



A bizonyítékok kezelése

- az igazságügyi informatikai szakértő a büntetőeljárásban -



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 eszközüül 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**.



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**.



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.**



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



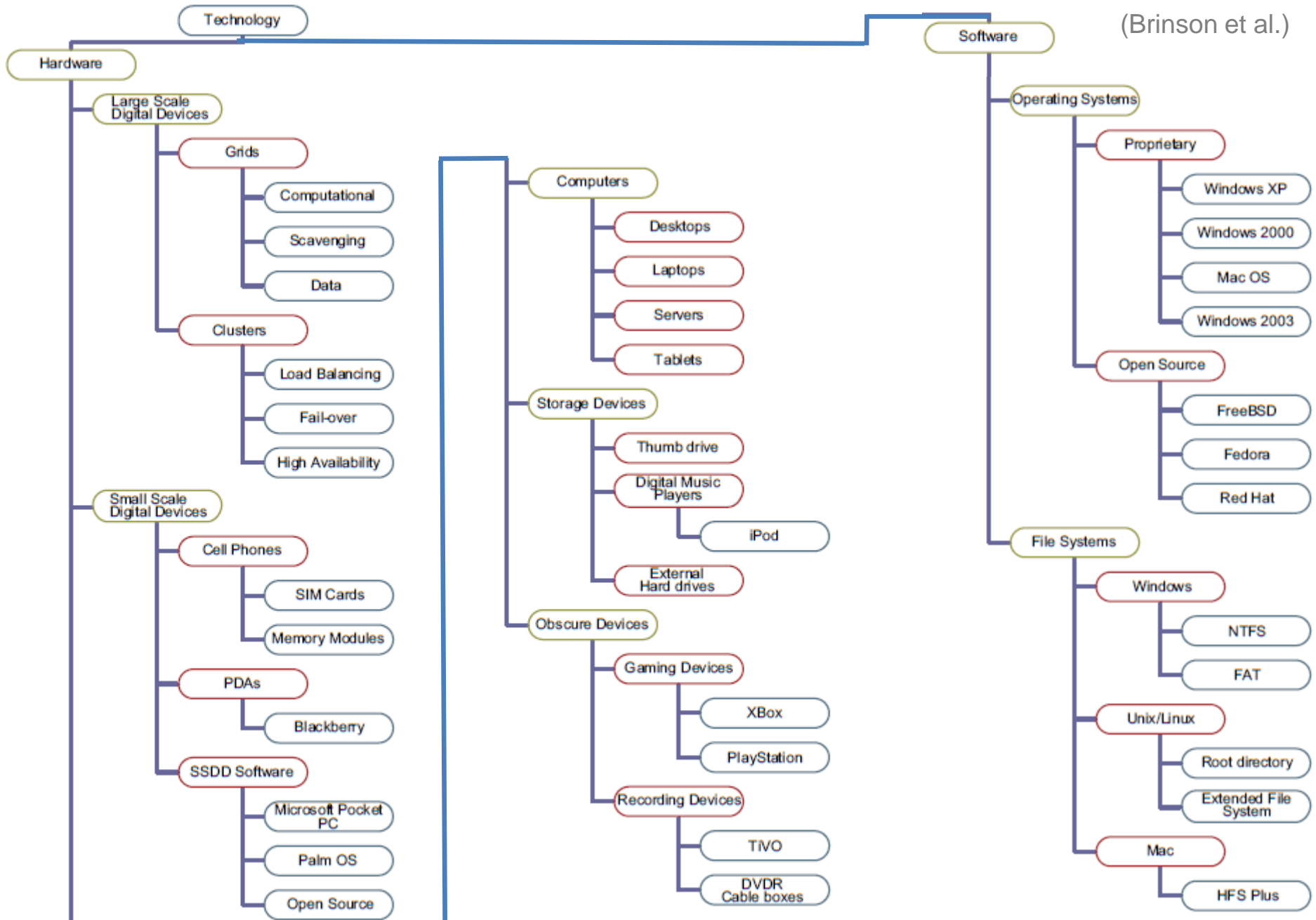
Extended Model of Cybercrime Investigations

- 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



“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: bekas3.freewb.hu

forrás: tamper.com



biztonsági szalag

biztonsági zárócímke



forrás: Adeptum Kft. – adeptum.hu



szemetes zsák



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 táruk 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



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)



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

Physical Location

Timezone

Description:
Identifies the current system time zone.

