MAGYAR IGAZSÁGÜGYI SZAKÉRTŐI KAMARA

6/2020.

MÓDSZERTANI LEVÉL

Az elektronikus adatok vizsgálatának általános alapelveiről

2020.

1 Tartalomjegyzék

1 A MÓDSZERTANI LEVÉL KIDOLGOZÁSÁBAN RÉSZT VEVŐK ADATAI

Dr. Máté István Zsolt	igazságügyi informatikai szakértő, Magyar Igazságügyi Szakértői Kamara Informatikai és Hírközlési Szakmai Tagozat elnöke
Dr. Darabos Zoltán	igazságügyi informatikai szakértő, COMPU-CONSULT Kft.
Morber Szilárd Krisztián	igazságügyi informatikai szakértő, Nemzetbiztonsági Szakszolgálat Szakértői Intézete
Sándor Gábor	igazságügyi informatikai szakértő, informatikai osztályvezető, Nemzetei Szakértői és Kutató Központ Informatikai Szakértői Osztály

A MÓDSZERTANI LEVÉL HATÁLYBA LÉPÉSÉNEK IDŐPONTJA

A módszertani levél hatálybalépésének időpontja: 2020. „ ”

I. MÓDSZERTANI LEVÉL TÉMÁJA

A módszertani levél valamennyi igazságügyi informatikai szakértői szakterületre és eljárástípusra vonatkozóan meghatározza az elektronikus adat és az elektronikus adat hordozójának azonosításakor alkalmazandó eljárásokat, azok sorrendiségét és tartalmát.

II. KIADÁS INDOKOLÁSA

A Magyar Igazságügyi Szakértői Kamara Informatikai és Hírközlési Szakmai tagozata az informatikai igazságügyi szakértői tevékenység során alkalmazandó alapvető tevékenységek maghatározásával és tartalmi leírásával ki kívánja alakítani

- a szakértői vizsgálatok egységes módszertanát,
- az alkalmazandó eljárások minimum követelményeit,
- a vizsgálatok megismételhetőségét és összehasonlíthatóságát,
- az egyes folyamatok akkreditálásának alapait.

III. HATÓKÖR

A módszertani levél személyi hatálya kiterjed az igazságügyi informatikai szakértőkre, eseti szakértőkre, szaktanácsadókra, technikusokra az elektronikus adatok helyszíni rögzítőire és valamennyi fel nem sorolt, az elektronikus adatok vizsgálatával kapcsolatba kerülő természetes személyre.

A módszertani levél tárgyi hatálya az elektronikus adatokkal - informatikai terminológiában digitális adat vagy számjegykódolt adat - kapcsolatos igazságügyi informatikai szakértő tevékenység alábbi részterületeire vonatkozik:

- az elektronikus adat azonosítása,
- az elektronikus adat megőrzése, megóvása,
- az elektronikus adatok összegyűjtése,
- az elektronikus adat kinyerése,
- az elektronikus adat vizsgálata,
- az elektronikus adat elemzése,

A módszertani levél eljárási hatálya kiterjed valamennyi igazságügyi informatikai szakértő tevékenységet igénylő eljárásfajtára, különösen:

- büntetőeljárásra,
- polgári eljárásra,
- közigazgatási eljárásra,
- hatósági eljárásra,
- magán szakértői megbízásra.

A módszertani levél területi hatálya kiterjed:

- helyszíni vizsgálatokra,
- laboratóriumi vizsgálatokra.

IV. MEGHATÁROZÁSOK

A módszertani levél tartalmához kapcsolódó alapfogalmak meghatározásának célja az a módszertani levélben szereplő leírások egységes értelmezésének megteremtése a magyar nyelvű informatikai-jogi fogalomtérben. Egyes esetekben az egységes magyar nyelvű fogalom, hiányából adódóan a meghatározás szövege leíró jellegű vagy egymással azonos jelentéstartalmú de a szakmai szóhasználatban még nem véglegesedett kifejezéseket is tartalmaz. Az egyes kifejezések esetén az azonos jelentést vagy- különösen az informatikai és a jogi szaknyelv különbségeiből adódó – egyenértékű szóhasználatot a meghatározások és a módszertani levél szövege külön jelzi. A szöveg tartalmának egyértelműsége érdekében esetenként a vonatkozó angol szaknyelvi kifejezés is megadásra kerül.

IV.1 Alapfogalmak

adat

Az informatikai értelemben vett adat egy vagy több jelből álló sorozat, amelynek értelmét meghatározott értelmezési folyamat(ok) adják meg. Az adat kizárólag értelmezés után válhat információvá.

bájt (byte)

Az adattárolás alapegysége, 1 bájt 8 bitből áll. A bájt szabványos rövidítése: „B".

bináris

Kettes alapú számrendszeren alapuló ábrázolás.

bit

Az információ alapegysége, illetve egyben az információt hordozó közlemény (adat) hosszának is egyik alapegysége, jelentése: bináris számjegy. Előbbi jelentésében a bit az információtartalom egysége, míg utóbbi jelentésében a bit az adatmennyiség egysége. A bit szabványos rövidítése: „b".

bűnjel

Bizonyítékként felhasználható tárgy vagy adat; a hatóság által biztosított (lefoglalt) nyomhordozó, amely a bűncselekménnyel összefüggésbe hozható.[1]. A bűnjelen tárolt digitális adatok képezik az informatikai szakértői vizsgálat tárgyát.

digitális adat

Az információ diszkrét, nem folytonos ábrázolása. A digitális adatok kvantált – számokká alakított – értékek, amelyeket jellemzően binárisan ábrázolnak. A magyar jogi szaknyelvben elektronikus adat.

[1] A fogalom jogi aspektusainak részleteit a 11/2003. (V. 8.) IM-BM-PM együttes rendelet tartalmazza

digitális adat másolata

A digitális adat másolata, mely abból a célból készült, hogy biztosítsa az adat megbízhatóságát, beleértve magát a digitális adatot és az ellenőrzés módszerét is. A magyar jogi szaknyelvben elektronikus adat, az angol nyelvű szakirodalomban digital evidence copy.

digitális adathordozó

Olyan eszköz, amely digitális adatok tárolására alkalmas. A digitális adathordozók a digitális eszközök részhalmazát képezik. Adattárolási elvük változatos lehet, különösen:

- mágneses,
- optikai,
- magneto-optikai,
- elektronikus,

azonban az adatok tárolása minden esetben digitális, többnyire bináris. Az adathordozó lehet háttértároló vagy folyamatos áramellátást igénylő[2] tároló.

digitális ábrázolás

Valamely változó jelenségnek, vagy fizikai mennyiségnek diszkrét (nem folytonos), megszámlálhatóan felaprózott, s így számokkal meghatározható, felírható értékeinek halmaza.

digitális bizonyíték

A digitális bizonyíték olyan digitális adat, amely egy bűncselekmény eseményeinek feltárására, valamely állítás igazolására vagy vitatott kérdés tisztázására, eldöntésére alkalmas. A digitális adat magyar jogi szaknyelveben bizonyítási eszközként megjelenő[3] elektronikus adat fogalmának szűkebb értelmezése.

digitális eszköz

Digitális adatok feldolgozására és / vagy tárolására használt (elektronikus) berendezés (angol szaknyelvben digital device). Feldolgozásnak minősül a digitális adatokon alkalmazott bármely művelet vagy műveletek összessége (létrehozás, törlés, módosítás, továbbítás, stb.).

digitális tárolóeszköz

Olyan eszköz, melyre digitális adatok rögzíthetők (angol szaknyelvben digital storage medium).

---

[2] angol nyelvű szakirodalomban volatile memory

[3] 2017. évi XC. törvény 165. § f)

digitális nyom

Egy adott cselekmény bekövetkezésekor annak nyomképző tulajdonságai által létrehozott digitális lenyomat (különösen digitális adat | elektronikus adat). Digitális nyomot képezhetnek az adott cselekmény során létrehozott, módosított vagy megsemmisített digitális adatok is.

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.[4] A magyar informatikai szaknyelvben digitális adat vagy számjegykódolt adat.

hasító érték

Hasítófüggvény eredményeként létrejövő számsorozat, digitális lenyomat. A hasító függvény egy tetszőleges hosszúságú bitfolyamból véges hosszúságú bitsorozatot, hasító értéket állít elő

hexadecimális

Tizenhatos alapú számrendszeren alapuló ábrázolás. A bináris értékeket a kisebb helyigényű (tömörebb) ábrázolás érdekében gyakran hexadecimális formában jelenítik meg.

információ

Az adat és a hozzátartozó tudás összessége, amely az adat értelmezéséhez szükséges. Információelméleti megközelítésben az információ a váratlanság mértéke, egy adatnak annál nagyobb az információ tartalma, minél több bizonytalanságot szüntet meg.

információtechnológia

Információ vagy adatok számítástechnikai eszközök segítségével történő kezelése. Az információtechnológia (IT) alapvető jellemzője az információ számszerűsítése, azaz kvantálása, digitalizációja, amelynek gépi ábrázolása az információ legkisebb önállóan értelmezhető alapegységére, a bitre alapul.

információs rendszer

Az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége;[5]

[4] 2017. évi XC. törvény 204. § (1)
[5] 2017. évi XC. törvény 10. § (1) 6.

lefoglalt tárterület

A digitális tárolóeszközökön (beleértve az operatív memóriát is) adatok (beleértve a metadatokat is) tárolására használatba vett tárterület (angol szaknyelven alloctated space).

tartós tár, háttértároló

Olyan digitális adathordozó, amely energiaellátás nélkül is képes a digitális adatok huzamosabb idejű tárolására, különösen:

- csak olvasható memória (ROM, PROM)
- digitális mágnesszalag (DAT)
- merevlemez
- hajlékony lemez (floppy)
- optikai lemez (CD-R, DVD-R, Blu-ray)
- lyukkártya, lyukszalag
- magneto-optikai lemez
- szilárdtestmeghajtó (SSD)
- flash tároló (memóriakártya, pendrive, EEPROM)

folyamatos energiaellátást igénylő tároló

Olyan adathordozó, amelynek energiaellátása megszűnésével a rajta tárolt digitális adatok megsemmisülnek, különösen:

- CPU regiszter
- gyorsítótár (cache)
- operatív tár (RAM)
- puffer (I/O data buffer)

IV.2 Alapelvek

átláthatóság

A szakértői feladatok ellátásával kapcsolatos elvárás, amely a nyitottság, a nyomonkövethetőség, és az ellenőrizhetőség követelményeit foglalja magában. Alapfeltétele a szabályozott folyamatokra épülő feladat-végrehajtás, a dokumentáltság és az adatok beavatkozásmentes kezelése.

eredetiség

A vizsgálati tárgyat lehetőség szerint – az egyedi körülmények esetenkénti mérlegelése alapján – eredeti állapotát megőrizve, roncsolásmentes és utólag rekonstruálható módon kell megvizsgálni. A szakértő által tett intézkedés általános esetben – amennyiben egyedi vagy különleges körülmények nem teszik azt megvalósíthatatlanná – nem változtathatja meg az eszközön vagy adathordozóin tárolt azon adatokat, amelyek később a bizonyítási folyamat során felhasználásra kerülhetnek.

megbízhatóság

A következetesen tervezett viselkedés és eredmény jellemzője (angol szaknyelvben reliability). Az alapelv akkor teljesül, ha az adott vizsgálati eljárások eredménye megismételhető és ismételten előállítható. A megbízhatóság alapfeltétele a dokumentáltság, mely különösen az ellenőrző függvények, az időbélyegek, valamint a (lehetőség szerint) bevizsgált szakértői eszközök és validált módszerek alkalmazásának körülményeit tartalmazza.

megismételhetőség

Annak a vizsgálati módszernek a jellemzője, amely *azonos* vizsgálati környezetben azonos eredményt ad (angol szaknyelvben repeatability). Az alapelv akkor teljesül, ha az adott vizsgálati módszerrel, az arról készült dokumentáció alapján, egy szakképzett független személy ugyanarra az eredményre jut minden különösebb útmutatás vagy értelmezés nélkül.

ismételt előállíthatóság

Annak a vizsgálati módszernek a jellemzője, amely *különböző* vizsgálati környezetben azonos eredményt ad (angol szaknyelvben reproducibility). Az alapelv akkor teljesül, ha ugyanaz a vizsgálati módszer kerül alkalmazásra, különböző eszközök (beleértve a hardver és szoftver eszközöket is) és különböző feltételek között és a vizsgálati módszer ugyanarra az eredményre jut. Az eredeti vizsgálatot követően a vizsgálat bármikor újra előállíthatónak kell lennie

IV.3 Alaptevékenységek

azonosítás

Az a folyamat – beleértve a keresést is – amely során felismerik és dokumentálják a lehetséges digitális nyomokat (angol szaknyelvben identification) Az azonosítás fogalma a digitális nyom feltételezhető hordozójának *felismerését* és annak egyedi azonosításra alkalmas *jelöléssel történő ellátását* egyaránt tartalmazza.

bevizsgálás

A szakértői vizsgálatok során felhasznált algoritmus (szoftver) vagy digitális eszköz (hardver) rendeltetésszerű működésének ellenőrzése. Bevizsgálás az alábbi esetekben szükséges:

- új eszköz szakértői vizsgálati célra való bevezetése előtt;
- bevizsgált eszközben bekövetkező változás/változtatás (pl. frissítés) esetén;
- bevizsgált eszköz működésével kapcsolatban tapasztalt anomália esetén.

