
# Workshop
# Digital Forensics

Eng. Selene Giupponi

Head of Digital Forensics Unit

# Who am I

Resecurity

- **Computer Engineering Degree** + **Master in Computer Forensics & Digital Investigations**
- Active Member of the **IT Engineer Commission**, Engineers Association of the Latina Province
- **Digital Forensics Court Trial Witness** on e-crimes and ICT enhanced crimes
- Consultant for multiple **Law Enforcement agencies** around the world
- Advisor @ **European Courage Focus Group** – Cyber Terrorism & Cybercrime
- **ITU** Roster of Experts Official Member
- **HTCC** HIGH TECH CRIME CONSORTIUM Member
- Trainer at **NATO**, **INTERPOL**
- **CIFI** - Certified Information Forensics Investigator
- **ECSO** Founder Member
- Council Member @**Women4Cyber** Foundation
- @**Women4Cyber** Italy Founder Member – Segretario Generale
- **Managing Director Europe, Resecurity Inc.**

UNIVERSITÀ DI PARMA

# Courses and Certifications in D.F.

- 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.

# Agenda

- Key concepts of Digital Forensics.
- The importance of Digital Forensics today.
- The different phases of D.F.:
  - Identification
  - Preservation
  - Extraction
  - Analysis
  - Report
  - Chain of Custody
- Live Analysis vs. Dead Analysis.
- Other type of D.F.: 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.
- Conclusions

# 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 that the source is mentioned.

# 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

# 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 Mayor sent images of child pornography over internet


# DF –introduction/3

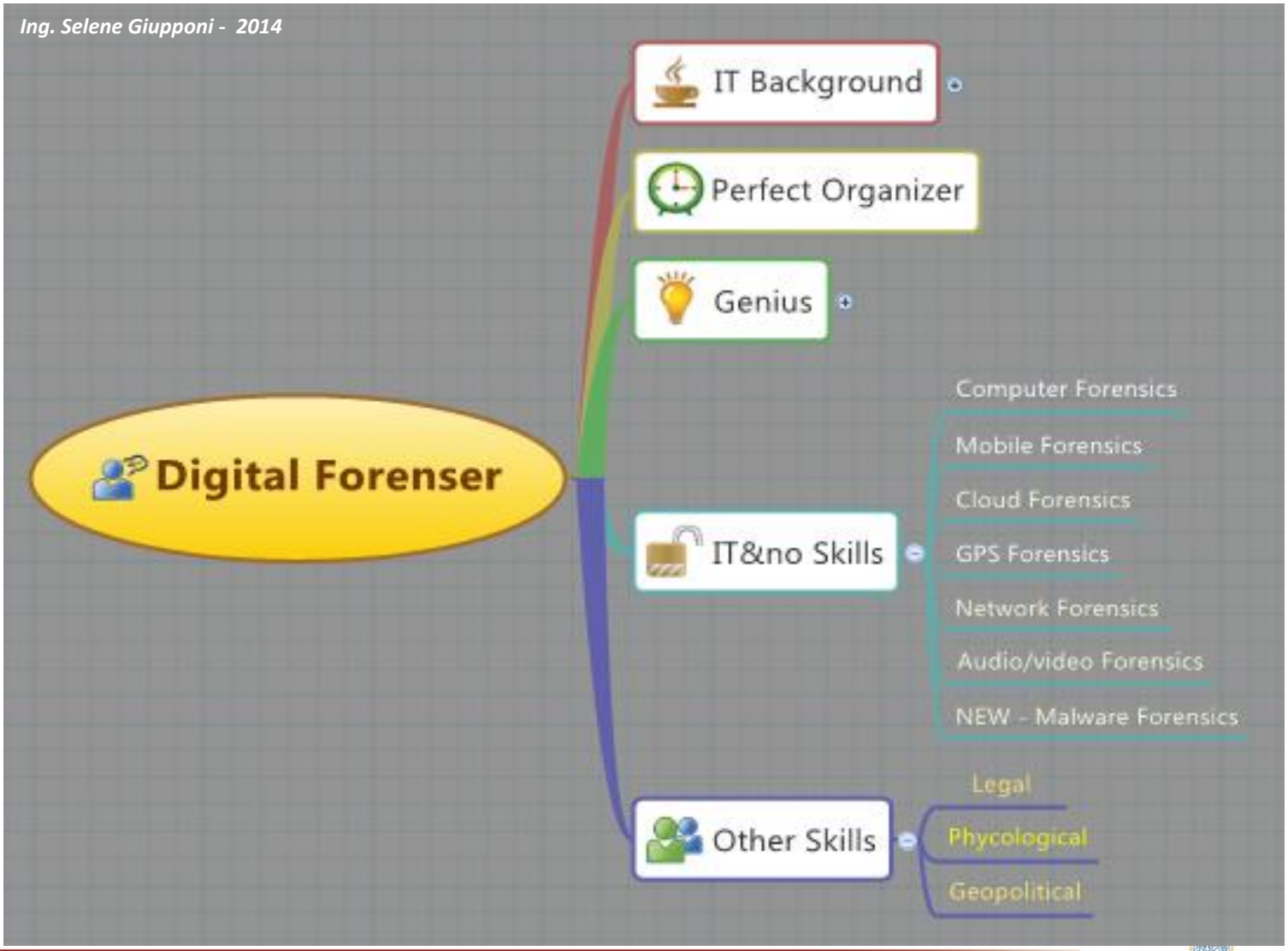
- It is therefore clear how the analysis of digital evidences is necessary even for crimes that have nothing to deal with the technology.
- **Cyberbullying** and **cyberstalking** through Facebook, and other Social Networks.
- Were not brought to the attention of the general public many other cases,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

# Use of DF Today

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

# DF – Introduction/4

*Ing. Selene Giupponi - 2014*



# Digital Forensics Introduction

- 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:

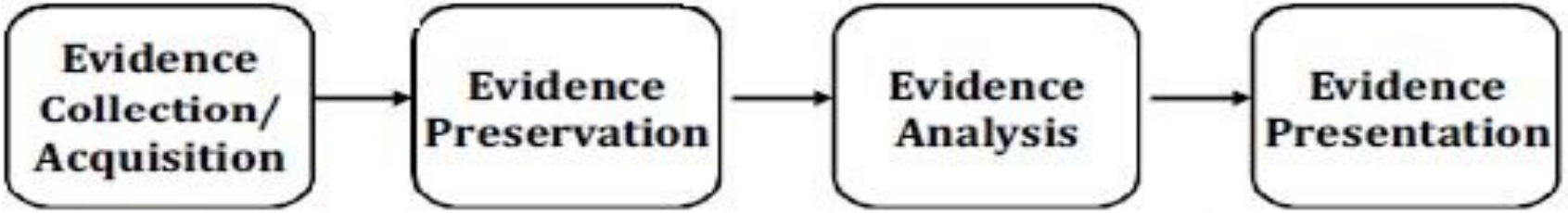
- A digital storage device
- Personal computers, notebook computers, external hard drive, floppy, tape, CD / DVD, memory card, USB drive, ...
- Mobile phones, SIM, SmartPhone, Tablet, SatNav, ...
  An Intranet / Internet
- Interception of data traffic
  Web pages, Blog, Social Network, Chat / IM, P2P,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

# Digital Forensics

**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 *storage devices*.


# Digital Forensics

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 wich 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.

# CSI - Investigations


- Goal: To explain the current state of Digital Artifact

# Digital Forensics Introduction

- 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.

# Digital Evidences

- 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

**Digital Forensics**

- **Dead Analysis**
- **Live Analysis**


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

**That's why:**

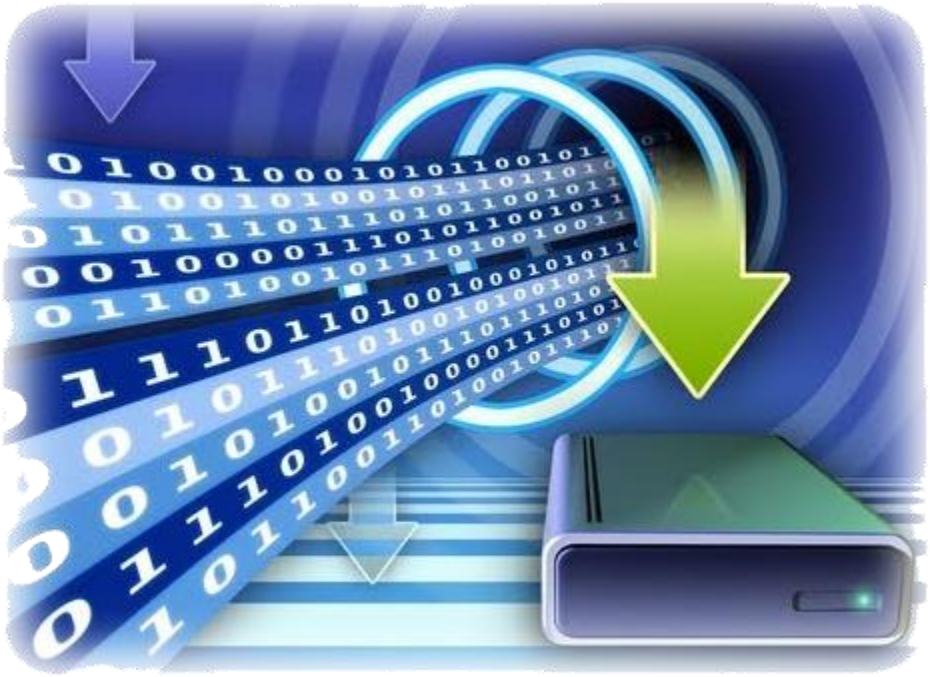
We must think about new tools, instruments and methodologies that will be be applied to the Evidence Collection & Acquisition phases.

# Digital Data

Digital data, by nature immaterial, can be typically found in the field in three different modes:

sequestered
copied
Intercepted

Any other situation can be traced back to one of these three.



# Operating steps

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

# 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)

# Hard Disk

# Hard Disk

- A hard disk is an example of non-volatile storage device
  The data is recorded magnetically on the hard disk

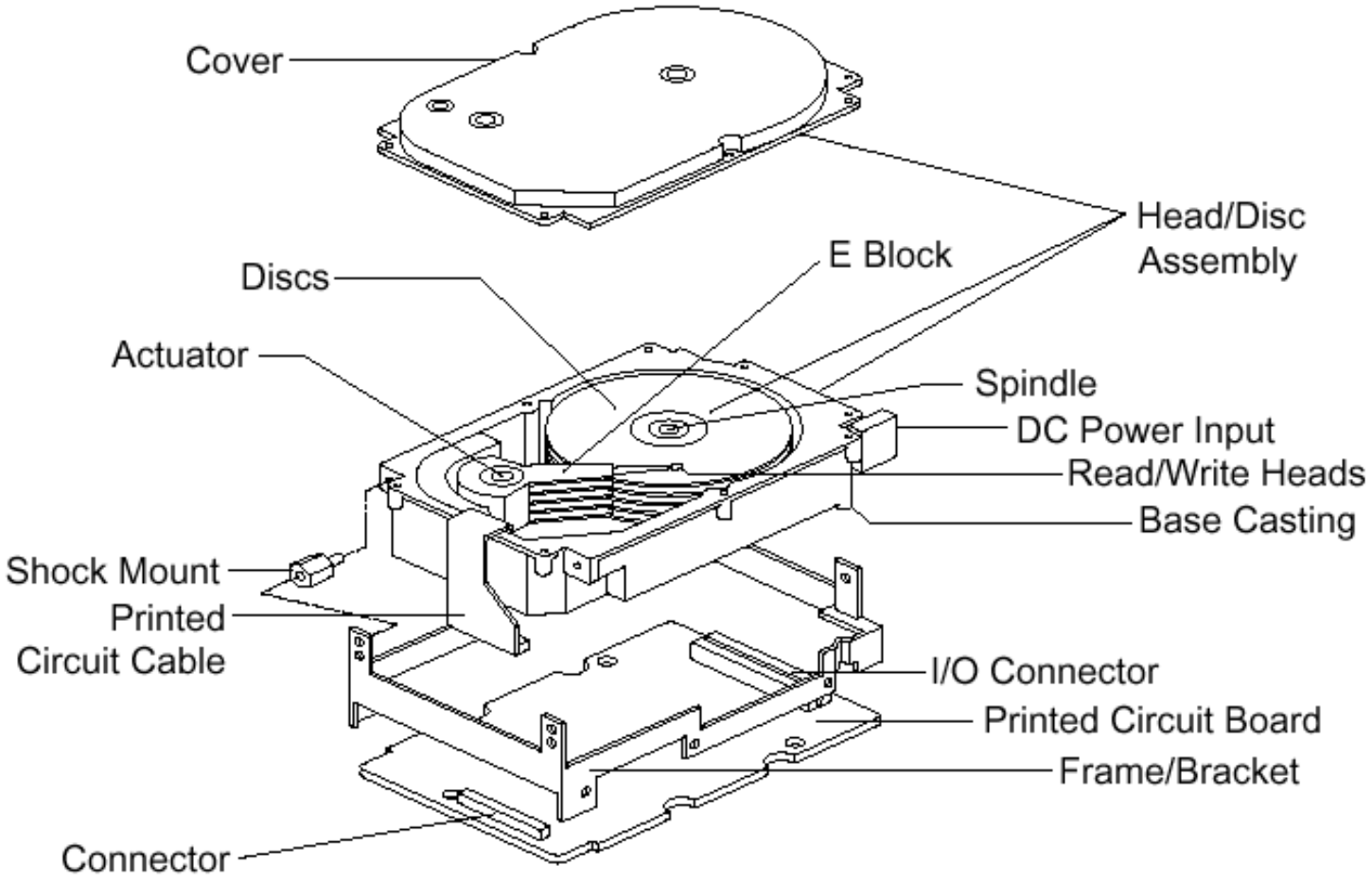
- The main components of a hard drive are:
  - Cylinders (cylinders)
  - Heads (heads)
  - Dishes (platters)

- Each plate is divided into tracks
  Each track is divided into sectors (typically 512 bytes)

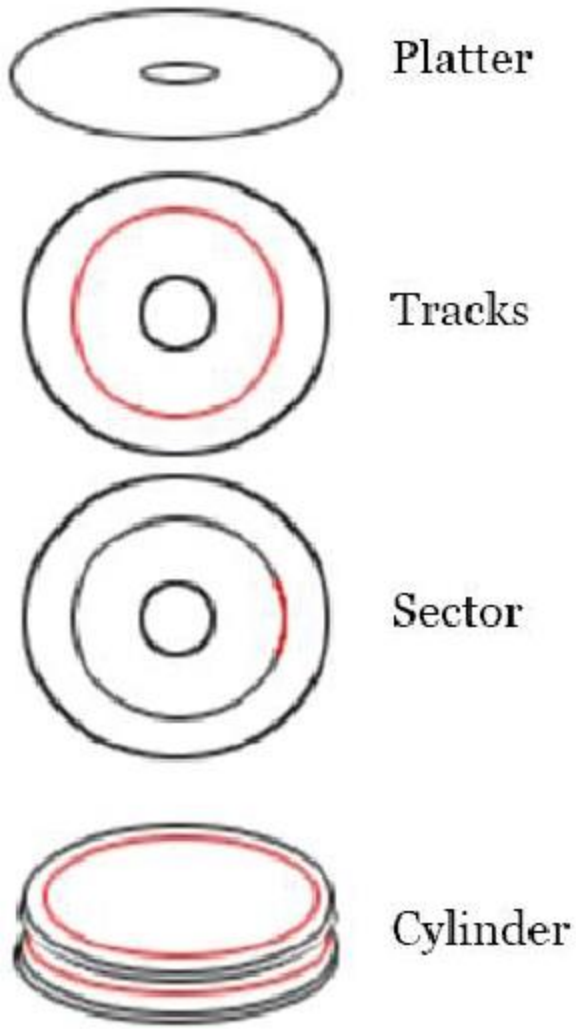
# Hard Disk

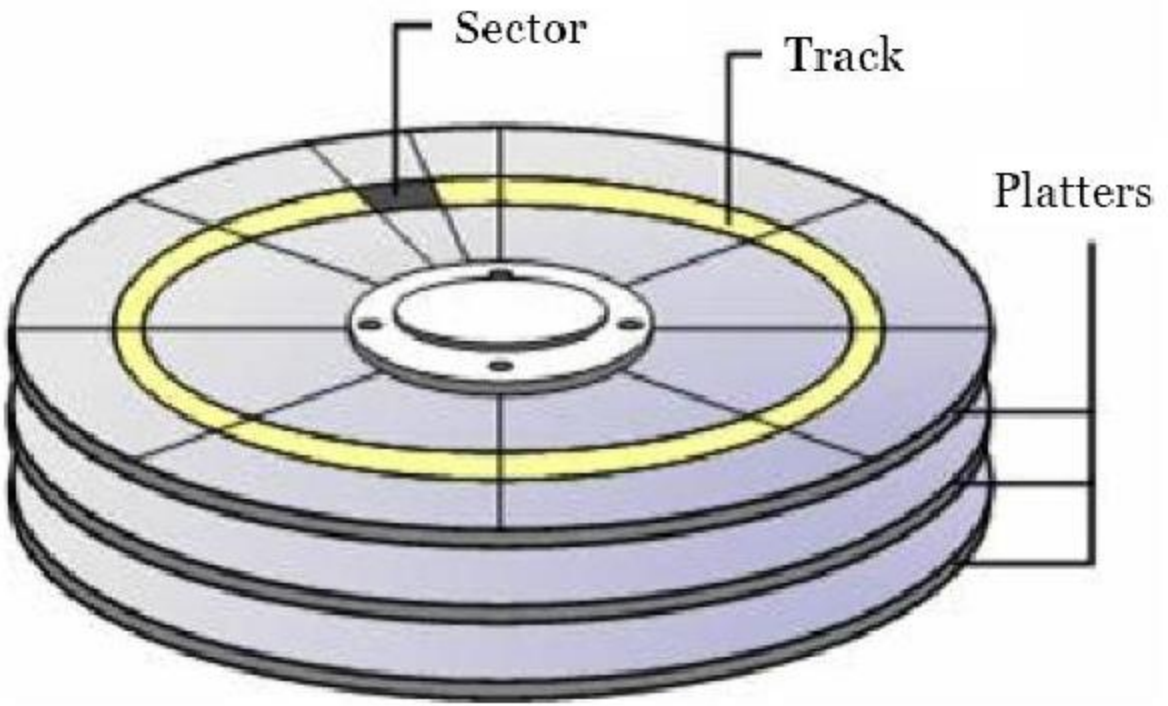
- When organizing data logic sectors are aggregated into clusters
- A hard disk is composed of a stack of plates, with read / write positioned above and below each plate
- During the rotation of the plates, the head moves from inside to outside (and vice versa) to read and write data

# Hard Disk


Cover
Head/Disc Assembly
E Block
Discs
Actuator
Spindle
DC Power Input
Read/Write Heads
Base Casting
Shock Mount
Printed Circuit Cable
I/O Connector
Printed Circuit Board
Frame/Bracket
Connector

# 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: 65mm
IDC50m (SCSI-1)
Aprox: 79mm
IDC50f (SCSI-1)
Aprox: 67mm
HD50m (SCSI-2)
Aprox: 36mm
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**

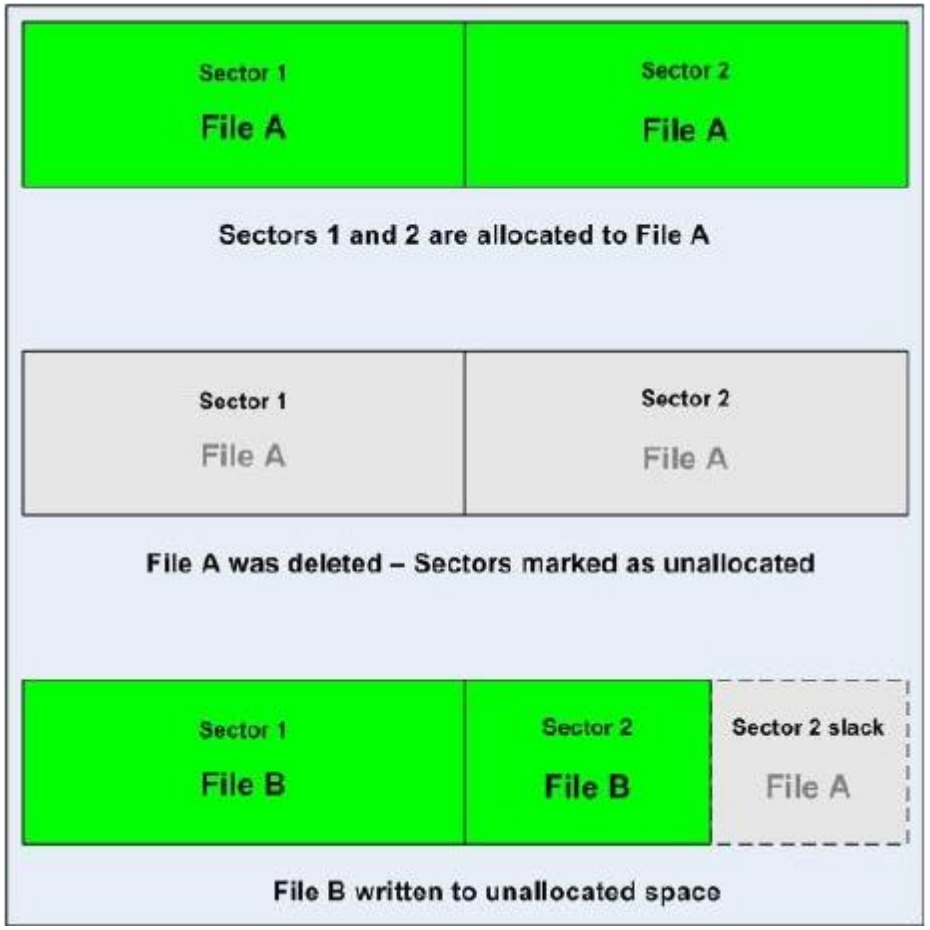
| Address | | | Description | | Size in bytes |
|---|---|---|---|---|---|
| Hex | Oct | Dec | | | |
| 0000 | 0000 | 0 | Code Area | | 440 (max. 446) |
| 01B8 | 0670 | 440 | Optional Disk signature | | 4 |
| 01BC | 0674 | 444 | Usually Nulls; 0x0000 | | 2 |
| 01BE | 0676 | 446 | **Table of primary partitions** (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, Ipod)**
- **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



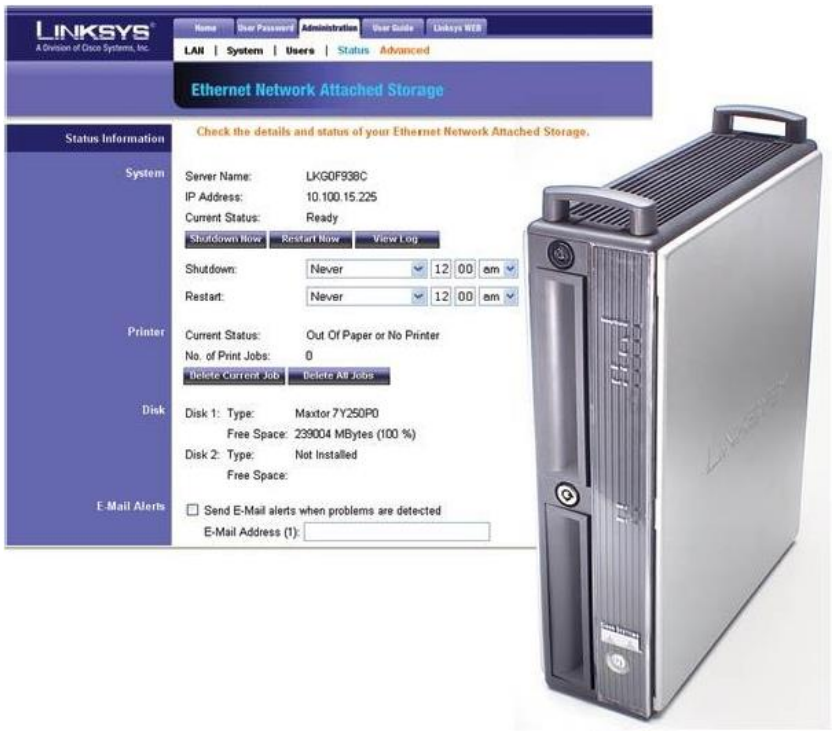
# SSD

- The 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

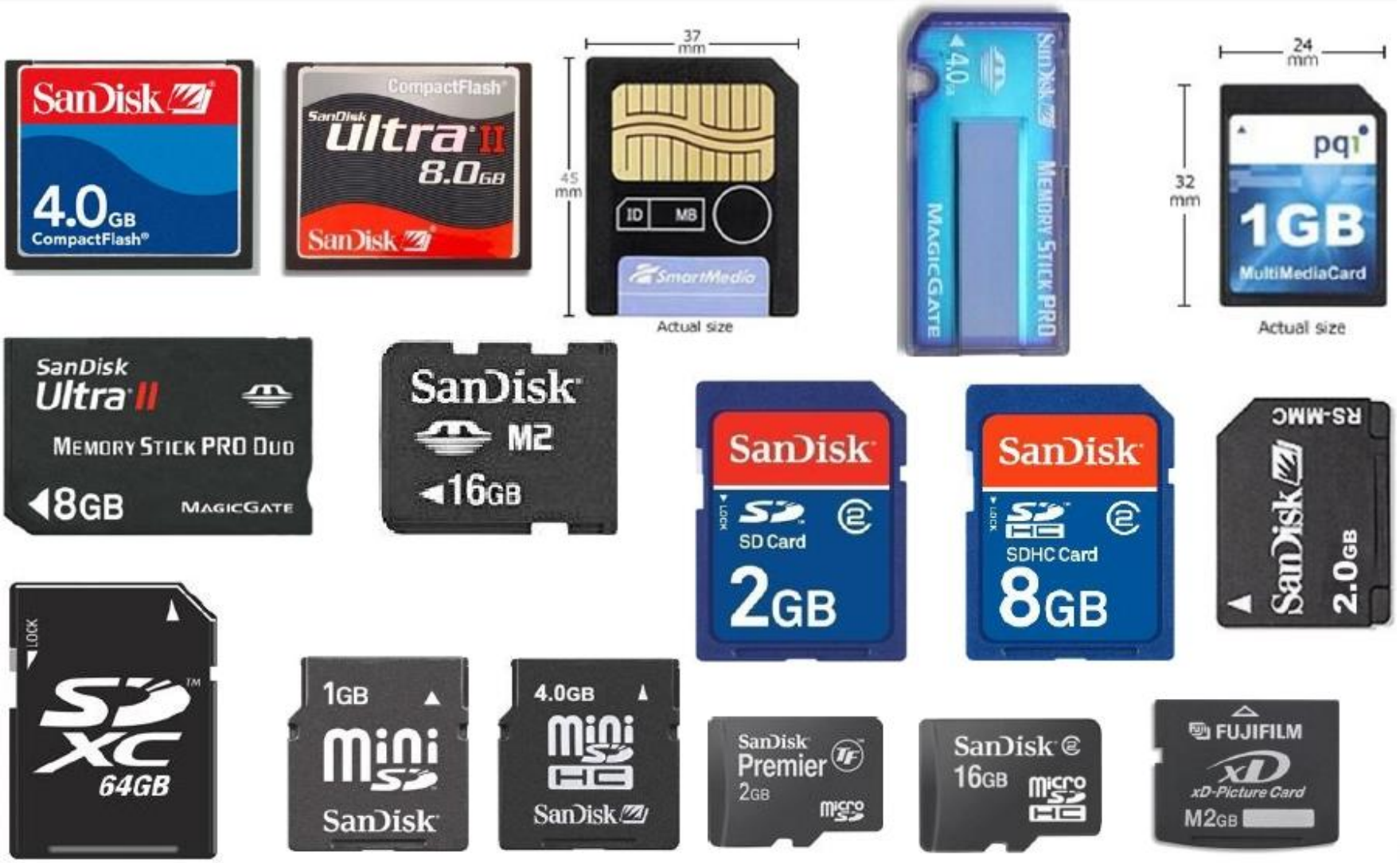


# Floppy disk, ZIP/JAZ, CD, DVD, BluRay



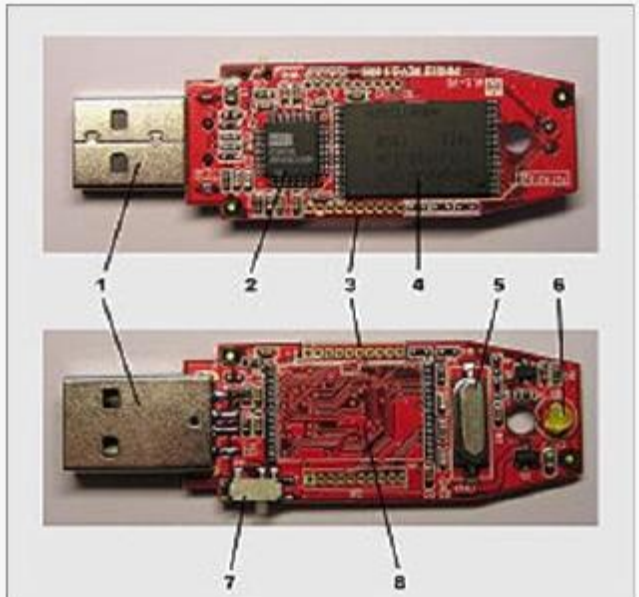



# Memory Card


SanDisk
4.0GB
CompactFlash®
CompactFlash
SanDisk ultra II
8.0GB
SanDisk
37 mm
45 mm
ID
MB
SmartMedia
Actual size
SanDisk
4.0
MEMORY STICK PRO
MAGICGATE
24 mm
32 mm
pqi
1GB
MultiMediaCard
Actual size
SanDisk Ultra II
MEMORY STICK PRO DUO
8GB
MAGICGATE
SanDisk
M2
16GB
SanDisk
SD Card
2GB
SanDisk
SDHC Card
8GB
RS-MMC
SanDisk
2.0GB
LOCK
SD XC
64GB
1GB
mini SD
SanDisk
4.0GB
mini SD HC
SanDisk
SanDisk
Premier
2GB
micro SD
SanDisk
16GB
micro SD HC
FUJIFILM
xD
xD-Picture Card
M2GB

# 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

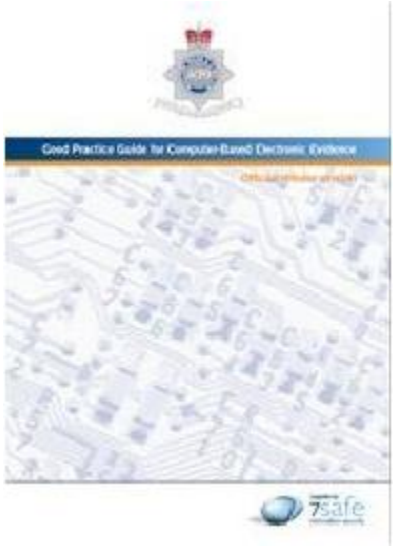
# USB

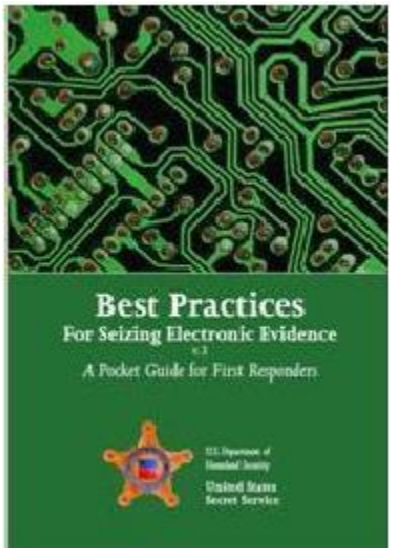

# MP3, Video cameras, Cameras, Tablet

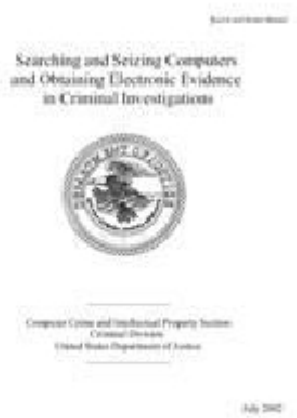



# Best Practices Internazionali

- 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




# 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***

# Best Practices for the computer turned off

- Make sure the computer is off. Some screen saver mode or the computer can bring up the computer as off when it is still running
- Remove the battery in the case of a laptop, checking first that is not in standby
- Disconnect the power and other devices from the computer side (to avoid problems in the event of a UPS)

# Best Practices for the computer turned off

- Label the ports and cables so that they can rebuild the computer later
- Make sure that all the items have been signed and compile a report for each seizure
- Search the crime scene journals, notes or pieces of paper with passwords, which are often found attached to or near the computer
- Assess whether to ask the user information on the setup of the system, including password
- Take detailed notes of all transactions carried out in relation to IT devices

