Az igazságügyi informatikai szakértő feladatai

Bevezetés

Az igazságügyi informatikai szakértő feladata a tudomány és a műszaki fejlődés eredményeinek felhasználásával az adott ügyben felmerülő szakkérdés eldöntése (2016. évi XXIX. törvény az igazságügyi szakértőkről [Szaktv.] 3. §), amely az igazságügyi szakértői nyilvántartásban bejegyzett szakterületei [9/2006. (II.27.) IM rendelet] valamelyikébe esik:

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

A szakértő a feladatot kirendelés alapján [Be. 189. § (1)] végzi. A szakértői vizsgálat tartalma szempontjából a kirendelő határozat központi eleme a szakértőhöz intézett kérdések vagy feladatok meghatározása, illetve a kirendelés indokolása. A kérdések és feladatok esetén a kirendelő az ügy szempontjából értékes adattípusok, információk vagy körülmények kinyerésére, azonosítására vonatkozóan rendelkezik, míg a kirendelés indokolásánál valamennyi lényeges körülményt megadja a szakértő részére, amely a vizsgálat elvégzéséhez szükséges. A kérdések és feladatok, valamint az indokolásban szerepeltetendő körülmények részleteit az egyes vizsgálattípusoknál tárgyaljuk részletesen.

A szakértő a kirendelő határozat alapján elkészített igazságügyi informatikai szakértői véleményben foglalja össze a vizsgált informatikai szakkérdésre vonatkozó megállapításait. Amennyiben a kirendelő eldöntendő kérdéseket tett fel, úgy az ezekre vonatkozó válasz a szakértői vélemény szövegében található, abban az esetben, ha valamely körülményre, állapotra vonatkozó kérdések szerepeltek a kirendelésben, úgy az ezekre vonatkozó adatok jellemzően a szakértői vélemény elektronikus/digitális mellékletén találhatók. Az eldöntendő kérdésre adott válaszok közvetlenül felhasználhatók, míg a körülményre, állapotra vonatkozók további elemzést és értékelést tehetnek szükségessé, különösen nagy mennyiségű forrásadat esetén.

https://doi.org/10.36250/01004_10

Az igazságügyi informatikai szakértő munkája a szakértői vélemény átadásakor részben lezárul, abban az esetben, ha a szakértői vélemény tartalma valamilyen körülmény [Be. 197. § (1)] miatt nem értelmezhető, úgy a szakértői vélemény kiegészítése kérhető.

A fenti tevékenység elvégzése az igazságügyi informatikai szakértő részéről több elkülönült tevékenységből áll, amelyek informatikai szakmai részleteiről és a büntetőeljárással összefüggő kapcsolatairól a következő alfejezetekben esik szó. A további szövegben a magyar nyelvű terminológia mellett – az angol nyelvű szakirodalom későbbi könnyebb használata érdekében – megadjuk az angol szakkifejezéseket is.

Az elektronikus adatok forrásai

Az elektronikus adatok önmagukban nem állnak rendelkezésre, azokat valamilyen információs rendszer tartalmazza (tárolórendszer hordozza). Az információs rendszerek technológiai nézőpontból tekinthetők tisztán hardver- vagy tisztán szoftverrendszernek. A gyakorlatban általában a két komponenst különböző mértékben tartalmazó komplex rendszerekkel találkozhatunk, amelyek közül a leggyakoribbak az alábbiak:[108]

Számítógépek, különösen:
- kiszolgáló számítógép *(server),*
- asztali számítógép *(desktop computer),*
- hordozható számítógép *(laptop, notebook computer),*
- táblaszámítógép *(tablet).*

Tárolóeszközök, különösen:
- memóriakártyák,
- USB-kulcsok,
- külső csatlakoztatású tárak *(external HDD, SSD),*
- hálózatra csatolt tárak *(network attached storage).*

[108] Ashley Brinson – Abigail Robinson – Marcus Rogers: A *cyber forensics ontology: Creating a new approach to studying cyber forensics*. *Digital Investigation,* (2006), 3. 37–43.

Kis mérettartományú digitális eszközök, különösen:
- mobiltelefonok *(featurephone),*
- okostelefonok *(smartphone),*
- egyéb kommunikációs és kiegészítő eszközök (SIM-, memóriakártya).

Nagy mérettartományú digitális eszközrendszerek, különösen:
- számítógépfürt *(computer cluster),*
- számítási rácsok *(computer grid),*
- felhőszolgáltatások *(cloudcomputing)*
- infrastruktúra-szolgáltatás (IaaS),
  - platformszolgáltatás (PaaS),
  - szoftverszolgáltatás (SaaS).

Egyéb eszközök, különösen:
- játékgépek (PlayStation, Xbox stb.),
- tartalomrögzítők (DVR),
- mágnesszalagos archiválórendszerek.

Az elektronikus adatokból megismerhető információk típusai

Az egyes adathordozókról kinyert elektronikus adatok információtartalma esetről esetre változó, azonban az egyes adathordozó-típusokon megtalálható információk fajtái az adott eszköz használati módjainak ismerete és tapasztalati adatok alapján előre jelezhetők. A szakértői vizsgálat alá vont adathordozók legnagyobb mennyiségét kitevő mobilkommunikációs eszközök és a tárolók (együttesen a vizsgált eszközök több mint 80%-át teszik ki) vonatkozásában a jellemző információtípusok az alábbiak.[109]

Univerzális integrált áramköri kártya:
- nemzetközi mobilelőfizető-azonosító – (*international mobile subscriber identity* – IMSI) – maximálisan 15 számjegyből áll
  - országkód (*mobile country code* – MCC), 3 számjegy
  - hálózatkód (*mobile network code* – MNC), 2 vagy 3 számjegy
  - előfizető azonosító (*mobile subscriber identification number* – MSIN)
- gyorstárcsázás hívószámai (*abbreviated dialing numbers* – ADN),

[109] Ehogan Casey: *Digital evidence and computer crime.* Amsterdam, Elsevier, 2011. 37.