érvényesség megerősítése

Annak megerősítése objektív bizonyítékok révén, hogy a rendeltetésszerű használat, vagy alkalmazás követelményei teljesültek egy adott dologra vonatkozóan (angol szaknyelvben validation). Az tevékenység lehetővé teszi az igazságügyi informatikai szakértői vizsgálatok során alkalmazott módszerek és eszközök működésének ellenőrzését.

felülvizsgálat

Annak megerősítésé objektív bizonyítékok által, hogy a meghatározott követelmények teljesültek (angol szaknyelvben verification).

felügyeleti lánc fenntartása

A felügyeleti lánc a potenciálisan értékes elektronikus adatok és hordozóik mozgatásának és kezelésének dokumentálása révén lehetővé teszi az elektronikus adatok és hordozói pontos, ellenőrizhető nyomon követhetőségét, beleértve az egyes időpillanatokban az elektronikus adatokért és hordozóikért felelős személy meghatározását is. A felügyeleti lánc fenntartása a nyomon követési dokumentáció folyamatos, pontos vezetését jelenti.

megerősítés

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

megőrzés

Az a folyamat melynek során megvédik és fenntartják a lehetséges digitális nyom eredeti állapotát (angol szaknyelvben preservation).

V. BEVEZETÉS

V.1 A témakör hazai helyzete, a témaválasztás indoklása

Az igazságügyi informatikai szakértők gyakorlati tevékenységét a vonatkozó jogszabályokon kívül a szakértői módszertani levél szabályozza, illetve ez utóbbi útmutatást nyújt a szakértőnek „a szakértői tevékenység egységes és magas színvonalú ellátása érdekében"[6-7]. Jelen módszertani levél a tudomány és a műszaki fejlődés nemzetközi és hazai eredményeinek – szakirodalmának és szabványainak – feldolgozása és felhasználása révén kívánja az igazságügyi informatikai szakértői tevékenység gyakorlását támogatni.

V.2 Kapcsolat a hivatalos hazai és külföldi szakmai irányelvekkel

A Digital Forensic Research Workshop szervezet 2001-es első konferenciáján tárgyalta és kialakította a digitális adatok kezelésére vonatkozó vizsgálati eljárásmodelljét, melyben az alábbi műveleteket azonosította.[8]:

1 - Identification	a digitális adat hordozójának azonosítása,
2 - Preservation	a digitális adat megőrzése, megóvása,
3 - Collection	a digitális adat hordozóinak összegyűjtése,
4 - Acquisition	a digitális adat kinyerése,
5 - Examination	a digitális adatok vizsgálata,
6 - Analysis	a digitális adatok elemzése,
7 - Presentation	a digitális adatok bemutatása,
8 - Decision	döntés a digitális adatok alapján.

A későbbiekben a digital forensic science szakterület kutatói ezt a modellt bővítették, egészítették ki saját preferenciáik alapján. Jelen módszertani levél a nemzetközi kutatói és alkalmazói szakmai irányelvekkel történő összhang biztosítása érdekében a tartalom tudományos és szakmai elemeinek alapforrásaként a Digital Forensics Research Workshop 2001-ben elfogadott módszartanát tekinti az 1 – 6 területekre koncentrálva.

---

[6] 2005. évi XLVII. törvény 30/A §

[7] 2016. évi XXIX. törvény 89. § (1)

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

Az alapvető tudományos és módszartani forráson kívül jelen módszertani levél különösen az alábbi nemzetközi szabványokban, a Scientific Working Group on Digital Evidence szervezet dokumentumaiban, az European Network of Forensic Science Institutes dokumentumaiban szereplő ajánlásokat tekinti releváns forrásoknak:

V.2.1 Nemzetközi szabványok

MSZ EN ISO/IEC 27037:2016 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence. European Committee for Standardization. Brussels, 2016. pp. 48. [Útmutató a digitális bizonyítékok azonosításához, összegyűjtéséhez, megszerzéséhez és megőrzéséhez]

MSZ EN ISO/IEC 27041:2016 Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method. European Committee for Standardization. Brussels, 2016. pp.28. [Útmutató az incidenskivizsgálási módszer alkalmasságának és megfelelőségének biztosításához]

MSZ EN ISO/IEC 27042:2017 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence. European Committee for Standardization. Brussels, 2016. pp.22. [Útmutató a digitális bizonyítékok elemzéséhez és értelmezéséhez]

MSZ EN ISO/IEC 27043:2016 Information technology — Security techniques — Incident investigation principles and processes. European Committee for Standardization. Brussels, 2016. pp.42. [Incidenskivizsgálási elvek és folyamatok]

MSZ EN ISO 21043-1:2018 - Forensic Sciences. Part 1: Terms and definitions. European Committee for Standardization, Brussels, 2018. pp.11. [Bűnügyi tudományok (bűnügyi technika) 1. rész: Szakkifejezések és meghatározásuk]

ISO 21043-2 - Forensic sciences - Part 2 - Recognition, recording, collecting, transport and storage of items. International Organization for Standardization. Geneva, 2019. pp.13. [Bűnjelek felismerése, rögzítése, összegyűjtése, szállítása és tárolása]

V.2.2 SWGDE[9] ajánlásai

Best Practices for Computer Forensics. SWGE, 2014. ver.: 3.1, pp.12.

Best Practices for Digital Evidence Collection. SWGE, 2018. ver.: 1.0, pp.7.

Best Practices for Computer Forensic Acquisitions. SWGE, 2018. ver.: 1.0, pp.11.

Best Practices for Computer Forensic Examination. SWGE, 2018. ver.: 1.0, pp.8.

V.2.3 ENFSI[10] ajánlásai

Best Practices for Digital Evidence Collection. ENFSI, 2015. ver.: 01, pp.68.

Best Practice Manual for the Forensic Examination of Digital Technology ENFSI-BPM-FIT-01, 2015

[9] SWGDE – Scientific Working Group on Digital Evidence
[10] ENFSI - European Network of Forensic Science Institutes

VI. A MÓDSZERTANI LEVÉL SZAKMAI RÉSZLETEZÉSE

VI.1 A digitális adatok kezelésének alapelvei

VI.1.1 Általános követelmények

VI.1.1.1 Relevancia

Megállapíthatónak kell lennie az elektronikus adat jelentőségének, egyben bizonyíthatónak, hogy a beszerzett elektronikus adatok a vizsgálat szempontjából relevánsak, vagyis olyan értékes információkat tartalmaznak, amelyek az adott incidens vagy eset vizsgálatát segítik és ebből adódóan okot szolgáltattak az elektronikus adat begyűjtéséhez és megszerzéséhez.

VI.1.1.2 Megbízhatóság

A potenciálisan értékes elektronikus adatok és hordozói kezeléséhez használt folyamatoknak hitelesíthetőnek és megismételhetőnek kell lenniük oly módon, hogy a vizsgálatok eredménye ismételten előállítható legyen.

VI.1.1.3 Megfelelőség

Megállapíthatónak és igazolhatónak kell lennie annak, hogy a vizsgálathoz elegendő (megfelelő mennyiségű és minőségű) potenciálisan értékes elektronikus adatot tartalmazó adathordozó összegyűjtése történt meg.

VI.1.2 Hitelesíthetőség

Az elvégzett tevékenységek megfelelő dokumentálásával lehetővé kell tenni azok független vagy egyéb érdekelt fél általi értékelését. A dokumentációnak az egyes megoldási módok közötti választás okaira is ki kell térnie.

VI.1.3 Megismételhetőség

Az egyes tevékenységek (vagyis a vizsgálat) megismételhetők akkor, ha ugyanazokat az eredményeket a következő feltételeket betartva állítják elő:

- ugyanazzal a mérési eljárással és módszerrel,
- ugyanazokkal az eszközökkel és azonos feltételek mellett és
- az eredeti vizsgálatot követően bármikor megismételhetően történik.

Az egyes tevékenységek dokumentáltságának olyan szintűnek kell lennie, hogy valamennyi leírt folyamat elvégzésével külön útmutatás vagy értelmezés nélkül ugyanazon eredmények legyenek elérhetők.

A dokumentációban rögzíteni kell azokat a körülményeket, melyek az egyes folyamatok megismételhetőségét befolyásolják vagy kizárják.

VI.1.4 Újra előállíthatóság

A vizsgálat eredményei reprodukálhatók akkor, ha a tevékenységeket a következő feltételeket betartva hajtják végre:

- ugyanazzal a méréséi módszerrel,
- különböző eszközök és különböző feltételek mellett és
- az eredeti vizsgálat után bármikor elvégezhető.

VI.1.5 Indokoltság

Az egyes tevékenységek során képesnek kell lenni annak igazolására, hogy a potenciális digitális adathordozók kezelésére használt valamennyi intézkedést és módszert a digitális adat kinyeréséhez megfelelő volt. Ez igazolható az egyes tevékenységek és módszerek reprodukálásával vagy validálásával.

VI.2 Általános vizsgálati eljárás

VI.2.1 Vizsgálati tárgy azonosítása – felismerés és megkülönböztetés

VI.2.1.1 A felismerés általános elvei

Az elektronikus adat hordozóinak felismerése az egyes digitális eszközcsoportok alapvető jellemzői alapján történhet általános esetben.

Az egyes eszközök felismerése és osztályba sorolása elsődlegesen fizikai jellemzőik alapján történik. A művelet során az adott eszköz osztály általános megjelenési jellemzőit kell összevetni a kérdéses eszköz jellemzőivel, majd a hasonlóság alapján kell elvégezni az elsődleges besorolást.

Amennyiben az eszköz elektronikus úton kiolvasható digitális azonosítót is tartalmaz, úgy azt a végleges azonosításhoz fel lehet használni és adott esetben a két azonosítási mozzanat összesített adatai felhasználva lehet véglegesíteni az eszköz azonosítását akár az elsődleges besorolás módosításával (pl. USB kulcs ➔ kriptovaluta hardveres pénztárca; HDD ➔ SSD, CD ➔ DVD stb.).

VI.2.1.2 A megkülönböztetés általános elvei

A megkülönböztetésnél elsődlegesen figyelembe vehetők az egyes eszközök gyári feliratai, azonosító és műszaki tartalmú címkéi, melyek a továbbiakban egyedi azonosítóként használhatók, vagy egyedi azonosító képzésben alkalmazhatók.

Amennyiben az kérdéses rendszer több komponensből áll, úgy azokat egyenként szükséges azonosítani (felismerni) és elkülöníteni: egyrészt az elektronikus adatokat potenciálisan tartalmazó, másrészt az elektronikus adatokat nem tartalmazó komponenseket. Az különleges kialakítású eszközök esetén különösen ügyelni kell az elektronikus adat tárolási képességekre vonatkozó megállapítással (pl. LCD monitor ➔ all-in-one PC).

A nem általános megjelenésű, vagy rejtett funkcionalitású eszközök felismeréséhez az egyes eszköz osztályok méret jellemzői, csatlakozó tulajdonságai és általános fizikai elhelyezkedésük ad támpontot. A nem általános megjelenésű, vagy rejtett funkcionalitású eszközök azonosítása esetenként eltérő eljárással történhet.

VI.2.1.3 A felismerés és megkülönböztetés elveinek gyakorlati alkalmazása

A szakértői vizsgálatot megelőzően a vizsgálatra átvett tárgyakról és azok csomagolásáról, illetőleg a csomagolás bontási folyamatáról képi (digitális fénykép és/vagy videó) dokumentáció készülhet. A vizsgálatra átvett tárgyak előzetes felmérése során beazonosításra és dokumentálásra kerül az eszközök jellege, márkája, típusa, egyedi azonosítóik, valamint külső ismertetőjegyeik, általános állapotuk.

A vizsgálatra átvett tárgyak azonosítása után megállapításra kerül, hogy a szakértőt kirendelő dokumentumban feltüntetett és a ténylegesen átvett tárgyak egymásnak megfelelnek-e, szükség esetén a leírásuk pontosításra kerül a kirendelő vagy megbízó értesítése mellett.

A szakértőt kirendelő dokumentumban foglaltak alapján megállapításra kerül, hogy az abban feltett kérdések megválaszolásához szükséges-e a vizsgálatra átvett tárgyakban tárolt adatok mentése.

Amennyiben az adatmentéshez szükséges és lehetséges a vizsgálat tárgyát képező eszköz roncsolás nélküli szétszerelése (különösen beépített tároló eltávolítása számítógépből, laptopból vagy egyéb eszközből), úgy a szerelési folyamatról is digitális képi dokumentáció készülhet. A vizsgálat végeztével az eszközök eredeti - összeszerelt - állapotukba kerülnek helyreállításra.

Az eredeti fizikai állapotot tartósan és helyreállíthatatlan módon megváltoztató roncsolásos vizsgálatra a kirendelő vagy megbízó kifejezett írásos felhatalmazása alapján kerülhet sor a roncsolásmentes vizsgálatnál írt dokumentálás mellett.

Amennyiben szükséges az adatmentés, akkor további vizsgálatok során megállapításra kerül, hogy a vizsgálatra átadott tárgyak milyen adathordozókat tartalmaznak, majd megtörténik a fellelt adathordozók jellegének, márkájának és típusának azonosítása és dokumentálása. Ezzel egy időben az egyes adathordozók saját jelölést is kapnak.

VI.2.2 Vizsgálati tárgy állapotnak felmérése

Az adatmentés megkezdése előtt eszközfelmérés történik, melynek célja az adathordozók, illetve az azokat működtető eszközök mechanikai, elektronikai és informatikai ellenőrzése. Az eszközfelmérés folyamata különösen a következő lépéseket tartalmazhatja:

- Mechanikai eszközfelmérés: Az eszközök, azok tartozékai és részegységei fizikai épségének, működőképességének ellenőrzése manuális vizsgálattal. A mechanikai eszközfelmérés célja annak megállapítása, hogy az eszközök részegységei fizikai integritás szempontjából alkalmasak-e az adatmentési folyamat megkezdésére.
- Elektronikai eszközfelmérés: Az eszközök elektronikai működőképességének és a kommunikációs részegységeinek vizsgálata. Az elektronikai eszközfelmérés célja annak megállapítása, hogy az eszközök elektronikai működőképesség szempontjából alkalmasak-e a digitális nyomrögzítés megkezdésére.

