

Computer Forensics

Marzaioli Alessio
0522500081
alexmarz@hotmail.it

Pisano Francesco
0522500137
aslan84@hotmail.it

Indice – Parte I

- **Introduzione alla Computer Forensics**
 - Una definizione
 - Il processo di Computer Forensics
- Identificazione
- Conservazione
 - Tools per la copia bit stream
 - Write Blocker Sw su Linux
 - Write Blocker Hw
 - Verifica dei dati
 - Collisioni sulle funzioni hash
 - Scelta della giusta funzione di hash
 - Duplicatori Hw
- Analisi
 - Investigation Tools: Caratteristiche generiche
- Presentazione

Dalla digital forensics alla computer forensics

■ Digital forensics: Una definizione

“è la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico al fine di essere valutato in un processo giuridico e studia, ai fini probatori, le tecniche e gli strumenti per l'esame metodologico dei device digitali.”

Dalla digital forensics alla computer forensics



- Pertanto la computer forensics è un ramo della digital forensics riguardante le prove legali che è possibile ricercare in un computer ed i suoi dispositivi di memorizzazione

E' una scienza in grande crescita...

- Nasce nel 1984 nei laboratori dell' FBI;
- Esistono molte organizzazioni che se ne occupano oggi:
 - Il Digital Forensic Research Workshop (DFRWS), lo European Network of Forensic Science Institute - Forensic Information Technology Workgroup (ENFSI-FITWG), lo Scientific Working Group on Digital Evidence (SWGDE), il National Institute of Standards and Technology - Computer Forensic Tool Testing (NIST-CFTT) e altri!

Hanno lavorato SOPRATTUTTO per la definizione della materia e successivamente nella ricerca di strumenti validi per la digital forensics.

Il processo di computer forensics

E' suddiviso in 4 fasi:

- Identificazione;
- Conservazione;
- L'Analisi;
- Presentazione dei risultati.

Indice – Parte I

- **Introduzione alla Computer Forensics**
 - Una definizione
 - Il processo di Computer Forensics
- **Identificazione**
- **Conservazione**
 - Tools per la copia bit stream
 - Write Blocker Sw su Linux
 - Write Blocker Hw
 - Verifica dei dati
 - Collisioni sulle funzioni hash
 - Scelta della giusta funzione di hash
 - Duplicatori Hw
- **Analisi**
 - Investigation Tools: Caratteristiche generiche
- **Presentazione**

Identificazione

- Individuazione dei potenziali contenitori di informazioni:
 - Desktop e laptop computer;
 - Dispositivi di storage connessi in rete;
 - Server;
 - CD/DVD;
 - Memorie USB, SD,MS/PRO-MMC,XD e così via;
 - Fotocamere digitali, PDA, smartphone, ebook reader e cellulari;
 - Lettori MP3 e registratori digitali.

Indice – Parte I

- Introduzione alla Computer Forensics
 - Una definizione
 - Il processo di Computer Forensics
- Identificazione
- Conservazione
 - Tools per la copia bit stream
 - Write Blocker Sw su Linux
 - Write Blocker Hw
 - Verifica dei dati
 - Collisioni sulle funzioni hash
 - Scelta della giusta funzione di hash
 - Duplicatori Hw
- Analisi
 - Investigation Tools: Caratteristiche generiche
- Presentazione

Conservazione

Consiste nell'acquisizione bit stream del device.

- Fondamentale mantenere inalterato il contenuto del device per permettere la ripetibilità dell'esame
 - Legge n° 48/2008 del Consiglio Europeo
“..adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.”
- Sconsigliato, dunque, lavorare **direttamente** sul dispositivo!

Tools e comandi per la copia bit stream

- Per windows ne esistono diversi:
BitStream, SafeBack ma anche dd per windows!
- Per Linux vari tools nelle distribuzioni forensi:
Air, Ddrescue, Dcfldd, dc3dd e diverse varianti del classico comando dd

Write Blocker

- Garantisce un blocco dell'accesso in scrittura, per mantenere l'integrità della prova
- Esistono due differenti metodologie per garantire il write blocking:
 - Write blocker software;
 - Write blocker hardware.

Write Blocker Software

- Agisce sull'operazione di mounting dell'hard disk da parte del sistema operativo;
- A seconda del sistema operativo utilizzato si possono adottare opportuni accorgimenti per consentire un accesso in modalità di sola lettura.

Linux.. ti semplifica la vita

- In ambiente Linux i volumi possono essere montati direttamente in modalità read only.
- Le distribuzioni per analisi forense montano (tramite il comando mount) per default un volume in read only.

Write Blocker Software: Vantaggi

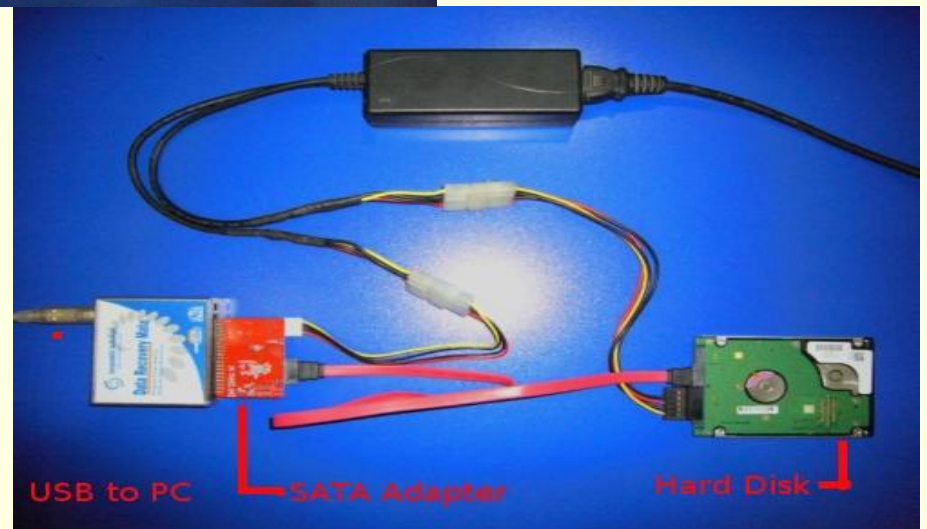
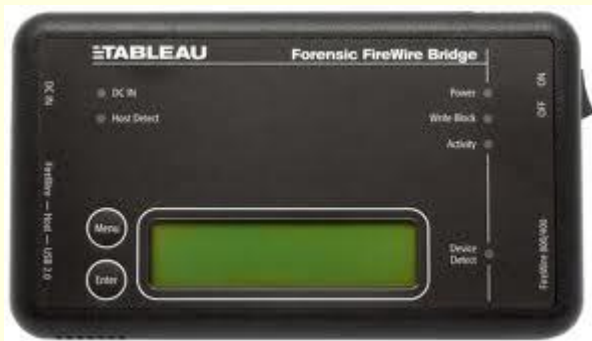
La scelta di un write blocker software è indubbiamente economica, perché non richiede l'acquisto di particolari dispositivi.

Ovviamente il digital forensier deve testare costantemente la validità di questa metodologia con la nascita e lo sviluppo dei nuovi standard di connessione.

Write Blocker Hardware

- Un write blocker hardware è un dispositivo fisico che viene posto tra l'hard disk e la macchina di acquisizione forense. Questi dispositivi sono anche più comprensibili per interlocutori non tecnici.
- Integrano diverse tipologie di interfaccia (IDE, SATA, SCSI, USB, Firewire ecc.) e vengono collegati alla macchina di acquisizione tramite connessione USB o Firewire.
- Ovviamente esistono anche strumenti di write blocking per altri tipi di risorse, come i card reader forensi, ecc.

