



EUROPEAN UNION



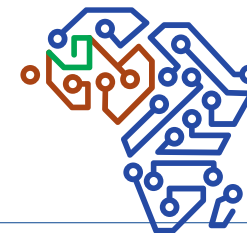
Projet financé par l'Union Européenne
Projet mis en œuvre par Expertise France

Basics of a CSIRT: Software environment Workshop on Digital Forensics

Accra, August 9 – 13, 2021



**ORGANISED CRIME: WEST AFRICAN RESPONSE ON
CYBERSECURITY AND FIGHT AGAINST CYBERCRIME**



OCWAR-C

OCWAR-C – CS8 – CSIRT Trainings, Accra (Ghana) August 2021



Index



Introduction: The Teacher

Key concepts of Digital Forensics

The importance of Digital Forensics today

The different phases of DF: Identification, Preservation, Extraction, Analysis, Report, Chain of Custody

Live Analysis vs. Dead Analysis

Other types of DF: Mobile & Cloud Forensics

Instruments to be used for each phase

Case Studies

Practice on your own computer and on the instruments carried by the trainer

Conclusion



Workshop on Digital Forensics



DISCLAIMER

The information contained in this presentation are for educational purposes only and informative, the author is not responsible if it is as incorrectly to damage people or things.

The author holds the intellectual property and is not allowed to use for different purposes.

The contents of this presentation may be used or reproduced, provided only if the source is mentioned.



Workshop on Digital Forensics



INTRODUCTION: THE TEACHER

- Computer Engineering Degree + Master in Computer Forensics & Digital Investigations
- Active Member of the IT Engineer Commission, Engineers Association of the Latina Province
- CLUSIT Member (ITALIAN INFORMATION SECURITY ASSOCIATION)
- IISFA Member (INFORMATION SYSTEM FORENSICS ASSOCIATION)
- Technical Assessor at Civil and Criminal Court
- Official Trainer NATO & US NAVY
- VP & Head of Digital Forensics Unit @ Security Brokers,
- Advisor @European Courage Focus Group – Cyber Terrorism & CyberCrime
- ITU ROSTER OF EXPERTS





Workshop on Digital Forensics



INTRODUCTION: THE TEACHER

- Postgraduate Course in Computer Forensic University at the University of Camerino, organized by the Postal and Communications (Ministry of Interior) and the University of Camerino (Polo Computer and Law);
- Advanced Course in "Digital Forensics" at IISFA (Information Systems Forensics Association Italian Chapter);
- Certification CIFI - Certified Information Forensics Investigator;
- SPEKTOR - Official Certified Trainer (Accredited SPEKTOR Forensics Intelligence Training n.82);
- SPEKTOR - Official Certified Trainer (Accredited SPEKTOR Phone Intelligence Training n.83);
- Cellebrite Ufed Certification - Data Extraction - Logical and Physical Analysis.

THE ORIGINS

- At first the Digital Forensics has been used only for technological crimes (the "Common").
 - Computer intrusions;
 - Web defacement;
 - Damaging / Theft of data;
 - Pedophilia Online;
 - Phishing / Whaling;
 - Identity Theft and Fraud Banking.
- In other cases, the computers were simply ignored





Workshop on Digital Forensics



DF INTRODUCTION / 1

- Some cases "not ICT" solved in recent years which has been read in the international media:
 - **Phone fraud**: analysis devices "GSM-box" -like in order to identify the technological Modus Operandi and the criminal business model.
 - **Industrial espionage**: to support company in the resolution and subsequent actions in court (theft of designs and industrial projects).
 - **Pedophilia online**: digital analysis of electronic evidence in support to Law Enforcement, PC and smartphone seized to the suspect.



DF INTRODUCTION / 2

- Real Cases:
- BTK Killer: Serial Killer arrested by investigating letters sent via floppy disk;
- <http://allday.com/post/1070-the-terrifying-true-story-of-the-btk-killer>
- David Riley: AirForce Major sent images of child pornography over internet

The Washington Post

Crime

Air Force major charged in child pornography case



DF INTRODUCTION / 3

- It is therefore clear how the analysis of digital evidences is necessary even for crimes that have nothing to deal with technology.
- **Cyberbullying** and **cyberstalking** through Facebook, and other Social Networks.
- Were not brought to the attention of the general public many other cases, fixed with the merits of digital evidence.



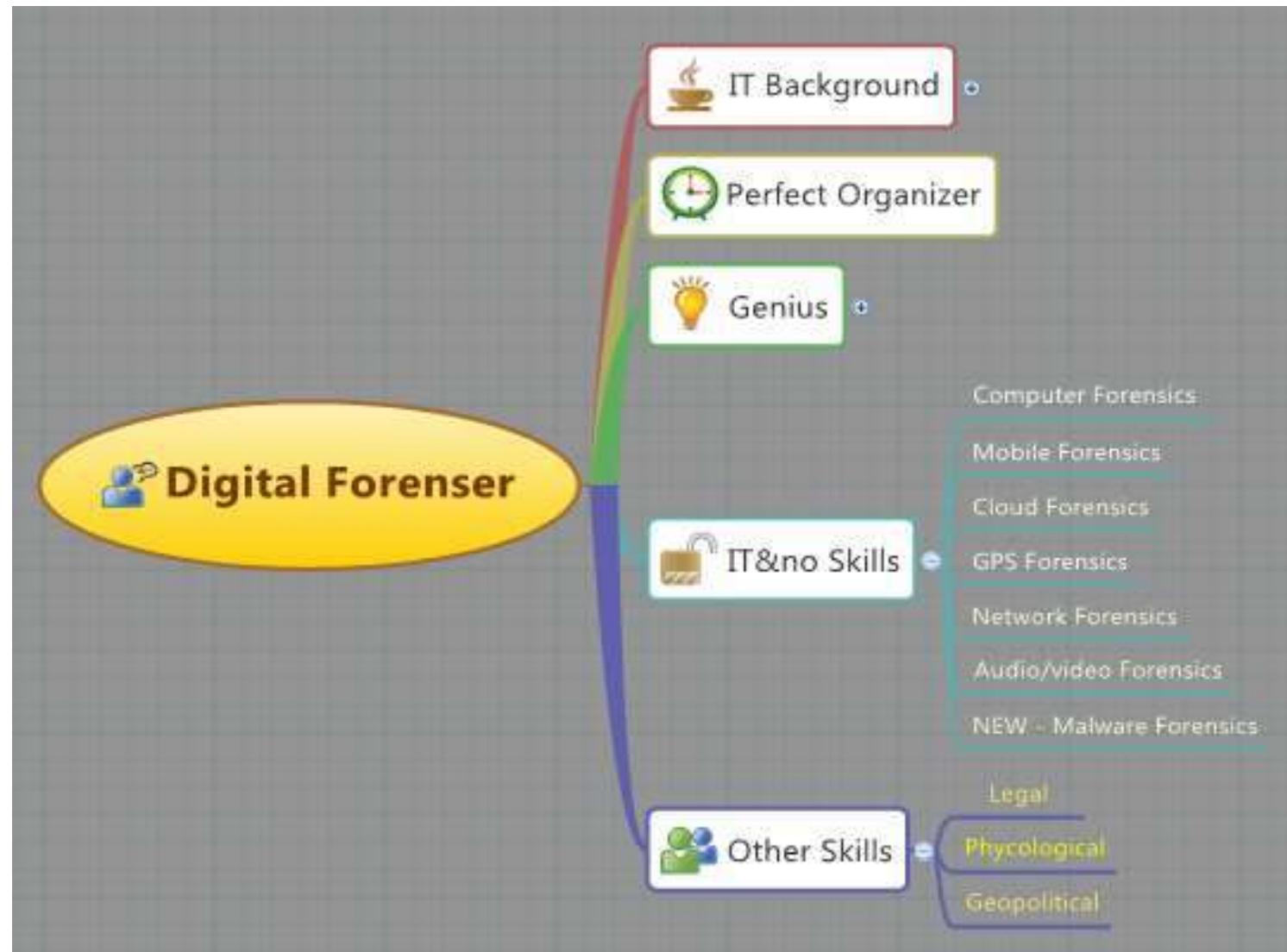
Workshop on Digital Forensics



USE OF DF TODAY

- Criminal Investigations
 - Child Pornography, e-Crimes, identify thieves;
- Civil litigation
 - eDiscovery
- Intelligence
 - Terrorist Attacks

DF INTRODUCTION / 4





Workshop on Digital Forensics



KEY CONCEPTS OF DIGITAL FORENSICS / 1

- A digital evidence can be defined as any information which has probative value that is stored or transmitted in digital form

A digital evidence can then be extracted by:

- A digital storage device
- Personal computers, notebook computers, external hard drive, floppy, tape, CD / DVD, memory card, USB drive, ...
- Mobile phones, SIM, SmartPhone, Tablet, SatNav, ...
An Intranet / Internet
- Interception of data traffic
Web pages, Blog, Social Network, Chat / IM, P2P, etc.

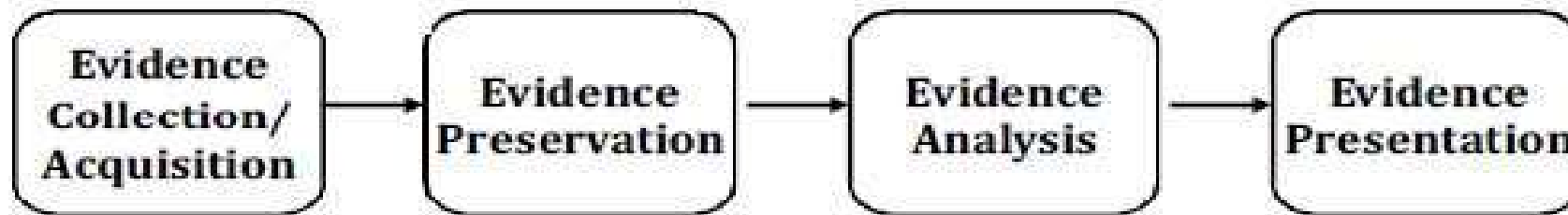
KEY CONCEPTS OF DIGITAL FORENSICS / 2

Digital Forensics is the science about how to **obtain, preserve, analyze** and **document digital evidences** from electronic devices such as: Tablet PCs, Servers, PDAs, fax machines, digital cameras, iPods, Smartphones (Mobile Forensics) and all of those stor



THE DIFFERENT PHASES OF DF

Computer Forensics phases:



- **Identification, Collection and Acquisition;**
- **Preservation**(Chain of Custody);
- **Analysis:** extracting those data significant to the investigation;
- **Evidence Presentation:** it's the final and the most important phase, during which *not-experts are capable as well* to understand the job which has been done (think about Lawyers, Prosecutors, Judges, etc...). It's a good practice to write down a document in which all of the gained data and its extracted results are analyzed and explained, step by step.



Workshop on Digital Forensics



DF INTRODUCTION / 5

- A digital evidence is fragile by nature, that is easily modified.
- If the device that contains the information of interest is turned off, the data that have not been saved can go permanently lost.
- If the device is found off turning involves changes to the system and / or the data contained therein.
- If the device is connected to the Internet or a corporate network, can be access from the outside with the goal of erase informations.
- If the digital evidence is located on the Internet (website, social network profile, etc.), Can be changed and / or removed from the owner page.



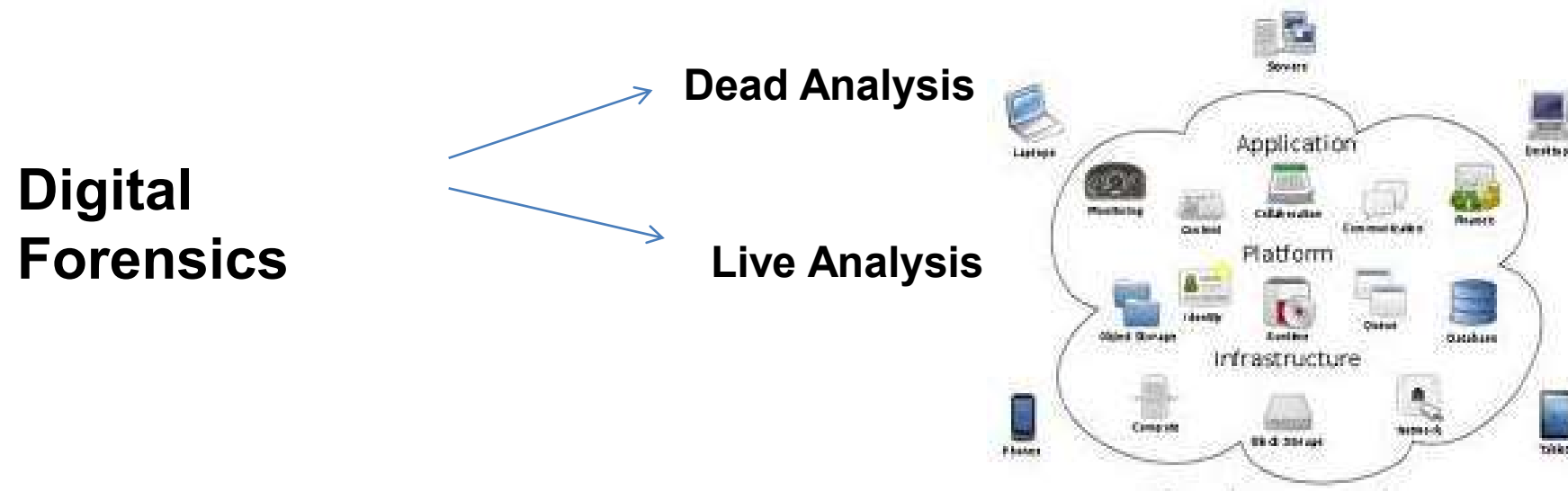
Workshop on Digital Forensics



DIGITAL EVIDENCE

- The digital data can be divided into two categories:
- volatile data
 - Data stored in volatile memories that are lost if you turn off the device that saves;
Users connected, open files, network information, running processes, mapping of processes on ports, RAM contents, clipboard contents, services running, shell commands;
- Non-volatile data
 - Data stored in mass storage and that is not lost if you turn off the device that saves data and program files, hidden files, slack space, swap files, index.dat files, unallocated clusters, unused partitions, hidden partitions, registry, event.

DEAD ANALYSIS VS LIVE ANALYSIS



Within the arrival of the Cloud, we've found ourselves in front of totally-new scenarios...

That's why:

We must think about new tools, instruments and methodologies that will be applied to the Evidence Collection & Acquisition phases.



Workshop on Digital Forensics



OPERATING STEPS

- ***Preparation and Identification***
- Acquisition and Retention
- Analysis
- Evaluation and presentation





Workshop on Digital Forensics



IDENTIFICATION

The identification step is done at the analysis of crime scenes
The identification process must follow the so-called "best practices"
The digital containers of interest during the investigation of a crime scene are (non-exhaustive list ...):

- Personal computers, notebooks and servers
- Hard disk not inserted in the computer (dismantled or external)
- Solid state drives
- Network Attached Storage (NAS)
- Floppy disks
- Backup tapes
- Cartridges ZIP / JAZ
- CD / DVD / BluRay
- Memory card
- USB Drives
- MP3 Player, Camcorders, Digital Cameras
- Network devices (Router, Switch, Firewall, IDS / IPS, Syslog Server)
- Mobile devices (mobile phones, SIM, SmartPhone, Tablet, SatNav)





Workshop on Digital Forensics



EUROPEAN UNION

THE ORIGINS





HARD DISK



EUROPEAN UNION





HARD DISK

- A hard disk is an example of non-volatile storage device
The data is recorded magnetically on the hard disk
- The main components of a hard drive are:
 - Cylinders (cylinders)
 - Heads (heads)
 - Dishes (platters)
- Each plate is divided into tracks
Each track is divided into sectors (typically 512 bytes)

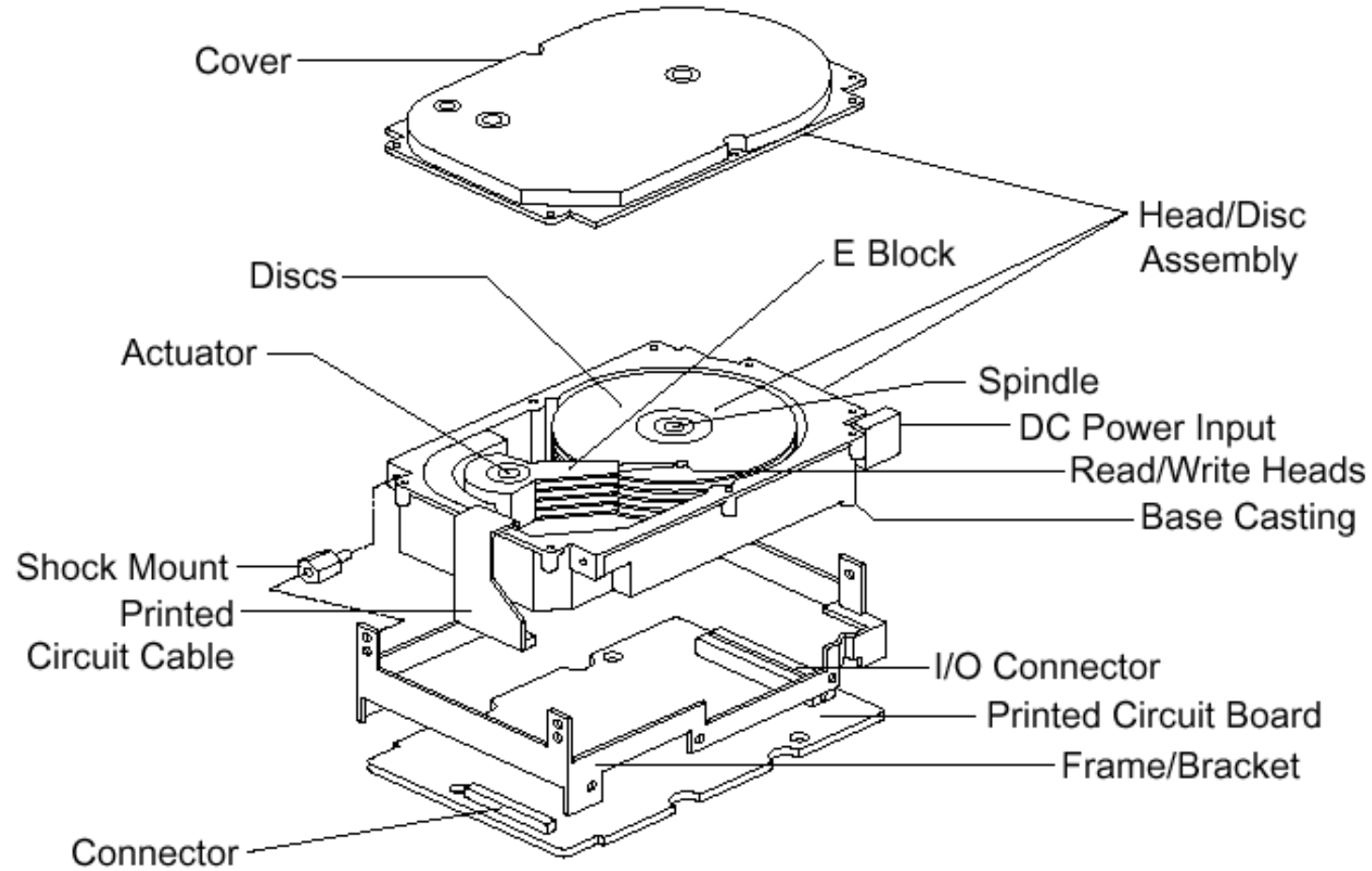


HARD DISK

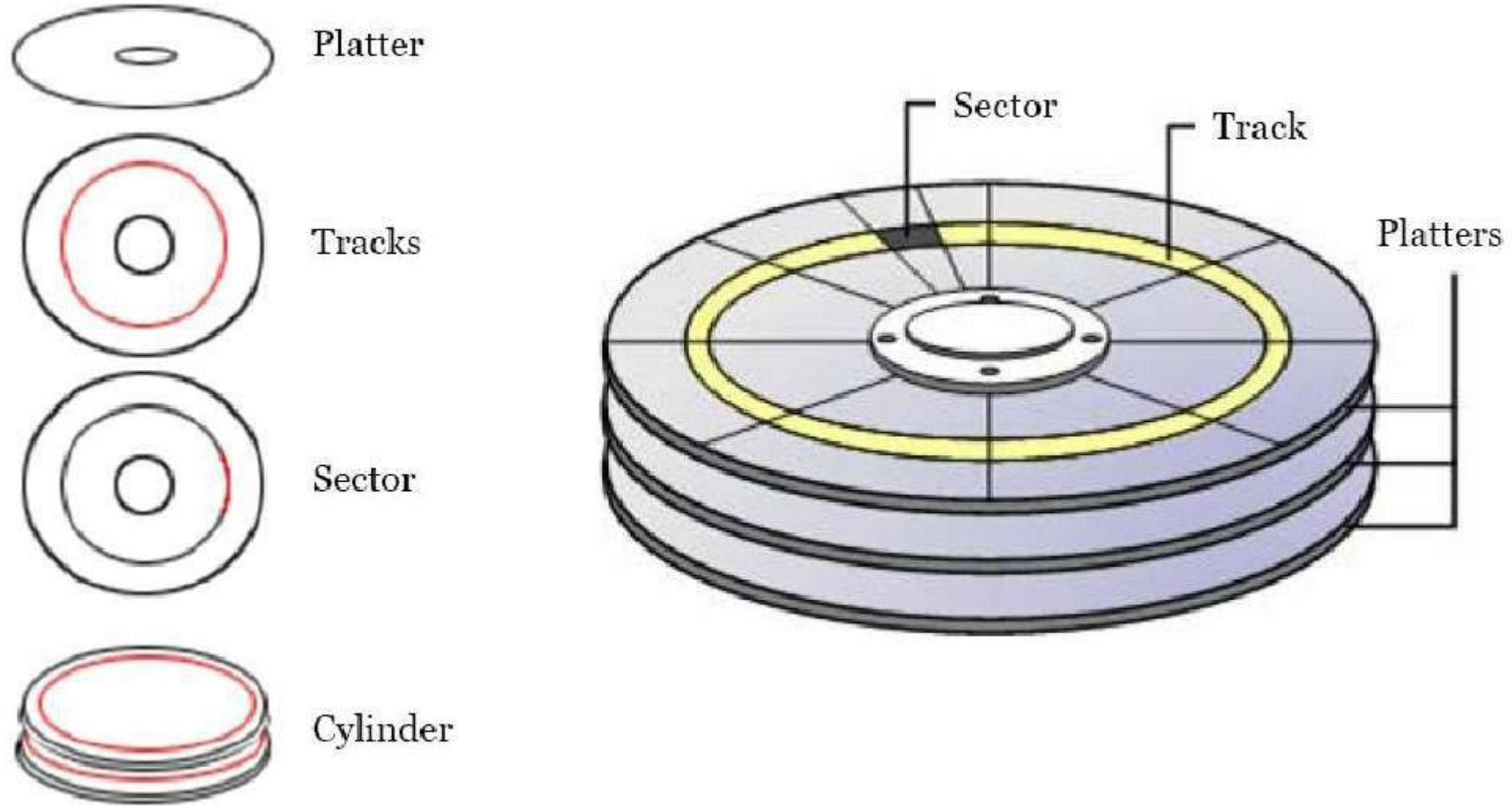
- When organizing data logic sectors are aggregated into clusters
- A hard disk is composed of a stack of plates, with read / write positioned above and below each plate
- During the rotation of the plates, the head moves from inside to outside (and vice versa) to read and write data



HARD DISK



HARD DISK





HARD DISK

There are several interfaces to connect a hard disk with a computer:

- **SCSI (Small Computer System Interface)**
- **IDE/EIDE (Integrated Drive Electronics/Enhanced IDE)**
- **Parallel ATA (Advanced Technology Attachment)**
- **Serial ATA (Advanced Technology Attachment)**
- **Fibre Channel**

HARD DISK



DB25m (Mac-SCSI)
Aprox: 38mm



C50m (SCSI-1)
Aprox: 63mm



IDC50m (SCSI-1)
Aprox: 78mm



IDC50f (SCSI-1)
Aprox: 67mm



HD50m (SCSI-2)
Aprox: 34mm



HD68m (SCSI-3)
Aprox: 47mm



HD68f (SCSI-3)
Aprox: 46mm



VHDC68m (SCSI-4)
Aprox: 32mm





PARTITIONING (MBR)

- The operation of partitioning consists to creation of a logical division of the hard disk
- Each partition can be formatted with a different **file system** (depending on your operating system)
- A partition can be primary or extended
- A primary partition contains a single file system
- An extended partition can be divided into logical drives
- The first sector of a hard disk is the **Master Boot Record**, which contains information on the physical and logical structure (partitions) of the disc

Structure of a Master Boot Record

| Address | | | Description | Size in bytes | |
|---------------------------------|------|-----|--|---|---|
| Hex | Oct | Dec | | | |
| 0000 | 0000 | 0 | Code Area | 440 (max. 446) | |
| 01B8 | 0670 | 440 | Optional Disk signature | 4 | |
| 01BC | 0674 | 444 | Usually Nulls; 0x0000 | 2 | |
| 01BE | 0676 | 446 | Table of primary partitions (Four 16-byte entries, IBM Partition Table scheme) | 64 | |
| 01FE | 0776 | 510 | 55h | MBR signature; 0xAA55 ^[1] | 2 |
| 01FF | 0777 | 511 | AAh | | |
| MBR, total size: 446 + 64 + 2 = | | | | 512 | |



FILE SYSTEM

- A file system determines the way in which files are stored on a hard disk
- Specific rules on the name of the file, the characters that you can use and the maximum length
- Generally allows you to organize data in a hierarchical (directory)
The main file system are:
- **NTFS (New Technology File System)**
 - (Microsoft Windows 2000/XP/2003/2008/Vista/7/8)
- **FAT32 (Windows 9x, Flash USB, Memory Card, Ipad)**
- **EXT (Linux)**
- **HFS/HFS+/UFS (Machintosh)**
- **ISO 9660/Joliet/UDF/CDFS (CD, DVD, BluRay)**
- **ZFS (Sun Solaris)**

Cluster e Slack Space

- A cluster is the smallest unit of data allocation on a hard disk
- The minimum size of a cluster is equal to one sector
- The formatting schemes used for creating clusters of variable size (2-32 sectors typically)
- Each read / write disk takes at least one cluster
- The unoccupied space in a cluster is called slack space



SSD

Solid state disks (SSD) are permanent storage devices that use solid state memory

The advantages of a solid state disk with respect to a magnetic disk are:

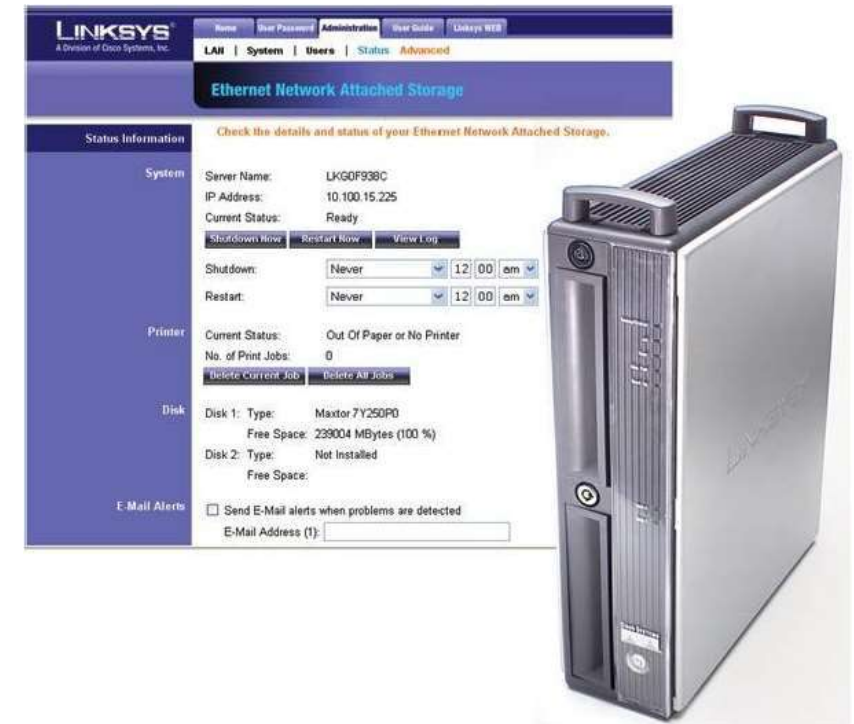
- Reduced use of electric current
- Data access in reading and writing faster
- increased reliability



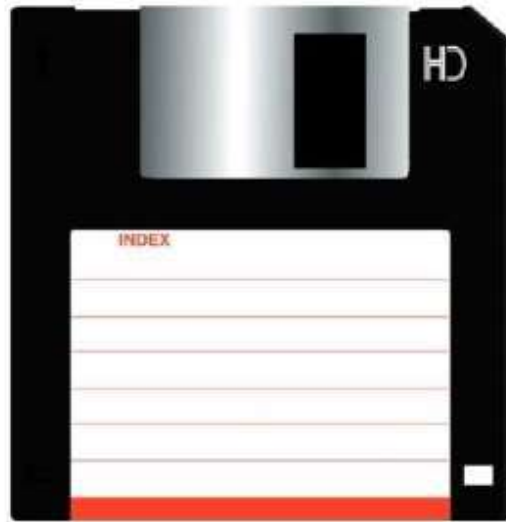
NETWORK ATTACHED STORAGE (NAS)

A Network Attached Storage (NAS) is a device directly connected to a network that provides centralized access to data to different clients.

It consists in a number of hard disks and from a hardware device, said NAS Head, which acts as an interface between the NAS and the clients of the network
Generally supports RAID configurations.



Floppy disk, ZIP/JAZ, CD, DVD, BluRay

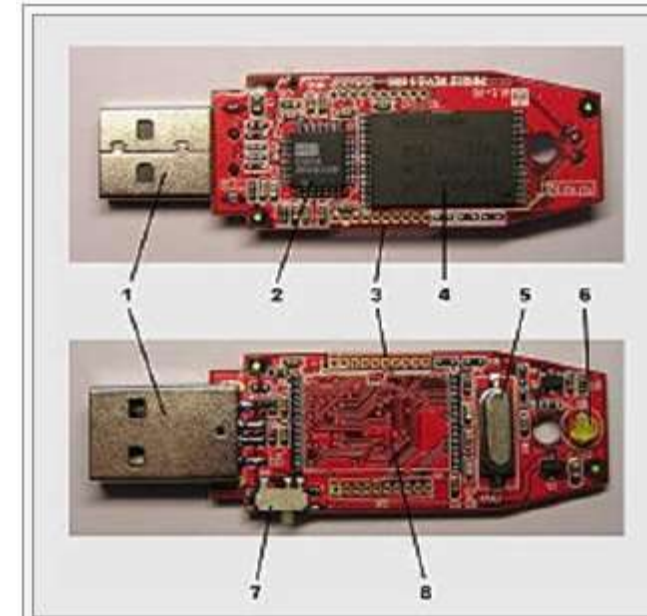



MEMORY CARDS



USB DRIVES

A USB flash drive is a permanent storage device, portable and rewritable with a USB interface
It is supported by modern operating systems



Una chiave USB priva di involucro esterno. 

