DOI: 10.38146/BSZ.2018.7-8.2

GAÁL TIBOR

A digitális bizonyítékok jelentőségének növekedése a büntetőeljárásokban

A technológia emberre, illetve társadalomra gyakorolt hatása folyamatosan tetten érhető mindennapi életünkben. Tehát nem az a kérdés, hat-e ránk, hanem az, hogy hogyan. A XX. század közepétől fokozott érdeklődés mutatkozik a társadalomtudományok részéről ennek vizsgálatára. A legismertebb tudományos műhely a Torontói Egyetemen jött létre és Torontói Iskola néven vált ismertté. Jelesebb képviselői *Harold Innis, Marshall McLuhan, Joshua Meyrowitz, Neil Postman* és még folytathatnánk a sort. Közülük Innis volt az első, aki felhívta a figyelmet a technika társadalomra gyakorolt hatásaira[1]. A hatás mibenléte még nem tisztázott ugyan, de az mindenképpen megállapítható, hogy a technológia és azon belül a digitális/elektronikus szolgáltatások és eszközök használata mélyen beivódott a mindennapjainkba.

Elfogadva tehát a hatás tényét kimondhatjuk, hogy ennek nyomai megtalálhatók akkor is, amikor büntetőeljárást folytatunk, szinte függetlenül az eljárást kiváltó cselekmény típusától. Ez azt jelenti, hogy a büntetőeljárást végző nyomozók olyan digitális/elektronikus nyomokra bukkanhatnak munkájuk során, amiknek a felhasználásával, helyes értelmezésével az adott ügy megoldásához juthatnak el. Azonban ez a folyamat nem olyan egyszerű, s ez egyben új ismeretek, készségek, képességek elsajátítását, s nem utolsósorban – a digitális/elektronikus nyomok bizonyítékként történő felhasználását biztosító – új eljárások alkalmazását igényli a nyomozó hatóságok tagjai és a nyomozó hatósággal együttműködő szakértők és szaktanácsadók részéről is.

1 A Torontói Iskola egyik előzményeként vagy szellemi forrásaként tekinthetünk *Hajnal István*ra (1892–1956). A Széchenyi-díjas magyar történész, egyetemi tanár, az MTA tagja, a történelemtudományok doktora írástörténeti és technikatörténeti munkáiban a technikai változásokat a történelem egyik fontos alakítójának tekintette. Továbbá http://okt.ektf.hu/data/nadasia/file/tananyag/informaciotortenelem/29_04/432_harold _innis.html

A digitális bizonyíték fogalma

Hazai jogszabályi háttér

Ahhoz, hogy a digitális nyomból hogyan válik digitális bizonyíték, pontosan ismernünk kell a digitális bizonyíték fogalmát. Azonban a jogszabályaink nem definiálják pontosan, mit értünk digitális bizonyítékon. Tehát más módon kell meghatározni a fogalmát.

Nézzük először, hogy a magyar jogban hogyan definiáljuk a bizonyíték fogalmát! A büntetőeljárásról szóló 1998. évi XIX. törvény a bizonyítás általános szabályai között határozza meg a bizonyítás eszközeit.

A bizonyítás eszközei a 76. § (1) bekezdésében szerepelnek: *„A bizonyítás eszközei a tanúvallomás, a szakvélemény,* a tárgyi bizonyítási eszköz, *az okirat és a terhelt vallomása."*

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.*

(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."

A jogszabály szövege nem utal közvetlenül a digitális bizonyítékra, azonban minden olyan tárgy, amely *„… műszaki, vegyi vagy más eljárással adatokat rögzít…",* a digitális bizonyíték meghatározásának közvetett definíciója lehet. A hangsúly az adatrögzítésen van.

A jogszabály a 149. § (1) bekezdésében megnevezi az „információs rendszer"-t, bár annak tartalmát nem definiálja.

„A házkutatás a ház, lakás, egyéb helyiség, az azokhoz tartozó bekerített hely vagy a jármű átkutatása, továbbá az ott elhelyezett információs rendszer vagy ilyen rendszerben tárolt adatokat tartalmazó adathordozó átvizsgálása az eljárás eredményessége érdekében."

A 149. §-ban az adattárolási funkcióra helyeződik a hangsúly. Ez visszautal a tárgyi bizonyítási eszköznél írtakra, amely szerint az adatok rögzítése vagy rögzítettsége döntő motívum az ilyen jellegű bizonyítéktípus esetében.