- Informatikai eszközfelmérés: A felmérés célja megállapítani, hogy a vizsgált eszközök vonatkozásában rendelkezésre áll-e az adatmentési folyamat megkezdéséhez szükséges eszközrendszer (hardver és szoftver).

Az eszközfelmérés eredményeképpen megállapítható, hogy az adathordozó eszköz alkalmas-e a szakértőt kirendelő dokumentumban feltett kérdések megválaszolásához szükséges adatmentés megkezdéséhez, valamint rendelkezésre áll-e digitális nyomrögzítés megkezdéséhez szükséges eszközrendszer.

VI.2.3 Vizsgálati tárgy állapotnak megóvása

A szakértői vizsgálat minden részfolyamata során az egyedileg azonosított digitális adathordozókat egymástól elkülönített módon az adott digitális adathordozó sajátosságainak megfelelő módon kell megőrizni. A megóvás az a folyamat melynek során megvédik és fenntartják a digitális adat hordozó és a lehetséges digitális adat eredeti állapotát.[11] A folyamatba beleértendő az illetéktelen hozzáféréstől vagy a digitális adat hordozó eltüntetéstől történő megóvása is a felügyeleti lánc (chain of custody) folyamatos fenntartása révén.

A megőrzés során különösen az alábbi körülményekre kell figyelemmel lenni

VI.2.3.1 Elektromágneses mezők

Meg kell védeni a digitális adat hordozót a különféle elektromágneses sugárzások (pl. rádió, röntgen eszközök stb.) káros hatásaitól, beleértve az elektrosztatikus feltöltődést is. A védelem eszközei különösen:

- Faraday tasak (izolációs tasak, nyomkövetés elleni védelem és RF árnyékolás);
- több rétegű alufólia csomagolás
- Lehetőség szerint antisztatikus feltöltődés elleni védelem biztosítása
- egyéb alkalmas eszköz felhasználásával.

[11] Kapcsolódó szabvány: ISO/IEC 27037:2012(E) 3.15.

VI.2.3.2 Fizikai szennyeződés

A fizikai szennyeződés, különösen a por a szigeteletlen mozgó alkatrészeket tartalmazó, vagy érzékeny felületű adathordozókat (hajlékonylemezek, optikai lemezek) károsítja. A védelem eszközei és eljárásai különösen:

- digitális adat hordozók kezelésekor a szakértő lehetőség szerint viseljen nem szálmentes, tiszta és száraz kesztyűt,
- a csomagolásnak mentesnek kell lennie a portól, zsírtól, kémiai szennyező anyagoktól, amelyek elősegítik a korróziót, valamint a nedvesség lecsapódását;
  - ~ bűnjeltasak,
  - ~ bűnjelzsák,
  - ~ ipari zsugorfólia,
  - ~ egyéb alkalmas eszköz felhasználásával.

VI.2.3.3 Mechanikai károsodás

A mechanikai rezgések, behatások különösen a finommechanikai alkatrészeket tartalmazó adathordozókat károsítja. A védelem eszközei és eljárásai különösen:

- a kisebb terjedelmű digitális adat hordozók mechanikai védelmét a megfelelő csomagolóanyag és csomagoló segédanyagok kiválasztásával és alkalmazásával kell biztosítani:
  - ~ buborékfóliás csomagolás,
  - ~ tárolódoboz levegő alapú térkitöltővel,
  - ~ egyéb alkalmas eszköz felhasználásával.
- a nagyobb terjedelmű digitális adat hordozók mechanikai védelmét az adott tárgy megfelelő elhelyezésével és rögzítésével szükséges megoldani.
  - ~ rögzítés szállítás közben,
  - ~ megfelelő szállítóeszköz használata,
  - ~ egyéb alkalmas eszköz felhasználásával

VI.2.3.4 Adatmódosulás

Különösen élő számítógépes rendszer esetén meg kell védeni a kérdéses rendszert a lehetséges káros beavatkozásoktól (pl. távoli hozzáférés, adattörlő eljárás elindulása stb.). Amennyiben káros beavatkozás észlelhető, úgy egyrészt az adott eszköz el kell különíteni a számítógépes rendszer (pl. számítógépes hálózat) többi elemétől, másrészt a rendszer vagy rendszerkomponens áramellátását azonnali beavatkozással meg kell szüntetni (pl. tápellátás kábelének azonnali lecsatlakoztatása, akkumulátor azonnali eltávolítása). A káros beavatkozást – a folyamat megszakítását követően – részletesen dokumentálni szükséges a rendelkezésre álló adatok alapján.

VI.2.4 Vizsgálat

Az eljáró szakértő az eszközfelmérés alapján elvégzi a szükséges vizsgálatokat, amely a kirendelő dokumentumban megfogalmazott kérdések tartalmától függően a következő módszerek alkalmazását jelenti:

- Digitális nyomrögzítés
- Vizuális adatrögzítés
- Adattartalom hozzáférhetőségének biztosítása
- Adatok elemzése

Az alkalmazandó vizsgálati módszer vagy módszerek kiválasztása az eljáró szakértő felelősségi körébe és kompetenciája közé tartozik. A leggyakoribb vizsgálatok módszereiről és azok alkalmazásáról szükség esetén önálló módszertani levél kerül kiadásra.

VI.2.4.1 Digitális nyomrögzítés

A digitális adat kinyerése az adatok meghatározott köréről készített másolat létrehozásának folyamata.

A kinyerés alapelve: a forrásadatok változásainak legteljesebb mértékű minimalizálása olyan hardver és / vagy szoftver komponensek alkalmazásával, melyek lehetővé teszik a forrásadatok megváltoztatás nélküli kezelését.

A digitális adatok kinyerésének három alapvető esete azonosítható, melyek a következők:

- adatkinyerés bekapcsolt digitális eszközről
- adatkinyerés kikapcsolt digitális eszközről
- adatkinyerés olyan bekapcsolt digitális eszközről, amelyen nem lehet leállítani (pl. kritikus infrastruktúra komponens vagy egyéb ok miatt)

Valamennyi esetben pontos másolatot kell készíteni azon adathordozókon tárolt adatokról, melyekről feltételezhető hogy releváns információkat tartalmaznak.

A digitális adatmentés metódusának kiválasztása az eszközfelmérés eredményének figyelembevételével történik. Igazságügyi másolat készítése akkor lehetséges, amennyiben az adathordozó mechanikai, elektronikai és informatikai szempontból is alkalmas az adatmentésre.

VI.2.4.1.1 A DIGITÁLIS NYOMRÖGZÍTÉSHEZ KAPCSOLÓDÓ FOGALMAK MEGHATÁROZÁSA

Fizikai másolat

A fizikai adatmásolás az adathordozó eszközszintjén történik, vagyis az adathordozó minden címezhető adattároló területének (szektorának) adattartalma másolásra és mentésre kerül. Fizikai mentés esetén lehetséges a fájlrendszer által nem lefoglalt tárterületekről is adatokat kinyerni, helyreállítani. Fizikai adatmentésre alkalmas digitális nyomrögzítési fajták:

- hiteles másolat
- hiteles lemezkép (fizikai lemezkép)
- memóriakép

Logikai másolat

A logikai adatmásolás az adathordozó fájlrendszerének szintjén történik, vagyis a rendelkezésre álló jogosultsági szinten a fájlrendszer által nyilvántartott adattartalom (fájlstruktúra) kerül másolásra és mentésre. Logikai mentés esetén nem lehetséges a fájlrendszer által allokálatlan tárterületekről adatokat kinyerni, helyreállítani, mivel ezek az adatok csak az adathordozó eszközszintjén vannak jelen. Törölt állományok helyreállítása csak abban az esetben lehetséges, amennyiben ezt a fájlrendszer vagy az operációs rendszer beállításai kifejezetten támogatják (pl. Lomtár használata). Logikai adatmentésre alkalmas digitális nyomrögzítési fajták:

- hiteles lemezkép (logikai lemezkép)
- hiteles mentés
- hiteles letöltés

Fizikai lemezkép

Fizikai adatmásolás útján létrehozott hiteles lemezkép.

Logikai lemezkép

Logikai adatmásolás útján létrehozott hiteles lemezkép.

Igazságügyi másolat

A digitális adatok másolata, amely teljesíti a hitelt érdemlőség követelményeit és abból a célból készül, hogy biztosítsa a vizsgálati anyag eredeti adattartalmának rögzítését, valamint a további vizsgálatok elvégzését. Az igazságügyi másolat fogalmába beleértendő az eredeti és a másolt adatok egyezőségét igazoló, illetve az egyezőség ellenőrzését lehetővé tevő algoritmusok futtatási eredménye is, amennyiben azok létrehozása technikailag lehetséges.

Hiteles másolat

Az igazságügyi másolat egy fajtája. A hiteles másolat a vizsgált adathordozó adattartalmának szektorról szektorra történő másolása során keletkezik egy másik - azonos vagy nagyobb tárolókapacitású - adathordozóra. A hiteles másolat elkészítésének eredménye egy klónozott adathordozó.

Hiteles lemezkép

Az igazságügyi másolat egy fajtája. A hiteles lemezkép a vizsgált adathordozó adattartalmának (fizikai lemezkép esetén) blokkról blokkra vagy (logikai lemezkép esetén) fájlról fájlra történő másolása során keletkezik egy - vagy több - adatállományba, amely(ek)nek (együttes) adattartalma bitre pontosan megegyezik a forráslemezével (logikai lemezkép esetén a forrásfájlokéval). A hiteles lemezkép elkészítésének eredménye egy vagy több lemezkép állomány.

Hiteles mentés

Az igazságügyi másolat egy fajtája. A hiteles mentés folyamata során a releváns állományok kinyerése közvetlenül a fájlrendszerből történő adatmásolás által történik meg. A hiteles mentés elkészítésének eredménye egy másolt fájlstruktúra.

Hiteles letöltés

Az igazságügyi másolat egy fajtája. A hiteles letöltés folyamata során a releváns állományok kinyerése az online társzolgáltatás által biztosított felületen keresztül kezdeményezett fájlátvitel által történik meg. A hiteles letöltés elkészítésének eredménye a letöltött állományok összessége.

Memóriakép

Az igazságügyi másolat egy fajtája. A memóriakép készítése során a vizsgált digitális eszköz operatív tárának (RAM) - vagy egyéb folyamatos áramellátást igénylő tárolójának - adattartalma kerül másolásra egy vagy több adatállományba. A memóriakép elkészítésének eredménye az operatív tár pillanatnyi adattartalmáról készített memóriakép állomány.

Fizikai felülíráson alapuló teljes törlés

Digitális adathordozó adattároló területeinek igazságügyi törlése. Az adathordozó teljes törlése során ismert ismétlődő jelsorozattal (tipikusan logikai nullával) töltik fel az adathordozó minden egyes címezhető adattárolásra képes egységét (szektorát). A teljes törlés célja, hogy a művelet után az adathordozóra kerülő adatok ne keveredhessenek korábbi adatok maradványaival. teljes törlésen átesett adathordozó előkészítésére kizárólag hiteles másolat készítése esetén van szükség.

VI.2.4.1.2 A DIGITÁLIS NYOMRÖGZÍTÉSHEZ FELHASZNÁLT ESZKÖZÖK

Adat-visszaírás elleni eszközök

- Hardveres adat-visszaírás elleni eszközök
- Szoftveres adat-visszaírás elleni eszközök

Adatmásoló eszközök

- Hardveres adatmásoló eszközök
- Szoftveres adatmásoló eszközök

Ellenőrző függvények

- hibafelismerő és -javító függvények
  - ciklikus redundancia ellenőrzés (CRC)
  - ellenőrző összeg (checksum) képzés
- kriptográfiai hasítófüggvények, különösen
  - MD5
  - SHA-1
  - SHA-2 (SHA-256)

VI.2.4.1.3 FIZIKAI ADATKINYERÉS

A fizikai adatkinyerés az adathordozó eszközszintjén történik, vagyis az adathordozó minden címezhető adattároló területének (szektorának) adattartalma kerül másolásra és mentésre. Fizikai mentés esetén lehetséges a fájlrendszer által allokálatlan tárterületekről is adatokat kinyerni, helyreállítani. Fizikai adatmentésre alkalmas digitális nyomrögzítési fajták különösen a következők:

- hiteles másolat
- hiteles lemezkép (fizikai lemezkép)
- memóriakép

VI.2.4.1.4 LOGIKAI ADATKINYERÉS

A logikai adatkinyerés az adathordozó fájlrendszerének szintjén történik, vagyis a fájlrendszer által nyilvántartott adattartalom (fájlstruktúra) kerül másolásra és mentésre. Logikai mentés esetén nem lehetséges a fájlrendszer által allokálatlan tárterületekről adatokat kinyerni, helyreállítani, mivel ezek az adatok csak az adathordozó eszközszintjén vannak jelen. Törölt állományok helyreállítása csak abban az esetben lehetséges, amennyiben ezt a fájlrendszer vagy az operációs rendszer beállításai kifejezetten támogatják (pl. Lomtár használata). Logikai adatmentésre alkalmas digitális nyomrögzítési fajták különösen a következők:

- hiteles lemezkép (logikai lemezkép)
- hiteles mentés

- hiteles letöltés

VI.2.4.1.5 ADATKINYERÉSI MÓDOK

A digitális nyomrögzítés vonatkozásában öt, alapvetően különböző adatletöltési metódus által nyerhetők ki hitelesen adatok.

- Hiteles másolat készítése
- Hiteles lemezkép készítése
- Hiteles mentés készítése
- Hiteles letöltés készítése
- Memóriakép készítése

A digitális nyomrögzítés során - amennyiben a szakértőt kirendelő hatóság másképp nem rendelkezik - törekedni kell a minél teljesebb körű adatrögzítésre, ezért az igazságügyi másolat fajtáját ennek megfelelően kell kiválasztani.