- legutóbb tárcsázott hívószámok (*last numbers dialed* – LND),
- egyszerű szöveges üzenetek (*short message service* – SMS),
- egyszerű multimédia-üzenetek (*enhanced messaging service* – EMS),
- bejövő hívások adatai (*EF incoming call information* – EF ICI),
- kimenő hívások adatai (EF *outcoming call information* – EF OCI).

Funkcionális mobiltelefon *(featurephone):*
- telefonkönyv-bejegyzések,
- híváslisták,
- naptárbejegyzések,
- jegyzetek,
- digitális fényképek,
- digitális hangfelvételek,
- digitális videófelvételek,
- egyéb készülékspecifikus adatok.

Okostelefon *(smartphone):*
- telefonkönyv-bejegyzések,
- híváslisták,
- naptárbejegyzések,
- jegyzetek,
- digitális fényképek,
- digitális hangfelvételek,
- digitális videófelvételek,
- internethasználattal kapcsolatos adatok,
  - böngészési előzmények,
  - elektronikus levelezés,
  - azonnali üzenetküldő programok használatával kapcsolatos adatok,
  - letöltött fájlok és dokumentumok,
- GPS-adatok,
- vásárlási adatok,
- pénzügyi adatok,
- egyéb készülék- és/vagy szolgáltatásspecifikus adatok,
- telepített alkalmazások által tárolt egyedi formátumú adatok.

Táblagépek:
- okostelefonokkal azonos adatkörök,
- számítógép-specifikus adatok.

Memóriakártya:
- funkcionális mobiltelefonokkal azonos adatkörök,
- okostelefonokkal azonos adatkörök,
- számítógép-specifikus adatok.

Merevlemezes adattárolók:
- beépített adattárolók,
  - felhasználói adatok, különösen
    - internethasználat adatai,
    - kommunikációs adatok (levelezés, azonnali üzenetküldés stb.),
    - mobiltelefonok biztonsági mentései,
  - működtető rendszer adatai, különösen
    - telepítés ideje,
    - felhasználók adatai,
    - telepített alkalmazások adatai,
    - fájlrendszer adatai,
    - a rendszer hardver- és szoftverkomponenseinek adatai,
    - a rendszer használati eseményeinek adatai,
- külső csatlakozású adattárolók, különösen
  - archivált adatok (dokumentumok, digitális képek, videók, hangfelvételek),
  - mobiltelefonok biztonsági mentései,
- nagy tárolókapacitású hálózati adattárolók (SAN, NAS), különösen
  - archivált adatok (dokumentumok, digitális képek, videók, hangfelvételek),
  - napi használat adatai (dokumentumok, elektronikus levelezés, digitális képek, videók, hangfelvételek).

Szilárdtest adattárolók:
- felhasználói adatok, különösen
  - internethasználat adatai,
  - kommunikációs adatok (levelezés, azonnali üzenetküldés stb.),
- működtető rendszer adatai, különösen
  - telepítés ideje,

- felhasználók adatai,
- telepített alkalmazások adatai,
- fájlrendszer adatai,
- a rendszer hardver- és szoftverkomponenseinek adatai,
- a rendszer használati eseményeinek adatai.

Memóriakártyák, USB-kulcsok:
- mobiltelefonok működési adatai,
- mobiltelefonok biztonsági mentései,
- felhasználói adatok (különösen digitális fényképek, videók, hangfelvételek, dokumentumok).

Optikai adathordozók:
- telepítőkészletek,
- archivált felhasználói adatok (különösen digitális fényképek, videók, hangfelvételek, dokumentumok).

A kibernyomozói és szakértői munka kapcsolata

A tématerülettel foglalkozó szakirodalom és nemzetközi szabványok az alcímben írt kapcsolatot két fő nézőpontból tárgyalják, egyrészt a munkafolyamatok osztályozása, másrészt a tevékenységek meghatározása révén.

A fő munkafolyamatok azok, amelyekben a kibernyomozó és a szakértő önállóan vagy együtt vesz részt, de mindenképpen egymás munkáját befolyásolva. A munkafolyamatok tipikusan sorfolytonosan követik egymást, míg a folyamaton belüli tevékenységek egymással egy időben is végezhetők.

Készenlét

A készenlét *(readiness)* elsősorban azokat a szervezeten (a nyomozó hatóság és a szakértői intézmény) belüli tevékenységeket foglalja össze, amelyek a következő szakaszokban beszerzendő bizonyítási eszközök – különösen az elektronikus adatok *(potential digital evidence, digital evidence)* – felhasználhatóságával, a költséghatékony és folyamatos működéssel, valamint az információbiztonsággal kapcsolatosak.

Ezek közül kiemelendő a kibernyomozók és szakértők rendszeres képzése és továbbképzése, a korábbi esetek feldolgozása és tipizálása, az egységes módszertanok, eszközkészletek használatának bevezetése és az egyes tevékenységi csoportokat végző egységek közötti eszköz- és információforgalmi kapcsolatok kialakítása és fenntartása. Ennek érdekében két alaptevékenységet kell végrehajtani, a tervezést és a felkészülést.

Tervezés

A tervezés *(plan)* fázisában kerül sor a vizsgálati folyamat során alkalmazandó módszerek és eljárások kidolgozására és meghatározására az alábbi területeken:

- elektronikus adatok lehetséges tárolóeszközeinek azonosítása,
- összegyűjtése,
- megóvása a külső behatásoktól,
- elektronikus adat kinyerése, megszerzése (amennyiben szükséges),
- elektronikus adatok lehetséges tárolóeszközeinek szállítása,
- tárolása.

Ekkor kell megtervezni a részt vevő személyek felkészültségi szintjének mérését és az ismeretek, készségek szinten tartásának lejárásait is.

Felkészülés

A felkészülés *(prepare)* során be kell gyakorolni a felhasználandó eszközök – különösen a hardver- és szoftverkomponensek – készségszintű használatát oly módon, hogy azok alkalmazása a kijelölt módszerekkel és eljárásokkal együttesen történjen.