A jogszabály azonban azt is kifejti, hogy a büntetőeljárásban csak olyan adatforrás, illetve törvényes adatforrás és adat képezhet bizonyítékot, amely büntetőjogilag releváns tényre vonatkozik.

Összegezve tehát elmondható, hogy a magyar szabályozás önállóan nem definiálja a digitális bizonyíték fogalmát, mindamellett biztos támpontként nevesíti az adatrögzítés mozzanatát, külön megemlítve az információs rendszert mint az adatrögzítési aktus eszközét.

Az új Be. a bizonyítás eszközeit a 165. §-ban sorolja fel.

„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

f) az elektronikus adat.”

Az f) pontban nevesített elektronikus adat pontosítását a jogszabály 205. §-ában találhatjuk meg.

„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.”

Az új büntetőeljárási törvény egyes digitális bizonyítékként használható adatok beszerzését már ügyészi engedélyhez köti. Ilyen például az elektronikus hírközlési szolgáltatóktól származó adat [262. § (1) bekezdés c) pont]. Ezzel a jogalkotó érzékelteti, hogy ez egy olyan digitálisbizonyíték-forrás, amely szenzitív adatokat tartalmaz.

Kitekintés az Amerikai Egyesült Államok jogszabályi hátterére

Hasonlóan a magyar joghoz a szövetségi szabályozás csak általános kereteket fogalmaz meg[2].

2 https://www.rulesofevidence.org/article-i/rule-101/

„101. szabály – hatókör; meghatározások

(6) egy hivatkozás bármilyen írásos anyagra, vagy más hordozóra, beleértve az elektronikusan tárolt információt is."[3]

Észrevehető, hogy a hangsúly az adatrögzítésre helyeződik, függetlenül attól, hogy azt milyen közvetítő eszközön tárolták. A szöveg csak utalást tesz az elektronikus tárolási formára, de a digitális bizonyíték kifejezést nem találjuk meg a jogszabály szövegében.

Az Amerikai Egyesült Államokban 1998-ban alakult meg a digitális bizonyítékokkal foglalkozó tudományos csoport *(Scientific Working Group on Digital Evidence; SWGDE)*. A csoport munkájának eredménye egy olyan szabványosítási folyamat, amely lehetővé teszi a digitális bizonyítékok egységes kezelését. A tudományos csoport szerint a digitális bizonyíték nem más, mint bizonyító erejű információk, amelyeket bináris formában tároltak, vagy továbbítottak[4].

Ebben a definícióban a hangsúlyt a bináris formában tárolt adatra helyezték. Nincs szó az adat tárolására szolgáló adathordozóról.

Azonban a szervezet nem feledkezik meg arról, hogy a digitális adat más, mint a legtöbb tárgyi bizonyíték, azaz legtöbbször nem kézzelfogható tárgyként van jelen, amelyet a nyomozó hatóság egyszerűen lefoglal, vagy egyéb korlátozó intézkedéssel gondoskodik eredeti állapotának megőrzéséről. A teljesség igénye nélkül elmondhatjuk, hogy a digitális bizonyíték korlátlan számban többszörözhető, méghozzá úgy, hogy közben nem változik a minősége. A digitális bizonyíték nem mindig található meg egyetlen fizikai helyen (például felhőalapú szolgáltatások). Az is előfordulhat, hogy a digitális bizonyíték nem egyben van, hanem darabokból állítható össze (például a merevlemezeken található kötetek egymástól elkülönülő könyvtáraiban tárolt részdokumentumok egymáshoz illesztésével). Ezek alapján a tudományos csoport más fogalmak bevezetését is indokoltnak tartotta, ilyen az eredeti digitális bizonyíték, a többszörözött digitális bizonyíték, vagy a másolat fogalma.

Egyéb amerikai szakirodalomban a digitális bizonyítékok másfajta jellegzetességére is felhívják a figyelmet. Ezek az osztályra és egyénre vonatkozó *(class characteristics, individual characteristics)* jellegzetességek[5]. Értelemszerűen az osztályjellemzők az információk csoportját vagy csoportjait, míg

3 Rule 101 – Scope; Definitions (6) a referencetoanykind of written material or any other medium includes electronically stored information.