VI.2.4.1.6 A DIGITÁLIS NYOMRÖGZÍTÉSHEZ SZÜKSÉGES ESZKÖZRENDSZER ELŐKÉSZÍTÉSE

Az adatmentés metódusának kiválasztása után - amennyiben indokolt - megtörténik a digitális nyomrögzítés során felhasznált eszközrendszer bevizsgálása. Bevizsgálás az alábbi esetekben szükséges:

- új eszköz (szoftver/hardver) szakértői vizsgálati célra való bevezetése előtt;
- bevizsgált eszközben bekövetkező változás/változtatás (pl. frissítés) esetén;
- bevizsgált eszköz működésével kapcsolatban tapasztalt anomália esetén.

Az adat-visszaírás ellen alkalmazott védelmi megoldások bevizsgálásának lépései:

1. a teszteléshez használt adathordozó eszköz előkészítése,
2. az adathordozó eszköz írhatóságának tesztelése,
3. az adatváltozás ellenőrzése az adathordozó eszközön,
4. az adat-visszaírás elleni megoldás aktiválása,
5. az adat-visszaírás elleni megoldás tesztelése írási próbákkal,
6. az adatok változatlanságának ellenőrzése az adathordozó eszközön.

A digitális nyomrögzítéshez alkalmazandó eszközrendszer bevizsgálása után - amennyiben hiteles másolat készül - megtörténik a cél adathordozó(k) előkészítése, azaz fizikai felülíráson alapuló teljes törlése.

A fizikai felülíráson alapuló teljes törlés lépései:

1. a művelet alá vont adathordozó eszköz előkészítése, csatlakoztatása;
2. az adathordozó eszköz valamennyi címezhető szektorának feltöltése logikai nulla értékekkel;
3. a fizikai felülíráson alapuló teljes törölt állapot ellenőrzése összegképző ellenőrző függvény segítségével.

Az előkészítési munkafázis utolsó lépése során megtörténik a visszaírás elleni védelmi megoldás aktiválása és az előkészített eszközök csatlakoztatása.

VI.2.4.1.7 IGAZSÁGÜGYI MÁSOLAT KÉSZÍTÉSE

Az igazságügyi másolat készítésének elsődleges célja a digitális nyomok eredetben való rögzítése, vagyis a vizsgálati anyag eredeti adattartalmának megóvása, valamint a további vizsgálatok elvégzésének elősegítése. Az igazságügyi másolatnak számos fajtája van attól függően, hogy a digitális adatmásolás milyen körülmények között hajtható végre.

VI.2.4.1.8 HITELES MÁSOLAT KÉSZÍTÉSE

A másolás megvalósítása történhet hardveres vagy szoftveres eszköz útján is. A hiteles másolat készítése során alapvető követelmény a forrás adathordozó adat-visszaírás elleni védelme, a cél adathordozó esetén pedig a használatot megelőzően elvégzett fizikai felülíráson alapuló teljes törlés, amely művelet az arról készült audit jelentéssel vagy azzal azonos tartalmú egyéb forrásból származó adattal igazolható. A hiteles másolat a fizikai paramétereitől eltekintve logikailag teljesen megegyezik a forrás adathordozó adattartalmával, ezért az eredeti adathordozót helyettesítő futásidejű vizsgálatokra is alkalmas az eredeti, vagy ahhoz hasonló paraméterekkel rendelkező számítástechnikai eszköz segítségével.

Kriptográfiai hasítófüggvények segítségével a hiteles másolat adattartalmából képzett hasítóérték a vizsgált adathordozó adattartalmából képzett hasítóértékkel összevethető, így az adattartalom egyezősége, illetve változatlansága ellenőrizhető és bizonyítható.

VI.2.4.1.9 HITELES LEMEZKÉP KÉSZÍTÉSE

A másolás megvalósítása történhet hardveres vagy szoftveres eszköz útján is. A lemezképek tárolása fájlként történik, melyből következően nem szükséges minden forrás adathordozónak egy fizikai cél adathordozót megfeleltetni, amint az a hiteles másolat esetében szükséges.

A hiteles lemezkép továbbá alkalmas az eredeti adathordozót helyettesítve futásidejű vizsgálatok elvégzésére virtualizált számítástechnikai környezetben. A hiteles lemezkép készítése során alapvető követelmény a forrás adathordozó adat-visszaírás elleni védelme, ugyanakkor a cél adathordozó fizikai felülíráson alapuló teljes törlése – az adattárolás jellegéből következően – nem szükséges.

Kriptográfiai hasítófüggvények segítségével a keletkezett lemezkép állományok adattartalmából képzett hasítóérték a vizsgált adathordozó adattartalmából képzett hasítóértékkel összevethető, így az adattartalom egyezősége, illetve változatlansága ellenőrizhető és bizonyítható.

VI.2.4.1.10 HITELES MENTÉS KÉSZÍTÉSE

A hiteles mentés során a releváns állományok kinyerése közvetlenül a fájlrendszerből történő másolás által történik. A másolási folyamat végeztével a kinyert állományok hitelességét a másolandó és a másolt állományok adattartalmából képzett kriptográfiai hasítóértékek összevetése biztosítja, így az adattartalom egyezősége, illetve változatlansága ellenőrizhető és bizonyítható. Hiteles mentés készítése kizárólag akkor indokolt, amennyiben hiteles lemezkép vagy hiteles másolat készítése nem lehetséges vagy egyéb okból nem célravezető.

VI.2.4.1.11 HITELES LETÖLTÉS KÉSZÍTÉSE

A hiteles letöltés során a releváns állományok kinyerése az online társzolgáltatás által biztosított felületen keresztül kezdeményezett hálózati fájlátvitel által történik. A letöltési folyamat végeztével a kinyert állományok hitelességét a szolgáltató digitális tanúsítványa által biztosított védett csatorna és a letöltött állományok adattartalmából képzett kriptográfiai hasítóértékek biztosítják, így az adattartalom eredetisége, illetve az adatok letöltés utáni változatlansága ellenőrizhető és bizonyítható. Hiteles letöltés készítése kizárólag akkor indokolt, amennyiben hiteles lemezkép vagy hiteles másolat készítése nem lehetséges, mivel a releváns adatokat tartalmazó adathordozó(k) fizikailag nem elérhető(ek), virtualizáltak.

VI.2.4.1.12 MEMÓRIAKÉP KÉSZÍTÉSE

Memóriakép készítése során a vizsgált digitális eszköz operatív tára (RAM) – vagy egyéb folyamatos áramellátást igénylő tárolójának – adattartalmának másolása történik egy vagy több adatállományba. Memóriakép készítése kizárólag akkor indokolt, amennyiben a bekapcsolt állapotú digitális eszköz operatív tára vélhetően olyan releváns változékony adatokat tartalmaz, amelyek az eszköz kikapcsolásával visszavonhatatlanul elvesznek, ezáltal akadályozzák a szakértői vizsgálatot. A memóriakép kriptográfiai hasítófüggvénnyel bitre pontosan azért nem hitelesíthető, mivel az operatív tár tartalma a memóriakép készítése során is folyamatosan változik.

Kriptográfiai hasítófüggvények segítségével a keletkezett lemezkép állományok adattartalmából képzett hasítóérték a vizsgált adathordozó adattartalmából képzett hasítóértékkel összevethető, így az adattartalom egyezősége, illetve változatlansága ellenőrizhető és bizonyítható.

A művelet során keletkező memóriakép állomány adattartalmáról kriptográfiai hasítófüggvénnyel készített hasító érték készítése révén biztosítható a rögzített adatok utólagos változatlanságának ellenőrizhetősége.

VI.2.4.1.13 ADATKINYERÉS EREDMÉNYÉNEK DOKUMENTÁLÁSA ÉS ÉRTÉKELÉS

A digitális nyomrögzítési módszer alkalmazása után – amennyiben a kiválasztott metódus azt lehetővé teszi – ellenőrizni kell a forrás adattartalomból és a másolt adattartalomból képzett kriptográfiai hasítóértékek egyezőségét.

Amennyiben a digitális nyomrögzítés során naplózott kommunikáció került alkalmazásra, akkor ellenőrizni szükséges a keletkezett naplóállomány tartalmát.

Amennyiben a forrás adathordozó vagy az átviteli csatorna hibás működése miatt olvashatatlan vagy következetlen tartalmú adatterületek kerülnek azonosításra, dokumentálni kell a hiba kiterjedését (mely szektorok érintettek), valamint hogy a mérettartó másolatok (lemezképek) esetében a hibás forrásadatok milyen logikai értékekkel lettek helyettesítve (bitmintázat). Az olvasható adattartalom egyezőségét hibás forrás adathordozó esetében is szükséges igazolni, ezért az olvasható adatterületek tartalmáról részleges kriptográfiai hasítóértéket kell készíteni.

Az adatmentési folyamat során bekövetkezett másolási hibák előfordulásának tényét fel kell tüntetni a szakértői véleményben.

- egyedi azonosító (gyártó, modellszám, sorozatszám, eszközcímke stb.),
- a digitális adat forrása (az adathordozó eszköz megtalálásának helyszíne és helye),
- egyedi vizsgálati azonosítók (ügyszám, helyszín azonosító, nyomozócsoport azonosítója stb.),
- megszerzett adatok hasító értékei (helyszíni adatmentés esetén),
- Az adathordozók azonosításakor, összegyűjtésekor és az adat kinyerésekor készített digitális fényképek (üggyel kapcsolatos azonosítókkal)
- az adatkinyerést végző személy neve és beosztása
- az adatkinyerés dátuma és ideje
- az adatkinyerés során felmerült hibák leírása
- a szervezet által előírt további dokumentáció

VI.2.4.2 Vizuális adatrögzítés

A vizuális adatrögzítés metódusának kiválasztása az eszközfelmérés eredményének figyelembe vételével történik.

A vizuális adatrögzítési módszer elsősorban abban az esetben alkalmazandó, amikor a vizsgált digitális eszköz működőképes, azonban informatikai szempontból alkalmatlan a digitális nyomrögzítésre.

A vizuális adatrögzítés vonatkozásában az alábbi metódusok alkalmazásával rögzíthetőek egy digitális eszköz képernyőjén vagy kijelzőjén megjelenő adatok.

- Képernyőkép készítése
- Képernyőfelvétel készítése
- Kijelzőfotó készítése
- Videófelvétel készítése
- Szemrevételezés és dokumentálás

A vizuális adatrögzítés során - amennyiben a szakértőt kirendelő hatóság másképp nem rendelkezik - törekedni kell a minél teljesebb körű adatrögzítésre, ezért az adatrögzítés metódusát ennek megfelelően kell kiválasztani. Ennek megfelelően - amennyiben az műszakilag megvalósítható - törekedni kell a közvetlen, digitális alapú képernyőkép-rögzítési módszerek alkalmazására az optikai képrögzítési metódusokkal szemben.

VI.2.4.2.1 A VIZUÁLIS ADATRÖGZÍTÉSHEZ KAPCSOLÓDÓ FOGALMAK MEGHATÁROZÁSA

Képernyőkép (screenshot)

Digitális eszköz képernyőjén működés közben megjelenő adattartalomról szoftveres úton készített digitális képállomány. A képi adattartalom közvetlenül digitális formában kerül rögzítésre, optikai torzítás és mintavételi zaj nélkül.

Kijelzőfotó

Digitális eszköz képernyőjén vagy kijelzőjén működés közben megjelenő adattartalomról optikai fényképezés útján készített analóg vagy digitális fénykép. A fénykép készítése során optikai torzítás és mintavételi zaj lép fel. A kijelzőfotók készítésének folyamata a kifotózás.

Képernyőfelvétel (screencast)

Digitális eszköz képernyőjén működés közben megjelenő adattartalomról szoftveres úton készített digitális videóállomány. A képi adattartalom közvetlenül digitális formában kerül rögzítésre, optikai torzítás és mintavételi zaj nélkül. A képernyőfelvétel adott esetben dokumentáló hangsávot is tartalmazhat.

Képernyőtükrözés

Egy digitális eszköz kijelzőjén vagy képernyőjén megjelenő adattartalmak eredetben és valós időben történő másolása és megjelenítése egy másik készüléken.

VI.2.4.2.2 A VIZUÁLIS ADATRÖGZÍTÉSHEZ SZÜKSÉGES ESZKÖZÖK

Optikai (mozgó)képrögzítéshez szükséges eszközök

- fényképezőgépek;
- videókamerák;
- fényképező állványok;
- fotódobozok.

Kijelzők digitális adattartalmának rögzítéséhez szükséges eszközök

- screenshot (képernyőkép) készítő szoftverek;
- screencast (képernyőfelvétel) készítő szoftverek és hardverek;
- képernyőtükrözésre alkalmas szoftverek és hardverek.

VI.2.4.2.3 A VIZUÁLIS ADATRÖGZÍTÉSHEZ SZÜKSÉGES ESZKÖZRENDSZER ELŐKÉSZÍTÉSE

A vizuális adatrögzítési metódus kiválasztása után – amennyiben indokolt – megtörténik az adatrögzítés során felhasznált eszközrendszer bevizsgálása. A rendeltetésszerű működés meglétének ellenőrzése után megtörténik az eszközök előkészítése az adatrögzítésre.

Videókamera esetében fontos az akkumulátor töltöttségének ellenőrzése vagy a készülék folyamatos tápellátásának biztosítása legalább a felvétel becsült időtartama erejéig, valamint a videófelvétel rögzítéséhez szükséges tárterület biztosítása.

A vizsgálati eszköz segítségével létrehozott képernyőképek és képernyővideók készítéséhez, illetve a képernyőtükrözéshez szükséges szoftverek telepítését vagy futtatását megelőzően – amennyiben a végrehajtás sikeressége kétséges – célszerű a rögzítéshez felhasználandó szoftverek (a vizsgálandó eszközzel) típusazonos eszközön történő bevizsgálása.