Sono visibili:

- 1) connettore USB
- 2) chip di gestione del protocollo USB
- 3) pin per test industriali
- 4) memoria flash
- 5) quarzo dell'oscillatore
- 6) diodo led di funzionamento
- 7) interruttore per il blocco della scrittura
- 8) spazio per una seconda memoria flash

USB DRIVES





Workshop on Digital Forensics



MP3, Video cameras, Cameras, Tablet





Workshop on Digital Forensics



INTERNATIONAL BEST PRACTICES

There are detailed guidelines with the correct methods of acquisition :

- RFC3227 - Guidelines for Evidence Collection and Archiving (2002)
- USA – Department of Justice - Searching and Seizing Computers (2002)
- USA – IACP - Best Practices for Seizing Electronic Evidence (2006)
- USA – DoJ – Electronic Crime Scene Investigation v. 2 (2008)
- UK – ACPO – Computer Based Evidence Guidelines v.4 (2008)
- ISO 27037 (Draft) - Guidelines for identification, collection, acquisition and preservation of digital evidence





Workshop on Digital Forensics



Best Practices for the computer turned off

- Make it safe the scene and take control of the area that contains the device
Persons away present from all computers and power devices
Photograph or make a video recording of crime scenes and of all relevant components. If there is not a camera, draw the scene and tagging ports and cables so that the system can be reconstructed later
- ***DO NOT TURNED ON A COMPUTER IN ANY CIRCUMSTANCES***



Workshop on Digital Forensics



Best Practices for the computer turned on

- Make it safe the scene and take control of the area that contains the device
- Persons away present from all computers and power devices

Taking pictures or make a video recording of crime scenes and of all relevant components. If there is not a camera, draw the scene and tagging ports and cables so that the system can be reconstructed later

- Assess whether to ask the user information on the setup of the system, including password

Record the information on the monitor, carrying photographs and transcribing the text visible

- ***Do not touch the keyboard or click the mouse.***



CHAIN OF CUSTODY

- The digital evidence must be handled and stored very carefully to avoid contamination, damage and any action that could make it unusable
- All the actions taken should be carefully documented
- You must establish a chain of custody that identifies all the people who have had access to the original media
- The chain of custody must contain some basic information, such as:
 - Identification data of the case (number, investigator, nature and brief description)
 - Identification data of the holder (manufacturer, model, serial number)
 - Data identified the seizure (date and start time custody, place)
- Whenever the supports under investigation be conducted by a new investigator, in the chain of custody must be added information containing:
 - Name of the person who has taken over the support
 - Date and time of delivery and the date and time of return

Transportation and preservation of artifacts

Once the supports have been identified and it started a chain of custody, you have to worry about appropriately preserved and transport them to the laboratory

The appropriate storage conditions depends on the support
Some examples are:

- Anti-static bags (hard disk)
- Carrying suitcases
- The Faraday cages (mobile devices)





Workshop on Digital Forensics



Preservation of artifacts in the lab





Workshop on Digital Forensics



OPERATING STEPS

- Preparation and Identification
- **Acquisition and Retention**
- Analysis
- Evaluation and presentation



FUNDAMENTAL RULE

Preserve the Original!



Workshop on Digital Forensics



FORENSIC COPY

- The original must never be used to analyze data · To ensure the acquisition of all the data on the device is appropriate (where possible) to make a copy bit-to-bit (or bit-stream or forensics copy or image) of the original media, or an exact copy of the original media
- This is different from a simple data backup, which consists in copying files known and drop deleted files, slack space, unallocated space, etc.
- The acquisition is usually carried out by reading each bit of the original media (preventing any possible write) and writing an image file on an external (USB disk or network)
- The format "image" is the most used RAW (or dd, named Linux tool used to make the copy)

Duplication can be done via software or hardware



System hour and boot sequence

- Before proceeding with acquisition of the hard disk is necessary to extract from the machine being analyzed information relating to:
 - BIOS used and parameters of CMOS
 - Boot sequence
 - Date and time settings into the CMOS
- In particular, the date and time are needed to verify the real-time any divergence and rebuild a correctly sequence of events

Hardware Acquisition : duplicators

- It is the ideal solution in terms of speed and reliability
- The products are very expensive and we must follow the evolution of technology (IDE, SATA, SCSI,?)





Software Acquisition

- http://www.cftt.nist.gov/tool_catalog/index.php



Computer Forensics Tool Catalog

Home | **Tool Search** | Forensic Tool Taxonomy | Vendors | Contacts

| |
|--|
| Forensic Tool Functionalities |
| Cloud Services |
| Deleted File Recovery |
| Disk Imaging |
| Email Parsing |
| File Carving |
| Forensics Boot Environment |
| Forensic Tool Suite (Mac Investigations) |
| Forensic Tool Suite (Windows Investigations) |
| GPS Forensics |
| Hardware Write Block |
| Hash Analysis |
| Image Analysis (Graphics Files) |
| Infotainment & Vehicle Forensics |
| Instant Messenger |
| Media Sanitization/Drive Re-use |

Home > Tool Search

Search for forensic tools by functionality

Search Results for Disk Imaging: 16 tools found

(Note: search results are displayed in alphabetical order. The ordering of these results does not and is not intended to imply recommendation or endorsement by NIST. Any mention of commercial products is for information only.)

| | | | | | | | | | |
|---|---|-------------------------------|---|------------------------------------|-------------------------------|------------------------------|---|-----------------|-----------------|
| Result 1 of 16 | CFID : Covert Forensic Imaging Device | | | | | | | | |
| Version: | 2.0 | | | | | | | | |
| Tool Release Date: | July 2012 | | | | | | | | |
| Available Test Reports: | Under evaluation | | | | | | | | |
| Vendor: | Teel Technologies | | | | | | | | |
| Vendor Website: | http://www.scecanada.com | | | | | | | | |
| URL to Tool Description: | http://www.scecanada.com/cfid | | | | | | | | |
| Technical Parameters reported by vendor: | Tool host OS / runtime environment | Supported evidence interfaces | Supported target/destination interfaces | Types of data that may be acquired | Supported acquisition methods | Supported image file formats | Support for restoring the contents of an image file to a device | Hash algorithms | Data encryption |
| | | | | | | | | | no |





Software Acquisition

- The main operating systems that provide application solutions (native or additional) for copying forensics data are Linux and Windows
- To minimize the risk of alteration, consider using **write blocking** devices, which prevent hardware level writing on the original media
- On **Linux**, the data acquisition can be done by using the *native dd* or a variant with higher performance, or DCFLDD. There are also graphical tools like Guymager and AIR
- These commands can realize a copy bit-by-bit of an entire hard disk to an image file, from any disk that the operating system is able to interpret
- To satisfy needs of practical use was be developed some distributions of Linux Live, which allow the computer boot from CD or USB external memory for the acquisition
- The main ones are **DEFT, CAINE, RAPTOR, PALADIN** and **SANS - SIFT**



EUROPEAN UNION

Tsurugi

- [Tsurugi-linux.org](https://tsurugi-linux.org)



DEFT



- <http://www.deftlinux.net/it/>





CAINE

- <http://www.caine-live.net/>



EUROPEAN UNION





RAPTOR



- <https://www.forensicsandediscovery.com/Pages/Raptor.aspx>

Forward Discovery Raptor Toolbox

File

Image Verify Mount Find Unallocated Format Wipe Update Tasks

SUSPECT on Partition 1 of Physical device LEXAR JD FIREFLY 67CBAA08124140180607 1

Destination

Device E01 dmg dd (Raw) Segment file size (MB) 2000

TARGET on Partition 1 of Physical device WD 1200BEVExternal 5758455830363430323

Name Suspect_Drive Verify after creation

Additional Destination (Optional)

Device E01 dmg dd (Raw) Segment file size (MB) 2000

TARGET on Partition 1 of Physical device WD 1200BEVExternal 5758455830363430323

Name Suspect_Drive_Archive Verify after creation

Start



Paladin



- <http://sumuri.com/product-category/paladin/>





SANS

- <http://digital-forensics.sans.org/community/downloads>





Software Acquisition

- In Windows there are several user programs that allow copying forensics data
Since the disc is connected to a Windows operating system is necessary to ensure the blocking to write access, use a write blocker (hardware or software)
- The main acquisition tool available in the Windows environment are:
 - **AccessData FTK (Forensic Toolkit) Imager (freeware)**
 - **Tableau Imager (freeware)**
 - **R-Drive Image**
 - **Drive Snapshot**
 - **Safeback**



EUROPEAN UNION

FTK Imager

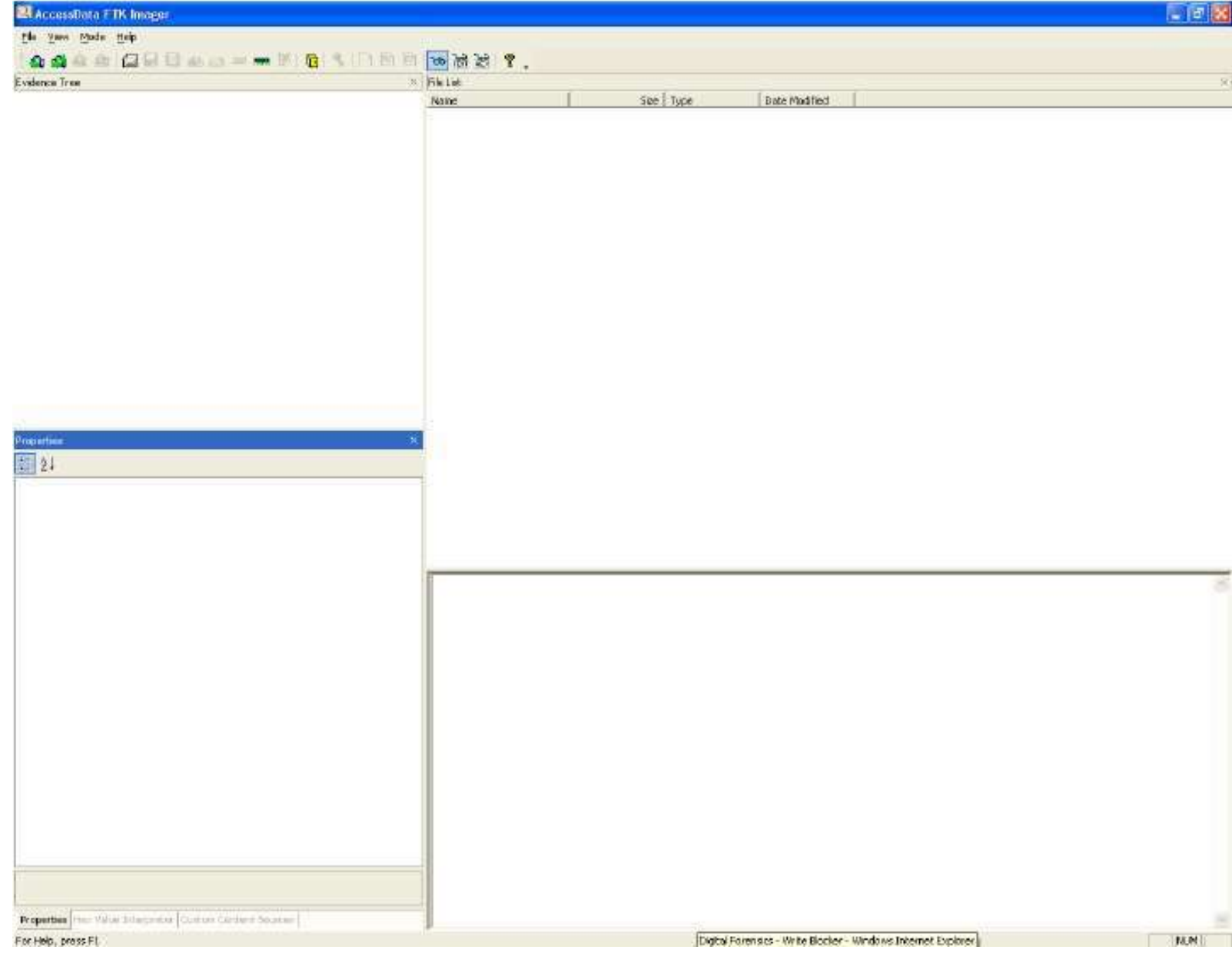




Tableau Imager

Tableau Imager

File Settings Help

Storage Devices

| | Device ID | Device Size | Device Information | Forensic Bridge Information |
|--|--------------------|------------------|---|-----------------------------|
| | \\.\PhysicalDrive0 | 320.0 GB | Hitachi HTS723232L95 (ATA) #908030CF4102EN8H2563 | |
| | \\.\PhysicalDrive1 | 0 bytes | RICOH R5C822 (Unknown) #0001 | |
| | \\.\PhysicalDrive2 | 0 bytes | RICOH R5C592 (Unknown) #0001 | |
| | \\.\PhysicalDrive3 | ⚠ 5.3 GB/80.0 GB | ST380815 A5 (SATA) #6QZ5CSTA | 135s Read-Only Mode |

Acquisition Queue

| Job | Device ID | Status | Started | Elapsed Time | Time Remaining | Finished |
|-----|--------------------|------------|--------------------------|--------------|----------------|--------------------------|
| 1 | \\.\PhysicalDrive3 | Finished | Wed Oct 21 16:38:24 2009 | 1 min 43 sec | - | Wed Oct 21 16:40:08 2009 |
| 2 | \\.\PhysicalDrive3 | 26% | Wed Oct 21 16:40:19 2009 | 25 sec | 1 min 12 sec | |
| 3 | \\.\PhysicalDrive0 | Waiting... | | - | - | |

Write Blocker Hardware

- During the acquisition of data from the hard disk, it is necessary to ensure a block to write access to maintain the integrity of the support
- Directly connecting hard disk to a computer acquisition can be data changes in it (ie. The date of last access)





Hardware vendors

The principal manufacturers of hardware for digital forensics are:

- **Tableau** - <http://www.tableau.com/>
- **Logicube** - <http://www.logicubeforensics.com/>
- **Intelligent Computer Solutions** - <http://www.ics-iq.com/>
- **Wiebetech** - <http://www.wiebetech.com/>
- **Voom Technologies** - <http://www.voomtech.com/>
- **MyKey Technology** - <http://www.mykeytech.com/>
- **ForensicPC** - <http://www.forensicpc.com/>



Write Blocker Software

- The write block at software level it may get used on the operation of mounting the hard disk from the operating system.
- Depending on the operating system used on the acquisition forensics machine, you can take proper precautions to prevent the bidirectional flow of communication and allow access in read-only mode.
- Linux volumes can be mounted directly in read only mode.
- The forensics Linux distributions adopt this technique.
- Under Microsoft Windows (from Windows XP SP2 onwards), it is possible to act at the level of system log to write-protect USB devices.
- Some useful free tools for the write lock of the USB ports in the Windows environment are:
Bytescout USB Locker
Document Solutions USB Write Blocker

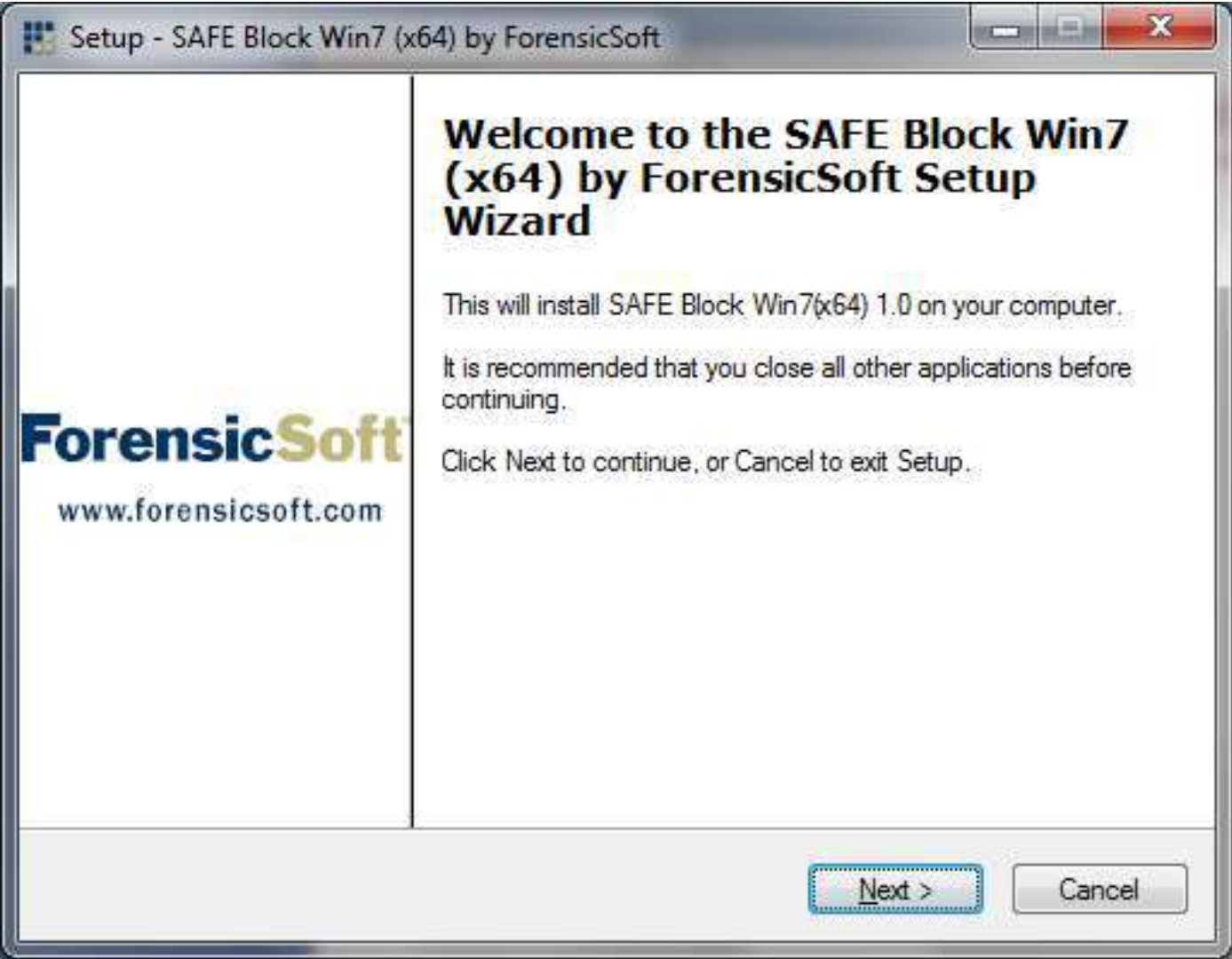


Write Blocker Software





Write Blocker Software



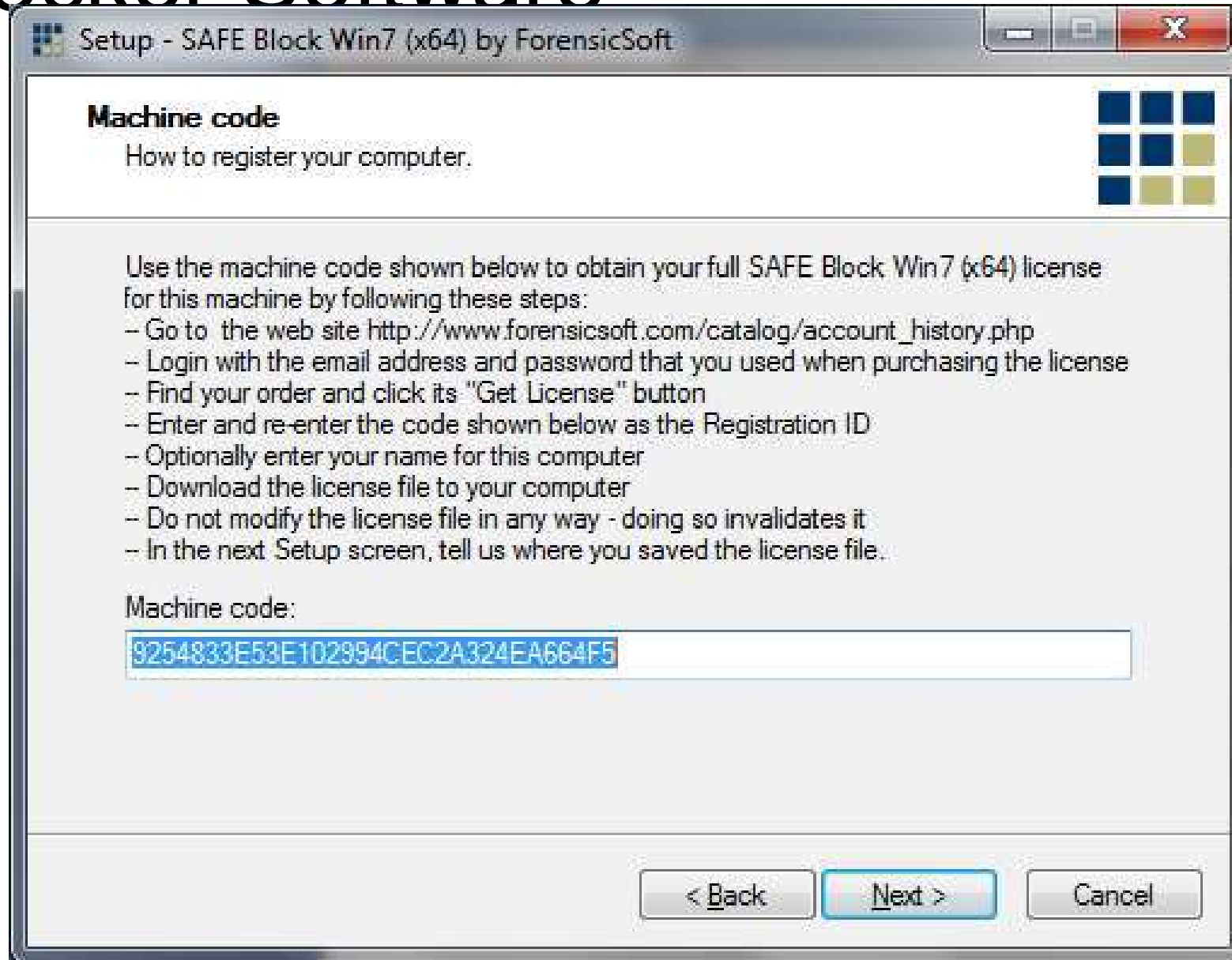


Write Blocker Software



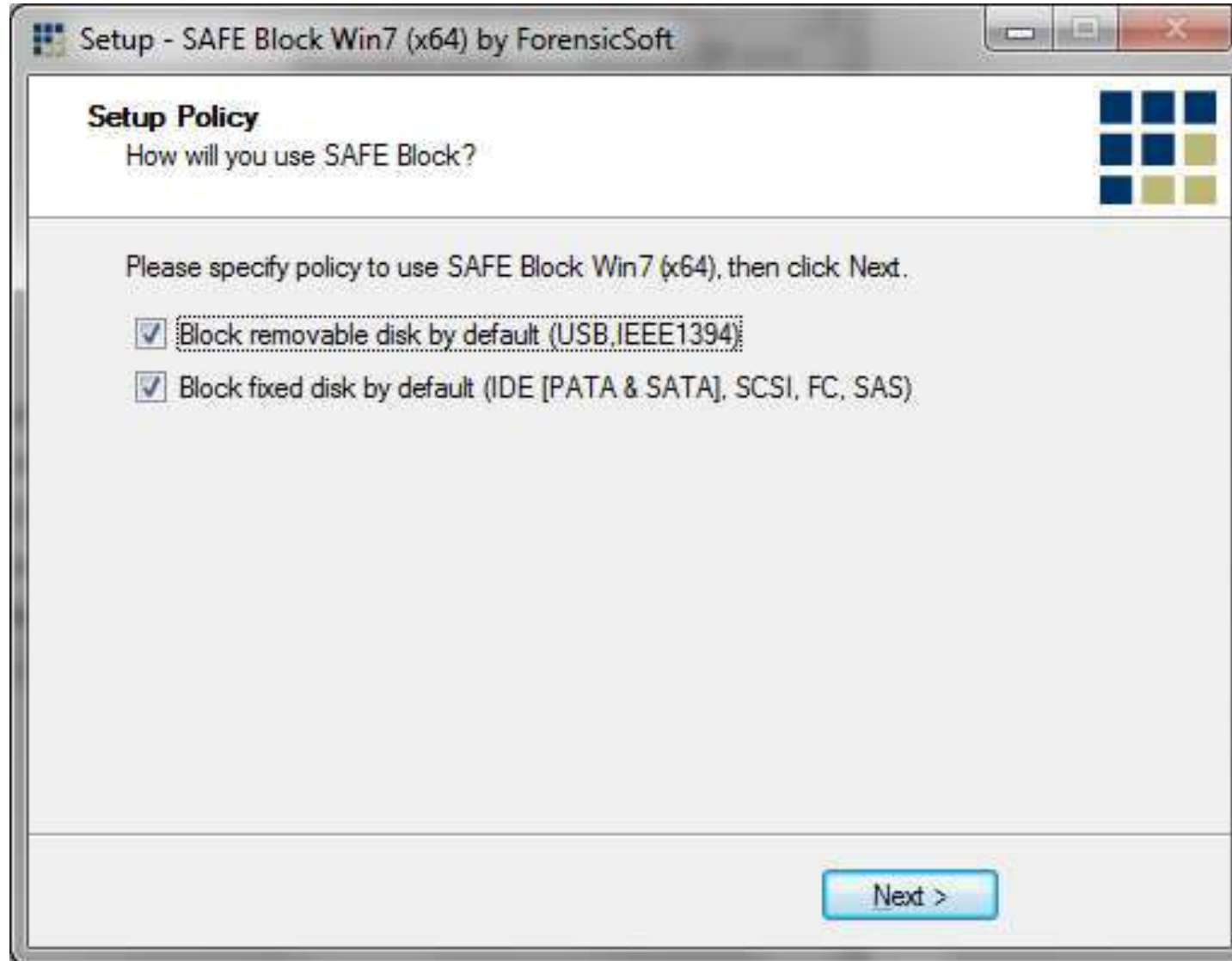


Write Blocker Software



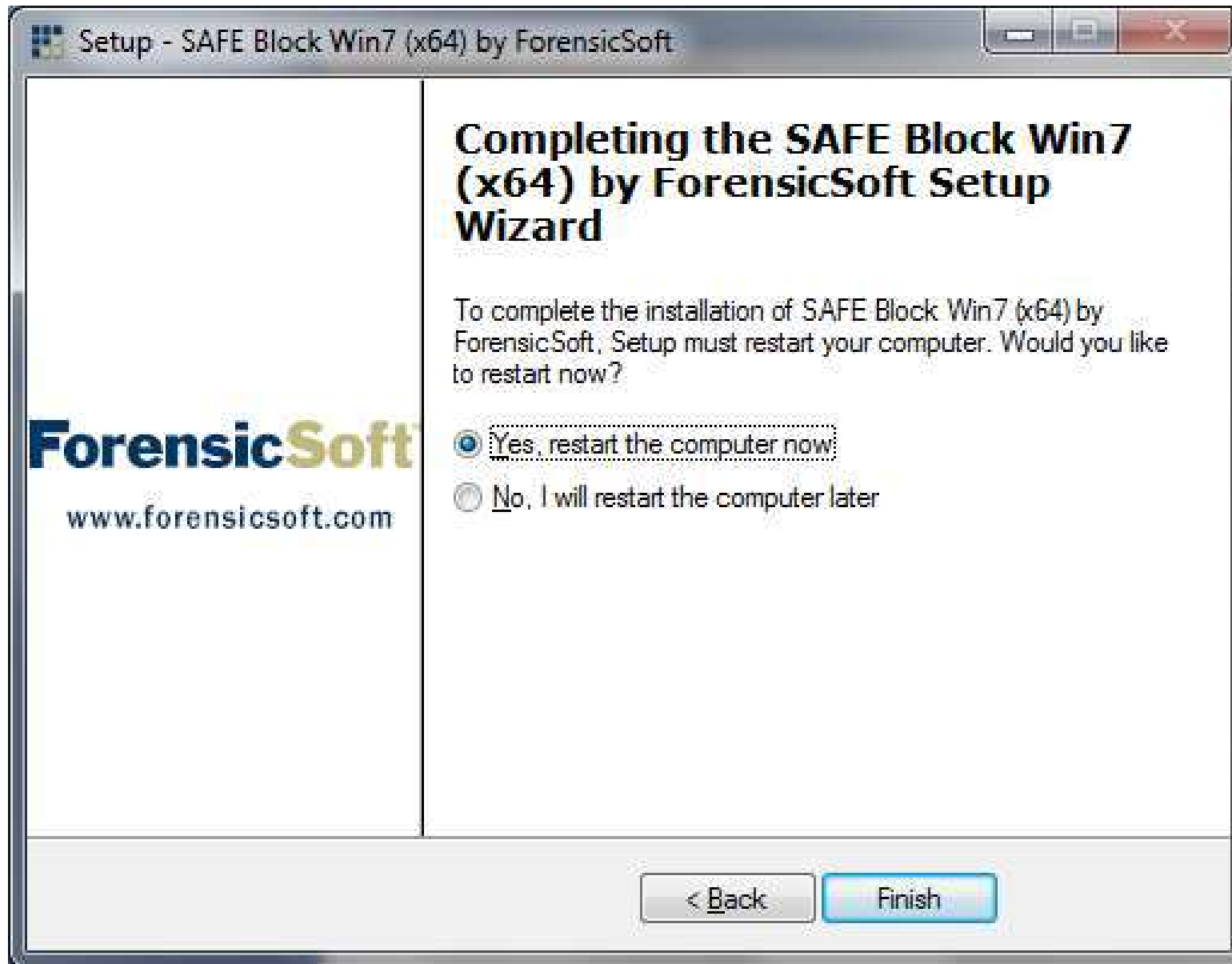


Write Blocker Software





Write Blocker Software



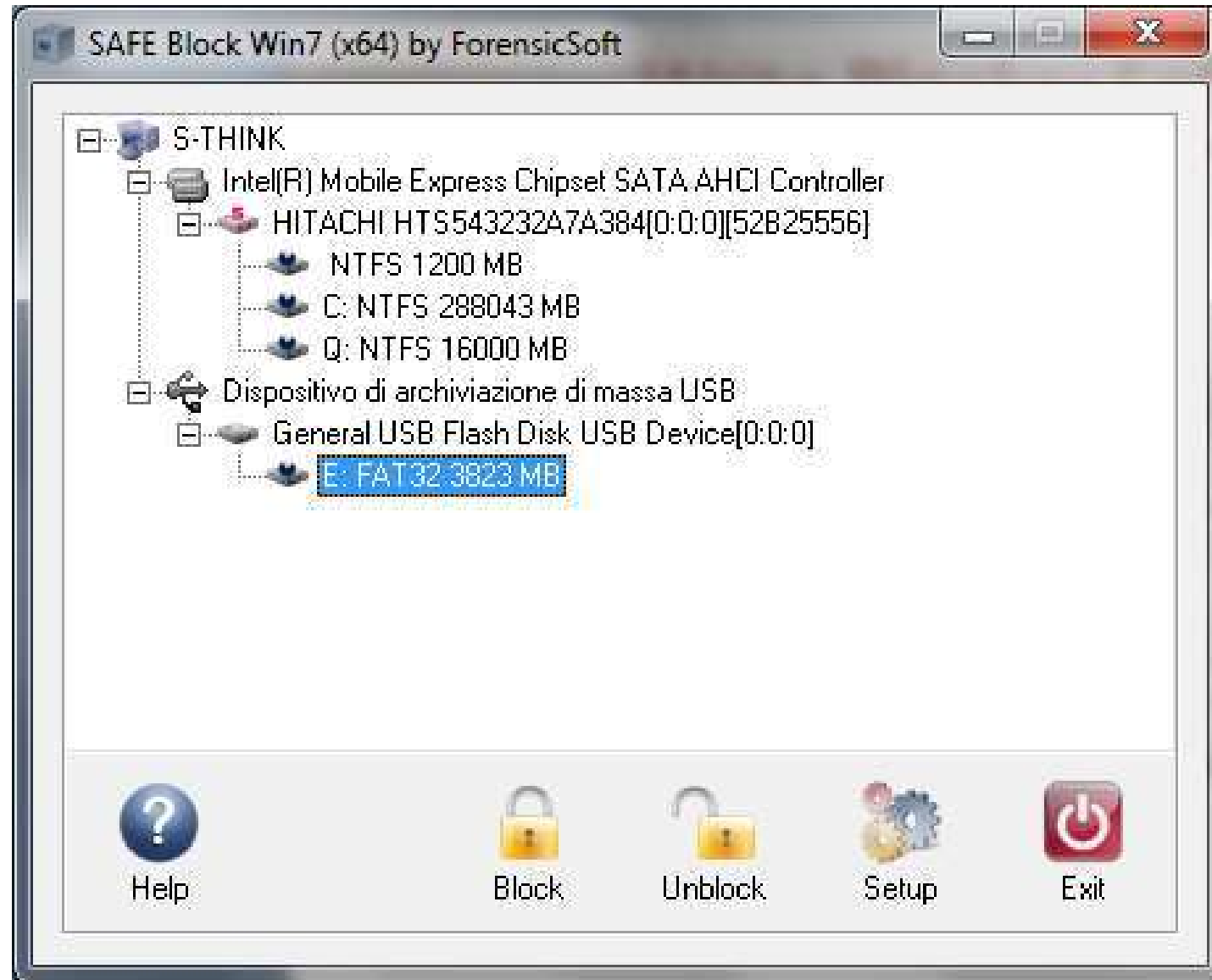


Write Blocker Software





Write Blocker Software





Checking the integrity copy

- How can I verify compliance and the next integrity of the copy?
- Verify bit to bit: Requires a very long time and it is possible only by placing the original
- ***Using hash functions***



