Magyar Rendészet 2014/2. 29–38.

A bizonyítékok kezelése. Az igazságügyi informatikai szakértő a büntetőeljárásban

MÁTÉ István Zsolt

Az emberi tevékenység digitális nyomaival lépten-nyomon találkozhatunk a mindennapi életben. Ezek a nyomok a büntetőeljárásban dolgozó igazságügyi informatikai szakértő számára bizonyítékok – legtöbbször digitális bizonyítékok – lesznek. A bizonyítékok kezelése a felkutatás, összegyűjtés, megőrzés és bemutatás ideje alatt jelentősen befolyásolja a felhasználás sikerességét. Az írásban bemutatásra kerülnek a digitális bizonyítékok kezelésének legfontosabb követelményei és módszerei, valamint a hazai gyakorlatban jelentkező problémák egyaránt.

A technológia hatása

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 nyomozati szakában 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 teszik.

A bűnjeltől a digitális bizonyítékig

A büntetőeljárás során a nyomozó hatóság munkáját – a szakértői törvény (2005. évi XLVII. törvény) 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. §-a 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.[1] A jogszabály imént idézett részében definiált bűnjel válik majd a bizonyítás során legtöbbször tárgyi bizonyítási eszközzé, bizonyítékká.

A digitális bizonyíték

Mivel az előzőekben többször előkerült az elektronikus vagy digitális bizonyíték fogalma, szükséges meghatározni azt, mielőtt a kezelésével kapcsolatos eljárásokat taglalnánk. Elsőként a definíció hiányával szembesülünk, legalábbis jogszabályi szinten. A Be. rögzített adatról tesz említést a 115. § (2) bekezdésében, s ez utalhat az elektronikus vagy digitális tartalomra, de nincs ez másként a 28 U.S. Code Federal Rules of Evidence (Szövetségi Bizonyítási Szabályok Törvénykönyve) Rule 101. Scope, Definitions (hatály és meghatározások) részében sem, ahol az „electronically stored information" (elektronikusan tárolt információ) szövegrésszel találkozhatunk.

A pontos meghatározást a témakörrel tudományos igénnyel foglalkozó munkacsoportok szakmai anyagaiban találhatjuk meg:

„Information of probative value that is stored or transmitted in binary form"[2]

– azaz bizonyító erejű információk, melyeket bináris formában tároltak vagy továbbítottak.

„Information stored or transmitted in binary form that may be relied upon in court"[3]

– vagyis bináris formában tárolt vagy továbbított információ, melyre a bíróságon hivatkozni lehet.

A nemzetközi szervezet (IOCE – International Organization on Computer Evidence, avagy Számítógépes Bizonyítékok Nemzetközi Szervezete) és az USA-beli központtal működő társaság (SWGDE – Scientific Working Group on Digital Evidence, avagy Digitális Bizonyítékok Tudományos Munkacsoportja) egyaránt a bináris tárolásra helyezi a hangsúlyt, amely mellett a bíróságon történő felhasználhatóság is egyenrangú szempontként szerepel. Tremmel Flórián a törvényesség mellett erre is felhívja a figyelmet, amikor azt mondja, hogy „a büntetőeljárásban csak az adatforrás, méghozzá a törvényes adatforrás és az adat, mégpedig a büntetőjogilag releváns tényre vonatkozó adat együtt képez bizonyítékot."[4]

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

1 Ciardhuáin (2004) 6.
2 A Scientific Working Group on Digital Evidence definíciója.
3 Az International Organization on Computer Evidence definíciója.
4 Tremmel (2012) 14.

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[5] szakértői munka szempontjából releváns részei alapján vesszük sorra az elvégzendő tevékenységeket.

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 (szerver). Ezek nemcsak megjelenésükben, de egyéb jellemzőikben is eltérnek egymástól, így számos csoportosítási megközelítésre adnak módot.

Eogan Casey javaslata[6] szerint a következő típusokat különíthetjük el egymástól:

– *open computer systems (általános számítógéprendszerek)* – idetartoznak az asztali vagy hordozható számítógépek, kiszolgáló gépek;
– *communication systems (kommunikációs rendszerek)* – ezek közé sorolhatók a telefonrendszerek, a vezeték nélküli telekommunikáció, internet, hálózatok;
– *embedded computer systems (beágyazott számítógéprendszerek)* – ez jellemzően mobil eszközök, memóriakártyák, kép- és hangeszközök formájában jelenik meg.

