárása és csomagolása.

A feladat gyakran 1-2 óra időtartamú, eszközigénye minimális, a szakértőtől a bizonyítékok kezelésére vonatkozó ismereteket és gyakorlati tapasztalatot igényel.

---

[94] FINSZTER Géza: A kriminalisztika elmélete és a praxis a büntetőeljárási reform tükrében. Budapest, 2005-2007. p.132.

Az egyszerű helyszíneken történő házkutatás gyakran szakértő, vagy szaktanácsadó jelenléte nélkül történik, s a lefoglalás szakszerűsége az eljárást vezető és közreműködők informatikai ismeretén és erre vonatkozó tapasztalatán múlik[95].

Átlagos helyszín

Az ügyek többségében átlagos helyszínnel kerül kapcsolatba a szakértő. Ezeknél az eseteknél nem ritkán a gazdasági bűncselekménnyel kapcsolatos nyomozás zajlik, a gyanúsítottak lakhelye és/vagy munkahelye a házkutatás helyszíne.

Különösen több helyszín esetén van szerepe az előkészítésnek, melynek során szükséges tisztázni a következő körülményeket az egyszerű helyszínnél felsoroltakon felül:

- a művelet célja (logikai, fizikai, vagy kettős célú vizsgálat),
- mikor ismerheti meg a szakértő a kezdési időpontot és helyszínt,
- lesz-e előzetes eligazítás, egyeztetés (időpont, helyszín),
- több helyszín esetén a szakértő mozgását ki biztosítja (nyomozó hatóság, szakértő),
- az egyes helyszíneken ki az eljárást vezető személy.

Az átlagos helyszínen végzett szakértői munka jellemzően logikai átvizsgálást is tartalmaz. Bár a nyomozó hatóság elsődleges célja a releváns bizonyítékok lehető leggyorsabb (azonnali) beszerzése, a szakértő elsődleges feladatai közé tartozik annak eldöntése, hogy ez a helyszínen elvégezhető e (különösen az időfaktor miatt), vagy az érintett és előzetesen átvizsgált eszközök lefoglalását javasolja-e.

Komplex helyszín

A komplex helyszínek a szakértői gyakorlatban ritkán előforduló (évi 1-2 eset) vizsgálati terepek. Az ügyekben rendszerint rendkívül magas elkövetési érték (>1 Mrd HUF) jelenik meg, mely alapján az egy időben akár száznál is több helyszínen, több szakértő, vagy szakértői csoport dolgozhat jelentős nyomozói létszám mellett. Mivel az ügyek mennyisége, s ebből adódóan a szakértők ez irányú gyakorlata is kicsi, illetve kevés, szükséges a megfelelő módszertani háttér kimunkálása a szakértői oldalról és annak bemutatása, egyeztetése a nyomozói oldallal.

A bemutatott körülmények miatt indokolt, hogy jelen tanulmány is erre a komplex helyszínen történő házkutatás során végzett igazságügyi informatikai szakértői vizsgálatra fókuszáljon.

A művelet megkezdését megelőzően mindenképpen szükséges az előzetes egyeztetés, illetve a vizsgálatot közvetlenül megelőző eligazításon történő részvétel a szakértő(k)

[95] ILLÉSI Zsolt: Számítógép hálózatok krimináltechnikai vizsgálata. in Hadmérnök 2009 december pp. 170-183 Budapest, 2009. Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar. pp.181-182.

részéről. Az átlagos helyszínnél felsoroltakon kívül a következő tényezők tisztázása szükséges:

- az adott helyszínen, helyszíneken várható-e számítógép-hálózatok közötti kommunikációs kapcsolatok (pl. internet szolgáltatóknál végzett vizsgálat),
- a vizsgálat során leállítható-e a hardver infrastruktúra egésze, vagy része,
- a vizsgálatból adódóan lassulhat-e a számítógéprendszer működése,
- várhatóan történik-e házkutatást megelőzően erőszakos behatolás, mely a számítógép rendszer működését befolyásolná (pl. megfigyelő rendszer),
- a számítógép rendszer működését felügyelő személyzet várható létszáma és elhelyezkedése.

A felsoroltakon kívül még számos tényező befolyásolhatja a komplex helyszíneken történő vizsgálatot, melyekre a következőkben térek ki.

9.1.2 A házkutatás megkezdése

A házkutatás során végzett vizsgálatban résztvevő szakértő a helyszíni eljárásvezető irányítása mellett végzi munkáját, tőle kapja kézhez a – gyakran a műveletet közvetlenül megelőzően – a kirendelő határozatot, melyet az eljárást szenvedőnek, vagy jogi képviselőjének bemutat az igazságügyi szakértői státuszt igazoló fényképes szakértői igazolvány mellett.

Mivel a kirendelő határozat részletesen tartalmazza azokat a kérdéseket, melyre a szakértőnek a vizsgálat során választ kell adnia, a kirendelő határozat részletes megismerése (esetleg lemásolása az eljárást szenvedő részéről) nem megengedhető. Ugyanez vonatkozik a szakértő által önállóan végzett szakértői szemlére is.

A vizsgálat megkezdését megelőzi a helyszínre történő kivonulás, illetve a vizsgálat konkrét helyére történő bejutás. Számítógép rendszerek vizsgálatakor mindkét esetben az időtényező minimalizálása a legfontosabb, amint az a következőkben láthatjuk.

9.1.3 Helyszíni szakértői vizsgálat szabályai

A helyszíni vizsgálat első lépésében a szakértőnek meg kell határoznia a várható bizonyítékok időérzékenységi sorrendjét (Order of Volatility), s a vizsgálatot e sorrend alapján haladéktalanul meg kell kezdenie. A művelet előzetes egyeztetése során ki kell térni a várható eszközök és tartalmak időérzékenységére és előzetes sorrend felállítása is szükséges lehet, amint azt a korábbiakban idézett példa is mutatja[96]:

1. Registers and Cache, processzor regisztereinek és a gyorsítótárak tartalma
2. Routing Tables, számítógépes hálózati útvonalválasztó útvonaltáblája

[96] BRAID im. p.9

3. Arp Cache, címfeloldási protokoll gyorsítótára (az IP címek és a fizikai címek megfeleltető táblázata);

4. Process Table, feladatokat tartalmazó tábla tartalma;

5. Kernel Statistics and Modules, operációs rendszer rendszermag-statisztika és rendszermag-modulok tartalma;

6. Main Memory, operatív tár tartalma;

7. Temporary File Systems, ideiglenes fájlrendszer tartalma;

8. Secondary Memory, másodlagos memória tartalma;

9. Router Configuration, útvonalválasztó eszközök beállításai;

10. Network Topology, számítógépes hálózati összeköttetés-rendszer.

Amennyiben nem indokolt a bevetési egység általi bejutás a helyszínre, a késedelem lehetőséget ad az eljárást elszenvedőnek a bizonyítékok módosítására.

A fentiek mellett különös gondot kell fordítani az élő (on-line) rendszerek megfelelő felmérésére és kezelésére, különösen a felhőszolgáltatások területén. A házkutatás megfelelő időzítésével elérhető, hogy a vizsgálat alá vont felhasználók a munkájukhoz szükséges felhőszolgáltatásokba bejelentkezve végezzék tevékenységüket, melyek ez által közvetlenül elérhetővé válnak akár a mentés, akár a távoli rendszerek feltérképezése tekintetében.

9.1.4 Esettanulmányok

Esettanulmány (25/2013. szakértői ügyszám)

Az 1978. évi IV. törvény (régi Btk.) 310. § (1) bekezdés a) pontjában meghatározott költségvetési csalás bűntett elkövetésének gyanúja miatt indult nyomozás során két fős szakértői csoport és húsz fő nyomozó jelent meg a házkutatás helyszínén, mely egy 24/24 munkarendű irodaház volt biztonsági szolgálattal. A helyszínre történő bejutás és szakértői vizsgálat megkezdése a körülmények miatt két órát vettek igénybe, holott a vizsgálatot egyeztetés előzte meg a szakértői csoport és a nyomozócsoport részéről.

Esettanulmány (27/2013. szakértői ügyszám)

A régi Btk. 310. § (1) bekezdésében meghatározott költségvetési csalás bűntett elkövetésének gyanúja miatt indult nyomozás során öt fős szakértői csoport és több mint 150 fő nyomozó jelent meg több házkutatási helyszínen. A fő helyszín több cég által nappali munkarendben használt irodaház volt 9:00 órai munkakezdéssel. A szakértők és a nyomozók a munkakezdést megelőzően egy órával

a helyszínen voltak, s az első munkavállaló megérkezését követően megkezdődhetett a helyszín szakértői biztosítása.

9.1.5 Általános vizsgálati irányelvek

A házkutatás során nem csak a szakértőnek, de valamennyi résztvevőnek (beleértve az eljárást elszenvedőt is) be kell tartania a "Preserve everything but change nothing", azaz őrizz meg mindent, ne változtass semmin alapelvet. Ezt akár kényszerítő intézkedéssel is kikényszerítheti az eljárásvezető, különösen akkor, ha adat merül fel a bizonyítékok befolyásolására, például vizsgálat alá vont rendszerek engedély nélküli lekapcsolása, távoli hozzáférés biztosítása.

A teljes vizsgálat során, majd azt követően is biztosítani kell a felügyeleti lánc (Chain of Custody) megszakítatlanságát, ami leegyszerűsítve a kinyert bizonyítékok dokumentált mozgását jelenti.

Esettanulmány (08/2017. szakértői ügyszám)

> Az új Btk. 396. § (1) bekezdésének a) pontjába ütköző, és az (5) bekezdés a) pontja szerint minősülő költségvetési csalás bűntett elkövetésének gyanúja miatt indult nyomozásban több helyszínen történt házkutatás, három fő szakértő részvételével. Az egyik helyszínen – ahol nem volt szakértői jelenlét – az eljárás alá vont személy a helyszínen használt asztali számítógépet öltözőszekrényébe elrejtette, majd a későbbiekben azt saját lakóhelyére szállította.

A helyszíni vizsgálat során szükséges betartani valamely szakértői módszertan lépéseit, ezzel szabályozva és egyben ellenőrizve is a munkafolyamatot. A számos ajánlás közül a CIARDHUÁIN által ajánlott kiterjesztett módszertan vonatkozó lépéseit javasolt követni[97]:

5. A digitális bizonyíték felkutatása és azonosítása (Search for and identify evidence)
6. A digitális bizonyíték összegyűjtése (Collection of evidence)
7. A digitális bizonyíték szállítása (Transport of evidence)
8. A digitális bizonyíték tárolása (Storage of evidence)

A vizsgálat során keletkeznek olyan döntési pontok, melyek feloldása a szakértő(k) és az eljárásvezető együttműködését igénylik, a következőkben ezeket tekintjük át röviden.

[97] CIARDHUÁIN i.m. pp. 5-8.

9.1.5.1 Helyszínen nem vizsgálható eszközök, tartalmak

A megfelelő előkészítés ellenére a szakértői és nyomozócsoport kerülhet olyan helyzetbe, melyet azonnali döntéssel kell megoldani. Ezek közé tartozik egy adott eszköz, vagy rendszer helyszíni, illetve laboratóriumi vizsgálata közötti választás. A döntést megelőzően mérlegelni kell a következőket:

- rendelkezésre állnak-e a helyszíni vizsgálathoz szükséges fizikai és személyi feltételek, illetve ezek pótolhatók-e
  - adatmentéshez szükséges tárolókapacitás,
  - hiteles mentést támogató eszközök (forensic bridge, duplicator stb.),
  - számítógépes hálózat felderítésének hardver és szoftver komponensei,
  - szakértői csoport létszáma.
- a vizsgálat (akár helyszíni, akár laboratóriumi) érint-e az eljárást elszenvedőn kívül más természetes vagy jogi személyt,
  - a helyszíni vizsgálatból/lefoglalásból eredő szolgáltatás leállás, vagy lassulás következményei,
  - harmadik személy vagy szervezet adatainak ideiglenes elérhetetlensége (pl. könyvelő irodákban történő vizsgálat esetén)

A döntés a műveletet központilag irányító parancsnok feladata, ehhez a szakértőnek minden lehetséges műszaki információt meg kell adnia.

9.1.6 Szakértő részvétele kihallgatáson

A házkutatások során foganatosított kihallgatások egy részénél informatikai szakmai kérdések is felmerülhetnek, mely estben szakértői támogatás is szükséges a kihallgatást végző nyomozó számára. A szakértő kihallgatáson történő részvételét már az előkészítés során a szakértőt kirendelő határozatban jelezni kell, illetve a kihallgatott személlyel a kihallgatást megelőzően közölni kell.

A szakértő feladata a kihallgatott személy által előadott műszaki tartalom közérthető nyelvre történő fordítása, valamint az ügy szempontjából releváns kérdések megfogalmazása lehet.

ESTET TANULMÁNY[98]

A Nemzeti Adó- és Vámhivatal Bűnügyi Főigazgatóság Központi Nyomozó Főosztály XXX osztály nyomozást folytatott az új Btk. 396. § (1) bekezdés a) pontjába ütköző és az (5) bekezdés a) pontja szerint minősülő költségvetési csalás bűntett és más bűncselekmények elkövetésének gyanúja miatt ismeretlen tettes ellen folyamatban lévő büntetőügyben.

Az eljárás során igazságügyi informatikai szakértő kirendelésére került sor, tekintettel arra, hogy XXX XXX tanúkihallgatása során különleges szakértelmet igénylő személy jelenléte szükséges és indokolt.

Az igazságügyi informatikai szakértő feladata a következő volt:

> *„A tanúkihallgatás alkalmával a kirendelt szakértő feladata, hogy szakkérdéseket tegyen fel, illetve a tanúkihallgatást követően a tanú által elmondottakat vesse össze a XXX által használt informatikai rendszerekkel és a korábban az ügyben készített szakvéleményeivel."*[99]

A tanúkihallgatás során a szakértővel történt előzetes egyeztetést követően feltett kérdések fő típusai a következők voltak:

Szakmai végzettségre vonatkozó informatikai szakkérdések

> „**TANÚ:** Kérdésre elmondom, hogy informatikus vagyok, de a főiskolát nem végeztem el, egy szemeszter után ott hagytam. Középfokú végzettséggel rendelkezem. Érettségi után elvégeztem az ECDL tanfolyamot, ami felsőfokú képesítést adott."

Válasz szakértői értékelése

[98] 11/2017 szakértői ügyszám, az idézetek a szakértői vélemény szövegéből származnak a jogszabályi előírásoknak megfelelő anonimizálás mellett

[99] 60100/XXX/20XX. bü. sz. ügy kirendelő határozatának részlete (11/2017 szakértői ügyszám)

„Az ECDL[100] (European Computer Driving License) képzés nem ad felsőfokú végzettséget. A képzést követően letehető ECDL vizsga nemzetközi, belépő szintű (entry level), vagy alapszintű (base level) tudásról szóló igazolást adott a kérdéses időszakban. Az ECDL vizsga 1997-től volt elérhető Magyarországon a Neumann János Számítógép-tudományi Társaságon (mint licensz tulajdonos) keresztül."

Alkalmazott informatikai biztonsági szabványokkal kapcsolatos kérdések:

„Volt-e rendszeres éves felülvizsgálat egyes tanúsítási rendszerek esetén? Volt-e eltérés, vagy tanúsítvány visszavonás ezeknél az ellenőrzéseknél? Tud-e arról, hogy az információbiztonsági szabályzatot megszegték volna, amíg Ön volt felelős ebben a témakörben? Milyen mértékű volt a szabályszegés és mire vonatkozott?"

A kérdés annak a ténynek a vizsgálatára vonatkozott, mi szerint az információbiztonsági tanúsítás megszerzésében történt-e harmadik személy tényleges közreműködése, vagy nem.

„**TANÚ**: ISO-nál kétévente van tanúsítvány megújítás és követő újítás volt évente, emlékeim szerint a NATO-val nem foglalkoztunk a minősítés megszerzését követően. Nincs tudomásom arról, hogy bármelyiket visszavonták volna, de a NATO-ról nem tudok nyilatkozni, mert nincs róla információm. XXX XXX volt, aki azzal foglalkozott azzal, hogy az ISO-nak megfeleljünk, mert az ISO minősítés megszerzésére is volt felkészülés, amit egy személy vagy cég végzett, de nevet nem tudok hozzá mondani. Az ISO minősítés megszerzéséhez segítséget vett a cég igénybe. Úgy tudom, hogy nem volt szabályszegés."

Válasz értékelése:

„A minőségbiztosítás, minőségirányítás területén[101] szokásos eljárás szerint a tanúsításra történő felkészítést végző szervezet és annak munkatársai (ez a feladat jellemzően több minőségbiztosítási szakember munkáját jelenti) részt vesznek a minőségbiztosítási, minőségirányítási rendszer fenntartásának, megújításának folyamatában is. A rendszer kiépítésekor szerzett ismerek így a fenntartás során hasznosulnak, elmélyülnek a támogató szervezet munkatársaiban.

A válaszban említett szakmai team jelenléte arra utal, hogy a tanúsításra történő felkészítést külső szervezet végezte. A felkészítéssel kapcsolatosan nem merült fel adat arra vonatkozóan, hogy abban XXX XXX részt vett volna."

[100] Szakértő 1997-2013 időszakban ECDL vizsgáztatóként tevékenykedett

[101] Szakértő rendelkezik Minőségbiztosítási felülvizsgáló és tanúsító szakképesítéssel (OKJ 53 5401 05), valamint Vállalati Auditor (TÜV Rheinland Akadémia) oklevéllel

Az informatikai vonatkozású szabványokra vonatkozó kérdések esetén a szakértő részéről szükséges a minőségbiztosításban és minőségirányításban szerzett ismeretek és készségek megléte, mely alapján a témakörre vonatkozó válaszok szakszerű értékelése megtörténhet. Az elméleti tudás mellett a gyakorlati szempontok is fontosak, hiszen ez alapján szűrhető ki a tanúvallomásokból a gyakorlati minőségbiztosításban nem használatos életszerűtlen mozzanat, mely a nyomozók számára fontos információt nyújthat.

Szoftverfejlesztés gyakorlati megvalósításával kapcsolatos kérdések:

> „A tanúsítási rendszerekkel (szabványokkal) összeegyeztethető-e az anonim hozzáférés a fejlesztési adatokhoz? Történt-e anonim hozzáférés a fejlesztési adatokhoz, forráskódokhoz?"
>
> „**TANÚ**: Nem, nem egyeztethető össze. Nem. Ismereteim szerint nem történt."

Válasz értékelése:

> „A kérdés érinti a bizalmasság, titkosság, valamint az információbiztonság fogalmát, mely az MSZ ISO/IEC 27001:2006 szerint:
>
> «3.3. bizalmasság, titkosság (confidentiality)
>
> Olyan tulajdonság, amely biztosítja, hogy az információt jogosulatlan egyének, entitások vagy folyamatok számára nem teszik hozzáférhetővé, és nem hozzák azok tudomására.
>
> [ISO/IEC 13335-1:2004]
>
> 3.4. információbiztonság (information security)
>
> Az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá, egyéb tulajdonságok, mint a hitelesség, a számonkérhetőség, a letagadhatatlanság és a megbízhatóság, szintén ide tartozhatnak.
>
> [ISO/IEC 17799:2005]»[102]

[102] Magyar Szabványügyi Testület: MSZ ISO/IEC 27001:2006. p.22.

Az informatikai biztonság szabályozása az „Információbiztonsági Szabályzat" című dokumentumban történt meg a vizsgált időszakban, mely legalább az alábbi változáson ment át:

Kiadás adatai Dátum	Verzió	Megváltozott fejezetek / a változások oka
2009.09.10.	1.	Első kiadás
2009.09.16	2.	Tanúsító audit I. szakaszának auditori észrevételei alapján
2010.03.23.	3.	Vezetőségi átvilágítás döntések átvezetése
2011.11.15.	4.	Aktualizálás
2012.09.05.	5.	Formai változások, egységesítés a többi szabályzóval

A válasz megfelel a hatályos szabályozásnak."

A kérdés tisztázásával kizárhatóvá vált az ügyben érintett informatikai fejlesztés egy mozzanata, mely a nyomozás során korábban begyűjtött adatok szerint anonim VPN hozzáférésen keresztül történt, nem azonosított felhasználókkal, a fejlesztő cég belső fejlesztési környezetére kapcsolódva.

A tanúkihallgatáson a szakértő közreműködésével beszerzett válaszok (az idézett kérdéstípusok mindegyike esetén több kérdés/válasz együttes értékelése történt meg) alapján az ügyben több tényszerű megállapítás is történt:

„A tanúkihallgatás során Tanú részéről tett nyilatkozatok egy része nem egyezett a korábbi vizsgálatok és tanúkihallgatások során beszerzett információkkal, valamint az általuk megalapozott következtetésekkel a következő területeken:

MINŐSÉGBIZTOSÍTÁS

A XXX Kft. által fejlesztett szoftverek önálló, XXX Kft. által végzett minőségbiztosítási tevékenységgel azonos, vagy azt megközelítő minőségű[103], minőségbiztosítási. vagy szoftver minőség ellenőrzési, vagy szoftver tesztelési feladatokra XXX XXX-nak sem képesítései, sem képessége és készségei nem álltak rendelkezésre.

A „minőségbiztosítás"-ként felsorolt tevékenységek XXX XXX által történt tényszerű – XXX XXX tanúvallomásában szereplő módon megtörtént – elvégzése a rendelkezésre álló adatok alapján kizárható."

KÜLSŐ ANONIM HOZZÁFÉRÉSEK

A XXX Kft. informatikai rendszereinek működésére vonatkozó szabályok kizárták a külső, anonim hozzáférést a gazdasági társaság informatikai rendszerének

[103] Az erre vonatkozó adatokat a 27/2016 szakértői ügyszám alatt a 60100-XX/20XX. bü. sz ügyben készített igazságügyi informatikai szakértői vélemény tartalmazza a 30-39. oldalon

bármely részéhez (függetlenül attól, hogy az leválasztott, ún. sziget rendszer volt-e, vagy sem).

A VPN kapcsolaton keresztüli, távmunkában végzett fejlesztést a XXX Kft. szabályzatai és kockázatelemzési dokumentumai kizárták, ezzel egyezően a 20XX.XX.XX-i adatmentés tartalmában és a 20XX. évi házkutatás során lefoglalt, mintegy 1,5 TB-nyi adatban nincs nyoma annak, hogy a fejlesztés során alkalmaztak volna VPN kapcsolaton keresztüli, alvállalkozói szoftverfejlesztési megoldásokat.

A tanú nyilatkozata szerinti „teljesítmény mérés", azaz „ezek mindegyikét ellenőrizni kellett, hogy milyen mértékű a fejlesztési aktivitás"[104] ellentmond, mind az informatikai szakmai normáknak, mind a gazdaságossági szempontoknak. Ezt igazolja azon ellentmondás, mi szerint a saját fejlesztők tehermentesítése volt az „anonim fejlesztők" igénybe vételének az oka, ugyanakkor a fejlesztést XXX XXX nyilatkozata szerint rövid időn belül a saját fejlesztők vették át.

Összefoglalva: a fejlesztő1 … fejlesztő10 felhasználói nevű, anonim hozzáférésekre vonatkozóan semmiféle adat nem merült fel, ugyanakkor az anonim felhasználók működését valamennyi információbiztonsági szabályzat tiltotta, a szakmai és gazdaságossági szempontok alapvető normáinak sem felelt meg. Ebből adódóan kizárható külső anonim fejlesztők időleges alkalmazása a kérdéses rendszerek fejlesztésében."

Amint az esettanulmányban megfigyelhető volt a tanú szakmai állításainak ellenőrzése és értékelése volt az igazságügy informatikai szakértő alapvető feladata. Tekintettel arra, hogy a szakértő az ügy korábbi szakaszában is közreműködött, így képes volt az előzményként rendelkezésre álló információk – beleértve a korábbi házkutatás során mentett jelentős mennyiségű adattömeget is – együttes értékelésére. Ez utóbbi szempont túlmutat az igazságügyi szakértők tanúkihallgatások során történő alkalmazásán, felveti az egy ügy – egy szakértő kérdését. E kérdés megítélésénél azonban a nyilvánvaló előnyök mellett fel kell ismerni és figyelembe kell venni a hátrányokat is. E kérdés vizsgálata önálló kutatás tárgya lehet.

A fentiekben bemutatottak mellett a házkutatások során végzett tanúkihallgatások – megfelelő krimináltaktikai[105] előkészítés mellett – a szakértővel, vagy szakértői csoportokkal történő szoros együttműködéssel tehetők hatékonyabbá, s a későbbi bizonyítás szempontjából is eredményessé.

[104] XXX XXX tanú nyilatkozata

[105] FINSZTER im. p. 19

9.2 Gyakori vizsgálat típusok

A tanulmány első részében (lásd: Empirikus kutatás – a szakterületi felosztás validálása részt) kiderült, hogy az igazságügyi informatikai szakértői vizsgálatok túlnyomó része eszköz vizsgálat, ezért a következőkben azokat az alapvető vizsgálati lépéseket tekintjük át melyek a leggyakrabban vizsgált eszközök (tárolók, mobiltelefonok, okostelefonok) esetén használatosak.

9.2.1 Tárolóeszközök vizsgálata

Amint az a tanulmány első részében (lásd 13. oldal) ismertetett kutatásból is kitűnt, az igazságügyi informatikai szakértői vizsgálatok túlnyomó részét a tárolóeszközök vizsgálata teszi ki, ezért kiemelten fontos e terület alapos bemutatása. Az ISO/IEC 27037 szabványnál ismertetett elméleti megközelítést most a gyakorlattal ötvözve tekintjük át ismét:

Azonosítás

> Az a folyamat – beleértve a keresést is – amely során felismerik és dokumentálják a lehetséges digitális bizonyítékokat.
>
> *[3.7 – identification, forrás: ISO/IEC 27037:2012, 3.12]*

A lehetséges digitális bizonyítékok felismerése és dokumentálása nem kizárólag a házkutatás (lásd részletesen a 117. oldalon) során merül fel, hanem a szakértői tevékenység első operatív lépéseként is definiálhatjuk.

A vizsgálandó eszközök átvétele a szakértő részére átadott dokumentumok – kirendelő határozat, vagy végzés, bűnjeljegyzék[106] – alapján történik.

PÉLDA 1

„1. A szakértői vizsgálat tárgya: a fenti számú ügyben lefoglalt

- *1 db fekete színű, SP feliratú, 336000091 gyári számú asztali számítógép fellelhető adatállomány,*
- *1 db MSIVR610X NOTEBOOK feliratú, ICID4104A-AR5BXB63 gyári számú laptopon fellelhető adatállomány."*[107]

Az átvételkor az eszközök tételes ellenőrzésére van szükség a fenti dokumentumok alapján, amennyiben az lehetséges. A tételes átvételre akkor van lehetőség, ha az eszközök csomagolása azt lehetővé teszi, illetve a bűnjelcímkék[108] feliratozása olvasható és azonosítható a kérdéses eszközön. Amennyiben tétel azonosításra nincs mód, úgy

[106] Lásd: Bűnjeljegyzék p.209

[107] 39/2016 – kirendelő határozat. Máté István Zsolt – Szakértői ügynyilvántartás.

[108] Lásd: 15.3 Bűnjel címke. p.210

mennyiségi átvétel történhet, illetve az átadás átvételi jegyzőkönyvben rögzíthető az eltérés.

Előfordulhat, hogy az átvett eszközök között a bűnjeljegyzéken nem szereplő tételek is megjelennek. Ez a helyzet különösen mobiltelefonok és okostelefonok átvételekor tapasztalható, amikor az egyes komponensek (pl. SIM kártya, memóriakártya stb.) nem kerülnek önállóan jelölésre az átvételi iratokon. Ebben az esetben a szakértő a megtalálás helyének eszközazonosítóját, valamint az eszköz nevét használja azonosításra, esetleg a tételszámot alszámmal (/1, /2 stb.) látja el.

A vizsgálatnak ebben a szakaszában kell rögzíteni az eszközök esetleges sérüléseit is, megfelelő képi dokumentálás mellett[109].

A laboratóriumi vizsgálat megkezdésekor az átadás-átvétel során beazonosított eszközök csomagolásának felbontása is dokumentálandó lépés. Ekkor kerül sor a csomagolóanyag (bűnjel tasak, műanyag, vagy textil bűnjelzsák, egyéb csomagolás) sértetlenségéről történő megbizonyosodásra, a zárócimkék ellenőrzésére és a felbontási folyamat képi dokumentálására[110]. Ez a lépéssorozat alapozza meg az igazságügyi informatikai szakértői vélemények szokásos bevezető mondatát:

> *„A szakértői vizsgálat tárgyát képező eszközöket a «kirendelő hatóság», «székhely címe» sz. alatti székhelyén, sértetlen állapotban, azonosító címkével lezárva vettem át."*

Az eszközök azonosítási folyamatának lezárásaként a vizsgált tároló egyedi azonosítóját is tartalmazó képi[111] és elektronikus adatsort[112] rögzíti a szakértő. Utóbbi mozzanat részben átfedést mutat az adatok megszerzésével, tekintettel arra a körülményre, hogy az eszköz belső azonosítóinak kiolvasása már szakértői hardverek és szoftverek felhasználásával történik.

Azoknál az eszközöknél, ahol a tároló önálló burkolatban van elhelyezve, pl. külső merevlemez, okostelefon etc., szükséges a burkolatok megbontása[113] és a tárolóhoz, vagy eszköz azonosítóhoz történő közvetlen hozzáférés.

Összefoglalva: az azonosítás elsődlegesen a bűnügyi helyszínen, rendszerint házkutatás keretében történő, megfelelő (informatikai) szakmai felkészültségű személy által végzett tevékenység, másrészt a szakértő által az eszközök átvételekor végzett azonosító tevékenységként írható le.

---

[109] Lásd: 15.4 Sérült bűnjel állapotának rögzítése. p.211.

[110] Lásd: 15.5 Bűnjel csomagolsának felbontása. p.212.

[111] Lásd: 15.6 Bűnjel egyedi azonosítójának rögzítése. p.214.

[112] Lásd: 15.7 Bűnjel egyedi elktronikus azonosítójának rögzítése. p.215.

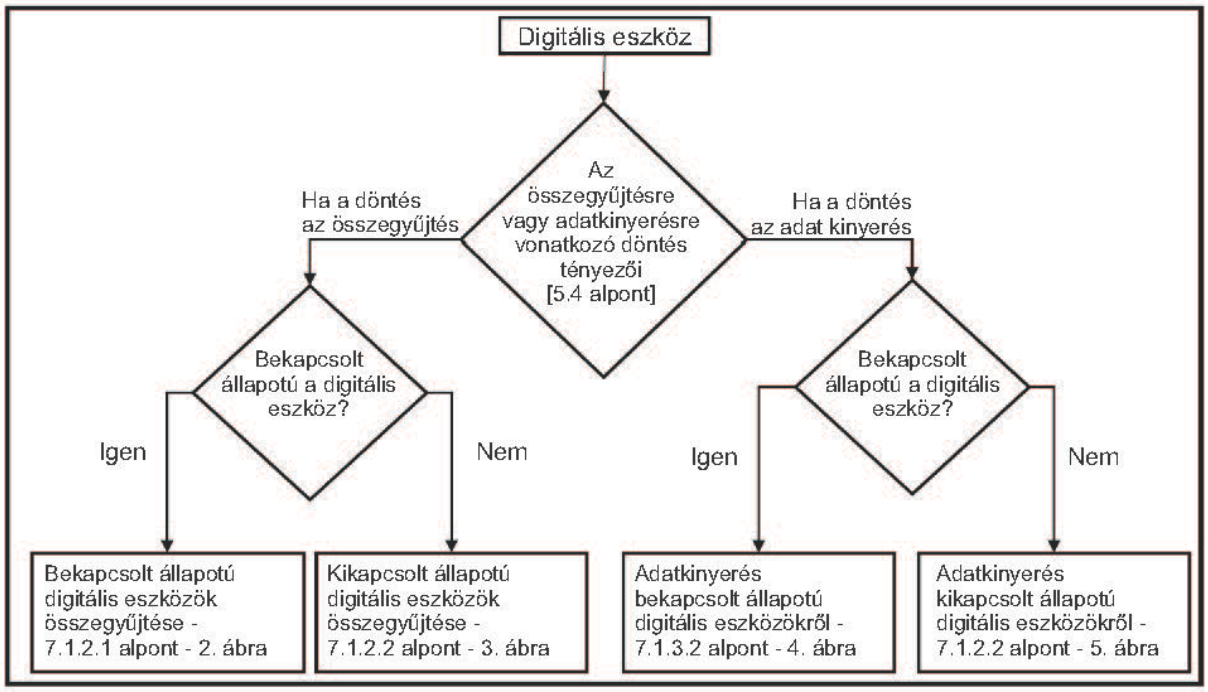
[113] Lásd: 15.8 Burkolat megbontása sz egyedi azonosító rögzítése céljából. p.217.

Összegyűjtés

> *Összegyűjtés*. A potenciális digitális bizonyítékot tartalmazó fizikai tárgyak összegyűjtésének folyamata. *[3.3 – collection, forrás: ISO/IEC 27037:2012, 3.3]*

A meghatározásból is kitűnik, hogy az összegyűjtés szorosan kapcsolódik a helyszíni vizsgálatokhoz, a potenciális digitális bizonyítékok azonosítását követő lépésként. A fizikai tárgyak – ahogy azt „A Digital Forensic Science eredete és tartalma" fejezetben a 25. oldalon olvashattuk – különböző típusú és komplexitású bűnügyi helyszínen történő összegyűjtésekor egyben folytatódik az azonosításnál megkezdődött dokumentációs folyamat is, mely alkalmas a felügyeleti lánc (Chain of Custody) fenntartásának igazolására is.

Az összegyűjtéssel kapcsolatos döntési folyamatot segédletekkel támogatja, melynek első mozzanata annak eldöntése, hogy történik-e helyszíni adatkinyerés (aquisition), vagy az eszközök összegyűjtését követően laboratóriumi vizsgálatra kerül sor. A döntési folyamat lépéseit az alábbi ábrán mutatom be:



1. ábra - segédlet a lehetséges digitális bizonyítékok összegyűjtésére vagy az adatok kinyerésére vonatkozó döntéshez

5. ábra - Segédlet lehetséges digitális bizonyítékok összegyűjtésére vagy az adatok kinyerésére vonatkozó döntéshez[114]

Az ábrán látható döntést megalapozó tényezők jellemzően a vizsgálandó rendszer műszaki és fizikai paramétereit jelentik, melyek általánosan a következők:

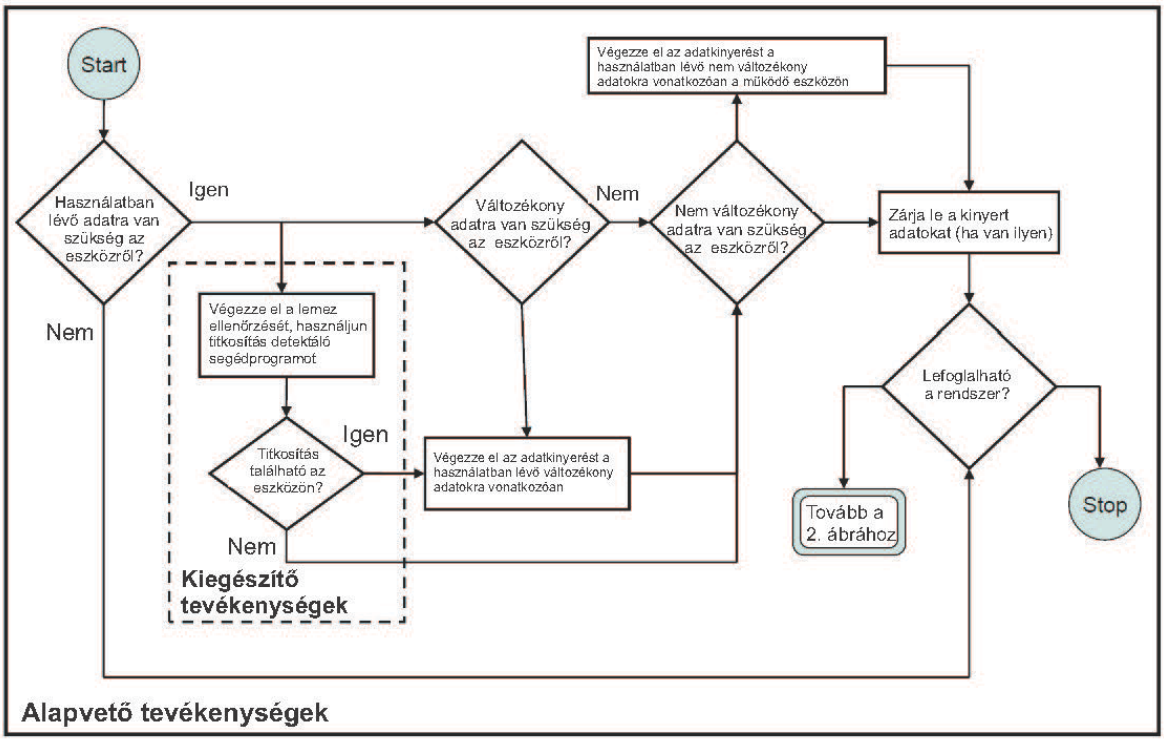
- a vizsgálandó rendszer tároló komponense elkülöníthető-e
  - ~ felhő alapú tárolás,

[114] ISO/IEC 27037:2012 (p.29 – Figure 1) alapján, a szerző fordítása

    - ~ több gazdasági társaság által használt közös tárhely,
    - ~ egyéb elkülönítést gátló körülmény
- a vizsgálandó rendszer bekapcsolt állapotú-e (élő, vagy online rendszer)
    - ~ bekapcsolt állapotú rendszer esetén a tárolás távoli eszközön történik (felhőalapú, vagy távoli eléréssel – VPN, Remote Desktop – történő hozzáférés),
    - ~ bekapcsolt állapotú rendszer esetén a mentendő adatok mennyisége és az adatkinyerésre rendelkezésre álló adatátviteli csatornák sebessége milyen mértékű vizsgálati időt feltételez
- a vizsgálandó rendszerhez történő távoli kapcsolódás kizárható-e
    - ~ a vizsgálandó rendszer nagy távolságú hálózathoz kapcsolódik
    - ~ a vizsgálandó rendszer helyi vezetékes hálózathoz kapcsolódik
    - ~ a vizsgálandó rendszer helyi vezeték nélküli hálózathoz kapcsolódik

A fenti körülményeken kívül az adott helyszínre jellemző egyéb tényezők is felmerülhetnek, mint döntést megalapozó adat.

Amennyiben a döntés az eszközök összegyűjtése, úgy elsődlegesen meg kell győződni arról, hogy bekapcsolt állapotú rendszerről, vagy rendszer komponensről van-e szó, ugyanis a további tevékenységeket e körülmény lényegesen befolyásolja, ahogy azt a következő ábrán láthatjuk:



4. ábra - Segédlet bekapcsolt állapotú digitális eszközökről történő adatkinyeréshez

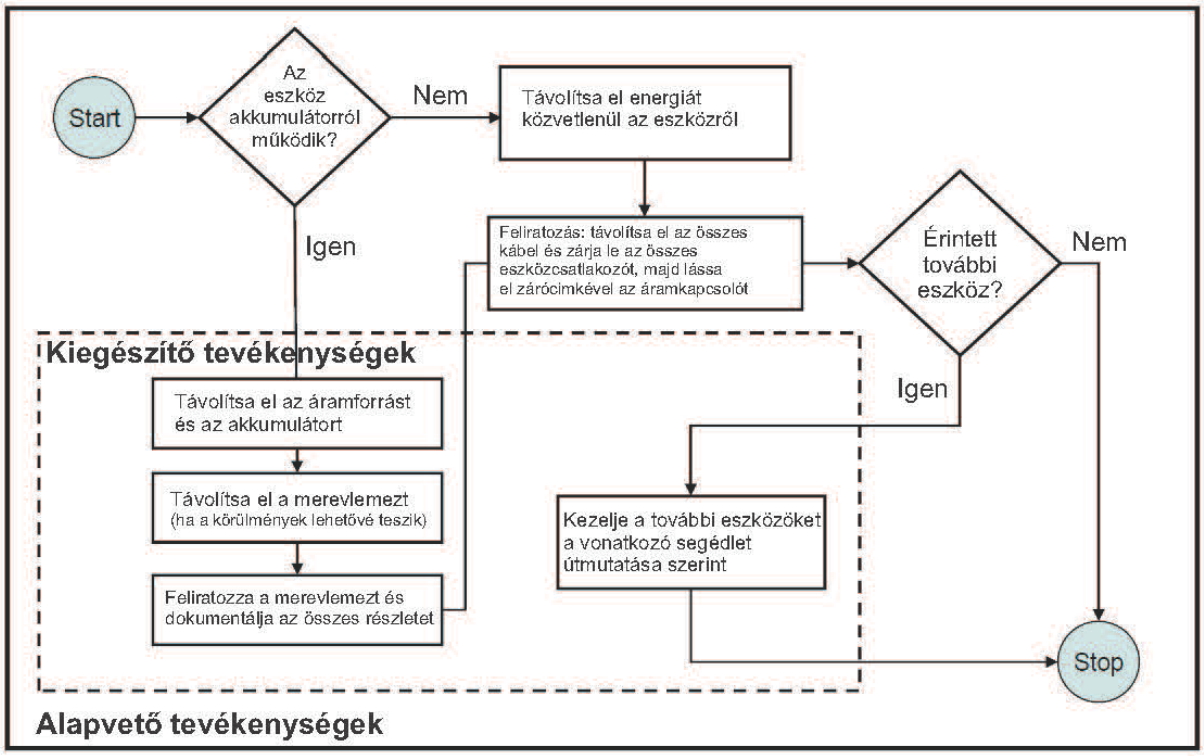
6. ábra - Segédlet bekapcsolt állapotú digitális eszközökről történő adatkinyeréshez[115]

A potenciális digitális bizonyítékok összegyűjtésének folyamatában itt kap kiemelt hangsúlyt és figyelmet a digitális bizonyítékok helyszíni vizsgálója (Digital Evidence First Responder, DEFR), aki az összegyűjtés szakmai irányítójaként és a szakmai döntésekért felelős személyként jelenik meg.

A legnagyobb kockázatot az összegyűjtés esetén a bekapcsolt állapotú rendszerek jelentik, különösen akkor, ha változékony (volatile) adatok is megtalálhatóak a rendszerben. Amennyiben az összegyűjtés helyszínén nem tud közvetlenül megjelenni a DEFR pozícióban lévő személy (különösen több helyszínes vizsgálat esetén gyakori), úgy a rendszerre vonatkozó döntés meghozatala előtt szakmai konzultáció szükséges vele, valamely csatornán.

A kikapcsolt állapotú rendszerek esetén (lásd: a következő ábrán) az előzőekhez hasonlóan fontos döntés az akkumulátorok eltávolítása (különösen mobiltelefonok és okostelefonok esetén), valamint a tárolók (merevlemez, szilárdtest lemez etc.) eltávolítása is. A magyarországi gyakorlatban egyikre sem kerül sor, ami egyrészt az eszközök távolról történő ébresztését és törlését (Apple okostelefonok), vagy egyéb nem kívánt eseményt is okozhat.

[115] ISO/IEC 27037:2012 (p.34 – Figure 4) alapján, a szerző fordítása



3. ábra - Segédlet kikapcsolt állapotú digitális eszközök összegyűjtéséhez

7. ábra - Segédlet kikapcsolt állapotú digitális eszközök összegyűjtéséhez[116]

Az összegyűjtés következő mozzanataként, mintegy megelőlegezve a megőrzési (preservation) tevékenységet, biztosítani kell egyrészt az eszközök állapotának megváltoztathatatlanságát, másrészt a folyamatos dokumentálással fenn kell tartani a felügyeleti láncot.

Az eszközök biztosításának szokásos módja az egyes készülékek csomagolása, melyre rendelkezésre állnak papír, műanyag vagy textil alapanyagú bűnjel tasakok és zsákok, másrészt – különösen nagyobb kiterjedésű eszközök esetén – speciális (felbontáskor nyomot hagyó) lezárócímkék.

Gyakori hiba az, hogy az egyébként helyes lezárócímke alkalmazást (az eszköz csatlakozópontjainak lezárása) követően nem kerül sor a tárolóegységet tartalmazó rész (pl. számítógép ház, laptop HDD fedőburkolat etc.) megfelelő lezárására, így az esetleges észrevétlen beavatkozás nem zárható ki a későbbiekben (lásd a 15.9 és 15.10 részben a 249-250. oldalon).