Hash Function

- http://en.wikipedia.org/wiki/Cryptographic_hash_function
- Ideal Cryptographic hash function
 - Four important properties of a hash function:
 - Easy to generate the hash value
 - Impossible to know the hash in advance
 - Impossible to modify the data without changing the hash
 - Different data should not produce the same hash



Hash Function

- Hash functions are used more :
- **MD5 (128 bit)**
- **SHA-1 (160 bit)**
- **SHA-256/224 (256 o 224 bit)**
- **SHA-512/384 (512 o 384 bit)**
- **Tiger (192, 160 o 128 bit)**
- **Whirlpool (512 bit)**
- The acquisition tools (hardware or software) can calculate the hash of the original disk image and verify the copy process



Funzioni hash

- Connect the disk to scan on a write blocker, using the appropriate interface (IDA, SATA, SCSI)
- Connect the write blocker to the acquisition workstation, using an interface supported (USB, FireWire, eSATA)
- Connect a target disk to the computer (USB, Firewire, eSATA, Network)
- Start the acquisition program and create a disk image
- Calculate the hash of the hard disk original (MD5 and SHA1)
- Calculate the image hash (MD5 and SHA1)
- Compare hashes to verify the integrity of the copy



Acquisition with Tableau Disk Monitor



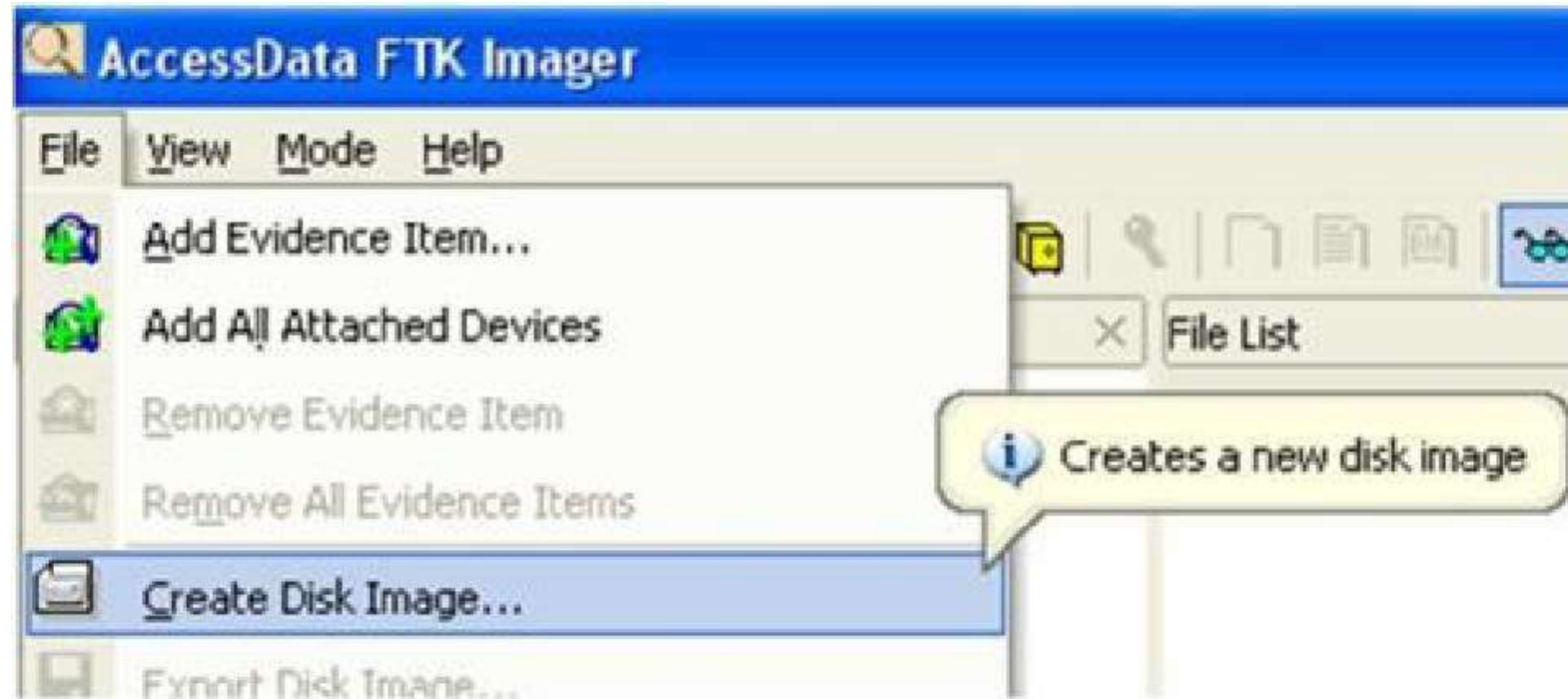
The screenshot shows the Tableau Disk Monitor application. The main window displays a table of disks, with Disk 2 selected. A secondary window, 'Disk 2 Details', provides a comprehensive list of properties for the selected disk.

| Disk ID | Disk Size | Disk Information | Forensic Bridge Information |
|---------|-----------|--|---------------------------------|
| 0 | 149 GB | SAMSUNG HM160HI (ATA) Serial #: 31535757444a533037313633301 | |
| 1 | 698 GB | WD My Passport D70A (USB) Serial #: (empty) | |
| 2 | 28 GB | QUANTUM FIREBALLci20.30 (IDE) Serial #: 353104964304 | Tableau T35es Read-Only Mode |

| Property | Value |
|------------------------------------|----------------------------|
| Disk Information (General) | |
| Vendor | (empty) |
| Model | QUANTUM FIREBALLci20.30 |
| Revision | APL0900 |
| Serial number | 353104964304 |
| Bus type | IDE |
| Device type | Direct Access |
| Removable media? | No |
| Sector size | 512 bytes |
| HPA in use? | No |
| DCO in use? | No |
| Security extensions in use? | No |
| Reported capacity | 28 GB (58.633.344 sectors) |
| HPA capacity | 28 GB (58.633.344 sectors) |
| DCO capacity | 28 GB (58.633.344 sectors) |
| Forensic Bridge Information | |
| Vendor | Tableau |
| Model | T35es |
| Description | (not available) |
| Serial number | 000ecc20 0035b214 |
| Bus type | USB |
| Bridge access mode | Read-Only |
| Read-only declaration | Declares Read-Only |
| Write error declaration | Declares Write Errors |

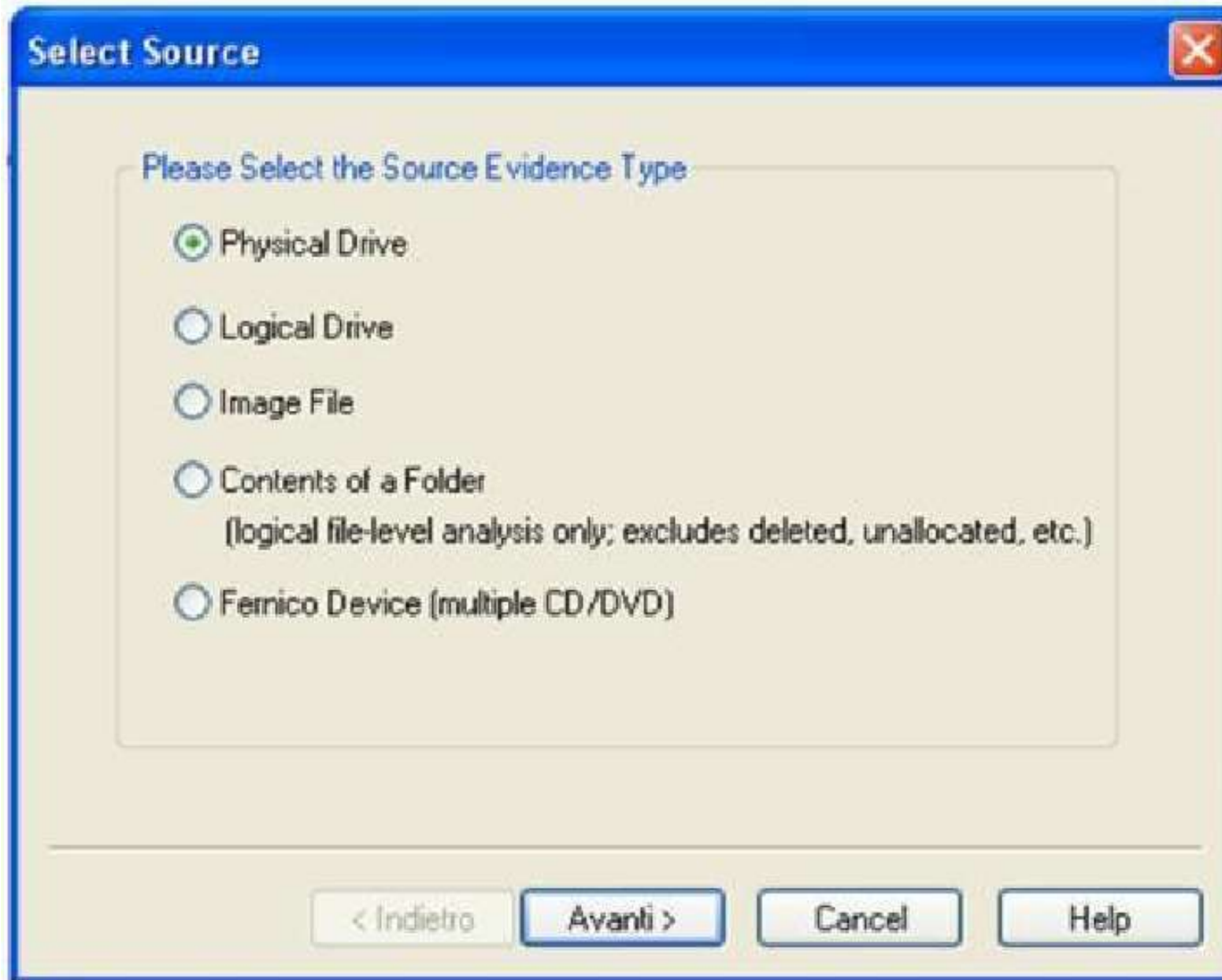


Acquisition with FTK Imager



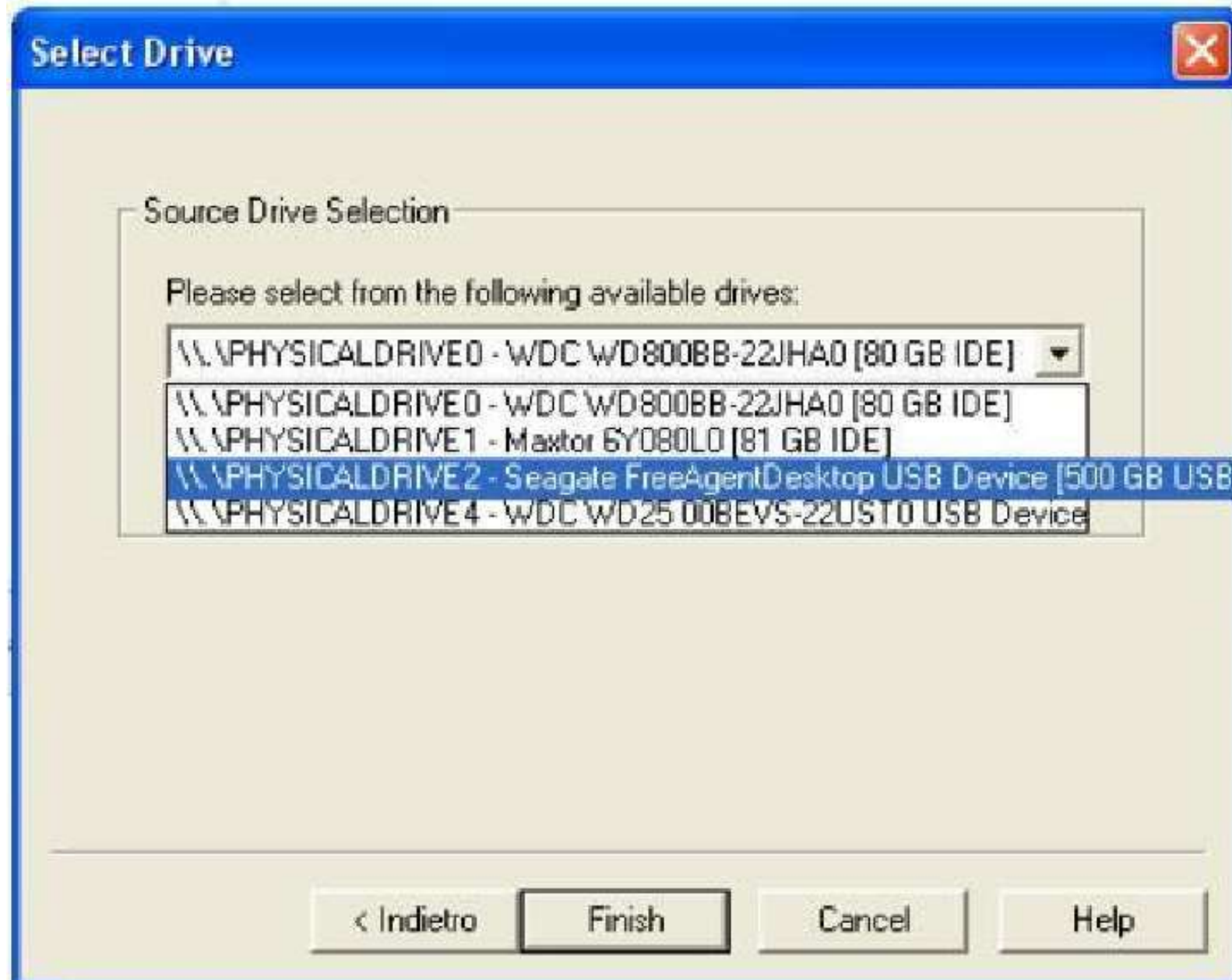


Acquisition with FTK Imager





Acquisition with FTK Imager





Acquisition with FTK Imager



Create Image [X]

Image Source
\\.\PHYSICALDRIVE2

Starting Evidence Number: 1

Image Destination(s)

Add... Edit... Remove

Verify images after they are created Precalculate Progress Statistics
 Create directory listings of all files in the image after they are created

Start Cancel



Acquisition with FTK Imager





Acquisition with FTK Imager



Create Image

Evidence Item Information

Case Number:

Evidence Number:

Unique Description:

Examiner: **Ing . Selene Giupponi**

Notes:

< Indietro Avanti > Cancel Help

Start Cancel



Acquisition with FTK Imager



Create Image

Select Image Destination

Image Destination Folder
I:\image_hdd

Image Filename (Excluding Extension)
image_hdd

Image Fragment Size (MB) 1500
For Raw and E01 formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 0

< Indietro



Acquisition with FTK Imager



Create Image

Image Source
\\.\PHYSICALDRIVE2

Starting Evidence Number: 1

Image Destination(s)
I:\image_hdd [raw/dd]

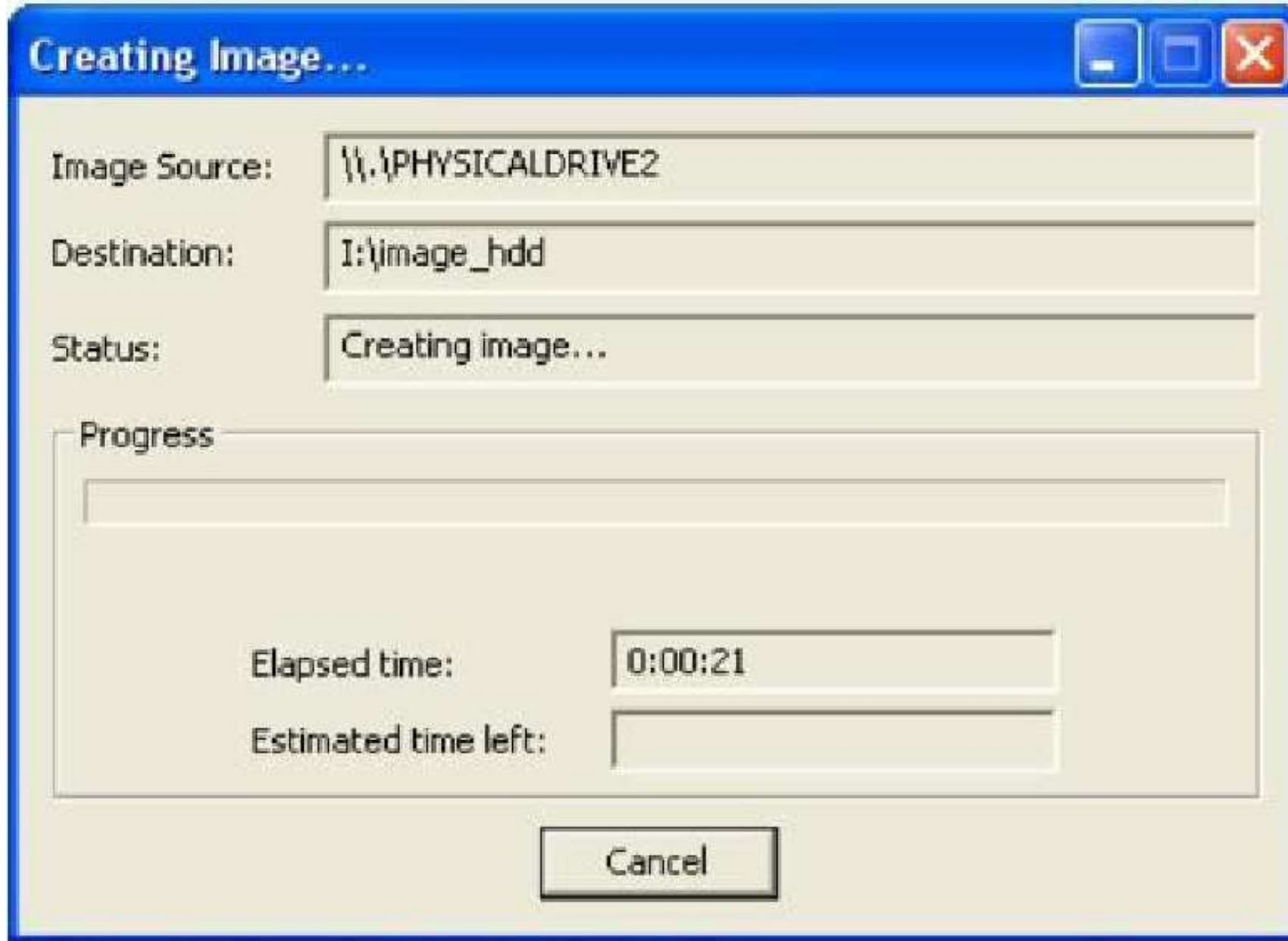
Add... Edit... Remove

Verify images after they are created Precalculate Progress Statistics
 Create directory listings of all files in the image after they are created

Start Cancel



Acquisition with FTK Imager





Acquisition with FTK Imager



Drive/Image Verify Results

| | |
|----------------------|--|
| General | |
| Name | compactflash-1.001 |
| Sector count | 15872 |
| MD5 Hash | |
| Computed hash | 09501e08071fcd63c6d52e23cbfe2c3d |
| Report Hash | 09501e08071fcd63c6d52e23cbfe2c3d |
| Verify result | Match |
| SHA1 Hash | |
| Computed hash | 66a2c1d40cc84366d0fca879c43f4e0b66c64bbb |
| Report Hash | 66a2c1d40cc84366d0fca879c43f4e0b66c64bbb |
| Verify result | Match |
| Bad Sector List | |
| No bad sectors found | |

Close



Operating steps

- Preparation and Identification
- Acquisition and Retention
- ***Analysis***
- Evaluation and presentation



Analysis

The evaluation mode differs depending on the type of case investigated.

This phase includes (non exhaustive list ...):

Identification of the logical structure of the disk partitions

Metadata of the file system

Activities of file carving

Extracting information about the operating system

Analysis of the main application software

Analysis of the file contents (visible, deleted and carving)

Generation of the timeline of computer use

Search by keywords



Analysis Tools

- For the analysis of files we can use different tools
- ***Forensic Toolkit***
- Software for analyze the logical structure of a disk
- Software data recovery / file carving
- Software for analysis (registry, user profile, Recycle Bin, Recent Files and links LNK, Event Log, Prefetch, Thumbnails, Print Spooler, Pagefile, Hiberfil)
- Software for the analysis of application software (Internet browsing, E-mail, chat, file sharing)
- Password cracking programs
- Virtualization systems
- Analyzers, network packets
- hexadecimal editor
- File viewer, video player and audio



Forensics Toolkit



Strong Opposition

opensource vs proprietor

Like in any other field of information technology the compromise is in the middle, or use open source as long as you can, but also proprietary tools to not ruin his life!



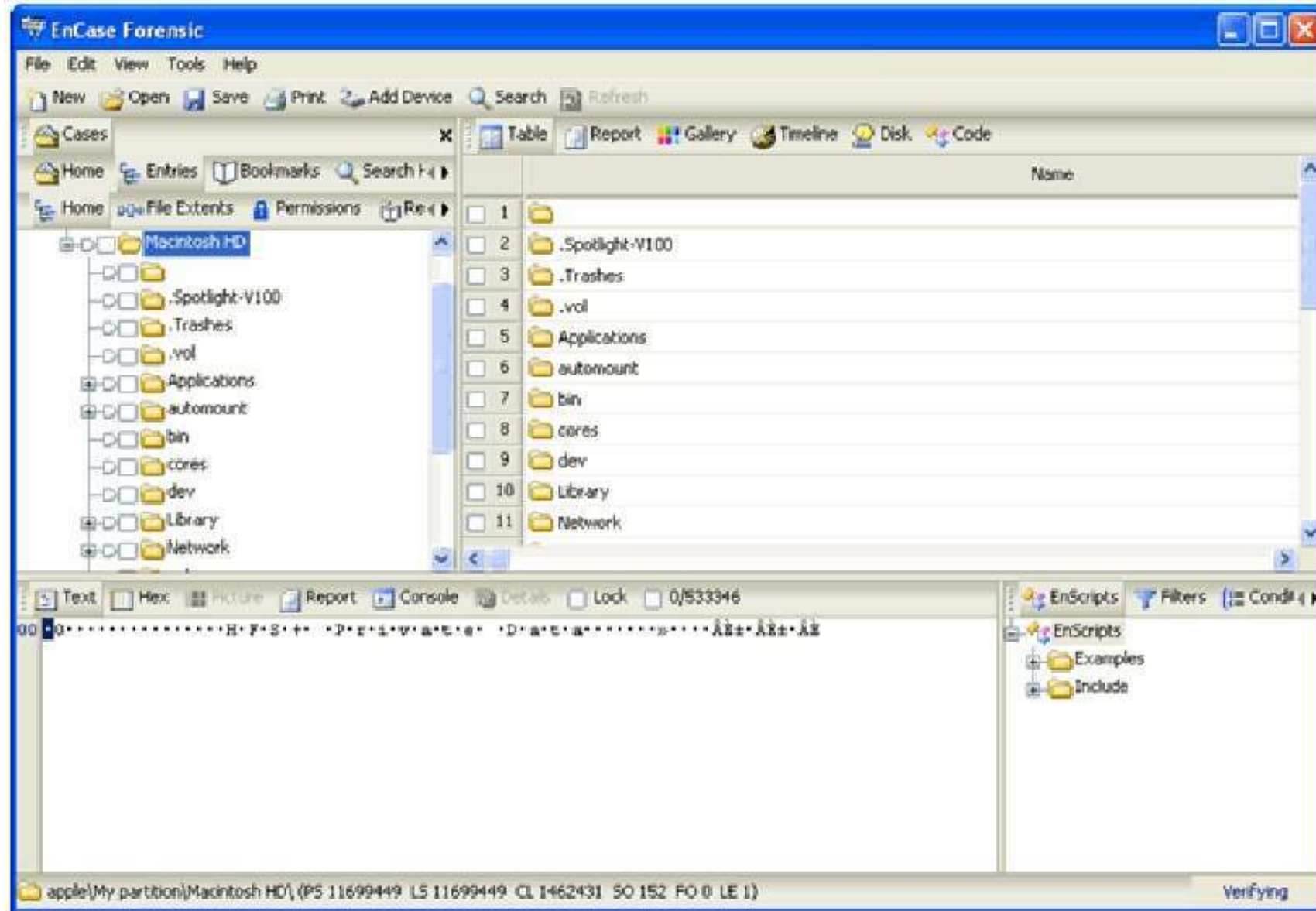
Commercial Forensic Toolkit

The most important commercial forensics toolkit are:

- **Encase** (Guidance Software)
- **Forensic Toolkit** (AccessData) - FTK
- **X-Ways Forensic** (X-Ways)
- **P2 Commander** (Paraben Corporation)
- **Pro Discover** (Technology Pathways)
- **Macintosh Forensic** (Blackbag)



Encase





FTK – Access Data



AccessData FTK, version 1.70.1 build 07.03.20 -- c:\waf\

File Edit View Tools Help

Overview Explorer Graphics E-Mail Search Bookmarks

| Evidence Items | | File Status | | File Category | |
|--------------------|--------------|--------------------|-----|------------------|-----|
| Evidence Items | 1 | OFF Alert Files | 0 | Documents | 0 |
| File Items | | Bookmarked Files | 0 | Spreadsheets | 0 |
| Total File Items | 1117 | Bad Extensions | 13 | Databases | 0 |
| Checked Items | 0 | Encrypted Files | 2 | Graphics | 7 |
| Unchecked Items | 1117 | From E-mail | 0 | Multimedia | 0 |
| Flagged Thumbnails | 0 | Corrupted Files | 278 | E-mail Messages | 0 |
| Other Thumbnails | 7 | From Recycle Bin | 0 | E-mail Attach | 110 |
| Filtered In | 1117 | Duplicate Items | 0 | Archives | 0 |
| Filtered Out | 0 | OLE Objects | 0 | Folders | 71 |
| Unfiltered | Filtered | Flagged Ignore | 0 | Stock/Free Space | 140 |
| All Items | Actual Files | NTFS Ignorable | 0 | Other Known Type | 21 |
| | | Data Corrupt Files | 0 | Unknown Type | 732 |

| | | | |
|-----------------------------|--|-----------------------|----------|
| 8 Bit | | | |
| 32 Bit Word | | | |
| Flowmap File Header | | | |
| Magic Number | | | |
| Version | | Reserved | |
| Flow Index Entry | | | |
| Client (Source) IP | | | |
| Server (Destination) IP | | | |
| IP Protocol | | Flags | Instance |
| Client Port/ICMP Type | | Server Port/ICMP Code | |
| Offset to First Data Stream | | | |

| File Name | Full Path | Recycle Bin | Ext | File Type | Category | Subst | Cr Date | Mod Date |
|-----------|------------------------------|-------------|-----|----------------|----------|-------|---------------------|---------------------|
| img1.png | G:\MSBDSKPRO\FAT16\img1.png | | png | PNG File (P... | Graphic | | 20/06/2007 19:45:22 | 20/06/2007 19:45:22 |
| img2.png | G:\MSBDSKPRO\FAT16\img2.png | | png | PNG File (P... | Graphic | | 20/06/2007 19:45:22 | 20/06/2007 19:45:22 |
| img3.png | G:\MSBDSKPRO\FAT16\img3.png | | png | PNG File (P... | Graphic | | N/A | 09/07/2006 21:00:00 |
| img4.png | G:\MSBDSKPRO\FAT16\img4.png | | png | PNG File (P... | Graphic | | 20/06/2007 19:45:22 | 20/06/2007 19:45:22 |
| img5.png | G:\MSBDSKPRO\FAT16\img5.png | | png | PNG File (P... | Graphic | | 20/06/2007 19:45:22 | 20/06/2007 19:45:22 |
| img6.png | G:\MSBDSKPRO\FAT16\img6.png | | png | PNG File (P... | Graphic | | 20/06/2007 19:45:22 | 20/06/2007 19:45:22 |
| img7.png | G:\MSBDSKPRO\FAT16\img7.png | | png | PNG File (P... | Graphic | | 20/06/2007 19:45:22 | 20/06/2007 19:45:22 |
| img8.png | G:\MSBDSKPRO\FAT16\img8.png | | png | PNG File (P... | Graphic | | 20/06/2007 19:45:22 | 20/06/2007 19:45:22 |
| img9.png | G:\MSBDSKPRO\FAT16\img9.png | | png | PNG File (P... | Graphic | | 20/06/2007 19:45:22 | 20/06/2007 19:45:22 |
| img10.png | G:\MSBDSKPRO\FAT16\img10.png | | png | PNG File (P... | Graphic | | 20/06/2007 19:45:22 | 20/06/2007 19:45:22 |

7 Listed 0 Checked Total G:\MSBDSKPRO-FAT16\img1.png





X-Ways Forensics



The screenshot displays the X-Ways Forensics application window. The main pane shows a file list for the NTFS image. A context menu is open over the file 'Tipped 1.jpg'. Below the file list, a gallery view shows thumbnails of various images, including a woman's face and a man's face.