# Best Practices for 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***.

# Best Practices for computer turned on

- If it is considered necessary or indispensable, extract the information that should be definitely lost by removing the current (running processes, network status, etc.) (LIVE FORENSICS)
- Ensure that all actions performed and the changes made to the system are known and recorded · If there is not a specialist to analyze live, disconnect power and other devices from the computer side (to avoid problems in the event of a UPS) without closing any program
- Remove all other outgoing connections from your computer to the network or to other external devices
- Make sure that all the items have been signed and compile a report for each seizure
- Search on the fall of crime journals, notes or pieces of paper with passwords, which are often found attached to or near your computer
- Take detailed notes of all transactions carried out in relation to IT devices

# 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

# Chain of Custody

**Corporation X**
**Security Investigations**
This form is to be used for one to ten pieces of evidence

| | | | |
|---|---|---|---|
| Case No.: | | Investigating Organization: | |
| Investigator: | | | |
| Nature of Case: | | | |
| Location where evidence was obtained: | | | |

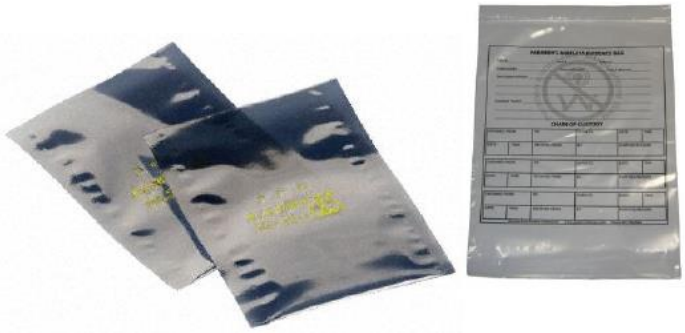
| | Description of evidence: | Vendor Name | Model No./Serial No. |
|---|---|---|---|
| Item #1 | | | |
| Item #2 | | | |
| Item #3 | | | |
| Item #4 | | | |
| Item #5 | | | |
| Item #6 | | | |
| Item #7 | | | |
| Item #8 | | | |
| Item #9 | | | |
| Item #10 | | | |

| | | | |
|---|---|---|---|
| Evidence Recovered by: | | Date & Time: | |
| Evidence Placed in Locker: | | Date & Time: | |

| Item # | Evidence Processed by | Disposition of Evidence | Date/Time |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | Page ___ of ___ |

# 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)



# Preservation of artifacts in the lab


# Operating steps

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

# Fundamental Rule

**Preserving the Original!**

# Forensics Copy

- The original must never be used for 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.scgcanada.com |
| **URL to Tool Description:** | http://www.scgcanada.com/cfid |

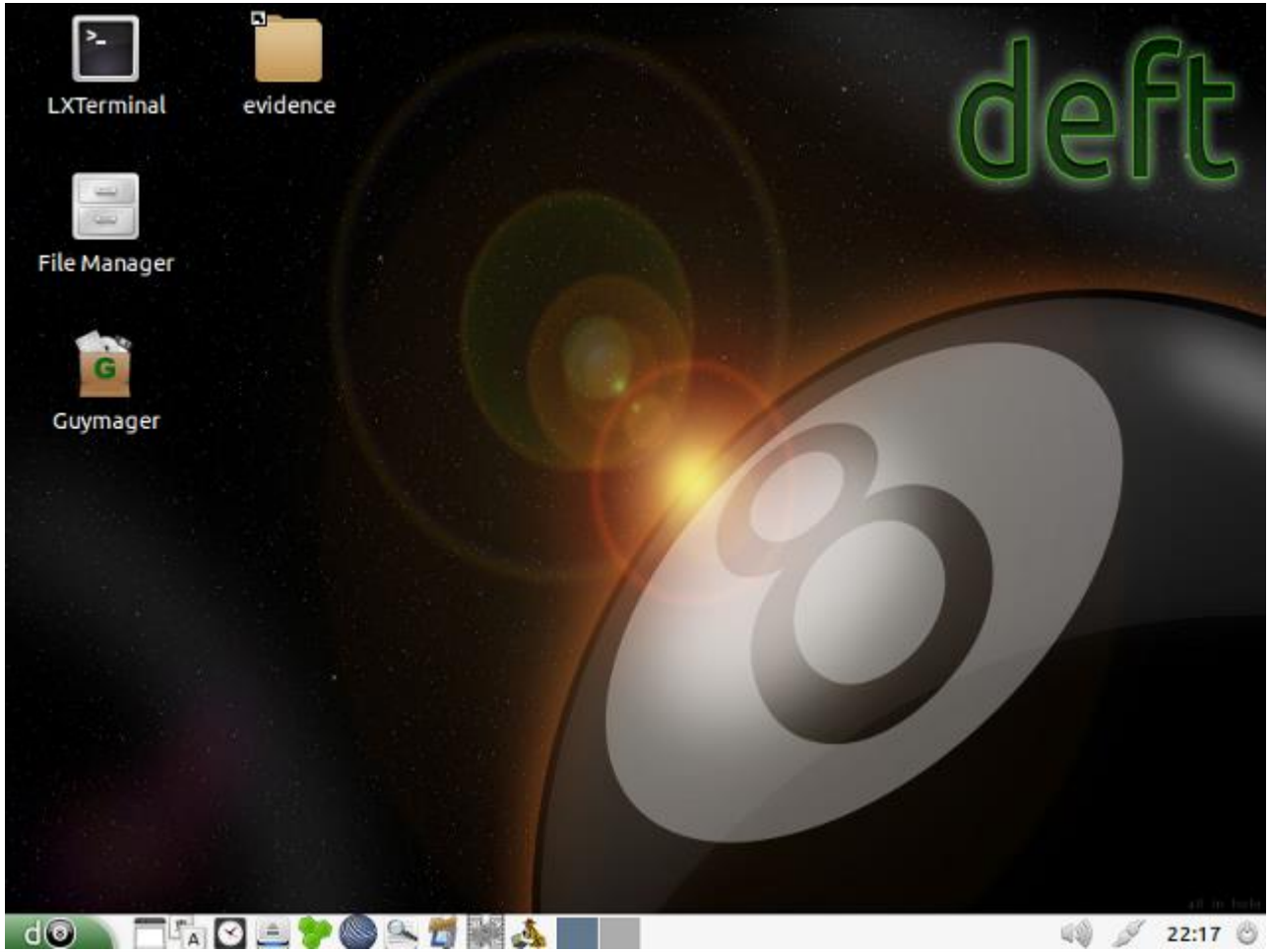
| **Technical Parameters reported by vendor:** | Tool host OS / runtime environment | Supported evidence interfaces | Supported target/destination interfaces | Types of data that may be acquired | Supported acquisition methods | Supported image file formats | Support for restoring the contents of an 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**

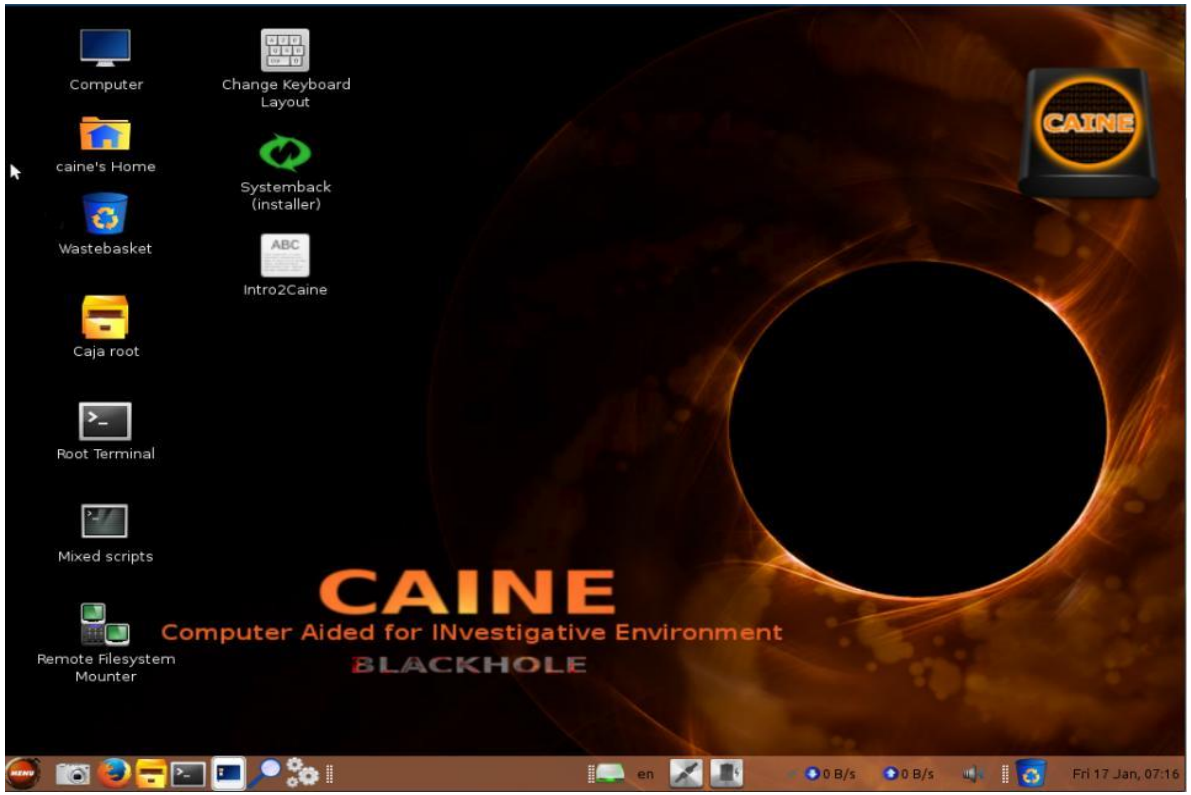
# DEFT

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



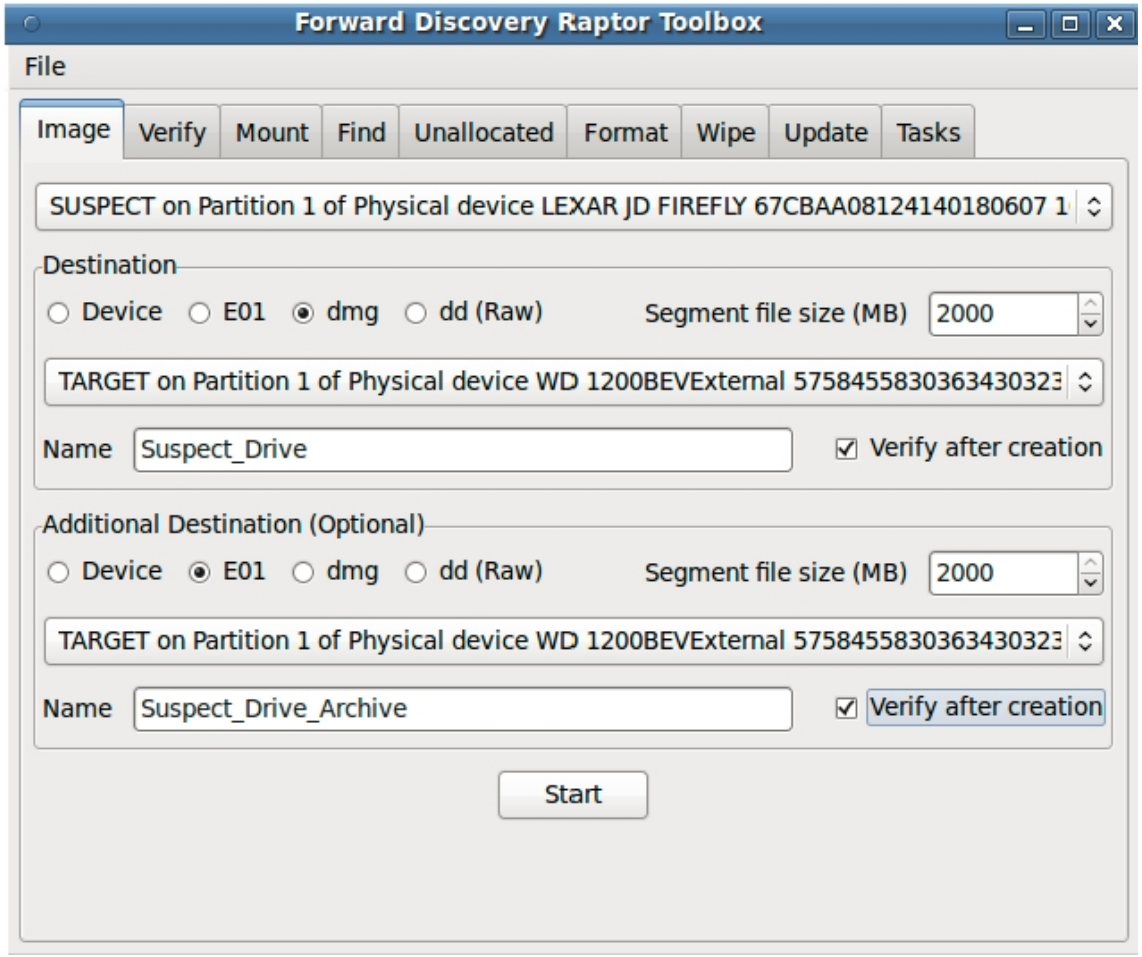
# CAINE

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



# RAPTOR

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

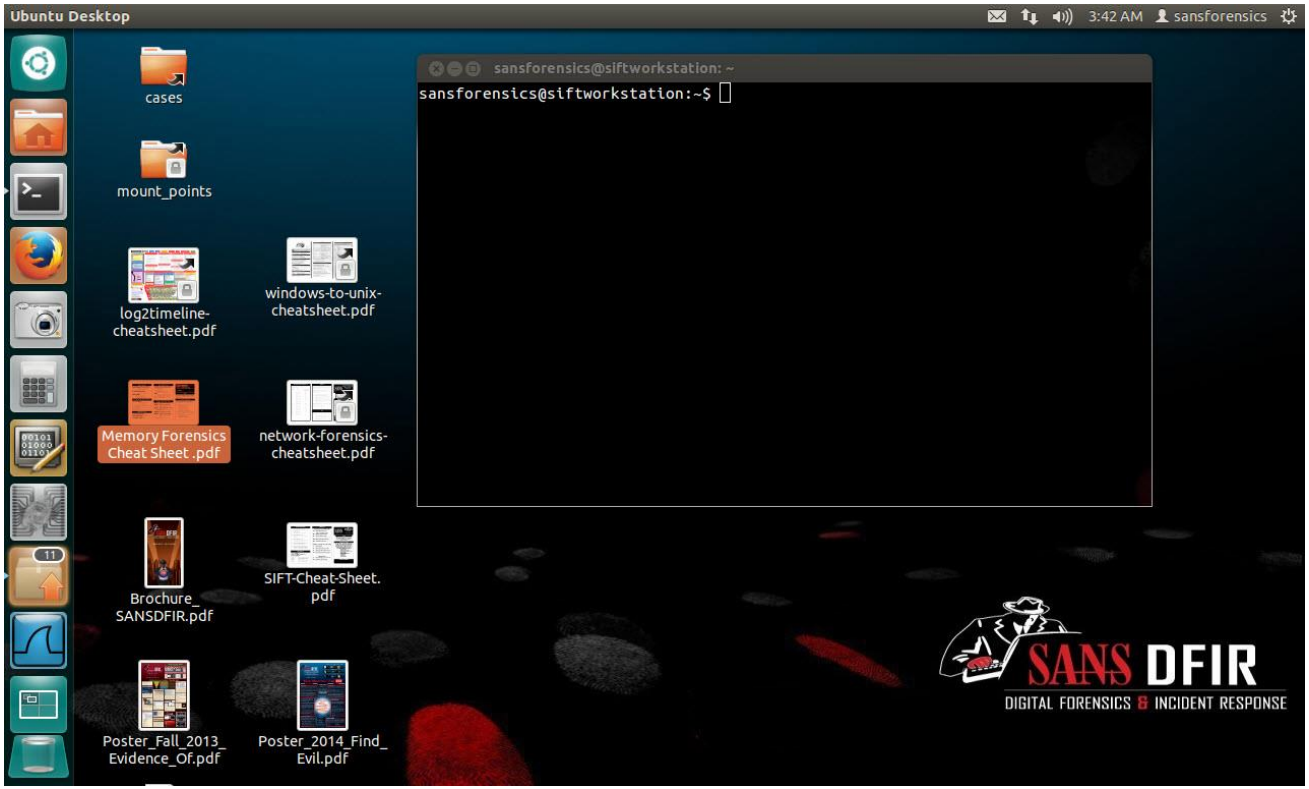


# Paladin

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

# SANS

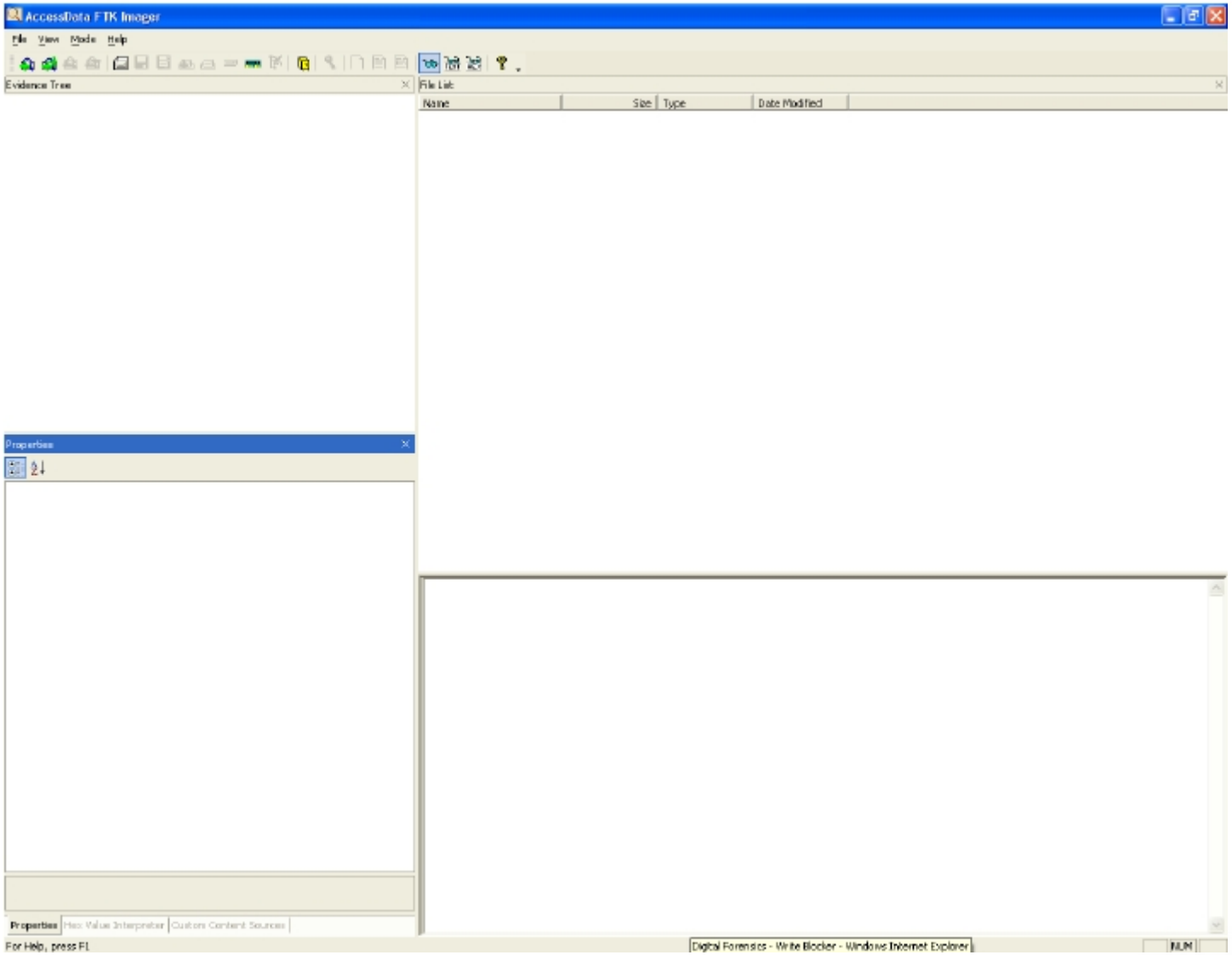
- http://digital-forensics.sans.org/community/downloads



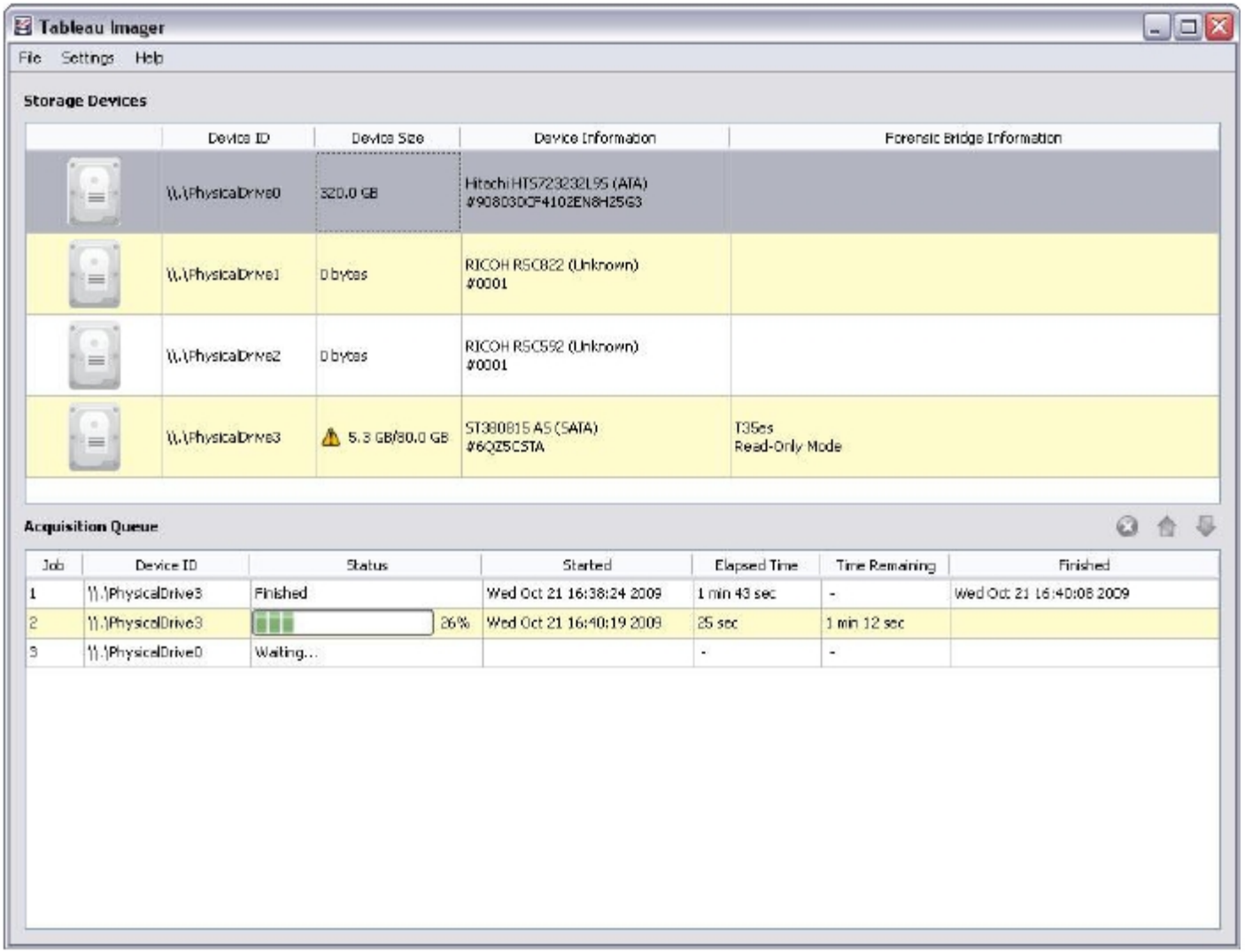
# Software Acquisition

- 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**

# FTK Imager


AccessData FTK Imager
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Properties
Properties
Hex Value Interpreter
Custom Content Sources
For Help, press F1
Digital Forensics - Write Blocker - Windows Internet Explorer
NUM

# Tableau Imager



# 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 or modify of a file)



# Hardware vendors

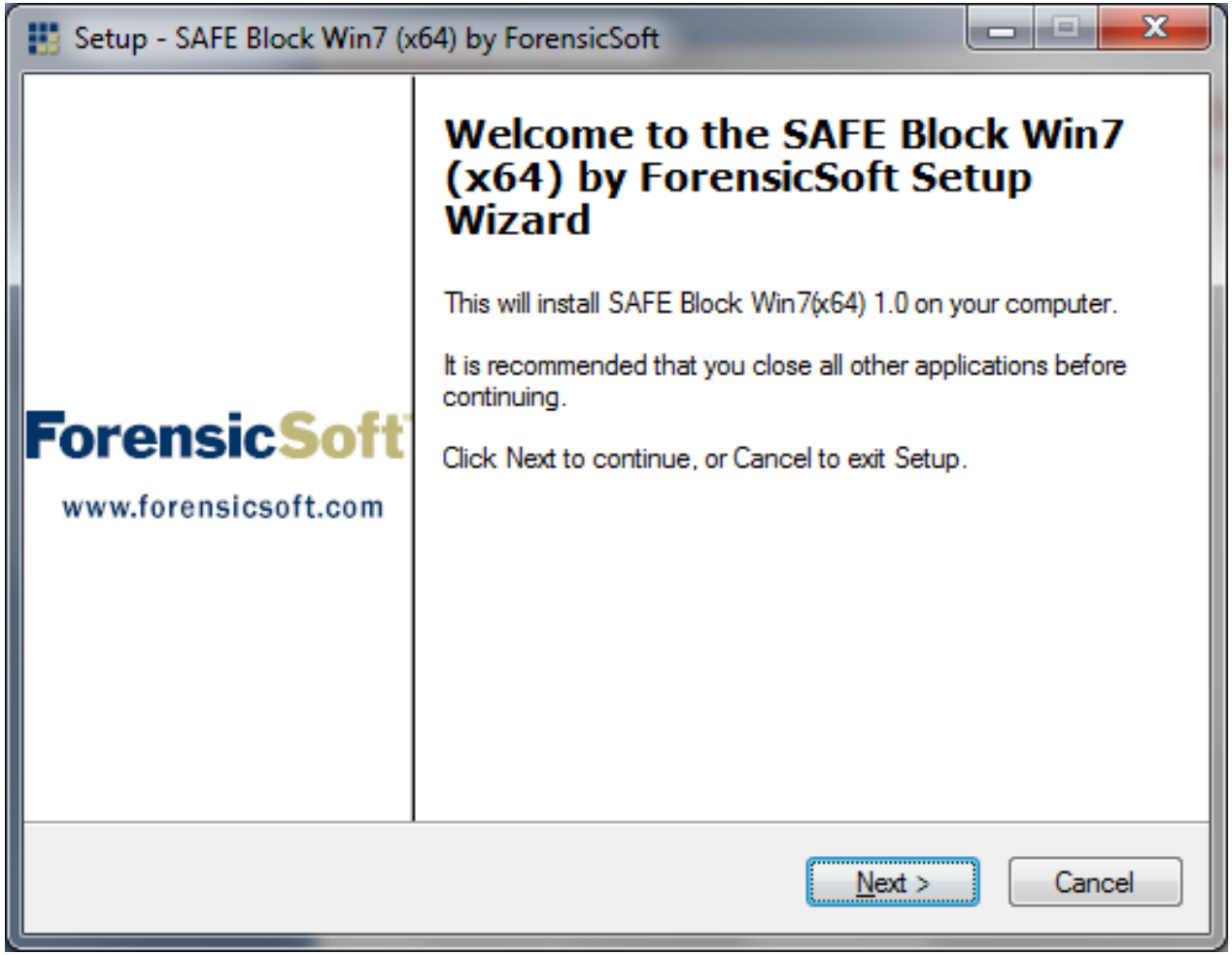
- The principal manufacturers of hardware for digital forensics are:
- **Tableau** - http://www.tableau.com/
- **Logicube** - http://www.logicubeforensics.com/
- **Intelligent Computer Solutions** - http://www.ics-iq.com/
- **Wiebetech** - http://www.wiebetech.com/
- **Voom Technologies** - http://www.voomtech.com/
- **MyKey Technology** - http://www.mykeytech.com/
- **ForensicPC** - http://www.forensicpc.com/

# Write Blocker Software

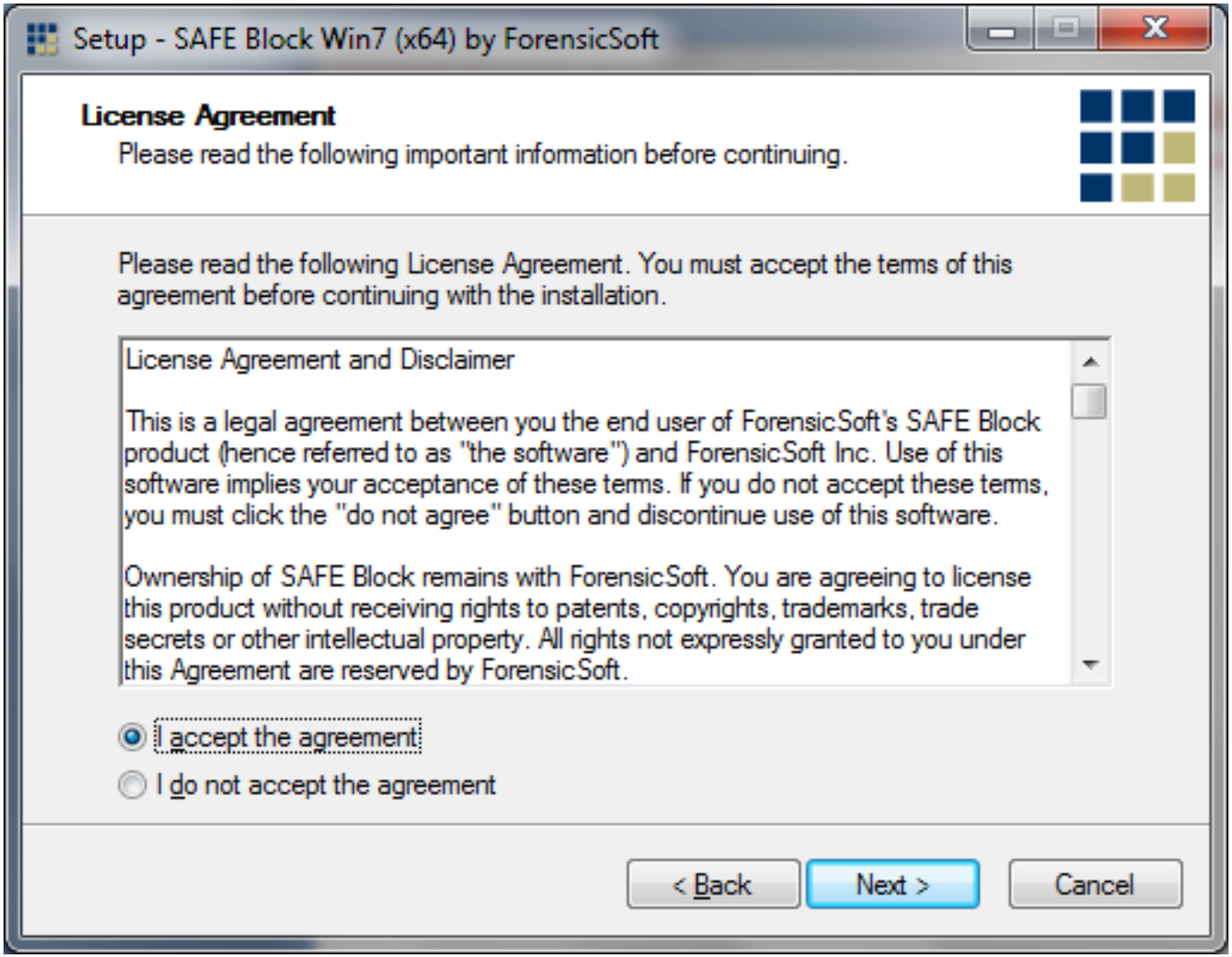
- The write block at software level it may get used on the operation of mounting the hard disk from the operating system.
- Depending on the operating system used on the acquisition forensics machine, you can take proper precautions to prevent the bidirectional flow of communication and allow access 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

