



UNIVERSITÀ
DI PARMA

Workshop Digital Forensics

Eng. Selene Giupponi
Head of Digital Forensics Unit

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

Courses and Certifications in D.F.

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

Agenda

- Key concepts of Digital Forensics.
- The importance of Digital Forensics today.
- The different phases of D.F.:
 - Identification
 - Preservation
 - Extraction
 - Analysis
 - Report
 - Chain of Custody
- Live Analysis vs. Dead Analysis.
- Other type of D.F.: Mobile & Cloud Forensics.
- Instruments to be used for each phase.
- Case studies.
- Practice on your own computer and on the instruments carried by the trainer.
- Conclusions

Disclaimer

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

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

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



the Origins

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



DF –introduction/1

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

DF –introduction/2

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

The Washington Post

Crime

Air Force major charged in child pornography case

DF –introduction/3

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

Use of DF Today

- ＊ Criminal Investigations

- ＊ Child Pornography, e-Crimes, identify thieves;

- ＊ Civil litigation

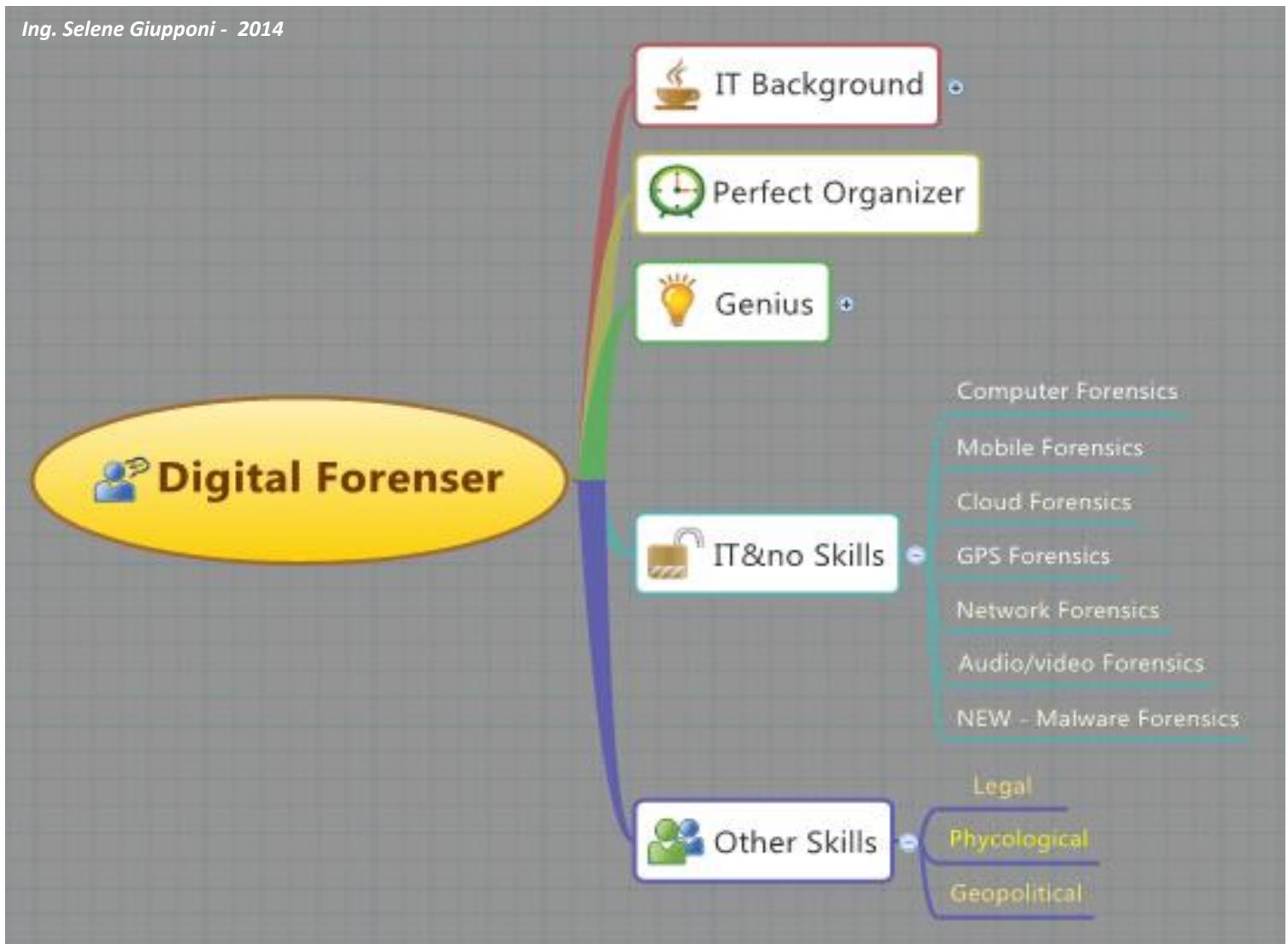
- ＊ eDiscovery

- ＊ Intelligence

- ＊ Terrorist Attacks

DF – Introduction/4

Ing. Selene Giupponi - 2014



Digital Forensics Introduction

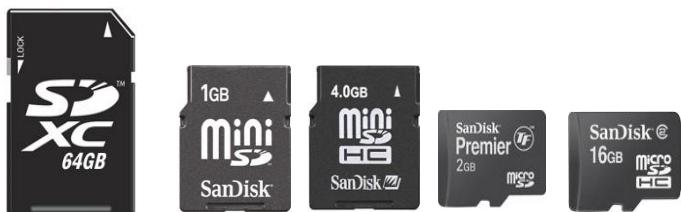
- * A digital evidence can be defined as any information which has probative value that is stored or transmitted in digital form

A digital evidence can then be extracted by:

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

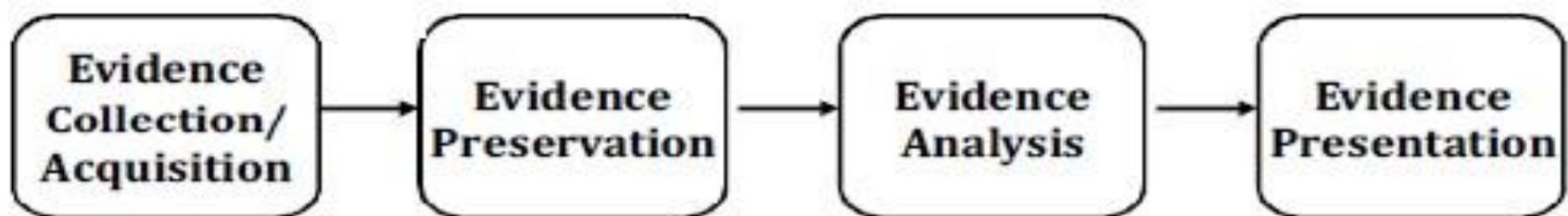
Digital Forensics

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



Digital Forensics

Computer Forensics phases:



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

CSI - Investigations



* Goal: To explain the current state of Digital Artifact

Digital Forensics Introduction

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

Digital Evidences

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

Dead Analysis vs Live Analysis

Digital Forensics

Dead Analysis
Live Analysis



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

That's why:

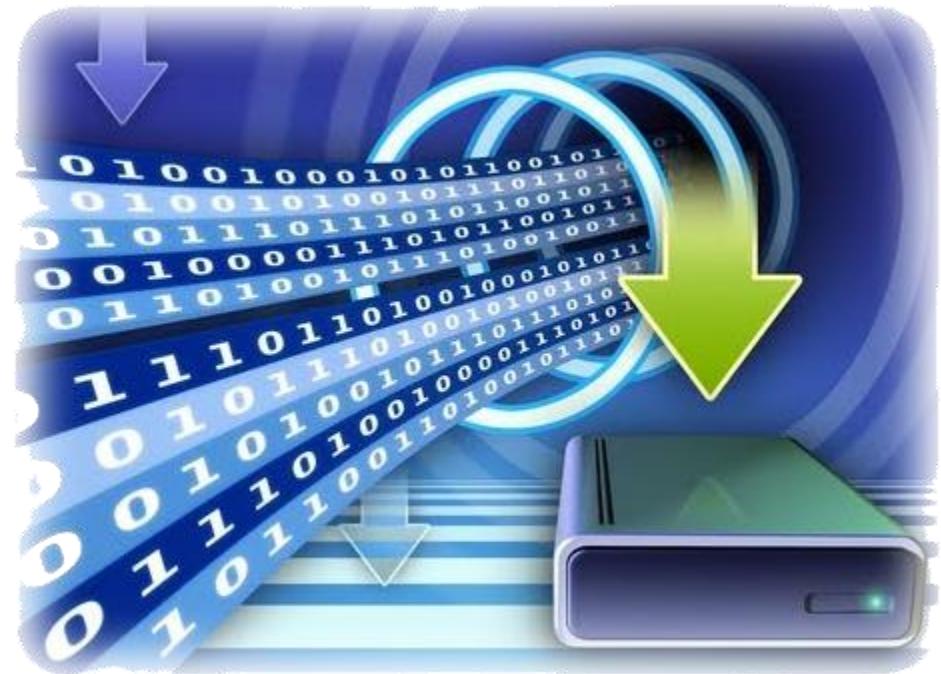
We must think about new tools, instruments and methodologies that will be applied to the Evidence Collection & Acquisition phases.

Digital Data

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

- sequestered
- copied
- Intercepted

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



Operating steps

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



Identification

- * The identification step is done at the analysis of crime scenes
The identification process must follow the so-called "best practices"
The digital containers of interest during the investigation of a crime scene are (non-exhaustive list ...):
 - Personal computers, notebooks and servers
 - Hard disk not inserted in the computer (dismantled or external)
 - Solid state drives
 - Network Attached Storage (NAS)
 - floppy disks
 - Backup tapes
 - Cartridges ZIP / JAZ
 - CD / DVD / BluRay
 - Memory card
 - USB Drives
 - MP3 Player, Camcorders, Digital Cameras
 - Network devices (Router, Switch, Firewall, IDS / IPS, Syslog Server)
 - Mobile devices (mobile phones, SIM, SmartPhone, Tablet, SatNav)



Hard Disk



UNIVERSITÀ
DI PARMA

Hard Disk

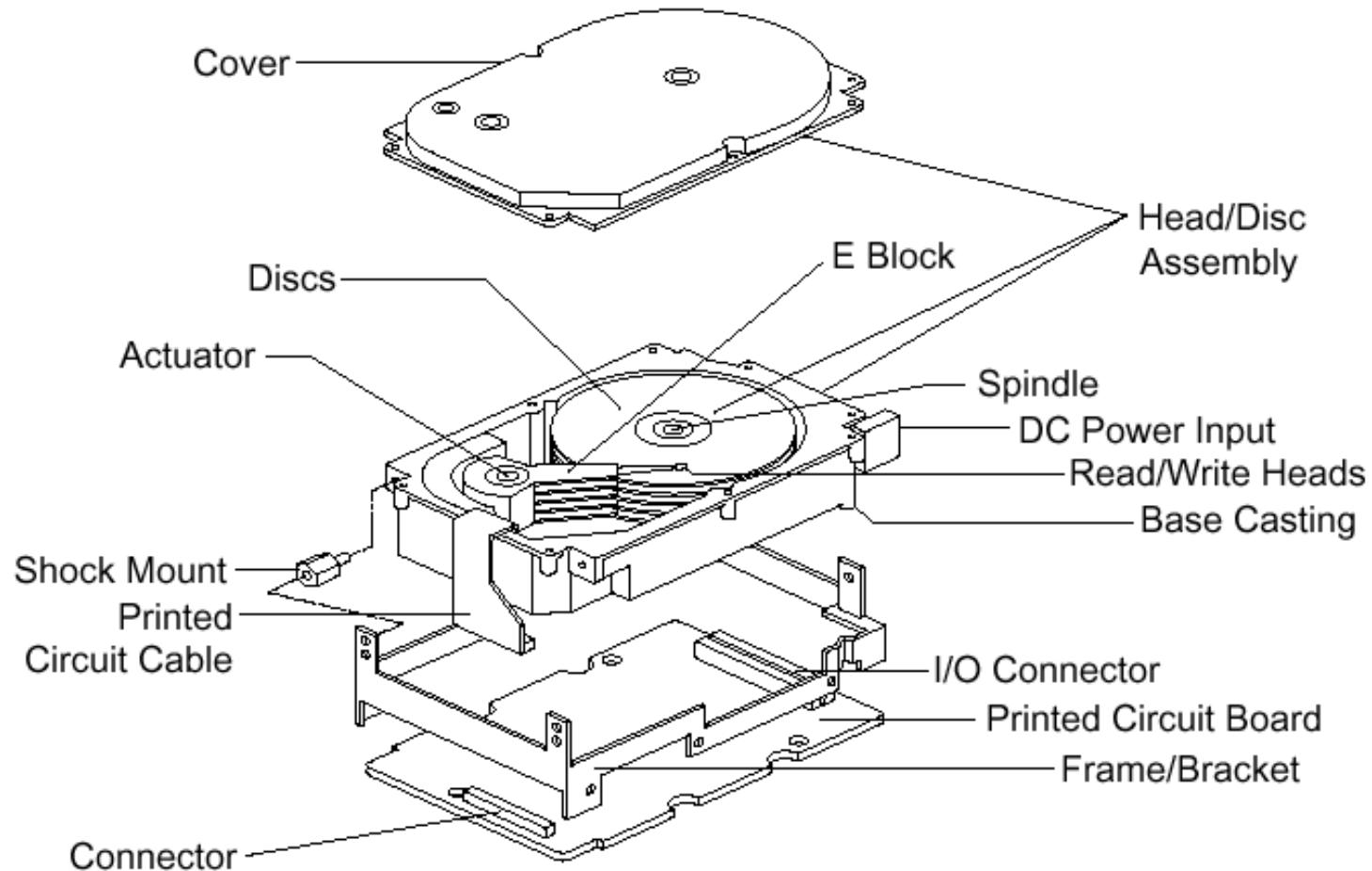
- ＊ A hard disk is an example of non-volatile storage device
The data is recorded magnetically on the hard disk
- ＊ The main components of a hard drive are:
 - ＊ Cylinders (cylinders)
 - ＊ Heads (heads)
 - ＊ Dishes (platters)
- ＊ Each plate is divided into tracks
Each track is divided into sectors (typically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

Hard Disk

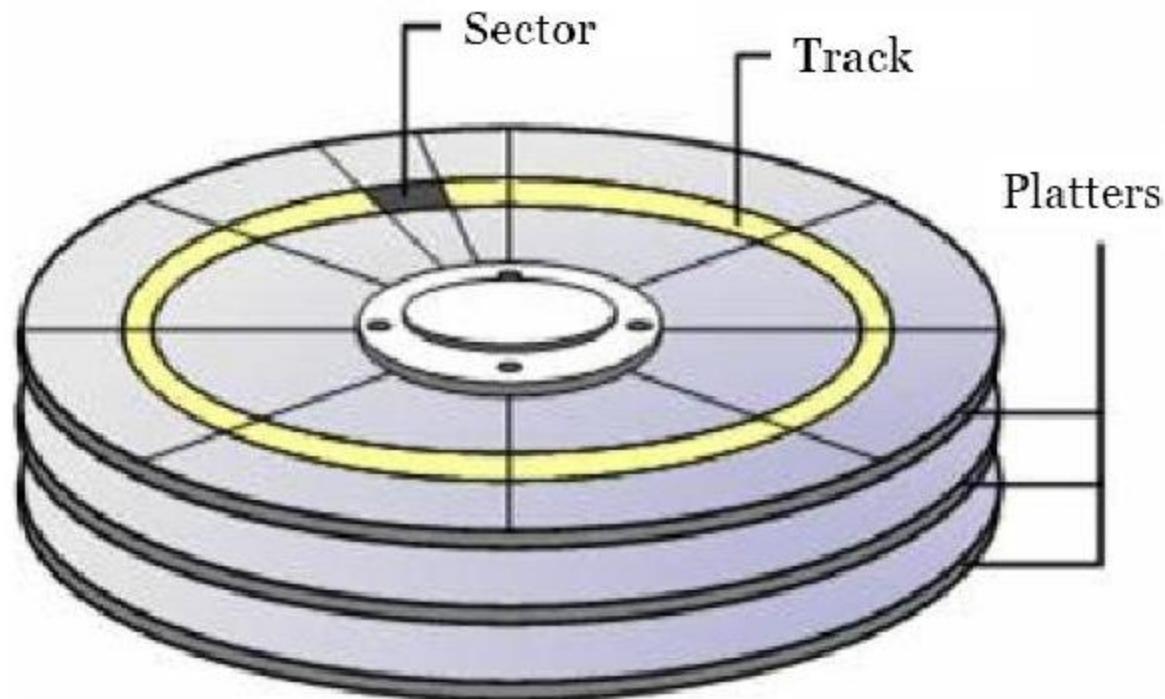
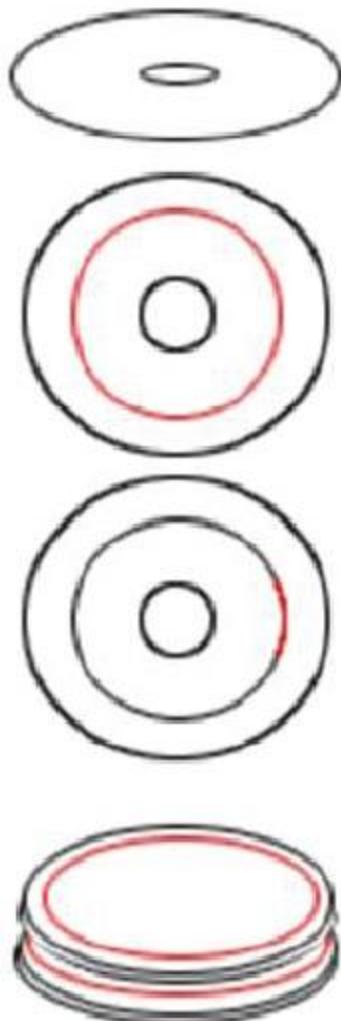
- ＊ When organizing data logic sectors are aggregated into clusters
- ＊ A hard disk is composed of a stack of plates, with read / write positioned above and below each plate
- ＊ During the rotation of the plates, the head moves from inside to outside (and vice versa) to read and write data



Hard Disk



Hard Disk



Hard Disk

- * There are several interfaces to connect a hard disk with a computer
 - * **SCSI (Small Computer System Interface)**
 - * **IDE/EIDE (Integrated Drive Electronics/Enhanced IDE)**
 - * **Parallel ATA (Advanced Technology Attachment)**
 - * **Serial ATA (Advanced Technology Attachment)**
 - * **Fibre Channel**

Hard Disk



DB25m (Mac-SCSI)
Aprox: 35mm



C50m (SCSI-1)
Aprox: 65mm



IDC50m (SCSI-1)
Aprox: 79mm



IDC50f (SCSI-1)
Aprox: 67mm



HD50m (SCSI-2)
Aprox: 36mm



HD68m (SCSI-3)
Aprox: 47mm



HD68f (SCSI-3)
Aprox: 46mm



VHDC68m (SCSI-4)
Aprox: 32mm



Partitioning (MBR)

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

Structure of a Master Boot Record

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



File System

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

Cluster e Slack Space

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



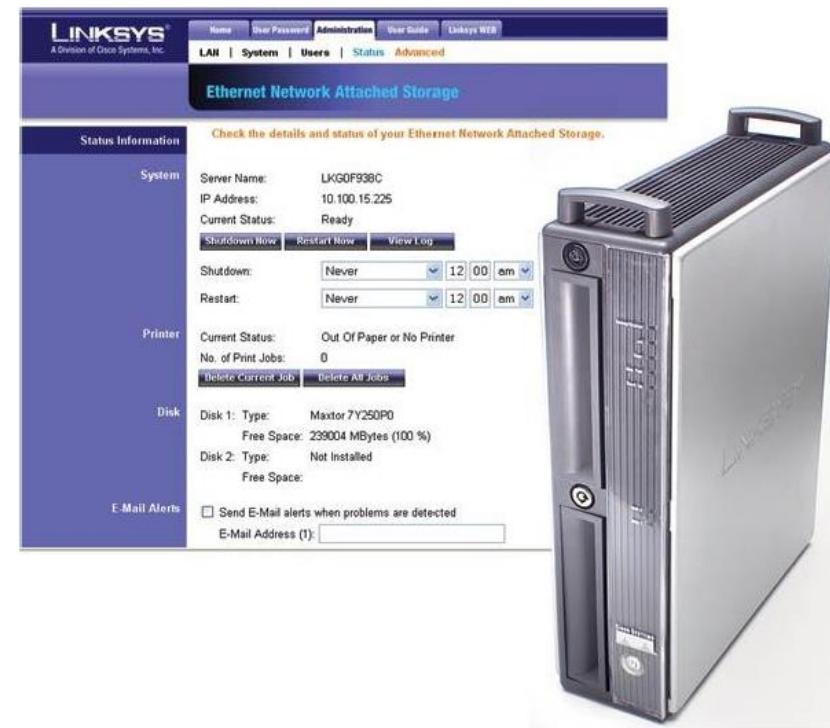
SSD

- * The solid state disks (SSD) are permanent storage devices that use solid state memory
The advantages of a solid state disk with respect to a magnetic disk are:
 - * Reduced use of electric current
 - * Data access in reading and writing faster
 - * increased reliability

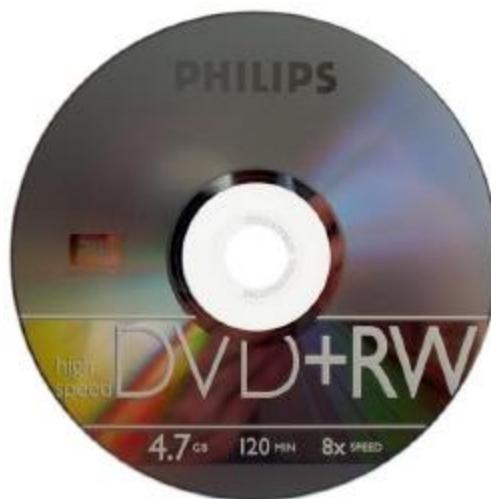
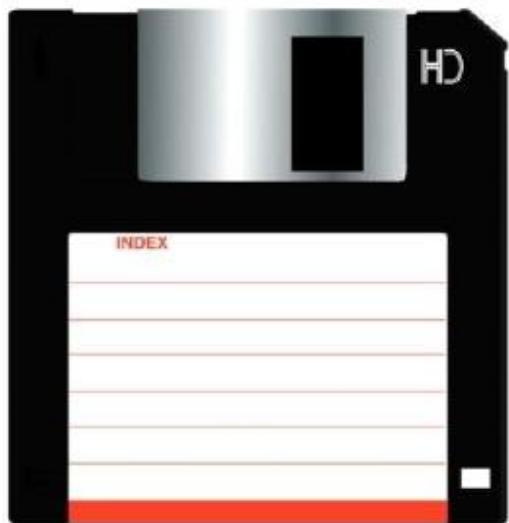


Network Attached Storage (NAS)

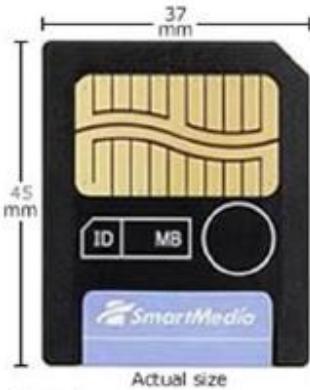
- ＊ A Network Attached Storage (NAS) is a device directly connected to a network that provides centralized access to data to different clients
- It consists in a number of hard disks and from a hardware device, said NAS Head, which acts as an interface between the NAS and the clients of the network
- Generally supports RAID configurations



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

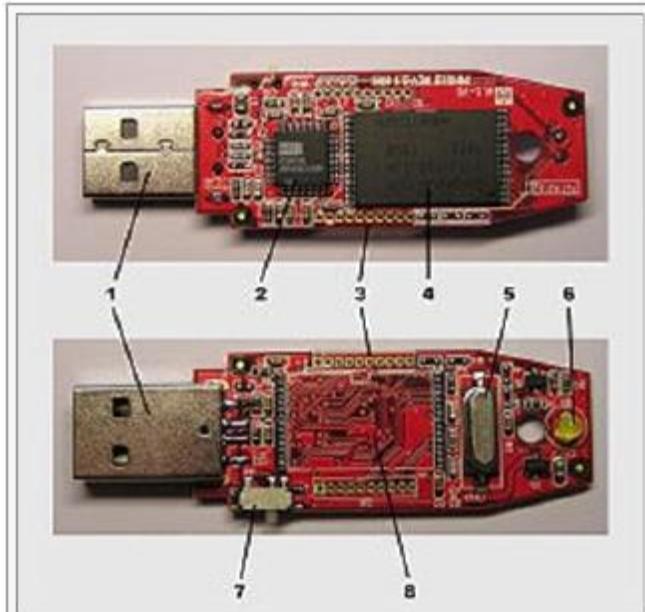


Memory Card



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



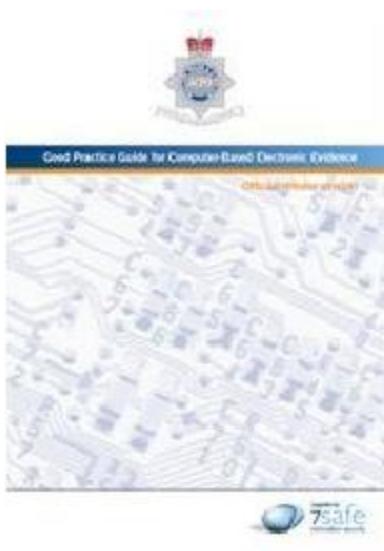
UNIVERSITÀ
DI PARMA

MP3, Video cameras, Cameras, Tablet



Best Practices Internazionali

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



Best Practices for the computer turned off

- ＊ Make it safe the scene and take control of the area that contains the device

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

Best Practices for the computer turned off

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



Best Practices for the computer turned off

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

Best Practices for computer turned on

- ＊ Make it safe the scene and take control of the area that contains the device
- ＊ Persons away present from all computers and power devices
Taking pictures or make a video recording of crime scenes and of all relevant components. If there is not a camera, draw the scene and tagging ports and cables so that the system can be reconstructed later
- ＊ Assess whether to ask the user information on the setup of the system, including password
Record the information on the monitor, carrying photographs and transcribing the text visible
- ＊ ***Do not touch the keyboard or click the mouse.***

Best Practices for computer turned on

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



Chain of Custody

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

Chain of Custody



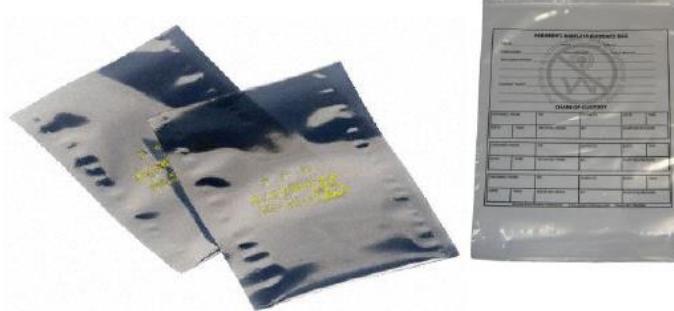
Transportation and preservation of artifacts

* 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



Preserving the
Original!