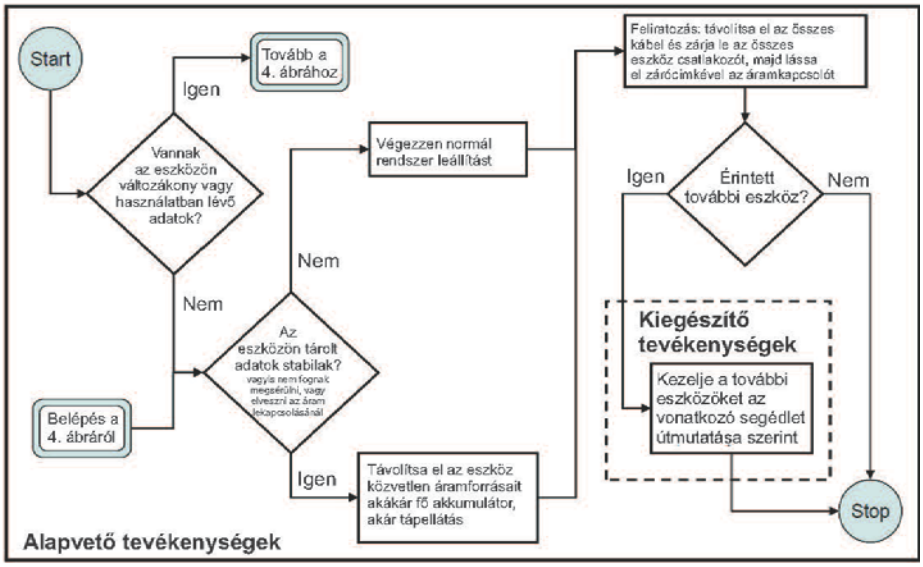
Adatok megszerzése

> *Adatok megszerzése.* Az adatok meghatározott köréről készített másolat létrehozásának folyamata. *[3.1 – acquisition]*

[116] ISO/IEC 27037:2012 (p.32 – Figure 3) alapján, a szerző fordítása

Az adatok megszerzése elsődlegesen lehet helyszíni és laboratóriumi, míg a helyszíni mentés különbözhet egymástól attól függően, hogy a vizsgált eszköz bekapcsolt, vagy kikapcsolt állapotú-e.

Az alábbiakban látható ábra ad támogatást a bekapcsolt állapotú eszközökről történő mentéshez.



2. ábra - Segédlet bekapcsolt állapotú digitális eszközök összegyűjtéséhez

8. ábra - Segédlet bekapcsolt állapotú digitális eszközök összegyűjtéséhez[117]

A vizsgálat fő folyamata az adatok változékonyságára vonatkozó döntéstől függ: amennyiben ilyen adatok (pl. főmemória [RAM] tartalma, futó folyamatok, számítógépes hálózati kapcsolatok) mentése szükséges, úgy a digitális bizonyítékok helyszíni vizsgálója (DEFR) – aki tipikusan az igazságügyi informatikai szakértő – elvégzi az élő adatok mentését az erre alkalmas szoftver és hardver eszközök felhasználásával. A felhasznált eszközök nem származhatnak magáról az eszközről (az eszközön futó alkalmazások megbízhatósága nem ellenőrizhető). A kinyert változékony adatokat a szakértő valamely fájltárolóba (pl. lemezkép állomány, tömörített állomány etc.) helyezi el, majd a tároló állományról ún. hash lenyomatot készít. A hash kód (mely egy számsorozat) igazolja, hogy a fájltárolóba helyezett adatokban nem történt változás (megőrzési funkció).

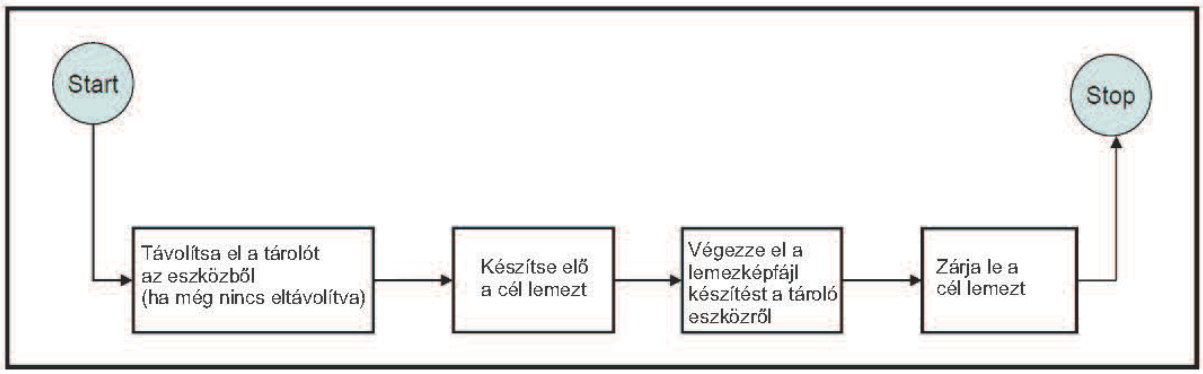
A nem változékony adatok kinyerése hagyományos lemezképfájl készítő alkalmazásokkal (pl. AccessData FTK Imager[118], Tableau Imager etc.) történhet. Ezek a másolatok rendszerint gyári bontatlan állapotú adattárolókra kerülnek, hash kódos ellenőrzéssel és végül biztonsági szalagos lezárással.

[117] ISO/IEC 27037:2012 (p.30 – Figure 2) alapján, a szerző fordítása

[118] Lásd: 15.14 AccessData FTK Imager, p.235.

Élő rendszereknél esetenként előfordulhat kódolt, titkosított, vagy más módon védett adatok jelenléte. Ezeket titkosítás azonosító szoftverekkel szükséges feltárni, illetve a hozzáférési adatokat a hatósági eljárás megfelelő előkészítésével és időzítésével (pl. munkakezdést közvetlenül követő időszak) hagyományos módszerekkel is meg lehet szerezni (a felhasználók bejelentkeznek saját adataikkal és megkezdik a munkát).

A kikapcsolt állapotú digitális eszközökről történő adatkinyerés rendszerint a szakértői laboratóriumban történik. Amennyiben valamely körülmény miatt szükséges a helyszíni mentés, úgy annak lefolytatása a következő ábrán látható módon történik. A tárolót el kell távolítani a rendszerből – semmiképpen nem szabad az eszközt áram alá helyezni, bekapcsolni –, majd a céllemez (adattár) előkészítését követően megfelelő hardver eszközzel elvégezhető az adattár bitről-bitre történő, vagy célzott részleges mentése.



5. ábra - Segédlet kikapcsolt állapotú digitális eszközökről történő adatkinyeréshez

9. ábra - Segédlet kikapcsolt állapotú digitális eszközökről történő adatkinyeréshez[119]

Míg a teljes körű – bitről-bitre történő mentéshez Forensic Duplicator (lásd: 15.11, p.252), illetve Forensic Imager (lásd: 15.12, p.253) használatos, míg a részleges célzott mentések Forensic Bridge (lásd: 15.13, p.254) segítségével valósíthatók meg. A műveletekhez használt hardver eszközök a saját működésükről napló állományokat készítenek (lásd: 15.15, p.256), melyek a dokumentációs cél mellett azonosítási feladatokra is alkalmasak egyben.

A célzott mentés esetén, mivel nem kerül minden adat a cél adattárolóra, a forrás adattárolóról teljes tartalomjegyzék készítése szükséges, melyet a másolási művelethez használt szoftverrel (pl. Accessdata FTK Imager, lásd: 15.16, p.257) lehet megvalósítani.

Megőrzés

> *Megőrzés.* Az a folyamat melynek során megvédik és fenntartják a lehetséges digitális bizonyíték eredeti állapotát. *[3.15 – preservation]*

[119] ISO/IEC 27037:2012 (p.35 – Figure 5) alapján, a szerző fordítása

Amint az a meghatározásból kiolvasható, a megőrzés nem statikus, pillanatnyi beavatkozást jelent, hanem egy állapot fenntartásának a folyamatát, mely lényegében már az összegyűjtéssel elkezdődik, illetve ténylegesen az adatok mentésétől egészen a büntetőeljárás végső lezárásáig tart. Az igazságügyi informatikai szakértő nézőpontjából a folyamat felügyelete és nyomon követése a helyszíni vizsgálatkor kezdődik meg, amikor az egyes eszközök egyedi azonosítót kapnak (unique evidence identifier), mely alapján a későbbiekben nyomon követhetővé válik, hogy ki férhetett hozzá az eszközhöz, illetve az eszköz mely időpontban mely földrajzi helyen volt megtalálható. Ezt a dokumentációt a változás minden mozzanatánál frissíteni kell, mely biztosítja az eszközzel kapcsolatos események utólagos rekonstruálhatóságát.

A megőrzés alapvető művelete a becsomagolás, melyen egyrészt az eszköz és a benne található digitális bizonyíték állagának megóvása és a változások kiküszöbölése a cél, másrészt azonosítási célokat is szolgál.

A védelmi célokat alapvetően a következő szempontok figyelembe vételével lehet megvalósítani:

- digiális eszközök kezelésekor a szakértő lehetőség szerint viseljen szöszmentes (lint-free) kesztyűt (ez a magyarországi gyakorlatból hiányzik), mely tiszta és száraz,
- meg kell védeni a digitális eszközt a különféle elektromágneses sugárzások (pl. rendőrségi rádió, röntgen eszközök etc.) káros hatásaitól, beleértve a statikus elektromosságot is,
- a csomagolásnak mentesnek kell lennie a portól, zsírtól, kémiai szennyező anyagoktól, amelyek elősegítik az oxidáció okozta korróziót, valamint a nedvesség lecsapódását a tárolók mágneses rétegére,
- Minimálisra csökkentsük a nyomtatás lehetőségét (a szalag egyik szalagjától a szomszédos hurokig történő jelátvitel), ami akkor is előfordulhat, ha a szalagokat hosszabb ideig tárolják aktív használat nélkül, ami rossz minőségű jelet eredményez.

9.2.2 Szerzői joggal kapcsolatos ügyek

Az igazságügyi informatikai szakértői gyakorlat felhalmozott tapasztalatai alkalmat adnak az egyes ügytípusok jellegzetességeinek összefoglalására. A kétszázötvennél több ügyet tartalmazó archívumban az „előkelő" negyedik (más számítás szerint a második – lásd az írásban részletesen) helyen szerepelnek a szerzői joghoz kapcsolódó ügyek. Mivel a szakértő a nyomozati szaktól a bírói szakig részt vehet a büntetőeljárásban, rátekintése nyílik az 1978. évi IV. törvény (régi Btk.) 329/A. és 329/B. § szerinti [a 2012. évi C. törvény (új Btk.) 385. § és 386. §] cselekmények nyomozására és az ítélethozatalra is. A szakértő nézőpontja – függetlenségéből adódóan – lehetőséget ad a

rendszer működésében tapasztalható hibák azonosítására és a jó gyakorlatok feltárására egyaránt. Jelen írás ezt a szakértői nézőpontot felhasználva mutatja be a szerzői joghoz kapcsolódó ügytípusokat a büntetőeljárásokban, s egyben bepillantást enged az igazságügyi informatikai szakértői munka mindennapjaiba is.

A szerzői jog eredete és annak hatása napjaink szabályozására

A szerzők az idők kezdetétől jelen vannak a mindennapokban. Munkásságukat – legyen az anyagi (szobrászat, építészet stb.), vagy szellemi (mese, eposz stb.) – magukból a művekből ismerhetjük, személyük az ókorig homályban maradt.[120] A szerzőkkel kapcsolatos első utalás a római jogban figyelhető meg a szerzők és a könyvkereskedők közötti szerződések formájában, bár ezek az ügyletek – a jogforrásokban történő említés hiányában – még nem részesültek jogi védelemben.[121]

Ugyanakkor megállapítható, hogy a szerzői művek többszörözésének gyakorlata már ebben az időszakban is megfigyelhető volt, s ez a gyakorlat máig hatóan érvényesül. Az egyik legszemléletesebb korabeli példa talán VERGILIUS Georgica című tankölteményének sorsa, mely az egyik első tömegesen másolt szerzői mű volt.[122]

A következő jelentős esemény a szerzői joggal kapcsolatosan a könyvnyomtatás megjelenése és az azzal kapcsolatos privilégiumok kiadása volt, melyek az új technológia elterjedését ösztönözték.[123] Ezek közé a privilégiumok közé tartozott I. MÁRIA királynőnek a könyviparosok céhe (Stationers' Company) részére kiadott kiváltságlevele (1557), mely a nyomtatás és könyvkereskedelem ellenőrzését tette lehetővé a céh részére.[124]

Az első komolyabb, máig érvényesülő hatás ebben a korszakban alakult ki: megjelent a privilégiumokat kijátszó kalóz figurája, mely visszaköszön napjaink szerzői jogi eseteinél. Ugyanekkor alakul rögzített szókapcsolattá a right „to copy", illetve a „stationers' copyright" kifejezésekből a ma is használt copyright szó.[125] A privilégiumok

[120] MÁTÉ István Zsolt: A multimédia technológiák kulturális hatásai. PTE-BTK Kommunikáció és Médiatudományi Tanszék, 2012. p.17.
[121] NÓTÁRI Tamás: A magyar szerzői jog fejlődése. Lectum Kiadó, 2010. p.21.
[122] LÁSZLÓ Zoltán (szerk.): Vergilius. http://www.literatura.hu/irok/ okor/vergilius/vergilius.htm [2014.01.10.]
[123] BODÓ Balázs: Szükség törvényt bont. ELTE, 2010. p. 51. http://doktori.btk.elte.hu/phil/bodobalazs/ disszertacio.pdf [2013.01.10.]
[124] PART Krisztina Katalin: A szerzői jogi szabályozás kialakulása Angliában, Németországban és az Egyesült államokban. in Iparjogvédelmi és szerzői jogi szemle 2006/4. Szellemi Tulajdon Nemzeti Hivatala, 2006. p.142., http://www.sztnh.gov.hu/kiadv/ipsz/200608-pdf/08-part-krisztina.pdf [2014.01.10.]
[125] PART Krisztina Katalin im. p. 142.

tulajdonosai és a kalózok (akik nem ritkán a másik csoportból kerültek ki) harca vezetett a napjaink szerzői jogi rendszerét megalapozó jogszabályig: a Statute of Anneig (Anna Királynő Törvénye).

> *„... és bármilyen könyv – melyet már megalkottak / összeállítottak és nem nyomtattak ki és nem adtak ki, vagy ezután fognak megalkotni / összeállítani – szerzője és az ő engedményese vagy kijelöltje rendelkezzen a nyomtatás vagy újranyomtatás egyedüli szabadságával ezen könyvre vagy könyvekre vonatkozóan tizennégy évig az első kiadás napjától számítva és nem tovább;"*[126]

A szerzői jog alapjainak lerakásától kezdődő, s napjainkig tartó folyamat részleteit most terjedelmi ok miatt nem tudjuk áttekinteni, de az Amerikai Egyesült Államok példáján keresztül, a nevezetesebb események felsorolásával képet kaphatunk a bejárt útról és egyben megérkezhetünk jelen tanulmány tulajdonképpeni tárgyához, a számítógépes programok szerzői jogi védelméhez is.

- 1790 az első szerzői jogi törvény alkotmányba iktatása (könyvek, térképek és térképészeti alkotások)
- 1802 a védelem kiterjesztése az újságokra
- 1831 a védelem kiterjesztése a zeneművekre
- 1856 a védelem kiterjesztése a drámai művekre
- 1865 a védelem kiterjesztése a fotográfiákra
- 1870 a védelem kiterjesztése a műalkotásokra (képzőművészet)
- 1912 a védelem kiterjesztése a mozgóképekre (korábban fotográfiaként kezelték)
- 1953 a védelem kiterjesztése a nem irodalmi drámai művekre
- 1980 a védelem kiterjesztése a számítógépes programokra
- 1990 a védelem kiterjesztése az építészeti művekre[127]

Látható a felsoroltakból, hogy az eredetileg a könyvterjesztés körülményeit szabályzó szerzői jog miként terjesztette ki hatókörét a tőle távol eső területekre is.

Napjaink hazai szerzői jogi szabályozása, különös tekintettel a számítógépes programalkotásokra

A szerzői jogról szóló 1999. évi LXXVI. törvény (Szjt.) 1. §-a rendelkezik a szerzői jogi védelem tárgyáról. A jogszabály az informatikai tartalmakra vonatkozóan a d) pontban ad útmutatást, amikor is a védelem tárgyát a következőképpen jelöli meg: „a számítógépi programalkotás és a hozzá tartozó dokumentáció (a továbbiakban: szoftver)

[126] Statute of Anne. London, 1710. British Library, 8 Anne c. 19. p.1., a szerző fordítása http://www.copyrighthistory.com/anne.html [2012.02.01.]

[127] PART Krisztina Katalin im. p. 151.

akár forráskódban, akár tárgykódban vagy bármilyen más formában rögzített minden fajtája, ideértve a felhasználói programot és az operációs rendszert is".

A jogszabály ugyanebben a szakaszban egy kivételt is meghatároz a hagyományos informatikai értelemben szintén szoftvernek tekinthető adatbázis vonatkozásában a p) pontban, miszerint a védelem tárgya: „a gyűjteményes műnek minősülő adatbázis". A látszólagos, vagy tényleges ellentmondást a VII. fejezet igyekszik feloldani, amikor pontosítja az adatbázis fogalmát, méghozzá szűkítő értelemben az adatbázis-tartalomra vonatkoztatva.

A fenti szűkítő megfogalmazás (adatbázis tartalom) nem oszlatja el a kétségeket az adatbázis szerkezet védettségét illetően (a szerzőét semmiképpen), különösen annak a fényében, hogy a jogalkotó a 60/A. § (3) pontjában a következőképpen fogalmaz: „Az adatbázisra vonatkozó rendelkezések nem alkalmazhatók a számítástechnikai eszközökkel hozzáférhető tartalmú adatbázis előállításához vagy működtetéséhez felhasznált szoftverre." Ez a megfogalmazás arra utal, hogy az előállításhoz és működtetéshez használt rendszerek is védettek, mint szoftverek, de továbbra sem nyer tisztázást az adatbázis tartalom és a működtető szoftver között „lebegő" adatbázis szerkezet helyzete.

A fenti kérdés tisztázása még akkor is szükséges, ha a szövegek alapján nyilvánvaló, hogy az adatbázis kezelő szoftver is a szerzői jogi védelem tárgyának tekintendő, mint szoftver, s az adatbázis tartalom is annak, mint gyűjteményes mű (adatok rendszerezett halmaza a leegyszerűsített informatikai definíció szerint). Ugyanakkor figyeljünk fel arra a következményre, miszerint az adatbázis szerkezete nem áll védelem alatt, holott az informatikai szempontból az adatbázis egyik legfontosabb része.

Bár a szakértői gyakorlatban még jelentek meg adatbázis szerkezetre vonatkozó, az ismertetett szempontot használó, kihasználó ügyek, nem hagyhatjuk figyelmen kívül a Big Data jelenséghez (a közeljövő stratégiai fontosságú eleméhez[128]) kapcsolódóan azt a tényt, hogy a gigászi mennyiségű adatfolyamokból történő adatkinyerés kulcsa az információk reorganizációja, újraszervezése, melyben az adatbázis szerkezetek kiemelt szerepet kaphatnak. Amennyiben ezek az elemek nem nyernek pontosan definiálható, a fenti kétségeket kizáró védelmet, az jelentős hátrányt okozhat egyes fejlesztőknek. Megjegyzendő ugyanakkor, hogy az Európai Bíróság kiterjedt adatbázis-jogi gyakorlatának tanulmányozása e kérdés tisztázásában is segítséget nyújthat.

[128] Cisco: Cisco Connected World Technology Report. http://www.cisco.com/en/US/netsol/ns1120/index.html [2014.01.11.]

A leggyakrabban sértett jogok

Mivel a szakértői gyakorlatban szinte kizárólag a vagyoni jogokkal és a szerzői jog védelmére szolgáló műszaki intézkedés megkerülésével kapcsolatos vizsgálatok szerepelnek, a következőkben csak ezekre térünk ki részletesen.

Ezek közül a többszörözés joga és a terjesztés joga nevezhető meg, mint leggyakrabban sértett vagyoni jog, ezekhez zárkózik fel a szerzői jog védelmére szolgáló műszaki intézkedés megkerülése. A többszörözéskor (Szjt. 18. §) anyagi hordozón történő, bármilyen módú végleges, vagy időleges rögzítésről beszélünk, míg a terjesztés esetén (Szjt. 23. §) a forgalomba hozatalra történő felkínálást értjük.

Többszörözés

A szoftverek a gyakorlatban valamely adathordozón találhatóak meg, melyek a számítógépbe beépített mágneses, vagy elektronikus tárolási elvű adattárak (HDD, SSD), vagy cserélhető optikai, vagy elektronikus tárolási elvű eszközök (CD, DVD, Blu-Ray Disc, pendrive, memory card stb.). Mivel szoftverek esetén a jogszabály kizárja a szabad felhasználást (Szjt. 35. §), ezért az adott szoftverből alaphelyzetben egy (vagy a felhasználási szerződésben meghatározott darabszámú) telepített és legalább egy biztonsági másolat [Szjt. 59. § (2) bekezdés szerint] tárolható (hacsak a felhasználási szerződés többen nem engedélyez).

Terjesztés

A szoftverek terjesztésének minősül az Sztj. 23. § (1) alapján a műpéldány nyilvánosság számára hozzáférhetővé tétele forgalomba hozatallal, vagy forgalomba hozatalra felkínálással. E két módozat a leggyakrabban valamilyen cserélhető adathordozón pl. CD, DVD történő terjesztés (időben korábbi gyakorlat), illetve valamely nyilvános hálózaton a tartalom megosztásával történik pl. DC hub (Direct Connect elosztó), FileShare, Torrent és más technológiák (jelenlegi gyakorlat).

A szerzői jog védelmére szolgáló műszaki intézkedés megkerülése

Bár nem tartozik a vagyoni jogok közé, mégis itt célszerű említést tenni a szerzői joggal kapcsolatos ügyek harmadik leggyakoribb típusáról. Az Szjt. 95. § (1) alapján ez a magatartás azonosan minősül – egészen pontosan „A szerzői jog megsértésének következményeit kell alkalmazni...” – az előzőekben ismertetett vagyoni jogok megsértésével. A gyakorlatban a kódgenerátorok (keygen), a feltört programkódok (crack), illetve illegális licenc fájlok vagy sorozatszámok felhasználásáról beszélhetünk, egyéb kevésbé elterjedt módszerek mellett.

A szerzői jog megsértésének büntetőjogi vonatkozásai

A régi Btk. 329/A. § és 329/B. §-ában meghatározott tényállások közül – a szakértői ügystatisztika alapján – a leggyakoribb az (1) bekezdés szerinti alapeset, amikor a gya-

núsított „...haszonszerzés végett, vagy vagyoni hátrányt okozva megsérti..." a jogtulajdonos szerzői, vagy ahhoz kapcsolódó jogát. Az alapeset és a jogok védelmét biztosító műszaki intézkedés kijátszásának alapesete (készít, előállít) együttesen és az utóbbi önálló gyanúsításként egyforma mértékben jelentkezik, míg a műszaki intézkedés kijátszásához kapcsolódóan az „...átad, forgalomba hoz, vagy azzal kereskedik" tényálláshoz kapcsolódó esetek nagyobb számban jelentkeznek (részletesen lásd a következő táblázatban).

20. táblázat - Szerzői joggal kapcsolatos ügyek időbeli megoszlása[129]

Jogszabály hely (Régi Btk. szerint)	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	
329/A. § (1)	0	3	3	3	1	0	2	**12**
329/A. § (1), 329/B. §	0	1	1	0	0	0	0	**2**
329/B. § (1)	0	0	2	0	0	0	0	**2**
329/B. § (1) b)	0	0	0	7	1	0	0	**8**

A feldolgozott esetek darabszáma (24) még akkor sem adhat okot általános következtetés levonására, ha figyelembe vesszük azt a tényt, miszerint az összes ügy (250) közül a darabszám tekintetében leggyakoribb öt ügytípus (161) közül – ha mind a négy felsorolt tényállást egynek tekintjük – a második helyen szerepel a szerzői joggal kapcsolatos normasértés ügytípusa.

A mennyiség mindenesetre jelzi, hogy nem elhanyagolható problémával állunk szemben, ugyanakkor arra a gyakorlatra is fel kell figyelnünk, hogy szerzői jogi területtől eltérő gyanúsítások esetén a nyomozó hatóságok szakértőt kirendelő határozataiban gyakran szerepel a következőhöz hasonló kérdés: „vizsgálatra megküldött adathordozón találhatók-e olyan adatok, szoftver programok, melyek sértik a szerzői jogokat?". Mivel a válasz az esetek többségében igen, a nyomozó hatóság „biztos pontként" tekinthet a szerzői jog megsértésére: abban az esetben tehát, ha az eredeti gyanúsítás nem igazolható az informatikai rendszerből kinyert adatokkal, úgy végső megoldásként a szerzői jog megsértése maradhat.

Az írás összefoglalójában említett független nézőpontból tekintve (mint szakértő) az ismertetett módszer nem tűnik korrektnek, különösen, ha részleteiben megvizsgáljuk a kérdést. Nyilvánvaló, hogy a feltett kérdésre a szakértőnek pontos választ kell adnia, s ez megfelelő munkaidő ráfordítással jár. A kapott eredmény kiértékelése, vagyis a jogtulajdonos meghatározása, a „kárérték" kalkulációja és egyéb járulékos adatok összegyűjtése akár jelentősen is növelheti a szakértői költségeket (a bizonyítás kérdéseit a későbbiekben részletezem). A kapott „eredményt" esetenként az interneten láthatjuk

[129] MÁTÉ István Zsolt: Szakértői ügynyilvántartás. 2014. (elektronikus)

viszont városi legendák, vagy megalapozottnak tűnő blogbejegyzések formájában.[130] A hatás intézménykommunikációs szempontból mindenképpen negatív, s ha figyelembe vesszük azt a tényt, hogy a vádemelés a szerzői jogi mellékszál esetében ritkán történik meg, a fentiekben írt gyakorlat felülvizsgálata indokoltnak látszik.

ESETTANULMÁNY (1)

> A tiltott pornográf felvétellel visszaélés bűntett [régi Btk. 204. § (2) bekezdés] gyanúja miatt indult büntetőügyben a hét érintett személytől lefoglalásra került más eszközök mellett 7 db személyi számítógép és egy darab merevlemez. Mindegyik esetében kérte a nyomozó hatóság szerzői jog megsértésének vizsgálatát. A bírói szakban (a tárgyalásra a szakértőt is beidézték) a vád „csak" a tiltott pornográf felvétellel visszaélésre vonatkozott.

A szakértő a nyomozási és a bírói szakaszban

A büntetőeljárásról szóló 1998. évi XIX törvény (Be.) 99. § (1) bekezdése szerint „Ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges, szakértőt kell alkalmazni". Ez alapozza meg az igazságügyi informatikai szakértő részvételét az eljárásban, melyre a bíróság, az ügyész és a nyomozó hatóság végzése, vagy kirendelése alapján kerül sor. Leggyakrabban a nyomozó hatóság rendeli el a szakértői vizsgálatot, néhány esetben pedig bírói végzés alapján, ügyészi felkérésre a saját szakértői gyakorlatomban eddig nem volt példa. Ez utóbbit magyarázhatja az a körülmény, miszerint a nyomozást az ügyész végzi vagy végezteti [Be. 28. § (3) bekezdés], így az ügyész általi szakértői kirendelés a nyomozó hatóságon keresztül jut érvényre.

A szakértők kirendelése

A szakértők kirendelésének első lépése a szakértő megtalálása területi és/vagy kompetencia köri keresés alapján.

A szakértői névjegyzék(ek)

A keresés természetes helye az igazságügyi szakértői tevékenységről szóló 2016. évi XXIX. törvény a szerint az igazságügyi szakértői névjegyzék, melyet jelenleg az Igazságügyi Minisztérium (IM) vezet, s elektronikus formában is elérhető a minisztérium honlapján a https://inyr.im.gov.hu/szakertok címen. A jegyzékben több szempont szerint kereshet a kirendelő, melyek közül a területi kamaránkénti és szakterületenkénti keresés látszik célszerűnek. A 18 szakterületen belüli 294 kompetenciakör mellett az adatbázis további 1655 db szakterületre nem besorolt vizsgálati területet tartalmaz.

[130] HORVÁTH Zoltán: A mosoly országából a röhej országába. http://rohe-jorszaga.blog.hu/2012/06/03/erre_egyszeruen_nem_talalok_szavakat_601 [2014.01.12.]

A bőség zavarát ellensúlyozva a következőkben az informatikai szakterületekre (összesen 6 kompetenciakör) koncentrálunk, melyek a következők:

- informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver) 82 fő
- informatikai biztonság 79 fő
- informatikai rendszerek tervezése, szervezése 94 fő
- stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység 23 fő
- számítástechnikai adatbázis, adatstruktúrák 74 fő
- szoftverek 96 fő

A szerzői jogi esetekben (jelen írásban csak a számítógépi programalkotásokkal foglalkozunk) a szoftver szakterület kijelölését követően a Captcha teszten (Completely Automated Public Turing Test To Tell Computers and Humans Apart) túljutva választható ki a szakértő személye.

Hasonló, bár nem jogszabályból fakadó kötelezettségen alapul a Magyar Igazságügyi Szakértői Kamara nyilvántartása, mely a http://miszk.hu/igazsagugyi-szakertoi-nevjegyzek címen érhető el[131]. Itt az előzőnél egyszerűbben – az ember/gép teszt kihagyásával – juthat el a kirendelő a szakértő elérhetőségeihez. A hagyományos papír alapú keresést előnyben részesítők a MISZK által 2010-ben kiadott Igazságügyi szakértői kézikönyvben[132] is kereshetnek.

ÁRAJÁNLAT-KÉRÉS

Az elmúlt néhány évben gyakorlattá vált a nyomozó hatóságok részéről az előzetes árajánlat kérése három vagy több szakértőtől. Ez több kérdést vet fel: a szakértőnek meg kell ismernie a feladat részleteit ahhoz, hogy pontos árkalkulációt tudjon készíteni. A szerzői joggal kapcsolatos ügyekben az árajánlatkérés vizsgálandó számítógépek, vagy adathordozók mennyiségének megadásában merül ki:

- 12246 db CD/DVD elemzése eredetiség megállapítása, jogtulajdonos azonosítása NAV
- számítógépek és navigációs készülékek vizsgálata házkutatás során NAV
- 1 db számítógép, 45 db CD/DVD vizsgálata Rendőrség[133]

[131] A MISZK honlapjának 2017 áprilisában történt átalakítását követően a névjegyzék átmenetileg nem érhető el

[132] HORVÁTH Gyöngyi dr., KUTACS Mária dr., SOÓS László dr., VAJDOVITS Éva dr.: Igazságügyi szakértői kézikönyv Budapest, 2006. HVGOrac

[133] MÁTÉ István Zsolt: Szakértői ügynyilvántartás/árajánlatok. 2014. (elektronikus)

Mivel az igazságügyi informatikai szakértők a büntetőeljárásban kötött (4 000 Ft/óra) óradíjjal dolgoznak, az árajánlat inkább nevezhető árkalkulációnak, illetve költségkalkulációnak, mint árajánlatnak. Tartalma szerint a várható munka mennyiségének meghatározásán alapul, amely a fenti példa alapján csak szakértői tapasztalatból következő becslés lehet.

Az ajánlatkérést követően 2–3 héttel, esetenként 1–2 hónappal később kerül sor a szakértő kirendelésére, mely a legalacsonyabb ár alapján történik. A szakértők gyakran nem kapnak visszajelzést arról, hogy nem fogadták el az árkalkulációjukat, csupán a kirendelés hiányából következtethetnek erre a tényre.

Bíróság általi szakértő kirendelésnél – akár szerzői joggal kapcsolatos a büntetőügy, akár más területet érint – a bíróság nem kér előzetes árkalkulációt. A szakértő egyes esetekben a végzés kézhezvételekor értesül a kirendelésről, más esetekben a bírósági titkár, vagy tisztviselő, ritkábban maga a bíró keresi meg előzetesen a szakértőt, egyeztetve a kompetencia területet és az üggyel kapcsolatos egyéb körülményeket (elfogultság, szabad szakértői kapacitás stb.).

KIRENDELŐ HATÁROZAT/VÉGZÉS

A nyomozó hatóság a szakértő kirendelését kirendelő határozattal kezdeményezi, melyet leggyakrabban a vizsgálandó eszközök átvételekor kap kézhez a szakértő. Ha nem történt előzetes egyeztetés (az árkalkuláción kívül), a szakértő ekkor kerülhet először az ügy tényleges tartalmával kapcsolatba, illetve ekkor lehet tisztázni az esetleges elfogultsággal kapcsolatos kérdéseket is.

Valamennyi ügytípus esetén fontos a szakértőnek feltett kérdések megfelelő minősége. A szerzői jogot érintő ügyek leggyakoribb, vagy legtipikusabb kérdései a következők (valamennyi idézett szöveg a saját szakértői archívumból származik):

1 SZ. MINTA

Laboratóriumi vizsgálat (egy tétel) kirendelő határozata (kirendelő hatóság: Rendőrség):

(1) A szekértő állapítsa meg tételesen, hogy a lefoglalt winchester milyen programokat tartalmaz és azok teljes, shareware stb. verziók-e.
(2) A teljes értékű programok esetén állapítsa meg, hogy eredetiek, vagy másoltak, ki a jogtulajdonosuk és másolásukkal mekkora az okozott vagyoni hátrány.
(3) A szakértő csoportosítsa az illegális programokat összesítő táblázatban, mely összefoglalóan tartalmazza a sértett jogtulajdonosokat és a részükre okozott vagyoni hátrányt.
(4) A szakértő állapítsa meg, hogy a fenti számítógépen teljes értékű, illegálisan telepített programok mikor és milyen telepítési névvel lettek feltelepítve az adott számítógépre.

(5) A szakértő terjessze elő mindazon észrevételét, amit az ügy érdemi elbírálása szempontjából fontosnak tart.

2 SZ. MINTA

Laboratóriumi vizsgálat (több tétel) kirendelő határozata (kirendelő hatóság: Rendőrség):

(1) A szakértő állapítsa meg tételesen, hogy a lefoglalt winchesterek, CD- és DVD lemezek milyen programokat tartalmaznak és azok teljes shareware stb. verziók-e.
(2) …

3 SZ. MINTA

Helyszíni vizsgálat kirendelő határozata (kirendelő hatóság: NAV):

(1) Szükséges megállapítani, hogy a házkutatás során talált GPS készülékeken, számítógépeken, illetve adathordozókon található-e iGO Primo szoftver.
(2) Továbbá szükséges ezen szoftverek telepítésének, licenc számának és verziójának helyben történő meghatározása.

4 SZ. MINTA

Laboratóriumi vizsgálat (a nyomozási szakaszban kiadott szakértői vélemény kiegészítése a bírói szakaszban felmerült új adatok miatt) kirendelő határozata (kirendelő: Bíróság):

1) A vádlott által a 2013.××.××- én tartott tárgyalás során becsatolt software-ek megfeleltethetők-e a vád tárgyát képező és az eljárás során a vádlottól lefoglalt számítógépen, illetve adathordozókon talált software-ek eredeti példányaként?
   a) A vádlott által használt számítógépen azonosított Mio Map. Mio 3.3, Mio C320. Mio CS20 és CorelDraw Graphics Suite X3 nevű programok származhatnak-e a becsatolt CD-kről, létrejöhettek-e a csatolt CD-k telepítése útján?
   b) A vádlottól lefoglalt 8 db optikai lemezen található Corel Draw 12, Windows Vista. Microsoft Office 2007 nevű software-ek lehetnek-e a becsatolt adathordozókról készített biztonsági másolatok?
2) A vádlott számítógépén nem eredetiként beazonosított licence file-ok származhatnak-e egy közös forrásból, azok tekinthetők-e egymás olyan variánsának, melyekben kizárólag a programot működtető eszköz képernyőjének felbontását, a GPS port számát, illetve a skint módosították? Amennyiben igen, úgy megállapítható -e, hogy ezek „forrása" a nyomozás során lefoglalt, CNS logóval ellátott SD kártyán található eredeti software lett volna?
3) Az IGO programhoz tartozó – korábban nem eredetiként azonosított – licenc fileok származhatnak-e a vádlott által becsatolt navigációs programokat tartalmazó CD-kről ?

4) Az eredeti IGO programot milyen módon lehetett frissíteni 2008 során? Szükség volt-e ehhez olyan felhasználói beavatkozásra, mely bizonyos adatállományok felülírásával, illetve a licence file módosításával járt, vagy a frissítési művelet automatikusan elvégezte ezeket?
5) A vádlott által becsatolt CorelDraw 9 jelzésű CD-n található program birtoklása lehetővé tette-e a felhasználó számára, hogy programját magasabb verziószámú (10, 11 vagy 12) alkalmazásra frissítse új program vásárlása nélkül?

A szövegek olvasásakor több megfigyelést tehetünk, melyek gyakoriságuk alapján kiterjeszthetők és kirendelési gyakorlatként is értelmezhetők. Az első szembeötlő tény az első és második minta hasonlósága, melyre a második minta esetén a … jelzés is utal. Azonos rendőri szerv azonos előadójától származik a két szöveg, két különböző ügyre vonatkozik és azt a gyakorlatot illusztrálja, melyet másolás/beillesztés, vagy copy/paste kirendelésnek nevezhetünk. Ebben az esetben egy korábban elkészített kirendelő határozat szövege él tovább és a változások csak az ügy specifikus adatokban jelennek meg (esetenként ott sem).

Ez a gyakorlat – értékítélettől függetlenül – felvet egy igényt, mely nem más, mint a kirendelések esetén használható szövegminták iránti igény. Nem véletlen, hogy egy-egy „jól sikerült" szöveg, vagy szövegrészlet éveken keresztül megjelenik a kirendelő határozatokban. Természetesen ellenpélda is akad, amikor elírások ismétlődnek éveken keresztül, mint a következő példában:

5 SZ. MINTA

Laboratóriumi vizsgálat (adócsalás bűntett) kirendelő határozata (kirendelő hatóság: VP):

1) Az átadott laptopok merevlemezein található adattartalmat lehetőség szerint kérem számítástechnikai adathordozókra (DVD lemezre) archiválni, kiemelten a Microsoft World (sic!), Excel fájlokat, dokumentumokat, e-mail-eket, belső levelezéseket, valamint minden szöveges fájlt.

A második megfigyelés, mely szintén általánosítható a szerzői joggal kapcsolatos ügyek esetén, az „okozott vagyoni hátrány" meghatározása. Ez a szófordulat a copy/paste kirendelés tipikus következménye, s egyben a bírói hatáskör (jogkérdés eldöntése) átruházása a szakértőre.

Az idézett módon feltett kérdésekkel kapcsolatosan legalább két szakértői magatartás lehetséges: elsőként a kirendelő határozatban szereplő kérdés(ek) utólagos, szakértő általi kijavítása. Ez semmiképpen nem javasolható eljárás, még akkor sem, ha logikailag helyes eredményre vezetne, hiszen a kialakuló személyközi feszültség (előadó vs. szakértő) csökkentheti az eljárás eredményességét. A másik (ajánlott) módszer a kiren-

delő határozat szövegének jogszabályszerű értelmezése, vagyis ahol a határozat vagyoni hátrányt említ, ott a szakértő nettó kiskereskedelmi árat fog megadni, ahogy azt a Szerzői Jogi Szakértői Testület (erről később még részletesen szólok) egyik szakértői véleménye is teszi.[134] Ez a megoldás egyrészt biztosítja a jogszerű magatartást az igazságügyi informatikai szakértő részéről, másrészt nem zavarja meg az ügy előadója és a szakértő közötti emberi viszonyrendszert sem.

Az SZJSZT imént idézett szakértői véleménye csak akkor alkalmazható, ha a kirendelő hatóság (vagy a bíróság) feltett kérdésében nincs az ÁFA tartalomra vonatkozó határozott utalás. Ha a kirendelő tételesen kéri az ÁFÁ-val növelt összeget (lásd a következő példában), akkor a szakértő a fentiekben írt megoldást nem alkalmazhatja.

6 SZ. MINTA

Laboratóriumi vizsgálat [régi Btk. 329/B. § (1) bekezdés b) pontja alapján] kirendelő határozata (kirendelő hatóság: Rendőrség):

1) A vizsgálatra megküldött adathordozókon találhatók-e olyan adatok, szoftver programok, melyek sértik a szerzői jogokat?
2) Amennyiben igen, akkor kérem, hogy szíveskedjen megállapítani, kinek a jogai sérültek, hány esetben, ki a jogtulajdonos, és jogsértés estén külön-külön, adathordozókra és jogtulajdonosokra lebontva, mekkora az okozott vagyoni hátrány ÁFÁval növelt értéke.

Folytatva a megfigyelések bemutatását, nézzük meg a helyszíni vizsgálat (házkutatás során végzett szakértői munka) kirendelő határozatának részletét a 3. sz. mintában. Jól érzékelhető, hogy a kirendelést adatgyűjtés előzte meg, melynek során a nyomozók valószínűsítették, hogy a házkutatás helyszínén milyen eszközöket (navigációs készülékek, számítógépek és adathordozók) és milyen szoftvereket (iGO Primo) találnak majd. A megfelelő előkészítés rendszerint hozzájárul a házkutatás sikeréhez, esetenként azonban a nem megbecsülhető tényezők módosíthatják a vizsgálat irányát. A 3. sz. mintához tartozó ügyben a vizsgálat helyszínén négy darab számítógép került előtalálásra, a számítógépek összes tárolókapacitása 4 490 GB volt, ami kb. 1 000 db hagyományos DVD lemez tárolókapacitásának felel meg. A kérdéses esetben a helyszínen csak annak megállapítása történhetett meg, hogy az egyes eszközök tartalmaznak navigációs szoftver mentéseket, de ezek értékelése és egyenkénti mentése laboratóriumi vizsgálat során vált csak lehetségessé (időfaktor!).

A nyomozási szakasz során adott szakértői vélemények kiegészítése válik szükségessé a bírói szakaszban, amennyiben a vélemény tartalma nem pontosan érthető (homályos), vagy új adatok merülnek fel, mint a 4. sz. minta esetén. Időnként előfordul, hogy

[134] Szerzői Jogi Szakértő Testület: SZJSZT 15/2000/1-2. sz. szakértői vélemény. 2000. p.2. http://www.sztnh.gov.hu/testuletek/szjszt/SZJSZT_szakvelemenyek/2000/2000PDF/szjszt_szakv_2000_015.pdf, [2014.01.15.]

az ügy azonosítása nem egyértelmű, tekintettel arra, hogy a bírói végzések nem tartalmazzák a nyomozási szakaszban kapott, a nyomozó hatóság által kiadott ügyszámot (formátuma: hatóság_azonosító/ügyszám/évszám ügytípus), illetve a szakértő saját ügyszámát sem, így az eset visszakeresése némi időt vehet igénybe. Tekintettel arra, hogy a nyomozási szakasz és a bírói szakasz között hosszú idő is eltelhet, a keresést megkönnyítheti, ha a szakértő felveszi a kapcsolatot a végzést kiállító bíróval és bekéri az azonosításhoz szükséges adatokat.

A 4. sz. minta tartalmi értékelésekor kiemelendő, hogy a feltett kérdések pontosan meghatározott tárgyhoz kötődnek (különösen a korábban tárgyalt mintákkal összevetve), mindazonáltal a körülmények gondos megfogalmazásán (különösen a szóhasználaton) érződik az informatikai specializáció hiánya. Ez olyan fontos kérdés, hogy az ügyek bizonyítási és bemutatási szakaszáról szóló részben visszatérünk rá.

A kirendelő határozat/végzés átvétele az egyes esetekben különböző: a nyomozó hatóság általi kirendelésnél az eszközök átvételekor, vagy a házkutatásnál történő közreműködés esetén a házkutatás megkezdését megelőzően kerül rá sor. A bírósági kirendeléseknél a postán keresztüli továbbítás a legáltalánosabb forma, az esetleges eszközök átvétele a kirendelő végzés (és az igazságügyi szakértői igazolvány) felmutatásával történik meg a kirendelő bíróság megfelelő ügykezelő csoportjánál.

A szakértői vizsgálat

Amint azt a korábbiakban láthattuk, a szerzői joggal kapcsolatos ügyekben a vagyoni jogok megsértésével összefüggésben az egyes szoftverek státuszának, majd abból adódóan a nettó kiskereskedelmi árnak a meghatározása a szakértő feladata. A másik ügytípusban a szerzői jog védelmére szolgáló műszaki intézkedés megkerülésének igazolása, vagy elvetése a vizsgálat tárgya.

Az ügyek közös tulajdonságai közül elsőként említendő az a tény, hogy kizárólag Windows operációs rendszer környezetben működő szoftverek vizsgálata zajlott a jelen írás alapjául szolgáló 24 esetben. Ez természetesen nem zárja ki a más működtető rendszereken futó programokkal történő visszaélést (különféle UNIX változatok, Linux disztribúciók, MacOS verziók, vagy más, egzotikus rendszerek), ugyanakkor utal arra, hogy a személyi/irodai használat ezeken a rendszereken (Windows különböző verziói) a leggyakoribb, ezáltal a szerzői jog megsértése is erre a környezetre koncentrálódik. Az egyéb rendszerekre vonatkozó gyakorlati példák (esetek) hiányában a következőkben a Windows rendszerek környezetében történő jogsértések vizsgálatára koncentrálunk.