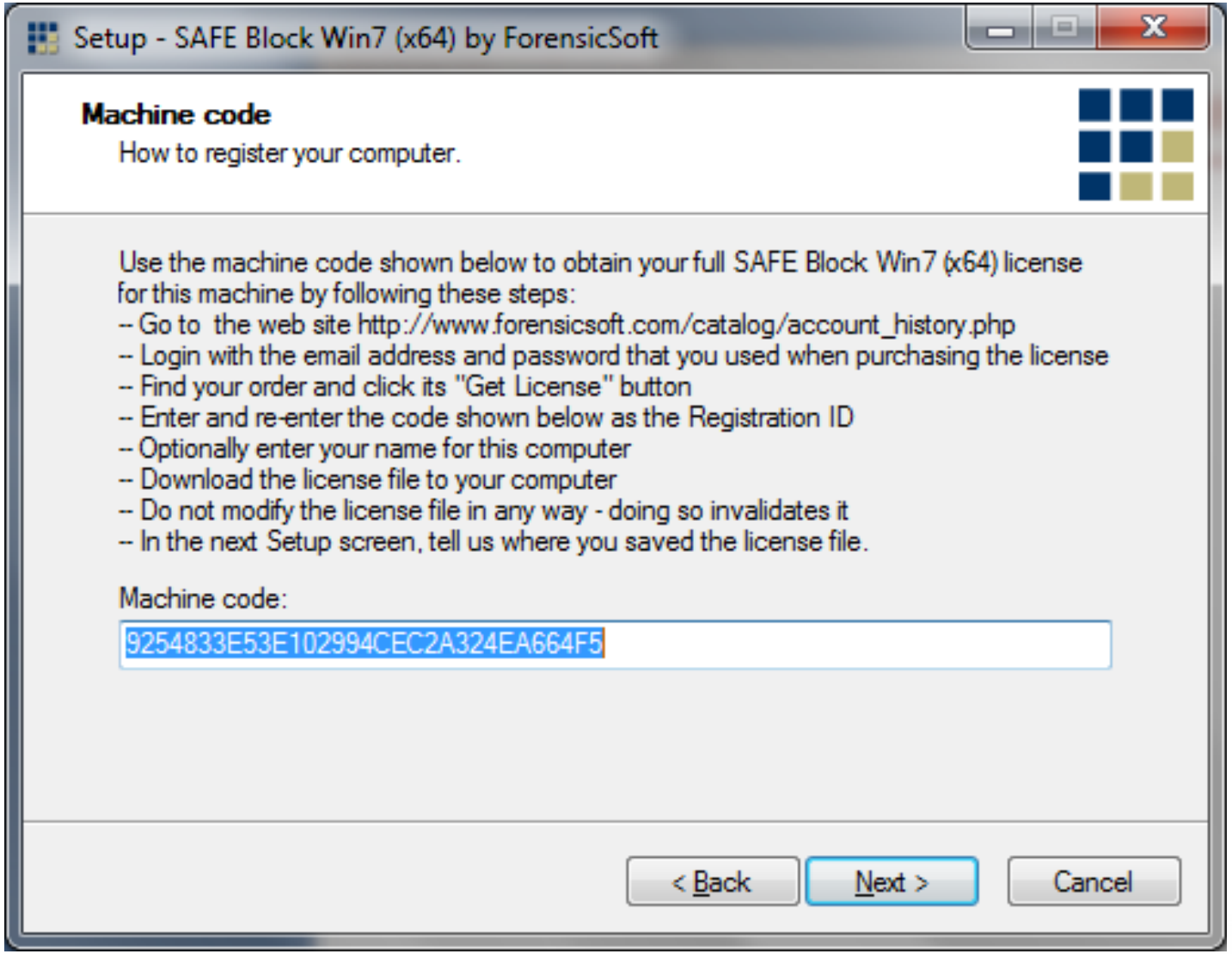

# Write Blocker Software



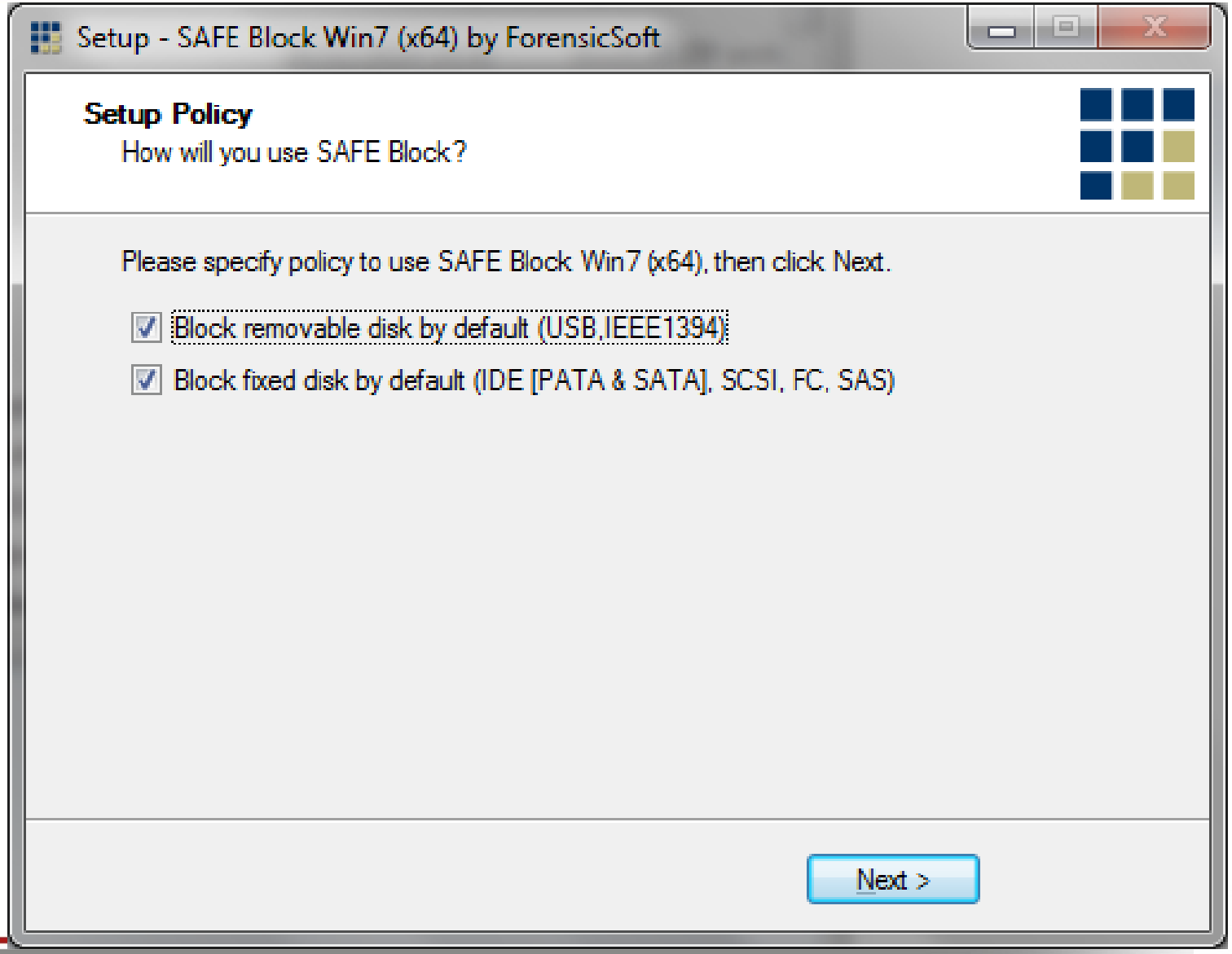
# Write Blocker Software



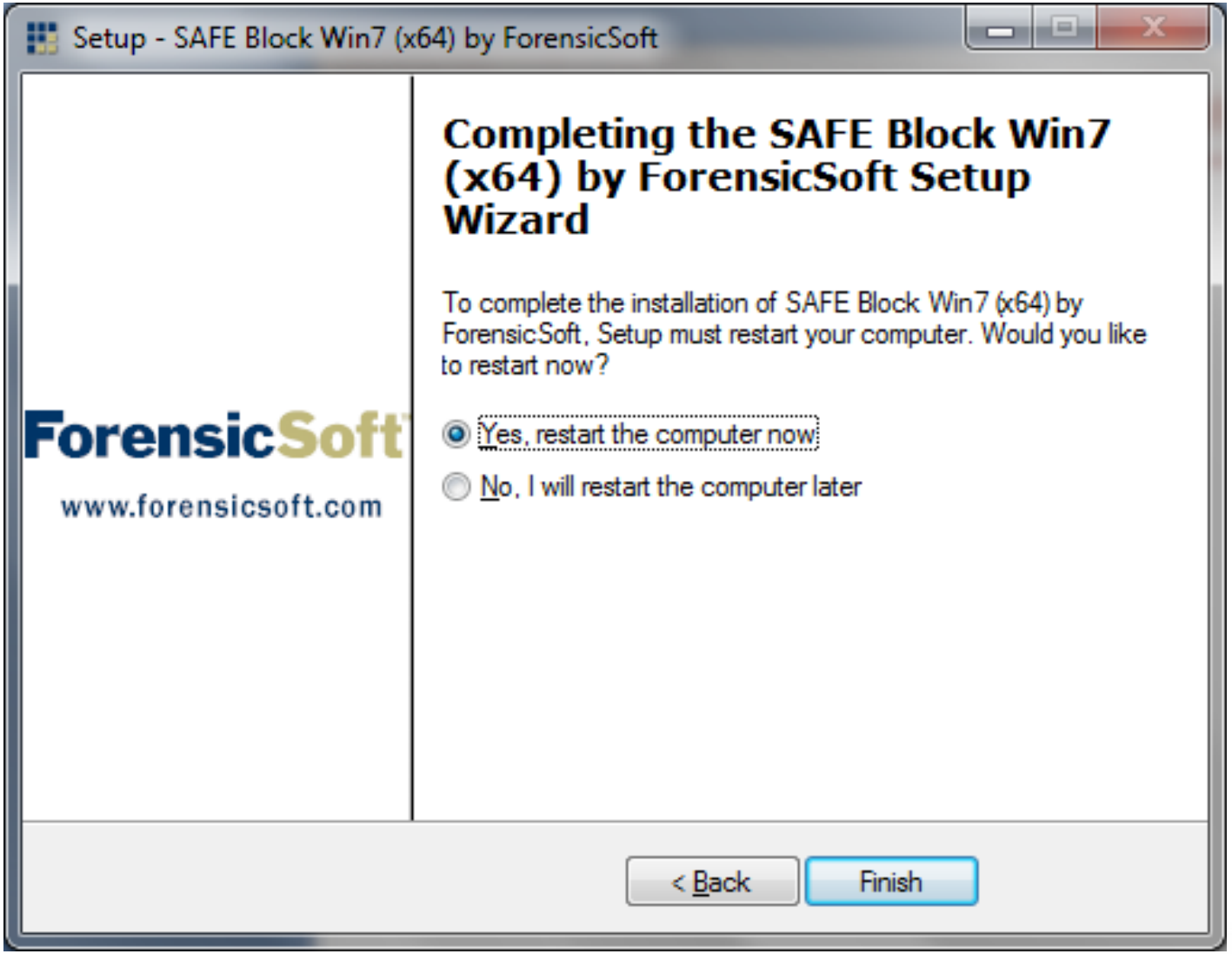
# Write Blocker Software



# Write Blocker Software

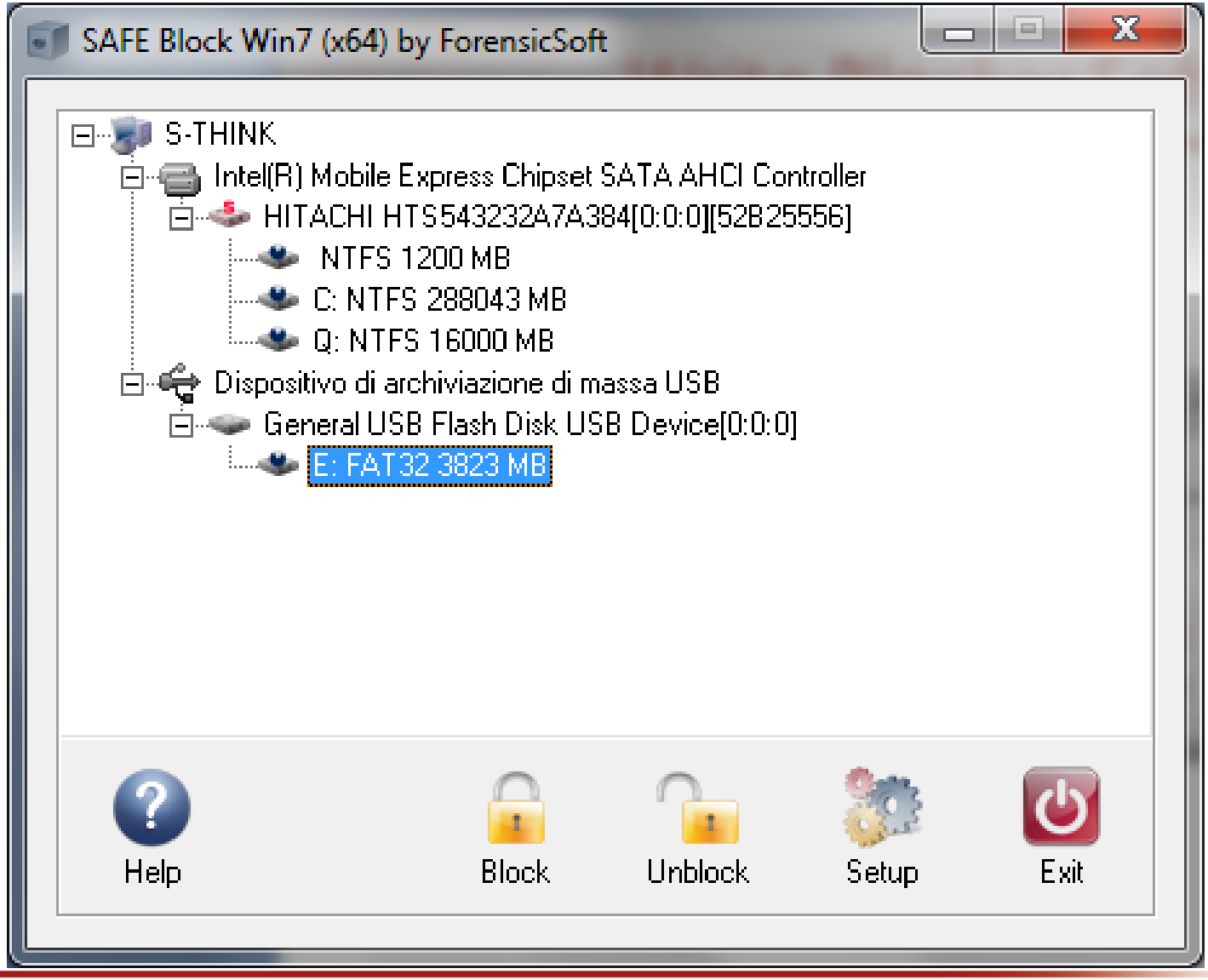


# Write Blocker Software



# 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

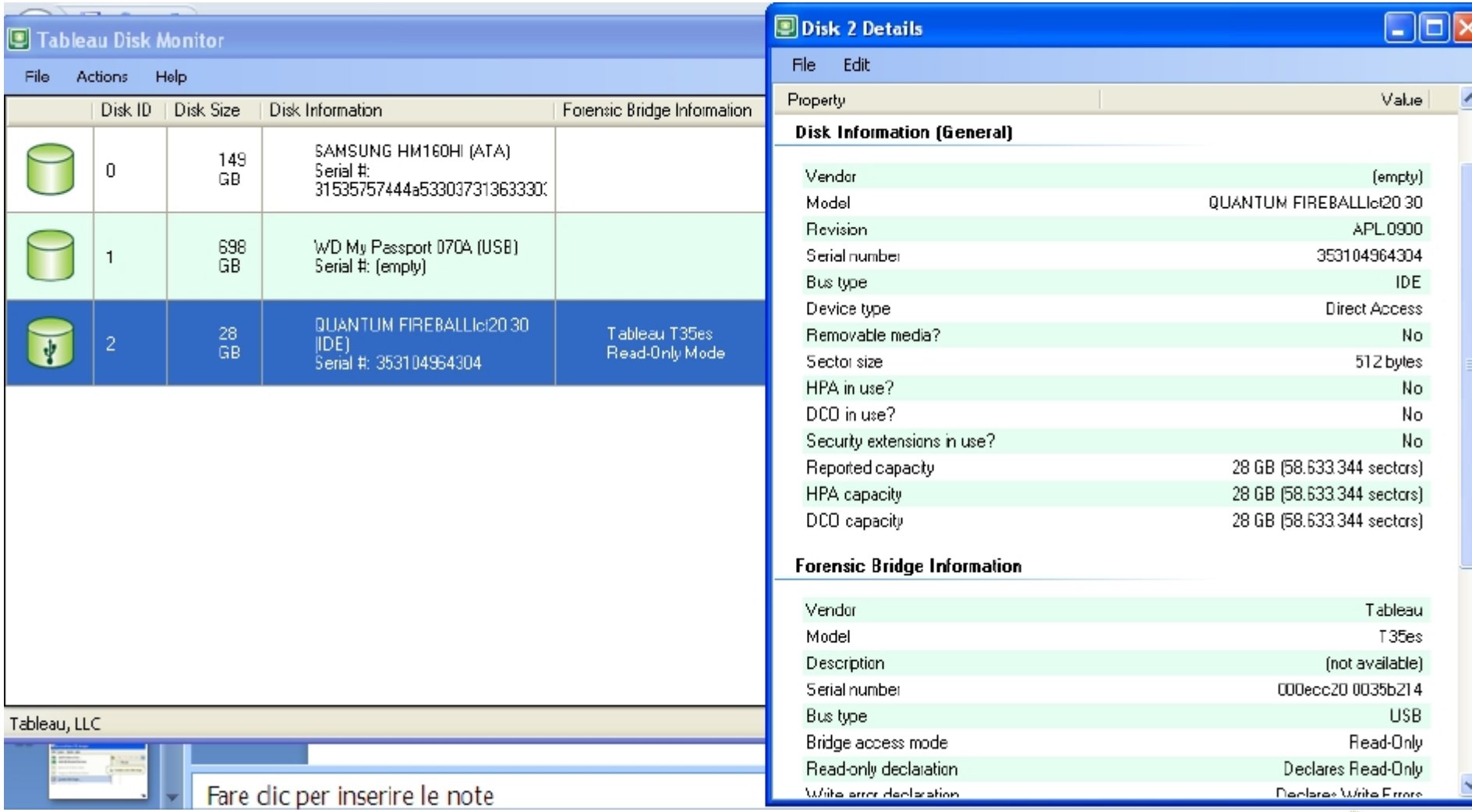
# Hash Function

- Cryptographic hash functions commonly used in Digital Forensic
  - MD5
    - Produces a 128-bit (16-byte) hash value
    - First published in 1992
  - SHA-1
    - Produces a 160-bit message digest
    - First published in 1995
  - SHA-2
    - A set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512)
    - First published in 2001

# Funzioni hash

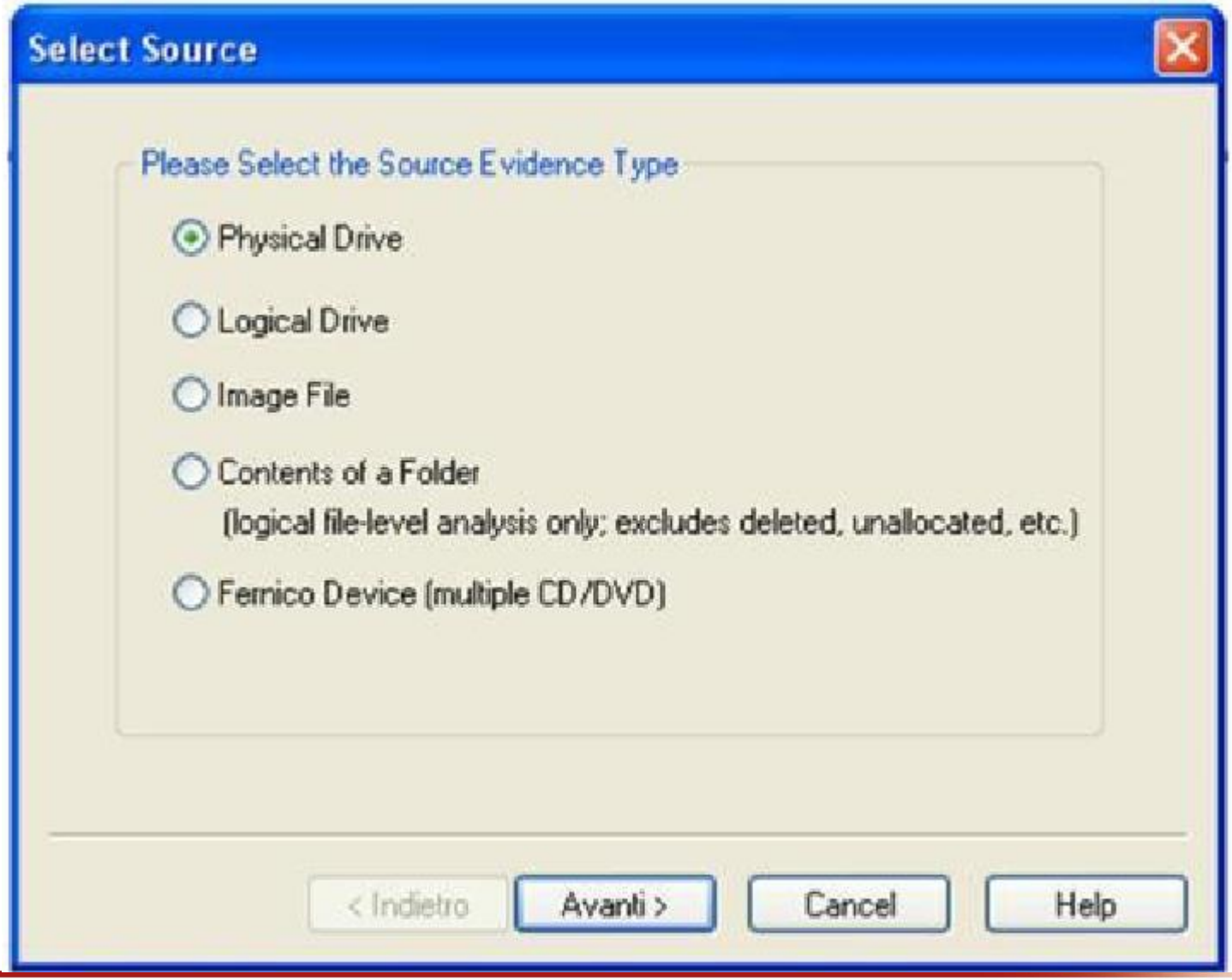
- Connect the disk to scan on a write blocker, using the appropriate interface (IDA, SATA, SCSI)
- Connect the write blocker to the acquisition workstation, using an interface supported (USB, FireWire, eSATA)
- Connect a target disk to the computer (USB, Firewire, eSATA, Network)
- Start the acquisition 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