Forensics Copy

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

Duplication can be done via software or hardware

System hour and boot sequence

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

Hardware Acquisition : duplicators

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



Software Acquisition

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

Computer Forensics Tool Catalog

Home

Tool Search

Forensic Tool Taxonomy

Vendors

Contacts

Forensic Tool Functionalities

Cloud Services

Deleted File Recovery

Disk Imaging

Email Parsing

File Carving

Forensics Boot Environment

Forensic Tool Suite (Mac Investigations)

Forensic Tool Suite (Windows Investigations)

GPS Forensics

Hardware Write Block

Hash Analysis

Image Analysis (Graphics Files)

Infotainment & Vehicle Forensics

Instant Messenger

Media Sanitization/Drive Re-use

Home > Tool Search

Search for forensic tools by functionality

Search Results for Disk Imaging: 16 tools found

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

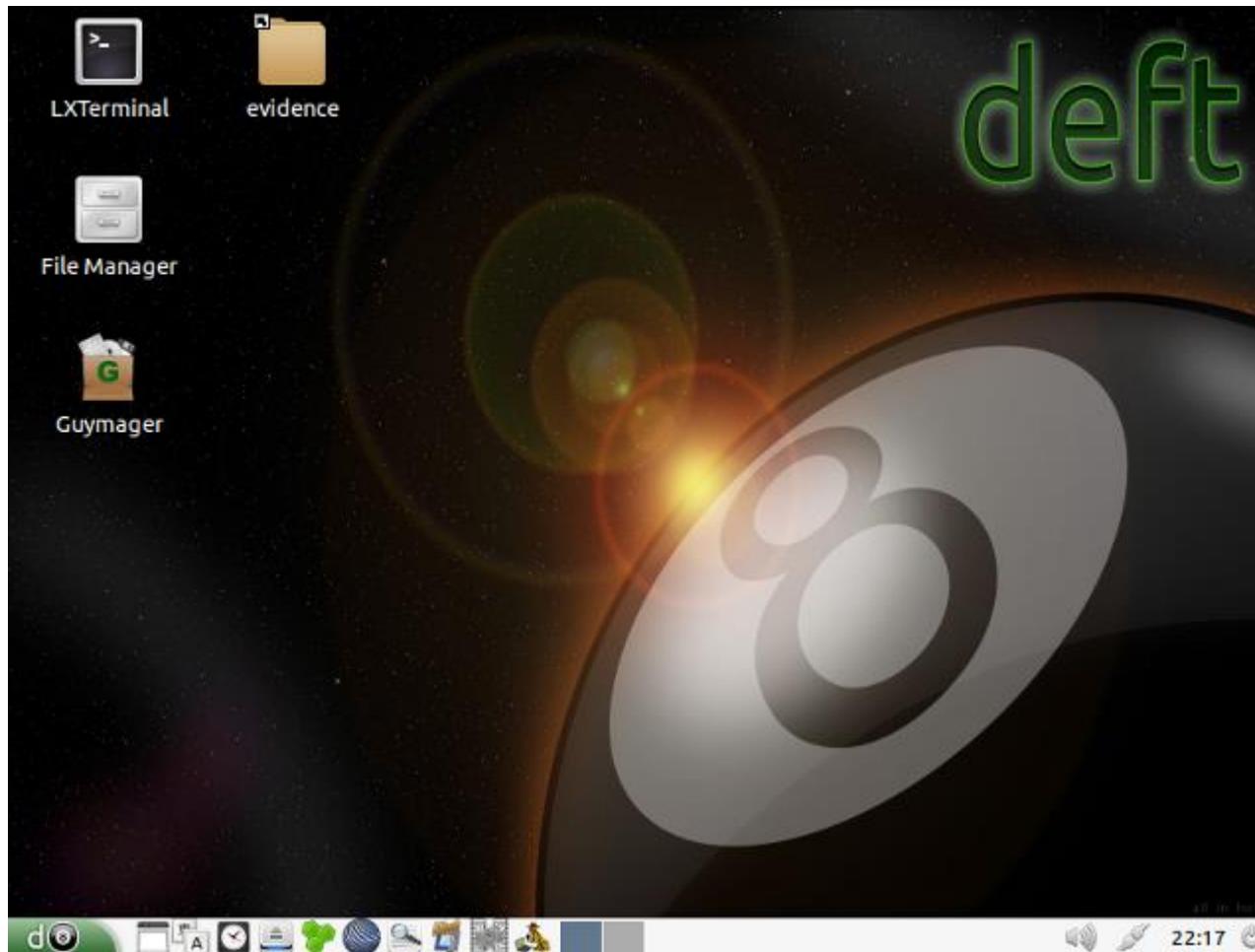
Result 1 of 16	CFID : Covert Forensic Imaging Device								
Version:	2.0								
Tool Release Date:	July 2012								
Available Test Reports:	Under evaluation								
Vendor:	Teel Technologies								
Vendor Website:	http://www.scecanada.com								
URL to Tool Description:	http://www.scecanada.com/cfid								
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

Software Acquisition

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

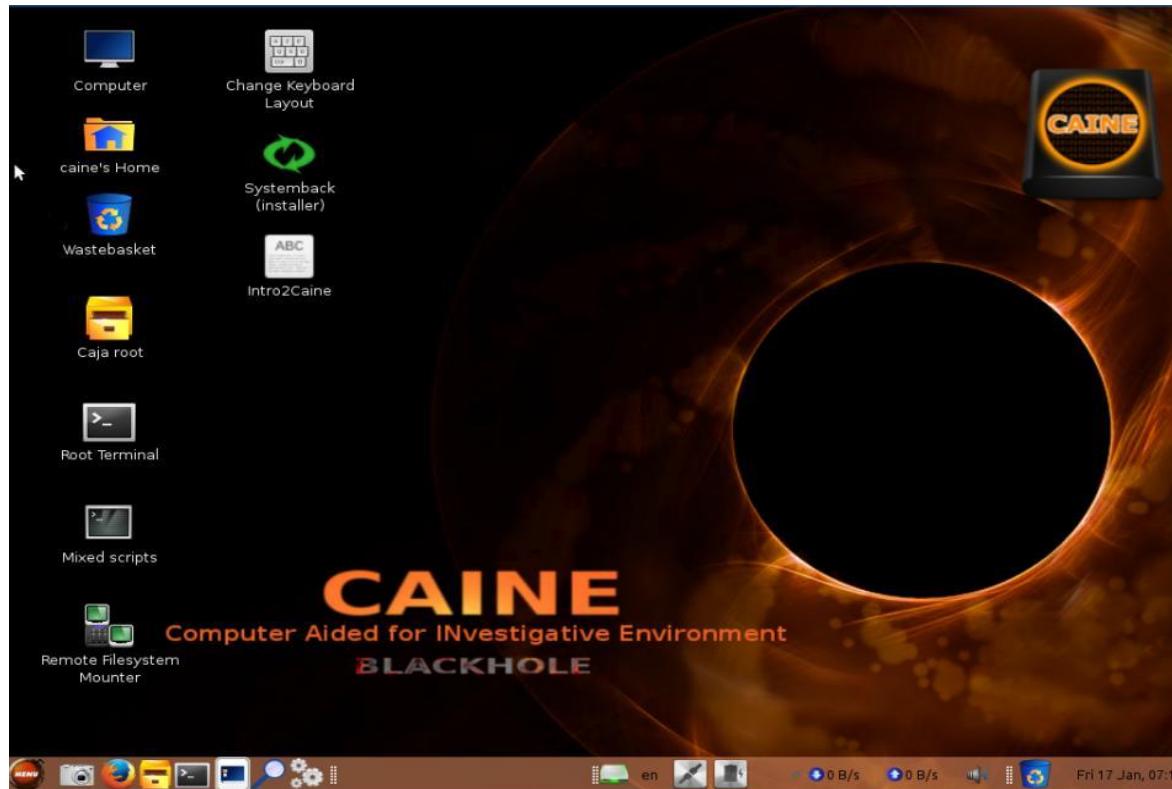
DEFT

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



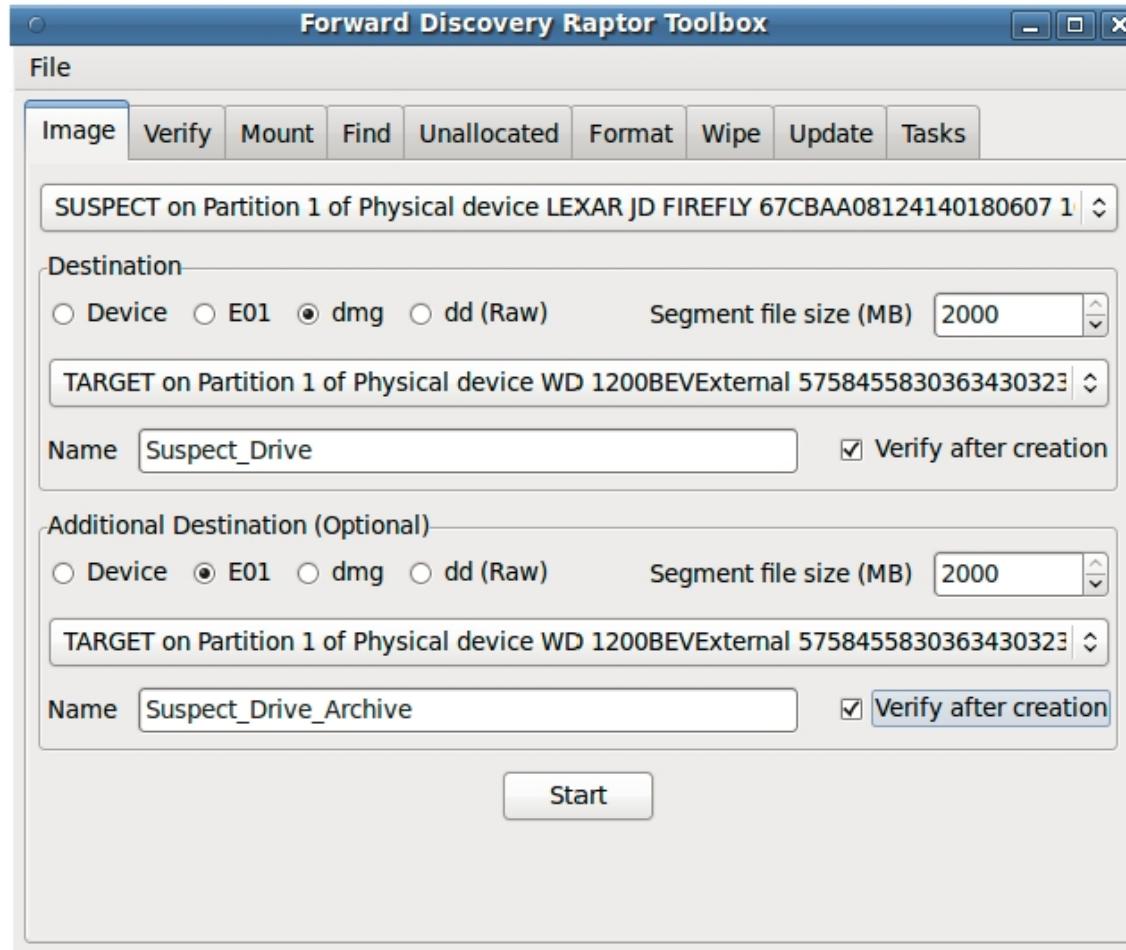
CAINE

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



RAPTOR

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



Paladin

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



UNIVERSITÀ
DI PARMA

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

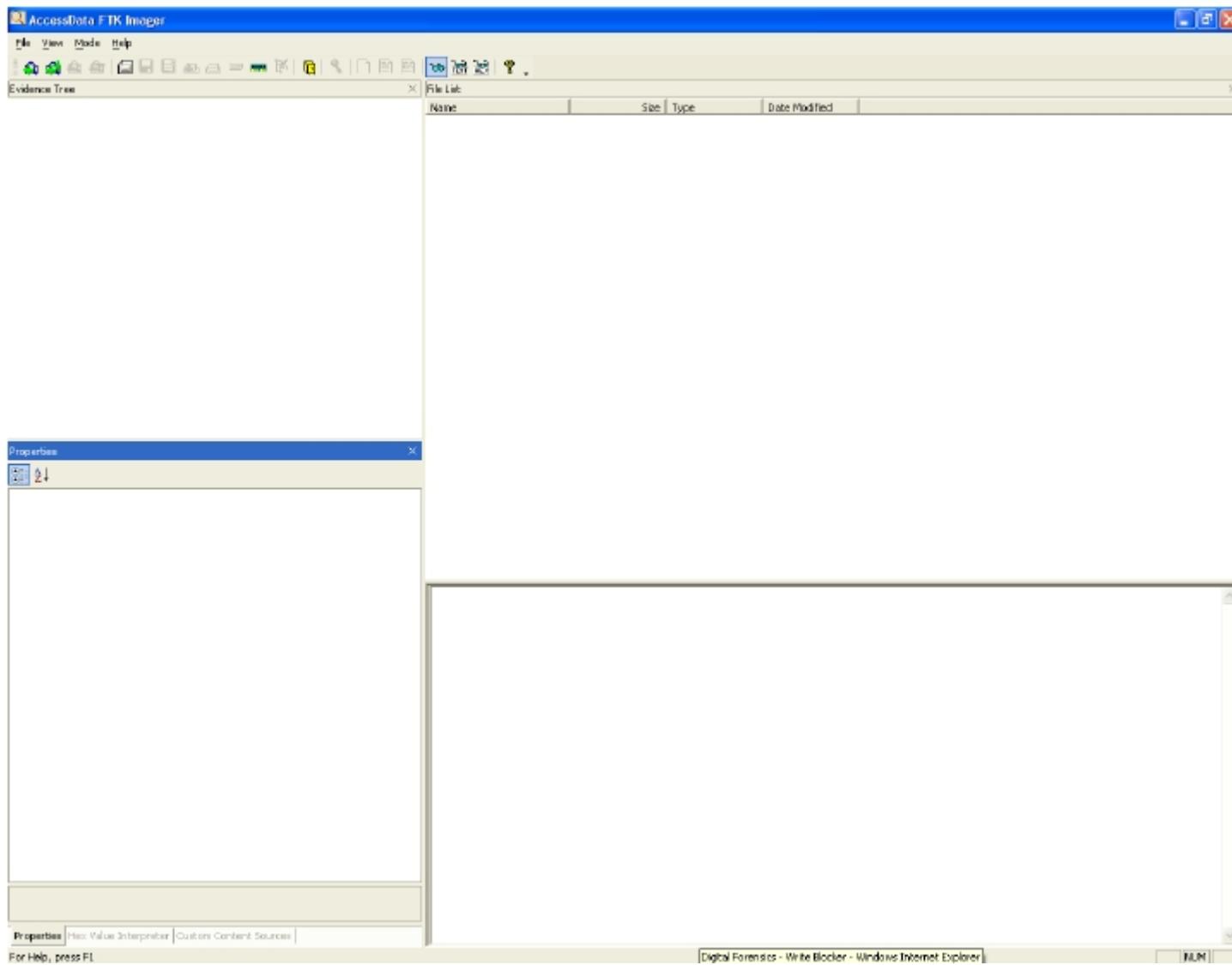
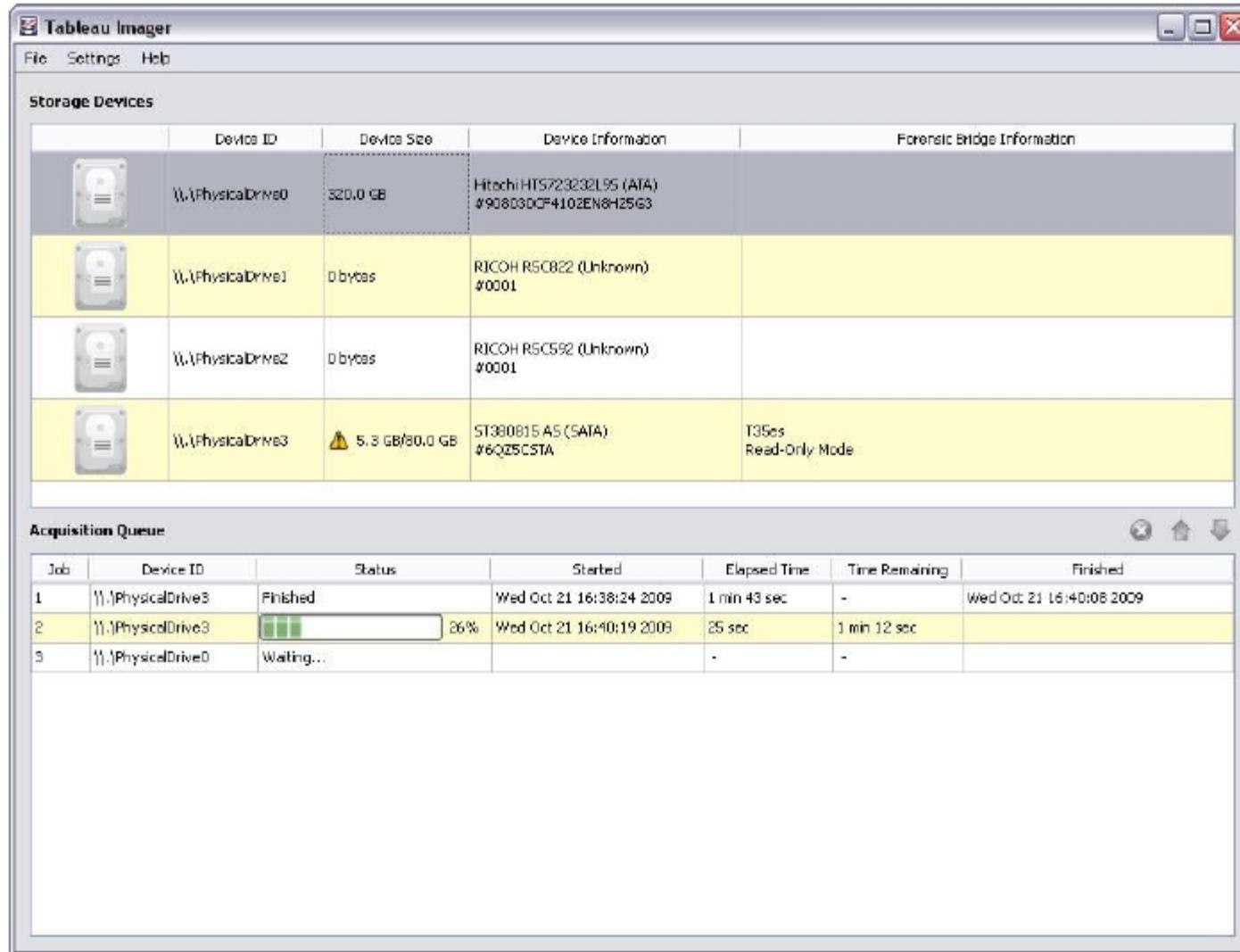


Tableau Imager



Write Blocker Hardware

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



Hardware vendors

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

Write Blocker Software

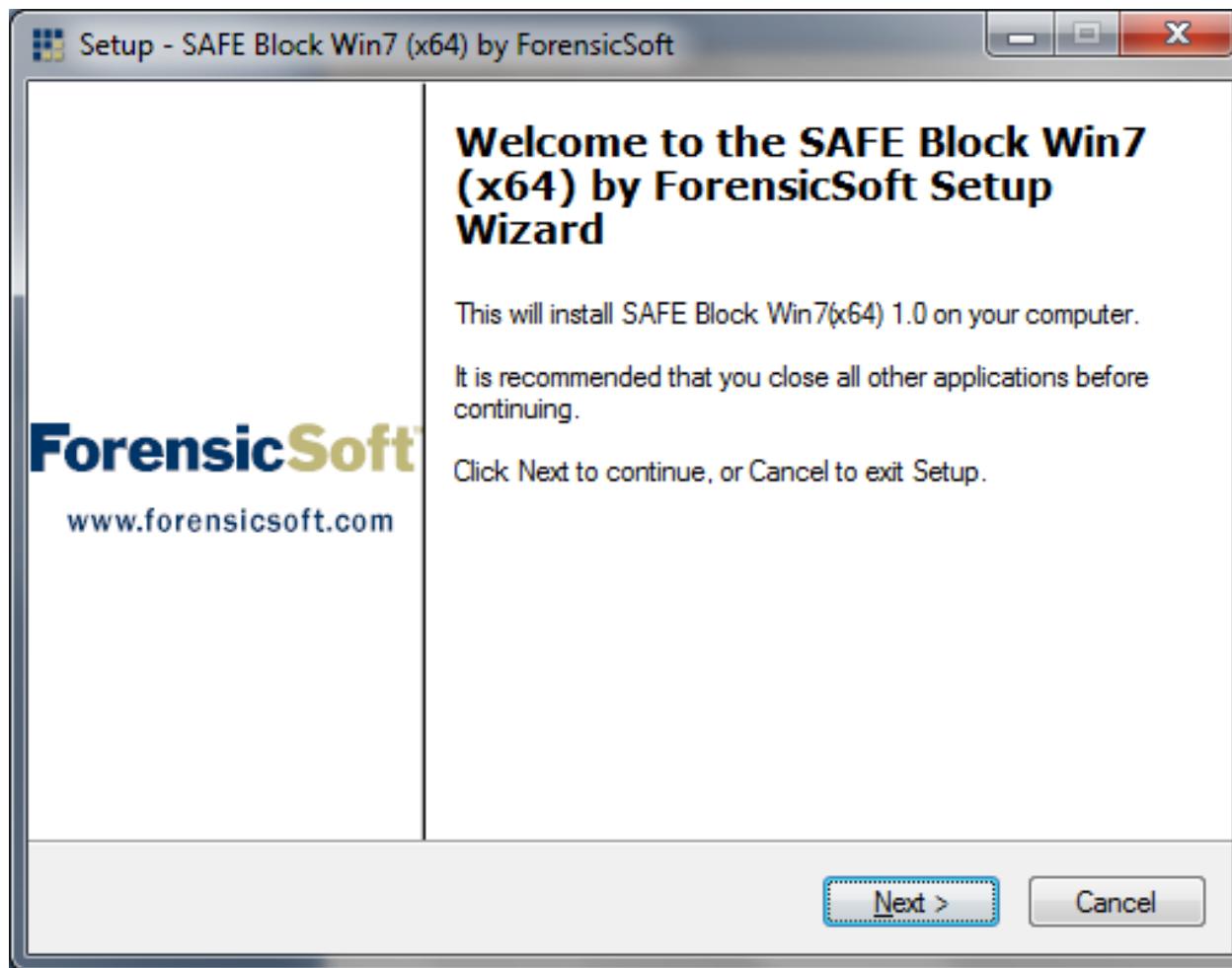
- * The write block at software level it may get used on the operation of mounting the hard disk from the operating system.
- * Depending on the operating system used on the acquisition forensics machine, you can take proper precautions to prevent the bidirectional flow of communication and allow access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