- A potenciálisan elektronikus adatot vagy ahhoz kapcsolódó kiegészítő információkat tartalmazó digitális eszközök és analóg információhordozók felismerésének, összegyűjtésének, megóvásának, szállításának és tárolásának begyakorlása, különös tekintettel a rejtett funkcionalitású eszközökre és a kiemelt darabszámban előforduló (mobilkommunikációs és tároló-) eszközökre vonatkozóan.
- Alapvető és eszköz- (hardver- és szoftver-) specifikus ismeretek begyakorlása és számonkérése.

Folyamatindítás

A vizsgálandó esemény bekövetkezése, pontosabban annak észlelése megnyitja *(initialization)* a vizsgálati eljárás aktív szakaszát.

Észlelés

Az észleléskor *(incident detection)* kerül sor az eseménnyel érintett információs rendszer elsődleges azonosítására. Az észlelés tipikus forrásai a következők:

- az adott rendszert megfigyelő, üzemeltető személyek bejelentése,
- behatolásérzékelő rendszer (*intrusion detection system* – IDS) jelzése,
- behatolásmegelőző rendszer (*intrusion prevention system* – IPS) jelzése,
- naplóelemző rendszerek *(log-analysing system)* riasztási adatai,
- változáskövető rendszerek *(change tracking system)* riasztási adatai,
- egyéb.

Az észlelést követően a bejelentési adatok alapján közvetlenül meg kell határozni az esemény elsődleges tartalmát egy osztályozási (besorolási) folyamat révén. Ennek során azonosítani kell az esemény típusát – például különleges személyes adatokkal történő visszaélés, gyermekpornográfia, költségvetési csalás stb. –, amely alapján a vizsgálat várható iránya (például milyen típusú eszközökön valószínűsíthető az adott cselekményhez kapcsolódó elektronikus adat jelenléte). Az osztályba sorolást oly módon kell elvégezni, hogy az ne változtassa meg a feltételezhetően elektronikus adatot tartalmazó információs rendszer állapotát, vagyis a vizsgálat ezen szakaszában a cselekménnyel érintett információs rendszereken elemző szoftver még nem futtatható (megváltoztatná a rendszer állapotát).[110]

Reagálás

Az észlelést követően a reagálás *(respond)* során a rendelkezésre álló adatok és az elvégzett osztályba sorolás információi alapján meg kell kezdeni a feltételezhetően releváns elektronikus adatokat tartalmazó eszközök felmérését,

[110] ISO/IEC 27043:2015, 14–15.

azonosítását, az esetleges kockázatok elhárítását vagy csökkentését. Ennek keretében kerülhet sor egy adott eszköz számítógépes hálózatról történő leválasztására vagy a kapcsolat fenntartására:

– amennyiben a releváns elektronikus adat feltételezhetően a helyi információs rendszeren található, úgy a számítógépes hálózati kapcsolat megszüntetendő a távoli hozzáférésből adódó adatmódosulás megakadályozása érdekében;
– ugyanakkor ha a releváns elektronikus adat feltételezhetően a távoli információs rendszeren található (például távoli asztal kapcsolat, bejelentkezett állapotú felhőszolgáltatás stb.), úgy a kapcsolat nem szakítható meg, illetve azonnal meg kell kezdeni a feltételezhetően releváns elektronikus adatok megszerzését.

Az egyes műveletek végrehajtása során különös figyelmet kell fordítani az elektronikus adatok, illetve az azokat tartalmazó eszközök sértetlensége megőrzésének. Ennek érdekében mérlegelni kell az élő rendszerekkel kapcsolatos tevékenységeket, úgymint a működő információs rendszer leállítása, adatok megnyitása szerkesztésre stb.[111]

Megszerzési folyamatok

Az észlelést és reagálást követően kerülhet sor a potenciálisan releváns elektronikus adatok megszerzésére *(acquisitive process),* amely az elektronikus adatok hordozóinak felismerésétől és azonosításától kezdődően az elektronikus adatok megszerzéséig tart, s magában foglalja a hordozóeszközök összegyűjtését és megóvását is. A továbbiakban – terjedelmi okokból – a leggyakoribb eszköztípusokra vonatkozó eljárásokat tekintjük át.[112]

Felismerés és azonosítás

Az elektronikus adatokat tartalmazó eszközök általában – különösen a nagy mérettartományba eső berendezések esetén – jól azonosíthatók, elhelyezkedésük

[111] ISO/IEC 27043:2015, 15.
[112] ISO/IEC 27043:2015, 15.

a használat általános módjából adódóan előre jelezhető. A méret, a használati hely és a működési jellemzők alapján az egyes eszköztípusok felismerése és azonosítása *(identify)* az alábbiak szerint történik:

Számítógépek

Az általánosan használt asztali (álló vagy fekvő kivitelben) számítógépek a 60 × 30 × 60 cm és 32 × 10 × 32 cm (magasság × szélesség × hosszúság) mérettartományba esnek, tömegük jellemzően 1–15 kg közé esik, színük korábban világosszürke, napjainkban inkább fekete, alakjuk általában téglatest.

Egyes készülékek azonban jelentősen eltérhetnek a fenti általános értékektől, így a szélsőségesen kis mérettartományú (*ultra small formfactor* – USFF) eszközök mérete 18 × 6 × 18 cm is lehet, illetve az egy áramköri lapból álló eszközök (például Raspberry Pi) akár 6 × 3 cm méretű és 7 gramm tömegű formában is megjelenhetnek. A kisebb méretű eszközök potenciális adattartalma a lehetséges tárolóeszközök kis fizikai mérete miatt közel azonos lehet a „normál" méretű számítógépek adattartalmával.

A különleges kialakítású számítógéptípusoknál – mint az All-in-One PC-é és az iMac számítógépek – a számítógép vezérlő- és tárolóegységei a kijelzővel azonos modulban helyezkednek el, így megjelenésük alapján könnyen összetéveszthetők egy önálló kijelzővel. Méretük (a képernyő átlóját figyelembe véve) általában 23–27 hüvelyk (58–68 cm) közötti.