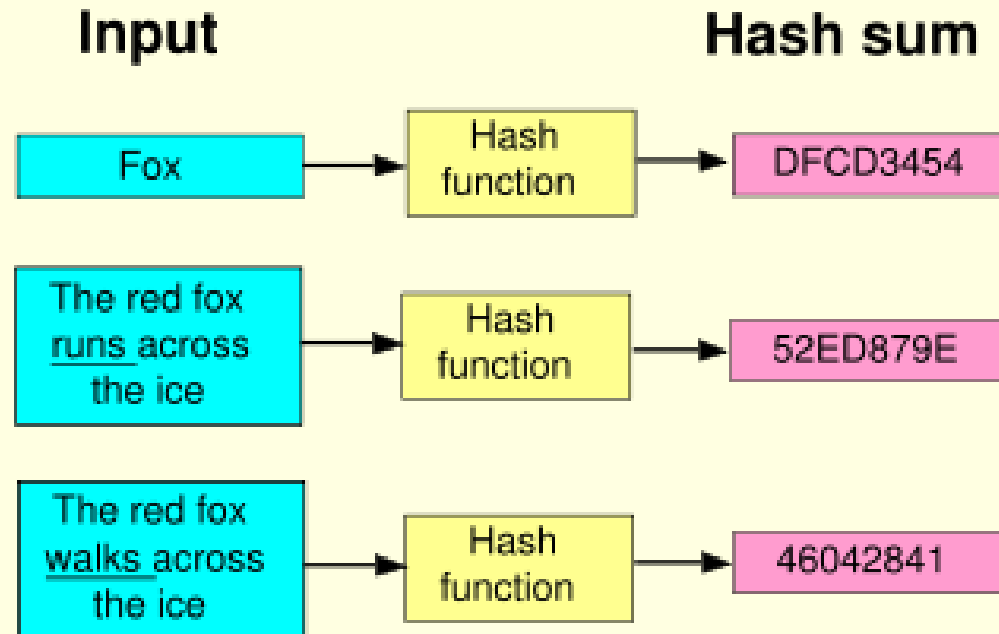
Write Blocker: Qualche esempio



Verifica

- L'ultimo passo della conservazione è la verifica della congruità del dato copiato. Esistono due tipi di verifica dei dati:
 - Verifica bit a bit -> tempi di elaborazione elevati;
 - Funzioni hash.

Funzioni Hash



- Due tipi di funzioni hash:
 - MD5 (Message Digest Algorithm);
 - SHA-0, SHA-1, SHA-2 (Secure Hash Algorithm).

Scelta dell'algoritmo di hash...1

■ L'hash MD5 e le collisioni

- Nel 2005 da Xiaoyun Wang e Hongbo Yu individuarono due sequenze diverse con stesso valore di hash;
- Sono stati scritti due file PostScript diversi con stesso valore hash;
- Possibilità di costruire due programmi diversi con stesso valore di hash.

■ L'hash SHA-1 e le collisioni

- Xiaoyun Wang, Yiqun Lisa Yin, e Hongbo Yu sono riusciti a trovare una tecnica che è 2000 volte più veloce dell'attacco a forza bruta per individuare una collisione;

Scelta dell'algoritmo di hash...2

Due possibili soluzioni:

- Scegliere un algoritmo di hash più “sicuro”;
 - NIST (National Institute of Standard and Technology) ha proposto diversi standard.
- Applicare un doppio hash (MD5 e SHA-1) rendendo di fatto impossibile una collisione.

Duplicatori Hardware

- Utilizzati per la creazione di una copia forense dell'hard disk originale;
- Dispositivi che integrano funzionalità di write blocking del supporto originale, duplicazione dei dati su un altro supporto e valutazione della correttezza e completezza del processo attraverso opportuni strumenti di validazione (nella maggior parte dei casi utilizzando un algoritmo di hash come MD5, SHA1 o entrambi);
- Il vantaggio: maggiore transfer rate durante la copia.

Duplicatori Hardware



Indice – Parte I

- Introduzione alla Computer Forensics
 - Una definizione
 - Il processo di Computer Forensics
- Identificazione
- Conservazione
 - Tools per la copia bit stream
 - Write Blocker Sw su Linux
 - Write Blocker Hw
 - Verifica dei dati
 - Collisioni sulle funzioni hash
 - Scelta della giusta funzione di hash
 - Duplicatori Hw
- Analisi
 - Investigation Tools: Caratteristiche generiche
- Presentazione

Analisi

Dopo l'acquisizione dei dati si passa all'analisi
Si utilizzano tools in grado di fornire l'analisi su:

- Dati volatili;
- File di swap;
- File logici;
- File di registro delle configurazioni;
- E-mail;
- Log delle applicazioni e di sicurezza;
- File temporanei;
- Log di sistema;
- Spazio libero;
- Cache del browser;
- History file;
- File cancellati.

Alcuni software per l'analisi

- The Sleuth Kit/ Autopsy;
- La distribuzione Helix;
- Guidance Software EnCase;
- Access Data FTK.

Indice – Parte I

- Introduzione alla Computer Forensics
 - Una definizione
 - Il processo di Computer Forensics
- Identificazione
- Conservazione
 - Tools per la copia bit stream
 - Write Blocker Sw su Linux
 - Write Blocker Hw
 - Verifica dei dati
 - Collisioni sulle funzioni hash
 - Scelta della giusta funzione di hash
 - Duplicatori Hw
- Analisi
 - Investigation Tools: Caratteristiche generiche
- Presentazione

La presentazione dei risultati

“Contrariamente a quanto si possa pensare la mia idea è che il risultato di una indagine tecnica poggia al 50% sulla pura attività tecnica ed al rimanente 50% sulla professionalità, preparazione e capacità espositiva di chi porta tali risultati nell'ambito dibattimentale”

Marco Mattiucci

La presentazione deve essere..

- *Sintetica*: dato che non necessita di riportare eccessivi particolari tecnici dell'analisi ma solo ciò che interessa dal punto di vista giuridico.
- *Semplificata*: colui che legge e valuta l'esito è di principio un fruitore inesperto nel settore informatico e quindi, nell'ipotesi che sia possibile, bisogna eliminare terminologie non consuete e spiegare a livello elementare quanto rilevato.
- *Asettica*: non deve contenere giudizi personali dell'operatore né tanto meno valutazioni legali sulle informazioni rilevate a meno che tali considerazioni non siano state espressamente richieste.

Indice - Parte II

- Ambiente Hardware ed Attività dell'indagato
 - Ambiente hardware/software
 - Attività dell'indagato
- Identificazione
 - Il nostro caso
- Conservazione
 - Conservazione tramite Write Blocker
 - Write Blocker Tableau
 - GuyMager
 - Air 2.0
 - Duplicazione su supporto ottico
- Analisi
 - Attività di analisi
 - Strumenti utilizzati
- Incidenti di percorso
- Conclusioni

Ambiente hardware/software

- La nostra macchina forense:
 - AMD athlon 1.1 GHz;
 - 1 GB RAM(400 MHz);
 - HDD1 40 GB;
 - HDD2 20 GB.
- Una distribuzione forense di Linux
 - Caine 2.0;
 - Installata su HDD1.
- Write Blocker;
- 5 supporti ottici (DVD).



Attività dell'indagato: Sanitizzazione (Wiping) dell'hdd con air 2.0.0

The screenshot displays the AIR 2.0.0 interface, which is used for automated image and restore operations. The main window is titled "AIR 2.0.0 - Automated Image & Restore - 2010-02-17". It features a "File" menu and a "Help" button. The configuration section includes fields for "Source device/file:" (set to /dev/zero) and "Destination device/file:" (set to /dev/sdb). Both "Source Block Size:" and "Dest. Block Size:" are set to 32768. There are checkboxes for "Custom Block Size:" which are currently unchecked. The "Options" section includes "Compression:" (None), "Hash 1:" (md5), "Hash 2:" (sha1), "Verify:" (Yes), and "Use DC3DD" (checked). Other options include "Split Image" (unchecked), "Cryptcat" (unchecked), "DD Count:" (empty), "Skip (Input):" (0), "Seek (Output):" (0), "Conv:" (noerror, sync), and "iflag:" (direct). A "Key:" field contains phi_1.618. The "Connected devices" section shows icons for SDA, SDB, ZERO, NULL, and NET. At the bottom, there are "Start", "Stop", and "Exit" buttons, and a "Show Status Window..." button. The status bar at the bottom indicates "Working... SOURCE = /dev/zero DEST = /dev/sdb".