Write Blocker Software

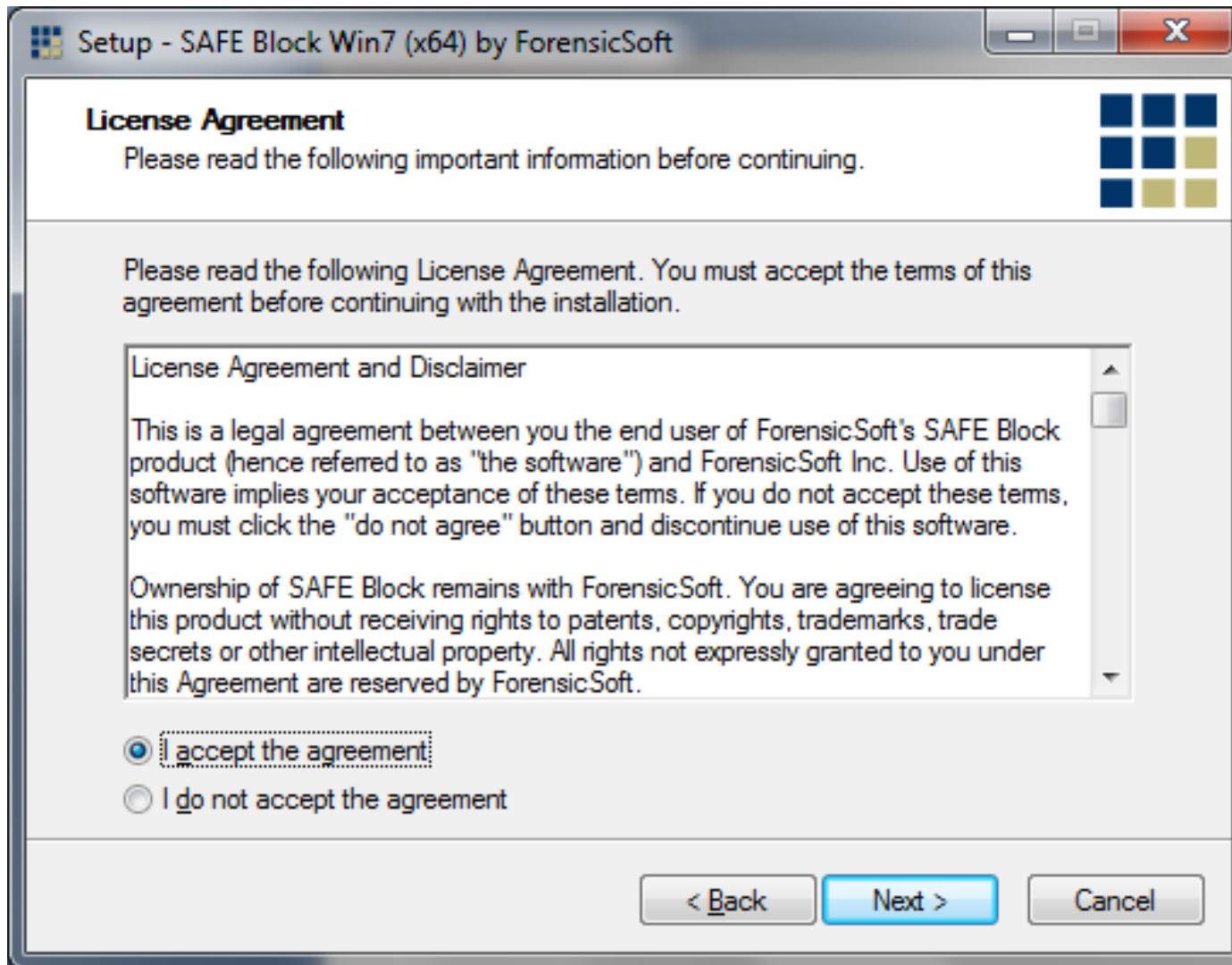


UNIVERSITÀ
DI PARMA

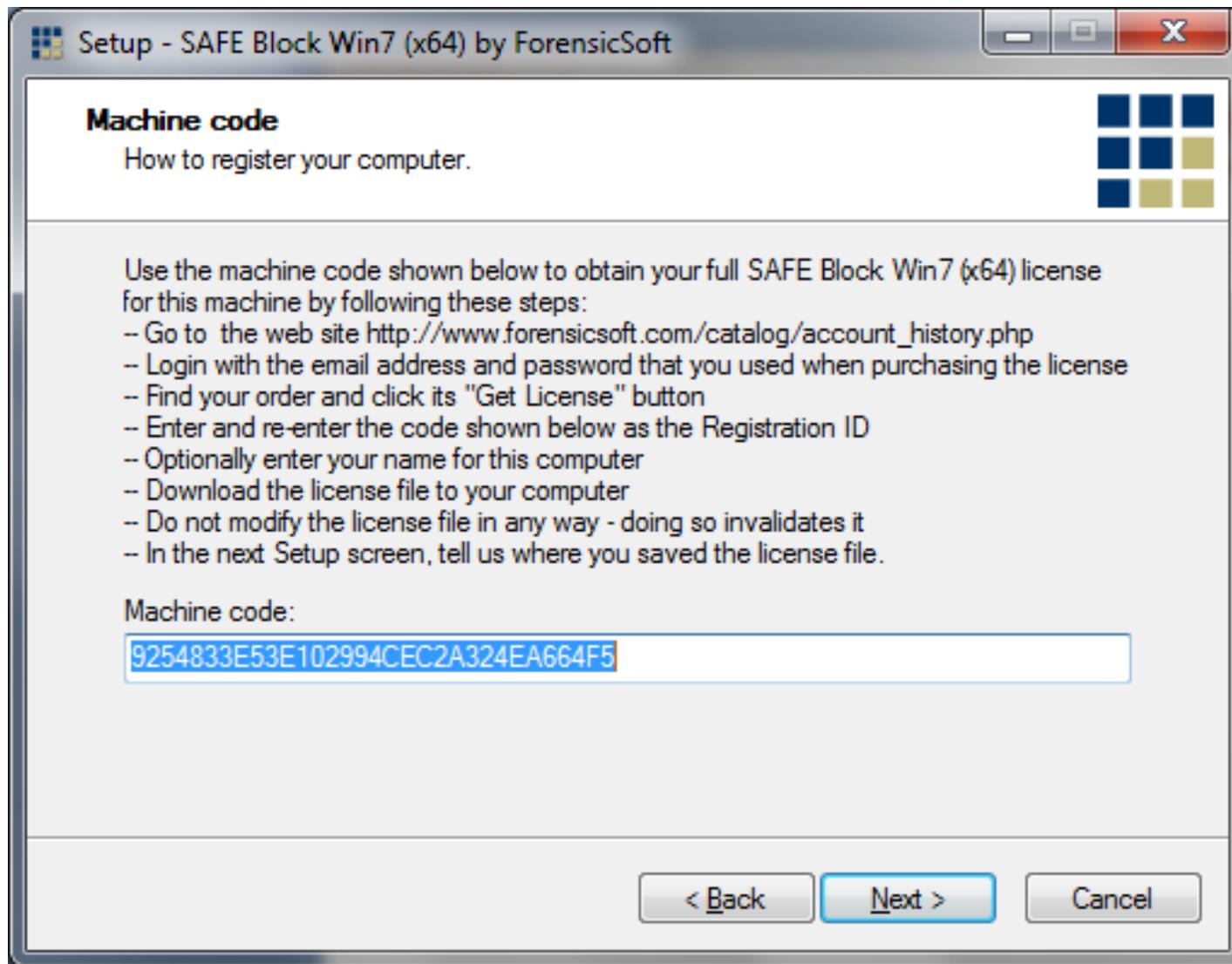
Write Blocker Software



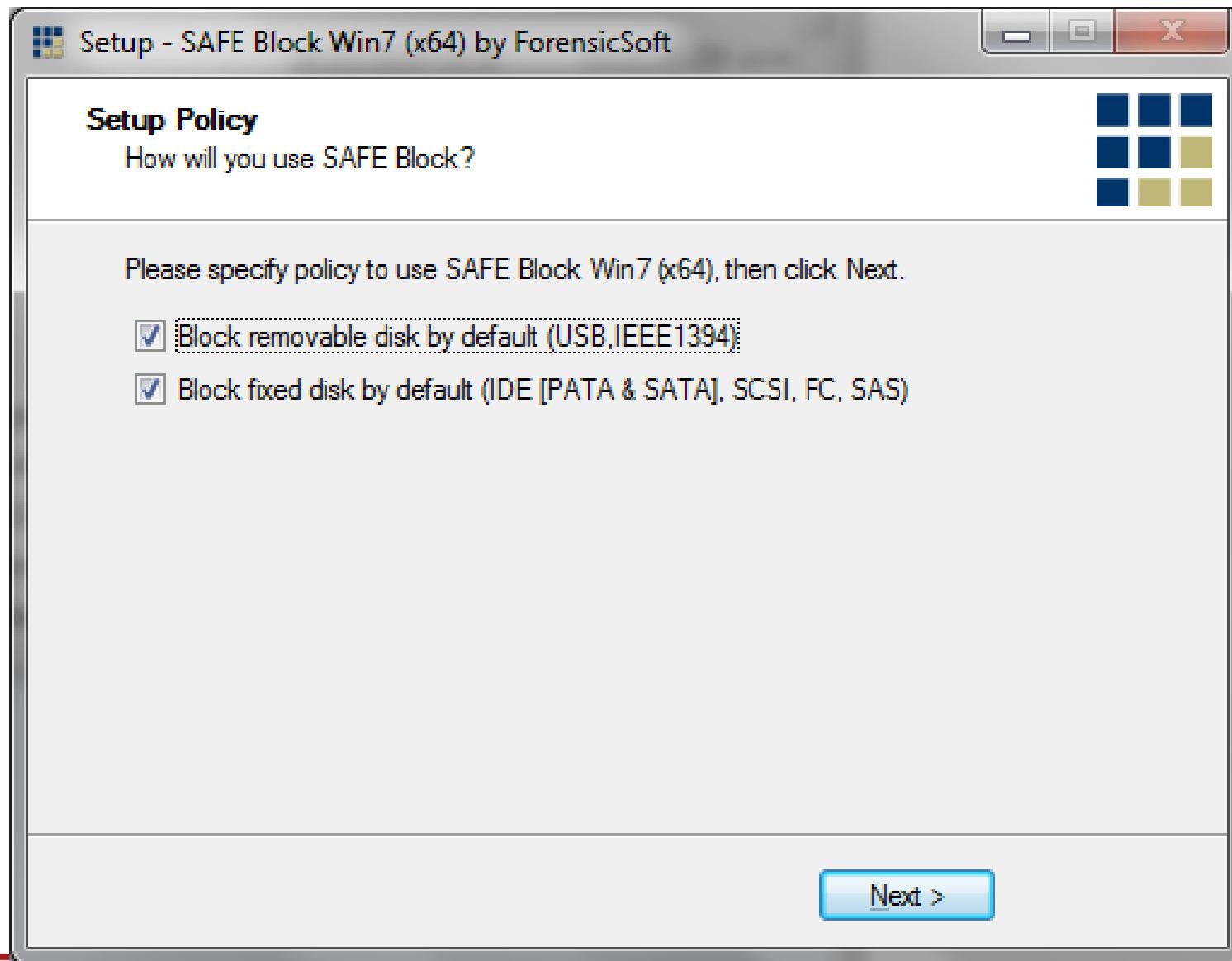
Write Blocker Software



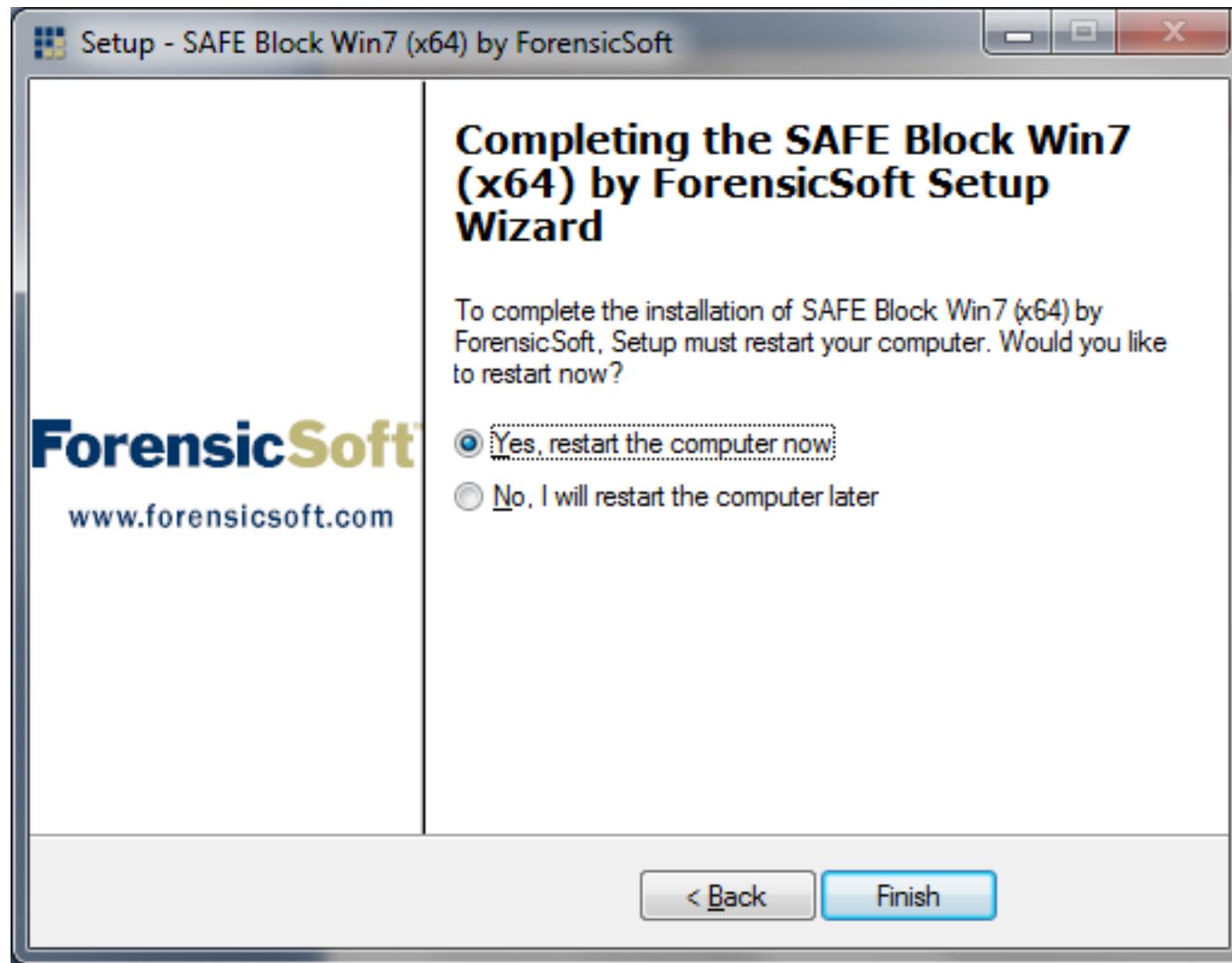
Write Blocker Software



Write Blocker Software



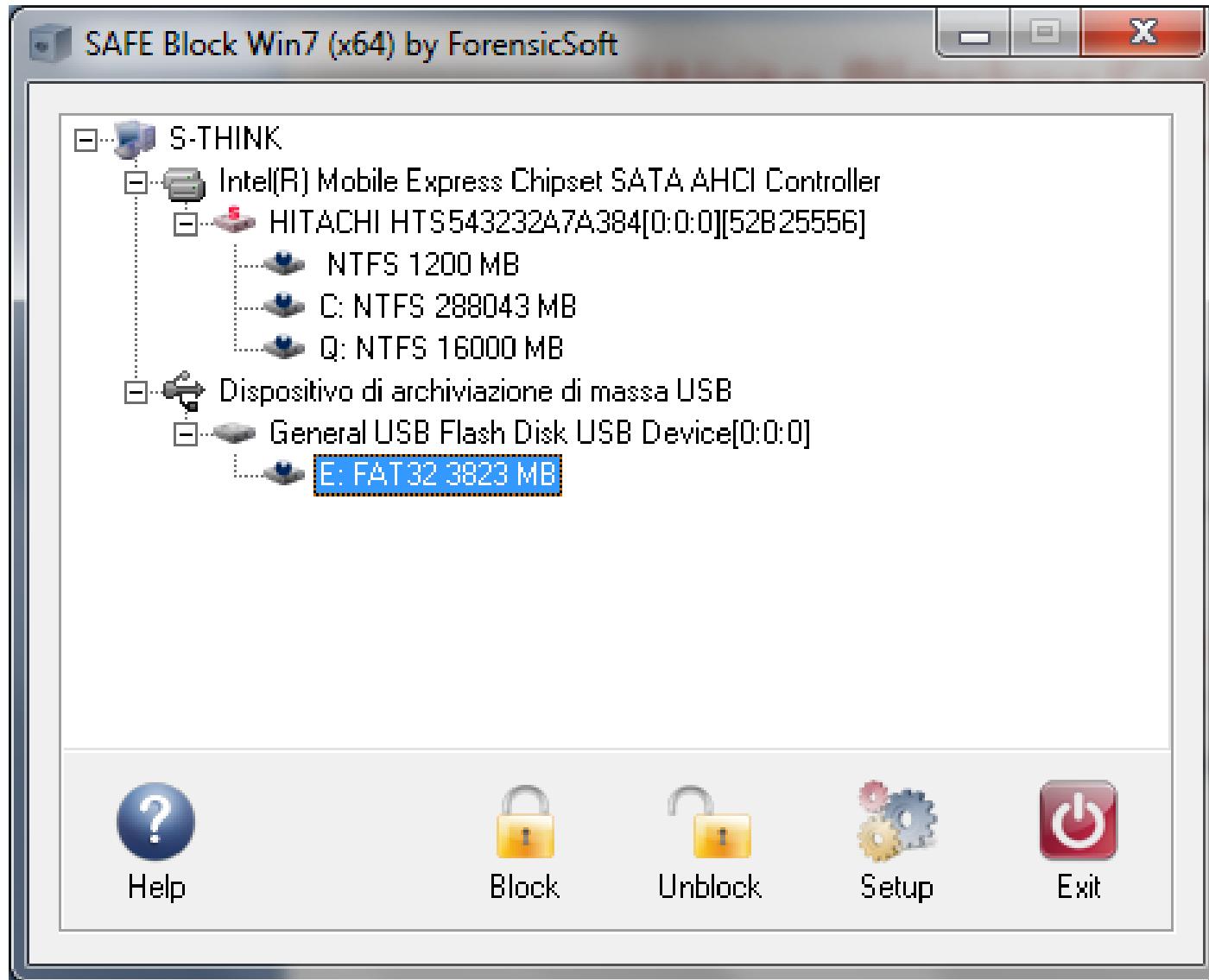
Write Blocker Software



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

Hash Function

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



Hash Function

► Cryptographic hash functions commonly used in Digital Forensic

- MD5

- Produces a 128-bit (16-byte) hash value
- First published in 1992

- SHA-1

- Produces a 160-bit message digest
- First published in 1995

- SHA-2

- A set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512)
- First published in 2001

Funzioni hash

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

Acquisition with Tableau Disk Monitor

Tableau Disk Monitor

File Actions Help

Disk ID	Disk Size	Disk Information	Forensic Bridge Information
0	149 GB	SAMSUNG HM160HI (ATA) Serial #: 31535757444a53303731363330	
1	698 GB	WD My Passport 070A (USB) Serial #: (empty)	
2	28 GB	QUANTUM FIREBALLIc20.30 (IDE) Serial #: 353104964304	Tableau T35es Read-Only Mode

Tableau, LLC

Fare clic per inserire le note

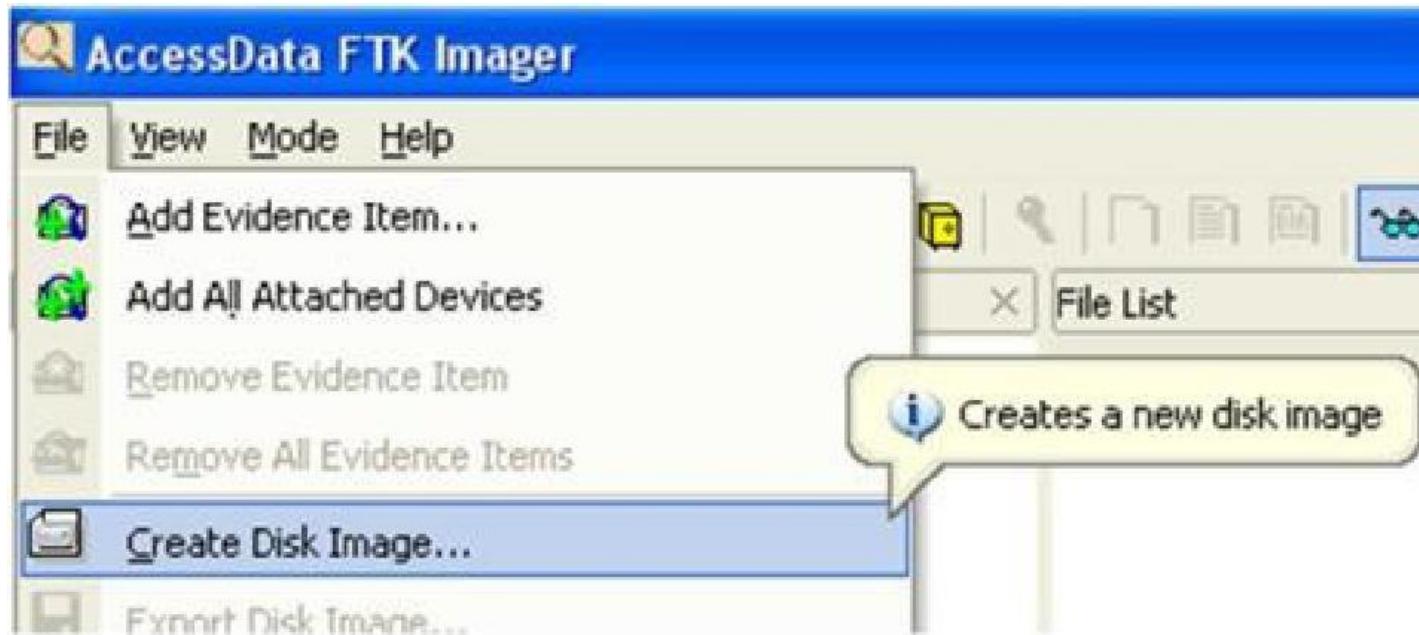
Disk 2 Details

File Edit

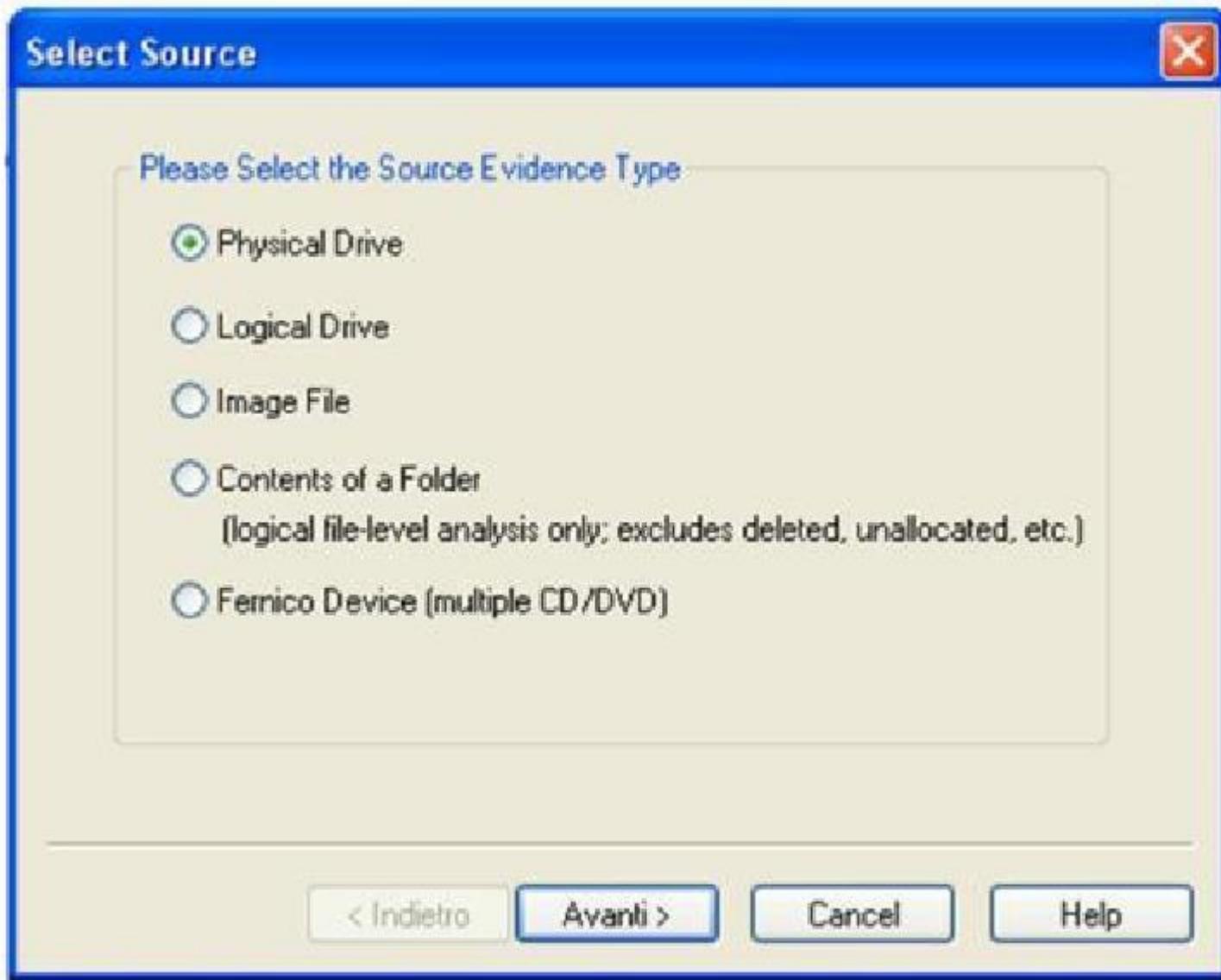
Property	Value
Disk Information (General)	
Vendor	(empty)
Model	QUANTUM FIREBALLIc20.30
Revision	APL.0900
Serial number	353104964304
Bus type	IDE
Device type	Direct Access
Removable media?	No
Sector size	512 bytes
HPA in use?	No
DCO in use?	No
Security extensions in use?	No
Reported capacity	28 GB (58.633.344 sectors)
HPA capacity	28 GB (58.633.344 sectors)
DCO capacity	28 GB (58.633.344 sectors)
Forensic Bridge Information	
Vendor	Tableau
Model	T35es
Description	(not available)
Serial number	000ecc20 0035b214
Bus type	USB
Bridge access mode	Read-Only
Read-only declaration	Declares Read-Only
Write error declaration	Declares Write Errors



