Azonosító: v1.0 – 2019.

A digitális adattároló eszközök vizsgálatának általános eljárásai

1 Tartalomjegyzék

1 A MÓDSZERTANI LEÍRÁS KIDOLGOZÁSÁBAN RÉSZT VEVŐK ADATAI 5
2 A MÓDSZERTANI LEÍRÁS HATÁLYBA LÉPÉSÉNEK IDŐPONTJA 5
1 MÓDSZERTANI LEÍRÁS TÉMÁJA 6
2 KIADÁS INDOKOLÁSA 6
3 HATÓKÖR 6
4 MEGHATÁROZÁSOK 7
4.1 Fogalmak 7
4.1.1 Merevlemezes tároló (Hard Disk Drive) 7
4.1.2 Szilárdtest meghajtó (Solid State Drive) 7
4.1.3 Memóriakártya (Memory Card) 7
4.1.4 USB tár (USB drive, pendrive USB key) 7
4.1.5 Optikai tárolók (CD, DVD, BluRay) 7
4.1.6 Hasító érték (Hash Value) 7
4.2 Rövidítések 8
5 BEVEZETÉS 9
5.1 A témakör hazai helyzete, a témaválasztás indoklása 9
5.2 Kapcsolat a hivatalos hazai és külföldi szakmai irányelvekkel 9
5.2.1 Nemzetközi szabványok 10
5.2.2 SWGDE ajánlásai 11
5.2.3 ENFSI ajánlásai 11
6 A MÓDSZERTANI LEÍRÁS SZAKMAI RÉSZLETEZÉSE 12
6.1 A tárolóeszközök kezelésének általános alapelvei 12
6.2 A tárolóeszközök kezelésének specifikus alapelvei 12
6.2.1 Bekapcsolt állapotú tárolóeszköz kezelése 12
6.2.2 Kikapcsolt állapotú tárolóeszköz kezelése 13
6.3 Adatkinyerés tárolóeszközökről 13
6.3.1 Fizikai adatkinyerés 13
6.3.2 Logikai adatkinyerés 13
6.3.2.1 Célzott tartalomkinyerés 14
6.4 Adatkinyerés dokumentálása 14
6.5 Tárolóeszközökről kinyerhető adatok 14
6.5.1 Merevlemezes adattárolók 14

6.5.2 Szilárdtest adattárolók 16
6.5.3 Memóriakártyák, USB kulcsok 16
6.5.4 Optikai adathordozók 16
6.6 Tárolóeszközökről kinyert adatok érvényességének megerősítése 17
7 JAVASLAT A MÓDSZERTANI LEÍRÁS ALKALMAZÁSÁHOZ 18
7.1 1. Az alkalmazás feltételei a hazai gyakorlatban 18
7.1.1 Fizikai adatkinyerés 18
7.1.2 Logikai adatkinyerés 18
7.2 2. Alkalmazást segítő dokumentumok listája 19
7.3 3. A gyakorlati alkalmazás mutatói 19
8 A MÓDSZERTANI LEÍRÁS FELÜLVIZSGÁLATI TERVE 20
8.1 Évenkénti tartalomfrissítő felülvizsgálat 20
8.2 Rendkívüli felülvizsgálat 20
8.3 Háromévenkénti technológiamegújító felülvizsgálat 20
9 SZAKIRODALOM 21
9.1 Jogszabályok 21
9.2 Szabványok 22
9.3 Ajánlások 22
10 MELLÉKLETEK 23

1 A MÓDSZERTANI LEÍRÁS KIDOLGOZÁSÁBAN RÉSZT VEVŐK ADATAI

Dr. Máté István Zsolt	igazságügyi informatikai szakértő, Magyar Igazságügyi Szakértői Kamara Informatikai és Hírközlési Szakmai Tagozat elnöke, Nemzeti Szakértői és Kutató Központ Pécsi Intézet
Sándor Gábor	igazságügyi informatikai szakértő, informatikai osztályvezető, Nemzeti Szakértői és Kutató Központ Kaposvári Intézet

2 A MÓDSZERTANI LEÍRÁS HATÁLYBA LÉPÉSÉNEK IDŐPONTJA

2019. december „ ”.

