EUROPEAN UNION

EXPERTISE FRANCE

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

Index

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.

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 ASSOCIATIOI**
- Technical Assessor at Civil and Criminal Court
- Official Traininer NATO & US NAVY
- VP & Head of Digital Forensics Unit @ Security Brokers,
- Advisor @European Courage Focus Group – Cyber Terrorism & CyberCrime
- ITU ROSTER OF EXPERTS

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

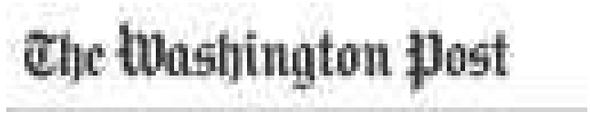
- At first the Digital Forensics has been used only for technological crimes (the "Common").
  - Computer intrusions;
  - Web defacement;
  - Damaging / Theft of data;
  - Pedophilia Online;
  - Phishing / Whaling;
  - Identity Theft and Fraud Banking.
- In other cases, the computers were simply ignored

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



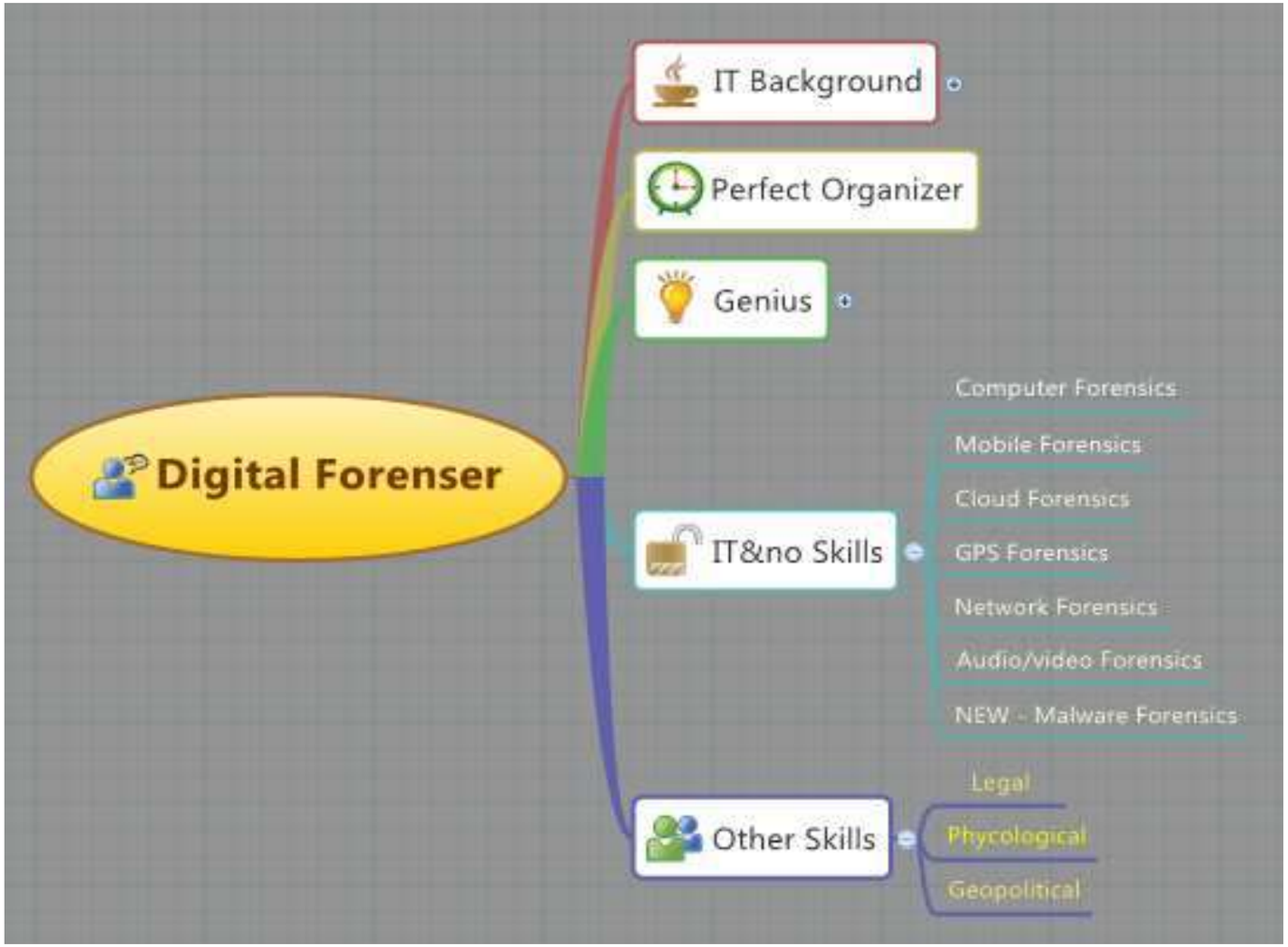
DF INTRODUCTION / 3

- It is therefore clear how the analysis of digital evidences is necessary even for crimes that have nothing to deal with 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



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:

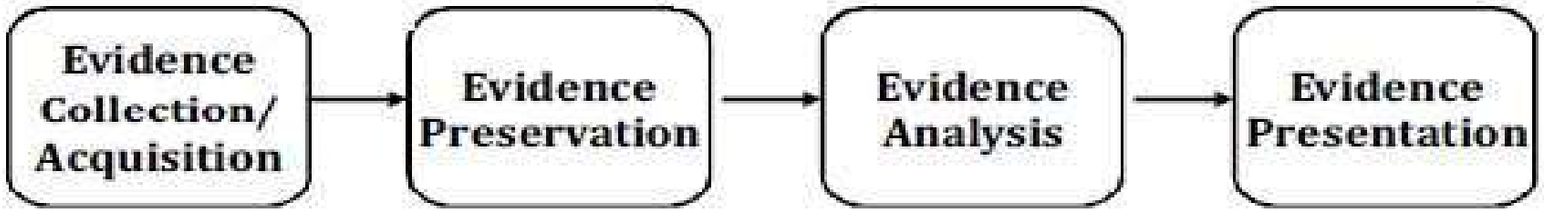
- A digital storage device
- Personal computers, notebook computers, external hard drive, floppy, tape, CD / DVD, memory card, USB drive, ...
- Mobile phones, SIM, SmartPhone, Tablet, SatNav, ...
  An Intranet / Internet
- Interception of data traffic
  Web pages, Blog, Social Network, Chat / IM, P2P,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

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.

DIGITAL EVIDENCE

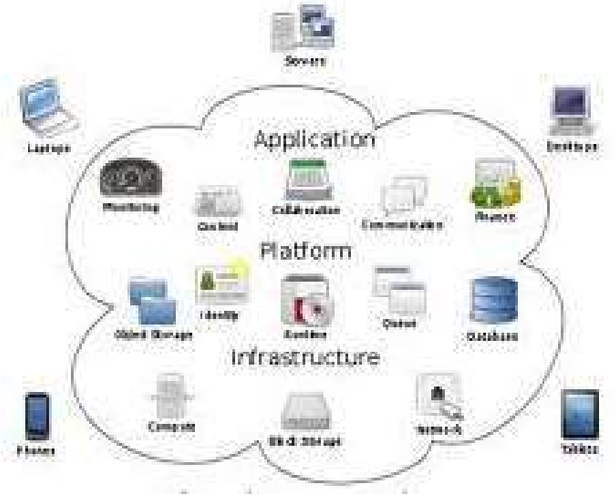
- The digital data can be divided into two categories:
- volatile data
  - Data stored in volatile memories that are lost if you turn off the device that saves;
    Users connected, open files, network information, running processes, mapping of processes on ports, RAM contents, clipboard contents, services 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

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.

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)

THE ORIGINS

HARD DISK

HARD DISK

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

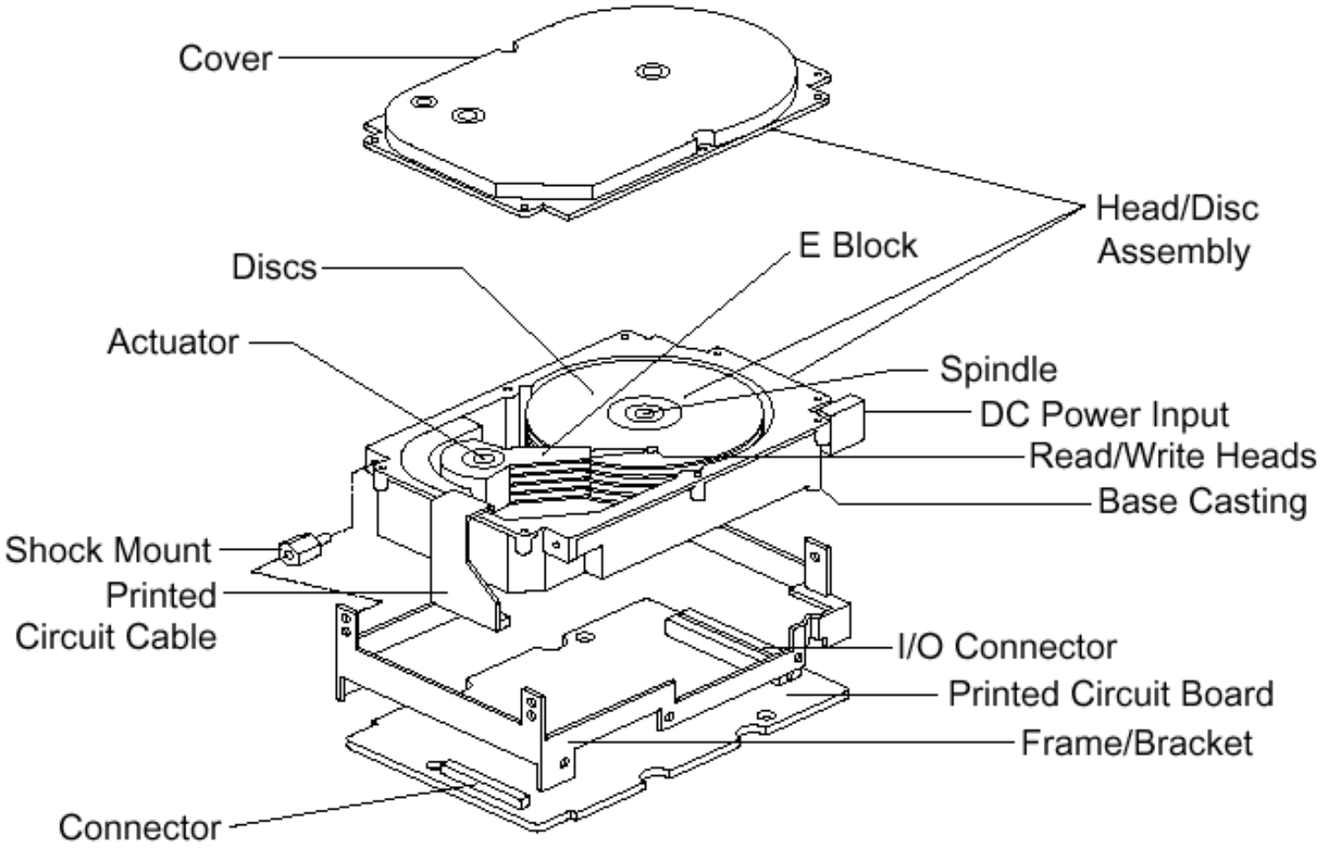
- The main components of a hard drive are:
  - Cylinders (cylinders)
  - Heads (heads)
  - Dishes (platters)

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

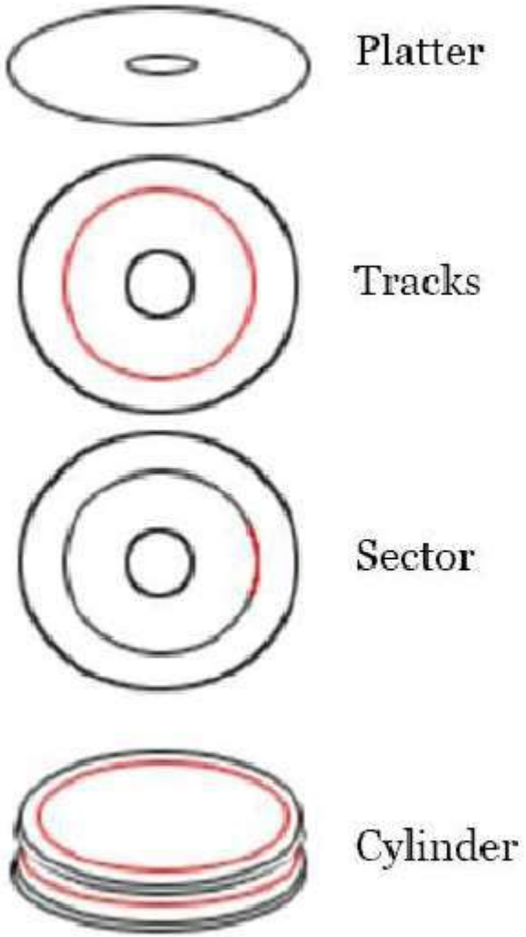
HARD DISK

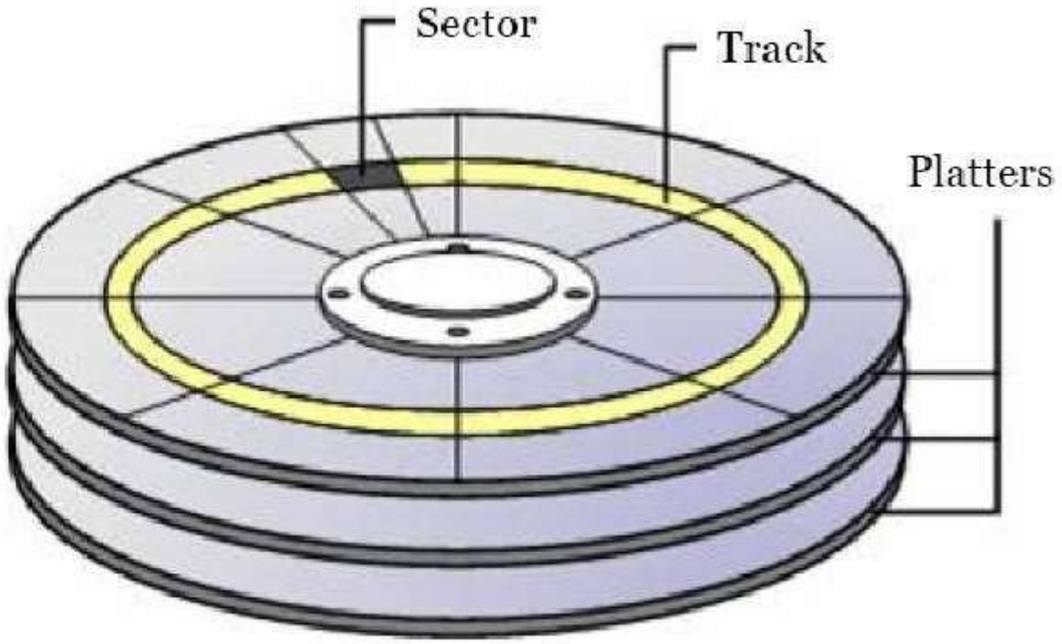
- When organizing data logic sectors are aggregated into clusters
- A hard disk is composed of a stack of plates, with read / write positioned above and below each plate
- During the rotation of the plates, the head moves from inside to outside (and vice versa) to read and write data

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: 35mm
HD68m (SCSI-3)
Aprox: 47mm
HD68f (SCSI-3)
Aprox: 45mm
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

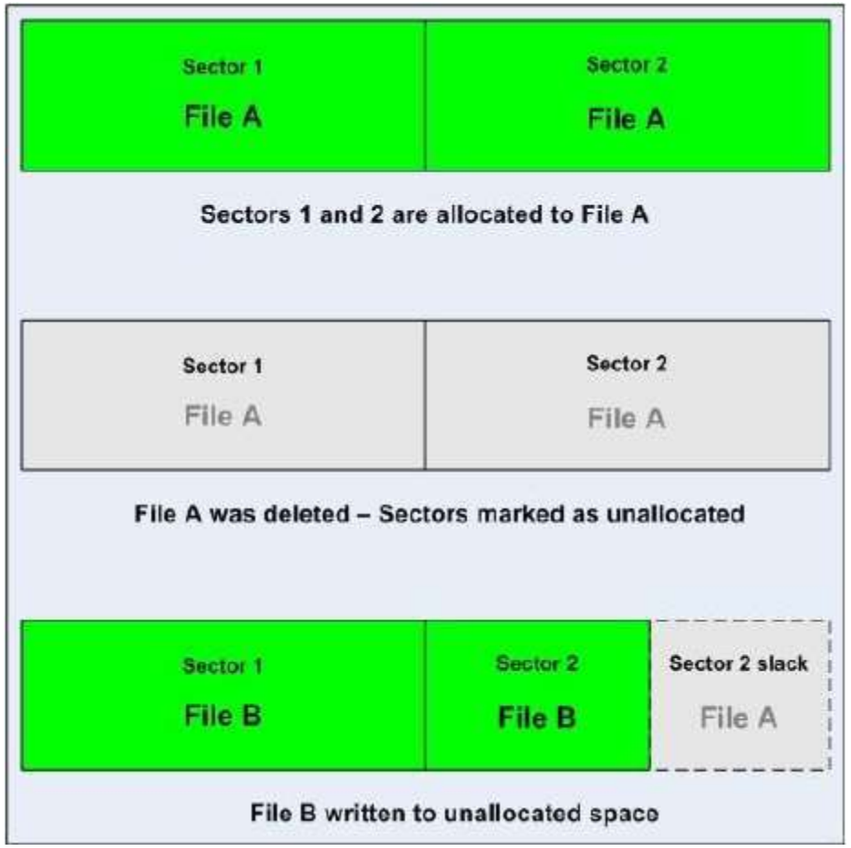
Address			Description		Size in bytes
Hex	Oct	Dec			
0000	0000	0	Code Area		440 (max. 446)
01B8	0670	440	Optional Disk signature		4
01BC	0674	444	Usually Nulls; 0x0000		2
01BE	0676	446	**Table of primary partitions** (Four 16-byte entries, IBM Partition Table scheme)		64
01FE	0776	510	55h	MBR signature; 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



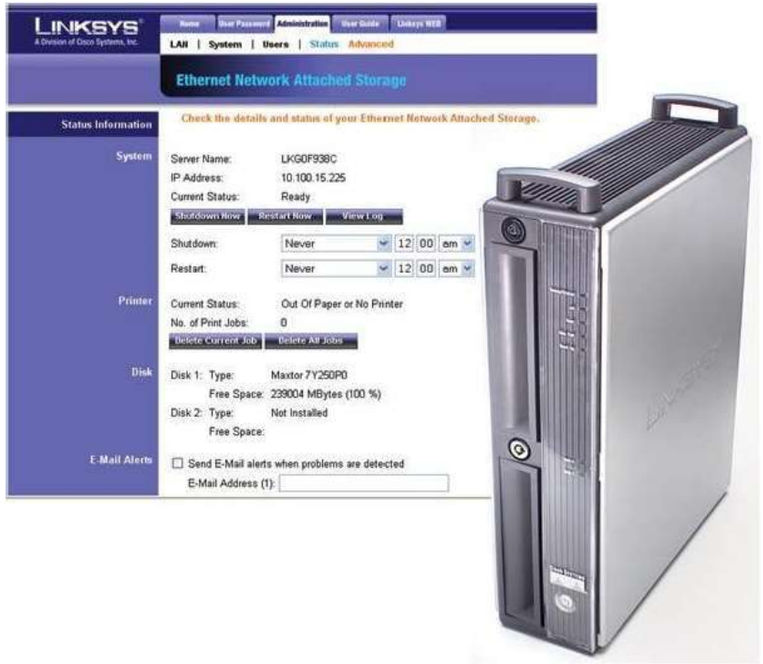
SSD

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

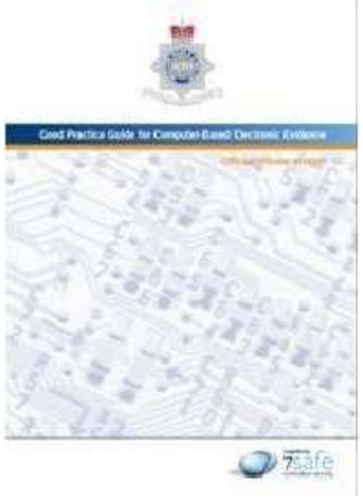
USB DRIVES

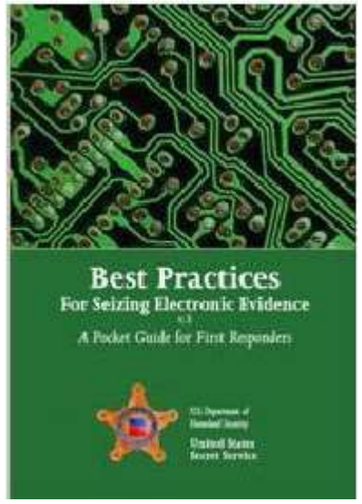
MP3, Video cameras, Cameras, Tablet

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





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 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

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

EUROPEAN UNION

FUNDAMENTAL RULE

Preserve the Original!

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**

Tsurugi

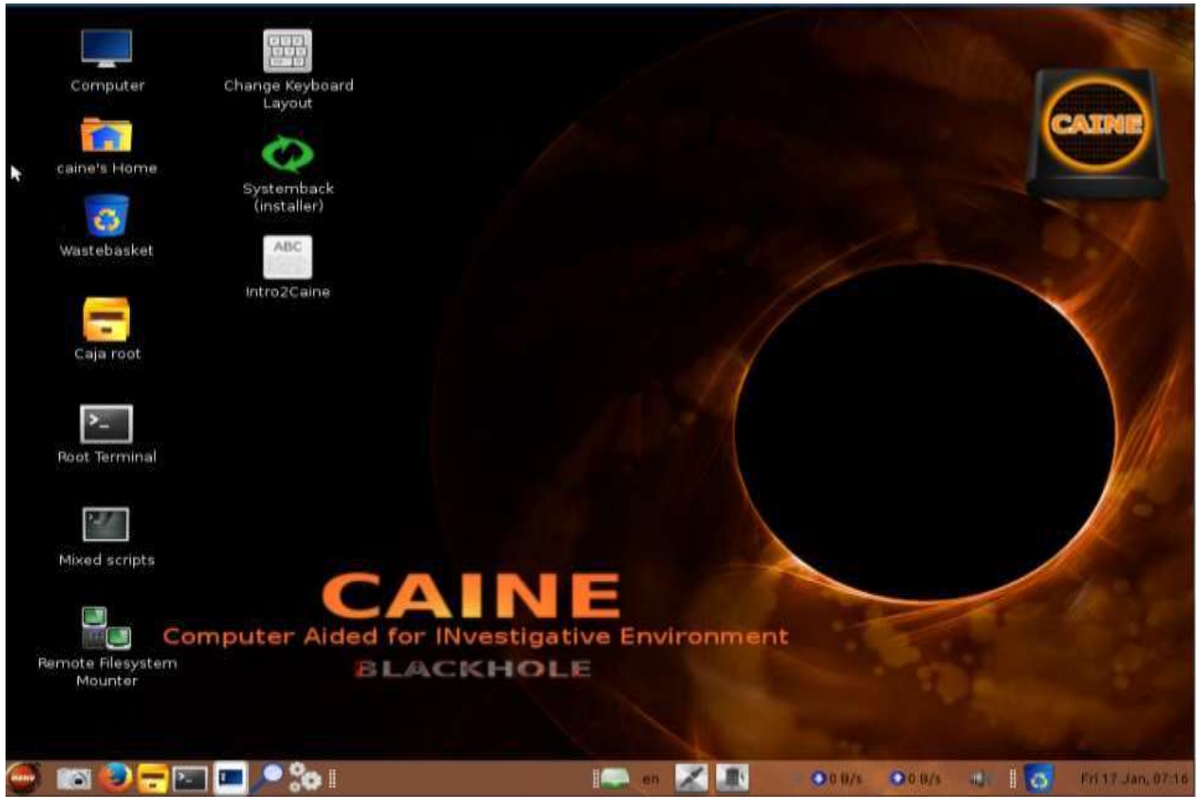
- Tsurugi-linux.org

DEFT

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

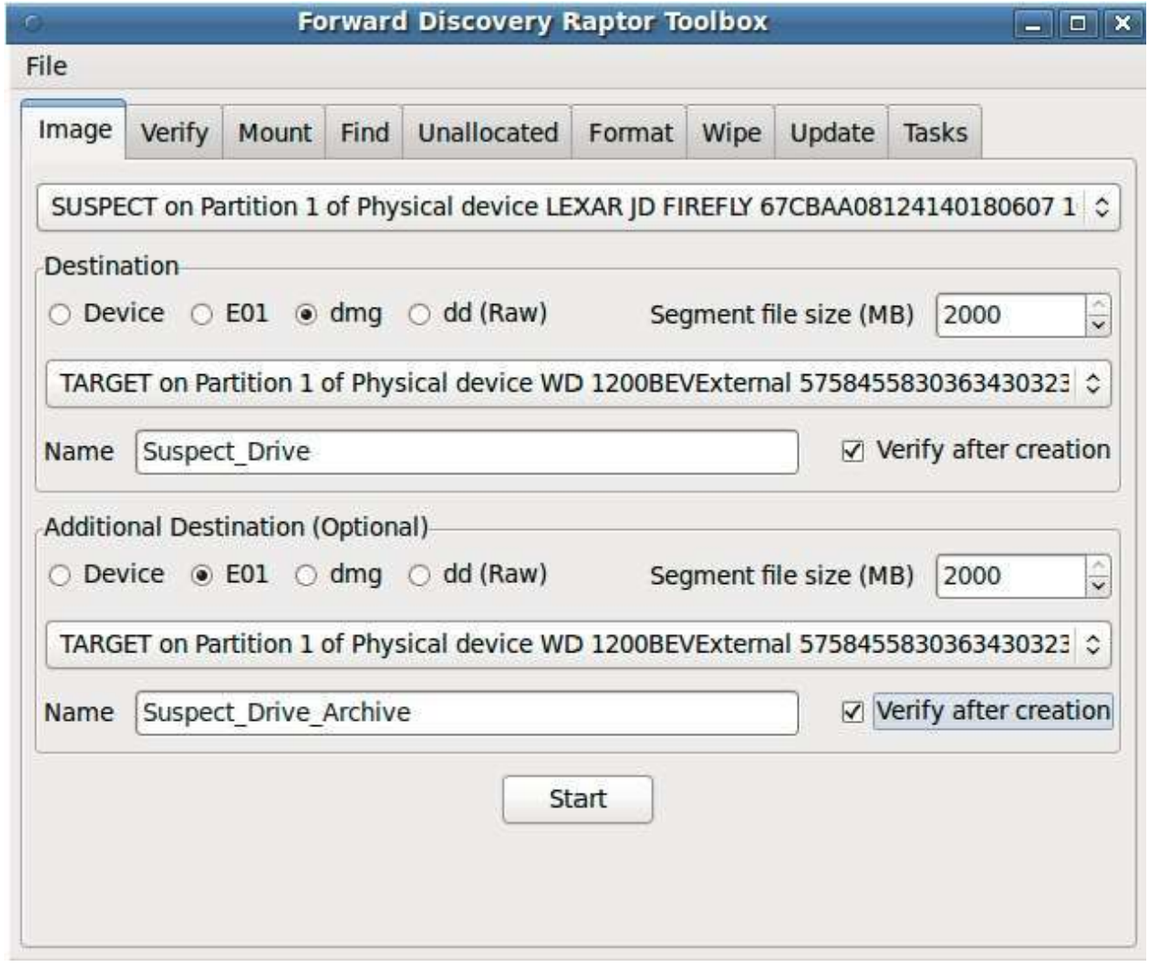
CAINE

- 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

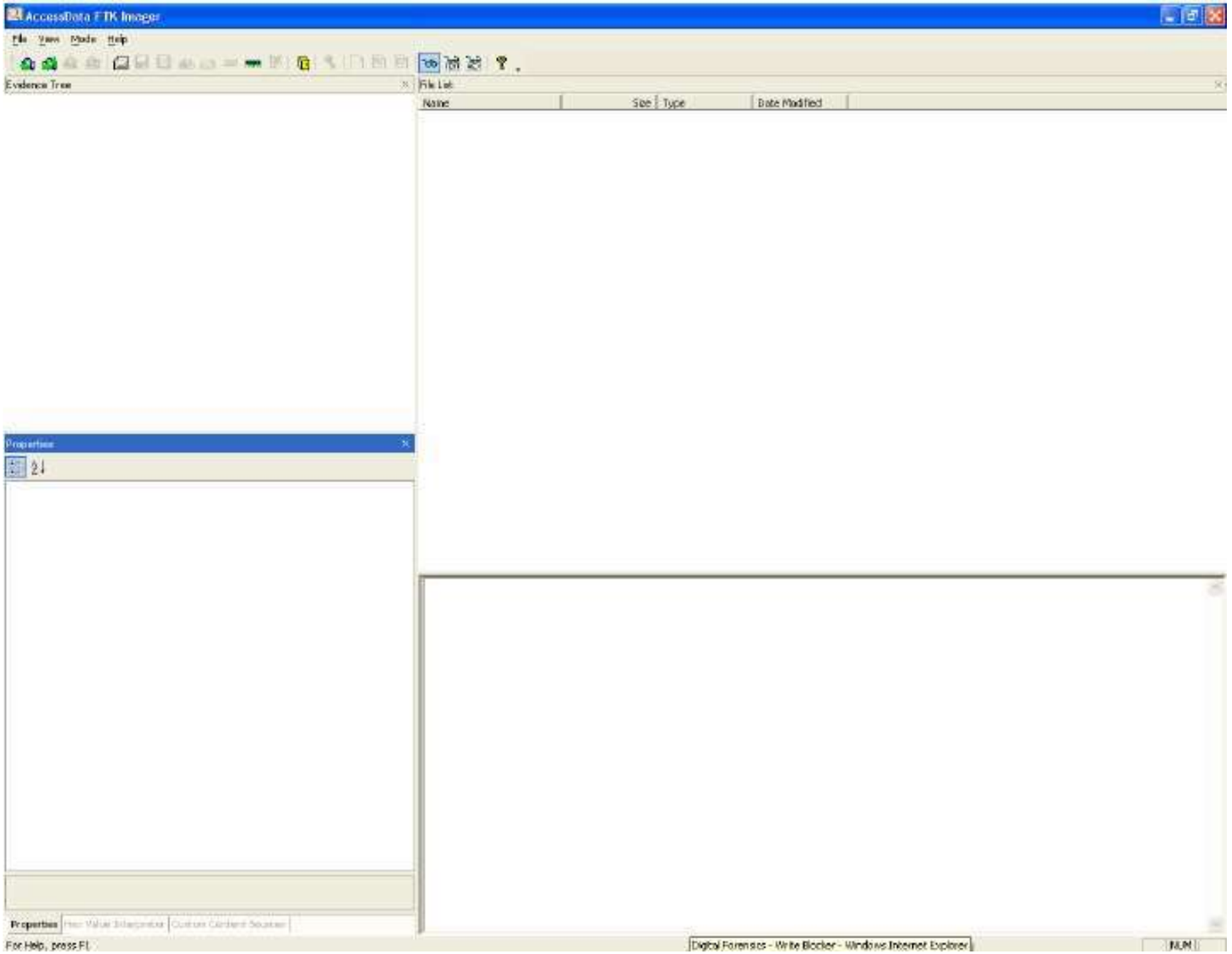
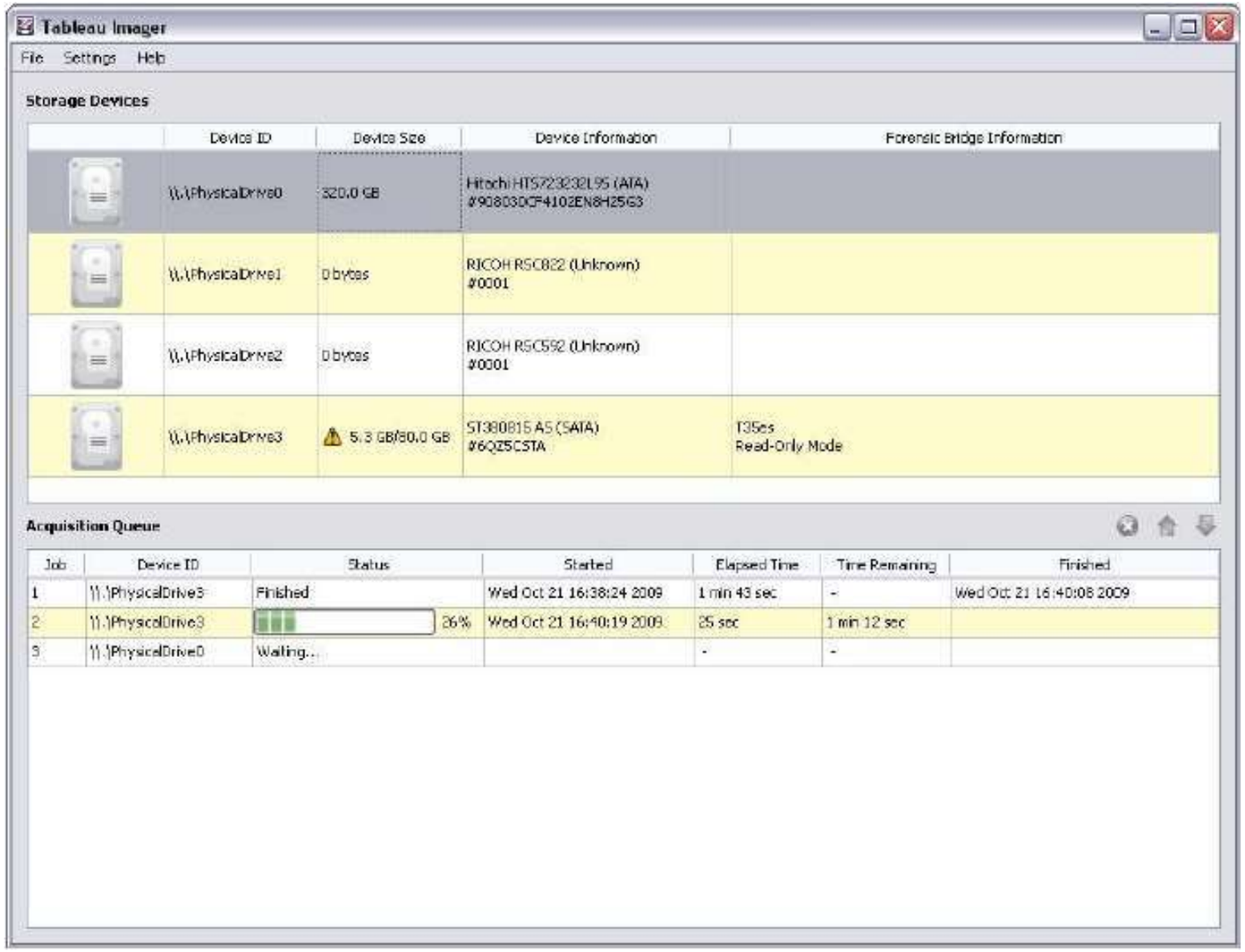