Vagyoni jogok megsértésével kapcsolatos ügyek vizsgálata

A vagyoni hátrányt a bíróság állapítja meg, így a szakértő a nyomozáshoz, a vádemeléshez, majd a későbbi bírói döntéshez szükséges alapanyagot szolgáltatja. Ez vonatkozhat a számítógépes rendszer különféle komponenseire:

- operációs rendszer,
- segédprogram,
- irodai programcsomag,
- grafikai alkalmazás,
- játékprogram.

Az egyes szoftverek használatára vonatkozó adatokat elsődlegesen a regisztrációs adatbázis tartalmazza, melynek állományai alaphelyzetben a \WINDOWS\system32 \config könyvtárban találhatók. A bizonyításhoz ennek a könyvtárnak a tartalmát kell menteni oly módon, hogy az adattartalom közben ne módosuljon. Ennek részleteiről itt terjedelmi okokból nem tudunk szólni, de más írásokban[135] részletesen megtalálható a vonatkozó követelményrendszer[136]. A szoftverek telepítési adatait a software állományból tudjuk kinyerni. Az operációs rendszerre vonatkozóan a következő táblázatban található formátumú adatokat (a product key értéke anonimizált) kapunk:

21. táblázat - Windows Install értékei a regisztrációs adatbázisból

Property	Value
ProductName	Microsoft Windows XP
Owner	ADMIN
Organization	
ProductID	55274-648-2936177-23006
ProductKey	PYFYH-xxxxx-Q2TFB-xxxxx-32X84
ProductVersion	Uniprocessor Free 5.1.2600.xpsp.080413-2111
InstallDate	2009.01.18 17:46
ServicePack	Szervizcsomag 3
SystemRoot	C:\WINDOWS

[135] MÁTÉ István Zsolt: A digitális bizonyíték. in Konferenciakötet - Jogász Doktoranduszok Országos Szakmai Találkozója. Károli Gáspár Református Egyetem Állam- és Jogtudomány Kar. 2014.
[136] MÁTÉ István Zsolt: A bizonyítékok kezelése - az igazságügyi informatikai szakértő a büntetőeljárásban. in Konferenciakötet - Rendészeti Ágazat Doktoranduszainak V. Országos Fóruma. Rendészeti Doktoranduszok Országos Egyesülete.

A telepített programok adatait az előző példában látotthoz hasonlóképpen tudjuk kinyerni. A termékkulcsok kinyeréséhez esetenként speciális programra van szükség (Magical Jelly Bean Keyfinder, productkeyexplorer stb.). A kinyert adatokon kívül szükséges a teljes fájlrendszer átvizsgálása abból a célból, hogy a regisztrációs adatbázisban nyomot nem hagyó szoftverek és a telepítő készletek (tárolt szoftver) helyét is azonosítani tudjuk. A további munkához a következő adatok szükségesek:

- a szoftver megnevezése, verziószámmal együtt,
- a szoftver gyártójának a megnevezése (amennyiben tárolódik a regisztrációs adatbázisban),
- a telepítés, vagy mentés időpontja.

A felsorolás első két tétele az azonosításhoz nélkülözhetetlen, a verziószám, illetve a telepítés, vagy mentés időpontját pedig a kiskereskedelmi ár meghatározásánál használhatjuk fel. A rendelkezésre álló információk mellett szükséges az egyes szoftverek (különösen a shareware termékek) licensz feltételeit tartalmazó állományok beszerzése is (ezek gyakran a telepítési könyvtárban, vagy a telepítő csomagban megtalálhatók, illetve a gyártó weboldalán hozzáférhetők). A licensz szövegéből megtudhatjuk az esetleges kipróbálási időszakra vonatkozó szabályokat és azt összevethetjük a telepítési dátum adataival.

Fontos hangsúlyozni, hogy a telepítési dátum és idő nem abszolút értékű (nem a szó einsteini értelmében tekintve azt), azonban a számítógép-használati szokások megfigyelése alapján nagy valószínűséggel állíthatjuk, hogy az adott számítógép rendszerideje és a helyi (zóna) idő jelentősen nem tér el egymástól, hiszen az a számítógép üzemszerű használatát tartósan és kedvezőtlenül befolyásolná.

Mindezeket figyelembe véve megkezdődhet a vizsgálat legkimerítőbb szakasza: a szoftverek azonosítása és az adott időszakra vonatkozó nettó kiskereskedelmi ár meghatározása.

A vizsgálattal kapcsolatos leggyakoribb problémák a következők:

- a termék életciklusa lezárult,
- a termék gyártóját felvásárolták (esetleg többször is),
- a termék adott verziószámára vonatkozóan nincs árinformáció,
- a terméket Magyarországon nem forgalmazták.

Mivel jelenleg nincs egységes gyakorlat az igazságügyi informatikai szakértői vizsgálatok területén,[137] ezért egyéni, de következetesen véghezvitt eljárási gyakorlatot kell minden szakértőnek kialakítania, erre látunk egy példát az alábbiakban.

[137] MÁTÉ István Zsolt: Digital Forensic Science – szabványosítási törekvések „régen" és ma. in Konferenciakötet – ISZAK2013 konferencia. Budapesti Igazságügyi Szakértői Kamara, 2013. p.6.

Az egyes szoftverek nettó kiskereskedelmi árát a nyilvános árlisták tartalma alapján határozhatjuk meg oly módon, hogy az adott verzióra az adott időszakban érvényes legkisebb nettó árat vesszük figyelembe, vagy több különböző ár-információk esetén azok átlagát (számtani közép értékét) képezzük. A legegyszerűbb esetben rendelkezésre áll az adott szoftver adott verziójának nettó kiskereskedelmi ára forintban. Amennyiben a termék magyarországi forgalomban nem beszerezhető, úgy a külföldi nyilvános árlistákat vehetjük alapul. Itt a szoftver árát az adott napra érvényes deviza középárfolyammal válthatjuk át forintra a kérdéses pénznemből (leggyakrabban USD, EUR és GBP). Az árak összesítését forintban végezzük oly módon, hogy a szakértői vélemény szövegében pontosan feltüntetjük a számítási módot és az adatok forrását, például a következőképpen:

„A szoftverek kiskereskedelmi árának megállapításakor – amennyiben elérhető volt – a magyarországi kiskereskedelmi árakat alkalmaztam, amennyiben ez nem volt beszerezhető, úgy a nemzetközi online kereskedelem árait vettem figyelembe, USD, EUR és GBP pénznemekben. Az árak átváltásánál a Magyar Nemzeti Bank adott napon érvényes deviza középárfolyamát vettem figyelembe."[138]

Abban az esetben, ha az adott szoftver kérdéses verziószámára vonatkozó árat nem találunk, úgy az adatok interpolálásával becsülhetjük meg a vizsgálandó termék árát, ahogy azt a következő példa is mutatja:

„Amennyiben a kérdéses szoftver adott verziója nem volt már beszerezhető, a termék árát az elérhető verzió árából kalkuláltam a következők szerint: a fő verziószám értékének egy ponttal történő változását 10%-ban vettem figyelembe. Példa: 5.0 verzió ára = 8.0 verzió ára – 30%."[139]

A bemutatott példák természetesen több ponton vitathatóak, azonban egyéb irányelv, vagy módszertani útmutatás hiányában következetes alkalmazása egységesítheti egy-egy szakértő munkáját.

A vizsgálat során meg kell állapítani a jogtulajdonos kilétét és annak székhelyét, elérhetőségét. Az információk beszerzésének elsődleges forrásai a regisztrációs adatbázisból kinyert adatok, illetve a telepítési, vagy tárolási könyvtárban megtalálható szöveges tartalmú állományok (lincensz fájlok, leírások stb.). A következő forráscsoport az interneten elérhető termék, vagy gyártó honlapja lehet, ahol a Contact oldalon található információkat lehet felhasználni. Ennek hiányában a Whois szerverek, vagy nyilvános cégadatbázisok adatai alapján határozható meg a jogtulajdonos címe, amint azt a következő példa is mutatja:

[138] MÁTÉ István Zsolt: 22/2010. sz. igazságügyi informatikai szakértői vélemény in Szakértői archívum. 2010. p.7.

[139] MÁTÉ István Zsolt: 22/2010. sz. igazságügyi informatikai szakértői vélemény im. p.7.

Keresendő domain: ea.com (Electronic Art: Fifa××, Battlefield×, Titanfall stb.); kereső: oyetools.com; a keresés eredménye[140]:

…

Registrant Name:	Domain Administrator
Registrant Organization:	Electronic Arts Inc.
Registrant Street:	209 Redwood Shores Parkway
Registrant City:	Redwood City
Registrant State/Province:	CA
Registrant Postal Code:	94065
Registrant Country:	US
Registrant Phone:	+1.6506281500
Registrant Phone Ext:	
Registrant Fax:	
Registrant Fax Ext:	
Registrant Email:	hostmaster2@ea.com
Registry Admin ID:	

…

Amennyiben a szakértő a kinyert és feltárt adatokat adatbázisba szervezi, melyet az egyes ügyek megoldását követően a friss adatokkal bővít, úgy rendelkezésére áll egy komplex adatforrás, melyben időbeliségre vonatkozó információk is szerepelni fognak. Ezt az adatbázist a különféle termék-eladást támogató, vagy ajánlat-összegyűjtő honlapok ár/idő diagramjainak adataival is ki lehet egészíteni. Több szakértő privát adatbázisának egybeépítése, vagy közös szakértői adatbázis létrehozása kívánatos lenne, de ennek egyelőre nincsenek meg a pénzügyi feltételei. Az adatbázis (mintát lásd a következő táblázatban) kiépítését a Magyar Igazságügyi Szakértői Kamara Informatikai és Hírközlési Szakmai Tagozata támogathatná, a fenntartás költségeit a használati díjból befolyó bevételek révén teremthetné elő a tagozat.

22. táblázat - Szoftver adatbázis minta (a szerző adatbázisának részlete)

Szoftver	Jogtulajdonos/ Forgalmazó	Jogtulajdonos címe
18 Wheels Of Steel Voll Aufs Gas	SCS Software	23 Jana Masaryka 120 00 Prague 2 Czech Republic
18 Wheels os Steel: Haulin	SCS Software	23 Jana Masaryka, 120 00 Prague 2 Czech Republic
2 PopCap Zuma Deluxe	PopCap Games, Inc.	2401 4th Ave, Suite 810 Seattle, WA 98121

[140] Oyetools.com keresés: http://www.oyetools.com/search.php?target=ea.com&queryType=all [2014.01.17.]

Szoftver	Jogtulajdonos/ Forgalmazó	Jogtulajdonos címe
9Th Company	Lesta Studio	Russia, 198013, St.Petersburg Moskovsky Prospekt 18, Office 1
ACDSEE Pro 2	ACD Systems International Inc.	200 - 1312 Blanshard Street Victoria, British Columbia Canada V8W 2J1 Fax: 1.866.544.0291
ACDSee6 PowerPack	ACD Systems International Inc.	200 - 1312 Blanshard Street Victoria, British Columbia Canada V8W 2J1
AD Stream Recorder v3.3.2	Ardsoft	nem ismert
Age of Empires	Microsoft Magyarország Kft.	1031, Budapest, Graphisoft Park 3.
Akadémiai MoBiMouse Plus - Angol v5.0	Akadémiai Kiadó	Budapest XI. kerület, Prielle Kornélia u. 19/D
Alcohol 120%	Alcohol Soft	Noldevej 15 6372 Bylderup-Bov Bylderup-Bov, 6372 DK

Egyes esetekben a leggondosabban összeállított szakértői vélemény is kiegészítésre szorulhat akár a nyomozási, akár a bírói szakaszban. Ez utóbbi esetben a kiegészítés oka lehet az eredeti szakértői véleményben szereplő megállapítások, esetleg fogalmak pontosítása (amint azt a következő 2. esettanulmányban is látni fogjuk), illetve olyan új körülmények felmerülése, melyek az eredeti szakértői vélemény valamely részletét módosítják (lásd a 3. esettanulmányt).

ESETTANULMÁNY (2)

A ××× Városi Bíróság 2.B.×××/2009/××/III. sz. végzésében szakértői véleményének kiegészítésére hívta fel a szakértőt. A vádlott által használt számítógépen voltak olyan programok, melyeket csak tároltak, de nem futtattak. A bíróság kérte a jogdíjköteles programok telepített/tárolt megoszlás szerinti kigyűjtését. A kigyűjtés eredménye jogtulajdonosonként a következő táblázatban olvasható.

23. táblázat - Szoftverek jogtulajdonosonként összesített értéke

Összeg / Összesen	Állapot		
Tulajdonos	**tárolt**	**telepített**	**végösszeg**
Adobe Systems, Inc.		905 852	905 852
Autodesk		832 650	832 650
C. Ghisler & Co.	8 400		8 400
Corel Corporation	17 510		17 510
DigiCart Kft		583 200	583 200
Microsoft Magyarország Kft.	98 970	246 471	345 441
Nero AG		15 897	15 897
P. & A. America, Inc.		14 229	14 229
Végösszeg	124 880	2 598 299	2 723 179

Amint az a fenti példában látszik, legalább egy jogtulajdonos esetén előfordult, hogy az általa fejlesztett szoftverek tárolt és telepített állapotban is megtalálhatóak voltak. A példában ez három különböző szoftvert jelentett: Microsoft Windows XP Professional, Microsoft Vista Home Premium, Microsoft Office Professional Edition 2003. Nem ritka azonban az a jelenség, hogy egy adott szoftver több példányban, adott esetben telepítő készlet, telepítő készlet image állományban, telepítő készlet tömörített állományban változatokban is előfordul. Különösen a navigációs programokra jellemző, hogy a vizsgálat alá vett számítógépeken több másolat található meg belőlük.

A fentiekben bemutatott „szoftvergyűjtési" gyakorlat a büntetőeljárás bírói szakaszában válik kulcsfontosságúvá, amikor a számítógépes programalkotások illegálisan használt, vagy tárolt darabszámának a meghatározása válik szükségessé. Megfigyelésem szerint nincs egységes gyakorlat e kérdés megítélésében, s a szakértő részletesen kimunkált véleményében szereplő darabszámok így alku tárgyává válhatnak a tárgyalás során.

A bírói szakaszban is felmerülhetnek új adatok, melyek a szakértői vélemény kiegészítésére és/vagy annak szóbeli „megvédésére" adhatnak okot. Ilyenek lehetnek például a vádlott által utólag becsatolt szoftver licenszek, eredeti telepítő készletek és más hasonló adatok, ahogy azt a következő esettanulmányban is látni fogjuk.

ESETTANULMÁNY (3)

> *„A ××× Bíróság Budapesten, 2013. ××× ××. napján - tárgyaláson kívül meghozta az alábbi*
>
> *VÉGZÉST*
>
> *A bíróság a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésnek vétség és más bűncselekmények miatt ××× ××× ellen folyamatban lévő büntetőügyben a szakértői vélemény (67/2009.) kiegészítését rendeli el.*
>
> *…*

A vádlott által a 2013 . ××× ×××- én tartott tárgyalás során becsatolt software-ek megfeleltethetők-e a vád tárgyát képező és az eljárás során a vádlottól lefoglalt számítógépen, illetve adathordozókon talált software-ek eredeti példányaként?

…

A vádlott által becsatolt CorelDraw 9 jelzésű CD-n található program birtoklása lehetővé tette-e a felhasználó számára, hogy programját magasabb verziószámú (10, 11 vagy 12) alkalmazásra frissítse új program vásárlása nélkül?"

A korábbiakban a 4. sz. mintában már bemutatott eset egy részletét most más szemszögből tekintjük át ismét. Az új adat felmerülése – szoftver műpéldányok becsatolása – tette szükségessé a szakértői vélemény kiegészítését, illetve a vádlott védekezése, mely azon alapult, hogy a becsatolt műpéldányokról díjmentesen frissíthette az adott alkalmazást.

A szakértő ebben a helyzetben az általa kötelezően tárolandó szakértői véleményét tekintheti át, mely ebben az ügyben négy évvel korábban készült. Az ügy kapcsolódó adataira (digitális bizonyítékok) nem vonatkozik a kötelező tárolás, a szakértő saját döntésén alapulhat a bizonyításhoz mentett tartalmak megőrzése. Amint azt másutt[141] már részletesen kifejtettem, azon álláspontot támogatom, miszerint a szakértő az egyes ügyek mentett digitális bizonyítékait saját szakértői archívumában tárolja. Jelen esettanulmány példája is azt mutatja, hogy a rendszer működése szempontjából hasznos az adatok tárolása, mely szükségtelenné teszi a korábban vizsgált eszköz ismételt vizsgálatát. Ugyanakkor felveti azt a kérdést is, hogy a digitális bizonyítékok tárolásának költségei mi módon kerülnek megtérítésre.

A szakértői archívum és az újonnan becsatolt bizonyítékok összevetése során ebben az ügyben a licensz szerződések vizsgálata kapta a központi szerepet. Olyan fogalmak használata és magyarázata vált szükségessé, mint a System Beta 2 Kit, Release Candidate, vagy az Academic licensz.

Ebben az esetben a szakértő egy szerződést értelmez, ami látszólag túlmutat a kompetencia területén, lévén a szerződések jogi természetű iratok. Az ellentmondás feloldása a műszaki tartalom értékelése és annak bemutatása révén nyilatkozik meg, ahogy azt a következő példában is látjuk:

„Az Academic változat felhasználása a Corel Corporation végfelhasználói licensz szerződése szerint kizárólag oktatási célokat szolgálhat:

„A szoftver akadémiai változatai nem használhatók kereskedelmi, szakmai vagy egyéb nyereségorientált célokra."

[141] MÁTÉ István Zsolt: A bizonyítékok kezelése - az igazságügyi informatikai szakértő a büntetőeljárásban. in Rendészeti Ágazat Doktoranduszainak V. Országos Fóruma konferenciakötet. 2014.

Az Academic licensz teljes leírása az http://www.corel.com/en/eula/ címen olvasható, angol nyelven (ACADEMIC SOFTWARE rész).

Az Corel Corporation üzleti és oktatási licencei között mintegy nyolcszoros árkülönbség figyelhető meg (CorelDRAW X6 változat esetén), ezért az üzleti és oktatási licencek között nincs átjárás (upgrade). A cég üzletpolitikája alapján rendszerint az adott szoftver kettővel korábbi verziójáról lehet kedvezményes áron frissítést vásárolni. A CorelDRAW X6 változat esetében a CorelDRAW X5 és X4 változatokról lehet üzleti frissítést igényelni (aktuálisan 83.820 Ft + ÁFA)."[142]

A műszaki intézkedés megkerülésével kapcsolatos ügyek vizsgálata

Az előző példában tárgyalt egyszeresen és többszörösen tárolt szoftverpéldányokkal összefüggésben tárgyalhatjuk a szerzői jog védelmére szolgáló műszaki intézkedés megkerülését célzó „megoldások" vizsgálatát is. A leggyakoribb formája e jogsértésnek a kódgenerátorok (keygen), a feltört és módosított programkódok (cracked program) és a különféle (többnyire mennyiségi licensz-konstrukciókból származó) legális sorozatszámok „újrafelhasznált" változatainak tárolása.

A vizsgálat alá vont számítógépeken és tárolókon megtalálható könyvtárszerkezetek gyakran utalnak a bennük található tartalomra (a felhasználó is ez alapján azonosítja a tartalmakat), így a szakértő a tárolókról készített tartalomjegyzékben az előzőekben felsorolt kulcsszavakra szűrve megtalálhatja a gyanús tartalmakat.

ESETTANULMÁNY (4)

A Nemzeti Adó- és Vámhivatal ××× Regionális Bűnügyi Igazgatósága a Btk. 329/A. § (1) bekezdés I. fordulatába ütköző és a (3) bekezdése szerint minősülő szerző vagy szerzői joghoz kapcsolódó jogok megsértése bűntettének gyanúja miatt folytatott nyomozás során házkutatást tartott, melynek során az ××× által fejlesztett navigációs szoftverek 63 műpéldányát találta meg a szakértő a vizsgálat alá vont számítógépeken és adathordozókon. A szoftver műpéldányok mellett – az alábbiak szerint – kódgenerátor programok és a hozzájuk tartozó leírások is megtalálhatóak voltak:

\Keygenek\ Garmin GMAPSUPP.IMG key editor V0.2\ GarminKeyTool.exe

\Keygenek\ Garmin GMAPSUPP.IMG key editor V0.2\readme.txt

„Garmin img fájlok adatainak kiolvasására. (mapID, nyitókód)"

Más könyvtárakban útmutatásszerű leírások voltak megtalálhatók a sorozatszámok használatára vonatkozóan, amint azt a következő példában is láthatjuk:

[142] MÁTÉ István Zsolt: 10/2013. sz. igazságügyi informatikai szakértői vélemény. Máté István Zsolt, 2013. p.3. (nem nyilvános irat)

„Telepítés:

Kapcsolja ki az internetet!

A telepítés után indítsa el a szoftvert, a térkép aktiváláshoz válassza az "online"

aktiválást, illessze be a serialt mind a két csíkba okézni. A pc-én meg lehet tervezni az

útvonalat, és töltse fel az új térképet GPS készülékére!

serial: CD3C×××××7GY3×××××W68WQ66"

A szoftveres megoldások mellett, de jelentősen alacsonyabb számban előfordulnak a műszaki intézkedések hardveres módon történő kijátszására tett kísérletek. Ezekben az esetekben az informatikai eszközt – többnyire játékkonzolt – teszik „alkalmassá" másolt tartalmak futtatására. Az ügyek bizonyítékai között megtalálható (PlaySation játékkonzolok esetén) a MOD BO 760 chippel felszerelt áramköri panel a PlayStation játékkonzol alaplapjával összeforrasztva, vagy önállóan, a „chip tuning" beépítési leírása, a módosított gépen futó másolt játékprogramok.

ESETTANULMÁNY (5)

Aktualitásánál és tárgyánál fogva is ide kívánkozik az Európai Bíróság által a C-355/12. sz. ügyben hozott ítélete. A Nintendo vállalatok valamint a PC Box és 9Net között folyamatban lévő ügyben az előzetes döntéshozatal iránti kérelem az információs társadalomban a szerzői és szomszédos jogok egyes vonatkozásainak összehangolásáról szóló, 2001. május 22-i 2001/29/EK európai parlamenti és tanácsi irányelv 6. cikkének értelmezésére irányult.[143]

A Nintendo vállalatok által előterjesztett kérdések az 4. sz. mini esettanulmányban ismertetetthez hasonló, de azt „ipari" mennyiségben megvalósító cselekményre vonatkoznak. A Nintendo vállalatok által forgalmazott DS és Wii konzolokon csak a gyártó által megfelelő kóddal ellátott fizikai adathordozókat lehetett lejátszani (a gyártó szándéka szerint), ezzel megakadályozva a jogdíjköteles játékok illegális másolatainak használatát. Ez a megoldás egyben megakadályozta azon játékok futtatását is, melyek nem a Nintendo vállalatoktól származtak.

A PC Box mod chipeket és game copiereket (működés módosító áramkör és játék másoló) forgalmazott saját honlapján keresztül, melynek tárhely szolgáltatója a 9Net volt. A Nintendo vállalatok szerint a PC Box és a 9Net elsődleges célja a játékok védelmére

[143] Bírósági ítélet a C-355/12. sz. ügyben. http://curia.europa.eu/juris/document/document.jsf?text=&docid=146686&pageIndex=0&doclang=hu&mode=req&dir=&occ=first&part=1&cid=631579 [2014.01.26.]

szolgáló műszaki intézkedés kijátszása volt, míg a PC Box álláspontja szerint a konzolokat alkalmassá tették azok teljes kihasználására, azaz a gyártótól független szoftverek is futtathatóvá váltak a módosítás révén.

Terjedelmi okokból most csupán a bíróság döntésének lényegi elemeit emeljük ki: a 2001. május 22-i 2001/29/EK európai parlamenti és tanácsi irányelvben szereplő „hatásos műszaki intézkedés" nem csupán a szerzői jog jogosultja által védeni kívánt művek hordozójába, hanem az ahhoz hozzáférést biztosító eszközökbe beépített megoldásra is vonatkozik. Ez kissé leegyszerűsítve azt jelenti, hogy a játékkonzolokba épített védelem megfelel az idézett irányelvnek. (Megjegyzendő, hogy az ítéletet a fentiektől eltérő megközelítésben interpretálták egy hazai hírportálon,[144] ezért javasolt az eredeti ítélet tanulmányozása.)

Az Európai Bíróság ugyanakkor a nemzeti (olasz) bíróság elé utalta annak megvizsgálását, hogy a harmadik fél (független gyártó) tevékenységét kevésbé korlátozó megoldások és azok bevezetése milyen költségeket és milyen hatásokat vonnak maguk után. Ugyanígy a nemzeti bíróságnak kell megítélnie azt is, hogy mi a célja a műszaki intézkedést megkerülő eszközöknek.

[144] Jogszerűnek nyilvánította a másolásvédelmek feltörését az EU http://pcforum.hu/hirek/15776/Jogszerunek+nyilvanitotta+a+masolasvedelmek+feltoreset+az+EU.html [2014.01.31]

Az igazságügyi informatikai szakértői vélemény

Az előzőekben bemutatott szerzői joggal kapcsolatos vizsgálatok eredményét a szakértő igazságügyi informatikai szakértői véleményben foglalja össze. Tartalmáról részben a Szaktv[2005]/ Szaktv[2016]., részben pedig a 31/2008. (XII. 31.) IRM rendelet az igazságügyi szakértői működésről (Iszm.) szabályozza. Kötelező tartalmi elemei az Iszm. 10. § (1) bekezdése szerint:

a) a vizsgálat tárgyára, a vizsgálati eljárásokra és eszközökre, a vizsgálat tárgyában bekövetkezett változásokra vonatkozó adatok (lelet),
b) a vizsgálat módszerének rövid ismertetése,
c) a szakmai megállapítások összefoglalása (szakmai ténymegállapítás),
d) a szakmai ténymegállapításokból levont következtetések, ennek keretében a feltett kérdésekre adott válaszok (vélemény).

A szakértői vélemény elsődleges felhasználói nem informatikai szakemberek, hanem nyomozók, ügyészek, ügyvédek és bírák. Ebből adódóan a szakértői vélemények elsődleges kommunikációs célja a közérthetőség. Ugyanakkor nem feledkezhetünk meg arról a körülményről sem, hogy a szakértői vizsgálat megismételhetősége érdekében a legrészletesebb szakmai kritériumoknak is meg kell felelnie. A követelmények teljesítésének leggyakoribb formája az adatok, megállapítások és a vélemény közérthető, míg a vizsgálati módszerek szakmai nyelven történő megfogalmazása.

Szerzői Jogi Szakértői Testület

A szerzői joghoz kapcsolódó ügyekben a módszertani leírás részben kell pontosan rögzíteni az egyes szoftverekre vonatkozó számítások részleteit. Ebben a szakértő elsődleges segítsége, mint iránymutatás a korábbiakban már említett Szerzői Jogi Szakértői Testület. A testület létrehozásáról és működéséről az Szjt. rendelkezik a 101. §-ban, ahol a feladatai is felsoroltatnak: „Szerzői jogi jogvitás ügyben felmerülő szakkérdésekben a bíróságok és más hatóságok szakvéleményt kérhetnek a ... szakértő testülettől”.

Bár a testület által kiadott szakértői vélemények az egyes ügyek szakkérdéseinek megválaszolására korlátozódnak, hatásuk ugyanakkor megfigyelhető az igazságügyi informatikai szakértők munkájától kezdődően az ügyvédi munkáig egyaránt.

Ennek talán legmarkánsabb kifejeződése a testület által SZJSZT 15/2000/1-2 számon kiadott szakértői vélemény, melyben a testület tagjai meghatározták a vagyoni hátrány kiszámításának néhány paraméterét. A szakértői vélemény második oldalának következő sorai gyakran hangzanak el a védelem részéről a tárgyalóteremben, s mutatnak egyben irányt a szakértők számára munkájuk egységes elvégzésére: „Az eljáró tanács az elnökség fent említett állásfoglalására is figyelemmel, fenn kívánja tartani azt a gyakorlatot, hogy a Testület az ilyen esetben a műpéldányok kiskereskedelmi árát veszi alapul vagyoni hátrányként, amelybe azonban az ÁFA-t nem számítja bele.”

A kiskereskedelmi ár forrására vonatkozóan is található információ az idézett szakértői véleményben, mégpedig a Szombathelyi Városi Bíróságnak a B.895/1994/6. számú ügyben hozott ítéletének indoklása formájában, mely szerint: „Ez az ár vagy a terjesztésre jogosult természetes vagy jogi személy valamelyikének nyilvános árlistájából tudható meg, vagy a szoftver előállítására vonatkozó szerződésből következik. Amennyiben több terjesztésre jogosult természetes vagy jogi személy és ezzel együtt több – egymástól eltérő – árlista létezik, elsősorban a szoftver eredeti forgalmazója vezérképviseletének árait kell figyelembe venni.”.

A fentiek alapján a szerzői joggal kapcsolatos ügyekben dolgozó igazságügyi informatikai szakértő a kalkulációjában hivatkozhat a Szerzői Jogi Szakértői Testület által kialakított gyakorlatra, mely a vagyoni hátrány számításának egységesítését is elősegíti.

Természetesen ez a megközelítés is vitatható, ez különösen a védői oldalról merül fel a következőképpen: a szakértő a kiskereskedelmi árat egy vagy több ár beszerzésével határozta meg, ha több árat vett figyelembe, akkor a legalacsonyabb, legmagasabb vagy átlag árat alkalmazta-e. Ezekre a kérdésekre – minthogy nem szakkérdések – a bíróság joga és feladata a választ megadni.

A szakértői vélemény kommunikáció-tudományi megközelítésben

Amint arról korábban szó esett, a szakértői vélemény célzott írásmű, nem csupán tartalmi szempontból, hanem a befogadók tekintetében is. Az információ megfelelő átviteléhez szükséges legfontosabb komponenseket vegyük most sorra:

Amennyiben a kommunikáció egyik „legegyszerűbb" modelljét vesszük alapul (Shannon-Weaver modell), akkor az alapvető szereplők jól azonosíthatók: Információ forrás/Adó – szakértő, Címzett/Vevő – kirendelő (nyomozó hatóság, ügyészség, bíróság), a kommunikációs Csatorna a szakértői vélemény.

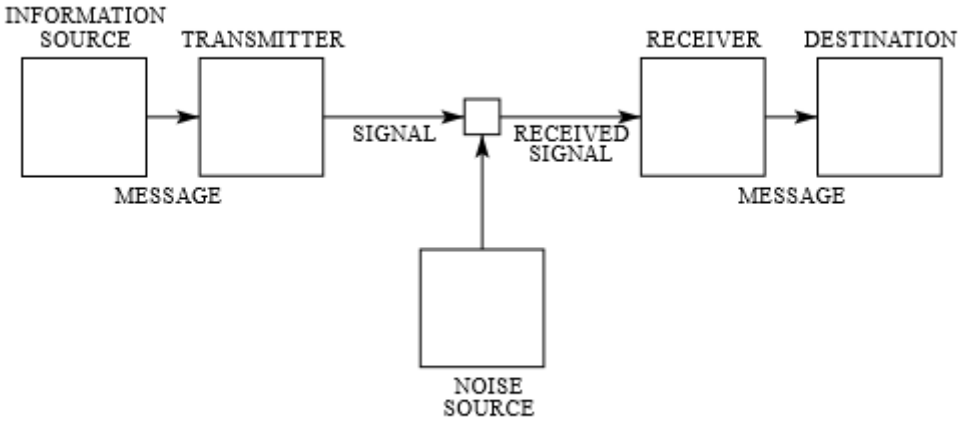


Fig. 1 — Schematic diagram of a general communication system.

10. ábra - Általános kommunikációs rendszer sematikus ábrája[145]

Árnyaltabban tekintve a vevő oldal (ahogy azt a korábbiakban részleteztük) egyszerre szakmai és nem szakmai közönség (ti. informatikai szakértő és kriminalisztikai és/vagy jogi szakértők). Ebből adódóan az Üzenet kódolásához szaknyelvi és köznyelvi megfogalmazást kell használnunk. Ennek legcélszerűbb formája a szakmai és köznyelvi tartalom elválasztása, melyet a szakértői vélemény módszertani részének és vélemény részének elkülönülése természetes módon szolgáltat a szakértő számára. Az így Kódolt üzenet eljuttatásánál figyelemmel kell lenni arra a körülményre, hogy a címzettek egy része a digitális tartalmakat különböző, itt nem részletezett okok miatt nem tudja fogadni, így a köznyelvi tartalomnak (jelenleg) mindenképpen a hagyományos nyomtatott szakértői vélemény formát kell tekintenünk.

[145] SHANNON, Claude Elwood: A Mathematical Theory of Communication. in The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948. p.2.

Bár a Shanon-Weaver modell a híradástechnikai szemléletből adódóan nem írja, nem írhatja le pontosan az emberi kommunikációt, még kevésbé annak egy speciális esetét, az igazságügyi informatikai szakértői vélemény által közvetített tartalmak működési mechanizmusát, mégis rávilágít azokra a kritikus pontokra, melyek meghatározzák a szakértői munka eredményességét. E szempontok részletes vizsgálata és összefüggéseik feltárása külön tanulmányt érdemel.

Összefoglalás

Az igazságügyi informatikai szakértő munkája – amint azt a szerzői joggal kapcsolatos ügyek körülményeinek áttekintése során felvillantottuk – komplex, interdiszciplináris felkészültséget igényel. Alapvető elem az informatika tudomány, melynek eredményeit, módszertanait és az abból adódó következtetéseket a kommunikáció tudomány által feltárt elméleti háttérre alapozott célirányosan kidolgozott gyakorlattal összekapcsolva interpretálhatjuk a jogtudomány által uralt közegben. E közegnek egy kis szelete a szerzői jog és a szerzői joghoz kapcsolódó jogok vizsgálata, melynek három évszádos alapjait napjaink digitális korszakváltása rengeti. Nem nehéz megjósolni, hogy a következő években számos változásra kell felkészülni ezen a jogi és informatikai szakterületen, ebből adódóan a szakértői vélemény kialakítás módszertani hátterének egyre jelentősebb szerep jut.

9.2.3 Szoftverrendszer fejlesztési költségeinek vizsgálata[146]

Az igazságügyi informatikai szakértő munkája során gyakran dolgozik célszoftverekkel, illetve szakértői módszertanok mentén, melyek segítik az információk hiteles kinyerését egy vizsgálat alá vett számítógépes rendszerből. Előfordulnak ugyanakkor olyan ügyek is, melyek megoldásához új módszereket, vagy módszertant kell alkalmazni. Ezek közé tartozik az egyedileg fejlesztett informatikai rendszerek fejlesztési költségének vizsgálata is.

Ebben a fejezetben bemutatásra kerül egy módszertan és annak kifejlesztési folyamata, mely segítségével jól közelíthető egy rendszer fejlesztési költsége abban az esetben, ha a vizsgálatot végző szakértőknek a fejlesztés során keletkezett iratok alapján kell munkájukat elvégezniük, s más információ nem áll rendelkezésükre.

A módszertan kidolgozásának folyamata esettanulmány keretében kerül bemutatásra, mely az 1978. évi IV. törvény (régi Btk.) 319. § (1) bekezdésébe ütköző és a (3) bekezdés d. pontja szerint minősülő különösen jelentős vagyoni hátrányt okozó hűtlen kezelés bűntettének gyanúja miatt ismeretlen tettes ügyében folytatott nyomozással összefüggő szakértői vizsgálat körülményeit részletezi, kitérve a szakértői vélemény módosításának lehetőségére új adat felmerülése esetén, a tartalom vizuális bemutatására és a minősített iratokkal történő szakértői munkára is.

Az adatok felhasználását a z igazságügyi szakértői tevékenységről szóló 2005. évi XLVII. törvény (Szaktv.[2005]) teszi lehetővé, melyben a 12. § (3) szerint: „Ha jogszabály másként nem rendelkezik, az (1) bekezdésben foglaltak nem zárják ki a szakértői vizsgálat során feltárt tényeknek és adatoknak tudományos vagy oktatási célra - személyazonosításra alkalmatlan módon - történő felhasználását.”, illetve ezzel azonosan a

Bevezetés

Az informatikai rendszerek tervezésével és kivitelezésével kapcsolatban induló büntetőeljárásokban szinte kivétel nélkül igénybe veszi a nyomozó hatóság az igazságügyi informatikai szakértő munkáját. A körülmények ugyan ügyről-ügyre változnak, ugyanakkor egyes közös vonások lehetővé teszik az egységes vizsgálati módszertan, vagy az arra vonatkozó javasolt vizsgálati eljárás kidolgozását és tesztelését.

Jelen írásban a nagy értékű fejlesztési projektek utólagos, projektdokumentumok és egyes működő szoftverkomponensek elemzése alapján történő értékelésére láthatunk módszertani példát, mely Máté István Zsolt és Begella Zoltán igazságügyi informatikai szakértők által került kidolgozásra a Nemzeti Adó- és Vámhivatal Bűnügyi Főigazgatósága Központi Nyomozó Főosztálya számára végzett, 01/2013 szakértői ügyszámú, igazságügyi szakértői vizsgálat során.

[146] A fejezetben az értékelési módszertan kidolgozása idején hatályos jogszabályokra történik hivatkozás

A szakértői kirendelés tárgya

A Nemzeti Adó- és Vámhivatal Bűnügyi Főigazgatósága Központi Nyomozó Főosztály ××× Osztály ×× nyomozást folytatott a régi Btk. 319. § (1) bekezdésében meghatározott és a (3) bekezdés d) pontja szerint minősülő különösen jelentős vagyoni hátrányt okozó hűtlen kezelés bűntett és más bűncselekmények elkövetésének gyanúja miatt ismeretlen tettes ellen folyamatban levő bűnügyben.

A büntetőeljárásról szóló 1998. évi XIX. törvény (Be.) 99.§ alapján a nyomozó hatóság kirendelte Máté István Zsolt igazságügyi informatikai szakértőt és – az ügy komplexitására és a feldolgozandó információ mennyiségére tekintettel, a kirendelt szakértő kérésére – társszakértőként Begella Zoltán igazságügyi informatikai szakértőt.

A vizsgálat során – a kirendelő határozat szerint – a következő kérdésekre kellett választ adniuk a szakértőknek:

> *„1. Kérem állapítsa meg a ××× rendszer szerződéskori piaci értékét összességében, illetve a vállalkozói szerződés mellékletében meghatározott ár táblázatban megjelölt bontásban is.*
>
> *Amennyiben a számított piaci érték és a vállalkozói szerződés mellékletében meghatározott összegek között eltérés van, határozza meg a különbözetet.*
>
> *a) Kérem állapítsa meg a Hardverek és Szoftverek szerződéskori piaci értékét,*
>
> *b) Kérem állapítsa meg a fejlesztési költségeket a fejlesztési idő és fejlesztői létszám figyelembe vételével." (NAV 60100-××/2010. bü.)*

A kirendelő hatóság a határozatban azonos tartalmú, a rendszer két további verziójára vonatkozó kérdések is szerepeltek, továbbá a rendszerek közötti kapcsolatok és különbségek részletes elemzése is. A vizsgálandó három fejlesztési projekt időbelisége mellett a kirendelő további három, azonos fejlesztési nagyságrendű, de eltérő szakterületre vonatkozó informatikai projekt megvalósítására vonatkozóan is feltette a fentiekben ismertetett kérdéstípusokat.

Szakértői kompetencia megállapítása

A szakértői vizsgálat megkezdését megelőzően az ügyben eljáró szakértőnek és társszakértőnek elsőként meg kell vizsgálnia, hogy a Be. 103. § szerinti kizárási okok nem állnak-e fent. Amennyiben egyik kizárási feltétel sem teljesül, úgy a szakértők megvizsgálják, hogy a kirendelés a kompetenciakörükbe tartozik-e.

Az igazságügyi szakértői szakterületekről a 9/2006. (II. 27.) IM rendelet (Szak. rend.) intézkedik, ahol az informatika vonatkozásában az alábbi szakterületeket adja meg:

1. informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver)
2. informatikai biztonság
3. informatikai rendszerek tervezése, szervezése
4. stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység
5. számítástechnikai adatbázis, adatstruktúrák
6. szoftverek

Bár mindkét kijelölt szakértő rendelkezett valamennyi, a fentiekben felsorolt kompetencia területre vonatkozó jogosultsággal, felmerült a kérdés, hogy a kirendelő határozat nem érint-e egyéb – pl. közgazdasági – szakterületet.

A kirendelő határozat kérdéseinek értelmezése során a szakértők megállapítottak, hogy a vizsgálat várhatóan a felsorolásban szereplő 1., 3. és 6. kompetenciaterületet érintik. Mivel a Szak. rend. nem korlátozta egyik felsorolt területen belül sem az informatikai szakértő véleményadási lehetőségét (pl. kivételek felsorolásával), ezért a szakértők megállapították, hogy a feltett kérdésekre saját kompetencia területükön belül válaszolni jogosultak.

Szakkérdések és jogkérdések elkülönítése, definíciók

A szakértői kirendelések esetén nem ritkán kéri a kirendelő jogkérdés eldöntését a szakértőtől. Ezek a kérdések gyakran az okozott kár, vagy az érték meghatározására vonatkoznak. Jelen vizsgálat esetében a szakértőknek az egyes felhasznált fogalmakat azonosítaniuk, illetve pontosítaniuk kellett, elkerülendő a szakértői vélemény későbbi kompetencia túllépésen alapuló támadhatóságát.

A szakértők a „piaci érték” fogalmát pontosították, illetve határozták meg részleteiben a vizsgálat megkezdése előtt:

A vizsgált rendszer piaci értéke

A vizsgált rendszerek egyedi fejlesztésű, meghatározott feladat elvégzésére kifejlesztett célrendszerek. Ennek oka az, hogy a szoftver egy adott ország, meghatározott jogszabályi keretei és működési körülményeire készült, azaz piaci alapon máshol más partnereknek nem értékesíthető. Ebből adódóan a szakértők a piaci értéket a fejlesztéshez felhasznált, hardver, szoftver, fejlesztési munkaóra és nyereség összetevőkből kalkulálták.

A szakértői véleményekben a fejlesztési érték és a piaci érték azonos tartalmú. Az összefoglalóban a szakértők a piaci érték kifejezést használják a fentiekben ismertetett tartalommal.[147].

A hardverek és szoftverek szerződéskori piaci értékének meghatározásánál a szakértők definiálták a fogalmi kereteket. Megállapították, hogy az egyes (vizsgált rendszerekre vonatkozó) szerződések hardver és szoftver komponensek üzembeállítását is tartalmazták.

Az egyes komponensek piaci értékét a termékek lista árából kalkulálták a szakértők. A kalkuláció során a hardver vagy szoftver külföldi devizában megadott árát vették figyelembe, mivel ezek (a vizsgálat időszak adatait figyelembe véve) kevésbé voltak változékonyak, mint az adott időszakra vonatkozó forint árak. A forintra történő átváltás valamennyi kalkuláció esetén egységesen az adott időszak deviza középárfolyamának átlagával történt. Amennyiben nem állt rendelkezésre a termék lista ára, úgy a termékhez legközelebb álló teljesítményű rendszer (hardver) árát vették figyelembe a szakértők, szoftverek esetében pedig az adott rendszer magasabb verziószámú változatának árát használták a kalkuláció alapjául.

A forrásadatok minőségéből adódó pontatlanságot a szakértők a véleményalkotás részben értékelték a következő definíció szerint: „… a projekt értékelése egy olyan összeget jelent, amely felülről közelíti a projekt tényleges, a Vállalkozó számára felmerülő költségeit”[148].

Az informatikai rendszer szoftveres komponenseinek fejlesztési költségét a következő számítással kalkulálták a szakértők:

Fejlesztési érték = (hardver komponensek nettó ára + szoftverkomponensek nettó ára + szolgáltatások nettó ára) + 100% árrés.

Fejlesztési érték és a munkateljesítmény összevetésének módszere

A járulékos költségektől megtisztított bruttó beszerzési ár, vagyis a fejlesztési érték és a ténylegesen valószínűsíthető fejlesztési munka összevethetősége érdekében a fejlesztési értékek a fejlesztési időszakra vonatkozó projekt személyzet munkabérre alakítják át a szakértők. Ennek metodikája a következő:

A szolgáltatások értékének meghatározásakor figyelembevételre került az adott időszakra vonatkozó mérnöki és programozói átlagkereset értéke az USA Munkaügyi Minisztérium statisztikái és felmérései (részletesen lásd később) alapján, valamint

[147] MÁTÉ István Zsolt – BEGELLA Zoltán: Igazságügyi informatikai szakértői vélemény, 01/2013 szakértői ügyszám, (nem nyilvános irat), Máté-Begella, 2013. p.35.
[148] MÁTÉ István Zsolt – BEGELLA Zoltán: Igazságügyi informatikai szakértői vélemény, 01/2013/4 szakértői ügyszám, (nem nyilvános irat), Máté-Begella, 2013. p.24.