1 MÓDSZERTANI LEÍRÁS TÉMÁJA

A módszertani leírás a digitális adattároló eszközökre (különösen a merevlemezekre és a szilárdtest meghajtókra) (a továbbiakban: tárolóeszközök) vonatkozóan meghatározza az alkalmazandó vizsgálati eljárásokat.

2 KIADÁS INDOKOLÁSA

A Nemzeti Szakértői és Kutató Központ az igazságügyi informatikai szakértői tevékenység során alkalmazandó, a tárolóeszközök vizsgálatára vonatkozó alapvető tevékenységek meghatározásával 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.

3 HATÓKÖR

A módszertani leírás személyi hatálya kiterjed a Nemzeti Szakértői és Kutató Központ igazságügyi informatikai szakértőire, szakértő jelöltjeire, az informatikai technikusokra, valamint a felsorolt személyekkel a szakértői vélemények kialakításában együttműködő külsős személyekre, különösen társszakértőkre és szakkonzultánsokra.

A módszertani leírás tárgyi hatálya a tárolóeszközök vizsgálatával kapcsolatos igazságügyi informatikai szakértő tevékenységre.

A módszertani leírás eljárási hatálya kiterjed valamennyi – a Nemzeti Szakértői és Kutató Központ által befogadott – igazságügyi informatikai szakértő tevékenységet igénylő eljárásfajtára, különösen:

- büntetőeljárásra,
- polgári eljárásra,
- közigazgatási eljárásra,
- hatósági eljárásra,

A módszertani leírás területi hatálya kiterjed:

- helyszíni vizsgálatokra Magyarország területén,
- laboratóriumi vizsgálatokra Magyarország területén,

4 MEGHATÁROZÁSOK

4.1 Fogalmak

4.1.1 Merevlemezes tároló (Hard Disk Drive)

Egy vagy több mágnesezhető felületű korongot tartalmazó, hosszútávú adattárolásra szolgáló eszköz.

4.1.2 Szilárdtest meghajtó (Solid State Drive)

Mechanikai alkatrészeket nem tartalmazó, elektronikus tárolási elvű, hosszútávú adattárolásra szolgáló eszköz.

4.1.3 Memóriakártya (Memory Card)

Szabványos interfésszel rendelkező, eltávolítható, tartós adattárolásra alkalmas tárolómédium, mely különösen kis mérettartományú, hordozható eszközökben – különösen kamerákban és telefonokban – alkalmaznak.[1]

4.1.4 USB tár (USB drive, pendrive USB key)

Speciális, elektronikusan törölhető és újraprogramozható memóriát (EEPROM) és integrált USB (universal serial bus) interfészt tartalmazó tartós tárolásra használatos eszköz.

4.1.5 Optikai tárolók (CD, DVD, BluRay)

Az adatokat műanyag korongra felvitt fényvisszaverő felületen, spirálvonalban tároló, lézeres adat-kiolvasású – csak olvasható, írható, írható-törölhető kivitelű–, különféle adatsűrűségű, hosszútávú adattárolásra alkalmas médium.

4.1.6 Hasító érték (Hash Value)

A hasító függvény visszatérési értéke (eredménye). A hasító függvény egy üzenetet feldolgozva kimenetként egy hasító értéket állít elő oly módon, hogy egy tetszőleges hosszúságú bitfolyamból véges hosszúságú bitsorozatot állít elő.[2]

---

[1] https://www.techopedia.com/definition/2788/memory-card

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

4.2 Rövidítések

CD	Compact Disk, op
DVD	Digital Versatile Disk
HDD	Hard Disk Drive
MD5	Message-Digest algorithm 5
MDC	Modification Detection Code
NAS	Network Attached Storage
SAN	Storage Area Network
SHA	Secure Hash Algorithm
SSD	Solid State Drive
USB	Universal Serial Bus

5 BEVEZETÉS

5.1 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"[3-4]. Mivel a korábbi időszakban a szakterületre vonatkozó módszertani levelek nem kerültek kiadásra, így az egységes gyakorlat követelményét megalapozó iránymutatás nem került a szakértők elé. E hiányosságot kívánja megszüntetni jelen módszertani leírás.

