A bizonyítékok kezelése

- az igazságügyi informatikai szakértő a büntetőeljárásban -

Máté István Zsolt

Miről lesz szó?

- A bűnjel vagy bizonyíték?
- A digitális bizonyíték fogalma és típusai
- A digitális bizonyíték kezelése az igazságügyi informatikai szakértői munkafolyamatban elmélet vs. gyakorlat

DEFINÍCIÓK

A bűnjel

A bűnjel definícióját a **11/2003. (V. 8.) IM-BM-PM együttes rendelet** tartalmazza a következőképpen:

„1. § (1) Azt a **lefoglalt dolgot** (a továbbiakban: bűnjel), amely az eljárás során a **bizonyítás eszközéül szolgál**, valamint, amelyet az eljárás során azonosítani, megvizsgálni, valamint megtekinteni szükséges …”

A bizonyíték

*A bizonyítás eszközei**

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

::: 1998. évi XIX. törvény a büntetőeljárásról

A tárgyi bizonyítási eszköz

115. § (1) Tárgyi bizonyítási eszköz minden olyan tárgy (dolog), amely a bizonyítandó tény bizonyítására alkalmas, … az **elkövető nyomait hordozza**, vagy **a bűncselekmény elkövetése útján jött létre**, amelyet **a bűncselekmény elkövetéséhez eszközül használtak**, vagy **amelyre a bűncselekményt elkövették**.

::: 1998. évi XIX. törvény a büntetőeljárásról

Elektronikus adat lefoglalása

67. § (1) Az elektronikus úton rögzített adatot a hatóság adathordozóra történő **rögzítés (átmásolás) útján foglalja le**, vagy a helyszínen lefoglalt adathordozóról **az adatokat szakértő bevonásával menti le**.

::: 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

Angolszász definíciók

Rule 101. Scope; Definitions

(6) a reference to any kind of written material or any other medium **includes electronically stored information**.

(Federal Rules of Evidence)

Digital Evidence – Information **stored or transmitted in binary form** that may be relied upon in court.

(International Organization on Computer Evidence)

Digital Evidence – Information of probative value that is **stored or transmitted in binary** form.

(Scientific Working Group on Digital Evidence)