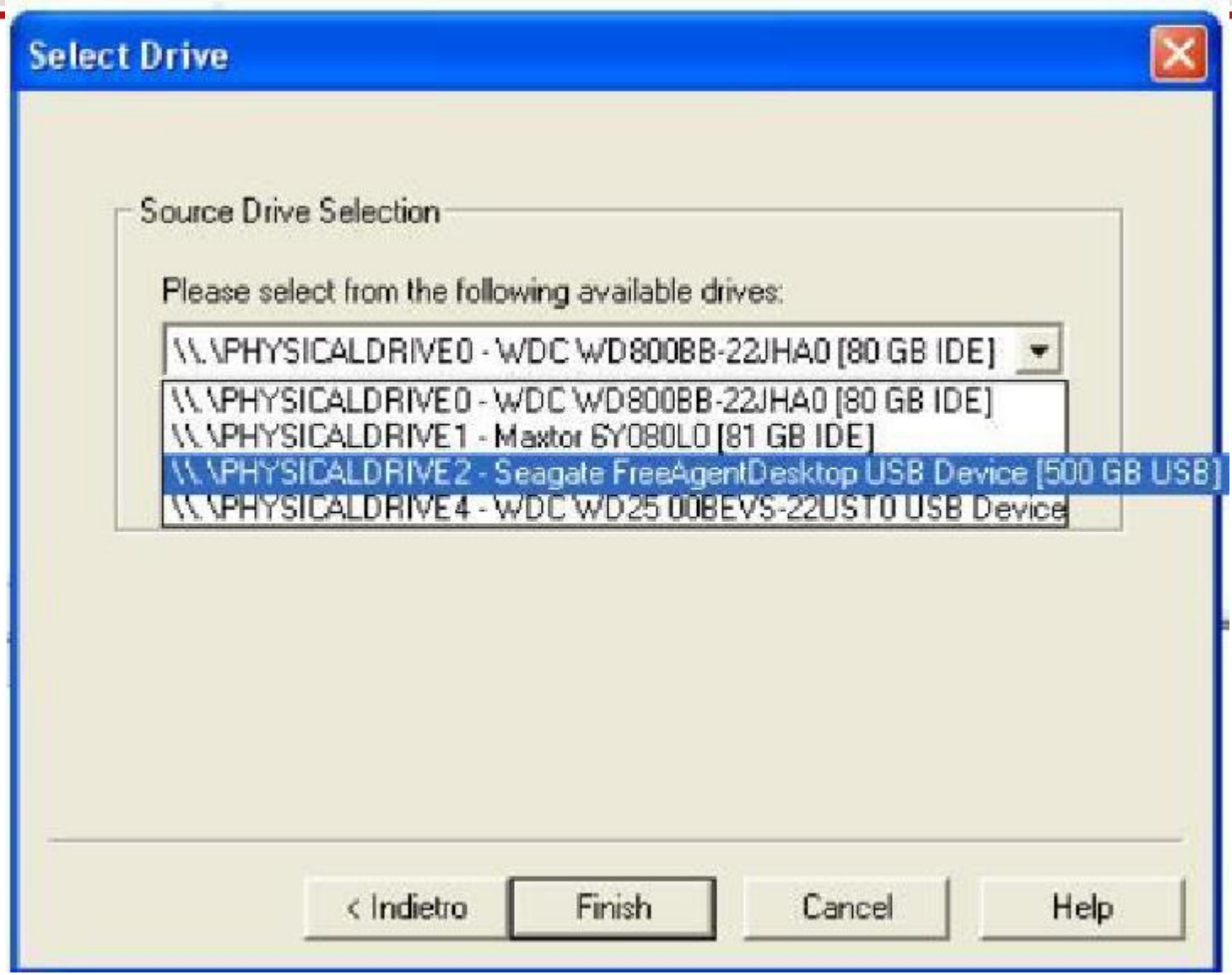


# Acquisition with FTK Imager

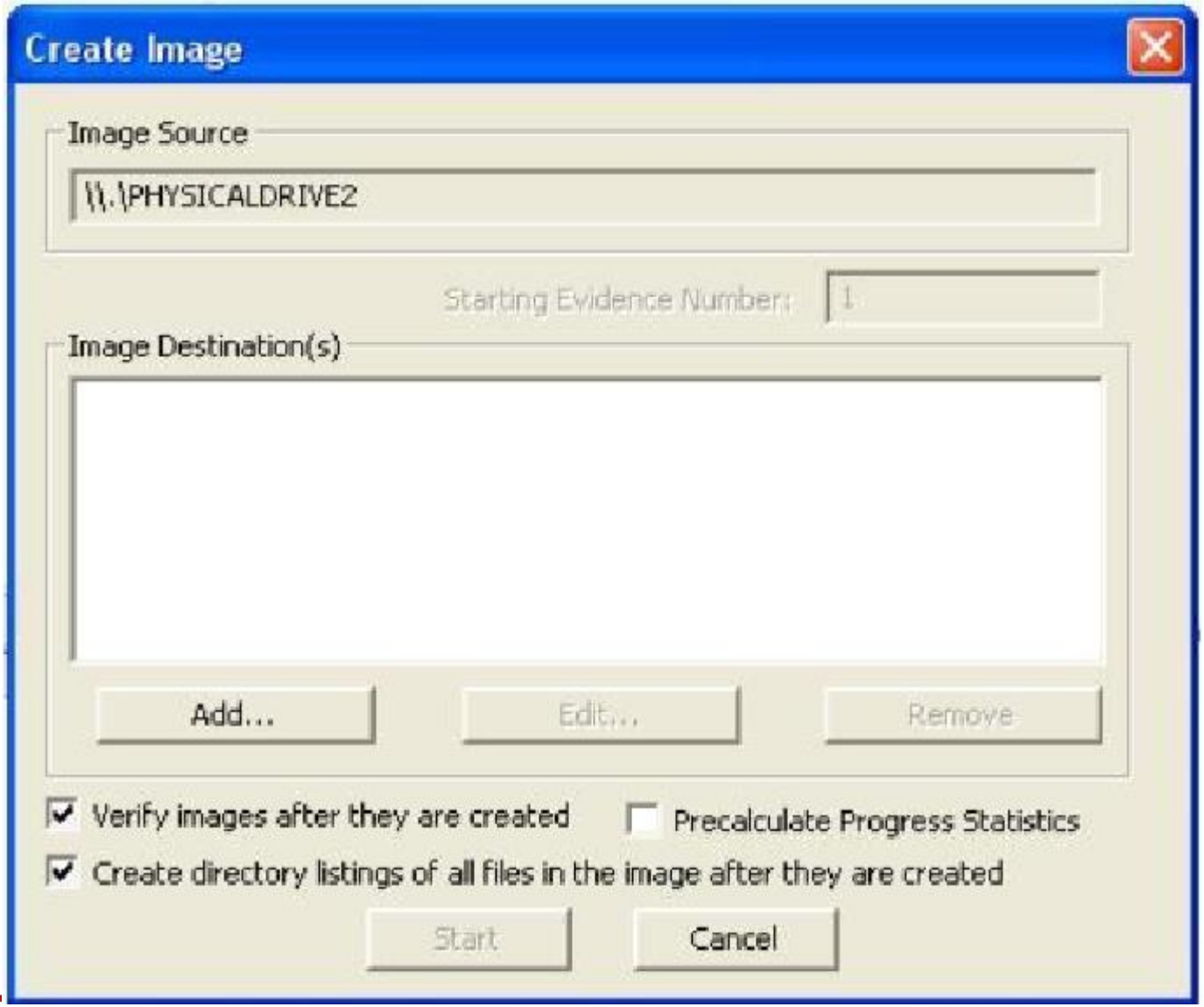
# Acquisition with FTK Imager



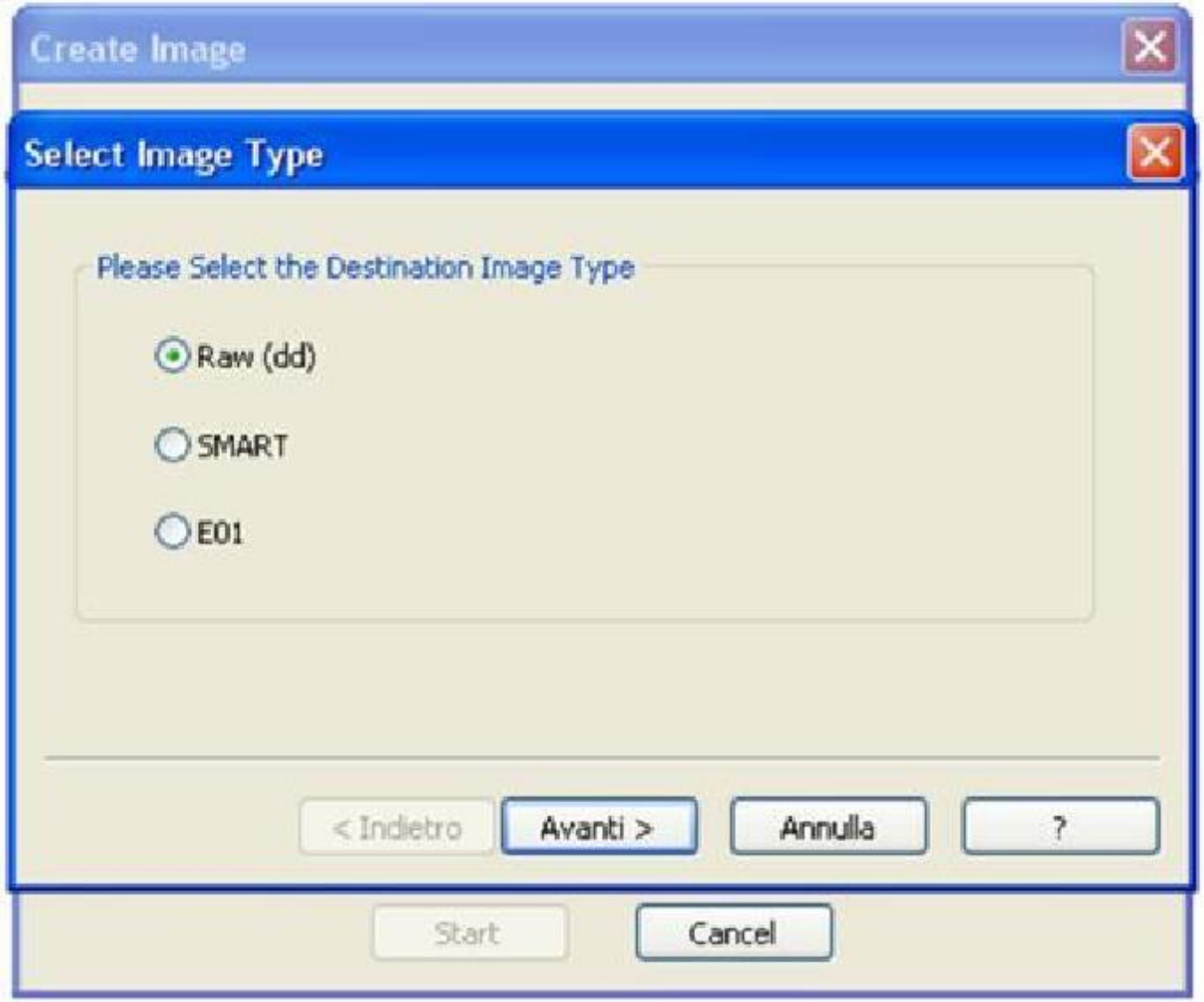
# Acquisition with FTK Imager



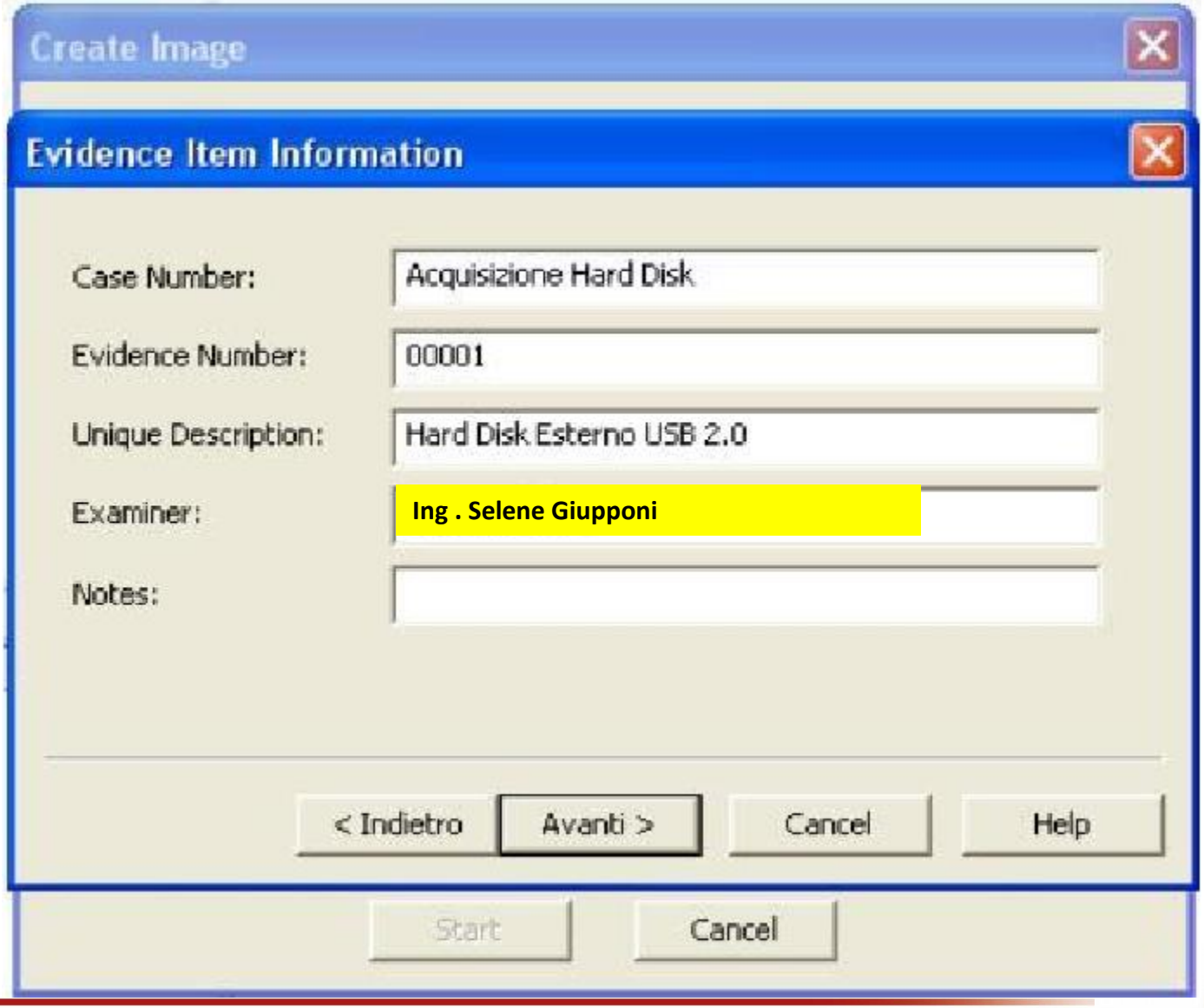
# Acquisition with FTK Imager



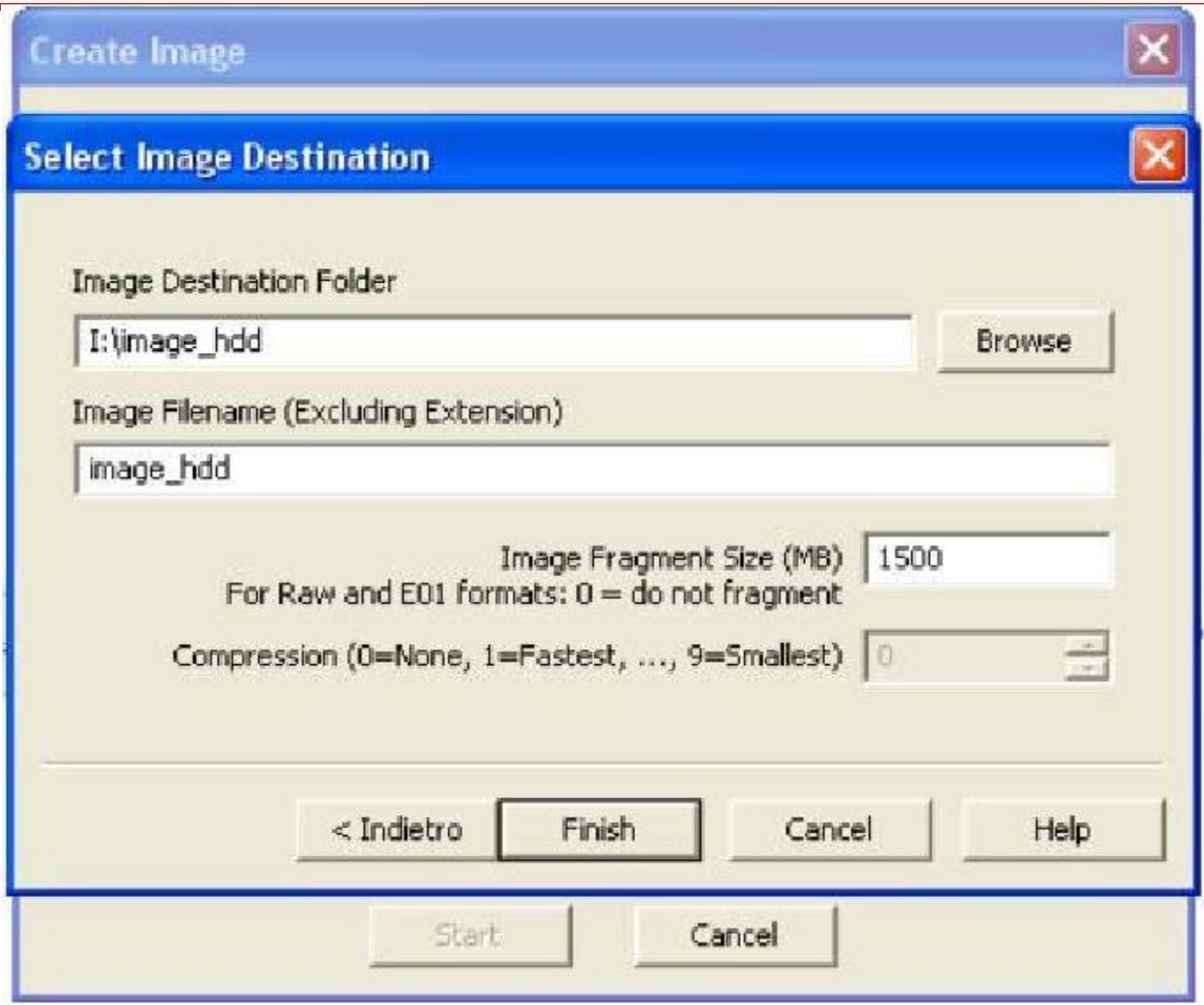
# Acquisition with FTK Imager



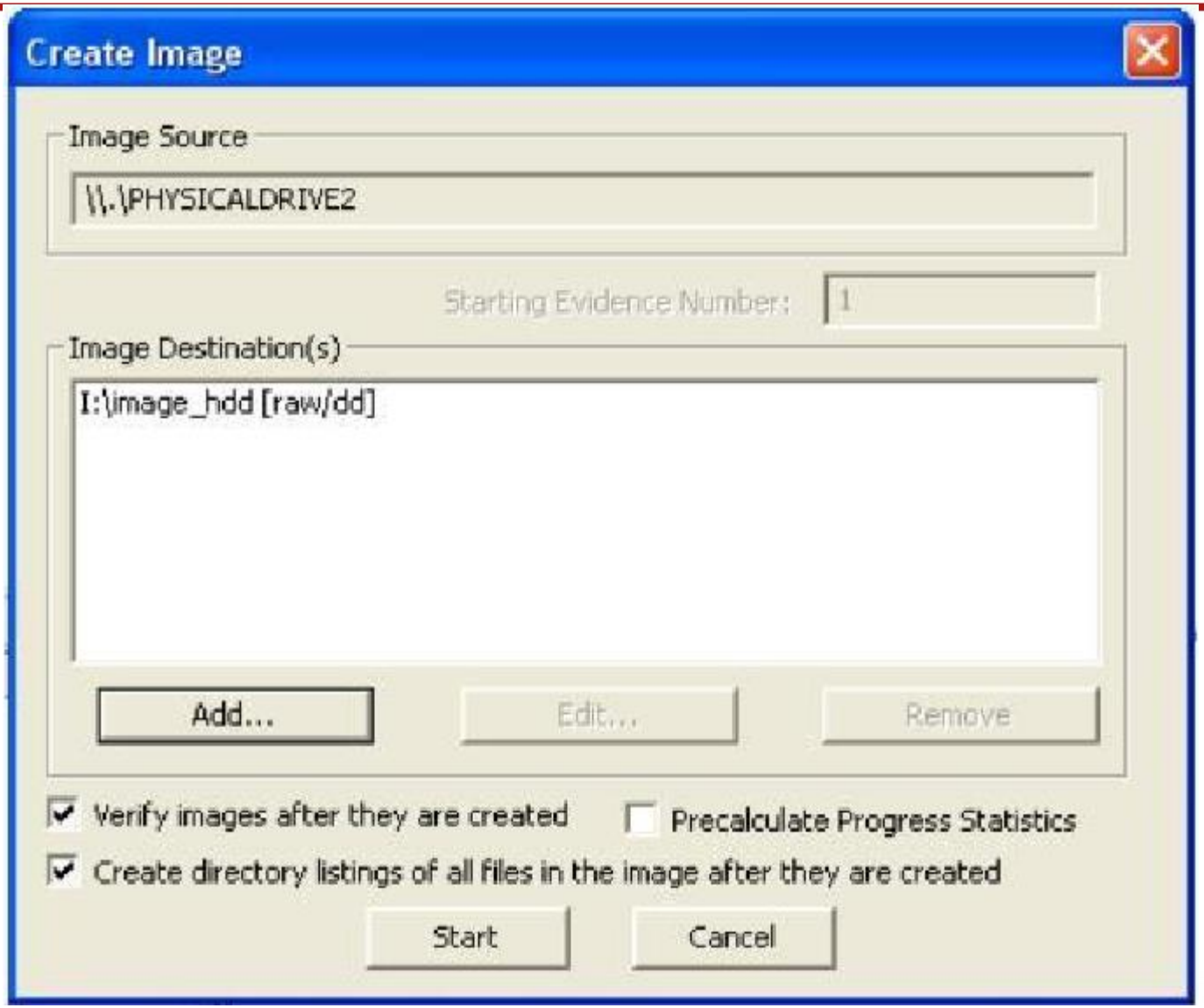
# Acquisition with FTK Imager



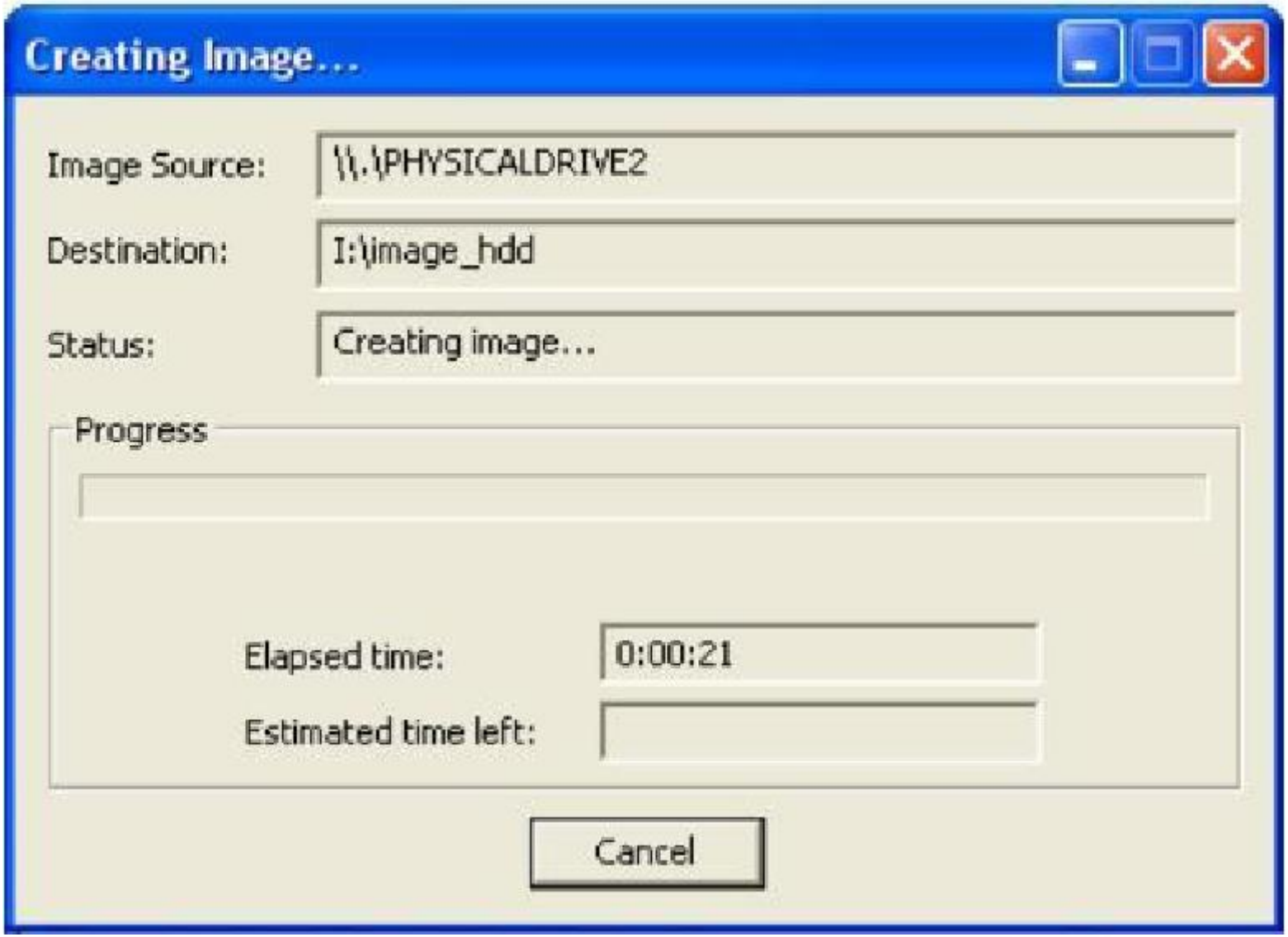
# Acquisition with FTK Imager



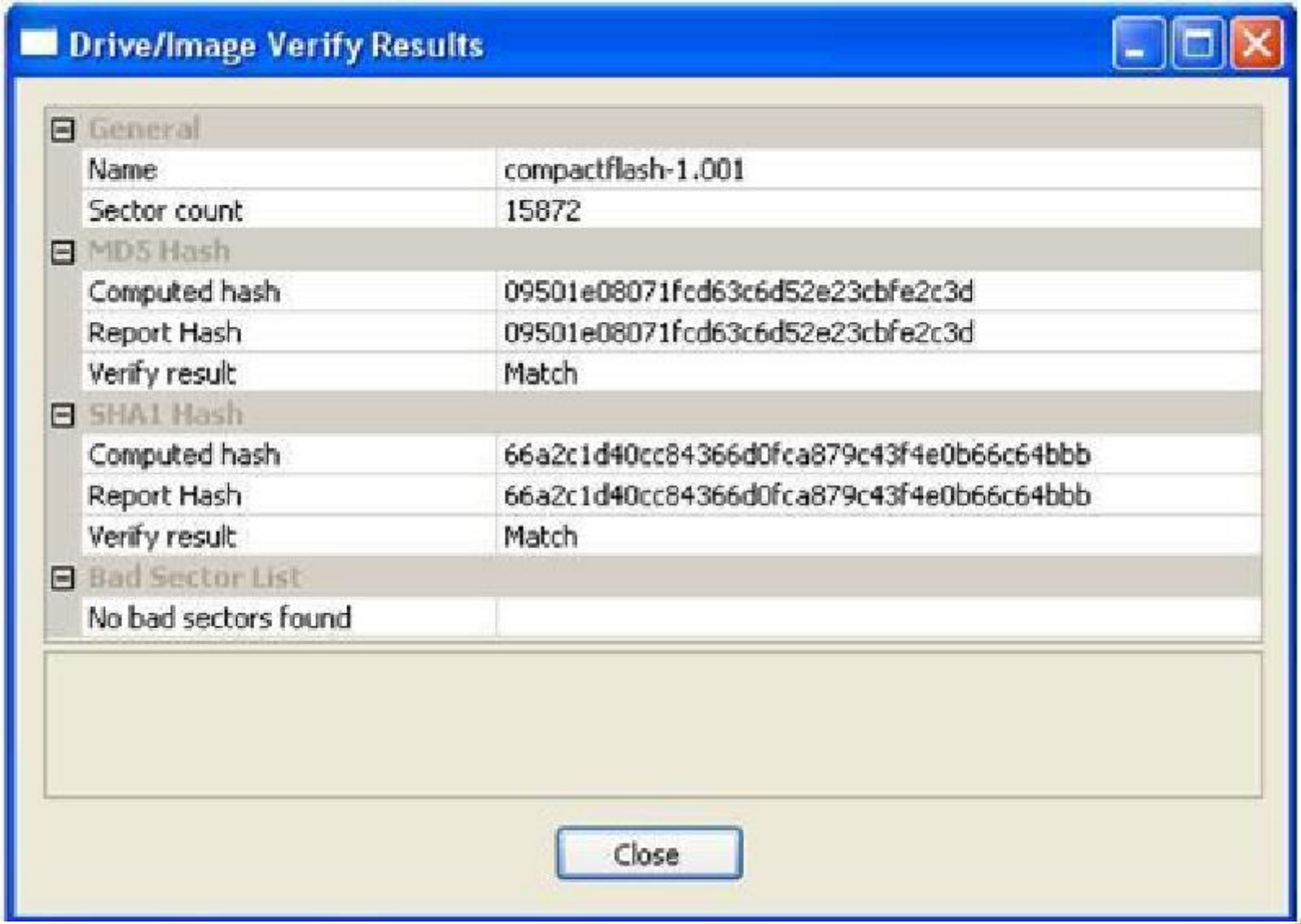
# Acquisition with FTK Imager



# Acquisition with FTK Imager



# Acquisition with FTK Imager



# Operating steps

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

# Analysis

- The evaluation mode differ 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

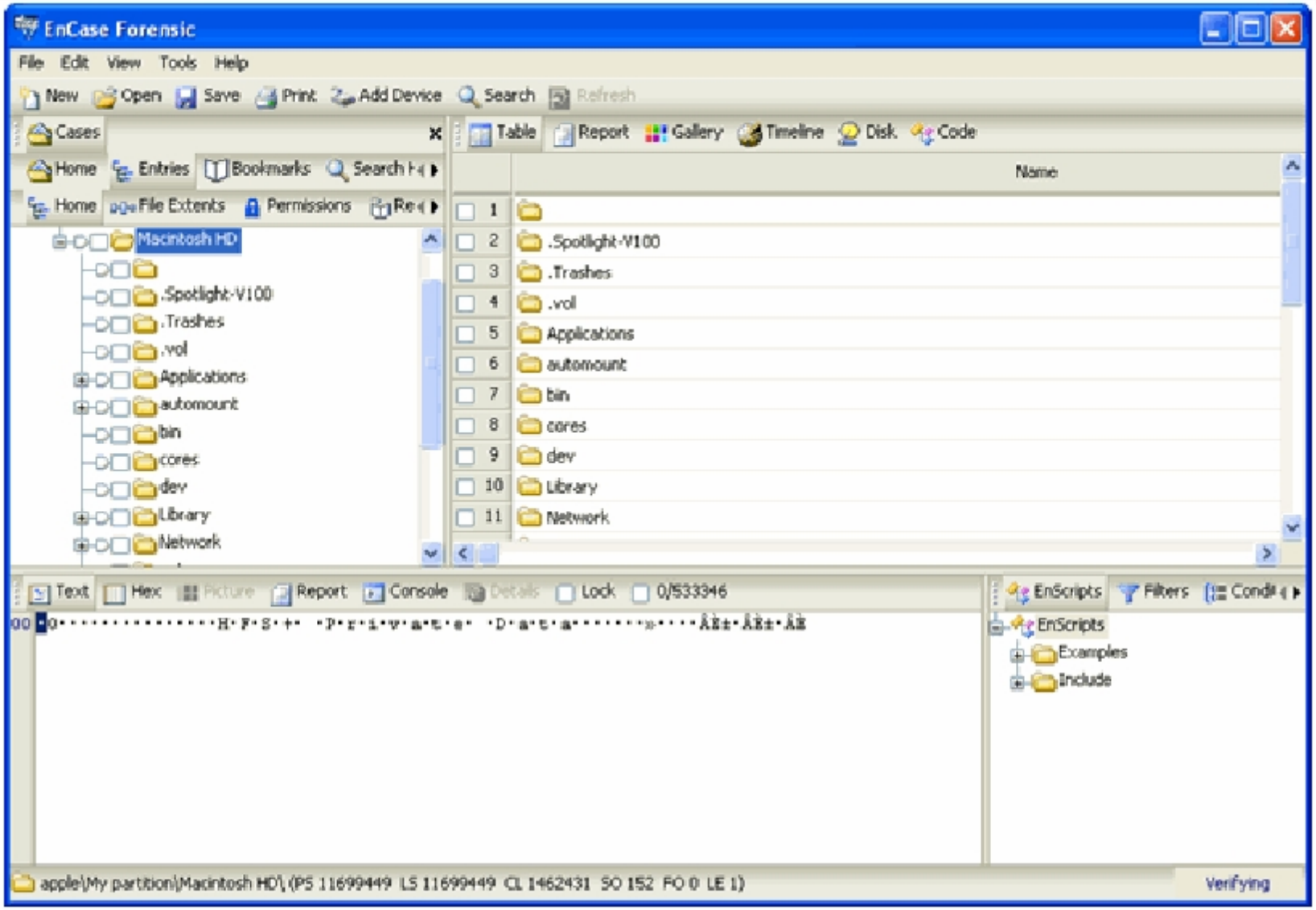
opensource vs proprietor

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

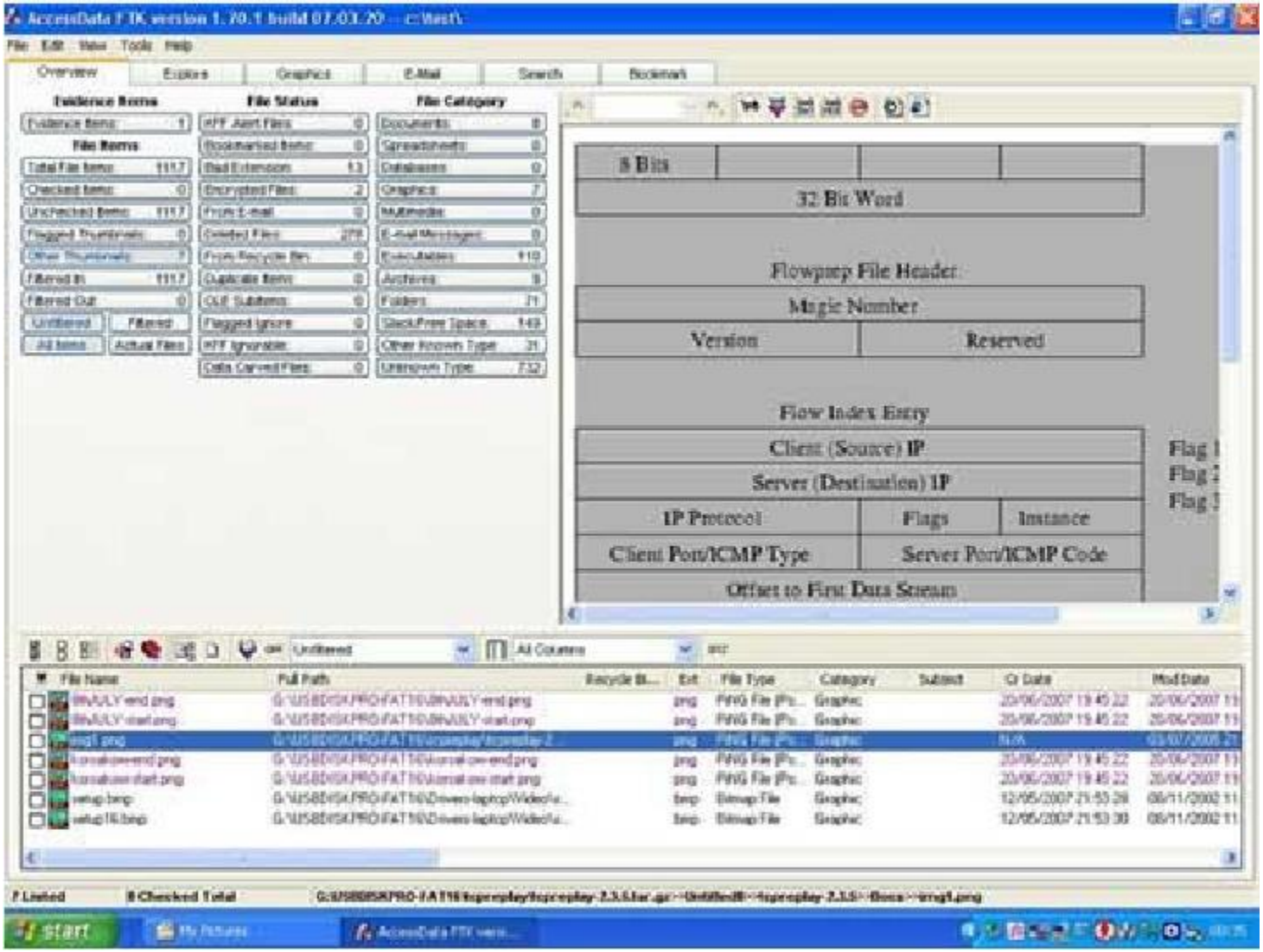
- The most important commercial forensics toolkit are:
  - **Encase** (Guidance Software)
  - **Forensic Toolkit** (AccessData) - FTK
  - **X-Ways Forensic** (X-Ways)
  - **P2 Commander** (Paraben Corporation)
  - **Pro Discover** (Technology Pathways)
  - **Macintosh Forensic** (Blackbag)