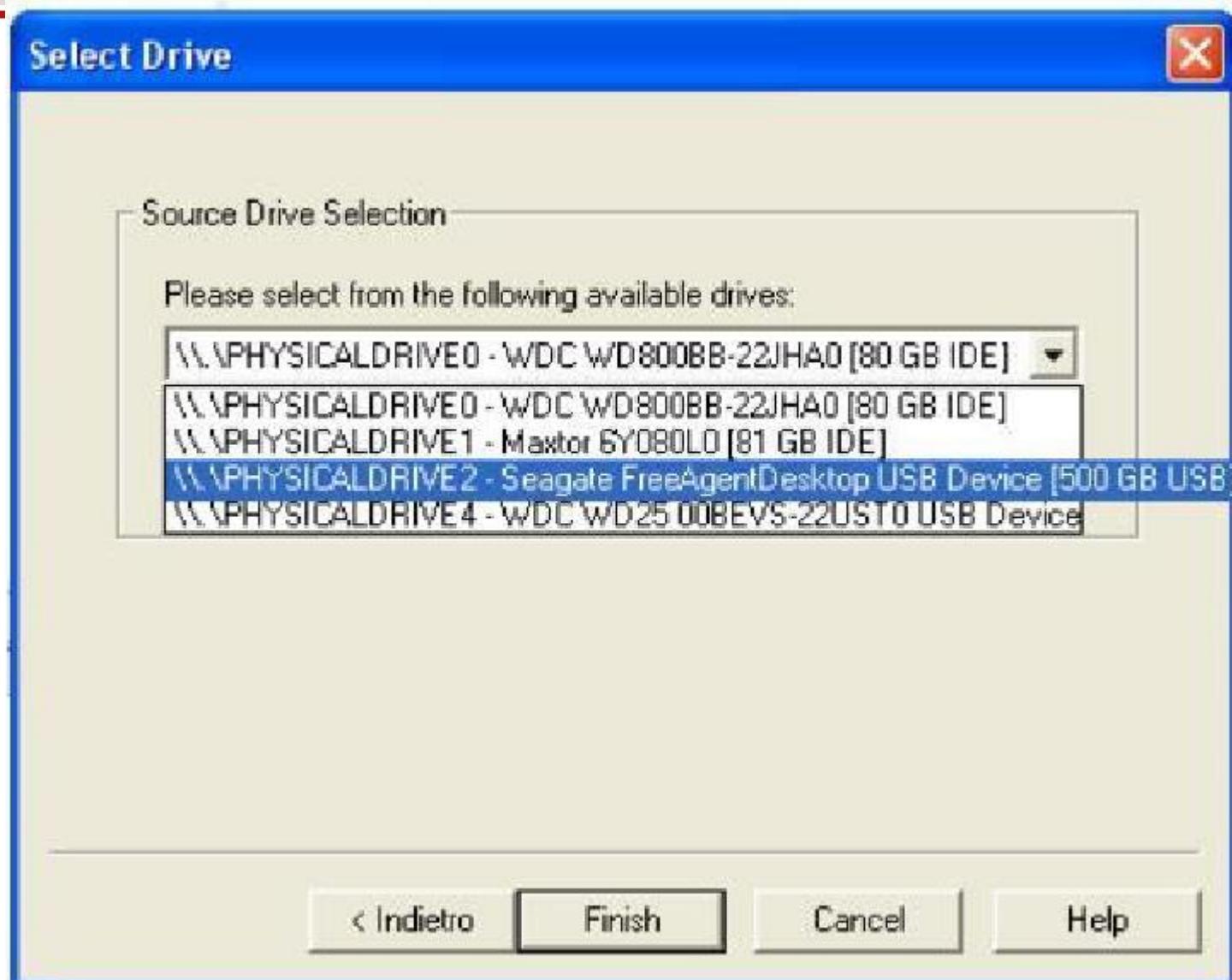
Acquisition with FTK Imager



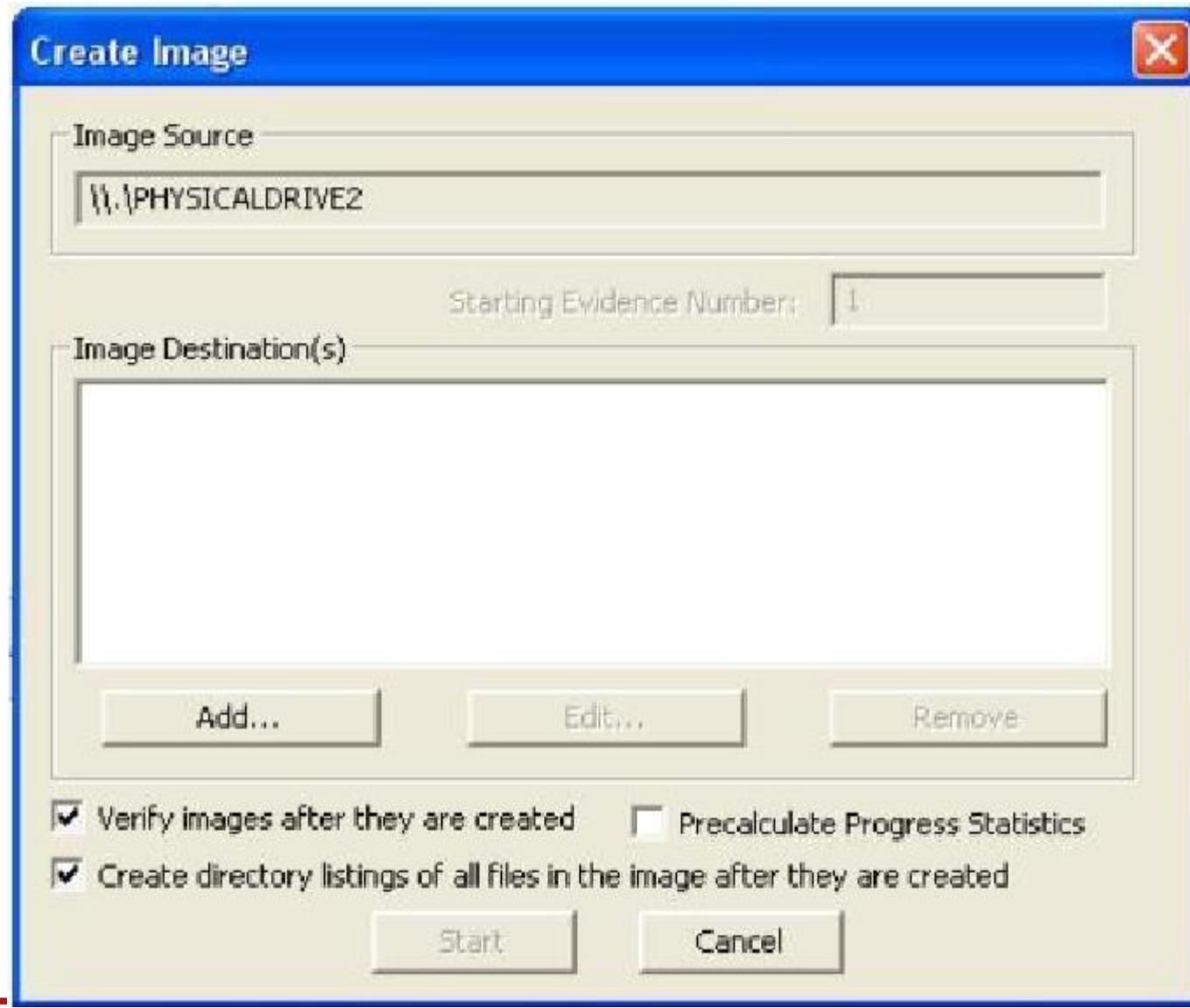
Acquisition with FTK Imager



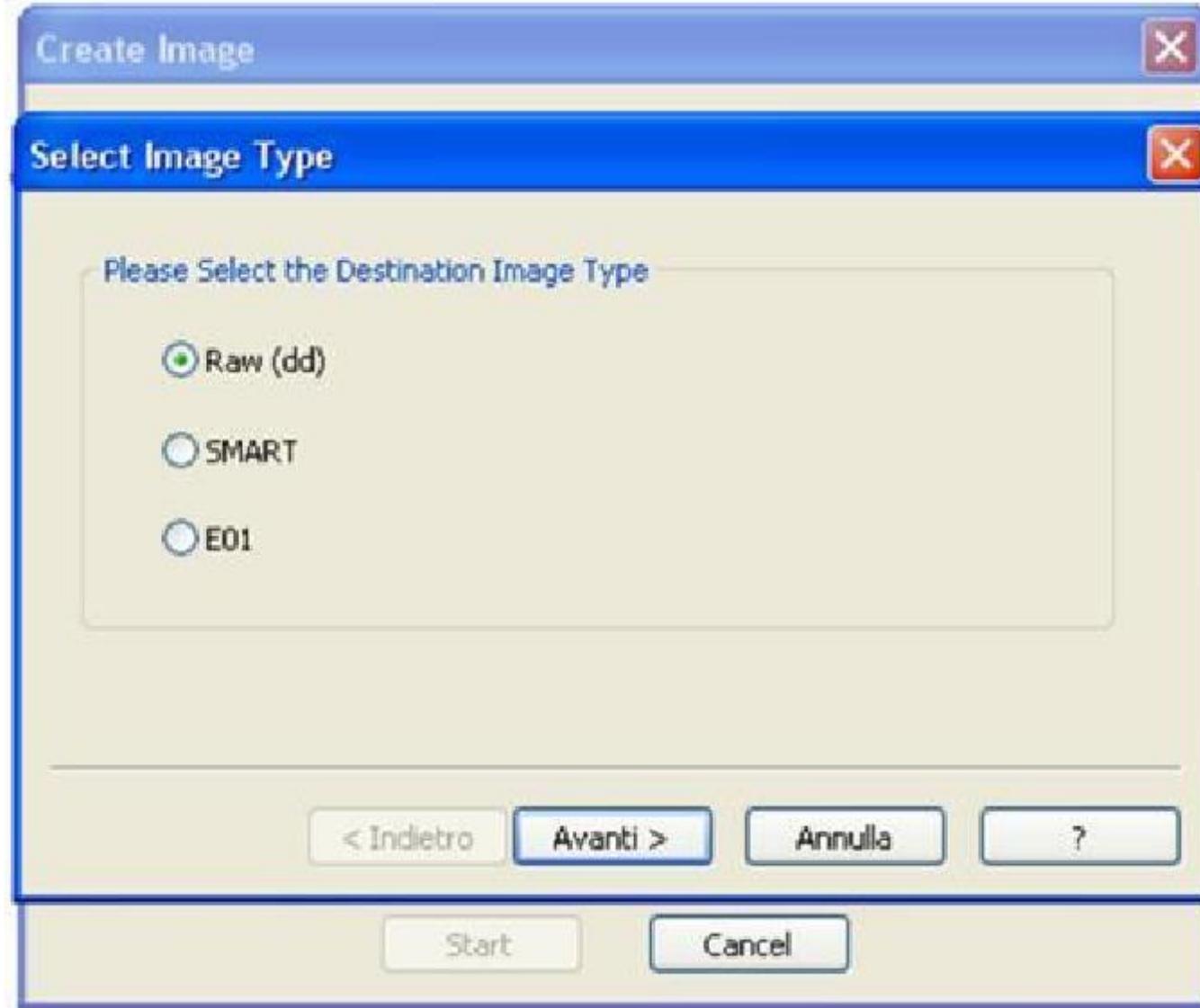
Acquisition with FTK Imager



Acquisition with FTK Imager



Acquisition with FTK Imager



Acquisition with FTK Imager

Create Image

Evidence Item Information

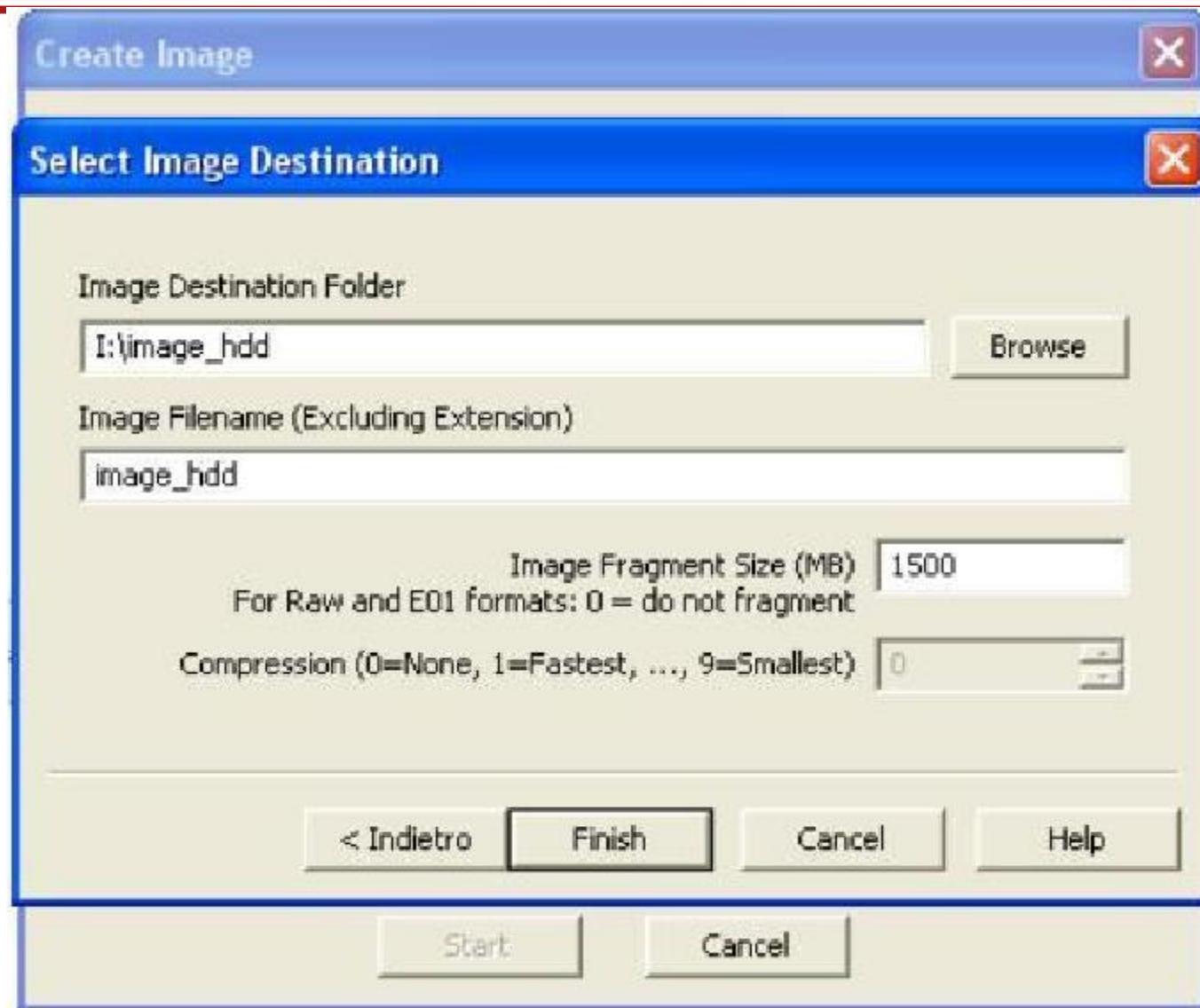
Case Number:	Acquisizione Hard Disk
Evidence Number:	00001
Unique Description:	Hard Disk Esterno USB 2.0
Examiner:	Ing . Selene Giupponi
Notes:	

< Indietro Avanti > Cancel Help

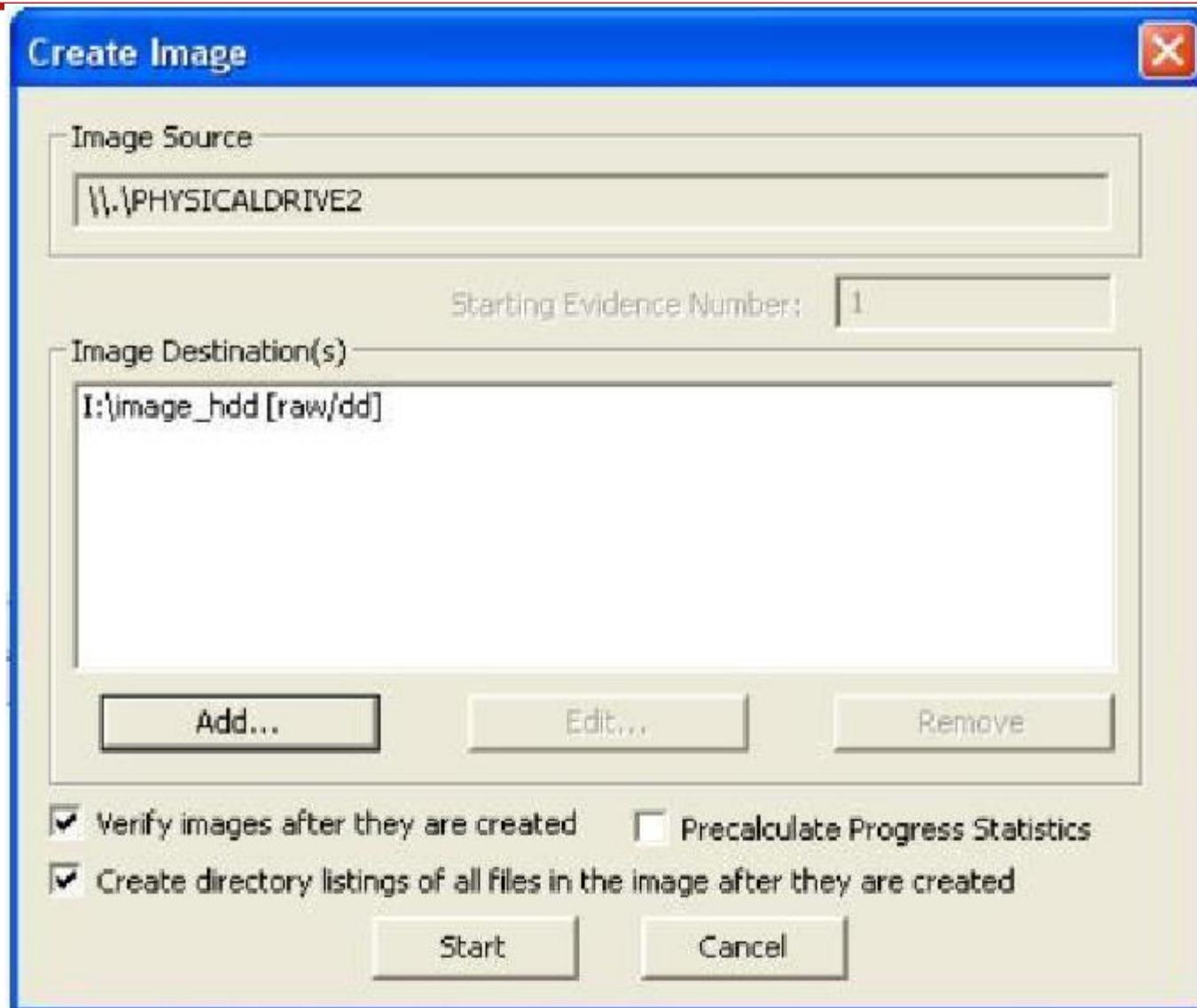
Start Cancel



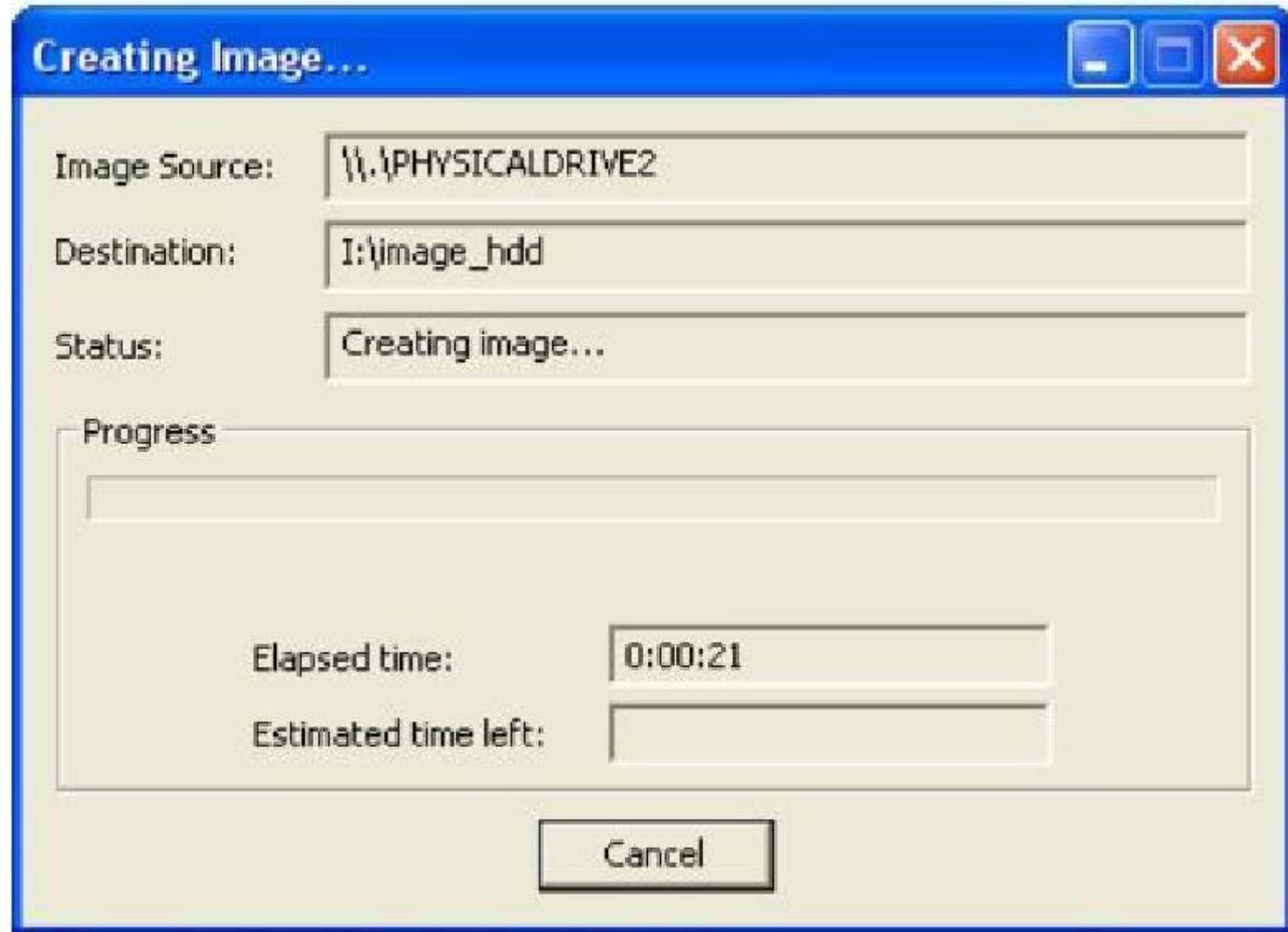
Acquisition with FTK Imager



Acquisition with FTK Imager



Acquisition with FTK Imager



Acquisition with FTK Imager

■ Drive/Image Verify Results

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

Close



Operating steps

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

Analysis

- * The evaluation mode differ depending on the type of case investigated

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

Identification of the logical structure of the disk partitions

Metadata of the file system

Activities of file carving

Extracting information about the operating system

Analysis of the main application software

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

Generation of the timeline of computer use

Search by keywords



Analysis Tools

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

Forensics Toolkit

Strong Opposition

opensource vs proprietor

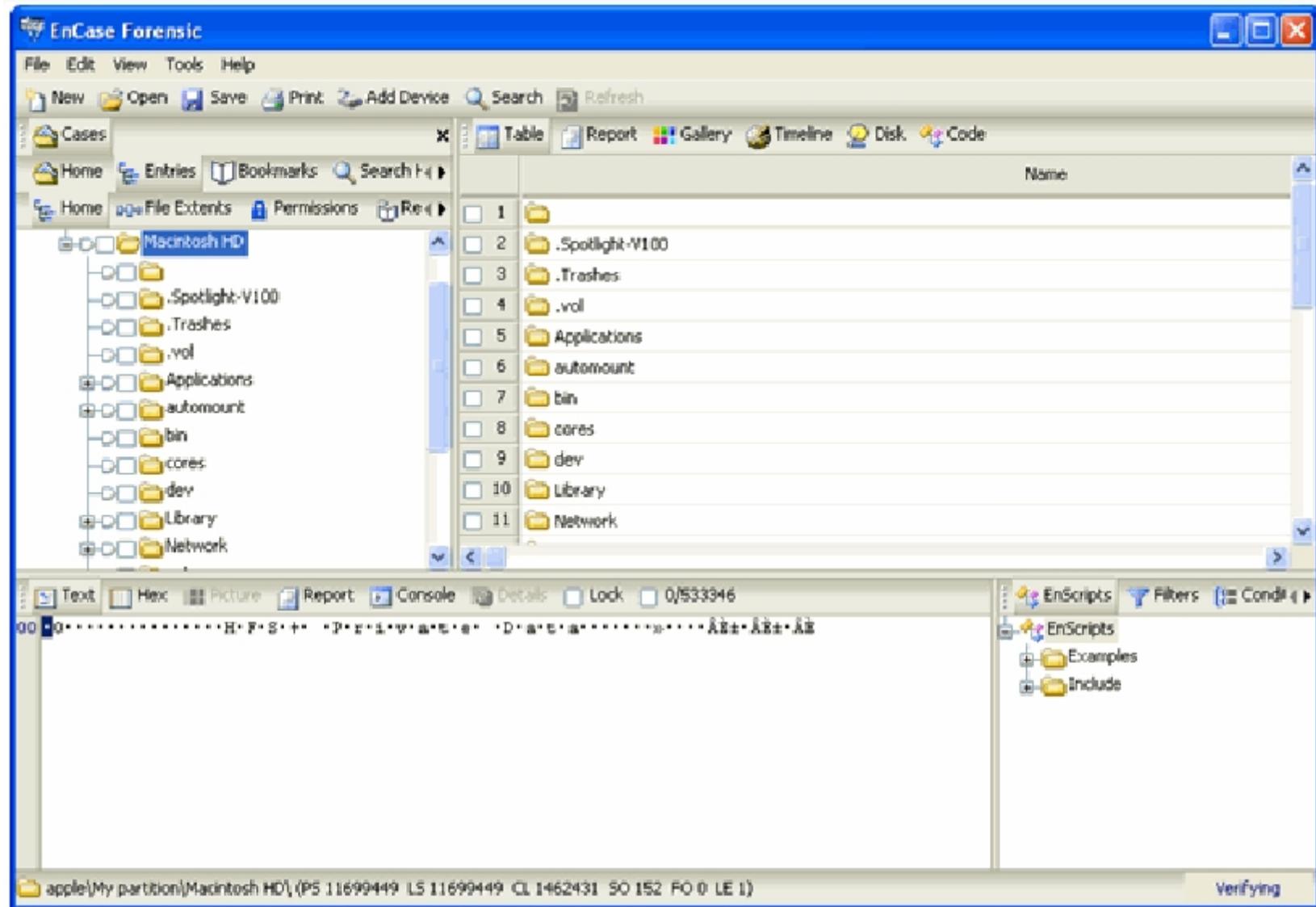
Like in any other field of information technology
the compromise is in the middle, or use open
source as long as you can, but also proprietary
tools to not ruin his life!