AccessData FTK Imager
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Properties
Properties
For Help, press F1
Digital Forensics - Write Blocker - Windows Internet Explorer
NUM

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 acces

Hardware vendors

The principal manufacturers of hardware for digital forensics are:

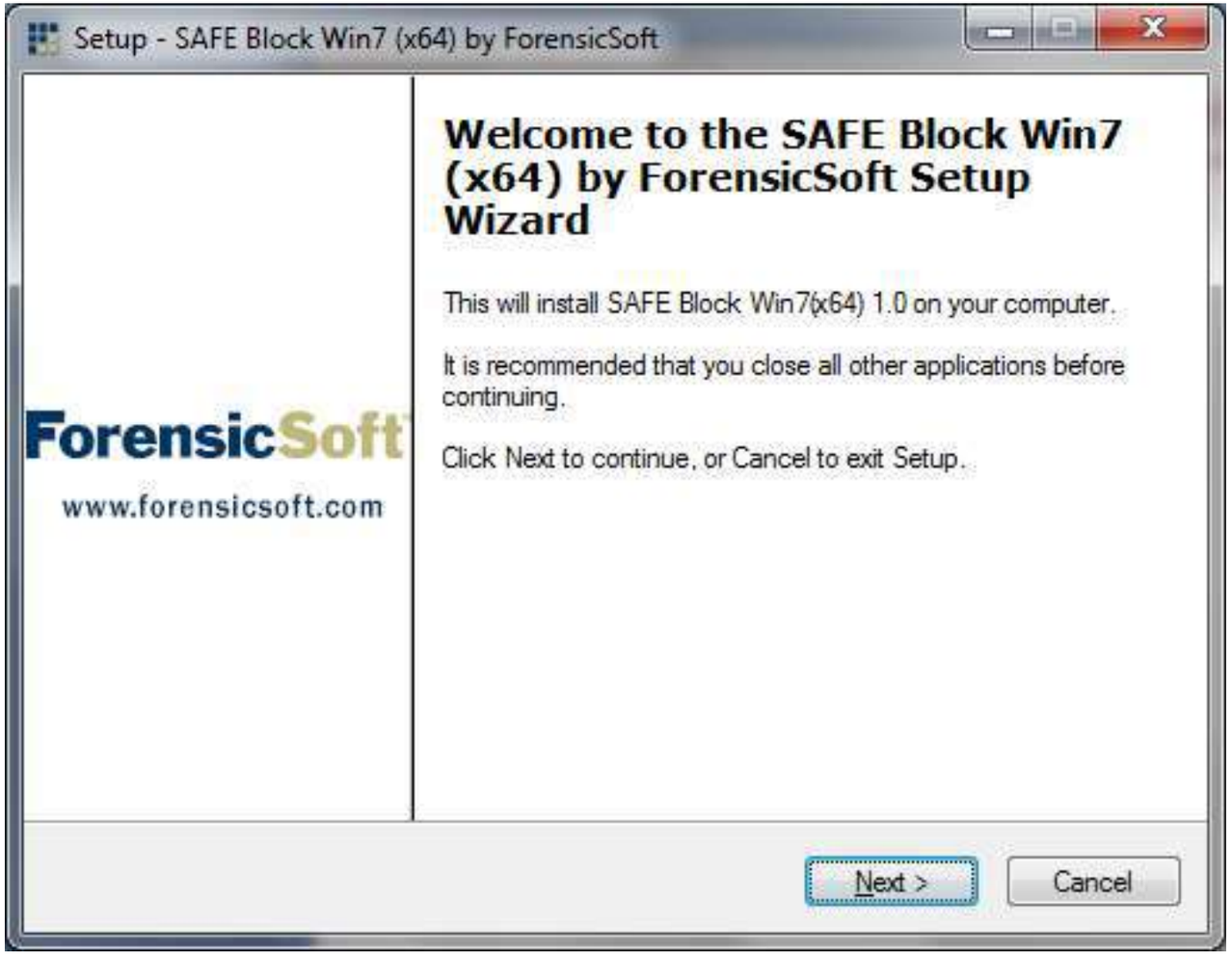
- **Tableau** - http://www.tableau.com/
- **Logicube** - http://www.logicubeforensics.com/
- **Intelligent Computer Solutions** - http://www.ics-iq.com/
- **Wiebetech** - http://www.wiebetech.com/
- **Voom Technologies** - http://www.voomtech.com/
- **MyKey Technology** - http://www.mykeytech.com/
-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

Write Blocker Software

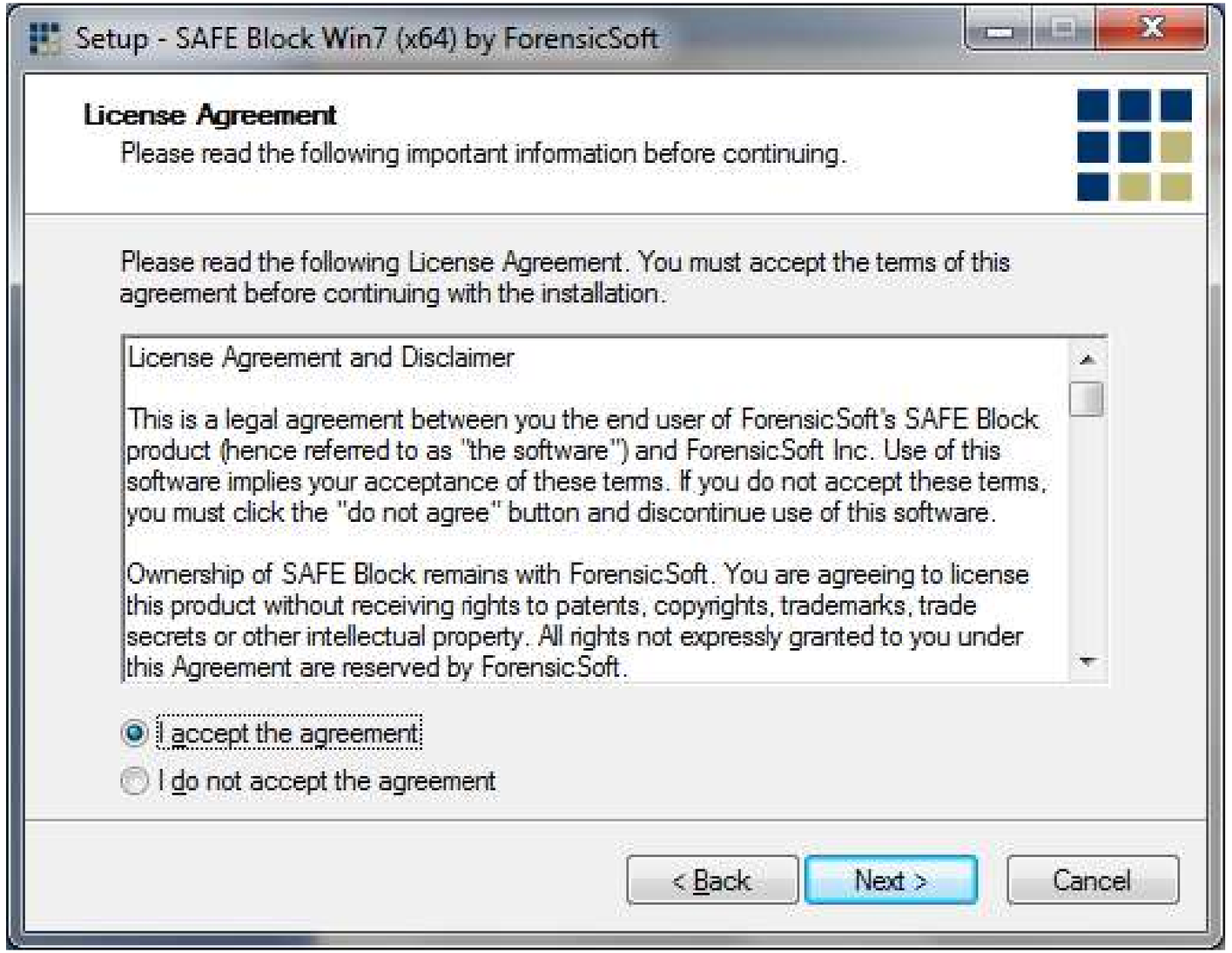
- The write block at software level it may get used on the operation of mounting the hard disk from the operating system.
- Depending on the operating system used on the acquisition forensics machine, you can take proper precautions to prevent the bidirectional flow of communication and allow access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