Az átlagnál nagyobb méretű és tömegű eszközök jellemzően a játékgépek *(gamer computer)* és a kiszolgáló gépek *(server computer)* közül kerülnek ki. A nagyobb számítási teljesítmény mellett ezekben az eszközökben több tároló is elhelyezkedhet, illetve a kiszolgáló számítógépek esetén távoli kapcsolódások is gyakoriak. Míg a gamer számítógépek megjelenése gyakran extravagáns (a formát és a színt is beleértve), addig a server számítógépek tipikusan *tower* (torony), *blade* (keskeny álló kivitel) vagy *rackmount* (keskeny fekvő kivitel) elrendezésűek.

A hordozható számítógépek vezérlő- és tárolóegységei és a kijelző (az all-in-one eszközökhöz hasonlóan) egybeépített, ezeknél azonban két különálló modulként (amelyeket esetenként külön is lehet választani) kerülnek kivitelezésre. Méretüket a képátló nagyságával szemléltetve az eszközkategória a 7 hüvelytől (netbook, 2in1 tablet) a 10,6 és 16,4 hüvelyk közötti (minilaptop, laptop, notebook) eszközökön át az akár 18,4 hüvelykes képátlójú multimédia vagy gamer

laptopokig terjed. Vastagságuk az 10 mm-től az 52 mm-ig terjed, az előbbiek az ultravékony eszközök közül, míg az az utóbbiak az ütésálló kivitelű készülékek közül kerülnek ki.

A számítógépek többnyire – a kiszolgálógép kivételével – személyhez kapcsolódó berendezések, ezért az elhelyezkedésük is ennek megfelelő. Gyakori a fali vagy padlóba süllyesztett elektromos csatlakozók közelében történő elhelyezés, valamint a vezetékes számítógépes hálózati kapcsolat is. Ez utóbbi nyomvonalának végigkövetése (kábelek vagy kábelcsatornák) lehetővé teszik a nem tipikus helyen elhelyezett eszközök azonosítását is. A kiszolgálógépek fizikai elhelyezkedése (helyben) általában kis méretű, hűtött, zárt helyiségben történik, vagy távoli helyszínen (adatközpont, fizikai- vagy virtuálisszerver-bérlet, felhőinfrastruktúra-szolgáltatás stb.).

A számítógépek egyedi azonosítása a gyári számmal *(serial number)* történik, ennek hiányában az operációs rendszer licenckódja (amennyiben van ilyen) is használható. A gyártófüggetlen eszközök esetében leíró típusú azonosító alkalmazható, amely egy egyedi sorszámot és az adott helyszín, helyiség és eszköz megnevezését tartalmazza.[113]

Tárolóeszközök

A tárolók a kis méretskálájú eszközök közé tartoznak fizikai méretük alapján. Az eszközökön tárolható elektronikus adatok tekintetében azonban rendkívül széles spektrumot mutatnak.

Méret és adattartalom tekintetében a SIM-kártyák a legkisebb tárolók közé tartoznak, amelyek nano (12,3 × 8,8 mm), micro (15 × 12 mm) és standard (25 × 15 mm) kivitelben és 128–256 KB adattároló kapacitással érhetők el. Önállóan kevésbé fordulnak elő, általában valamilyen mobilkommunikációra képes eszközbe behelyezve vagy abban végleges módon rögzítve lelhetők fel, különösen mobiltelefonokban, táblaszámítógépekben, laptopokban. A SIM-kártyák felismerésekor a hozzáférési adatok (mint PIN-kódok és PUK-kódok) megszerzésére is kísérletet kell tenni a bankkártyaméretű (54 × 85,6 mm) kódkártyák vagy a potenciális kódokat tartalmazó jegyzetek felkutatásával. A SIM-kártyák egyedi azonosítása az ICCID (*integrated circuit card identifier,* integrált

[113] Gárdonyi Gergely – Anti Csaba László: *Krimináltechnikai kézikönyv.* Budapest, Semmelweis, 2020. 229–238.

áramköri kártyaazonosító) által történik, amelynek számsorozata a kártya felületén olvasható, illetve elektronikusan kiolvasható az eszközről.

A memóriakártyák a tárolókapacitás tekintetében mutatnak széles spektrumot: míg a 2000. év előtti gyártású kártyák leggyakoribb tárolókapacitása 2–128 MB közé esett, addig napjainkban a 16–32–128 GB kapacitású tárolók az elterjedtek. Méretük a PCMCI-kártyák 85,6 × 54 mm-es méretétől a micro-SD-kártyák 15 × 11 mm-es méretéig terjed általában. A kártyatípusok közül napjainkban a *secure digital card* (SD card) tartozik a legelterjedtebbek közé, standard (32 × 24 mm), mini (21,5 × 20 mm) és a korábban már említett mikro méretkivitelben. A memóriakártyák általában eltávolítható tárolók, de egyes esetekben (például drónokban) a végleges (ragasztott) rögzítés is előfordul. A mikroméretű tárolók alkalmasak rejtett funkciójú (például óraként, tollként, kulcstartóként azonosítható) eszközökben történő elhelyezésre, ezért felismerésük esetenként rendkívüli körültekintést igényel.

A nagy kapacitású külső tárak *(external drive)* az adatok archiválására és hordozására is alkalmas eszközök. Alaphelyzetben a tárak tokozása (védőburkolata) a beépített tároló méretét követi, így 3,5 hüvelykes – asztali számítógépekben alkalmazott – tárak 146,99 × 101,85 mm-e, a 2,5 hüvelykes – hordozható számítógépekben alkalmazott – tárak 100 × 69,85 mm-es méretéhez közelítenek. Az asztali kivitelű tárolók kevésbé, míg a hordozható és ütésálló eszközök erősebben robusztus kivitelűek.

Asztali kivitelű és hálózatra csatolt tárak (*network attached storage* – NAS) esetén több merevelemez (leginkább 3,5 hüvelykes méretű) is elhelyezkedhet a tokozásban vagy eszközházban, így annak mérete is ehhez alkalmazkodik.