# Encase

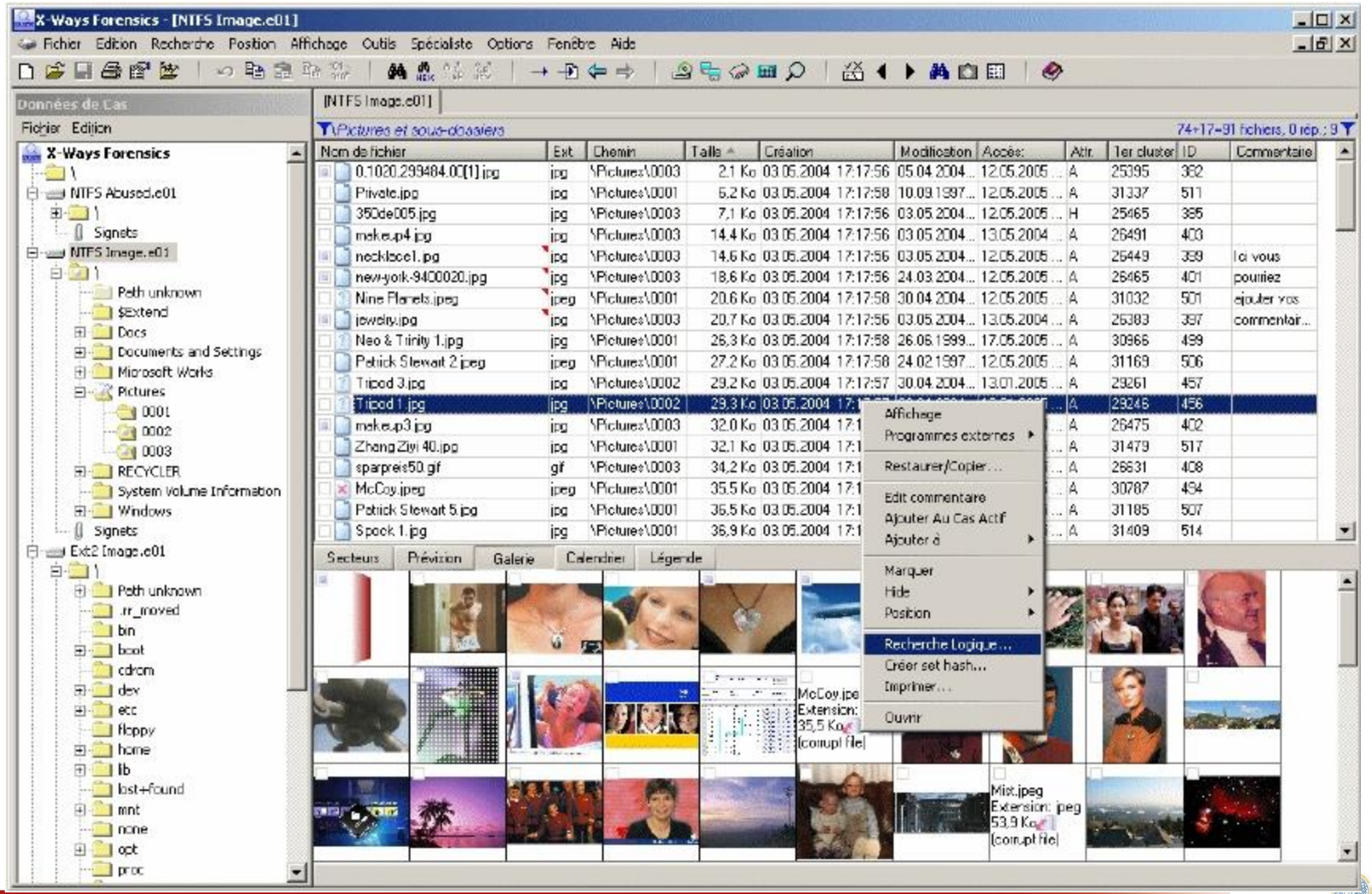



UNIVERSITÀ DI PARMA

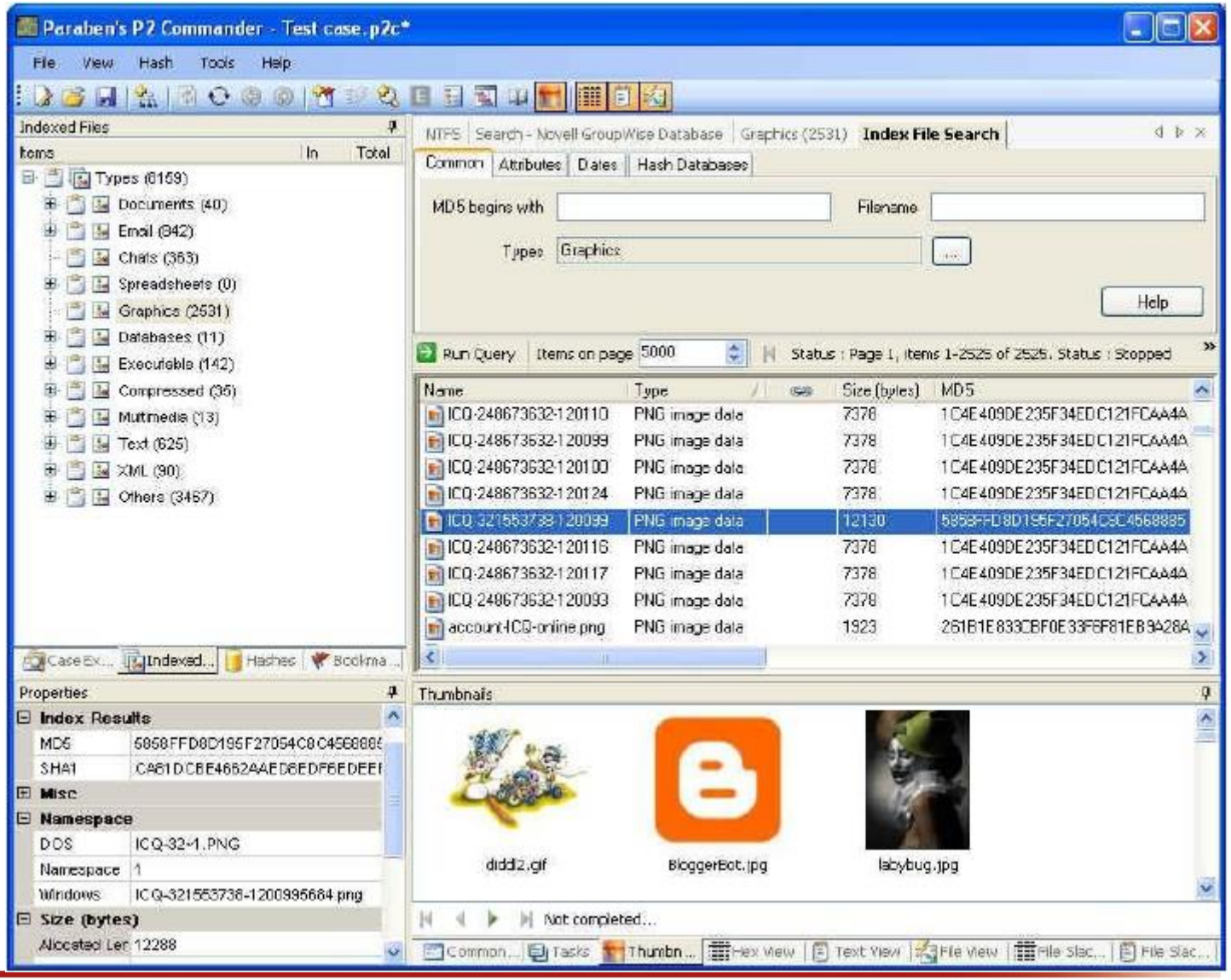
# FTK – Access Data



# X-Ways Forensics

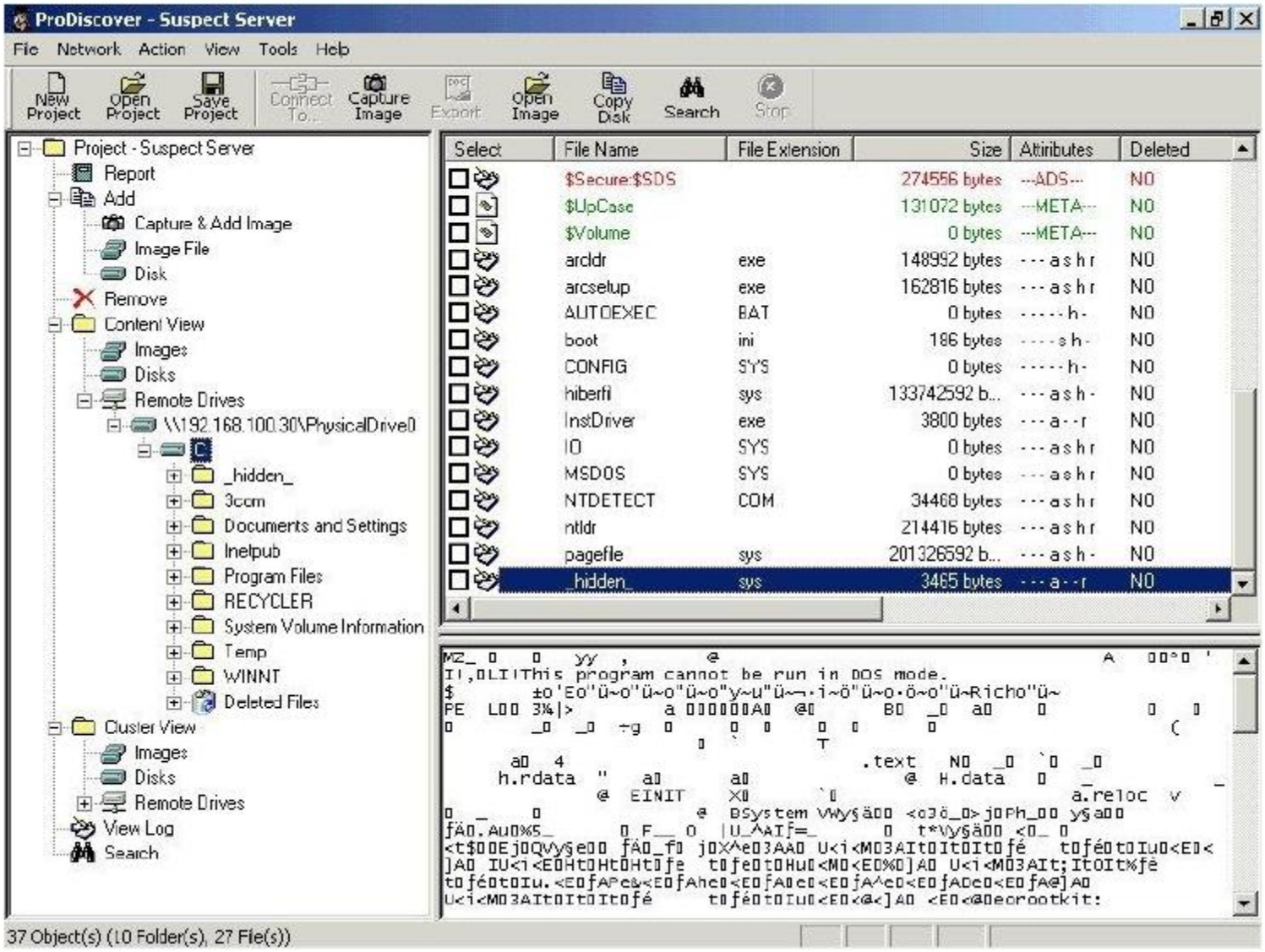


# Paraben P2 Commander




UNIVERSITÀ DI PARMA

# ProDiscover




UNIVERSITÀ DI PARMA

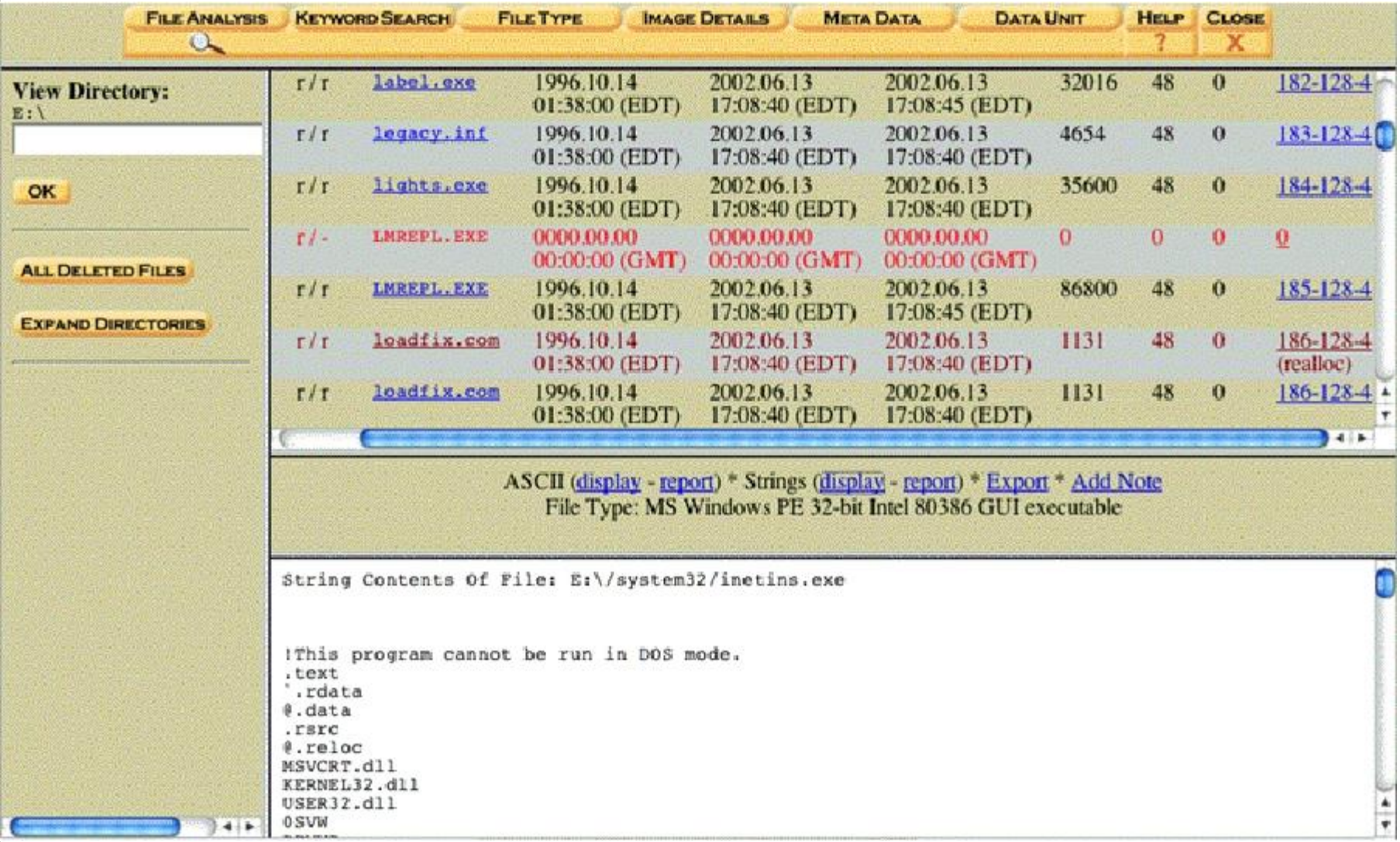
# Forensics Toolkit  opensource

- 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 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



# The Sleuth Kit – File Content


UNIVERSITÀ DI PARMA

# The Sleuth Kit – Hash Database

**NSRL Lookup**

a3e1a9ba1345f76c69a1e97f9d8b8f43 lmrepl.exe
a3e1a9ba1345f76c69a1e97f9d8b8f43 lmrepl.exe

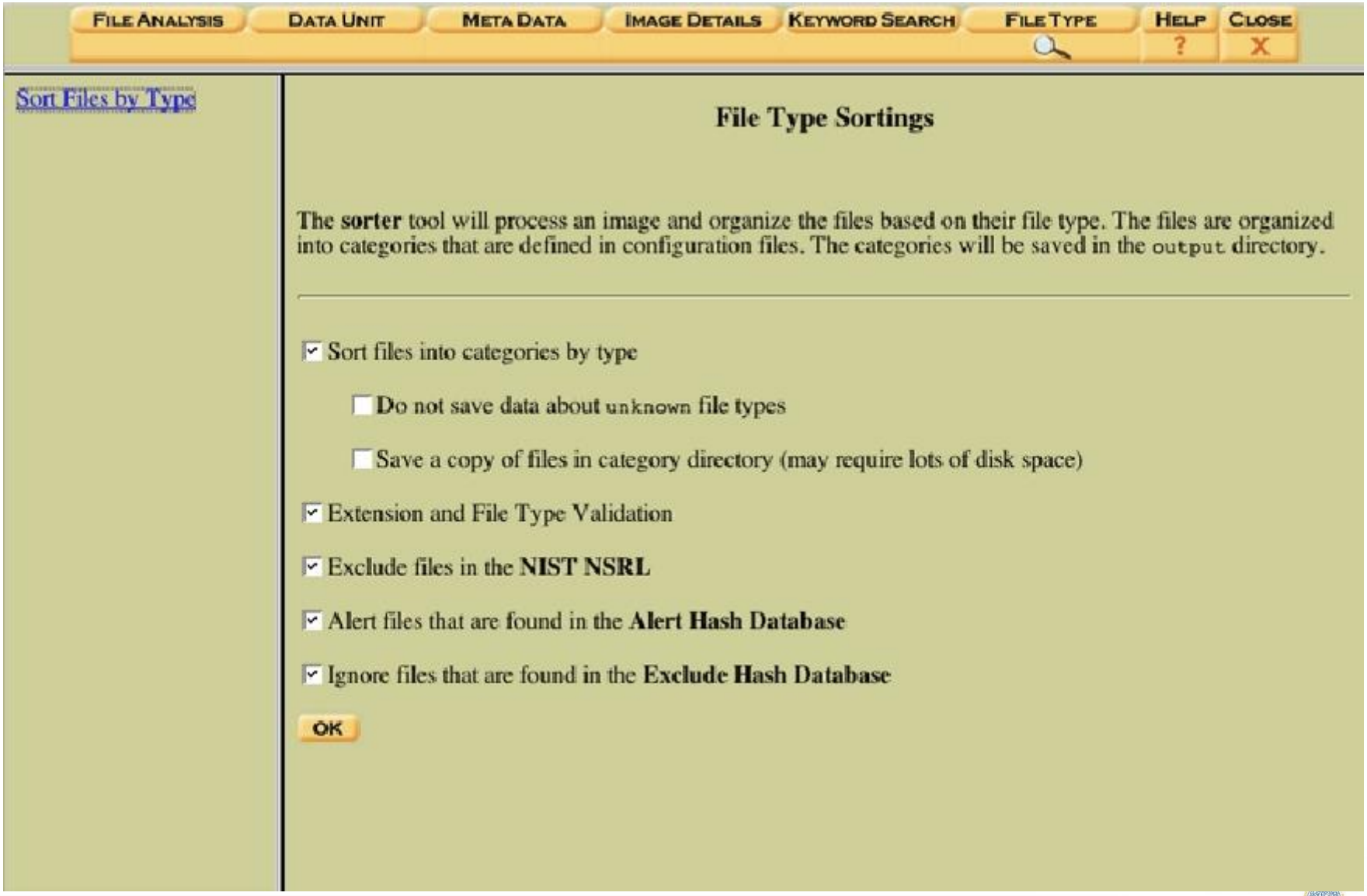
**Exclude Database Lookup**

a3e1a9ba1345f76c69a1e97f9d8b8f43 Hash Not Found

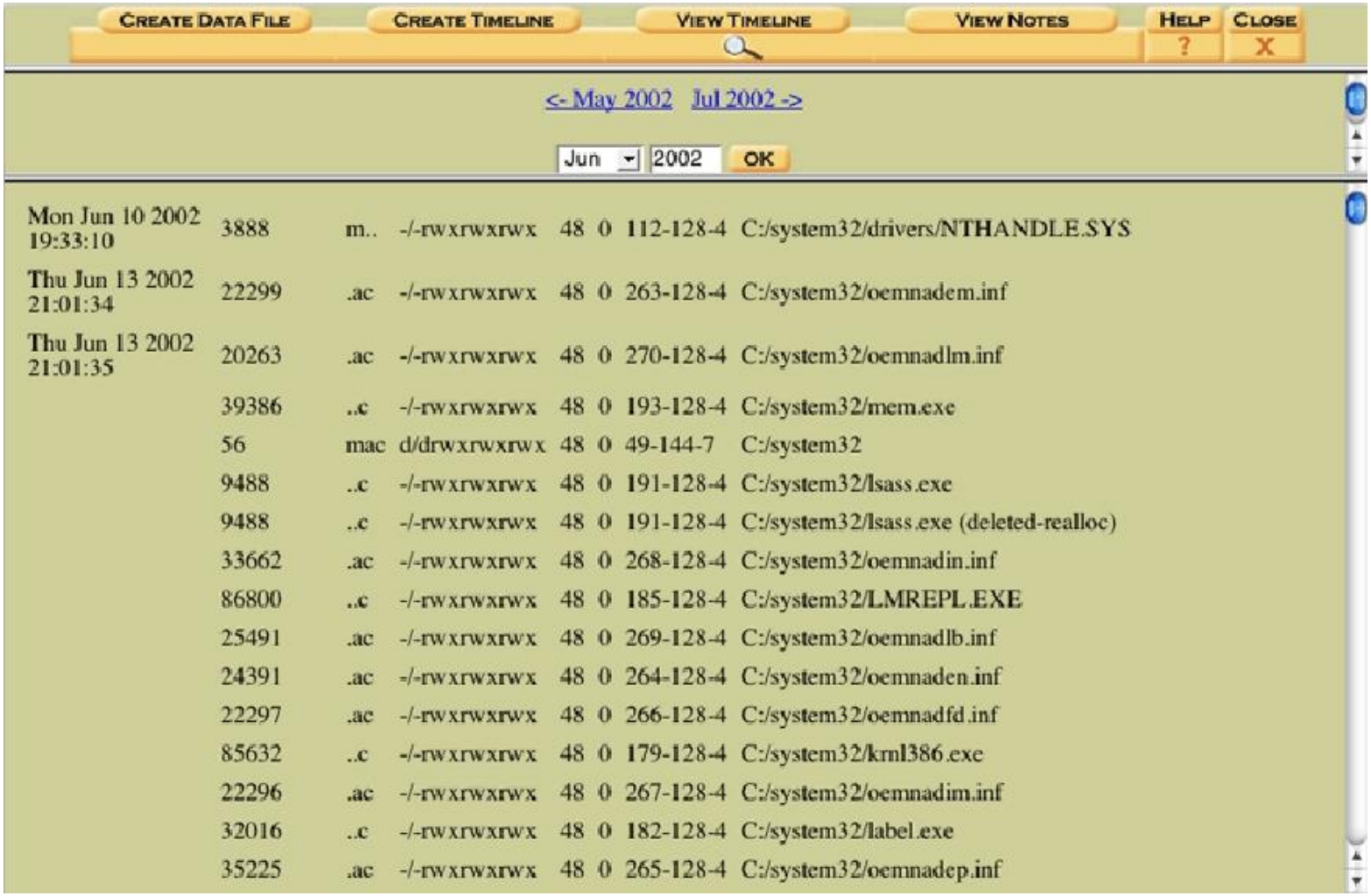
**Alert Database Lookup**

a3e1a9ba1345f76c69a1e97f9d8b8f43 Hash Not Found

# The Sleuth Kit - File Type Sorting

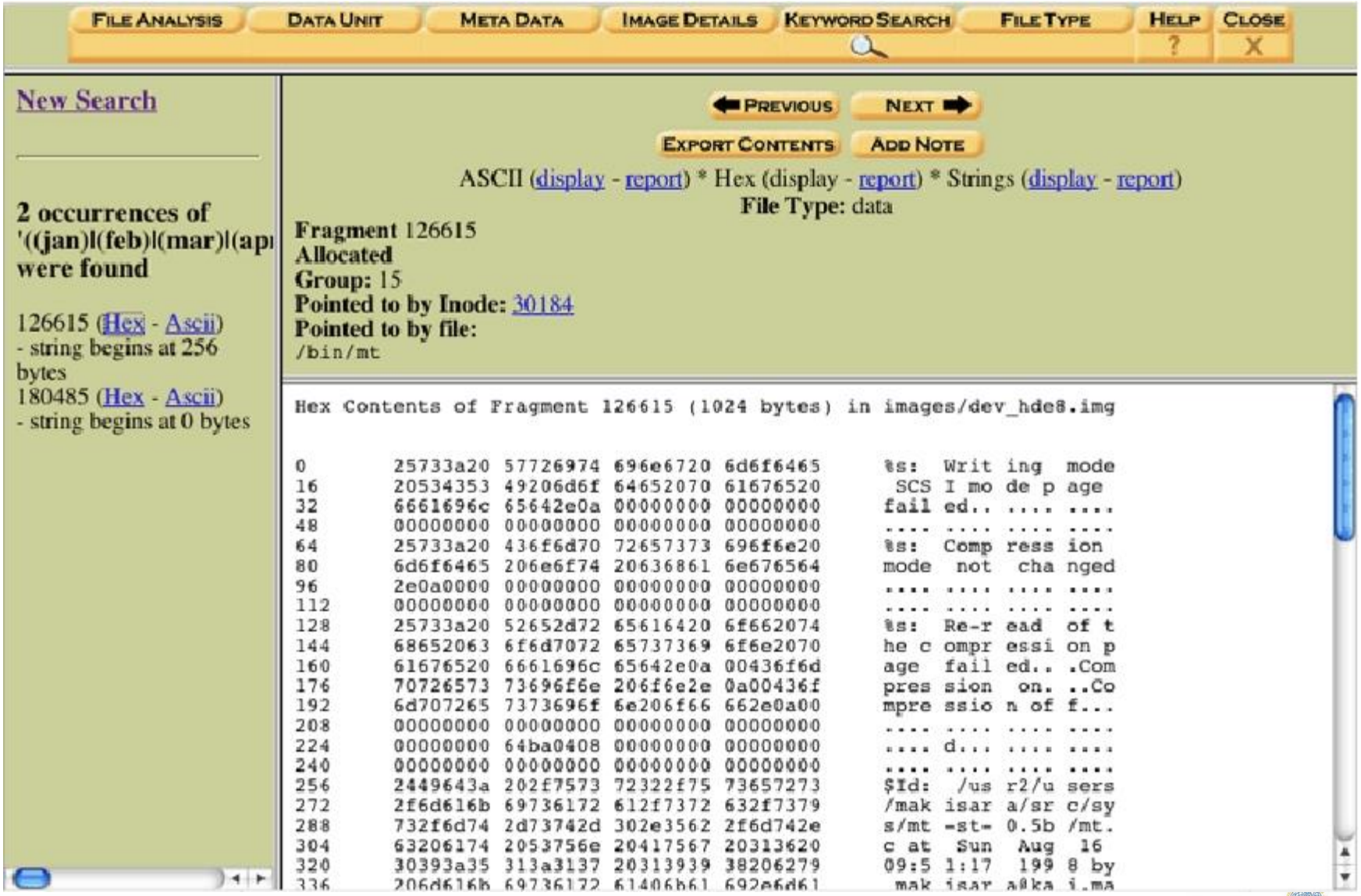


# The Sleuth Kit - Timeline

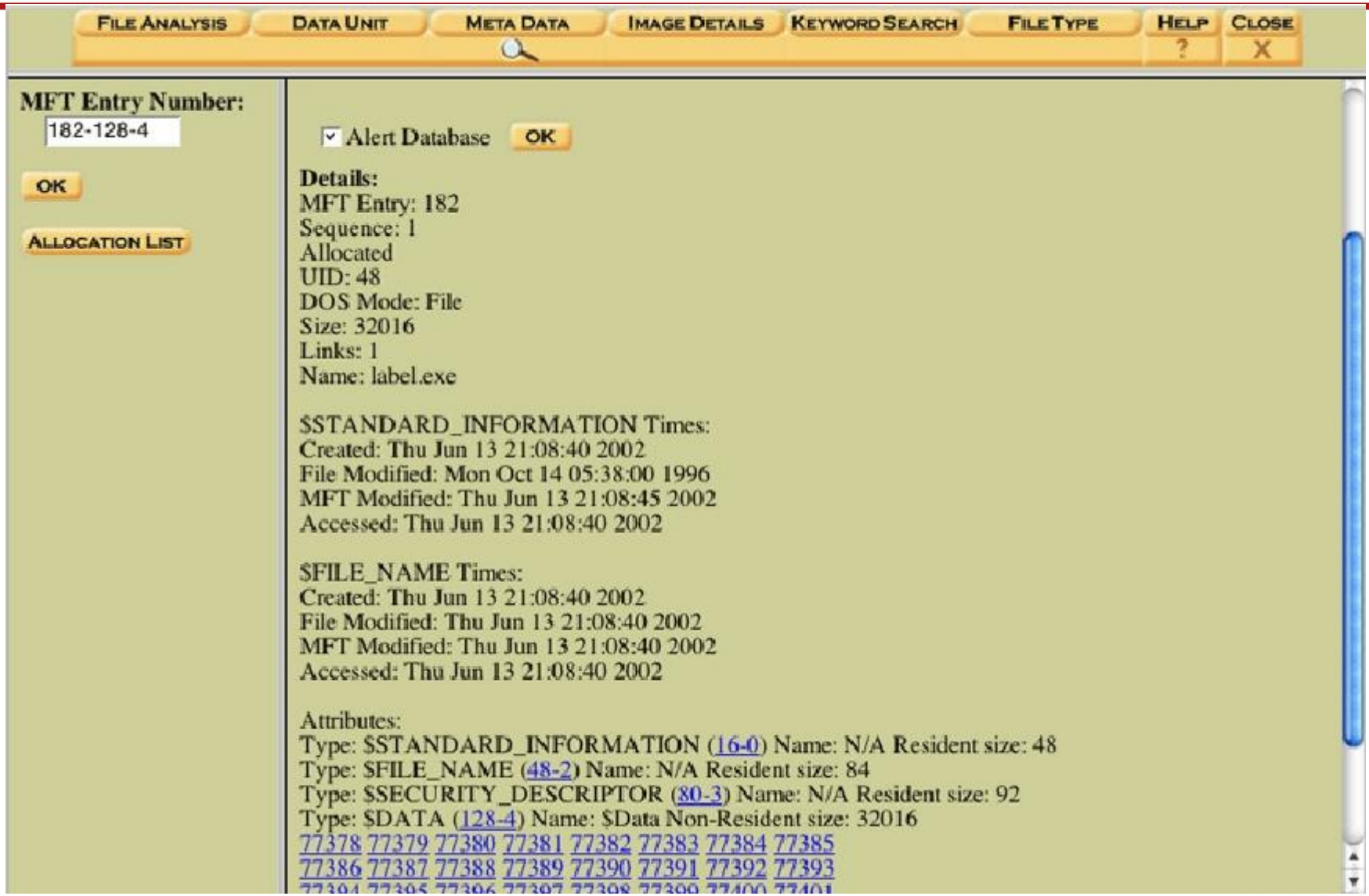



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Mon Jun 10 2002 19:33:10 | 3888 | m.. | -/-rwxrwxrwx | 48 | 0 | 112-128-4 | C:/system32/drivers/NTHANDLE.SYS |
| Thu Jun 13 2002 21:01:34 | 22299 | .ac | -/-rwxrwxrwx | 48 | 0 | 263-128-4 | C:/system32/oemnadem.inf |
| Thu Jun 13 2002 21:01:35 | 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/krnl386.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 |

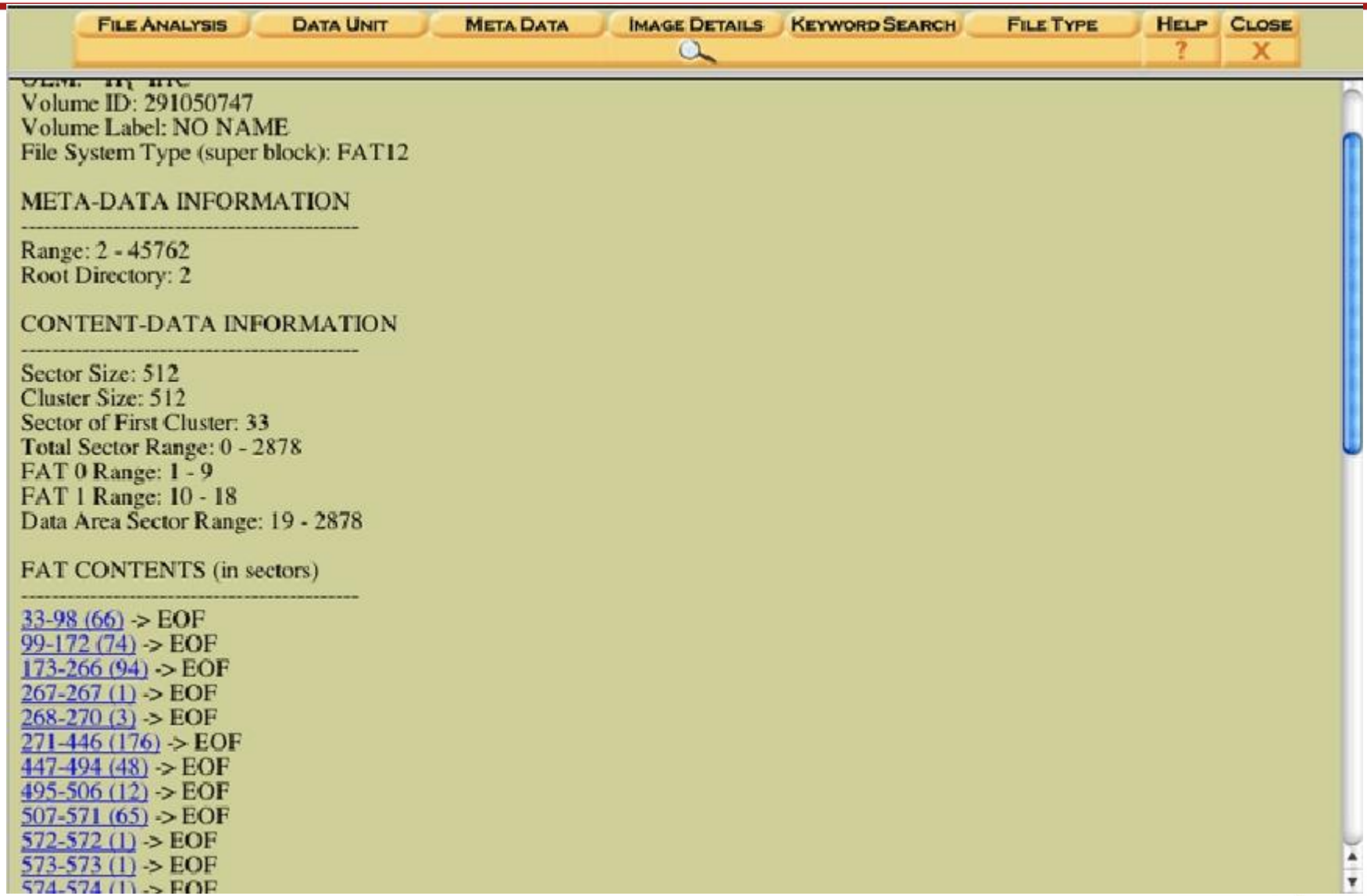
# The Sleuth Kit – Key word search



# The Sleuth Kit – Metadata Analysis



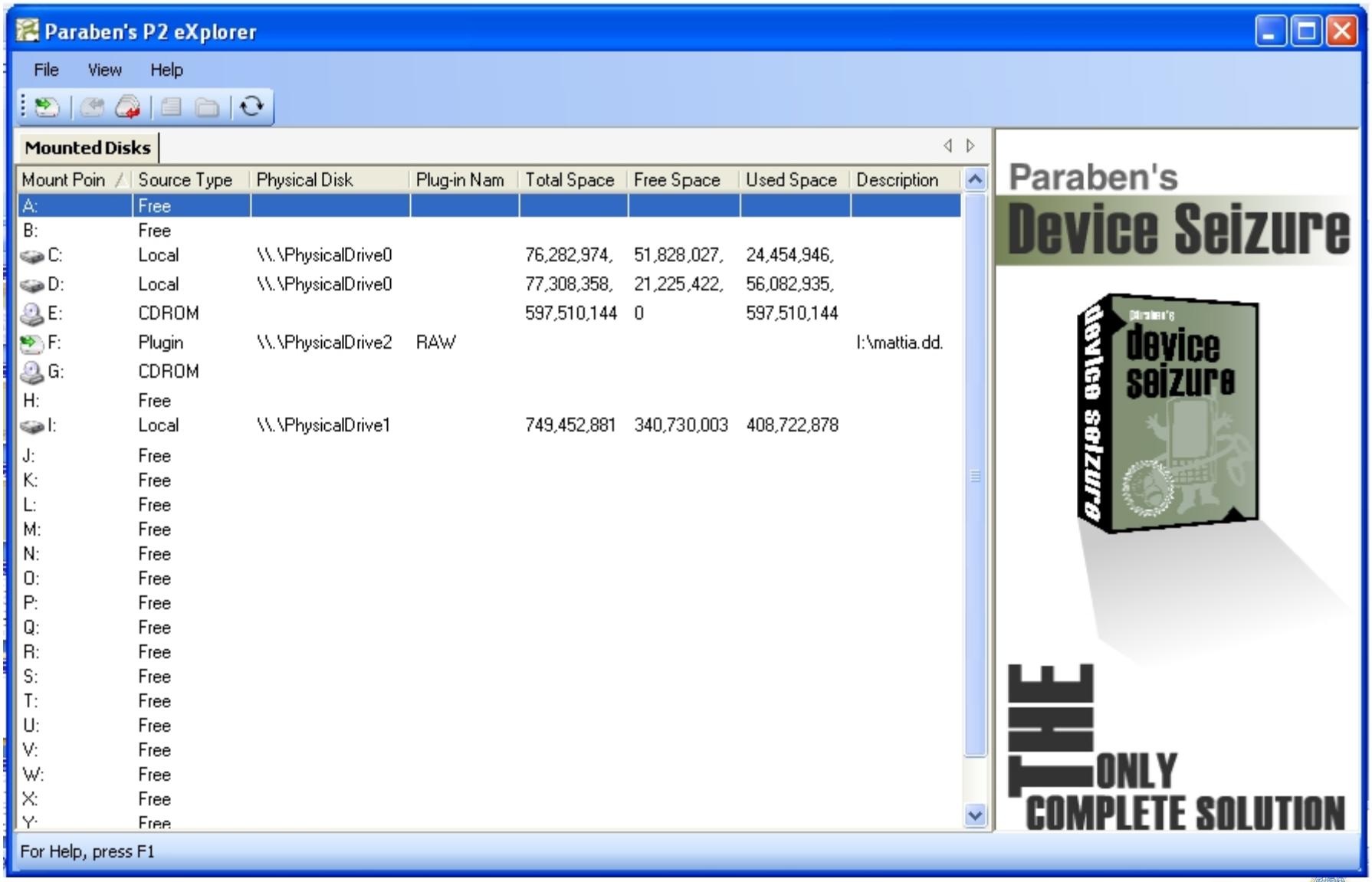
# The Sleuth Kit – Image Details



# 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



# 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** – Mostra le partizioni di un volume
- **MFT Ripper** (commerciale)
- **AnalyzeMFT.py** (opensource)
- **MFTView** (freeware)
- **NTFSWalk** (freeware)
- **Windows Journal Parser** (freeware)