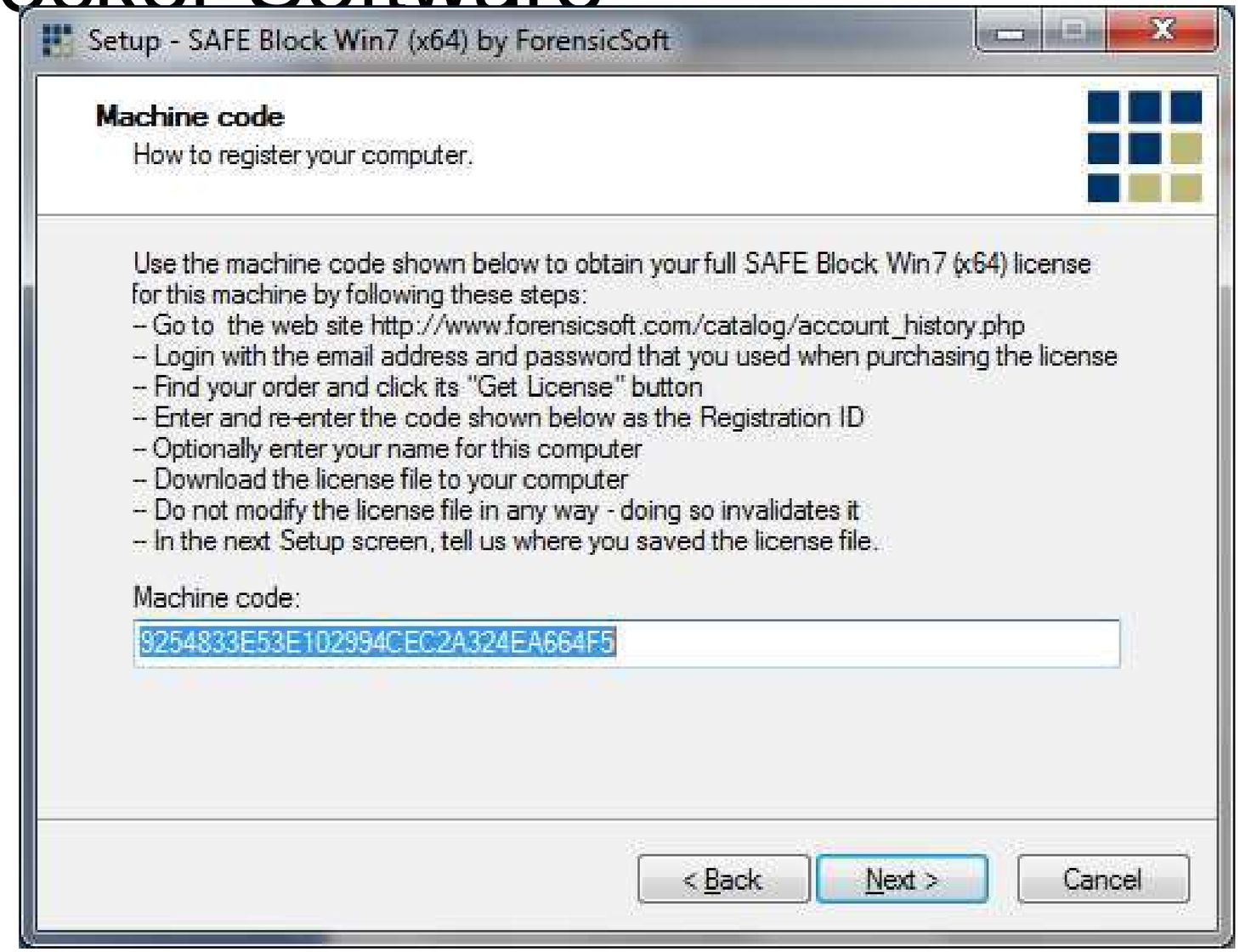
Write Blocker Software



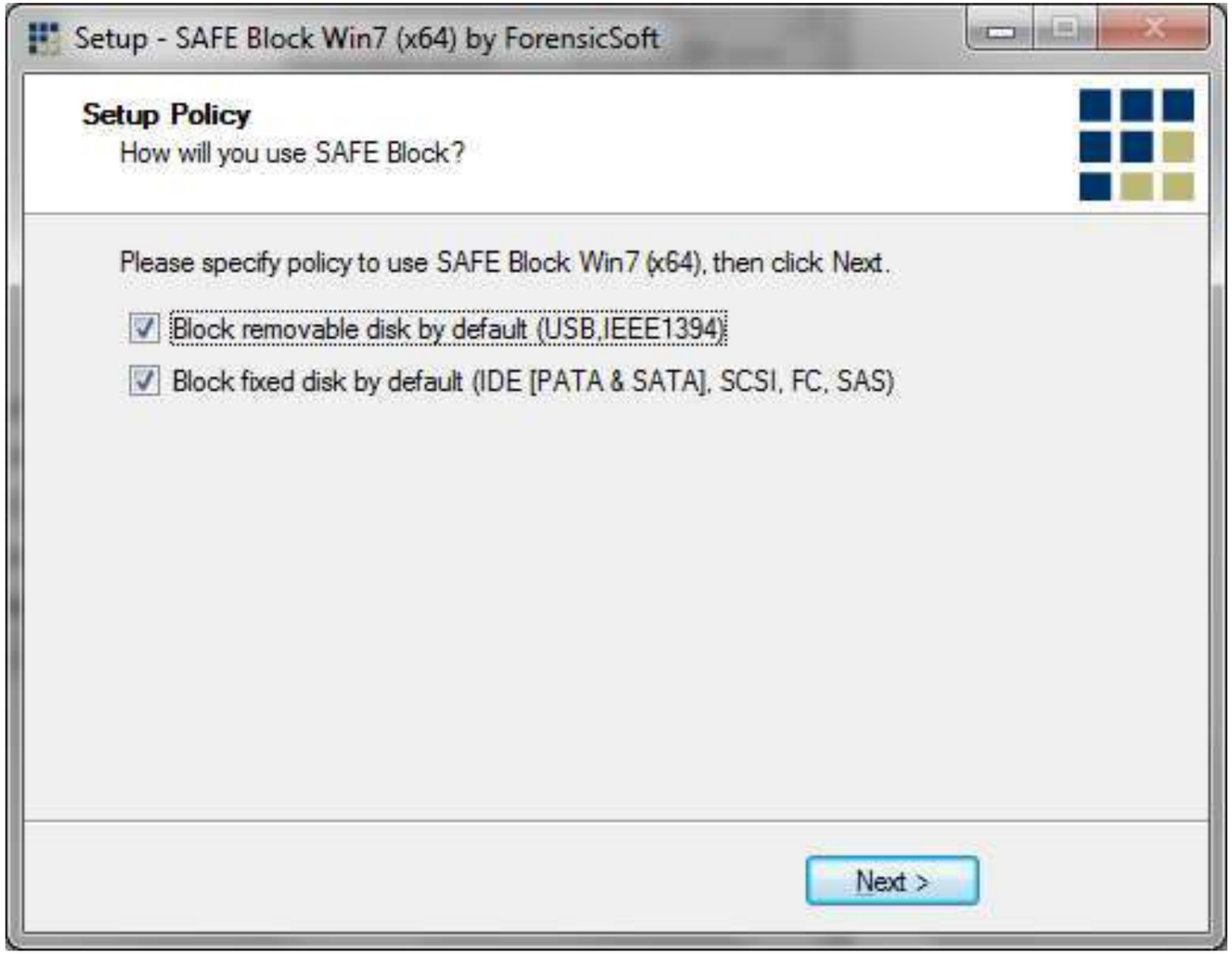
Write Blocker Software



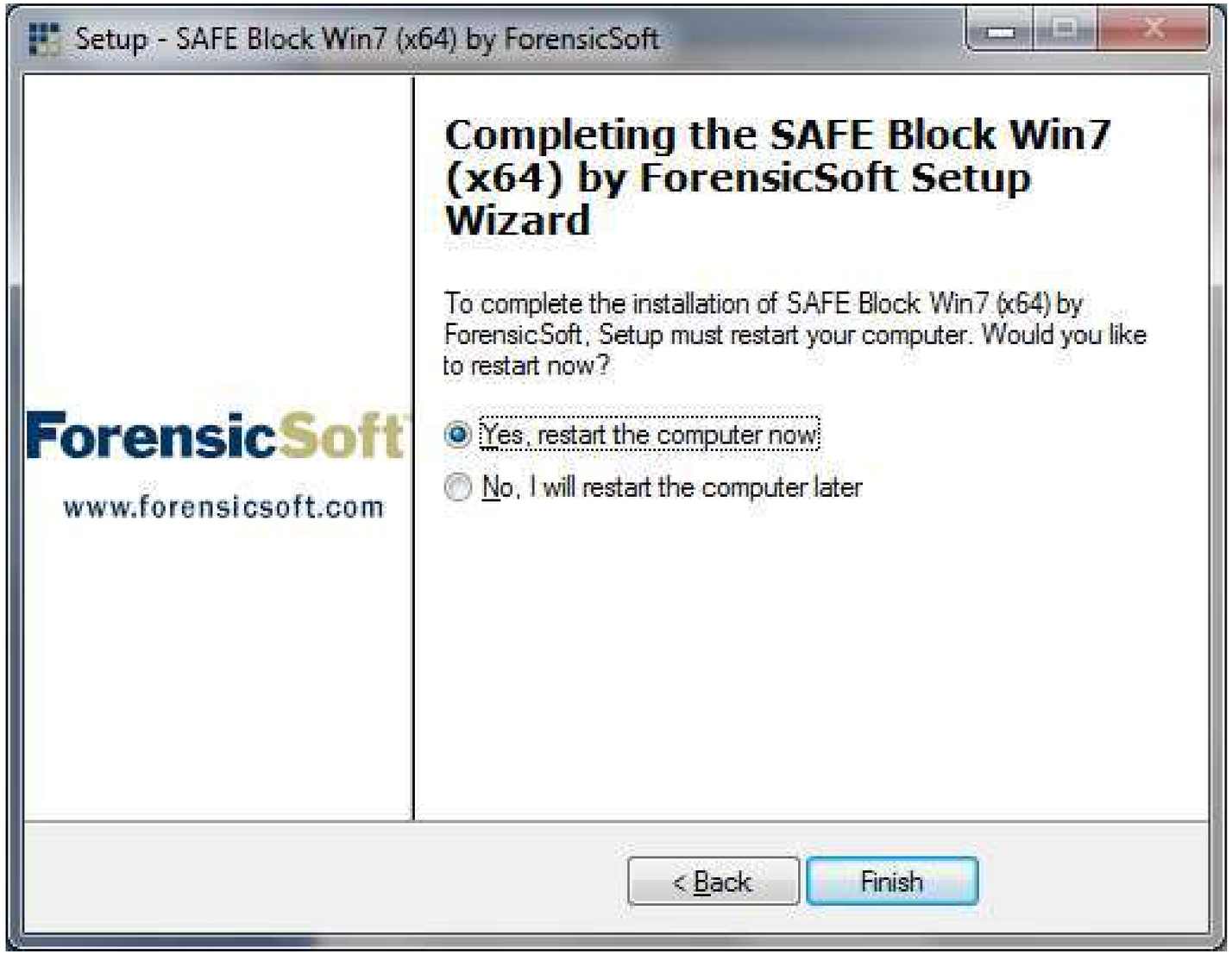
Write Blocker Software



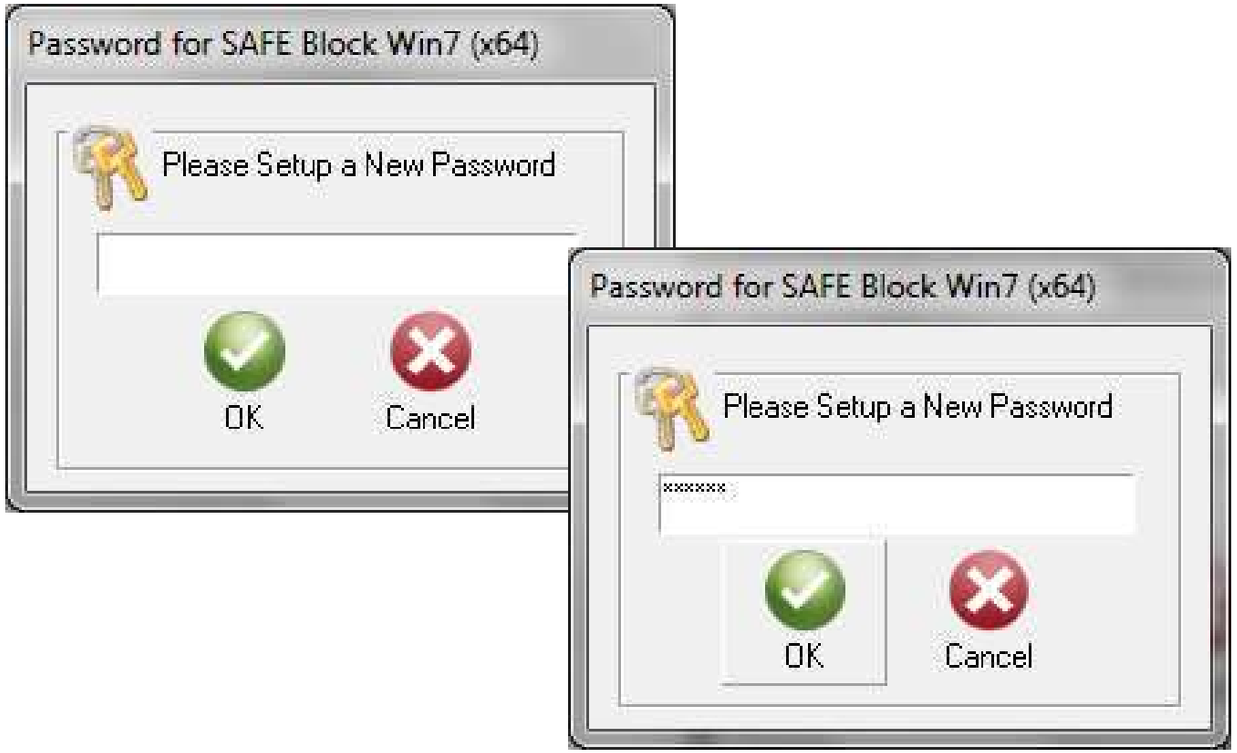
Write Blocker Software



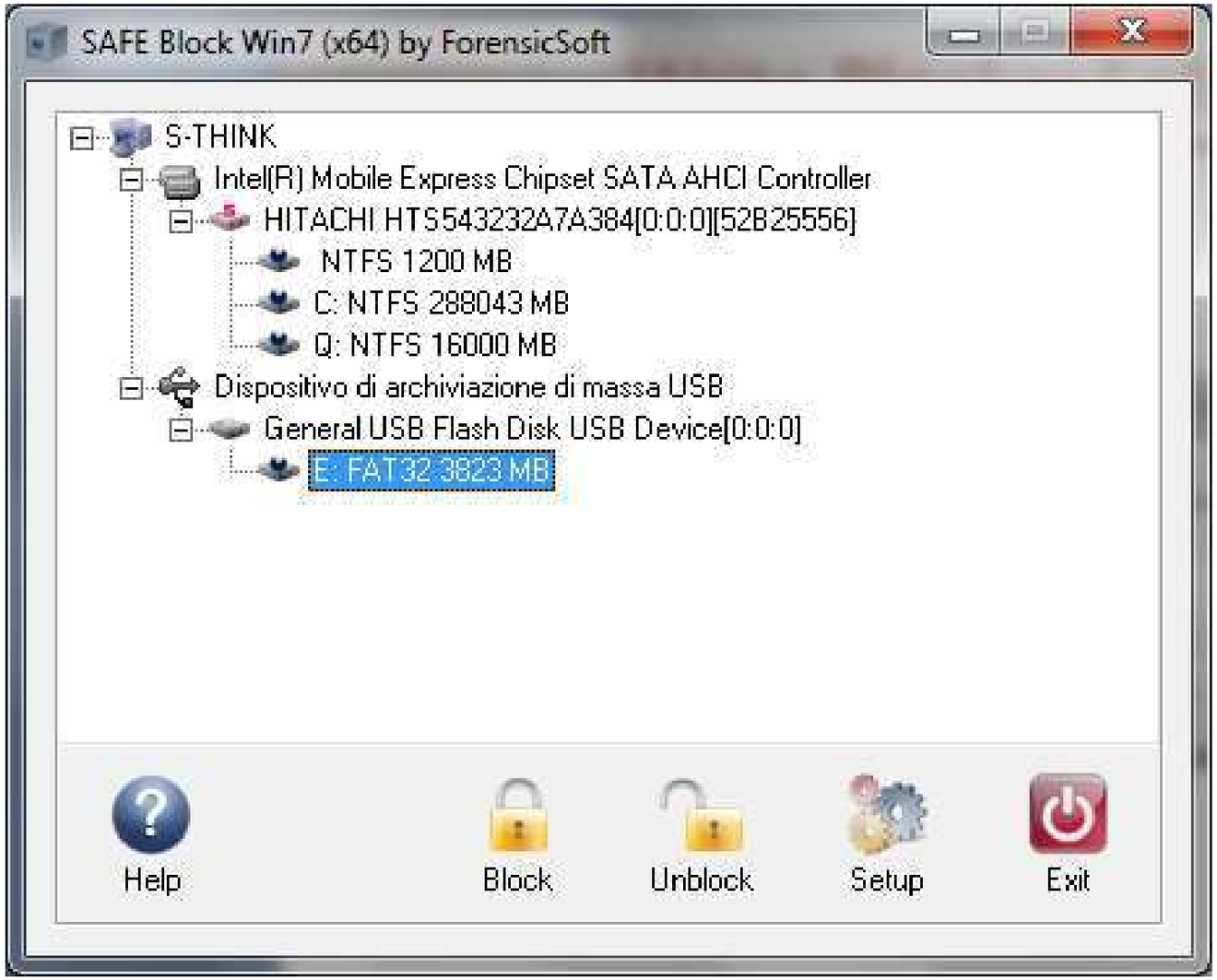
Write Blocker Software



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

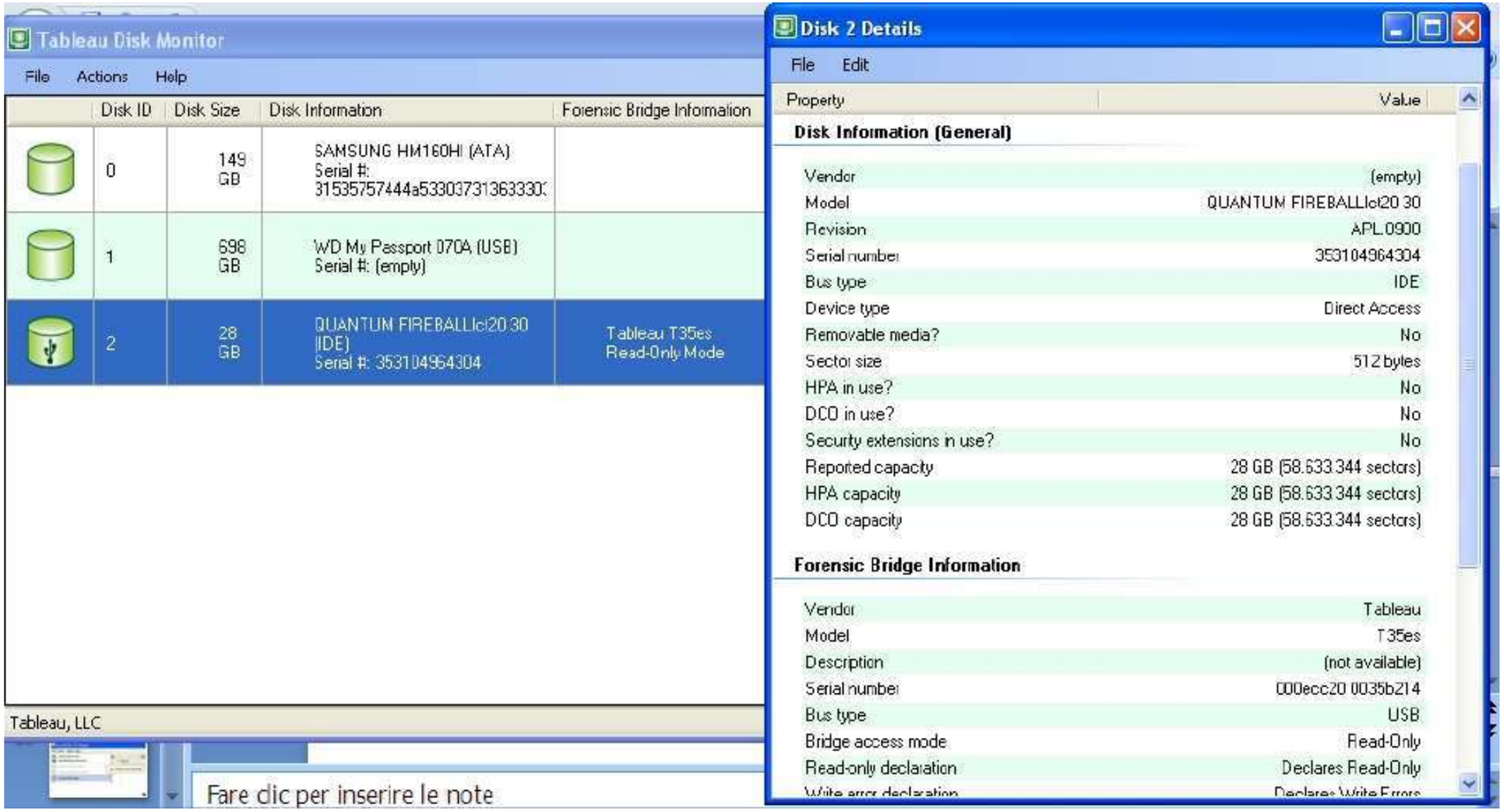
Hash Function

- 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

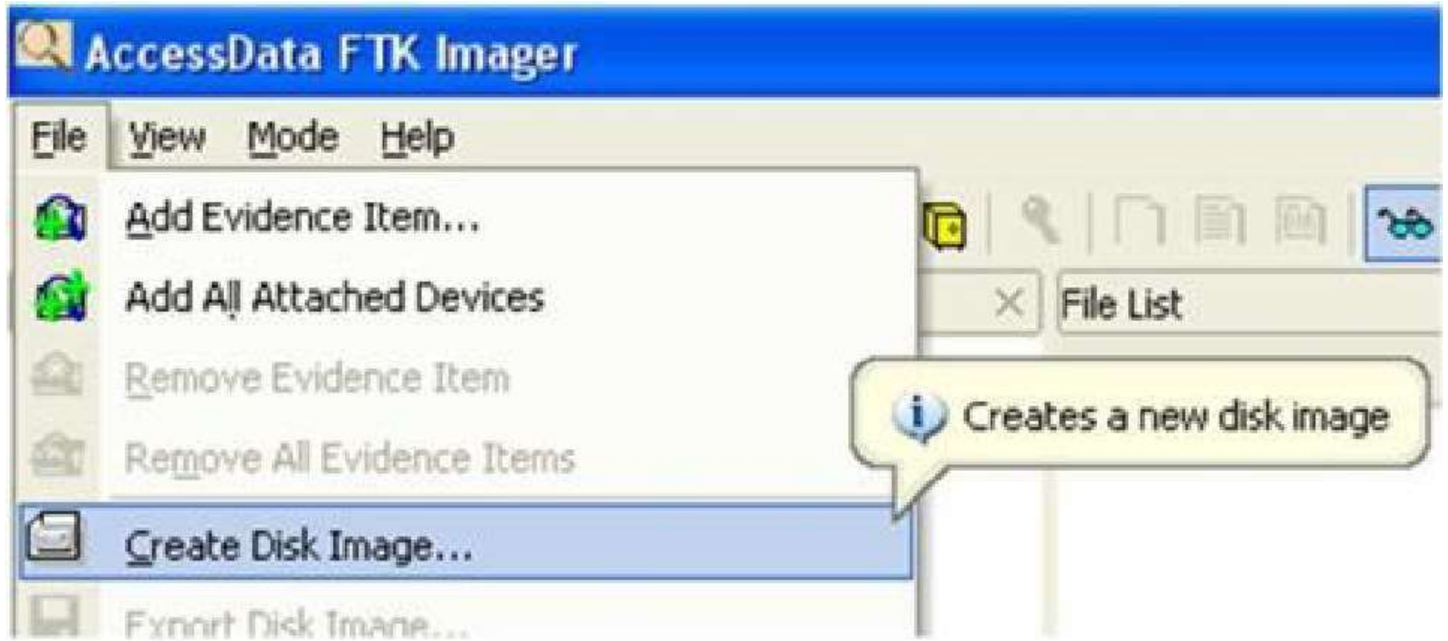
Funzioni hash

- 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

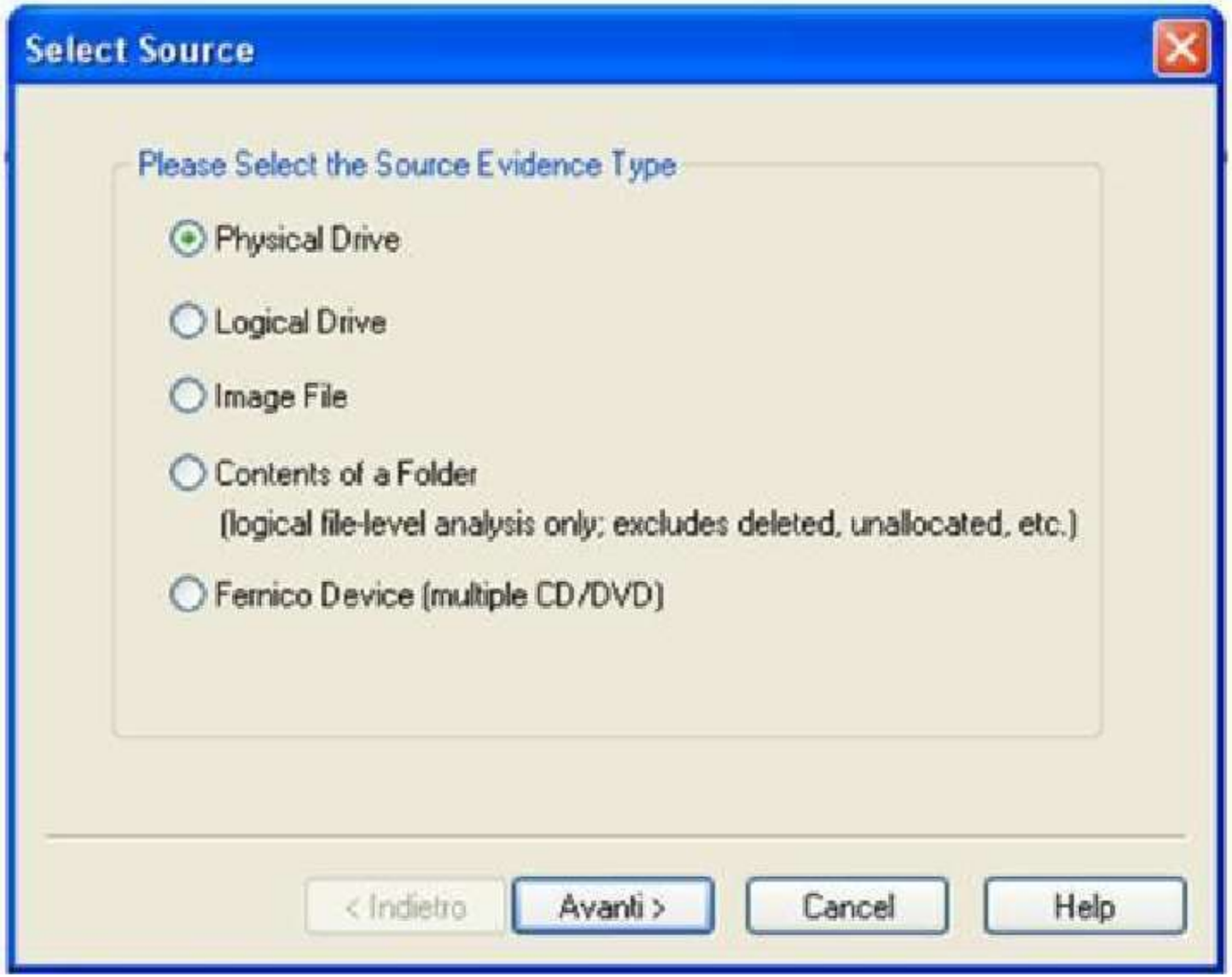
Acquisition with Tableau Disk Monitor



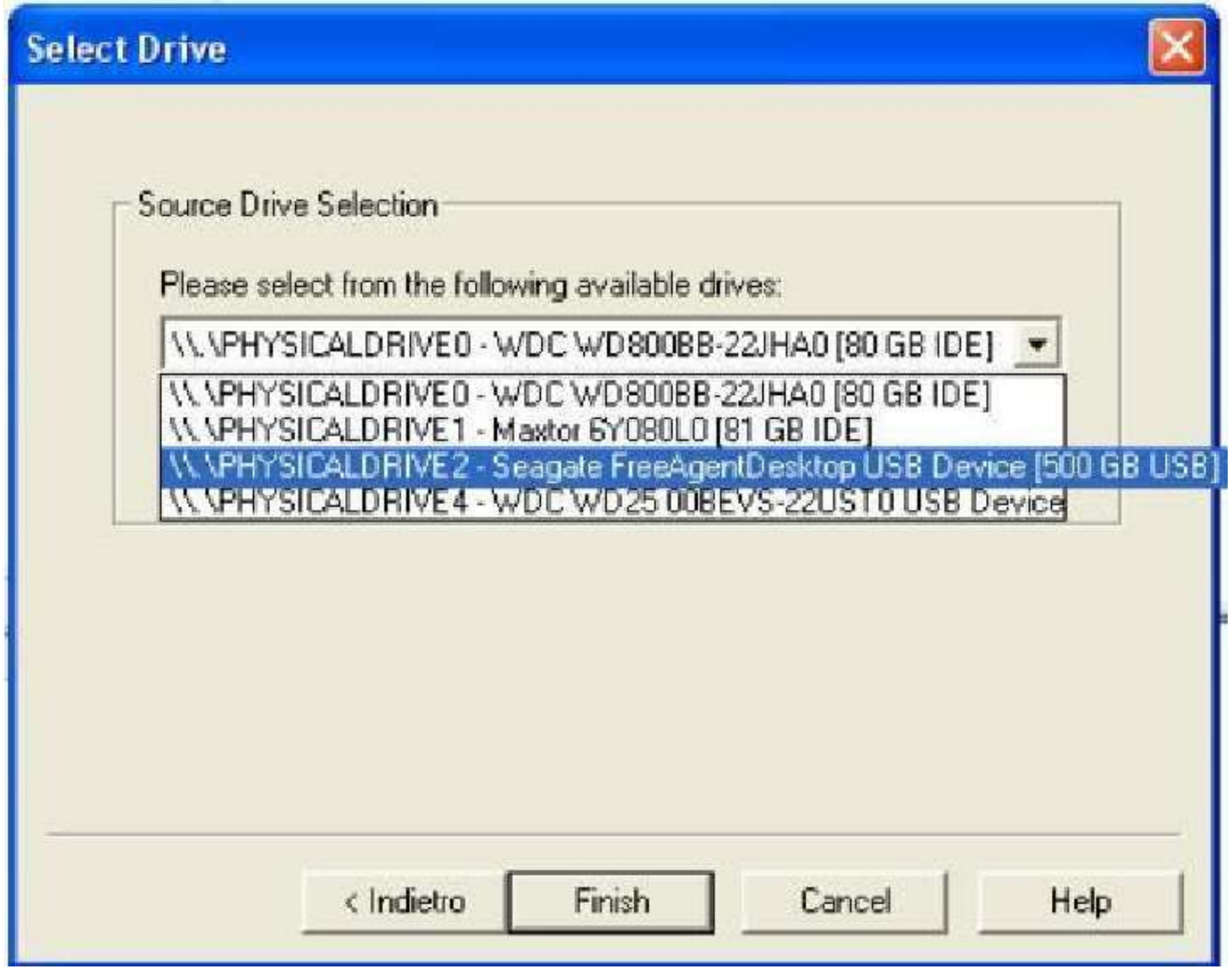
Acquisition with FTK Imager



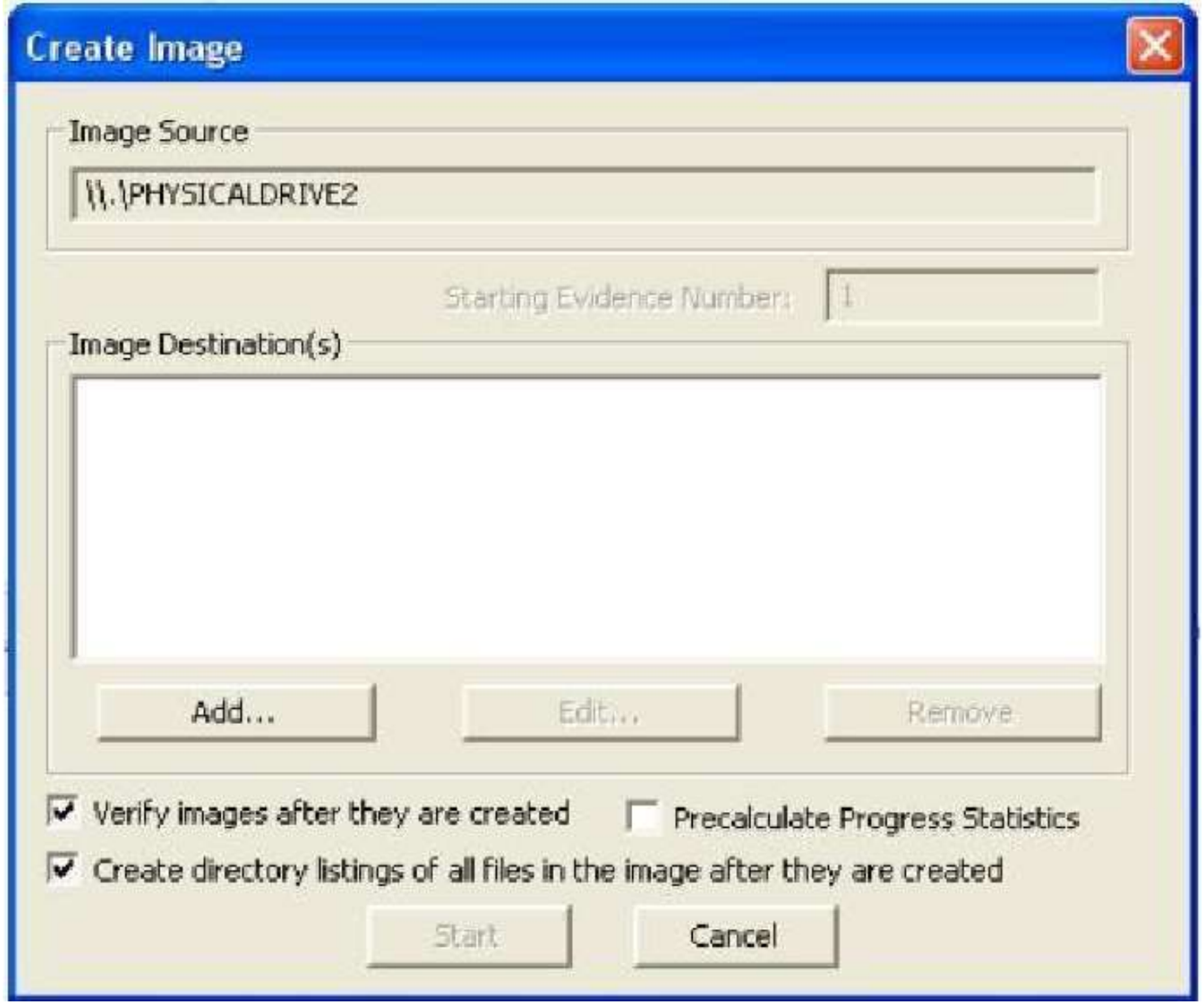
Acquisition with FTK Imager



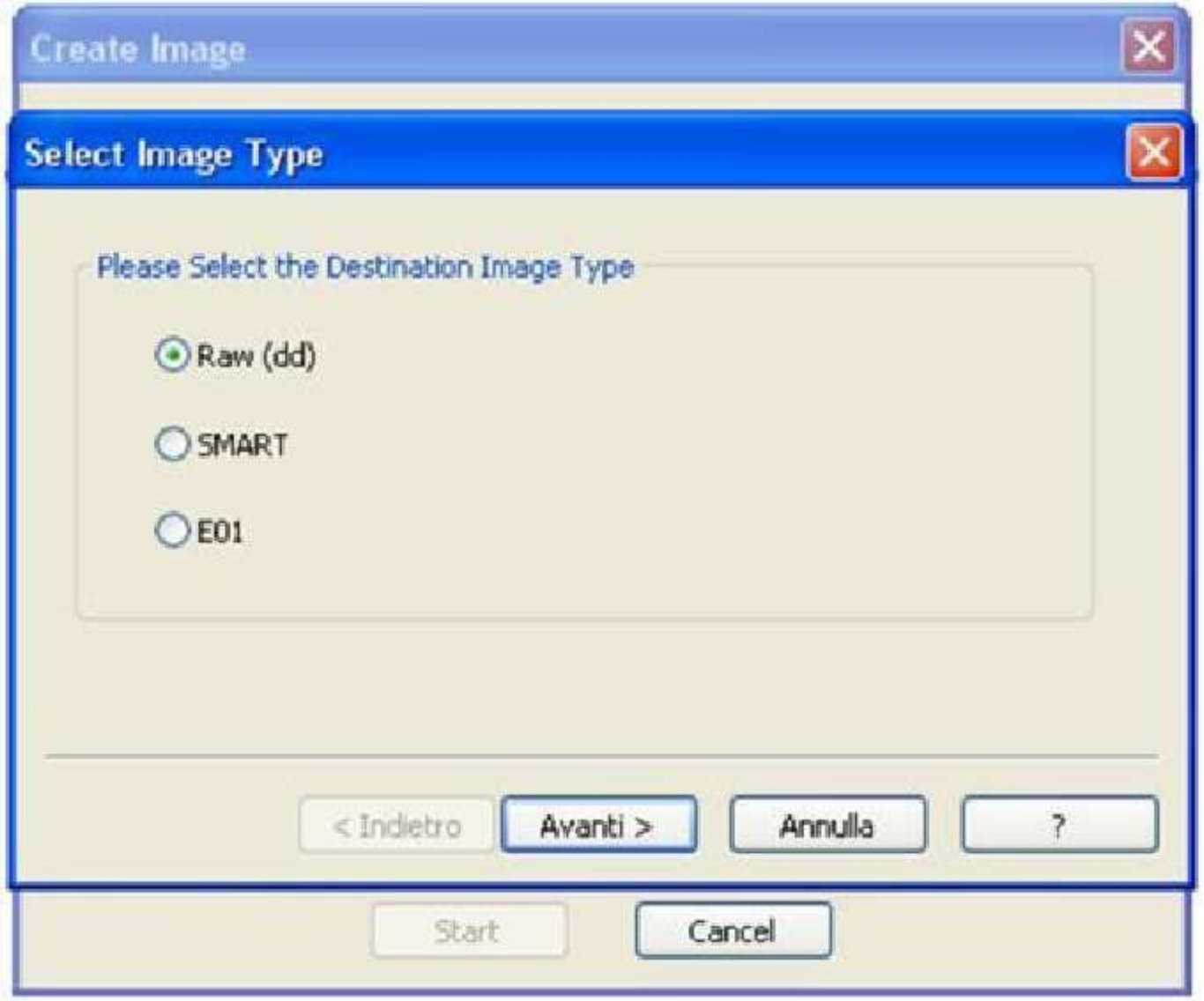
Acquisition with FTK Imager



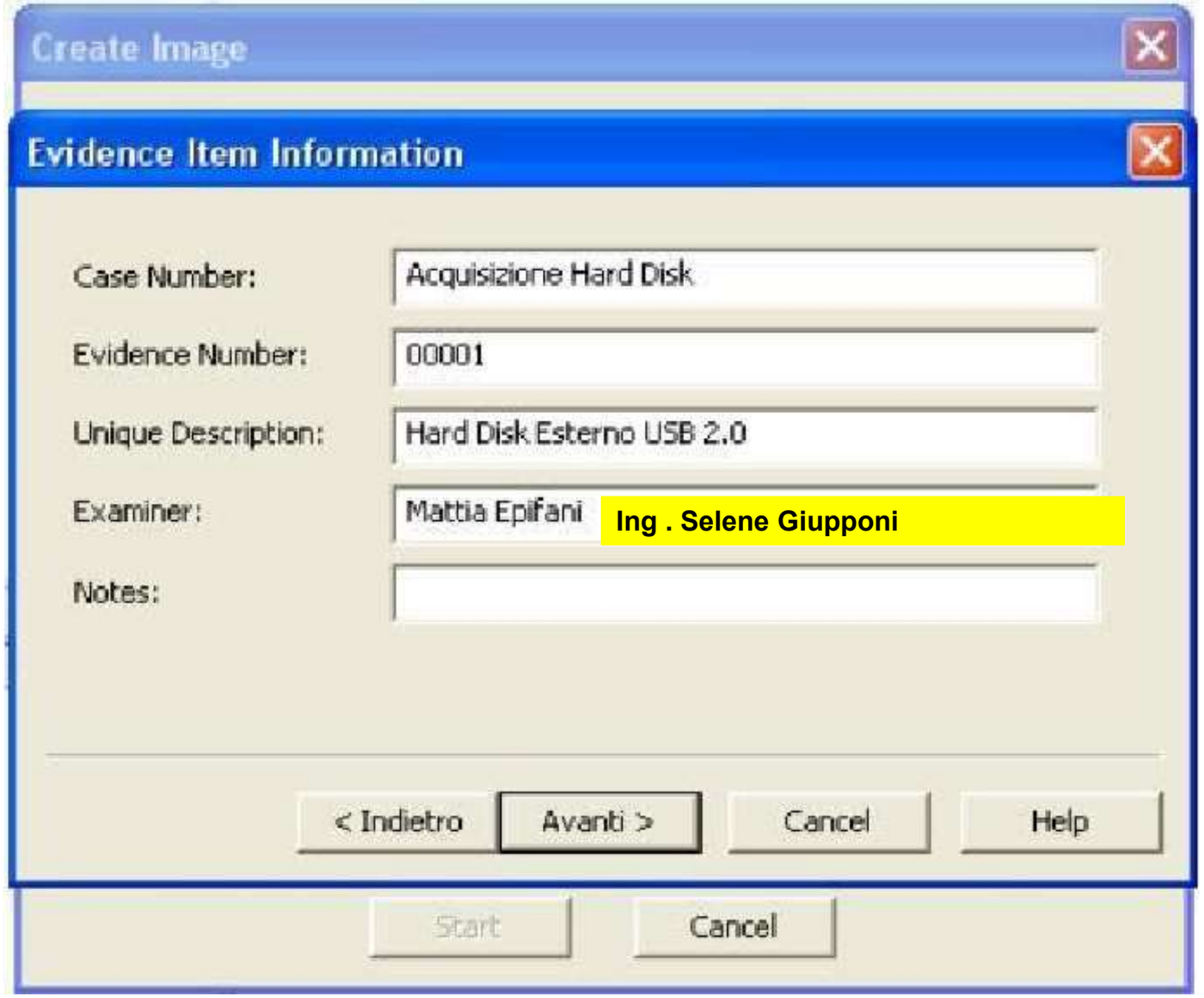
Acquisition with FTK Imager



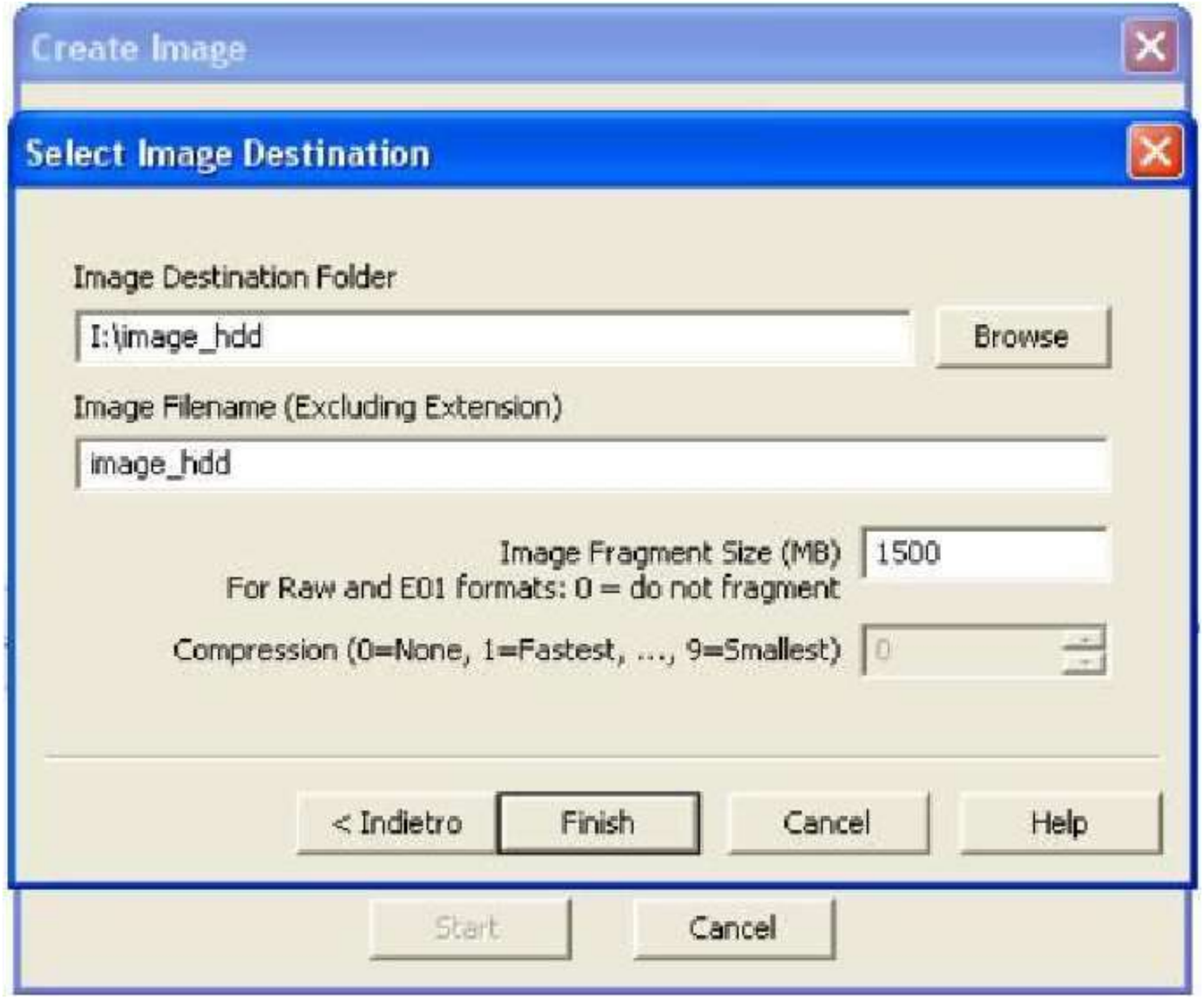
Acquisition with FTK Imager



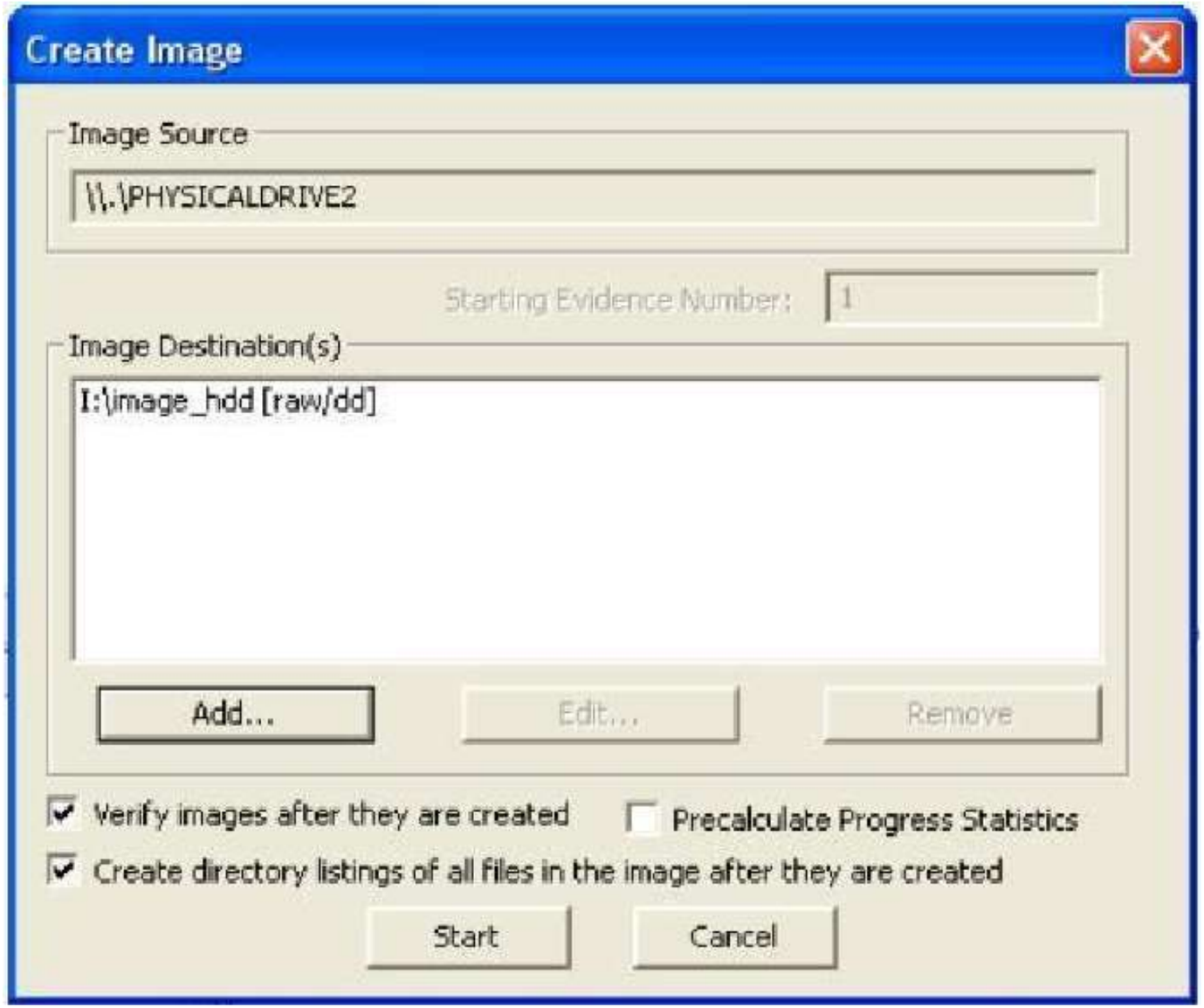
Acquisition with FTK Imager



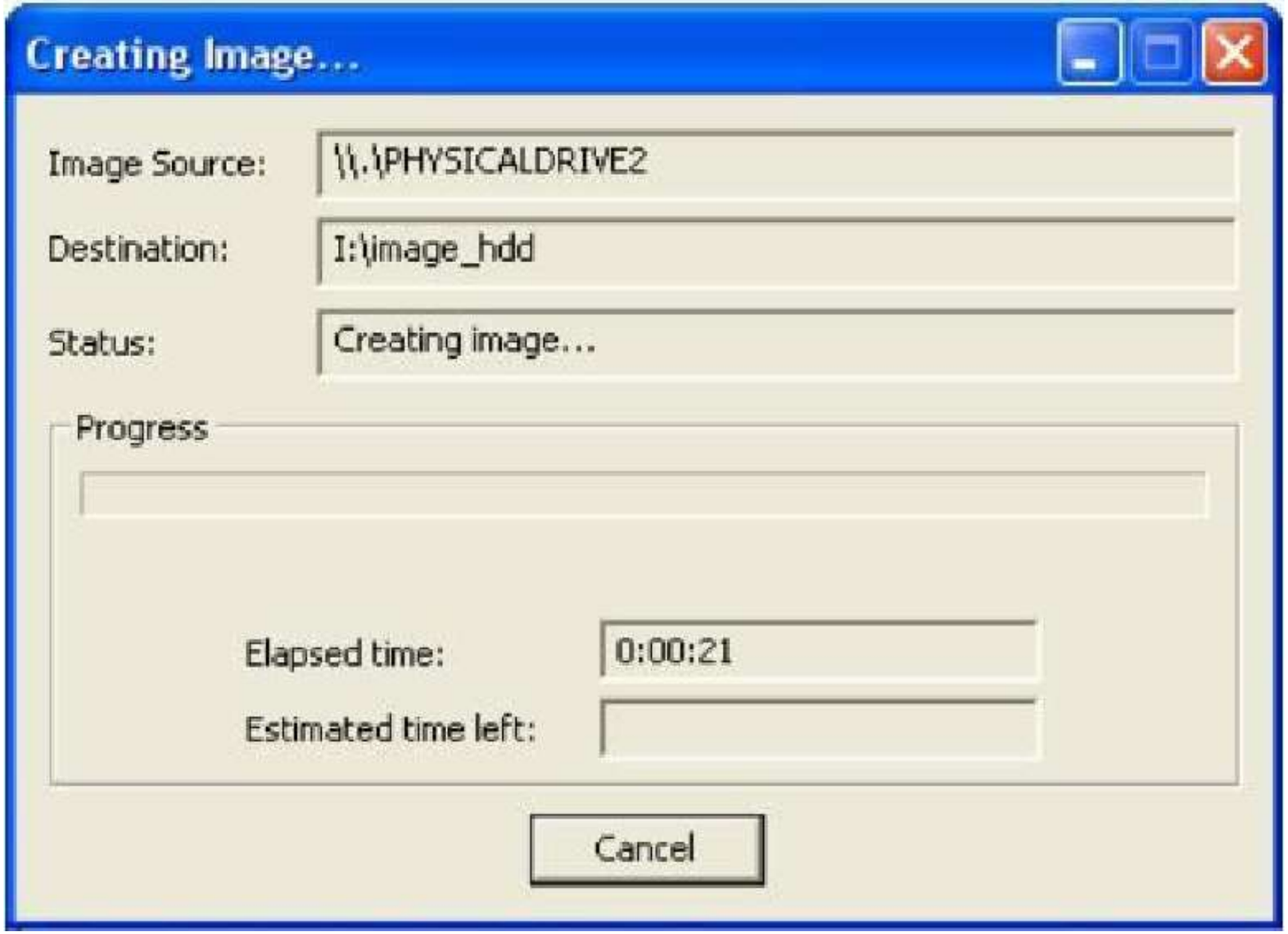
Acquisition with FTK Imager