USD/HUF közötti átváltás céljából az adott devizanem MNB középárfolyamának éves átlaga.

Az egyes eszközök beszerzési áraira vonatkozó tartalmak a szakértői vélemény mellékletét képezik a források pontos megjelölésével együtt.

Az átlagos munkabér kalkulációjához az alábbi tapasztalati táblázatot használják a szakértők, ahol a relatív munkadíjakat a fejlesztési munkát végző programozói munkadíj (1,00) arányában határozzák meg.

24. táblázat - Munkadíj arányok

Projekt csoport	Munkadíj arány
Projektvezetés	2,50
Szervezés	1,80
Vezető Programozó - Mérnök	1,80
Programozó - Tesztelő	1,00
Adminisztrációs munkatárs	0,20
Oktatás - Bemutatás	0,50
Hot-Line	0,15
Üzemeltetés	1,00

A munkadíjak abszolút értékének meghatározásához a szakértők az Amerikai Egyesült Államok Munkaügyi Minisztériuma (United States Department of Labor) Munkaügyi Statisztikai Hivatalának (Bureau of Labor Statistics) adatait használták fel, a szoftverfejlesztők (software developers / computer programmer) munkadíjának megállapítására. Az így meghatározott abszolút bér az Amerikai Egyesült Államokban 2005 évben az Amerikai fogyasztói kiadások felmérés (U.S. Consumer Expenditure Interview Survey) alapján[149] 4 141 USD/hó volt. A 2010. évre vonatkozó adatok (Occupational Outlook Handbook) szerint[150] a fejlesztői óradíj 43,52 USD/óra volt

[149] U.S. Consumer Expenditure Interview Survey, http://www.worldsalaries.org/usa.shtml, (2013. 02.11.)

[150] Occupational Outlook Handbook http://www.bls.gov/ooh/Computer-and-Information-Technology/Software-developers.htm (2013.06.08.)

Az előzőek alapján a vizsgálandó rendszerek (××× / ××× / ××× / ×××) időbeliségét figyelembe véve a szakértők az egyes évekre vonatkozóan az alábbi óradíj időskálát kalkulálták a 2005. és 2010. évi adatok lineáris interpolációjával:

25. táblázat - IT átlag óradíj kalkuláció időskálája

Év	Óradíj USD
2005	25,9
2006	29,4
2007	32,9
2008	36,5
2009	40,0
2010	43,5

A szakértők valamennyi rendszer esetén a fentiekben ismertetett vizsgálati módszertant alkalmazták.

A fejlesztési folyamat egyes részeinek azonosítása érdekében a szakértők a következő definíciókat alkották meg:

Előkészítési szakasz

A projekt közvetlen előkészítésének időszaka. Ebben az időben kell felállítani azokat a szervezeti, szervezési kereteket, amelyek a projektet működtetik. Elő kell készíteni és meg kell kötni a megfelelő szerződéseket, elő kell készíteni a hivatalos anyagokat, a szükséges dokumentációkat. Meg kell keresni a témához értő szakértőket.

A szervezők lefektetik a projekt alapjait. Ebben az esetben a konkrét jogszabályváltozások listáit. Meghatározzák a funkciólistát, és azok elsődleges megvalósítási sorrendjét.

A vezető programozó meghatározza a használt programozási nyelvet, a szükséges licencszámmal. Megkeresi és kijelöli azokat a Tool Kit[151]-eket, amelyekkel optimálisan kihasználhatók a programozói kapacitások, amivel a programozási idő rövidíthető le jelentősen. Jelen esetben ez a Java fejlesztő környezetet.

Az előzetes szervezési dokumentumok alapján felállítja, és megszervezi a programozó teameket. A programozó előkészíti, telepíti, kipróbálja a fejlesztői környezetet. Optimális esetben előkészíti a többi programozó gépét a csoportmunkára. A rendszer-mérnökök összeállítják a tesztrendszert, és elkezdik az éles rendszer felépítését.

A fázis végére elkészül az igazgatási és informatikai rendszerterv első változata, mely a további fázisok során válik véglegessé.

[151] fejlesztési eszközkészlet

Programozási fázis

A programozók elkezdik a lebontott feladatok elkészítését, az „üzleti”, és/vagy „műveleti logika” kódolását. A programkódok még hiányosak, de alaprutinok, a megfelelő interfészek, azaz minden olyan rész, amire a későbbi munka alapul már végleges formát ölt, tesztelhető és ellenőrizhető.

Megkezdődik a tesztelés, és annak visszacsatolása a programozásra, és szükség esetén a szervezésre. Az időszak végére a program strukturálisan kész. Az interfészek készek, gyakorlatilag béta szinten hibátlanok, strukturálisan, és input-output szinten már nem változnak.

A program az időszak végére részben működőképes, részben bemutatható (××× ág), a funkciók mindegyike alapszinten működik, és első gyakorlati tesztelésre kész. A program már bemutatható, egyes részei oktathatók. Elkezdődik az éles rendszer üzemi tesztje.

A rendszert kiszolgáló hardverek konfigurálása és tesztelése megtörténik.

A program már a felhasználó számára bemutatásra kerülhet, hogy az esetleges megjegyzéseit még meg tudja tenni. A GUI (grafikus felhasználói felület) és az I/O (be- és kimeneti) funkciók véglegesek, és stabilak. Az operátori interfészek még változhatnak, jobban alkalmazkodva a megrendelő igényeihez.

A programban már lényegi változtatás nem lehetséges. Ha ez mégis megtörténik, akkor azt át kell vezetni a rendszerterveken, és meg kell vizsgálni, hogy milyen strukturális változásokat indukál, illetve milyen határidő módosítást eredményez.

Az időszak végére a már stabilnak nevezhető programmal együtt véglegesednek az akkorra már valószínűleg többszörösen módosított rendszertervek.

Elkészül az informatika rendszerterv végső változata A tesztelők visszacsatolásai alapján véglegesedik a programkód, és elkészül a felhasználói dokumentáció. Elkészül az üzemeltetési dokumentáció. Megtörtént a program béta tesztje.

Befejeződik a komplex rendszer éles-üzemi tesztje, és finomhangolása. Ekkorra a teljes hardver állomány üzemkész, és működése eléri a kívánt megbízhatósági, rendelkezésre állási százalékot. Ez minimum: 99,5%

Az időszak végére a program már átadható üzemeltetésre, bevezethető állapotú. A program használatával kapcsolatos problémákat a hot-line felveszi és továbbítja a programozók felé, hibajavítás, vagy módosítás végett.

A programozói teamek azon része, ahol már módosítás nem lehetséges feloszlik. Csak azok maradnak meg, akikhez köthető programrészekben még változások lehetségesek, továbbá a megszűnt teamek programkódját szükség esetén javítani képes programozók.

Üzemeltetési fázis

A programot az üzemeltetés átveszi. A programozói munkacsoportok feloszlanak. Csak annyi programozó marad, amely a szórványosan előforduló hibákat javítani tudja. Ezeknek a programozóknak hosszú távon az is feladata, hogy az esetleges apróbb módosításokat elvégezzék. A vizsgált rendszer esetében ez csak minimális mértékű lehet a feladat jellegéből adódóan. Minden jelentősebb módosítás egyben rendszerterv módosítást és engedélyezést igényel.

Mivel a program már betesztelt, leoktatott és gyakorlatban működött, ezért a hot-line feladata is a közvetlen napi munka ellátása. A bevezetési szakaszhoz képest az esetszám lecsökken, beáll egy átlagos értékre.

A szakértők az egyes rendszerek fejlesztési szakaszaira vonatkozóan – a projektekben elemzett dokumentációk, a rendszerek részletes elemzése során kialakított metodika figyelembe vételével, valamint személyes szakértői munkatapasztalatuk alapján – kalkulálják a teljes projektlétszámot, melynek figyelembe vételével történi a piaci érték meghatározása[152].

Az eredeti vizsgálati metodika a definíciós résznél tartalmazta a vizsgálat alá vont szoftver rendszerek, illetve azok funkcionális komponenseinek azonosításához használt rövidítéseket, valamint a rövidítések pontos kifejtését is. Ezen adatokat jelen tanulmány az ügy anonimizálása miatt nem tartalmazza.

A definíciók indoklása és értékelése

Az egy évet meghaladó vizsgálatsorozat alatt, majd azt követően jelen tanulmány előkészítése során több kérdés és kritika is megfogalmazódott a munkadefiníciókkal összefüggésben, melyek feltétlenül választ igényelnek.

Elsőként maga a megközelítési mód igényel magyarázatot. A vizsgálat során a szakértők nem fértek hozzá a rendszerek teljes körű, részletes fejlesztési dokumentációjához, illetve az egyes programváltozatok közül is csupán az időben legutolsó változatok közvetlen vizsgálatát tudták elvégezni teszt környezetben. Mivel ezen körülmények a vizsgálat megkezdésekor ismertek voltak, a szakértők feladata volt annak a munkaeszköznek (értsd: módszer) a kidolgozása is, mely a nem teljes körű kiinduló adatokból is képes közelítő eredményt szolgáltatni. A hiányos adatok miatt a „fordított projekt tervezés", vagyis az egyes projektelemek részletes visszafejtése a bázis adatokhoz nem volt lehetséges.

[152] MÁTÉ-BEGELLA, 01/2013/4. im. pp.36-41.

Új adatok figyelembevételének módszerei

Az alapvetően tervezési célú módszertanok használatát a szakértők a vizsgálat során felmerült új adatok miatt (az ügyhöz adatot szolgáltató intézmény egyik vezetőjének nyilatkozata) végezték el. A nyilatkozat szerint

„A ××× és jogelődje – az ××× Zrt., mint vezetői tanácsadó cég közreműködésével – az ××× Zrt., a ××× Kft., valamint a ××× Kft.-vel, mint fejlesztőkkel kötött szerződések során a vállalkozói díj megállapítására a következő módszereket, illetve mértéket alkalmazta: Egyrészt, a HW és SW beszerzésekre általában a „Total cost of ownership" becslést alkalmaztuk (TCO, teljes körű birtoklási költség: egy eszköz birtoklásának összes pénzügyi következménye, a kezdeti vásárlási áron felül jellemzően idetartozik még a karbantartás, elhelyezési díjak, oktatási költségek, fogyó eszközök, belső és külső támogatás, tőkekamat, stb.).

Másrészt, a fejlesztési tevékenység elvégzésére irányuló költségbecslés az ISO/IEC JTC1 SC7 határozatában elfogadott Nemzetközi Szabvány alapján került meghatározásra. Megnevezése: ISO/IEC 19761 'Software Engineering[153] – COSMIC-FFP – A functional size measurement method' http://www.cosmicon.com/. (A funkciópont-számolás célja, hogy különböző technológiákkal történő szoftverfejlesztések hatékonyságának összehasonlítása lehetővé váljon.)

A vállalkozói díj megállapításának mértékéül az IVSZ által közölt átlagos óradíjakat vették alapul (http://ivsz.hu/hu/hirek-es-esemenyek/hirek/ivsz-hirek/2012/05/2012-atlagos-oradijak), melyekkel kapcsolatban az ××× ×××× úr megjegyezte, hogy a gazdasági recesszió következtében a 2××× előtti díjak sem tértek el jelentősen a mostani, illetve tavalyi díjaktól."[154].

A nyilatkozatban szereplő adatok alapján a szakértők elvégezték a COSMIC Full Function Point Measurment Method módszertan elsődleges vizsgálatát, mely kiterjedt a módszertan időbeli és tartalmi hatályára, valamint a módszertan kérdéses rendszerekkel kapcsolatos alkalmazása nyomainak feltárására.

Az elemzés során a szakértők megállapították, hogy a COSMIC (Common Software Measurement International Consortium) egy kanadai szervezet, mely céljának tekinti az újonnan fejlesztett szoftverek méretezésére és teljesítmény mérésére vonatkozó eljárások kidolgozását. Az adatszolgáltatótól származó információ pontos szakmai értékelhetőségének okán a szakértők részleteiben tanulmányozták a hivatkozott módszereket és szabványokat. Az erre vonatkozó vizsgálat a következőket tárta fel:

[153] https://www.iso.org/standard/54849.html

[154] MÁTÉ-BEGELLA, 01/2013/4. im. p.8.

A COSMIC eljárás életciklusa a következőképpen alakult:

- Full Function Points (FFP, UQAM, 1997)
- COSMIC-FFP (1999) v2.0
- COSMIC (v2.2) become an ISO standard yet in 2003 (ISO/IEC 19761)
- COSMIC (2007) v3.0

A ××× rendszerek költségtervezési időszakában a COSMIC v2.2 eljárás változat volt érvényben, mely a Full Function Point Measurment Method (FFP) nevű eljárást valósítja meg. A ××× szervezet ×××× funkciójú munkatársa tévesen hivatkozott a Functional Size Measurement Method (FSM) nevű eljárásra, mely a COSMIC v3.0 változatától (2007- től) volt érvényes (lásd a DVD mellékleten a COSMIC_Method_v2.2_Measurement_ Manual.pdf és a COSMIC_Method_v3.0_Measurement_Manual.pdf dokumentumokat[155]). A szakértők a ××× rendszerek vizsgálata során sem közvetlen sem közvetett utalást nem találtak arra, hogy a megrendelő milyen tervezési módszert alkalmazott a költségek kalkulálásakor. A megvizsgált v2.2 tervezési eljárás változat szerint:

> *„A CISMIC-FFP mérési módszer kialakítása oly módon történt, hogy az alkalmazható legyen a következő szoftvercsoportokra:*
>
> - *Üzleti szoftverek, melyek jellemzően az üzleti adminisztrációt támogatják, mint például a banki, biztosítási, könyvelési, személyzeti, beszerzési, forgalmazási vagy gyártási ügyek kezelése. Az ilyen szoftvereket gyakran „adat gazdag" szoftvernek nevezik, mivel összetettségét nagymértékben meghatározza a valós világból származó nagy mennyiségű adat kezelése.*
> - *Valós idejű szoftver, melynek feladata a valós események nyomon kövtése vagy ellenőrzése. Ilyeneke lehetnek a telefonközpontok és üzenetküldő szoftverek, eszközökbe épített szoftverek, melyek a háztartási készülékeket, felvonókat, gépjármű motorokat kezelik a folyamtok ellenzése és automatikus adatgyűjtés céljából, valamint a számítógépek operációs rendszerein belül működő szoftverkomponensek.*
> - *A fenti tulajdonságokat vegyesen tartalmazó rendszerek, mint például a légitársaságok vagy hotelek valós idejű foglalási rendszerei"*[156]

Az eljárás a fenti leírás alapján egyrészt általános üzleti szoftverekre (bank, biztosítás, könyvelés, személyzeti nyilvántartás, beszerzés, elosztás vagy gyártás) vonatkozik, melyek ún. adatgazdag szoftvereknek nevez a leírás. A másik szoftver típus – ahol az eljárás alkalmazható – az ún. valós idejű szoftverek, mint a telefonközpont és üzenetkezelő szoftverek, készülékekbe beágyazott szoftverek (pl. háztartási gépek esetén),

[155] Az 1/2013 sz igazságügyi informatikai szakértői vélemény eredeti hivatkozása

[156] Measurement Manual (The Cosmic Implementation Guide For ISO/IEC 19761: 2003) Version 2.2 January 2003, p.15 (a szező fordítása)

liftek és jármű motorok folyamatainak vezérlése és adatainak gyűjtése. Harmadrészt a módszer alkalmas (a kidolgozók szerint) vegyes rendszereknél, úgymint valós idejű repülőgépjegy vagy hotel foglalási rendszerek.

A leírás nem erősíti meg (de nem is zárja ki), hogy egyedi (tehát nem valamilyen szokásos munkameneten alapuló) célszoftver fejlesztés tervezési támogatására is alkalmas lenne.

Ugyanakkor a komplexitásra utaló kizárások (lásd alább) közé sem tartozik a ××× rendszerek fejlesztési folyamata.

> *A COSMIC-FFP mérési módszert még nem úgy tervezték, hogy figyelmebe vegye a szoftverek, vagy azok részeinek funkcionális méreteit, amelyek funkcionális részeit:*
>
> – *komplex matematikai algoritmussal, vagy más speciális és komplex szabályokkal jellemezhetők, mint például a szakértői rendszerek, szimulációs szoftverek, öntanuló szoftverek, időjárás előrejelző rendszerek stb.*
> – *folyamatosan változó értékű adatok feldolgozása, mint a hangok, vagy videók egy számítógépes játékszoftverben, vagy egy elektronikus hangszerben."*[157]

Összességében megállapítható, hogy az eljárás alkalmas a szoftverek méretezésének előzetes tervezéséhez hozzájárulni, különösen szabványosított, vagy általános célú (lásd a fenti felsorolást) üzleti alkalmazások esetén.

A szakértők ugyanakkor nem találtak arra vonatkozó adatot az áttekintett dokumentációban, ami a tervezési eljárás használatára utalt volna.[158]

A bemutatott érvelés mutatja, hogy az egyedi esetekre kidolgozott vizsgálati módszerek már a felhasználás során ki vannak téve a gyakorlat próbájának és a nyomozási szakaszban felmerülő új adatok indokolttá teszik az elvégzett vizsgálatok eredményének újraértékelését. Ezt minden esetben végre kell hajtani, függetlenül attól, hogy az újonnan felmerülő információ minősége, annak megbízhatósága magasfokú-e, vagy nyilvánvalóan az adatot szolgáltató felelősségének csökkentését igyekszik szolgálni, mint a vizsgált esetben.

[157] A szerző fordítása

[158] MÁTÉ-BEGELLA, 01/2013/4. im. pp.9-12.

A vizsgálati eredmények vizuális bemutatása

Mivel a vizsgálandó rendszerek (eredeti kirendelésben egy rendszer három változata) fejlesztési dokumentációja több, mint tízezer oldalnyi iratot tett ki, melyhez további elektronikus iratok (CD és DVD adathordozón) kapcsolódtak, az adatgazdagság az elkészített igazságügyi informatikai szakértői véleményekben is megjelent.

Tekintettel arra, hogy a forrásinformációk és az azokból kalkulált eredmények érthető bemutatása jelentősen befolyásolja a szakértői vélemények későbbi felhasználhatóságát, a szakértők több vizuális módszert is alkalmaztak az adatok bemutatásakor.

Azoknál az adattípusoknál, ahol a részletek összevonását követően egy összesített eredményt kellett bemutatni, az alapinformációk táblázatos formában kerültek bemutatásra. A következő táblázat például a ×××3 változat előkészítési fázisának kalkulált létszám és munkadíj adatait tartalmazza:

26. táblázat - Fejlesztési fázisonkénti összesítő tábla

Projekt csoport	Munkadíj arány	Havibér	Létszám Előkészítés	
			Fő	Bér
Projektvezetés	2,50	3 985 765	2	5 797 472
Szervezés	1,80	2 869 751	3	6 261 280
Vezető Programozó - Mérnök	1,80	2 869 751	2	4 174 176
Programozó - Tesztelő	1,00	1 594 306	1	1 159 488
Adminisztrációs munkatárs	0,20	318 861	2	463 792
Oktatás - Bemutatás	0,50	797 153	0	0
Hot-Line	0,15	239 146	0	0
Üzemeltetés	1,00	1 594 306	0	0
Összesítés			**10**	**17 856 208**

Hasonló részletező táblázatok készültek a valamennyi programváltozat valamennyi fejlesztési szakaszáról. Tekintettel arra, hogy ezek a részletes táblák nem teszik lehetővé a teljes körű áttekintés (nem is ez a feladatuk), a szakértők az egyes programokra, illetve programváltozatokra vonatkozóan összesített, fejlesztési időt és fejlesztési költségeket egyaránt tartalmazó táblázatokat is készítettek (lásd a következő ábrán).

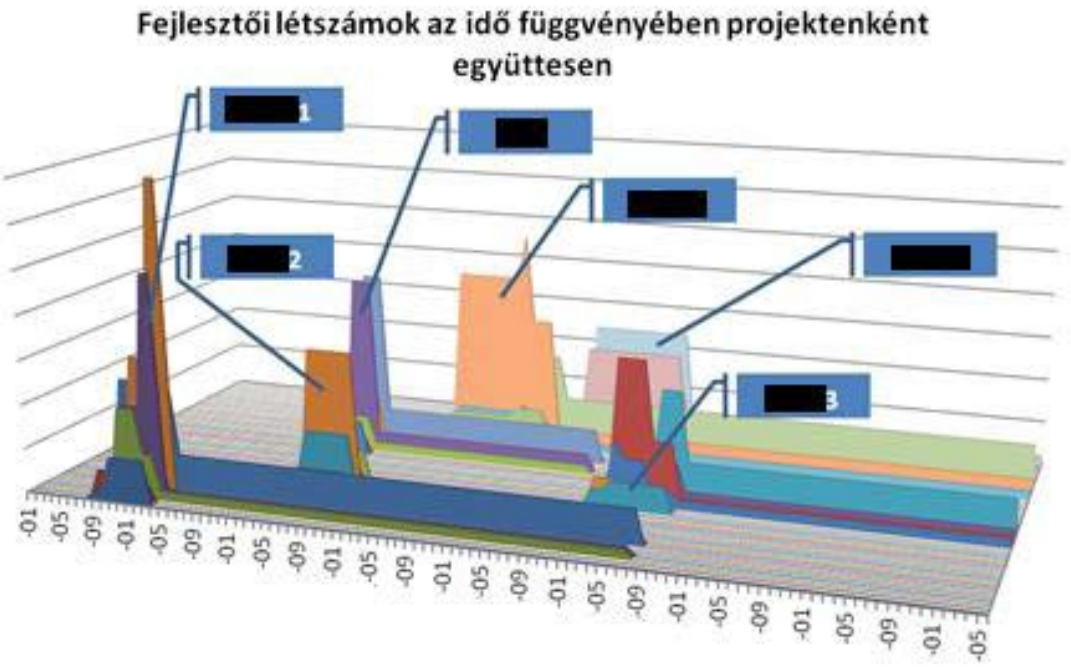
27. táblázat - Fejlesztési projektenkénti összesítő tábla

Projekt csoport	Munkadíj arány	Havibér	Létszám Előkészítés Fő	Előkészítés Bér	Programozás Fő	Programozás I.fázis Bér	Üzemeltetés Fő	Üzemeltetés Bér	Összesen	Összesen
Projektvezetés	2,50	2 661 123	1	3 870 720	4	26 127 414	0	0	5,00	29 998 134
Szervezés	1,80	1 916 009	3	8 360 768	2	**9 405 882**	0	0	5,00	17 766 650
Vezető Programozó - Mérnök - Oktatás	1,80	1 916 009	1	2 786 912	4	**18 811 710**	1	47 638 777	6,00	69 237 399
Programozó	1,00	1 064 449	1	1 548 288	20	**52 254 774**	2	52 932 096	23,00	106 735 158
Adminisztrációs munkatárs	0,20	212 890	1	309 664	2	1 045 116	0	0	3,00	1 354 780
Oktatás	0,50	532 225	0	0	5	6 531 840	0	0	5,00	6 531 840
Hot-Line	0,15	159 667	2	464 480	20	7 838 208	4	15 879 410	26,00	24 182 098
Üzemeltetés	1,00	1 064 449	1	1 548 288	3	7 838 208	1	26 466 048	5,00	35 852 544
		Összesítés	10	18 889 120	60	129 853 152	8	142 916 331	**78,00**	**291 658 603**

Fázis	**Tól**	**Ig**	**Munka nap**	**Naptári nap**
Előkészítés	2006.12.28	2007.02.12	32	46
Programozás I.fázis	2007.02.13	2007.05.02	54	78
Üzemeltetés	2007.05.03	2009.07.01	547	790
Összesen:			633	
Napi Munkaóra			8	
Programozói óradíj (USD)	32,90			
USD/HUF árfolyam	183,83			

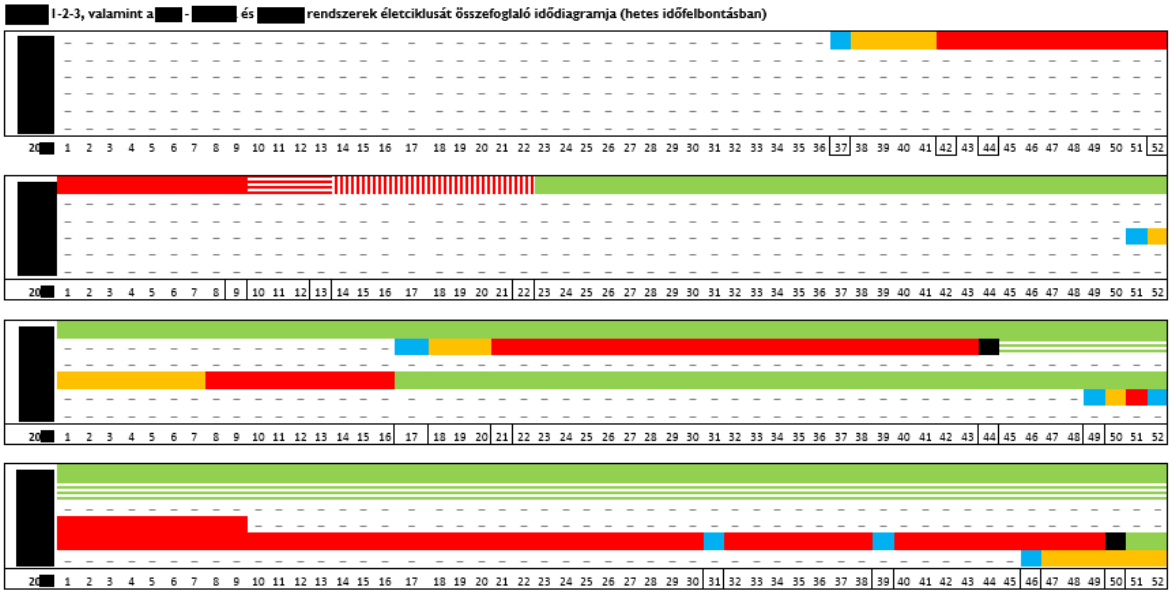
Fejlesztési érték		
(a) Hardver - szoftver - szolgáltatás		**299 244 915**
(b) Számított bérköltség adatok		**291 658 603**
(c) Számított összes költség (b) + (c)		**590 903 518**
(d) Nyereség	**100%**	**590 903 518**
Kalkulált fejlesztési érték	**(c) + (d)**	**1 181 807 036**

A fejlesztési projektek időbeliségét, különösen a párhuzamos fejlesztéseket táblázatban ábrázolni célszerűtlen, ezért a szakértők színkódolt idődiagramot alkalmaztak (lásd a következő ábrát).



2. diagram - Fejlesztési projektek párhuzamosságainak idődiagramja

Mivel a kirendelő hatóság szempontjából az egyes különálló projektek fejlesztési szakaszainak is volt jelentősége (egybeesések), ezért a szakértők a projektidőszakok szerint végezték el a színkódolást, melynek segítségével áttekinthetővé vált az egyes feladattípusok párhuzamos elvégzése a különböző projektek esetén, vagy a párhuzamosság hiánya (színkódokat lásd a következő ábrán).



3. diagram - Időbeli és mennyiségi adatok projektenkénti párhuzamos ábrázolása

A mennyiségi és időbeliségi adatok párhuzamos megjelenítésére a szakértők háromdimenziós, színkódolt ábrát használtak, melyek segítségével a komplex adatösszefüggések is gyorsan áttekinthetővé váltak (lásd a következő ábrán).

4. diagram - Idő diagram színkódjai

Összességében megfogalmazható, hogy a komplex, nagy mennyiségű adatot tartalmazó vizsgálati eredmény grafikus megjelenítése nem öncélú művelet, hanem a vizsgálati eredmény értelmezésének fontos kelléke, mellyel minden olyan esetben élniük kell a szakértőknek, amikor a táblázatos bemutatás már nem mutatja be megfelelően az összefüggéseket.

A vizsgálati eredmények megfelelő értelmezése és könnyű áttekinthetősége nem csupán a nyomozati munkát, de a vádemelési, a védelemi és a döntéshozatali tevékenységeket is hatékonyan segíti.

Minősített adatok felhasználása a vizsgálat során

A szakértők a vizsgálatuk során elemzett nagy mennyiségű információ között több alkalommal találkoztak minősített adatokra történő utalással, illetve a szakértői vizsgálat zárásakor minősített adatokat is felhasználtak a szakértői vélemény kiegészítéséhez.

E körülmények miatt is szükséges áttekinteni a minősített adatok szakértők általi kezelésének szabályait és annak gyakorlati eljárásait egyaránt.

A minősített adatok védelméről szóló 2009. évi CLV. (Mavtv.) törvény tartalmazza a minősített adatok létrejöttének, kezelésének és megszűnésének alapvető szabályait, illetve a Be. 70/C § rendelkezik a büntetőeljárásban történő felhasználás módjáról.

A fenti jogszabályok a büntetőeljárás során kirendelt vagy bevont igazságügyi szakértőknek lehetővé teszi a minősített adatokhoz történő hozzáférést az általános szabályokban foglalt nemzetbiztonsági ellenőrzés, személyi biztonsági tanúsítvány, valamint titoktartási nyilatkozat és felhasználói engedély nélkül [Mavtv. 14. § (2)].

A szakértők az esettanulmányban szereplő ügy vizsgálata során tudomást szereztek arról a körülményről, hogy az ügyben minősített adatokkal történő munka várható, ezért mindketten elvégezték a Nemzeti Biztonsági Felügyelet szervezésében megtartott titkos ügykezelő vizsgára felkészítő tanfolyamot. Az ügy vizsgálata során ezeket az elméleti ismereteket hasznosították, illetve annak gyakorlati alkalmazására vonatkozó megfigyeléseket is tettek.

A minősített adatokat, legyenek azok bármilyen hordozón (tipikusan papír, optikai adathordozó, mágneses lemez vagy szalag stb.) zárt rendszerben kezelik. Az adatokhoz történő hozzáférés adminisztratív és fizikai módon biztosított környezetben történik, ennek legfontosabb, a szakértőket is érintő eljárásai kerülnek ismertetésre a következőkbe az esettanulmányhoz kapcsolódóan.

A Mavtv. 2010. április 1-én lépett hatályban, azonban átmeneti rendelkezéseinek egy része az esettanulmányban ismertetett ügy vizsgálati időszaka alatt lett hatályos. A törvény úgy rendelkezett, hogy a jogszabály hatálybalépéséig keletkezett minősített adatokat legkésőbb 2011. december 31-ig felül kell vizsgálni a minősítő, vagy az NBF

részéről, illetve a levéltárban lévő, vagy egy adott szerv jogelődjénél készített, vagy saját készítésű minősített iratot legkésőbb 2013. június 30-ig felül kell vizsgálni és a törvény szerint kell a továbbiakban eljárni. A gyakorlatban ez azt jelentette, hogy a szakértői vizsgálat időszakában (2013 második félév) már csak olyan minősített adattal kerülhettek kapcsolatba a szakértők, melyek felülvizsgálata megtörtént és nemzeti minősített adat esetén a következő besorolások valamelyikébe esett: Szigorúan titkos, Titkos, Bizalmas, Korlátozott terjesztésű.

Az előzekben ismertetett körülményekből adódóan a szakértők véletlenszerű módon nem kerülhetnek kapcsolatba minősített adattal, azonban szükséges a minősített adat felismeréséhez szükségez információkkal rendelkeznie ahhoz, hogy a minősített adattal visszaélés tényállást még gondatlanságból se követhesse el.

A nemzeti minősített adat (a továbbiakban csak ezzel az adattípussal foglalkozunk) alaki kellékeit a 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről határozza meg. Ezek a 38. § (1) szerint a következők:

- a készítő megnevezése
- a minősítési szint megnevezése
- az érvényességi idő,
- a minősítő nevét és beosztása.

Amennyiben a szakértő munkája során ilyen alaki kellékekkel ellátott iratot, vagy elektronikus adatot talál, haladéktalanul értesítenie kell a minősítőt (az irat adataiban szerepel), illetve ennek hiányában (pl. megszűnt szervezet, el nem érhető minősítő stb.) az Nemzeti Biztonsági Felügyeletet.

Az esettanulmányban szereplő ügy vizsgálata során egy esetben merült fel nem szabályos módon átadott minősített adat gyanúja, amikor a szakértők által átvett CD adathordozó felületén a TÜK felirat szerepelt. Bár a kérdéses felirat nem felel meg a minősített adattal szemben támasztott formai követelményeknek, a szakértők mégis úgy látták, hogy az adat átadójától információt kérnek az adathordozó minősített voltára vonatkozóan. Az elektronikus adatok felhasználása csak akkor vette kezdetét, amikor a nemleges válasz megérkezett a szakértőkhöz.

A minősített adatokhoz történő szabályos hozzáférés a büntetőeljárás során tipikusan a nyomozó hatóság közreműködésével valósul meg, ahogy az esettanulmányban szereplő ügy feldolgozásakor is történt. Ez annak a következménye, hogy a szakértők nem tudják megteremteni a jogszabályok által előírt fizikai és adminisztratív védelmet (részletesebben lásd a 90/2010. (III. 26.) Korm. rendeletben).

A minősített adat felhasználásának körülményei, elsősorban az adminisztratív védelem miatt kisebb előkészítést igényelnek. Ebből adódóan az adatok megismerése és felhasználása előre egyeztetett időpontban történik a nyomozó hatóság azon objektumában, mely megfelel a jogszabályok által előírt fizikai és adminisztratív védelmi feltételeknek. Az iratok (legyenek azok hagyományos papír alapúak, vagy elektronikus adatok) átvétele a titkos ügykezelőtől történik, aki iktatókönyvben, kartonon, vagy elektronikusan rögzített módon átadja a minősített adatokat a szakértő részére. Amennyiben a felhasználáshoz számítógépet is igénybe kell vennie a szakértőnek, úgy arról a nyomozó hatóság gondoskodik, méghozzá a fizikai védelem előírásainak megfelelő hálózatra nem csatlakoztatható, számítógép formájában. A számítógéphez történő hozzáférés adatait (felhasználó név és jelszó) a szakértő lezárt borítékban veszi át, melyet a minősített adat átvételét, valamint a vizsgálathoz nem szükséges személyek távozását követően használ fel. A minősített adat megismerését követően a szakértő elkészíti a szakértői vélemény azon részét, mely a minősített adatot tényleges, vagy alapinformációként (mint forrás adat pl. számítások esetén) tartalmazza. Amint véglegesíti a dokumentumot menti a megkapott számítógép adattárolójára, mely nem lehet más, mint a merevlemez (az adattárolót is befogadni alkalmas csatlakozók letiltott állapotban kell, hogy legyenek), majd a kérdése iratot vagy iratrészt a nyomozó hatóság megfelelő jogosultsággal rendelkező munkatársa segítségével, az előre meghatározott példányszámban kinyomtatja a vizsgálat helyszínén.

A minősített adatok felhasználásával készített igazságügyi informatikai szakértői véleményeknél célszerű oly módon eljárni, hogy a minősített adatokat tartalmazó rész a szakértői vélemény különálló mellékleteként készül el. Ebben az esetben a minősítést (a vonatkozó jogszabályok szerint) csak a mellékletre vonatkozóan kell megismételni, így maga a szakértői vélemény nyílt irat lehet, s a melléklet kerülhet a felhasznált legmagasabb minősítésű szintű irat szerinti védelmi kategóriába.

A minősített adat felhasználását követően a keletkezett nyomatokat teljes körűen átveszi a titkos ügykezelő, a vizsgálathoz felhasznált számítógép merevlemezéről a mentett adatot törli a szakértő, majd átadja a nyomozó hatóság munkatársának, aki gondoskodik a törölt adat visszaállíthatatlanságáról (többszörös fizikai felülírás az üresnek jelölt tárterületre vonatkozóan).

Amennyiben a fenti eljárásnak megfelelően tevékenykedik a szakértő a vizsgálat alatt, úgy az általa felhasznált minősített adat kezelése is megfelelő lesz, a szakértői vélemény ezáltal nem lesz alaki, vagy eljárási hiba miatt felhasználhatatlan.

A vizsgálati eljárás külföldi minősített adat esetén is hasonló elemeket tartalmaz, az adatok kezelésében közreműködő szervezetek köre más lehet a vonatkozó jogszabályoknak megfelelően.

Eredmények

A csaknem egyéves időtartamot átfogó rendkívül nagy mennyiségű iratot és kapcsolódó elektronikus adatot is magában foglaló, minősített adatok felhasználását is igénylő ügy feldolgozása során a szakértők létrehoztak egy olyan vizsgálati módszert, mely alkalmas a nem kielégítő részletességű adatsorokból történő, felülről korlátos értékhatárok megállapítására.

A vizsgálati módszer a bemutatott körülmények alapján különösen az egyedi, nagy méretű (országos felhasználású) és kiemelkedően magas fejlesztési költségű projektek elemzésére alkalmas. Ezen körülmények kompenzálják az adatminőségbeli hiányosságokat, melyek megakadályozták más, standard eljárások alkalmazását.

A vizsgálati módszertant a szakértők az esettanulmányban szerelő ügyet követően újabb, hasonló paraméterekkel rendelkező ügy esetén is alkalmazták. A két ügy azonos módszertan szerint történt feldolgozását követően egymástól különböző eredményt mutattak be a szakértők. Míg a jelen tanulmányban bemutatott ügy esetén egyértelműen igazolható volt a fejlesztési költségek jelentős, a nemzetközi fejlesztési költségszinteket is többszörösen meghaladó felülárazása, úgy a másik ügy esetén hasonló megállapítás nem volt megtehető.

Ez egyrészt igazolja azt, hogy a módszertan nem ún. egy kimenetű eljárás, azaz nem csak egy eredményt ad vissza a vizsgálat, másrészt azonban a bemeneti adatok minősége felveti a módszer további finomításának lehetőségét, illetve kényszerét is. Tekintettel azonban arra a körülményre, hogy a vizsgálttal azonos nagyságrendű és komplexitású ügy, mely igazságügyi informatikai szakértő közreműködését igényli kis számban fordul elő, a fejlesztésre szánt ráfordítások ésszerű megtérülésére nem lehet számítani.

A módszertan továbbfejlesztésére, mint ahogy kifejlesztésére is – nagy valószínűséggel – egyedi ügyek feldolgozásakor kerülhet sor. Ez esetben pedig fontos további szempont lehet a szakértői vizsgálat érvényességi szintjének növelés, melyhez akár a Bayes-hálók[159] módszerét is felhasználhatják a szakértők.

[159] ORBÁN József: A Bayes-hálók rendészeti alkalmazhatóságának vizsgálata. in Gaál Gyula -Hautzinger Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények. XIV kötet. Pécs 2013. p.379-386.

Összefoglalás

A társadalomtudományok a 20. század közepétől intenzíven érdeklődnek a technológiának a társadalomra gyakorolt hatása iránt. Ez állt Harold INNIS és Marshall MCLUHAN munkásságának fókuszában, amikor az emberi gondolkodás technológia általi módosulását vizsgálták. Bár a hatás mibenléte még nem tisztázott részletesen, az mindenképpen megállapítható, hogy a technológia, pontosabban az elektronikus és/vagy digitális eszközök, szolgáltatások használata mélyen beépült a mindennapok szövetébe[160].

Ez hatás nyilvánvaló a büntetőeljárásban is, amikor a gazdasági bűncselekmények csaknem mindegyike igényli az igazságügyi informatikai szakértő (mint az új típusú technológiához speciálisan értő szereplő) közreműködését akár nyomázási, akár bírósági szakaszban.

Az ügyek komplexitása és adatmennyisége esetenként új szakértői módszerek kifejlesztését igényli. Jelen fejezet bemutatta azt az utat, mely révén létrejött egy vizsgálati metódus az egyedi fejlesztésű, rendkívül nagy értékű szoftverek fejlesztési költségeinek vizsgálatára. A módszertan nem csupán önmagában mutat újdonságot, és egyben válaszol a nyomozó hatóság által feltett kérdésekre, de megmutatja azt is – vagy legalábbis támpontot ad arra vonatkozóan – hogy mi módon érdemes egyedi feladatokhoz egyedi vizsgálati módszert alkotni. Ez a példa – a szerző várakozásai szerint – egyrészt vitára, másrészt új elképzelések, módszertanok kialakítása irányába mozdítja el az igazságügyi informatikai szakértők közösségét, akik ennek révén széles spektrumú választ tudnak majd adni a 21. század következő évtizedének kihívásaira is.

[160] Máté István Zsolt: A bizonyítékok kezelése - az igazságügyi informatikai szakértő a büntetőeljárásban. in Rendészeti Doktoranduszok V. Országos Fóruma konferencia kötet, Budapest 2014.

9.3 Különleges vizsgálat típusok

Az igazságügyi informatikai szakértői vizsgálatok – jelen tanulmányban tárgyalt – második csoportját azok az ügyek képezik, mely számosságukban ugyan az általános vizsgálati eseteknél kevesebbszer fordulnak elő, ugyanakkor rávilágítanak egyes technológiák jellegzetességeiből adódó digitális bizonyíték típusokra. Ezek az ügyek azért lehetnek fontosak, mert általuk bővül a szakértői eszköztár, úgy a módszertanok, mint a bizonyítékok kezelése területén, s ez a későbbikeben – az ügytípusokban bekövetlező változás esetén – előnyt jelenthet a gyorsabb reagálóképesség és nagyobb megalapozottság révén.

A következő fejezetben a különleges vizsgálati típusok közül két terület vizsgálunk meg részletesen a számítógépes nyomatok azonosíthatóságát, illetve a felhőszolgáltatásokból történő digitális bizonyíték kinyerésének lehetőségét. Jól prognosztizálható, hogy az utóbbi terület a közeljövőben jelentős mértékben megjelenik az igazságügyi informatikai szakértői vizsgálatok esetén, így az előzőekben jelzett adapációs előnyök hamarosan éreztethetik hatásukat.

9.3.1 Számítógépes nyomatok tracking dot alapú azonosítása[161]

Bár a fejezet címe egy jól meghatározott módszer bemutatására utal, az írás tárgyköre ennél bővebb: arra kívánja felhívni a figyelmet, hogy az igazságügyi informatikai szakértői módszerek mit sem érnek, ha a nyomozó hatóság munkatársai nem ismerik ezeket a lehetőségeket, s ez által a büntetőeljárás során releváns adatok kerülhetik el a bűnjellé, majd bizonyítékká válást.

Tágabb perspektívából tekintve a kérdést, a digitális írástudás és a rendészet kapcsolatát kell vizsgálnunk abban a korszakban, amikor a bűnügyi helyszínek a valós és a virtuális térben egyaránt feltűnhetnek, amikor az eszköz használatból eredő digitális nyomok felismerése, vagy szem elől tévesztése döntheti el a büntetőeljárás sikerességét.

A következőkben egy olyan eljárás kerül bemutatásra, mely műszaki tartalmát tekintve több évtizedes múltra tekinthet vissza, ugyanakkor napjaink magyarországi bűnfelderítési gyakorlatában új elemként jelenik meg. A témát esettanulmány formájában tekintjük át, mely kapcsán nem csupán a szakértő, de a nyomozó nézőpontját is megismerhetjük.

[161] A fejezetben a kutatás időszakában hatályos jogszabályokra történik hivatkozás

A kutatás jogszabályi és műszaki háttere

Az esettanulmányok a valóságban megtörtént események tanulságait gyűjtik össze, s ebből adódóan számos valódi adatot kell tartalmazniuk. Az igazságügyi szakértői tevékenységről szóló 2005. évi XLVII. törvény (Szaktv.[2005]) kötelezi a szakértőt a titoktartásra a tudomására jutott tényekre és adatokra vonatkozóan, ugyanakkor fel is hatalmazza azok tudományos vagy oktatási célra történő felhasználására is. Ezt a felhasználást – a jogszabály szerint és a szakértői etikai normák alapján is – meg kell előzni a személyazonosításra alkalmas adatok eltávolításának, mint ahogy az a jelen tanulmányban felhasznált ügyek esetében is megtörtént.

A vizsgálat műszaki környezeteként a címben is meghatározott számítógépes nyomattal összefüggésbe hozható berendezéseket, eszközöket, adathordozókat tekinthetjük. Ezek közül a legfontosabbakat vizsgáljuk meg a következőkben.

A számítógépes nyomat létrehozása alapvetően három komponens együttműködését igényli: szoftver (pl. szövegszerkesztő program), hardver (pl. nyomtató) és adathordozó (pl. papír). Az ismertetendő vizsgálati eljárás e három tényezőből kettőre, a hardverre és az adathordozóra koncentrál. Az adathordozó részletes vizsgálatával keresi a választ arra kérdésre, hogy a nyomatot mely eszközzel készítették, az eszköz milyen gyártmány, illetve mi az egyedi azonosítója a készüléknek. Mindezeket az információkat az adathordozón hátrahagyott nyomat elemzésével tárja fel a vizsgálatot végző igazságügyi informatikai szakértő.