Location: SYSTEM HIVE
SYSTEM\CurrentControlSet\Control\TimeZoneInformation

Interpretation:

- Time activity is incredibly useful for correlation of activity
- Internal log files and date/timestamps will be based off of the system time zone information
- You might have other network devices and you will need to correlate information to the Time Zone information collected here.

VISTA/Win7 Network History

Description:

- Identify networks that the computer has been connected to
- Networks could be wireless or wired.
- Identify domain name/intranet name
- Identify SSID
- Identify Gateway MAC Address

Location: SOFTWARE HIVE

- SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged
- SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed
- SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Na\Cache

Interpretation:

- Identifying intranets and networks that a computer has connected to is incredibly important
- Not only can you tell the intranet name, you can tell the last time the network was connected to based on the last write time of the key
- This will also list any networks that have been connected to via a VPN
- MAC Address of SSID for Gateway could be physically triangulated

Cookies

Description:
Cookies give insight into what websites have been visited and what activities may have taken place there.

Location: Internet Explorer

XP %userprofile%\Cookies
Win7 %userprofile%\AppData\Roaming\Microsoft\Windows\Cookies

Location: Firefox

XP %userprofile%\Application Data\Mozilla\Firefox\Profiles*random text*.default\cookies.sqlite
Win7 %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles*random text*.default\cookies.sqlite

Account Usage

Last Login

Description:
Lists the local accounts of the system and their equivalent security identifiers.

Location:

- C:\windows\system32\config\SAM
- SAM\Domains\Account\Users

Interpretation:

- Only the last login time will be stored in the registry key

Last Password

Description:
Lists the last time the password was changed.

Location:

- C:\windows\system32\config\SAM
- SAM\Domains\Account\Users

Interpretation:

- Only the last password change time will be stored in the registry key

Deleted File or File Knowledge

XP Search - ACMRU

Description:
You can search for multiple things through the search assistant on a Windows XP machine. The search assistant will remember a user's search terms for filenames, computers, or words that are inside a file. This is an example of where you can find the "Search History" on the Windows system.

Location: NTUSER.DAT HIVE
NTUSER.DAT\Software\Microsoft\Search Assistant\ACMRu####

Interpretation:

- Search the Internet - ####-5001
- All or part of a document name - ####-5603
- A word or phrase in a file - ####-5604
- Printers, Computers and People - ####-5647

Win7 Search - WordWheelQuery

Description:
Keywords searched for from the START menu bar on a Windows 7 machine.

Location: Win7 NTUSER.DAT HIVE
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

Interpretation:
Keywords are added in Unicode and listed in temporal order in an MRU list

Last Visited MRU

Description:
Tracks the specific executable used by an application to open the files documented in the OpenSaveMRU key. In addition, each value also tracks the directory location for the last file that was accessed by that application.

Location:

XP NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
Win7 NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidIMRU

Interpretation:
Tracks the application executables used to open files in OpenSaveMRU and the last file path used.

Thumbs.db

Description:
Hidden file in directory where pictures on Windows XP machine exist. Catalogs all the pictures and stores a copy of the thumbnail even if the pictures were deleted.

Location:
Each directory where pictures resided that were viewed in thumbnail mode. Many cameras also will auto generate a thumbs.db file when you view the pictures on the camera itself.