The "AIR Session Status" window is open, showing the "Session Log" and "Bitstream Data". The "Session Log" contains the following text:

```
command line: dc3dd status=noxfer of=/dev/sdb seek=0 obs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
sector size: 512 (assumed)
warning: sector size not probed, assuming 512
dc3dd 6.12.3 started at 2002-10-29 07:51:28 +0100
command line: dc3dd hash=md5,sha1 hashlog=/tmp/hash.log status=noxfer if=/dev/ze
ro skip=0 conv=noerror,sync iflag=direct ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
sector size: 512 (assumed)
```

The "Bitstream Data" section shows the following progress and throughput information:

Progress	Avg. Throughput
3790.00MB (3.70GB)	23.54MB/sec
3800.00MB (3.71GB)	23.46MB/sec
3820.00MB (3.73GB)	23.44MB/sec
3830.00MB (3.74GB)	23.35MB/sec

At the bottom of the "AIR Session Status" window, there are buttons for "Add Comment to Log...", "Clear...", "Save...", and "Close".

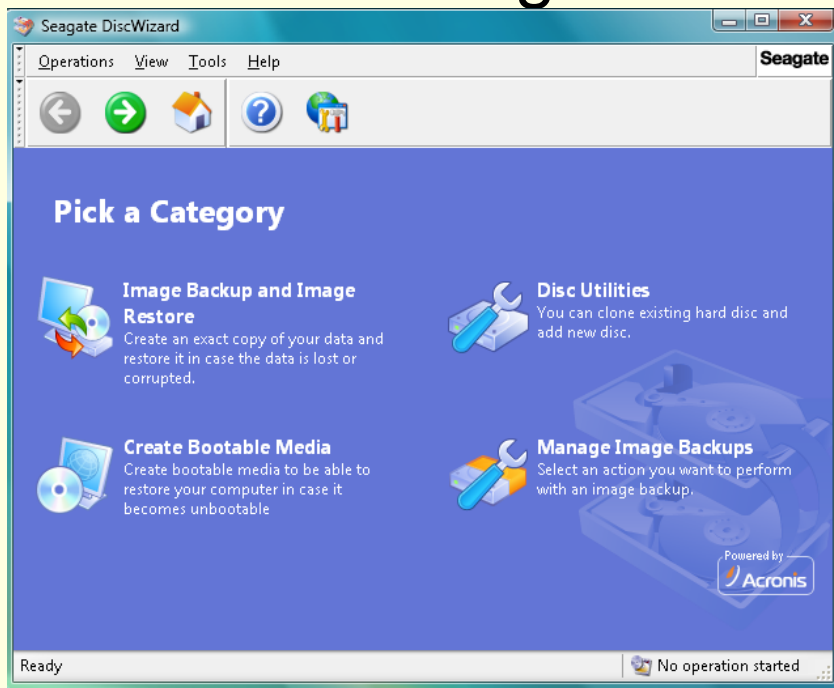
Caine Interface

Attività dell'indagato: Software utilizzati

- Seagate DiscWizard;
- TrueCrypt;
- Acronis True Image Trial (Disco di boot);
- OpenOffice;
- AcrobatReader.

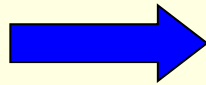
Seagate DiscWizard

- Versione Free di Acronis TrueImage per hdd Maxtor/Seagate



TrueCrypt

- Software Free per creazione di partizioni ed archivi criptati



L'attività dell'indagato



- Navigazione di un profilo facebook;
- Controllo della propria casella di posta ed invio di una mail;
- Download di foto da facebook;
- Download di video da pendrive;
- Visualizzazione di foto e video;
- Apertura di un documento pdf da browser;
- Creazione di una cartella crittografata con RSA a 1024bits;
- Creazione di una cartella nascosta;
- Creazione di una partizione virtuale crittografata con inserimento di dati.

Il nostro proposito:

Malfattore, Ti prenderò!



Indice - Parte II

- Ambiente Hardware ed Attività dell'indagato
 - Ambiente hardware/software
 - Attività dell'indagato
- Identificazione
 - Il nostro caso
- Conservazione
 - Conservazione tramite Write Blocker
 - Write Blocker Tableau
 - GuyMager
 - Air 2.0
 - Duplicazione su supporto ottico
- Analisi
 - Attività di analisi
 - Strumenti utilizzati
- Incidenti di percorso
- Conclusioni

Identificazione

- Abbiamo sequestrato un hard disk (S/N WMA6K3300935)