Napjainkban ezek a hátrahagyott nyomok négy nyomtatási mód egyikével jönnek létre a leggyakrabban. Ezek közül a legrégebbi és napjainkban egyre kevéssé használt az impact (ütéses elvű) nyomtatási eljárás, melynek leggyakoribb eszközei dot matrix (tűs), a daisy-wheel (margaréta fejes) és line (sor) nyomtatók. Az irodai, vagy a magán használat során az ink-jet (tintasugaras), illetve az electro-photographic elvű eszközök (lézer- és LED nyomtatók) jelennek meg, míg az üzleti (elsősorban a kereskedelmi) területen a thermal elvű eszközök (hőnyomtató) is megfigyelhetők.

A vizsgálati eljárás a tintasugaras és lézernyomtatók által készített nyomatok azonosítására alkalmas, így a továbbiakban e két területtel foglalkozunk részletesen. Mielőtt ezt megtennénk, tisztázni kell, hogy a vizsgálat egyáltalán az igazságügyi informatikai szakértő kompetenciakörébe tartozik-e?

A szakértői kompetenciakör a számítógépes nyomat azonosításban

Az igazságügyi szakértői szakterületekről a 9/2006. (II. 27.) IM rendelet (Szak. rend.) intézkedik, ahol az informatika vonatkozásában az alábbi szakterületeket adja meg:

1. informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hard-ver)
2. informatikai biztonság
3. informatikai rendszerek tervezése, szervezése
4. stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység
5. számítástechnikai adatbázis, adatstruktúrák
6. szoftverek

A számítógépes nyomatok vizsgálata az informatikai szakterületen belül a perifériák (1.) tárgykörébe tartozik. Ugyanakkor nem hagyható figyelmen kívül az a tény sem, hogy a nyomtatókkal közvetlenül létrehozott – a létrehozás fizikai körülményei által meghatározott – nyomatok vizsgálat a kriminalisztikai okmányszakértő kompetencia-körét is érintheti.

Az idézett jogszabály ugyan nem határozza meg tételesen az okmányszakértés konkrét szakterületét, csak annak elnevezését [Szak. rend. 46 § (1) c.]. A tartalmi leírást ezért másodlagos forrásból, a Bűnügyi Szakértői és Kutató Intézet Írás- és Okmányszakértői Laboratóriumának szakterület leírásából idézzük:

„A kriminalisztikai okmányvizsgálat kompetenciája a köznyelvi értelemben vett okmányoknál nagyobb körre terjed ki. A leggyakrabban előforduló személyi- és közlekedési okmányokon kívül vizsgálat tárgya lehet például: sorsjegy, bélyeg, postai csekk, boríték, elismervény, szerződés, vagy akár egy - a bűncselekmény helyszínén talált - papírdarab is.

A leggyakrabban felmerülő kérdések:

- Az okmány eredeti vagy hamisítvány?
- Milyen eljárással (nyomdai úton, irodatechnikai eszközök segítségével, egyéb módon) készí-tették?
- Egyes részeit (pl. adatok, arckép) megváltoztatták, illetve kicserélték-e?
- Van-e az okmányon látens (szabad szemmel nem látható) írás, tartalma rekonstruálható-e?
- Valamely bélyegzőnyomat egy meghatározott bélyegzőtől származik-e?
- Az irat elkészítéséhez egy, vagy több különböző tollat használtak?”[162]

[162] Bűnügyi Szakértői és Kutató Intézet Írás- és Okmányszakértői Laboratórium honlapja. http://bszki.hu/page.php?295, utolsó hozzáférés: 2014.07.18

A meghatározásból látható, hogy az okmányszakértő joggal tart igényt a vizsgálati szakterületen történő szakértői vélemény kiadás jogára, ugyanakkor nem hagyható figyelmen kívül, hogy az informatikai szakértő – aki a technológiai háttér avatott ismerője – a nyomatok technológiai kialakításával összefüggésben mindenképpen rendelkezik kompetenciával.

A szakértői véleménynek a büntetőeljárásból kompetenciatúllépés miatti kizárása megakadályozható együttes szakértői vélemény kibocsátásával, melynek elkészítése során az okmányszakértő és az informatikai szakértő együttműködik. Ezt a módszert célszerű alkalmazni mindazon ügyek esetén, ahol kétség merül fel a szakértői kompetencia vonatkozásában, akár a kirendelt szakértő, akár a kirendelő hatóság részéről.

Számítógépes nyomat azonosítás módszerei

A számítógépes nyomatok azonosítására két alapvető módszer áll a szakértő rendelkezésére: a dokumentumok egyedi jellemzőinek vizsgálatán alapuló ún. passzív technikák, valamint a rejtett információk feltárását célzó ún. aktív technikák.

Passzív azonosítási technikák

A passzív azonosítási eljárások során a szakértők abból indulnak ki, hogy a nyomtatók előállítása során létrejövő egyedi jegyek (unique characteristics) miatt nincs két egyforma nyomtató, s ez által két egyforma nyomat sem. A különbségeket okozhatják mechanikai eltérések, illetve a működés jellegzetességeiből is adódhatnak. Ez utóbbira közismert példa a lézernyomtatók esetében megfigyelhető csíkozás (banding), melyet a fényérzékeny hengeren megjelenő nagyobb, illetve kisebb töltési szintből adódó eltérő festékmennyiség felvétel okozhat. Az így kialakuló csíkok frekvenciája jellemző lehet az adott nyomtatótípusra, így, ha adatbázisba szervezzük a csíkozási mintázatokat, matematikai elemző eljárással azonosíthatjuk a nyomtató típust[163].

A passzív technikák közül a szöveges nyomatok karakterkép alapján történő azonosítása emelhető ki. A karakterképzés (különösen a karakter alakját érintő) különbségeit felhasználó vizsgálati módnál a festék túlszóródás (karakter mentén képződő festékmaradványom mennyisége és minősége), a karakterek szegélyének egyenetlensége, a karakter képzéséhez felhasznált festék mennyisége és még néhány tényező rögzítése és vizsgálata adja kiindulási pontot. A művelet során a karakterkép rögzítése, előfeldolgozása (jellemzők azonosítása és tárolása), majd ezt követően a nyomtatótípusok karakter adatbázisának elemeivel történő összehasonlítást követően a nyomtató típusának azonosítására kerül sor. Az összehasonlító adatbázisnak ebben az esetben is jelentős szerep jut (nagyobb, részletesebb adatbázis esetén nagyobb találati arány), amit

[163] MACE, John: Printer Identification Techniques and Their Privacy Implications. University of Newcastle upon Tyne, Computing Science, 2010. p.2.

jelez a vizsgálati mód találati pontossága, mely a paraméterektől függően 25-82% közötti[164] lehet.

Aktív azonosítási technikák

Az előzőektől eltérően, amikor a szakértő a nyomatképzés során természetes módon létrejövő jellemzőket vizsgálta, az aktív technikák alkalmazása esetén a nyomtató gyártója szándékolt módon helyez el azonosításra alkalmas jelzéseket a nyomatokon. Ezen módszer nagy mértékben hasonlóságot mutat a biztonsági okmányok jelölésénél alkalmazott megoldásokkal, így nem vitatható, hogy a nyomat azonosítás e típusánál az okmányszakértők ismeretanyagára és tapasztalatára is szükség lehet.

A biztonsági jelölők (security deterrents) esetén amint az angol elnevezésből is következik az elrettentés az elsődleges cél. Az eredetileg minőségbiztosítási célú eljárás jól alkalmazható forenzikus nyomatazonosítások esetén is. A biztonsági jelölő egyfajta színkód, mely keretszerűen helyezkedik el, hat különböző színt alkalmaz a keret 56 részterületén. A szakértők ezekből a színkódokból képzett ún. funkció vektorok (feature vector) alapján azonosíthatják a nyomtatókat.[165]

A másik kiemelendő aktív technika a nyomkövető kódokkal történő nyomat jelölés, melynek használata az 1980-as évekre nyúlik vissza, amikor megjelentek az első színes fénymásoló berendezések és lézernyomtatók. A színes nyomtatási technológia vezető cége a Xerox biztonsági jelölést épített be az eszközeibe, tekintettel arra, hogy készülékei papírpénz előállítására is alkalmasak voltak[166]. Ez a biztonsági megoldás a tracking dots (nyomkövető jelek) eljárás, melynek nyomatazonosításban történő felhasználását a következő esettanulmányban mutatjuk be.

Esettanulmány – tracking dots alapú nyomatazonosítás

A Nemzeti Adó- és Vámhivatal Bűnügyi Főigazgatósága Központi Nyomozó Főosztály ××× nyomozást folytatott az 1978. évi IV. törvény (régi Btk.) 310. § (1) bekezdésben meghatározott és a (4) bekezdése szerint minősülő az adóbevételt különösen nagy mértékben csökkentő adócsalás bűntett elkövetésének megalapozott gyanúja miatt ××× ××× és társai ügyében. A nyomozás során nagy mennyiségű, számítógépes nyomat formátumú számla került lefoglalásra, melynek elemzését és az ügy szempontjából lényeges információk (nyomtató azonosító kódja) kinyerését rendelte el a nyomozó hatóság.

---

[164] MACE, John, i. m. p.3.

[165] GAUBATZ, Matthew D. – SIMSKE Steven J.: "Printer-scanner identification via analysis of structured security deterrents." Information Forensics and Security, 2009. WIFS 2009. First IEEE International Workshop on. IEEE, 2009.

[166] MACE, John, i. m. p.5.

A szakértőhöz összesen 81 db számítógépes nyomat érkezett, mellyel kapcsolatosan a következő kérdésre kellett választ adni:

> *„1. Nyilatkozzon a szakértő arról, hogy a részére átadott 81 db nyomtatott, eredeti számla számlaképenkénti, tracking dots kódok szerinti vizsgálata alapján a számlákat egy nyomtatóból nyomtatták-e ki. Ennek során, amennyiben lehetséges, a szakértő a nyomtató típusán kívül annak sorozatszámát is állapítsa meg. Továbbá a szakértő tételesen, számlánként állapítsa meg, hogy melyek azok a számlák, amelyek egy nyomtatóból lettek kinyomtatva, és melyek azok, amelyek nem, illetve ez mely számlák esetében nem állapítható meg."*[167]

A szakértői vélemény idézett része alapján feltételezhető, hogy a nyomozó hatóság munkatársa naprakész a számítógépes nyomatazonosítási technikák területén. E kérdés tisztázása azért is szükséges, mert a büntetőeljárásba bevont szakértők munkájával összefüggő alapvető követelményre világít rá.

Az ügy előadója a kirendelést megelőzően telefonon egyeztetett a szakértővel a tekintetben, hogy a számítógéppel előállított számlák azonosítására milyen szakértői módszerek állnak rendelkezésre. Itt szükséges megjegyezni, hogy a nyomozók és a szakértők kapcsolatában meg kell lennie annak a közvetlenségnek, mely alapján a nyomozó mer kérdezni (informatika vagy szakértői eljárást érintő területen), illetve a szakértő válaszol ezekre a kérdésekre.

A szakértő kirendelését megelőzte egy előzetes, személyes konzultáció is, melynek során a szakértő (az ügy részleteinek megismerése nélkül) digitális mintákat vett az vizsgálandó anyagból, annak megállapítása végett, hogy a nyomatok tartalmaznak-e tracking dot jeleket. A mintavétel eredménye alapján került sor a kirendelésre.

Megjegyzendő, hogy az előzetes mintavétel alkalmas lehet a nyomozás során felmerülő költségek mérséklésére, mivel csak abban az esetben érdemes egy vizsgálati eljárást lefolytatni, ha az várhatóan eredményt ad (ez lehet akár kizáró eredmény is). A hasonló esetekben történő előzetes mintavétel (mint a szakértői eljárás megindításának feltétele) fontos része lehetne a büntetőeljárás nyomozási szakaszának, akár eljárási cselekményként definiálva is.

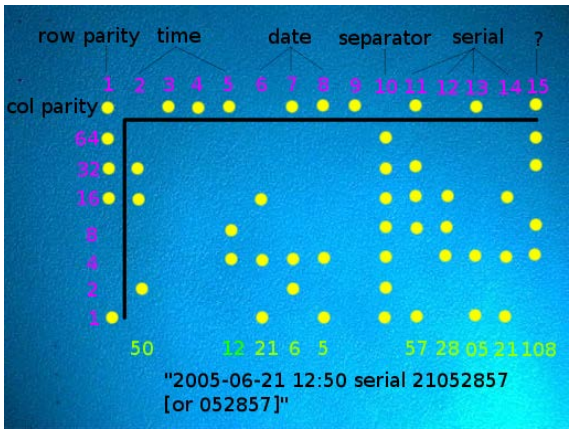
Az előzetes mintavétel alapján (nyomkövető jelek voltak megtalálhatóak a számlarészleteken digitális mikroszkópkamerás megfigyeléssel) elindult az igazságügyi informatikai szakértői vizsgálat, melynek ismertetését megelőzően szükséges a tracking dots azonosítás részletesebb áttekintése.

---

[167] MÁTÉ István Zsolt: Igazságügyi informatikai szakértői vélemény, szakértői ügyszám: 07/2014., p.4. (nem nyilvános irat)

A nyomkövető jelek a számítógépes nyomat teljes felületén megjelenő mikroszkopikus méretű sárga színű pontok, melyek mintázat szerűen ismétlődnek. A pontok szabad szemmel nem láthatók, csak mintegy 60 ×-os nagyítástól válnak észrevehetővé. A sárga pontok mintázata egy 8 × 15 pontból álló mátrixban rendeződik el, s mivel az azonosítás gyártónként eltérhet, az egyes információblokkok tartalma is különböző lehet. A kódok azonosítását az Electronic Frontier Foundation alapítvány Machine Identification Code Technology (Eszközazonosító kódtechnológia) projektje végezte el, melyet DocuColor Tracking Dot Decoding Guide című tanulmányában hozzáférhetővé is tett.[168]

A következőkben e tanulmány alapján mutatjuk be a nyomkövető jelek értelmezését.



11. ábra - Tracking dots tárolási szerkezet[169]

A nyolc sorból és tizenöt oszlopból álló kódtáblázat első sora és első oszlopa az ún. paritás biteket tartalmazza. Ezek olyan hibajelző kódok, melyek segítségével észlelhetők a mátrixban lévő esetleges hibák. Valamennyi oszlop és valamennyi sor (az első sort kivéve) páratlan paritású, ami azt jelenti, hogy az adatbitekből az adott sorban vagy oszlopban páratlan darabszámú helyezkedik el. Abban az esetben, ha az adatbitek páros darabszámúak, a paritás bit 1 értéket vesz fel, egyébként 0 étéket.

Az egyes oszlopokban a következő információk kódoltak (balról jobbra):

1: paritás bit

2: perc érték, a nyomtatás időpontja

3-4: használaton kívül

5: óra, a nyomtatás időpontja

6: nap, a nyomtatás időpontja

7: hónap, a nyomtatás időpontja

[168] DocuColor Tracking Dot Decoding Guide. Electronic Frontier Foundation.
online: https://w2.eff.org/Privacy/printers/docucolor/, utolsó hozzáférés: 2014.06.06

[169] Forrás: https://w2.eff.org/Privacy/printers/docucolor/

8: év, a nyomtatás időpontja

9: használaton kívül

10:elválasztó, értéke tipikusan 1 valamennyi pozícióban

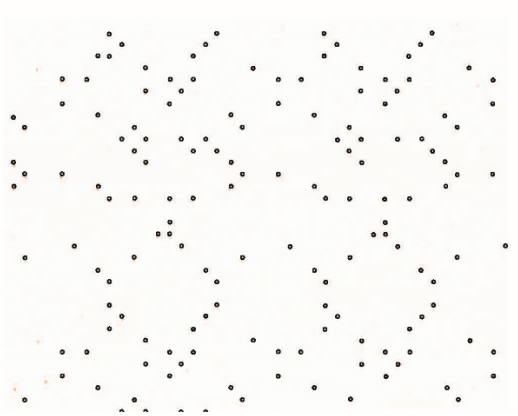
11-12-13-14: nyomtató sorozatszáma binárisan kódolt decimális számmal,

15: ismeretlen, leggyakrabban üres

A projekt keretében összesen 200 nyomtató vizsgálatára került sor, melyek közül 136 nyomtató esetén sikerült az egyedi azonosítási kódok meghatározása. Az így létrejött adatbázishoz a projekt egy számítógépes programot is kifejlesztett (elérhető a https://w2.eff.org/Privacy/ printers/docucolor/#program hivatkozáson), mely a kódmintázat megadását követően azonosítja a nyomatot létrehozó eszközt (amennyiben annak típusa szerepel az adatbázisban).

Az esettanulmányban szereplő ügyre visszatérve, elsőként a számlaképeket tartalmazó nyomatok egyedi azonosítása történt meg a kirendelő határozatban szereplő felsorolás sorrendjében adott sorszám révén. Ezt követően az egyes nyomatokról egy teljes terjedelmű (A/4 méretű), de alacsony felbontású (600 dpi, mintegy 360 000 képpont négyzethüvelykenként) digitális kép készült 24 bites színmélységgel (> 16 millió szín megkülönböztetésével). A tracking dot azonosítás céljaira a számlakép 3 × 6 centiméteres részlete került digitalizálásra 2400 dpi (mintegy 5,7 millió képpont négyzethüvelykenként) felbontásban, azonos színmélység mellett.

A létrejött digitális állományokat ezt követően a szakértő grafikus szoftverrel dolgozta fel oly módon, hogy a nagy részletességű képen elkülönítette a papír színétől eltérő részleteket egy ún. színmaszk segítségével. A színmaszk érzékenységének módosításával az ún. képzaj kiszűrhető volt az esetek nagy részében. A színmaszkos feldolgozást követően 50 nyomat esetében történt további vizsgálat. Ezek a nyomatok tartalmaztak értékelhető minőségű nyomkövető kódot, a többi nyomatról vagy hiányzott a kód, vagy a képzaj miatt nem volt azonosítható.



12. ábra - Nyomkövető jelek mintázata[170]

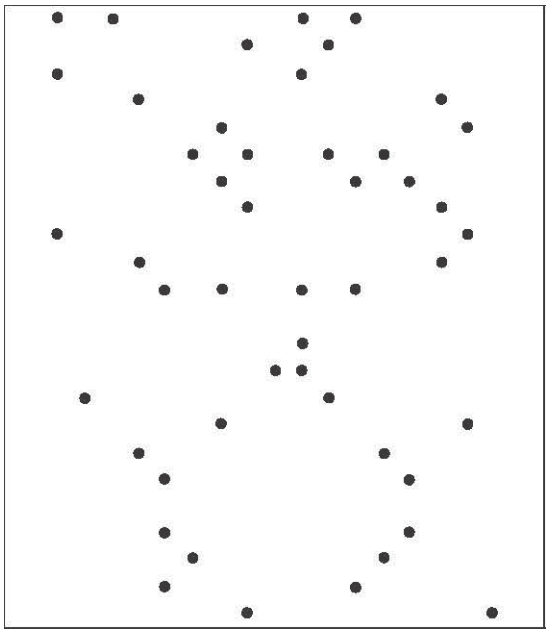
Az egyes nyomatokról kinyert kódokat a szakértő táblázatban ábrázolta, mely alapján elvégezte a típusazonosítást.

28. táblázat - Számítógépes nyomatok vizsgálati eredményei - összefoglaló táblázat

Státusz	Mennyiség
Ismeretlen	1
Nem tartalmaz nyomkövető kódot	53
Nyomkövető kódot tartalmaz	**136**
Tisztázatlan	10
Összesen	**200**

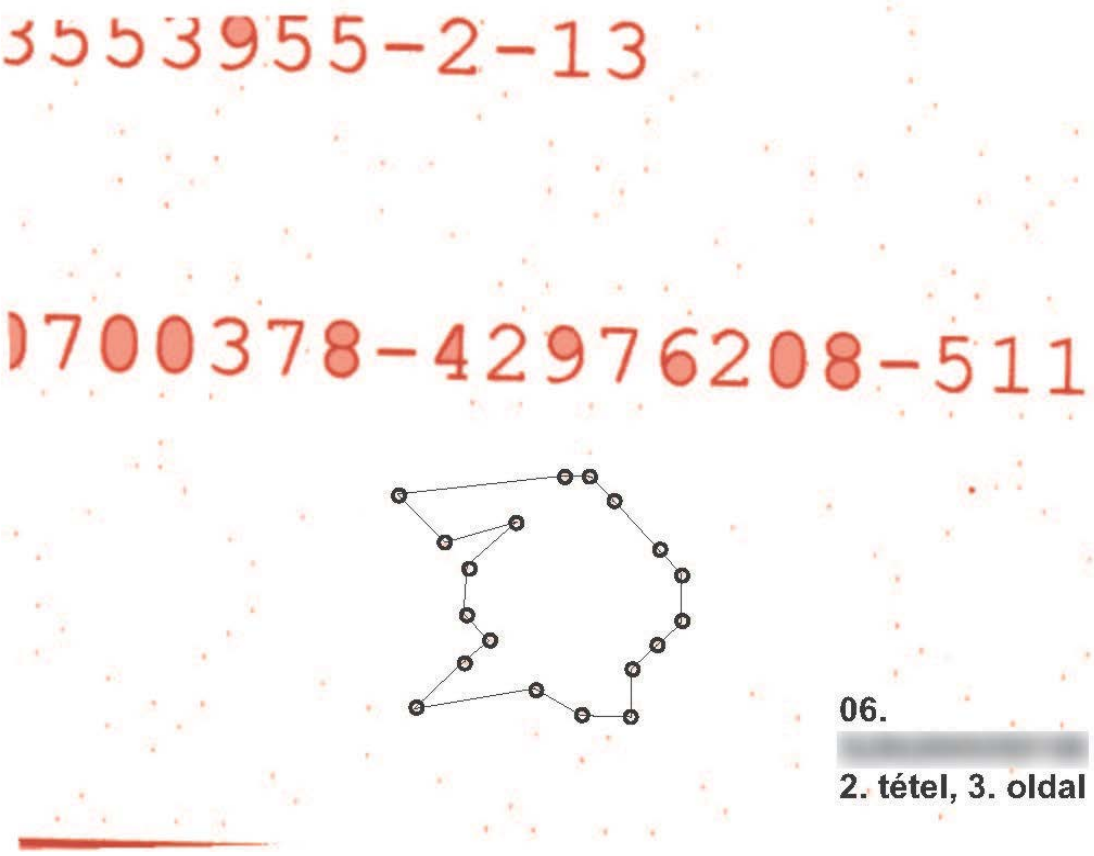
Megállapítható volt, hogy a mintázat nem szerepel az MICT Projekt adatbankjában, ezért a konkrét nyomtató típus és egyedi nyomtató azonosító megállapítására nem volt lehetőség.

[170] MÁTÉ István Zsolt: Igazságügyi informatikai szakértői vélemény, szakértői ügyszám: 07/2014., vizsgálati alapanyag feldolgozott részlete. (nem nyilvános irat)



13. ábra - A nyomatokon azonosított egyedi mintázat

A vizsgálat folytatásában a szakértő megvizsgálta, hogy a nyomatok azonos, vagy különböző eszközökből származnak-e. Ehhez az első vizsgált kódmintázaton felvett egy 19 nyomkövető jelből álló zárt sokszög alakzatot, mely komplexitásából adódóan azonosításra alkalmasnak mutatkozott.



14. ábra - Azonosítást lehetővé tevő mintázat

A folytatásban a szakértő megvizsgálta, hogy a sokszög alakzat mely nyomatokon illeszthető pontosan (darabszám és elhelyezkedés tekintetében egyaránt) a kérdéses nyomatokon szereplő tracking dot jelekre. Megállapítást nyert, hogy az alakzat valamennyi, azaz mind az ötven részletes vizsgálat alá vont számlakép részleten pontosan illeszkedik, így a szakértő megállapíthatta, hogy a nyomatok nagy valószínűséggel azonos eszköztől származtak, de annak típusára vonatkozóan nem tudott nyilatkozni.

A számítógépes nyomatok azonosítása mellett az egyes ügyekben fontos lehet egy-egy eszköz használatának kizárása is. A Somogy Megyei Rendőr-főkapitányság Bűnügyi Igazgatóság ××× Osztály által történt kirendelés esetében a szakértőnek egy adott eszköz használatára vonatkozóan kellett nyilatkoznia szintén a tracking dots vizsgálati módszer alkalmazásával.

A kirendelő határozat szerint a Somogy Megyei Rendőr-főkapitányság Bűnügyi Igazgatóság ××× Osztály nyomozást folytatott a Büntető Törvénykönyvről szóló 2012. évi C. törvény 373. § (3) bekezdés b) pontjába ütköző és a (2) bekezdés b) pontjának be) alpontja szerint minősülő kisebb kárt okozó üzletszerűen elkövetett csalás bűntettének megalapozott gyanúja miatt ××× ××× ellen folyamatban lévő büntetőügyben. A szakértőnek a következő kérdésre kellett választ adnia:

> *„A szakértő nyilatkozzon arra vonatkozóan, hogy a lefoglalt Konica Minolta magicolor 2400 típusú nyomtatóból kinyomtatott tesztoldal és a szintén lefoglalt, és a szakértőnek átadott bűnjelek (×××/×××- ×/2014. bü. számú bűnjelek közül: 3,4,6,7,8 -as tételek, ××× feliratú lap 2 db, 2 db ××× feliratú matrica, és 1 db excel táblázatos papírlap) összevetése alapján azonos e az eredet, illetve így a jelzett nyomtatóból kerültek-e kinyomtatásra."*

Ebben az esetben a szakértő kizáró véleménye azon alapult, hogy a kérdéses nyomatokon nem voltak megtalálhatók a nyomkövető jelek, míg a teszt oldalakon a nyomkövető jelek azonosíthatók voltak.

Összefoglalás

Az ismertetett két eset nem csupán arra világít rá, hogy a nyomozó hatóság és adott esetben az ügyészség és bíróság munkatársai részére is szükségszerű az egyes szakértői módszerek ismerete (a felhasználhatóság felismerésének szintjén), de arra is, hogy a büntető eljárás nyomozási szakaszában a szakértő és a nyomozó hatóság közötti kommunikáció nem csak az eljárás minőségét, eredményességét, de gazdaságosságát is meghatározhatja. A költséghatékony bűnüldözés a 21. század egyik kihívása lehet, különösen a komplexebbé váló ügyekből adódó növekvő szakértői részvétel miatt. E kihívásokra a helyes válaszokat a gyakorlat és az ezt megalapozó kutatás adhatja meg.

9.3.2 A Cloud Forensics módszertani jellemzői

A felhőszolgáltatásokkal kapcsolatos forenzikus vizsgálatok módszertani meghatározása a már szabványosított computer forensic követelményeivel összehasonlítva történhet meg a legegyszerűbben. A vonatkozó nemzetközi szabvány az ISO/IEC 27037:2012, Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence (Információtechnológia - Biztonsági eljárások – Segédlet a digitális bizonyítékok azonosításához, összegyűjtéséhez, kinyeréséhez és megőrzéséhez).

A két terület követelmény- és eljárásrendszere az Incident Management and Forensics Working Group 2013-as tanulmánya alapján[171] az alábbiak szerint foglalhatók össze.

Az ellenőrizhetőség (Auditability)

A hagyományos számítógépvizsgálat során a szakértő dokumentálja az elvégzett műveleteket, felsorolja azokat az eszközöket amelyeket megvizsgál (merevlemez, optikai vagy SSD tár stb.), leírja a vizsgálathoz használt szakértői berendezések főbb adatait (pl. forezikus duplikátor, írásvédő stb. A követelmény teljesülése esetén utólag megállapíthatóvá válik, hogy az eljárás tartalmazott-e olyan lépést mely a bizonyíték módosulásához vezetett (pl. írásvédő eszköz hiánya, berendezés bekapcsolása stb.). A követelmény a szakértői vélemény és annak mellékletei formájában valósul meg.

A felhőszolgáltatás esetén a szakértő nem fér hozzá a fizikai eszközhöz, mely a megszerzendő tartalmat tárolja, ráadásul az tartalom több eszközön történő megoszlása (az adatok több kiszolgáló gép több háttértárolóján elosztva találhatók) sem követhető a szakértő által. A tűnékeny (volatile) adatokhoz történő hozzáférés (pl. memória tartalom) az előzőekhez hasonlóan nem valósítható meg. A szakértő a felhőszolgáltatáshoz annak szoftveres komponensein keresztül férhet hozzá, a szolgáltatás típusától függő (lásd részletesen a felhőszolgáltatás műszaki tartalma részt) eltérő mélységben.

A dokumentálhatóság az előzőekből adódóan a szakértő által alkalmazott szoftver és hardver eszközök dokumentálását, valamint a felhőszolgáltatás különböző hozzáférési szintjeihez történő kapcsolódás leírását tartalmazhatja. A vizsgált tartalomra vonatkozó adatok hiánya megbízhatósági deficitet jelent a felhőszolgáltatás vizsgálatának hátrányára.

A megismételhetőség (Repeatability)

A követelmény teljesítésének alapja a szakértő tevékenységének pontos dokumentálása. A leírás részletességének el kell érnie azt a szintet, mely alapján az eljárás minden

[171] Incident Management and Forensics Working Group. 2013. Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing. pp.13-17.

lényeges mozzanata megismételhetővé válik. A leírásnak tartalmaznia kell az alkalmazott eljárások és módszerek leírásán kívül az vizsgálatnál használt eszközök pontos adatait és vizsgálati körülmények (a módszerek és eszközök kapcsolat) leírását is. Ez a követelmény a szakértői vélemény vizsgálatról szóló részében valósul meg.

A felhőszolgáltatások esetében az előzőekben márt tárgyaltak szerint csak a szakértői oldal módszerei és eszközrendszere kerülhet rögzítésre. A felhőszolgáltatás oldalának dokumentálását az idézett tanulmány a pillanatkép (snapshot) módszerrel látja – korlátozott módon – megvalósíthatónak. A pillanatkép módszerrel a vizsgált rendszer egyes jól meghatározott időpontokban (pl. időbélyeggel hitelesítve) megvalósult aktuális állapotát rögzítjük. Így az alapállapot és a változások nyomon követése révén a rendszer módosulása megismételhetővé válik.

A reprodukálhatóság (Reproducibility)

A reprodukálhatóság követelménye a megismételhetőséghez hasonlóan a pontos dokumentáltságon alapul. A hagyományos computer forensics típusú vizsgálat esetén a módszerek és eszközök paraméterei mellett teljesülnie kell a bizonyíték változatlanul hagyása feltételének is. El a gyakorlatban azt jelenti, hogy a vizsgálat során az eredeti digitális bizonyítékot (definíciót lásd a digitális bizonyítékokról szóló részben) tartalmazó fizikai eszköz nem változhat meg, nem semmisülhet meg. Ezt a követelményt a hagyományos vizsgálatok során sem minden esetben képes teljesíteni a szakértő, különösen az változékony adatok (memória tartalom, aktív hálózati eszközök adattáblái stb.), illetve az élő rendszerek vizsgálatakor.

A felhőszolgáltatások esetében a pillanatkép módszer alkalmazását tekinthetjük a gyakorlatban is megvalósítható megoldásnak. Az egyes rendszerállapotok (pillanatképek) eredeti vizsgálati körülményekkel azonos paraméterekkel történő elemzése (visszajátszása) teljesítheti a követelmény által szabott feltételek teljesülését. A korábbiakhoz hasonlóan érezhető, hogy ez esetben sem teljes a computer és cloud terület módszertana közötti azonosság, ami a felhőszolgáltatás mögötti műszaki tartalom jellegéből, annak komplexitásából vezethető le.

Az igazolhatóság (Justifiability)

Az igazolhatóság követelménye az első olyan feltétel, melyet mindkét vizsgálati területen azonosnak tekinthetünk. A követelmény akkor teljesül, ha a vizsgálatot végző szakértő bemutatja azoknak az eljárásoknak és módszereknek a műszaki, tudományos hátterét, mely az adott időszakban érvényes minőségi szinten biztosítja a hiteles bizonyítékok szolgáltatását. A követelmény kiterjed az alkalmazott eszközökre, illetve azok használati módjára is.

A követelmény teljesülése a szakértői véleményben szereplő vizsgálati részben történik oly módon, hogy a szakértő az egyes vizsgálati mozzanatoknál feltünteti az azt

alátámasztó szakirodalmi hivatkozásokat. A hivatkozások összegzése történhet valamely szabványos idézési rendszer (pl. Harvard, ISO 690-2:1997, MLA, APA stb.) szerint a szakértői vélemény mellékletében.

A módszerekre és eljárásokra vonatkozó általános követelmények után fókuszáljuk figyelmünket a digitális bizonyítékok kezelésével kapcsolatos közvetlen tevékenységekre.

Az azonosítás (Identification)

A számítógépes rendszer vizsgálatának első lépéseként fel kell állítani a potenciálisan vizsgálandó eszközök, vagy komponensek változékonysági sorrendjét (Order of Volatily), mely első helyen tartalmazza a legváltozékonyabb elemeket (pl. processzor regiszter és gyorsítótár tartalmak, számítógépes hálózati útvonalválasztó útvonaltáblája, számítógép memória tartalma stb.), melyekből legelsőként kell begyűjteni az adatokat. A rejtett bizonyítékok beazonosítása szintén e követelmény teljesítéséhez tartozik. Ezek lehetnek a méretükből (memóriakártyák, SSD tárak), elhelyezésükből (kettős felhasználású eszközök, hálózati tárak, távoli elérésű eszközök), vagy egyéb tulajdonságukból adódóan nehezen azonosítható tárgyak, adatok, szoftverek.

A felhőszolgáltatások esetén a korábbiakban már említett pillanatkép adatok alapján, az egyes szolgáltatástípusok esetén eltérő adatkörök megfigyelésével történhet (itt nem fizikai eszközök azonosításáról, hanem csak adatokról beszélhetünk) az azonosítás mozzanata.

A szoftver-szolgáltatás (SaaS) esetén az igénybe vett alkalmazás szintjén létrejött naplófájlokból kinyerhető információk – pl. felhasználói engedély hibák, felhasználói fiókkezelési hibák (ki, mit, mikor tett), sebességproblémák – lehetnek potenciális bizonyítékok.

A platform-szolgáltatás (PaaS) esetén a program specifikus naplófájlok, a javítócsomag állapotok, a hitelesítési hibák, az operációs rendszer ún. kivételei (hibái) és a kapcsolódó figyelmeztetések, valamint a rosszindulatú programok elleni rendszerek üzenetei válhatnak majd digitális bizonyítékká.

Végül az infrastruktúra-szolgáltatásnál (IaaS) a rendszer szintű naplófájlok, hypervisor rendszerek eseményei és naplóállományai, virtuális gépek nyers (raw) állományai, memóriatartalom pillanatképek, behatolás érzékelők és tűzfalak eseményei, hálózati események és hálózati adatcsomag megfigyelés, tárlók naplóállományai, mentések képezhetik a kinyerhető adatokat.

Megfigyelhető, hogy a három különböző szolgáltatás esetén eltérő karakterisztikájú potenciális bizonyítékok nyerhetők ki. Ezek (jellegükből adódóan) különböző erősségű bizonyítékot szolgáltatnak majd. E körülmény felveti a digitális bizonyíték fogalmára vonatkozó megállapítások árnyalását (részletesen lásd később).

Az összegyűjtés (Collection)

A hagyományos vizsgálati eljárásban az összegyűjtés során a digitális bizonyítékot tartalmazó eszközt eltávolítják eredeti helyéről, majd laboratóriumban ellenőrzött körülmények között vizsgálják azt, későbbi kinyerés és elemzés céljából.

A definíció már a computer forensics környezetben sem tökéletes, hiszen egy számítógépes hálózati környezetben a fizikai eszközök elmozdítása az esetek jelentős részében nem valósítható meg, vagy legalábbis nem célszerű (a vizsgált ügyhöz nem kapcsolódó személyek, szervezetek jogai sérülhetnek általa).

Ha ezt a szempontot kiterjesztjük a felhőszolgáltatásokra, akkor belátható, hogy a fizikai eszköz eltávolítása nem csupán azért nem valósítható meg, mert több felhasználó (szervezet) osztozik a hardver és szoftver erőforrásokon, hanem azért sem, mert a fizikai eszközök gyakran más ország(ok) joghatósága alatt, illetve szétszórtan (különböző fizikai helyeken) találhatóak. Ebből a körülményből adódóan az összegyűjtést egyes esetekben csak maga a Cloud Service Provider (Felhőszolgáltató) tudja megvalósítani. Ez utóbbi esetben a bizonyíték hitelességének definíciója szorul felülvizsgálatra.

A kinyerés (Acquisition)

A számítógép rendszerek vizsgálatakor a kinyerés során másolat készül a lehetséges digitális bizonyítékot hordozó eszköz(ök) tartalmáról. Itt is érvényesek a fizikai eszközökre az összegyűjtésnél tett megállapítások. Ezek mellett a hagyományos adatkinyerő eszközök (forensic duplicator, forensic bridge stb.) nem használhatók, ugyanakkor előtérbe kerülnek a szoftveres (network forensics területén alkalmazott) megoldások, melyek esetenként megsérthetik a bizonyíték megváltoztatásának tilalmát (lásd az esettanulmányt).

Az előzőekből következik, hogy kinyerésnek a felhőszolgáltatások esetében a logikai elemekre kell koncentrálnia, nem a fizikai tárakra.

A megőrzés (Preservation)

A digitális bizonyítékok megőrzésével kapcsolatos eljárások mindkét terület esetén a lehetséges digitális bizonyítékok integritásának megőrzését jelentik. Ebben a szakaszban a kinyert bizonyítékokat megvédjük az illetéktelen hozzáféréstől vagy eltüntetéstől. A követelményt a felügyeleti lánc (chain of custody) fenntartásával biztosíthatjuk, ugyanakkor könnyen belátható, hogy ennek fenntartása a különböző földrajzi és jogi környezeten keresztül nem egyszerű feladat.

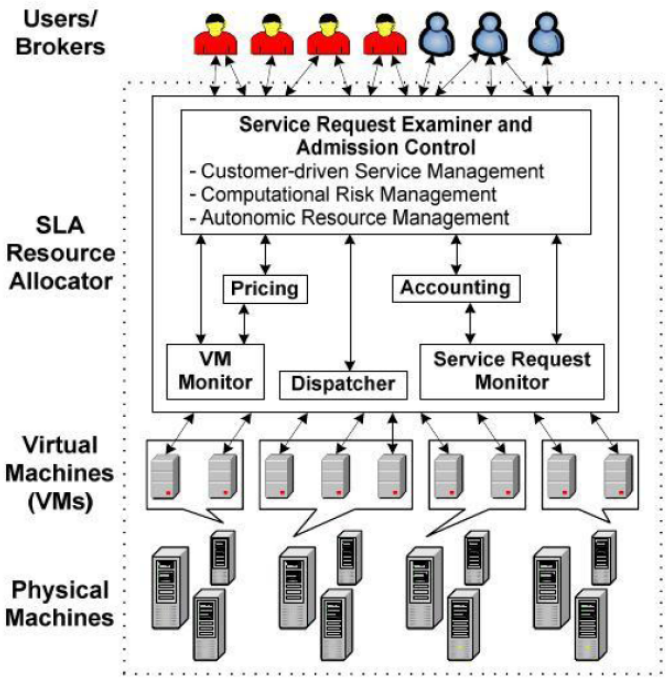
A felhőszolgáltatás műszaki tartalma

Az előzőekben bemutatott követelményrendszer már előre jelzi az igazságügyi informatikai szakértő előtt álló problémák egy részét. A teljes kép kialakításához és annak megértéséhez nélkülözhetetlen röviden áttekinteni a felhőszolgáltatások mögött üzemelő műszaki tartalom néhány alapvető komponensét.

A felhőszolgáltatások fizikai alapját számítógépek, a gépeket összekötő informatikai hálózat és annak különféle eszközei (kapcsolók [switch], útvonalválasztók [router] stb.) adják. Ezek az eszközök lehetnek egy (single-site), vagy több (distributed datacenters) földrajzi helyen, a fizikai kialakításuk lehet egységes, vagy vegyes összetételű egyaránt.

Ezeket a fizikai eszközöket és a kapcsolódást biztosító hálózatot a hypervisor programok kezelik és fogják össze egy, vagy több virtuális géppé. Ezek a rendszerek teszik lehetővé, hogy a felhasználó a sok rendszerkomponenst egyet eszközként, egy virtuális számítógépként lássa. A hypervisor programok két fő csoportba sorolhatók: az ún. natív hypervisor közvetlenül kezeli a hardvereket (pl. Citrix, XenServer), ami azt jelenti, hogy a fizikai gépeken nem fut rendszerszoftver, hanem a hypervisor kezeli valamennyi háttérszámítógép erőforrásait (processzort, memóriát, tárterületet). A másik típus az ún. a hosztolt hypervisor, mely esetében a fizikai gépeken operációs rendszerek működnek és azok rendszerkörnyezetében futnak (pl. VMWare Workstation, VirtualBox) a virtuális számítógépeket létrehozó hypervisor programok.

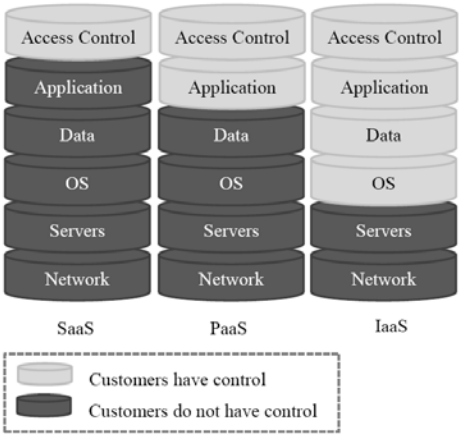
A hypervisorok által létrehozott környezetben valósul meg maga a valós idejű szolgáltatás (service level agreement layer), amely a felhasználói bejelentkezést, a szolgáltatások igénybevételét, annak minőségének ellenőrzését és ellenértékének kiszámítását is lehetővé teszi (lásd az alábbi ábrán).



15. ábra - Felhőszolgáltatás műszaki háttere[172]

A felhasználó a szolgáltatási modelltől függően különböző mértékben gyakorol ellenőrzést a felhőszolgáltatás imént bemutatott szintjei felett. A szervekhez és az azokat összekötő hálózati infrastruktúrához történő hozzáférés mindhárom szolgáltatási modell esetében tiltott a felhasználók számára. Az IaaS esetén az operációs rendszer szintjétől felfelé, a PaaS esetén az alkalmazások szintjétől felfelé, addig a SaaS esetén csupán a hozzáférés szintjén gyakorol ellenőrzést a felhasználó[173].

[172] REILLY, Denis - WREN, Chris - BERRY, Tom: Cloud Computing: Pros and Cons for Computer Forensic Investigations. in International Journal Multimedia and Image Processing Volume 1, Issue 1, March 2011 online, 2011. Infonomics Society, online: http://www.infonomics-society.org/IJMIP/. p.27.
[173] ZAWOAD, Shams, and RAGIB, Hasan. "Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems." *arXiv preprint arXiv:1302.6312* (2013). p.5



16. ábra - A felhasználó hozzáférési szintjei a különböző szolgáltatási modellek esetén[174]

Amint arra korábban már utaltunk a felhő környezetben néhány alapvető forensics követelmény nem teljesül teljes mértékben: mivel felhőszolgáltatás fizikai szintjéhez, ahol az adatok eltárolása történik maga a felhasználó sem rendelkezik felügyeleti jogkörrel, így ezen adatok digitális bizonyítékként történő kinyeréséhez sem lesz elegendő a felhasználói oldal adatinak (pl. felhasználói nevek, jelszavak stb.) a megszerzése a szakértő részéről, hanem a szolgáltatói együttműködés is szükséges lesz, amint azt a következő példából is láthatjuk.

Bizonyítékok kinyerése a felhőszolgáltatásokból

A digitális bizonyítékok kinyerésének lehetőségét és az alkalmazható módszereket (beleértve a megvalósításhoz szükséges szoftvereket is) DYKSTRA és SHERMANN vizsgálta meg egy esettanulmányban, melynek tárgya az Amazon EC2 (Amazon Elastic Compute Cloud - Amazon Web Services) volt. A kutatók a felhőszolgáltatás három különböző szintjéről kísérelték meg az adatok (bizonyítékok) kinyerését:

1. A virtuális gépen működő operációs rendszer szintjéről (guest OS)
2. A virtuális gép szintjéről (virtual machines / virtualization layer)
3. A fizikai hardvereken futó operációs rendszer szintjéről (host OS)

[174] ZAWOAD, Shams, and RAGIB, Hasan. im. p.3.

Az adatok kinyeréséhez az igazságügyi informatikai szakértői gyakorlatban alkalmazott szoftvereket használták fel:

- EnCase (Guidance)
- FTK (Access Data)
- Fastdump
- Memoryze

Az esettanulmány adatai[175] szerint mindhárom esetben kinyerhető volt a bizonyíték a rendszerből, a kinyerés módja azonban megkérdőjelezi a későbbi felhasználhatóságot.

Az első két esetben a kutatók távoli hozzáférésen keresztül ügynök programot (agent) juttattak a vizsgálandó rendszerbe (ezzel meg is változtatták annak eredeti tartalmát), majd ezekkel a programokkal kinyerték a szükséges információt. A harmadik esetben a szolgáltatótól rendelték meg az export végrehajtását. Bár mindhárom esetben sikeres adatkinyerés történt, a valóságos (tehát nem a kísérlet szerinti szimulált) helyzetben a kinyert bizonyítékok hitelessége kérdésessé válhat akár a nyomozási, akár a bírósági szakaszban.