4 Scientific Working Groupson Digital Evidence and Imaging Technology: SWGDE and SWGIT Digital & Multimedia Evidence Glossary. version: 2.7, SWGDE/SWGIT https://www.swgde.org/documents

5 Eoghan Casey: Digital Evidence and Computer Crime. Elsevier, Amsterdam, 2011

az egyénre vonatkozók magára az egyedre vonatkozó jellemzőket teszik a büntetőeljárásban definiálhatóvá. Utóbbi megközelítés rendszerszintű (adat és annak hordozója), míg az előbbi kizárólag adatorientált megközelítést mutat.

Utóbbi megközelítést példával szemléltetve egy papírra írógéppel készített dokumentum esetében a betűképzés módja az osztályjellemzőket (milyen írógéppel készült), míg annak a betűképzés során keletkezett hibái az írógép egyedi jellegzetességére utalhatnak (melyik írógéppel készült).

Ha ugyanez a dokumentum például Word szövegszerkesztővel készült dokumentumként áll rendelkezésre, akkor a dokumentumból kiolvasható, hogy milyen verziójú Worddel készült a dokumentum (osztályjelleg). Ha a dokumentumban egy olyan időpontra történik hivatkozás, amikor a dokumentum készítéséhez használt verzió még nem állt rendelkezésre (egyedi jelleg), akkor a dokumentum valódiságával kapcsolatban kétely ébredhet bennünk.

További példát tekintve egy adott hírközlési szolgáltató által hűségidővel eladott mobiltelefon a szolgáltató hálózatához van kötve (tehát nem hálózatfüggetlen), és hordozza annak összes tulajdonságait (osztálytulajdonság). Amikor egy szolgáltatást vesz igénybe a szolgáltató hálózatán, és kap például egy IP-címet, akkor már egyedi jellemzőket is hordoz, amelyek csak erre az egyetlen mobiltelefonra jellemzők (egyedi tulajdonság).

Casey a digitális bizonyítékokat három csoportba sorolja: számítógéprendszerek (szerverek, asztali és hordozható számítógépek és azok tartozékai), kommunikációs rendszerek (vezetékes telefon, wireless rendszerek, számítógépes hálózatok, internet stb.) és beágyazott számítógépes rendszerek (például GPS, mobiltelefon, videófelvevő stb.). Ezek a csoportok a gyakorlati tapasztalatokhoz jóval közelebb állnak, mint a digitális bizonyítékokkal foglalkozó tudományos csoport szervezet definíciói.

Összegezve elmondható, hogy a magyar jogszabályi háttér szinte megegyezik az amerikaival. Azonban a digitális bizonyíték kezelése, elemzése, vizsgálata tárgyában szinte semmilyen ajánlásunk, szabványunk nincs. Ez az idézi elő, hogy mind a nyomozó hatóságok, mind a szakértők, szaktanácsadók, vagy elemző-értékelők nehezen azonosítják, kezelik, vizsgálják, elemzik, értékelik a digitális bizonyítékokat. Ha megteszik azt – mivel különböző módszerekkel vizsgálódnak –, azok eredménye nehezen összehasonlítható. Az is elmondható, hogy a hatóságok alkalmazottai nem minden esetben vannak felkészülve a digitális bizonyítékok eljárásban történő felhasználására, illetve adott esetben megfelelő eszközeik sincsenek azok kezeléséhez.

A bűnjeltől a digitális bizonyítékig jutás folyamata

Természetesen a nyomozó hatóságok szakértőket és szaktanácsadókat, illetve szervezeten belül elemző-értékelőket vehetnek igénybe a digitális bizonyíték(ok) büntetőeljárásban történő sikeres felhasználásának érdekében. Azonban ehhez az említett szereplők sokkal szorosabb munkájára van szükség. A gyakorlatban jelenleg ez úgy zajlik, hogy a büntetőeljárásban azonosított lehetséges digitális bizonyítékot egy szakértő kirendelésével másolják le úgy, hogy annak eredetivel megegyezése bizonyítható legyen. Majd egy újabb szakértő (lehet a mentést elvégző is) kirendelésével, vagy egy elemző-értékelő felkérésével megkezdődhet az adatok elemzése, végezetül pedig következik az adatok értékelése. Az értékelés után döntés születik arról, hogy a lehetséges digitális bizonyíték törvényes digitális bizonyíték lehet-e. Ezt a döntést értelemszerűen a nyomozó hatóság, ügyészség, bíróság illetékese hozza meg.