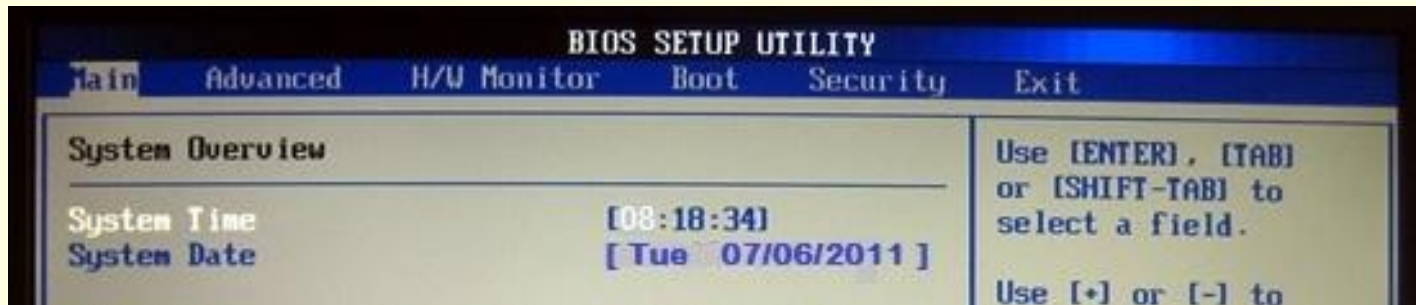


Indice - Parte II

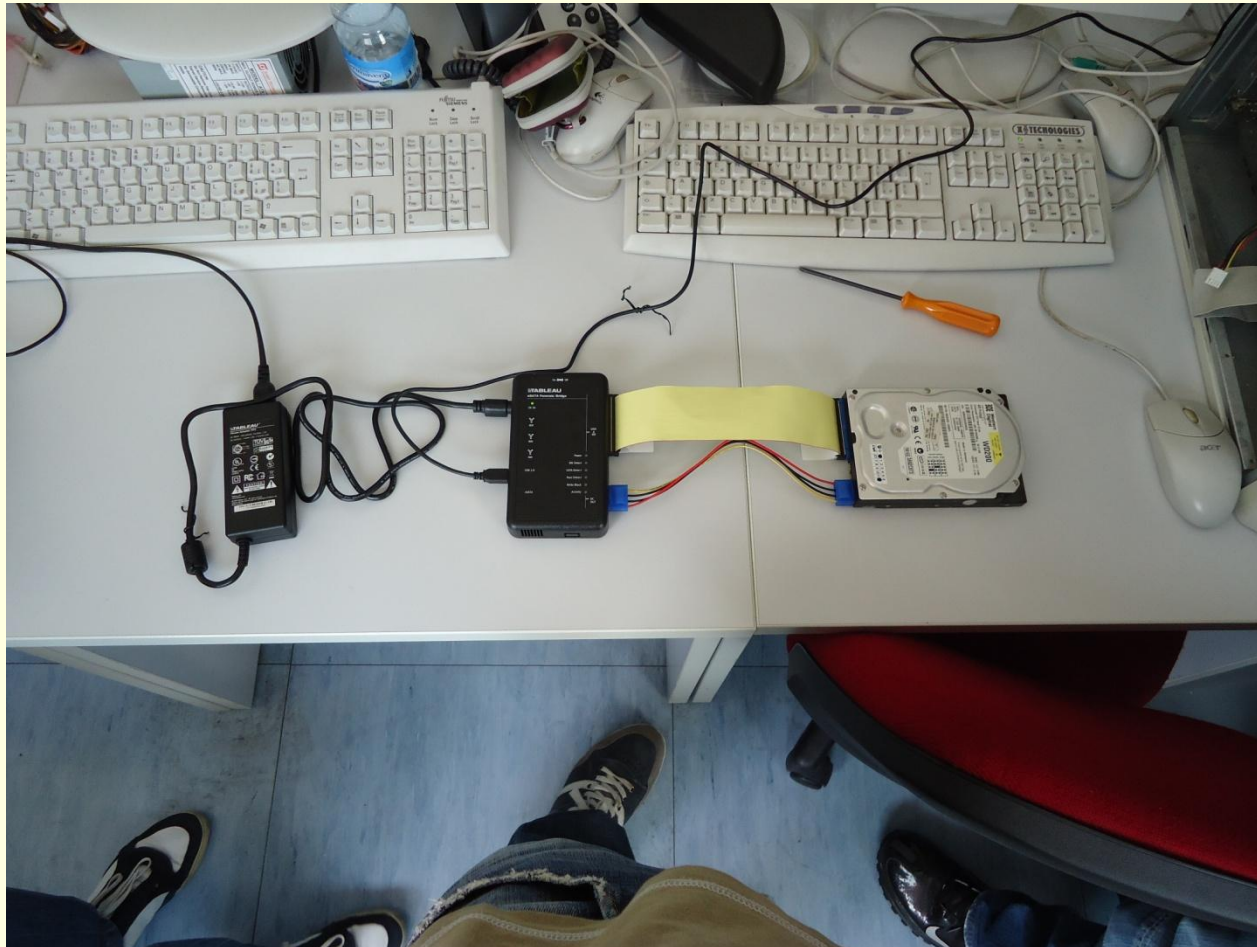
- Ambiente Hardware ed Attività dell'indagato
 - Ambiente hardware/software
 - Attività dell'indagato
- Identificazione
 - Il nostro caso
- Conservazione
 - Conservazione tramite Write Blocker
 - Write Blocker Tableau
 - GuyMager
 - Air 2.0
 - Duplicazione su supporto ottico
- Analisi
 - Attività di analisi
 - Strumenti utilizzati
- Incidenti di percorso
- Conclusioni

Sincronizzazione data/ora

- Prima di addentrarci nella parte che riguarda la copia forense dell'hd, è opportuno sincronizzare la data e l'ora della macchina in esame, accedendo al bios.



Conservazione: Utilizzo del write blocker



Write Blocker Tableau T35es

- Host side;
- One eSATA Signal Connector;
- FireWire Two 9-pin FireWire800 (1394B);
- One 6-pin FireWire400 (1394A);
- One USB Mini-B (5 pin, USB2.0 high/full/low speed);
- DC Input DC In: 5-pin Mini-DIN connector for use with Tableau TP2 power supply;
- Device side;
- SATA Signal Connector;
- IDE Signal Connector DC Output 4-pin male "drive power" connector.



Write Blocker e seriali

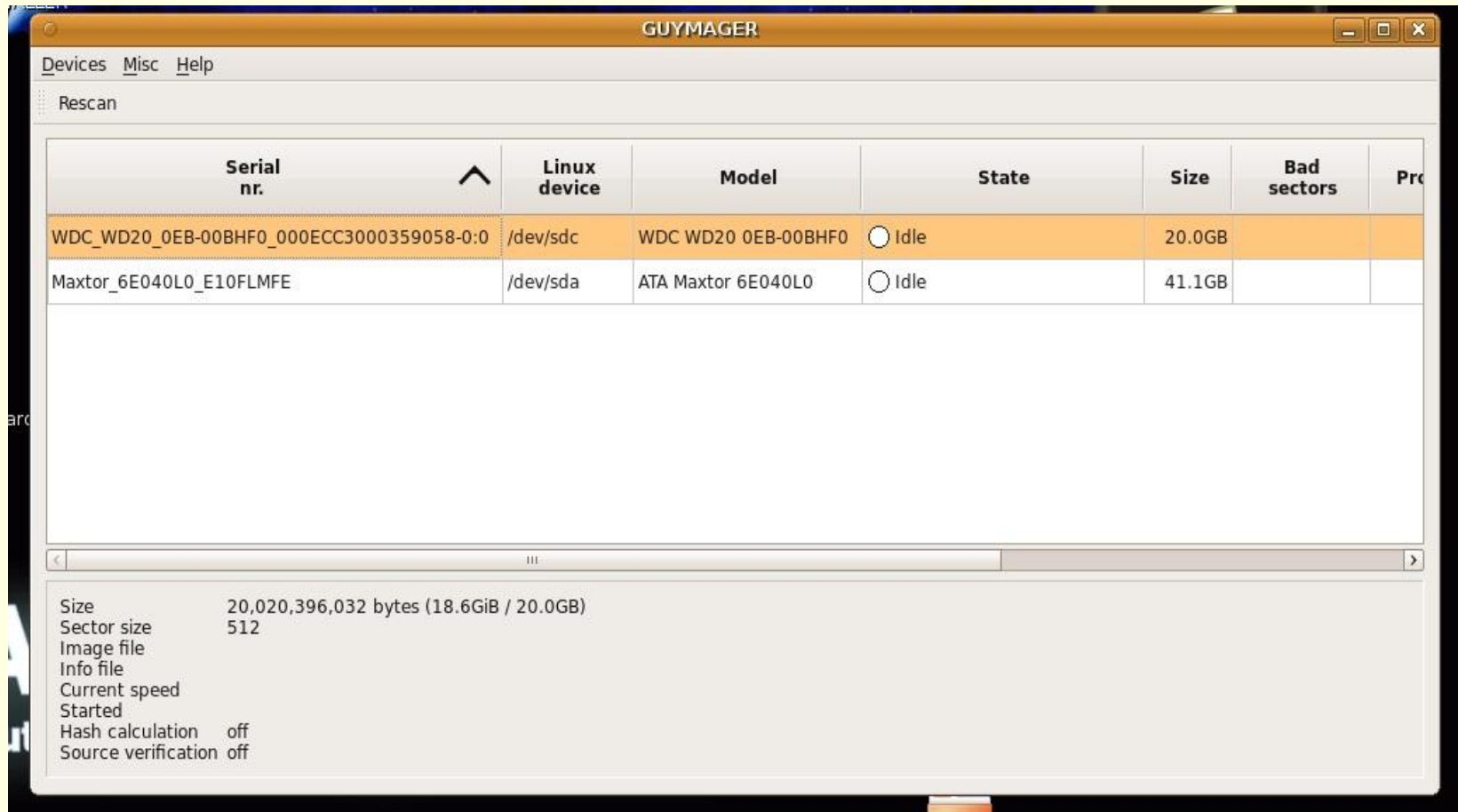
Serial nr.	Linux device	Model	State	Size	Bad sectors	Pro
WDC_WD20_0EB-00BHF0_000ECC3000359058-0:0	/dev/sdc	WDC WD20 0EB-00BHF0	Idle	20.0GB		

- Il seriale dell' hdd è diverso!
- Soluzioni:
 - Più facile ma pericolosa: Collegare direttamente l'hdd alla macchina forense;
 - Utilizzare Tableau Disk Monitor: Fornisce informazioni del device come se fosse collegato direttamente alla macchina.

Conservazione: Guymager

- Guymager è un tool grafico per l'acquisizione bit stream di un device digitale focalizzato principalmente su alcune caratteristiche:
 - L'interfaccia user-friendly
 - La possibilità di utilizzare tecniche avanzate per l'acquisizione a velocità superiore (multi thread, pipeline)
 - La possibilità di sfruttare le architetture multi processore
 - Completamente open source

Guymager: Selezione dei dispositivi



Guymager: Formati supportati

- *.dd, comando UNIX per effettuare copia e conversione dei file (*cit. Wikipedia*);
- *.ewf, utilizzo della libreria libewf, è alla base dei formati creati da EnCase;
- *.aff, è un formato per la memorizzazione di immagini di dischi e relativi metadati forensi, supportato da Sleuthkit e Autopsy.