A tárolók rendszerint egyedi gyártási számmal rendelkeznek, így megkülönböztetésükhöz ez használható, vagy ennek hiányában a számítógépeknél ismertetett egyedi azonosítási módszer szerint lehet eljárni.[114]

Mobilkommunikációs eszközök és táblagépek

A hagyományos és okostelefonok mellett itt tárgyaljuk a táblaszámítógépek felismerését és azonosítását is, elsősorban a nagy mértékű eszköz és funkcionális hasonlóság miatt.

[114] Vö. Gárdonyi – Anti (2020): i. m. 229–238.

A készülékek mérete a mini (68 × 28 × 12 mm – L8Star BM10) mérettől a normál funkcionális méreten (104 × 44 × 16,3 mm – Samsung B100) és a normál okostelefon-méreten át (146,2 × 70,9 × 8,3 mm – Samsung Galaxy A1) a tabletek (254 × 167 × 6,1 mm – Sony Xperia Z4 Tablet LTE) mérettartományáig terjed. Az eszközök felismerését nehezítheti a szokásos készülékkülalaktól történő jelentős eltérés (cigarettásdoboz, toll vagy műanyag figura kivitelű eszközök), amely esetén az adott területen végzett elektromágneses hullámelemzéssel (élő mobilwifi, Bluetooth-kapcsolatok) lehetséges a bekapcsolt működő eszközök azonosítása. Kikapcsolt készülékek esetén a ferromágneses detektorok alkalmazása ajánlott.

A mobilkommunikációs eszközök gyakran tartalmaznak kivehető másodlagos tárat (memóriakártya), illetve SIM-kártyát. Ezek kezelésekor és azonosításakor minden esetben rögzíteni kell az eszközök kapcsolatát (mely készülékben volt eredetileg a tároló vagy a SIM).

A mobilkommunikációs eszközök egyedi gyári azonosítóval rendelkeznek, amely a készülékház külső burkolatán, illetve a készülékház belső felületén elhelyezett címkén olvasható. Eltávolított azonosító esetén az adat elektronikusan kiolvasható vagy a számítógépeknél ismertetett egyedi azonosítási módszer szerint lehet eljárni.

Egyéb eszközök

A fentiektől eltérő eszközök felismerésekor és azonosításuk esetén a korábban ismertetett általános eljárásokat kell alkalmazni, figyelembe véve az adott eszköztípus sajátosságait is. Így például drón azonosítása esetén a kivehető memóriakártyát a tárolóknál bemutatott módon kell kezelni, míg a digitális videórögzítők esetén a számítógépeknél írtak alkalmazandók.

A hardveres kriptopénztárcák (általában pendrive-hoz hasonló kialakítású eszközök) azonosítása során meg kell kísérelni a hozzáférést biztosító PIN-kódok és a fizetési tranzakciók érvényesítéséhez szükséges privát kulcsok (alfanumerikus karakterláncok) beszerzését is.

Amennyiben az elektronikus adatok hordozója nem jelen lévő fizikai eszköz, hanem távoli szolgálatás (például felhőtárhely, elektronikus levelezési fiók stb.), úgy az elektronikus adatok forrásának egyedi azonosításához a szolgáltatás elnevezése és a hozzáférés felhasználó azonosítója szolgálhat (például Gmail: valaki@gmail.com).

Összegyűjtés

Az összegyűjtés *(collect)* során azokat a fizikai tárgyakat, amelyek potenciálisan elektronikus adatokat tartalmazhatnak, az eredeti helyükről ellenőrzött környezetbe, majd további vizsgálatra szállítják. Ennek során részletesen dokumentálni kell az eszköz eredeti helyét, annak kapcsolatait más eszközökkel (például eltávolítható másodlagos tárak), valamint ekkor kell beszerezni az egyes eszközökön található elektronikus adatokhoz történő hozzáférést lehetővé tevő adatokat és kiegészítő eszközöket is, amelyek tipikusan a következők lehetnek:

- felhasználói azonosítók (bejelentkezési név, e-mail-cím),
- jelszavak, képernyőlezárási minták, hozzáférési kódok,
- elektromos tápellátás kábelei és adapterei,
- adatátviteli kábelek (telefonkészülékek esetén),
- egyéb kapcsolódó információkat tartalmazó hordozók és kiegészítő eszközök.

Az összegyűjtés során (beleértve a szállítási fázist is) az adott eszköz és az azon potenciálisan megtalálható elektronikus adat integritásának megőrzése érdekében a megóvásra vonatkozó eljárások betartása szükséges.

Megóvás

Az elektronikus adatok és az azokat hordozó tárgyak (eszközök, berendezések) megóvása *(preserve)* során kiemelt figyelmet kell fordítani az alábbi veszélyforrások elhárítására.

A mechanikai sérülések az egyes berendezések és eszközök egymáshoz ütődése, leesése, vibrációja, vagy más mechanikai hatások során keletkeznek, amelyek ellen a készülékek elsődleges védőtokozása (például számítógépház, telefon elő- és hátlapja stb.) nyújt védelmet. Azok az eszközök, amelyek az elektronikus adat kiolvasásához szükséges mozgó alkatrészt is tartalmaznak (különösen a merevlemezek), a fizikai károsodás másodlagos hatásai (például író-olvasó fej sérülése, adatfelület sérülése) miatt károsodhatnak. A komplex eszközök (például mobiltelefon, okostelefon, tablet) kijelzőjének sérülése az adattartalom kinyerését nehezítheti, vagy az ezzel kapcsolatos költségeket növelheti.

A mechanikai sérülések elkerülése gondos csomagolással (buborékfóliás, légpárnás térkitöltők alkalmazása) és megfelelő rögzítéssel oldható meg.