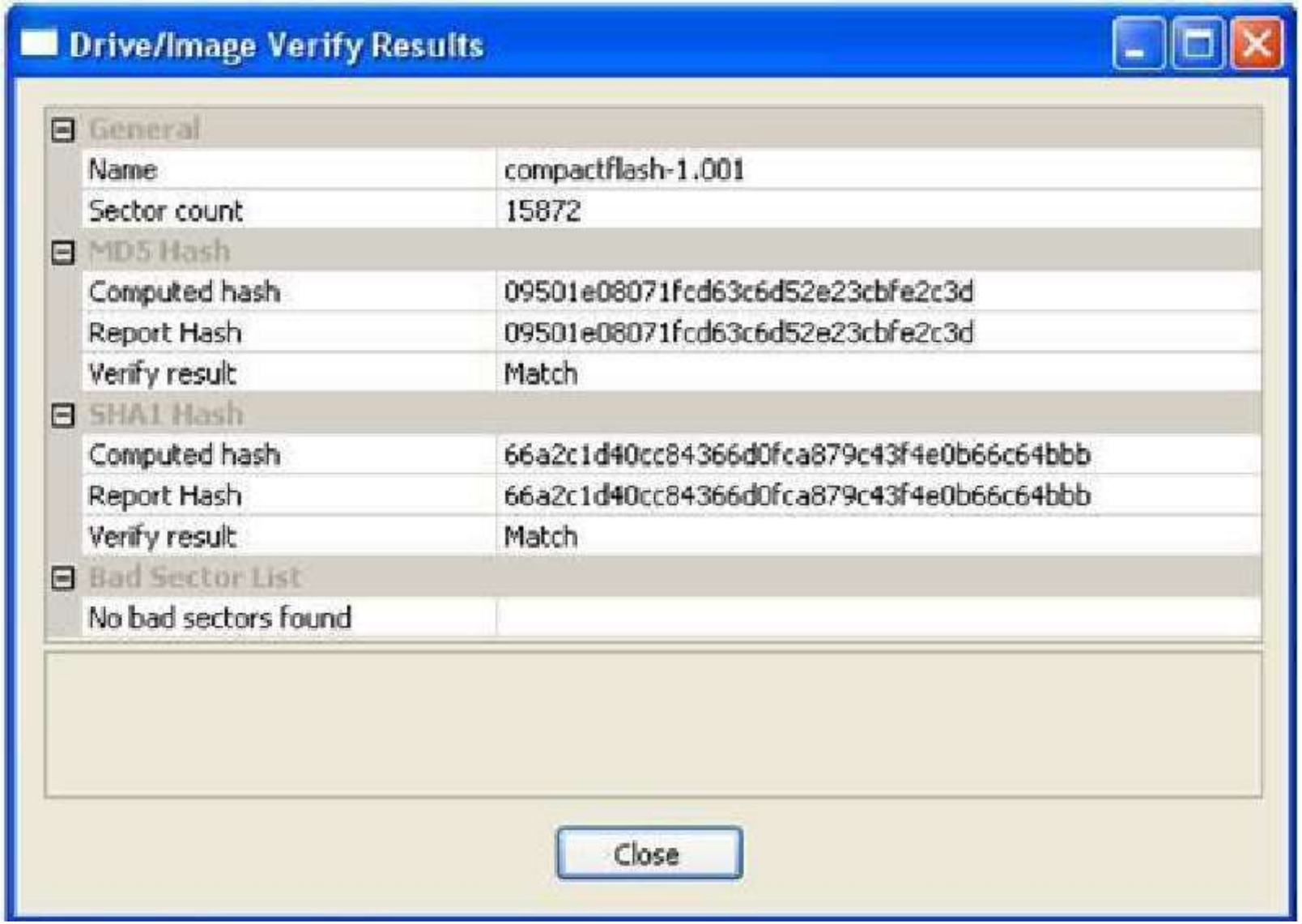
Acquisition with FTK Imager



Acquisition with FTK Imager



Acquisition with FTK Imager



Operating steps

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

Analysis

The evaluation mode 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

<u>opensource vs proprietor</u>

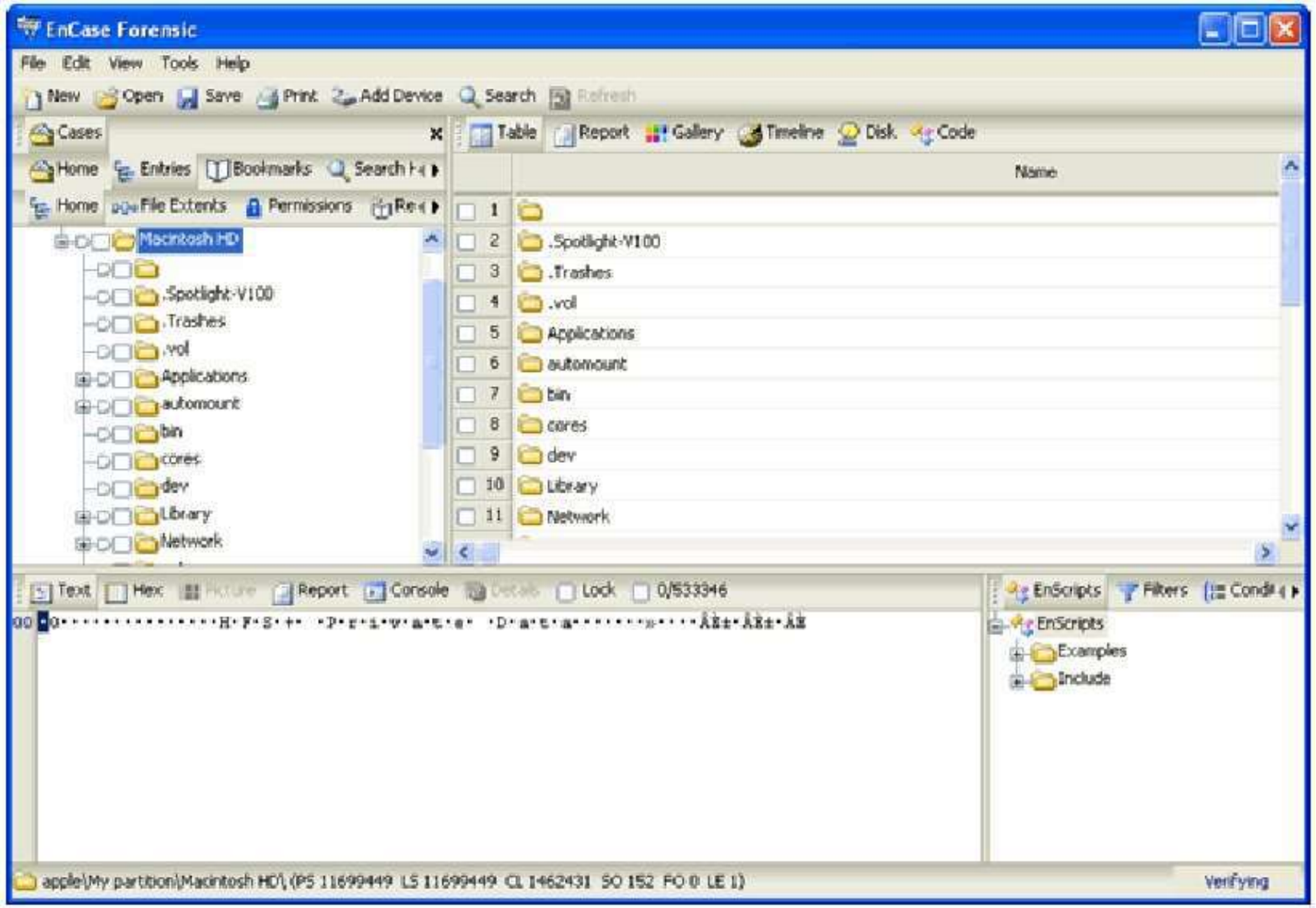
Like in any other field of information technology the compromise is in the middle, or use open source as long as you can, but also proprietary tools to not ruin his life!

Commercial Forensic Toolkit

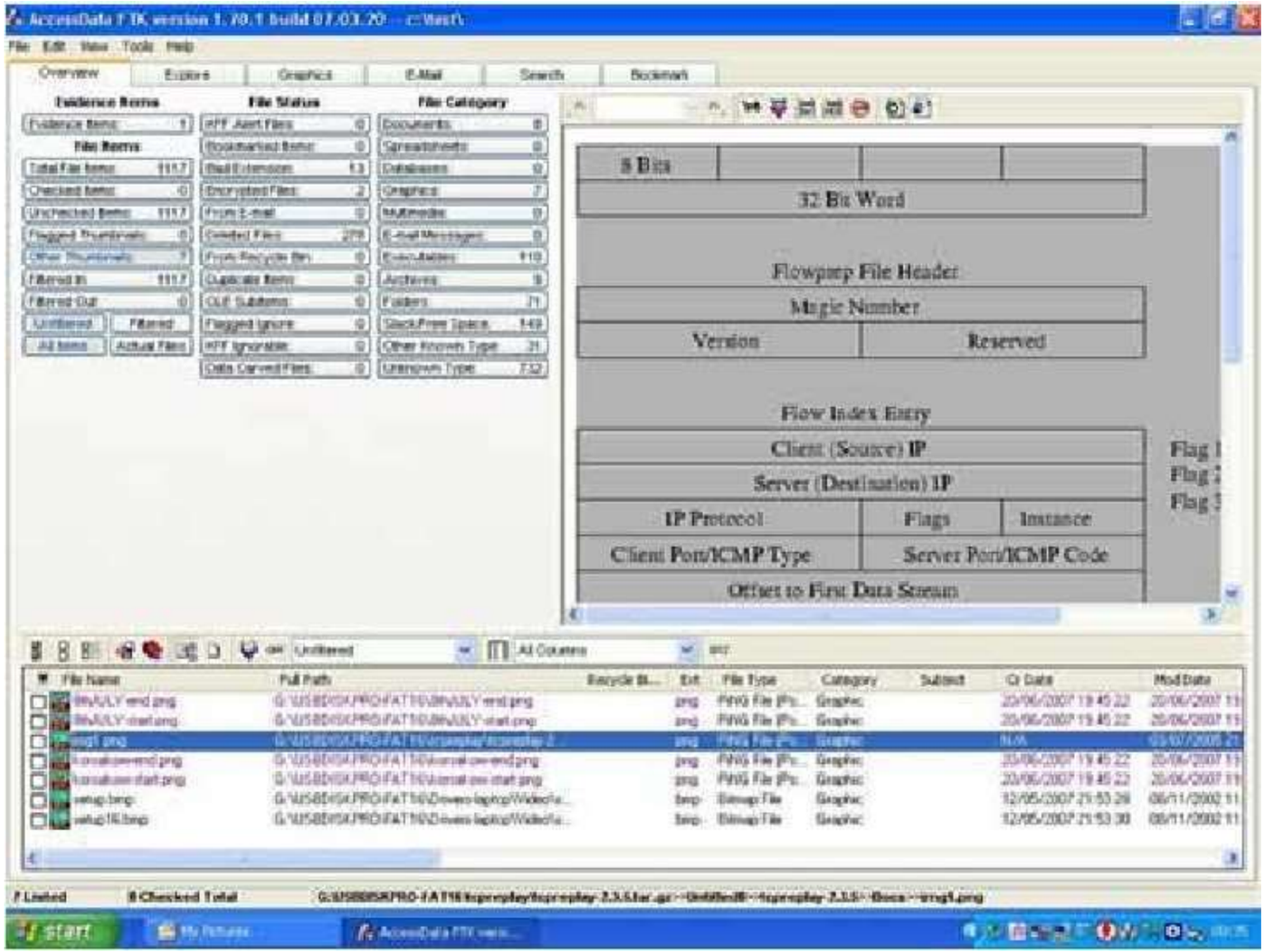
The most important commercial forensics toolkit are:

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

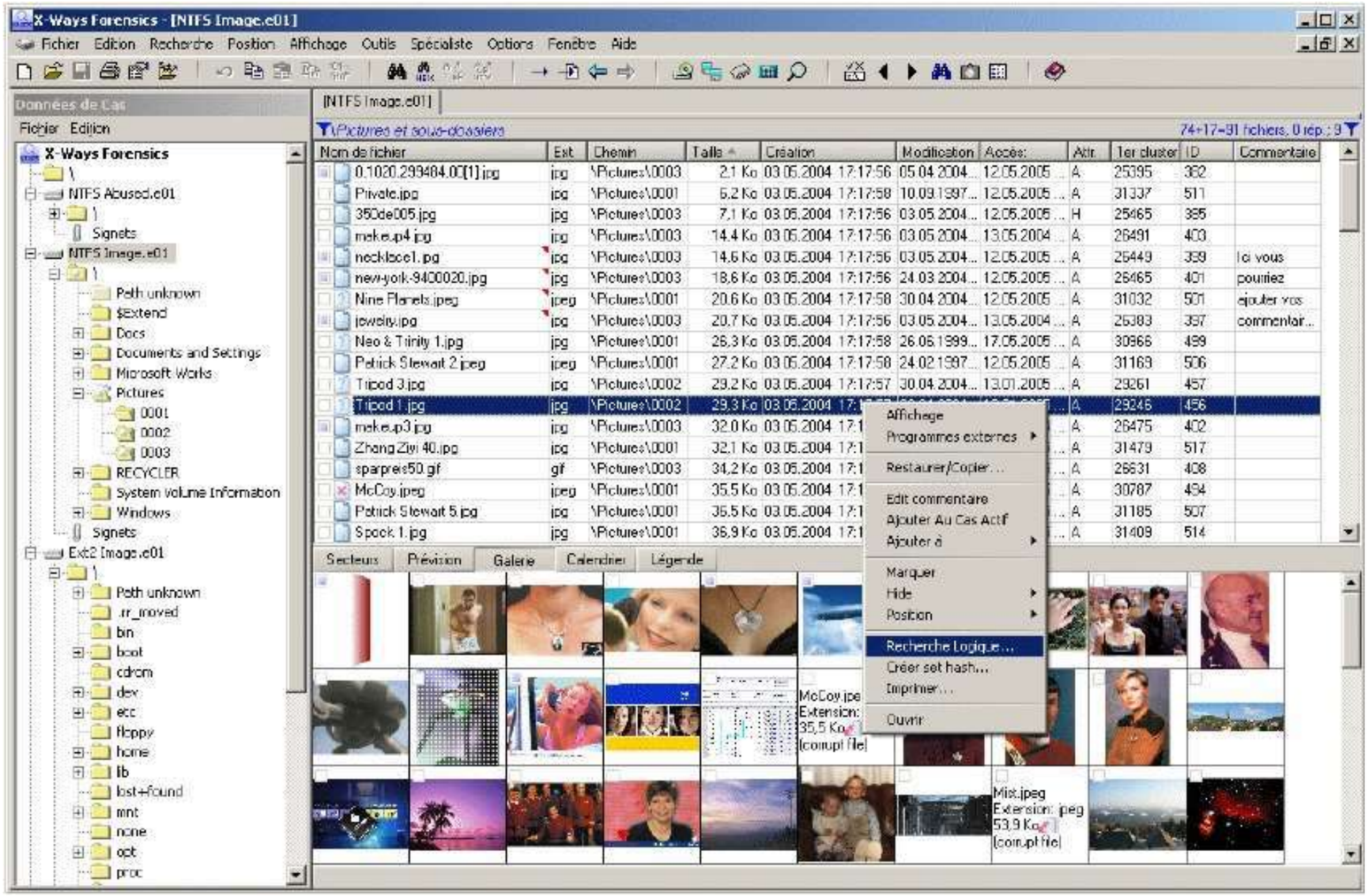
Encase


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases
Home Entries Bookmarks Search
Home File Extents Permissions
Table Report Gallery Timeline Disk Code
Name
Macintosh HD
.Spotlight-V100
.Trashes
.vol
Applications
automount
bin
cores
dev
Library
Network
Text Hex Report Console Lock 0/533946
EnScripts Filters
EnScripts
Examples
Include
apple\My partition\Macintosh HD\ (PS 11699449 LS 11699449 CL 1462431 SO 152 FO 0 LE 1)
Verifying