| Nom de fichier | Ext | Chemin | Taille | Création | Modification | Accès | Atr | Ter cluster | ID | Commentaire |
|-------------------------|------|----------------|---------|---------------------|---------------|------------|-----|-------------|-----|--------------|
| 0.1020.299404.00[1].jpg | jpg | \Pictures\0003 | 2.1 Ko | 03.05.2004 17:17:56 | 05.04.2004... | 12.05.2005 | A | 25395 | 362 | |
| Private.jpg | jpg | \Pictures\0001 | 6.2 Ko | 03.05.2004 17:17:58 | 10.09.1997... | 12.05.2005 | A | 31337 | 511 | |
| 350de005.jpg | jpg | \Pictures\0003 | 7.1 Ko | 03.05.2004 17:17:56 | 03.05.2004... | 12.05.2005 | H | 25465 | 395 | |
| makeup4.jpg | jpg | \Pictures\0003 | 14.4 Ko | 03.05.2004 17:17:56 | 03.05.2004... | 13.05.2004 | A | 26491 | 403 | |
| necklace1.jpg | jpg | \Pictures\0003 | 14.6 Ko | 03.05.2004 17:17:56 | 03.05.2004... | 12.05.2005 | A | 25449 | 359 | ici vous |
| new-york-9400020.jpg | jpg | \Pictures\0003 | 18.6 Ko | 03.05.2004 17:17:56 | 24.03.2004... | 12.05.2005 | A | 26465 | 401 | pourriez |
| Nine Planets.jpeg | jpeg | \Pictures\0001 | 20.6 Ko | 03.05.2004 17:17:58 | 30.04.2004... | 12.05.2005 | A | 31032 | 501 | ajouter vos |
| jewelry.jpg | jpg | \Pictures\0003 | 20.7 Ko | 03.05.2004 17:17:56 | 03.05.2004... | 13.05.2004 | A | 25383 | 357 | commentar... |
| Neo & Trinity 1.jpg | jpg | \Pictures\0001 | 26.3 Ko | 03.05.2004 17:17:58 | 26.05.1999... | 17.05.2005 | A | 30966 | 499 | |
| Patrick Stewart 2.jpeg | jpeg | \Pictures\0001 | 27.2 Ko | 03.05.2004 17:17:58 | 24.02.1997... | 12.05.2005 | A | 31169 | 506 | |
| Tipped 3.jpg | jpg | \Pictures\0002 | 29.2 Ko | 03.05.2004 17:17:57 | 30.04.2004... | 13.01.2005 | A | 29261 | 457 | |
| Tipped 1.jpg | jpg | \Pictures\0002 | 29.3 Ko | 03.05.2004 17:17:57 | 30.04.2004... | 13.01.2005 | A | 29246 | 456 | |
| makeup3.jpg | jpg | \Pictures\0003 | 32.0 Ko | 03.05.2004 17:17:58 | 03.05.2004... | 13.05.2004 | A | 26475 | 402 | |
| Zhang Ziyi 40.jpg | jpg | \Pictures\0001 | 32.1 Ko | 03.05.2004 17:17:58 | 03.05.2004... | 13.05.2004 | A | 31479 | 517 | |
| sparpreis50.gif | gif | \Pictures\0003 | 34.2 Ko | 03.05.2004 17:17:58 | 03.05.2004... | 13.05.2004 | A | 26631 | 408 | |
| McCoy.jpeg | jpeg | \Pictures\0001 | 35.5 Ko | 03.05.2004 17:17:58 | 03.05.2004... | 13.05.2004 | A | 30787 | 494 | |
| Patrick Stewart 5.jpg | jpg | \Pictures\0001 | 35.5 Ko | 03.05.2004 17:17:58 | 03.05.2004... | 13.05.2004 | A | 31185 | 507 | |
| Spock 1.jpg | jpg | \Pictures\0001 | 35.9 Ko | 03.05.2004 17:17:58 | 03.05.2004... | 13.05.2004 | A | 31409 | 514 | |

Paraben P2 Commander

The screenshot displays the Paraben P2 Commander interface. The main window is titled "Paraben's P2 Commander - Test case p2c*". The interface is divided into several sections:

- Indexed Files:** A tree view on the left showing file types and their counts: Types (6159), Documents (40), Email (942), Chats (363), Spreadsheets (0), Graphics (2531), Databases (11), Executable (142), Compressed (35), Multimedia (13), Text (625), XML (90), and Others (3457).
- Search Panel:** A search configuration area with tabs for "Common", "Attributes", "Dates", and "Hash Database". The "Common" tab is active, showing "MD5 begins with" and "Filename" input fields. The "Type" is set to "Graphics".
- Search Results Table:** A table listing search results with columns for Name, Type, Size (bytes), and MD5. The selected row is "ICQ-321553738-120099" with a size of 12130 bytes and MD5 "5858FFD0D195F27054C8C456888E".
- Properties Panel:** A panel on the bottom left showing "Index Results" with MD5 and SHA1 hashes, "Misc" information, "Namespace" details, and "Size (bytes)" information.
- Thumbnails:** A panel on the bottom right displaying three image thumbnails: "didd2.gif", "BloggerBot.jpg", and "labybug.jpg".



ProDiscover



ProDiscover - Suspect Server

File Network Action View Tools Help

New Project Open Project Save Project Connect To... Capture Image Export Open Image Copy Disk Search Stop

Project - Suspect Server

- Report
- Add
 - Capture & Add Image
 - Image File
 - Disk
- Remove
- Content View
 - Images
 - Disks
 - Remote Drives
 - \\192.168.100.30\PhysicalDrive0
 - _hidden_
 - 3com
 - Documents and Settings
 - Inetpub
 - Program Files
 - RECYCLER
 - System Volume Information
 - Temp
 - WINNT
 - Deleted Files
- Cluster View
 - Images
 - Disks
 - Remote Drives
- View Log
- Search

| Select | File Name | File Extension | Size | Attributes | Deleted |
|--------------------------|----------------|----------------|----------------|------------|---------|
| <input type="checkbox"/> | \$Secure:\$SDS | | 274556 bytes | ---ADS--- | NO |
| <input type="checkbox"/> | \$UpCase | | 131072 bytes | ---META--- | NO |
| <input type="checkbox"/> | \$Volume | | 0 bytes | ---META--- | NO |
| <input type="checkbox"/> | arldr | .exe | 148992 bytes | ---a-s-h-r | NO |
| <input type="checkbox"/> | arcsetup | .exe | 162816 bytes | ---a-s-h-r | NO |
| <input type="checkbox"/> | AUTOEXEC | .BAT | 0 bytes | ----h- | NO |
| <input type="checkbox"/> | boot | .ini | 186 bytes | ----s-h- | NO |
| <input type="checkbox"/> | CONFIG | .SYS | 0 bytes | ----h- | NO |
| <input type="checkbox"/> | hiberfil | .sys | 133742592 b... | ---a-s-h- | NO |
| <input type="checkbox"/> | InstDriver | .exe | 3800 bytes | ---a--r | NO |
| <input type="checkbox"/> | ID | .SYS | 0 bytes | ---a-s-h-r | NO |
| <input type="checkbox"/> | MSDOS | .SYS | 0 bytes | ---a-s-h-r | NO |
| <input type="checkbox"/> | NTDETECT | .COM | 34468 bytes | ---a-s-h-r | NO |
| <input type="checkbox"/> | ntldr | | 214416 bytes | ---a-s-h-r | NO |
| <input type="checkbox"/> | pagefile | .sys | 201326592 b... | ---a-s-h- | NO |
| <input type="checkbox"/> | hidden | .sys | 3465 bytes | ---a--r | NO |

```
MZ_0 0 yy , @
I,0LIIThis program cannot be run in DOS mode.
$   ±0'E0'û~0'û~0'û~0"y~u"û~.i~ô"û~o.ô~o'û~Richo"û~
PE LDD 3%|> a 000000A0 @0 B0_0 ad 0 0 0
0 _0 _0 +g 0 0 0 0 T
a0 4 .text NO_0 `0 _0
h.rdata " a0 a0 @ H.data 0 _
@ EINIT X0 i a.reloc v
0 _ 0 @ Bsystem vwy$â00 <03ô_0>j0Ph_00 y$â00
fâ0.Au0%5_ 0 F__0 |U_ÂATf=_ 0 t*vysâ00 <0_ 0
<t$00Ej0QVysê00 fâ0_f0 j0X^e03Aâ0 U<i<M03AIT0IT0IT0fé tofé0tIU0<E0<
JAD IU<i<E0Ht0Ht0Ht0ife tofé0t0HU0<M0<E0%0JAD U<i<M03AIT;IT0IT%fé
to fé0t0IU.<E0fA^e0<E0fA^e0<E0fA^e0<E0fA^e0<E0fA^e0<E0fA^e0<E0fA^e0
U<i<M03AIT0IT0IT0fé to fé0t0IU0<E0<a<JAD <E0<â0ecrootkit:
```





Forensics Toolkit opensource

- The principal forensic toolkit opensource are :
- **The Sleuth Kit** (Brian Carrier)
- **Autopsy Forensic Browser**
- **Digital Forensics Framework**
- **OSForensics**
- **SIFT SANS**
- **Volatility Framework**
- **DEFT, CAINE, Paladin**



The Sleuth Kit



- It offers different modes of analysis
- File Listing: analysis of the files and folders, including deleted files
- File Content: content of the raw files, hexadecimal or ASCII
- Hash Databases: file search known through comparison of hash files to exclude "good". Uses the database of the National Software
- Reference Library (NSRL) NIST
- File Type Sorting: recognition and sorting files by type
- Timeline of File Activity, keyword search
- Metadata analysis
- Details of the acquired image



The Sleuth Kit – File Analysis



FILE ANALYSIS | KEYWORD SEARCH | FILE TYPE | IMAGE DETAILS | META DATA | DATA UNIT | HELP | CLOSE

| | | | | | | | | |
|-----|-----------------------------|------------------------------|------------------------------|------------------------------|-------|----|---|--|
| r/r | label.exe | 1996.10.14 01:38:00 (EDT) | 2002.06.13 17:08:40 (EDT) | 2002.06.13 17:08:45 (EDT) | 32016 | 48 | 0 | 182-128-4 |
| r/r | legacy.inf | 1996.10.14 01:38:00 (EDT) | 2002.06.13 17:08:40 (EDT) | 2002.06.13 17:08:40 (EDT) | 4654 | 48 | 0 | 183-128-4 |
| r/r | lights.exe | 1996.10.14 01:38:00 (EDT) | 2002.06.13 17:08:40 (EDT) | 2002.06.13 17:08:40 (EDT) | 35600 | 48 | 0 | 184-128-4 |
| r/- | LMREPL.EXE | 0000.00.00 00:00:00 (GMT) | 0000.00.00 00:00:00 (GMT) | 0000.00.00 00:00:00 (GMT) | 0 | 0 | 0 | 185-128-4 |
| r/r | LMREPL.EXE | 1996.10.14 01:38:00 (EDT) | 2002.06.13 17:08:40 (EDT) | 2002.06.13 17:08:45 (EDT) | 86800 | 48 | 0 | 185-128-4 |
| r/r | loadfix.com | 1996.10.14 01:38:00 (EDT) | 2002.06.13 17:08:40 (EDT) | 2002.06.13 17:08:40 (EDT) | 1131 | 48 | 0 | 186-128-4 (realloc) |
| r/r | loadfix.com | 1996.10.14 01:38:00 (EDT) | 2002.06.13 17:08:40 (EDT) | 2002.06.13 17:08:40 (EDT) | 1131 | 48 | 0 | 186-128-4 |

ASCII (display - report) * Strings (display - report) * Export * Add Note
File Type: MS Windows PE 32-bit Intel 80386 GUI executable

String Contents Of File: E:\system32/inetins.exe

```
!This program cannot be run in DOS mode.
.text
.rdata
.data
.rsrc
.reloc
MSVCRT.dll
KERNEL32.dll
USER32.dll
0SVW
```



The Sleuth Kit – File Content



This file is currently being viewed in a **sanitized environment**
HTML files have been edited to disable scripts and links. Pictures have been replaced by place holders

NORMAL **EXPORT CONTENTS**

As an owner of **Red Hat Linux 6.2** you are entitled to all of these benefits:

- Priority Online Access**
No more late-night visits to congested mirror sites! As a Red Hat Linux 6.2 owner, you will receive free access to priority.redhat.com, our preferred customer update service, offering high bandwidth connections day and night. Priority Online Access is the most advanced system available to update your Linux system.

If you are already registered or would simply like to browse redhat.com, use the following links:

- Read the Installation and Getting Starting Guides:**
www.redhat.com/manual
- Search and browse our mailing list archives:**
www.redhat.com/mailling-lists
- Access our online support**



The Sleuth Kit – Hash Database



NSRL Lookup

a3e1a9ba1345f76c69a1e97f9d8b8f43 lmrepl.exe
a3e1a9ba1345f76c69a1e97f9d8b8f43 lmrepl.exe

Exclude Database Lookup

a3e1a9ba1345f76c69a1e97f9d8b8f43 Hash Not Found

Alert Database Lookup

a3e1a9ba1345f76c69a1e97f9d8b8f43 Hash Not Found



The Sleuth Kit - File Type Sorting



The screenshot shows the 'File Type Sortings' dialog box in the Sleuth Kit application. The dialog has a title bar with buttons for 'FILE ANALYSIS', 'DATA UNIT', 'META DATA', 'IMAGE DETAILS', 'KEYWORD SEARCH', 'FILE TYPE', 'HELP', and 'CLOSE'. The 'FILE TYPE' button is active. The main content area contains the following text and options:

Sort Files by Type

File Type Sortings

The **sorter** tool will process an image and organize the files based on their file type. The files are organized into categories that are defined in configuration files. The categories will be saved in the **output** directory.

- Sort files into categories by type
 - Do not save data about unknown file types
 - Save a copy of files in category directory (may require lots of disk space)
- Extension and File Type Validation
- Exclude files in the **NIST NSRL**
- Alert files that are found in the **Alert Hash Database**
- Ignore files that are found in the **Exclude Hash Database**

OK



The Sleuth Kit - Timeline



| CREATE DATA FILE CREATE TIMELINE VIEW TIMELINE VIEW NOTES HELP CLOSE | | | | | | |
|---|-------|-----|--------------|------|-----------|---|
| <- May 2002 Jul 2002 -> | | | | | | |
| Jun 2002 OK | | | | | | |
| Mon Jun 10 2002 19:33:10 | 3888 | m.. | -/-rwxrwxrwx | 48 0 | 112-128-4 | C:/system32/drivers/NTHANDLE.SYS |
| Thu Jun 13 2002 21:01:34 | 22299 | .ac | -/-rwxrwxrwx | 48 0 | 263-128-4 | C:/system32/oemnadem.inf |
| Thu Jun 13 2002 21:01:35 | 20263 | .ac | -/-rwxrwxrwx | 48 0 | 270-128-4 | C:/system32/oemnadlm.inf |
| | 39386 | .c | -/-rwxrwxrwx | 48 0 | 193-128-4 | C:/system32/mem.exe |
| | 56 | mac | d/drwxrwxrwx | 48 0 | 49-144-7 | C:/system32 |
| | 9488 | .c | -/-rwxrwxrwx | 48 0 | 191-128-4 | C:/system32/lsass.exe |
| | 9488 | .c | -/-rwxrwxrwx | 48 0 | 191-128-4 | C:/system32/lsass.exe (deleted-realloc) |
| | 33662 | .ac | -/-rwxrwxrwx | 48 0 | 268-128-4 | C:/system32/oemnadin.inf |
| | 86800 | .c | -/-rwxrwxrwx | 48 0 | 185-128-4 | C:/system32/LMREPL.EXE |
| | 25491 | .ac | -/-rwxrwxrwx | 48 0 | 269-128-4 | C:/system32/oemnadlb.inf |
| | 24391 | .ac | -/-rwxrwxrwx | 48 0 | 264-128-4 | C:/system32/oemnaden.inf |
| | 22297 | .ac | -/-rwxrwxrwx | 48 0 | 266-128-4 | C:/system32/oemnadfd.inf |
| | 85632 | .c | -/-rwxrwxrwx | 48 0 | 179-128-4 | C:/system32/kml386.exe |
| | 22296 | .ac | -/-rwxrwxrwx | 48 0 | 267-128-4 | C:/system32/oemnadim.inf |
| | 32016 | .c | -/-rwxrwxrwx | 48 0 | 182-128-4 | C:/system32/label.exe |
| | 35225 | .ac | -/-rwxrwxrwx | 48 0 | 265-128-4 | C:/system32/oemnadep.inf |



The Sleuth Kit – Key word search



FILE ANALYSIS DATA UNIT META DATA IMAGE DETAILS **KEYWORD SEARCH** FILE TYPE HELP CLOSE

← PREVIOUS NEXT →
EXPORT CONTENTS ADD NOTE

ASCII ([display](#) - [report](#)) * Hex ([display](#) - [report](#)) * Strings ([display](#) - [report](#))
File Type: data

Fragment 126615
Allocated
Group: 15
Pointed to by Inode: [30184](#)
Pointed to by file:
/bin/mt

Hex Contents of Fragment 126615 (1024 bytes) in images/dev_hde8.img

| | | | | | |
|-----|----------|----------|----------|----------|---------------------|
| 0 | 25733a20 | 57726974 | 696e6720 | 6d6f6465 | %s: Writing mode |
| 16 | 20534353 | 49206d6f | 64652070 | 61676520 | SCS I mode page |
| 32 | 6661696c | 65642e0a | 00000000 | 00000000 | failed.. |
| 48 | 00000000 | 00000000 | 00000000 | 00000000 | |
| 64 | 25733a20 | 436f6d70 | 72657373 | 696f6e20 | %s: Compression |
| 80 | 6d6f6465 | 206e6f74 | 20636861 | 6e676564 | mode not changed |
| 96 | 2e0a0000 | 00000000 | 00000000 | 00000000 | |
| 112 | 00000000 | 00000000 | 00000000 | 00000000 | |
| 128 | 25733a20 | 52652d72 | 65616420 | 6f662074 | %s: Re-read of t |
| 144 | 68652063 | 6f6d7072 | 65737369 | 6f6e2070 | he c ompressi on p |
| 160 | 61676520 | 6661696c | 65642e0a | 00436f6d | age failed.. .Com |
| 176 | 70726573 | 73696f6e | 206f6e2e | 0a00436f | pression on. ..Co |
| 192 | 6d707265 | 7373696f | 6e206f66 | 662e0a00 | mpre ssio n of f... |
| 208 | 00000000 | 00000000 | 00000000 | 00000000 | |
| 224 | 00000000 | 64ba0408 | 00000000 | 00000000 | d... |
| 240 | 00000000 | 00000000 | 00000000 | 00000000 | |
| 256 | 2449643a | 202f7573 | 72322f75 | 73657273 | \$Id: /us r2/u sers |
| 272 | 2f6d616b | 69736172 | 612f7372 | 632f7379 | /mak isar a/sr c/sy |
| 288 | 732f6d74 | 2d73742d | 302e3562 | 2f6d742e | s/mt -st- 0.5b /mt. |
| 304 | 63206174 | 2053756e | 20417567 | 20313620 | c at Sun Aug 16 |
| 320 | 30393a35 | 313a3137 | 20313939 | 38206279 | 09:5 1:17 199 8 by |
| 336 | 206d616b | 69736172 | 61406b61 | 692e6d61 | mak isar a0ka i.ma |



The Sleuth Kit – Metadata Analysis



FILE ANALYSIS DATA UNIT META DATA IMAGE DETAILS KEYWORD SEARCH FILE TYPE HELP CLOSE

MFT Entry Number: 182-128-4

Alert Database OK

OK

ALLOCATION LIST

Details:
 MFT Entry: 182
 Sequence: 1
 Allocated
 UID: 48
 DOS Mode: File
 Size: 32016
 Links: 1
 Name: label.exe

SSTANDARD_INFORMATION Times:
 Created: Thu Jun 13 21:08:40 2002
 File Modified: Mon Oct 14 05:38:00 1996
 MFT Modified: Thu Jun 13 21:08:45 2002
 Accessed: Thu Jun 13 21:08:40 2002

SFILE_NAME Times:
 Created: Thu Jun 13 21:08:40 2002
 File Modified: Thu Jun 13 21:08:40 2002
 MFT Modified: Thu Jun 13 21:08:40 2002
 Accessed: Thu Jun 13 21:08:40 2002

Attributes:
 Type: SSTANDARD_INFORMATION (16-0) Name: N/A Resident size: 48
 Type: SFILE_NAME (48-2) Name: N/A Resident size: 84
 Type: SSEURITY_DESCRIPTOR (80-3) Name: N/A Resident size: 92
 Type: \$DATA (128-4) Name: \$Data Non-Resident size: 32016
[77378](#) [77379](#) [77380](#) [77381](#) [77382](#) [77383](#) [77384](#) [77385](#)
[77386](#) [77387](#) [77388](#) [77389](#) [77390](#) [77391](#) [77392](#) [77393](#)
[77394](#) [77395](#) [77396](#) [77397](#) [77398](#) [77399](#) [77400](#) [77401](#)



The Sleuth Kit – Image Details



The screenshot shows the 'IMAGE DETAILS' tab of The Sleuth Kit. The interface includes a menu bar with options: FILE ANALYSIS, DATA UNIT, META DATA, IMAGE DETAILS (selected), KEYWORD SEARCH, FILE TYPE, HELP, and CLOSE. The main content area displays the following information:

Volume ID: 291050747
Volume Label: NO NAME
File System Type (super block): FAT12

META-DATA INFORMATION

Range: 2 - 45762
Root Directory: 2

CONTENT-DATA INFORMATION

Sector Size: 512
Cluster Size: 512
Sector of First Cluster: 33
Total Sector Range: 0 - 2878
FAT 0 Range: 1 - 9
FAT 1 Range: 10 - 18
Data Area Sector Range: 19 - 2878

FAT CONTENTS (in sectors)

[33-98 \(66\)](#) -> EOF
[99-172 \(74\)](#) -> EOF
[173-266 \(94\)](#) -> EOF
[267-267 \(1\)](#) -> EOF
[268-270 \(3\)](#) -> EOF
[271-446 \(176\)](#) -> EOF
[447-494 \(48\)](#) -> EOF
[495-506 \(12\)](#) -> EOF
[507-571 \(65\)](#) -> EOF
[572-572 \(1\)](#) -> EOF
[573-573 \(1\)](#) -> EOF
[574-574 \(1\)](#) -> EOF



Mount image DD



- There are different software that allow you to "mount" an image in RAW / DD and use it in the operating system as a local disk read-only
The main tools are:
 - **AccessData FTK Imager** (freeware)
 - **P2Explorer** (freeware)
 - **IMDisk** (freeware)



Mount image DD – P2 Explorer



The screenshot shows the Paraben's P2 Explorer application window. The 'Mounted Disks' table is as follows:

| Mount Point | Source Type | Physical Disk | Plug-in Name | Total Space | Free Space | Used Space | Description |
|-------------|-------------|--------------------|--------------|-------------|-------------|-------------|--------------|
| A: | Free | | | | | | |
| B: | Free | | | | | | |
| C: | Local | \\.\PhysicalDrive0 | | 76,282,974 | 51,828,027 | 24,454,946 | |
| D: | Local | \\.\PhysicalDrive0 | | 77,308,358 | 21,225,422 | 56,082,935 | |
| E: | CDROM | | | 597,510,144 | 0 | 597,510,144 | |
| F: | Plugin | \\.\PhysicalDrive2 | RAW | | | | I:\mattia.dd |
| G: | CDROM | | | | | | |
| H: | Free | | | | | | |
| I: | Local | \\.\PhysicalDrive1 | | 749,452,881 | 340,730,003 | 408,722,878 | |
| J: | Free | | | | | | |
| K: | Free | | | | | | |
| L: | Free | | | | | | |
| M: | Free | | | | | | |
| N: | Free | | | | | | |
| O: | Free | | | | | | |
| P: | Free | | | | | | |
| Q: | Free | | | | | | |
| R: | Free | | | | | | |
| S: | Free | | | | | | |
| T: | Free | | | | | | |
| U: | Free | | | | | | |
| V: | Free | | | | | | |
| W: | Free | | | | | | |
| X: | Free | | | | | | |
| Y: | Free | | | | | | |

The right side of the window features a promotional banner for 'Paraben's Device Seizure' with the text 'THE ONLY COMPLETE SOLUTION' and an image of the software box.



Analysis of metadata from filesystem



Analysis of the file containing the metadata of file systems allows you to extract information of interest and are the basis for understanding the partitioning and the timeline of a system

Examples of metadata are:

- **File Allocation Table (FAT16/FAT32)**
- **Master File Table (NTFS)**
- **Catalog File (HFS+)**



File Allocation Table (FAT)

- In a FAT file system metadata associated with a file / folder are:
- Name of the file or folder
- Date and time of file creation
- Date and time of last modification
- Date of last access
- Starting cluster of the file
- Filesize



Master File Table (MFT) - NTFS

- In an NTFS filesystem metadata associated with a file / folder are:
- Name of the file or folder
- Date and time of file creation
- Date and time of last modification
- Date and time of last access
- Date and time of last modification of the entry in the MFT
- Filesize
- Another useful item is the UsrJournal

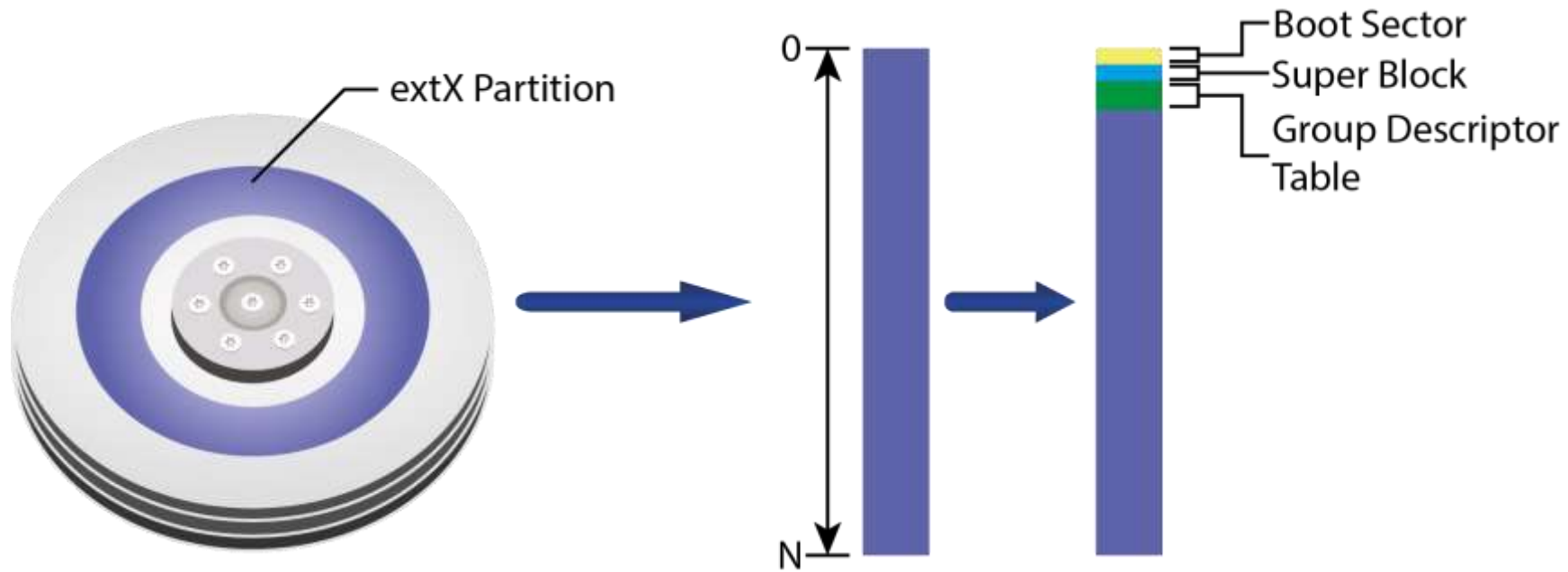


Analyzing metadata from file systems - Tools

- **MMLS** – shows volume partitions
- **MFT Ripper** (commercial)
- **AnalyzeMFT.py** (opensource)
- **MFTView** (freeware)
- **NTFSWalk** (freeware)
- **Windows Journal Parser** (freeware)