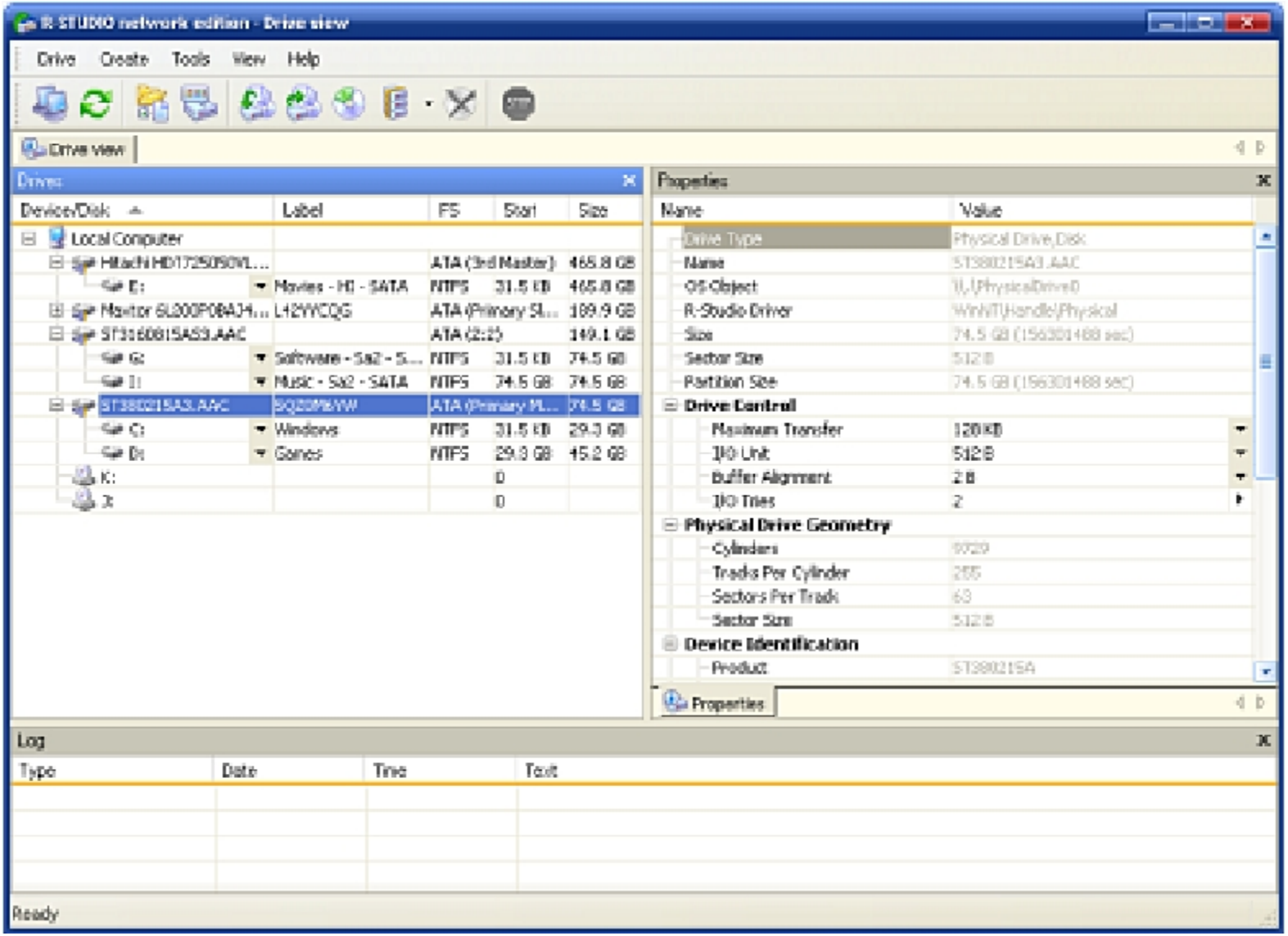
# Deleted Files

- 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



# 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

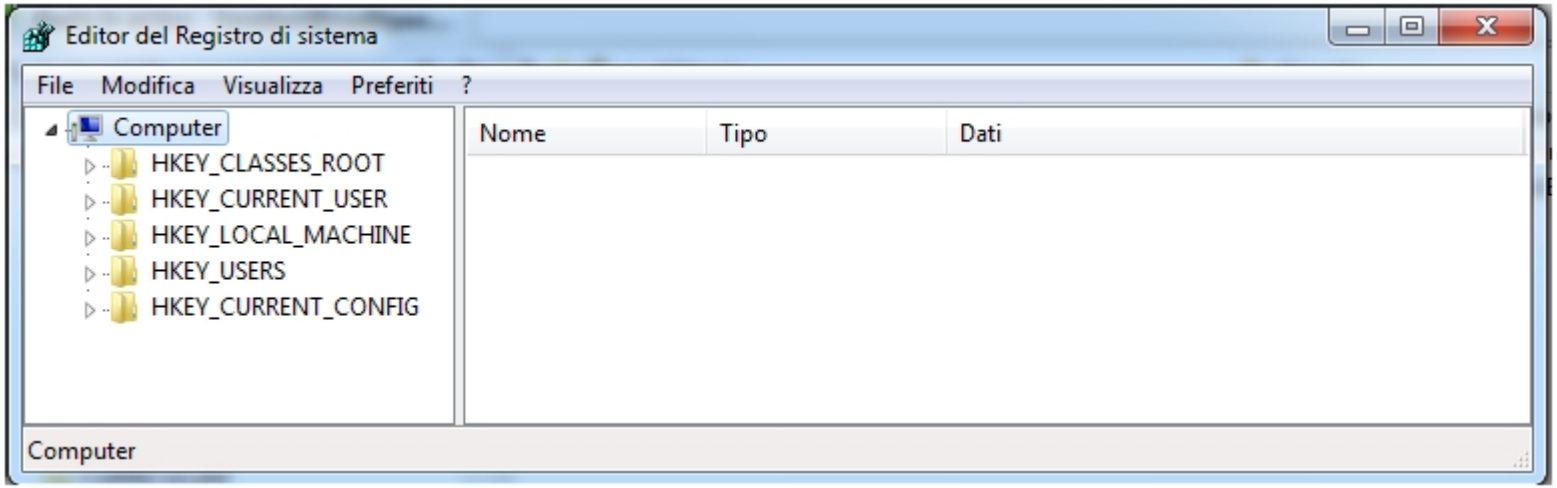
- The file Netsetup.log is located in the Windows \ Debug and contains information about the workgroup or domain configured on the computer
  The file is created during the operating system and stores installation it all changes regarding Any adjustment of the working group, domain or enabling file sharing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

# Windows Registry

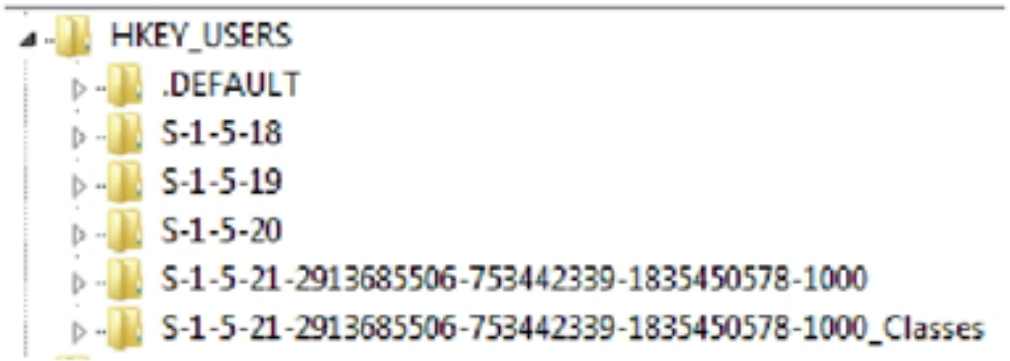
- The Windows registry contains very significant forensics data from our point of view
- The registry is a hierarchical database of configuration data for the operating system and most of the programs installed
- The user interacts with the registry typically through the configuration utility of the 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 |
|---|---|
| HKU\.DEFAULT | **%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** |
| HKU\SID | **Documents and Settings*Username*\ntuser.dat** |

# Windows Registry

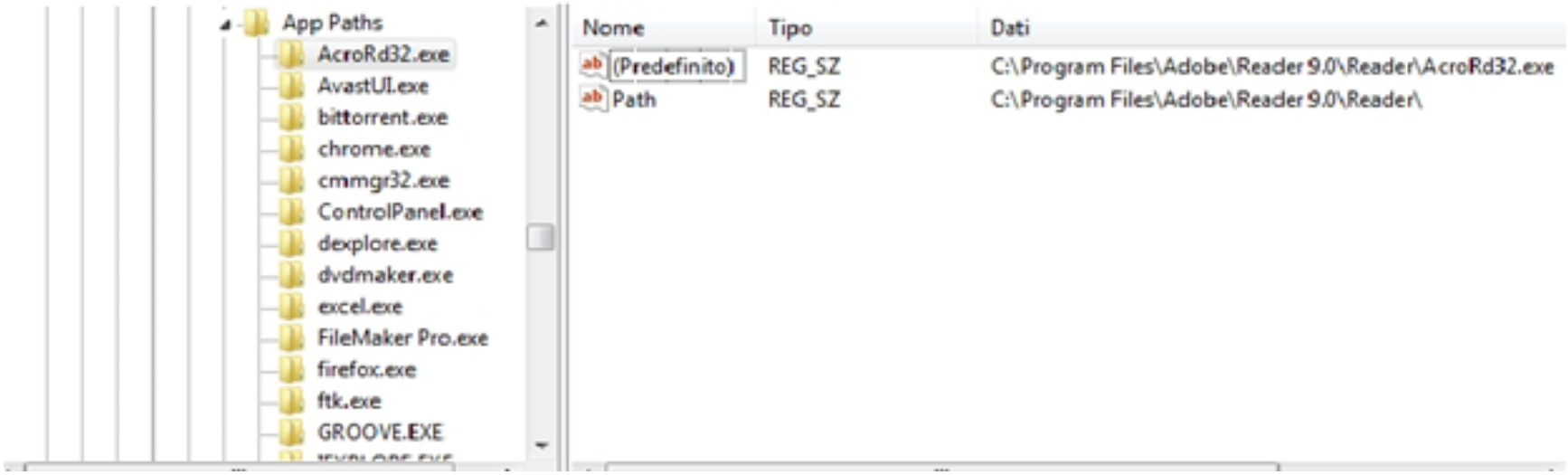
The key is:

**HKLM\SYSTEM\CurrentControlSet\Control\hivelist**

| Nome | Tipo | Dati |
|---|---|---|
| (Predefinito) | REG_SZ | (valore non impostato) |
| \REGISTRY\MACHINE\BCD00000000 | REG_SZ | \Device\HarddiskVolume2\Boot\BCD |
| \REGISTRY\MACHINE\HARDWARE | REG_SZ | |
| \REGISTRY\MACHINE\SAM | REG_SZ | \Device\HarddiskVolume3\Windows\System32\config\SAM |
| \REGISTRY\MACHINE\SECURITY | REG_SZ | \Device\HarddiskVolume3\Windows\System32\config\SECURITY |
| \REGISTRY\MACHINE\SOFTWARE | REG_SZ | \Device\HarddiskVolume3\Windows\System32\config\SOFTWARE |
| \REGISTRY\MACHINE\SYSTEM | REG_SZ | \Device\HarddiskVolume3\Windows\System32\config\SYSTEM |
| \REGISTRY\USER\.DEFAULT | REG_SZ | \Device\HarddiskVolume3\Windows\System32\config\DEFAULT |
| \REGISTRY\USER\S-1-5-19 | REG_SZ | \Device\HarddiskVolume3\Windows\ServiceProfiles\LocalService\NTUSER.DAT |
| \REGISTRY\USER\S-1-5-20 | REG_SZ | \Device\HarddiskVolume3\Windows\ServiceProfiles\NetworkService\NTUSER.DAT |
| \Registry\User\S-1-5-21-2913685506-753442339-1835450578-1000 | REG_SZ | \Device\HarddiskVolume3\Users\Mattia\NTUSER.DAT |
| \Registry\User\S-1-5-21-2913685506-753442339-1835450578-1000_Classes | REG_SZ | \Device\HarddiskVolume3\Users\Mattia\AppData\Local\Microsoft\Windows\UsrClass.dat |

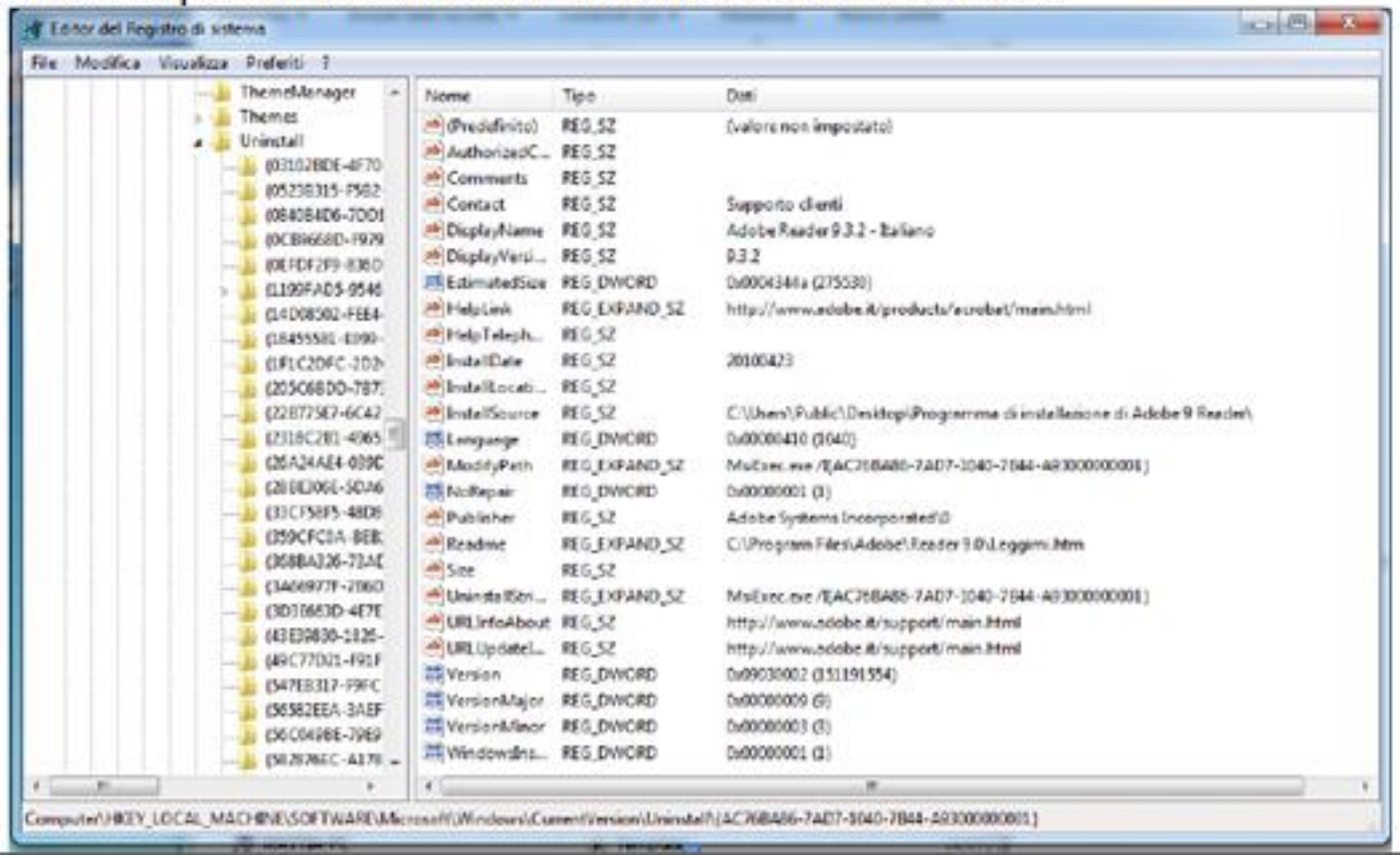
# Windows Registry – Hive Software

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



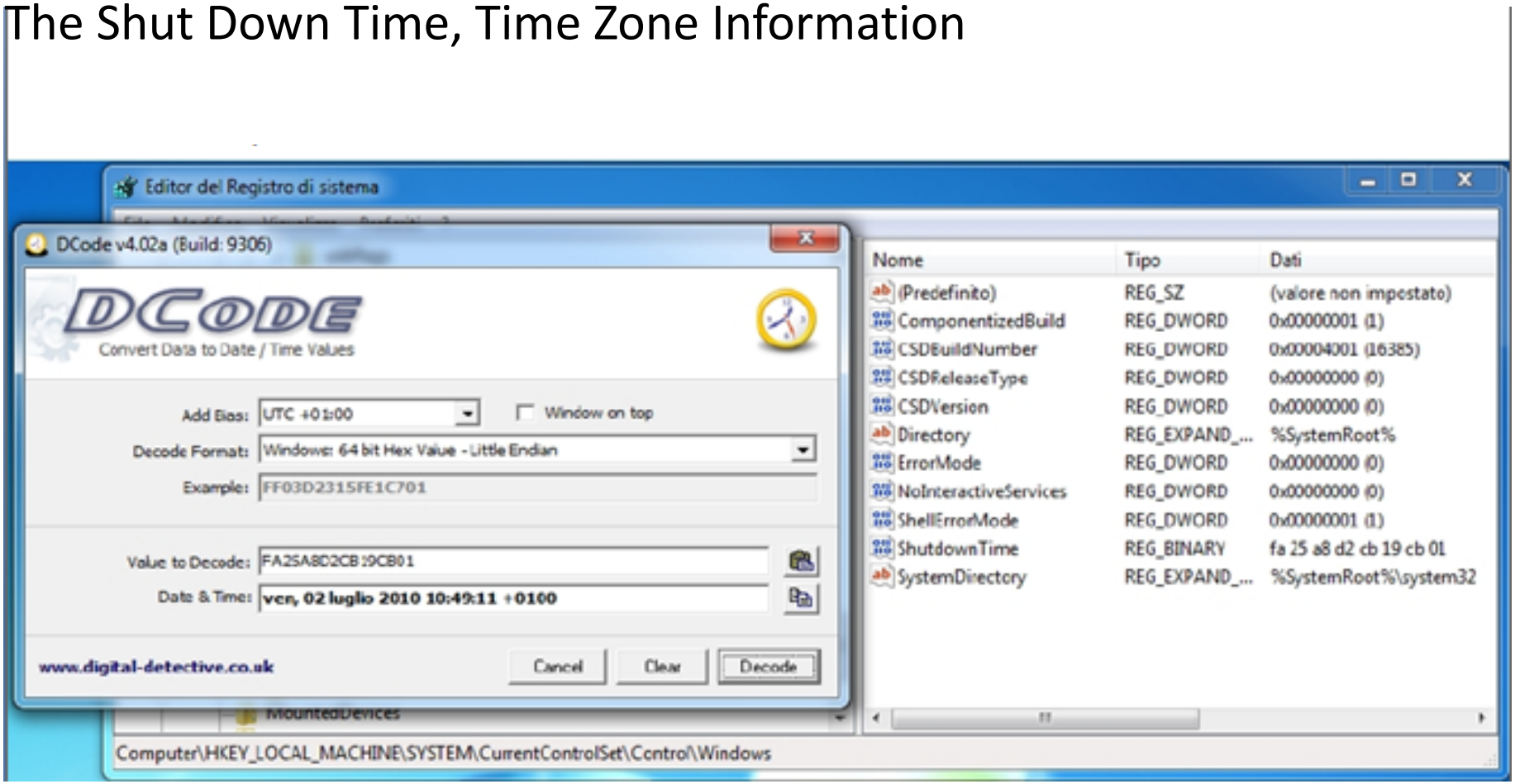
# Windows Registry – Hive Software

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



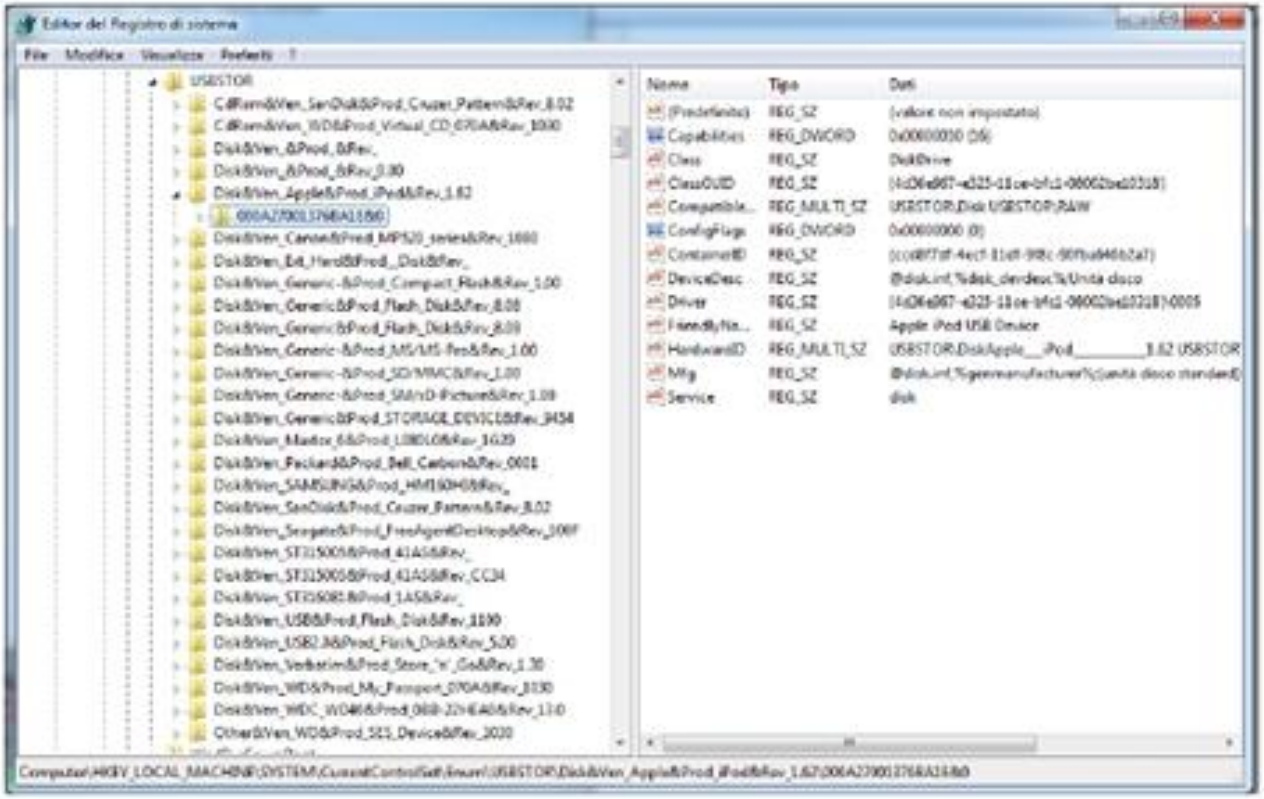
# Windows Registry – Hive Software

The Shut Down Time, Time Zone Information



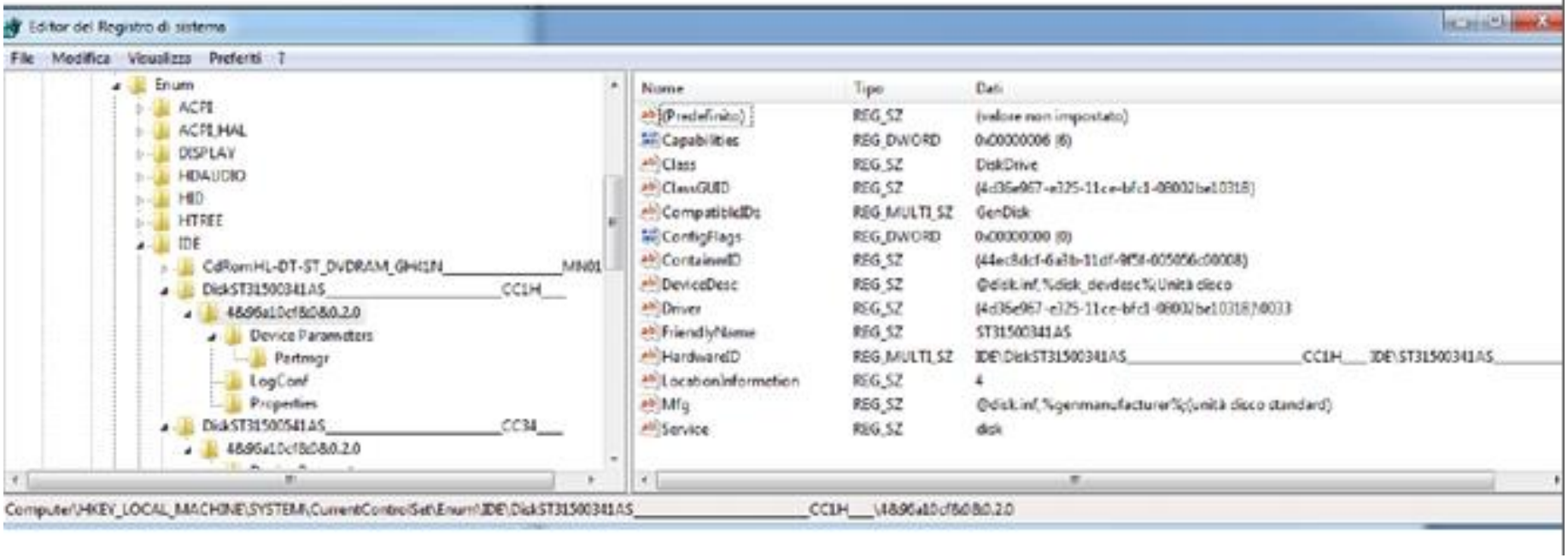
# Windows Registry – Hive System - USB

## HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR



# Windows Registry – Hive System - IDE

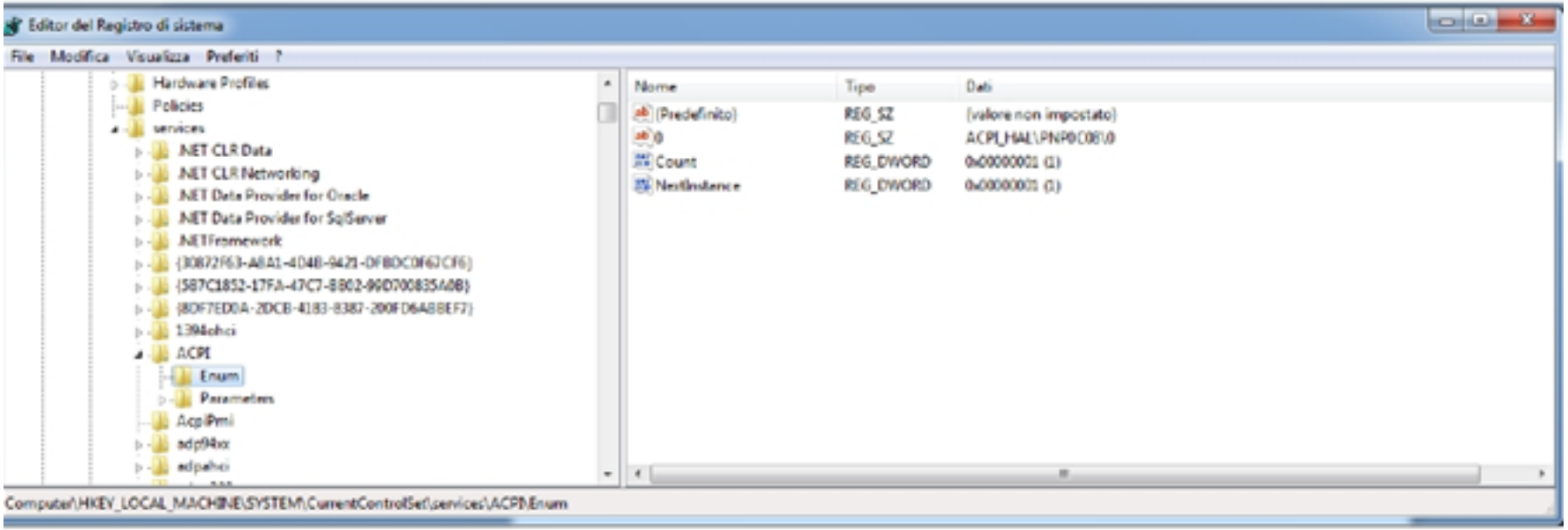
**HKLM\SYSTEM\CurrentControlSet\Enum\IDE**