Commercial Forensic Toolkit

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

Encase



FTK – Access Data

The screenshot displays the AccessData FTK interface with several windows open:

- File Status:** A table showing file status counts. Key entries include:
 - Total File Items: 1117
 - Bad Extensions: 13
 - Corrupted Files: 2
 - Decrypted Files: 279
 - Encrypted Files: 2
 - From Email: 10
 - Hidden Files: 279
 - Protected By Virus: 1117
 - Recovered Files: 1117
 - Recovered Items: 1117
 - Uncompressed Items: 1117
 - Unprotected Items: 1117
 - Unknown Items: 1117
 - Untracked Items: 1117
 - Unverified Items: 1117
 - Verified By Virus: 1117
 - Filtered In: 1117
 - Filtered Out: 0
 - Unfiltered: 1117
 - Filtered: 0
 - All Items: 1117
 - Actual Files: 1117
 - HTT Ignorable: 0
 - Data Corrupt Files: 0
- File Category:** A table showing file category counts. Key entries include:
 - Documents: 88
 - Code/Script: 8
 - Databases: 9
 - Graphics: 71
 - Multimedia: 9
 - Email Message: 9
 - Binaries: 110
 - Archives: 9
 - Folders: 71
 - BlockFree Space: 143
 - Other Known Type: 21
 - Unknown Type: 732
- Memory Dump View:** A large window showing memory dump details. It includes sections for:
 - 8 Bits
 - 32 Bit Word
 - Flowdump File Header
 - Magic Number
 - Version
 - Reserved
- Flow Index Entry:** A table showing flow index entry details. It includes sections for:
 - Client (Source) IP
 - Server (Destination) IP
 - IP Protocol
 - Flags
 - Instance
 - Client Port/ICMP Type
 - Server Port/ICMP Code
 - Offset to First Data Stream
- File List View:** A table listing files with columns: File Name, Full Path, Record #, Ext, File Type, Category, Subject, Cr Date, Mod Date. Key entries include:
 - INVAVY-end.png
 - INVAVY-start.png
 - invavt.png
 - Karakorum-end.png
 - Karakorum-start.png
 - setup.bmp
 - setup1.bmp
- Bottom Status Bar:** Shows the following information:
 - 1 Listed
 - 8 Checked Total
 - C:\USERS\SAK\PRO\FA\116\superplay\superplay-2.5.5tar.gz - Untarred - Superplay-2.5.5 - Done - setup1.png

X-Ways Forensics

X-Ways Forensics - [NTFS Image.e01]

Fichier Edition Recherche Position Affichage Outils Spécialiste Options Fenêtre Aide

Données de l'as Fichier Edition

INTFS Image.e01

T\Picture et sous-dossiers 74+17=91 fichiers, 0 rep., 9 T

Nom de fichier	Ext	Chemin	Taille	Création	Modification	Accès	Attr.	1er cluster	ID	Commentaire
0:1020:299484.0[1].jpg	jpg	\Picture\003	2.1 Ko	03.05.2004 17:17:56	05.04.2004...	12.05.2005...	A	25395	362	
Pivote.jpg	jpg	\Picture\001	5.2 Ko	03.05.2004 17:17:58	10.09.1997...	12.05.2005...	A	31337	511	
350de005.jpg	jpg	\Picture\003	7.1 Ko	03.05.2004 17:17:56	03.05.2004...	12.05.2005...	H	25465	385	
makeup4.jpg	jpg	\Picture\003	14.4 Ko	03.05.2004 17:17:56	03.05.2004...	13.05.2004...	A	26491	403	
necklace1.jpg	jpg	\Picture\003	14.6 Ko	03.05.2004 17:17:56	03.05.2004...	12.05.2005...	A	26449	389	Ici vous pouriez
new-york-940020.jpg	jpg	\Picture\003	18.6 Ko	03.05.2004 17:17:56	24.03.2004...	12.05.2005...	A	26465	401	ajouter vos commentai...
Nine Planets.jpeg	jpeg	\Picture\001	20.6 Ko	03.05.2004 17:17:58	30.04.2004...	12.05.2005...	A	31032	501	
jewelry.jpg	jpg	\Picture\003	20.7 Ko	03.05.2004 17:17:56	03.05.2004...	13.05.2004...	A	26383	397	
Neo & Trinity 1.jpg	jpg	\Picture\001	26.3 Ko	03.05.2004 17:17:58	26.06.1999...	17.05.2005...	A	30966	499	
Patrick Stewart 2.jpeg	jpeg	\Picture\001	27.2 Ko	03.05.2004 17:17:58	24.02.1997...	12.05.2005...	A	31169	506	
Ticod 3.jpg	jpg	\Picture\002	29.2 Ko	03.05.2004 17:17:57	30.04.2004...	13.01.2005...	A	29261	457	
Ticod 1.jpg	jpg	\Picture\002	29.3 Ko	03.05.2004 17:17:57	30.04.2004...	13.01.2005...	A	29245	456	
makeup3.jpg	jpg	\Picture\003	32.0 Ko	03.05.2004 17:17:58	30.04.2004...	13.01.2005...	A	26475	402	
Zhang Ziyi 40.jpg	jpg	\Picture\001	32.1 Ko	03.05.2004 17:17:58	30.04.2004...	13.01.2005...	A	31479	517	
sparprie50.gif	gif	\Picture\003	34.2 Ko	03.05.2004 17:17:58	30.04.2004...	13.01.2005...	A	26631	408	
McCoy.jpg	jpeg	\Picture\001	35.5 Ko	03.05.2004 17:17:58	30.04.2004...	13.01.2005...	A	30787	484	
Patrick Stewart 5.jpg	jpeg	\Picture\001	35.5 Ko	03.05.2004 17:17:58	30.04.2004...	13.01.2005...	A	31185	507	
Spock 1.jpg	jpg	\Picture\001	36.9 Ko	03.05.2004 17:17:58	30.04.2004...	13.01.2005...	A	31409	514	

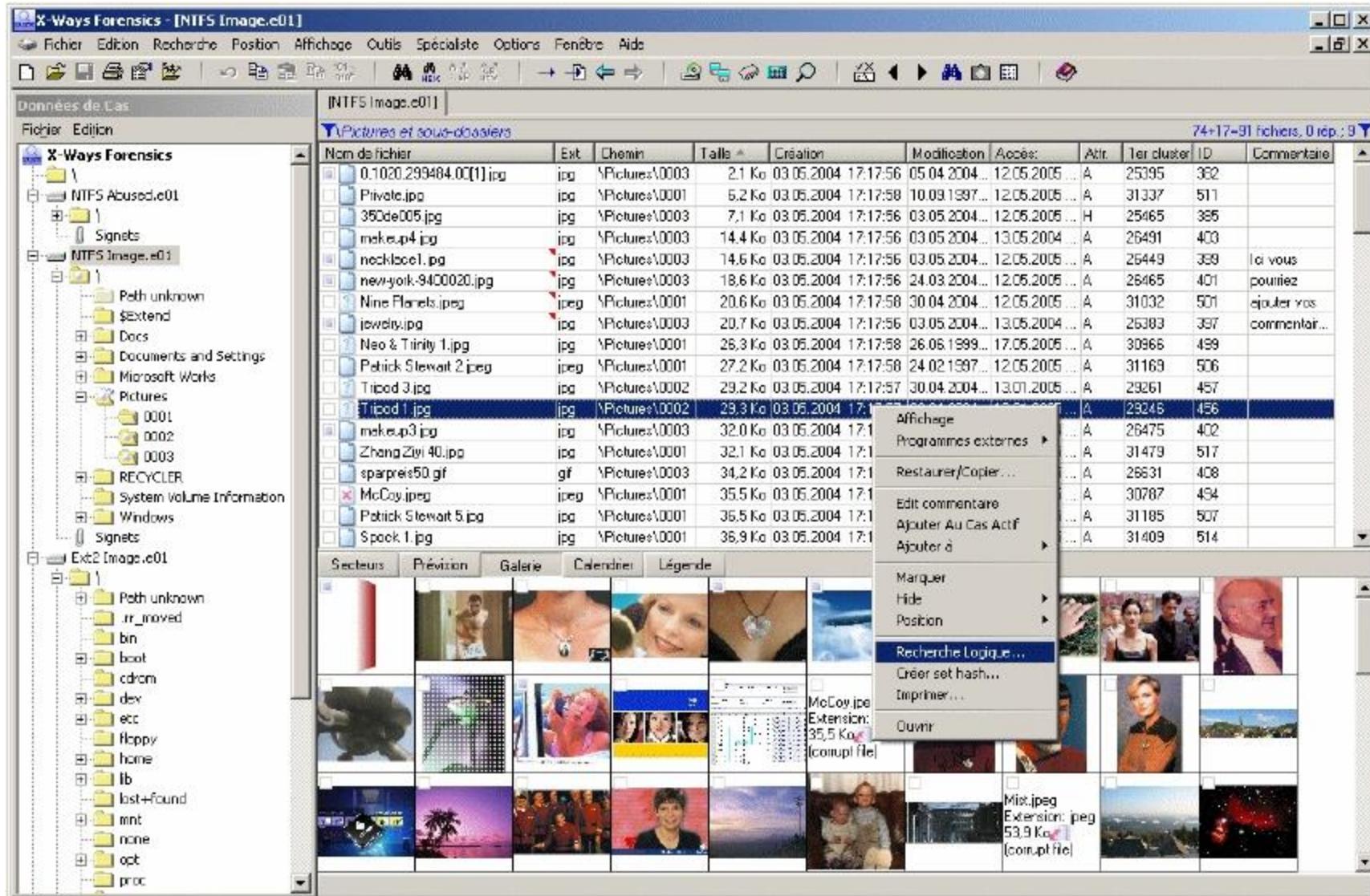
Secteurs Prévision Galerie Calendrier Légende

McCoy.jpg Extension: 35,5 Ko [corrupt file]

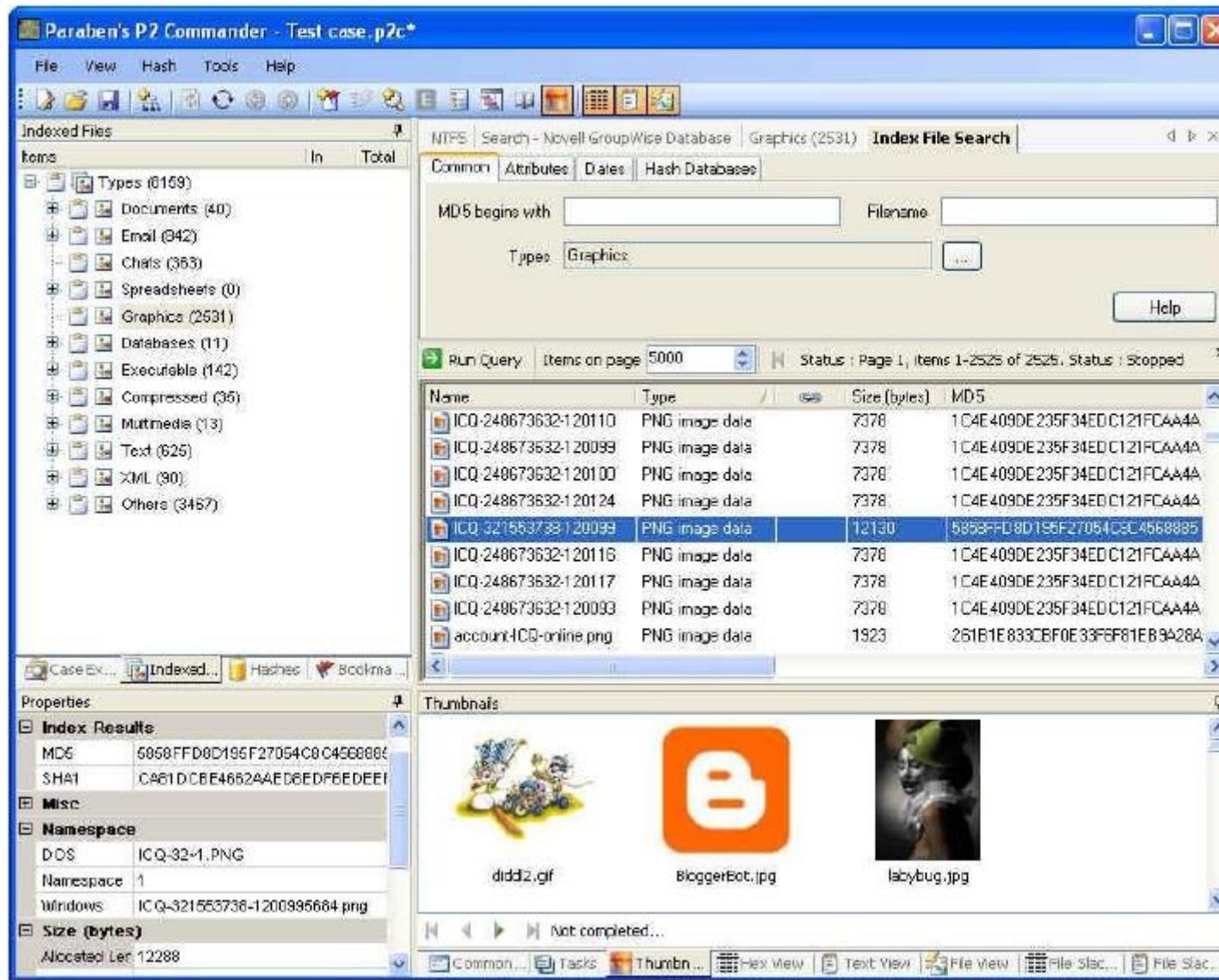
Mix.jpg Extension: jpeg 53,9 Ko [corrupt file]

Contextual menu for the selected file "McCoy.jpg":

- Affichage
- Programmes externes...
- Restaurer/Copier...
- Edit commentaire
- Ajouter Au Cas Actif
- Ajouter à
- Marquer
- Hide
- Position
- Recherche logique...
- Créer set hash...
- Imprimer...
- Ouvrir



Paraben P2 Commander



ProDiscover

ProDiscover - Suspect Server

File Network Action View Tools Help

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

Project - Suspect Server

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

37 Object(s) (10 Folder(s), 27 File(s))

Select	File Name	File Extension	Size	Attributes	Deleted
<input type="checkbox"/>	\$Secure:\$SDS		274556 bytes	--ADS--	NO
<input type="checkbox"/>	\$UpCase		131072 bytes	--META--	NO
<input type="checkbox"/>	\$Volume		0 bytes	--META--	NO
<input type="checkbox"/>	ardldr	exe	148992 bytes	---ashr	NO
<input type="checkbox"/>	arcsetup	exe	162816 bytes	---ashr	NO
<input type="checkbox"/>	AUTOEXEC	BAT	0 bytes	----h-	NO
<input type="checkbox"/>	boot	ini	186 bytes	----sh-	NO
<input type="checkbox"/>	CONFIG	SYS	0 bytes	----h-	NO
<input type="checkbox"/>	hiberfil	sys	133742592 b...	---ash-	NO
<input type="checkbox"/>	InstDriver	exe	3800 bytes	---a--r	NO
<input type="checkbox"/>	IO	SYS	0 bytes	---ashr	NO
<input type="checkbox"/>	MSDOS	SYS	0 bytes	---ashr	NO
<input type="checkbox"/>	NTDETECT	COM	34468 bytes	---ashr	NO
<input type="checkbox"/>	ntldr		214416 bytes	---ashr	NO
<input type="checkbox"/>	pagefile	sys	201326892 b...	---ash-	NO
<input type="checkbox"/>	_hidden_	sys	3465 bytes	---a--r	NO

MZ_ 0 0 YY , @
II,0LI!This program cannot be run in DOS mode.
\$ ±0'EO"Ü~o"Ü~o"y~u"Ü~i~o"Ü~o.Ü~o"Ü~Richo"Ü~
FE L00 3%> a 000000A0 @I 80 _0 a0 0 0 0 0 C
0 _0 _0 +g 0 0 0 0 0 0 T
a0 4 .text NO _0 _0
h.rdata " a0 a0 @ H.data 0
@ EINIT XI _0 a.reloc v
0 _0 @ System VMy\$@0 <03_0>j0PH_00 y\$@0
fÄ0,AU0%5_ 0 F_ 0 I_U^ATf= 0 t*Vysä00 <0_ 0
<t\$00Ej0QVyg@0 fÄ0_f0 j0X@e03AA0 U<i<M03AIt@It@It@f@ tof@toiu<E0<
]A0 IU<I<E0Ht@Ht@Ht@f@ t@f@t@H@u@<MD<ED@D]A0 U<i<M03AIt; It@It@f@
tof@toiu.<E0fAp@<E0fAhc@<E0fA@e@<E0fA@e@<E0fA@e@<E0fA@e@>A0
U<i<M03AIt@It@It@f@ t@f@t@t@u@<E0<@-]A0 <E0<@Decorrootkit:



Forensics Toolkit opensource

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

The Sleuth Kit

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

The Sleuth Kit – File Analysis

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

View Directory:
E:\

OK

ALL DELETED FILES

EXPAND DIRECTORIES

	File Type	File Name	Creation Date	Last Modified	Last Accessed	Size	Permissions	Owner	Group
r/r	label.exe	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	2002.06.13 17:08:45 (EDT)		32016	48	0	182-128-4
r/r	legacy.inf	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	2002.06.13 17:08:40 (EDT)		4654	48	0	183-128-4
r/r	lights.exe	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	2002.06.13 17:08:40 (EDT)		35600	48	0	184-128-4
r/-	LMREPL.EXE	0000.00.00 00:00:00 (GMT)	0000.00.00 00:00:00 (GMT)	0000.00.00 00:00:00 (GMT)		0	0	0	0
r/r	LMREPL.EXE	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	2002.06.13 17:08:45 (EDT)		86800	48	0	185-128-4
r/r	loadfix.com	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	2002.06.13 17:08:40 (EDT)		1131	48	0	186-128-4 (realloc)
r/r	loadfix.com	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	2002.06.13 17:08:40 (EDT)		1131	48	0	186-128-4

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

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

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



The Sleuth Kit – File Content

This file is currently being viewed in a **sanitized environment**

HTML files have been edited to disable scripts and links. Pictures have been replaced by place holders

NORMAL

EXPORT CONTENTS

INVESTIGATION SITE

IMAGE SANITIZED

QUARANTINE

INVESTIGATION SITE

IMAGE SANITIZED

INVESTIGATION SITE

IMAGE SANITIZED

QUARANTINE

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

Priority Online Access

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

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

Read the Installation and Getting Starting Guides:
www.redhat.com/manual

Search and browse our mailing list archives:
www.redhat.com/mailing-lists

Access our online support



The Sleuth Kit – Hash Database

NSRL Lookup

a3e1a9ba1345f76c69a1e97f9d8b8f43 lmrepl.exe
a3e1a9ba1345f76c69a1e97f9d8b8f43 lmrepl.exe

Exclude Database Lookup

a3e1a9ba1345f76c69a1e97f9d8b8f43 Hash Not Found

Alert Database Lookup

a3e1a9ba1345f76c69a1e97f9d8b8f43 Hash Not Found

The Sleuth Kit - File Type Sorting

The screenshot shows the 'FILE TYPE' tab selected in the top navigation bar of the Sleuth Kit interface. The main content area is titled 'File Type Sortings'. A descriptive text explains that the sorter tool processes an image and organizes files by type, saving categories in an output directory. Below this, several configuration options are listed with checkboxes:

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

An 'OK' button is located at the bottom left of the dialog.

The Sleuth Kit - Timeline

The screenshot shows the main interface of The Sleuth Kit - Timeline. At the top, there is a menu bar with five buttons: CREATE DATA FILE, CREATE TIMELINE, VIEW TIMELINE, VIEW NOTES, and HELP CLOSE. Below the menu is a search bar with a magnifying glass icon. The main area displays a list of file timeline entries. The entries are sorted by date and time, with the most recent entry at the top. Each entry includes the date and time, file ID, file type, permissions, file size, offset, and path. The interface has a light green background and a yellow header bar.

Date	File ID	Type	Permissions	Size	Offset	Path
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/oemnadm.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/oemnadef.inf
	22297	.ac	-/-rwxrwxrwx	48 0	266-128-4	C:/system32/oemnadfd.inf
	85632	.c	-/-rwxrwxrwx	48 0	179-128-4	C:/system32/kml386.exe
	22296	.ac	-/-rwxrwxrwx	48 0	267-128-4	C:/system32/oemnadim.inf
	32016	.c	-/-rwxrwxrwx	48 0	182-128-4	C:/system32/label.exe
	35225	.ac	-/-rwxrwxrwx	48 0	265-128-4	C:/system32/oemnadep.inf



The Sleuth Kit – Key word search

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

New Search

2 occurrences of '(jan)|(feb)|(mar)|(apr)' were found

126615 (Hex - Ascii)
- string begins at 256 bytes
180485 (Hex - Ascii)
- string begins at 0 bytes

Fragment 126615
Allocated
Group: 15
Pointed to by Inode: 30184
Pointed to by file:
/bin/mk

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

EXPORT CONTENTS ADD NOTE

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

0	25733a20	57726974	696e6720	6d6f6465	ts: Writ ing mode
16	20534353	49206d6f	64652070	61676520	SCS I mo de p age
32	6661696c	65642e0a	00000000	00000000	fail ed...
48	00000000	00000000	00000000	00000000
64	25733a20	436f6d70	72657373	696f6e20	ts: Comp ress ion
80	6d6f6465	206e6f74	20636861	6e676564	mode not cha nged
96	2e0a0000	00000000	00000000	00000000
112	00000000	00000000	00000000	00000000
128	25733a20	52652d72	65616420	6f662074	ts: Re-r ead of t
144	68652063	6f6d7072	65737369	6f6e2070	he c ompr essi on p
160	61676520	6661696c	65642e0a	00436f6d	age fail ed.. .Com
176	70726573	73696f6e	206f6e2e	0a00436f	pres sion on.. .Co
192	6d707265	7373696f	6e206f66	662e0a00	mpre ssio n of f...
208	00000000	00000000	00000000	00000000
224	00000000	64ba0408	00000000	00000000 d...
240	00000000	00000000	00000000	00000000
256	2449643a	202f7573	72322f75	73657273	\$Id: /us r2/u sers
272	2f6d616b	69736172	612f7372	632f7379	/mak isar a/sr c/sy
288	732f6d74	2d73742d	302e3562	2f6d742e	s/mt -st- 0.5b /mt.
304	63206174	2053756e	20417567	20313620	c at Sun Aug 16
320	30393a35	313a3137	20313939	38206279	09:5 1:17 199 8 by
336	206d616b	69736172	61406b61	692a6a61	mak isar a@ka i.ma



The Sleuth Kit – Metadata Analysis

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

MFT Entry Number:
182-128-4

Alert Database OK

OK ALLOCATION LIST

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

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

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

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



The Sleuth Kit – Image Details

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

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

META-DATA INFORMATION

Range: 2 - 45762
Root Directory: 2

CONTENT-DATA INFORMATION

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

FAT CONTENTS (in sectors)

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

Mount image DD

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

Mount image DD – P2 Explorer

Paraben's P2 eXplorer

File View Help

Mounted Disks

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

For Help, press F1

Paraben's Device Seizure

Paraben's device seizure

THE ONLY COMPLETE SOLUTION



Analysis of metadata from filesystem

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

Examples of metadata are:

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

File Allocation Table (FAT)

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



Master File Table (MFT) - NTFS

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

Analyzing metadata from file systems - Tools

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

Deleted Files

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

Data Recovery Tools

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

Demo R-Studio

The screenshot shows the R-STUDIO network edition interface. The main window is titled "R-STUDIO network edition - Drive view". The menu bar includes "Drive", "Create", "Tools", "View", and "Help". Below the menu is a toolbar with icons for various functions. The left pane is titled "Drive view" and contains a tree view of drives:

Device/Disk	Label	FS	Start	Size
Local Computer				
Hitachi HD172509WV...		ATA (3rd Master)	465.8 GB	
E:	Movies - HD - SATA	NTFS	31.5 kB	465.8 GB
Maxtor 6L200P08A2H... L42WCQG		ATA (Primary Sl...	189.9 GB	
ST3160815AS3.JAC		ATA (2:2)	149.1 GB	
G:	Software - Sd2 - S...	NTFS	31.5 kB	74.5 GB
H:	Music - Sd2 - SATA	NTFS	74.5 GB	74.5 GB
ST380015AS3.JAC	SG200MWW	ATA (Primary Pl...	74.5 GB	
C:	Windows	NTFS	31.5 kB	29.0 GB
D:	Games	NTFS	29.0 GB	45.2 GB
K:			0	
Z:			0	

The drive "ST380015AS3.JAC" is selected. The right pane displays its properties:

Name	Value
Drive Type	Physical Drive/Disk
Name	ST380015AS3.JAC
Os Object	\Device\PhysicalDrive0
R-Studio Driver	Win32Handle\Physical
Size	74.5 GB (156301488 sec)
Sector Size	512B
Partition Size	74.5 GB (156301488 sec)
Drive Control	
Maximum Transfer	128kB
I/O Unit	512B
Buffer Alignment	2B
I/O Tries	2
Physical Drive Geometry	
Cylinders	9729
Tracks Per Cylinder	255
Sectors Per Track	63
Sector Size	512B
Device Identification	
Product	ST380015A

The bottom left pane is titled "Log" and contains a table with columns "Type", "Date", "Time", and "Text". The bottom right status bar says "Ready".