Az elektromágneses terek elsősorban a mágneses tárolási elvű adathordozókat érintik (merevlemezes tárak, mágnesszalagos egységek) oly módon, hogy a tárolóterület egyes részein megváltoztathatják az információ rögzítésére szolgáló mágneses jelölők tulajdonságait, és ezzel megnövelhetik a hibás adatbitek számát, amely bizonyos mérték felett már nem korrigálható a beépített hibajavító megoldásokkal. Az elektromágneses terek ellen elsődleges távoltartással, amennyiben ilyen térben történő eszközelhelyezés vagy mozgatás történik, úgy Faraday-tasakkal vagy a Faraday-kalitka elvét megvalósító csomagolóanyaggal védekezhetünk.

A készülék irányából származó jelátvitelt (mobilkommunikáció, wifi- vagy Bluetooth-kapcsolat) az adott eszköz „repülőgép üzemmódba" *(airplane mode)* történő kapcsolásával érhetjük el, amennyiben az adott berendezés nincs lezárt állapotban. Lezárt (például jelkóddal védett) eszköz esetén a leárnyékolás (például Faraday-tasak, fémfóliás csomagolás stb.) megvédheti a készüléket a távolról (például mobilkommunikáción keresztül történő) módosítástól, ugyanakkor az árnyékolásból eredő jelvesztés miatt a készülék magasabb teljesítmény alkalmazásával próbálhatja meg felvenni a kapcsolatot a mobilkommunikációs hálózattal. A magasabb teljesítmény következménye az akkumulátor lemerülése, illetve túlmelegedése lehet, ezért az ismertetett esetben a folyamatos tápellátás (például power bank) mellett a készülék hűtéséről (például jégakku alkalmazásával) is gondoskodni kell. Mindezen tevékenységek végrehajtása akkor szükséges, ha a készülék kikapcsolása valamilyen okból nem lehetséges, vagy nem célszerű (jelkódos védelem vagy kikapcsolás utáni zárolás).

A statikus elektromosság elsősorban az elektronikus elvű adattárak (SSD, pendrive, memóriakártya), illetve az integrált vezérlőelektronikával szerelt eszközök (például merevlemezes tárolók) esetében okozhat károkat az adathoz történő hozzáférés útvonalának megszakítása vagy az adat egyéb módon történő elérhetetlenné tétele révén. A veszély csökkenthető az eszközök és csomagolásuk földelése segítségével.

Az extrém környezeti hőmérséklet, a por és a nedvesség elleni védekezést elsődlegesen a felsorolt hatások elkerülésével, másodlagosan megfelelő ellenintézkedéssel (aktív vagy passzív hűtés) és csomagolással (védőfólia) kell megoldani.

Megszerzés

Az elektronikus adatok megszerzése *(acquire)* elsődlegesen a szakértői laboratóriumban történik a statikus elemzés részben írtak szerint. Szükség esetén az elektronikus adatok megszerzésére az eszköz megtalálásának eredeti helyszínén is sor kerülhet az élő rendszer elemzése részben írtak szerint.

Az elektronikus adatok megszerzése az erre a célra megfelelő szakismeretekkel és gyakorlattal rendelkező és arra feljogosított személy feladata, aki lehet szakértő, szakkonzultáns vagy a nyomozó hatóság szakképzett munkatársa is.

Az elektronikus adatok vizsgálati modelljei

Az elektronikus adatok vizsgálata alapvetően két megközelítést jelent: a statikus elemzés során a korábban megszerzett vizsgálati tárgy, bűnjel elemzése szakértői laboratóriumban, míg az élő rendszer elemzése során a vizsgálati tárgy elsődleges azonosítása (felismerése) a valóságos vagy virtuális helyszínen történik, amelyet közvetlenül követ az elektronikus adatok megszerzése, majd azok elemzése (akár a helyszínen, akár szakértői laboratóriumban).

Statikus elemzés

Az elnevezés arra utal, hogy a vizsgálat az eredeti környezetéből kiemelt, kikapcsolt állapotú eszköz (mint az elektronikus adatot hordozó tárgy) vizsgálatára vonatkozik.

Azonosítás

A szakértői munka a megfelelően azonosított, károsító hatásoktól megvédett és a vizsgálat helyszínére – szakértői laboratórium – szállított vizsgálati tárgy, bűnjel ismételt azonosításával indul, amelynek alapdokumentuma a szakértői vizsgálatot elrendelő irat (határozat) és a szakértő részére rendelkezésre bocsátott egyéb iratok, adatok. Elsőként a vizsgálati tárgyak, bűnjelek mennyiségi ellenőrzését kell elvégezni az átvételi iratok adatai alapján. Ekkor kell meggyőződni arról is, hogy az egyes eszközök tartalmaznak-e további, elektronikus adat

önálló tárolására alkalmas egységeket – mint mobiltelefon esetén a SIM-kártya és memóriakártya –, illetve az egységként átadott berendezések – mint asztali számítógép, laptop stb. – esetén ekkor kell megállapítani az adott eszközben található adattárolók mennyiségét és típusát is. A minőségi azonosítás során – az átvételi iratok alapján – ellenőrizni és szükség esetén korrigálni kell az átvett eszközök, berendezések gyártmány-, típus- és egyéb minőségi adatait (mint mobiltelefon esetén az IMEI-azonosító, sorozatszám stb.). A véglegesített adatokat – az esetleges eltérésekre történő figyelemfelhívással együtt – fel kell tüntetni a vizsgálat eredményét tartalmazó szakértői véleményben.[115]

Vizsgálat előkészítése

A statikus elemzés – lehetőség szerint – az elektronikus adat másolatán történik, ezért a szakértői vizsgálat előkészítése a feltehetően elektronikus adatot tartalmazó eredeti vizsgálati tárgy, bűnjel tartalmának bitazonos másolásával kezdődik. A másoláshoz az erre a célra rendszeresített célhardver (*forensic duplicator,* forenzikus adatmásoló berendezés), illetve célhardver és célszoftver (*forensic writeblocker,* forenzikus írásvédő és *forensic imager,* forenzikus lemezképkészítő alkalmazás) eszközökkel történik.