VI.2.4.2.4 KÉPERNYŐKÉP KÉSZÍTÉSE

Képernyőképek készítése során a vizsgált digitális eszköz képernyőjén működés közben megjelenő releváns adattartalomról szoftveres úton digitális képállományok kerülnek létrehozásra. A képernyőkép létrehozható natív módon (azaz közvetlenül a vizsgált eszköz segítségével, amennyiben biztosítható a bizonyítási eljárás során felhasznált egyéb adatok változatlansága), illetve képernyőtükrözés segítségével a másolt képernyőt fogadó eszközön futtatott képrögzítő szoftver által.

VI.2.4.2.5 KÉPERNYŐFELVÉTEL KÉSZÍTÉSE

Képernyőfelvétel készítése során a vizsgált digitális eszköz képernyőjén működés közben megjelenő releváns adattartalomról, valamint a digitális eszköz működtetésének és kezelésének folyamatáról szoftveres úton digitális videófelvételek kerülnek létrehozásra. A képernyőfelvétel létrehozható natív módon (azaz közvetlenül a vizsgált eszköz segítségével, amennyiben biztosítható a bizonyítási eljárás során felhasznált egyéb adatok változatlansága), illetve képernyőtükrözés segítségével a másolt képernyőt fogadó eszközön futtatott videórögzítő szoftver által.

VI.2.4.2.6 KIJELZŐFOTÓ KÉSZÍTÉSE

A kifotózás során a digitális eszköz képernyőjén vagy kijelzőjén működés közben megjelenő adattartalomról optikai fényképezés útján készülnek analóg vagy digitális fényképek. Mivel a fénykép készítése során optikai torzítás és mintavételi zaj lép fel, ezért lehetőség szerint inkább képernyőképek készítésére kell törekedni. Kijelzőfotók készítésére akkor kerülhet sor, amennyiben az műszakilag célszerűen nem megvalósítható.

VI.2.4.2.7 VIDEÓFELVÉTEL KÉSZÍTÉSE

Videófelvétel során a digitális eszköz képernyőjén vagy kijelzőjén működés közben megjelenő adattartalomról optikai fényképezés útján készülnek analóg vagy digitális mozgóképfelvételek. Mivel a videófelvétel készítése során optikai torzítás és mintavételi zaj lép fel, ezért lehetőség szerint inkább képernyőfelvételek készítésére kell törekedni. Videófelvétel készítésére akkor kerülhet sor, amennyiben az műszakilag célszerűen nem megvalósítható, illetve amennyiben a képernyőtartalmon felül az eszköz kezelését is szükséges folyamatában dokumentálni.

VI.2.4.2.8 SZEMREVÉTELEZÉS ÉS DOKUMENTÁLÁS

Amennyiben a vizsgált digitális eszköz képernyőjén vagy kijelzőjén megjelenő információk valamely oknál fogva sem digitálisan, sem pedig optikai úton nem rögzíthetőek célszerűen, akkor a megjelenített adatok szemrevételezéssel és írásos dokumentáció formájában kerülnek rögzítésre. Ezen adatrögzítési metódus eredménye a szemrevételezési jegyzőkönyv.

VI.2.4.2.9 A VIZUÁLIS ADATKINYERÉS EREDMÉNYÉNEK DOKUMENTÁLÁSA ÉS ÉRTÉKELÉSE

A vizuális adatrögzítési módszer alkalmazása után ellenőrizni kell a rögzített adatok felhasználhatóságát. A felhasználhatóság ellenőrzésének szempontjai - különösen az optikai képrögzítést használó metódusok esetében - a megfelelő fókuszáltság, a megfelelő fényerő- és kontrasztarány, valamint a képileg rögzített szöveg olvashatósága. Ez utóbbi esetében ellenőrizni szükséges a képileg rögzített szöveg alkalmasságát a későbbi leiratozásra vagy optikai karakterfelismerésre. A szemrevételezés és dokumentálás metódusának alkalmazása után a szemrevételezési jegyzőkönyv ellenőrzése szükséges. Az átadásra kerülő digitális kép- és mozgóképfelvételek laikustól is elvárható módon megjeleníthető formátumokat kell, hogy kövessenek.

VI.2.4.3 Adattartalom hozzáférhetőségének biztosítása

Az adattartalom hozzáférhetősége biztosítására szolgáló metódus kiválasztása az eszközfelmérés eredményének, valamint az adattartalom feldolgozási módszer alkalmazása során felmerülő adathozzáférési akadályok figyelembe vételével történik. Minden esetben az adathozzáférési akadály elhárítására leginkább alkalmas metódus kerül kiválasztásra.

VI.2.4.3.1 A MÓDSZERHEZ KAPCSOLÓDÓ FOGALMAK MEGHATÁROZÁSA

Chip

Integrált áramköri lapka, jellemzően különféle kivezetésű tokban helyezkedik el, amely nyomtatott áramkörre (NYÁK) van forrasztva.

Chip-off

Az integrált áramköri lapkának egy digitális eszköz nyomtatott áramköréről való eltávolítására irányuló módszer. A módszer irányulhat a lapka beültetésének előkészítésére vagy a lapka adattartalmának közvetlen kiolvasására.

JTAG

A Joint Test Action Group által kidolgozott ipari szabvány[12], amely a nyomtatott áramkörök tesztelésére irányul. A szabvány meghatározza egy olyan interfészt használó hibakeresési port használatát, amely nem igényli a rendszercímre és az adatbuszokra való közvetlen külső kapcsolódást. Az interfész a chipen lévő teszt hozzáférési porthoz (TAP) csatlakozik, amely a chip tesztregisztereihez ad hozzáférést. A JTAG szabványt követő eszközök lehetővé teszik, hogy az adott vizsgálati eszköz alaplapján meghatározott szervizpontokhoz csatlakoztatva közvetlenül el lehessen érni az adattárolásért felelős memóriát.

[12] IEEE 1149.1 - IEEE Standard for Test Access Port and Boundary-Scan Architecture

PIN

Személyes azonosítószám (Personal Identification Number). A PIN tudás alapú felhasználó hitelesítési forma, virtuális számzár.

PUK

PIN feloldó kulcs (PIN Unlock Key). A PUK segítségével átírható az elfelejtett vagy ismeretlen PIN.

ICCID

A SIM kártya integrált áramköri lapkájának (illetve eSIM esetében a virtuális SIM kártya) azonosítószáma (integrated circuit card identifier).

IMSI

Nemzetközi mobil előfizetői azonosító (international mobile subscriber identity). A mobil felhasználó egyedi azonosítására alkalmas kód, mely tartalmazza az előfizetőre vonatkozó összes információt, beleértve a hozzárendelt előfizetői hívószámot.

IMEI

Nemzetközi mobileszköz azonosító (International Mobile Equipment Identity). Az IMEI tartalmazza a típusengedélyező kódot, a gyártói/összeszerelői kódot, illetve a készülék egyedi azonosítóját.

ISP

Az In-system Programming vagy In-Circuit Serial Programming (ICSP) egyes programozható logikai eszközök (PLC), mikrokontrollerek és beágyazott eszközök azon tulajdonsága, amely által az áramkörbe való beépítésük után is programozhatóak maradnak.

NYÁK

Nyomtatott áramkör.

SIM

Előfizető azonosító modul (subscriber identification module), amely biztonságosan tárolja az IMSI és ICCID azonosítókat és egyéb adatokat, amelyek a mobilszolgáltatás előfizetőjének azonosítására szolgálnak. A modul tartalmazhatja továbbá a kártya saját operációs rendszerét, alkalmazásokat, az operációs rendszer patch fájljait, valamint az előfizető által feltöltött személyes információkat (biztonsági kódok, telefonkönyv, stb.).

Szolgáltató

Információtechnológiai szükségletet kielégítő fél, aki a nyújtott szolgáltatásával vagy termékével kapcsolatban teljes jogú adatkezelő, ezért termékéről vagy felhasználóiról érdemi felvilágosítást képes adni. Jelen értelmezésben szolgáltatónak minősülnek a távközlési hálózatok üzemeltetői, a digitális eszközök gyártói vagy a szoftverek programozói is.

Kulcstér

A matematikailag lehetséges kulcsok halmaza (titkosítás területén).

Brute-force támadás

A titkosító algoritmus ismeretében az alkalmazott kulcs meghatározásának folyamata a teljes kulcstér végig próbálása útján.

TPM

A Trusted Platform Module egy biztonságos kriptoprocesszor nemzetközi szabványa (ISO/IEC 11889). A TPM egy dedikált mikrokontroller, amelyet hardverek integrált kriptográfiai kulcsok segítségével történő biztosítására terveztek.

VI.2.4.3.2 A MÓDSZERHEZ SZÜKSÉGES ESZKÖZÖK

A módszer alkalmazása során elsősorban az elektronikai működőképesség helyreállításának metódusának végrehajtásához szükségesek az alábbi anyagok:

- Ultrahangos tisztító berendezés által használt szerves oldószerek
  - etanol (etil-alkohol)
  - metanol (metil-alkohol)
- Általános víztaszító tisztítószer
- Forrasztási műveletekhez felhasznált anyagok
- Hőelvezetéshez felhasznált anyagok

VI.2.4.3.3 A MÓDSZERHEZ SZÜKSÉGES ESZKÖZRENDSZER ELŐKÉSZÍTÉSE

Az adattartalomhoz való hozzáférhetőség biztosításának metódusa kiválasztása után - amennyiben indokolt - megtörténik a metódus alkalmazásához szükséges eszközrendszer előkészítése. Az adathozzáférési akadályok elhárítására különösen az alábbi metódusok és azok kombinációi alkalmazhatóak:

VI.2.4.3.4 Szolgáltatói adatkérés

Adatkérés a szolgáltatótól vagy az eszköz gyártójától.

A gyártótól való adatkérés magába foglalja a vizsgált eszközhöz, illetve annak felhasználójához köthető olyan információkat, amelyeket kizárólag vagy leginkább az eszköz gyártója vagy forgalmazója ismerhet.

Az adatkérés eredménye a közvetlenül a szolgáltatótól vagy gyártótól származó adatok összessége, amelyek vagy nem igényelnek további adatrögzítést, vagy pedig további adatrögzítési módszerek alkalmazását teszik lehetővé.

VI.2.4.3.5 Felhasználói hitelesítés feloldása

A feloldási kísérlet különösen az alábbi módokon történhet

- hardveres,
- szoftveres,
- manuális (tulajdonoshoz/profilhoz köthető adatok alapján)

A feloldási kísérlet különösen az alábbi hitelesítési módokra irányulhat

- tudás alapú hitelesítés
  - ~ jelzár feloldása
  - ~ számzár (PIN) feloldása
  - ~ jelszó feloldása
- tulajdonság alapú hitelesítés feloldása
  - ~ biometrikus jellemző azonosítása (ujjnyom, arcgeometria, stb.)
  - ~ egyéb mért jellemzők azonosítása (pulzus, testhő, stb.)
  - ~ biometrikus minta beszerzése
  - ~ a mért jellemzők szimulálása
- birtoklás alapú hitelesítés feloldása
  - ~ token alkalmazása
  - ~ hardverkulcs (dongle) alkalmazása

A felhasználói hitelesítés feloldása után lehetővé válhat a digitális nyomrögzítés vagy a vizuális adatrögzítés.

VI.2.4.3.6 TITKOSÍTÁS FELOLDÁSA

A titkosítás feloldása az alábbi általános lépések végrehajtása alapján történik:

- a titkosítás jellegének azonosítása
  - teljes lemeztitkosítás;
  - kriptopartíció;
  - kriptokonténer;
  - fájlrendszer alapú titkosítás;
  - fájl szintű titkosítás;
  - egyéb titkosítás.
- a titkosító szoftver, szabvány és az általa használt algoritmusok azonosítása
  - a titkosító szoftverek és szabványok azonosítása;
  - a titkosító algoritmusok és eljárások azonosítása;
- a titkosító kulcs hasítóértékének kinyerése
  - a behúzókötet (boot volume) szektoraiból;
  - a logikai kötet szektoraiból;
  - közvetlenül a kriptokonténer állományból;
  - egyéb adatforrásból (hardverkulcs, hálózati csomagelfogás, stb.);
    - kulcstörés
  - brute-force alapú – a teljes kulcstér végig próbálása;
  - szótár alapú – a valószínű kulcsok generált halmazának végig próbálása;
  - a felsoroltak kombinációja;
- a titkosított adattartalom visszafejtése
  - sikeres kulcstörés esetén a nyílt adattartalom hozzáférhetővé tétele;
  - amennyiben lehetséges/szükséges, a titkosító kulcs előállításához felhasznált eredeti hitelesítő adat (jelszó, PIN, biometrikus sablon, stb.) kinyerése.

A titkosítás sikeres feloldása után lehetővé válik a digitális nyomrögzítés.

VI.2.4.3.7 ELEKTRONIKUS HOZZÁFÉRÉS BIZTOSÍTÁSA

Az elektronikus hozzáférés biztosítására a digitális eszköz részlegesen vagy teljesen működésképtelen állapota esetén kerül sor különösen a következő módokon:

- JTAG alapú hozzáférés
  - közvetlen memória olvasás vagy írás biztosítása hozzáférési tesztportokon (TAP) keresztül érintkezőlábak vagy vezetékforrasztás segítségével
- ISP (In-system Programming) alapú hozzáférés
  - közvetlen memória olvasás vagy írás biztosítása ISP-képes beágyazott eszközök programozása útján
- Áramköri alapú közvetlen hozzáférés
  - a vizsgált áramköri lapka eltávolítása és megtisztítása (chip-off)
  - közvetlen adatolvasás a chip érintkezőiről (NAND read)

VI.2.4.3.8 Elektronikai működőképesség helyreállítása

Az eszköz adathordozóján tárolt adatok kinyerése érdekében szükség lehet a digitális eszköz működőképességének helyreállítására. A működőképesség helyreállítása nem a digitális eszköz teljes javítására irányul, mindössze a rajta tárolt adattartalom rögzítésének lehetővé tételére.