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

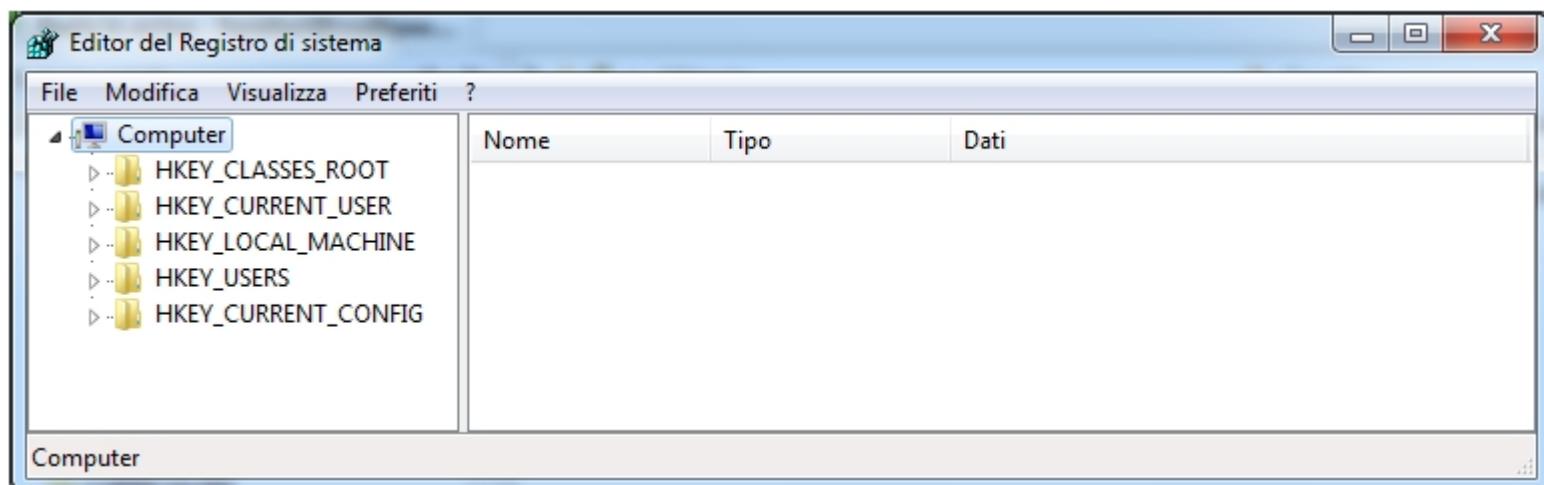
- * The file Netsetup.log is located in the Windows \ Debug and contains information about the workgroup or domain configured on the computer
The file is created during the operating system and stores installation it all changes regarding Any adjustment of the working group, domain or enabling file sharing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

Windows Registry

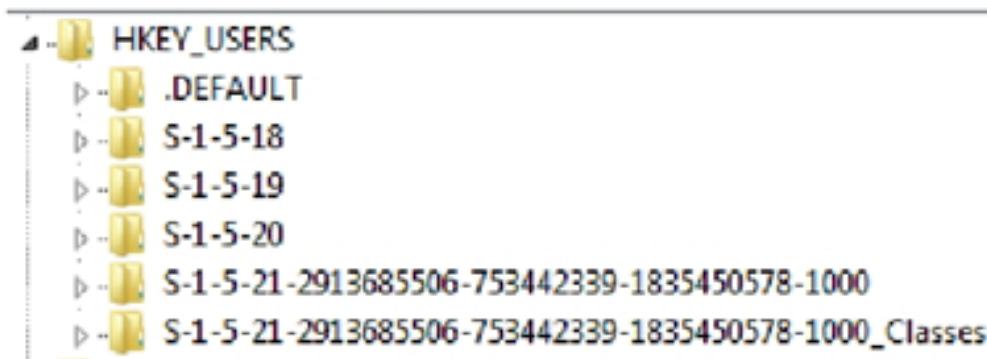
- * The Windows registry contains very significant forensics data from our point of view
- * The registry is a hierarchical database of configuration data for the operating system and most of the programs installed
- * The user interacts with the registry typically through the configuration utility of 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\Harddisk\Volume2\Boot\BCD
\REGISTRY\MACHINE\HARDWARE	REG_SZ	
\REGISTRY\MACHINE\SAM	REG_SZ	\Device\Harddisk\Volume3\Windows\System32\config\SAM
\REGISTRY\MACHINE\SECURITY	REG_SZ	\Device\Harddisk\Volume3\Windows\System32\config\SECURITY
\REGISTRY\MACHINE\SOFTWARE	REG_SZ	\Device\Harddisk\Volume3\Windows\System32\config\SOFTWARE
\REGISTRY\MACHINE\SYSTEM	REG_SZ	\Device\Harddisk\Volume3\Windows\System32\config\SYSTEM
\REGISTRY\USER\DEFAULT	REG_SZ	\Device\Harddisk\Volume3\Windows\System32\config\DEFAULT
\REGISTRY\USER\S-1-5-19	REG_SZ	\Device\Harddisk\Volume3\Windows\ServiceProfiles\LocalService\NTUSER.DAT
\REGISTRY\USER\S-1-5-20	REG_SZ	\Device\Harddisk\Volume3\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
\Registry\User\S-1-5-21-2913685506-753442339-1835450578-1000	REG_SZ	\Device\Harddisk\Volume3\Users\Mattia\NTUSER.DAT
\Registry\User\S-1-5-21-2913685506-753442339-1835450578-1000_Classes	REG_SZ	\Device\Harddisk\Volume3\Users\Mattia\AppData\Local\Microsoft\Windows\UsrClass.dat



Windows Registry – Hive Software

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

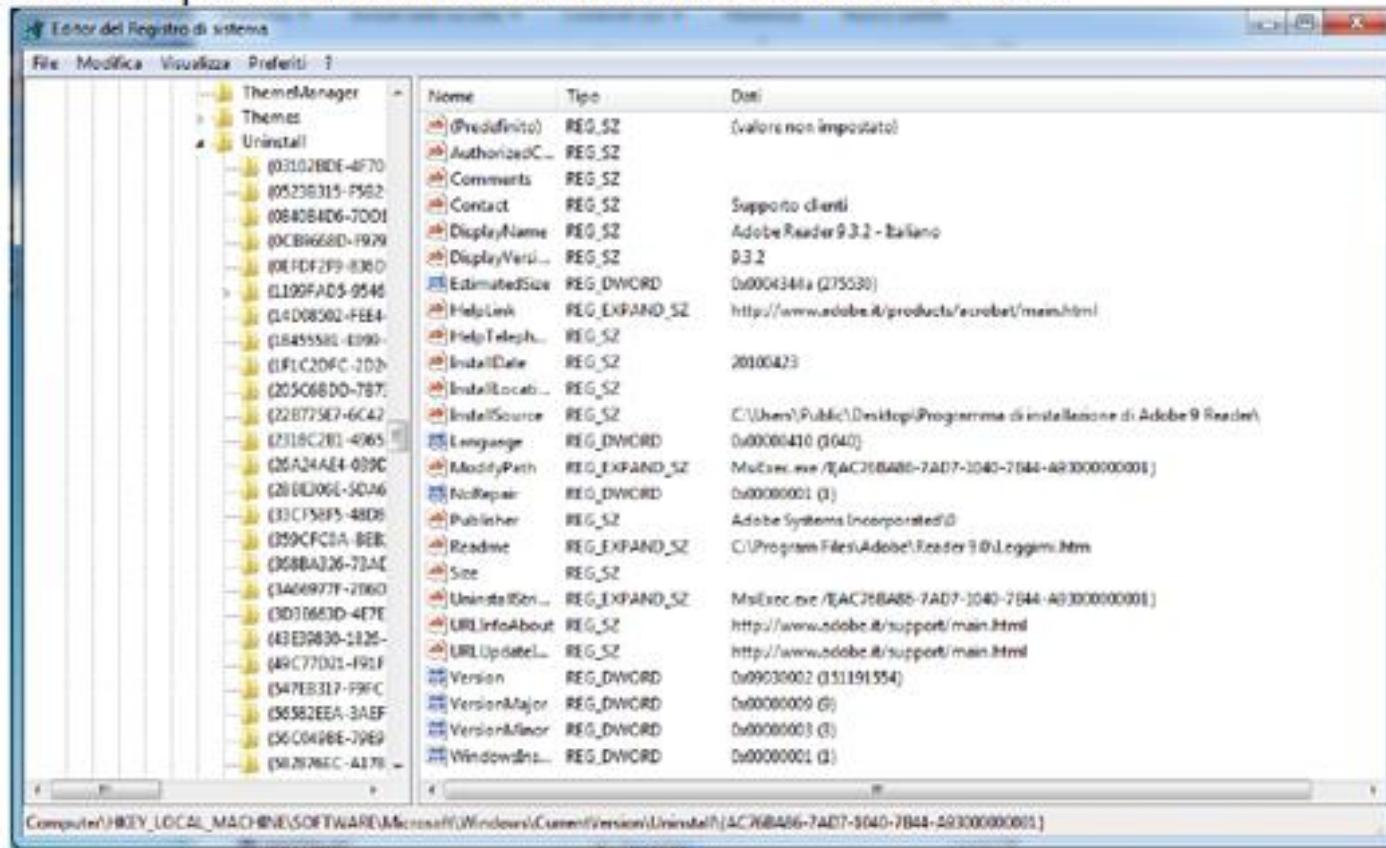
The screenshot shows the Windows Registry Editor interface. On the left, a tree view displays the key **HKLM\Software\Microsoft\Windows\CurrentVersion\AppPath**. Under this key, there is a single subkey named **App Paths**, which contains several entries corresponding to application executables. On the right, a table view shows two registry entries:

Nome	Tipo	Dati
ab (Predefinito)	REG_SZ	C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe
ab Path	REG_SZ	C:\Program Files\Adobe\Reader 9.0\Reader\

Windows Registry – Hive Software

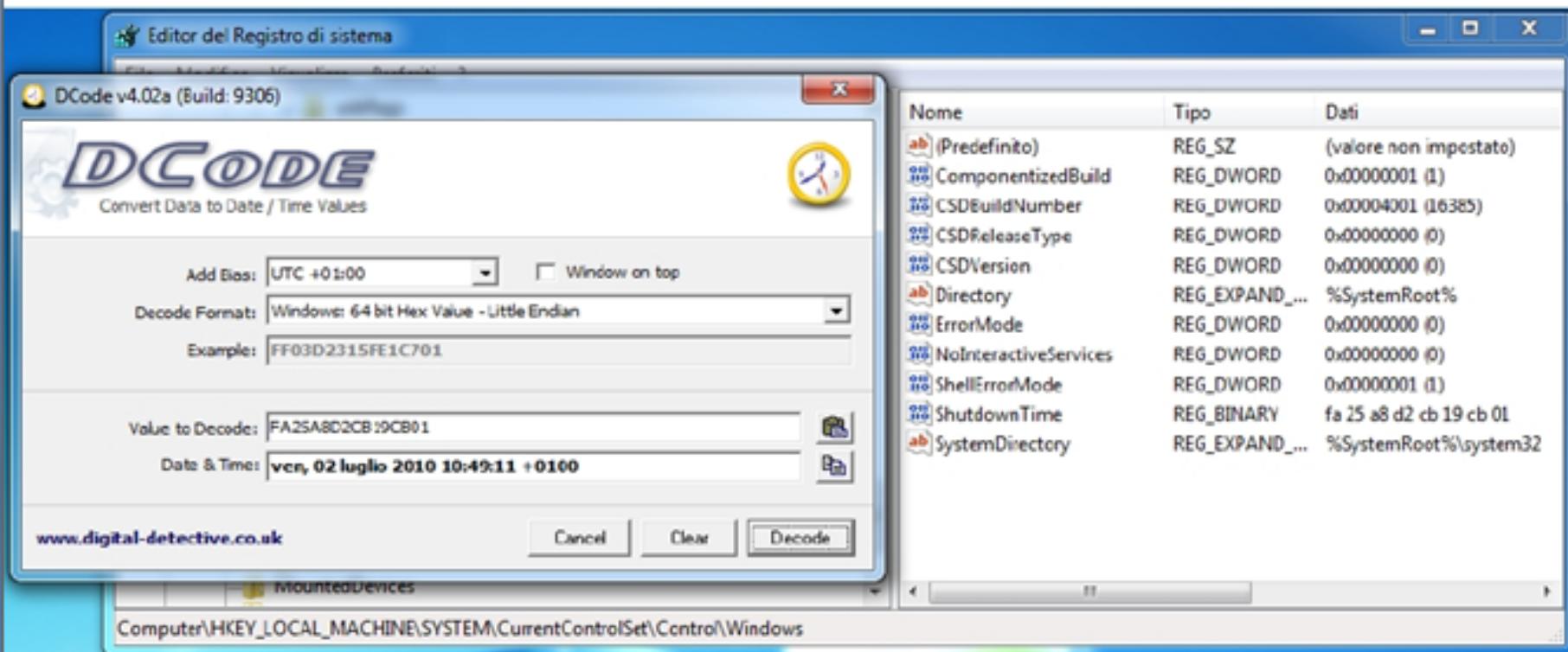
- Analogamente, la chiave

HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall
contiene i percorsi di disinstallazione dei vari software



Windows Registry – Hive Software

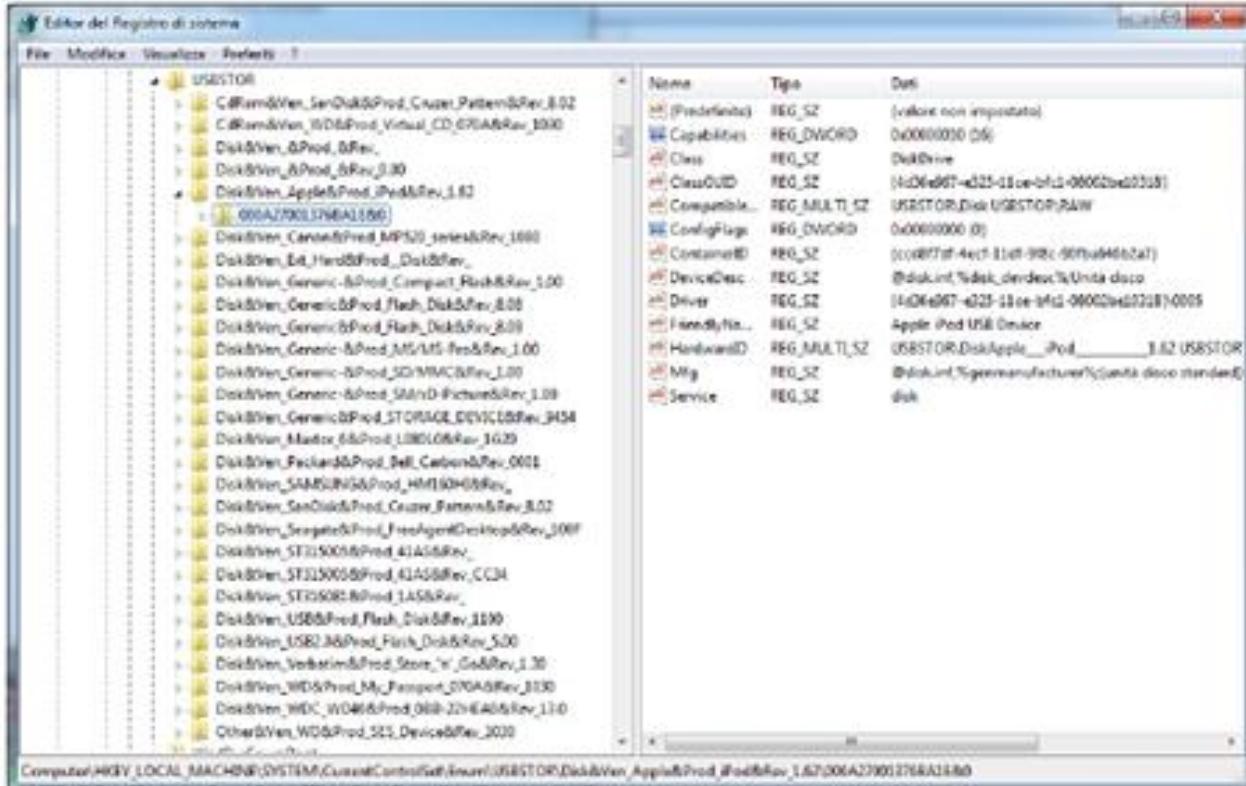
The Shut Down Time, Time Zone Information



Windows Registry – Hive System - USB

3

HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR



Windows Registry – Hive System - IDE

HKLM\SYSTEM\CurrentControlSet\Enum\IDE

The screenshot shows the Windows Registry Editor interface. The left pane displays a tree view of registry keys under 'Enum'. The 'IDE' key is expanded, showing two sub-keys: 'CdRomHL-DT-ST_DVDRAM_GHINN...' and 'DiskST31500341AS...'. The 'DiskST31500341AS...' key has two sub-keys: '4896a10cf8080.2.0' and 'DiskST31500541AS...'. The '4896a10cf8080.2.0' key contains three sub-keys: 'Device Parameters', 'LogConf', and 'Properties'. The right pane shows a table of registry values for the 'DiskST31500341AS...' key. The table has columns for 'Nome' (Name), 'Tipo' (Type), and 'Dati' (Data). The values listed are:

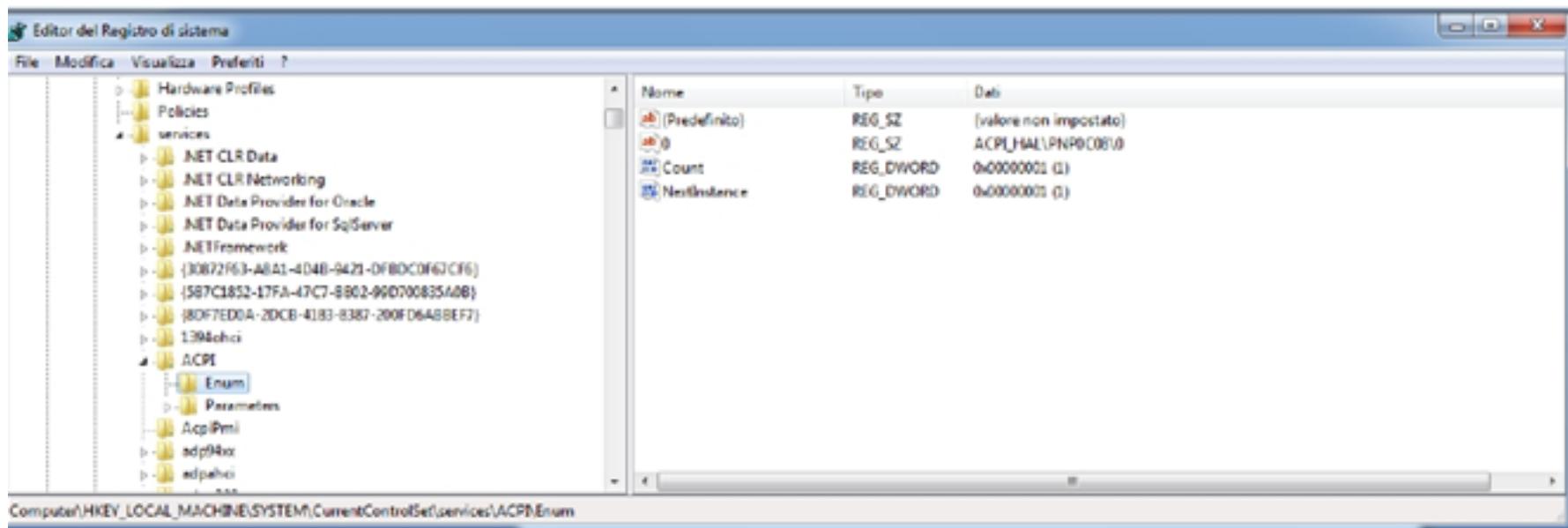
Nome	Tipo	Dati
(Predefinito)	REG_SZ	(valore non impostato)
Capabilities	REG_DWORD	0x00000006 (6)
Class	REG_SZ	DiskDrive
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	GenDisk
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainedID	REG_SZ	{44e83dcf-6a1b-11cf-9f5f-005056c00008}
DeviceDesc	REG_SZ	@disk.inf%disk_devdesc%Unità disco
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\003
FriendlyName	REG_SZ	ST31500341AS
HardwareID	REG_MULTI_SZ	IDE\DiskST31500341AS..._CC1H..._IDE\ST31500341/S...
LocationInformation	REG_SZ	4
Mfg	REG_SZ	@disk.inf%genmanufacturer%\unità disco standard
Service	REG_SZ	disk

The status bar at the bottom shows the full path: Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\IDE\DiskST31500341AS... and the selected key: CC1H..._4896a10cf8080.2.0.