Amennyiben műszaki vagy üzemeltetési okból a statikus vizsgálat nem lehetséges, úgy a vizsgálatot az élő rendszerek vizsgálati eljárása szerint kell lefolytatni.

Abban az esetben, ha nincs mód bitazonos másolat készítésére, úgy a statikus elemzés – az írásvédelem biztosítása mellett – elvégezhető az elektronikus adat eredeti tárolóján is. Egyes esetekben, ha az adatokhoz történő hardverközeli hozzáférés nem lehetséges valamilyen okból, úgy az adatokat az eredeti (natív) fájlrendszer felhasználásával történő másolás módszerével kell megszerezni, és a további szakértői vizsgálatot az így kinyert adatokon kell elvégezni.

[115] Máté István Zsolt: *Az igazságügyi informatikai szakértő a büntetőeljárásban.* PhD-dolgozat. Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, 2018. 130.

Vizsgálat

A statikus elemzés során a bitazonos másolatból az adatok helyreállítása – törölt adatok visszaállítása *(data recovery),* adatok összeállítása fájltöredékekből *(file carving)* –, csoportosítása és értelmezése történik. Mind a csoportosítás, mind az értelmezés történhet szoftveres eljárással, szoftveres eljárással emberi közreműködéssel, illetve kizárólag emberi közreműködéssel. Az adatcsoportosítás általános területei a következők:

- releváns fájltípusok (dokumentumok, táblázatok, adatbázisok, képek, mozgóképek, hangok stb.) kigyűjtése;
- adatok időbeli elhatárolása *(timeline);*
- metaadatok alapján történő kiválogatás (létrehozó eszköz, jogosultság stb.);
- képi tartalom azonosítása és elhatárolása, különösen az alábbi tartalmakra vonatkozóan:
  - pénz,
  - dokumentum,
  - kábítószer,
  - szexuális tartalom,
  - önkényuralmi jelképek,
  - fegyverek;
- mozgóképi tartalom azonosítása és elhatárolása a képi tartalomnál írtak szerint.

Az adatértelmezés különösen a következő műveleteket jelenti:

- optikai karakterfelismerés szöveget tartalmazó képi adatokon,
- kulcsszavas keresés szöveges tartalomban,
- az adott fájltípus betöltése olvasó *(reader)* vagy megtekintő *(viewer)* alkalmazásba,
- napló- *(log-)* állomány betöltése naplóelemző *(log analyzer)* alkalmazásba,
- egyéb állományspecifikus műveletek.

Élő rendszer elemzése

Az élő rendszer elemzése *(live analysis)* során nincs lehetőség bitazonos másolat készítésére, mivel

– egyedi hardver nem teszi lehetővé a tároló eltávolítását;
– különleges csatolófelület *(interface)* miatt nem csatlakoztatható a másolóeszközhöz;
– használatban lévő, kiemelt fontosságú eszköz tartalmazza az adatot (orvosi berendezés, komplex, nem megbontható szerkezetű informatikai rendszer stb.);
– egyéb akadályozó tényezők miatt.

A fenti esetekben előzetes helyzetfelmérés alapján (tehát nem az adott helyszínen ad hoc módon) kockázatelemzéssel kell meghatározni az adatmegszerzés kivitelezhetőségét, a megszerzési prioritásokat és kockázatokat, különösen az alábbi szempontok figyelembevétele mellett:
– az élő (bekapcsolt) rendszerekről történő adatmegszerzés megváltoztatja a rendszer állapotát, amely a rendszer instabilitását is okozhatja;
– titkosított tárolóeszközök esetén a rendszer kikapcsolása megakadályozhatja az adatokhoz történő hozzáférést, ezért a titkosítás jelenlétét megfelelő eszközzel ellenőrizni kell;
– az élő rendszerek külső kapcsolatai (vezetékes vagy vezeték nélküli számítógépes hálózati kapcsolat) vagy távoli vezérlés jelenléte befolyásolhatja az adatmegszerzés folyamatát.[116]

A felsorolt kockázatok értékelését és az egyes adatforrások azonosítását (statikus vizsgálattal azonos eljárás szerint) követően meg kell határozni az adatok megszerzésének sorrendjét, amelyet az adatok változékonysága *(order of volatility)* határoz meg az alábbiak szerint (amennyiben az adott ügy szempontjából releváns):
– processzorregiszter és gyorsítótár-tartalmak,
– számítógépes hálózati útvonalválasztó útvonaltáblája,
– címfeloldási protokoll (ARP) gyorsítótára (az IP-címek és a fizikai címek megfeleltethető táblázata),
– feladat-végrehajtási tábla *(processtable),*
– operációs rendszer rendszermag-statisztika és rendszermagmodulok tartalma *(kernel statistics and modules),*
– operatív tár tartalma *(main memory),*
– ideiglenes fájlrendszer tartalma *(temporary file systems),*

[116] ISO/IEC 27037:2012, 25–27.

– másodlagos memória tartalma *(secondary memory),*
– útvonalválasztó eszközök beállításai *(router configuration),*
– számítógépes hálózati összeköttetés-rendszer *(network topology),*
– további adatok.[117]

Az adatmegszerzés során a fentiek mellett folyamatosan gondoskodni kell a kérdéses rendszer tápellátásának biztosításáról oly módon, hogy azt sem technikai, sem emberi esemény, illetve beavatkozás ne zavarhassa meg.