Guymager: Schermata di acquisizione

The screenshot shows a dialog box titled "Acquisition parameters for /dev/sda". It is divided into three main sections: "File format", "Destination", and "Hash computation".

File format

- Linux dd raw image (file extension .dd)
- Expert Witness Format, sub-format Encase5 (file extension .Exx)
- Advanced forensic image (file extension .aff)

Case number:

Evidence number:

Examiner:

Description:

Notes:

Destination

Image directory:

Image filename (without extension):

Info filename (without extension):

Hash computation

- Calculate hashes (MD5 and SHA-256)
- Re-read source after acquisition for verification (takes twice as long)

Buttons:

Air 2.0.0

- Air 2.0.0, come Guymager, è un tool grafico che permette l'acquisizione di un device digitale fornendo una serie di servizi aggiuntivi:
 - comprimere l'immagine con gzip/bzip2;
 - dividere l'immagine in sotto immagini (split);
 - lavorare in una rete TCP/IP tramite netcat/cryptcat;
 - verificare l'immagine con hash MD5,SHA1/256/384/512;
 - la possibilità di fare una sanitizzazione (wiping) del disco.

Air 2.0.0: Interfaccia grafica

Taglia input

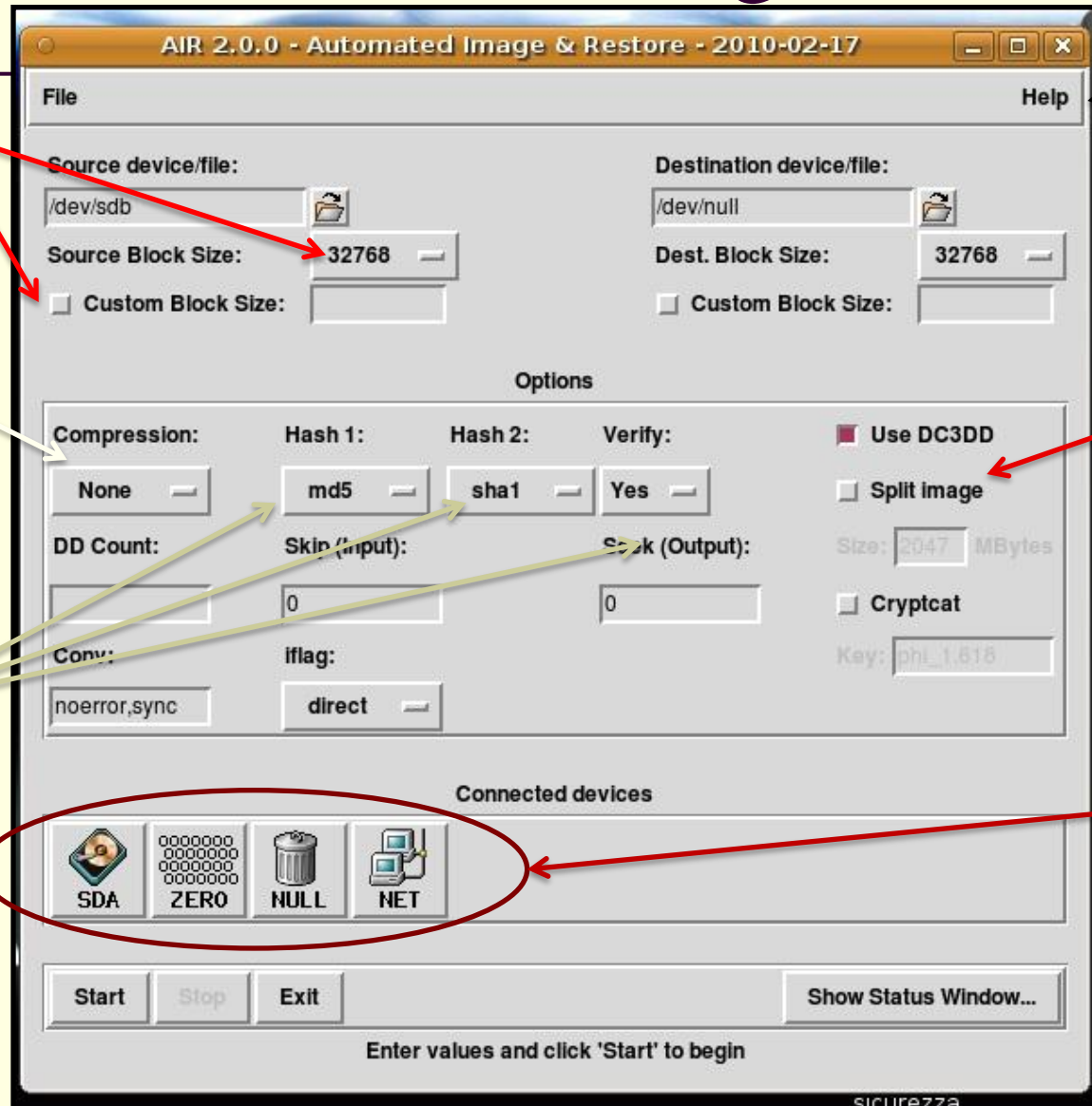
Copressione dati

Codifica

For more info

Taglia file generati

Selezione dei vari dispositivi



Conservazione: Log restituito da Air

```
File Modifica Formato Visualizza ?

Start DC3DD (md5 sha1): Tue Jun 7 13:07:10 CEST 2011
Hash will be calculated on /dev/sdb.

Command-line:
dc3dd hash=md5,sha1 hashlog=/tmp/hash.log status=noxfer if=/dev/sdb skip=0 conv=noerror,sync iflag=direct ibs=32768 2>> /usr/local/share/air/logs/air.image.log | air
warning: sector size not probed, assuming 512
dc3dd 6.12.3 started at 2011-06-07 13:07:10 +0200
command line: dc3dd hash=md5,sha1 hashlog=/tmp/hash.log status=noxfer if=/dev/sdb skip=0 conv=noerror,sync iflag=direct ibs=32768
compiled options: DEFAULT_BLOCKSIZE=32768
sector size: 512 (assumed)

md5 TOTAL: 0d60d96c8f7544f1be33ae29d1ce40d3
sha1 TOTAL: af21c46ca57debb75b18a8e819b016ca452ee900
39102336+0 sectors in
39102336+0 sectors out
dc3dd completed at 2011-06-07 19:18:09 +0200
Command completed: Tue Jun 7 19:18:12 CEST 2011

Start VERIFY: Tue Jun 7 19:18:12 CEST 2011
Verifying...

Command-line: cat /media/sda2/Immagine/img.* | air-counter 2>> /usr/local/share/air/logs/air.buffer.data | dc3dd hash=md5,sha1 hashlog=/tmp/verify_hash.log status=no
VERIFY SUCCESSFUL: Hashes match
Orig = md5 TOTAL: 0d60d96c8f7544f1be33ae29d1ce40d3
sha1 TOTAL: af21c46ca57debb75b18a8e819b016ca452ee900
Copy = md5 TOTAL: 0d60d96c8f7544f1be33ae29d1ce40d3
sha1 TOTAL: af21c46ca57debb75b18a8e819b016ca452ee900

Command completed: Tue Jun 7 19:37:45 CEST 2011

*** Comment ***
Acquisizione tramite AIR 2.0.0 dell' hdd, con windows xp, da analizzare.
L' immagine in formato dd è stata scomposta in blocchi da 4.6 gb e verrà successivamente memorizzata su supporti ottici (5 dvd).
Sono stati verificati gli hash MD5 e SHA-1 che, tra copia ed originale, coincidono.
L'operazione è stata effettuata tramite collegamento dell' hdd con un write blocker tableau con interfaccia IDE in entrata ed USB 2.0 in uscita.
*** End Comment ***
|
```