5.2 Kapcsolat a hivatalos hazai és külföldi szakmai irányelvekkel

A Digital Forensics Research Workshop szervezet 2001-es első konferenciáján tárgyalta és kialakította a digitális adatok kezelésére vonatkozó vizsgálati eljárásmodelljét, melyben az alábbi műveleteket azonosította[5]:

Identification	a digitális adat hordozójának azonosítása
Preservation	a digitális adat megőrzése, megóvása
Collection	a digitális adat hordozóinak összegyűjtése
Examination	a digitális adatok vizsgálata
Analysis	a digitális adatok elemzése
Presentation	a digitális adatok bemutatása
Decision	döntés a digitális adatok alapján

A későbbiekben a Digital Forensic Science kutatói ezt a modellt bővítették, egészítették ki saját preferenciáik alapján. Jelen módszertani leírás 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 módszertanát tekinti az alábbi területekre koncentrálva:

Identification	a digitális adat hordozójának azonosítása
Preservation	a digitális adat megőrzése, megóvása
Collection	a digitális adat hordozóinak összegyűjtése
Aquisition	a digitális adat kinyerése
Examination	a digitális adat vizsgálata
Analysis	a digitális adatok elemzése

[3] 2005. évi XLVII. törvény 30/A §

[4] 2016. évi XXIX. törvény 89. § (1)

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

Presentation	a digitális adatok bemutatása

Az alapvető tudományos és módszartani forráson kívül jelen módszertani leírás 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:

5.2.1 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]

5.2.2 SWGDE[6] 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.

5.2.3 ENFSI[7] ajánlásai

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

---

[6] SWGDE – Scientific Working Group on Digital Evidence

[7] ENFSI - European Network of Forensic Science Institutes

6 A MÓDSZERTANI LEÍRÁS SZAKMAI RÉSZLETEZÉSE

6.1 A tárolóeszközök kezelésének általános alapelvei

A különböző adattárolók[8] vizsgálata során a következő alapelvek alapján kell eljárni:

- minimalizálni kell a hozzáférés mértékét,
- minden változást dokumentálni és indokolni szükséges,
- a vizsgálati eszközökre vonatkozóan be kell tartani a bűnjel és a vizsgálati tárgy kezelési szabályokat,
- a vizsgálati eszközök mozgatásakor (szervezeten belüli és/vagy szervezetek közötti átadás-átvétel) fenn kell tartani a felügyeleti lánc (Chain of Cutody) folyamatosságát a dokumentálás által.