Casey az egyes bizonyítéktípusokból az osztály- és egyéni jellemzők (class and individual characteristics) alapján von le következtetéseket, s ezt a cipőtalplenyomat példájával magyarázza, ahol a cipőtalplenyomat mérete az osztályjellemző, míg a talpfelület egyedi mintázata, sérülései révén létrejövő lenyomat az egyéni jellemző.[7] Brinson és társai a hagyományos informatikai megközelítéshez hasonlóan osztályozzák a cybercrime technológiai oldalát. A hardveroldalon:

– *Large Scale Digital Device – nagy léptékű digitális eszközök* (Grids, Clusters – elosztott számítási rendszerek, számítógépfürtök);
– *Small Scale Digital Device – kis léptékű digitális eszközök* (Cell Phones, PDAs, SSDD Software [sic!] – mobiltelefonok, kézi számítógépek vagy okostelefonok, kis léptékű eszközök szoftverei);
– *Computers – számítógépek* (Desktops, Laptops, Servers, Tablets – asztali számítógépek, hordozható számítógépek, kiszolgáló számítógépek, táblagépek);
– *Storage Devices – tárolóeszközök* (Thumb Drive, Digital Music Player, External Hard Drives – memóriakártyák és flash tárolók, digitális zenelejátszók, külső merevlemezek);
– *Obscure Devices – vegyes eszközök* (Gaming Devices, Recording Devices – játékkonzolok, video- és egyéb jelrögzítők).

5 Ciardhuáin uo. 6–7.
6 Casey (2011) 7–8.
7 Uo. 653.

A gyakorlat szempontjából egyik megközelítés sem ad kézzelfogható előnyt a szakértő vagy a nyomozó hatóság 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 azon műveleti sorrend formájában, melyet akár változékonysági rendnek (Order of Volatility) is nevezhetünk. Ez a sorrend Matthew Braid szerint a következő is lehet:[8]

1. táblázat: Order of Volatility

1. Registers and Cache – processzorregiszter 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 rendszermagmodulok tartalma	10. Network Topology – számítógépes hálózati összeköttetés-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 (szerver), mely a legtöbb digitális bizonyítékot tartalmazhatja, ugyanakkor távoli hozzáféréssel (LAN, WIFI, mobilhálózat stb.) manipulálható a tartalma (vö.: pénzdíjas szoftverletöltés infrastruktúrája). A felkutatás és azonosítás első számú objektuma ezért a kiszolgáló gép, megjegyezve, hogy komplex hálózati környezetben pszeudohálózatok 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.

8 Braid (2001) 6.

A tipikus eljárás az előzőek szerint, hogy minden online eszközt offline eszközzé kell alakítani (amennyiben ezt a felhatalmazás lehetővé teszi), oly módon, hogy megszüntetjük az eszközök közötti kapcsolatokat,[9] 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, amely 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 kartonlapok esetenként nem alkalmasak 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 házkutatásban részt vevő szakértő is alkalmazhat (alkalmaznia kell) egyedi azonosító jelzést.

Az ügyek egy részében a vizsgálat alá vont számítógépes rendszer jellege (pl. könyvelőiroda) vagy műszaki jellemzői (pl. internetszolgáltató szerverterme) miatt nincs lehetőség a komplett számítógépes rendszer lefoglalására és az azt követő laboratóriumi vizsgálatra. Amennyiben a szakértői kirendelés egy konkrét adatkör (pl. egy vagy több cég könyvelési adatai) megszerzésére vonatkozik, a szakértőnek – különös tekintettel a Be. 151. § (2) bekezdésében foglaltakra – a kérdéses adat célzott kinyerése a feladata.

A célzott adatkinyerés csaknem minden esetben házkutatás során történik, ezért nélkülözhetetlen az előzetes egyeztetés a nyomozó hatóság és a szakértő(k) között. Itt kell meghatározni a szakértői csoport létszámát, figyelemmel a helyszínek számára és a várható adatmennyiségre, illetve szakértői oldalról a művelethez felhasználandó speciális eszközökre. Ez utóbbiak közé sorolhatók a nagy sebességű helyszíni adattöbbszörözést biztosító eszközök (Forensic Duplicator, Forensic Write Blocker stb.), melyek különböző csatolófelületű (IDE, SATA, SCSI stb.) tárolókról képesek gyors, bithű másolatot készíteni. Ezeket az eszközöket a kikapcsolt (offline) rendszereknél vehetik igénybe a szakértők. Online, le nem kapcsolható rendszerekről történő mentés esetén a szoftveres megoldások (Forensic Toolkit, EnCase, Belkasof Evidence Center stb.) kerülhetnek előtérbe, melyekkel elsőként a vizsgált rendszeren található tartalmak digitális ujjlenyomatát (hash kód) rögzíthetik a szakértők, majd a kívánt tartalmak célzott mentése is megtörténhet.