- Alkatrésztisztítás
  - szennyeződés miatt működésképtelen alkatrészek tisztítása
- Alkatrészcsere
  - kijelző csere
  - tasztatúra csere
  - csatlakozó aljzat csere
  - egyéb, a működőképesség biztosításához szükséges alkatrészek cseréje
- Integrált áramköri lapka eltávolítása és/vagy átültetése
  - típusazonos digitális eszköz felhasználása alkatrészdonorként vagy befogadó áramkörként
  - működőképes NYÁK biztosítása chip kiforrasztásával vagy kicsiszolásával a donor eszközből (chip-off)
  - a vizsgált chip beültetése a donor áramkörbe forrasztással (reballing) vagy stencilezéssel

Az elektronikai működőképesség helyreállítása a bűnjel eredeti állapotának megváltozásával járhat, ezért a metódus alkalmazása előtt a szakértőt kirendelő hatóság előzetes írásbeli hozzájárulása szükséges.

Az elektronikai működőképesség helyreállítása után lehetővé válhat a digitális nyomrögzítés vagy a vizuális adatrögzítés.

VI.2.4.3.9 Adattároló tömbök adattartalmához való hozzáférés biztosítása

Amennyiben egy információtechnológiai eszköz több digitális adathordozó kombinációjából álló logikai lemez segítségével valósítja meg az adattárolást, akkor a digitális nyomrögzítés megkezdése előtt szükség lehet az adattárolási megoldás azonosítására és az adattartalom közvetlen hozzáférhetőségének biztosítására.

Lemeztömb (RAID)

A RAID (Redundant Array of Independent Disks - független lemezek redundáns tömbje) egy olyan tárolási technológia, amelynek segítségével az adatok elosztása vagy replikálása több fizikailag független adathordozón, egy (vagy több) kötet létrehozásával valósul meg.

A RAID tömbök szakértői vizsgálatot befolyásoló tényezői különösen a következők:

- jelszavazott vagy más módon védett RAID vezérlő
- ismeretlen, ritka vagy egyedi RAID megvalósítási fajta
- ismeretlen az elemek sorrendje a tömbben
- az elemek sorozatszámát (vagy más egyedi jellemzőjét) nyilvántartó vezérlő

Elsődlegesen a tömb által képezett logikai lemez szintjén (és nem az elemek szintjén) kell megvalósítani az adatmentést. A logikai lemezek kezeléséhez különösen az alábbi eszközöket és műveleteket szükséges alkalmazni:

- eredeti RAID konfiguráció szerinti vezérlő hardver,
- külső adathordozóról történő rendszerbetöltés (boot) RAID kezelésre alkalmas működtető rendszer alkalmazásával,
- RAID konfiguráció emulálására alkalmas szoftver.

Másodlagosan – amennyiben a logikai lemez adatmentése nem lehetséges – a RAID tömb elemenkénti (a RAID tömböt alkotó fizikai adathordozók egyenkénti) adatmentése szükséges. A RAID tömb elemeiről készült önálló lemezképek felhasználásával – a RAID tömb részletes paramétereinek ismeretében – a RAID tömb adattartalmához történő hozzáférés megkísérelhető.

Amennyiben a RAID tömb helyreállítása sikeres megkezdődhet a digitális nyomrögzítés.

LEMEZFÜRT (CLUSTERED FILE SYSTEM)

A fürtölt fájlrendszer egy olyan tárolási technológia, amelynek segítségével az adatok elosztása vagy többszörözése több hálózatba kötött, de fizikailag független számítógép adathordozóin, egy (vagy több) logikai lemez létrehozásával valósul meg. Lemezfürtöket általában felhő alapú tárolás megvalósítására alkalmaznak, a lemezfürtben részt vevő adattárolók száma működés közben is rugalmasan bővíthető.

Lemezfürtök megvalósításának gyakori módja a lemez-megosztásos fájlrendszer, amely egy adattároló hálózat (storage area network, SAN) segítségével blokk-szintű közvetlen lemez-hozzáférést biztosít több számítógép részére.

Lemezfürt esetében csak a fürtölt fájlrendszer által megvalósított logikai lemezek adattartalmához szükséges a hozzáférést biztosítani. Mivel a lemezfürt több hálózatba kötött – ezért szükségszerűen bekapcsolt állapotban lévő – informatikai eszközből áll, különös körültekintéssel szükséges eljárni a lemezfürtök adattartalmához való hozzáférés biztosítása, illetve az azt követő digitális nyomrögzítés során.

Amennyiben a lemezfürt adattartalma hozzáférhető, akkor ezután megkezdődhet a digitális nyomrögzítés.

VI.2.4.4 Adatok elemzése

A digitális adatok elemzését oly módon kell elvégezni (pl. másolat elemzése, írásvédő használata stb.), hogy a digitális adat módosulásának lehetősége minimális legyen.

Amennyiben a vizsgálat az elemzés során az eredeti digitális nyom megváltozik, akkor ennek tényét, okait és hatásait részletesen ismertetni kell a vizsgálatról szóló dokumentumokban.

Az elemzést oly módon kell elvégezni és dokumentálni, hogy független szakértő képes legyen a vizsgálat és elemzés folyamatait követni és megítélni az egyes meghozott döntések helyességét, illetve a dokumentáció alapján a vizsgálatot azonos eredménnyel elvégezni.

VI.2.4.4.1 Az elemzéssel kapcsolatos fogalmak meghatározása

Adattöredékek összerendelése

Strukturált adatok nyers adatfolyamból történő kinyerése az eredeti fájlrendszerre vonatkozó ismeretek hiányában fájlformátum specifikus jellemzők keresése és azonosítása révén (angol nyelvű szakirodalomban data carvig, file carving, magyar nyelvű szoftverlokalizációs terminológia szerint adatvésés).

Obfuszkáció

Az obfuszkáció egy olyan program-transzformáció, mely a program eredeti funkcionalitásának megőrzésével a program forráskódját vagy akár a működését változtatja meg, azzal a céllal, hogy a programban információt rejtsen el (pl. közvetlenül olvasható, kereshető karakterláncok rejtése). A szoftverfejlesztés területén elterjedt kódobfuszkáció kifejezés olyan obfuszkációs technikákra utal, melyek célja megnehezíteni a program működésének megértését, statikus vagy dinamikus elemzését, illetve ismeretlen forráskód esetén a kód visszafejtését.

VI.2.4.4.2 Az elemzéshez felhasznált eszközök és azok jellemzői

Az elemzéshez a szakértő hardver és szoftver eszközök kombinációját használja, melyek támogatják a vizsgálati folyamatokat és megfelelnek az alábbi követelményeknek

- **felülvizsgálhatóság**

  A felülvizsgálat annak megerősítésé objektív bizonyítékok által, hogy a meghatározott követelmények teljesültek (angol nyelvű szakirodalomban *verification*). *Az ellenőrzés csupán arra nyújt biztosítékot, hogy a termék megfelel a vonatkozó előírásoknak.*

- **érvényesség**

  Az érvényesítés annak megerősítése objektív bizonyítékok révén, hogy a rendeltetésszerű használat, vagy alkalmazás követelményei teljesültek egy adott dologra vonatkozóan (angol nyelvű szakirodalomban validation). *Érvényesítést hajtanak végre a folyamaton annak érdekében, hogy az megfeleljen a célnak, vagyis annak biztosítására, hogy a folyamat a várt eredményekkel, ellentmondás mentesen, megismételhetően és reprodukálható módon valósuljon meg.*

- **megerősíthetőség**

  A megerősítés objektív bizonyíték hivatalos ellenőrzése arra vonatkozóan, hogy egy folyamat megfelelő (vagy továbbra is alkalmas) a meghatározott célra (angol nyelvű szakirodalomban confirmation).

A felsorolt feltételeknek megfelelő eszközök (hardver és szoftver) különösen a következők lehetnek:

- törölt állományok helyreállítására alkalmas szoftverek és hardverek;
- adatvésésre alkalmas szoftverek;
- szoftveres szűrők;
- kereső algoritmusok;
- adatbázis szoftverek;
- optikai karakterfelismerő szoftverek;
- digitális adatfeldolgozó és -elemző szoftverek;
- digitális könyvjelzőzésre alkalmas szoftverek;
- digitális jelentések készítésére alkalmas szoftverek és hardverek;
- manuális elemzést elősegítő szoftverek.

VI.2.4.4.3 Az elemzés során keletkező nyilvántartások

Az elemzés során az eljárást végző szakértőnek és az eljárásban résztvevő személyeknek a felügyeleti lánc betartása mellett az elemzés során megfelelő részletességű feljegyzést szükséges készítenie az elvégzett tevékenységekről.

A dokumentálást olyan kell elvégezni és dokumentálni, hogy független szakértő képes legyen a vizsgálat és elemzés folyamatait követni és megismételni a vizsgálatokat azonos eredménnyel.

Az eljáró szakértő a szakértői vizsgálatokról feljegyzéseket készít, melyek tartalmazzák különösen az elvégzett digitális nyomrögzítés, a vizuális adatrögzítés, az adattartalom feldolgozás, illetve az adattartalom hozzáférhetőségével kapcsolatos eredmények, továbbá minden olyan információ, melyek a szakvélemény megállapításait támasztják alá, az elvégzett műveleteket részletezik. A feljegyzések - szüksége szerint - a szakértői vélemény tartalmi részét képezhetik. A szakértő a feljegyzéseket saját nyilvántartási rendszere szerint azonosítja és tárolja.

> *Valamennyi feljegyzést azonosítóval, futó sorszámmal, a lapok alján dátummal, aláírással lát el az eljáró szakértő, majd azokat feltünteti az ügydosszié tartalomjegyzékében.*

Amennyiben kijelzőfotók és videófelvételek készítéséhez fényképezőgépek és videókamerák kerültek felhasználásra, akkor a különböző ügyek és bűnjelek felvételeinek keveredésének megakadályozása céljából az adatok rögzítése és másolása után törölni kell a készülékek adathordozóján elhelyezkedő adatokat.

Az eljáró szakértő a szakértői véleményhez szükség esetén szakértői adathordozót készít.

A szakértői adathordozó a szakértői vélemény melléklete, amely a szakértői vélemény elektronikus példányát, a vizsgálati anyagról készített képi dokumentációt, illetve - amennyiben a vizsgálat során feltárásra került - az eredetben rögzített digitális nyomokat, valamint a terjedelmi vagy gyakorlati okok miatt papír alapon meg nem jelenített/jeleníthető adatokat tartalmazza illetve tartalmazhatja. A szakértői adathordozó tartalmilag a szakértői vélemény szerves részét képezi, attól logikailag nem elválasztható.

A szakértői adathordozó adattartalmának általános felépítése:

- a vizsgálati tárgyakról, illetve a szerelési folyamatról készített képi dokumentáció,
- a vizsgált adathordozók digitális adattartalmának igazságügyi másolatai (amennyiben átadásuk szükséges),
- az adattartalom elemzése során készített digitális jelentések, vizsgálati eredmények,

- az átadott adatok megjelenítéséhez adott esetben szükséges speciális szoftverek (amennyiben átadásuk szükséges),
- a szakértői adathordozón elhelyezett állományok tartalmi és mennyiségi ellenőrizhetőségét biztosító hiteles állománylista,
- a szakértői vélemény elektronikus példánya,
- egyéb, szükség szerint értelemszerűen létrehozott könyvtárstruktúrák (amennyiben átadásuk szükséges).

A szakértői adathordozó pontos könyvtárszerkezetét a szakértői vélemény melléklete tartalmazhatja digitális formában.

VI.2.4.4.4 Az eredeti állapot igazolásának eszközei

A szakértői adathordozón átadásra kerülő fájlok sértetlenségének ellenőrizhetősége érdekében az eredeti állapot igazolására alkalmas, valamely alkalmas eszközzel automatikusan ellenőrizhető formátumú igazoló adatot kell létrehozni, melyet a szakértői véleménnyel együtt (annak mellékleteként) digitális formában kell átadni a kirendelőnek / megbízónak.

Egyedi digitális lenyomat (hash value, hasító függvény érték)

A hasító vagy hash függvény definíció szerint „A hash függvény egy üzenetet feldolgozva kimenetként egy hash kódot állít elő. Pontosabban a hash függvény egy tetszőleges hosszúságú bitfolyamból véges hosszúságú bitsorozatot állít elő."[13] A digitális adat eredeti állapotát a digitális adat megszerzésekor vagy kinyerésekor készített egyedi digitális lenyomat igazolja.

Az egyedi digitális lenyomat vonatkozhat egy vagy több digitális bizonyítékra, vagy azok csoportjára.

Az eredeti állapot igazolására alkalmas egyirányú, kulcs nélküli módosítás azonosító kriptográfiai algoritmusok (Modification Detection Code - MDC) különösen a következők:

- MD5 (Message-Digest algorithm 5)[14] - használata még elfogadható abban az esetben, ha más típusú hasító érték előállítása nem megvalósítható,
- SHA-1 (Secure Hash Algorithm - 1) - használata még elfogadott,
- SHA-2 (Secure Hash Algorithm - 2)[15] - használata javasolt.

---

[13] Menezes, Alfred J., -van Oorschot, Paul C. and Vanstone, Paul C.: Handbook of Applied Cryptography, CRC Press, 1997. p. 321.