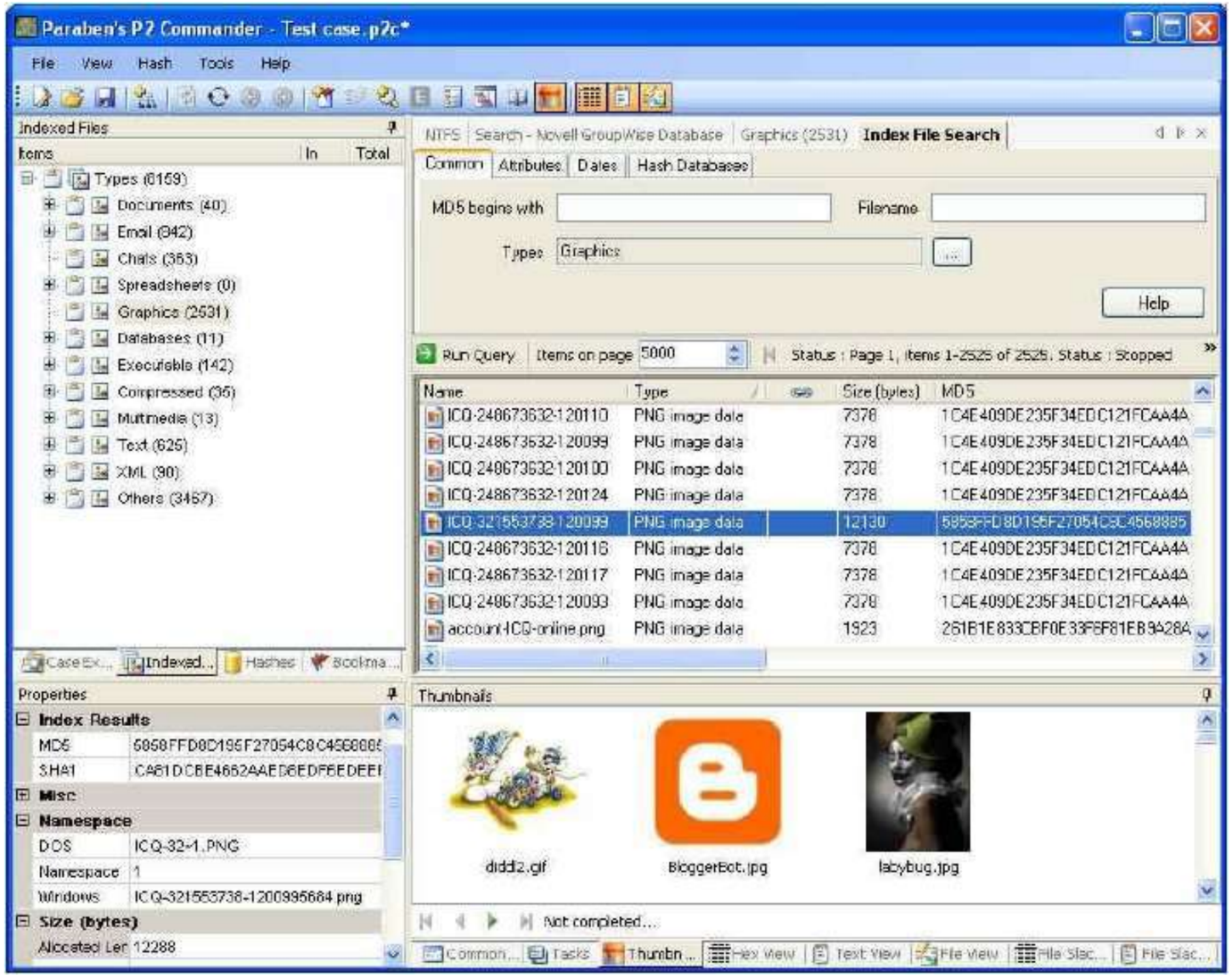
FTK – Access Data



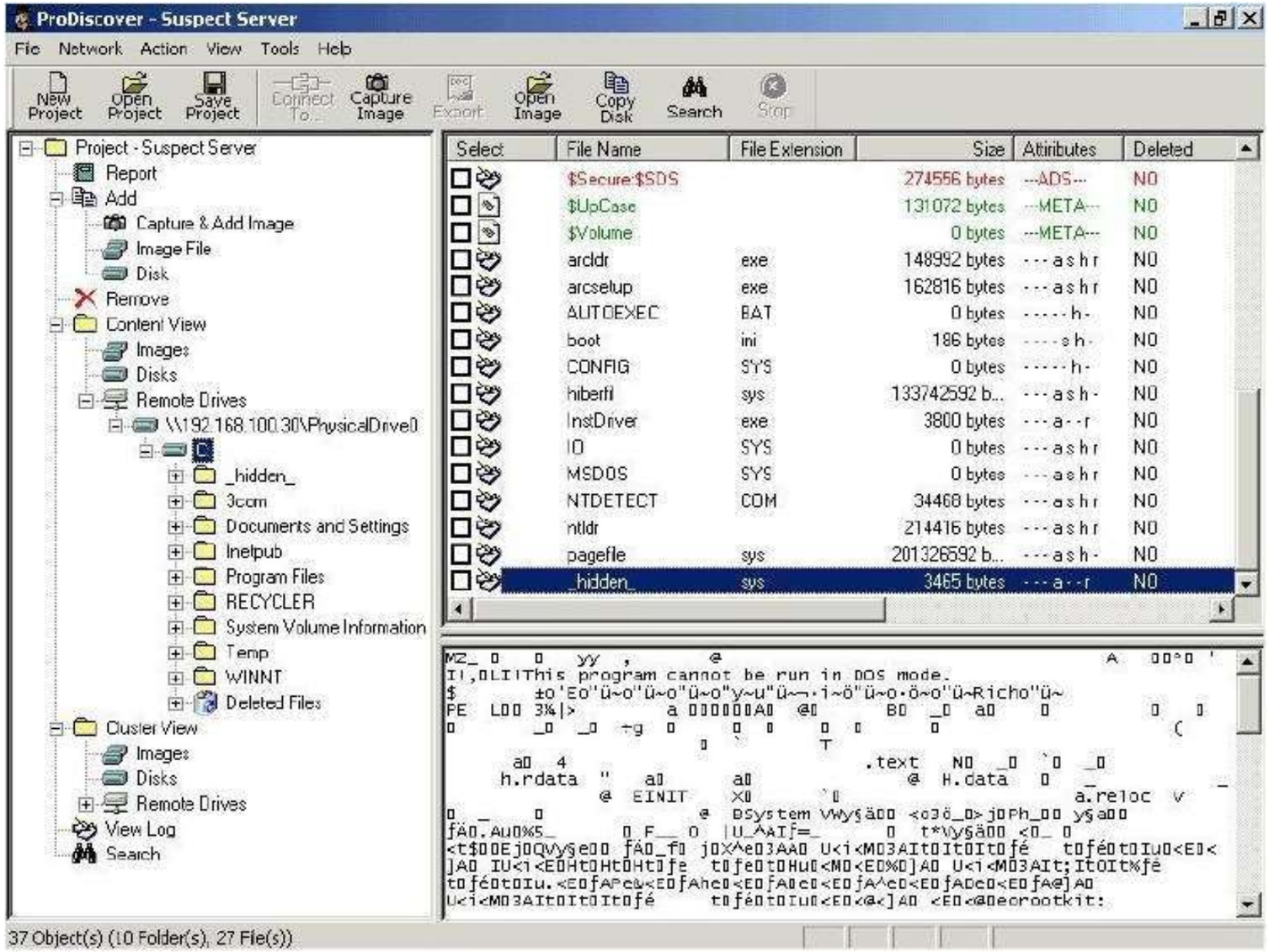
X-Ways Forensics



Paraben P2 Commander



ProDiscover



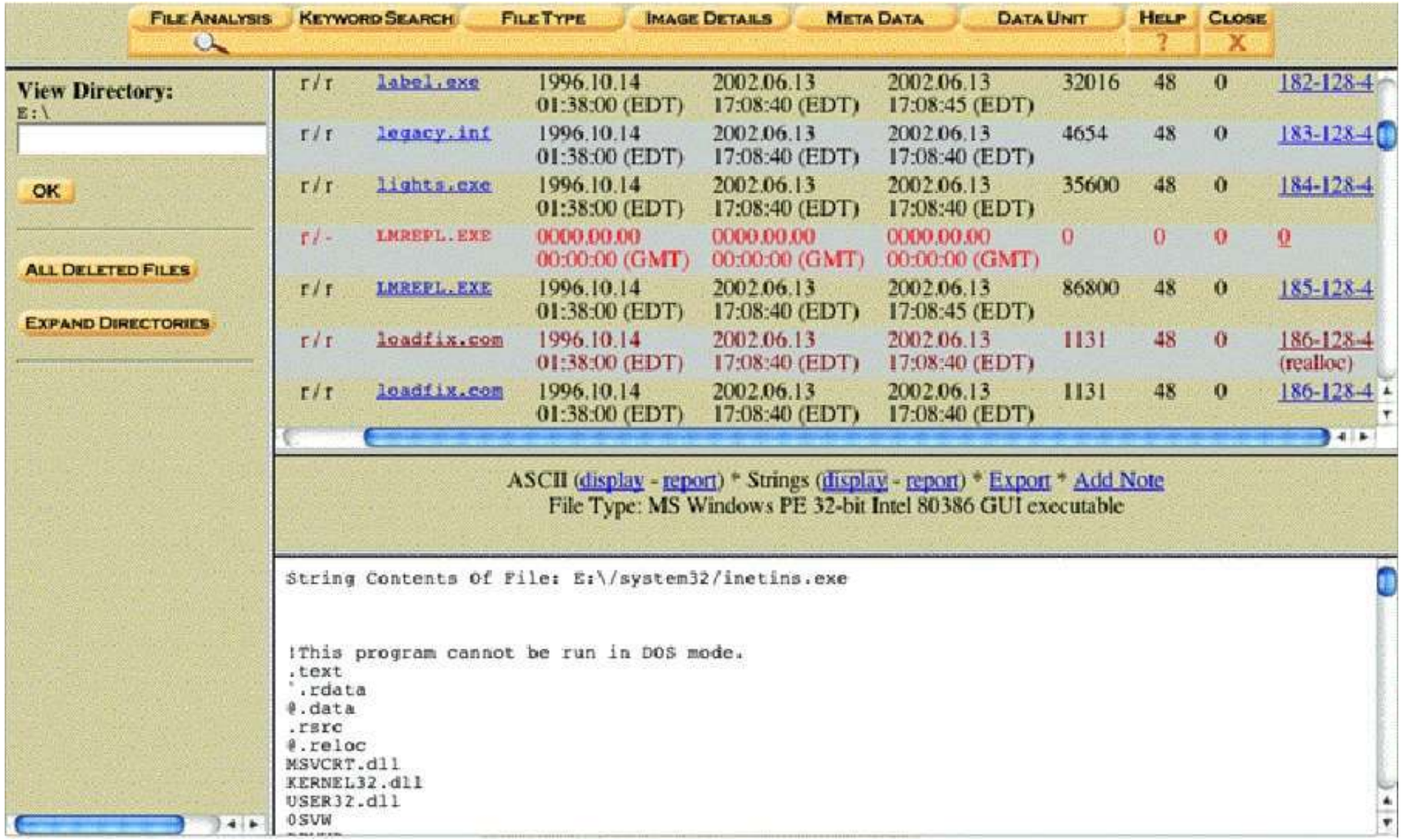
Forensics Toolkit opensource

- 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**

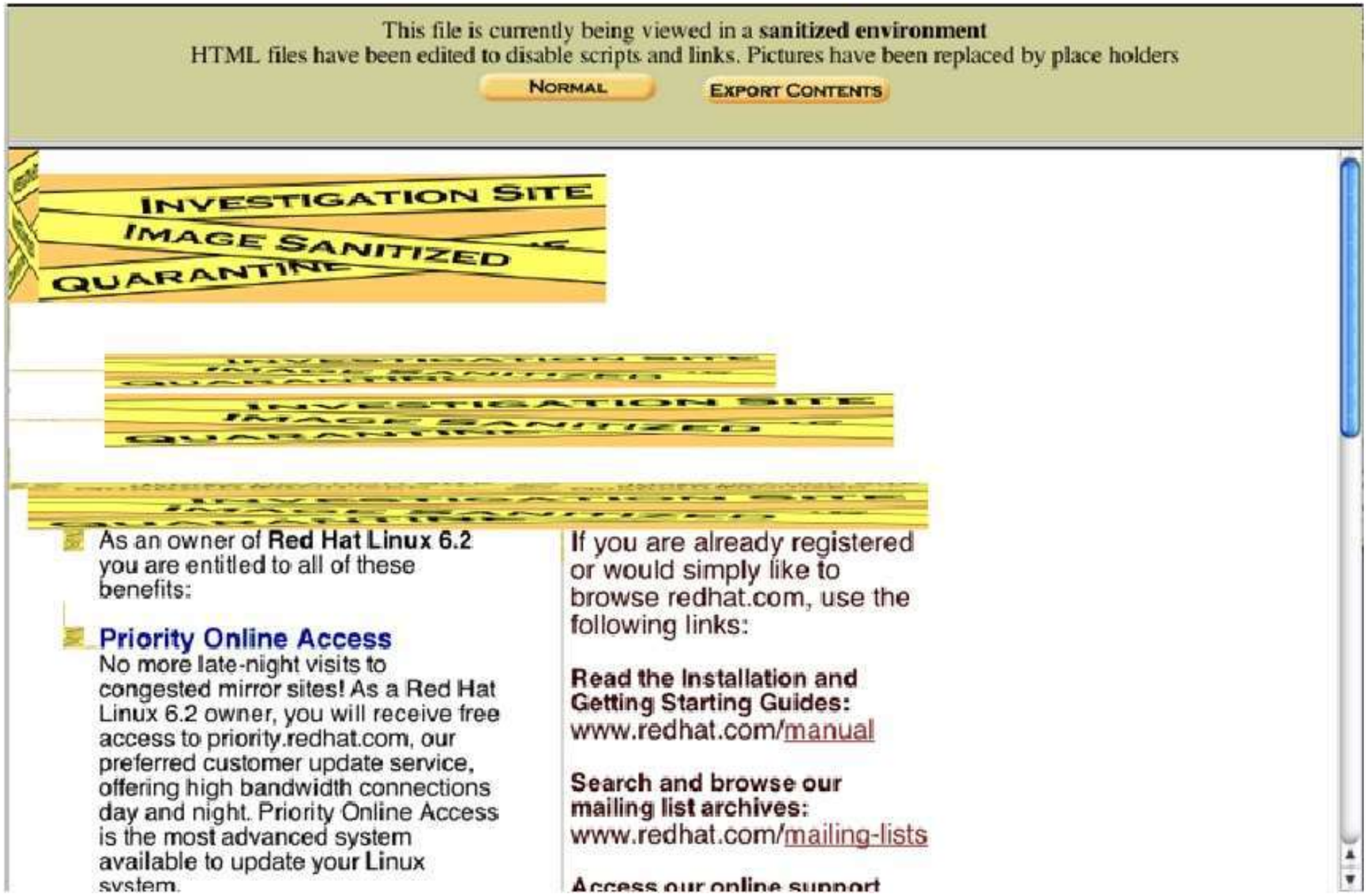
The Sleuth Kit

- 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

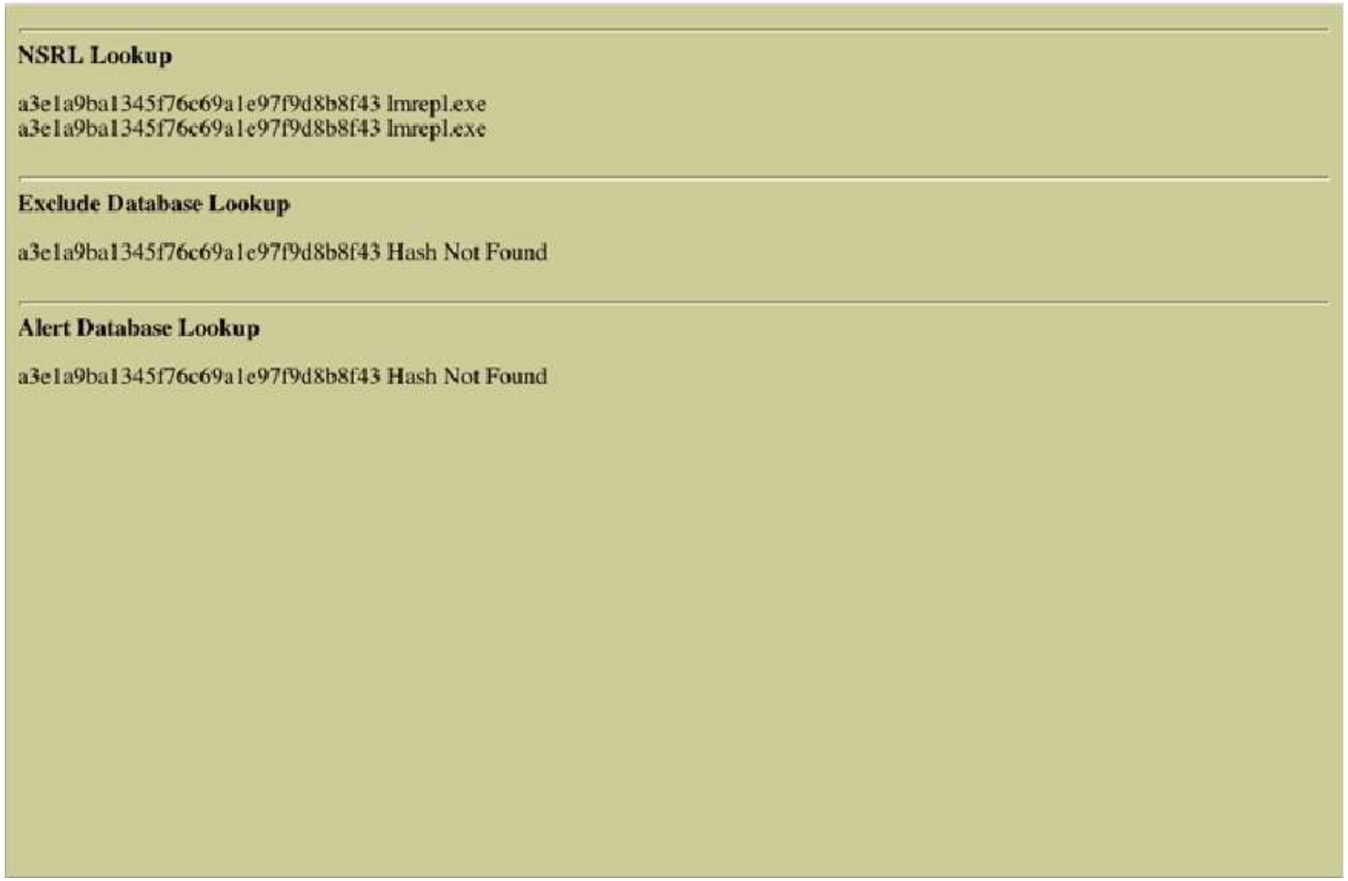
The Sleuth Kit – File Analysis



The Sleuth Kit – File Content



The Sleuth Kit – Hash Database



NSRL Lookup

a3e1a9ba1345f76c69a1e97f9d8b8f43 lmrepl.exe
a3e1a9ba1345f76c69a1e97f9d8b8f43 lmrepl.exe

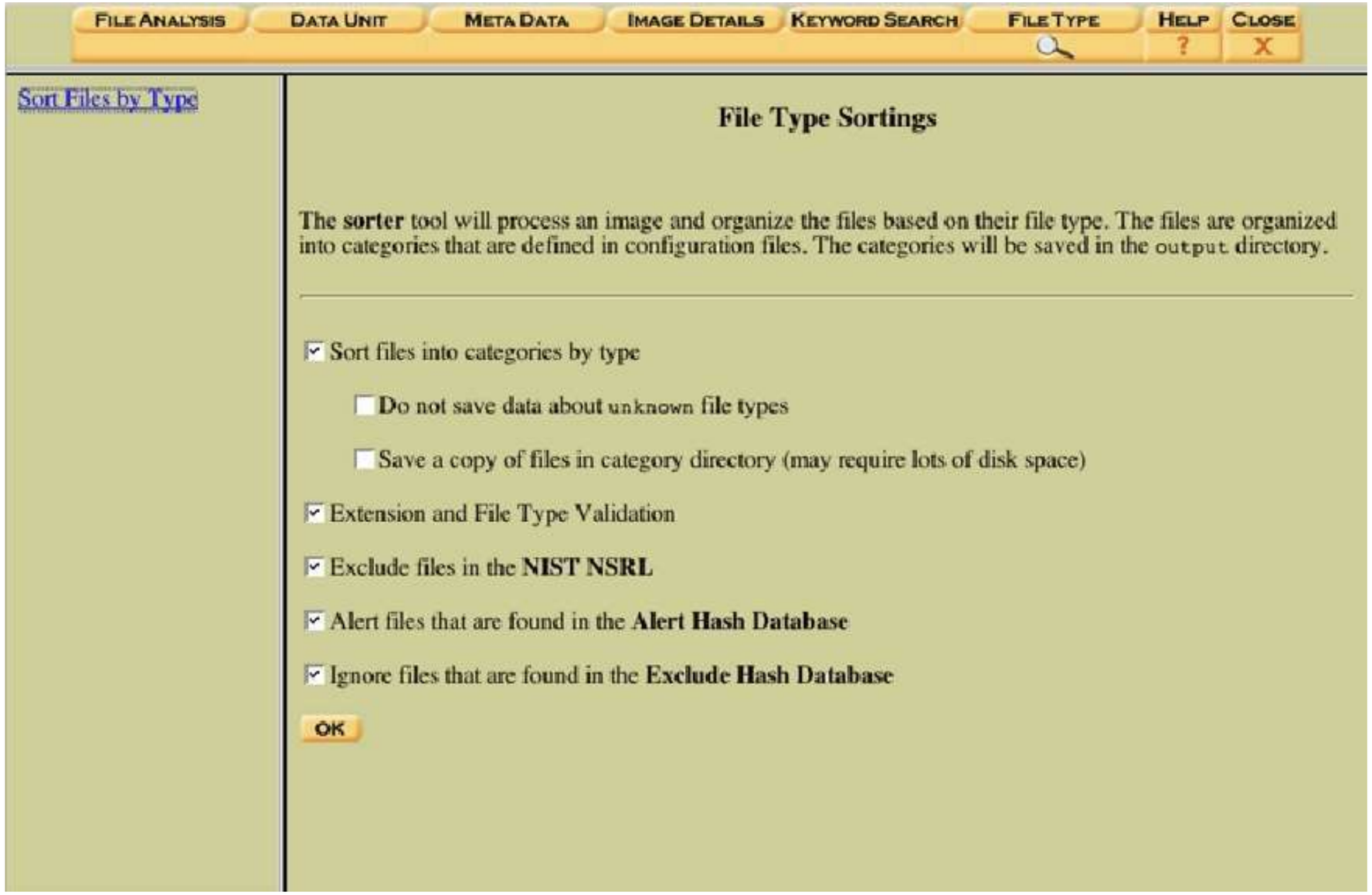
Exclude Database Lookup

a3e1a9ba1345f76c69a1e97f9d8b8f43 Hash Not Found

Alert Database Lookup

a3e1a9ba1345f76c69a1e97f9d8b8f43 Hash Not Found

The Sleuth Kit - File Type Sorting



The Sleuth Kit - Timeline

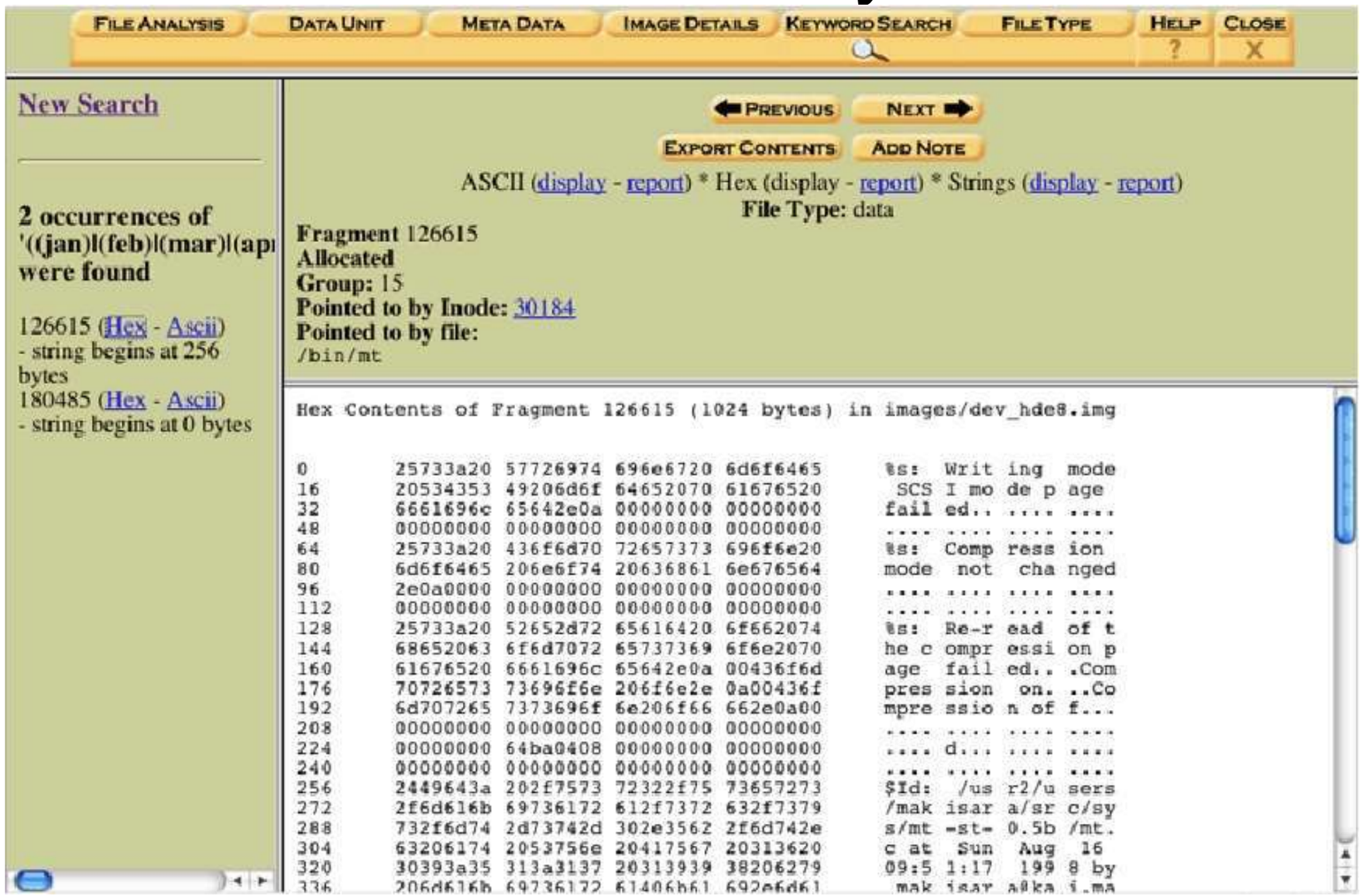
CREATE DATA FILE | CREATE TIMELINE | VIEW TIMELINE | VIEW NOTES | HELP | CLOSE

<- May 2002 Jul 2002 ->

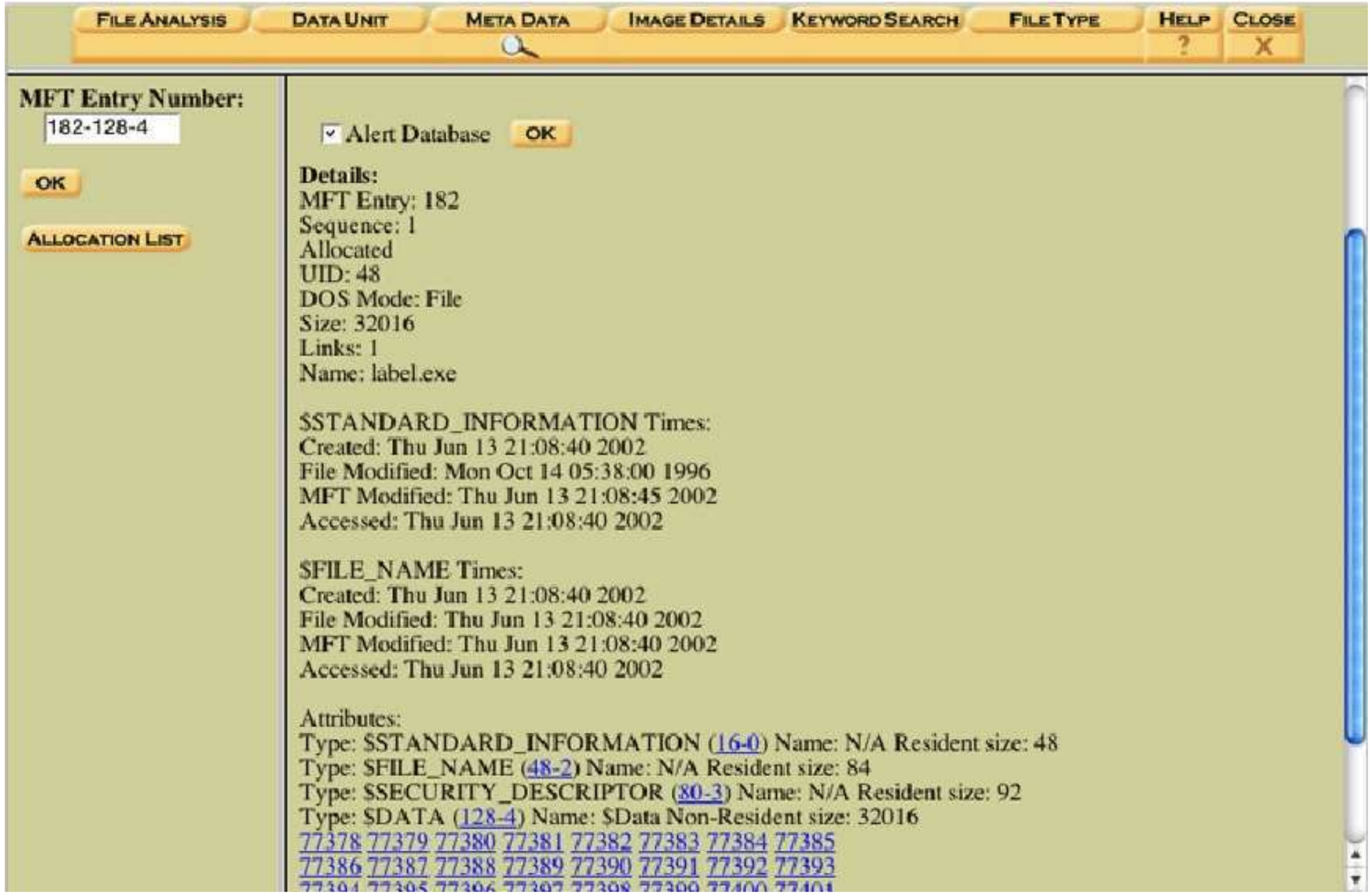
Jun 2002 OK

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/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

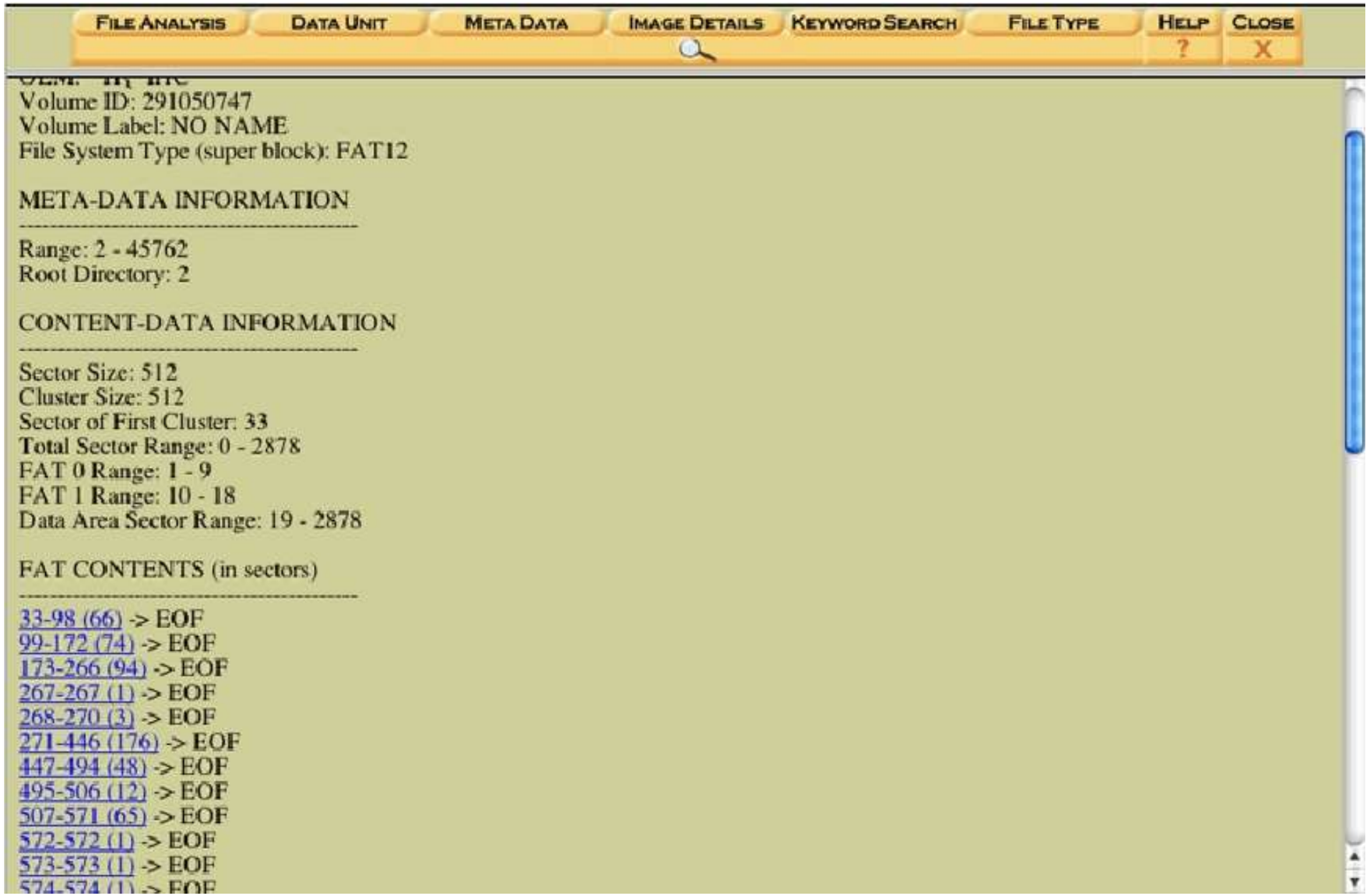
The Sleuth Kit – Key word search



The Sleuth Kit – Metadata Analysis



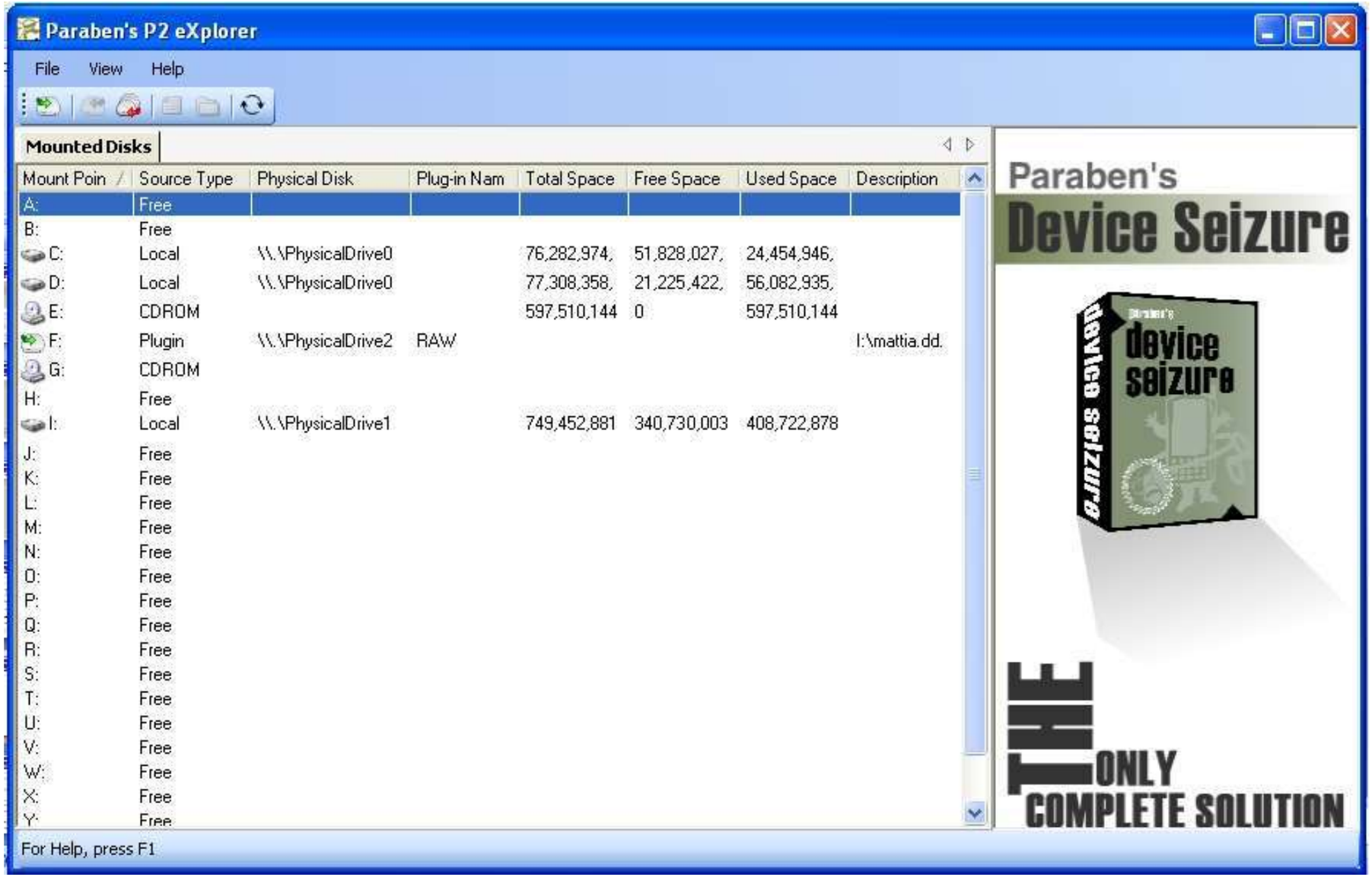
The Sleuth Kit – Image Details



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

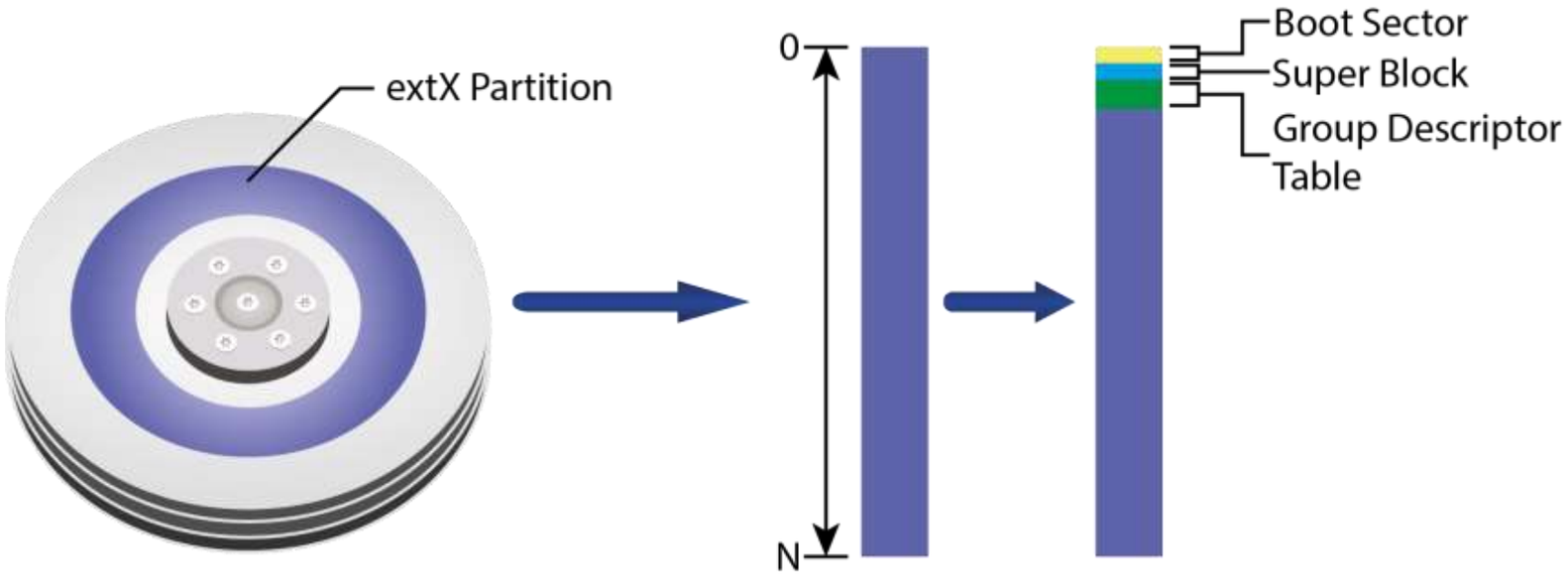
Master File Table (MFT) - NTFS

- 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

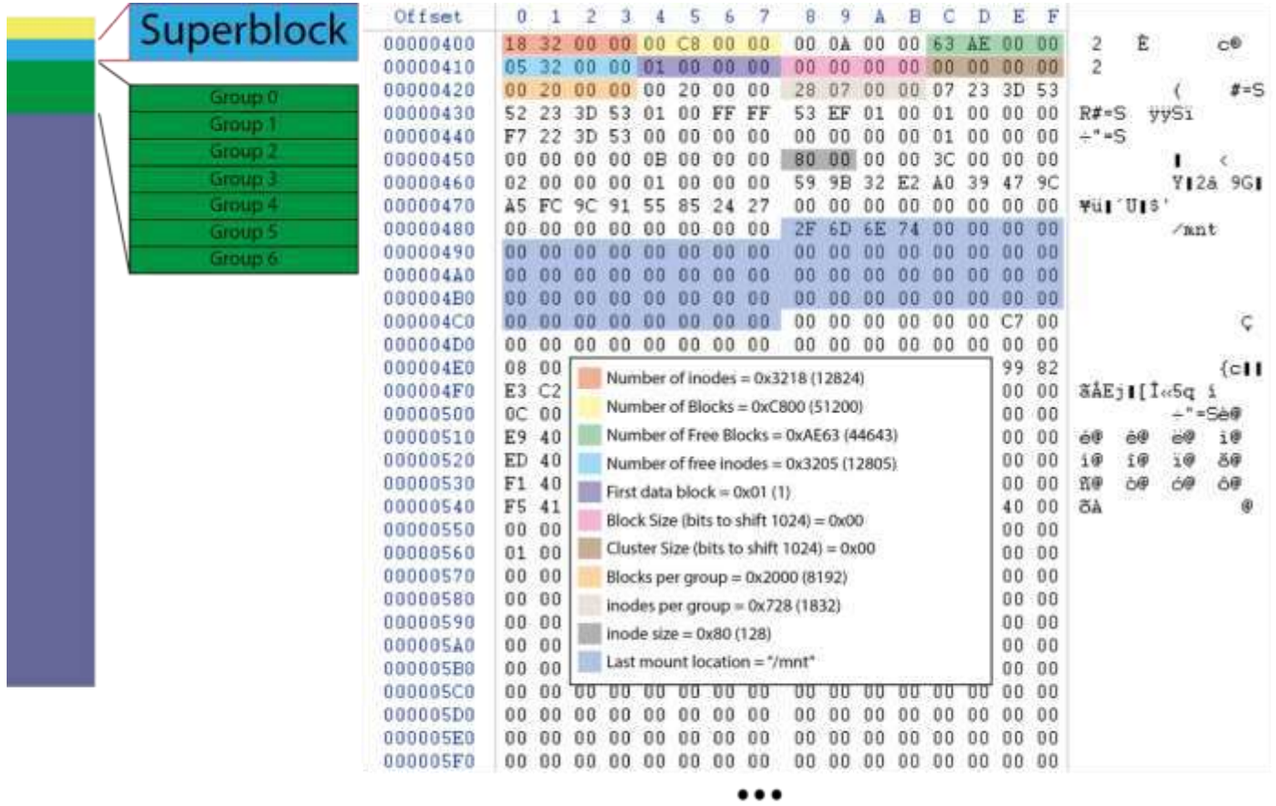
- **MMLS** – shows volume partitions
- **MFT Ripper** (commercial)
- **AnalyzeMFT.py** (opensource)
- **MFTView** (freeware)
- **NTFSWalk** (freeware)
- **Windows Journal Parser** (freeware)