A BIZONYÍTÉK ÉS A SZAKÉRTŐ

Extended Model of Cybercrime Investigations

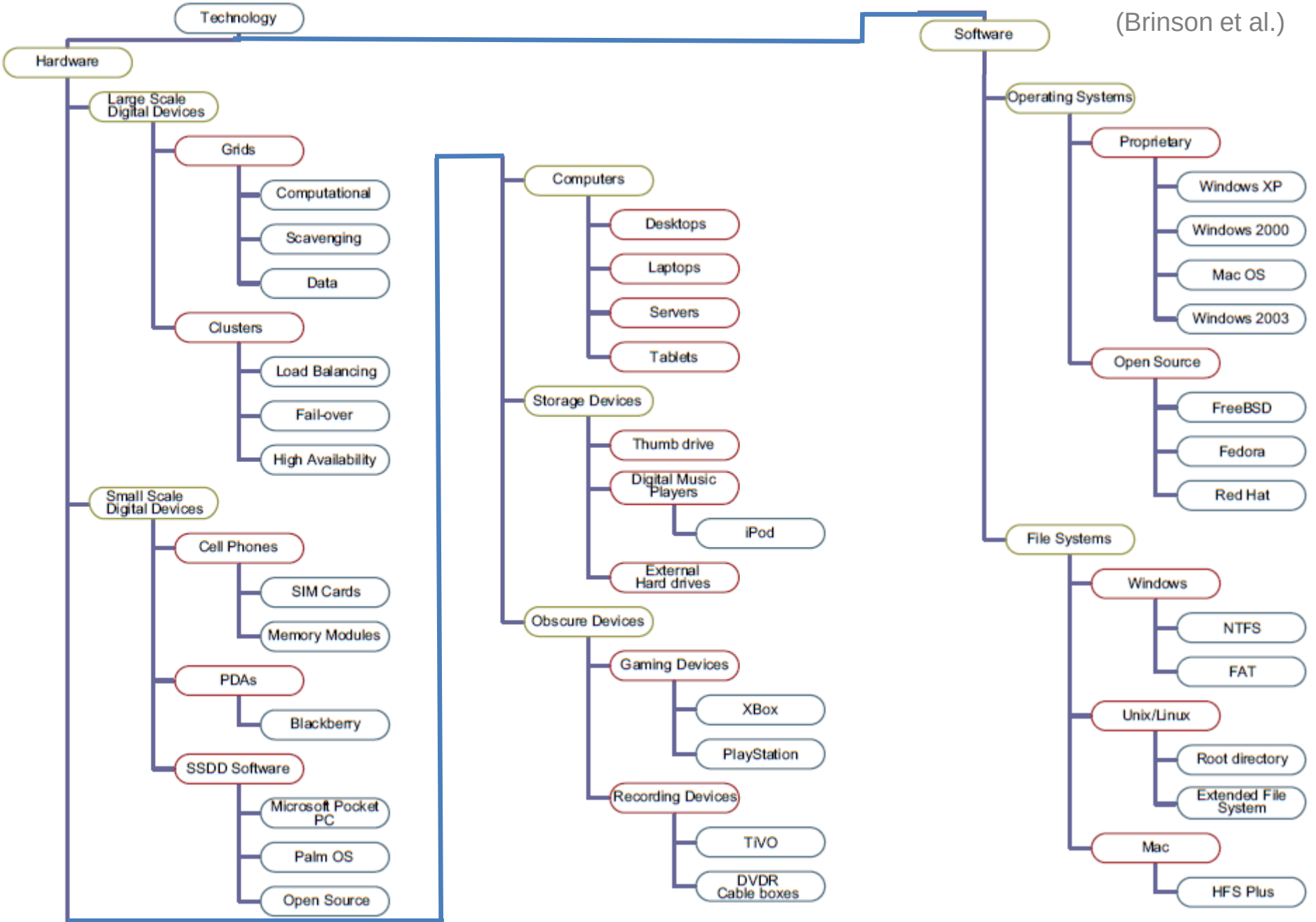
1) Awareness
2) Authorisation
3) Planning
4) Notification
5) Search for and identify evidence
6) Collection of evidence
7) Transport of evidence
7) Storage of evidence
8) Examination of evidence
10) Hypothesis
11) Presentation of hypothesis
12) Proof/Defence of hypothesis
13) Dissemination of information

::: Ciardhuáin, Séamus Ó.: An Extended Model of Cybercrime Investigations

“Preserve everything but change nothing”

5) **Search for and identify evidence -** a bizonyítékok felkutatása és azonosítása
6) **Collection of evidence -** A bizonyítékok összegyűjtése konzerválásra és elemzésre alkalmas módon, a jogszabályi előírások betartása mellett
7) **Transport of evidence** - a bizonyíték(ok) szállítása az érvényesség (validity) megőrzése mellett, beleértve a számítógépes hálózatokon történő továbbítást és a fizikai szállítást egyaránt
8) **Storage of evidence** - a bizonyíték(ok) tárolása oly módon, hogy annak integritása ne sérülhessen
9) **Examination of evidence** - a bizonyíték(ok) vizsgálata a rendelkezésre álló technikai eljárások és eszközök felhasználásával a bizonyítékok integritásának megőrzése mellett

(Brinson et al.)