Vizsgáljuk meg ezt a folyamatot lépésről lépésre! A büntetőeljárás során tehát a nyomozó hatóság munkáját az igazságügyi informatikai szakértő – ha tényállás megállapításához szakkérdés eldöntése szükséges (a Be. és a szakértői törvény alapján) –, vagy szaktanácsadó – a bizonyítási eszközök felkutatásának támogatása céljából (a Be. alapján) – segítheti.

Jellemzően tehát az informatikai szakértő vagy szaktanácsadó, esetleg elemző-értékelő – mint a nyomozó hatóság tagja, akinek speciális ismeretei vannak – a digitális bizonyítékok felkutatása, azonosítása során jut első körben szerephez, például házkutatáskor. 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" azonosítása, kiválasztása a legnehezebb feladat, különösen azért, mert a releváns eszköz, nyom azonosítása egy összetett környezetben nem egyszerű feladat. A jogszabály imént idézett részében definiált bűnjel válik majd a bizonyítás során legtöbbször tárgyi bizonyítási eszközzé, digitális bizonyítékká.

A digitális bizonyítékok kezelésének alapelvei

A szakértőnek tehát bináris adatokat kell keresnie egy tárolón, vagy bináris adatok átvitelének folyamatát kell megfigyelnie, rögzítenie. Jellemzően az

adatra fókuszálunk, de annak tárgyi megjelenését is keressük (például merevlemez, vagy hálózati kapcsolóeszköz[6]).

A digitális bizonyíték felkutatása és azonosítása

A bináris formában tárolt vagy továbbított adatok digitális eszközökön való megjelenése nagy változatosságot mutat (például a gépkocsi nyitásához használt, indítókulcsba szerelt RF-ID chip, személygépkocsi fedélzeti számítógépe, vagy internetszolgáltató kiszolgáló szervere stb.). A példaként felsoroltak nemcsak megjelenésükben, de egyéb jellemzőikben is lényegesen eltérhetnek egymástól. Így ezek csoportosítása többféleképpen is elvégezhető lenne.

A már említett Casey által javasolt digitálisbizonyíték-csoportok, vagy a *Brinson és társai* által javasolt osztályozások[7] sem igazán nyújtanak segítséget a nyomozó hatóság munkatársai vagy a szakértők számára.

Valamilyen tagolást mégis alkalmazni kellene. Amennyiben visszatérünk a definíciókhoz, és a gyakorlati szempontokat figyelembe véve próbáljuk a tagolást elvégezni, akkor online és offline eszközökről beszélhetünk. Az online eszköz olyan, amely más eszközökkel kapcsolatban áll(hat). A kapcsolatai révén az aktuális adattartalma módosul(hat). Mivel az offline eszközök nem állnak más eszközökkel kapcsolatban, így az adattartalmuk statikusnak tekinthető. A *Matthew Braid*-féle csoportosítás a következőkben foglalható össze[8]:

1. processzor regiszter és gyorsítótár-tartalmak *(Registers and Cache);*
2. számítógépes hálózatiútvonal-választó útvonaltáblája *(Routing Tables);*
3. címfeloldási protokoll gyorsítótára *(Arp Cache)* (az IP-címek és a fizikai címek megfeleltető táblázata);
4. a feladatok végrehajtási táblázata *(Process Table);*
5. operációs rendszer rendszermag-statisztika és rendszermag-modulok tartalma *(Kernel Statistics and Modules);*
6. operatív tár tartalma *(Main Memory);*

6 LAN switch, WAN router, bridge, set-top-box, IPTV vevőegység, gépjármű fedélzeti számítógép, SIM-kártyák stb.

7 Nagy mérettartományba eső eszközök; kis mérettartományba eső eszközök; számítógépek, mint asztali számítógépek, laptopok, kiszolgáló gépek és táblaszámítógépek; tárolóeszközök, mint elektronikus tárak, digitális zenelejátszók, külső merevlemezek; bizonytalan besorolású eszközök, mint játékgépek, felvevőeszközök.

8 Matthew Braid: Collecting Electronic Evidence After a System Compromise. AusCERT, Brisbane, 2001

7. ideiglenes fájlrendszer tartalma *(Temporary File Systems);*
8. másodlagos memória tartalma *(Secondary Memory);*
9. útvonalválasztó eszközök beállításai *(Router Configuration);*
10. számítógépes hálózati topológia *(Network Topology).*

Braid javaslata szerint a bizonyítékok felkutatásának és azonosításának a sorrendje mindig az aktuális helyszínre vagy esetre vonatkozó egyedi változékonysági sorrenden kell hogy alapuljon. A kritikus eszközök vagy rendszerek kerüljenek előre, míg a kevéssé változékonyak, azaz kevéssé kritikus eszközök a végére.