Ha a korábban bemutatott módszertani követelményeket és a szolgáltatások mögött működő műszaki tartalmat a szakértő nézőpontjából tekintjük, akkor következő feltételeknek (szintenként és halmozott jogosultságoknak) kell teljesülniük a sikeres bizonyíték kinyerés érdekében:

29. táblázat - Halmozott bizalmi rétegek IaaS környezetben[176]

6	Alkalmazások (Guest application/data) szintje
5	Virtuális rendszeren futó operációs rendszer (guest OS) szintje
4	Virtualizációs (virtualization) szint
3	Kiszolgáló operációs rendszer (host OS) szintje
2	Hardver (physical hardware) szint
1	Hálózati (network) szint

A hálózat (Network – layer 1) szintjén a kinyerhető adat a hálózaton mozgó adatcsomag (packet) lehet, mely hálózatfigyelés során az adatcsomagok kinyerésével (packet capture) valósítható meg, ennek eléréséhez fizikailag hozzá kell férnie a szakértőnek a hálózathoz. A követelmény a gyakorlatban nem teljesíthető.

A fizikai hardver (Physical hardware – layer 2) szintjén a szakértő a tárolókon (pl. merevlemezeken) megtalálható adatokat nyeri ki oly módon, hogy a hálózaton keresztül

[175] DYKSTRA – SHERMAN. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. in Digital Investigation 9 (2012) S90–S98. p.93.
[176] DYKSTRA – SHERMAN. im. p.93.

csoportosan, vagy egyenként hozzáfér a fizikai tárakhoz. A követelmény a gyakorlatban nem teljesíthető.

A kiszolgáló operációs rendszere (Host OS – layer 3) szintjén az infrastruktúra szolgáltatás (IaaS) esetében a szakértő hozzáfér a virtuális lemezek (tehát a fizikai adathordozókból képzett logikai tárterület) adatihoz, amennyiben rendelkezik a szolgáltatást igénybe vevő legmagasabb felhasználói jogosultsággal. Az adatkinyerés hitelessége a hagyományos eljárásoknak megfelelően a hálózat – hardver – kiszolgáló operációs rendszer egymásra épülő ún. bizalmi rétegeihez történő hozzáféréssel lehetséges (amint az a magasabb szinteken is megtörténik). A gyakorlatban a host OS szintű hozzáférés valósítható meg.

A virtualizációs (Virtualization - layer 4) szint a hypervisor programok szintje. Az itt fellelhető digitális bizonyítékok az ún. VMI (virtual machine introspection tool – virtuális gép önvizsgáló eszköz) révén érhetők el. Ezek a rendszerek a virtuális gépek biztonsági megfigyelő központjának alrendszeréből az ún. Introspection Library-ból (megfigyelési adatok tárhelye) emelik ki az információkat a virtuális gép futásával (működésével) kapcsolatban. Különösen a fizikai memória tartalom érintett ebben az adatkörben[177].

A virtuális gépen futó operációs rendszer (Guest OS – layer 5) szintjén már lehetőség van távoli hozzáférés segítségével forenzikus szoftverek futtatására (ahogy az esettanulmányban is tették). Ebben az esetben ún. servlet (a távoli operációs rendszer környezetében futó) alkalmazást juttatnak a vizsgálandó környezetbe, hasonlóan, mint egy számítógépes vírusfertőzés esetében. Az alkalmazás a vizsgálati adatokat a távoli asztal protokollon (Remote Desktop Protocol - RDP) keresztül juttatja el a szakértőhöz. Érzékelhető, hogy ennél a vizsgálati módszernél a vizsgálandó rendszer tartalma (pl. memória tartalom) megváltozik, így a bizonyíték fogalmának, karakterisztikájának is tükröznie kell ezt a tényt ebben a vizsgálati közegben.

Végül az adatok és alkalmazások (Guest application/data – layer 6) szintjén az elérendő adatok típusától függő (akár hagyományos computer forensics) eszközök használhatók, de a használat minőségi paraméterei (ellenőrizhetőség, megismételhetőség stb.) csak az összes hozzáférési szintet magába foglaló bizalmi lánc megléte esetén valósulhat meg. Az egy időben teljesülő feltételekre a szakértői gyakorlatban szinte soha (valójában soha) nincs példa.

Más kutatók az adatok kinyerésének vizsgálata helyett a kinyert adatok hitelességének ellenőrzésére és annak igazolására fókuszálnak. Megközelítésükben fontos szerepet játszik a felhőszolgáltató (Cloud Service Provider - CSP) együttműködése. Az adatok

[177] DOLAN-GABITT B, PAYNE B, LEE W. "Leveraging forensic tools for virtual machine introspection." Technical Report, Georgia Institute of Technology, GT-CS-11-05; 2011. p.1.

múltbéli birtoklásán alapuló bizonyítás (Proof of Past Data Possession - PPDP) esetében a felhőszolgáltatónál működtetett rendszer a felhőszolgáltatás valamennyi felhasználójának valamennyi adatáról „digitális ujjlenyomatot", azaz hash kódos ellenőrző számot generál, mely alapján agy algoritmus a későbbiekben el tudja dönteni, hogy a vizsgált állomány az adott időszakban, az adott tartalommal a tárolt adatok között volt-e[178]?

Hasonló koncepción alapul a leszármazási adatok tároló rendszere (Provenance Aware Storage System - PASS), melyet szintén a felhőszolgáltató üzemeltet és a felhőbe kerülő objektumokról – legyen az bármilyen is – gyűjt adatokat[179]. A későbbiekben ezek a származási adatok hasonlíthatók össze a potenciális bizonyíték adatival.

Amint az jól látható, mind az adatkinyerés, mind az adatok hitelességének vizsgálata nagymértékben függ a felhőszolgáltató együttműködésétől, mi több a felhőszolgáltató előzetes, az együttműködést megalapozó tevékenységétől (különféle szolgáltatások üzemeltetése a felhőben, későbbi kriminalisztikai felhasználás céljára). Ebből adódóan a kutatási eredményeket alkalmazni kívánó igazságügyi informatikai szakértők önállóan nem, vagy csak korlátozott eredménnyel képesek az adatok hiteles kinyerésére a felhőszolgáltatásokból. A felhőszolgáltatókkal történő együttműködés a nyomozó hatóságon (law enforcement) keresztül történhet, a nemzetközi bűnügyi együttműködés jogszabályi keretein belül. Ennek a körülmények több gyakorlati következménye is van: a szakértői tapasztalatok szerint a felhőszolgáltatók együttműködési hajlandósága függ az adatkérést megalapozó ügy büntetőjogi súlyától, esetleg az elkövetési értéktől (!); másrészt a nyomozó hatóságok a még nem kialakult adatkérési gyakorlat miatt eltekinthetnek a bizonyítékok beszerzésének ezen formájától.

A bizonyítékok megszerzése mellett azok bemutatása – a nyomozó hatóság, illetve a bíróság részére – okozhat nehézséget, tekintettel arra a körülményre, hogy a digitális bizonyíték, s azon belül a felhőszolgáltatásból származó speciális karakterisztikájú digitális bizonyíték értékelése a büntetőeljárás szereplőitől – legyenek azok nyomozók, ügyvédek, ügyészek, vagy bírák – a jelenleginél nagyobb informatikai felkészültséget igényel. Ennek hiányában az büntetőügyek kimenetelét esetenként jelentősen meghatározó digitális bizonyíték értékelésének felelőssége az ügyben eljáró igazságügyi informatikai szakértőre hárulhat. Ez nem csak messze túlmutat a szakértők büntetőeljárásban betöltött szerepkörén, de jelentősen torzíthatja jogszabályok által meghatározott felelősségi köröket is.

---

[178] ZAWOAD, Shams, and RAGIB, Hasan. "Towards building proofs of past data possession in cloud forensics." *SCIENCE* 1.4 (2012). p.202.

[179] MUNISWAMY - REDDY – MACKO – SELTZER. "Provenance for the Cloud." *FAST*. Vol. 10. 2010. p.2.

A digitális bizonyíték fogalmának differenciált használata

A felhőszolgáltatás speciális, a korábbi bűnügyi informatikai környezettől jelentősen eltérő karakterisztikája miatt felvetődik a bizonyíték, pontosabban a digitális bizonyíték fogalmának többrétegű meghatározása, mely az egyes vizsgálati környezetekre (pl. számítógép, hálózat, mobil eszköz, felhőszolgáltatás stb.) vonatkozóan definiálja magát a fogalmat, s teszi ezt oly módon, hogy a bizonyíték hitelességének és érvényességének mértékét az adott környezetben határozza meg.

A differenciálást ugyanakkor oly módon kell megvalósítani, hogy az ne zavarja meg a büntetőeljárásban a bizonyítékot felhasználó szereplők (bírák, ügyészek, ügyvédek, nyomozók) körében még le sem tisztult fogalomkört: pontosan a digitális bizonyíték fogalmát.

Csábítónak tűnik a szakértői véleményekben is gyakori valószínűségi megközelítés, mely esetén a bizonyíték erősségét, megfelelőségét %-os arányban kifejezve adhatja meg a szakértő. Ez a megoldás álláspontom szerint tévútra vezet, különösen annak fényében, hogy az informatikai szakterületen alkalmazott valószínűségek mögött álló tényeket (melyek megalapozzák a valószínűség mértékét) gyakran becsléseken, szakértői tapasztalaton, de legalábbis nem egzakt számításokon alapulnak.

Helyesebb megközelítésnek tűnik a korábbiakban ismertetett bizalmi szintek láncolatán alapuló osztályozás, mely azt határozza meg, hogy a bizonyíték kinyerése milyen közelségben volt a fizikai adatokhoz. A bizonyíték kinyerés módszertanának ugyanakkor minden szint esetében teljesítenie kell, a korábbiakban ismertetett eljárási paramétereket. A kinyert digitális bizonyíték erősségét, azaz a fizikai valósághoz közeli voltát a kinyerési szinteknek megfelelő skála jelezhetné.

Ebben az értelemben a fizikai hálózatból és annak hardver elemiből közvetlenül kinyert bizonyítékok lesznek a legerősebben – önálló számítógép, számítógépes hálózat, mobil eszköz és felhőszolgáltatás esetében egyaránt – a magasabb szinteken (a hardvertől távolabb) a bizonyíték erőssége csökkenne, tekintettel arra a körülményre, hogy a kinyeréskor a szakértő nem gyakorolt teljes felügyeletet a vizsgált rendszer körülményei felett. A megoldás előnye tovább az is, hogy a nem felhő alapú rendszerek (pl. önálló számítógép) vizsgálatakor felmerülő kényszermegoldások (pl. a rendszer bekapcsolása utáni vizsgálat) is kezelhetővé válik, az így kinyert bizonyítékot nem kell elutasítani a kinyerési környezetben beállt változás miatt, hanem e körülmény jelezhetővé válik a bizonyíték erősségének paraméterével.

E koncepció részletes kidolgozására (különös tekintettel a minőségi paraméter elnevezésére) csak megfelelő szakmai vitát követően kerülhet sor, melyben a szakértők álláspontja mellett az adatokat, bizonyítékokat felhasználók véleménye is teret kap.

Összefoglalás

A felhőszolgáltatások felhasználásával, az ellen, vagy annak érintettségével elkövetett bűncselekmények igazságügyi informatikai szakértői vizsgálata és a szakértői bizonyítás módszertana és eszközrendszere kialakulófélben van. A létrejövő rendszer alapját computer forensic és a network forensic eljárások és a velük kapcsolatban kialakított nemzetközi szabványok (ISO 27000 szabványkör) képezik.

Az adatok kinyerésének és hitelességük ellenőrzésének módszerei a szakterületre vonatkozó jelenlegi kutatások fókuszában állnak. A gyakorlati szakértői munkában történő alkalmazhatóságuk, illetve az ezzel kapcsolatos eljárások, módszertanok még nem véglegesek, egyes esetekben még nem alakultak ki. A digitális bizonyítékok felhőszolgáltatásból történő kinyerésére jelenleg a nemzetközi bűnügyi együttműködésen alapuló, a felhőszolgáltatók együttműködését is igénybevevő út látszik járhatónak.

A módszertani és eljárási körülmények alakulásakor nem szabad figyelmen kívül hagyni azt a fogalomkört, mely leírja, definiálja a büntetőeljárásban felhasználható, hiteles adatok jellemzőit. Ezek a jellemzők egyre messzebb kerülnek a tárgyi bizonyítási eszköz fogalmától, de a magyarországi gyakorlatban még gyökeret sem vert digitális bizonyíték definíciójától is távolodni látszik. Tudomásul kell venni, hogy a technológiai változások erős nyomást gyakorolnak a jogtudomány alapvetően konzervatív természetére, mintegy kikényszerítve az új fogalmak és definíciók bevezetését. Ebben természetesen nem hagyhatók magukra a jogászok, hanem valamennyi a terület közelebbi, vagy távolabbi perifériáján (ha jobban tetszik határterületén) mozgó szereplőnek – így az igazságügyi informatikai szakértőknek is – ki kell venniük a részüket. Különösen akkor, ha a megújítani kívánt területen több ismerettel, készséggel és képességgel rendelkeznek, mint a többi résztvevő.

Végső soron ismét megfogalmazható az a tétel, mely szerint a büntetőeljárás valamennyi szereplőjének érdeke és egyben feladata is a dinamikusan változó részterületek kihívásaira adandó válaszok megfogalmazásban való együttműködés és részével. Minden érintett megtalálhatja az általa preferált részterületet, hiszen akár a szervezeti, akár a gyakorlati, akár a tudományos megközelítés számára is akad feladat.

10 A Digital Forensic és a társadalomtudományok kapcsolata[180]

Az új típusú médiahasználat, a mindennapi élet interakciós helyzetinek átalakulása nem csupán azokat a területeket érintik, melyekről szívesen beszélünk (új típusú közösségi formák, generációs, nemi vagy kulturális különbségek a médiahasználatban), de a normasértés vagy a bűn fogalmával is kapcsolatba hozható. A „Z" generáció médiahasználatának – az azonnali üzenetküldő programokkal történő csevegésnek – e sajátos szempontból történő vizsgálata nem csak a bűnügyi vonatkozásokra ad választ, hanem megvilágítja a korosztály kommunikációs szokásait is.

10.1 Társadalomtudományi módszerek alkalmazása

A kommunikációs tartalom elemzésének módszerei – legyenek azok kvantitatív, vagy kvalitatív eljárások – számos tudományág eszköztárában megtalálták a helyüket. A jelentős kutatási potenciált mutató területek (pl. marketing kutatás, fogyasztási szokások kutatása) mellett olyan tudományterületek is léteznek, ahol kutatási kezdeményezések alig figyelhetők meg, noha a gyakorlat oldaláról erős igény mutatkozik rá. Ilyen tudományterület a Digital Forensic Science szövegkorpuszok elemzésével foglalkozó szakterülete, melynek körvonalai még csak formálódó félben vannak.

A Digital Forensic Science azokat a tudományos módszereket és eljárásokat foglalja magába, melyek a jogi eljárásokat látják el hiteles információval azon esetekben, ahol digitális adat és/vagy – a kifejezés tágabb értelmében vett – a számítógép rendszer is az ügy részét képezi[181]. Ilyen digitális adat lehet többek között az azonnali üzenetküldő programokkal (instant messenger, pl. Skype, ICQ, korábban az MSN stb.) folytatott beszélgetések során létrejött szövegtest. Ezek vizsgálata jellemzően a büntetőeljárás nyomozási szakaszában történik abból a célból, hogy megerősítse vagy cáfolja a vizsgálat alá vont személy kapcsolatát a nyomozás tárgyával. A vizsgálat adatkinyerési és adatelőkészítési (elő-feldolgozás) részét az igazságügyi informatikai szakértő végzi, aki a bűnügyi vonatkozások mellett számos egyéb megfigyelést is tehet.

A megfigyelt jelenségek részletes, társadalomtudományi eszközökkel végzett vizsgálata az érintett személyek és/vagy csoportok etnográfiai irányú megközelítése által olyan információkat is felszínre hozhatnak, melyek visszahatva az eredeti célra (bűnfelderítés) új eszközöket adhatnak a nyomozók és a terület iránt érdeklődő kutatók kezébe.

[180] A fejezetben a kutatás időszakában hatályos jogszabályokra történik hivatkozás

[181] MÁTÉ István Zsolt: Digital Forensic Science – szabványosítási törekvések „régen" és ma. in ISZAK 2013 Konferencia Kötet CD-ROM, Budapest, Budapesti Igazságügyi Szakértői Kamra, 2013. 1.p. ISBN: 978-963-08-7882-1.

10.2 A szakértői archívum adatainak tudományos célú felhasználhatósága

Az igazságügyi informatikai szakértői vizsgálat során végzett adatmentés, adatelemzés eredménye a digitális bizonyíték, melynek elsődleges felhasználása büntetőeljárás nyomozási szakaszában történik. A kinyert és a nyomozó hatóságnak átadott digitális tartalmak ezt követően nyomozati iratokhoz csatolva kerülnek a büntetőeljárás következő állomásaihoz. Az igazságügyi informatikai szakértőnél megtalálható eredeti mentésről közvetlenül nem rendelkezik jogszabály. A hazai szakértői gyakorlatban két eljárásmód honosodott meg: egyrészt a munka végeztével a szakértő minden hozzá került digitális tartalmat véglegesen töröl a számítógépéről és egyéb adathordozóiról, egyedül a szakértői vélemény dokumentum állományát tartja meg archívumában a vizsgálattal összefüggésben. A másik megközelítésben (jelen sorok szerzője ezt támogatja) a szakértő a mentett digitális bizonyítékokat a szakértői archívumában megőrzi[182].

Amennyiben a szakértő az archívumban történő tárolás mellett dönt, úgy felmerül a tárolt információk további felhasználhatóságának kérdése. Erre a választ a az igazságügyi szakértői tevékenységről szóló 2005. évi XLVII. törvényben (Szaktv.[2005]) találjuk meg, melyben a 12. § (3) szerint: „Ha jogszabály másként nem rendelkezik, az (1) bekezdésben foglaltak nem zárják ki a szakértői vizsgálat során feltárt tényeknek és adatoknak tudományos vagy oktatási célra - személyazonosításra alkalmatlan módon - történő felhasználását.”. Ez a felhatalmazás teszi lehetővé, hogy az igazságügyi informatikai szakértői vizsgálatok eredményét, a kinyert tartalmakat az eredeti céltól akár eltérő irányba végzett tudományos kutatás forrásaként felhasználhassuk.

10.3 Kulturális jelenségek azonosítása

A rendelkezésre álló, s immár jogszerűen fel is használható forrásadatok „újrahasznosításának” irányát részben meghatározzák azok a körülmények, melyek létrejöttükért felelősek. Ez nem más, mint a számítógép által közvetített információcsere (computer mediated communication) jelensége, mely kezdetben főként a technológiailag fejlett országokban (1970-es évektől), majd a 21. századra csaknem az egész világon elterjedté vált.[183] Az elterjedtségből eredő mindennapos használat majd az egymáshoz kapcsolódás (vö. internet) lehetősége létrehozta a „globális falut”[184], melyben viselkedési formák, törzsé és helyi népszokások alakultak ki, s egyben váltak vizsgálhatóvá a kom-

[182] MÁTÉ István Zsolt: A digitális bizonyíték. in Jogász Doktoranduszok V. Országos Szakmai Találkozója konferenciakötet, Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2014.

[183] SPEARS et al.: Social psychological theories of computer-mediated communication: Social pain or social gain? in The Handbook of Language and Social Psychology. Oxford, Wiley, 1990.

[184] MCLUHAN, E. – ZINGRONE F (eds.): Essential McLuhan. London, Routledge, 1997. ISBN 0-203-99296-2.

munikáció kutatók számára. A számítógépes térben történő jelenlét lenyomata, s a belőle levonható következtetések és megtehető előrejelzések nem csak a társadalomkutatók, de a kriminalisztika művelői számára is új utakat, kutatási mezőket nyitnak meg.

Az új kutatási területek egyik kiemelt területe az online kommunikáció tartalmi vizsgálata. Ezt a telekommunikáció részbeni komputerizálódása teszi vizsgálhatóvá oly módon, hogy a létrejövő szövegkorpuszok (azonnali üzenetküldő programokkal folytatott szöveges beszélgetések) tárolódnak a számítógépeken, melyek részben egyszerű adatkinyerési, részben forenzikus módszerekkel vizsgálhatóvá tehetők. Az igazságügyi informatikai szakértők munkájuk során rutin szerűen tárják fel a gyanúsítottak által folytatott elektronikus kommunikáció (elektronikus levelezés, instant messenger programok használata, közösségi oldalakon történő kapcsolattartás, SMS üzenetek stb.) különféle formáit és teszik hozzáférhetővé, elemezhetővé a nyomozóhatóság illetékes munkatársai számára.

A szakértő munkáját a legtöbb esetben megkönnyíti az a körülmény, hogy a kommunikáció szereplői természetes módon használják a kapcsolattartás különféle formáit, s nem alkalmaznak titkosítást, vagy egyéb fedő tevékenységet. Az esetek egy részben maga a felhasználó menti a kommunikációs tartalmakat (naplózott beszélgetések), utalva azok időrendjére is, így a szakértőnek „csupán" a szövegkódolási összhangot kell megteremtenie a kinyert szövegkorpuszok között, melyek kis részben képi információt is tartalmazhatnak (emotikonok stb.), s melyek az ügyek jellegétől függően alkalmasak lehetnek további kutatásra, a mögöttes társadalmi jelenségek, vagy viselkedési módok feltárására.

10.4 A tiltott pornográf felvétellel visszaélés és a sexting jelenség

A következőkben egy tiltott pornográf felvétellel visszaélés gyanúja miatt ismeretlen tettes ellen indított nyomozással összefüggésben készített igazságügyi informatikai szakértői vélemény mentett kommunikációs tartalmainak társadalomtudományi módszerekkel történő újra elemzését mutatom be, mint a kriminalisztikai tartalmak „újra hasznosításának" egyik lehetőségét.

Estelírás

A ××× Rendőrkapitányság „a Btk. 204. § (2) bekezdésébe ütköző és aszerint minősülő tiltott pornográf felvétellel visszaélés bűntett gyanúja miatt ismeretlen tettes ellen folyamatban lévő büntetőügyben a Be. 99. § (3) bekezdése es a 100. § (1) bekezdés első mondata alapján - figyelemmel a Be. 99. § (1) bekezdés és a 102. § (1) (2) bekezdésre" (44/2011) szakértőként rendelt ki. Az ügy nyomozása során további szakértői vizsgálatokra is sor került (45/2011, 46/2011, 53/2011 és 54/2011 szakértői ügyszámon).

Az ügyben sértettként szereplő fiatalkorú személy mobiltelefonnal két fényképet készített saját magáról, melyet barátja részére elküldött. Kapcsolatuk megszakadását követően a fényképek kikerültek egy weboldalra, majd a weboldal elérhetősége elsőként az iskolai közösség tagjai számára vált hozzáférhetővé, majd ezt követően a sértett édesanyja számára is. Ez utóbbi mozzanat hatására történt meg a fejjelentés, mely alapján elindult a nyomozás. A nyomozás során lefoglalásra került az iskolai közösség több tagjának számítógépe és mobiltelefonja, s a szakértő vizsgálat során egy számítógépen előtalálásra kerültek a keresett fényképfelvételek. A képek feltöltésére vonatkozóan digitális bizonyíték került elő, így az ügyészség a tiltott pornográf felvétel tartásával elkövetett cselekmény miatt emelt vádat az iskolai közösség egyik tagja ellen. A bírói szakaszban (2014) sor került a szakértő tárgyaláson történő meghallgatására is, ahol a szakértő a feltárt tények mellett az ügy mögötti kulturális jelenséget is bemutatta.

Jogszabályi háttér

Az 1978. évi IV. törvény (régi Btk.) 204. § (1) tartalmazza a tiltott pornográf felvétellel visszaélés tényállásának leírását a következőképpen: „Aki tizennyolcadik életévét be nem töltött személyről vagy személyekről pornográf felvételt megszerez, tart, bűntettet követ el". A (7)-ből megismerhetjük a felvétel és a pornográf felvétel definícióját is:

> *„E § alkalmazásában*
>
> *a) felvétel: a videó-, film-, vagy fényképfelvétel, illetőleg más módon előállított képfelvétel,*
> *b) pornográf felvétel: az olyan felvétel, amely a nemiséget súlyosan szeméremsértő nyíltsággal, célzatosan a nemi vágy felkeltésére irányuló módon ábrázolja," [régi Btk. 204. § (7)]*

A kutatás módszere

A kutatás módszereként a megfigyelés bizonyult használhatónak. Ez részben abból következik, hogy a szakértő – aki a kutatás alapanyagát kinyeri, szolgáltatja – a büntetőeljárás során szinte soha nem kerül közvetlen kapcsolatba sem a sértettel, sem a gyanúsítottal, sem a tanúkkal. Munkája során a vizsgálatra megkapott eszközökön fellelhető digitális nyomokat kell rögzítenie és a nyomozó hatóság számára értékelhető formában átadnia.

A módszert a következő alapvető tulajdonságok jellemzik az elsődleges vizsgálat során:

- nincs kapcsolat az elemzendő tartalom forrásával,
- a vizsgálat fókusza a szakértőtől független,
- a vizsgálat közvetett, hátrahagyott nyomok alapján történik.

A másodlagos vizsgálat jellemzői:

- nincs kapcsolat az elemzendő tartalom forrásával,
- a vizsgálat fókuszát a kutató határozza meg,
- a vizsgálat közvetett, hátrahagyott nyomok alapján történik.

A kutatás során alkalmazható megközelítési módokat a vizsgálat irányultsága határozza meg legerősebben, de nem kizárt az átjárás az egyes megközelítési módok között. Az esettanulmánnyal összefüggő kutatás során kriminalisztikai és társadalomtudományi megközelítésekkel történt a vizsgálat:

Kriminalisztikai nézőpont

A kriminalisztikai megközelítés célorientáltan a büntetőeljárásban történő felhasználhatóságra koncentrál. Alapvető mozzanatai[185] is erre utalnak:

- Identification – azonosítás
- Preservation – megóvás
- Collection – összegyűjtés
- Examination – vizsgálat
- Analysis – elemzés
- Presentation – bemutatás
- Decision – döntés

Az ügyek elsődleges vizsgálatánál jól használható módszertan „hiányossága" a mögöttes jelenségek iránti érzéketlenség. A módszer alkalmas a másodlagos vizsgálatok alapanyagának elfogultságtól mentes előkészítésére.

[185] PALMER, Gary et al.: A Road Map for Digital Forensic Research. First Digital Forensic Research Workshop. Utica, NY, USA, 2001.

Forenzikus nyelvészeti megközelítés

„A kriminalisztikai nyelvészet feladata a bűncselekmények nyelvi bizonyítékainak az elemzése. A legfontosabb kérdés, amelyre a hatóság a választ keresi, a ki tette – jelen esetben írta a szöveget?”[186]. Ez a megközelítési mód szintén az elsődleges vizsgálat során alkalmazható, illetve ismeretlen szerző esetén (pl. beazonosítatlan beszélgető-partner) alkalmas lehet a beszélgetésben résztvevők tulajdonságainak (pl. életkor, nem, iskolázottság, szakma stb.) behatárolásához. A forenzikus nyelvészet a következő módszereket alkalmazza:

- Nyelvi bizonyítékok: okiratok, szakértői vélemények[187],
- Nyelvészeti megközelítés (nyelvészeti szakkérdések)
  - ~ Formai jegyek vizsgálata,
  - ~ Szókészlet vizsgálata,
  - ~ Nyelvtani jegyek vizsgálata.

Tartalomelemzés

A tartalomelemzés a szövegkorpuszok vizsgálata, mely a szöveg mögöttes – nyíltan ki nem fejtett – mondanivalóját tárja fel kvantitatív és kvalitatív módszerek alkalmazásával. A módszer, melynek a hét fő komponensét az alábbiakban olvashatjuk[188] alkalmas a másodlagos vizsgálatok céljaira:

- Adatkészítés
- Egység meghatározás
- Mintavétel
- Adatrögzítés
- Adatredukció
- Következtetés
- Elemzés

[186] HUGYECZ Enikő Henriett: Ki a szerző? – Avagy hogyan profiloznak a laikusok? in E-nyelv Magazin 2011/03. Budapest, Inter Nonprofit Kft. 2011. online: http://e-nyelvmagazin.hu/2011/08/31/ki-a-szerzo-%e2%80%93-avagy-hogyan-profiloznak-a-laikusok/, hozzáférés: 2013.09.18.

[187] TREMMEL Flórián – FENYVESI Csaba: Kriminalisztika. Tankönyv és atlasz. Budapest-Pécs, Dialóg Campus Kiadó, 1998.

[188] KRIPPENDORFF, Klaus: A tartalomelemzés módszertanának alapjai. Balassi Kiadó, Budapest, 1995. p.57.

Kulturális antropológia és Netnográfia

Az etnográfiai leírás, más néven kulturális antropológia hasonlóságot mutat a tartalomelemzéssel, de vizsgálati területe jóval tágabb, nem korlátozódik a szövegekre, hanem kiterjed a társadalmi beszédfolyamatokra is, s megpróbálja azok jelentését kinyerni és rögzíteni[189].

A számítógépek által közvetített kommunikáció megjelenését követően jelent meg a kulturális antropológia alkalmazott altudományaként is értelmezhető netnográfia, mely elsősorban a vásárlói viselkedés vizsgálatára koncentrál, de fő felhasználási módjai alapján (lásd az alábbi felsorolásban) a másodlagos vizsgálatoknál jól hasznosíthatók:

- a „tiszta" kiberkultúrák és virtuális közösségek tanulmányozásának módszertanaként,
- a „származtatott" kiberkultúrák és vituális közösségek tanulmányázásának módszertanaként, valamint
- feltáró eszközként általános témák tanulmányozására.[190]

Kutatási adatok

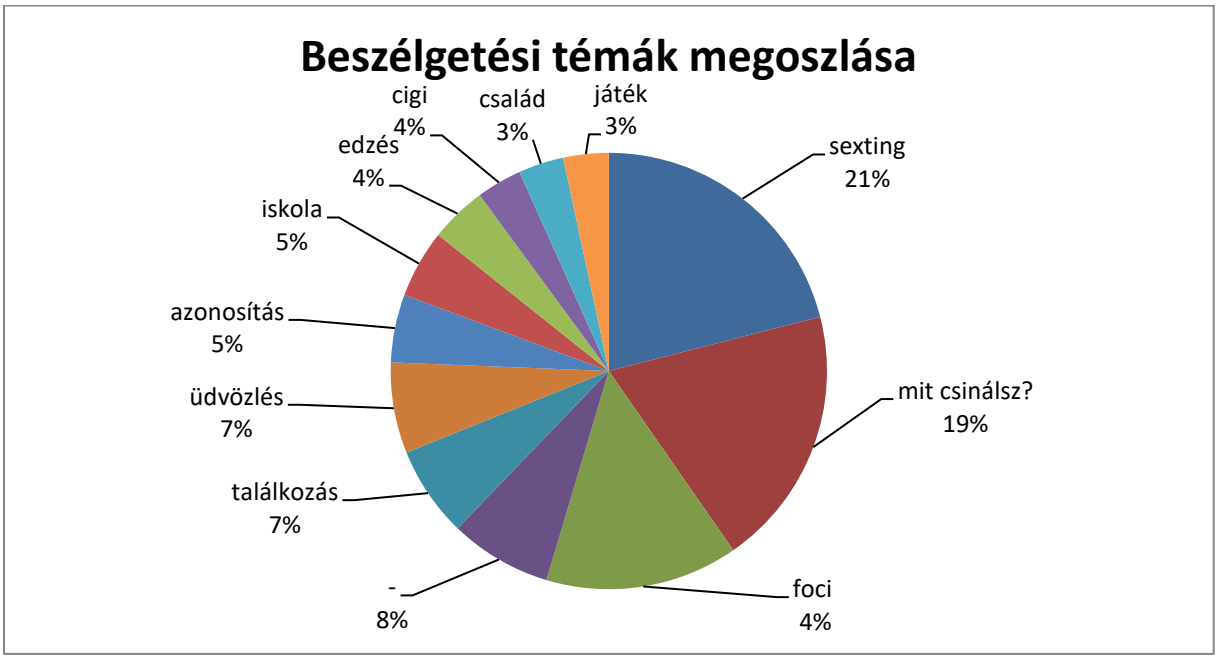
A részletes vizsgálat során a kinyert azonnali üzenetküldő programmal (MSN) folytatott beszélgetések közül egy 15 napos periódus szöveges kommunikációját vizsgáltam abból a célból, hogy a kommunikációban felfedezhető-e az elsődleges vizsgálatban érintett cselekménnyel (tiltott pornográf felvétellel visszaélés) kapcsolatos magatartás.

Az adatok feldolgozása során 150 üzenetcsoportot (beszélgetést) találtam, mely összesen 3 890 üzenetből állt, melynek 57%-át fiúk, 43%-át lányok küldték. A kommunikációban 56 szereplő volt azonosítható (37% fiú, 63% lány), a résztvevők 95%-a 18 éven aluliként volt azonosítható. Az összes beszélgetési idő 33 óra 6 percet tett ki és 31 beszélgetési témát foglalt magába.

[189] GEERTZ, Clifford: Az értelmezés hatalma. Budapest, Századvég Kiadó, 1994. 188.p.

[190] KOZINETS, Robert V.: On Netnography: Initial Reflections on Consumer Research Investigations of Cyberculture. in NA - Advances in Consumer Research Volume 25, eds. Joseph W. Alba & J. Wesley Hutchinson, Provo, UT : Association for Consumer Research, 1998. pp.366-371.

Az első 12 téma 4 alkalommal vagy annál többször került elő, megoszlásukat a következő diagram mutatja:



5. diagram - Beszélgetési témák megoszlása

Amint az megfigyelhető a legnagyobb számban a sexting témájú beszélgetések fordultak elő a kommunikációban, mely a kutatói kérdéssel kapcsolatban szoros összefüggést jelez.

A sexting jelenség

A beszélgetések témaköri besorolásánál (osztályozásánál) merült fel a szexuális tartalommal rendelkező szövegek csoportjának megnevezése. Mivel az azonnal üzenetküldő programok (korábban MSN, Skype, ICQ stb.) rendelkeznek kép és video küldési funkcionalitással, s a besorolandó beszélgetések rendszerint tartalmaztak képi üzeneteket is, a szakirodalmi egyezések alapján a sexting megnevezést alkalmaztam.

A sextingen első megközelítésben a Z generációhoz tartozó fiatalok körében telekommunikációs, vagy számítógéppel közvetített kommunikációban zajló szexuális tartalmú kép és/vagy szöveges tartalmak küldését, cseréjét értjük. A definíció kérdése az USA-ban is megfogalmazódott, amikor elsősorban a médiában a következőkben felsorolt viselkedési formákra kezdték alkalmazni a kifejezést (2009-2010):

a) egy kiskorú személy fényképet küld egy másik, általa ismert személynek
b) egy kiskorú olyan fényképet készít és / vagy terjeszt saját magáról, melyen szexuális tevékenységet folytat;
c) egy kiskorú személy tudatosan továbbítja egy másik fiatal meztelen testéről készített fényképet, annak tudta nélkül;
d) egy kiskorú személy ilyen fényképeket helyez el egy weboldalon;

e) egy tizenéves kér, vagy kényszerít egy másik fiatalt ilyen képek átadására;
f) egy osztálytárs rávesz és/vagy zsarol egy másik fiatalt fényképek küldésével kapcsolatosan;
g) egy felnőtt korú személy fényképet vagy videót küld egy kiskorú személynek, vagy fiatalokról készített kifejezetten szexuális tartalmú képeket küld, illetve
h) egy felnőtt küld szexuális tartalmú szövegeket vagy képeket egy másik felnőttnek.[191]

A kifejezetten nem jogi terminusként, hanem média-közszóként használt meghatározások jelentős egyezést mutatnak az esettanulmányban szereplő ügy elsődleges vizsgálati céljában meghatározott tiltott pornográf felvétellel visszaélés bűntettével. Ugyanez a kérdés merül fel LEARY idevágó tanulmányának címében is: Sexting vagy saját készítésű gyermekpornográfia:

A válasz megadása előtt vessünk egy pillantást a tengeren túli statisztikai adatokra két, egymástól független tanulmány alapján. A National Campaign felmérésben részt vett tizenévesek 20%-a küldött már magáról meztelen, vagy félig meztelen képeket online, a Cox felmérése válaszadóinak 19%-a küldött, kapott, vagy továbbított már szexuális utalású meztelen, vagy majdnem meztelen képet MMS, vagy e-mail útján.

Emlékeztetőül: bár az esettanulmányban vizsgált magyarországi mintában a beszélgetések 17%-a volt sexting tartalmú, ugyan akkor a felmérés kis mintán történt kevés résztvevővel, ezért a nagy mértékű egyezés ellenére sem vonhatunk le egyértelmű következtetéseket ezen adatokból. Az mindenesetre kijelenthető, hogy a USA-ban észlelt tendenciák megjelentek a magyarországi azonos életkori csoportokban is. Mivel a 2012. évi C. törvény (új Btk.) 204. § továbbra is büntetni rendeli az immár gyermekpornográfia megnevezéssel azonosított magatartást, azokat a jelenségeket, melyek a bűncselekmény elkövetéséhez vezethetnek kutatni szükséges és a kutatási eredményeket a bűnmegelőzési gyakorlatban hasznosítani kell.

A kutatási eredmények hasznosítása

A kutatás során feltárt tartalmak vizsgálatából egyértelműen kiderült, hogy az elsődleges vizsgálat célcselekményét (tiltott pornográf felvétellel visszaélés) megelőzte egy olyan kommunikációs és egyben eszközhasználati (telefon és instant messenger programok) gyakorlat, mely önmagában is jogszabályellenes volt (a régi Btk. is tiltotta az érintett típusú képek tartását). A szöveges tartalom elemzéséből az is nyilvánvaló, hogy a kommunikáció résztvevői ebben az időszakban nem voltak tudatában a cselekmény törvénybeütköző jellegének és mindennapi gyakorlatként éltek a sextinggel.

[191] LEARY, Mary G.: Sexting or Self-Produced Child Pornography? The Dialogue Continues – Structured Prosecutorial Discretion within a Multidisciplinary Response. in Virginia Journal of Social Policy and the Law. Vol. 17, No. 3, Spring 2010 Charlottesville, VA, USA, 2010. online: http://ssrn.com/abstract= 1657007, hozzáférés: 2013.10.26. p.500.

Bár jelen sorok szerzőjének nem célja és feladat sem a jogszabályok tartalmi vizsgálata és még kevésbé bírálata, az mindenképpen kijelenthető a vizsgálat eredményei alapján, hogy a régi Btk.-ban tiltott pornográf felvétellel visszaélés, az új Btk.-ban gyermekpornográfiaként szereplő cselekményt általában nem lehet azonosnak tekinteni a sexting jelenséggel. Az is megfogalmazható, hogy a sexting következménye lehet olyan cselekmény, melyet büntetőjogilag kell értékelni, s ennek részbeni okaként a sextinggel kapcsolatos hiányos ismeret is azonosítható.

A tizennyolcadik életévüket még be nem töltött fiatalok csoportja fogékony az új kommunikációs technológiák iránt, s szüleik generációjánál általában jobb szinten, készségszerűen kezelik azokat. Ugyanakkor a technológiahasználathoz nem társul a használat következményeivel kapcsolatos ismeretanyag, melynek pótlása szükséges az esettanulmányban vizsgált következmények elkerülése érdekében.

Az információ átadás módjai között szerepet kell kapnia valóságos eseményeken alapuló, hiteles személyek által bemutatott ügyeknek, melyek a kulturális jelenségek mögött rejlő veszélyeket és következményeket is megvilágítják. Ilyen megoldás lehet a sextinggel kapcsolatos ismeretek beépítése rendőrség által évek óta sikeresen alkalmazott DADA programba, vagy a témával foglalkozó, a korosztály kommunikációs igényeihez alkalmazkodó tartalmak kifejlesztése (vírusvideo, közösségi kommunikáció stb.).

A további kutatásokat lehetővé tevő tartalom újrahasznosítás területén az igazságügyi informatikai szakértői vizsgálatok eredményének, a digitális bizonyítékoknak központi, anonimizálható tárolása és annak kutatók általi feldolgozhatósága teremthetne megfelelő bázist. E lehetőség vizsgálatára egy önálló tanulmányban kerülhet sor.

11 A kutatás eredményei és azok felhasználása, az értekezés összefoglalása

Az igazságügyi informatikai szakértői tevékenység – tekintettel az informatika beágyazódására a mindennapi tevékenységekbe – egyre nagyobb jelentőségre tesz szert a büntetőeljárások területén. A korábbi időszak elszigetelt szakterületei egyre gyakrabban mutatnak átfedéseket, a határok nem ritkán összemosónak. A jelenben és még inkább a közeljövőben nélkülözhetetlenné válnak az igazságügyi informatikai szakértők csaknem valamennyi igazságügyi szakértői szakterület esetében a büntetőeljárásban.

Ennek a kihívásnak csak akkor képesek a szakterület képviselői megfelelni, ha munkájuk, hivatásuk megfelelő tudományos megalapozottsággal bír. Az alapvetésekhez tartozik az aktuális jogszabályi környezet ismerete, a nemzetközileg is elfogadott módszereken és eljárások használata, a szakterület nemzetközi és hazai szabványainak ismerete, a módszerek és eljárások megvalósításához szükséges, validált szoftver és hardver komponensek használata.

Jelen értekezés a felsorolt alapvető feltételek mindegyikére kitér, a szerző által meghatározott hangsúlyokkal, mely az adott tárgyart tématerületről szóló rész terjedelmében és részletességében mutatkozik meg.

Így az aktuális – de egyben változó – jogszabályi környezetről csupán pillanatképet mutat a tanulmány, helyet adva a közeljövőben véglegesítésre kerülő jogszabályok (pl. az új büntetőeljárásról szóló törvény) későbbi beemeléséhez, egyben rövid történeti és nemzetközi kitekintést is adva.

Az értekezés fókuszpontjában az igazságügyi informatikai szakértők szakmai munkája és annak tudományos megalapozása áll – ez egyben az írás legnagyobb terjedelmű önálló része. Itt kerülnek tárgyalásra a szakterület eredettörténeti és tudománytörténeti aspektusai, valamint a kriminalisztikán belül, illetve más, nagyobb tudományterületek interdiszciplináris terében történő pozicionálás is itt történik meg.

A szakterületen belüli tagozódás valós helyzetének feltárása empirikus kutatás segítségével valósult meg. Ennek forrásai a szerző, négyszáznál több saját ügyet tartalmazó szakértői ügynyilvántartása, melyet a jogszabályi kötelezettségen felüli, a kutatás szempontjait szolgáló adatokkal egészített ki és tett részletes elemzésre alkalmassá.

Bár a kutatás a fentiekben írt jellemzők miatt nem tekinthető reprezentatívnak, mégis alapul szolgál a szakterületen belüli hangsúlyok meghatározásához, mely segíti a módszertani rész fókuszpontjának megtalálását.

A kutatás közvetlen eredményeként az igazságügyi informatikai szakértői munka egyfajta térképe jön létre, mely az ügytípusok és vizsgálati területek mennyiségi és minőségi jellemzőit mutatja be. A kutatás időbeli vetülete az egyes cselekménytípusok változását, új elkövetési módok és területek megjelenését teszi kézzelfoghatóvá, s egyben előrejelzésként is szolgálhat a közeljövő tendenciáinak vonatkozásában.

Hasonlóan közvetlen kézzelfogható eredményként említhető az ügytípusokra és vizsgálati területekre vonatkozó minimális szakmai követelmények definiálása, honosítása és a kapcsoló „jó gyakorlatok" esettanulmányként történő bemutatása.

A közvetett eredményként tekinthető a digitális bizonyíték fogalmának, felhasználhatóságának, vizsgálati körülményeinek és eljárásainak bemutatása, értékelése kritikája és a szakértői gyakorlat tükrében.

Amint az az előzőekből következik, a szakmai rész kiemelten fontos momentuma a szakértői módszertanok és az azt megalapozó nemzetközi szabványok tárgyalása. A bevezető történeti áttekintés nem csupán tudománytörténeti jelentőségű, hanem a szakterületen mutatkozó fejlődés kezdőpontját és annak dinamikáját is mutatja. Ez által példaként is szolgál a magyarországi bevezetés szempontjából: tervezhetővé teszi az átmeneti, bevezető időszakot, ami az érdekeltek felkészülését, az ehhez szükséges tanítási és tanulási folyamatokat támogatja.