Csomagolás

biztonsági tasak

bűnjel tasak

forrás: alfahir.hu

forrás: tamper.com

biztonsági szalag

forrás: bekas3.freewb.hu

szemetes zsák

biztonsági zárócímke

::: forrás: Adeptum Kft. – adeptum.hu

biztonsági plomba

Bizonyíték típusok

Lage Scale Digital Devices

Server Clusters,Cloud/Grid computing

- A laboratóriumi vizsgálat általában nem oldható meg (szerver farmok, cloud computing)
- A bűnjel/bizonyíték lefoglalása az érdekelt őrizetében hagyása mellett történik
- A szakértő csak a helyszínen (ha van ilyen vö. cloud) vizsgál(hat)

Small Scale Digital Devices

PDA, smartPhone, SIM …

- Laboratóriumi vizsgálat megoldható (lefoglalás mellett)
- Az eszközök hosszú idő után kerülnek a szakértőhöz (1-12 hónap)
- Energiaellátás hiánya miatt adatok veszhetnek el
- Kellékek (tápellátás, adatkábel stb.) hiánya nehezíti a vizsgálatot

Bizonyíték típusok

Computers

Szerverek, asztali számítógépek, laptopok, tabletek

- A legnagyobb tömegben előforduló bizonyíték típus,
- „Csomagolási” problémák – PC, laptop
- All-in-one gépek „monitornak” látszanak
- Net/nano PC – médiaboxok és set-top-boxok nagy mértékű hasonlósága

Storage devices

Pendrive-ok, zene lejátszók, külső merevlemezek, SAN tárolók

- egyes tárolók kis méretük miatt nehezen észlelhetők (microSD…),
- A hálózati tárak nem nyilvánvaló helyeken is lehetnek,
- A növekvő kapacitások miatt a bizonyíték rögzítése megváltoztathatatlan tároló egyre nehezebb (vö. BluRay olvasó a kirendelőnél)

Bizonyítékok kezelése típusonként

Obscure devices

Játék eszközök (Xbox, Play Station) / Rögzítő eszközök (megfigyelő rendszerek, video rögzítők)

- A kis ügyszám miatt az egyes eszközök kezelése nehézkes a kirendelő és szakértő részéről egyaránt

Software

Operációs rendszer környezet / Fájlrendszer környezet / adatok

- Az adatelemző és helyreállító programok drágák vö. law enforcement price („csak” egy papíron múlik)

MÓDSZERTAN

Digital Forensics - eljárási szabályok

Minimal Handling of the Original – az eredetit csak minimálisan használd

Account for any change – tarts számon bármilyen változást

Comply with the rules of evidence – tartsd be a bizonyítás szabályait

Do not exceed your knowledge – ne lépd át saját tudásod határát

::: Matthew Braid: Collecting Electronic Evidence After a System Compromise p.13.

A bizonyíték öt alapelve

1. **Admissible – elfogadható**
   (jogszabályoknak megfelelően gyűjtött bizonyíték)
2. **Authentic – hiteles**
   (a bizonyíték kapcsolódik az eseményhez)
3. **Complete – teljes**
   (a bizonyítékokat nem csak egy nézőpont szerint gyűjtjük)
4. **Reliable – megbízható**
   (a begyűjtési és elemzési eljárások nem sértik a hitelességet)
2. **Believable – hihető**
   (bemutatása legyen könnyen érthető és világos)

::: Matthew Braid: Collecting Electronic Evidence After a System Compromise p.12.