6.2 A tárolóeszközök kezelésének specifikus alapelvei

6.2.1 Bekapcsolt állapotú tárolóeszköz kezelése

- A bekapcsolt tárolóeszközről történő adatkinyerés a rendszer állapotát megváltoztatja, mely akár a rendszer instabilitásához is vezethet. A titkosított tárolóeszközök esetében a rendszer leállítása a megakadályozhatja az adatokhoz történő hozzáférést, ezért a bekapcsolt tárolóeszközt tartalmazó rendszernél ellenőrizni kell a titkosítás jelenlétét. A kinyerést megelőzően mérlegelni kell ezeket a kockázatokat;
- A bekapcsolt állapotú tárolóeszközt tartalmazó rendszert elsőként le kell választani a kommunikációs hálózatról;
- Gondoskodni kell arról, hogy a bekapcsolt állapotú tárolóeszközt tartalmazó rendszer tápellátása a vizsgálat teljes időtartalma alatt folyamatos legyen,
- A bekapcsolt tárolóeszközt tartalmazó rendszerből történő adatkinyerés lépései
  - ~ tárolóeszköz bekapcsolt állapotának azonosítása,
  - ~ titkosítás azonosítása a bekapcsolt tárolóeszközön,
    - Δ változékony adatok mentése a bekapcsolt titkosított tárolóeszközről,
    - Δ nem változékony adatok mentése a bekapcsolt titkosított tárolóeszközről,
  - ~ változékony adatok mentése a bekapcsolt nem titkosított tárolóeszközről,
  - ~ nem változékony adatok mentése a bekapcsolt nem titkosított tárolóeszközről,
- Ki kell kapcsolni a bekapcsolt állapotú tárolóeszközt tartalmazó rendszert és a kikapcsolt állapotú tárolóeszköz kezelése eljárást kell lefolytatni.
- A teljes folyamatot részletesen dokumentálni kell

[8] Jelen módszertani leírás a merevlemezes tárak, szilárdtest meghajtók, optikai tárak, memória kártyák és USB tárak vizsgálatára vonatkozik, nem tartalmazza a mágnesszalagos egységek vizsgálati eljárásait.

6.2.2 Kikapcsolt állapotú tárolóeszköz kezelése

A kikapcsolt állapotú elektronikus eszközökről történő adatkinyeréskor a következő tevékenységek elvégzése szükséges:

- annak a ténynek az ellenőrzése, hogy az elektronikus eszköz valóban kikapcsolt állapotú-e;
- a tárolót el kell távolítani a kikapcsolt állapotú elektronikus eszközből, amennyiben az lehetséges;
- az eltávolított tárolót azonosítani kell;
- az adatkinyerést megbízható forrásból származó, ellenőrzött és hitelesített eszközzel szükséges elvégezni.

6.3 Adatkinyerés tárolóeszközökről

Az adatkinyerés 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

6.3.1 Fizikai adatkinyerés

- Az eszközön található adatok megkettőzése (duplikálása);
- Hardveres vagy szoftveres írásvédők használata szükséges (amennyiben az lehetséges) az eredeti adatok felülírásának megelőzésére;
- A művelethez olyan hardver és szoftver komponenseket kell alkalmazni, amelyek képesek az eredeti adathordozó teljes tartalmának bitazonos másolására;

6.3.1.1 Forenzikus klónozás

- A művelet során a teljes adatfolyam átmásolása történik egy másik adathordozóra;
- Élő rendszerből történő adatkinyerésnél ellenőrzött adathordozóról származó megbízható programokat (futtatható fájlok) kell alkalmazni;
- Élő rendszerből történő adatkinyerésnél a lehető legmagasabb szintű (hardver közeli) jogosultsággal kell a műveletet végrehajtani az összes beszerezhető adat kinyerése érdekében;

6.3.2 Logikai adatkinyerés

- Könyvtárak (mappák) és fájlok megszerzésének művelete az eredeti (natív) fájlrendszer használatával, amelyben az adatok fellelhetőek;
- A forenzikus lemezkép (forensic image) fájlt olyan hardver és szoftver komponensek alkalmazásával kell elkészíteni, amelyek alkalmasak az eredeti tárolómédium logikai szerkezetének rögzítésére;

6.3.2.1 Célzott tartalomkinyerés

- Fájlok vagy könyvtárak (mappák) tartalmának célirányos kinyerése egy tárolómédiumról vagy eszközről, elő-rendszerből fizikai vagy logikai kinyerés révén;
- Az adatok logikai másolásánál a metaadatok elveszhetnek, ezért olyan másolási megoldást kell alkalmazni, mely támogatja a metaadatok kinyerését is vagy a metaadatokat külön művelet során kell kinyerni;
- A célirányosan megszerzendő adatok tartalmazhatnak összetett vagy beágyazott fájlokat is, melyre figyelemmel kell lenni a műveletek elvégzése során;