Interpretation:

- Include:
- Thumbnail Picture of Original
- Last Modification Time
- Original Filename

File Opening / Creation

Open/Save MRU

Description:
In simplest terms, this key tracks files that have been opened or saved within a Windows shell dialog box. This happens to be a big data set, not only including web browsers like Internet Explorer and Firefox, but also a majority of commonly used applications.

Location:

XP NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
Win7 NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidIMRU

Interpretation:

- The *** key - This subkey tracks the most recent files of any extension input in an OpenSave dialog
- ??? (Three letter extension) - This subkey stores file info from the OpenSave dialog by specific extension

Last Visited MRU

Description:
Tracks the specific executable used by an application to open the files documented in the OpenSaveMRU key. In addition, each value also tracks the directory location for the last file that was accessed by that application. Example: Notepad.exe was last run using the C:\Users\Rob\Desktop folder

Location:

XP NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
Win7 NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidIMRU

Interpretation:
Tracks the application executables used to open files in OpenSaveMRU and the last file path used.

USB or Drive Usage

Key Identification

Description:
Track USB devices plugged into a machine.

Location:

- SYSTEM\CurrentControlSet\Enum\USBSTOR
- SYSTEM\CurrentControlSet\Enum\USB

Interpretation:

- Identify Vendor, Product, and Version of a USB device plugged into a machine
- Identify a unique USB device plugged into the machine
- Determine the time a device was plugged into the machine
- Devices that do not have a unique serial number will have an 'X' in the second character of the serial number.

First / Last Times

Description:
Determine temporal usage of specific USB devices connected to a Windows Machine.

Location: First Time

- Plug and Play Log Files
- XP C:\Windows\setupapi\log
- Win7 C:\Windows\inf\setupapi.devlog

Interpretation:

- Search for Device Serial Number
- Log File times are set to local time zone

Location: Last Time

- NTUSER.DAT HIVE: NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{GUID}

Interpretation:

- Using the Serial Number as the marker, you can determine the last time a specific USB device was last connected to the local machine

User

Description:
Find User that used the Unique USB Device.

Location:

- Look for GUID from SYSTEM\MountedDevices
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

Interpretation:
This GUID will be used next to identify the user that plugged in the device. The last write time of this key also corresponds to the last time the device was plugged into the machine by that user. The number will be referenced in the user's personal mountpoint's key in the NTUSER.DAT HIVE.

Browser Usage

History

Description:
Records websites visited by date & time. Details stored for each local user account. Records number of times visited (frequency). Also tracks access of local system files.

Location: Internet Explorer

XP %userprofile%\Local Settings\History\History.IE5
Win7 %userprofile%\AppData\Local\Microsoft\Windows\History\History.IE5

Location: Firefox

XP %userprofile%\Application Data\Mozilla\Firefox\Profiles*random text*.default\places.sqlite
Win7 %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles*random text*.default\places.sqlite

Cookies

Description:
Cookies give insight into what websites have been visited and what activities may have taken place there.

Location: Internet Explorer

XP %userprofile%\Cookies
Win7 %userprofile%\AppData\Roaming\Microsoft\Windows\Cookies

Location: Firefox

XP %userprofile%\Application Data\Mozilla\Firefox\Profiles*random text*.default\cookies.sqlite
Win7 %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles*random text*.default\cookies.sqlite

Cache

Description:
The cache contains...

- Gives...
- Ident...
- Pro...
- Ca...
- Ti...
- LP...
- XP...
- Win...
- Win...
- LP...
- XP...
- Win...