A módszertanok és eljárások önmagukban mit sem érnek. Szembesítésük a hazai gyakorlattal nem csupán azt a célt szolgálja, hogy a hibákat, hiányosságokat feltárja, hanem egyben egy helyzetképet is nyújt az értő olvasónak, akár a jogszabály előkészítés, vagy a gyakorlati alkalmazás oldaláról szemléi is a képet. Számukra fontos egy teljesebb, szélesebb horizont szemlélése, mely nem csupán a saját részterületük szűk fókuszában mutat éles, kontúros körvonalakat.

Ezt a képet a szerző esettanulmányszerű feldolgozási móddal közelíti meg, bepillantást engedve a 21. század várhatóan vezető bizonyítási eszközének a digitális bizonyíték (vö. elektronikus adat az új. Be. tervezetében) és annak beszerzése folyamatának, bemutatva a gyakori és különleges szakértői vizsgálati típusokat.

Az áttekintés semmiképpen nem a kézikönyv-szerű felhasználás irányába történő elmozdulást jelenti a tanulmány szempontjából, inkább egy eltérő nézőpont bemutatását, mely lehetővé teszi a tudományos megalapozottság életképességének vizsgálatát.

Elsősorban terjedelmi okokból csak ízelítő kerülhetett a szövegbe mindkét – gyakori és különleges – vizsgálat típusból, helyet hagyva egy későbbi kutatásnak is, mely a kevésbé frekventált részterületek feldolgozására fókuszálhat.

Végül, de nem mellékes szempontként – mintegy teret adva a kriminológiai aspektusnak is – az igazságügyi informatikai szakértői munka során megjelenő társadalomtudományi nézőpont is helyet kapott az értekezésben. Kevés olyan kutatás folyik, mely képes a jog – informatikai – társadalomtudomány terében érvényes adatokat szerezni,

s ezekből megállapításokat tenni. Az írás az erre alkalmas forrásadatok felhasználásával kísérletet tesz az új megközelítés alkalmazására és az abból kinyerhető releváns következtetések levonására.

Összefoglalva elmondható, hogy az értekezés – a szerző szándékával egyezően – kiinduló pontja és egyben szilárd alapja kíván lenni a szakterület kutatásának, mely a hivatásrenden belüli és a jogi, társadalmi környezetből származó külső kényszereknek is megfelelve – de nem korlátozva azok által – kijelöli a szakterület jövőbeli művelői előtt az utat.

A kijelölt úton azonban nem egy kutatónak kell végig mennie, hanem az igazságügyi informatikai szakértői közösség – melynek egyik letéteményese a magyar Igazságügyi Szakértői Kamara Informatikai és Hírközlési Szakmai Tagozata – valamennyi aktív tagjának, nem feledkezve meg az utánpótlásként szerepet kapó szakértőjelöltekről, valamint a jog, az informatika és a társadalomtudományok területein tanuló, vagy a területeken végzett hallgatókról sem.

12 Abstract

With consideration to how information technology has become embedded in our everyday lives, the activities of computer forensic specialists are becoming increasingly important in the field of criminal proceedings. The isolated specialist fields of previous times are becoming increasingly overlapped and the borders between them are often blurred. Currently, and even more so in the near future, computer forensic specialists are becoming essential in criminal proceedings in almost all forensic specialist fields.

Those operating in the specialist field are only able to meet this challenge if their work, their profession has an appropriate scientific background. This basically includes knowledge of the prevailing legislative environment, use of internationally recognised methods and procedures, knowledge of the field's international and domestic standards, and the use of the validated software and hardware components required for the implementation of the methods and procedures.

The present study deals with each of the basic conditions listed, with the emphases determined by the author, which is manifested in the length and degree of detail of the section on the topic under discussion.

Therefore, the essay presents merely a momentary picture of the current, yet changing, legislative environment, leaving space for the later insertion of the legislation to be finalised in the near future (e.g. the new act on criminal procedures), also providing a short historical and international outlook.

The focus of this work is the specialist work of the computer forensic specialist and its scientific basis, which is also the most extensive independent part of the essay. It is here that the origins of the specialist field and the history of its science are discussed, as is its position within forensics and within the interdisciplinary field of other, larger areas of science.

An investigation into the actual structure of the specialist field was performed via empirical research. The sources for this were the author's own records of some three hundred cases, which, in addition to the legal requirements, have been supplemented with data assisting the purpose of the research and made suitable for detailed analysis.

Although due to the features described above the research cannot be deemed to be representative, it still serves to identify the emphasis within the field, which helps to reveal the focus of the section on methodology.

13 Irodalomjegyzék

Az alábbiakban szereplő szakirodalmi hivatkozások elsősorban angolszász könyveket és szakcikkeket tartalmaznak, melyeket néhány angol nyelvű de ázsiai tartalom színesít. A magyar nyelvű szakirodalom elsősorban a kriminalisztika tárgyköréből származik, ami jelzi, hogy a bűnügyi informatika részletes monografikus feldolgozása még várat magára.

13.1 Felhasznált irodalom

BODÓ Balázs: Szükség törvényt bont. ELTE, 2010. Online: http://doktori.btk.elte.hu/phil/bodobalazs/ disszertacio.pdf [Hozzáférés: 2013.01.10.]

BRINSON, Ashley –ROBINSON, Abigail – ROGERS, Marcus: A cyber forensics ontology: Creating a new approach to studying cyber forensics. in digital investigation 3S (2006) S37 – S43, Amsterdam, 2006. online: http://www.dfrws.org/2006/proceedings/5-Brinson.pdf

CASEY, Ehogan: Digital Evidence and Computer Crime. Elsevier. Amsterdam, 2011.

CIARDHUÁIN, Séamus Ó.: An Extended Model of Cybercrime Investigations. in International Journal of Digital Evidence. Summer 2004, Volume 3, Issue 1, online, 2004. ijde.org online: www.ijde.org, hozzáférés: 2013.03.16

CISCO: Cisco Connected World Technology Report. http://www.cisco.com/en/US/netsol/ns1120/index.html [2014.01.11.]

CSOHÁNY Tibor: Aktív mágneses árnyékolás. TDK dolgozat, Budapesti Műszaki és Gazdaságtudományi Egyetem, Budapest, 2003.

DYKSTRA, Josiah –SHERMAN, Alan T.: Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. in Digital Investigation 9:S90--S98,2012 Amsterdam 2012. Elsevier.

DOLAN-GABITT B., PAYNE B., LEE W.: "Leveraging forensic tools for virtual machine introspection." Technical Report, Georgia Institute of Technology, GT-CS-11-05; 2011. p.1.

FENYVESI Csaba: A kriminalisztika, mint tudományág és mint egyetemi tantárgy. In Magyar Tudomány 2003/2 online 2003. Magyar Tudományos Akadémia, Online: http://epa.oszk.hu/00700/00775/ 00051/2003_02_04.html, hozzáférés: 2013.03.30

FINSZTER Géza: A kriminalisztika elmélete és a praxis a büntetőeljárási reform tükrében. Budapest, 2005-2007. online: users.atw.hu/be/letoltes/Krimjegyzet.doc, hozzáférés: 2013.03.30

GAUBATZ, Matthew D. – SIMSKE Steven J.: "Printer-scanner identification via analysis of structured security deterrents." Information Forensics and Security, 2009. WIFS 2009. First IEEE International Workshop on. IEEE, 2009.

GEERTZ, Clifford: Az értelmezés hatalma. Budapest, Századvég Kiadó, 1994. 188.p.

HORVÁTH Gyöngyi dr., KUTACS Mária dr., SOÓS László dr., VAJDOVITS Éva dr.: Igazságügyi szakértői kézikönyv Budapest, 2006. HVGOrac

HORVÁTH Zoltán: A mosoly országából a röhej országába. http://rohejorszaga.blog.hu/2012/06/03/erre_egyszeruen_nem_talalok_szavakat_601 [2014.01.12.]

HUEBNER, Ewa –BEM, Derek – BEM, Oscar: "Computer Forensics – Past, Present And Future" Sydney 2007. University of Western Sydney, online: http://www.securimetric.org/library/software/ Computer_Forensics_Past_ Present_Future.pdf, hozzáférés: 2013.03.16

HUGYECZ Enikő Henriett: Ki a szerző? – Avagy hogyan profiloznak a laikusok? in E-nyelv Magazin 2011/03. Budapest, Inter Nonprofit Kft. 2011. online: http://e-nyelv-magazin.hu/2011/08/31/ki-a-szerzo-%e2%80%93-avagy-hogyan-profiloznak-a-laikusok/, hozzáférés: 2013.09.18.

ILLÉSI Zsolt: Számítógép hálózatok krimináltechnikai vizsgálata. in Hadmérnök 2009 december pp. 170-183. Budapest, 2009. Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar.

Incident Management and Forensics Working Group. 2013. Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing. pp.13-17.

JOHNSON, Thomas A. (editor): Forensic Computer Crime Investigation. Boca Raton, FL, USA, 2005. CRC Press.

KARIJA, Tejas D.: Digital Evidence: An Indian Perspective. in Digital Evidence and Electronic Signature Law Review. Vol. 5. Pario Communication Ltd., Biggleswade, UK, 2008. pp. 214-220

KOZINETS, Robert V.: On Netnography: Initial Reflections on Consumer Research Investigations of Cyberculture. in NA - Advances in Consumer Research Volume 25, eds. Joseph W. Alba & J. Wesley Hutchinson, Provo, UT : Association for Consumer Research, 1998. pp.366-371.

KRIPPENDORFF, Klaus: A tartalomelemzés módszertanának alapjai. Balassi Kiadó, Budapest, 1995. p.57.

LÁSZLÓ Zoltán (szerk.): Vergilius. http://www.literatura.hu/irok/ okor/vergilius/vergilius.htm [2014.01.10.]

LEARY, Mary G.: Sexting or Self-Produced Child Pornography? The Dialogue Continues – Structured Prosecutorial Discretion within a Multidisciplinary Response. in Virginia Journal of Social Policy and the Law. Vol. 17, No. 3, Spring 2010 Charlottesville, VA, USA, 2010. online: http://ssrn.com/abstract= 1657007, hozzáférés: 2013.10.26. p.500.

LEE, Rob – SANS DFIR Faculty: Digital Forensics and Incident Response Poster. SANS Institute, Bethesda, MD, USA, 2012.

MACE, John: Printer Identification Techniques and Their Privacy Implications. University of Newcastle upon Tyne, Computing Science, 2010. p.2.

MANOLEA, Bogdan: The digital economy • where is the evidence? Theoretical and practical problems in understanding dlgital evidence in Romania. International Conference on Digital evidence. London, 26-27. June 2008., Conference Book pp. 226-230.

MÁTÉ István Zsolt: A bizonyítékok kezelése - az igazságügyi informatikai szakértő a büntetőeljárásban. in Konferenciakötet - Rendészeti Ágazat Doktoranduszainak V. Országos Fóruma. Rendészeti Doktoranduszok országos Egyesülete. 2014.

MÁTÉ István Zsolt: A digitális bizonyíték. in Konferenciakötet - Jogász Doktoranduszok Országos Szakmai Találkozója. Károli Gáspár Református Egyetem Állam- és Jogtudomány Kar. 2014.

MÁTÉ István Zsolt: A digitális bűnfelderítés gyakorlata, avagy az igazságügyi informatikai szakértő a büntetőeljárásban. in Pécsi Határőr Tudományos Közlemények XIV., Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs, 2013.

MÁTÉ István Zsolt: A multimédia technológiák kulturális hatásai. PTE-BTK Kommunikáció és Médiatudományi Tanszék, Pécs, 2012.

MÁTÉ István Zsolt: Digital Forensic Science – szabványosítási törekvések „régen" és ma. in Konferenciakötet – ISZAK2013 konferencia. Budapesti Igazságügyi Szakértői Kamara, 2013. (ISBN:978-963-08-7882-1)

MCLUHAN, Marshall: The Gutenberg Galaxy. Routledge & Kegan Paul, London, 1962.

MENEZES, Alfred J., –VAN OORSCHOt, Paul C. and VANSTONE, Paul C.: Handbook of Applied Cryptography, CRC Press, 1997. p. 321.

MUNISWAMY - REDDY – MACKO – SELTZER. "Provenance for the Cloud." *FAST*. Vol. 10. 2010.

NOLAN, Richard - O'SULLIVAN, Colin - BRANSON, Jake - WAITS, Cal: First Responders Guide To Computer Forensics Pittsburg 2005. Carnegie Mellon Software Engeneering Institute.

NÓTÁRI Tamás: A magyar szerzői jog fejlődése. Lectum Kiadó, 2010. p.21.

ORBÁN József Dr.: A Bayes-hálók rendészeti alkalmazhatóságának vizsgálata. in Gaál Gyula -Hautzinger Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények. XIV kötet. Pécs 2013. p.379-386.

PALMER, Gary et al.: A Road Map for Digital Forensic Research. First Digital Forensic Research Workshop. Utica, NY, USA, 2001.

PART Krisztina Katalin: A szerzői jogi szabályozás kialakulása Angliában, Németországban és az Egyesült álla-mokban. in Iparjogvédelmi és szerzői jogi szemle 2006/4. Szellemi Tulajdon Nemzeti Hivatala, 2006. p.142., http://www.sztnh.gov.hu/ki-adv/ipsz/200608-pdf/08-part-krisztina.pdf [2014.01.10.]

REILLY, Denis - WREN, Chris - BERRY, Tom: Cloud Computing: Pros and Cons for Computer Forensic Investigations. in International Journal Multimedia and Image Processing Volume 1, Issue 1, March 2011 online, 2011. Infonomics Society, online: http://www.infonomics-society.org/IJMIP/, hozzáférés: 2013.03.16

Scientific Working Groups on Digital Evidence and Imaging Technology: SWGDE and SWGIT Digital & Multimedia Evidence Glossary. version: 2.7, SWGDE/SWGIT, 2013. online: https://www.swgde.org/documents, hozzáférés: 2013.11.02.

SHANNON, Claude Elwood: A Mathematical Theory of Communication. in The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948. p.2.

SPEARS et al.: Social psychological theories of computer-mediated communication: Social pain or social gain? in The Handbook of Language and Social Psychology. Oxford, Wiley, 1990.

SZÁDECZKY Tamás: Szabályozott biztonság. Az informatikai biztonság szabályozásának elmélete, gyakorlata és az alkalmazás megkönnyítésére felállított módszertan. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, 2011. Pécs.

SZATHMÁRY Zoltán dr.: Bűnözés az információs társadalomban. Budapest, 2012. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskolája „Informatikai és Kommunikációs Jog" Program. 2012. Budapest.

TREMMEL Flórián – FENYVESI Csaba: Kriminalisztika tankönyv és atlasz. Budapest-Pécs, 2002. Dialóg Campus.

TREMMEL Flórián: Bizonyítékok a büntetőeljárásban. Dialóg Campus. Budapest, 2012. – (Kivonat a Kriminalisztikai Szakirányú Továbbképzési Szak (KSzT) hallgatói részére.), online: www.herke.hu/kszt/tf.doc, hozzáférés: 2013.11.02.

ZAWOAD, Shams, and **RAGIB, Hasan**. "Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems." *arXiv preprint arXiv:1302.6312* (2013).

ZAWOAD, Shams, and **RAGIB, Hasan**. "Towards building proofs of past data possession in cloud forensics." *SCIENCE* 1.4 (2012).

13.2 Feldolgozott irodalom

ADEMU, Inikpi O. - IMAFIDON, Dr Chris O. - PRESTON, Dr David S.: A New Approach of Digital Forensic Model for Digital Forensic Investigation. in International Journal of Advanced Computer Science and Applications, Vol. 2, No.12, 2011 New York, NY, USA, 2011. IJACSA Publications.

ALFÖLDI Ágnes Dóra: Gondolatok a büntetőeljárásbeli bizonyítás jelentőségéről és fogalmának elméleti megközelítéséről. in Jogelméltei Szemle 2/2011. Budapest, 2011. Jogelméleti Szemle online: http://jesz.ajk.elte.hu/alfoldi46.html, hozzáférés: 2013. 03.16

AYERS, Rick - JANSEN, Wayne: PDA Forensic Tools: An Overview and Analysis. Gaithersburg, MD, USA, 2004. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology

BALL, Craig: Six Articles on Computer Forensics for Lawyers Montgomery, Texas 2005. Craig Ball.

BELL, Graeme B. - BODDINGTON, Richard: "Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? In The Journal of Digital Forensics, Security and Law, Vol. 5(3), 2010. pp. 1-20. Maidens, VA, USA 2010. Association of Digital Forensics, Security and Law.

BEM, Derek –HUEBNER, Ewa: Computer Forensic Analysis in a Virtual Environment Sydney 2007. University of Western Sydney, Australia.

BERINO, Anthony J.: Forensic Science – Fundamentals & Investigations Mason, OH USA 2008. Cengage Learning.

BUI, Sonia – ENYEART, Michelle – Luong, Jenghuei: Issues in Computer Forensics. Santa Clara, CA, USA 2003. Santa Clara University online: http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/ Forensic%20Investi gation.pdf, hozzáférés: 2013.03.30

BUNTING, Steve: EnCase® Computer Forensics. Indianapolis, IN, USA, 2008. Wiley Publishing Inc.

CASELLAS CARALT, Núria: Modelling Legal Knowledge through Ontologies. OPJK: the Ontology of Professional Judicial Knowledge, online 2008. "Departament de Ci`encia Pol´ıtica i Dret P´ublic Universitat Aut`onoma de Barcelona" online: http://idt.uab.es /downloads/ncasellas/nuria_casellas_thesis.pdf, hozzáférés: 2013.03.30

COHEN, Fred Dr.: The Future of Digital Forensics. in 1st Chinese Conference on Digital Forensics online 2012. 1st Chinese Conference on Digital Forensics online: http://www. all. net/, hozzáférés: 2013.03.30

COWARD, Joseph: "Computer Forensics: Breaking down the 1's and 0's of cyber activity for potential evidence." online 2009. Infosecwriters.com. online: http://www.infosecwriters.com/text_resources/ pdf/JCoward_Forensics.pdf, hozzáférés: 2013.03. 30

DYKSTRA, Josiah - RIEHL, Damien: Forensic Collection of Electronic Evidence from Infrastructure-As-a-Service Cloud Computing. in Richmond Journal of Law & Technology, Volume XIX, Issue 1 online, 2012. University of Richmond "online: http://jolt.richmond.edu/wordpress/index.php/2012/11/ forensic-collectionof-electronic-evidence-from-infrastructure-as-a-service-cloud-computing/", hozzáférés: 2013.03.16

GARFINKEL, Simson - FARRELL, Paul - ROUSSEV, Vassil - DINOLT, George: Bringing science to digital forensics with standardized forensic corpora. in digital investigation 6 (2009) S2–S11, Amsterdam 2009. Elsevier

GIORDANO J, - MACIAG C.: Cyber forensics: a military operations perspective. In International Journal of Digital Evidence Summer 2002, Volume 1, Issue 2 online, 2002. ijde.org online: http://www.utica.edu /academic/institutes/ecii/publications/articles/A04843F3-99E5-632B-FF420389C0633B1B.pdf, hozzáférés: 2013.03.30

GREGG M.: The certified computer examiner certification. online, 2004. Anventure, LLC. online: http://www.gocertify.com/article/certifiedcomputerexaminer.shtml, hozzáférés: 2013.03.16

GRISPOS, George - STORER, Tim - GLISSON, William Bradley: Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics. in International Journal of Digital Crime and Forensics, 4,2012, Hershey, PA, USA 2012. Information Resources Management Association.

HARRILL, David Christopher - MISLAN, Richard P.: A Small Scale Digital Device Forensics ontology. in Small Scale Digital Device Forensics Journal, Vol. 1, No. 1, June 2007 online, 2007.

HORVÁTH Gyöngyi dr: Igazságügyi szakértői kézikönyv hatályosító pótfüzet Budapest, 2007. HVGOrac

ILLÉSI Zsolt: Az igazságügyi informatikai szakértés modellezése. in Hadmérnök 2010 december pp. 122-136 Budapest, 2010. Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar.

Иванов, Н. А.: Криминалистические классификации цифровой информации. in Вестник Омской юридической академии. 2013. № 1 (20). ISSN 2306-1340. pp. 81-84. online: http://cyberleninka.ru/article/n/kriminalisticheskie-klassifikatsii-tsifrovoy-informatsii, hozzáférés: 2016. január 10.

Jansen, Wayne - Ayers, Rick: Guidelines on Cell Phone Forensics. Gaithersburg, MD, USA, 2007. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology.

Jones, Robert: Internet Forensics. Sebastopol, CA, USA, 2006. O'Reilly Media, Inc.

Kármán Gabriella Dr. – Mészáros Ádám Dr. - Nagy László Tibor Dr. - Szabó Imre Dr.: A szellemi tulajdonjogokat sértő bűncselekmények vizsgálata Budapest, 2010. Országos Kriminológiai Intézet http://www.hamisitasellen.hu/hu/system/files/HENT_OKRI_empirikus_kutatas.pdf, hozzáférés: 2013. 03.16

Keyun Ruan, Joe Carthy, Tahar Kechadi, Mark Crosbie: Cloud forensics: An overview. in Advances in Digital Forensics VII Orlando, FL, USA 2011. National Center for Forensic Science online: http://cloudforensicsresearch.org/publication/ Cloud_Forensics_An_Overview_7th_IFIP.pdf, hozzáférés: 2013.03.16

Kipper, Gregory: Wireless Crime And Forensic Investigation. Boca Raton, FL, USA, 2007. Auerbach Publications.

Korinek László: A bűnügyi tudományok helyzete. In Magyar Tudomány 2007/12 online 2007. Magyar Tudományos Akadémia, online: http://www.matud.iif.hu /07dec.html, hozzáférés: 2013.03.30

Kumar, Nitish: Computer Forensics. in IEEE Security & Privacy 7-8/2005. online 2005. IEEE Computer Society online: http://www.academia.edu/2003320/Computer_forensics, hozzáférés: 2013.04.06

Laubscher, R. – Olivier, M.S. – Venter, H.S. – Rabe, D.J. – Eloff, J.H.P.: Computer Forensics For Computer-Based Assessment: The Preparation Phase. in Fifth Annual Information Security South Africa Conference, "Sandton, South Africa" 2005. Department of Computer Science, School of IT, University of Pretoria, South Africa, online: http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/100_ Article.pdf, hozzáférés: 2013.03.30

Liziczay Sándor Dr.: A modern kriminalisztikai eszközök bizonyítékként történő értékelése a büntetőeljárásban Budapest, NA. Fővárosi Törvényszék online: http://www.fovarositorvenyszek.hu/szellemi-muhelyunk/modern-kriminalisztikai-eszkozok-bizonyitekkent-torteno-ertekelese, hozzáférés: 2013. 03.16

Manolea, Bogdan: Theoretical and Practical Problems in Understanding Digital Evidence in Romania. in Digital Evidence and Electronic Signature Law Review. Vol. 5. Pario Communication Ltd., Biggleswade, UK, 2008. pp. 226-230.

MARAS, Marie-Helen: Conputer Forensics Cybercriminals, Laws and Evidences Sudbury, MA USA 2012. Jones & Bartlett Learning , LLC.

MARCELLA, Albert J. – GREENFIELD, Robert S. (editor): Cyber Forensics—A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. Boca Raton, FL, USA, 2002. Auerbach Publications.

MEYERS M, – ROGERS M.: Computer forensics: the need for standardization and certification. in International Journal of Digital Evidence Fall 2004, Volume 3, Issue 2 online, 2004. ijde.org Online: http://www2.tech.purdue.edu/cpt/courses/CPT499S /meyersrogers_ijde.pdf, hozzáférés: 2013.03.16

MEZEI Péter dr.: A digitális sampling és a fájlcserélés kihívásai a szerzői művek szabad felhasználására. Szeged, 2009. Szegedi Tudományegyetem, Állam- és Jogtudományi Kar.

MOLNÁR Beáta: Tudomány a bűnüldözésben, a bűnüldözés tudománya, a kriminalisztika Budapest, 2011. NA. online: http://www.slideshare.net/molnarbea/tudomny-a-bnldzsben-molnr-beta.

MOULTON, Scott A.: Computer Forensics - Error in Judgment. in Information Technology Security Awareness 2006 conference Gainesville, FL, USA 2006. University of Florida online: http://www.itsa. ufl.edu/archives/2006/presentations/moulton.pdf, hozzáférés: 2013.03.30

NAGY Zoltán András dr.: Bűncselekmények számítógépes környezetben. Budapest, 2009. Ad Librum Kft.,

NAGY Zoltán András dr.: Informatikai bűncselekmények. in Magyar Tudomány CVIII. 2001.8. 946-957.l. Budapest, 2001. Magyar Tudományos Akadémia,

NÉMETH Zoltán György: "A nyomozó hatóság bizonyításban játszott szerepe, a nyomozati tényfeltárás és a bizonyítás összefüggései. in Jogelméltei Szemle 2/2012." Budapest, 2012. Jogelméleti Szemle online: http://jesz.ajk.elte.hu/nemethz50.pdf, hozzáférés: 2013. 03.16

NOLAN, Richard - BAKER, Marie - BRANSON, Jake - HAMMERSTEIN, Josh - RUSH, Kris - WAITS, Cal - SCHWEINSBERG, Elizabeth: First responders guide to computer forensics: advanced topics Pittsburg 2005. Carnegie Mellon Software Engeneering Institute.

NOY N, MCGUINNESS D.: Ontology development 101: a guide to creating your first ontology. online, 2001. Knowledge Systems Laboratory, Online: http://protege.stanford.edu/publications/ontology_ development/ontology101-noy- mcguinness.html, hozzáférés: 2013.03.16

PESZLEG Tibor Dr.: Interneten, számítógépen történő nyomrögzítés. In Rendőrségi évkönyv 2005. online 2005. Országos Rendôr - fôkapitányság online: http://www.police.hu/data/cms191028/ REK05_023_034_peszleg.pdf, hozzáférés: 2013.03.30

PETHŐ Erzsébet Margit Dr.: A modern krimilalisztikai eszközök bizonyítékként történő értékelése a büntetőeljárásban Budapest, 2004. Fővárosi Törvényszék Online: http://www.fovarositorvenyszek.hu /sites/default/files/allomanyok/szellemimuhely/dr_petho_erzsebet_margit.pdf, hozzáférés: 2013.03. 16

POMFRET, Ian: Computer Forensics (presentation) Bucharest 2003. Trans-European Research And Education Networking Association online: http://www.terena.org/activities/tf-csirt/meeting4/ pomfret- computer-forensics.pdf, hozzáférés: 2013.03.30

PROSISE, Chris – Mandia, Kevin: Incident Response & Computer Forensics, New York, NY, USA, 2003. McGraw-Hill/Osborne.

PTERSO, Josheph L - RYAN, John P. - HOULDEN, Pauline J. - MIHAJLOVIC, Steven: Forensic Science and the courts: The Uses and Effects of Scientific Evidence in Criminal Case processing Washington, D.C 1986. US. Department of Justice national Institute of Justice.

ROGERS, Marcus K. - GOLDMAN, James - MISLAN, Rick - WEDGE, Timothy - DEBROTA, Steve: Computer Forensics Field Triage Process Model. In Conference on Digital Forensics, Security and Law, 2006. online 2006. Computer Forensics Field Triage Process Model, online: http://www.digitalforensics-conference.org/CFFTPM/CDFSL-proceedings2006-CFFTPM.pdf, hozzáférés: 2013.03.30

RUSSO, Armstrong H.: Electronic forensics education needs of law enforcement. online, 2004. The Colloquium for Information Systems Security Education, online: http://www.ncisse.org/publications/ cissecd/Papers/S4P02.pdf; hozzáférés: 2013. 03.16

SIEGEL, Jay - KNUPFER, Geoffrey – SAUKKO, Pekka (editor): Encyclopedia of Forensic Sciences, Waltham, MA, USA, 2000. Academic Press - Elsevier.

SLÉDER Judit: A büntetőeljárás megindítása. PhD dolgozat online 2010. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola online: http://doktori-iskola.ajk.pte.hu/files/tiny_mce/File/ Archiv2/Sleder_Judit/sleder_ertekezes.pdf, hozzáférés: 2013.03.30

STEPHENSON, Peter: Investigating Computer-Related Crime A Handbook For Corporate Investigators. Boca Raton, FL, USA, 2000. Crc Press.

TAYLOR, Mark – HAGGERTY, John – GRESTY, David – LAMB, David: Forensic investigation of cloud computing systems. in Network Security 2011(3):4--10,2011 Amsterdam 2011. Elsevier.

TÖBB SZERZŐ: Computer Forensics, Computer Forensics Part 1: An Introduction to Computer Forensics. Hong Kong 2004. "Information Security and Forensics Society (ISFS), c/o Center for Information Security and Cryptography Department of Computer Science The University of Hong Kong" online: http://www.isfs.org.hk, hozzáférés: 2013.03.16

TÖBB SZERZŐ: Forensic Examination Of Digital Evidence: A Guide For Law Enforcement Washington, D.C 2004. U.S. Department of Justice Office of Justice Programs National Institute of Justice.

TÖBB SZERZŐ: Handbook of Forensic Science. Washington, 1994. US. Department of Justice Federal Bureau of Investigation.

TYLER, Gene (editor): Cyber forensics in the cloud. in The Newsletter for Information Assurance Technology Professionals, Vol14_No1 Herndon, VA, USA 2011. "Information Assurance Technology Analysis Center (IATAC)

WALKER, Cornell: "Computer Forensics: Bringing the Evidence to Court" online 2005. Infosec writers.com. online: http://www.infosecwriters.com/text_resources/pdf /Computer_Forensics_to_ Court.pdf, hozzáférés: 2013.03.16

YASINSAC, Alec - ERBACHER, Robert - MARKS, Donald G. - POLLITT, Mark M. - Sommer, Peter: Computer Forensics Education. in Security & Privacy, IEEE, July-Aug. 2003, Volume: 1 , Issue: 4 , Page(s): 15 - 23 Los Alamitos, CA 2003. Institute of Electrical and Electronics Engineers.

13.3 Jogszabályok, jogi és szakértői források

2005. évi XLVII. törvény az igazságügyi szakértői tevékenységről (Szaktv.[2005])

2016. évi XXIX. törvény az igazságügyi szakértőkről (Szaktv.[2016])

1998. évi XIX. törvény a büntetőeljárásról (Be.)

1978. évi IV. törvény a Büntető Törvénykönyvről

2012. évi C. törvény a Büntető Törvénykönyvről

2009. évi CLV. törvény a minősített adat védelméről

1999. évi LXXVI. törvény a szerzői jogról

1995. évi CXIV. törvény az igazságügyi szakértői kamaráról

282/2007. (X. 26.) Korm. rendelet a szakterületek ágazati követelményeiért felelős szervek kijelöléséről, valamint a meghatározott szakkérdésekben kizárólagosan eljáró és egyes szakterületeken szakvéleményt adó szervekről

90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről

31/2008. (XII. 31.) IRM rendelet az igazságügyi szakértői működésről

9/2006. (II. 27.) IM rendelet az igazságügyi szakértői szakterületekről, valamint az azokhoz kapcsolódó képesítési és egyéb szakmai feltételekről

11/2003. (V. 8.) IM-BM-PM együttes rendelet a lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról

TÖRVF-Á/22/2/2015. A Kormány 2016. évi tavaszi törvényalkotási programja. online:http://www.parlament.hu/documents/10181/87979/Tvalk_program_2016_ tavasz.pdf/a1eac7dd-8247-413a-bada-0311579775f8

Federal Rules of Evidence. Cornell University Law School, 2011. online: http://www.law.cornell.edu/rules/ fre, hozzáférés: 2013.09.13.

Statute of Anne. London, 1710. British Library, 8 Anne c. 19. p.1., (a szerző fordítása) http://www.copyrighthistory.com/anne.html [2012.02.01.]

Российский Федеральный Центр Судебной Экспертизы при Министерстве юстиции Российской Федерации - Компьютерно-техническая экспертиза. online: http://www. sudexpert.ru/possib/comp.php, hozzáférés: 2016. január 10.

Bírósági ítélet a C 355/12. sz. ügyben. http://curia.europa.eu/juris/document/document.jsf?text=&docid=146686&pageIndex=0&doclang=hu&mode=req&dir=&occ=first&part=1&cid=631579 [2014.01.26.]

Szerzői Jogi Szakértő Testület: SZJSZT 15/2000/1-2. sz. szakértői vélemény. 2000. p.2. http://www.sztnh.gov.hu/testuletek/szjszt/SZJSZT_szakvelemenyek/2000/2000PDF/szjszt_szakv_2000_015.pdf, [2014.01.15.]

Igazságügyi Szakértői Névjegyzék. Online: https://szakertok.im.gov.hu/Shared/ SelectSzakteruletView, hozzáférés: 2016. január 9.

MÁTÉ István Zsolt: 10/2013. sz. igazságügyi informatikai szakértői vélemény. Máté István Zsolt, 2013. p.3. (nem nyilvános irat)

MÁTÉ István Zsolt: 25/2013. sz. igazságügyi informatikai szakértői vélemény. Máté István Zsolt, 2013. (nem nyilvános irat)

MÁTÉ István Zsolt: 22/2010. sz. igazságügyi informatikai szakértői vélemény in Szakértői archívum. 2010. p.7.

MÁTÉ István Zsolt: Szakértői ügynyilvántartás. 2014. (elektronikus)

MÁTÉ István Zsolt: Szakértői ügynyilvántartás/árajánlatok. 2014. (elektronikus)

13.4 Szabványok és egyéb források

E-szignó tudásbázis: https://e-szigno.hu/tudasbazis/fogalmak.html

Oyetools.com keresés: http://www.oyetools.com/search.php?target=ea.com&queryType=all [2014.01.17.]

Jogszerűnek nyilvánította a másolásvédelmek feltörését az EU http://pcforum.hu/hirek/15776/Jogszerunek+nyilvanitotta+a+masolasvedelmek+feltoreset+az+EU.html [2014.01.31]

ISO/IEC 19761:2011 Software engineering -- COSMIC: a functional size measurement method (https://www.iso.org/standard/54849.html)

ISO/IEC 27037:2012 Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence (https://www.iso.org/standard/44381.html)

14 Függelék

14.1 Informatikai szakterületek (2006 előtt)

Azonosító	Szakterület megnevezése
309	Informatika
1123	nagyvállalati rendszerszervezés
1125	nagyrendszerek tervezése
1126	rendszerprogramozás
1127	szoftver
1128	alkalmazott számítástechnika
1129	alkalmazói szoftverek
1130	számítógépes képfeldolgozás
1131	digitális képfeldolgozó berendezések
1132	számítógépes adatátvitel
1133	számítógépes vírusvédelem
1134	számítástechnikai adatbázis kezelés
1135	számítógép hálózatok
1136	hálózati szoftverek és alkalmazások
1137	szoftverfejlesztés
1138	rendszerszoftver
1139	hardver
1140	számítógépek és perifériák
1141	számítástechnikai és irodatechnikai berendezések
1142	pénztárgépek
1143	lakossági elektronikai és szórakoztató készülékek
1144	informatika
1145	információtechnika
1147	konzol hardver-szoftver (Sony, PSX, Nintendo)
1148	számítástechnikai hálózatok informatikája és adatvédelme
1149	informatikai alkalmazások
1150	információtechnológia és módszertan
1151	információs rendszer ellenőrzés, auditálás
1152	információ rendszerek ellenőrzése
1153	informatikai rendszerek
1154	közigazgatási informatika

14.2 Igazságügyi szakértői szakterületek és az azokhoz kapcsolódó képesítési feltételek az informatikai területeken [192]

Szakterület megnevezése	Képesítési feltétel
1. informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver)	a) villamosmérnök vagy b) okleveles villamosmérnök vagy c) okleveles rendszerinformatikus vagy d) mérnök-informatikus vagy e) okleveles mérnök-informatikus vagy f) okleveles fizikus
2. informatikai biztonság	a) villamosmérnök vagy b) okleveles villamosmérnök vagy c) okleveles rendszerinformatikus vagy d) mérnök-informatikus vagy e) okleveles mérnök-informatikus vagy f) okleveles programtervező matematikus vagy g) okleveles fizikus vagy h) okleveles matematikus vagy i) okleveles alkalmazott matematikus vagy j) programozó matematikus
3. informatikai rendszerek tervezése, szervezése	a) villamosmérnök vagy b) okleveles villamosmérnök vagy c) okleveles rendszerinformatikus vagy d) mérnök-informatikus vagy e) okleveles mérnök-informatikus vagy f) programozó matematikus vagy g) okleveles programtervező matematikus vagy h) okleveles informatika szakos tanár vagy i) számítástechnika szakos tanár vagy j) informatikai szakirányon végzett okleveles gazdaság-informatikus vagy k) okleveles fizikus vagy l) okleveles matematikus vagy m) okleveles alkalmazott matematikus
4. stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység	a) villamosmérnök vagy b) okleveles villamosmérnök vagy c) okleveles rendszerinformatikus vagy d) mérnök-informatikus vagy e) okleveles mérnök-informatikus
5. számítástechnikai adatbázis, adatstruktúrák	a) villamosmérnök vagy b) okleveles villamosmérnök vagy c) okleveles rendszerinformatikus vagy d) mérnök-informatikus vagy e) okleveles mérnök-informatikus vagy f) okleveles programtervező matematikus vagy g) okleveles alkalmazott matematikus vagy h) okleveles matematikus vagy i) programozó matematikus vagy j) okleveles informatika szakos tanár vagy k) számítástechnika szakos tanár
6. szoftverek	a) programozó matematikus vagy b) okleveles programtervező matematikus vagy c) okleveles informatika szakos tanár vagy d) számítástechnika szakos tanár vagy e) informatikai szakirányon végzett okleveles gazdaság-informatikus vagy f) okleveles alkalmazott matematikus vagy g) okleveles gazdaságmatematikai elemző szakos közgazdász vagy h) okleveles mérnök-informatikus vagy i) mérnök-informatikus vagy j) okleveles matematikus vagy k) villamosmérnök vagy l) okleveles villamosmérnök

[192] 9/2006. (II. 27.) IM rendelet az igazságügyi szakértői szakterületekről, valamint az azokhoz kapcsolódó képesítési és egyéb szakmai feltételekről 6. sz. melléklet A)

14.3 Az igazságügyi szakértői tevékenységre vonatkozó, vagy azzal kapcsolatos jogszabályok

2016. évi XXIX. törvény az igazságügyi szakértőkről[193]

2013. évi CCXL. törvény a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról

2013. évi XXXIV. törvény az építmények tervezésével és kivitelezésével kapcsolatos egyes viták rendezésében közreműködő szervezetről, és egyes törvényeknek az építésügyi lánctartozások megakadályozásával, valamint a késedelmes fizetésekkel összefüggő módosításáról

2012. évi II. törvény a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről

2010. évi XXXVIII. törvény a hagyatéki eljárásról

2009. évi CLV. törvény a minősített adat védelméről

2008. évi XLV. törvény az egyes közjegyzői nemperes eljárásokról

2007. évi CXXIII. törvény a kisajátításról

2006. évi V. törvény a cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról

2005. évi CXXXV. törvény a bűncselekmények áldozatainak segítéséről és az állami kárenyhítésről

2005. évi XLVIII. törvény az igazságügyi szakértő nemperes eljárásban történő kirendeléséről

2005. évi XLVII. törvény az igazságügyi szakértői tevékenységről[194]

2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól

1998. évi XIX. törvény a büntetőeljárásról

1997. évi XXXI. törvény a gyermekek védelméről és a gyámügyi igazgatásról

1995. évi CXIV. törvény az igazságügyi szakértői kamaráról

1994. évi LIII. törvény a bírósági végrehajtásról

1952. évi III. törvény a polgári perrendtartásról

233/2014. (IX. 18.) Korm. rendelet az Igazságügyi Hivatalról

[193] Hatályba lépett 2016.06.15-én

[194] Hatályon kívül helyezve 2016.06.15-én

351/2013. (X. 4.) Korm. rendelet a halottvizsgálatról és a halottakkal kapcsolatos eljárásról

282/2007. (X. 26.) Korm. rendelet a szakterületek ágazati követelményeiért felelős szervek kijelöléséről

210/2005. (X. 5.) Korm. rendelet az igazságügyi szakértői névjegyzék vezetéséről

149/1997. (IX. 10.) Korm. rendelet a gyámhatóságokról, valamint a gyermekvédelmi és gyámügyi eljárásról

39/2012. (VIII. 27.) KIM rendelet az ingatlan becsértékének bíróság általi megállapítására irányuló végrehajtási kifogás előterjesztésével együtt letétbe helyezendő szakértői díj előlegének összegéről

58/2009. (X. 30.) IRM rendelet az igazságügyi szakértői kamara által lefolytatott egyes közigazgatási hatósági eljárásokért fizetendő igazgatási szolgáltatási díjról

31/2008. (XII. 31.) IRM rendelet az igazságügyi szakértői működésről

27/2006. (X. 5.) IRM rendelet az igazságügyi szakértői alapismeretek oktatásáról és vizsgájáról

19/2006. (IV. 24.) IM rendelet az igazságügyi szakértői igazolványról

10/2006. (III. 7.) IM rendelet az igazságügyi szakértői tevékenység folytatásához szükséges jogi oktatásról és vizsgáról

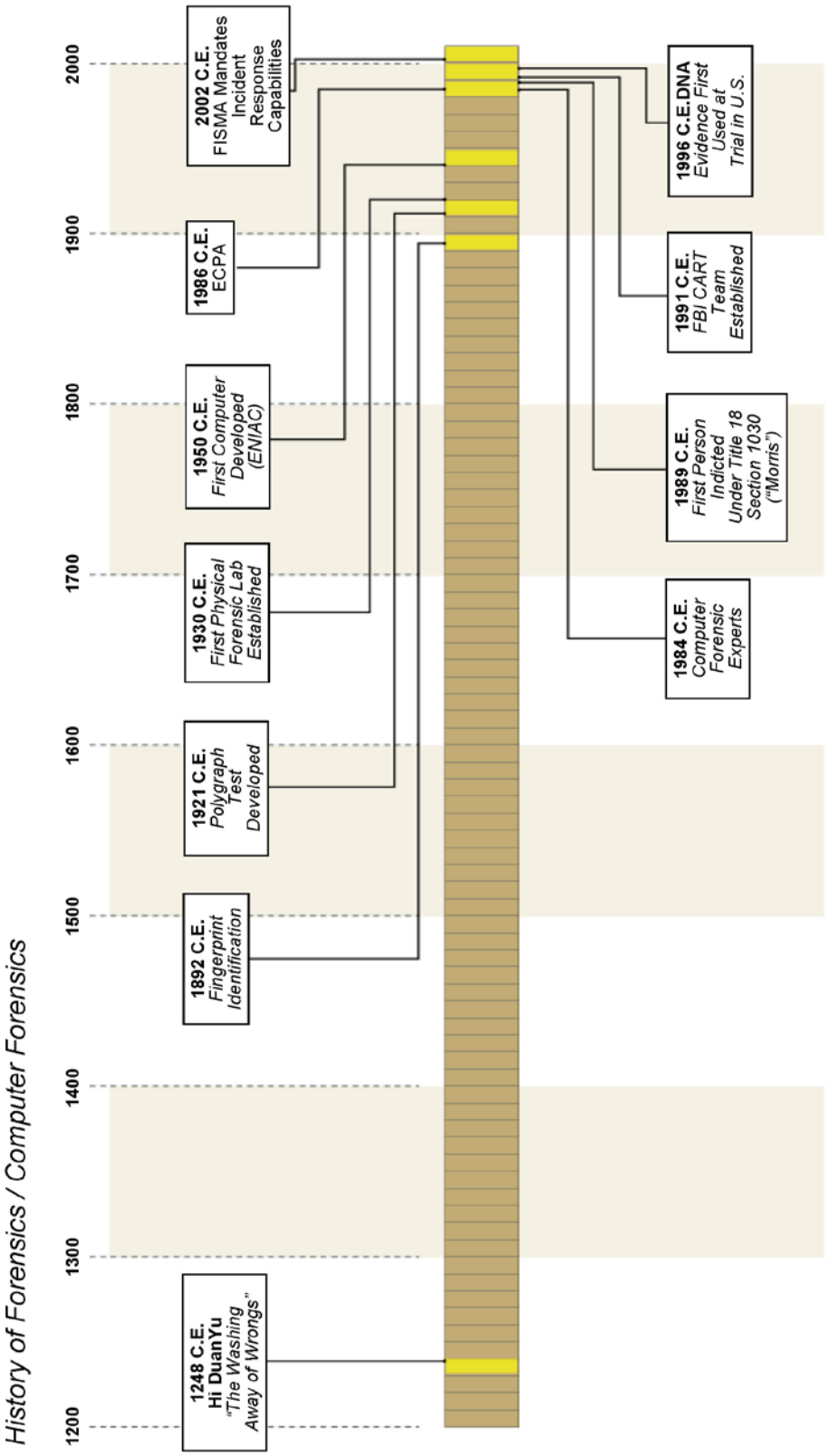
9/2006. (II. 27.) IM rendelet az igazságügyi szakértői szakterületekről, valamint az azokhoz kapcsolódó képesítési és egyéb szakmai feltételekről

4/2006. (I. 26.) IM rendelet az igazságügyi szakértői névjegyzékbe történő felvételi eljárás igazgatási szolgáltatási díjáról