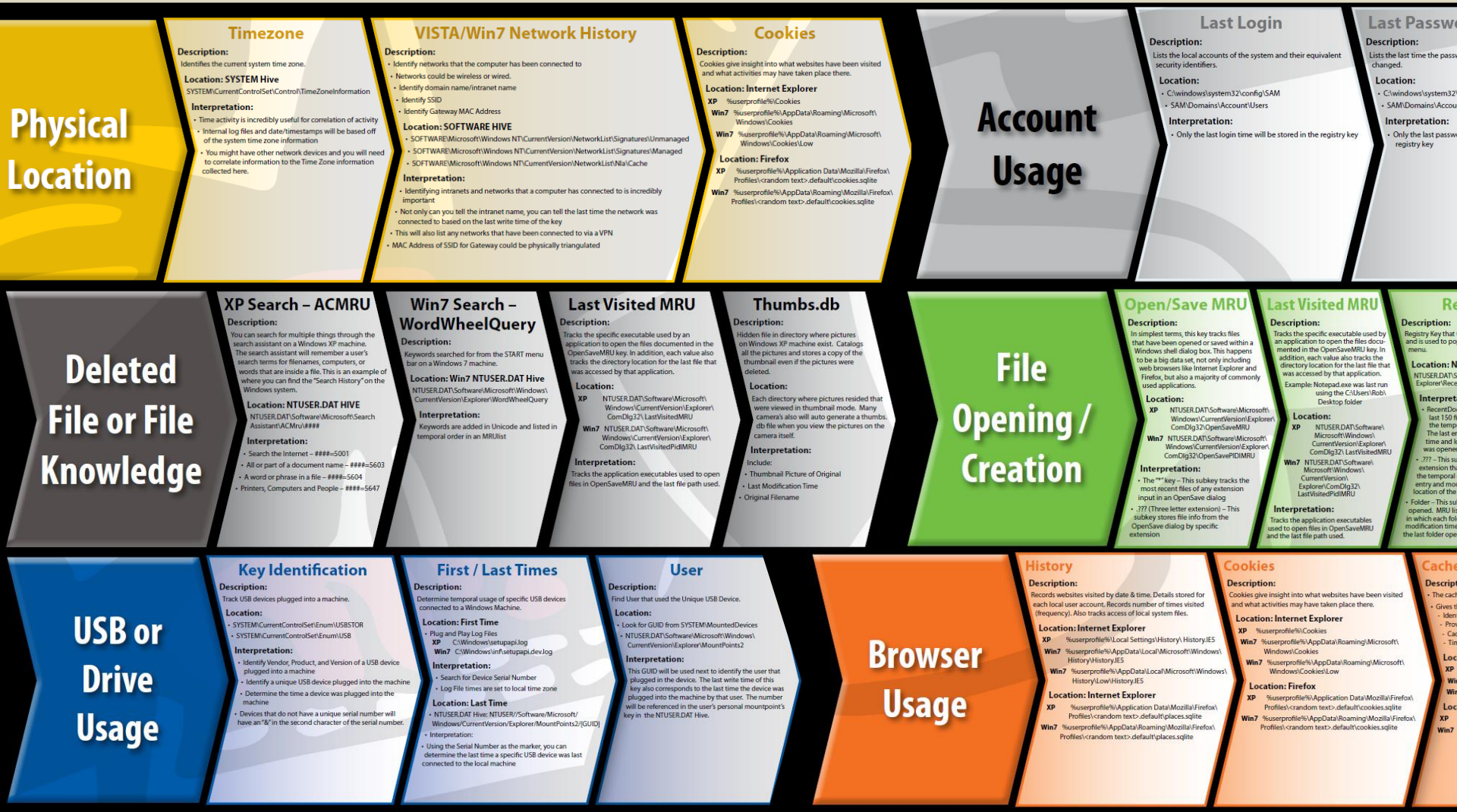
Order of Volatility

- registers, cache
- routing table, arp cache, process table, kernel statistics, memory
- temporary file systems
- disk
- remote logging and monitoring data that is relevant to the system in question
- physical configuration, network topology
- archival media

Chain of Custody

- **Where**, **when**, and **by whom** was the evidence discovered and collected.
- **Where**, **when** and **by whom** was the evidence handled or examined.
- **Who** had custody of the evidence, during **what period**. How was it stored.
- When the evidence changed custody, **when and how did** the transfer occur (include shipping numbers, etc.).

Standard procedures



(Lee, et al.)