A helyszínen végzett adatmegszerzés során figyelembe kell venni a vizsgálati tárgyak tárolókapacitásait és adatátviteli sebességét. Ezek az adatok általában csak a vizsgálat helyszínén, a vizsgálat megkezdését közvetlenül követően szerezhetők be, így a helyszíni vizsgálat időtartama ezen adatok és az ismert általános adatátviteli sebességek alapján becsülhető. Az élő rendszer vizsgálatánál használt leggyakoribb csatlakozótípusok és átviteli sebességek az egyes készülékek esetén a következők:

– Az USB 1.x – a fehér színkóddal jelölt 4 érintkezős csatlakozó csupán 1,5 MB/s maximális átviteli sebességre képes, előfordulása 2001 előtt gyártott eszközökön lehetséges, helyszíni adatmentésre nem alkalmas (1 DVD-nyi adatot körülbelül 1 óra alatt képes továbbítani).
– Az USB 2.x fekete színkóddal jelölt 4 érintkezős csatlakozó 60 MB/s maximális átviteli sebességre képes, előfordulása 2001 után gyártott eszközökön lehetséges, helyszíni adatmentésre korlátozottan alkalmas (1 DVD-nyi adatot körülbelül 1 perc alatt képes továbbítani).
– Az USB 3.x kék színkóddal jelölt 9 érintkezős csatlakozó 6251 280 MB/s maximális átviteli sebességre képes, előfordulása 2011 után gyártott eszközökön lehetséges, helyszíni adatmentésre alkalmas (1 DVD-nyi adatot körülbelül 4-8 másodperc alatt képes továbbítani).
– FireWire 400-800-1600-3200 [IEEE 1394 /1394b]: a 4-6-9 érintkezős csatlakozók 49 – 393 MB/s maximális átviteli sebességre képesek, előfordulásuk a nagyobb teljesítményű, elsősorban multimédiás célokra is szolgáló eszközökön gyakoribb, helyszíni adatmentésre alkalmas (1 DVD-nyi adatot körülbelül 12–96 másodperc alatt képes továbbítani).
– eSATA300/600: a 7 érintkezős csatlakozó 300–600 MB/s maximális átviteli sebességre képes, előfordulása 2004 után gyártott eszközökön

[117] Matthew Braid: *Collecting electronic evidence after a system compromise.* Brisbane, AusCERT, 2001. 13.

lehetséges, helyszíni adatmentésre alkalmas (1 DVD-nyi adatot körülbelül 8–16 másodperc alatt képes továbbítani).
– Thunderbolt 1/2/3: a 20 érintkezős csatlakozó 1,25–2,5 5 GB/s maximális átviteli sebességre képes, előfordulása 2011 után gyártott eszközökön lehetséges, helyszíni adatmentésre alkalmas (1 DVD-nyi adatot körülbelül 1–4 másodperc alatt képes továbbítani).

Amennyiben az adatokat helyi vagy nagy távolságú számítógépes hálózati kapcsolaton keresztül szükséges megszerezni, úgy az alábbi átviteli paraméterekkel kell kalkulálni:
– FastEthernet (100BASE-X) szabványú helyi hálózatok esetén 12,5 MB/s maximális átviteli sebességre lehet számítani ideális körülmények között (ha az adott hálózati szakaszon nincs egyéb adatforgalom, 1 DVD-nyi adatot körülbelül 6 perc alatt képes továbbítani).
– GigabitEthernet (1000BASE-X) szabványú helyi hálózatok esetén 125 MB/s maximális átviteli sebességre lehet számítani ideális körülmények között (ha az adott hálózati szakaszon nincs egyéb adatforgalom, 1 DVD-nyi adatot körülbelül 38 másodperc alatt képes továbbítani).

A fentiekre figyelemmel az élő rendszerből történő adatkinyerés időtartamát a megszerzendő adatok mennyisége (tárolási mérete) és az adatátvitel elméleti sebességének hányadosa adja. Az így kapott elsődleges elméleti megszerzési időt növelhetik az egyéb befolyásoló körülmények, úgymint párhuzamos adatforgalom, több adatforrásból azonos kimeneti csatornán történő adatkinyerés. Az elméleti adatmegszerzési idő kalkulációját követően mérlegelni kell annak veszélyét, hogy az adatátvitel megszakadhat-e. Ennek okai lehetnek:
– távoli hozzáférés a helyi eszközhöz,
– távoli rendszer lekapcsolása,
– távoli és helyi rendszer közötti adatkapcsolat megszakítása,
– helyi áramellátás kimaradása,
– eszközterhelésből adódó körülmények (például túlmelegedés).

Az élő rendszer vizsgálata esetén megszerzett adatok további vizsgálata a statikus vizsgálati eljárásnál ismertetett módon történik szakértői laboratóriumban.

Szakértői vélemény és annak felhasználása

Az elektronikus adatok kinyerését követően elkészülő igazságügyi informatikai szakértői vélemény tartalmazza mindazon körülmények leírását, amelyek a vizsgálat szempontjából releváns, így jellegzetes tartalmi elemei közé tartozik a jogszabályban előírtak közül különösen

- a vizsgálat módszerének általános leírása vagy hivatkozás a módszert leíró dokumentumra;
- a felhasznált eszközök felsorolása (hardver- és szoftvereszközök);
- a felhasznált szakirodalom és egyéb hivatkozások megadása;
- az egyes eszközök vizsgálatának leírása;
- a kinyert elektronikus adatok bemutatása nyomtatott és digitális formában.

A szakértői vélemény szövegében a szakértő számára feltett kérdésekre adott válaszok és az azokat alátámasztó, jellegzetesen a digitális mellékleten megtalálható elektronikus adatok a leghangsúlyosabbak, ezek értelmezése és felhasználása a kirendelő hatóság erre kijelölt munkatársának feladata.

A szakértői válaszok és különösen a digitális mellékleten megtalálható elektronikus adatok kezeléséhez felhasználói szintű informatikai ismeret szükséges, ami azt jelenti, hogy az erre kijelölt személynek a következőket kell végrehajtania:

- számítógép általános kezelése,
- szoftverek (fájlkezelő programok, irodai programok) kezelése,
- adathordozók (külső tárak, USB-kulcsok, optikai adathordozók stb.) kezelése,
- általánosan ismert fájltípusok kezelése (.pdf, .doc, .jpg stb.),
- kommunikációs alkalmazások (azonnali üzenetküldő programok, levelezőprogramok) kezelése,
- számítógépes hálózati ismeretek (böngészőprogramok, felhőszolgáltatások használata).

A felsorolt ismeretek és készségek révén a szakértői véleményben bemutatott elektronikus adatok információtartalma felhasználhatóvá válik az adott eljárásban.