Windows Registry – Hive System

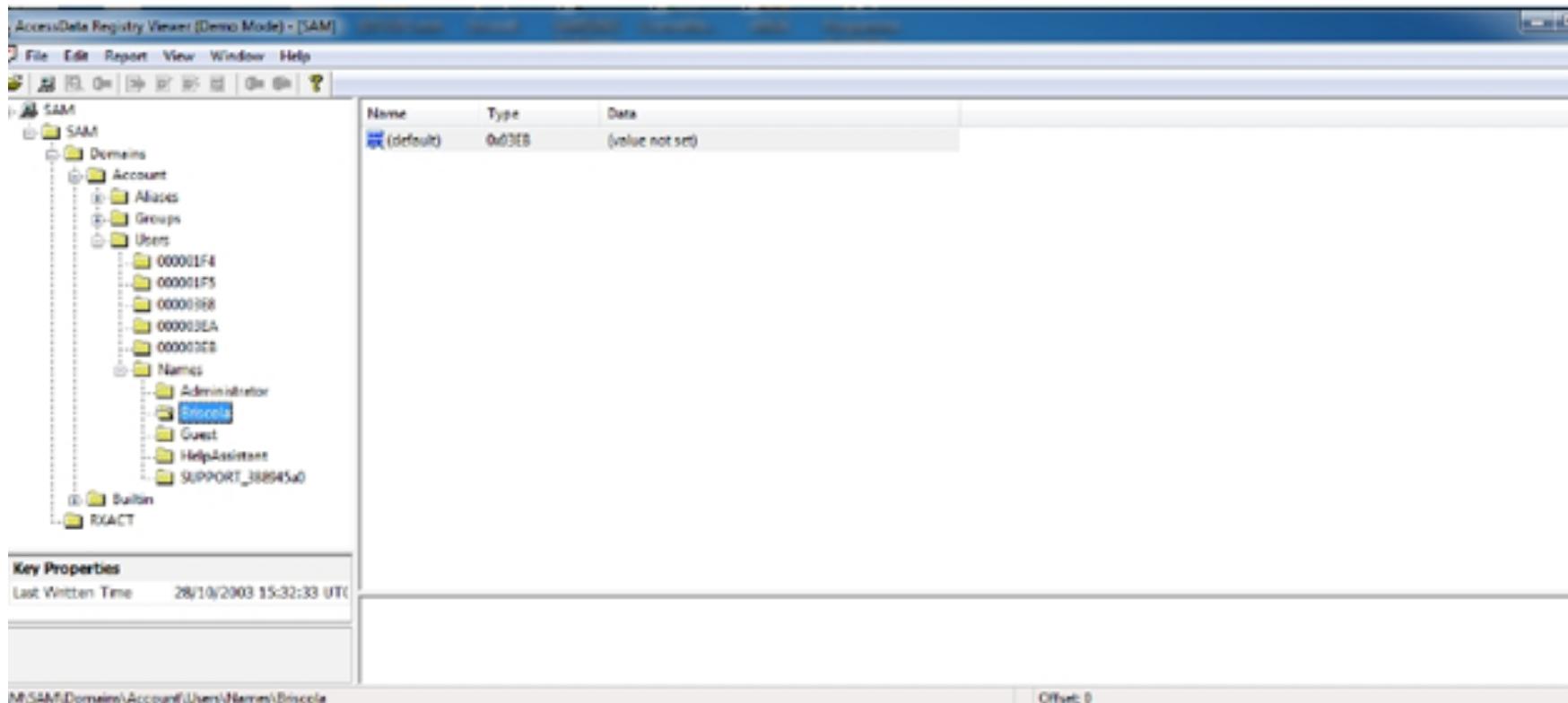
Services Installed in a Computer

HKLM\System\CurrentControlSet\Services



Windows Registry – Hive System

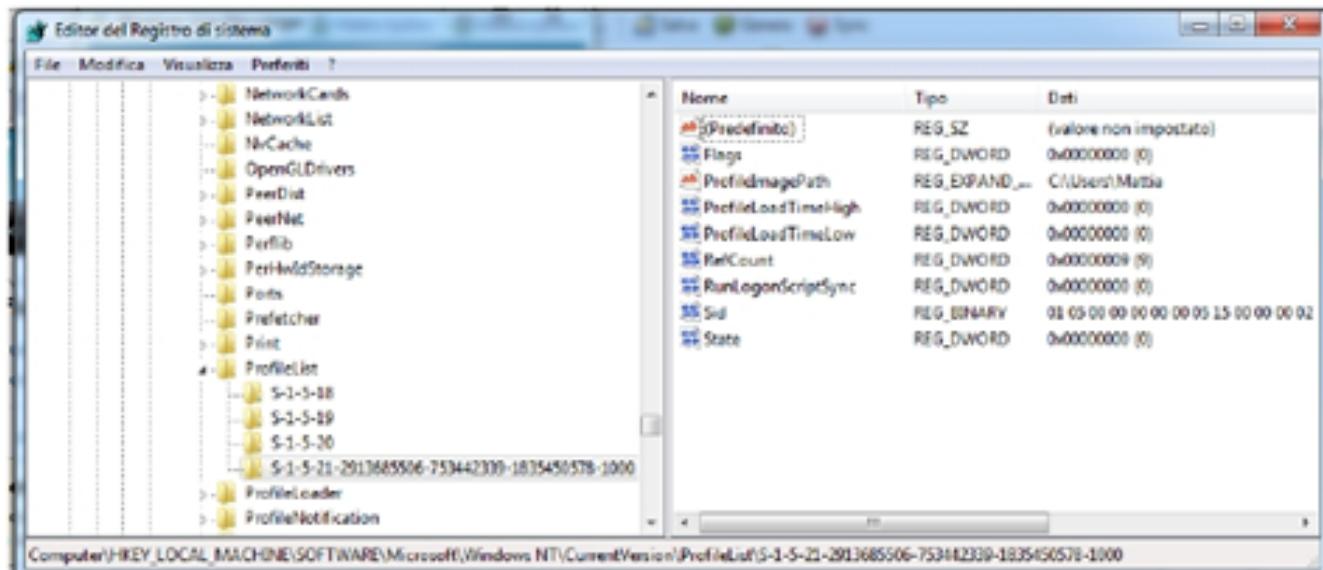
- La hive SAM contiene le informazioni sugli utenti e i gruppi configurati nella macchina
- Il file si trova nella cartella %SYSTEMROOT%\system32\config



Windows Registry – Hive SAM

USERS AND GROUP

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



Autorun

Chiave

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

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

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

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

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

HKLM\System\CurrentControlSet\Services

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

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



Autorun File

Nome file e percorso

%SYSTEMDRIVE%\autoexec.bat

%SYSTEMDRIVE%\config.sys

%WINDIR%\wininit.ini

%WINDIR%\win.ini

%WINDIR%\system.ini

%WINDIR%\dosstart.bat

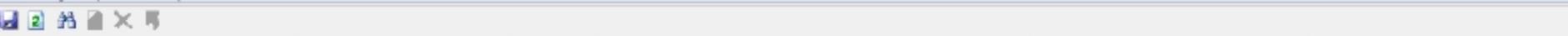
%WINDIR%\system\autoexec.nt

%WINDIR%\system\config.nt

%WINDIR%\system32\autochk.exe



Autoruns

Autoruns - Sysinternals: www.sysinternals.com			
File	Entry	Options	Help
			
AutumnEntry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> Adobe ARM	Adobe Reader and Acrobat... Adobe Systems Incorporated	c:\program files\common fil...	
<input checked="" type="checkbox"/> Adobe Reader... Adobe Acrobat SpeedLear...	Adobe Systems Incorporated	c:\program files\adobe\rea...	
<input checked="" type="checkbox"/> avast!	avast! Antivirus	AVAST Software	c:\program files\avast\softwa...
<input checked="" type="checkbox"/> GrooveMonitor	GrooveMonitor Utility	Microsoft Corporation	c:\program files\microsoft of...
<input checked="" type="checkbox"/> IAAnotif	Event Monitor User Notifica...	Intel Corporation	c:\program files\intel\intel m...
<input checked="" type="checkbox"/> iTunesHelper	iTunesHelper	Apple Inc.	c:\program files\tunes\itun...
<input checked="" type="checkbox"/> QuickTime Task	QuickTime Task	Apple Inc.	c:\program files\quicktime\...
<input checked="" type="checkbox"/> Samsung Panel...	Samsung Panel...		c:\windows\samsung\pane...
<input checked="" type="checkbox"/> SunJavaUpdate...	Java(TM) Platform SE binary	Sun Microsystems, Inc.	c:\program files\java\jre6\...
<input checked="" type="checkbox"/> TkBellExe	RealNetworks Scheduler	RealNetworks, Inc.	c:\program files\common fil...
<input checked="" type="checkbox"/> Vmware Hot Network Acc...	Vmware, Inc.		c:\program files\vmware\w...
<input checked="" type="checkbox"/> vmware-tray	Vmware Tray Process	Vmware, Inc.	c:\program files\vmware\w...
HKCU\Software\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> msnmegr	Windows Live Messenger	Microsoft Corporation	c:\program files\windows liv...
<input checked="" type="checkbox"/> RoboForm	RoboForm TaskBarIcon	Siber Systems	c:\program files\siber syste...
<input checked="" type="checkbox"/> Skype	Skype	Skype Technologies S.A.	c:\program files\skype\pho...
HKLM\SOFTWARE\Classes\Protocol\Filter			
<input checked="" type="checkbox"/> text/xml	Microsoft Office XML MIME...	Microsoft Corporation	c:\program files\common fil...
HKLM\SOFTWARE\Classes\Protocol\Handler			
<input checked="" type="checkbox"/> grooveLocalG...	GrooveSystemServices Mo...	Microsoft Corporation	c:\program files\microsoft of...
<input checked="" type="checkbox"/> livecall	Windows Live Messenger P...	Microsoft Corporation	c:\program files\windows liv...
<input checked="" type="checkbox"/> ms-help	Microsoft® Help Data Servi...	Microsoft Corporation	c:\program files\common fil...
<input checked="" type="checkbox"/> msnms	Windows Live Messenger P...	Microsoft Corporation	c:\program files\windows liv...
<input checked="" type="checkbox"/> skype-ie-addon..	Skype add-on for IE	Skype Technologies S.A.	c:\program files\skype\tool...
<input checked="" type="checkbox"/> skypeform	Skype for COM API	Skype Technologies	c:\program files\common fil...
HKLM\SOFTWARE\Microsoft\Active Setup\Uninstall Components			
<input checked="" type="checkbox"/> Microsoft Wind...	Windows Mail	Microsoft Corporation	c:\program files\windows m...
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks			
<input checked="" type="checkbox"/> Groove GFS St...	GrooveShellExtensions Mo...	Microsoft Corporation	c:\program files\microsoft of...
HKLM\Software\Classes\ShellEx\ContextMenuHandlers			
<input checked="" type="checkbox"/> avast!	avast! Shell Extension	AVAST Software	c:\program files\avast\softwa...
<input checked="" type="checkbox"/> Cover Designer	Cover Designer	Nero AG	c:\program files\nero\nero ...
<input checked="" type="checkbox"/> PSPad			c:\program files\pspad\edit...
<input checked="" type="checkbox"/> WinRAR			c:\program files\winrar\ver...
<input checked="" type="checkbox"/> XXX Groove G...	GrooveShellExtensions Mo...	Microsoft Corporation	c:\program files\microsoft of...
HKLM\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers			



Hive NETUSER

Chiave

HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\[GUID]\Count
HKU\Software\Microsoft\Windows\Shell\NoRoam\MUICache
HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
HKU\Software\Microsoft\Search Assistant\ACMru
HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\MapNetworkDriveMRU
HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions



Tools for the register analysis

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

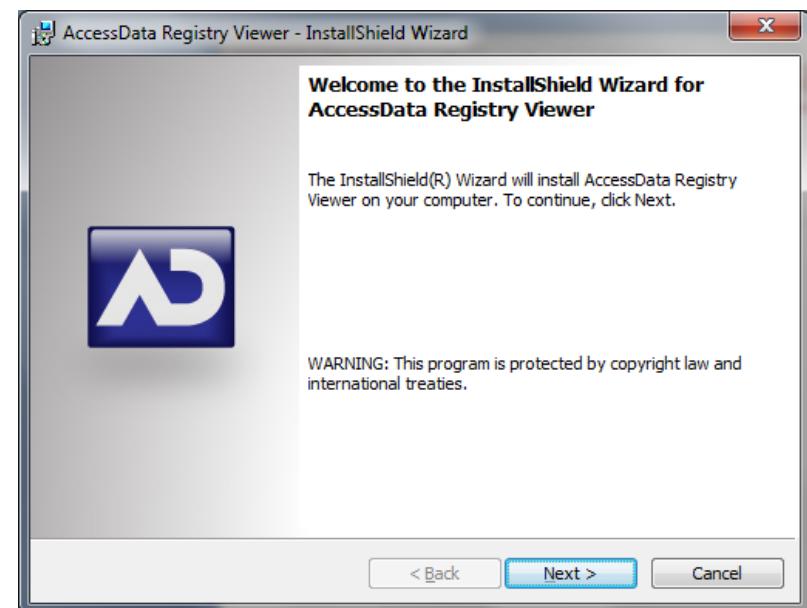
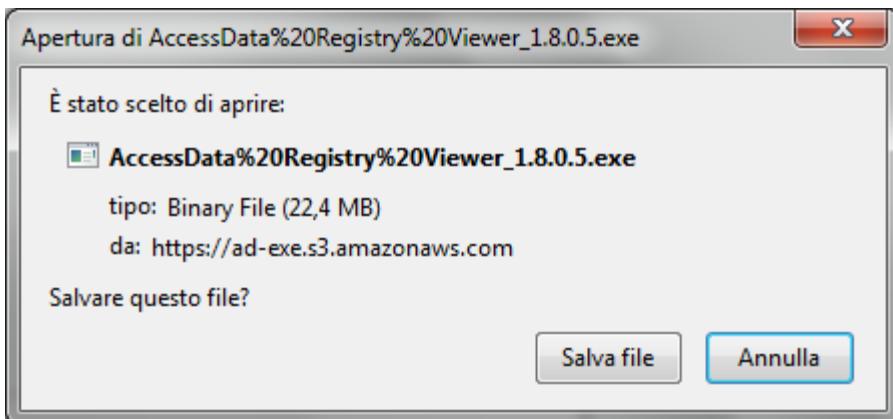
Tools for the register analysis



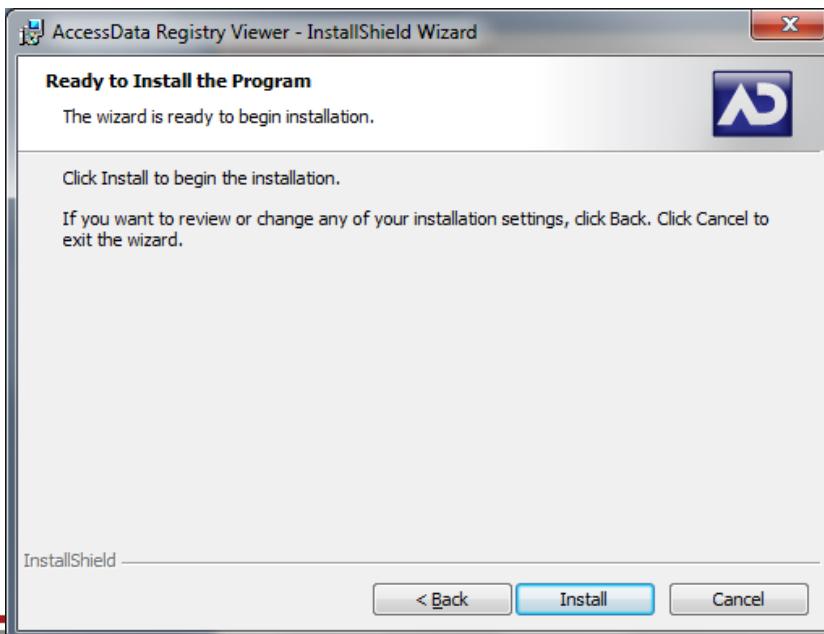
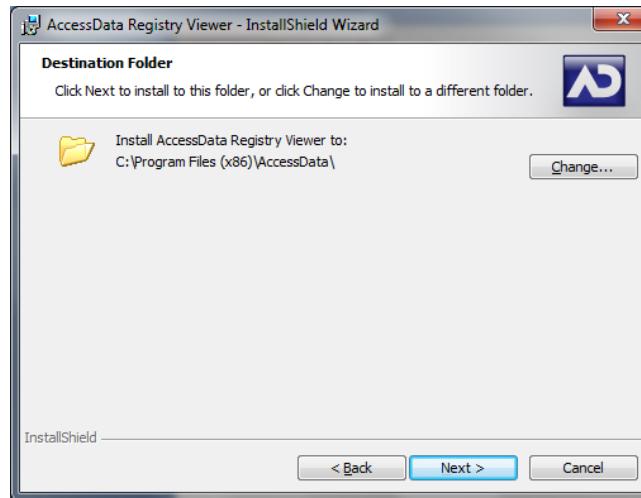
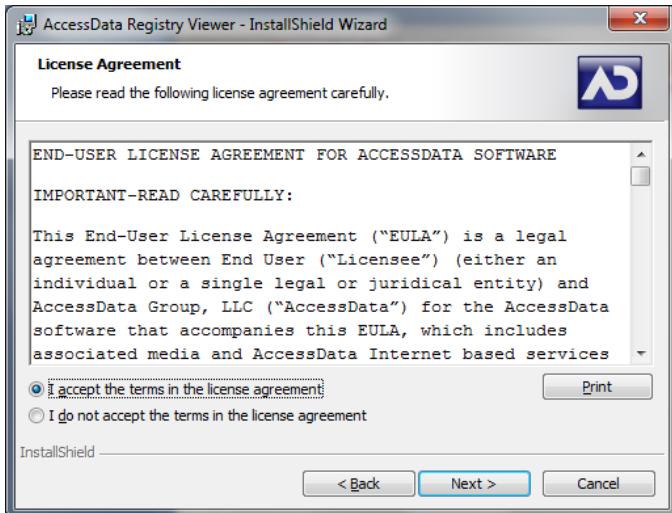
Registry Viewer 1.8.0.5

Release Date: Sep 23, 2014

[DOWNLOAD PAGE](#)



Tools for the register analysis



Recycle Bin

AccessData FTK Imager 2.6.1.62

File View Mode Help

Evidence Tree

- \$Secure
- + Documents and Settings
- + MSOCache
- + Programmi
- RECYCLER
 - S-1-5-21-823518204-725345543-6820033
 - Dc1
 - \$I30
 - Dc16.doc
 - Dc16.doc.FileSlack
 - desktop.ini
 - desktop.ni
 - INFO2
 - INFO2.FileSlack
- + 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 Alloc...	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.ni	1 KB	Regular File	12/01/2010 8.5...
INFO2	1 KB	Regular File	12/01/2010 9.1...
INFO2.FileSlack	4 KB	File Slack	

Custom Content Sources

Evidence:File System|Path|File Options

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

New Edit Remove Remove All Create Image

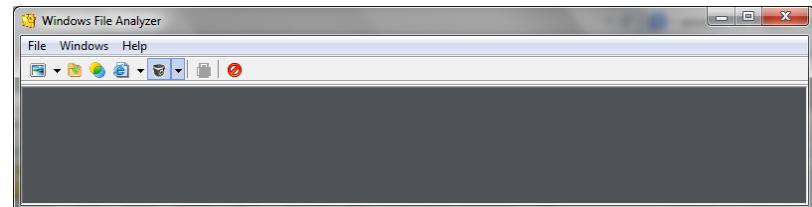
Properties | Hex Value Interpreter | Custom Content Sources

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

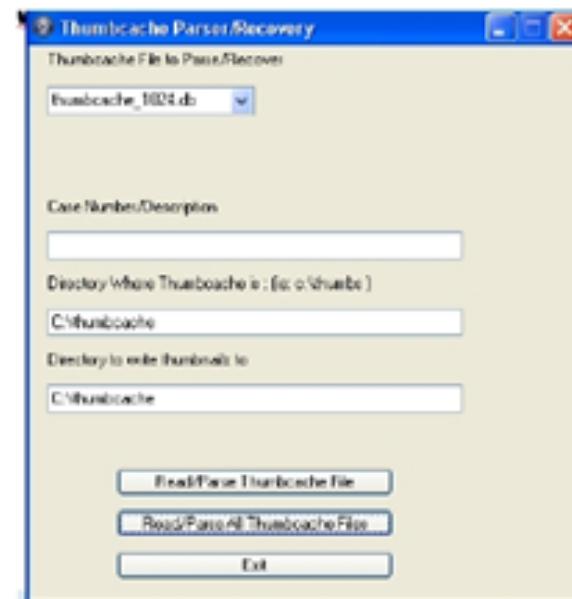
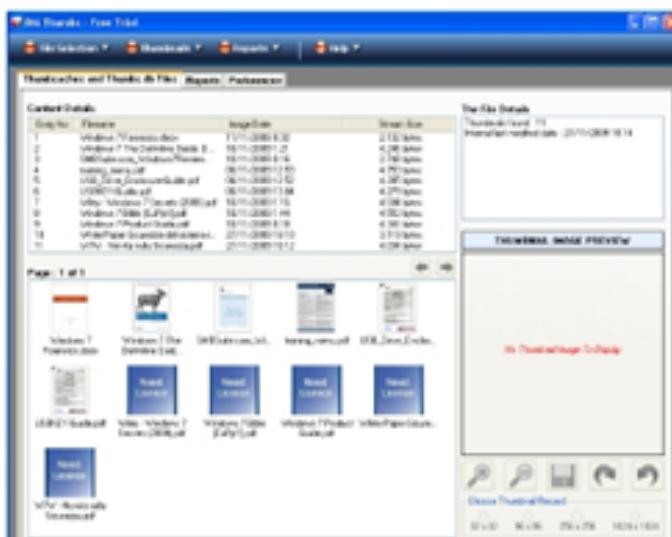
- “ Windows File Analyzer (www.mitec.cz)
-
- “ Win Forensic Analysis (<http://www.machor-software.com/>)
- “ Link Viewer (<http://www.gaijin.at/>)
- “ Lnkanalyser (<http://www.woany.co.uk/>)
- “ SimpleCarver (<http://www.simplecarver.com/>)

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

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



#1

Document the Process

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



#2



Know the Tools

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



#3



Use the Tools

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

#4



Keep it Legal

Never gain access to an account
illegally or deceptively.



#5

Verify the Owner



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



#6

Verify the Source

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



Internet Artifacts

#7



Testify!

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

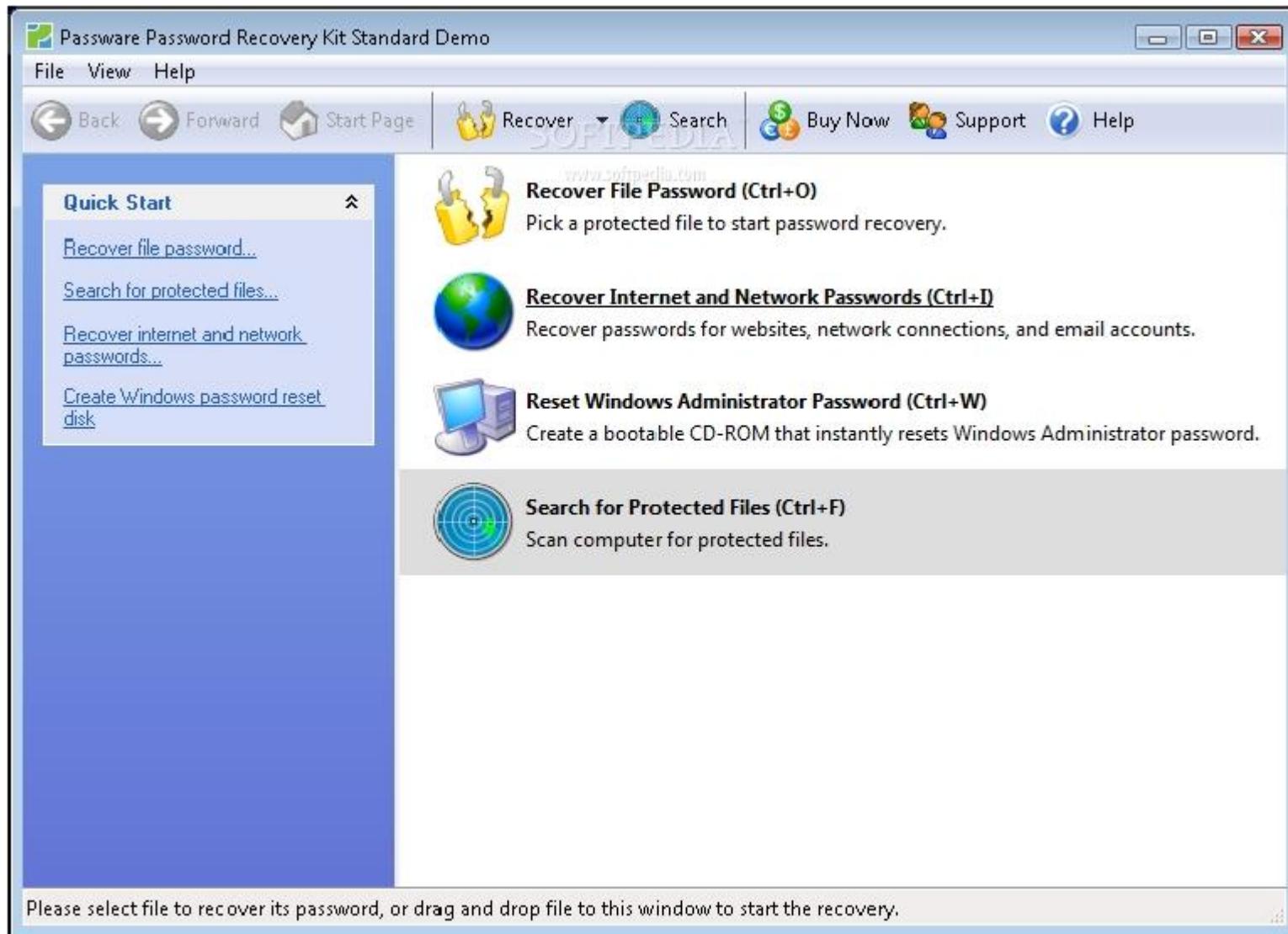


File password cracking

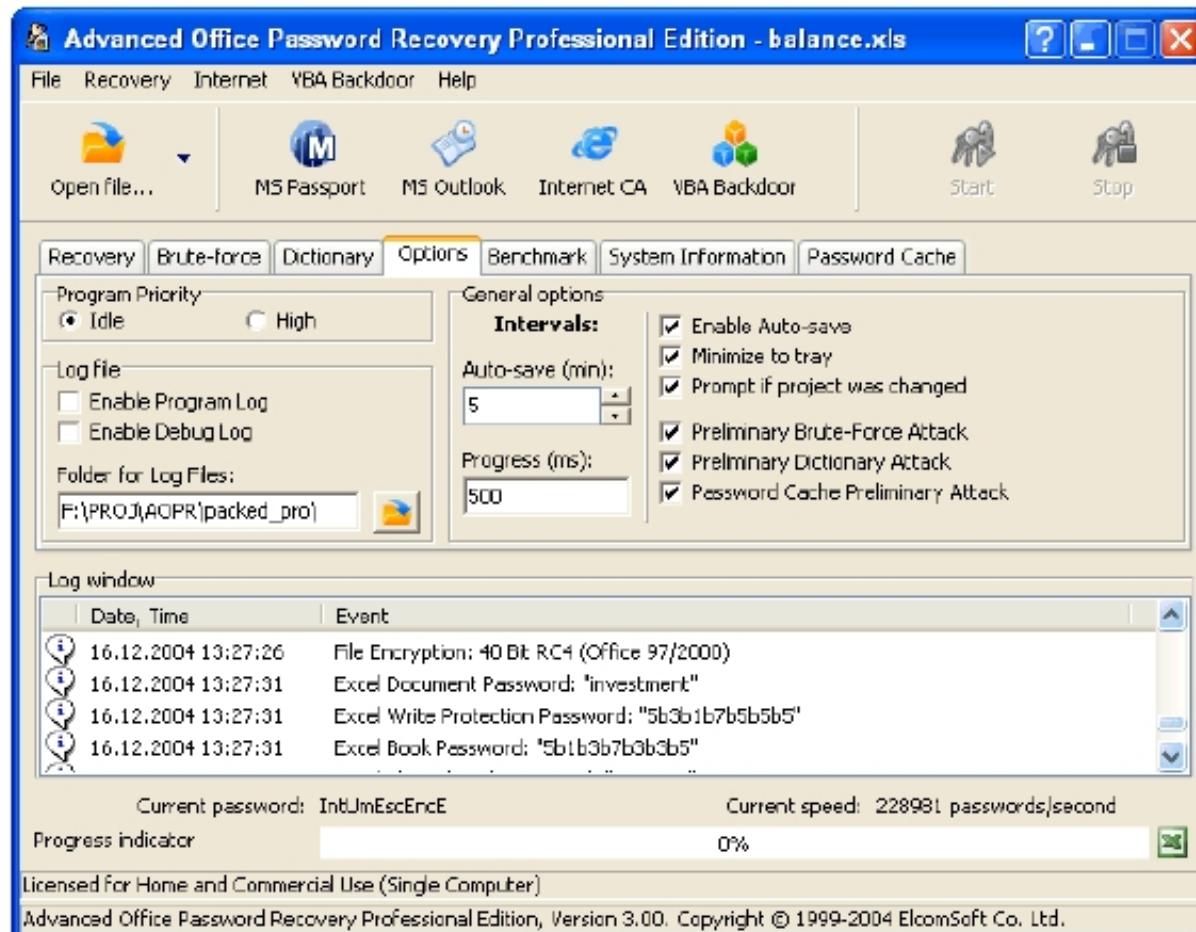
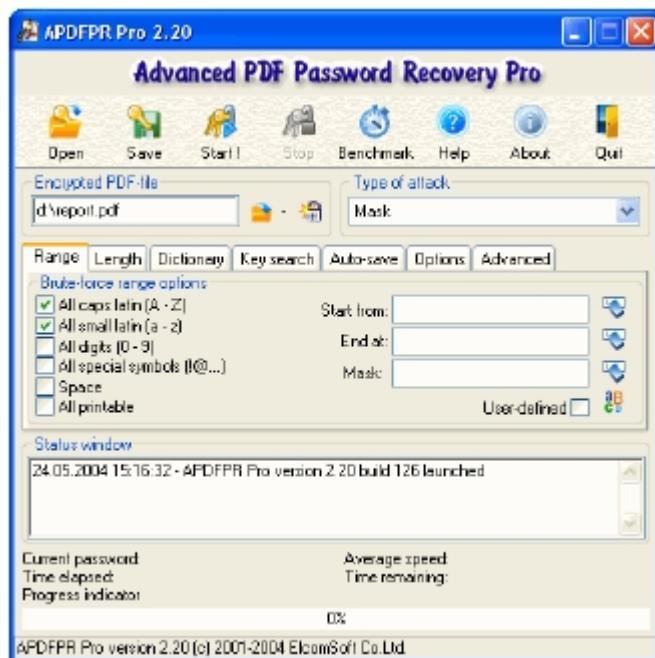
- Passware Kit (<http://www.lostpassword.com/>)
- ElcomSoft Password Recovery Bundle (<http://www.elcomsoft.com/>)
- LastBit Password Recovery (<http://lastbit.com/>)
- AccessData Password Recovery Toolkit (PRTK)
(<http://accessdata.com/>)
- Multi Password Recovery Portable (<http://passrecovery.com/>)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