6.4 Adatkinyerés dokumentálása

- Az adatkinyerés dokumentálása történhet automatikusan (a kinyerési eljáráshoz használt célszoftver funkciójának felhasználásával), vagy manuálisan (különösen a külső megfigyelésen alapuló vizuális adatkinyerés esetén),
- A dokumentációnak különösen az alábbi adatokat kell tartalmaznia a tárolóeszközre vonatkozóan:
  - ~ a tárolóeszközt tartalmazó informatikai eszköz/rendszer azonosító adatai,
  - ~ a tárolóeszköz gyártója és modell azonosítója,
  - ~ a tárolóeszköz egyedi azonosítója (sorozatszám),
  - ~ egyedi vizsgálati azonosítók (ügyszám, helyszín azonosító, nyomozócsoport azonosítója stb.),
  - ~ megszerzett adatok hasító értékei (amennyiben az indokolt),
  - ~ a tárolóeszköz, 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 egyéb szabályzatban előírt további dokumentáció.

6.5 Tárolóeszközökről kinyerhető adatok

A tárolóeszközről történt adatkinyerés során megszerzett adatok különösen az alábbiak lehetnek egyes eszköztípusonként:

6.5.1 Merevlemezes adattárolók

- beépített adattárolók
  - ~ felhasználói adatok, különösen
    - Δ internethasználat adatai,
    - Δ kommunikációs adatok (levelezés, azonnali üzenetküldés stb.)

- Δ mobiltelefonok biztonsági mentései,
- ~ működtető rendszer adatai, különösen
  - Δ telepítés ideje,
  - Δ felhasználók adatai,
  - Δ teleptett alkalmazások adatai,
  - Δ fájlrendszer adatai,
  - Δ a rendszer hardver és szoftver komponenseinek adatai,
  - Δ a rendszer használati eseményeinek adatai

– külső csatlakozású adattárolók, különösen
- ~ archivált adatok (dokumentumok, digitális képek, videók, hangfelvételek),
- ~ mobiltelefonok biztonsági mentései,

– nagy tárolókapacitású külső adattárolók (SAN, NAS), különösen
- ~ archivált adatok (dokumentumok, digitális képek, videók, hangfelvételek),
- ~ napi használat adatai (dokumentumok, elektronikus levelezés, digitális képek, videók, hangfelvételek

6.5.2 Szilárdtest adattárolók

- felhasználói adatok, különösen
  - ~ internethasználat adatai,
  - ~ kommunikációs adatok (levelezés, azonnali üzenetküldés stb.)
- működtető rendszer adatai, különösen
  - ~ telepítés ideje,
  - ~ felhasználók adatai,
  - ~ teleptett alkalmazások adatai,
  - ~ fájlrendszer adatai,
  - ~ a rendszer hardver és szoftver komponenseinek adatai,
  - ~ a rendszer használati eseményeinek adatai

6.5.3 Memóriakártyák, USB kulcsok

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

6.5.4 Optikai adathordozók

- telepítőkészletek,
- archivált felhasználói adatok (különösen digitális fényképek, videók, hangfelvételek, dokumentumok),

6.6 Tárolóeszközökről kinyert adatok érvényességének megerősítése

A vizsgálat során az adott tárolóeszközről kinyert adatok érvényességét hasító érték létrehozásával szükséges megerősíteni. Ezt a művelet elvégezhető az adott eszközről logikai vagy fizikai adatkinyerési módszerrel kimásolt adatokra vonatkozóan, illetve a külső megfigyelésen alapuló adatkinyerés során létrejött digitális képek és/vagy videófelvételekre vonatkozóan.