[14] http://www.ietf.org/rfc/rfc1321.txt

[15] https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/shs/SHAVS.pdf

Időbélyeg (time stamp)

Olyan időértéket tartalmazó paraméter, mely egy adott időpont viszonyát jelzi egy referencia időhöz (pl. a koordinált világidőhöz) képest.[16]

Digitális adat hordozójának teljes tartalomjegyzéke

Strukturált szöveges állomány, táblázat, adatbázis vagy egyéb állomány mely a digitális adat hordozó teljes tartalmára vonatkozó listát tartalmaz a következő adatokra vonatkozóan:

Filename	állománynév
Full Path	elérési útvonal a digitális adathordozón
Size (bytes)	méret
Created	létrehozási dátum és idő (nem időbélyeg)
Modified	módosítás dátuma és ideje (nem időbélyeg)
Accessed	hozzáférés dátuma és ideje (nem időbélyeg)
Is Deleted	logikai törlés állapota (yes/no)

VI.2.4.4.5 A MÓDSZERHEZ SZÜKSÉGES ESZKÖZRENDSZER ELŐKÉSZÍTÉSE

Az adatfeldolgozásnak számos metódusa van, amelyek a szakértőt kirendelő határozatban előírt szakértői feladatok jellegéhez illeszkednek. Minden esetben a szakkérdések megválaszolására leginkább alkalmas metódusok kerülnek kiválasztásra.

Az adatfeldolgozási metódus kiválasztása után - amennyiben indokolt - megtörténik a metódus alkalmazásához szükséges eszközrendszer előkészítése.

Az adatfeldolgozáshoz az alábbi metódusok és azok kombinációi alkalmazhatóak:

VI.2.4.4.6 TÖRÖLT ADATTARTALMAK HELYREÁLLÍTÁSA

Amennyiben a szakkérdés megválaszolása azt indokolja, szükség lehet a törölt állományok helyreállítására és/vagy a fájlrendszer által nem nyilvántartott digitális adatok kinyerésére.

Törölt állományok helyreállítása

A metódus alkalmazása során a fájlrendszer (vagy az operációs rendszer) által töröltként nyilvántartott, de más adatok által még felül nem írt allokálatlan tárterületeken elhelyezkedő állományok helyreállítása történik meg. Egy törölt állomány helyreállítása gyakorlatilag a fájlrendszer nyilvántartásában meglévő inaktív (allokálatlan) állománybejegyzések aktívvá (allokálttá) módosítása útján történik meg.

---

[16] Kapcsolódó szabvány: MSZ EN ISO/IEC 27037:2016, 3.22

Törölt állományok helyreállítása csak abban az esetben lehetséges, amennyiben ezt a fájlrendszer működési elve, vagy az operációs rendszer beállításai ezt kifejezetten támogatják (pl. Lomtár, Trashes, Lost & Found, stb. használata). Egy törölt állomány helyreállítása során a fájlrendszer működési elvétől függően a fájl eredeti elnevezése teljesen vagy csak részlegesen állítható helyre. Részleges helyreállíthatóság esetében a helyreállíthatatlan karaktereket helyettesítő karakterek jelölhetik.

Adattöredékek összerendelése

Az adattöredékek összerendelése (data carving, file carving, adatvésés) olyan metódus, amelynek során a fájlrendszer mellőzésével, az adathordozó egymást követő fizikai tárolóegységeiben (szektoraiban) egymást követően elhelyezkedő adatok kerülnek kinyerésre meghatározott ismérvek alapján.

A metódus alkalmazása során lényegében a fizikailag elérhető folytonos tárterület adatfolyamának olvasása során meghatározott kezdési és végződési minták alapján mesterséges állományok kerülnek kihasításra, létrehozásra. A kezdési (header, fejléc) és végződési (footer, lábléc) mintákat az adatvésés során keresett adott fájlformátum – az esetek többségében szabványban rögzített – jellemzői, adatstruktúrái határozzák meg.

Mivel az adattöredékek összerendelésével kinyert/előállított állományok nem rendelkeznek eredeti fájlnévvel, ezért a fájlneveik automatikusan kerülnek létrehozásra, célszerűen annak a szektorszámnak a feltüntetésével, amelytől az adatfolyam kinyerése megkezdődött.

VI.2.4.4.7 Adatok leválogatása

Amennyiben a szakkérdés megválaszolása azt indokolja, szükség lehet egyes adatok vagy adattípusok leválogatására.

Szűrés

Figyelembe véve a digitális adatok nagy mennyiségét szükségessé válhat a szakkérdés megválaszolása szempontjából releváns adatok leválogatása, amelyet digitális szűrők segítségével is meg lehet valósítani.

A szűrési feltételeknek lehetőség szerint igazodniuk kell a szakértőt kirendelő határozatban/végzésben feltüntetett szakkérdéshez. A digitális szűrő ezért számos összetett feltételből is állhat, például:

- fájlnév,
- fájlméret,
- fájlformátum,
- elérési út,

- aktív/törölt állapot,
- létrehozás/hozzáférés dátuma,
- jogosultságok,
- fiókbirtokos,
- metaadatok,
- egyéb jellemzők..

A szűrők alkalmazásának eredményeképpen megjelenő szűrt adattartalmat célszerű digitális könyvjelzővel megjelölni, vagy más módon (pl. logikai lemezkép létrehozásával) elkülöníteni az irreleváns adatoktól.

Könyvjelző alkalmazása

A szakkérdés megválaszolása szempontjából releváns adatokat a vizsgálat során alkalmazott egyes célszoftverekben digitális könyvjelzők (bookmark) segítségével lehet megjelölni.

A könyvjelzőkkel megjelölt releváns adatok exportálhatóak, illetve a szoftver által létrehozott digitális jelentésekben is kiemelésre kerülhetnek. A könyvjelzőzés összességében az esetlegesen relevanciával bíró adatok rendezett formában történő kigyűjtését segíti elő.

VI.2.4.4.8 AUTOMATIZÁLT KERESÉS

Az automatizált keresés olyan metódus, amelynek során a teljes hozzáférhető adattartalomból algoritmus segítségével automatikusan kiemelésre kerülnek az üggyel vélhetően összefüggésben lévő releváns adatok, a teljes adattartalom megjelenítése és manuális átvizsgálása nélkül.

Az automatizált keresés kizárólag nyílt adattartalomban képes jelsorozatokat felismerni, ezért a titkosított vagy más módon obfuszkált tartalmú adatok hozzáférhetőségét a keresést megelőzően biztosítani szükséges.

Az automatizált keresés alkalmazásához a metódus jellegéből fakadóan elengedhetetlen valamilyen keresési feltételt lehetővé tevő mintázat meghatározása. A keresési mintázat lehet statikus vagy dinamikus is.

Keresés statikus mintázat alapján

Statikus mintázatok alatt jellemzően meghatározott hosszúságú és adattartalmú karakterláncokat értünk, de statikus mintázatot képezhet egy rögzített hosszú bináris jelsorozat is (bár ez utóbbi inkább az adatvésés metódusára jellemző).

Karakterláncok tipikus példája azon kulcsszavak összessége, amelyet a szakértőt kirendelő hatóság – adott esetben az eljáró szakértővel egyeztetve – határoz meg az üggyel összefüggésben.

Keresés dinamikus mintázat alapján

Dinamikus mintázat alatt olyan jelsorozat értendő, amelynek hossza vagy adattartalmának egyes elemei egy meghatározott értékkészleten belül változhatnak, akár rekurzív módon is.

Egy adott dinamikus mintázat meghatározható változók – általában metakarakterek és reguláris kifejezések – segítségével (például telefonszámok, e-mail címek, IP címek esetében), illetve specifikus algoritmus – általában ellenőrző összegek – segítségével is (például bankkártyaszámok, bankszámlaszámok, adóazonosító jelek esetében).

Az automatikus keresés alkalmazásának eredményeképpen megjelenő releváns találatokat célszerű digitális könyvjelzővel megjelölni, vagy más módon elkülöníteni az irreleváns adatoktól.

VI.2.4.4.9 IDŐVONAL REKONSTRUKCIÓ

Az idővonal rekonstrukció célja a tényállással kapcsolatos releváns események digitális nyomainak időbeli sorrendben történő megjelenítése a szakkérdések megválaszolásának érdekében.

Az események vizualizációjának pontos módja – táblázat, eseménynapló, digitális jelentés, stb. – kötetlen, azonban a tartalma minden esetben célhoz kötött.

Az idővonal rekonstrukció tipikus tárgyai a

- rendszeresemények,
- biztonsági események,
- hálózati események,
- üzenetváltások,
- böngészési előzmények,
- egyéb, időben változó adatok.

Az idővonal rekonstrukció módot ad a különböző forrásokból származó adatok időbeli egyezésének összevetésére.

VI.2.4.4.10 MANUÁLIS ELEMZÉS

Az emberi tevékenységen - nem algoritmuson vagy automatizált folyamatokon - alapuló elemzés az adattartalom vizsgálata a digitális adatok megjelenítése és megtekintése útján. A manuális elemzési metódus felhasználható az automatikus elemzési módszerek eredményeinek ellenőrzésére, illetve az egyéb úton meg nem jeleníthető adatok vizsgálatára, elemzésére.

A manuális elemzési metódus tipikus eszközei a digitális adatok hexadecimális és/vagy bináris ábrázolására és szerkesztésére alkalmas szoftverek, illetve szükség esetén az eljáró szakértő által létrehozott vagy felhasznált egyedi szoftverek, algoritmusok.

VI.2.4.4.11 OPTIKAI KARAKTERFELISMERÉS (OCR)

Az optikai karakterfelismerés a képi úton rögzített szöveges adatok digitálisan szerkeszthető szövegállománnyá való átalakítása.

Az optikai karakterfelismerési metódus alapvető lépései:

- az OCR algoritmus kiválasztása (szoftver, nyelv, karakterkészlet, stb.);
- az OCR algoritmus alkalmazása a képi adatokat tartalmazó állományon;
- az automatikusan létrehozott eredmény szemrevételezése és a gépi tévesztések manuális hibajavítása (szakmai igény szerint).

VI.2.4.5 A vizsgálat eredményének átadása

Az eljáró szakértő a szakértői véleményben az átadott szakértői adathordozó jellegéhez - írásvédett-e vagy sem - illeszkedő ajánlást tüntet fel a szakértői adathordozó kezelésével kapcsolatosan.

Az aláírt, bekötött és a szükséges kiegészítőkkel (szakértői adathordozó, kísérőlevél, díjjegyzék) ellátott szakvéleményt és a vizsgálatra átvett tárgyakat a szakértő a saját vagy munkáltatója által előírt ügykezelési folyamat szerint adja át a kirendelő / megbízó részére.

VII. JAVASLAT A MÓDSZERTANI LEVÉL ALKALMAZÁSÁHOZ

VII.1 Az alkalmazás feltételei a hazai gyakorlatban

A módszertani levélben részletezett eljárások alkalmazásához a következő tárgyi eltételek szükségesek:

- szakértői számítógép,
- elektromágneses interferencia hatásait kizáró eszköz,
- vezetékes kapcsolódást lehetővé tevő kábel és adapterkészlet (eszközspecifikus adapterek, szabványos adapterek),
- bitazonos mentés készítésére alkalmas másolóberendezés,
- hardveres és/vagy szoftveres írásvédő eszköz (write blocker),
- vezetékes kapcsolódást lehetővé tevő kábel és adapterkészlet (eszközspecifikus adapterek, szabványos adapterek)
- bitazonos mentés készítésére alkalmas célszoftver (imager)
- törölt állományok helyreállítására alkalmas szoftverek és hardverek;
- adatvésésre alkalmas szoftverek;
- szoftveres szűrők;
- kereső algoritmusok;
- adatbázis szoftverek;
- optikai karakterfelismerő szoftverek;
- digitális adatfeldolgozó és -elemző szoftverek;
- digitális könyvjelzőzésre alkalmas szoftverek;
- digitális jelentések készítésére alkalmas szoftverek és hardverek;
- manuális elemzést elősegítő szoftverek.
- hibafelismerő és -javító függvények
- kriptográfiai hasítófüggvények
  - MD5
  - SHA-1
  - SHA-2 (SHA-256)
- Optikai (mozgó)képrögzítéshez szükséges eszközök
  - fényképezőgépek;
  - videókamerák;
  - fényképező állványok;
  - fotódobozok.
- Kijelzők digitális adattartalmának rögzítéséhez szükséges eszközök
  - screenshot (képernyőkép) készítő szoftverek;
  - screencast (képernyőfelvétel) készítő szoftverek és hardverek;
  - képernyőtükrözésre alkalmas szoftverek és hardverek.

- Ultrahangos tisztító berendezés által használt szerves oldószerek
- Általános víztaszító tisztítószer
- Forrasztási műveletekhez felhasznált anyagok
- Hőelvezetéshez felhasznált anyagok

VII.2 Alkalmazást segítő dokumentumok listája

Glossary. National Institute of Standard and Technology U.S. Department of Commerce Information Technology Laboratory Computer Security Resource Center - https://csrc.nist.gov/glossary

Computer Forensics Tools & Technics Catalog. National Institute of Standard and Technology U.S. Department of Commerce - https://toolcatalog.nist.gov/taxonomy/

VII.3 A gyakorlati alkalmazás mutatói

A módszertani levél gyakorlati alkalmazásának mérőszámai a következők:

- mobilkommunikációs eszközök vizsgálatára vonatkozó igazságügyi informatikai szakértői ügyek statisztikai adatai:
  - ügyek időszakra vonatkozó darabszáma,
  - a vizsgálatok átlagos időtartama,
  - a vizsgált tárolóeszközök mennyisége, minősége és kapacitása,
  - az általános tárolási funkcióval nem rendelkező vizsgálti tárgyak mennyisége, minősége és egyéb jellemzői.

VIII. A MÓDSZERTANI LEVÉL FELÜLVIZSGÁLATI TERVE

A módszertani levél karbantartása a vizsgálati eljárások minőségének fenntartása érdekében szükséges, ciklikus folyamat. Az felülvizsgálat - legyen az évenkénti tartalomfrissítő, rendkívüli vagy technológiamegújító felülvizsgálat - elvégzéséig, kiértékeléséig és eredményeinek beépítéséig az előző módszertani levél marad hatályban.