Copia dell'immagine su supporto ottico

- Tramite l'opzione split di Air;
- Copia su 5 dvd;
- Calcolo dell'hash md5 su ogni split per verificarne la correttezza;
 - Infatti un dvd è risultato corrotto!
- Lavoro sulla copia;

Indice - Parte II

- Ambiente Hardware ed Attività dell'indagato
 - Ambiente hardware/software
 - Attività dell'indagato
- Identificazione
 - Il nostro caso
- Conservazione
 - Conservazione tramite Write Blocker
 - Write Blocker Tableau
 - GuyMager
 - Air 2.0
 - Duplicazione su supporto ottico
- Analisi
 - Attività di analisi
 - Strumenti utilizzati
- Incidenti di percorso
- Conclusioni

Attività di analisi

■ Creazione di un nuovo caso con Autopsy

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a.	<input type="text"/>	b.	<input type="text"/>
c.	<input type="text"/>	d.	<input type="text"/>
e.	<input type="text"/>	f.	<input type="text"/>
g.	<input type="text"/>	h.	<input type="text"/>
i.	<input type="text"/>	j.	<input type="text"/>

Attività di analisi

- Nella successiva schermata occorre inserire l'immagine ottenuta in fase di conservazione (Autopsy supporta il "formato" split)

ADD A NEW IMAGE

1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter "" for the extension.

2. Type
Please select if this image file is for a disk or a single partition.

Disk Partition

3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

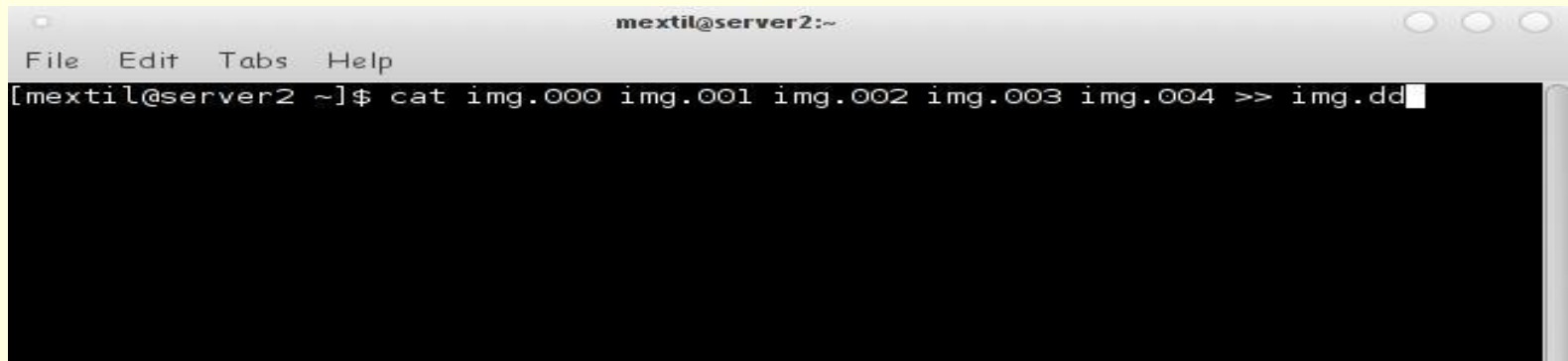
Symlink Copy Move

NEXT

CANCEL **HELP**

Attività di analisi

- Ottenere l'immagine intera da una splittata
 - Comando “cat” da terminale e redirezione “>>” su un file con estensione dd.
- Lavorare sulla copia ottenuta;
- Montare in sola lettura per copiare le cartelle di sistema e di registro.



```
mextil@server2:~  
File Edit Tabs Help  
[mextil@server2 ~]$ cat img.000 img.001 img.002 img.003 img.004 >> img.dd
```


Attività di analisi

- Ricerca file multimediali e documenti rilevanti;
- Ricerca di informazioni sulla navigazione;
- Ricerca di informazioni sul registro di sistema;
- Ricerca di informazioni di amministrazione del sistema;
- Ricerca di dati o partizioni criptate;
- Timeline dell'attività del sistema.

Strumenti utilizzati

- **Autopsy Forensic Browser**
 - Timeline dell'attività del sistema;
 - Navigazione dell'immagine dell'hdd e ricerca files per estensioni.
- OphCrack
 - Crack delle password di amministratore del sistema.
- Pasco
 - Estrazione delle informazioni di navigazione.
- LiveView e tools di Nirsoft
 - Ricerca delle password di completamento memorizzate dal browser.
- RegLookup e MiTeC Windows Registry Recovery
 - Estrazione delle informazioni dal registro di sistema.
- Tchunt/TCDDiscover e Passware kit enterprise
 - Ricerca\Decifrazione di una partizione cifrata con TrueCrypt.

Analisi:Autopsy

- Strumento di interfaccia grafica basato sul tool di analisi investigativa digitale The Sleuth Kit;
- Open Source per piattaforma Unix;
- Per ambiente windows Gygwin.

Tecniche per la ricerca dell'evidenza: Autopsy (1)

■ File Analysis

test:host1:vol2 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost:9999/autopsy?mod=1&submod=2&case=test&host=host1&inv=Pisano&vol=vol2

Autopsy localhost caine-live.net CFI - Computer For... CRIS The Sleuth Kit & Au... Unimo

test:host1:vol2 test:host1:vol2

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

Directory Seek

Enter the name of a directory that you want to view.
C: /

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

Current Directory: C:/

ADD NOTE GENERATE MD5 LIST OF FILES

DEL	Type	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
	r / r	\$AttrDef	2011-05-25 12:14:17 (CEST)	2011-05-25 12:14:17 (CEST)	2011-05-25 12:14:17 (CEST)	2011-05-25 12:14:17 (CEST)	2560	48	0	4-128-4
	r / r	\$BadClus	2011-05-25 12:14:17 (CEST)	2011-05-25 12:14:17 (CEST)	2011-05-25 12:14:17 (CEST)	2011-05-25 12:14:17 (CEST)	0	0	0	8-128-2
	r / r	\$BadClus:\$Bad	2011-05-25 12:14:17 (CEST)	2011-05-25 12:14:17 (CEST)	2011-05-25 12:14:17 (CEST)	2011-05-25 12:14:17 (CEST)	20012072960	0	0	8-128-1

File Browsing Mode

In this mode, you can view file and directory contents.

File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers

Done

Mon Jun 13, 5:19 PM

Tecniche per la ricerca dell'evidenza: Autopsy (2)

MD5 list

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost:9999/autopsy?mod=2&view=12&case=test&host=host1&inv=Pisano&vol=vol2&dir=/&meta=5

Autopsy localhost caine-live.net CFI - Computer For... CRIS The Sleuth Kit & Au... Unimo

test:host1:vol2 http://localh...&dir=/&meta=5

MD5 Values for files in C:/ (img.000-63-39086144)