Passware Password Recovery Kit



Elcomsoft Password Recovery Bundle



UNIVERSITÀ
DI PARMA

LastBit Password Recovery

>PasswordTools.com

PasswordTools

Home Support Order Help Exit

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

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

 Click here to Recover Document Password

 Information

Other Password Related Software:

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

Tools:

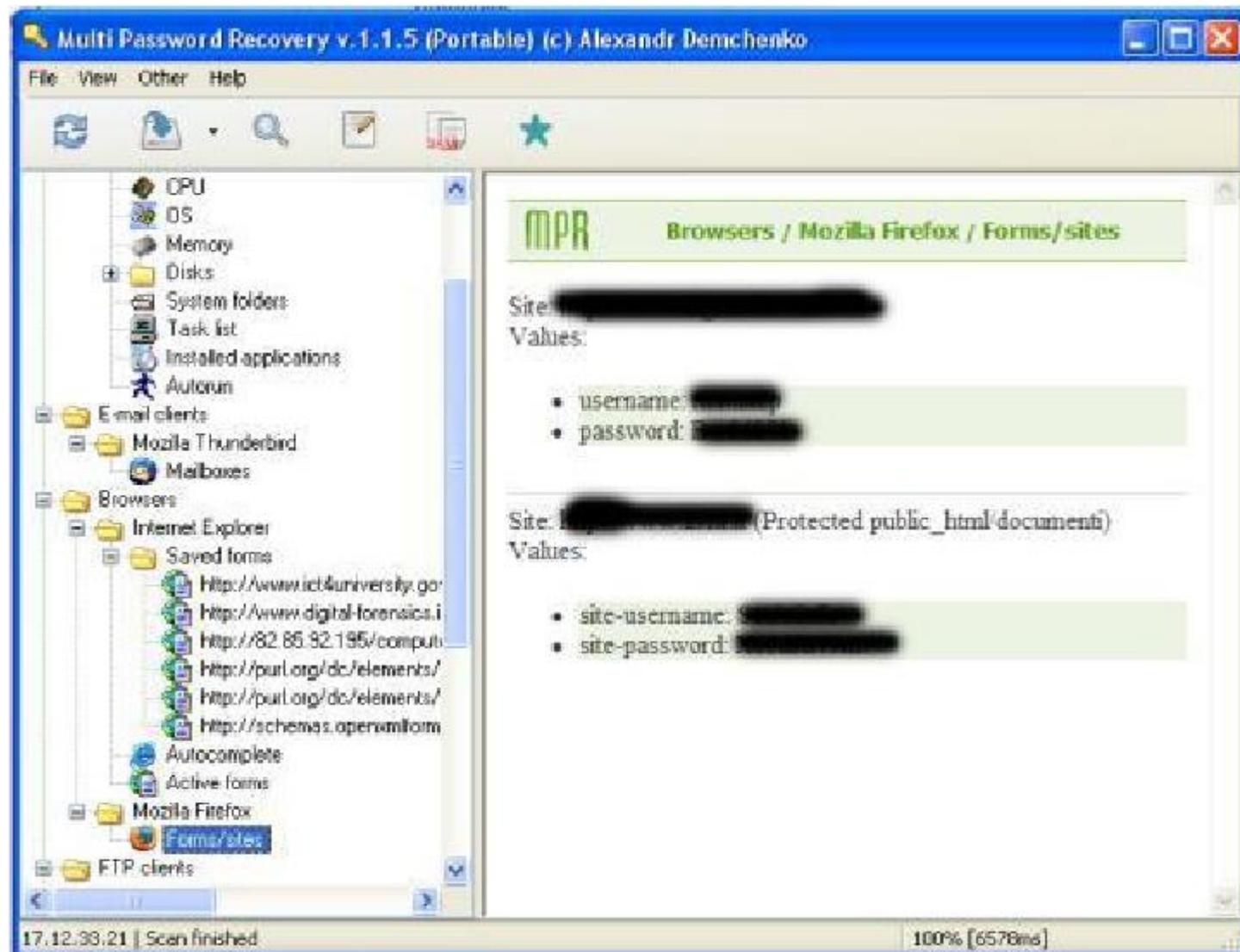
- Password Analyzing Service
estimate recovery password time and check if your password is weak.
- DiscoverIt!
find out what Windows hides behind asterisks.
- Find Password Protected Documents

Articles:

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

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

Multi Password Recovery Portable



Other interesting...

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



Analyzing CD/DVD

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

Operating steps

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

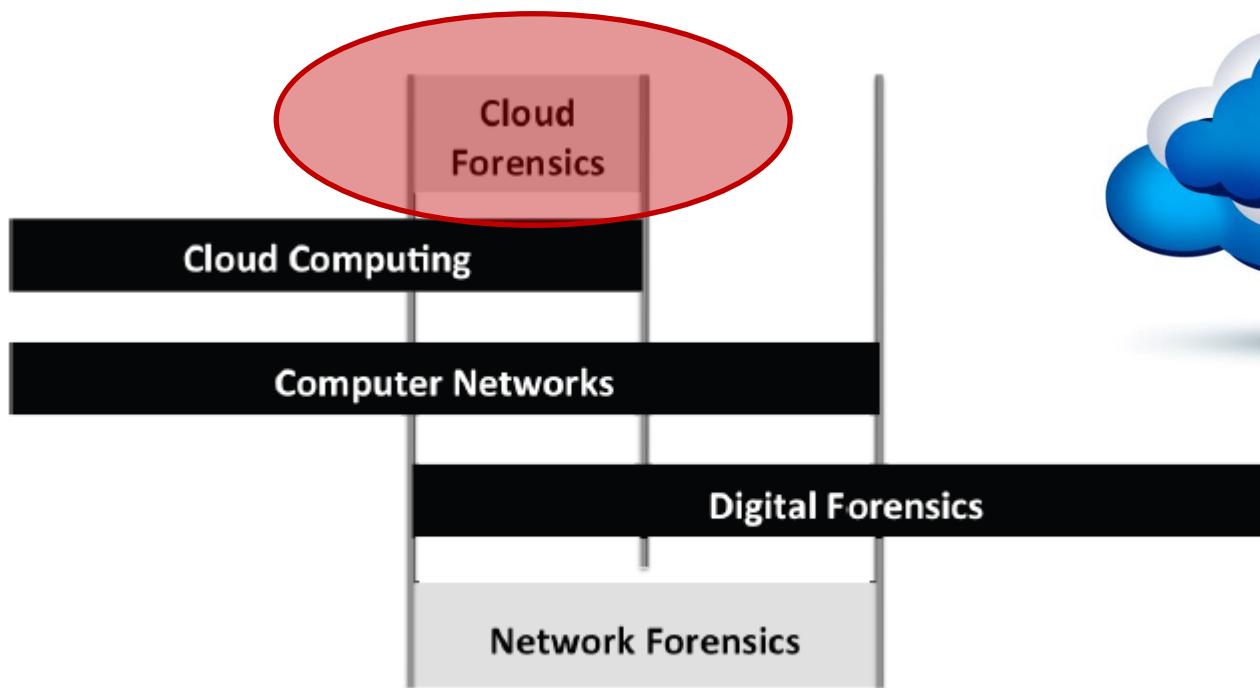


Evaluation and presentation

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

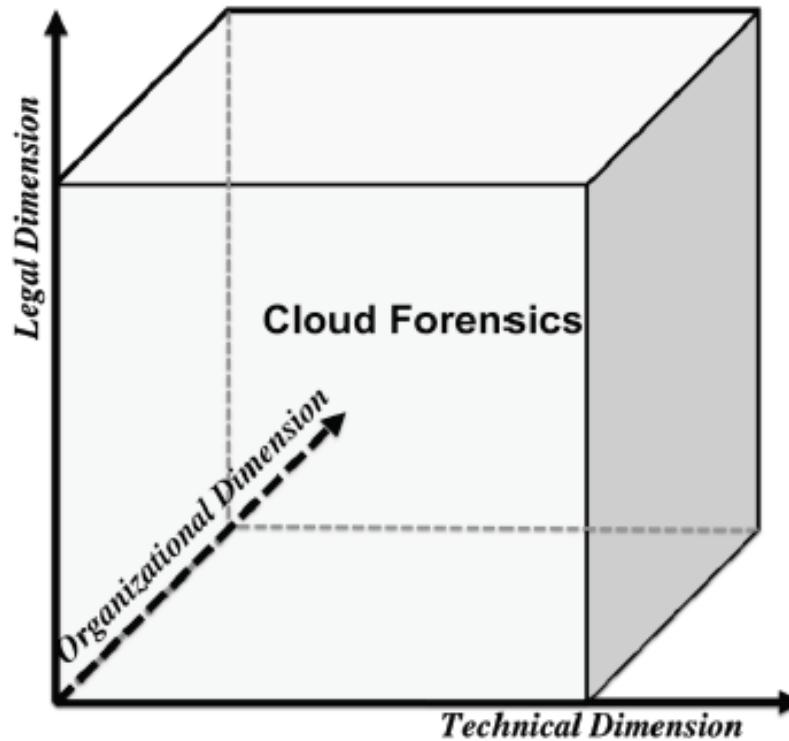
Cloud Forensics

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



3 Dimension

The 3 dimensions in Cloud Forensics



Tecnical

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

- **Forensics Data Collection** – The Cloud Forensics Collection is composed by the overall process of identification, collection, recording and acquisition of forensics data from those possible and available data sources into the Cloud. Data may be found both on Client and Provider (infrastructure) sides.

Each one of cloud's services model has got different tools and data collection procedures. There is not a standard sequence, as it happens in Computer Forensics: ahead those «easy to run» data (*RAM image*) are processed, then data with lower reliability. The collection's process must run data integrity procedures.

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



Tecnical/1

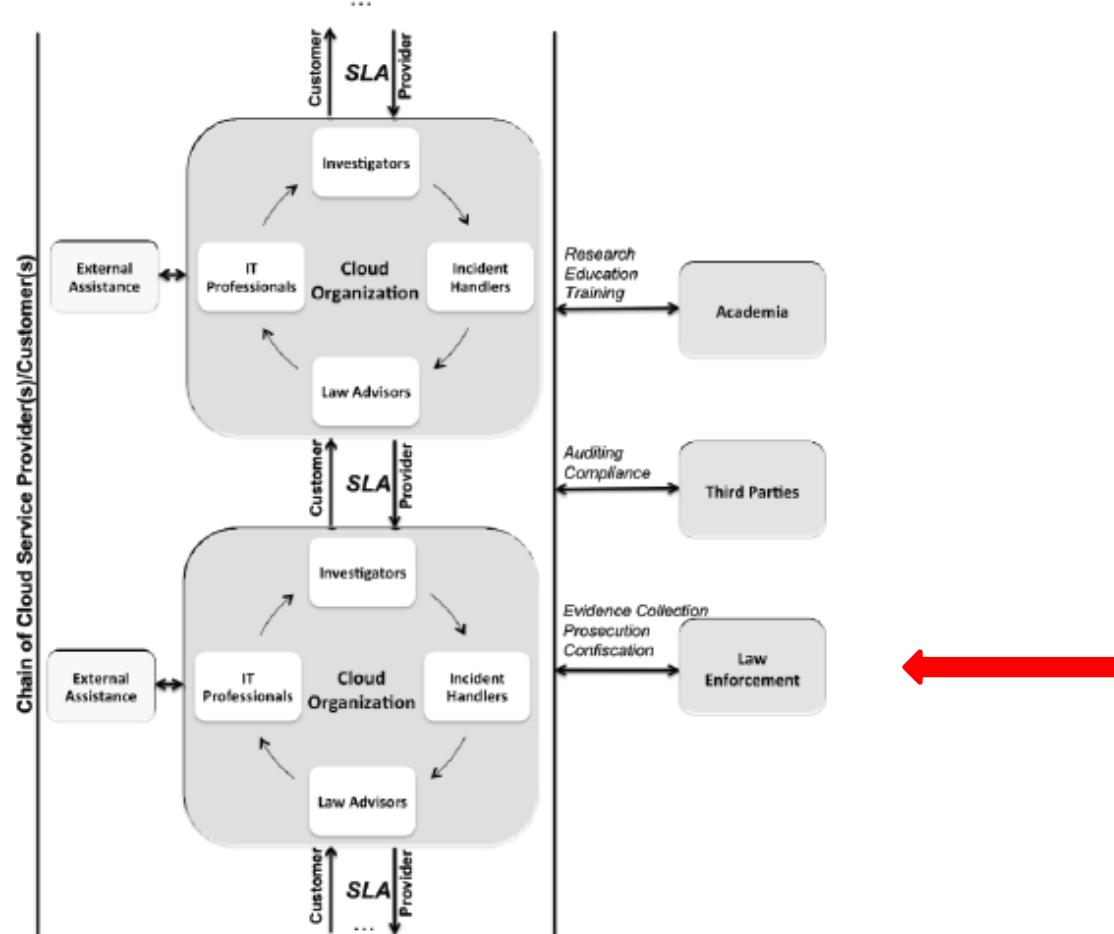
It is **not so** easy to develop those procedures and tools that must be used in order to physically identify the needed data into a given timeframe; then tracing the data itself (into a given timeframe) taking into consideration domestic jurisdictions.

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



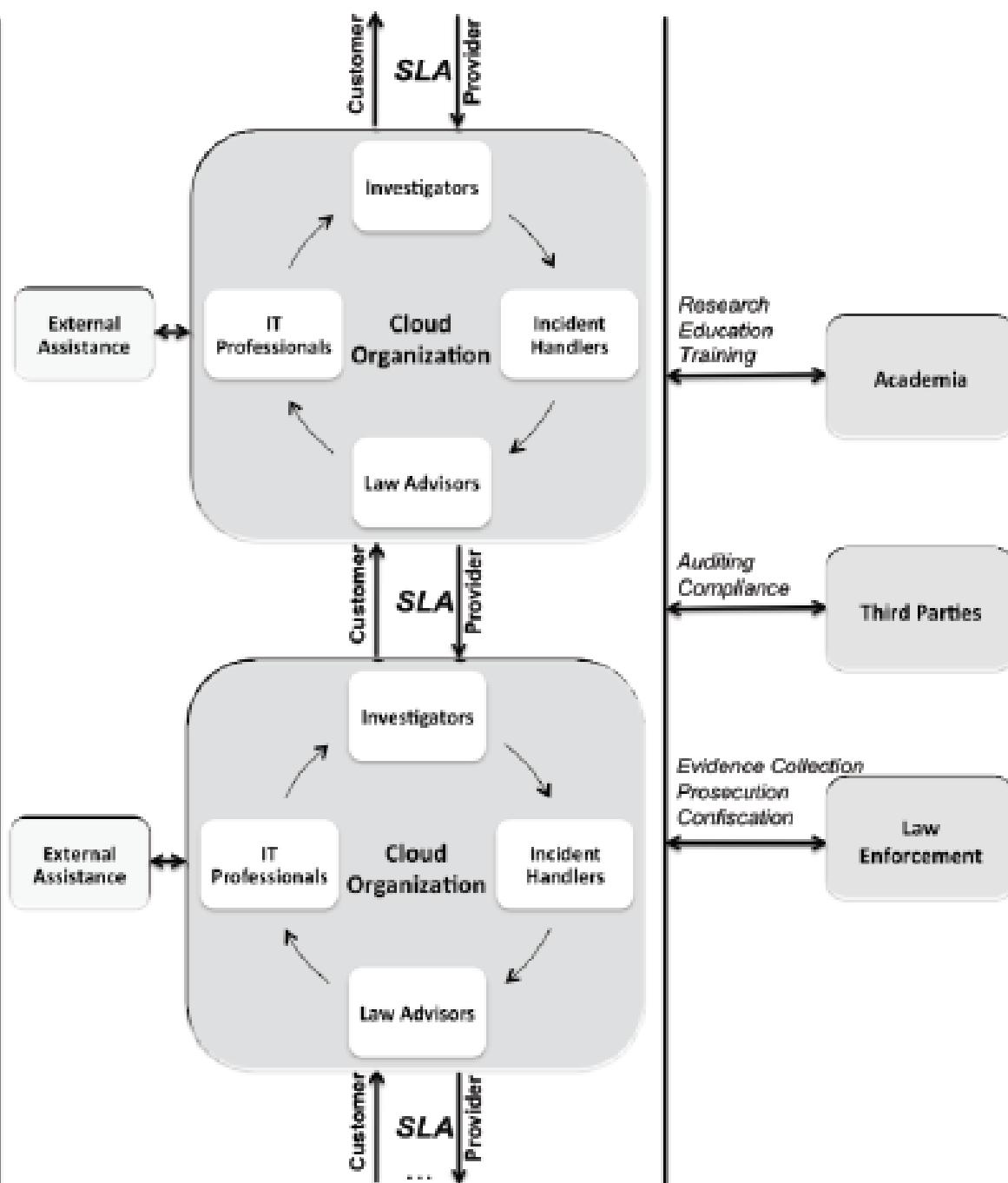
Organizational

Organizational dimension



Organizational dimension

Chain of Cloud Service Provider(s)/Customer(s)



Organizational

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

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

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

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

Legal

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

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

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

Legal dimension

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

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

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

Cloud information

From a investigative level, information can be found:



Cloud information/1

SERVER SIDE:

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

- ✓ Where the heck will we seize the data????
Or, «block» the account (access mode)??? Despite being the *only sure thing I have, when I've got one!!!*.
YOU CANNOT.

CLIENT SIDE:

- ✓ Yeah, I may run a «live analysis».... If credentials are given out (?)

- ✓ When lucky, I may be able to find out access credentials and configuration templates saved «in clear text» (and/or cached) rather than into local backups..

Methodologies

Data transit

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

Methodologies/1

- **Network analysis:** acquiring the whole network traffic of the workstation itself – when this is applicable (**NETWORK DUMP**). A hash printing must be done to the acquired files.
- **Log Analysis:** acquiring and examining log files from the firewall, antivirus, application programs, possible cache and temporary directories files from the clients.
- **Screenshots:** (not only that...)
 - ✓ Desktop screenshots;
 - ✓ Possible screenshots of running programs;
 - ✓ Reading out and commenting in «live mode».
- **Reporting:**
 - ✓ Each single activity must be reported in the clearest way as for Digital Forensics.
 - ✓ Even more carefully, giving Cloud Forensics a very-recent science, lacking of punctual lawful practices.
 - ✓ Last but not least, a final reporting is mandatory in order to supply validity and allow legal experts to fit it into a given and correct scenario.

Access?????

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



The Cloud -----

Access credentials:

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



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

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](https://www.academia.edu/7768658/Actionable_Evidence_in_the_Wake_of_Anti-Forensics_on_Windows_8_Systems)
- * <http://ac.els-cdn.com/S1877050914012113/1-s2.0-S1877050914012113-main.pdf? tid=fb848980-7551-11e4-8648-0000aacb35e&acdnat=1416995750 8ff475d9db450e5724b169e154496169>
- * <https://www.guidancesoftware.com/products/Pages/tableau/products/duplicators.aspx>
- * http://www.cftt.nist.gov/tool_catalog/index.php
- * <https://digital-forensics.sans.org/summit-archives/2012/practical-use-of-cryptographic-hashes-in-forensic-investigations.pdf>
- * <http://www.ltr-data.se/opencode.html/#lDisk>
- * <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)

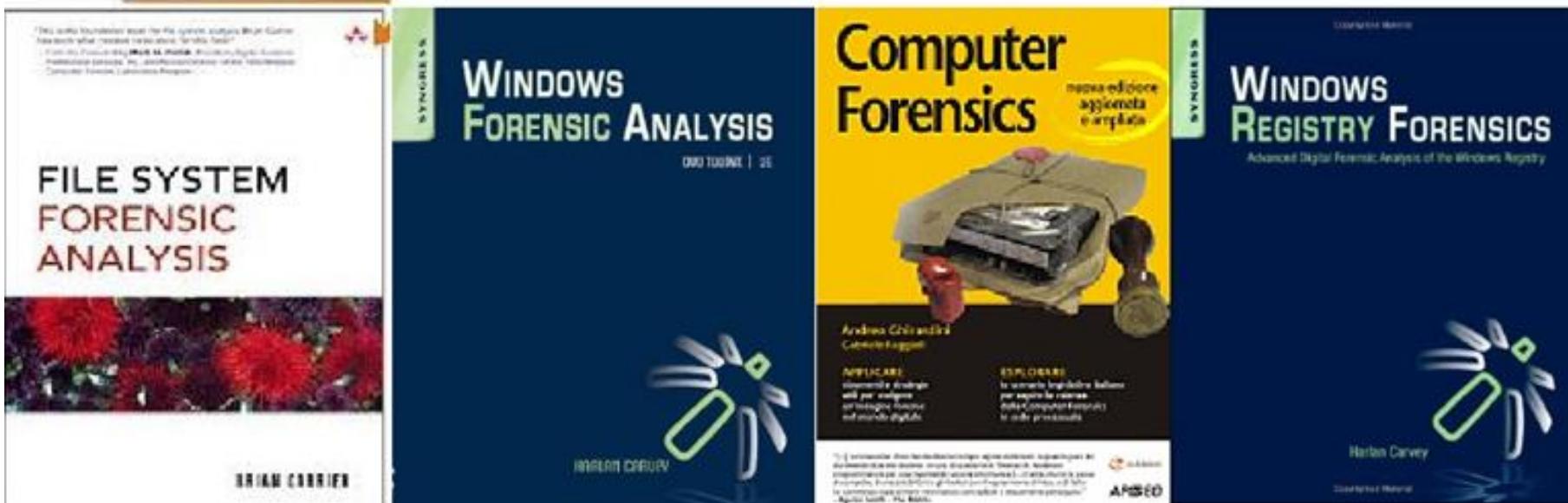
<http://www.cftt.nist.gov>



UNIVERSITÀ
DI PARMA

Books

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



sg@security-brokers.com

SecurityBrokers

GLOBAL CYBER DEFENSE & SECURITY SERVICES



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