VIII.1 Évenkénti tartalomfrissítő felülvizsgálat

A módszertani levél műszaki-informatikai tartalmi elmeit, minden évben legalább egy alkalommal részletesen át kell tekinteni és az előző felülvizsgálat óta megjelent technológiai (hardver és szoftver) megoldásokkal ki kell egészíteni amennyiben az szükséges.

A kinyert adatok érvényességének megerősítésére (validation) szolgáló algoritmusok megfelelőségét minden évenkénti tartalomfrissítő felülvizsgálat során értékelni kell, szükség esetén haladéktalanul át kell vezetni a kellő módosításokat.

A felülvizsgálat eredményéről és tartalmáról - elektronikus közlemény formájában - értesíteni kell a módszertani levél felhasználóit.

VIII.2 Rendkívüli felülvizsgálat

Amennyiben a módszertani levél tartalmát érintő rendkívüli technológiai esemény következik be - különösen a vizsgálati módok hitelességével, megbízhatóságával összefüggésben - úgy az érinett módszertani levél adott technológiával kapcsolatos részét haladéktalanul felül kell vizsgálni és a szükséges módosításokat el kell végezni.

A felülvizsgálat eredményéről és tartalmáról - elektronikus közlemény formájában - értesíteni kell a módszertani levél felhasználóit.

VIII.3 Háromévenkénti technológiamegújító felülvizsgálat

A módszertani levél teljes tartalmát minden harmadik évben részletesen át kell tekinteni és az előző technológiamegújító felülvizsgálat óta megjelent megoldásokkal, amennyiben az szükséges - úgy technológiai, mint eljárásbeli - ki kell egészíteni.

A felülvizsgálat eredményéről és tartalmáról - elektronikus közlemény formájában - értesíteni kell a módszertani levél felhasználóit.

IX. SZAKIRODALOM

ACPO Good Practice Guide for Digital Evidence, Association of Chief Police Officers, London, 2012.

Brinson, Ashley – Robinson, Abigail – Rogers, Marcus: A cyber forensics ontology: Creating a new approach to studying cyber forensics. in Digital Investigation, Elsevier. Amsterdam, 2006. pp.37-43.

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

Cohen, Fred: The Future of Digital Forensics. in 1st Chinese Conference on Digital Forensics online 2012. 1st Chinese Conference on Digital Forensics online: http://www. all. net/

Illési Zsolt: Az igazságügyi informatikai szakértés modellezése. in Hadmérnök 2010 december pp. 122-136 Budapest, 2010. Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar.

Illési Zsolt: Számítógép hálózatok kriminál technikai vizsgálata. in Hadmérnök 2009 december pp. 170-183. Budapest, 2009. Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar.

Jansen, Wayne - Ayers, Rick: Guidelines on Cell Phone Forensics. Gaithersburg, MD, USA, 2007. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology.

Johnson, Thomas A. (editor): Forensic Computer Crime Investigation. Boca Raton, FL, USA, CRC Press, 2005.

Lee, Rob – SANS DFIR Faculty: Digital Forensics and Incident Response Poster. SANS Institute, Bethesda, MD, USA, 2012.

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

Palmer, Gary et al.: A Road Map for Digital Forensic Research. First Digital Forensic Research Workshop. Utica, NY, USA, 2001. p.17. online: https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf

IX.1 Jogszabályok

1995. évi XXVIII. törvény a nemzeti szabványosításról

2017. évi XC. törvény a büntetőeljárásról

1998. évi XIX. törvény a büntetőeljárásról

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

IX.2 Szabványok

MSZ EN ISO/IEC 27037:2016 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.

MSZ EN ISO/IEC 27041:2016 Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method.

MSZ EN ISO/IEC 27042:2017 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence.

MSZ EN ISO/IEC 27043:2016 Information technology — Security techniques — Incident investigation principles and processes.

MSZ EN ISO 21043-1:2018 - Forensic Sciences. Part 1: Terms and definitions.

ISO 21043-2 - Forensic sciences - Part 2 - Recognition, recording, collecting, transport and storage of items.

IX.3 Ajánlások

SWGDE: Best Practices for Computer Forensic Acquisitions

SWGDE: Best Practices for Computer Forensic Examination

SWGDE: Best Practices for Computer Forensics

SWGDE: Best Practices for Digital Evidence Collection

SWGDE: Capture of Live Systems

SWGDE: Data Archiving

SWGDE: Position Paper Standards and Controls

Budapest, 2020. november 19.

Schváb Zoltán

Schváb Zoltán Gábor
Magyar Igazságügyi Szakértői Kamara
elnöke

A Magyar Igazságügyi Szakértői Kamara elektronikus adatok vizsgálatának általános alapelveiről szóló, fentiekben részletezett módszertani levelének kiadását az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény 90.§ (1)-(3) valamint a 91. § (2) bekezdésekben foglaltakra figyelemmel, a 90.§ (2) bekezdésében rögzített módon támogatjuk:

.....

Dr. Máté István Zsolt elnök

2020..... napján.

.....

Dr. Darabos Zoltán

2020..... napján.

.....

.....

Morber Szilárd Krisztián

2020..... napján.

.....

Sándor Gábor

2020..... napján.

MAGYAR IGAZSÁGÜGYI SZAKÉRTŐI KAMARA
Informatikai és Hírközlési Szakmai Tagozat
Levél: 1068 Budapest, Benczúr u 47 ; Tel : 06- 20- 9-679837, 06-70775-521,
email [redacted]

Tárgy	Módszertani levél elfogadása
Ügyintéző	Dr. Máté István Zsolt elnök, Informatikai és Hírközlési Szakmai Tagozat
Telefon	+36 (30) 236 7458
e-mail:	[redacted]

Dr. Máté István Zsolt
igazságügyi informatikai szakértő,
Magyar Igazságügyi Szakértői Kamara
Informatikai és Hírközlési Szakmai Tagozat elnöke

N Y I L A T K O Z A T

A Magyar Igazságügyi Szakértői Kamara Informatikai és Hírközlési Tagozata Módszertani Levél Bizottsága által kidolgozott „Az elektronikus adatok vizsgálatának általános alapelvei" című módszertani levelét, melynek tartalma megtalálható az alábbi állományokban:

01_Az elektronikus_adatok_vizsgálatának_általános_alapelvei_v5.2.pdf

MD5	682c9fe6648c83f7f1324fe2bb4a7160
SHA1	db8f619ea315ceb3d6dd0ee0f9b4388f1d625d8d
SHA-256	caa7764d4bc22fbcbbf80f69900b68a10ca5d0bb492257722c778e5e06bb093a

01_Az elektronikus_adatok_vizsgálatának_általános_alapelvei_v5.2.docx

MD5	1528cfd4ff161efaf76ccd91018cf8f1
SHA1	565464c5a7d06eb02eeff45c15e645606959e6a6
SHA-256	13b1278c8129ae291320a29b9ccd19996aeb4691faa83e60a36490f662436439

A módszertani levél tartalmát és szövegét:

ELFOGADOM / NEM FOGADOM EL

, PÉCS **', 2020. augusztus '** 19 **'.**

Tisztelettel:

Dr. Máté István Zsolt
igazságügyi informatikai szakértő,
Magyar Igazságügyi Szakértői Kamara
Informatikai és Hírközlési Szakmai Tagozat
elnöke

MAGYAR IGAZSÁGÜGYI SZAKÉRTŐI KAMARA
Informatikai és Hírközlési Szakmai Tagozat
Levél: 1068 Budapest, Benczúr u. 47.; Tel.: 06- 20- 9-679837, 06-70775-521,
email: mate.istvan@informatikaiszakerto.hu

Tárgy	Módszertani levél elfogadása
Ügyintéző	Dr. Máté István Zsolt elnök, Informatikai és Hírközlési Szakmai Tagozat
Telefon	+36 (30) 236 7458
e-mail:	mate.istvan@informatikaiszakerto.hu

Dr. Darabos Zoltán
igazságügyi informatikai szakértő,
COMPU-CONSULT Kft.

NYILATKOZAT

A Magyar Igazságügyi Szakértői Kamara Informatikai és Hírközlési Tagozata Módszertani Levél Bizottsága által kidolgozott „Az elektronikus adatok vizsgálatának általános alapelvei" című módszertani levelét, melynek tartalma megtalálható az alábbi állományokban:

01_Az elektronikus_adatok_vizsgálatának_általános_alapelvei_v5.2.pdf

MD5	682c9fe6648c83f7f1324fe2bb4a7160
SHA1	db8f619ea315ceb3d6dd0ee0f9b4388f1d625d8d
SHA-256	caa7764d4bc22fbcbbf80f69900b68a10ca5d0bb492257722c778e5e06bb093a

01_Az elektronikus_adatok_vizsgálatának_általános_alapelvei_v5.2.docx

MD5	1528cfd4ff161efaf76ccd91018cf8f1
SHA1	565464c5a7d06eb02eeff45c15e645606959e6a6
SHA-256	13b1278c8129ae291320a29b9ccd19996aeb4691faa83e60a36490f662436439

A módszertani levél tartalmát és szövegét:

ELFOGADOM / NEM FOGADOM EL

Budapest, 2020. augusztus 25.

Tisztelettel:

DR. DARABOS ZOLTÁN
igazságügyi szakértő

Dr. Darabos Zoltán
igazságügyi informatikai szakértő,
COMPU-CONSULT Kft.

MAGYAR IGAZSÁGÜGYI SZAKÉRTŐI KAMARA
Informatikai és Hírközlési Szakmai Tagozat
Levél: 1068 Budapest, Benczúr u. 47.; Tel.: 06- 20- 9-679837, 06-70775-521,
email: mate.istvan@informatikaiszakerto.hu

Tárgy	Módszertani levél elfogadása
Ügyintéző	Dr. Máté István Zsolt elnök, Informatikai és Hírközlési Szakmai Tagozat
Telefon	+36 (30) 236 7458
e-mail:	mate.istvan@informatikaiszakerto.hu

Morber Szilárd Krisztián
gazságügyi informatikai szakértő,
Nemzetbiztonsági Szakszolgálat Szakértői Intézete

NYILATKOZAT

A Magyar Igazságügyi Szakértői Kamara Informatikai és Hírközlési Tagozata Módszertani Levél Bizottsága által kidolgozott „Az elektronikus adatok vizsgálatának általános alapelvei" című módszertani levelét, melynek tartalma megtalálható az alábbi állományokban:

01_Az elektronikus_adatok_vizsgálatának_általános_alapelvei_v5.2.pdf

MD5	682c9fe6648c83f7f1324fe2bb4a7160
SHA1	db8f619ea315ceb3d6dd0ee0f9b4388f1d625d8d
SHA-256	caa7764d4bc22fbcbbf80f69900b68a10ca5d0bb492257722c778e5e06bb093a

01_Az elektronikus_adatok_vizsgálatának_általános_alapelvei_v5.2.docx

MD5	1528cfd4ff161efaf76ccd91018cf8f1
SHA1	565464c5a7d06eb02eeff45c15e645606959e6a6
SHA-256	13b1278c8129ae291320a29b9ccd19996aeb4691faa83e60a36490f662436439

A módszertani levél tartalmát és szövegét:

ELFOGADOM / NEM FOGADOM EL

' Budapest ', 2020. augusztus ' 19 . '.

Tisztelettel:

Morber Szilárd Krisztián
igazságügyi informatikai szakértő,
Nemzetbiztonsági Szakszolgálat Szakértői Intézete

MAGYAR IGAZSÁGÜGYI SZAKÉRTŐI KAMARA
Informatikai és Hírközlési Szakmai Tagozat
Levél: 1068 Budapest, Benczúr u. 47.; Tel.: 06- 20- 9-679837. 06-70775-521,
email: mate.istvan@informatikaiszakerto.hu

Tárgy	Módszertani levél elfogadása
Ügyintéző	Dr. Máté István Zsolt elnök, Informatikai és Hírközlési Szakmai Tagozat
Telefon	+36 (30) 236 7458
e-mail:	mate.istvan@informatikaiszakerto.hu

Sándor Gábor
igazságügyi informatikai szakértő,
informatikai osztályvezető,
Nemzetei Szakértői és Kutató Központ
Informatikai Szakértői Osztály vezetője

N Y I L A T K O Z A T

A Magyar Igazságügyi Szakértői Kamara Informatikai és Hírközlési Tagozata Módszertani Levél Bizottsága által kidolgozott „Az elektronikus adatok vizsgálatának általános alapelvei" című módszertani levelét, melynek tartalma megtalálható az alábbi állományokban:

01_Az elektronikus_adatok_vizsgálatának_általános_alapelvei_v5.2.pdf

MD5	682c9fe6648c83f7f1324fe2bb4a7160
SHA1	db8f619ea315ceb3d6dd0ee0f9b4388f1d625d8d
SHA-256	caa7764d4bc22fbcbbf80f69900b68a10ca5d0bb492257722c778e5e06bb093a

01_Az elektronikus_adatok_vizsgálatának_általános_alapelvei_v5.2.docx

MD5	1528cfd4ff161efaf76ccd91018cf8f1
SHA1	565464c5a7d06eb02eeff45c15e645606959e6a6
SHA-256	13b1278c8129ae291320a29b9ccd19996aeb4691faa83e60a36490f662436439

A módszertani levél tartalmát és szövegét:

ELFOGADOM / NEM FOGADOM EL

Kaposvár, 2020. augusztus 22.

Tisztelettel:

Sándor Gábor
igazságügyi informatikai szakértő,
informatikai osztályvezető,
Nemzetei Szakértői és Kutató Központ
Informatikai Szakértői Osztály vezetője