Az érvényesség megerősítésére alkalmas egyirányú, kulcs nélküli módosítás azonosító kriptográfiai algoritmusok (Modification Detection Code (MDC)) különösen a következők:

- MD5 (Message-Digest algorithm 5)[9]
- SHA-1 (Secure Hash Algorithm - 1)
- SHA-2 (Secure Hash Algorithm - 2)[10]

A tárolóeszközről kinyert adatok érvényességének megerősítésére (validation) szolgáló algoritmusok megfelelőségét különösen az egyes algoritmus validációs programok eredményeinek nyomonkövetésével kell biztosítani.[11]

[9] http://www.ietf.org/rfc/rfc1321.txt
[10] https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/shs/SHAVS.pdf
[11] https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program/

7 JAVASLAT A MÓDSZERTANI LEÍRÁS ALKALMAZÁSÁHOZ

7.1 Az alkalmazás feltételei a hazai gyakorlatban

A 6.3. pontban részletezett adatkinyerési eljárások alkalmazásához a következő tárgyi feltételek szükségesek:

7.1.1 Fizikai adatkinyerés

- 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),
- bitazonos mentés készítésére alkalmas célszoftver (imager)

7.1.2 Logikai adatkinyerés

- szakértői számítógép,
- elektromágneses interferencia hatásait kizáró eszköz,
- hardveres és/vagy szoftveres írásvédő eszköz (write blocker),
- vezetékes kapcsolódást lehetővé tevő kábel és adapterkészlet (eszközspecifikus adapterek, szabványos adapterek)
- hardveres és/vagy szoftveres írásvédő eszköz (write blocker),
- bitazonos mentés készítésére alkalmas célszoftver (imager)

7.2 Alkalmazást segítő dokumentumok listája

Ayers, Rick – Brothers, Sam –Jansen, Wayne: Guidelines on Mobile Device Forensics. National Institute of Standard and Technology U.S. Department of Commerce, 2014.

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

7.3 A gyakorlati alkalmazás mutatói

A módszertani leírás gyakorlati alkalmazásának mérőszámai a következők:

- adattároló eszközök vizsgálatára vonatkozó igazságügyi informatikai szakértői ügyek statisztikai adatai:
  - ügyek darabszáma,
  - a vizsgálat időtartama,
  - a tárolóeszközök mennyisége.

8 A MÓDSZERTANI LEÍRÁS FELÜLVIZSGÁLATI TERVE

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

8.1 Évenkénti tartalomfrissítő felülvizsgálat

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

A mobilkommunikációs eszközről 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 értesíteni kell a módszertani leírás felhasználóit.

8.2 Rendkívüli felülvizsgálat

Amennyiben a módszertani leírás tartalmát érintő rendkívüli technológiai esemény következik be – különösen a vizsgálati módok hitelességével, megbízhatóságával összefüggésben – úgy a kapcsolódó módszertani leírást az érintett technológiával összefüggő részét haladéktalanul felül kell vizsgálni és a szükséges módosításokat el kell végezni.

A felülvizsgálat eredményéről és tartalmáról haladéktalanul értesíteni kell a módszertani leírás felhasználóit.

8.3 Háromévenkénti technológiamegújító felülvizsgálat

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

A felülvizsgálat eredményéről és tartalmáról értesíteni kell a módszertani leírás felhasználóit.

9 SZAKIRODALOM

BASSHAM III, Lawrence E – HALL, Timothy A.: The Secure Hash Algorithm Validation System (SHAVS). National Institute of Standards and Technology Information Technology Laboratory Computer Security Division. 2014.

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.

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

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

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

KISSEL, Richard – REGENSCHEID, Andrew – SCHOLL, Matthew – STINE, Kevin: Guidelines for Media Sanitization. National Institute of Standard and Technology U.S. Department of Commerce, 2014.

9.1 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

9.2 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.

9.3 Ajánlások

SWGDE: Best Practices for Mobile Phone Forensics

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

10 MELLÉKLETEK

–

ZÁRADÉK

A dokumentum elektronikus aláírással hitelesített

29200-115/32/2019.ált.