A gyakorlatban leggyakrabban a következő eszközök lefoglalására kerül sor: kiszolgálógép (szerver), asztali gép, laptop, HDD, pendrive, DVD, memóriakártya, SIM-kártya, mobiltelefon, okostelevízió, GPS navigációs eszköz.

Ezek közül a legváltozékonyabb rendszer a kiszolgálógép (szerver), amely funkciójánál fogva a legtöbb digitális bizonyítékkal kecsegtethet. Azonban ennek tartalma valamilyen távoli hozzáféréssel (LAN, wifi, mobil hálózat stb.) könnyen manipulálható[9].

Jól érzékelhető, hogy a legváltozékonyabb rendszer ellentéte a megváltoztathatatlan adattartalmú adathordozó (CD, DVD-R, egyszer írható CD-ROM). Ezek megkeresése, azonosítása a nyomozás későbbi szakaszában sem okozhat problémát.

Online eszközök esetében a bevett gyakorlat, hogy az online eszközt offline eszközzé kell tenni, természetesen ezt csak megfelelő felhatalmazás birtokában teheti meg a nyomozó hatóság. Ha megszüntettük az online eszköz lehetséges kapcsolódásait, elkezdhető a vizsgálata. Ha a kapcsolatok nem szüntethetők meg teljeskörűen, akkor a vizsgálatkori állapotot mindenképpen rögzíteni kell.

Ez után szükséges az eszközök nyomozó hatóság és/vagy szakértő általi dokumentált azonosítása. Ez jellemzően a bűnjelcímkék használatával történik meg. Ezen jól olvashatóan fel kell tüntetni a bizonyíték sorszámát úgy, hogy azt ne lehessen eltávolítani. Ugyanilyen fontos, hogy fel legyen tüntetve a lefoglalás helyszíne, időpontja. Ha nincs az eszköznek egyedi azonosítója, akkor a nyomozó hatóság munkatársának és/vagy a szakértőnek kell alkalmaznia valamilyen egyedi azonosítást lehetővé tevő jelzést.

9 15000/390/2015. Bü. Szabolcs-Szatmár-Bereg MRFK Btk. 360. §-ban indult nyomozás során végrehajtott feladatok.

A digitális bizonyítékok összegyűjtése

A bizonyítékok összegyűjtése során az egyik legfontosabb az eredeti állapot megőrzése. Ez azért nagyon fontos, mert az e követelménynek megfelelés szavatolja, hogy a későbbiekben megakadályozhassunk mindenféle beavatkozást, illetve ekkor kell megkezdeni azt a dokumentálási folyamatot, amely végigköveti és felügyeli a bizonyíték kezelésének teljes folyamatát. Ennek segítségével dokumentálttá válik, hogy a bizonyíték mikor, hol és kinek a kezelésében volt, azzal mi történt, illetve történt-e az állapotában bármilyen változás.

Lényeges mozzanat a bűnjelek (később bizonyítékok) csomagolása. A bűnjelet olyan módon kell becsomagolni és megőrizni, hogy annak tartalma illetéktelen személy előtt rejtve maradjon. Ez kétféle követelményt jelent. Egyrészt csomagolóanyagként olyan eszközt, anyagot kell alkalmazni, amely a bűnjelet megóvja a károsodástól, s egyúttal azt is megakadályozza, hogy mérgezést, fertőzést stb. okozzon. Másrészt olyan csomagolóanyagot kell választani, amely nem átlátszó, illetve megóvja a bűnjelet a lehetséges károsodástól.

A gyakorlatban legtöbbször asztali számítógép, laptop, vagy ezeknél kisebb eszközök lefoglalására kerül sor. A számítógépek csomagolására két módszert alkalmaznak. Az egyik legelterjedtebb a műanyag vagy papírzsák ragasztószalaggal körbetekerve. A másik a számítógép elő- és hátlapjának A4-es papírral történő fedése körberagasztva körcímkékkel. A körcímkéken szerepel a lefoglalást elszenvedő aláírása. Mind a két megoldás megfelel a jogszabályi előírásoknak, bár az első tartósabb lehet.