# Windows Registry – Hive System

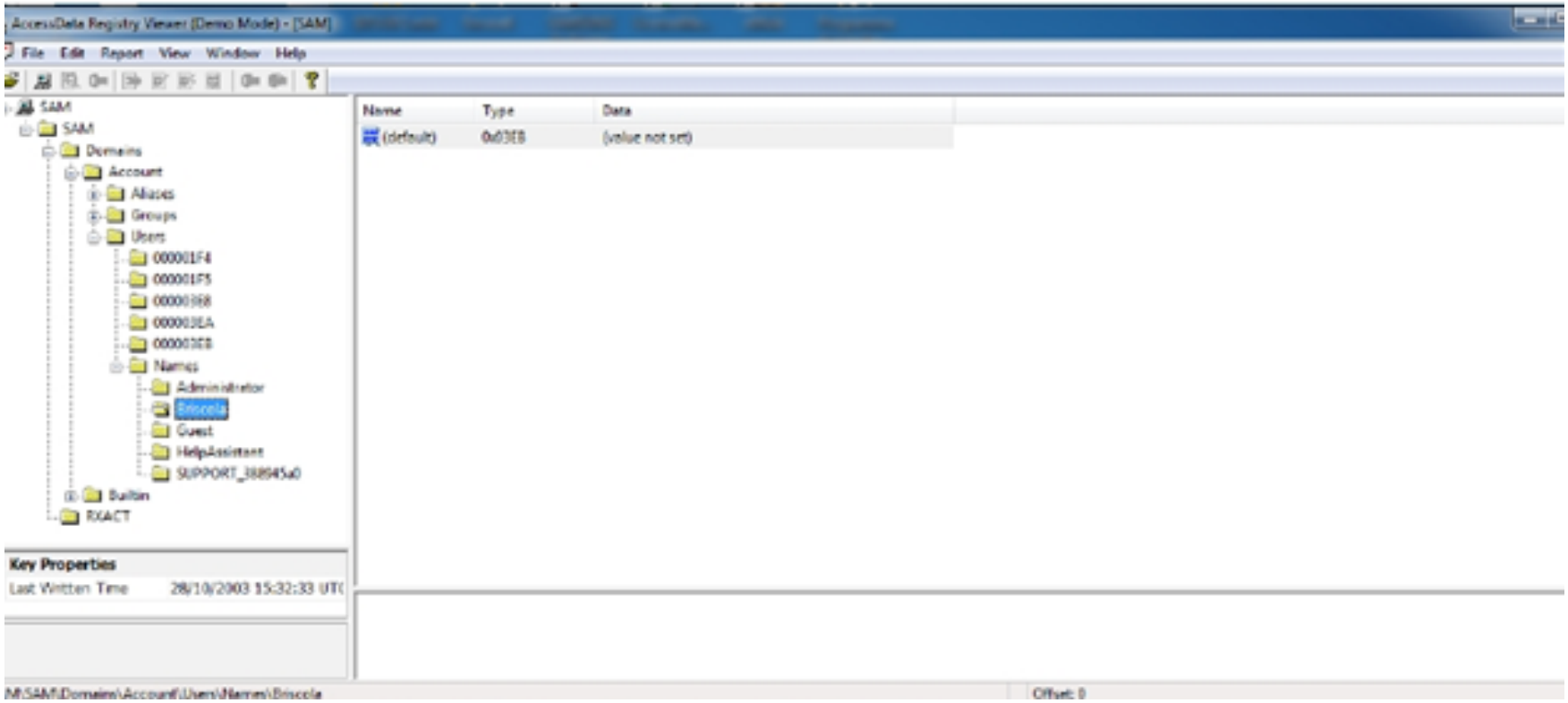
Services Installed in a Computer

**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

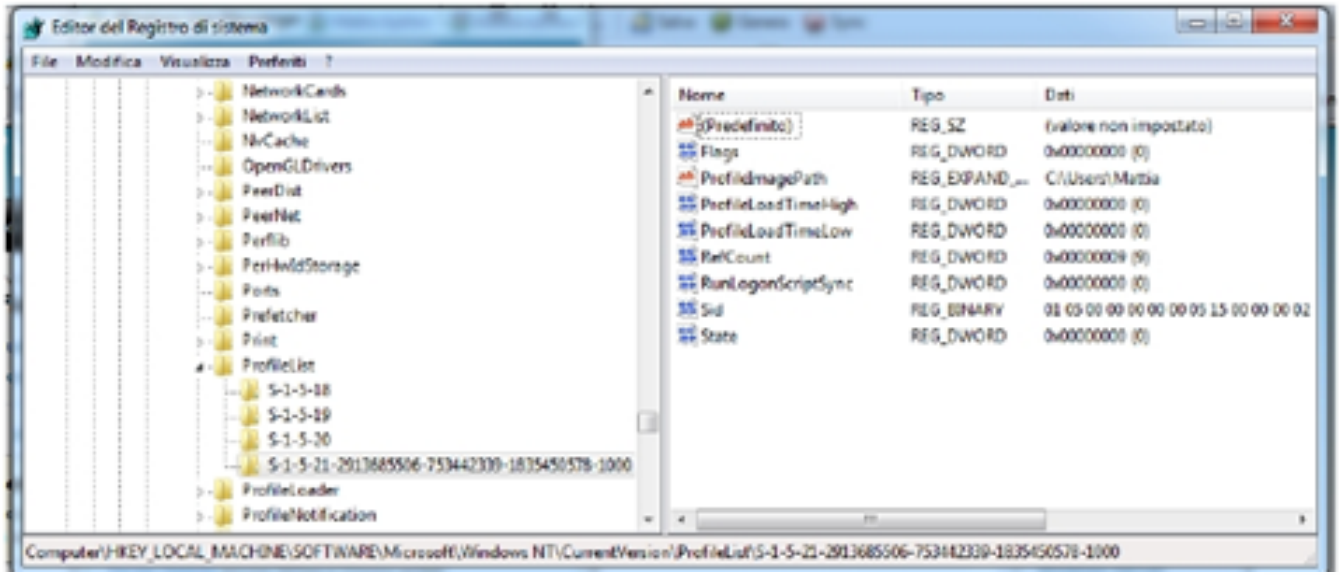



UNIVERSITÀ DI PARMA

# Windows Registry – Hive SAM

## USERS AND GROUP

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



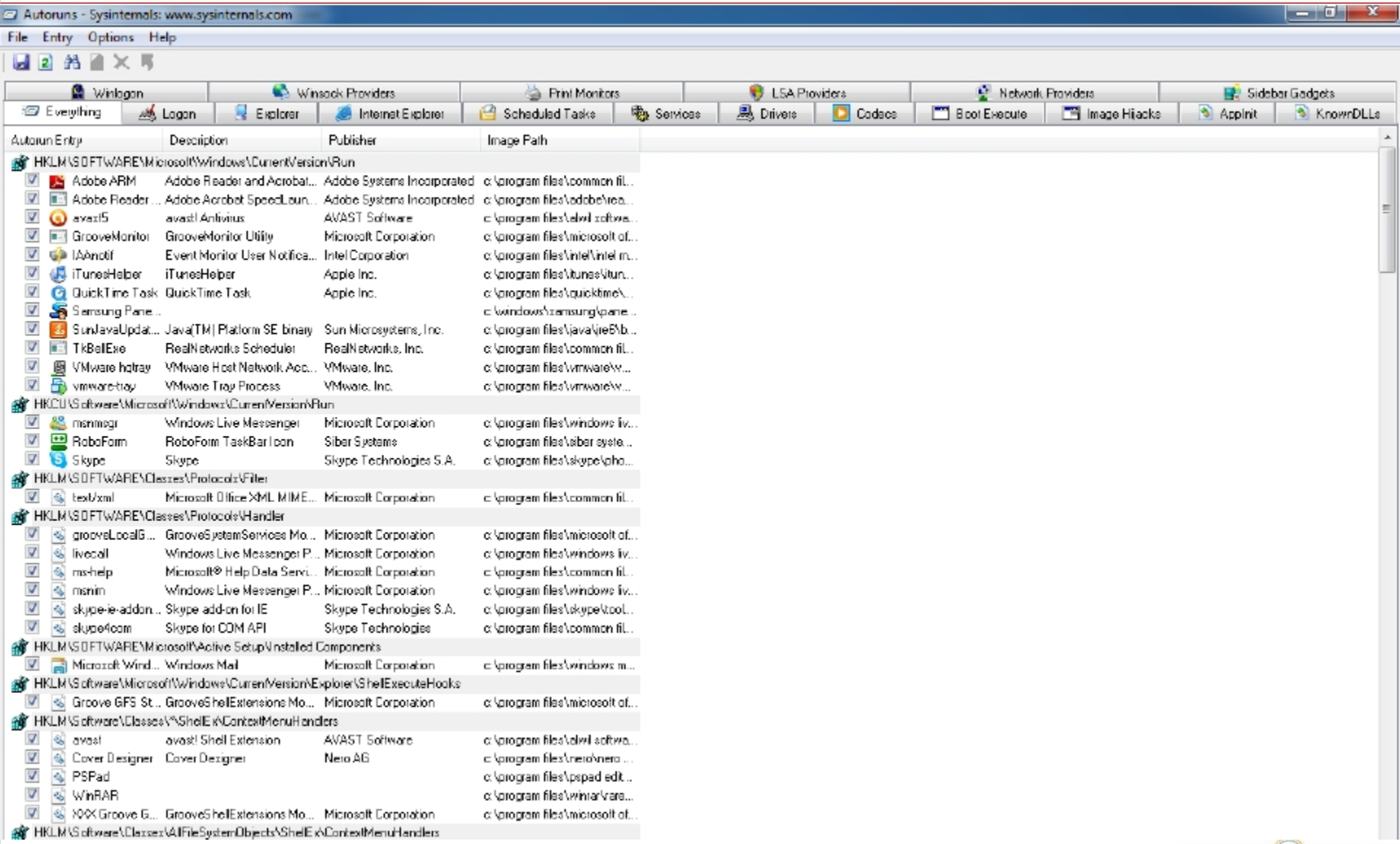
# Autorun

| 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\RunServicesOnes |
| 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


Autoruns - Sysinternals: www.sysinternals.com
File Entry Options Help
Winlogon
Winsock Providers
Print Monitors
LSA Providers
Network Providers
Sidebar Gadgets
Everything
Logon
Explorer
Internet Explorer
Scheduled Tasks
Services
Drivers
Codecs
Boot Execute
Image Hijacks
AppInit
KnownDLLs
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 SpeedLaun...
Adobe Systems Incorporated
c:\program files\adobe\rea...
avgui5
avast! Antivirus
AVAST Software
c:\program files\alwil softwa...
GrooveMonitor
GrooveMonitor Utility
Microsoft Corporation
c:\program files\microsoft of...
IAAnotif
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\jre6\b...
TkBellExe
RealNetworks Scheduler
RealNetworks, Inc.
c:\program files\common fil...
VMware hqtray
VMware Host Network Acc...
VMware, Inc.
c:\program files\vmware\v...
vmware-tray
VMware Tray Process
VMware, Inc.
c:\program files\vmware\v...
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
msnmsgr
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\pho...
HKLM\SOFTWARE\Classes\Protocols\Filter
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...
ms-help
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\alwil softwa...
Cover Designer
Cover Designer
Nero AG
c:\program files\nero\nero ...
PSPad
c:\program files\pspad edit...
WinRAR
c:\program files\winrar\rare...
XXX Groove G...
GrooveShellExtensions Mo...
Microsoft Corporation
c:\program files\microsoft of...
HKLM\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers

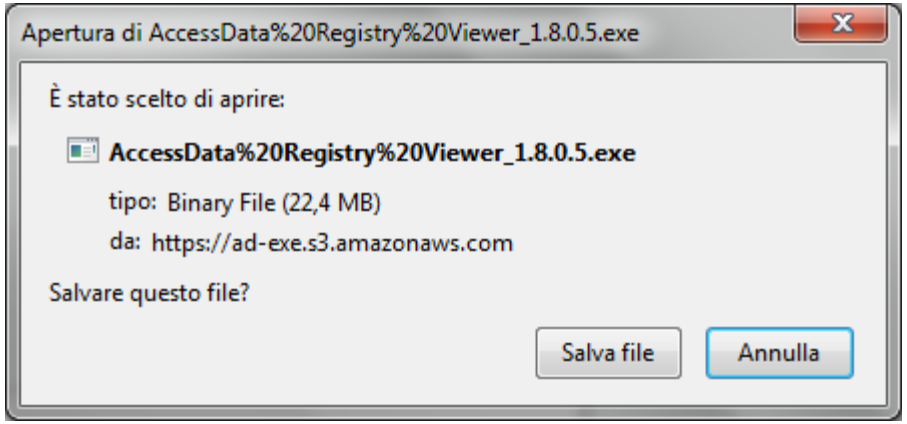
# Hive NETUSER

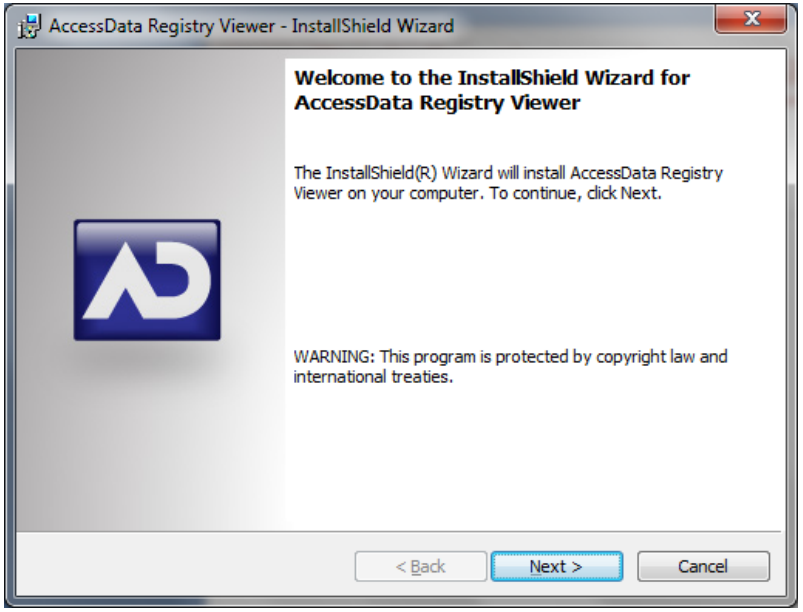
| Chiave |
| --- |
| HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\[GUID]\Count |
| HKU\Software\Microsoft\Windows\ShellNoRoam\MUICache |
| HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs |
| HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU |
| HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU |
| 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

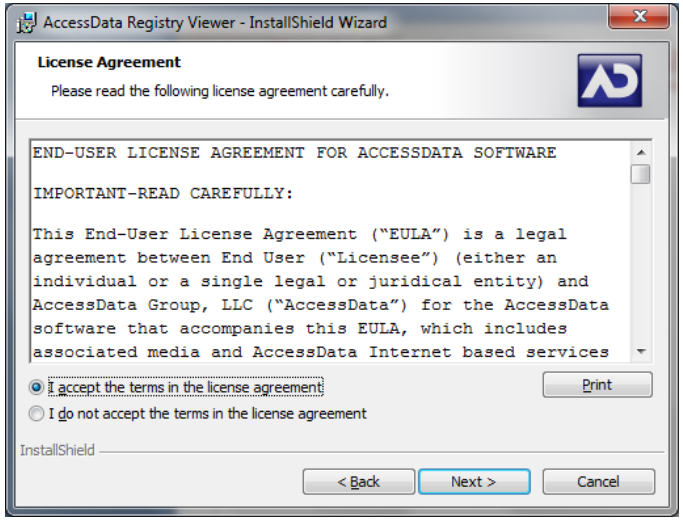
- **RegRipper (Harlan Carvey) O**penSource;
- **AccessData Registry Viewer - free**
- **Windows Registry Recovery** (www.mitec.cz) **free**
- **Windows Registry Analyzer** (www.mitec.cz) **free**
- **RegExtract** (www.woanware.co.uk) **free**
- **USBDeviceForensics** (www.woanware.co.uk)
- **ForensicsUserInfo**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

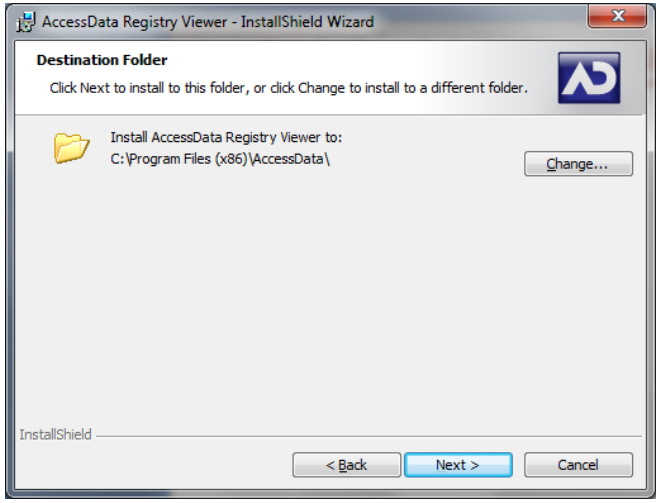
# Tools for the register analysis

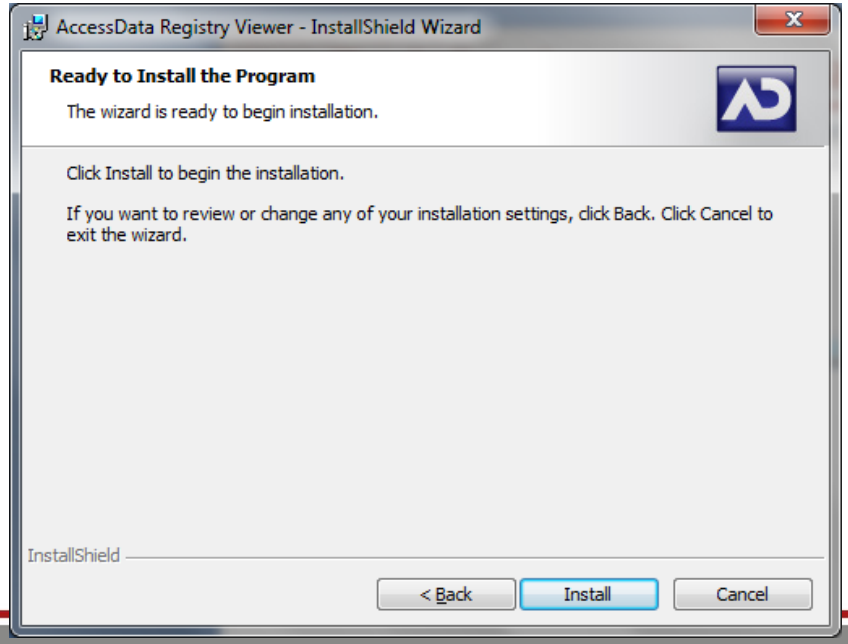



# Tools for the register analysis

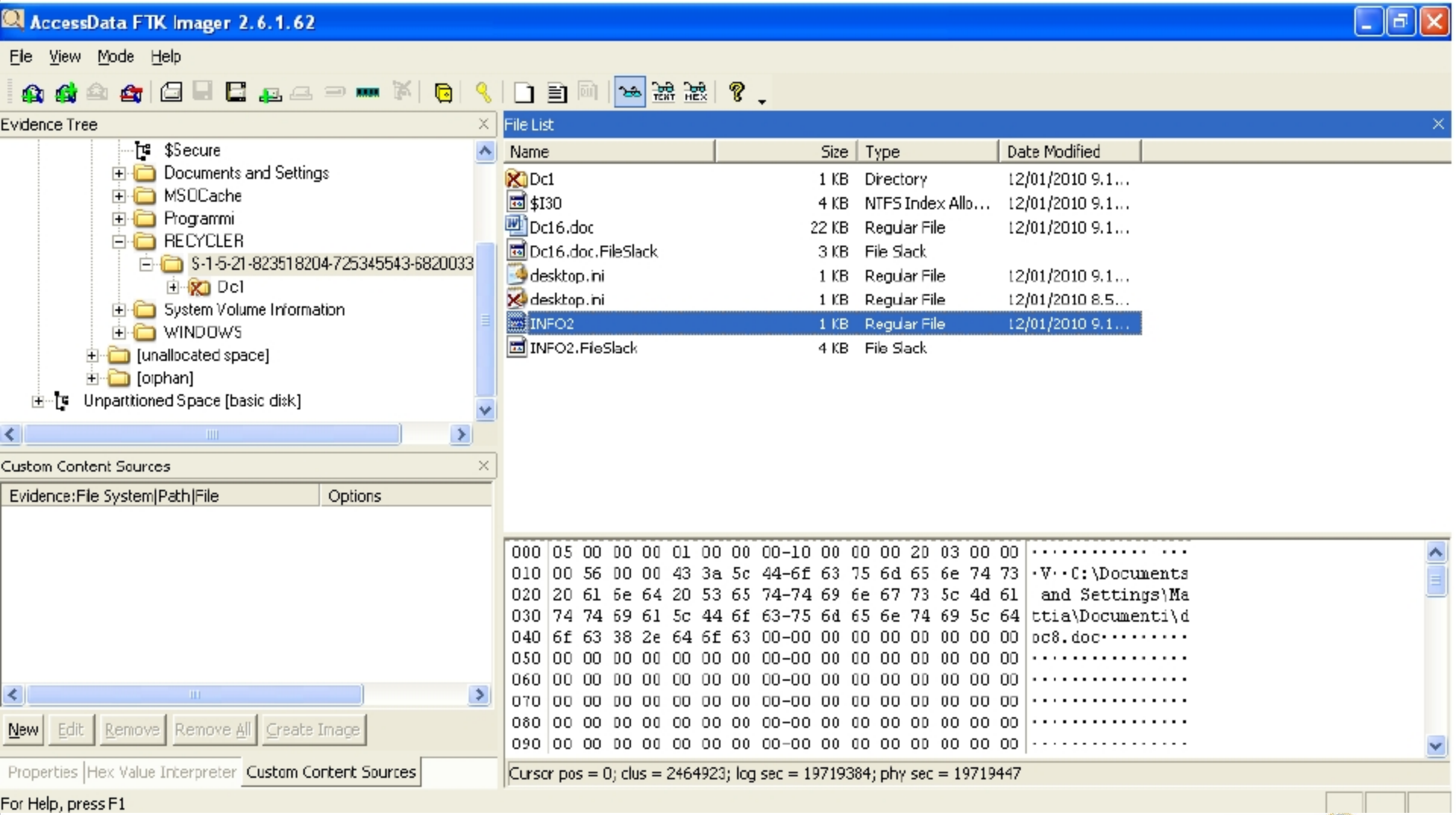



UNIVERSITÀ DI PARMA

# 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
Dc1
System Volume Information
WINDOWS
[unallocated space]
[orphan]
Unparttioned Space [basic disk]
File List
Name Size Type Date Modified
Dc1 1 KB Directory 12/01/2010 9.1...
$I30 4 KB NTFS Index Allo... 12/01/2010 9.1...
Dc16.doc 22 KB Regular File 12/01/2010 9.1...
Dc16.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
New Edit Remove Remove All Create Image
Properties Hex Value Interpreter Custom Content Sources
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
020 20 61 6e 64 20 53 65 74-74 69 6e 67 73 5c 4d 61
030 74 74 69 61 5c 44 6f 63-75 6d 65 6e 74 69 5c 64
040 6f 63 38 2e 64 6f 63 00-00 00 00 00 00 00 00 00
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
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

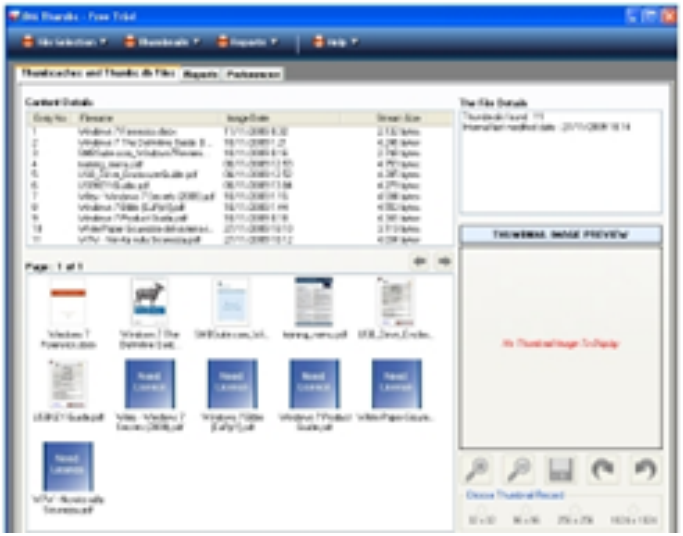
- **Windows File Analyzer** (www.mitec.cz)
  - 
- **Win Forensic Analysis** (http://www.machor-software.com/)
- **Link Viewer** (http://www.gaijin.at/)
- **Lnkanalyser** (http://www.woany.co.uk/)
- **SimpleCarver** (http://www.simplecarver.com/)

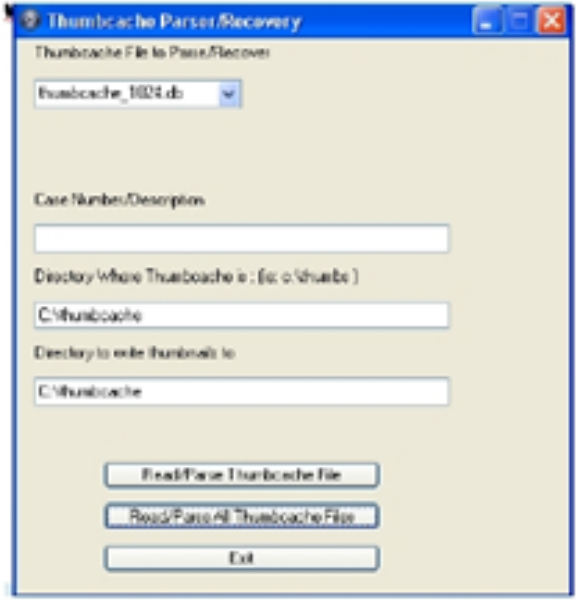
# Tools for analyzing registry

- **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

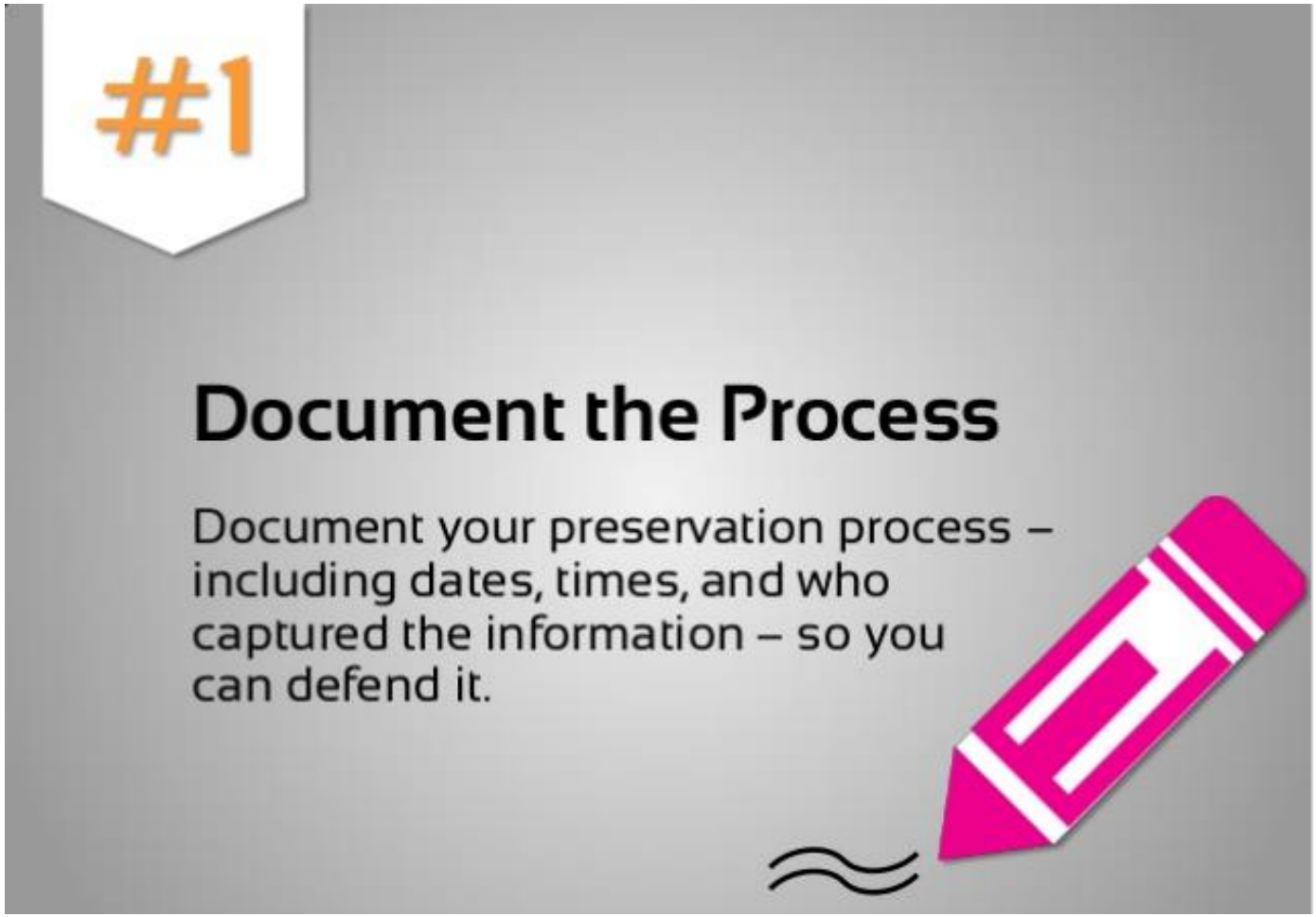




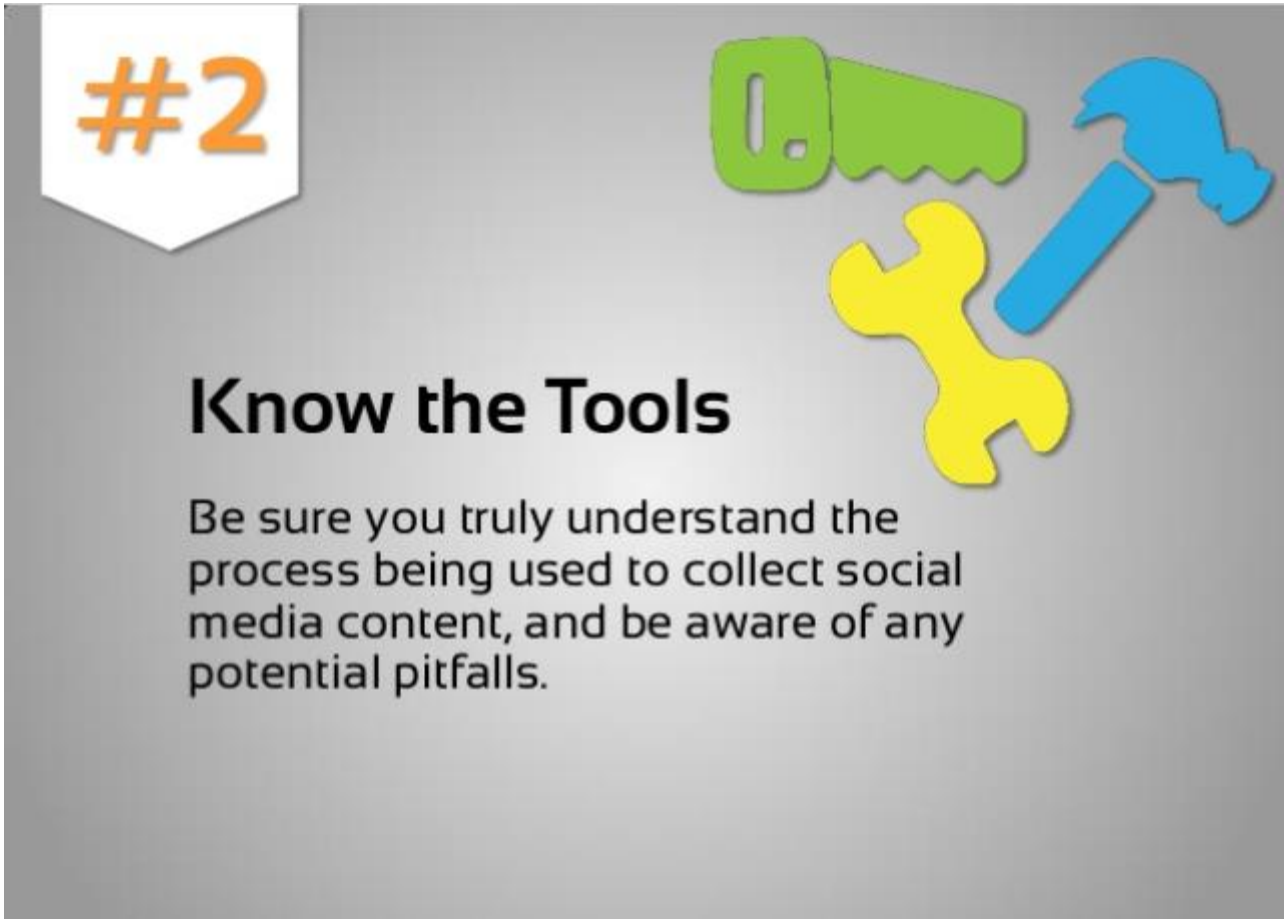
# Internet Artifacts

# Internet Artifacts

# Internet Artifacts



# Internet Artifacts



# Internet Artifacts

# Internet Artifacts

# 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.

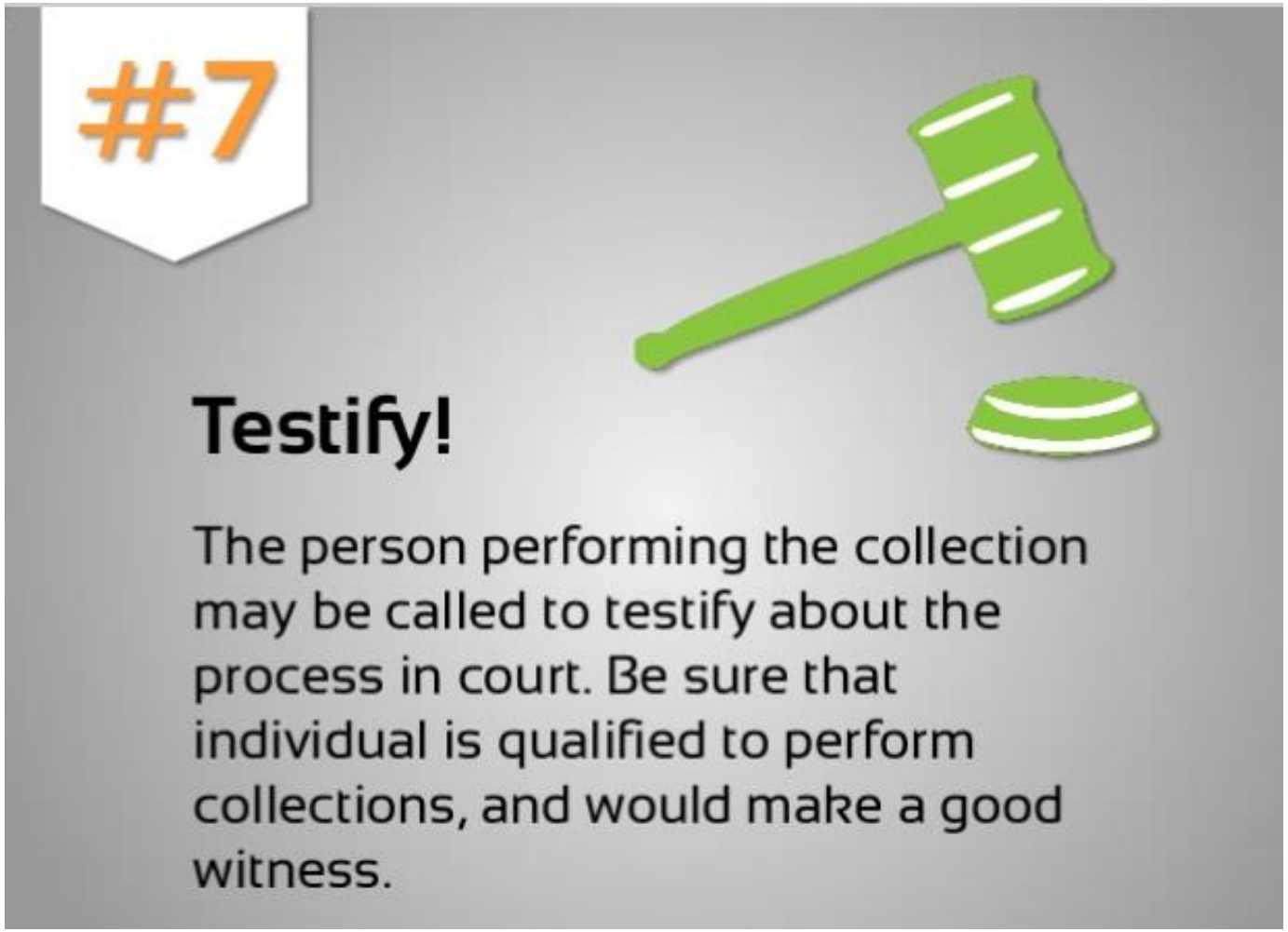
# Internet Artifacts

#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.