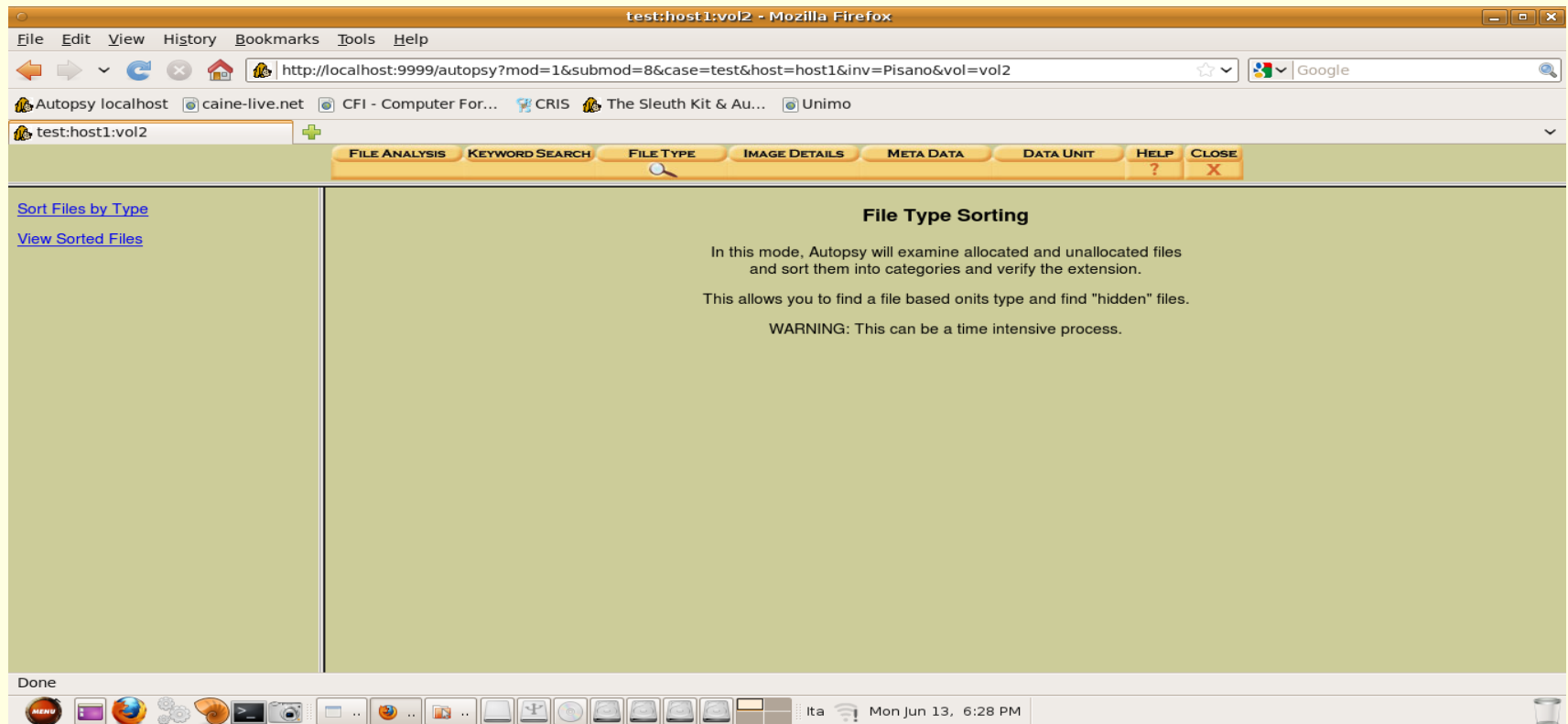
ad617ac3906958de35eacc3d90d31043	-	\$AttrDef
d41d8cd98f00b204e9800998ecf8427e	-	\$BadClus
d41d8cd98f00b204e9800998ecf8427e	-	\$BadClus:\$Bad
da620c8b35f471b0a8fale0fee37104b	-	\$Bitmap
ed1059bc9c3779d57eacafaca2b419b0	-	\$Boot
24be9fc84a327f6fdbfc1b42da38d2cc	-	\$LogFile
43dbbb8baf87e476bf4d54a82a008e03	-	\$MFT
7dd9cf4d1e68d68bfe64b13ef0323441	-	\$MFTMirr
bc43677ec6d0272168b1277db4ad3641	-	\$Secure:\$SDH
a7e65fe7044b132ac235b14185b25602	-	\$Secure:\$SII
5ea98e3badcafd4d121daf11b578cad65	-	\$Secure:\$SDS
6fa3db2468275286210751e869d36373	-	\$UpCase
d41d8cd98f00b204e9800998ecf8427e	-	\$Volume
d41d8cd98f00b204e9800998ecf8427e	-	AUTOEXEC.BAT
fa579938b0733b87066546afe951082c	-	boot.ini
0a1c64fa2acb40b53887ed734b68dc20	-	Bootfont.bin
d41d8cd98f00b204e9800998ecf8427e	-	CONFIG.SYS
5fdc58be9d17c233f802e8b23c3199a8	-	hiberfil.sys
d41d8cd98f00b204e9800998ecf8427e	-	IO.SYS
d41d8cd98f00b204e9800998ecf8427e	-	MSDOS.SYS
b2de3452de03674c6cec68b8c8ce7c78	-	NTDETECT.COM
56a91339a96f844349631fe302f42005	-	ntldr
bdc3f5f823a34ebfe70ec8153a6ccf3e	-	pagefile.sys

Done

Ita Mon Jun 13, 6:27 PM

Tecniche per la ricerca dell'evidenza: Autopsy (3)

■ File Type Sorting



Tecniche per la ricerca dell'evidenza: Autopsy (4)

■ Timeline of File Activity

The screenshot displays the Autopsy application interface within a Mozilla Firefox browser window. The address bar shows the URL: `http://localhost:9999/autopsy?tl=vol4&mod=6&view=1&submod=7&host=host1&case=test&inv=Pisano&x=23&y=9`. The application window has a toolbar with buttons for 'CREATE DATA FILE', 'CREATE TIMELINE', 'VIEW TIMELINE', 'VIEW NOTES', 'HELP', and 'CLOSE'. Below the toolbar, there are navigation links for '<- Apr 2011 Summary Jun 2011 ->' and a date selector set to 'May 2011'. The main area contains a table of file activity events.

Date	Time	File Size	Permissions	Process ID	Parent Process ID	File Path
Fri May 06 2011 01:51:08	13248968	m..b	r/rrwxrwxrwx	0	0	C:/WINDOWS/SoftwareDistribution/Download/9b1875a219d4d6675f947ad4d058d1caeb1a9be6
	13248968	m...	r/rrwxrwxrwx	0	0	C:/System Volume Information/_restore{FB4EBD2A-1976-4E37-BFAD-9C80EF016340}/RP5/A0004798.exe
Thu May 19 2011 15:15:00	5099520	m...	r/rrwxrwxrwx	0	0	C:/Documents and Settings/Test/Documents/Immagine/P1010514.JPG
	4850688	m...	r/rrwxrwxrwx	0	0	C:/Documents and Settings/Test/Documents/Immagine/P1010515.JPG
Wed May 25 2011 10:42:12	211	m...	r/rr-xr-xr-x	0	0	C:/boot.ini
Wed May 25 2011 10:42:13	464	m.cb	d/drwxrwxrwx	0	0	C:/Documents and Settings/All Users/Dati applicazioni/Microsoft/Network
	224	..b	d/drwxrwxrwx	0	0	C:/Documents and Settings/All Users/Dati applicazioni/Microsoft/Network/Connections
	392	..b	d/drwxrwxrwx	0	0	C:/Documents and Settings/All Users/Dati applicazioni/Microsoft/Network/Connections/Pbk
	853	.acb	r/rrwxrwxrwx	0	0	C:/Documents and Settings/All Users/Dati applicazioni/Microsoft/Network/Connections/Pbk/sharedaccess.ini
Wed May 25 2011 10:42:15	4375	..b	r/rrwxrwxrwx	0	0	C:/WINDOWS/Debug/NetSetup.LOG
Wed May 25 2011 10:42:32	16067	.a..	r/rrwxrwxrwx	0	0	C:/WINDOWS/system32/rsvp.ini
	3178	.a..	r/rrwxrwxrwx	0	0	C:/WINDOWS/system32/rsvpcnts.h

The taskbar at the bottom shows the system tray with the date 'Mon Jun 13, 6:31 PM' and the language 'Ita'.

Tecniche per la ricerca dell'evidenza: Autopsy (5)

Keyword Search

The screenshot shows the Autopsy software interface with the 'KEYWORD SEARCH' tab selected. The search results are displayed in a central pane, showing details for a specific fragment and its hex contents.