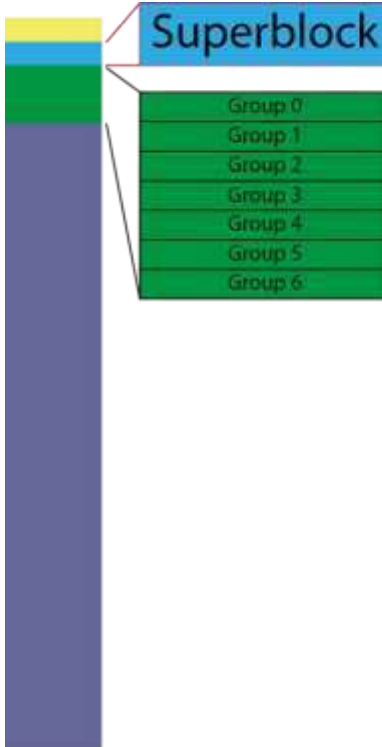
File System



Credits By George



File System

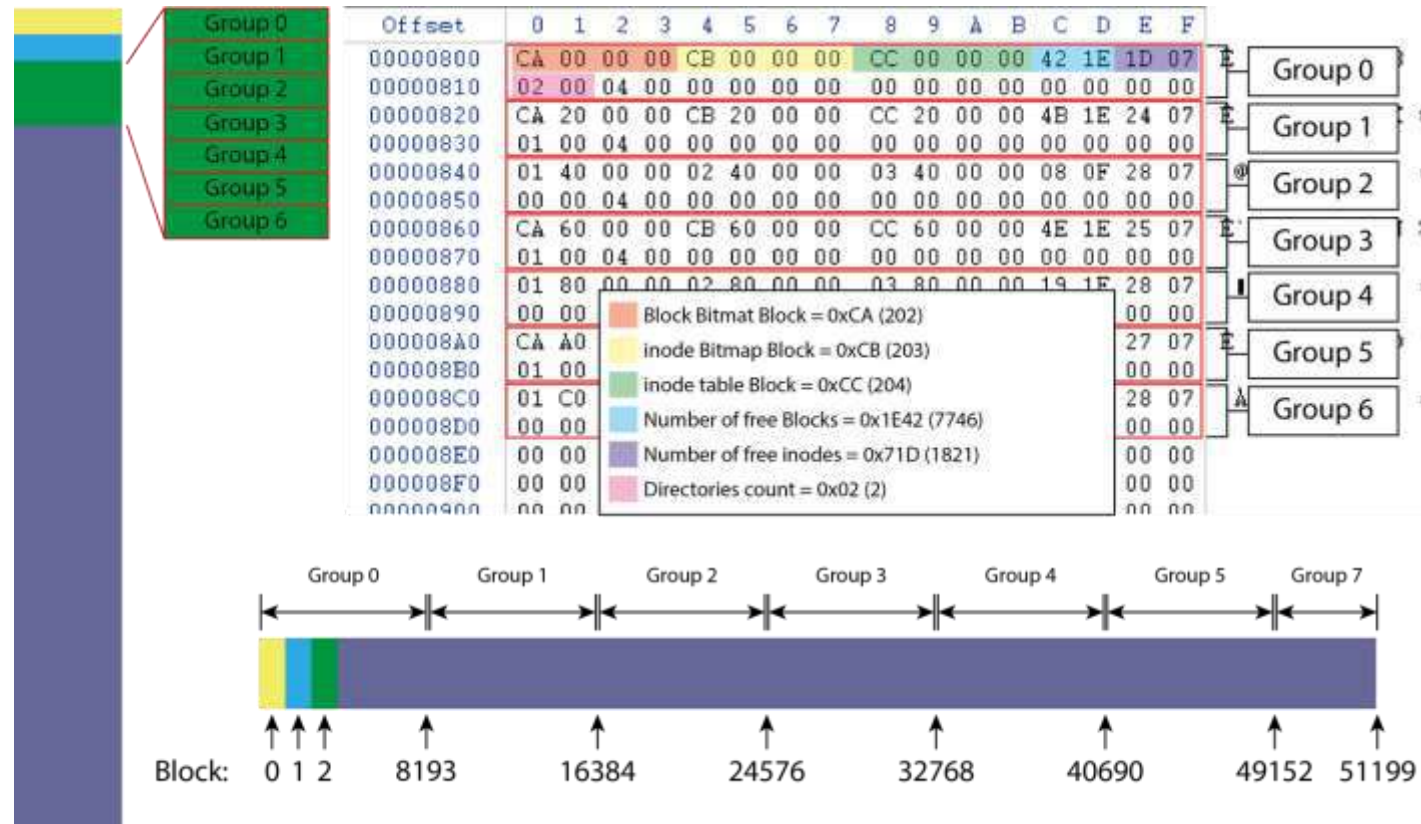
| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-------|---------------|
| 00000400 | 18 | 32 | 00 | 00 | 00 | C8 | 00 | 00 | 00 | 0A | 00 | 00 | 63 | AE | 00 | 00 | 2 E c@ |
| 00000410 | 05 | 32 | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 2 |
| 00000420 | 00 | 20 | 00 | 00 | 00 | 20 | 00 | 00 | 28 | 07 | 00 | 00 | 07 | 23 | 3D | 53 | (#=S |
| 00000430 | 52 | 23 | 3D | 53 | 01 | 00 | FF | FF | 53 | EF | 01 | 00 | 01 | 00 | 00 | 00 | R#=S yySi |
| 00000440 | F7 | 22 | 3D | 53 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | -"=S |
| 00000450 | 00 | 00 | 00 | 00 | 0B | 00 | 00 | 00 | 80 | 00 | 00 | 00 | 3C | 00 | 00 | 00 | I < |
| 00000460 | 02 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 59 | 9B | 32 | E2 | A0 | 39 | 47 | 9C | Y 2â 9G |
| 00000470 | A5 | FC | 9C | 91 | 55 | 85 | 24 | 27 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | Yü 'U s' |
| 00000480 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 2F | 6D | 6E | 74 | 00 | 00 | 00 | 00 | /mnt |
| 00000490 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000004A0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000004B0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000004C0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | C7 | Ç |
| 000004D0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000004E0 | 08 | 00 | | | | | | | | | | | | | | 99 82 | {c |
| 000004F0 | E3 | C2 | | | | | | | | | | | | | | 00 00 | 3AEj [I<<5q i |
| 00000500 | 0C | 00 | | | | | | | | | | | | | | 00 00 | -"=S@ |
| 00000510 | E9 | 40 | | | | | | | | | | | | | | 00 00 | @ @ @ i@ |
| 00000520 | ED | 40 | | | | | | | | | | | | | | 00 00 | i@ i@ i@ 8@ |
| 00000530 | F1 | 40 | | | | | | | | | | | | | | 00 00 | 8@ 0@ 0@ 0@ |
| 00000540 | F5 | 41 | | | | | | | | | | | | | | 40 00 | 0A @ |
| 00000550 | 00 | 00 | | | | | | | | | | | | | | 00 00 | |
| 00000560 | 01 | 00 | | | | | | | | | | | | | | 00 00 | |
| 00000570 | 00 | 00 | | | | | | | | | | | | | | 00 00 | |
| 00000580 | 00 | 00 | | | | | | | | | | | | | | 00 00 | |
| 00000590 | 00 | 00 | | | | | | | | | | | | | | 00 00 | |
| 000005A0 | 00 | 00 | | | | | | | | | | | | | | 00 00 | |
| 000005B0 | 00 | 00 | | | | | | | | | | | | | | 00 00 | |
| 000005C0 | 00 | 00 | | | | | | | | | | | | | | 00 00 | |
| 000005D0 | 00 | 00 | | | | | | | | | | | | | | 00 00 | |
| 000005E0 | 00 | 00 | | | | | | | | | | | | | | 00 00 | |
| 000005F0 | 00 | 00 | | | | | | | | | | | | | | 00 00 | |

- Number of inodes = 0x3218 (12824)
- Number of Blocks = 0xC800 (51200)
- Number of Free Blocks = 0xAE63 (44643)
- Number of free inodes = 0x3205 (12805)
- First data block = 0x01 (1)
- Block Size (bits to shift 1024) = 0x00
- Cluster Size (bits to shift 1024) = 0x00
- Blocks per group = 0x2000 (8192)
- inodes per group = 0x728 (1832)
- inode size = 0x80 (128)
- Last mount location = "/mnt"

Credits By George



File System



Credits By George



File System



| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 00033000 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | F7 | 22 | 3D | 53 | F7 | 22 | 3D | 53 |
| 00033010 | F7 | 22 | 3D | 53 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00033020 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00033030 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00033040 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00033050 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00033060 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00033070 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00033080 | ED | 41 | 00 | 00 | 00 | 04 | 00 | 00 | 1F | 23 | 3D | 53 | 1D | 23 | 3D | 53 |
| 00033090 | 1D | 23 | 3D | 53 | 00 | 00 | 00 | 00 | 00 | 00 | 06 | 00 | 02 | 00 | 00 | 00 |
| 000330A0 | 00 | 00 | 00 | 00 | 03 | 00 | 00 | 00 | B1 | 01 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000330B0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000330C0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000330D0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000330E0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000330F0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00033100 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |

- Mode = 0x41ED (Directory, rwxr-xr-x)
- User ID = 0 (root)
- File Size = 1024 bytes
- Access time = 0x533D231F (09:00:15 03/04/2014)
- Creation time = 0x533D31D (09:00:13 03/04/2014)
- Modification Time = 0x533D31D
- Group ID = 0 (root)
- Blocks = [0x01B1 (433), 0, 0, ..., 0]

Credits By George



File System



| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0006C400 | 02 | 00 | 00 | 00 | 0C | 00 | 01 | 02 | 2E | 00 | 00 | 00 | 02 | 00 | 00 | 00 |
| 0006C410 | 0C | 00 | 02 | 02 | 2E | 2E | 00 | 00 | 0B | 00 | 00 | 00 | 14 | 00 | 0A | 02 |
| 0006C420 | 6C | 6F | 73 | 74 | 2B | 66 | 6F | 75 | 6E | 64 | 00 | 00 | 29 | 07 | 00 | 00 |
| 0006C430 | 0C | 00 | 04 | 02 | 64 | 69 | 72 | 31 | 79 | 15 | 00 | 00 | 0C | 00 | 04 | 02 |
| 0006C440 | 64 | 69 | 72 | 32 | C9 | 23 | 00 | 00 | BC | 03 | 04 | 02 | 64 | 69 | 72 | 33 |
| 0006C450 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0006C460 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0006C470 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 0006C480 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |

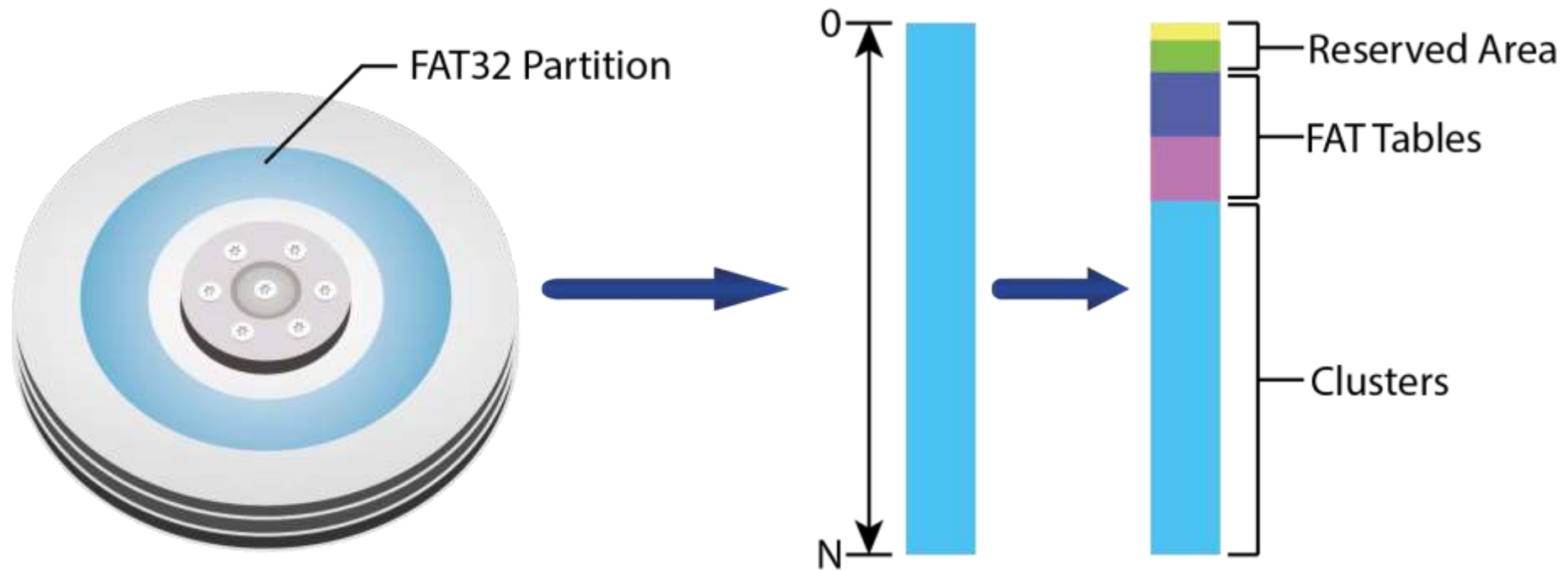
| |
|---------------|
| lost+found) |
| dirly |
| dir2É# % dir3 |

| Entry No 1 | Entry No 6 |
|------------------------------|------------------------------|
| inode = 0x02 (2) | inode = 0x23C9 (9161) |
| Record Length = 0x0C (12) | Record Length = 0x3BC (956) |
| Name Length = 0x01 (1) | Name Length = 0x04 (4) |
| File Type = 0x02 (Directory) | File Type = 0x02 (Directory) |
| File Name = . | File Name = "dir3" |
| Padding | Padding |

Credits By George



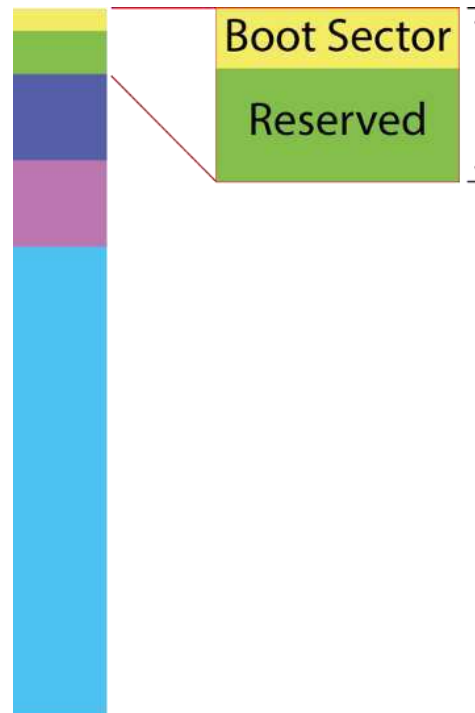
File System



Credits By George



File System

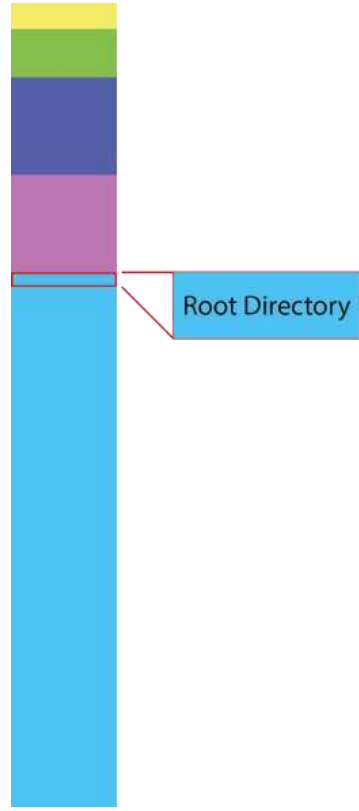



| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | |
|----------|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|
| 00000000 | EB | 58 | 90 | 61 | 6E | 64 | 72 | 6F | 69 | 64 | 20 | 00 | 02 | 40 | BC | 08 | èX android @% |
| 00000010 | 02 | 00 | 00 | 00 | 00 | F0 | 00 | 00 | 10 | 00 | 04 | 00 | 00 | 00 | 00 | 00 | è |
| 00000020 | 00 | 40 | 70 | 01 | 82 | 0B | 00 | 00 | 00 | 00 | 00 | 00 | 02 | 00 | 00 | 00 | @p |
| 00000030 | 01 | 00 | 02 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |)è / NO NAME |
| 00000040 | 00 | 01 | 29 | F0 | 09 | 2F | 04 | 4E | 4F | 20 | 4E | 41 | 4D | 45 | 20 | 20 | FAT32 úlÀ Dw |
| 00000050 | 20 | 20 | 46 | 41 | 54 | 33 | 32 | 20 | 20 | 20 | FA | 31 | C0 | 8E | D0 | BC | ú @è ^ È » ü |
| 00000060 | 00 | 7C | FB | 8E | D8 | E8 | 00 | 00 | 5E | 83 | C6 | 19 | BB | 07 | 00 | FC | ~ Àt ' í èè0af í |
| 00000070 | AC | 84 | C0 | 74 | 06 | B4 | 0E | CD | 10 | EB | F5 | 30 | E4 | CD | 16 | CD | Non-system di |
| 00000080 | 19 | 0D | 0A | 4E | 6F | 6E | 2D | 73 | 79 | 73 | 74 | 65 | 6D | 20 | 64 | 69 | sk Press any ke |
| 00000090 | 73 | 6B | 0D | 0A | 50 | 72 | 65 | 73 | 73 | 20 | 61 | 6E | 79 | 20 | 6B | 65 | y to reboot. |
| 000000A0 | 79 | 20 | 74 | 6F | 20 | 72 | 65 | 62 | 6F | 6F | 74 | 0D | 0A | 00 | 00 | 00 | |
| 000000B0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000000C0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000000D0 | <ul style="list-style-type: none"> OEM Name = "android " (contains space) Bytes Per Sector = 0x0200 = 512 Sectors Per Cluster = 0x40 = 64 Reserved Sectors = 0x08BC = 2236 Number of FAT Tables = 0x02 = 2 Sectors Per FAT = 0x0B82 = 2946 Root Directory Cluster = 0x02 = 2 Volume Serial Number = 0x042F09F0 = 70191600 | | | | | | | | | | | | | | | | |
| 000000E0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000000F0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000100 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000110 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000120 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000130 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000140 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000150 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000160 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000170 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000180 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000190 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000001A0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000001B0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000001C0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000001D0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000001E0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000001F0 | 2F | 3E | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 55 | AA | /> Uè |

Credits By George



File System



| | | |
|-----------|---|---------------|
| 0003F8000 | 4C 4F 53 54 20 20 20 20 44 49 52 10 00 00 44 B2 | LOST DIR D² |
| 0003F8010 | 9F 3D 4A 44 00 00 44 B2 9F 3D 04 00 00 00 00 00 | !-JD D²!- |
| 0003F8020 | 41 65 00 78 00 74 00 65 00 72 00 0F 00 3C 6E 00 | Ae x t e r <n |
| 0003F8030 | 61 00 6C 00 5F 00 73 00 64 00 00 00 00 00 FF FF | a l _ s d yy |
| 0003F8040 | 45 58 54 45 52 4E 7E 31 20 20 20 10 00 00 5D BC | EXTERN~1]% |
| 0003F8050 | 9F 3E 0C 2E 00 00 5D BC 0C 2E 05 00 00 00 00 00 | !?!?]%!? |
| 0003F8060 | 4 | Au s b S t äo |
| 0003F8070 | 7 | r a g e yyyy |
| 0003F8080 | 5 | USBSTO~1 µ |
| 0003F8090 | 3 | 9?9? µ 9? |
| 0003F80A0 | 4 | DCIM d |
| 0003F80B0 | C | Ä@rD Ä@ |
| 0003F80C0 | 41 41 00 6E 00 64 00 72 00 6F 00 0F 00 66 69 00 | ÄÄ n d r o fi |
| 0003F80D0 | 64 00 00 00 FF FF FF FF FF FF 00 00 FF FF FF FF | d yyyyyy yyy |
| 0003F80E0 | 41 4E 44 52 4F 49 44 20 20 20 20 10 00 64 67 B5 | ANDROID dgj |
| 0003F80F0 | DC 42 41 41 00 00 63 BF DC 42 00 00 00 00 00 00 | UNID 4:4D |

█ Directory/File Name (11 bytes) = LOST DIR (LOSTDIR)
█ Entry Attributes (1 byte) = 0x10 (ATTR_DIRECTORY)
█ First Cluster (High value) (2 bytes)
█ First Cluster (Low Value) (2 bytes) — Combined = 0x00000004
█ Entry/File Size (4 bytes) = 0x00000000

— Directory Entry (32 Bytes long)

Credits By George

File System



Primary FAT

| | 0 | 1 | 2 | 3 | |
|-----------|-------------|-------------|-------------|-------------|-----------------|
| 000117800 | F0 FF FF 0F | FF FF FF FF | FF FF FF 0F | 00 00 00 00 | yyy yyyyyyy |
| 000117810 | FF FF FF 0F | FF FF FF 0F | FF FF FF 0F | FF FF FF 0F | yyy yyy yyy yyy |
| 000117820 | FF FF FF 0F | FF FF FF 0F | FF FF FF 0E | 00 00 00 00 | yyy yyy yyy |
| 000117830 | FF FF FF 0F | FF FF FF | | FF FF 0F | yyy yyy ¼ yyy |
| 000117840 | FF FF FF 0F | FF FF FF | | FF FF 0F | yyy yyy e yyy |
| 000117850 | FF FF FF 0F | 16 00 00 00 | 17 00 00 00 | 19 00 00 00 | yyy |
| 000117860 | A2 00 00 00 | 1A 00 00 00 | 1C 00 00 00 | FF FF FF 0F | o yyy |
| 000117870 | 1D 00 00 00 | 1E 00 00 00 | 1F 00 00 00 | 20 00 00 00 | |
| 000117880 | 21 00 00 00 | 22 00 00 00 | 23 00 00 00 | 24 00 00 00 | ! " # \$ |
| 000117890 | 26 00 00 00 | FF FF FF 0F | 27 00 00 00 | 28 00 00 00 | & uvw ' / |

Root Directory Entry

Example:

File 1: First Cluster = 0x03 (3)

| | | | |
|------------------|-----------------|-------------|------------------|
| FF FF FF FF | FF FF FF FF | FF FF FF FF | 05 00 00 00 (5) |
| FF FF FF FF | 08 00 00 00 (8) | FF FF FF FF | 0B 00 00 00 (11) |
| 0A 00 00 00 (10) | FF FF FF FF | FF FF FF FF | 10 00 00 00 (16) |
| 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 |
| FF FF FF FF | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 |

File 2:
First Cluster = 0x07 (7)

Credits By George



File System



| | | | | | | | | | | | | | | | | | | |
|-----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---------|--------|
| 000408000 | 2E | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 10 | 00 | 00 | 44 | B2 | .. | D² |
| 000408010 | 9F | 3D | 9F | 3D | 00 | 00 | 44 | B2 | 9F | 3D | 04 | 00 | 00 | 00 | 00 | 00 | ! = ! = | D² ! = |
| 000408020 | 2E | 2E | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 10 | 00 | 00 | 44 | B2 | ... | D² |
| 000408030 | 9F | 3D | 9F | 3D | 00 | 00 | 44 | B2 | 9F | 3D | 00 | 00 | 00 | 00 | 00 | 00 | ! = ! = | D² ! = |
| 000408040 | 32 | 32 | 38 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 00 | 00 | 00 | 00 | 00 | 228 | |
| 000408050 | 21 | 00 | 7E | 40 | 00 | 00 | 00 | 00 | 21 | 00 | E4 | 00 | 00 | 80 | 00 | 00 | ! ~@ | ! ä |
| 000408060 | 32 | 33 | 31 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 00 | 00 | 00 | 00 | 00 | 231 | |

Credits By George



Deleted Files



- Deleting a file is a logical operation.
- The operating system only deletes references to the file areas of support assigned to that remittances are available to the operating system.
- The actual data are not deleted until they are overwritten by other files.
- The persistence of the data on the device can often recover (in whole or in part) the contents of deleted files.



Data Recovery Tools



- Some of the main data recovery software are:
- **Foremost** (opensource, Linux)
- **Scalpel** (opensource, Linux)
- **R-Studio** (commerciale, Windows)
- **Ontrack Recovery Pro** (commerciale, Windows)
- **Stellar Phoenix** (commerciale, Windows)
- **Recuva** (freeware, Windows)
- **PC Inspector File Recovery** (freeware, Windows)
- Drive Rescue



Demo R-Studio



The screenshot shows the R-Studio Drive view interface. The main window displays a tree view of drives on the local computer. The selected drive is ST380215A3.AAC, which is a 74.5 GB ATA (Primary Master) drive. The Properties pane on the right shows detailed information about the drive, including its name, OS object, size, sector size, and physical drive geometry.

| Device/Disk | Label | FS | Start | Size |
|------------------------|-----------------------|--------------------|---------|----------|
| Local Computer | | | | |
| Hitachi HD1725090VL... | | ATA (3rd Master) | | 465.8 GB |
| E: | Movies - HD - SATA | NTFS | 31.5 GB | 465.8 GB |
| Maxtor SL200P08A2H... | L42YYCQG | ATA (Primary SL... | | 189.9 GB |
| ST3160015A53.AAC | | ATA (2:2) | | 149.1 GB |
| G: | Software - Sa2 - S... | NTFS | 31.5 GB | 74.5 GB |
| I: | Music - Sa2 - SATA | NTFS | 74.5 GB | 74.5 GB |
| ST380215A3.AAC | SQZ0M6YW | ATA (Primary ML... | | 74.5 GB |
| C: | Windows | NTFS | 31.5 GB | 29.3 GB |
| D: | Games | NTFS | 29.3 GB | 45.2 GB |
| K: | | | 0 | |
| X: | | | 0 | |

| Name | Value |
|-------------------------|-------------------------|
| Drive Type | Physical Drive, Disk |
| Name | ST380215A3.AAC |
| OS Object | \\.\PhysicalDrive0 |
| R-Studio Driver | WinNT/Handle/Physical |
| Size | 74.5 GB (156301488 sec) |
| Sector Size | 512 B |
| Partition Size | 74.5 GB (156301488 sec) |
| Drive Control | |
| Maximum Transfer | 120 KB |
| I/O Unit | 512 B |
| Buffer Alignment | 2 B |
| I/O Tries | 2 |
| Physical Drive Geometry | |
| Cylinders | 9020 |
| Tracks Per Cylinder | 255 |
| Sectors Per Track | 63 |
| Sector Size | 512 B |
| Device Identification | |
| Product | ST380215A |



Windows Forensics



- Artifacts of the installation of the OS
 - Registry
 - user profile
 - trash
 - Recent Files and links LNK
 - event Log
 - prefetch folder
 - thumbnails
 - Pagefile.sys / hiberfil.sys



Setuplog.txt e Setupact.log



- The setuplog.txt file is located in the Windows system and is used to store information during setup of the operating system
- The most important information contained in this file is related to the time and date of installation of the operating system and all its components
- The setupact.log file is located in the Windows system and maintains a list of all actions performed during the graphical portion of the setup process
In Windows XP / 2003 are not stored timestamp of the shares, in Windows Vista / 7/8 are present



Setupapi.log



- The setupapi.log file is located in the Windows system and stores information of installation of hardware devices, service packs and hotfixes
 - This information can be very useful in the generation of a timeline of events
 - The information is written in the file sequentially, with a time stamp associated with each entry
- When a particular device is connected to the system you have to install a driver. The information is stored in the file on the installation setupapi.log



Setupapi.log



- Correlating information in this file and the date of last modification of the registry key on a USB device can determine the range of use of a device (first use date - the date last used)
- In Windows Vista / 7 setupapi.log the file has been divided into:
 - Setupapi.app.log: information about installing applications, hotfixes and service packs
 - Setupapi.dev.log: information about the installation of hardware devices
- Both files are in the folder C: \ Windows \ INF



Netsetup.log



- The file Netsetup.log is located in the Windows \ Debug and contains information about the workgroup or domain configured on the computer
The file is created during the operating system and stores installation it all changes regarding
Any adjustment of the working group, domain or enabling file sharing is stored



Windows Registry

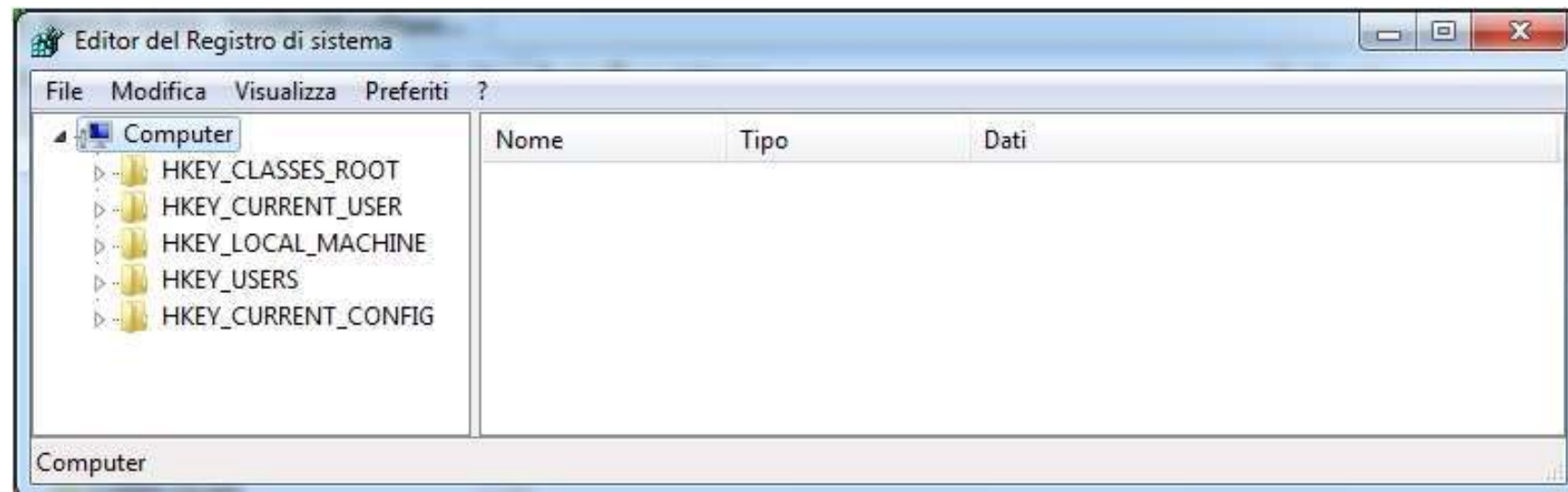
- The Windows registry contains very significant forensics data from our point of view
- The registry is a hierarchical database of configuration data for the operating system and most of the programs installed
- The user interacts with the registry typically through the configuration utility of the operating system (eg. The Control Panel) and applications
- The register was introduced since Windows 95 and, with several changes, is still present in Windows 7 and Windows Server 2008
- In all versions of Windows is a utility for finding and editing information, regedit



Windows Registry

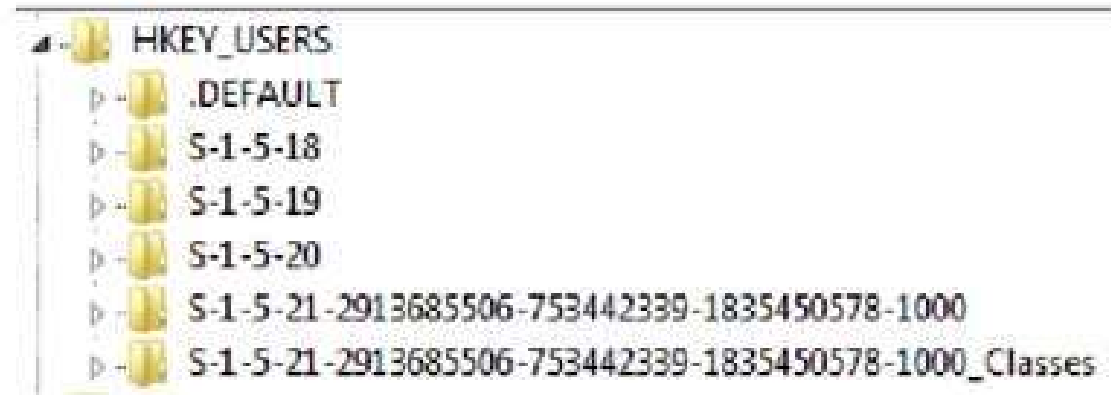


- At the physical level, the log is stored in files called hives
- The internal logic structure is conceptually similar to those of "folders" and Windows "file"
- The "Folders" registry keys are called
- The "file" of the register are those values





Windows Registry



| Chiave | Hive file |
|--------------------|--|
| <u>HKU\DEFAULT</u> | %SYSTEMROOT%\System32\config\DEFAULT |
| HKU\S-1-5-19 | Documents and Settings\LocalService\ntuser.dat |
| HKU\S-1-5-20 | Documents and Settings\NetworkService\ntuser.dat |
| <u>HKU\SID</u> | Documents and Settings\Username\ntuser.dat |



Windows Registry



The key is:

HKLM\SYSTEM\CurrentControlSet\Control\hivelist

| Nome | Tipo | Dati |
|--|--------|---|
| (Predefinito) | REG_SZ | (valore non importato) |
| \REGISTRY\MACHINE\SCD00000000 | REG_SZ | \Device\HarddiskVolume2\Boot\BCD |
| \REGISTRY\MACHINE\HARDWARE | REG_SZ | |
| \REGISTRY\MACHINE\SAM | REG_SZ | \Device\HarddiskVolume2\Windows\System32\config\SAM |
| \REGISTRY\MACHINE\SECURITY | REG_SZ | \Device\HarddiskVolume2\Windows\System32\config\SECURITY |
| \REGISTRY\MACHINE\SOFTWARE | REG_SZ | \Device\HarddiskVolume2\Windows\System32\config\SOFTWARE |
| \REGISTRY\MACHINE\SYSTEM | REG_SZ | \Device\HarddiskVolume2\Windows\System32\config\SYSTEM |
| \REGISTRY\USER\DEFAULT | REG_SZ | \Device\HarddiskVolume2\Windows\System32\config\DEFAULT |
| \REGISTRY\USER\5-1-5-19 | REG_SZ | \Device\HarddiskVolume2\Windows\ServiceProfiles\LocalService\NTUSER.DAT |
| \REGISTRY\USER\5-1-5-20 | REG_SZ | \Device\HarddiskVolume2\Windows\ServiceProfiles\NetworkService\NTUSER.DAT |
| \Registry\User\5-1-5-21-2913685506-753442339-1835450578-1000 | REG_SZ | \Device\HarddiskVolume2\Users\Mattia\NTUSER.DAT |
| \Registry\User\5-1-5-21-2913685506-753442339-1835450578-1000_Classes | REG_SZ | \Device\HarddiskVolume2\Users\Mattia\AppData\Local\Microsoft\Windows\UsrClass.dat |