File System



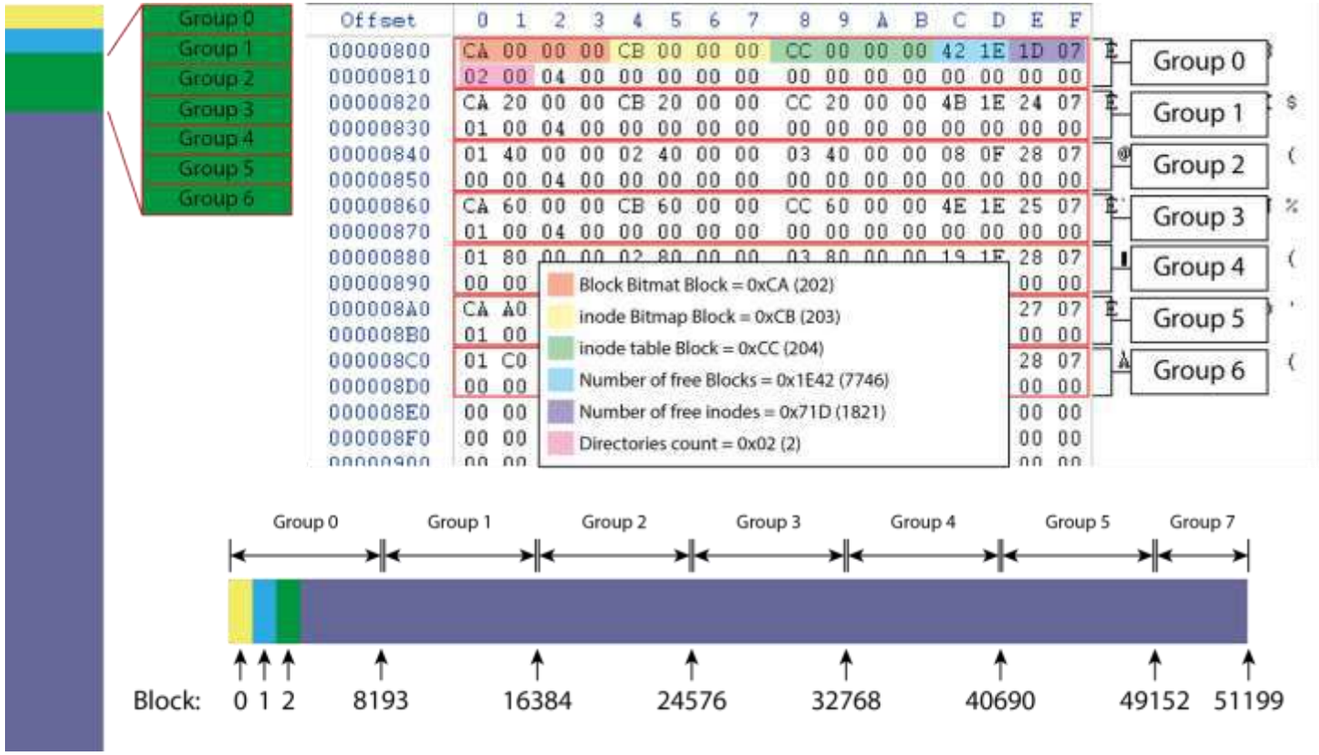
Credits By George

File System



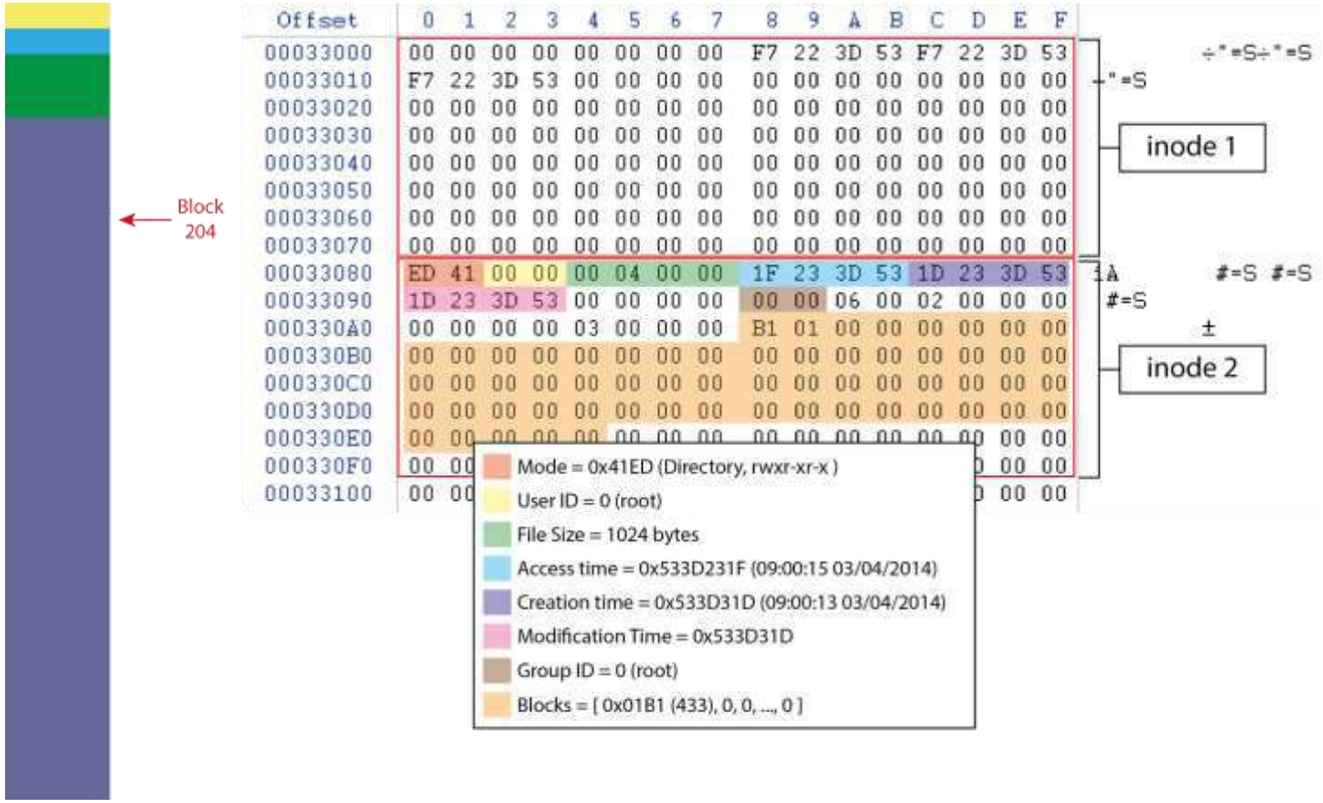
Credits By George

File System



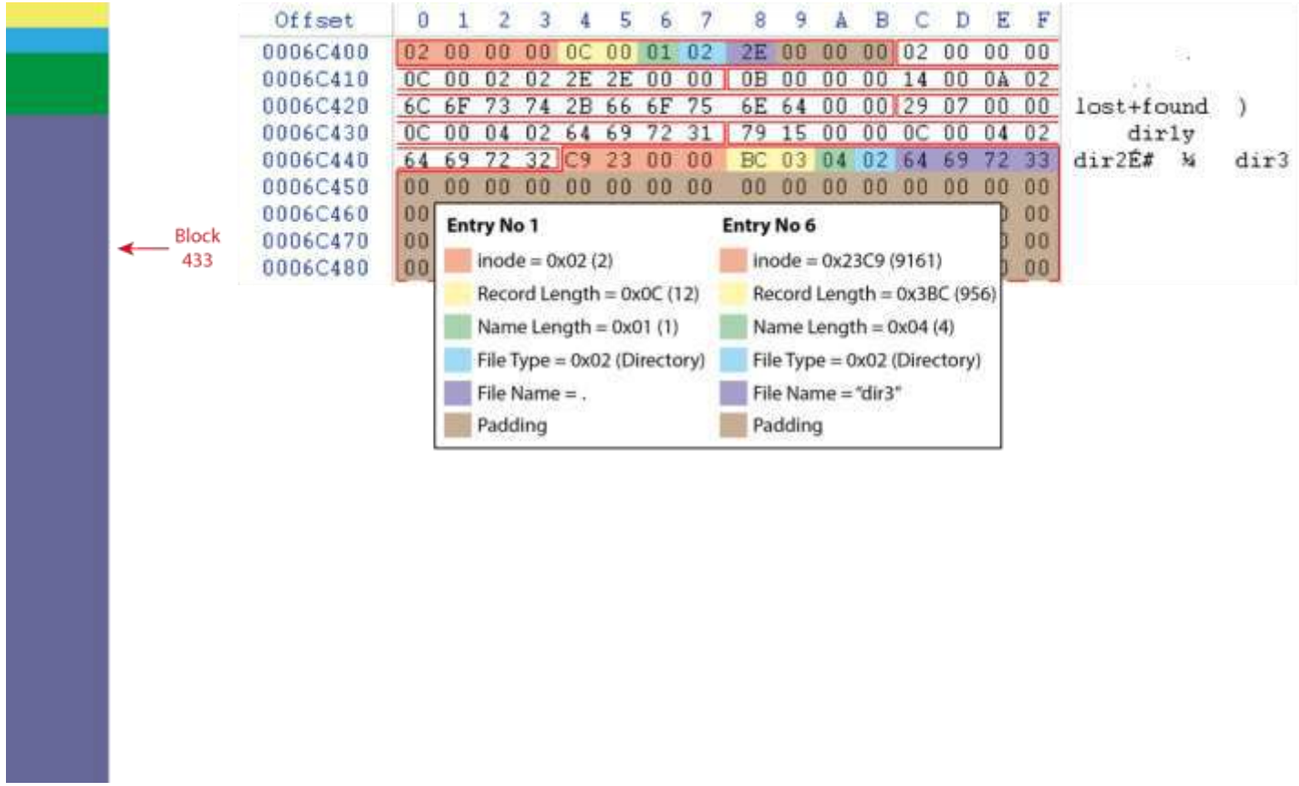
Credits By George

File System



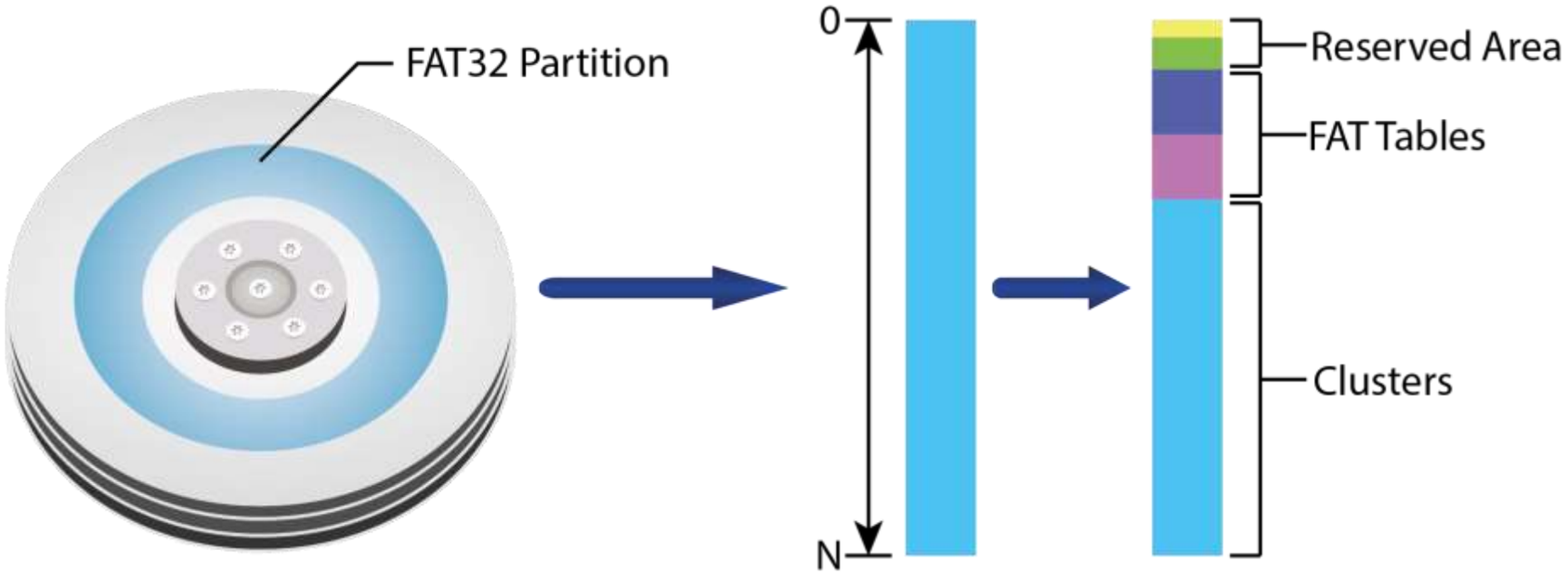
Credits By George

File System



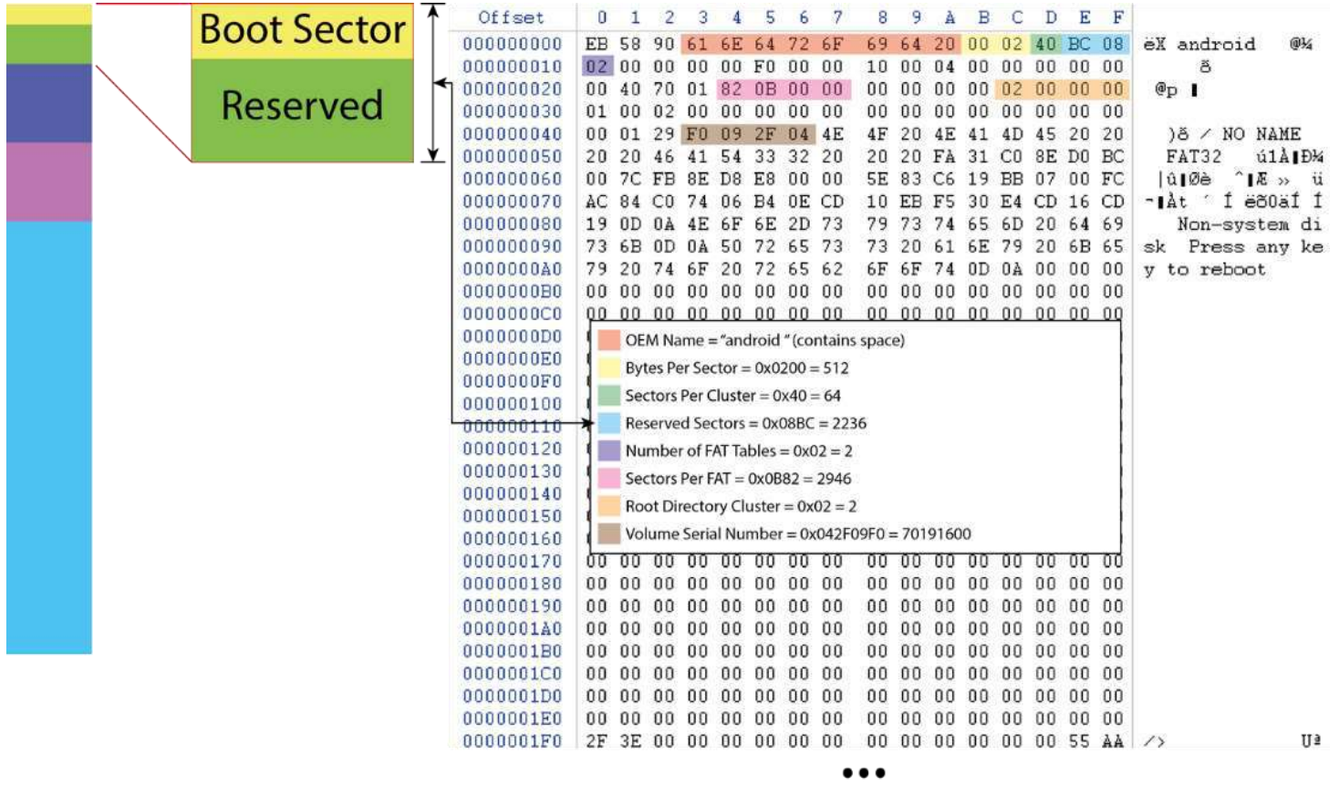
Credits By George

File System



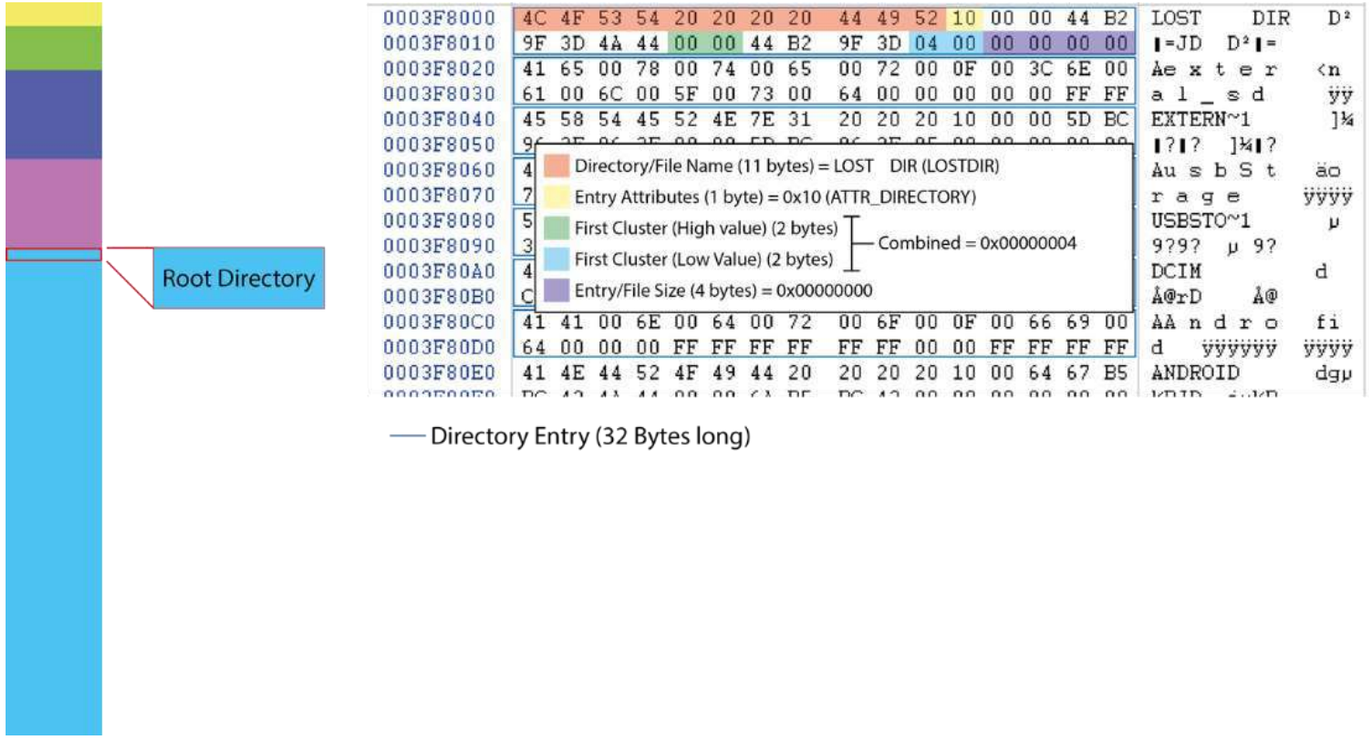
Credits By George

File System



Credits By George

File System



Credits By George

File System


```
          0        1        2        3
000117800 [F0 FF FF 0F][FF FF FF FF][FF FF FF 0F][00 00 00 00]
000117810  FF FF FF 0F  FF FF FF 0F  FF FF FF 0F  FF FF FF 0F
000117820  FF FF FF 0F  FF FF FF 0F  FF FF FF 0F  0E 00 00 00
000117830  FF FF FF 0F  FF FF FF FF  [Root Directory Entry]  FF FF 0F
000117840  FF FF FF 0F  FF FF FF FF                          FF FF 0F
000117850  FF FF FF 0F  16 00 00 00  17 00 00 00  19 00 00 00
000117860  A2 00 00 00  1A 00 00 00  1C 00 00 00  FF FF FF 0F
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
```

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) ← File 2: First Cluster = 0x07 (7)
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

Credits By George

File System

000408000	2E	20	20	20	20	20	20	20	20	20	20	10	00	00	44	B2
000408010	9F	3D	9F	3D	00	00	44	B2	9F	3D	04	00	00	00	00	00
000408020	2E	2E	20	20	20	20	20	20	20	20	20	10	00	00	44	B2
000408030	9F	3D	9F	3D	00	00	44	B2	9F	3D	00	00	00	00	00	00
000408040	32	32	38	20	20	20	20	20	20	20	20	00	00	00	00	00
000408050	21	00	7E	40	00	00	00	00	21	00	E4	00	00	80	00	00
000408060	32	33	31	20	20	20	20	20	20	20	20	00	00	00	00	00

Credits By George

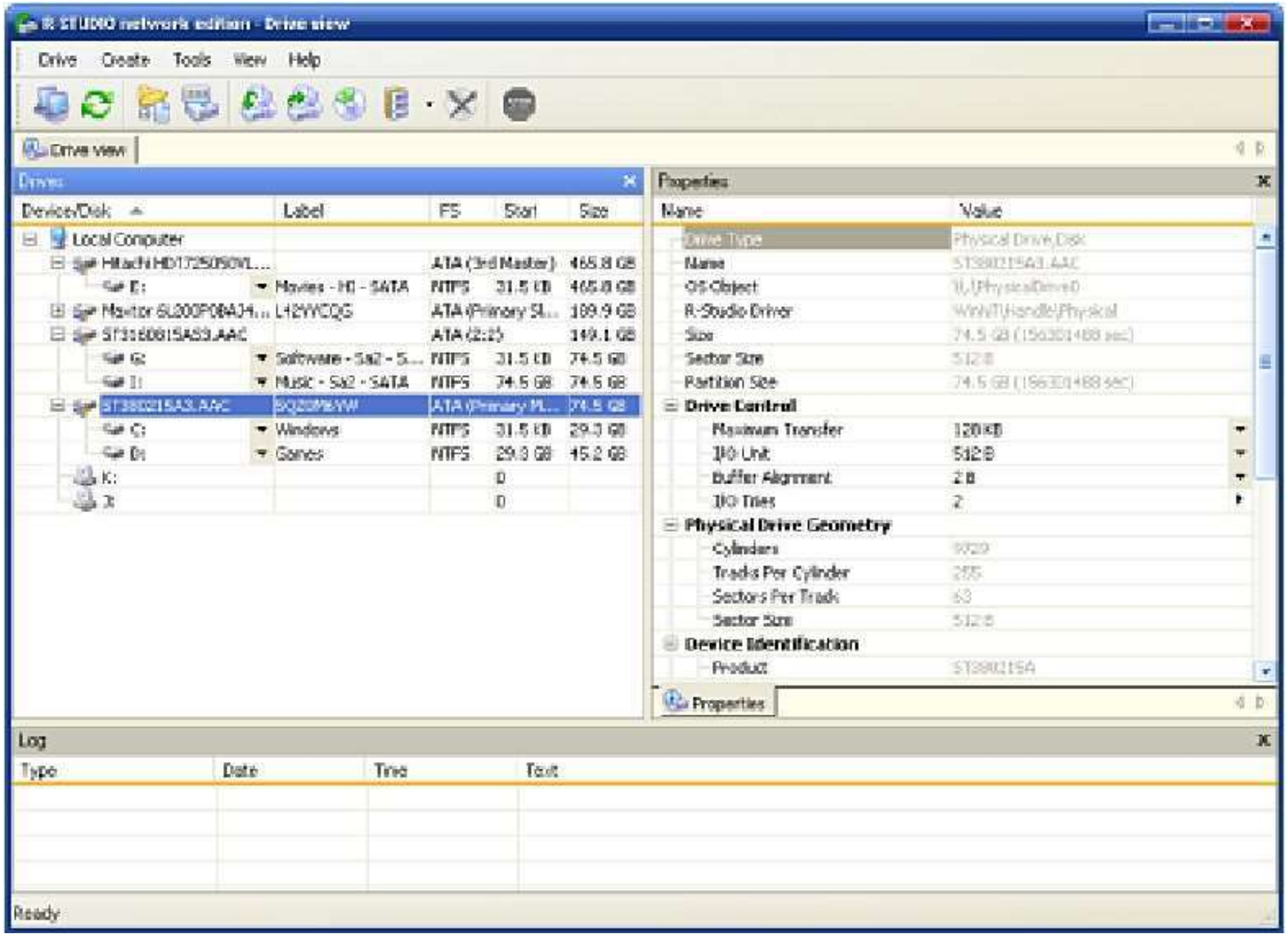
Deleted Files

- 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



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

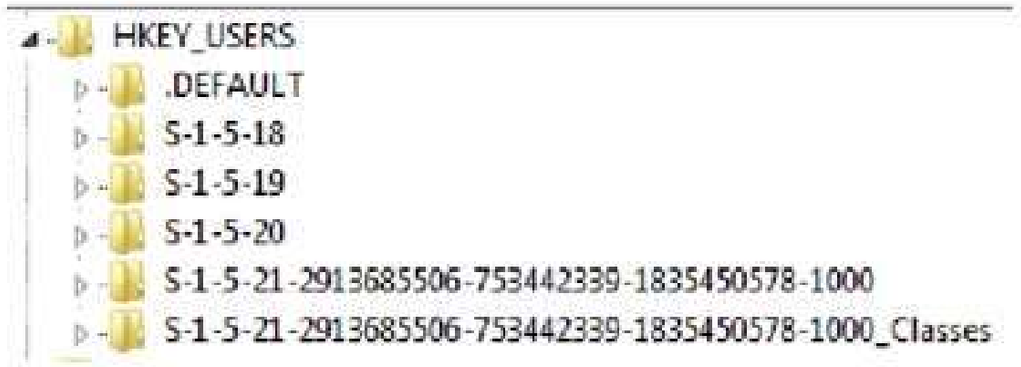
Windows Registry

- 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

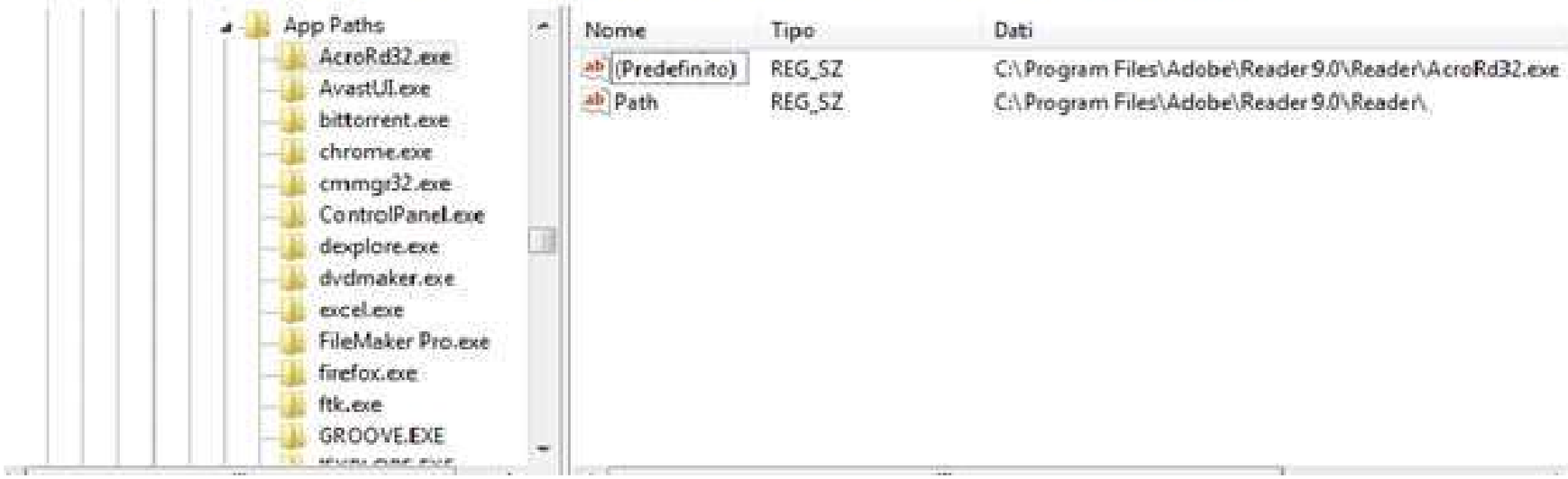
Nome	Tipo	Dati
(Predefinito)	REG_SZ	(valore non impostato)
\REGISTRY\MACHINE\BCD00000000	REG_SZ	\Device\HarddiskVolume2\Boot\BCD
\REGISTRY\MACHINE\HARDWARE	REG_SZ	
\REGISTRY\MACHINE\SAM	REG_SZ	\Device\HarddiskVolume3\Windows\System32\config\SAM
\REGISTRY\MACHINE\SECURITY	REG_SZ	\Device\HarddiskVolume3\Windows\System32\config\SECURITY
\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