Felvetődik a kérdés, hogy például milyen csomagolásban foglalható le egy működő okostelefon, amelyről tudjuk, hogy PIN-kóddal védett, és a tulajdonosa a hatósággal nem működik együtt, tehát a kódot nem árulja el, illetve nincs mentőegységünk, hogy a pillanatnyi állapotát kimenthessük. Egy szemeteszsák széles ragasztóval körbetekerve nem látszik a legbiztosabb megoldásnak. A bekapcsolt állapotban lefoglalt telefon esetében gondoskodni kell arról, hogy az akkumulátora ne merüljön le addig, amíg vizsgálhatóvá, vagy menthetővé válik. Ehhez nagyobb teljesítményű akkumulátort kell a telefonhoz csatlakoztatni. Arról is gondoskodni kell továbbá, hogy online állapotából offline állapotba hozzuk és tartsuk annak érdekében, hogy annak tartalmát ne lehessen távolról megváltoztatni. Ehhez valamilyen árnyékolásra képes csomagolóanyagba, például alufóliába kell csomagolni a telefont és a csatlakoztatott akkumulátort. Ez után már jöhet a nem átlátszó műanyag vagy papírzsák

és a ragasztószalag. Természetesen a lefoglalást követően, ha lehet, azonnal szakértőhöz kell juttatni az eszközt, és annak tartalmát haladéktalanul ki kell menteni. A lefoglalás során nem árt, ha nemcsak a telefont foglaljuk le, hanem annak tartozékait is, legfőképpen a telefonhoz tartozó töltőt.

Alapesetben az eszközökben található akkumulátorokat ki kell szerelni, s azokat az eszközökkel együtt kell lefoglalni. Az alvó állapotban lefoglalt eszközök magukban hordozzák annak kockázatát, hogy azok például LAN-szkenneres módszerrel felderíthetők, és ennek következtében illetéktelenek felügyelete alá kerülhetnek.

A digitális bizonyítékokká váló bűnjelek esetében véleményünk szerint nem szükséges a nem átlátszó csomagolóanyag megkövetelése. Ennek oka, hogy a digitális bizonyítékká váló bűnjel más, mint egy okirati bizonyíték, vagy egyéb tárgyi bizonyítási eszköz, mert tartalma, amely bináris formában van tárolva, közvetítőeszköz, például egy másik számítógép nélkül nem figyelhető meg, és ezen az sem változtat, hogy a csomagolása átlátszó-e, vagy nem.

A nagyon kis méretű eszközök megtalálása, azonosítása még a lefoglalást elszenvedő személy együttműködése esetén is nehézséget okozat.

A digitális bizonyítékok szállítása

A házkutatás helyszínén felkutatott és azonosított, majd – szigorú dokumentálás mellett – összegyűjtött digitális bizonyítékokat bűnjelraktárba szállítják. A digitális bizonyíték ennél a fázisnál van a legjobban kitéve a sérülésnek, illetve a kis méretű bűnjelek fokozott figyelmet igényelnek. A kis méretű bűnjelek szállításához célszerű gyűjtőcsomagolást használni, amellyel megakadályozható mind a sérülés, mind az elvesztés, elkeveredés.

A szállításra és a bűnjelraktárba történő átadás tételes azonosítással kell hogy történjen.

A szállítás két tipikus útvonalon szokott megtörténni. Az egyik a házkutatás helyszíne és a nyomozó hatóság bűnjelraktára közötti mozgatás, míg a másik a bűnjelraktár és a szakértő telephelye vagy a hatóságnál dolgozó elemző-értékelő munkahelye közötti szállítás.

Utóbbi esetben a szakértő vagy az elemző-értékelő a bűnjelraktárból kiadással egyidejűleg el kell hogy végezze a tételes átvételt és a csomagolás sértetlenségének ellenőrzését. Ennek dokumentálása történhet egy közepes felbontási képességű (öt megapixel vagy ennél nagyobb) digitális fényképezőgéppel, de az átadás-átvétel teljes képi dokumentálása lenne a legjobb. Az

itt észlelt eltéréseket (például sérült eszköz, csomagolás sérülése stb.) a szakértő a szakvéleményében (ami bizonyítékként értékelendő), míg az elemző-értékelő az általa készített értékelőjelentésben szerepelteti (ez nem bizonyíték ugyan, de sok esetben elégségesnek tartják az ügyészségek, bíróságok).