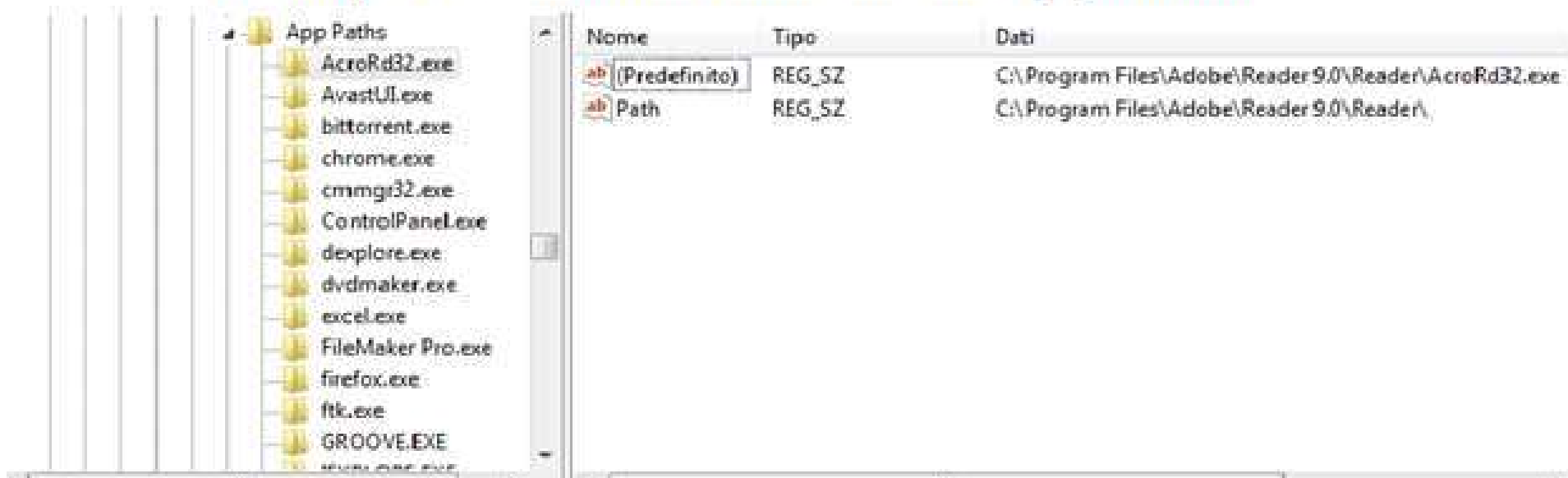


Windows Registry – Hive Software



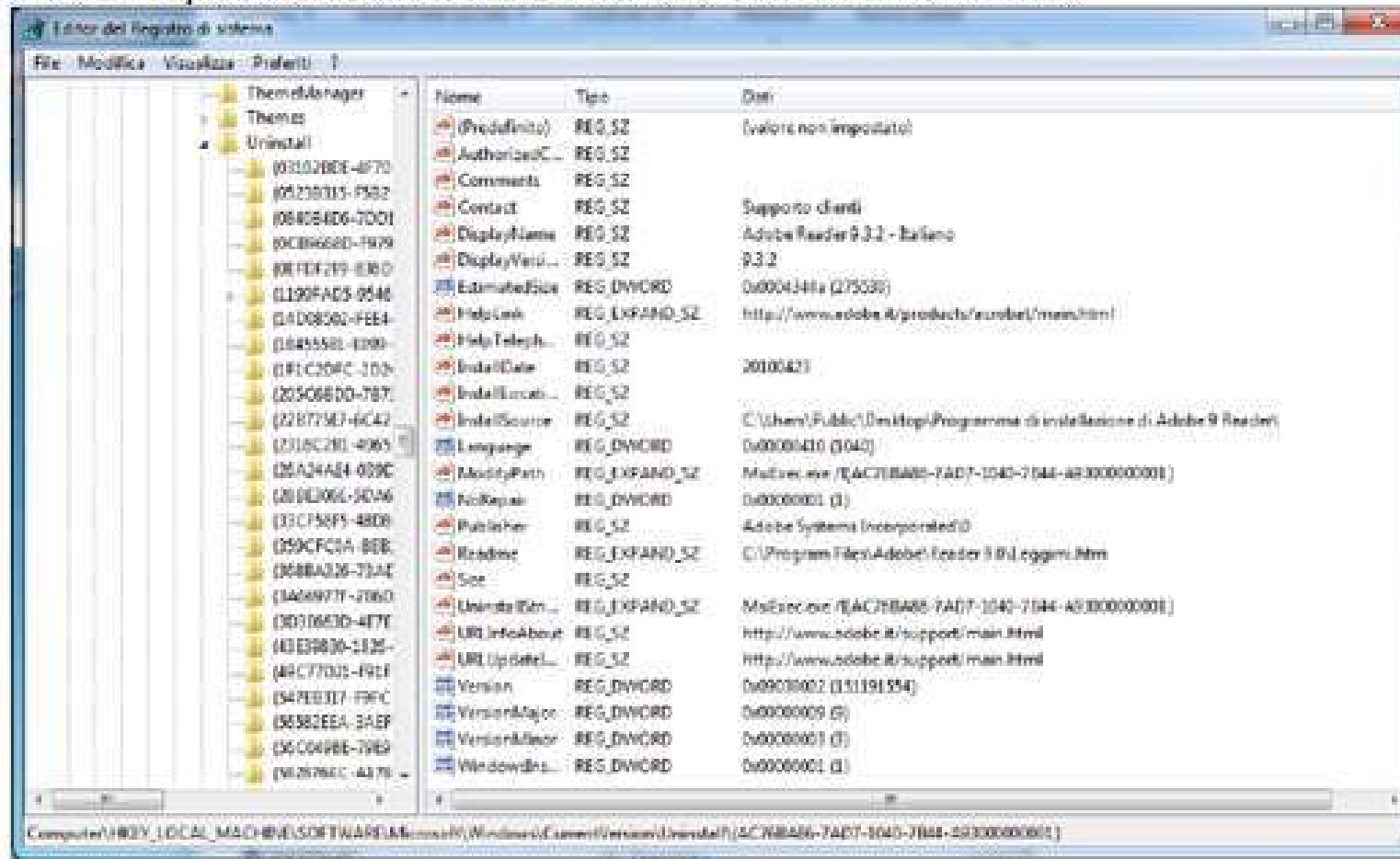
• La chiave

HKLM\Software\Microsoft\Windows\CurrentVersion\AppPath
contiene i percorsi di installazione delle varie applicazioni



Windows Registry – Hive Software

- Analogamente, la chiave **HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall** contiene i percorsi di disinstallazione dei vari software





Windows Registry – Hive Software



The Shut Down Time, Time Zone Information

Editor del Registro di sistema

DCode v4.02a (Build: 9306)

DCode
Convert Data to Date / Time Values

Add Bias: Window on top

Decode Format:

Example:

Value to Decode:

Date & Time:

www.digital-detective.co.uk

Cancel Clear Decode

| Nome | Tipo | Dati |
|-----------------------|----------------|-------------------------|
| (Predefinito) | REG_SZ | (valore non impostato) |
| ComponentizedBuild | REG_DWORD | 0x00000001 (1) |
| CSDBuildNumber | REG_DWORD | 0x00004001 (16385) |
| CSDReleaseType | REG_DWORD | 0x00000000 (0) |
| CSDVersion | REG_DWORD | 0x00000000 (0) |
| Directory | REG_EXPAND_... | %SystemRoot% |
| ErrorMode | REG_DWORD | 0x00000000 (0) |
| NoInteractiveServices | REG_DWORD | 0x00000000 (0) |
| ShellErrorMode | REG_DWORD | 0x00000001 (1) |
| ShutdownTime | REG_BINARY | fa 25 a8 d2 cb 19 cb 01 |
| SystemDirectory | REG_EXPAND_... | %SystemRoot%\system32 |

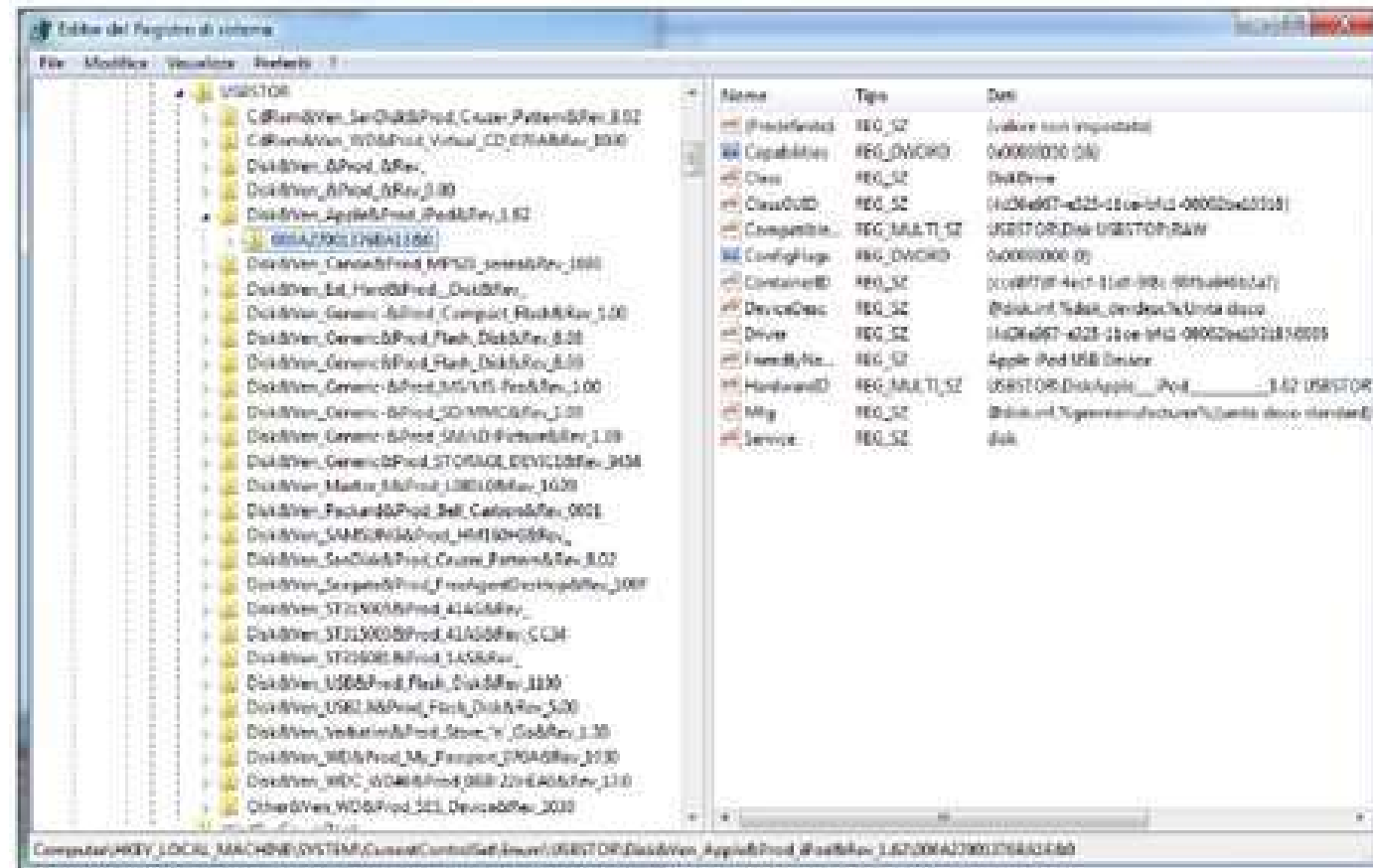
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows



Windows Registry – Hive System - USB



HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR





Windows Registry – Hive System - IDE



HKLM\SYSTEM\CurrentControlSet\Enum\IDE

The screenshot shows the Windows Registry Editor window. The left pane displays the tree structure expanded to **Enum\IDE**. The right pane shows a list of registry values for the selected key.

| Nome | Tip | Data |
|---------------------|--------------|--|
| (Default) | REG_SZ | (valore non impostato) |
| Capabilities | REG_DWORD | 0x00000000 (0) |
| Class | REG_SZ | DiskDrive |
| ClassGUID | REG_SZ | {4c35e977-4225-11c0-bf01-000000000000} |
| CompatibleIDs | REG_MULTI_SZ | {GenDisk} |
| ConfigFlags | REG_DWORD | 0x00000000 (0) |
| ContainerID | REG_SZ | {44e3dc1f-4a76-11d1-9f51-005006c00008} |
| DeviceDesc | REG_SZ | @disk.inf,%disk_devdesc%\Unità disco |
| Driver | REG_SZ | {4c35e977-4225-11c0-bf01-000000000000}\003f |
| FriendlyName | REG_SZ | ST31500341AS |
| HardwareID | REG_MULTI_SZ | IDE\DiskST31500341AS... CC1H... IDE\ST31500341AS |
| LocationInformation | REG_SZ | 4 |
| Mfg | REG_SZ | @disk.inf,%genmanufacturer%\%unità disco standard% |
| Service | REG_SZ | disk |

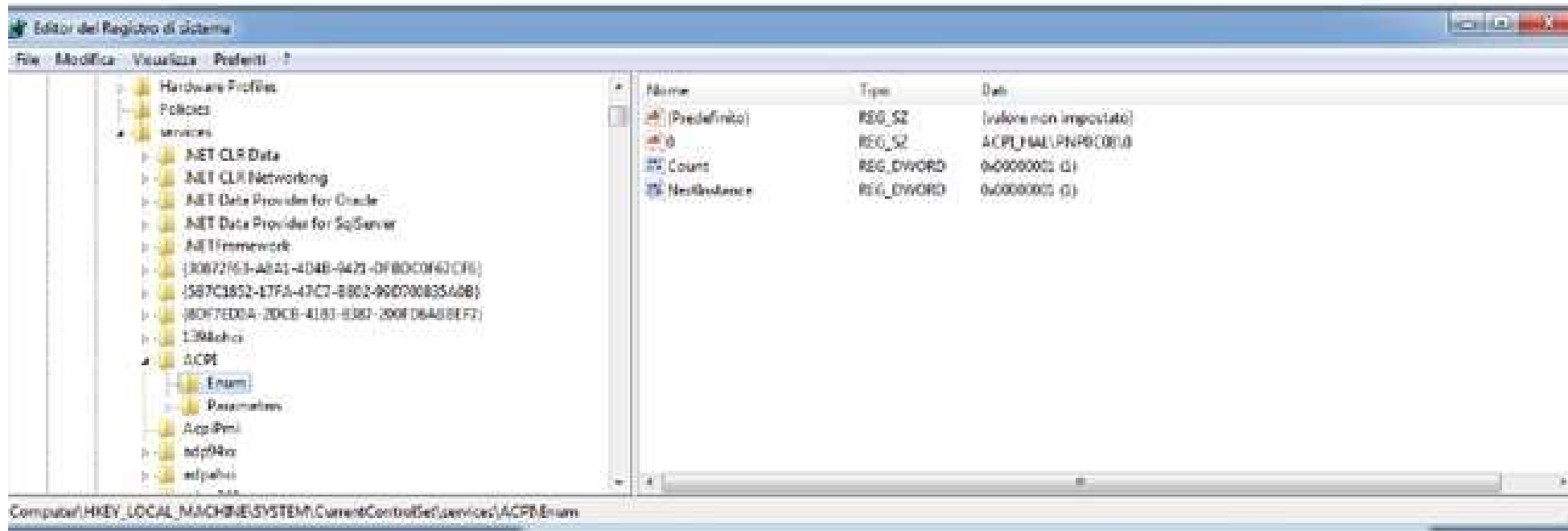


Windows Registry – Hive System



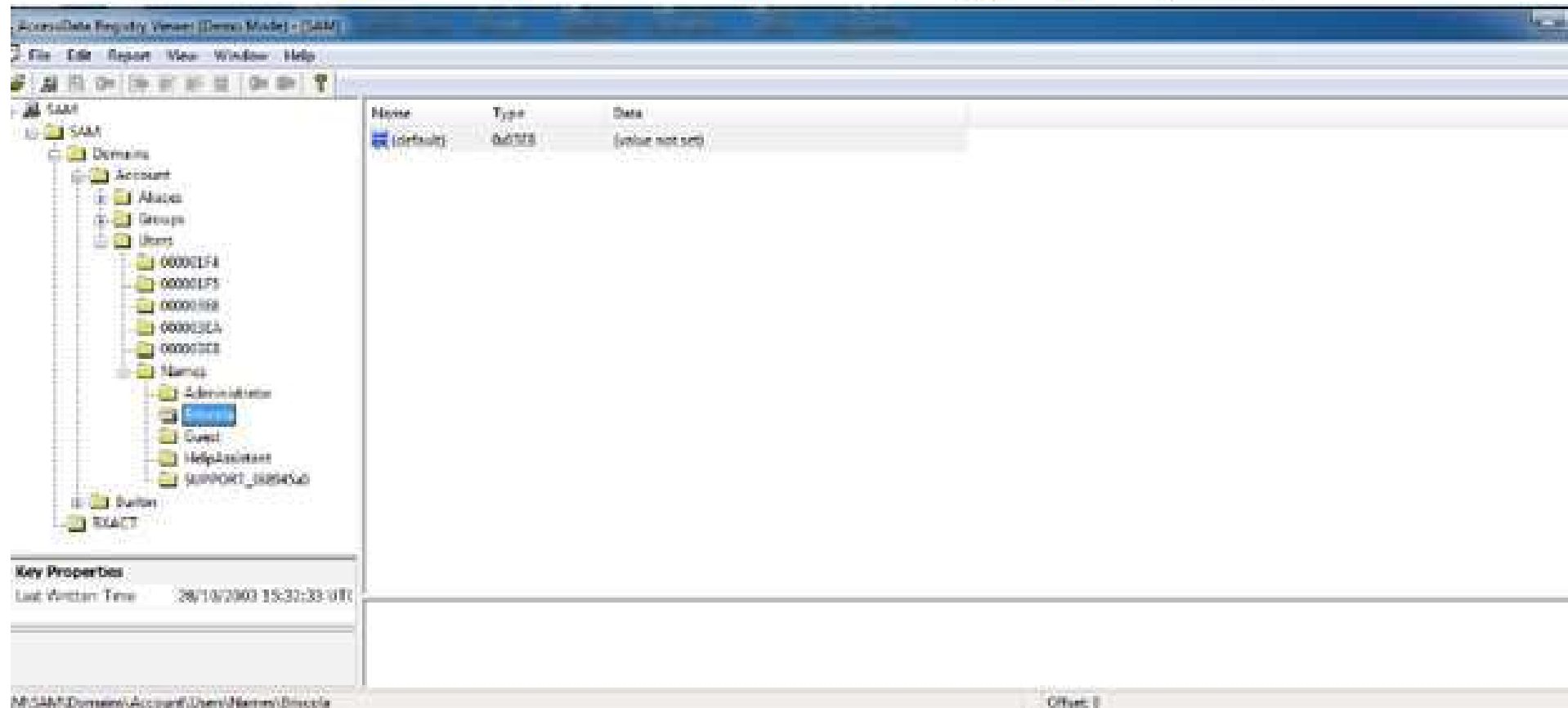
Services Installed in a Computer

HKLM\System\CurrentControlSet\Services



Windows Registry – Hive System

- La hive SAM contiene le informazioni sugli utenti e i gruppi configurati nella macchina
- Il file si trova nella cartella %SYSTEMROOT%\system32\config



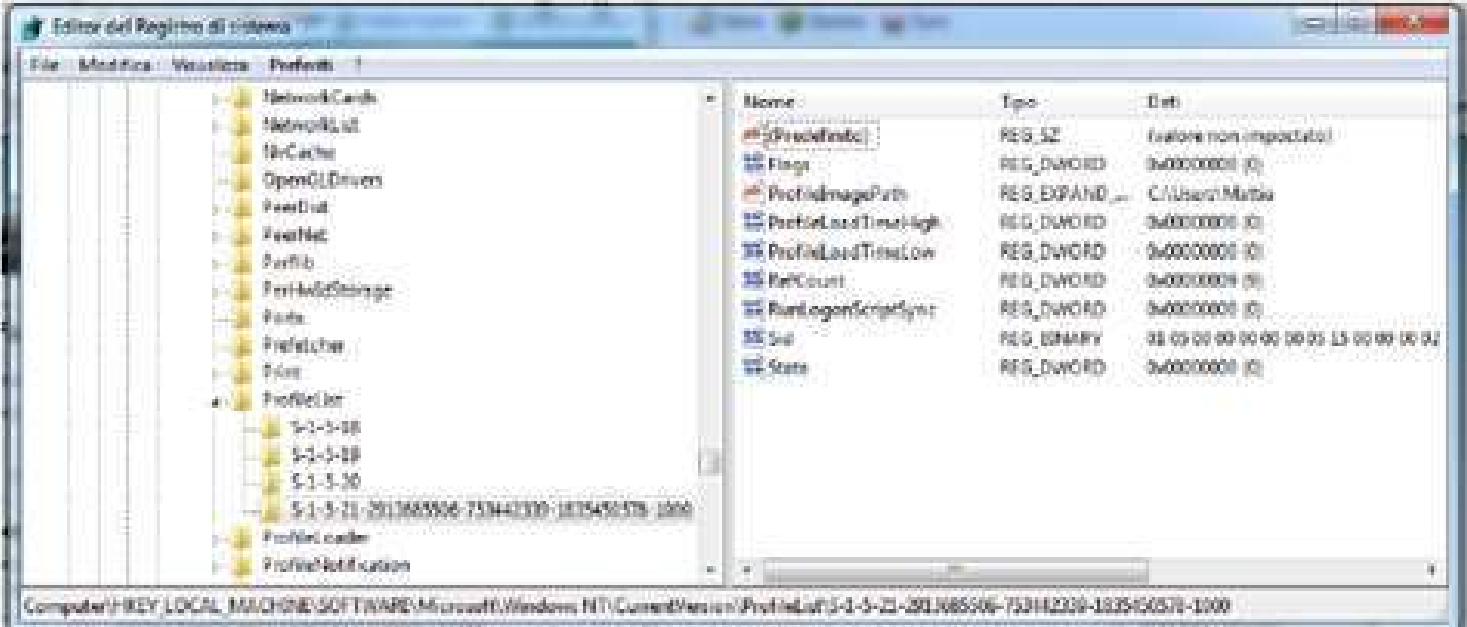


Windows Registry – Hive SAM



USERS AND GROUP

HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList





Autorun



Chiave

HKLM\Software\Microsoft\Windows\Current Version\Run

HKLM\Software\Microsoft\Windows\Current Version\RunOnce

HKLM\Software\Microsoft\Windows\Current Version\RunServices

HKLM\Software\Microsoft\Windows\Current Version\RunServicesOnce

HKLM\Software\Microsoft\Windows\Current Version\Winlogon

HKLM\System\CurrentControlSet\Services

HKU\Software\Microsoft\Windows\Current Version\Run

HKU\Software\Microsoft\Windows\Current Version\Run Once



Autorun File



Nome file e percorso

%SYSTEMDRIVE%\autoexec.bat

%SYSTEMDRIVE%\config.sys

%WINDIR%\wininit.ini

%WINDIR%\win.ini

%WINDIR%\system.ini

%WINDIR%\dosstart.bat

%WINDIR%\system\autoexec.nt

%WINDIR%\system\config.nt

%WINDIR%\system32\autochk.exe



Autoruns



The screenshot shows the Autoruns utility window from Sysinternals. The window title is "Autoruns - Sysinternals: www.sysinternals.com". The interface includes a menu bar (File, Entry, Options, Help), a toolbar, and a sidebar with various system components like Winlogon, Winsock Providers, and Network Providers. The main pane displays a table of startup items.

| Autorun Entry | Description | Publisher | Image Path |
|---|--------------------------------|----------------------------|-----------------------------------|
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run | | | |
| Adobe ARM | Adobe Reader and Acrobat... | Adobe Systems Incorporated | c:\program files\common fil... |
| Adobe Reader | Adobe Acrobat SpeedLoun... | Adobe Systems Incorporated | c:\program files\adobe\rea... |
| avast5 | avast! Antivirus | AVAST Software | c:\program files\avast\softw... |
| GrooveMonitor | GrooveMonitor Utility | Microsoft Corporation | c:\program files\microsoft of... |
| IAnotif | Event Monitor User Notifica... | Intel Corporation | c:\program files\intel\intel m... |
| iTunesHelper | iTunesHelper | Apple Inc. | c:\program files\itunes\itun... |
| QuickTime Task | QuickTime Task | Apple Inc. | c:\program files\quicktime\... |
| Samsung Pane... | | | c:\windows\samsung\pane... |
| SunJavaUpdat... | Java(TM) Platform SE binary | Sun Microsystems, Inc. | c:\program files\java\jre5\bi... |
| TkBellExe | RealNetworks Scheduler | RealNetworks, Inc. | c:\program files\common fil... |
| VMware hqtray | VMware Host Network App... | VMware, Inc. | c:\program files\vmware\w... |
| vmware-tray | VMware Tray Process | VMware, Inc. | c:\program files\vmware\w... |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Run | | | |
| msnmgr | Windows Live Messenger | Microsoft Corporation | c:\program files\windows liv... |
| RoboForm | RoboForm TaskBar Icon | Siber Systems | c:\program files\siber syste... |
| Skype | Skype | Skype Technologies S.A. | c:\program files\skype\pha... |
| HKLM\SOFTWARE\Classes\Protocols\Filer | | | |
| text/xml | Microsoft Office XML MIME... | Microsoft Corporation | c:\program files\common fil... |
| HKLM\SOFTWARE\Classes\Protocols\Handler | | | |
| grooveLocalG... | GrooveSystemServices Mo... | Microsoft Corporation | c:\program files\microsoft of... |
| livecall | Windows Live Messenger P... | Microsoft Corporation | c:\program files\windows liv... |
| msihelp | Microsoft® Help Data Servi... | Microsoft Corporation | c:\program files\common fil... |
| msnim | Windows Live Messenger P... | Microsoft Corporation | c:\program files\windows liv... |
| skype-ie-addon... | Skype add-on for IE | Skype Technologies S.A. | c:\program files\skype\tool... |
| skype4com | Skype for COM API | Skype Technologies | c:\program files\common fil... |
| HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components | | | |
| Microsoft Wind... | Windows Mail | Microsoft Corporation | c:\program files\windows m... |
| HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks | | | |
| Groove GFS St... | GrooveShellExtensions Mo... | Microsoft Corporation | c:\program files\microsoft of... |
| HKLM\Software\Classes\ShellEx\ContextMenuHandlers | | | |
| avast | avast! Shell Extension | AVAST Software | c:\program files\avast\softw... |
| Cover Designer | Cover Designer | Nero AG | c:\program files\nero\nero ... |
| PSPad | | | c:\program files\pspad edit... |
| WinRAR | | | c:\program files\winrar\var... |
| XXX Groove G... | GrooveShellExtensions Mo... | Microsoft Corporation | c:\program files\microsoft of... |
| HKLM\Software\Classes\FileSystemObjects\ShellEx\ContextMenuHandlers | | | |



Hive NETUSER



Chiave

HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\[GUID]\Count

HKU\Software\Microsoft\Windows\ShellNoRoam\MUICache

HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts

HKU\Software\Microsoft\Search Assistant\ACMrU

HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\MapNetworkDriveMRU

HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions



Tools for the register analysis



- **RegRipper (Harlan Carvey) OpenSource;**
- **AccessData Registry Viewer - free**
- **Windows Registry Recovery (www.mitec.cz) free**
- **Windows Registry Analyzer (www.mitec.cz) free**
- **RegExtract (www.woanware.co.uk) free**
- **USBDeviceForensics (www.woanware.co.uk)**
- **ForensicsUserInfo (www.woanware.co.uk)**

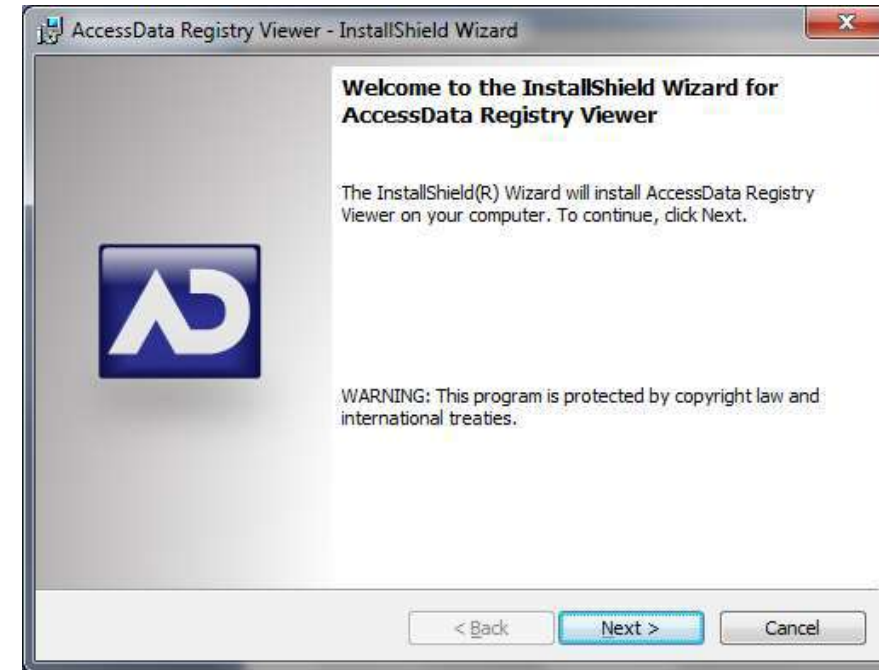
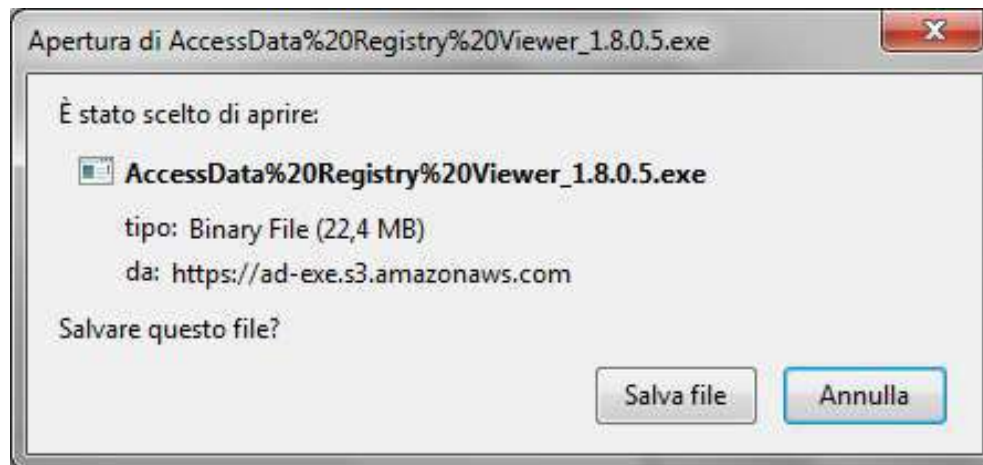
Tools for the register analysis