- La chiave

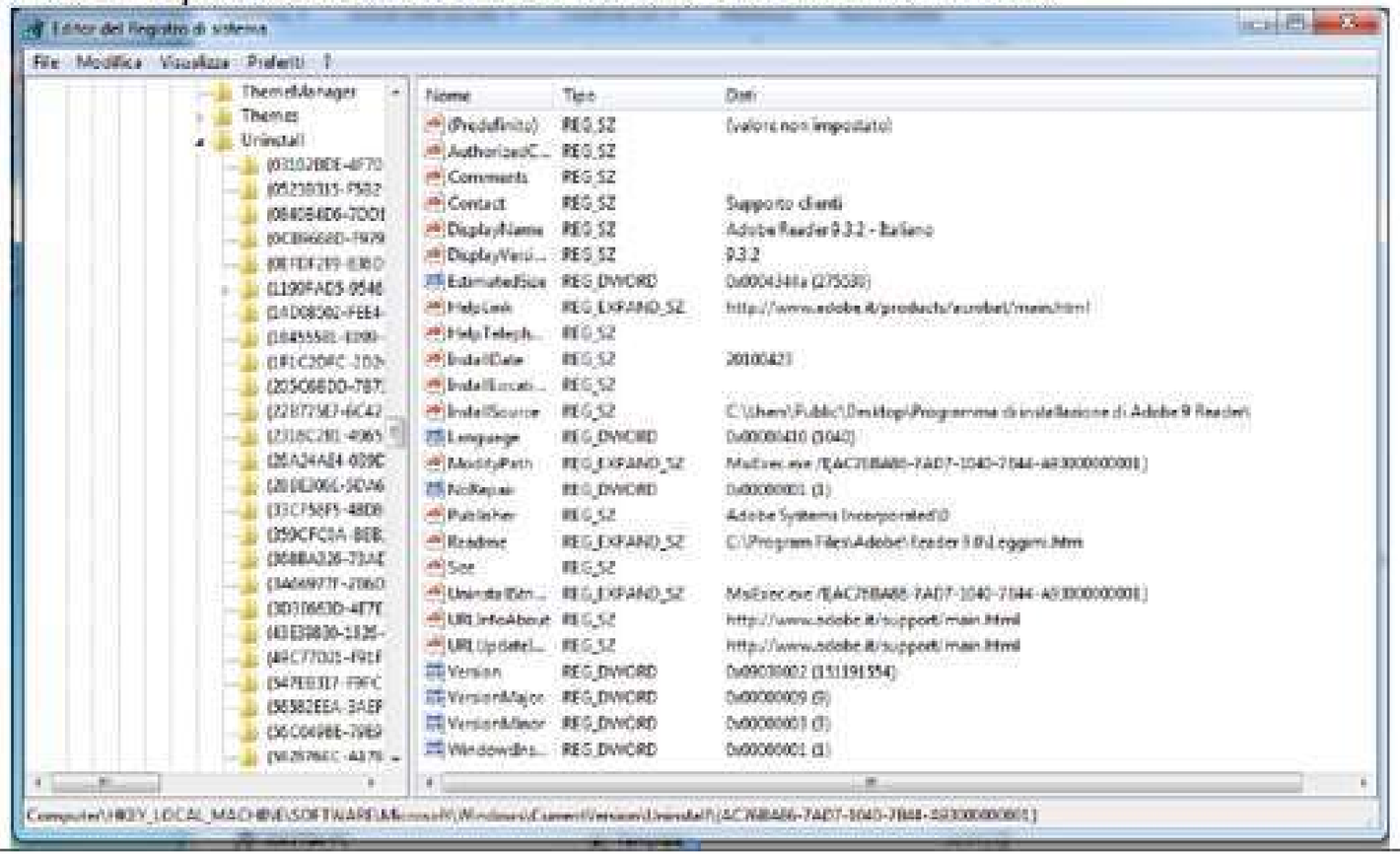
  HKLM\Software\Microsoft\Windows\CurrentVersion\AppPath

  contiene i percorsi di installazione delle varie applicazioni



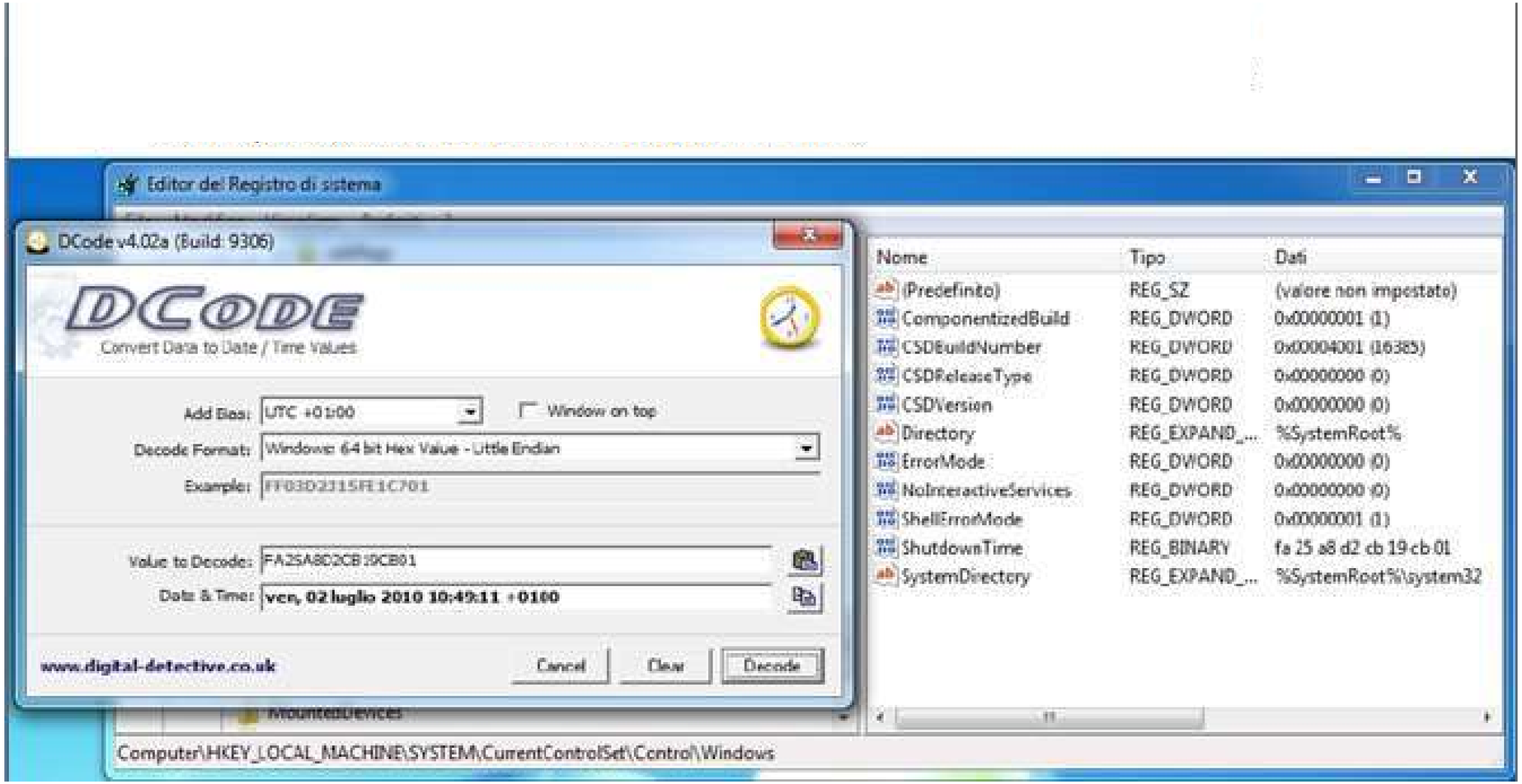
Windows Registry – Hive Software

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



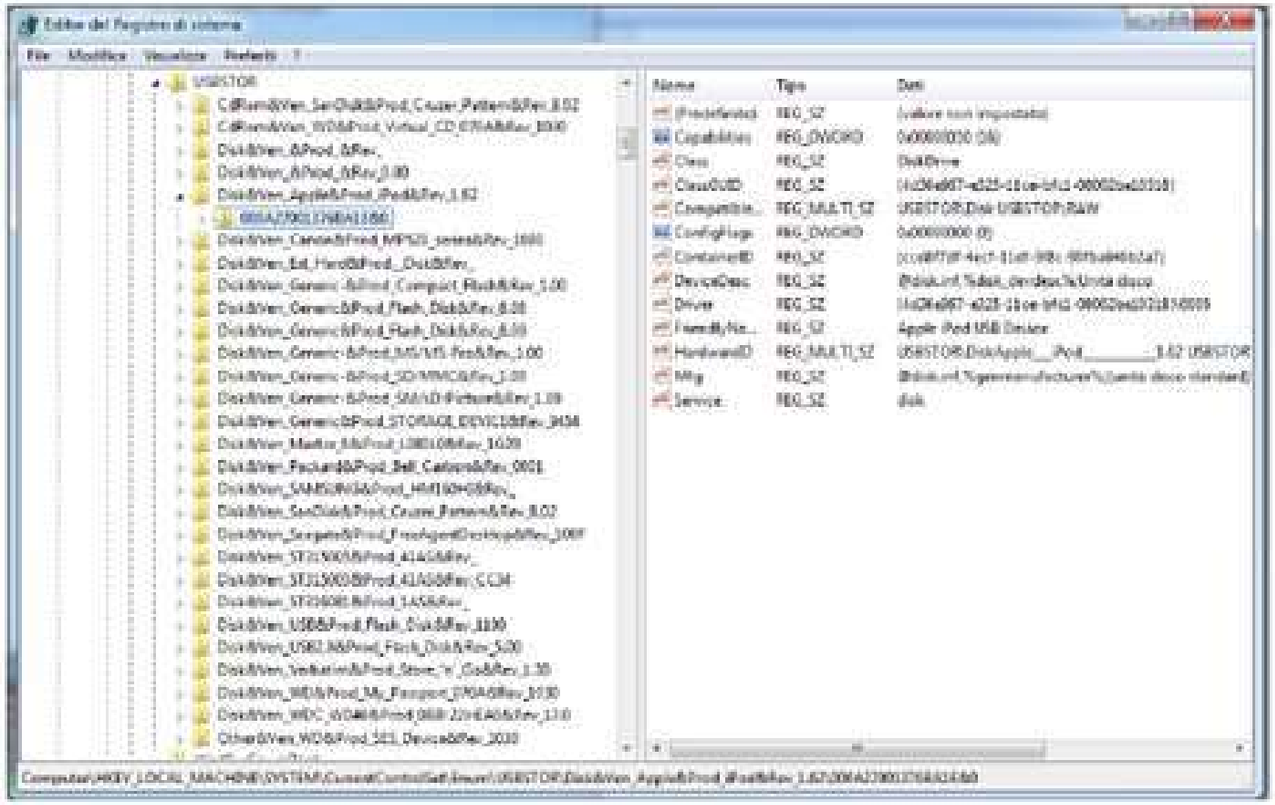
Windows Registry – Hive Software

The Shut Down Time, Time Zone Information



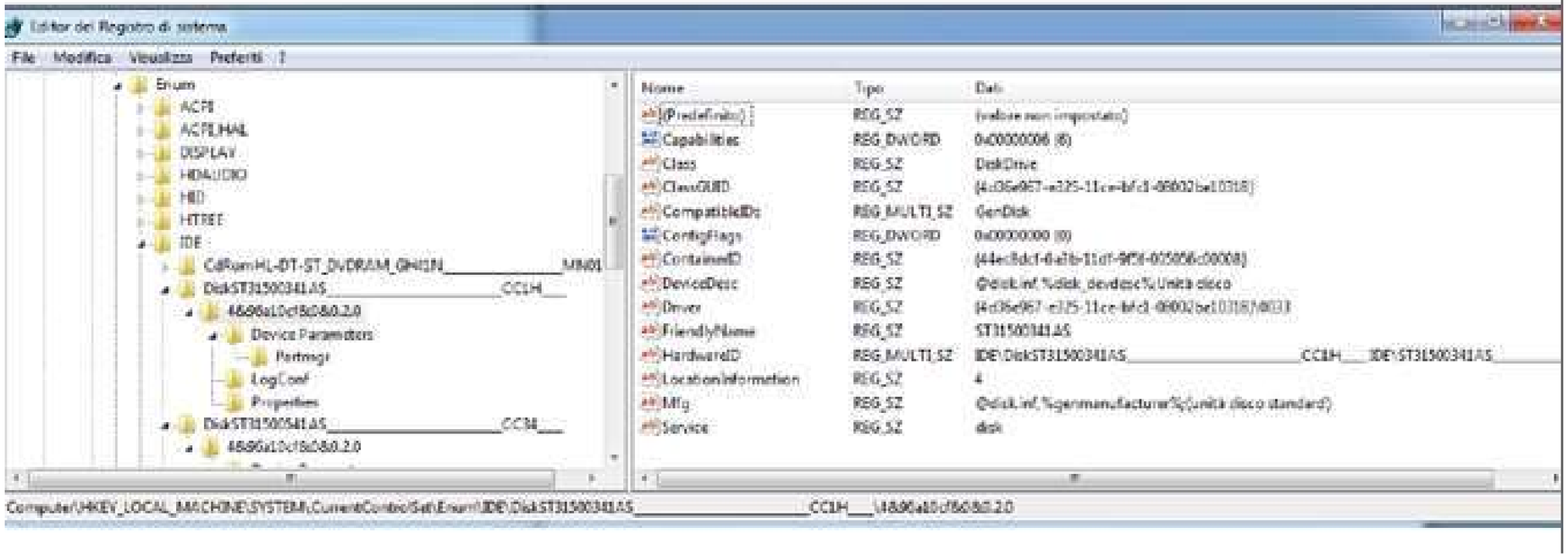
Windows Registry – Hive System - USB

HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR



Windows Registry – Hive System - IDE

HKLM\SYSTEM\CurrentControlSet\Enum\IDE



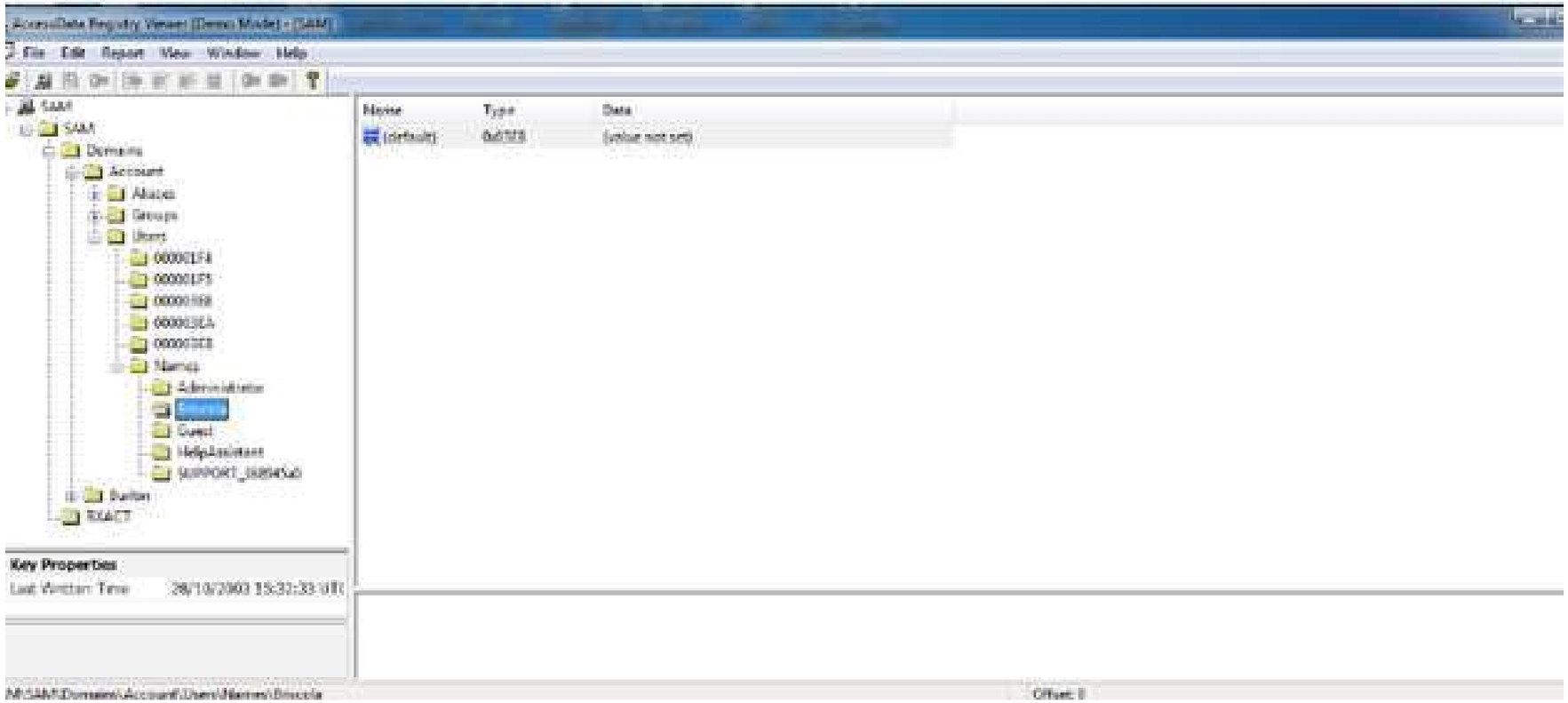
Windows Registry – Hive System

Services Installed in a Computer

HKLM\System\CurrentControlSet\Services

Windows Registry – Hive System

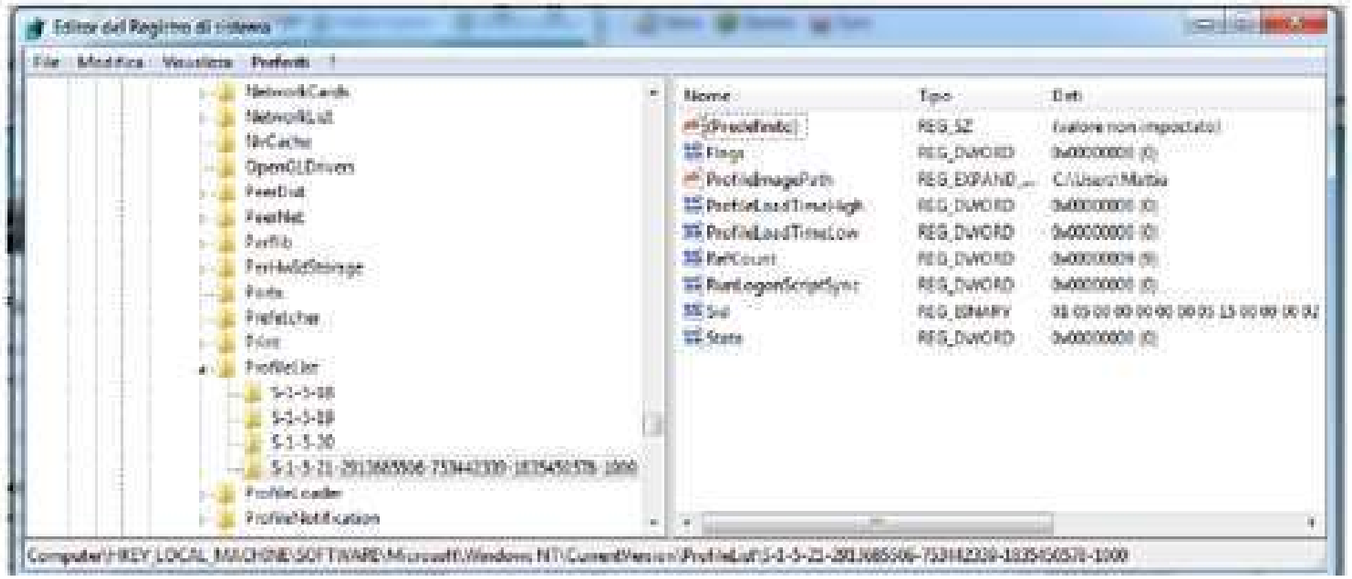
- La hive SAM contiene le informazioni sugli utenti e i gruppi configurati nella macchina
- Il file si trova nella cartella %SYSTEMROOT%\system32\config



Windows Registry – Hive SAM

USERS AND GROUP

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



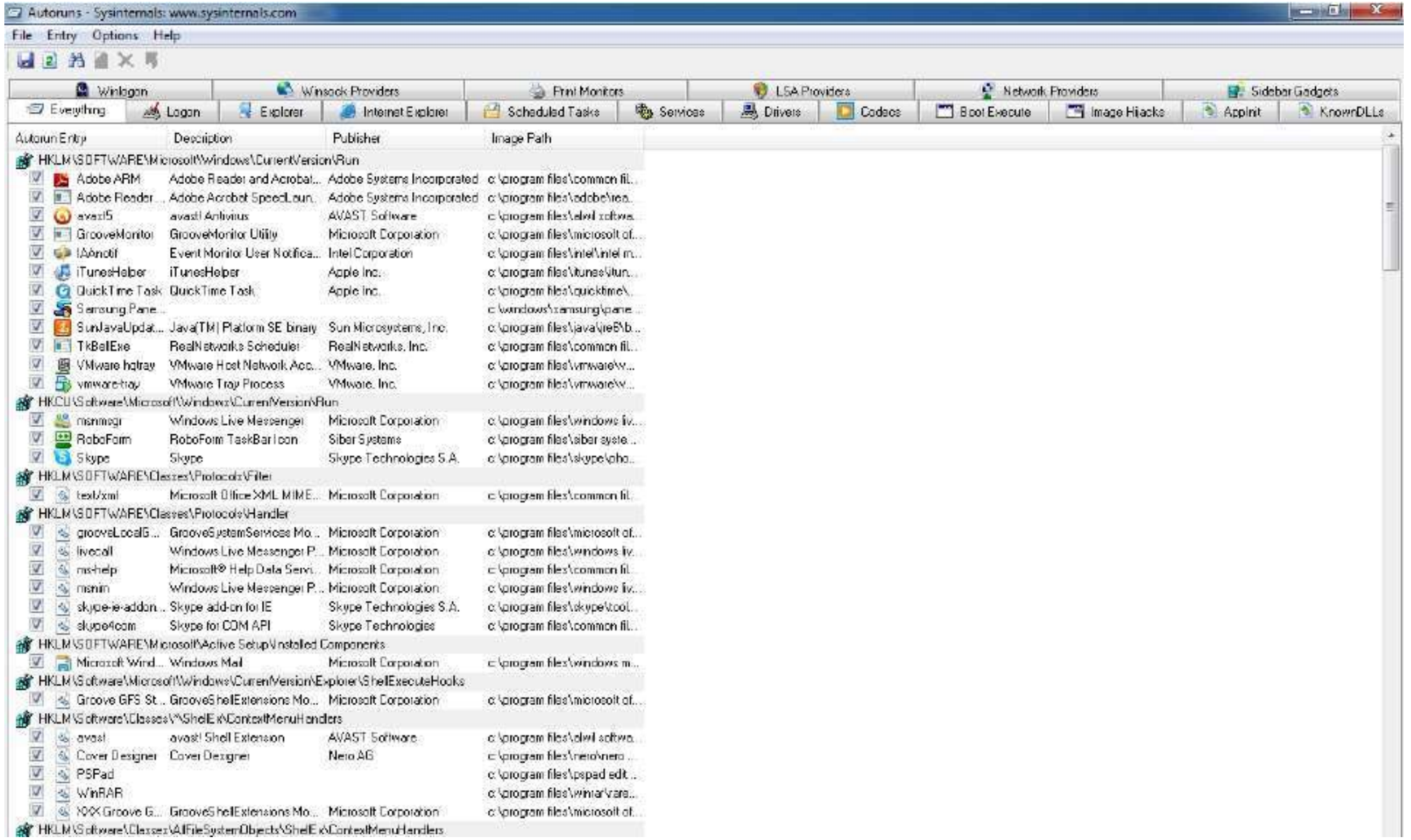
Autorun

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
Adobe Reader ...
Adobe Acrobat SpeedLaun...
Adobe Systems Incorporated
avast!5
avast! Antivirus
AVAST Software
GrooveMonitor
GrooveMonitor Utility
Microsoft Corporation
IAAnotif
Event Monitor User Notifica...
Intel Corporation
iTunesHelper
iTunesHelper
Apple Inc.
QuickTime Task
QuickTime Task
Apple Inc.
Samsung Pane...
SunJavaUpdat...
Java(TM) Platform SE binary
Sun Microsystems, Inc.
TkBellExe
RealNetworks Scheduler
RealNetworks, Inc.
VMware hqtray
VMware Host Network Acc...
VMware, Inc.
vmware-tray
VMware Tray Process
VMware, Inc.
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
msnmsgr
Windows Live Messenger
Microsoft Corporation
RoboForm
RoboForm TaskBar Icon
Siber Systems
Skype
Skype
Skype Technologies S.A.
HKLM\SOFTWARE\Classes\Protocols\Filter
text/xml
Microsoft Office XML MIME...
Microsoft Corporation
HKLM\SOFTWARE\Classes\Protocols\Handler
grooveLocalG...
GrooveSystemServices Mo...
Microsoft Corporation
livecall
Windows Live Messenger P...
Microsoft Corporation
ms-help
Microsoft® Help Data Servi...
Microsoft Corporation
msnim
Windows Live Messenger P...
Microsoft Corporation
skype-ie-addon...
Skype add-on for IE
Skype Technologies S.A.
skype4com
Skype for COM API
Skype Technologies
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
Microsoft Wind...
Windows Mail
Microsoft Corporation
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
Groove GFS St...
GrooveShellExtensions Mo...
Microsoft Corporation
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers
avast
avast! Shell Extension
AVAST Software
Cover Designer
Cover Designer
Nero AG
PSPad
WinRAR
XXX Groove G...
GrooveShellExtensions Mo...
Microsoft Corporation
HKLM\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers

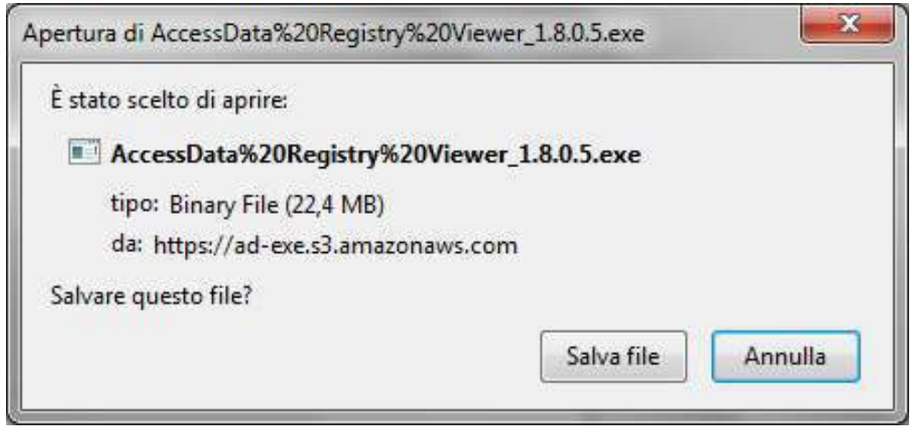
Hive NETUSER

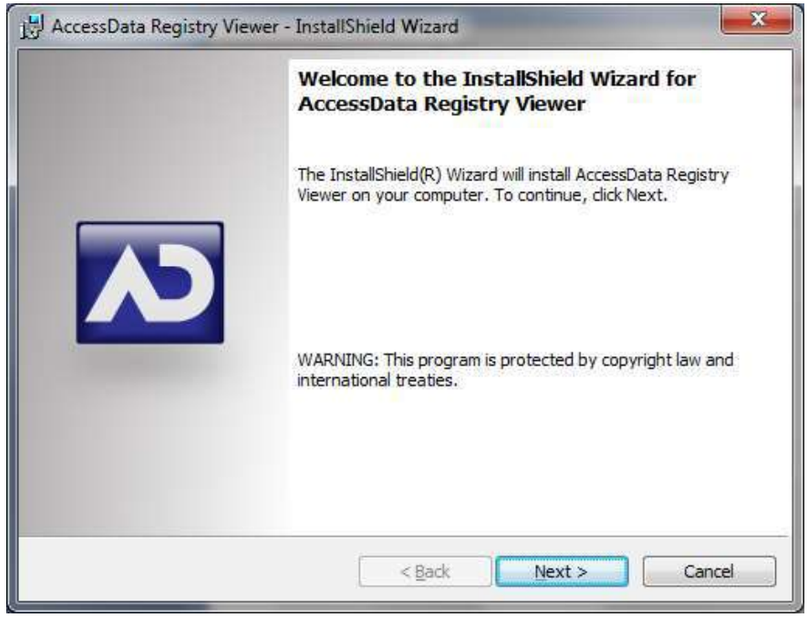
Chiave
HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\[GUID]\Count
HKU\Software\Microsoft\Windows\ShellNoRoam\MUICache
HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU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

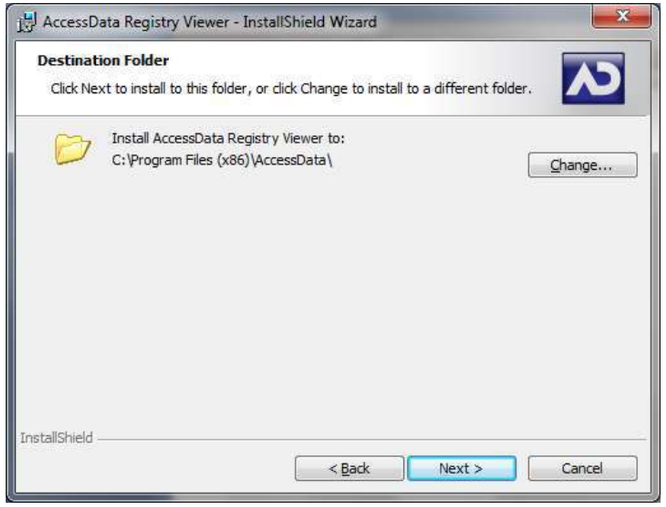
- **RegRipper (Harlan Carvey) O**penSource;
- **AccessData Registry Viewer - free**
- **Windows Registry Recovery** (www.mitec.cz) **free**
- **Windows Registry Analyzer** (www.mitec.cz) **free**
- **RegExtract** (www.woanware.co.uk) **free**
- **USBDeviceForensics** (www.woanware.co.uk)
- **ForensicsUserInfo**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

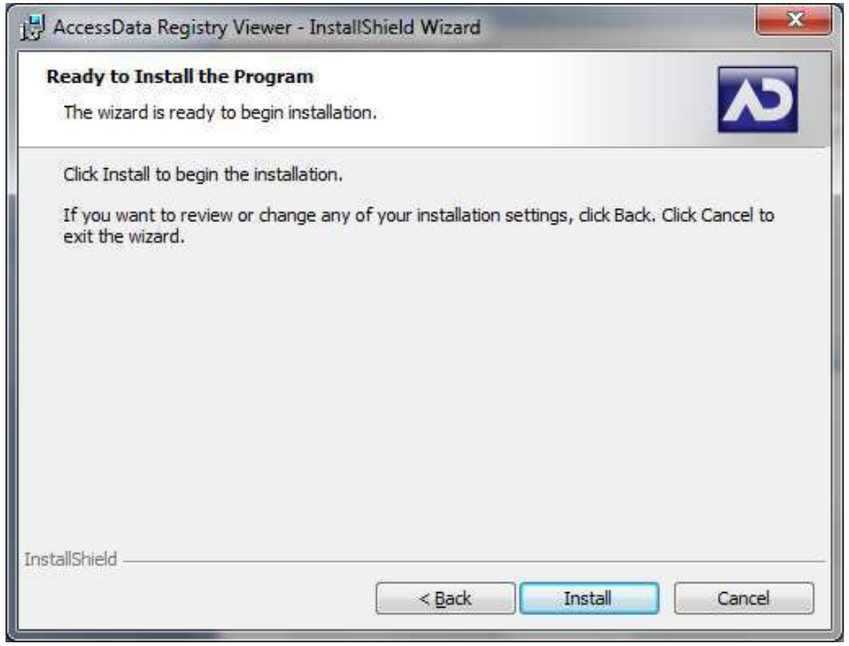
Tools for the register analysis



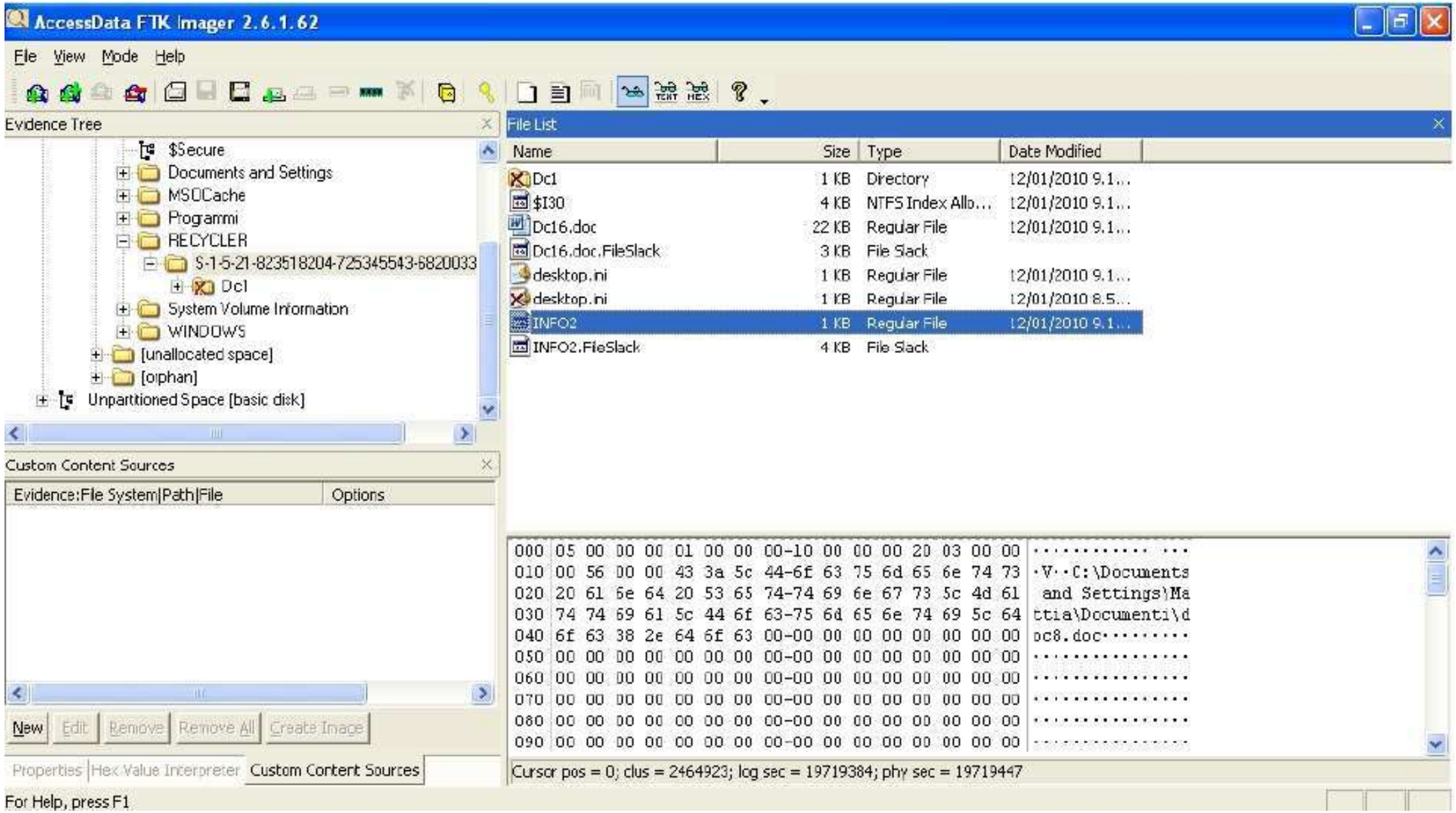


Tools for the register analysis





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]
Unpartitioned 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