Bizonyítékok összegyűjtése

A megjelölt eszközök összegyűjtése során a vizsgálatban részt vevő valamennyi munkatársnak ügyelnie kell az eredeti állapot megőrzésére. E tevékenység mottója a „Preserve everything but change nothing!" („Őrizz meg mindent, ne változtass semmin!")

9 Uo. 9.

lehet. Ezen követelmény 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 felügyelete alatt volt a bizonyíték, történt-e változás annak állapotában. Ez utóbbit a bizonyíték megfelelő csomagolása biztosíthatja. A lefoglalás szabályairól szóló rendelet 7. §-a rendelkezik a bűnjel (későbbi bizonyíték) csomagolásáról, s két lényeges követelményt támaszt: egyrészt a csomagolásnak (és megőrzésnek) olyannak kell lennie, hogy annak tartalma illetéktelen személy elől rejtve maradjon, másrészt a csomagolásra olyan anyagot kell felhasználni, amely megóvja a bűnjelet a károsodástól, és egyidejűleg megakadályozza azt is, hogy mérgezést vagy fertőzést okozzon.

A gyakorlatban 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 *„károsodástól megóvja"* követelményből fakadóan a szabványos kapcsolódási pontokhoz történő hozzáférés korlátozását is meg kell valósítani.

Az esetek jelentős részében a csomagolandó bűnjel asztali számítógép vagy ennél kisebb eszköz formájában kerül a nyomozó hatóság munkatársa és/vagy a szakértő elé. A számítógépek esetén a szemetes zsák plusz széles ragasztószalag a legelterjedtebb megoldás, mellette az eszköz előlapjának és hátlapjának A4-es 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 (ragasztófelület elenged), hogy a beavatkozástól a védőfelület leesik.

A jogszabályalkotók és/vagy a jogalkalmazók figyelmét mindenképpen érdemes felhívni arra a körülményre, amely a digitális bizonyítékká váló bűnjeleket megkülönbözteti az egyéb tárgyi bizonyítási eszközöktől és az okirati bizonyítéktól, mégpedig arra a körülményre, hogy a bizonyíték – jellegéből adódóan – közvetlenül akkor sem figyelhető meg, ha átlátszó csomagolásban van. A binárisan tárolt adat ugyanis – 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 bűnjelkezelő munkáját.

A számítógépnél kisebb méretű eszközök (pl. laptop, tablet, mobiltelefon stb.) esetén a csomagolás egyrészt egyszerűbb, másrészt rejtett problémát okozhat. Ennek veszélye különösen akkor áll fenn, ha az eszközt nem teljes egészében csomagoljuk be, ez a hordozható számítógépek (laptop, notebook, netbook, tablet) esetén tipikus. A csomagolás gyakran csak a vélt hozzáférési pontokat (elektromos csatlakozás, USB-, LAN-csatlakozók stb.) takarja el, és az eszköz hátlapján (alján) található, a tárolóeszközt burkoló felület rögzítőcsavarjait szabadon hagyja. 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 részt vevő állomány tagjait megfelelő szintű továbbképzéssel fel lehet készíteni. Ez Nelson és szerzőtársai szerint akár a következő is lehet:[10]