Registry Viewer 1.8.0.5

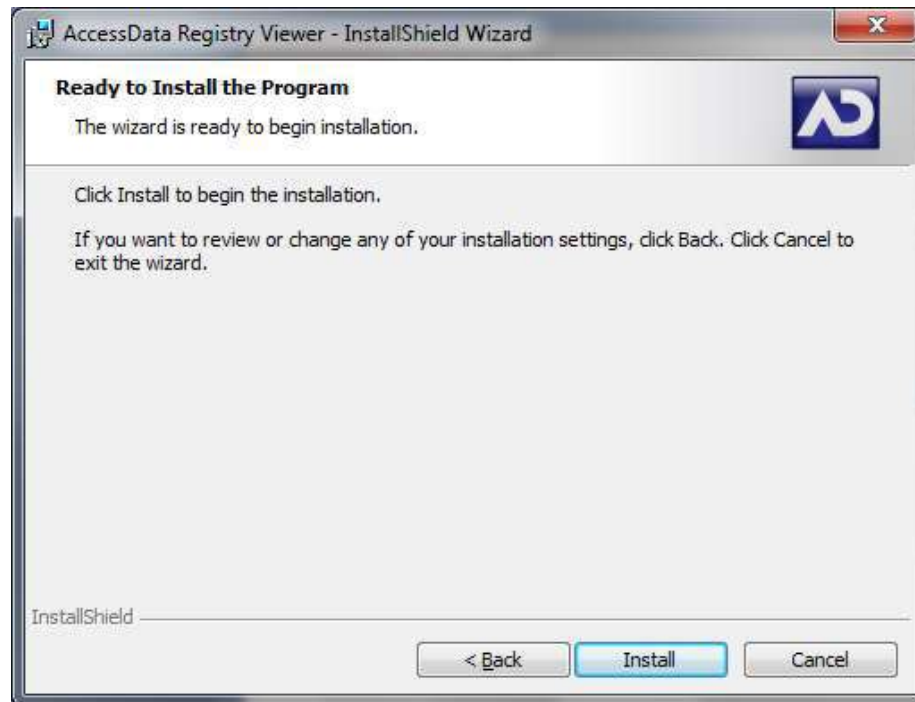
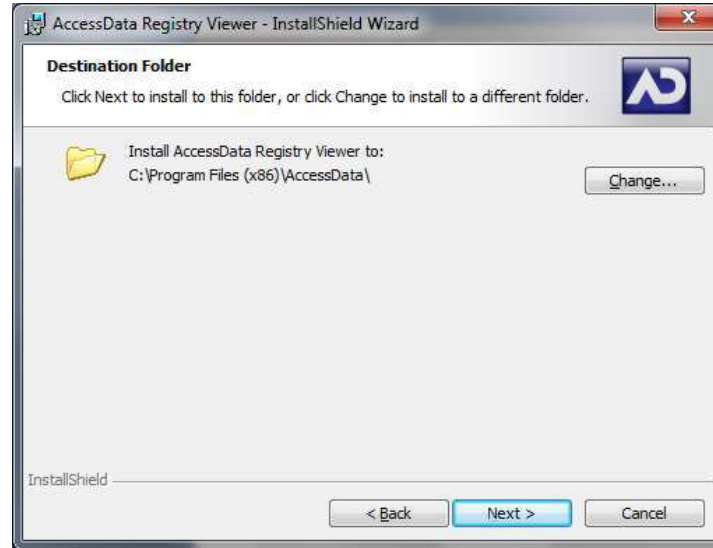
Release Date: Sep 23, 2014

[DOWNLOAD PAGE](#)





Tools for the register analysis





Recycle Bin



AccessData FTK Imager 2.6.1.62

File View Mode Help

Evidence Tree

- \$Secure
 - Documents and Settings
 - MSOCache
 - Programmi
 - RECYCLER
 - S-1-5-21-823518204-725345543-6820033
 - Dcl
 - System Volume Information
 - WINDOWS
 - [unallocated space]
 - [orphan]
- Unpartitioned Space [basic disk]

File List

| Name | Size | Type | Date Modified |
|--------------------|-------|--------------------|-------------------|
| Dcl | 1 KB | Directory | 12/01/2010 9.1... |
| \$I30 | 4 KB | NTFS Index Allo... | 12/01/2010 9.1... |
| Dcl6.doc | 22 KB | Regular File | 12/01/2010 9.1... |
| Dcl6.doc.FileSlack | 3 KB | File Slack | |
| desktop.ini | 1 KB | Regular File | 12/01/2010 9.1... |
| desktop.ini | 1 KB | Regular File | 12/01/2010 8.5... |
| INFO2 | 1 KB | Regular File | 12/01/2010 9.1... |
| INFO2.FileSlack | 4 KB | File Slack | |

Custom Content Sources

| Evidence:File System Path File | Options |
|--------------------------------|---------|
| | |

```

000 05 00 00 00 01 00 00 00-10 00 00 00 20 03 00 00 .....
010 00 56 00 00 43 3a 5c 44-6f 63 75 6d 65 6e 74 73 ····C:\Documents
020 20 61 6e 64 20 53 65 74-74 69 6e 67 73 5c 4d 61 and Settings\Ma
030 74 74 69 61 5c 44 6f 63-75 6d 65 6e 74 69 5c 64 ttia\Document1\d
040 6f 63 38 2e 64 6f 63 00-00 00 00 00 00 00 00 00 oc8.doc.....
050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
  
```

Cursor pos = 0; clus = 2464923; log sec = 19719384; phy sec = 19719447

Properties | Hex Value Interpreter | Custom Content Sources

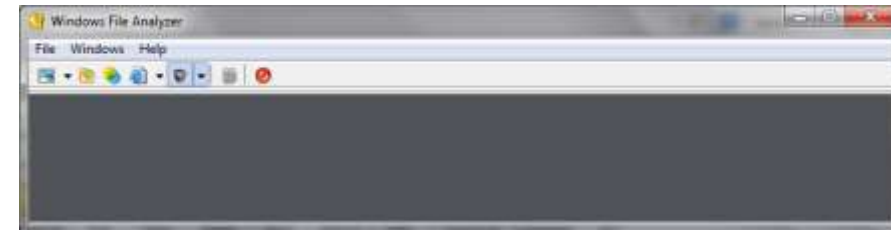
For Help, press F1



Recycle Bin - Tools



“ Windows File Analyzer (www.mitec.cz)



“ Rifiuti (www.foundstone.com)

“ Win Forensic Analysis (<http://www.machor-software.com/>)



Tools for analyzing link



- “ Windows File Analyzer (www.mitec.cz)
 -
- “ Win Forensic Analysis (<http://www.machor-software.com/>)
- “ Link Viewer (<http://www.gaijin.at/>)
- “ Lnkanalyser (<http://www.woany.co.uk/>)
- “ SimpleCarver (<http://www.simplecarver.com/>)



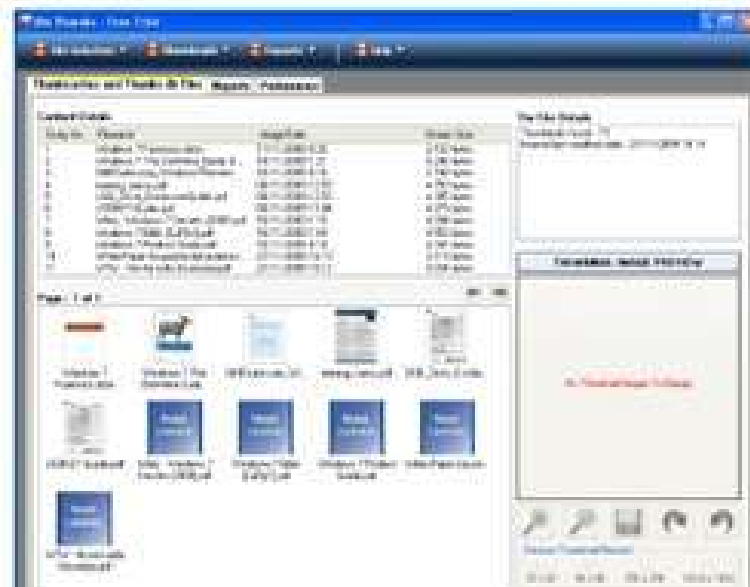
Tools for analyzing registry



- **Event Viewer (Microsoft)**
- **Event Log Explorer (<http://eventlogxp.com/>)**
- **MyEventViewer (<http://www.nirsoft.net>)**
- **Advanced Event Viewer (<http://www.advancedeventviewer.com>)**
- **GFI Events Manager**
- **www.EventID.net**
- **www.ultimatewindowsecurity.com**

Thumbnails tools

- Thumbcache Parser\Recovery (freeware)
- DMThumbs (commerciale)
- Thumbnail Expert (commerciale)
- ThumbsDb Viewer






Internet Artifacts





Internet Artifacts



**So what are the best practices
when preserving data from
social networking sites?**





Internet Artifacts



#1

Document the Process

Document your preservation process – including dates, times, and who captured the information – so you can defend it.





Internet Artifacts



#2



Know the Tools

Be sure you truly understand the process being used to collect social media content, and be aware of any potential pitfalls.



Internet Artifacts



#3



Use the Tools

Utilize built-in collection tools such as Facebook's "Download a Copy" utility to better understand what you get and don't get during collection.



Internet Artifacts



#4



Keep it Legal

Never gain access to an account illegally or deceptively.



Internet Artifacts



#5



Verify the Owner

Take steps to verify the ownership of an account. Do not assume an account belongs to someone simply because it has their name on it.

#6



Verify the Source

Do not assume anything about pictures collected from a social media account – where, when or by whom they were taken. Verify sources if possible.



Internet Artifacts

#7



Testify!

The person performing the collection may be called to testify about the process in court. Be sure that individual is qualified to perform collections, and would make a good witness.



File password cracking



- Passware Kit (<http://www.lostpassword.com/>)
- ElcomSoft Password Recovery Bundle (<http://www.elcomsoft.com/>)
- LastBit Password Recovery (<http://lastbit.com/>)
- AccessData Password Recovery Toolkit (PRTK) (<http://accessdata.com/>)
- Multi Password Recovery Portable (<http://passrecovery.com/>)
- Protected Storage Pass View, Network Password Recovery, Mail Pass View, MessenPass, PST Password (http://www.nirsoft.net/password_recovery_tools.html)



Passware Password Recovery Kit



Passware Password Recovery Kit Standard Demo

File View Help

Back Forward Start Page Recover Search Buy Now Support Help

Quick Start

- [Recover file password...](#)
- [Search for protected files...](#)
- [Recover internet and network passwords...](#)
- [Create Windows password reset disk](#)

Recover File Password (Ctrl+O)
Pick a protected file to start password recovery.

Recover Internet and Network Passwords (Ctrl+I)
Recover passwords for websites, network connections, and email accounts.

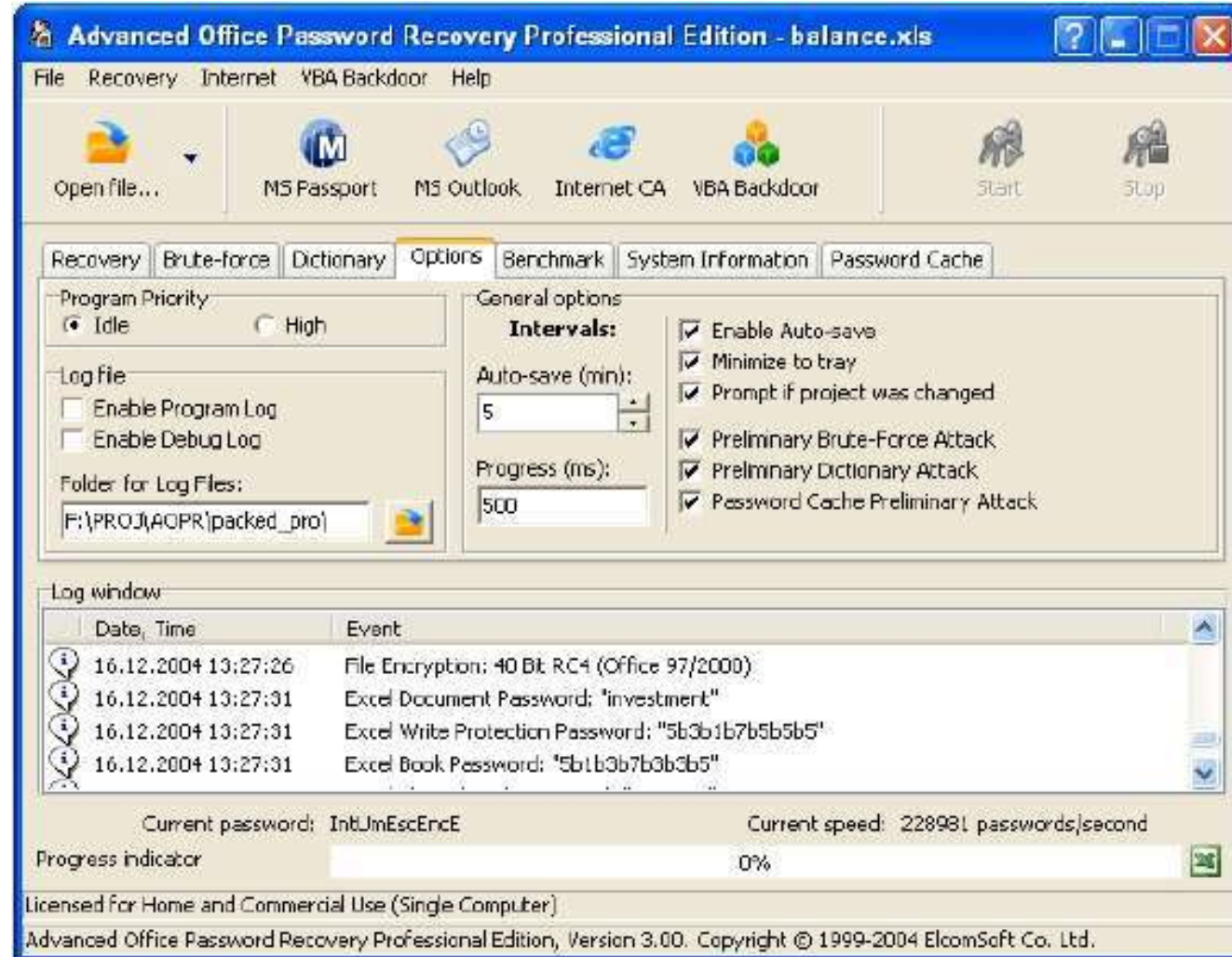
Reset Windows Administrator Password (Ctrl+W)
Create a bootable CD-ROM that instantly resets Windows Administrator password.

Search for Protected Files (Ctrl+F)
Scan computer for protected files.

Please select file to recover its password, or drag and drop file to this window to start the recovery.



Elcomsoft Password Recovery Bundle





LastBit Password Recovery



PasswordTools.com

PasswordTools Home Support Order Help Exit

Current version supports
Access, Word, Lotus Organizer, Excel, Outlook, VBA, Schedule+, Money, Symantec Act!, MS Backup, MS Project, Pocket Excel, OneNote, Zip/WinZip, PowerPoint (click to launch recovery module)

Your document type is not listed here? Drop us a note

 [Click here to Recover Document Password](#)

 [Information](#)

Other Password Related Software:

- Windows 95/98
- Windows NT/2000/XP/2003
- e-mail passwords
- IE Content Advisor
- VBA Password
- Secret Explorer

Tools:

- Password Analyzing Service**
estimate recovery password time and check if your password is weak.
- DiscoverIt!**
find out what Windows hides behind asterisks.
- Find Password Protected Documents**

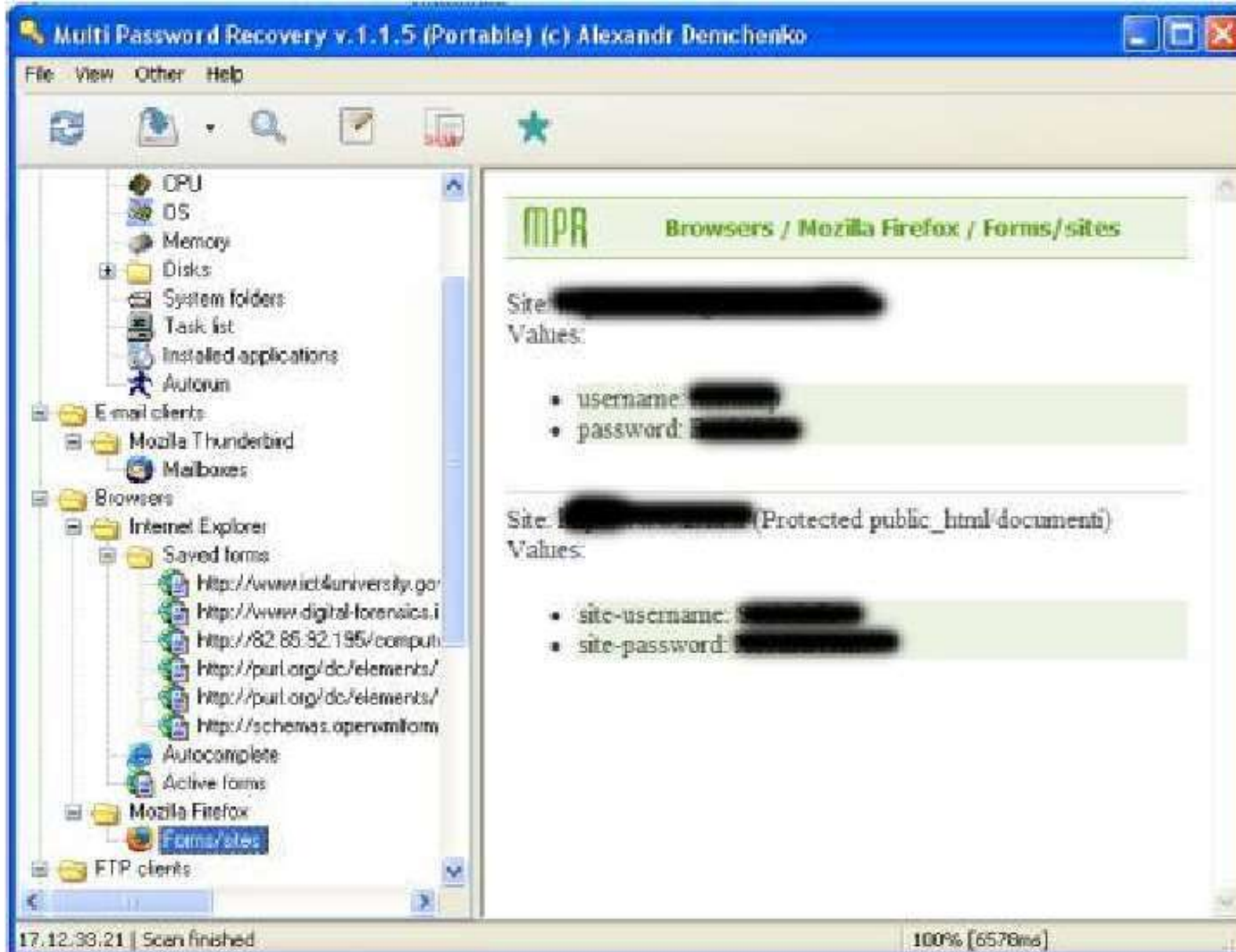
Articles:

- Password recovery methods
- Password types in MS Access.
- Password types in MS Word.
- Password types in MS Excel.

(c) 1997-2006 LastBit Software, support@lastbit.com



Multi Password Recovery Portable





Other interesting...



- Alternate Data Streams
- Steganografia
- Windows Shadow Copy (Vista/7)
- Encrypting File System
- BitLocker (Vista/7) e BitLockerToGo (7)



Analyzing CD/DVD



- CD Roller
 - (<http://www.cdroller.com/>)
- IsoBuster
 - (<http://www.isobuster.com/it/>)
- Abyssal CD/DVD Recovery
 - (<http://www.abyssoft.com/>)
- Recovery Toolbox for CD
 - (<http://www.recoverytoolbox.com/it/cd.html>)
- CD/DVD Inspector
 - (<http://www.infinadyne.com>)



Operating steps



- Preparation and Identification
- Acquisition and Retention
- Analysis
- **Evaluation and presentation**

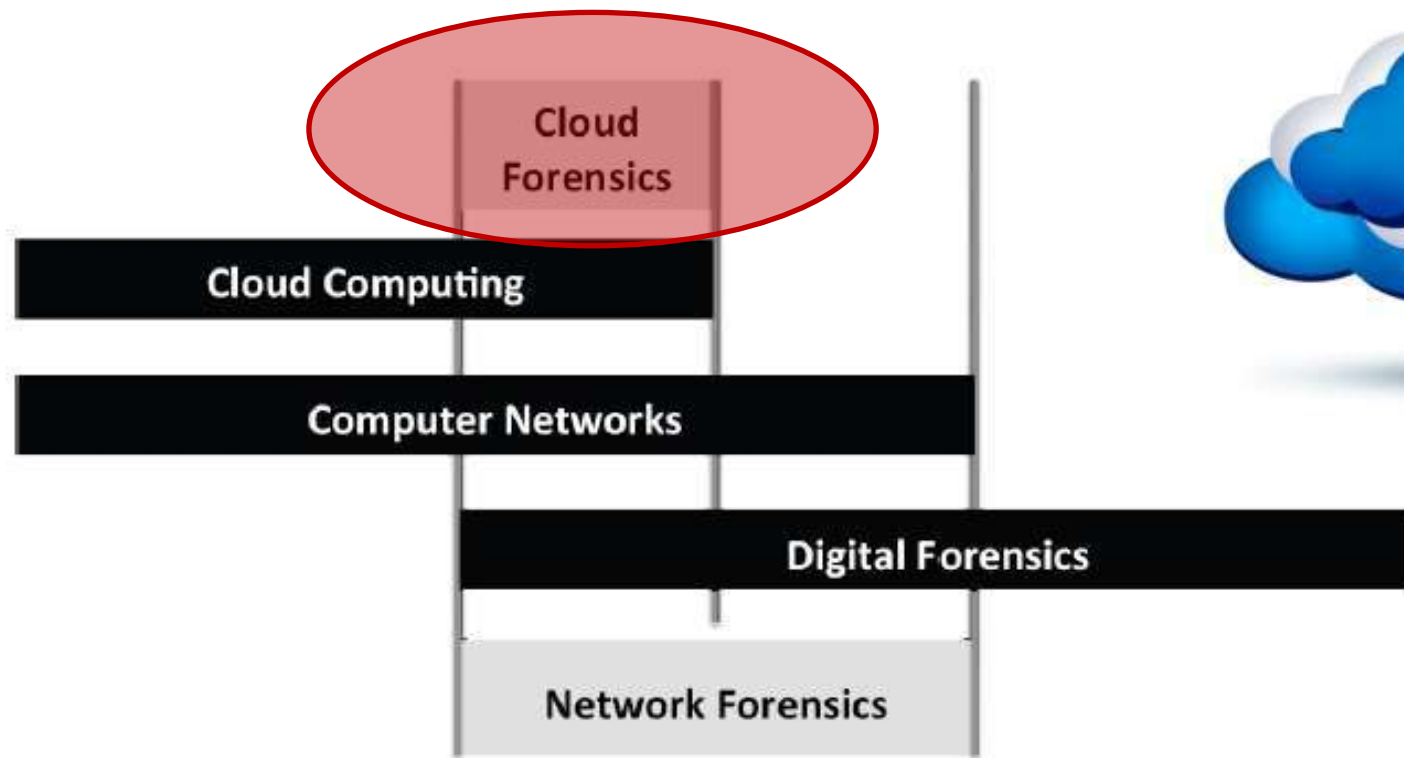


Evaluation and presentation



- The results and conclusions drawn should be presented in an easily understandable
- judges, lawyers, administrators do not usually have extensive computer skills
- However it is likely that the report be reviewed by a technical counterpart
- Simplicity and clarity, not superficiality and approximation

- So basically **what happens** with the DF into the Cloud perspective?!?
- Cloud Forensics calls for the **higher area**.

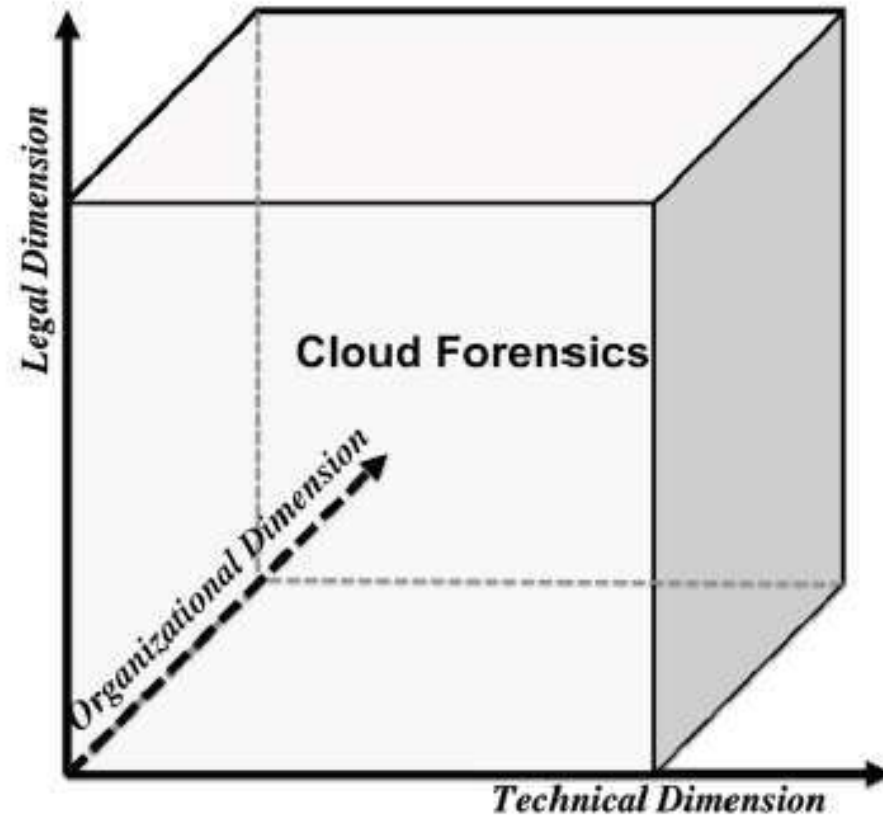




3 Dimensions



The 3 dimensions in Cloud Forensics





Technical



The Technical dimension develops a series of tools, plus extraction forensics procedures, into the cloud environment. The key aspects related to the Technical dimension are:

- **Forensics Data Collection** – The Cloud Forensics Collection is composed by the overall process of identification, collection, recording and acquisition of forensics data from those possible and available data sources into the Cloud. Data may be found both on Client and Provider (infrastructure) sides. Each one of cloud's services model has got different tools and data collection procedures. There is not a standard sequence, as it happens in Computer Forensics: ahead those «easy to run» data (*RAM image*) are processed, then data with lower reliability. The collection's process must run data integrity procedures.

- ✓ **Elastic, static and Live Forensics;**
- ✓ **Evidence Segregation:** another peculiarity of Cloud Computing resources groupment.
- ✓ **Virtual environments investigation** – virtualization is the key technology used into Cloud services delivery. Here we do use computer forensics tools into a virtualized environment (IF you will be able to find the virtualized server!!).



Technical/1



It is **not so** easy to develop those procedures and tools that must be used in order to physically identify the needed data into a given timeframe; then tracing the data itself (into a given timeframe) taking into consideration domestic jurisdictions.

- **Proactive preparedness:** here we mean those tools that can be used both on client-side and service provider ones.