21/2003. (VI. 24.) IM-PM-BM együttes rendelet a bűnügyi költségek előlegezéséről

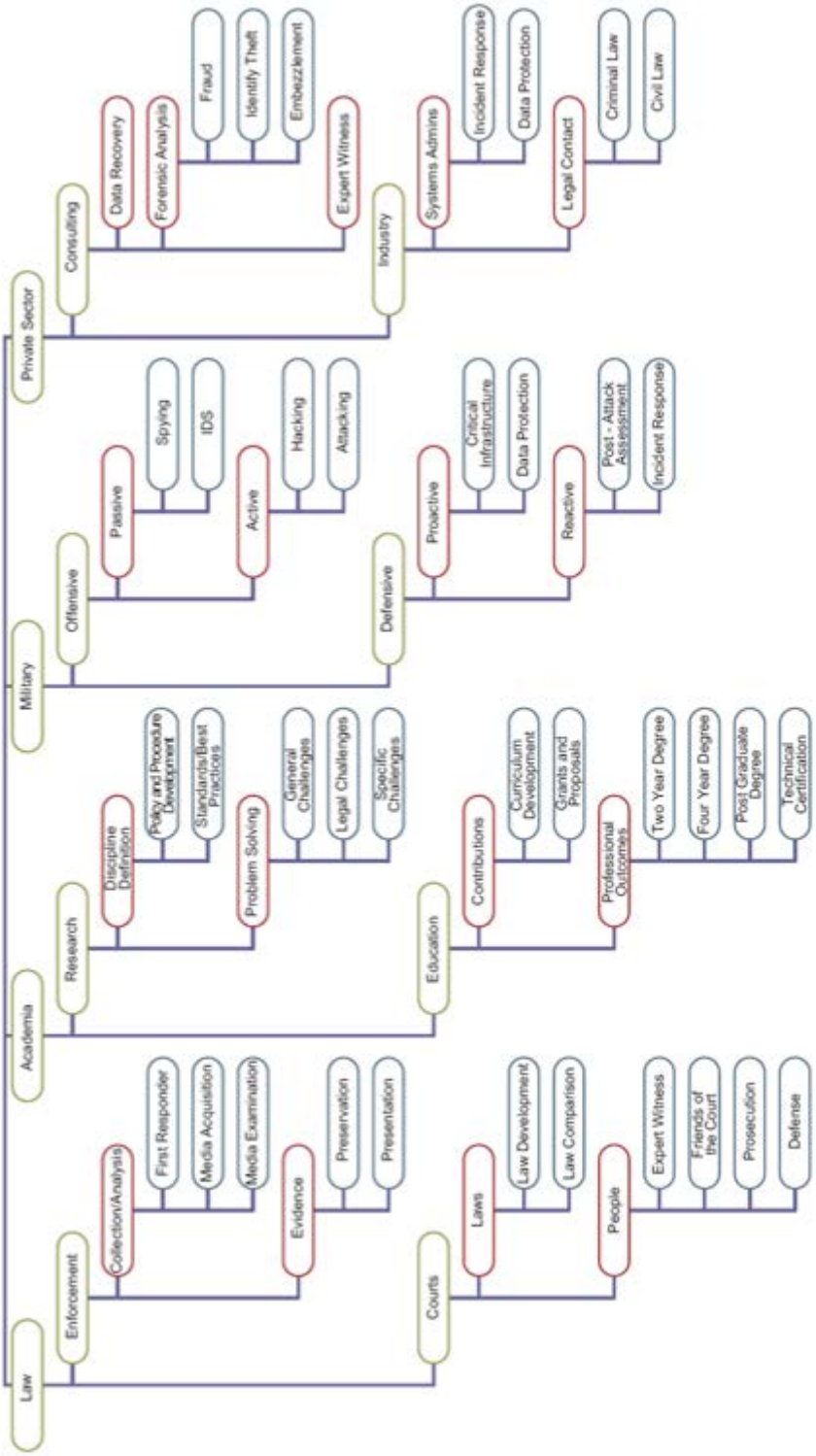
3/1986. (II. 21.) IM rendelet az igazságügyi szakértők díjazásáról

14.4 A forenzikus tudományok történeti áttekintése[195]



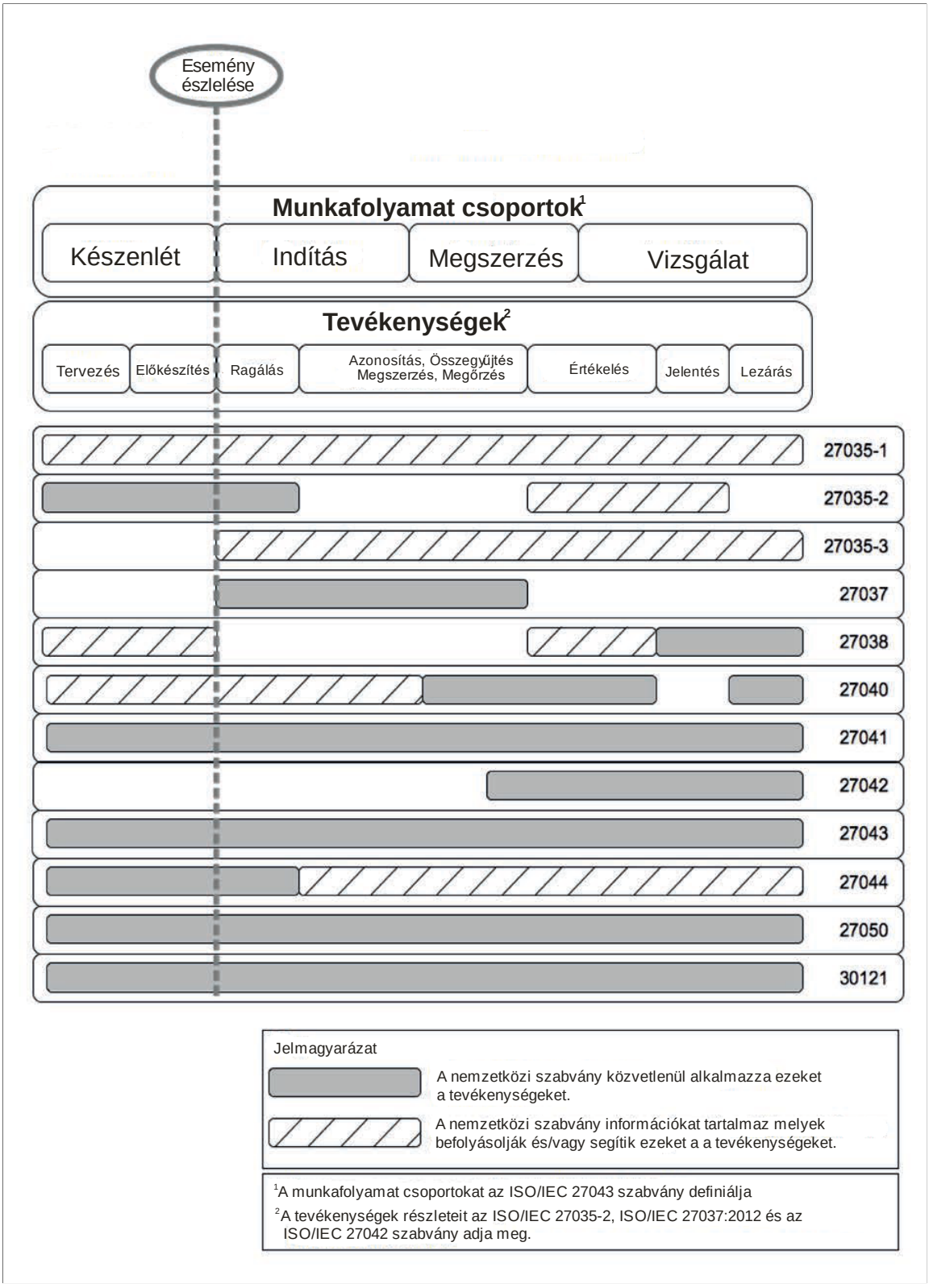
[195] NOLAN, et al. im. p. 3.

14.5 Szakterület felosztás[196]



[196] BRINSON et al., 2006. p.38.

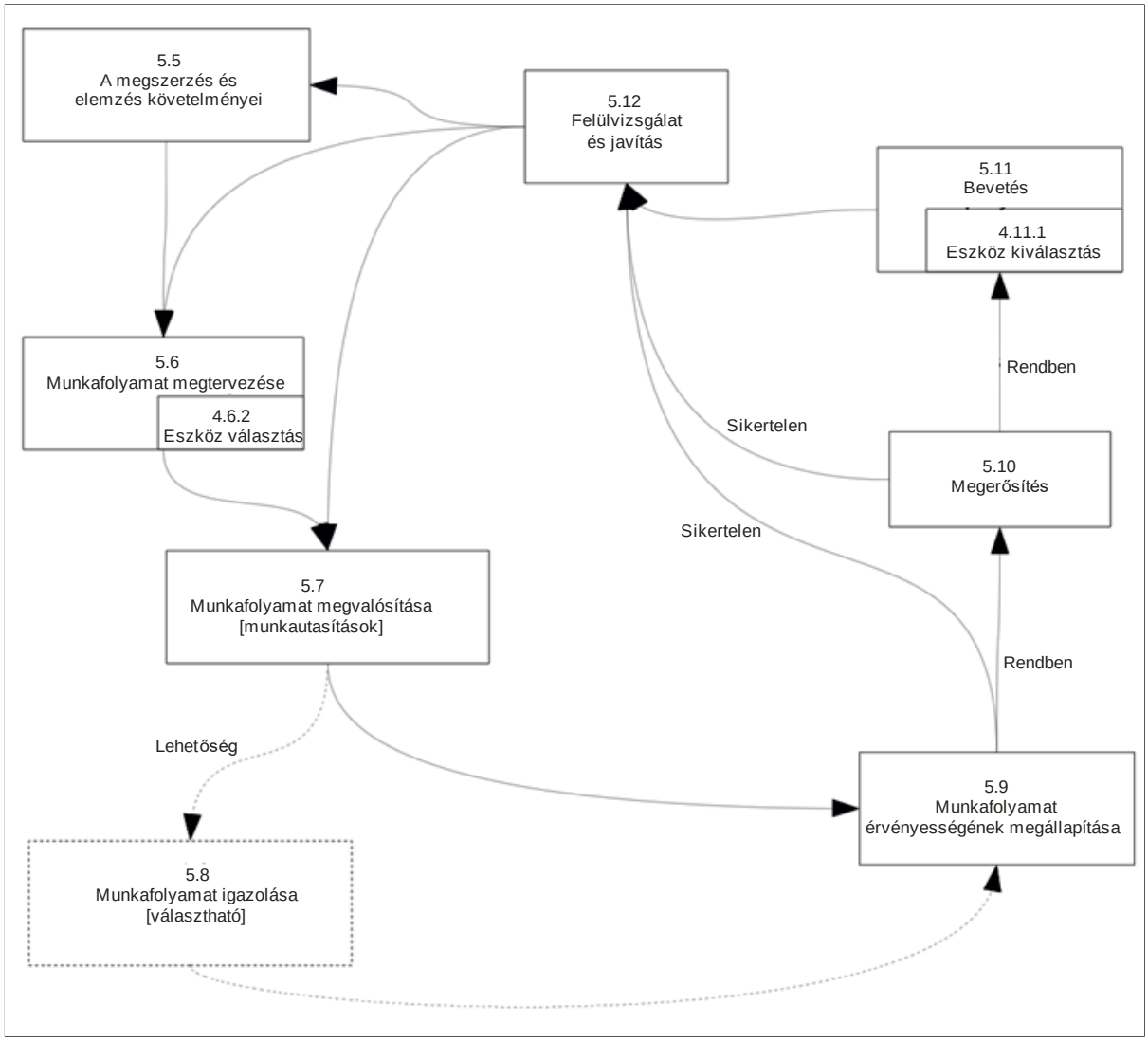
14.6 ISO/IEC 27000 szabványok viszonyrendszere



17. ábra – ISO/IEC 27041:2015 (p.viii – Figure 1.) alapján[197]

[197] A szerző fordítása

14.7 ISO/IEC 27000 szabványok viszonyrendszere



18. ábra - Fejlesztési és bevezetési munkafolyamatok, beleértve minőségbiztosítási szakaszt is[198]

[198] ISO/IEC 27041:2015 (p.5 – Figure 2.) alapján, a szerző fordítása

15 Illusztrációk

15.1 Bűnjeljegyzék[199]

Bűnjeljegyzék

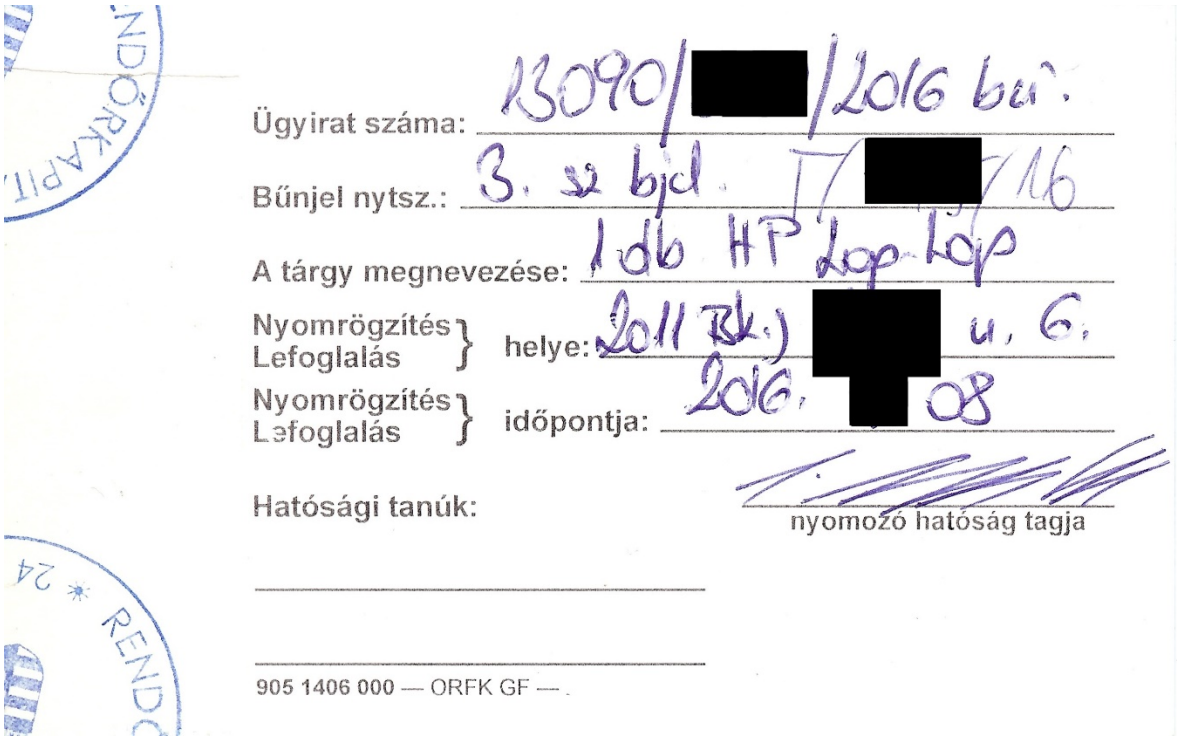
A fenti számú határozattal, a Btk. 396. §.-ába ütköző és 1 a) 5a) szerint minősülő költségvetési csalás elkövetésének – gyanúja miatt a Be. 151. §. (1), (3) bekezdése alapján lefoglalt bűnjelekről.

Sorszám	Mennyiség	Kereskedelmi megnevezése	Megjegyzés
1.	1 db	Samsung Galaxy S4 telefon	
2.	1 db	Samsung Galaxy Note 4 telefon	
3.	1 db	Nokia 6303 telefon	
4.	1 db	Alcatel telefon	
5.	1 db	Nokia RM 217 telefon	
6.	1 db	Nokia telefon	
7.	4 db	SIM kártya	
8.	1-30 o.	Vegyes irat	
9.	6 db	Bankkártya	
10.		[redacted] készpénz	
11.	1 db	Dell típusú laptop	
12.	1 db	[redacted] Kft. bélyegző	
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			

[199] 06/2016 bűnjel jegyzék (anonimizált részlet). Máté István Zsolt – Szakértői ügynyilvántartás.

15.2 Bűnjelek tételes átvétele[200]

15.3 Bűnjelcimke[201]



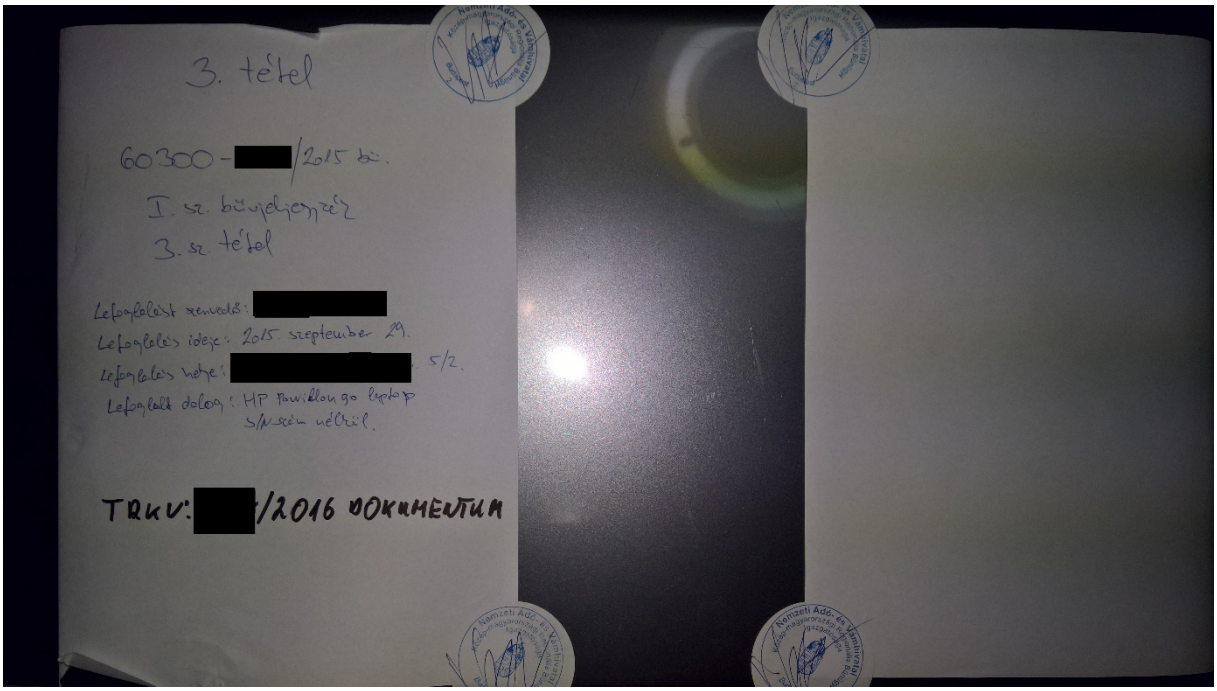
[200] 06/2016 – bűnjelek átvételkori állapotának rögzítése. Máté István Zsolt – Szakértői ügynyilvántartás.

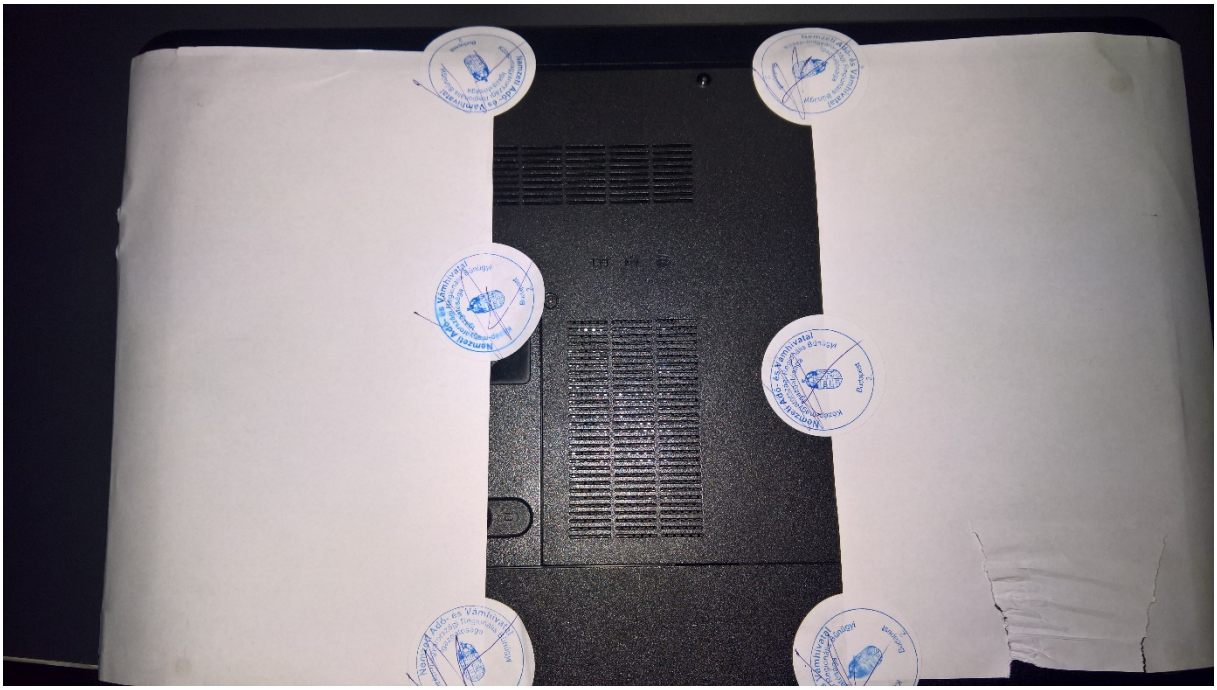
[201] 68/2016 – bűnjelcimke. Máté István Zsolt – Szakértői ügynyilvántartás.

15.4 Sérült bűnjel állapotának rögzítése[202]

[202] 09/2016 – sérült bűnjel állapotának rögzítése. Máté István Zsolt – Szakértői ügynyilvántartás.

15.5 Bűnjel csomagolásának felbontása[203]





[203] 40/2016 – eszköz csomagolás felbontása. Máté István Zsolt – Szakértői ügynyilvántartás.


TOSHIBA
MK6476GSX
DISK DRIVE
HDD2J92 C SL01 S
DC+5V 1.0A
DATE:26APR2012
010 A0/GS001A
S/N 420BSOYBS MQ6 EC.A
TOSHIBA CORPORATION
DO NOT REMOVE ANY LABELS.
DO NOT PUSH ON THE TOP COVER.
RATTLE NOISE IS NORMAL.
AVOID
DO NOT COVER BREATHING HOLE.
V10DHK2
FW Rev GS001C
Mod# MK6476GSX

15.6 Bűnjel egyedi azonosítójának rögzítése[204]

19. ábra - Merevlemez egyedi azonosítóval

[204] 46/2016 – Bűnjel egyedi azonosítójának rögzítése. Máté István Zsolt – Szakértői ügynyilvántartás.

15.7 Bűnjel egyedi elektronikus azonosítójának rögzítése[205]

```
   ----------------------Disk Information--------------------------
Vendor:                   ST316081
Model:                    2AS
Revision:                 E
Serial Number:            4LS0P5JW
Bus:                      SATA
Device:                   Direct Access
Capacity:                 160.0 GB (160,041,885,696 bytes)
Removable Media:          No
Cylinders:                19457
Tracks per Cylinder:      255
Sector per Track:         63
Bytes per Sector:         512
   -------------------------Bridge Information---------------------
Vendor:                   Tableau
Model:                    T35u
Description:              New Tableau Bridge
Serial number:            000ecc55 00358231
Channel:                  SATA
Bridge Access Mode:       Read-Only
Read-Only Declaration:    Declares Read-Only
Write Error Declaration:  Declares Write Errors
Firmware stepping:        5
Firmware build date:      Sep 15 2015
Firmware build time:      11:19:41
Firmware build type:      Debug
Drive Vendor:
Drive Model:              ST3160812AS
Drive Serial Number:      4LS0P5JW
Drive Revision:           3.AAE
      ----------------------- HPA/DCO Information ------------------
HPA Supported:            Yes
HPA in Use:               No
DCO Supported:            Yes
DCO in Use:               No
Security Supported:       Yes
Security in Use:          No
Reported Capacity:        160.0 GB (160,041,885,696 bytes)
HPA Capacity:             160.0 GB (160,041,885,696 bytes)
DCO Capacity:             160.0 GB (160,041,885,696 bytes)
    ------------------------------- End ----------------------------
```

[205] 10/2017 – Bűnjel egyedi elektronikus azonosítójának rögzítése (01 – Fujitsu PC tárolója). Máté István Zsolt – Szakértői ügynyilvántartás.

15.8 Burkolat megbontása az egyedi azonosító rögzítése céljából[206]

20. ábra - Digitális videorögzítő, megbontott eszközburkolattal[207]

[206] 10/2017 – Bűnjel egyedi elektronikus azonosítójának rögzítése (01 – Fujitsu PC tárolója). Máté István Zsolt – Szakértői ügynyilvántartás.

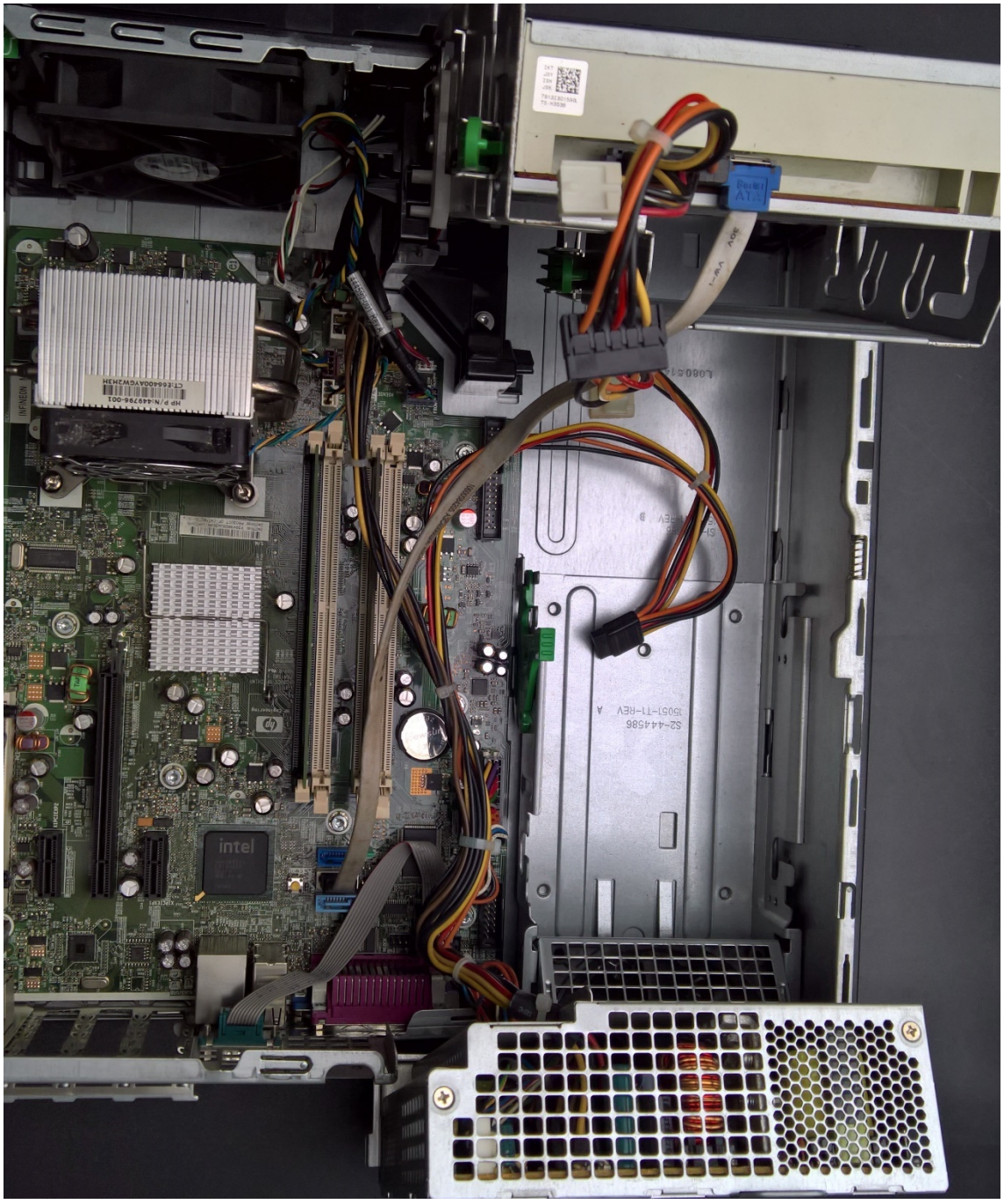
[207] 09/2015 – Eszközburkolat megbontása az egyedi eszközazonosítóhoz történő hozzáférés érdekében. Máté István Zsolt – Szakértői ügynyilvántartás.

15.9 Számítógép ház lezárási hibája az összegyűjtés során [208]

21. ábra - Számítógépház, lezárt csatlakozóval, lezáratlan burkolattal (jobb oldalon középen)

[208] Szakértői ügyarchívum, 21/2017 – Máté István Zsolt igazságügyi informatikai szakértő

15.10 Az összegyűjtés során alkalmazott nem megfelelő lezárás követlezménye (eltávolított tároló) [209]



22. ábra - Az összegyűjtés során alkalmazott nem megfelelő lezárás követlezménye (eltávolított tároló)

[209] Szakértői ügyarchívum, 21/2017 – Máté István Zsolt igazságügyi informatikai szakértő

23. ábra - [01] Samsung GT-I9300 okostelefon[210]

[210] 17/2016 – Eszközburkolat megbontása az egyedi eszközazonosítóhoz történő hozzáférés érdekében. Máté István Zsolt – Szakértői ügynyilvántartás.

15.11 Forensic Duplicator[211]

24. ábra - Tableau Forensic Duplicator lemezmásolat létrehozásához

[211] Forrás: https://www.guidancesoftware.com/tableau/hardware/td2u

15.12 Forensic Imager [212]

25. ábra - Forensic Imager lemezképfájl létrehozásához

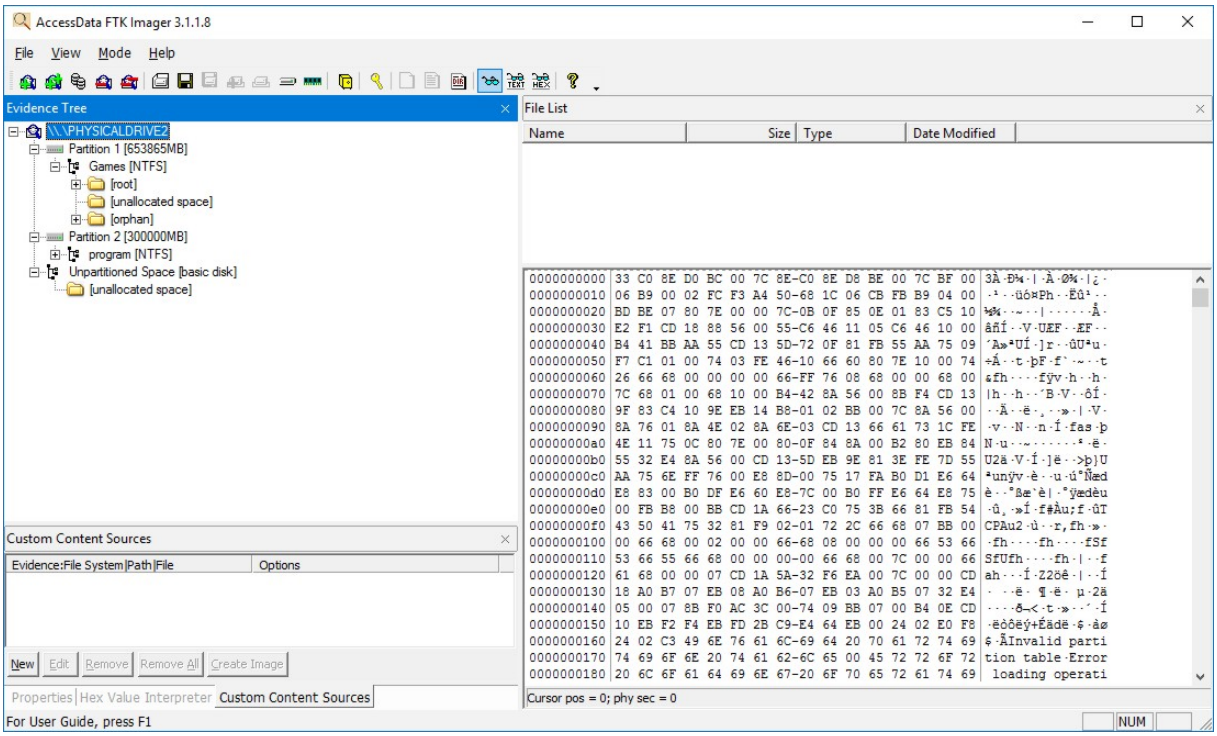
[212] Forrás: https://www.guidancesoftware.com/tableau/hardware/td3

15.13 Forensic Bridge [213]

26. ábra - Forensic writeblocker lemezképfájl lértrehozásához és célzott tartalmi mentéshez

[213] Forrás: https://www.guidancesoftware.com/tableau/hardware/t35u

15.14 AccessData FTK Imager[214]



27. ábra - AccessData FTK Imager

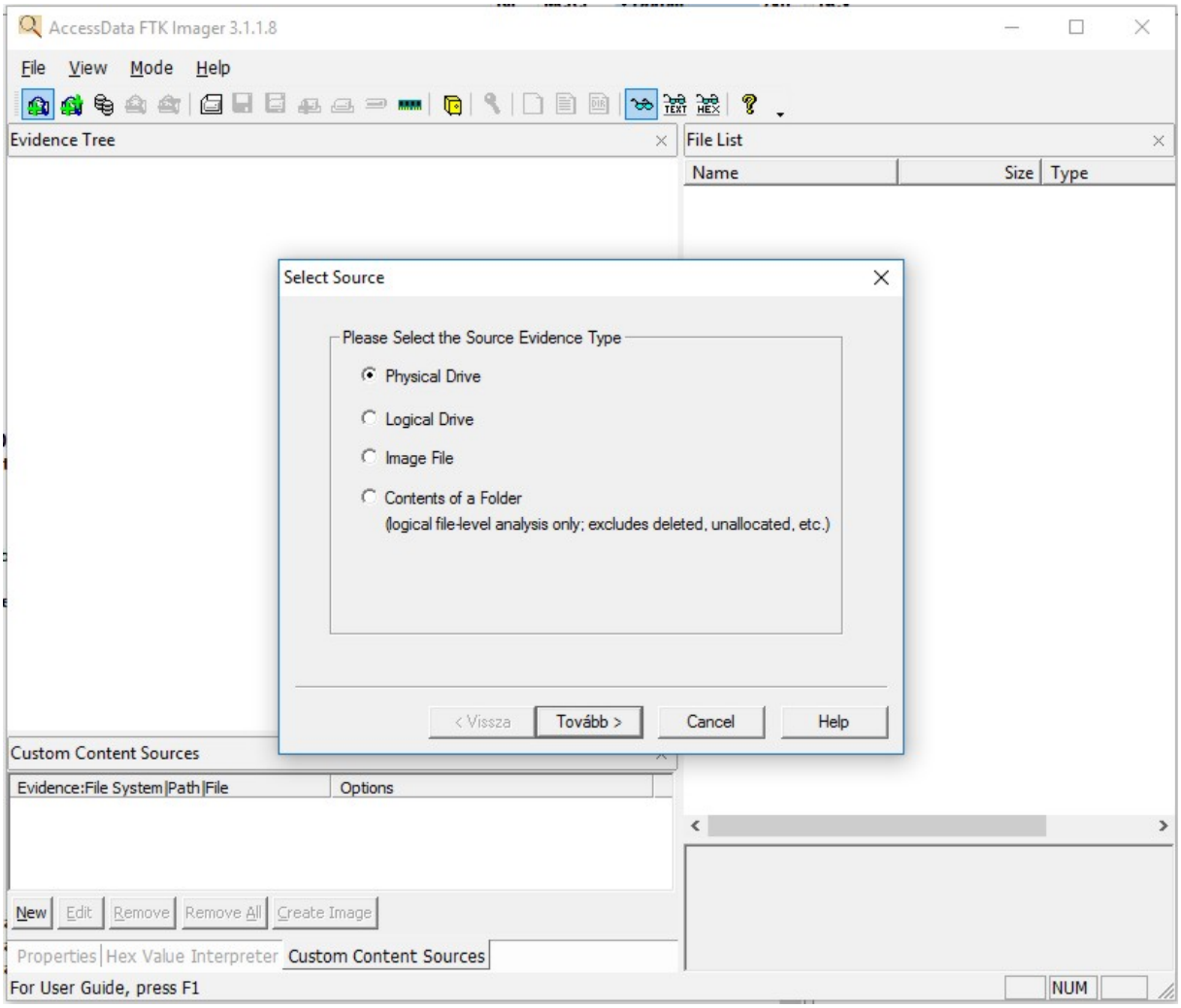
[214] 15/2017 – Adatkinyerés [28] Acer laptop eszközről - Máté István Zsolt – Szakértői ügynyilvántartás.

15.15 Lemezképfájl naplóállománya[215]

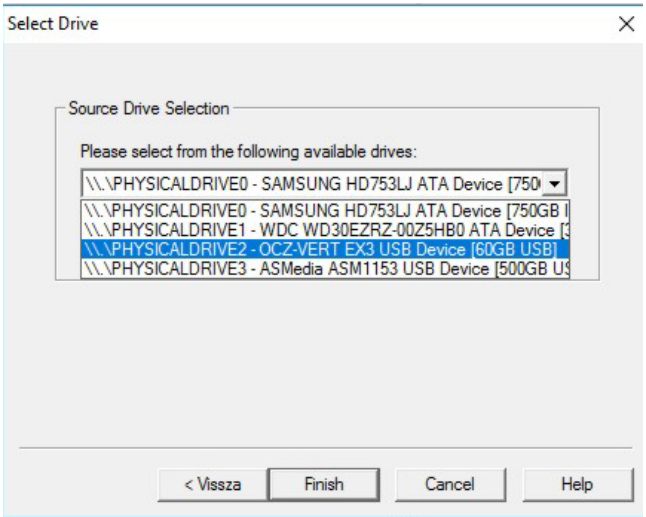
```
Created By AccessData® FTK® Imager 3.1.1.8

Case Information:
Acquired using:           ADI3.1.1.8
Case Number:              12/2016 - 60100-×××/2016 bü.
Evidence Number:          09 - Sietech USB 2.0
Unique description:       pendrive
Examiner:                 Máté István Zsolt
                          igazságügyi informatikai szakértő
Notes:

------------------------------------------------------------

Information for D:\12-2017\09_Sietech_USB2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type:             Logical
[Partition Information]
 Starting Sector:         32
 Sector Count:            511 456
 Source data size:        249 MB
 Sector count:            511456
[Computed Hashes]
 MD5 checksum:            28d1b0a52d011c10e7849204249afb24
 SHA1 checksum:           0727e7db83ee8f2169b94cee658c455ba52b751f

Image Information:
 Acquisition started:     Sun Apr 23 19:25:43 2017
 Acquisition finished:    Sun Apr 23 19:26:16 2017
 Segment list:
                          D:\12-2017\09_Sietech_USB2.E01

Image Verification Results:
 Verification started:    Sun Apr 23 19:26:16 2017
 Verification finished:   Sun Apr 23 19:26:18 2017
 MD5 checksum:            28d1b0a52d011c10e7849204249afb24 : verified
 SHA1 checksum:           0727e7db83ee8f2169b94cee658c455ba52b751f :
                          verified
```

[215] 10/2017 – Bűnjel egyedi elektronikus azonosítójának rögzítése (01 – Fujitsu PC tárolója). Máté István Zsolt – Szakértői ügynyilvántartás.

15.16 Lemez tartalomjegyzék készítés folyamata FTK Imager alkalmazással[216]

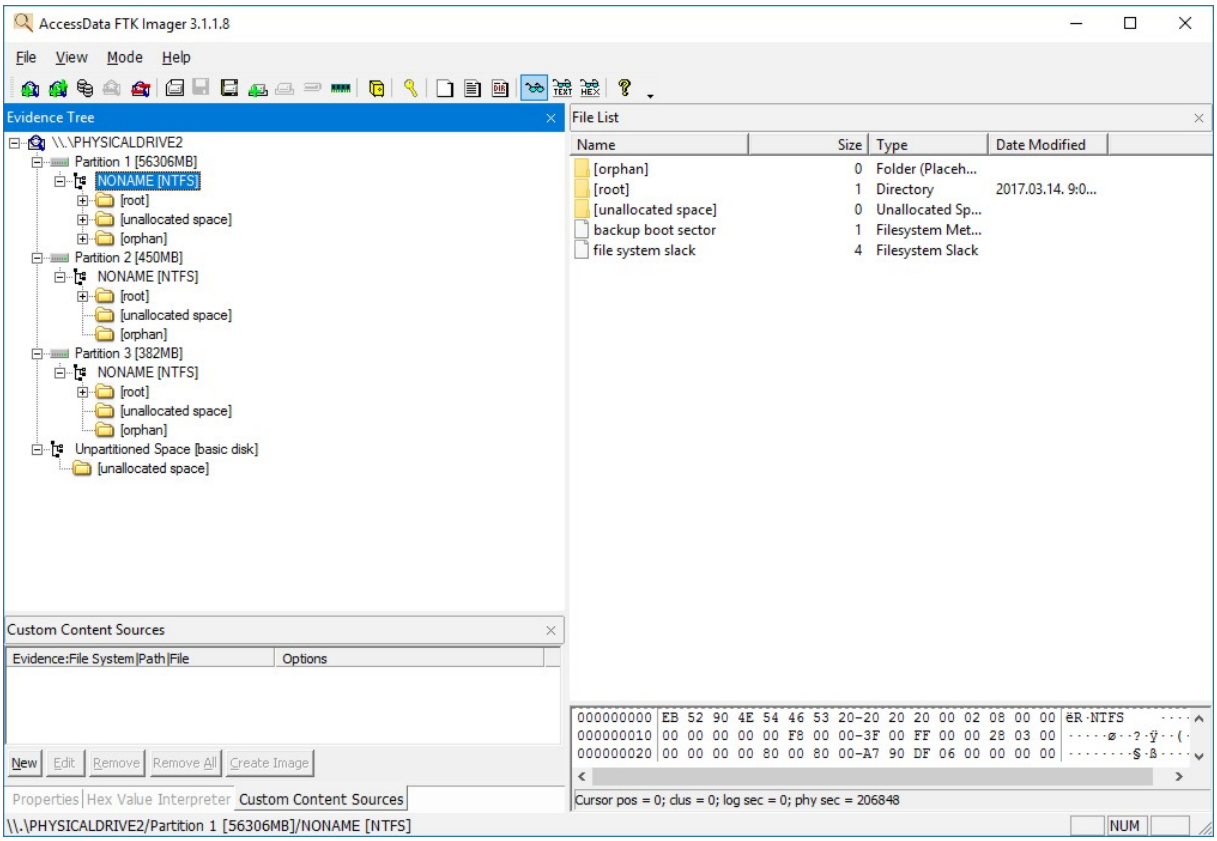


28. ábra – Adatforrás típusának kiválasztása

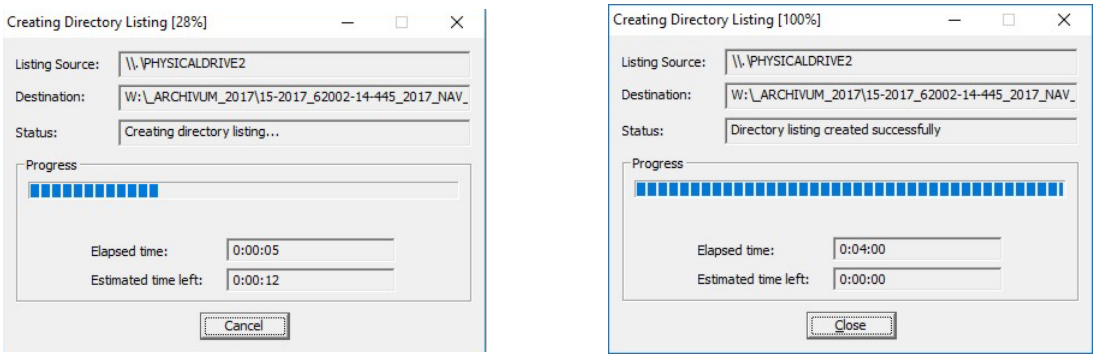


29. ábra - Fizikai lemez kiválasztása

[216] Forrás: https://www.guidancesoftware.com/tableau/hardware/t35u



30. ábra - Listázandó lemezterület (partíció) kiválasztása



31. ábra - Tartalomjegyzék készítése