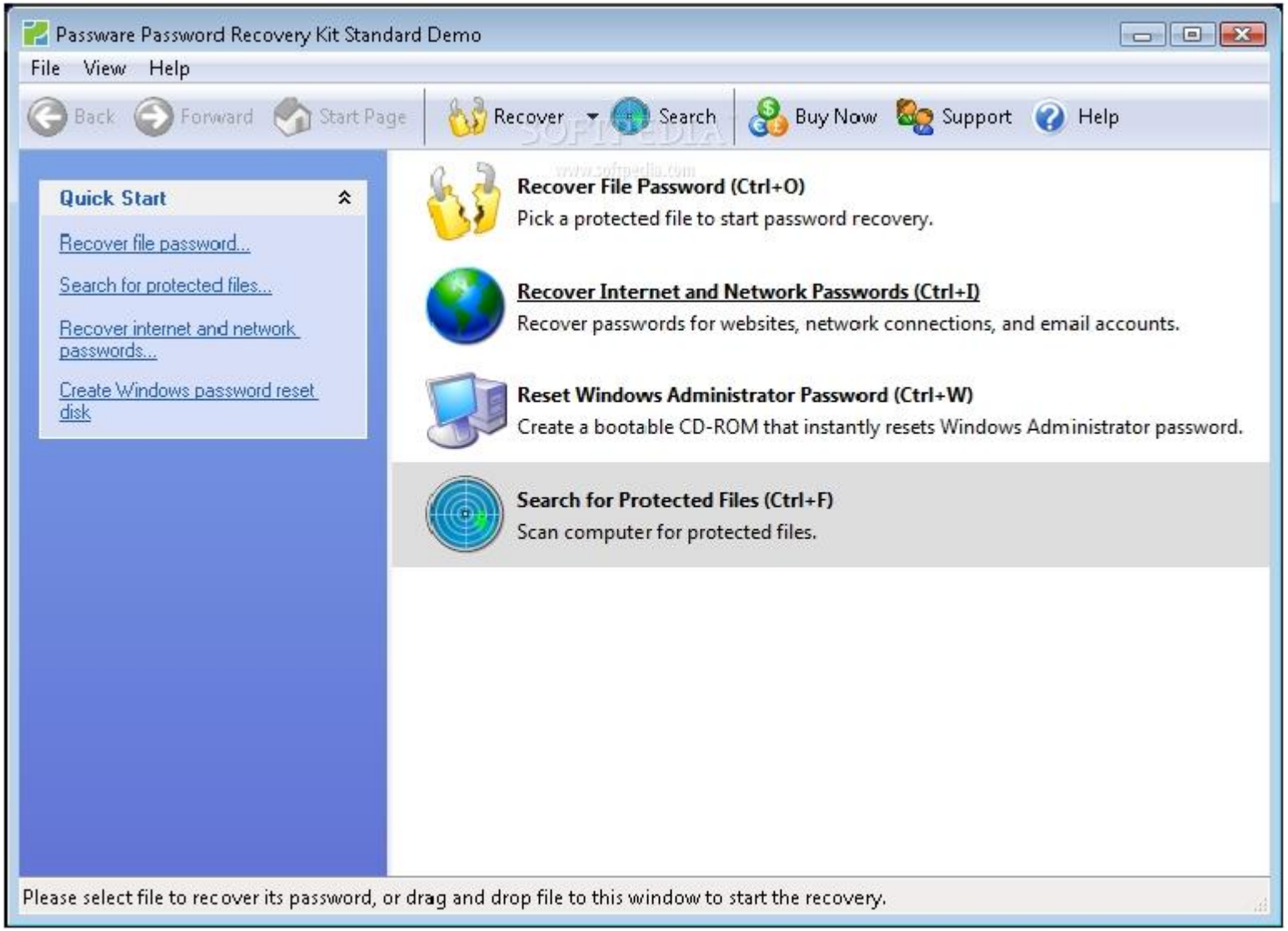
# Internet Artifacts



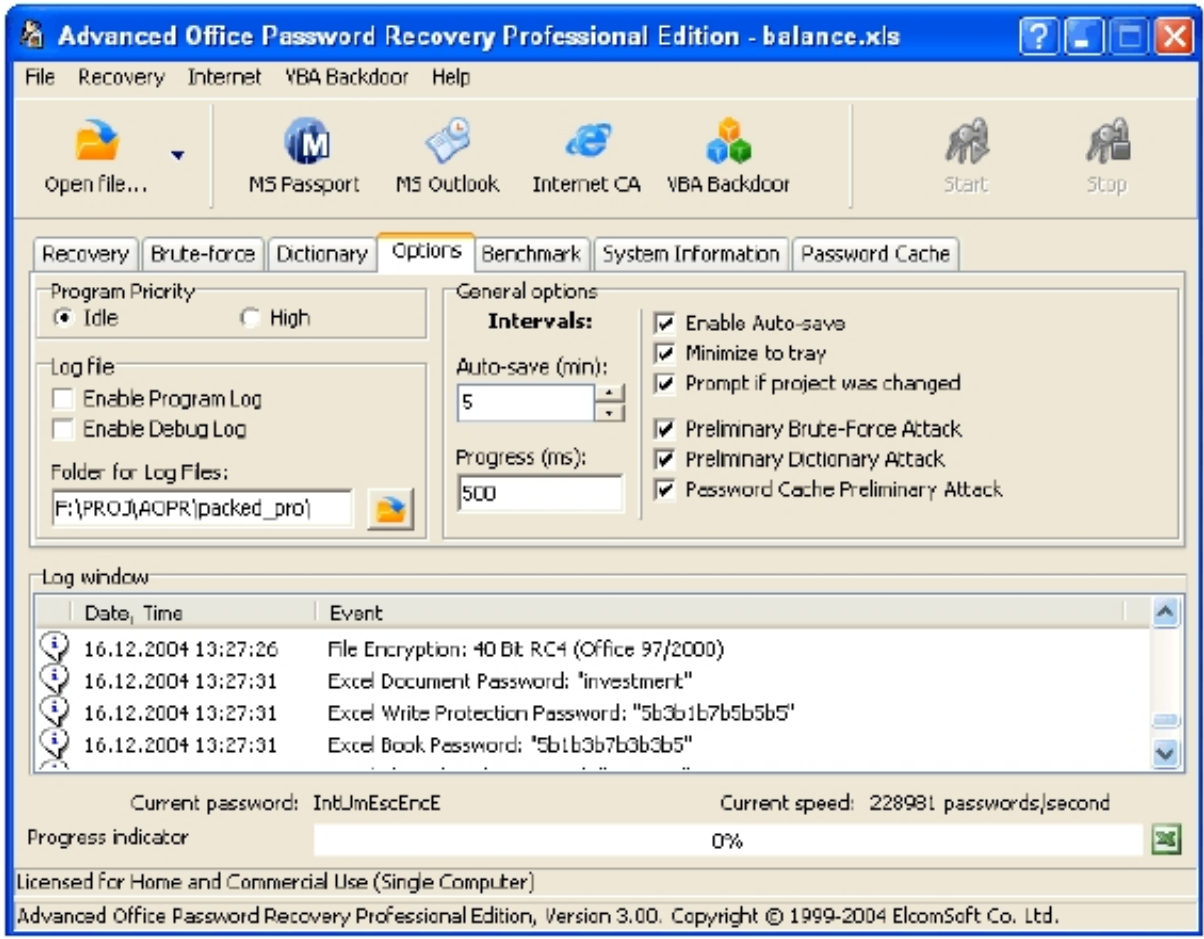
# File password cracking

- 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 Recory Kit

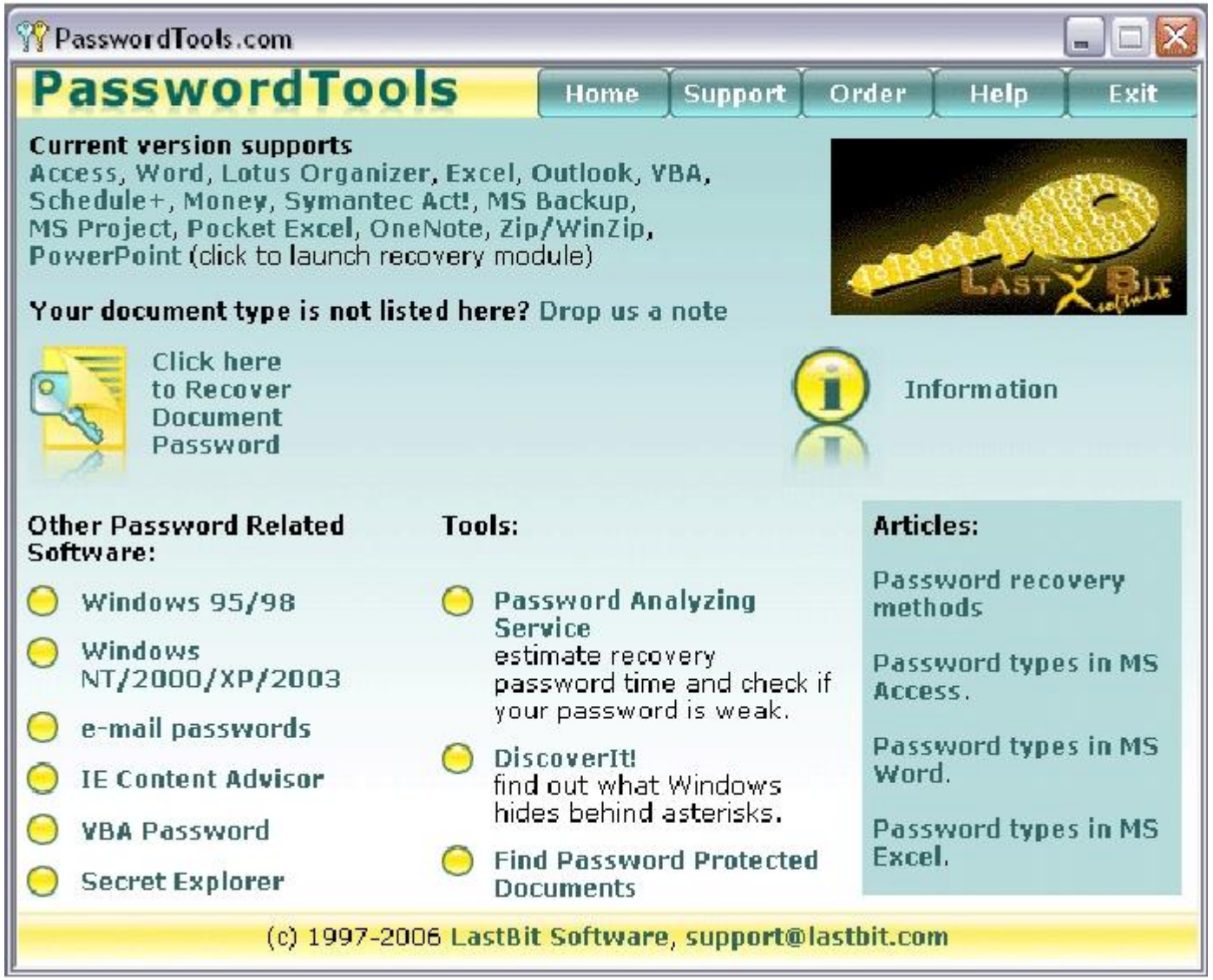


# Elcomsoft Password Recovery Bundle

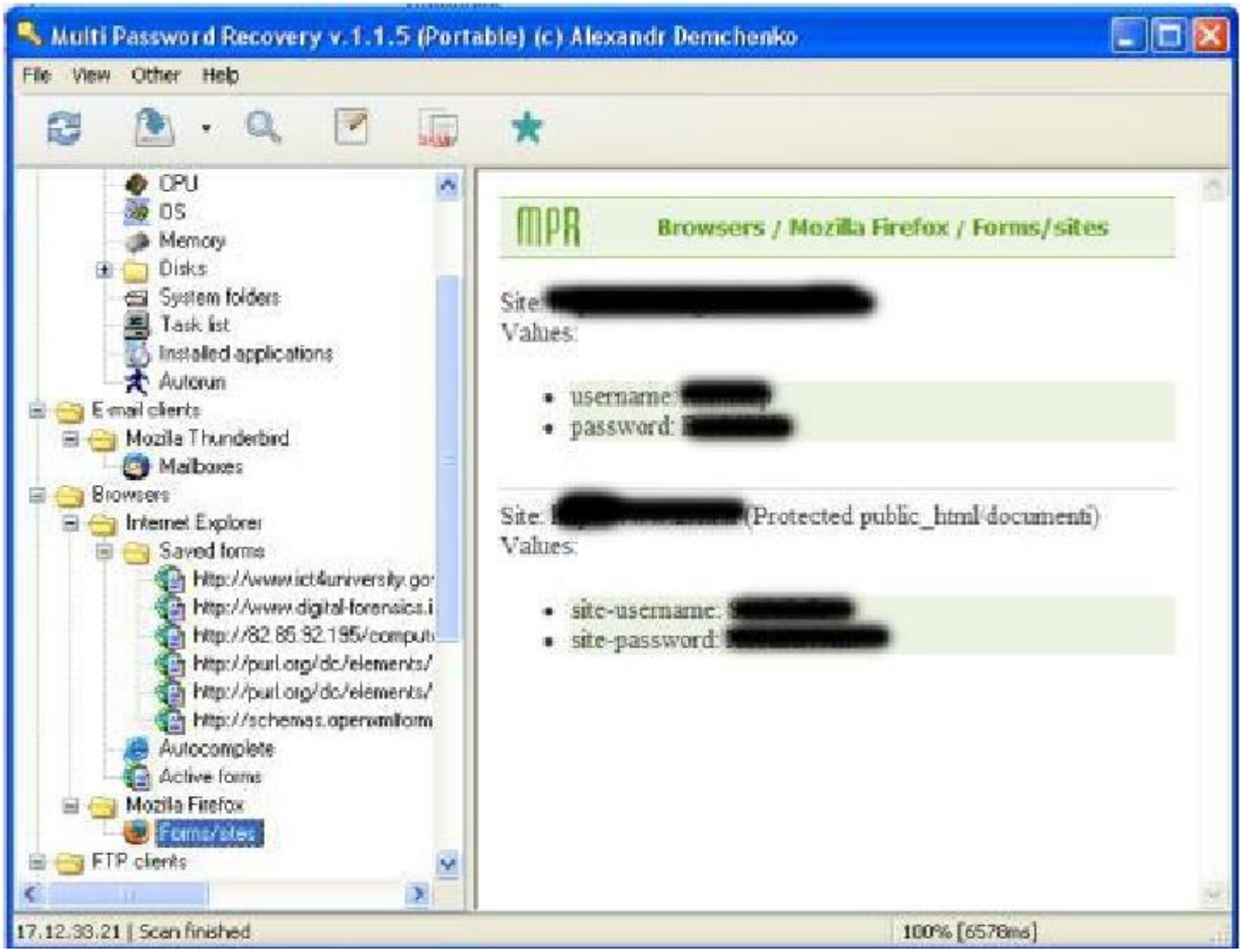

UNIVERSITÀ DI PARMA

# LastBit Passwor Recovery




UNIVERSITÀ DI PARMA

# Multi Password Recovery Portable




UNIVERSITÀ DI PARMA

# 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.abyssalsoft.com/)
- Recovery Toolbox for CD
  - (http://www.recoverytoolbox.com/it/cd.html)
- CD/DVD Inspector
  - (http://www.infinadyne.com)

# Operating steps

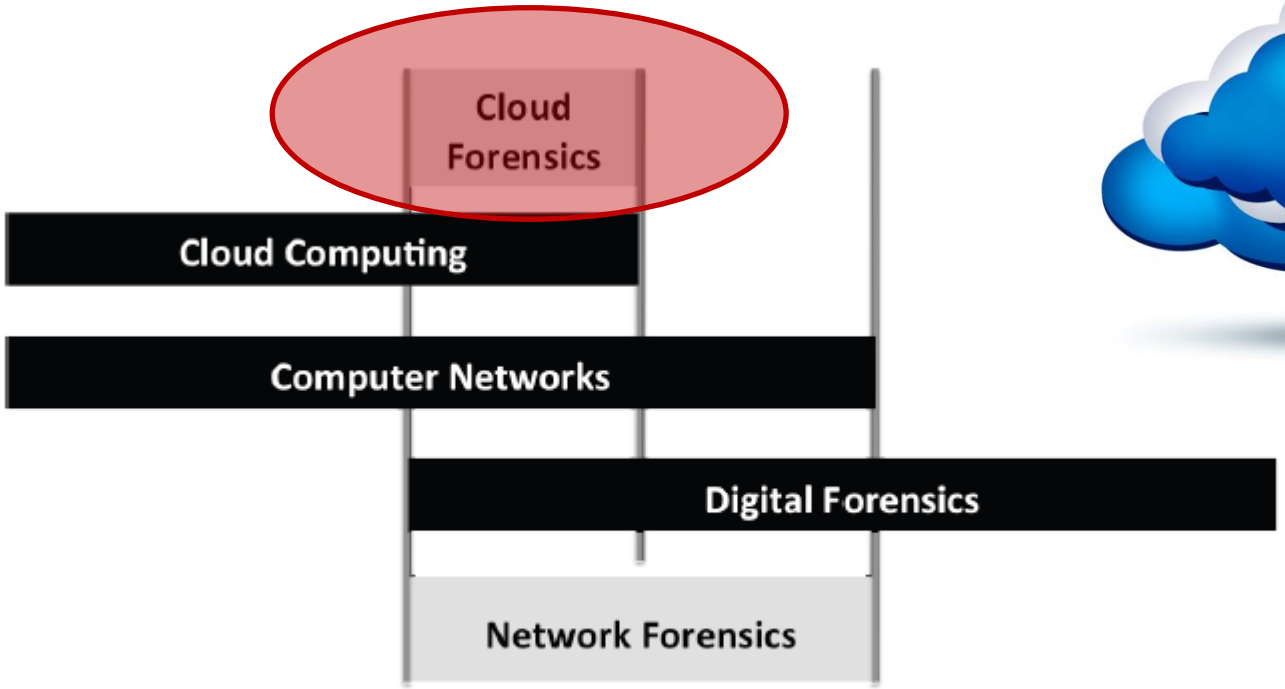
- Preparation and Identification
- Acquisition and Retention
- Analysis
- **Evaluation and presentation**

# 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

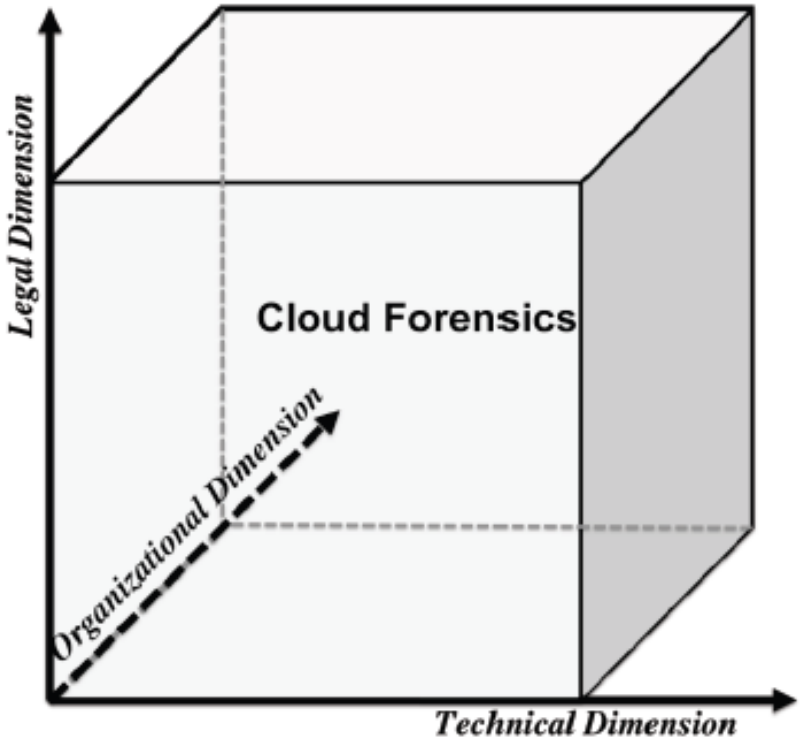
# Cloud Forensics

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




# 3 Dimension

The 3 dimensions in Cloud Forensics



# Tecnical

**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!!).

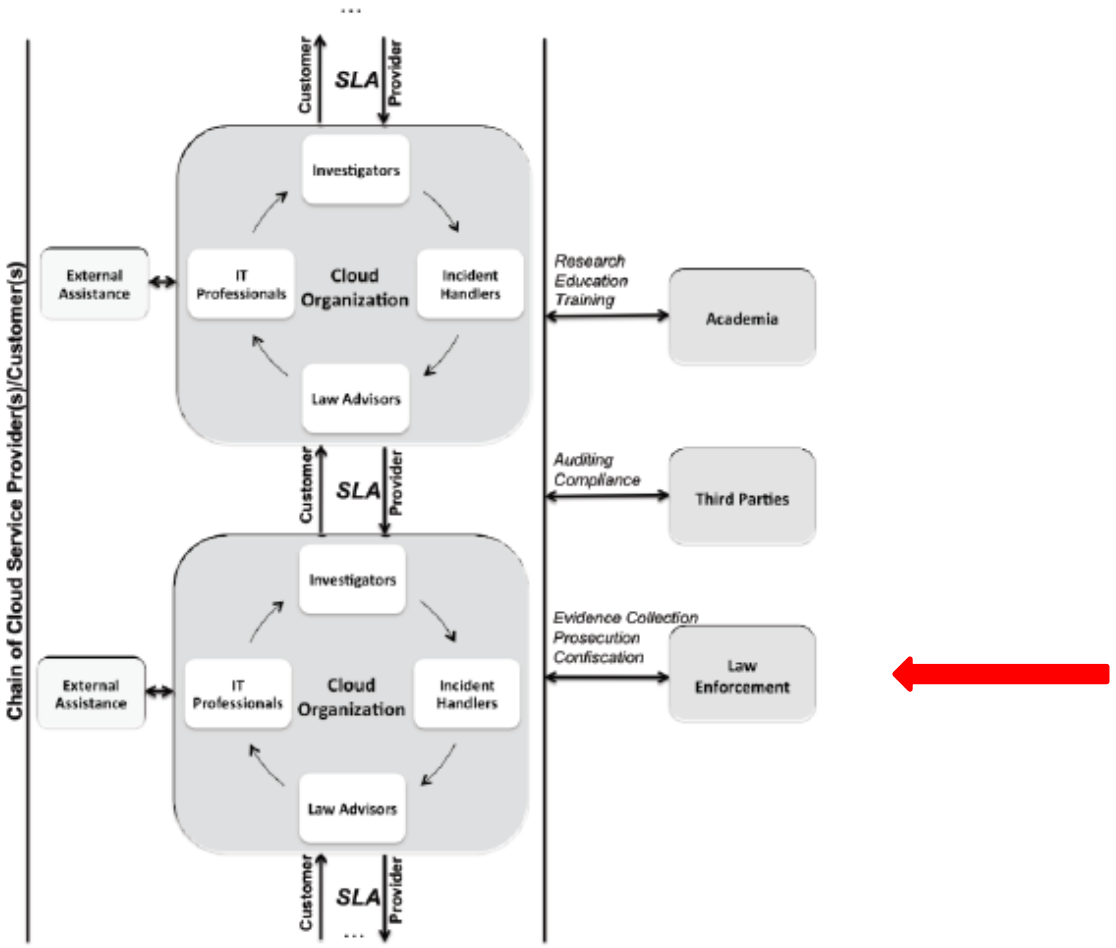
# Tecnical/1

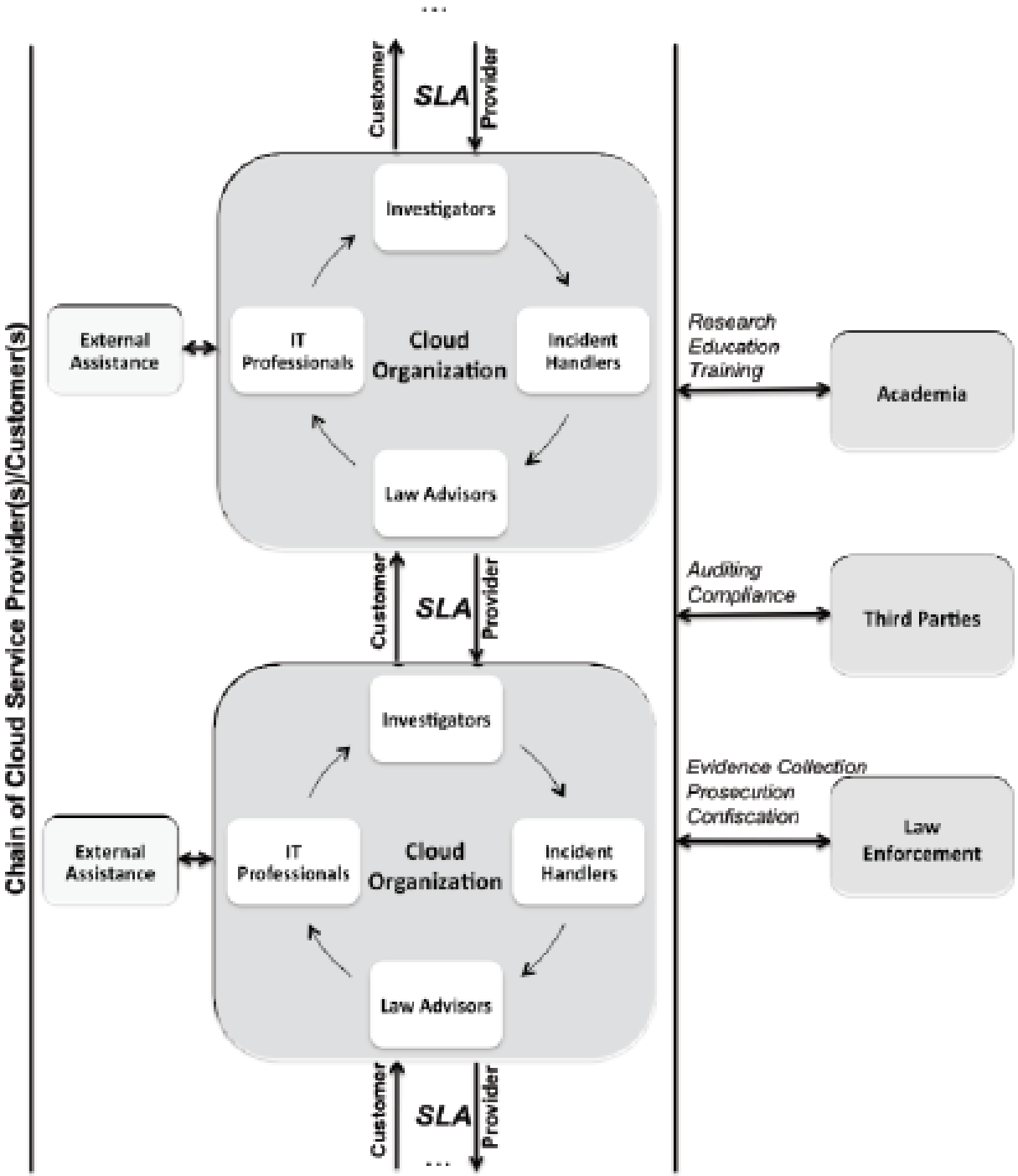
It is **not so** easy to develop those procedures and tools that must be used in order to physically identify the needed data into a given timeframe; then tracing the data itself (into a given  timeframe) tooking into consideration domestic juridictions.

• **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 developped 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 Investigatons 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-juridisctional 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 claryfing 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???**

# The Cloud -----

**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

**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=fb848980-7551-11e4-8648-00000aacb35e&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

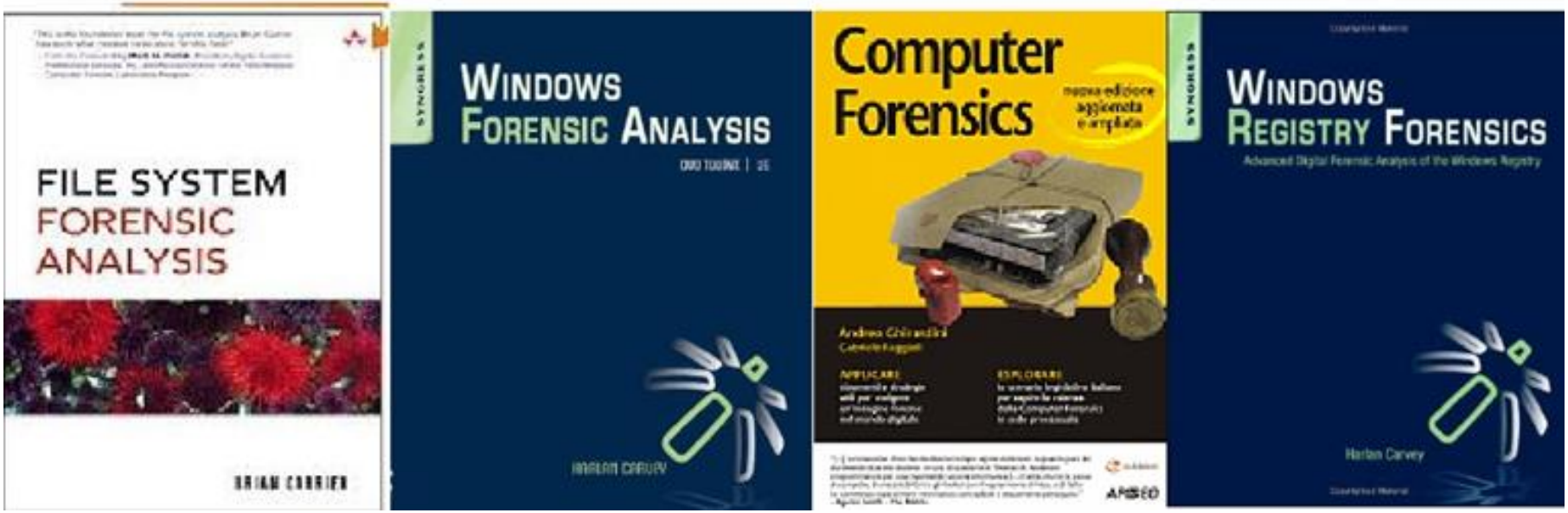
# Standardization

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



sg@security-brokers.com



Security Brokers scpa
Via Giuseppe Frua, 16 - 20146 Milano (Italy)
Email: info@security-brokers.com - Website: http://www.security-brokers.com