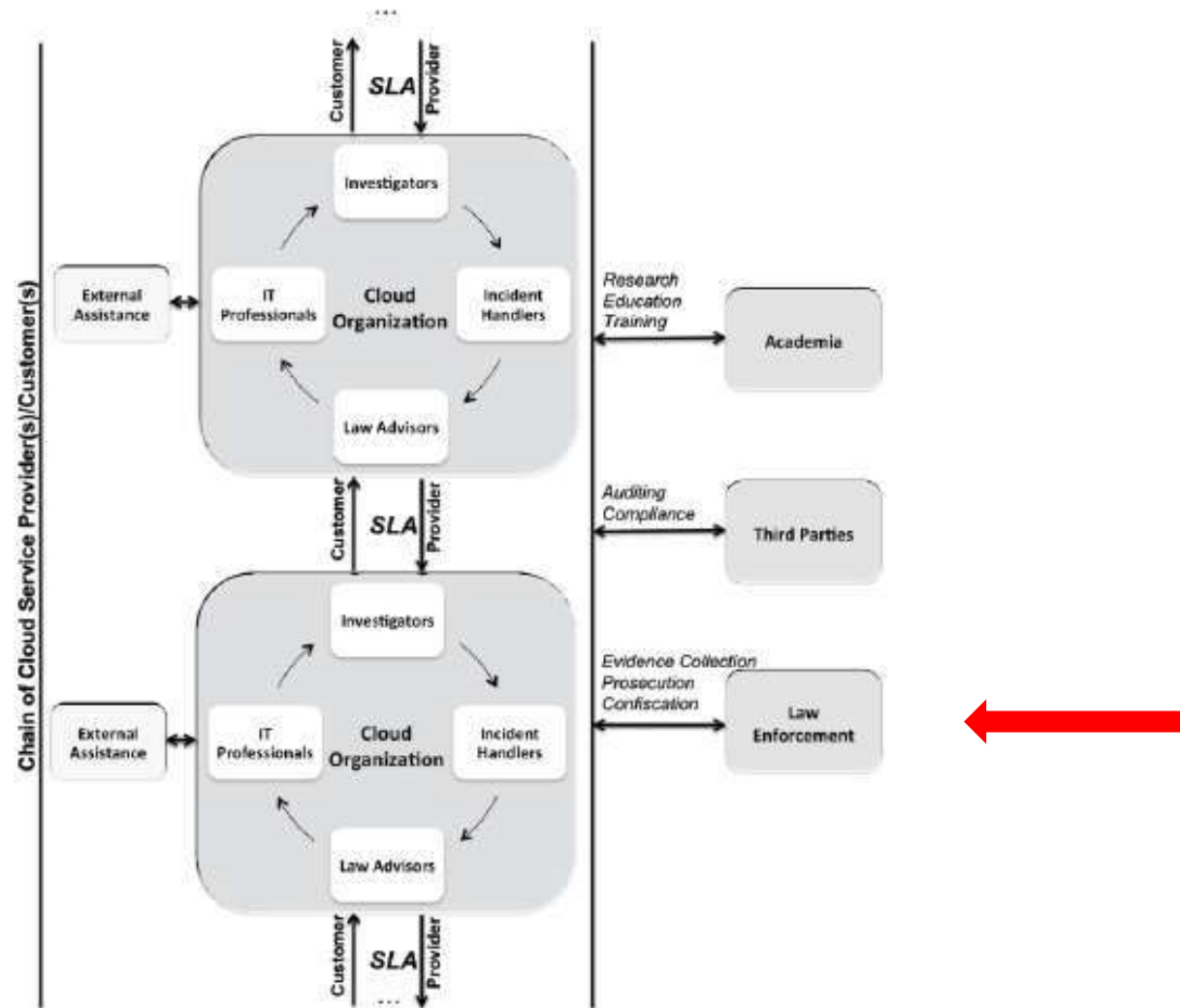




Organizational

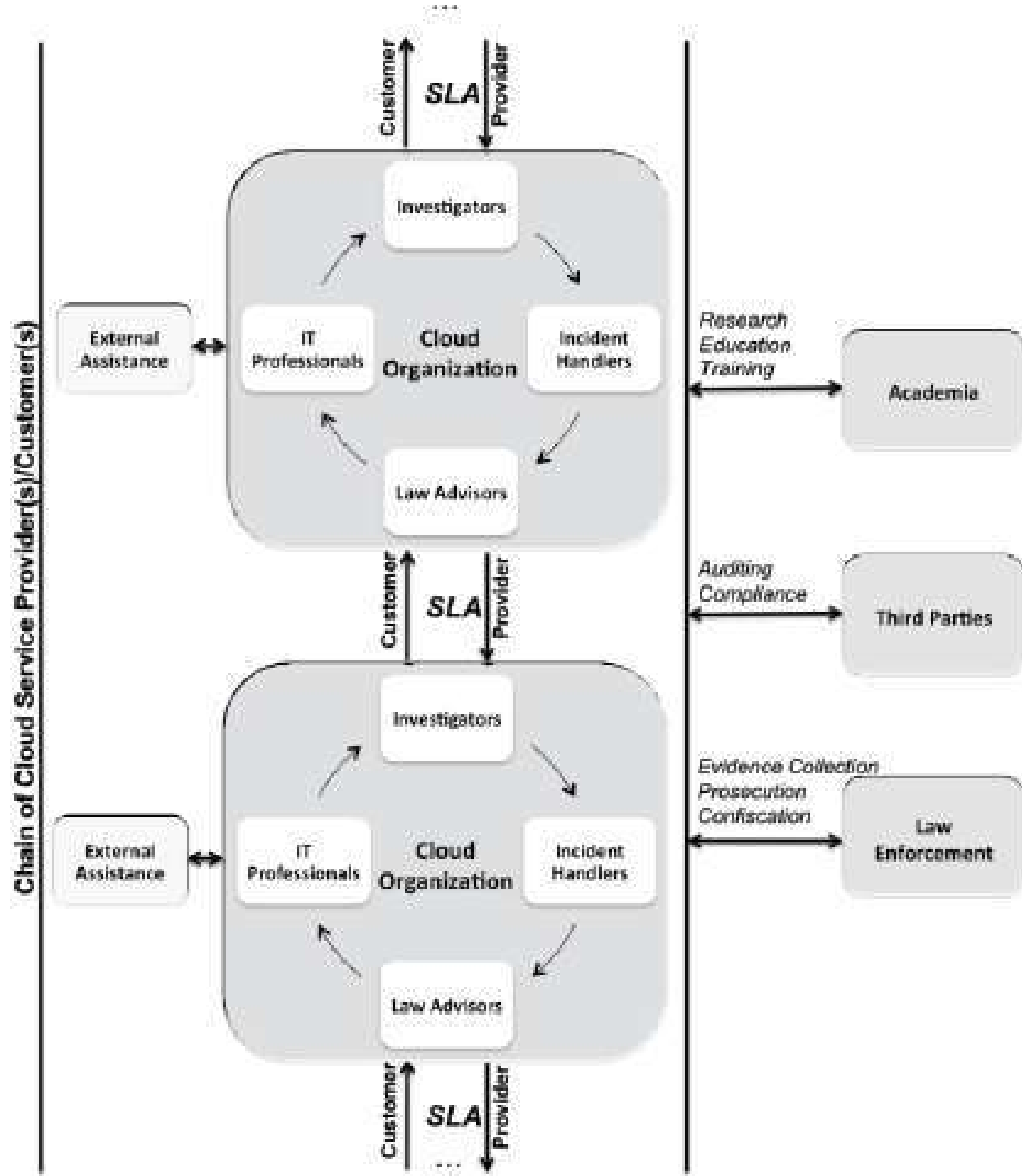


Organizational dimension





Organizational dimension





Organizational



Forensics investigations in cloud environment are always developed on two different sides: Computer Service Provider (CSP) e the Cloud's Customer one.

The organizational environment we've just seen is composed by basic and must-have parts, which would allow a total efficiency when running a cloud forensics.

In order to allow Forensics Investigations potentials, each Cloud Organization (thus including Providers, private companies and those given customer's services) a real collaboration among the different Business Units and Teams must be allowed:

- **Investigators:** they should be able to understand what's happened both on providers and customer's sides, in order to obtain a good (quality speaking) investigation and to obtain real results.
- **IT Professionals:** this group should include System, Network and Security Administrators,, ethical hackers, cloud security architects and technical support staff into the cloud organization itself;
- **Incident handlers:** a Team handling a variety of specific cloud security incidents such as: unauthorized access to data, data leaks and accidental data loss, confidentiality violation, inappropriate use of the data system, malware infections, internal and external attacks, DDoS attacks.



Legal



- **Legal Advisor:** its own importance is *crucial*.

The Cloud provider should definitely include legal advisors, since they are used to multi-jurisdictional issues. Also, each forensics activity onto the Cloud should not break punctual laws in specific jurisdictions, as well as those by different subjects which share the very same resources. Internal legal consultants must *speak with and cooperate* with Law Enforcement during the investigation.

- **External Support:** it's dramatically important for a Cloud Organization to learn which actions may be followed ahead, thanks to an external support, this clarifying on existing policies, guidelines and contracts that must be transparent to Customers buying services and to Law Enforcement.



Legal/1



Legal dimension

Multi-jurisdiction and Multi-tenancy are those main issues from a lawful PoV and the most fragile ones...

A «multi-tenant architecture» is the architecture in which we do find as many virtual boxes as for the Customers, while each Customer gets a separated data-space.

Internal regulations and contracts should be developed in order to assure forensics activities to not break the laws of the country where the data themselves are stored.

Cloud information

From a investigative level, information can be found:





Cloud information/1



SERVER SIDE:

- ✓ **Actual legislation (Italy) when executing a dataset copy from the ISP:**
- ✓ **Art. 254 bis C.P.P.** – «Sequestro di dati informatici presso Fornitori di Servizi Informatici, Telematici e di Telecomunicazioni».

- ✓ **Where the heck will we seize the data????**

Or, «block» the account (access mode)??? Despite being the *only sure thing I have, when I've got one!!!*

YOU CANNOT.

CLIENT SIDE:

- ✓ **Yeah, I may run a «live analysis».... If credentials are given out (?)**
- ✓ **When lucky, I may be able to find out access credentials and configuration templates saved «in clear text» (and/or cached) rather than into local backups..**



Methodologies



Data transit

- ✓ **Eavesdropping communication between the User and the Cloud's service? Rather than.... Injecting a spyware??**
- ✓ **As we should know, when a crime is done, it's too late to run this kind of operations.**
- ✓ **Remote acquisition? What about integrity checksums???**
- ✓ **i.e. Amazon has got all of the files's hash for those data uploaded onto (as a metadata).**
- ✓ **What about different ISPs?**



Methodologies/1



- ❑ **Network analysis: acquiring the whole network traffic of the workstation itself – when this is applicable (NETWORK DUMP).** A hash printing must be done to the acquired files.

- ❑ **Log Analysis:** acquiring and examining log files from the firewall, antivirus, application programs, possible cache and temporary directories files from the clients.
 - **Screenshots:** (not only that...)
 - ✓ Desktop screenshots;
 - ✓ Possible screenshots of running programs;
 - ✓ Reading out and commenting in «live mode».

 - **Reporting:**
 - ✓ Each single activity must be reported in the clearest way as for Digital Forensics.
 - ✓ Even more carefully, giving Cloud Forensics a very-recent science, lacking of punctual lawful practices.
 - ✓ Last but not least, a final reporting is mandatory in order to supply validity and allow legal experts to fit it into a given and correct scenario.



Access?????



What if.... we don't have credential access???



Access credentials:

- **Dropbox:** can be accessed via web if we've got the credentials.
- **iCloud:** it contains all of the saved information by a user, on all of the Apple's devices (iPhone, iPad, etc.....)





The Dark Cloud



The Dark Cloud

- ✓ CPU power to be used for distributed cracking
 - ✓ “CPU power” VS FPGUs VS Cloud
 - «paradigma»
- ✓ Targeted hacking attacks via APTs
 - ✓ Spear Phishing/Whaling towards technical staff and Cloud’s ISPs Management
- ✓ Web Applications Hacking: see Mario XXXX’s job VS Amazon, Google etc...
- ✓ (in a nutshell): cloud-based (also on the “Web App” side rather than “Mobile App” or “SaaS”)
- «templates»: one hole, a million (?) victims.





Antiforensics



Antiforensics

All of those techniques, tips and «methodologies» that may be able to slow down and/or «stop» the finding for digital evidences.

«Cloud» is *by default* a Antiforensics methodology (at least, it gives us tough times!!! ;)





Conclusions



✓ **Each scenario (environment) is different.**

✓ **The investigator (Law Enforcement) and the consultant are called in for new challenges + develop new approaches.**

WITHOUT BECOMING A «LAST-MINUTE» DIGITAL FORENSICS EXPERT!!





Links



- <http://uobrep.openrepository.com/uobrep/bitstream/10547/326231/1/hewling.pdf>
- http://www.cftt.nist.gov/disk_imaging.htm
- https://www.academia.edu/7768658/Actionable_Evidence_in_the_Wake_of_Anti-Forensics_on_Windows_8_Systems
- http://ac.els-cdn.com/S1877050914012113/1-s2.0-S1877050914012113-main.pdf?_tid=fb848980-7551-11e4-8648-0000aacb35e&acdnat=1416995750_8ff475d9db450e5724b169e154496169
- <https://www.guidancesoftware.com/products/Pages/tableau/products/duplicators.aspx>
- http://www.cftt.nist.gov/tool_catalog/index.php
- <https://digital-forensics.sans.org/summit-archives/2012/practical-use-of-cryptographic-hashes-in-forensic-investigations.pdf>
- <http://www.ltr-data.se/opencode.html/#ImDisk>
- <http://www.forensicsoft.com/index.php>



Links



- <http://www.mitec.cz/wfa.html>
- <https://code.google.com/p/thumbcache-viewer/>
- <http://www.iisfa.it/>
- <http://www.cftt.nist.gov/>
- <http://www.marcomattiucci.it/>
- <http://www.ictlex.net/>
- <http://www.deftlinux.net/>
- <http://www.caine-live.net/>



Links



<http://www.e-evidence.info/>
<http://www.forensicswiki.org/>
<http://www.forensicfocus.com/>
<http://www.opensourceforensics.org/>
<http://www.nirsoft.net>
<http://www.tzworks.net>
<http://redwolfcomputerforensics.com>
<http://www.mitec.cz>
<http://www.woanware.co.uk>
<http://www.sysinternals.com>
<http://www.passwordforensics.com>



Standardization



NIST CFTT (Computer Forensics Tool Testing)

<http://www.cftt.nist.gov>



Books

- “File System Forensic Analysis” (Carrier) – Wesley – 2002
- “Windows Forensic Analysis” (Carvey) – Syngress – 2009
- “Windows Registry Forensics” (Carvey) – Syngress - 2011
- “Computer Forensics” (Ghirardini, Faggioli) – Apogeo – 2009





Common issues (general view)



1. *Lack of knowledge*
2. *Law Enforcement behaviors*
3. *Costs*
4. *Lack of resources & Being “alone”*
5. *A case study from 1995*



Common issues: lack of knowledge



- As described in the book, among the main issues, we can find out:
 - Lack of **methodologies** and standard approaches
 - Lack of **tools** (hardware, software)
 - **Evolution of the hardware** VS the available investigative resources at that time (i.e. modem interception and devices speed/baudrate)
 - Lack of **experts!**



Common issues: Law Enforcement



- Seizes
 - Mousepads & monitors ?!?
 - Chain of Custody
- Lawyers, Public Prosecutors and Judges
 - How's the know-how of these actors in China nowadays?
- DF seen only on "computer crimes" cases (i.e. hacking)
 - Today DF can be applied to murders, kidnappings, child pornography, financial frauds, hacking incidents, insider trading, etc..
- No understanding of the basic terms (i.e. "hard drive", network, "Internet"...)
 - Nowadays (at least!) most people know what these words means (or they should...).



Common issues: costs

- The costs have always been one of the main issues when dealing with DF.
 - HW devices and SW solutions were definitely not “cheap” (this is still a problem, tough)
 - Forensics Experts costs VS Court Trial salaries
 - In Italy the fee defined by the Law Court for a DF Expert is equal to EUR 30 per day – *travel expenses included!!* (1 EUR = 8.2 RMB -> 246 RMB)
 - Well.. We do not pretend to “become rich”, right?While not even to loose money while working 😞



Common issues: being alone



- Ahead of the Internet boom, there were no “forums” or “boards” where somebody could ask for help.
- DF experts were very few ones...
 - Each one with its own “little garden” (*not loving* to share knowledge and experiences)
- The main issue here was the lack of people with whom **compare experiences and troubles**
 - Not even speaking about tools and shell scripts sharing!



Common issues: a case study (1995)



- On December 13th, 1995, the SCO (Central Operative Section of the National Police of Italy) entered at 6AM into an apartment in Turin, Italy.
- Since SCO's experience was related to Organized Crime (Mafia) and murders only, their knowledge of DF was equal to zero 😞



Common issues: a case study (1995)



- They sized **everything**:
 - Personal Computers (OK)
 - Floppy disks (OK)
 - CD-ROMS (OK)
 - General HW: modems, cell phones (**not OK**, OK)
 - Paper agendas, notepads (OK)
 - Printouts (OK)
 - Mouse (**not OK**)
 - Mousepads (**not OK!!**)



Common issues: a case study (1995)



- Furthermore, the DF analysis was executed as follows:
 - No Chain of Custody (**not OK**)
 - Manual signatures of the “tree” command printout (+1000 pages....) from the MS-DOS shell (**not OK**)
 - The “expert” hired from the Police (local University of Turin) *directly connected* the suspect’s hard drive (HP 5” ¼ 2 GB size) to its PC (**not OK**)
 - He wrote his report directly on the *suspect’s hard drive* (**not OK**)
 - Generally speaking, the whole DF analysis has been carried on in a “home-made” way -> very unprofessional!



DF today



- Today's Digital Forensics become a mix of issues and never-ending, unexpected “news”
 1. Host (Intel, Motorola, Mainframes,), Network, Mobile, GPS Navigator's Forensics
 2. “Weird” forensics (see next)
 3. Common issues (see later)
 4. Forensics Labs?
 5. Mobile Forensics
 6. Encryption
 7. A recent case study on Child Pornography & the Investigation Approach



“Weird” DF



- During my career the DF teams I worked with encountered **a lot** of “weird” requests
 - Sun Solaris Enterprise 10000
 - VAX/VMS
 - Sony Playstation, XBOX
 - Cloud Forensics (we’ll speak about this later)
 - Web Applications-related hacking crimes



Common issues



- There are a lot of issues when dealing with DF nowadays.
 - *Operating logistics* + geographically distributed DF teams (when executing seizure operations for/with the Law Enforcement)
 - Too many competitors VS few real experts (proving a *effective and real* field experience)
 - The “Big 4” joined in (from financial fraud analysts to DF experts)
 - HW&SW **cannot** replace human brains (i.e. Encase *won't fix* all of your problems!; you **do not mandatory** need a write blocker device!!)
 - Needed HW&SW is (still) too expensive 😞



Digital Forensics Lab(s)



- Building a DF lab means *technologies*, not products!
- Some people think that you *just can buy the right spare parts*. It's like a "shopping list":
 - ✓ A PC with Encase
 - ✓ "Some" Write Blockers
 - ✓ "Some" Terabytes
 - ✓ A software for mobile forensics + expansive CelleBrite UFED suitcase
 - ✓ That's it, ready to go!



Digital Forensics Lab(s)



- This kind of approach it's not totally wrong, but ...
 - your operating system is your enemy
 - you are tied to the limits of your software
 - you could become an “expert” using Encase/”UTK/FTK”/whatever but you are lost outside of your “environment”



Digital Forensics Lab(s)



Operating system troubles

- Microsoft Windows is a **desktop** operating system (oh, really ?? ;)
- It tries to help you (I said “it tries”, blue screen, viruses, malware, DLLs troubles are just some “incidents”).
- It doesn’t care about “changing the evidence” (?), “reading external media”(??), “mounting read only”(???), and so on...
- If you choose Windows, your operating *is your first enemy*. First of all you have to *defend yourself from it*.
- You need specific software/hardware to do this.



Digital Forensics Lab(s)



- You could have bought the best software in the world but the possible variations are TOO MANY, not mentioning our old friend Mr. Murphy ;)
 - Exotic architecture (just a simple AS/400 is enough sometimes)
 - Strange cases (not just those “easy-to-process” child pornographic file exchanges)
 - Software “ad hoc”
 - New technologies



Digital Forensics Lab(s)



- **Investigations are becoming bigger and wider**
 - Today's home user's hard drives are huge
 - Sometimes you have to collect (and deeply analyze!) dozens of computers to reach the evidence of a crime
 - Spreading data over dozens of external drives/server/whatever is dangerous and will slow down all your work
 - Also, “some machines” linked up together won't be enough...



Digital Forensics Lab(s)



- You must buy a back-end:
 - One or more server
 - You must upgrade your software to some sort of “enterprise edition”
 - You must choose between “having more servers but paying expensive licenses” or “saving license’s money and investing for a big server with an huge storage (SAN)”



Building a Digital Forensics Lab



- So we tried to *plan a new approach* for a computer forensics lab
- Our guidelines were:
 - Opening to every kind of digital evidence
 - Opening to raw or well documented formats
 - Opening to new technologies
 - Open Source everywhere (where possible)
 - Cheap hardware
 - Security
 - Redundancy



Building a Digital Forensics Lab



- First, we looked for the technologies:
 - GNU/Linux
 - OpenAFS
 - Live-CD Linux distributions (i.e. DEFT from Italy, with a Chinese-language installation guide: download it!!! - <http://www.deftlinux.net/>)
 - Cheap Hardware



Building a Digital Forensics Lab



- **GNU/Linux:**

- It's Unix: it's stable, it does what YOU want and not what *it wants*, it doesn't have wizards, witches, goblins or so on...
- It has the best filesystem support all over the world: it can mount more than 40 different filesystems, it supports more than 18 partition schemas
- It has the widest hardware support in the world, a very good one
- Oh, *it's free!*



Building a Digital Forensics Lab



- It's true: you can't build a (**real**) computer forensics lab without a *huge* repository
- You have some choices
 - ✓ A big server with a SAN connected through a Fiber Channel or iSCSI
 - ✓ Some different servers



Building a Digital Forensics Lab



- One big server with a SAN it's a good solution but has some drawbacks:
 - You have *only one machine*. If you need to work on many cases you can *exhaust its resources* if you are working “server side”
 - On the other hand if you work client side, *you could get old* while waiting for the files to transit on cable



Building a Digital Forensics Lab



- The best solution should be having *some application servers* in the back-end *working directly on the data* (motherboard's bus are faster than networks)
- But there are some troubles:
 - If you split data on various server *it's hard to find* everything you need
 - It's hard to find *sharing protocol smart enough...*
 - NFS is horrible: it's too server oriented, it hasn't good security (NFS stands for "Not For Security" as I often love to remind to my colleagues ;)
 - SaMBa is too complex to administer, it has security problems, it doesn't scale up well, it's too tied up with Microsoft's humors...
- So, we went hunting for something that would eventually fit our (weird, very specific) needs 😊



Building a Digital Forensics Lab



- **OpenAFS is an amazing technology!**
- It's a unique network filesystem
 - It was born as academic project (1989!)
 - IBM owned it for 10 years
 - It's Open Source since 2001
 - It's used worldwide... Fortune 500, IBM, CERN, IHEPs, Universities... more than 250 public cells on the Internet...



Building a Digital Forensics Lab



- OpenAFS is a global, federated, location independent open source storage system that provides pervasive data access from a broad range of heterogeneous devices scaling from handsets to super computers.



Building a Digital Forensics Lab



- Broad platform support
- UNIX
 - MacOS 10.3-10.8, Solaris (Sparc and x86) 7-11 and OpenSolaris
 - AIX 5.1-5.3; HPUX 11.0, 11i, 11i v2, 11i v3; IRIX 6.5;
 - NetBSD, FreeBSD and OpenBSD (server only)
 - Linux 2.4 and 2.6 (through .24) kernels
 - Fedora Core 3-7, RHEL3-5, Debian and others
 - Microsoft Windows
 - 2000, XP, Server 2003, Vista, Server 2008 (32-bit and 64-bit)
- 250 Public Cells (and an increasing number of known private cells)
- Growing number of developers
- Partnerships with academic CS departments



Building a Digital Forensics Lab



• OpenAFS Strengths

- Unified named space (like “CIFS”: but it works ;-P)
- WAN friendly
- NAT capable
- Authentication, Authorization, and Auditing
- Change notifications
- Distributed administration
- High availability
- Maintenance without downtime
- Data consistency



Building a Digital Forensics Lab



- **From a DF point of view:**
 - ✓ Building an HUGE repository with common hardware
 - ✓ Easy to find everything
 - ✓ Secure!
 - ✓ No downtime
 - ✓ Replication (see above)
 - ✓ Works well with BIG files
 - ✓ Works well with various architectures



Building a Digital Forensics Lab



- We built **two different Labs** with OpenAFS:
- Every single machine works both as a *OpenAFS node* and as an *analysis workstation*
- Every single computer is reachable through **SSH**, also with graphics (X-Window)
- *FreeNX* is an another interesting technology:
- Works well with low bandwidth
- It has the concept of “suspension” and “detached session”, like *screen*



Mobile Forensics

- As previously stated, Mobile Forensics is (already) the new DF's frontier.
- Reasons?
 - **Everyone has got a mobile phone!** (one at least)
 - Even poor countries / emerging ones (Africa, India, Brazil, etc..)
 - Today's mobile phones are just "fully-equipped PCs":
 - Powerful CPUs, Internet access (broadband), Camera, "Keyboard", Color display
 - Mobile phone users store important/critical information onto it:
 - Contacts/phone numbers
 - Personal picture/videos
 - E-banking
 -
 - Cybercrime easily realized how to heavily launch attacks towards them:
 - Zeus (and all of its variants)
 - Android , iPhone, Symbian, Windows CE, Windows Mobile malwares
 -



Encryption



- No matter if we're speaking about standard PCs, tablets or Mobile Phones.... Encryption tools are (somehow) easily available to everyone.
- This is a true pain/big problem for DF experts...**just like “the Cloud”** (as Dr. Fred Cohen pointed out earlier)



Case study: Child Pornography (and the Investigation Approach)



- Fighting Digital Pedophilia: **the “FDB” investigation case.**
- This case study is very interesting and **useful** because:
 - It shows the **power of combining** digital and real-life evidences
 - It shows the **power of a good investigation + Court trial strategy** by the General Attorney to solve the case
 - It has been **the first case in Italy** where a private DF lab and the Computer Crime Police Department (Italian Postal Police) worked together side-by-side



WARNING



- This case study reports real-life evidences from a Digital Pedophilia investigation.
- Some slides will show images that could offend the audience's sensibility.
- If you do not want this, please get out of the room now. Thanks.
- **NOTE: *this case study will not be included in the public release of this presentation***



Case study: the “FDB” investigation

- “FDB” is an Italian citizen, 55 years old, male.
- At this time he is jailed in Italy. The General Attorney obtained from to the Court a **grand total of 14 years of jail**. His crimes have been:
 - Children sexual abuse
 - Sexual Tourism (Italian law n. 28/2006)
 - Owning, spreading and creation of children pornography material



Case study: the “FDB” investigation /1

How this investigation began?

- A covert policeman exchanged child pornography images with “Mr. W” .
- Mr. W ADSL gets wiretapped.
- General Attorney said she *didn't want to spend time & money* just to trace “another child pornography pictures uploader”



Case study: the “FDB” investigation /2

- GA (General Attorney) asked to the police to *focus the investigation* on chat, emails, IM and any other mean of communication Mr. W may use.
- After one month of investigation, Police showed that Mr. W was one of the *most active commercial traders* for child pornography material around Europe.
- GA asked the Police to learn everything they could about Mr. W contacts.
- **Amont those contacts, one was FDB...**



Case study: the “FDB” investigation /3

- **First goal** hit by DF:
 - Mixing those data from IM logs and e-mail headers, we were *able to track FDB’s source IP!*
- FDB *didn’t use* its home Internet connection though.
 - Indeed, he did “all the job” from his work office.
- Police arrested him when at work, finding him *live* sharing child pornography material through P2P networks via E-mule.



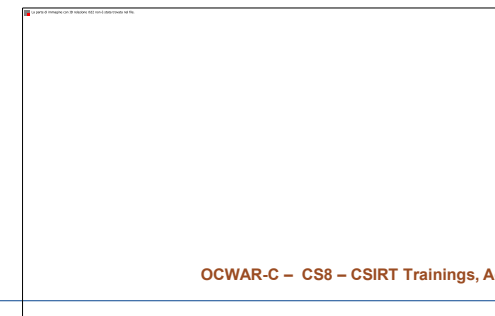
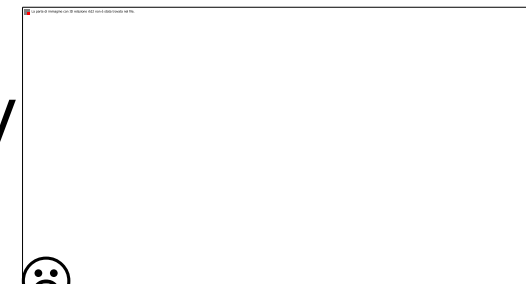
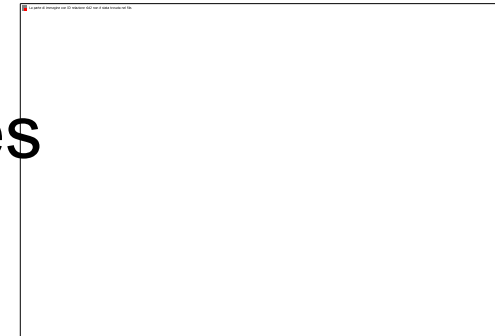
Case study: the “FDB” investigation /4

- Police seized the following material:
 - From the work office:
 - One PC
 - Three hard drives
 - From FDB’s house:
 - One PC
 - Two hard drives
 - 1.500 CDs and DVDs
- Along the **first month** of DF analysis & evidences gathering, we found:
 - **1.500.000 child pornography images**
 - **More than 300 children abuse videos**



Case study: the “FDB” investigation /5

- We had a real, big problem, tough...
- We’ve found out multiple minors’ porno images where an adult male was having sex with different teenagers, in different revealing sex positions.
- Nevertheless, *the face of the male subject was hidden by black paint.*
- We had *strong suspect & feelings* that the guy was FDB...
 - We didn’t have any evidences proofing this, tough 😞





Case study: the “FDB” investigation /6

- Among the evidences we brought to the Police and to the GA, we also found out *10 different videos*.
 - In the videos, a masked male subject had intercourses with girls aged between 5 and 15 years old.
- The videoclips where filmed by accomplices present on the crime scene.
- All of the 10 videos have been filmed in *two different locations only*.





Case study: the “FDB” investigation /7

- Time was not enough: the investigation *had to be finished by a grand total of 6 months*.
- GA decided to *close the investigation* on Mr. W, then *opened a new one* against FDB:
 - FDB was indicted *only* for owning and distributing child pornography material (minor crime);
 - The GA wanted FDB to think&hope he would have been prosecuted for two minor crimes... (strategy+psychology).
- In the meanwhile, our DF team and the Police had **6 more months** in order to gain proofs of FDB abusing minors in Thailand, Laos and Cambodia



Case study: the “FDB” investigation /8

- *We wrote a tool* in order to extract EXIF data from all of the seized pictures.
- Results were then *saved into a DB*.
 - Primary keys were time/date and digital camera brand/model.
- We passed out all of the above to the Police: their mission was to join the EXIF info with airplane tickets and hotel’s receipts of FDB’s travels.
- They matched multiple images shot when the suspect was in Southern-East Asia...



Case study: the “FDB” investigation /9

- In the meanwhile my team selected some of the images in order to study them deeper and find out evidences about the head-less man identity.
- Pictures were horrible tough, from a DF point of view:
 - Underexposed
 - 640x480 to 1024x768 in the best cases!
 - Shot during night-time or in rooms with very poor light conditions.



Case study: the “FDB” investigation /10

- Nevertheless, we found something there....
 - We found *two nevis* on the left hand, both of them *located between his thumb and his forefinger*.
- ***FDB had the same nevi.***
- And, this is **not** just a “digital forensics” job: it’s an *investigative one*.
 - **As I said earlier, software & hardware can’t beat the human mind!**



Case study: the “FDB” investigation /12

- We then *approached the videos*.
- We worked with iMove (yes, the Apple’s consumer video editing software) in order to save Quicktime movies into Bitmap sequences.
- QVGA video from low-light filmings didn’t had enough screen resolution in order to show the nevi (or any other kind of details).
- We found the masked man wearing huge skin-spots on the skin on his back, tough....
- **WE HAD A PROBLEM:** *FDB didn’t have **any** spots on his back (Police checked this out).*



Case study: the “FDB” investigation /13

- Summing up what we had as **evidences that we’d been able to bring at the Court Law**:
 - Videos have been shot (also) in Thailand;
 - FDB was in Thailand at that timeframe;
 - Videos showed skin spots;
 - The body was **very similar** to FDB’s one, tough...
 - But, FDB didn’t have **any** spots at the present time ☹️
- As I said earlier, a DF expert sometimes must also be a **lucky man**.



Case study: the “FDB” investigation /14

- Police investigators suggested *some kind of health disease*.
- As I said, we have been lucky: we found a **TIFF image** with a *fax sent from Bangkok*.
 - The fax showed FDB has been guested to a hospital in Bangkok for 3 days (just one week ahead the videos have been filmed!)
 - Reason? **He was DIABETIC.**
- Diabetic people *often have large spots on their skin*, especially after a serious hit.
 - **These spots are not permanent.**



Case study: the “FDB” investigation /15

Happy ending....

- GA packed up everything and ordered to the Police to pick up FDB (he was under home arrest) and **brought him to jail.**
- GA questioned FDB for many hours in jail, until **he confessed all of its crimes.**



The Future



- The way I see the future of DF is...intriguing, while it gives me a lot to worry about!
 - *IT & TLC* will grow, grow and grow up: we're living in a *Digital World*, thus *heavily depending on the ICT*. And, **this will just get worse**.
 - *Cybercrime* has (somehow) *moved towards the "end-user"* (which is much easier to be exploited).
 - Security Incidents, financial frauds, hacks and IT attacks will *target the so-called "new technology"*.
 - (most of) these new technologies will **not** be designed with Security in mind!
 - DF will **not** always be ready on time.
 - **Laws** (and judges, lawyers, sometimes the law enforcement) **will not be ready** (always too late, very generalist approach, lack of budget, lack of trainings).
 - Just as history teach us, criminals will always be one step ahead 😞



Thank you

Contact:

Eng. Selene Giupponi

Managing Director at Resecurity Europe

Selene.Giupponi@resecurity.com