Documentation

- Tárgyi bizonyítékok jelölése ügyszám/helyszín/tétel + szakértő saját azonosítója + eszköz azonosító
- Mentett adatok jelölése ügyszám/helyszín/tétel + elérési út +
- A vizsgálati eljárás dokumentálása a szakértői véleményben (a szakértői módszertani levél alapján [ha van ilyen])

A szakértői archívum feltárul

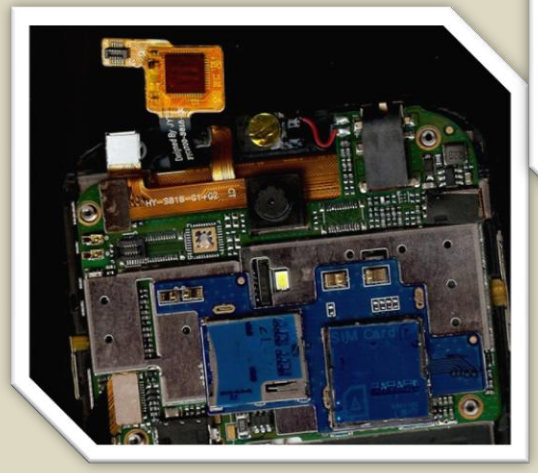
ESETTANULMÁNY

Small Scale Digital Devices

akkumulátor és SIM
(a készülékben maradjon, vagy külön tároljuk)

Védelem megkerülése
iPhone

régi rendszerek problémája
(GPS display)



árú hamis megjelölése
(az egyezőség mértéke – iPhone clone)

Large Scale Digital Devices

A keresett adat fizikai elhelyezkedésének meghatározása esetenként (Cloud) nem megoldható