(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: images.anandtech.com

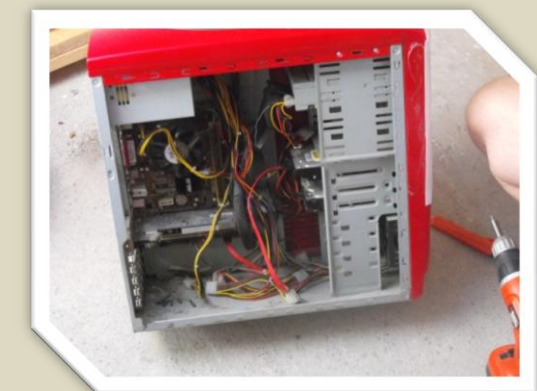
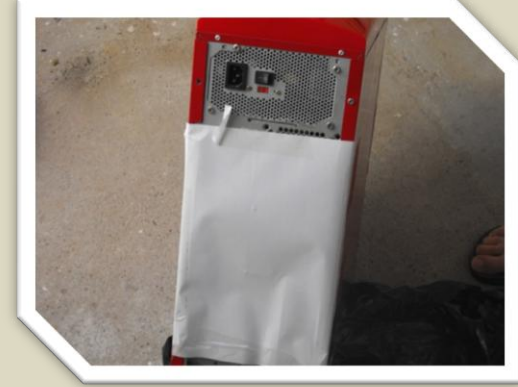


forrás: tik.ee.ethz.ch

A távoli vezérelhetőség miatt az élő rendszerek vizsgálata nehéz



Computers

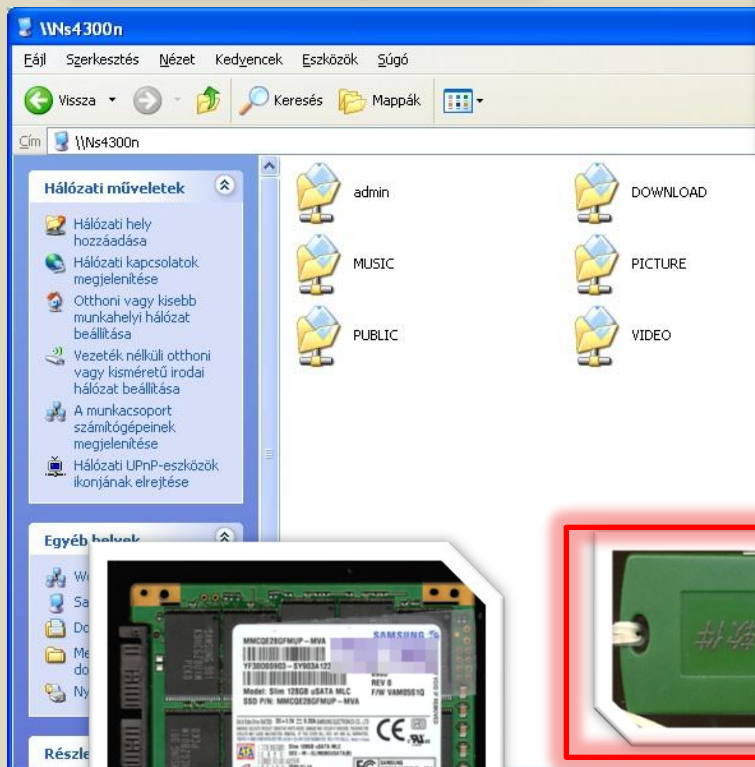
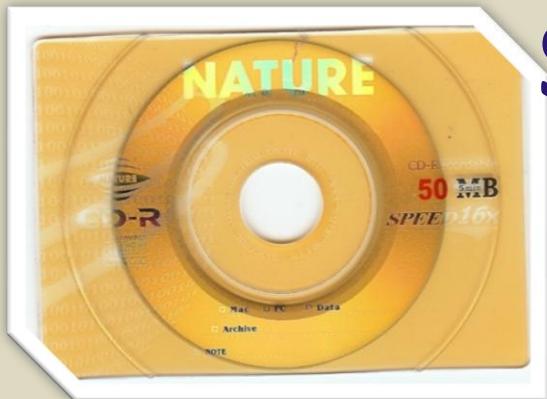