A szállítás közben tilos felügyelet nélkül hagyni a szállított bűnjeleket!

A digitális bizonyítékok tárolása

A bűnjelraktárban történő tároláskor gondot okozhat, ha a lefoglaláskor elmulasztották megszüntetni az eszköz alvó állapotát, majd az akkumulátorát kiszerelni. Így előfordulhat, hogy a bűnjelraktárban csörögni kezd egy mobiltelefon, ami az egyéb gondokon túl azzal is jár, hogy ez esetben már nem garantálható a bizonyíték eredeti állapota.

A szakértőnél történő tárolás esetében a kiszerelt alkatrészek nagy száma (például HDD-k, CD-k, DVD-k stb.) okozhat keveredést, különösen akkor, ha párhuzamosan több ügyben is érintett eszközökről van szó. Így ezek azonosítása és nyomon követése nehézséget okozhat a szakértőknek, a sértetlenség és a változatlanul hagyás jogszabály által előírt követelményének azonban mindenképpen meg kell felelni.

A digitális bizonyítékok vizsgálata

A bizonyítékok vizsgálata jellemzően szakértőre, ritkábban a nyomozó hatóság elemző-értékelő munkatársára van bízva. Önmagában ez a szakasz jelentős része a büntetőeljárásnak, azon belül a bizonyítékok kezelésének.

Hosszan lehetne foglalkozni azzal az eszközrendszerrel, amelynek segítségével a szakértők, illetve a nyomozó hatóságok tagjai a digitális bizonyítékok vizsgálatát végzik, ettől azonban jelen írásban eltekintünk. A vizsgálattal kapcsolatos követelményeket csak címszavakban soroljuk fel. A vizsgálatot jellemzően az eredeti digitális bizonyíték másolatán kell végezni, biztosítva ezzel az eredeti bizonyíték minimális használatát; kötelezően dokumentálni kell minden változást; a bizonyításhoz nélkülözhetetlen szabályokat be kell tartani; tilos olyan dolgot vizsgálni, amelyre a vizsgálatot végző tudása nem terjed ki.

A digitális bizonyítékok vizsgálatát és belőlük digitális bizonyítékok szerzését jellemzően szakértők kirendelésével oldják meg a nyomozó hatóságok.

Ritkábban alkalmaznak erre a célra elemző-értékelő munkatársat. Ennek oka, hogy nem minden nyomozó hatóságnál vannak meg azok az eszközök, amelyekkel a digitális bizonyítékok az előírásoknak megfelelően vizsgálhatók lennének, továbbá nem minden nyomozó hatóságnál áll rendelkezésre olyan elemző-értékelő munkatárs, aki végzettségénél és képzettségénél fogva végezheti ezt a tevékenységet. Ezért a jelenlegi gyakorlat szerint az elemző-értékelő munkatársak a szakértők által megszerzett digitális bizonyítékok értelmezésénél és a konkrét ügyben történő felhasználhatóság eldöntésénél kapnak nagyobb szerepet.

A digitális bizonyíték vizsgálatának végeztével a szakértő vagy az elemző-értékelő munkatárs mind a bűnjeleket, mind az azokból megszerzett digitális bizonyítékokat átadja a kirendelőnek.

Nincs olyan norma, vagy ajánlás, hogy mi történjen a szakértő vagy az elemző-értékelő munkatárs számítógépén található digitális bizonyítékokkal. A gyakorlat azt mutatja, hogy a szakértők egy része töröl mindent, míg a másik része nem. Az utóbbi egy sor kérdést vet fel, például meddig őrizhető meg a tárolt digitális bizonyíték, ki viseli a tárolás költségeit, stb.

A nem egységes gyakorlat bizonytalanságát egyértelműsítené egy norma vagy ajánlás.

A digitális bizonyítékok elemzése

A digitális bizonyítékok megszerzése után – jelen gyakorlat alapján – jellemzően a szakértő átadja a bizonyítékokat a nyomozó hatóságnak. Ezt követően az esetek egy részében az ügygazdák, egy másik részében az elemző-értékelő munkatársak elemzik és értékelik a megszerzett digitális bizonyíték és a konkrét ügy kapcsolatát.

Ha a nyomozó hatóság érintett tagjainak nincs meg a megszerzett digitális bizonyíték értelmezéséhez szükséges szaktudásuk, akkor szintén sor kerülhet igazságügyi szakértő bevonására.