forrás: tik.ee.ethz.ch

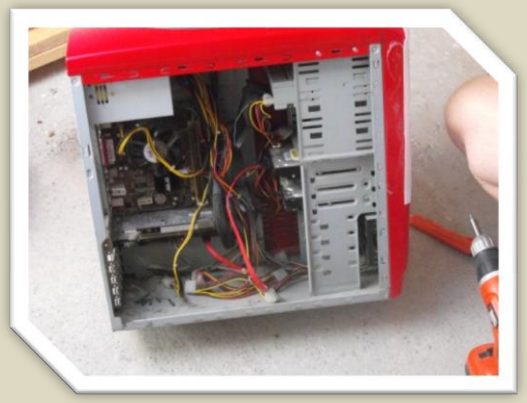
forrás: images.anandtech.com

A távoli vezérelhetőség miatt az élő rendszerek vizsgálata nehéz

Computers



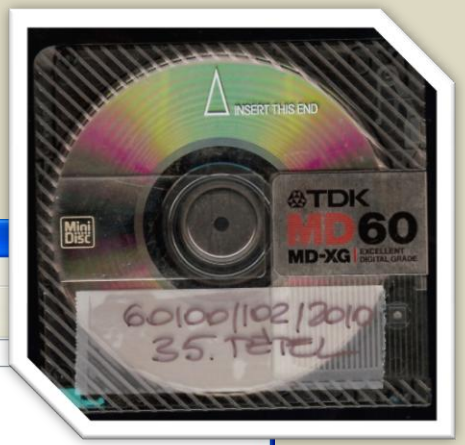


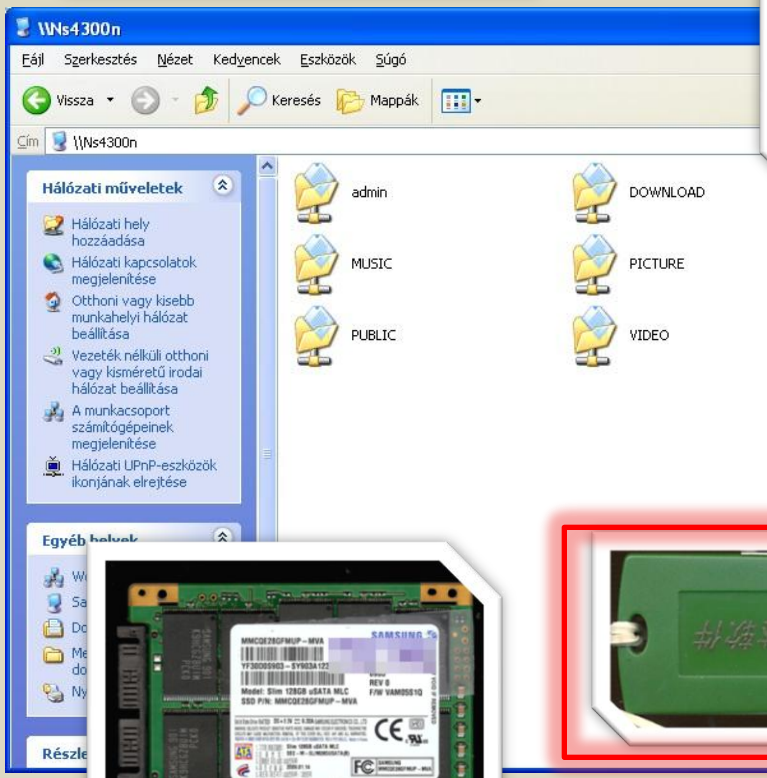



A bűnjel csomagolása

7. § (1) A hatóság a bűnjelet a lefoglaláskor vagy a letétbe helyezéskor - ha azt a jellege lehetővé teszi - becsomagolja és megőrzi olyan módon, hogy a tartalma illetéktelen személy előtt rejtve maradjon. Ha a bizonyítás érdekében szükséges, a hatóság a bűnjeleket külön-külön csomagolja (11/2003. (V. 8.) IM-BM-PM)