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

Bizonyítékok szállítása

A felkutatást és azonosítást, valamint a bizonyítékok összegyűjtését követően kerülhet sor – valamennyi lépés szigorú dokumentálása mellett (Chain of Custody) – a bizonyítékok elszállítására (a házkutatás helyszínéről a bűnjelraktárba). A szállítandó bűnjelek csomagolása ennél a lépésnél sérülhet meg, illetve a kisméretű eszközök fokozottan veszélyeztetettek. A szállítás esetén a digitális bizonyítékot tartalmazó bűnjeleket érdemes gyűjtőcsomagolásba 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 bűnjelraktára közötti mozgatás, illetve a bűnjelraktár és a szakértői telephely közötti szállítás. Ez utóbbi esetben a szakértőnek a tételes átvételt és a csomagolás sértetlenségének ellenőrzését már az átvétel helyszínén (a nyomozó hatóság bűnjelraktára/irodahelyisége) el kell végeznie. A dokumentálásra alkalmas bármely digitális fényképezőgép, mely képes legalább 3–5 megapixeles 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. a csomagolás vagy az eszköz sérülése) a későbbiekben a szakértői véleményben (amely 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 álló eszközök (pl. alvó üzemmódban lévő hordozható számítógép) növelhetik a szakér-

10 Nelson et al. (2004) 12.

tői 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 ezáltal illetéktelen kezekbe kerülhetnek. A mobiltelefonok és kézi számítógépek esetén az akkumulátoros tápellátás lehetővé teszi a tartalom esetleges módosulását, amely 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.

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 bűnjelraktárban 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, tételszám, 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.

Bizonyítékok vizsgálata

A bizonyítékok szakértői vizsgálata önmagában 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:[11]

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

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.

11 Braid uo. 5.

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 dokumentumállományát 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, ritkábban akár 3–4 év múltán is. A kérdés megnyugtató megválaszolásához az érintett szervezetek és szereplők szakmai egyeztetéssel és akár jogi eszközökkel történő szabályozására is szükség lehet.

Összefoglalás

A bűnjelek és a belőlük származó digitális bizonyítékok kezelése a büntetőeljárás jelentős tényezője. A bizonyítékok későbbi jogszerű és szakszerű felhasználásához a büntetőeljárásban részt vevő szervezetek és szereplők együttműködése és a jogszabályokban, valamint a szakmai protokollokban előírt követelményeknek a gyakorlatba történő átültetése szükséges. Az együttműködés hatékonyságának növelése célzott szakmai képzések és rendszeres szakmai tapasztalatcserék révén valósulhat meg, amikor a szlogenként gyakran emlegetett „best practices" valóban jó gyakorlatként épül be a mindennapi munkába.

IRODALOMJEGYZÉK

Braid, Matthew (2001): *Collecting Electronic Evidence After a System Compromise.* Brisbane, AusCERT.

Brezinski, D. – Killalea, T. (2002): *Guidelines for Evidence Collection and Archiving. The Internet Society.* Forrás: www.ietf.org/rfc/rfc3227.txt (2013. 11. 15.)

Casey, Ehogan (2011): *Digital Evidence and Computer Crime.* Amsterdam, Elsevier.

Ciardhuáin, Séamus Ó (2004): An Extended Model of Cybercrime Investigations. In: *International Journal of Digital Evidence,* Vol. 3. No. 1. 1–22.

International Organization on Computer Evidence (2000): *G8 Proposed Principles For The Procedures Relating To Digital Evidence.* Forrás: www.ioce.org/fileadmin/user_upload/2002/G8%20Proposed%20principles%20for%20forensic%20evidence.pdf (2013. 11. 2.)

Nelson, Bill – Phillips, Amelia – Enfinger, Frank – Steuart, Chris (2004): *Computer Forensics and Investigations.* Boston, Thomson Course Technology.

Scientific Working Groups on Digital Evidence and Imaging Technology (2013): *SWGDE and SWGIT Digital & Multimedia Evidence Glossary.* Forrás: www.swgde.org/documents (2013. 11. 2.)

Tremmel Flórián (2012): *Bizonyítékok a büntetőeljárásban.* Kivonat a Kriminalisztikai Szakirányú Továbbképzési Szak (KSzT) hallgatói részére. Budapest, Dialóg Campus. Forrás: www.herke.hu/kszt/tf.doc (2013. 11. 2.)

1998. évi XIX. törvény a büntetőeljárásról

2005. évi XLVII. törvény az igazságügyi szakértői tevékenységről

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
28 United States Code Federal Rules of Evidence

SUMMARY

Handling of Digital Evidence – IT Forensic Experts in Criminal Procedures
MÁTÉ István Zsolt

These days digital footprints of human activities can be met in everyday life. During criminal procedures these digital footprints are turned into digital evidence by forensic experts. Handling, collection, preservation and presentation of digital evidence can greatly influence the success of criminal procedures. In this paper we can see the most important requirements and methods of evidence handling as well as the challenges still present in the Hungarian practice.