Az e folyamatban részt vevő igazságügyi szakértő, vagy az elemző-értékelő munkatárs szorosan együtt kell hogy működjön az ügy előadójával.

Azonban nem szabad elfeledkeznünk arról, hogy a digitális bizonyítékok nyomozó hatóság munkatársai által történő vizsgálata függ néhány alapvető tényezőtől. Az egyik ilyen a nyomozó hatóság munkatársainak informatikai felkészültsége, tudása. A másik a rendelkezésükre álló eszközök milyensége, míg a harmadik a vizsgálandó bizonyítékok mennyisége. Itt gondolnunk kell

az első és a második tényezőre, mégpedig arra, hogy az elemzés elvégzéséhez van-e megfelelő eszköz a nyomozó hatóság birtokában, illetve van-e megfelelő kompetenciával felruházott személy, aki az elemzést képes elvégezni. Ha több elemző-értékelő munkatárs igénybevételére van szükség, akkor utóbbi két tényező halmozottan jelentkezik, mégpedig: rendelkezésre áll-e több megfelelő eszköz, illetve minden elemző-értékelőnek, akinek a részvételét tervezik az elemzésben, van-e szükséges kompetenciája.

A rendőrségen több fejlesztés is történt az utóbbi években, így rendelkezésre állnak olyan eszközök és alkalmazások, amelyek szükségesek az elemzésekhez, sok mérnök, mérnök-informatikus, informatikus végzettségű elemző-értékelő munkatárs dolgozik már a nyomozó hatóságoknál, de ez mégsem mondható általánosnak. Azoknál a szervezeti egységeknél, amelyeknél egyik tényező esetében sem állnak rendelkezésre megfelelő erőforrások, továbbra is egyetlen megoldás az igazságügyi szakértők bevonása az elemzésekbe.

Összegzés

Kijelenthető, hogy a digitális bizonyítékok szerepe – bizonyos ügytípusoknál különösen – egyre nagyobb mértékű. Ennek okán szükséges lenne a jogszabályi keretek és ajánlások pontosabb megfogalmazása, illetve a büntetőeljárásban részt vevők megfelelő szintű képzése és megfelelő eszközökkel való ellátása.

FELHASZNÁLT IRODALOM

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

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. http://www.dfrws.org/2006/proceedings/5-Brinson.pdf

Casey, Eoghan: Digital Evidence and Computer Crime. Elsevier, Amsterdam, 2011

Kunos Imre: Bűnelemzés. Tanfolyami jegyzet. ORFK, Budapest, 1997

Máté István Zsolt: A multimédia technológiák kulturális hatásai. PTE BTK Kommunikáció és Médiatudományi Tanszék, Pécs, 2012

Máté István Zsolt: A digitális bűnfelderítés gyakorlata, avagy az igazságügyi informatikai szakértő a büntetőeljárásban. In: **Gaál Gyula – Hautzinger Zoltán (szerk.):** Tanulmányok „A változó rendészet aktuális kihívásai" című tudományos konferenciáról. Pécs, 2013 [Pécsi Határőr Tudományos Közlemények XIV.]

Máté István Zsolt: Az igazságügyi informatikai szakértő a büntetőeljárásban. Doktori értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2017

Tremmel Flórián – Fenyvesi Csaba: Kriminalisztika tankönyv és atlasz. Dialóg Campus, Budapest–Pécs, 2002

Tremmel Flórián: Bizonyítékok a büntetőeljárásban. Dialóg Campus. Budapest, 2012

JOGSZABÁLYOK

1978. évi IV. törvény a Büntető Törvénykönyvről

1998. évi XIX. törvény a büntetőeljárásról

13/2001. (X. 2.) ORFK Utasítás

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

9/2006. (II. 27.) IM rendelet az igazságügyi szakértői szakterületekről, valamint az azokhoz kapcsolódó képesítési és egyéb szakmai feltételekről

282/2007. (X. 26.) kormányrendelet a szakterületek ágazati követelményeiért felelős szervek kijelöléséről, valamint a meghatározott szakkérdésekben kizárólagosan eljáró és egyes szakterületeken szakvéleményt adó szervekről

31/2008. (XII. 31.) IRM rendelet az igazságügyi szakértői működésről

2012. évi C. törvény a Büntető Törvénykönyvről

2016. évi XXIX. törvény az igazságügyi szakértőkről

2017. évi XC. törvény a büntetőeljárásról