Storage Devices





Obscure Devides

„Megfigyelő” rendszer

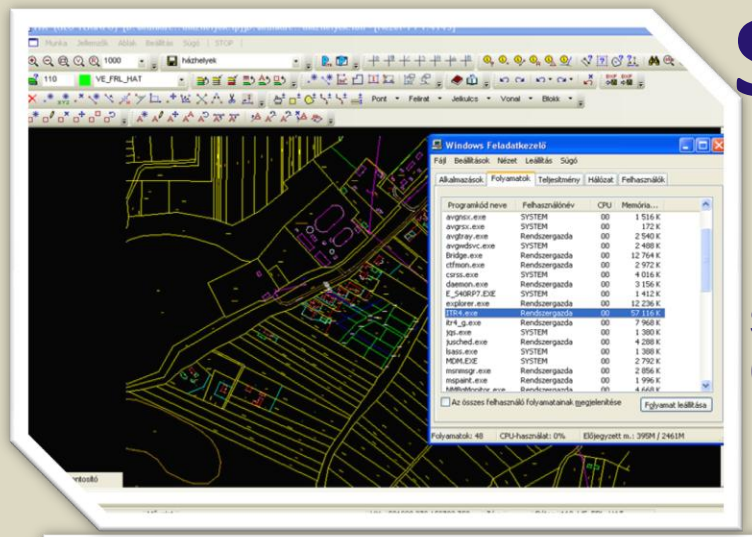
MP3 Player

Digitális videokamera

feltört PlayStation

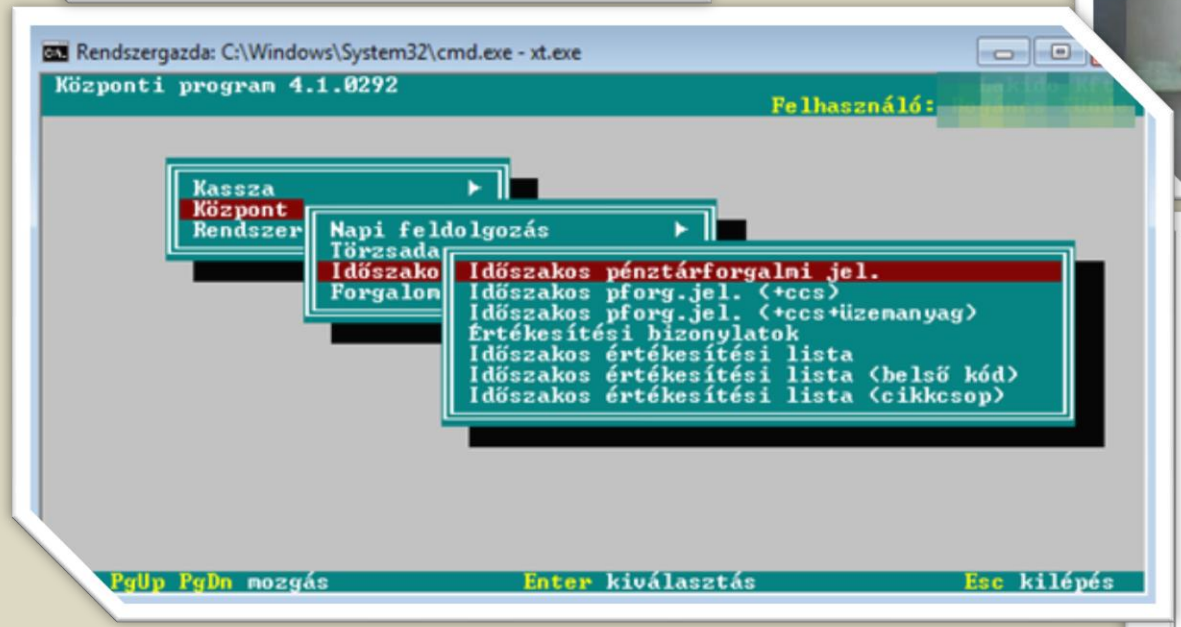
Digitális fényképezőgép

Software

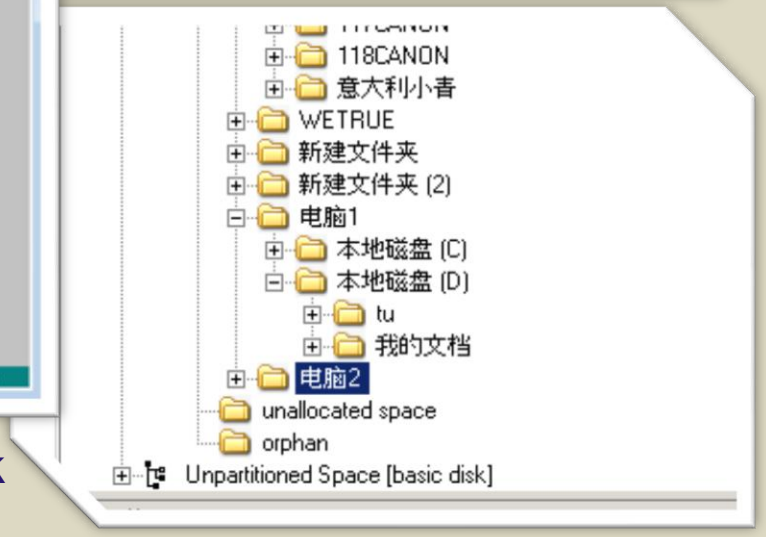


Feltört szoftverek (2009)

Fényképek előkészítése elemzésre



Könyvelési adatok



Idegen nyelvű tartalmak

Számítástechnikai rendszer útján rögzített adat megőrzésére kötelezés

Diachem ügy (2008)
Adatmentés „élő” rendszerről
[jogerős ítélettel lezárult]

1998. évi XIX. Tv. 158/A. §

(4) A megőrzésre kötelezést elrendelő a megőrzéssel érintett adatot fokozott biztonságú elektronikus aláírással **láthatja el.**

Szakirodalom

1. **Braid, Matthew**: Collecting Electronic Evidence After a System Compromise. AusCERT, Brisbane, 2001.
2. **Brezinski, D. – Killalea, T.**: Guidelines for Evidence Collection and Archiving. The Internet Society. 2002. online: http://www.ietf.org/rfc/rfc3227.txt, hozzáférés: 2013.11.15.
3. **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.
4. **Casey, Ehogan**: Digital Evidence and Computer Crime. Elsevier. Amsterdam, 2011.
5. **Ciardhuáin, Séamus Ó.**: An Extended Model of Cybercrime Investigations. in International Journal of Digital Evidence. ijde.org, online, 2004. pp.1-22.
6. **Lee, Rob – SANS DFIR Faculty**: Digital Forensics and Incident Response Poster. SANS Institute, Bethesda, MD, USA, 2012.


That's all Folks!