A bűnjel csomagolása

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



MP3 Player



Digitális videokamera



Digitális fényképezőgép

„Megfigyelő” rendszer



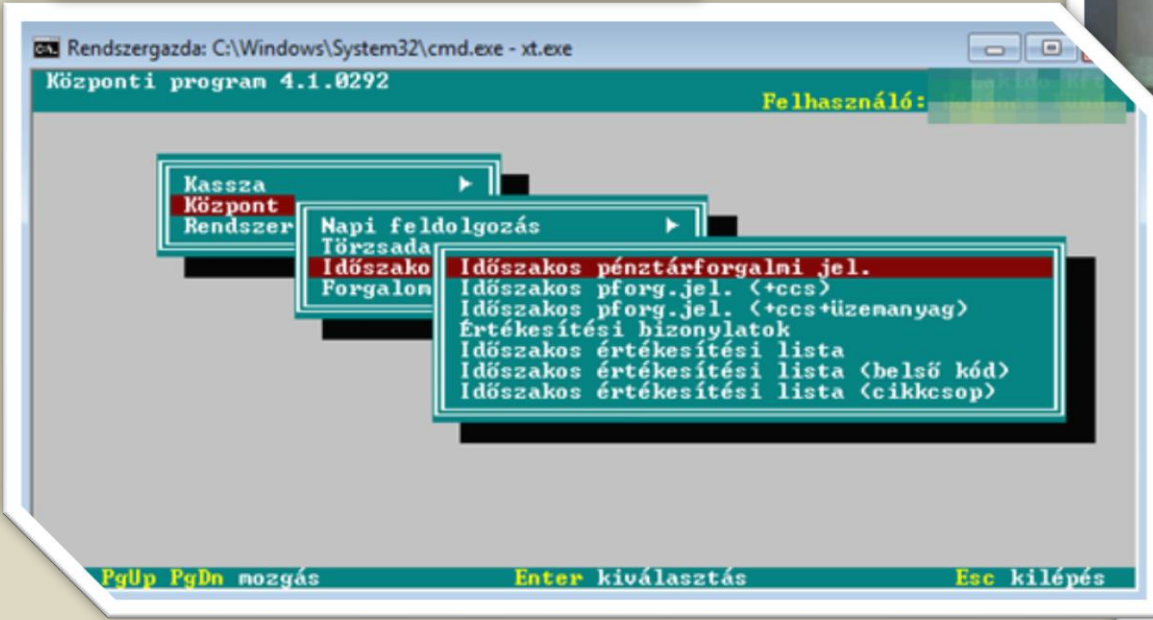
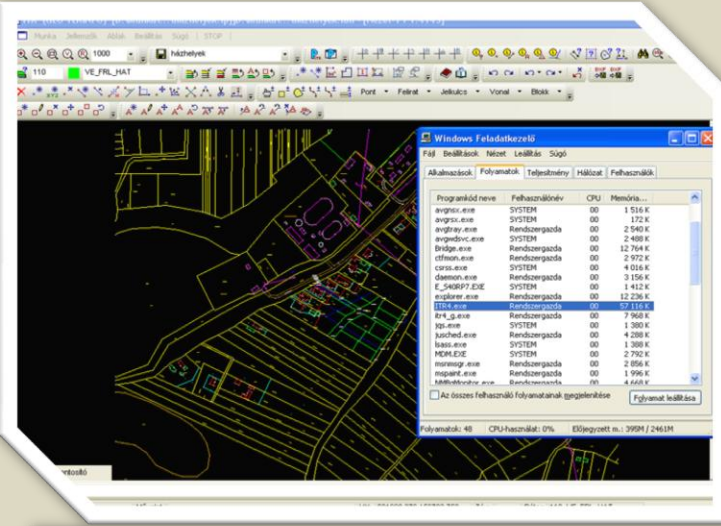
feltört PlayStation



Software

Fényképek előkészítése
elemzésre

Feltört
szoftverek
(2009)



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!