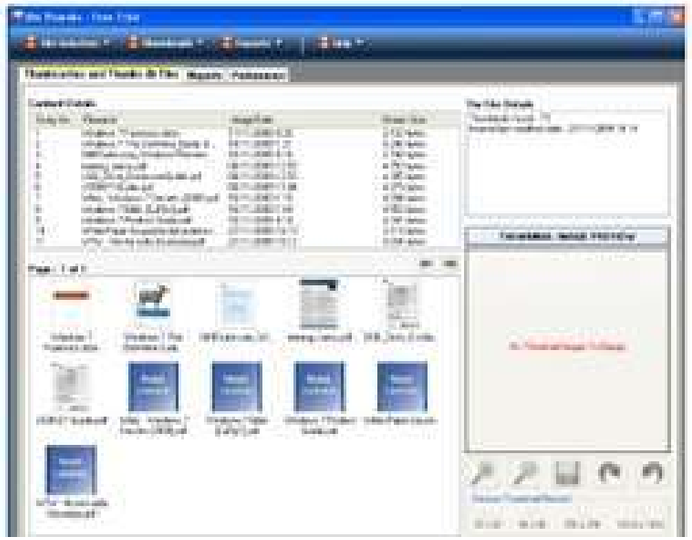
- Windows File Analyzer (www.mitec.cz)
  -
- Win Forensic Analysis (http://www.machor-software.com/)
- Link Viewer (http://www.gaijin.at/)
- Lnkanalyser (http://www.woany.co.uk/)
- SimpleCarver (http://www.simplecarver.com/)

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

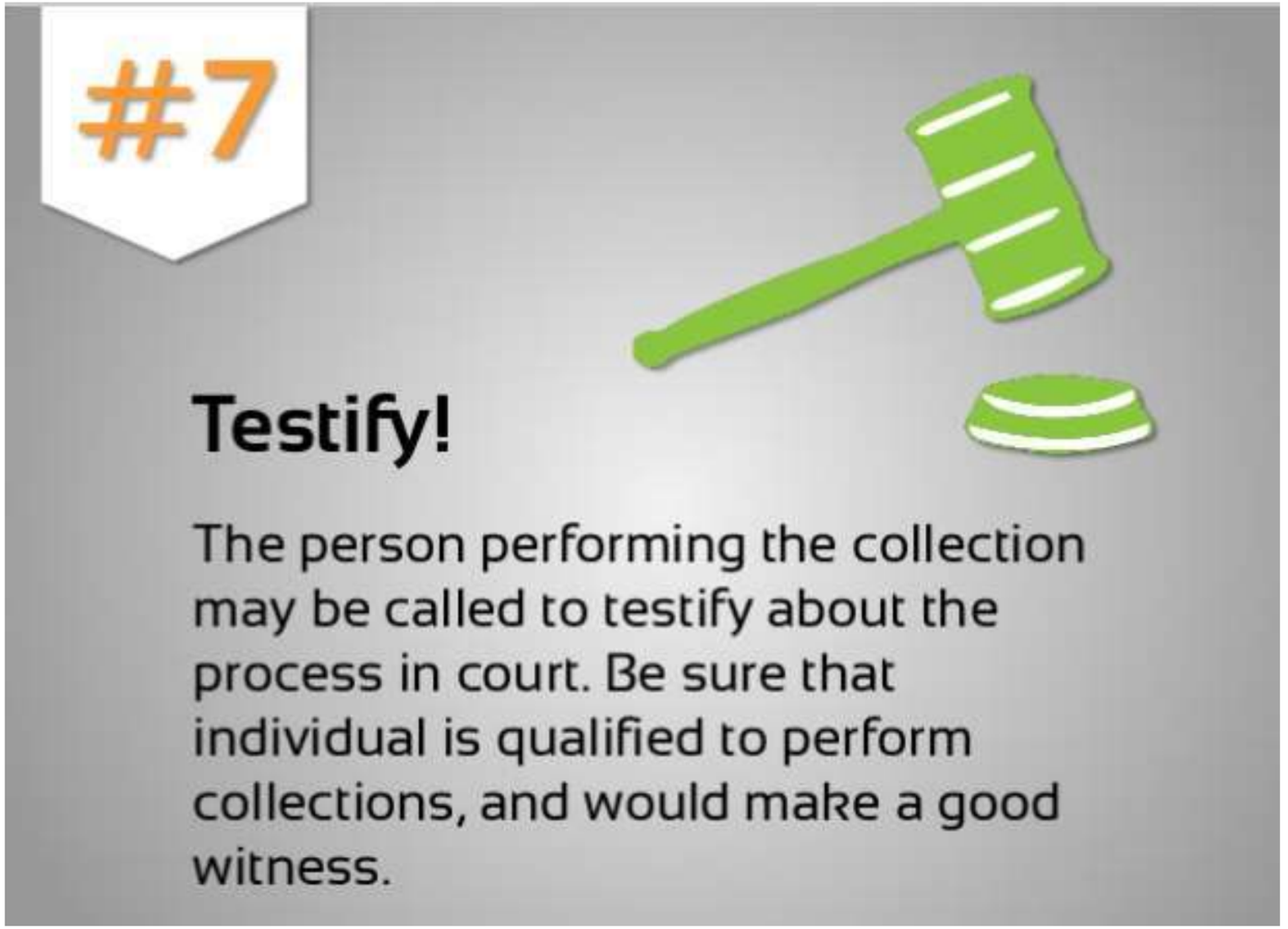
Internet Artifacts

Internet Artifacts

Internet Artifacts

Internet Artifacts

Internet Artifacts

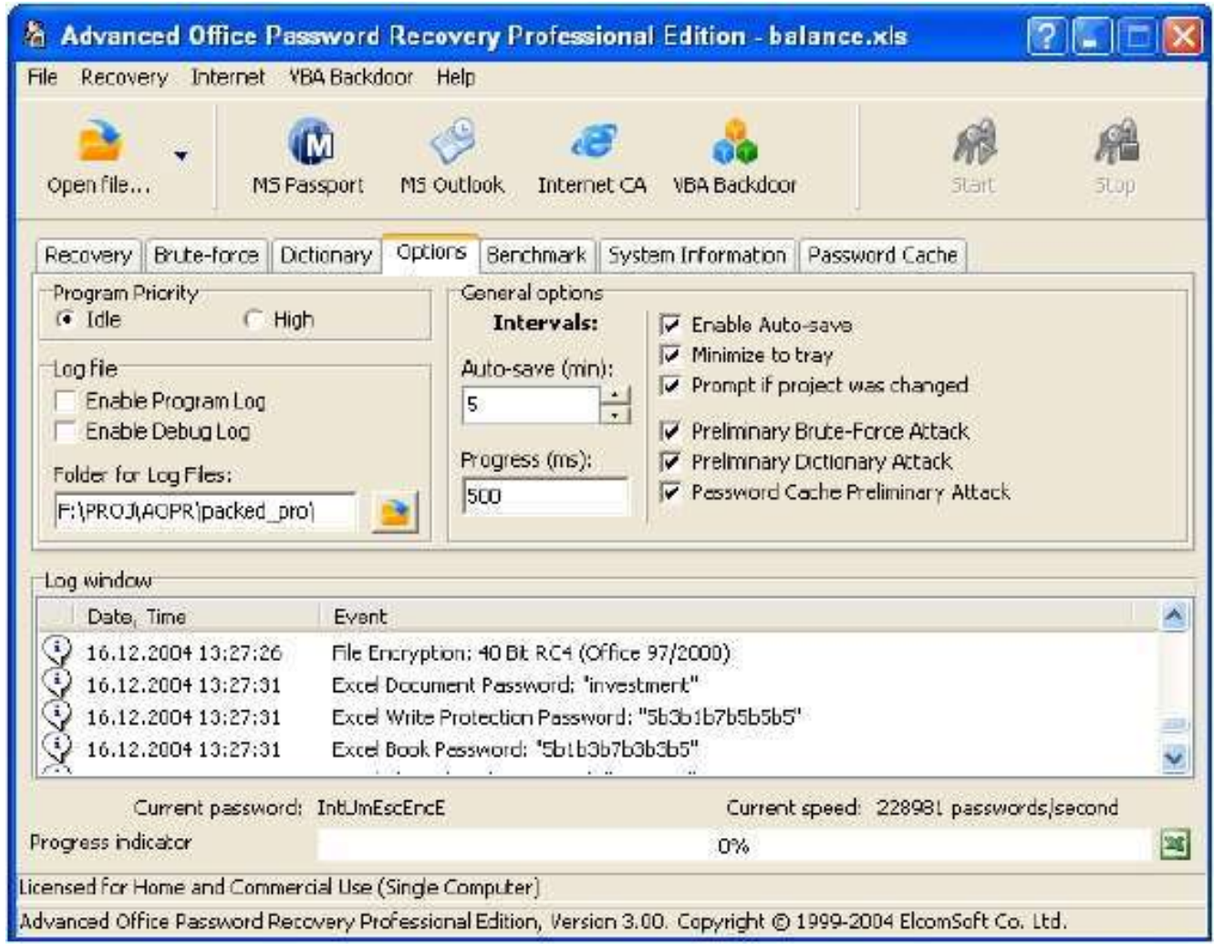


File password cracking

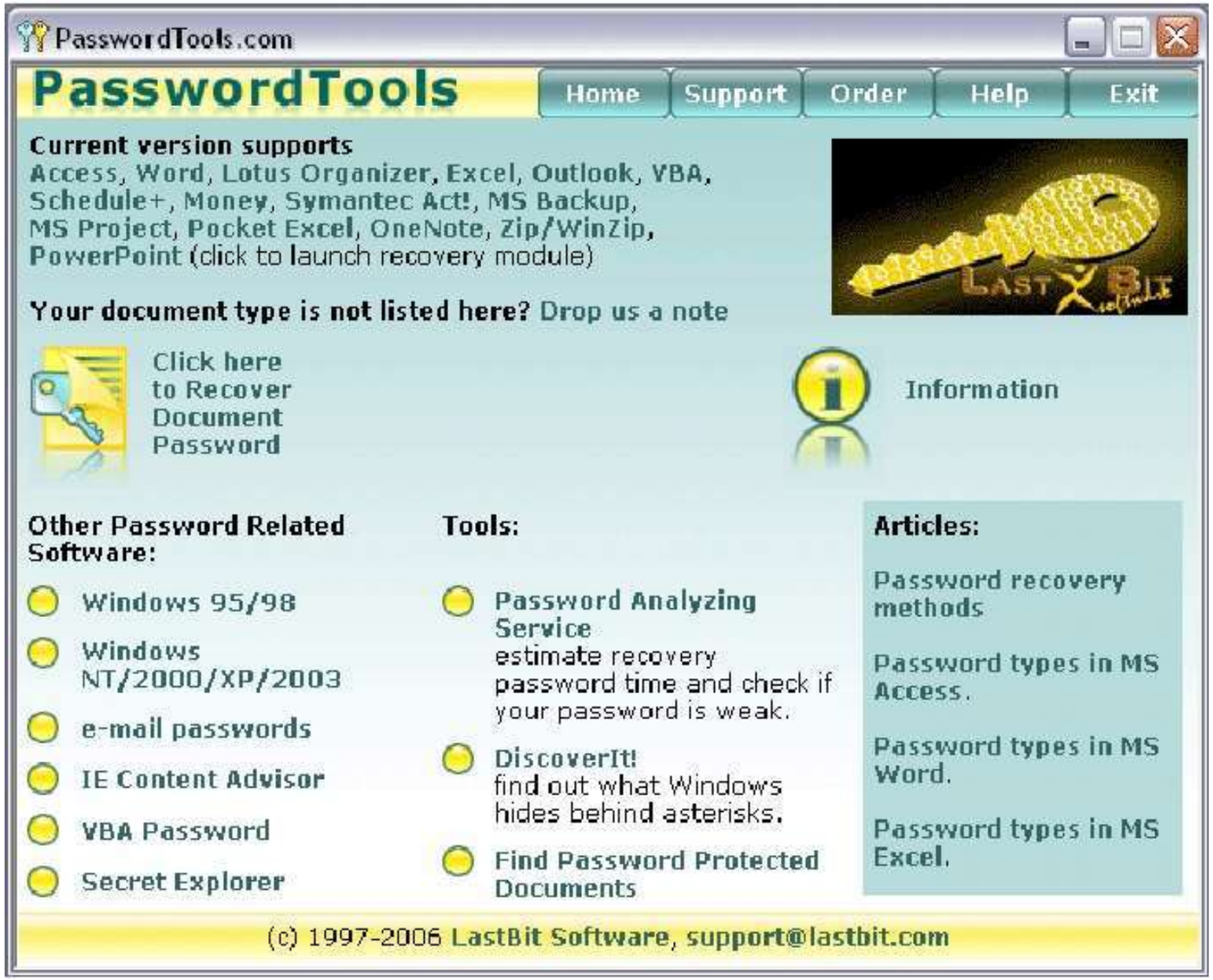
- Passware Kit (http://www.lostpassword.com/)
- ElcomSoft Password Recovery Bundle (http://www.elcomsoft.com/)
- LastBit Password Recovery (http://lastbit.com/)
- AccessData Password Recovery Toolkit (PRTK) (http://accessdata.com/)
- Multi Password Recovery Portable (http://passrecovery.com/)
- Protected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

Passware Password Recory Kit

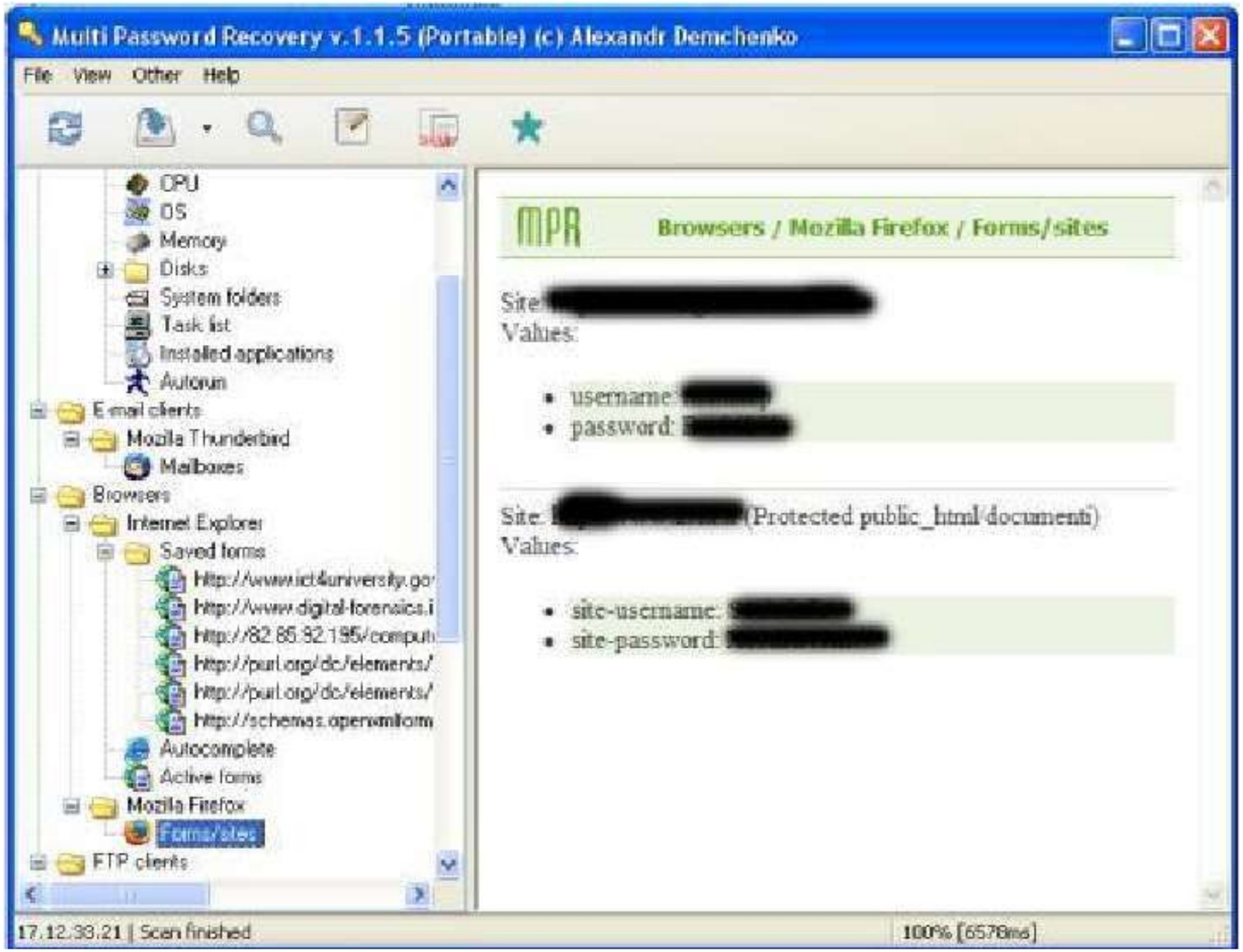
Elcomsoft Password Recovery Bundle



LastBit Passwor Recovery



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

Operating steps

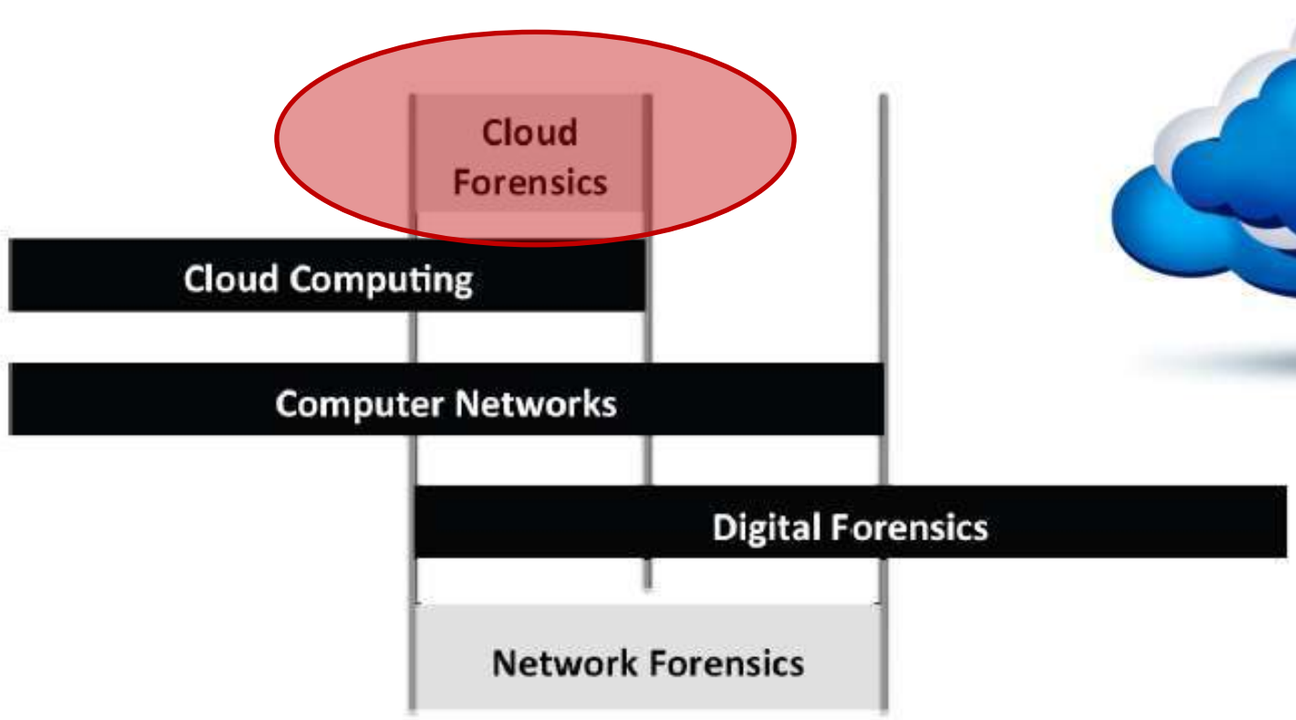
- Preparation and Identification
- Acquisition and Retention
- Analysis
- **Evaluation and presentation**

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

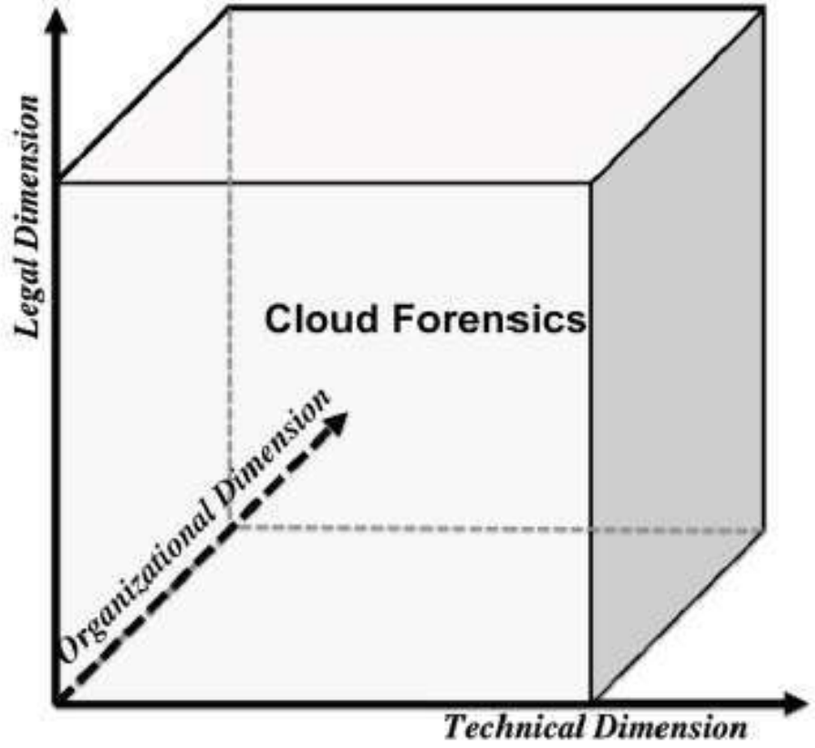
Cloud Forensics

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



3 Dimensions

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 <u>not</u> 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 <u>must</u> 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!!).

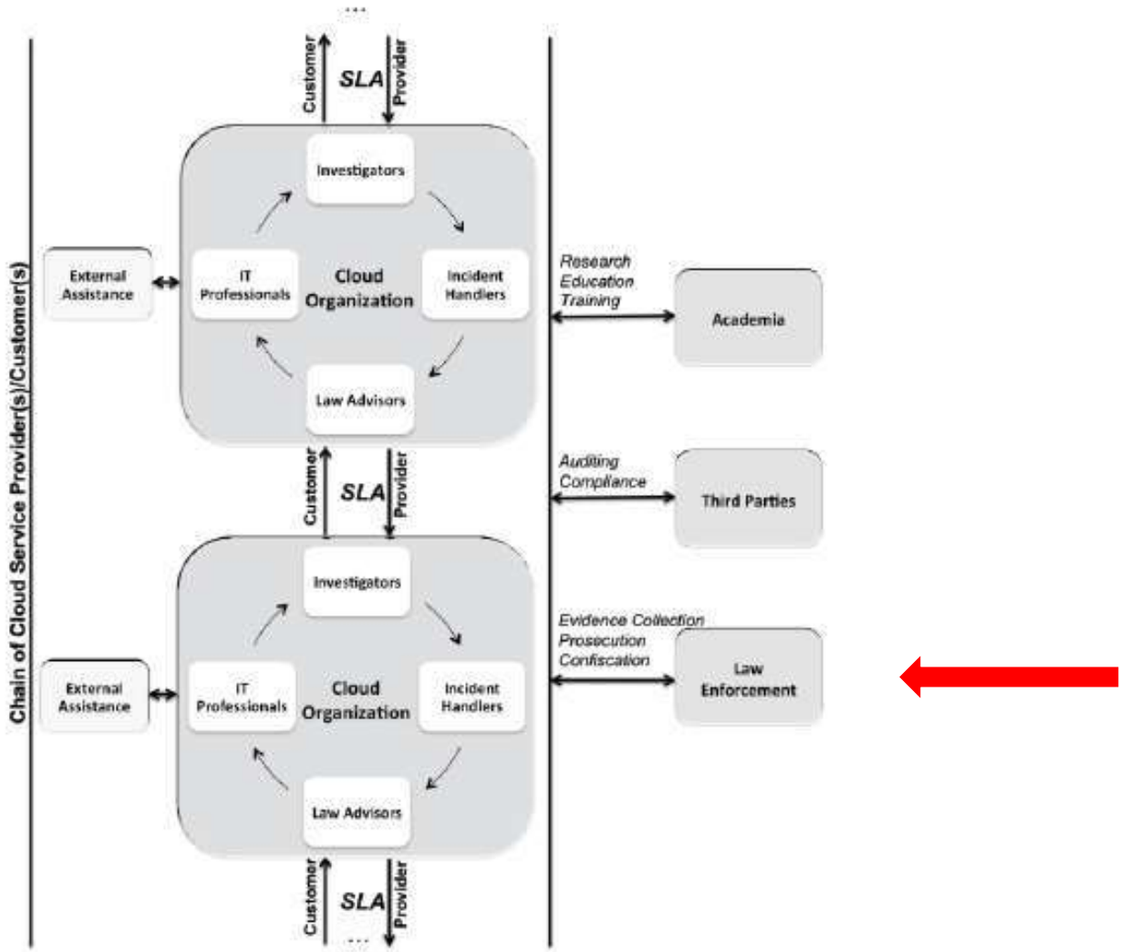
Tecnical/1

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.

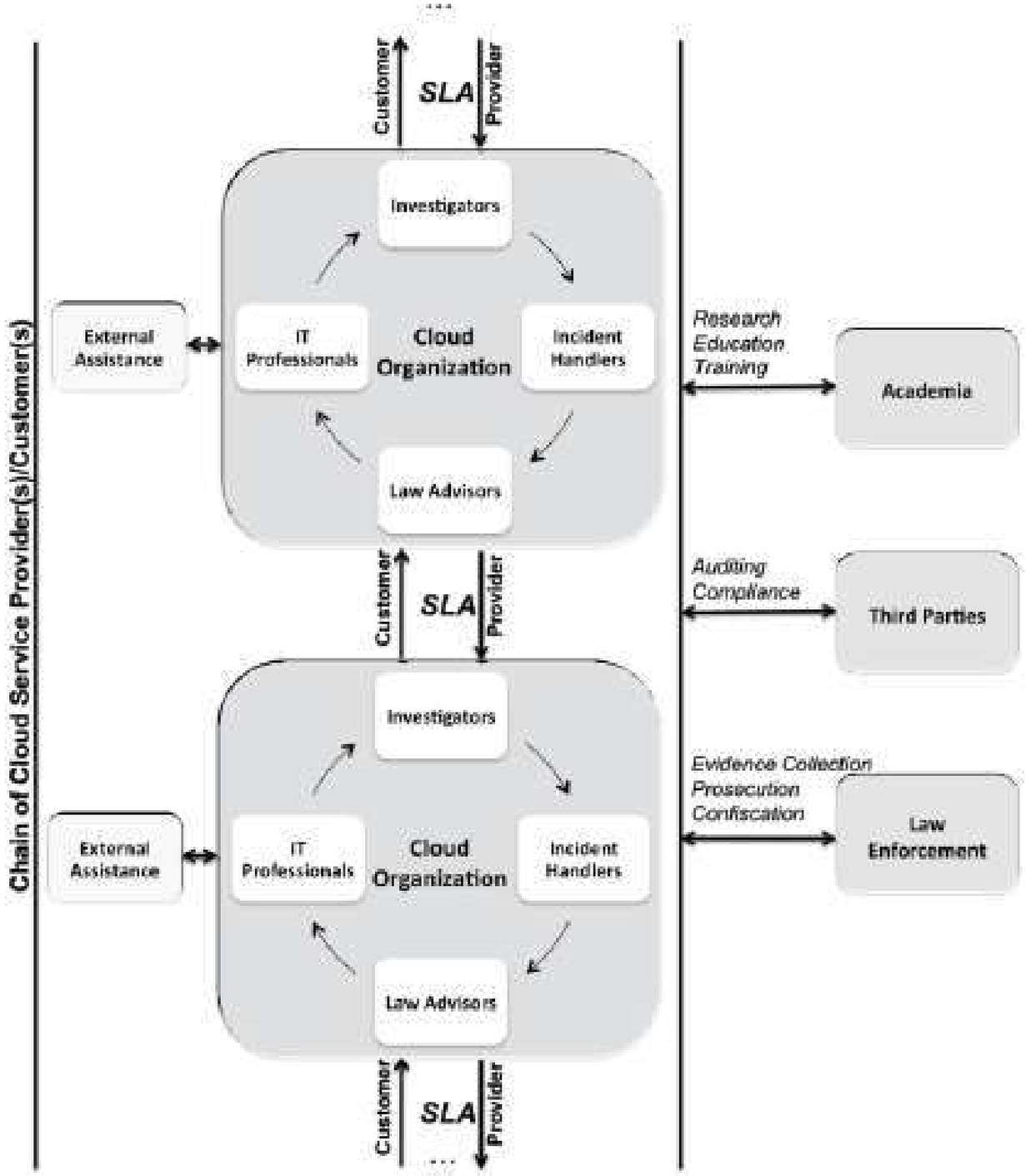
• **Proactive preparedness**: here we mean those tools that can be used both on client-side and service provider ones.

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!!!*.

<u>YOU CANNOT</u>.

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…..)

iCloud

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/S187705091401211 3/1-s2.0-S187705091401211 3-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

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 (proofing 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 expansive ☹

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 became 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 collagues ;)
    - 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

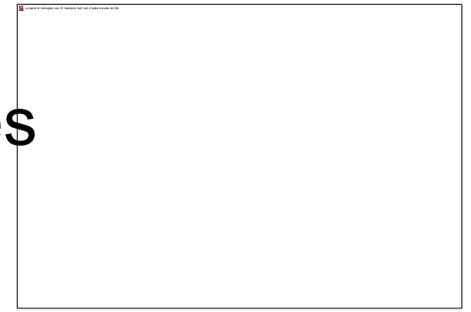
- **First goal** hit by DF:
  - Mixing those data from IM logs and e-mail headers, we were *able to track FDB’s source IP*!
- FDB *didn’t use* its home Internet connection tough.
  - Indeed, he did “all the job” from his work office.
- Police arrested him when at work, finding him *live* sharing child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

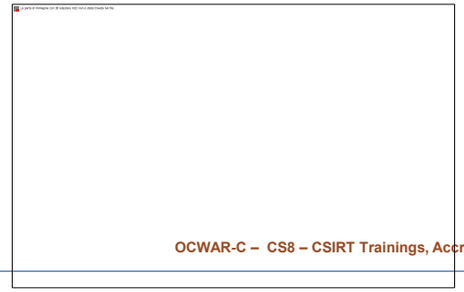
Case study: the “FDB” investigation /4

- 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

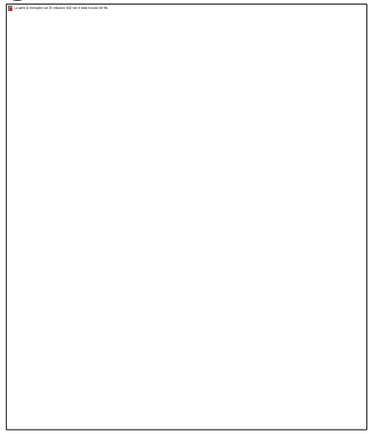
- We had a real, big problem, tough…
- We’ve found out multiple minors’ porno images where an adult male was having sex with different teenagers, in different revealing sex positions.
- Nevertheless, *the face of the male subject was hidden by black paint*.
- We had *strong suspect & feelings* that the 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 ad 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

OCWAR-C
12 Charles de Gaulle Street Asokoro,
Abuja - NIGERIA
contact@ocwarc.eu