New Search

2 occurrences of '((jan)l(feb)l(mar)l(apr)l(may)l(jun)l(jul)l(aug)l(sep)l(oct)l(nov)l(dec)l)' 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/mt

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

0	25733a20	57726974	696e6720	6d6f6465	%s: Writing mode
16	20534353	49206d6f	64652070	61676520	SCS I mode page
32	6661696c	65642e0a	00000000	00000000	failed.. ..
48	00000000	00000000	00000000	00000000
64	25733a20	436f6d70	72657373	696f6e20	%s: Compression
80	6d6f6465	206e6f74	20636861	6e676564	mode not changed
96	2e0a0000	00000000	00000000	00000000
112	00000000	00000000	00000000	00000000
128	25733a20	52652d72	65616420	6f662074	%s: Re-read of t
144	68652063	6f6d7072	65737369	6f6e2070	he c ompr essi on p
160	61676520	6661696c	65642e0a	00436f6d	age failed.. .Com
176	70726573	73696f6e	206f6e2e	0a00436f	pression on.. .Co
192	6d707265	7373696f	6e206f66	662e0a00	mpre ssio n of f...
208	00000000	00000000	00000000	00000000
224	00000000	64ba0408	00000000	00000000 d... ..
240	00000000	00000000	00000000	00000000
256	2449643a	202f7573	72322f75	73657273	\$Id: /usr2/users
272	2f6d616b	69736172	612f7372	632f7379	/mak isar a/sr c/sy
288	732f6d74	2d73742d	302e3562	2f6d742e	s/mt -st- 0.5b /mt.
304	63206174	2053756e	20417567	20313620	c at Sun Aug 16
320	30393a35	313a3137	20313939	38206279	09:5 1:17 199 8 by
336	206d616b	69736172	61406b61	692e6d61	mak isar a@ka i.ma

Tecniche per la ricerca dell'evidenza: Autopsy (6)

■ Meta Data Analysis

The screenshot displays the Autopsy web interface in a Mozilla Firefox browser window. The address bar shows the URL: `http://localhost:9999/autopsy?mod=1&submod=3&case=test&host=host1&inv=Pisano&vol=vol2`. The browser's address bar contains several tabs: Autopsy localhost, caine-live.net, CFI - Computer For..., CRIS, The Sleuth Kit & Au..., and Unimo. The Autopsy interface has a navigation bar with buttons for FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA (selected), DATA UNIT, HELP, and CLOSE. The main content area shows the following information:

MFT Entry Number: 1024

VIEW

ALLOCATION LIST

Pointed to by file:
C:/WINDOWS/system32/mscat32.dll

File Type:
PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit

MD5 of content:
c978beb1dcd0a7294faac7dd870d295c -

SHA-1 of content:
1243bd92a1a0e3464820e6c597c171016471279e -

Details:

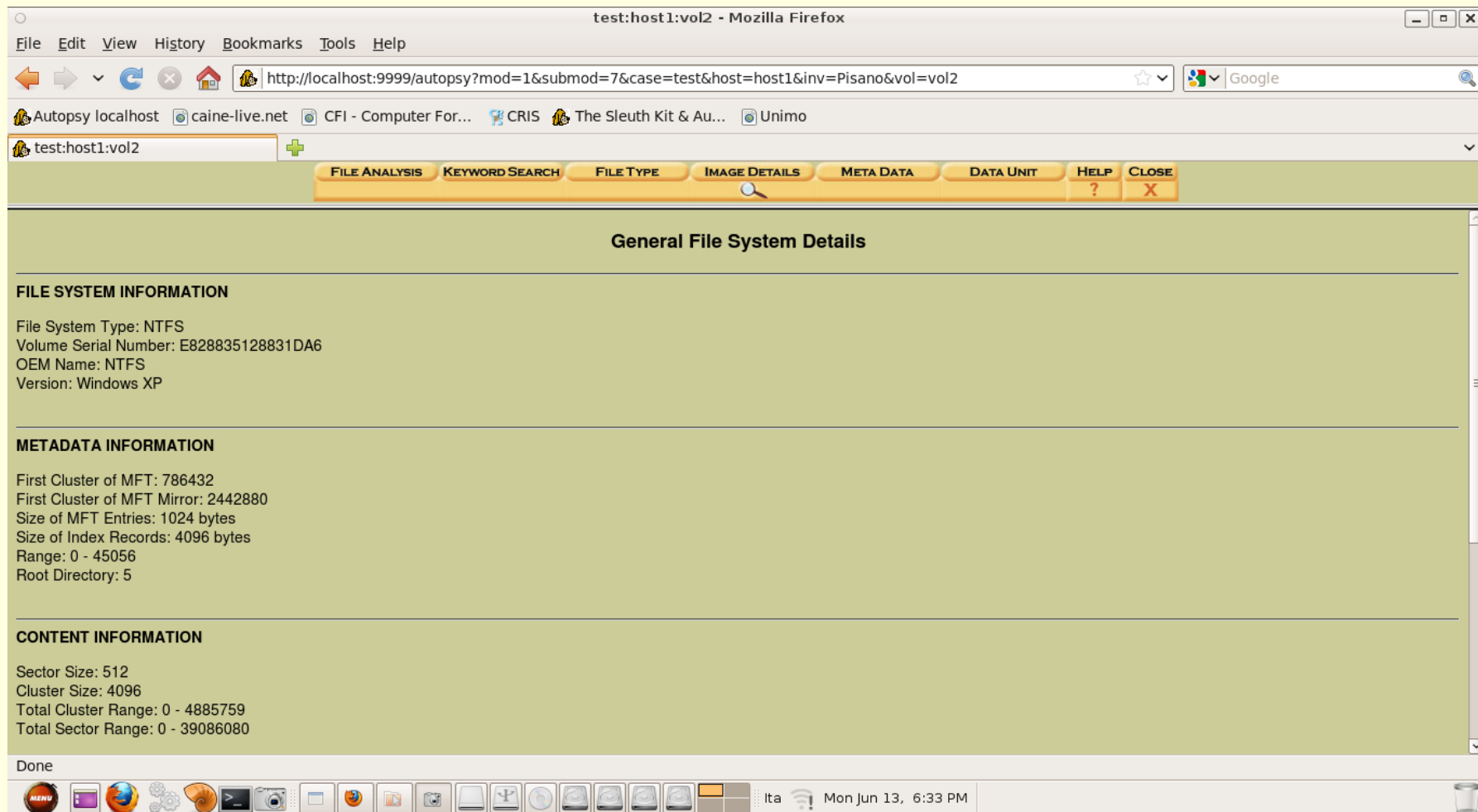
MFT Entry Header Values:
Entry: 1024 Sequence: 1
\$LogFile Sequence Number: 187554546
Allocated File
Links: 1

\$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 282 ()
Created: Fri Aug 31 14:00:00 2001
File Modified: Fri Aug 31 14:00:00 2001

The browser's status bar at the bottom shows "Done" and the system tray includes the date and time: "Mon Jun 13, 6:31 PM".

Tecniche per la ricerca dell'evidenza: Autopsy (7)

■ Image Details



The screenshot displays the Autopsy software interface within a Mozilla Firefox browser window. The browser's address bar shows the URL: `http://localhost:9999/autopsy?mod=1&submod=7&case=test&host=host1&inv=Pisano&vol=vol2`. The Autopsy application window has a menu bar with options: FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS (selected), META DATA, DATA UNIT, HELP, and CLOSE. The main content area is titled "General File System Details" and is divided into three sections:

- FILE SYSTEM INFORMATION**
 - File System Type: NTFS
 - Volume Serial Number: E828835128831DA6
 - OEM Name: NTFS
 - Version: Windows XP
- METADATA INFORMATION**
 - First Cluster of MFT: 786432
 - First Cluster of MFT Mirror: 2442880
 - Size of MFT Entries: 1024 bytes
 - Size of Index Records: 4096 bytes
 - Range: 0 - 45056
 - Root Directory: 5
- CONTENT INFORMATION**
 - Sector Size: 512
 - Cluster Size: 4096
 - Total Cluster Range: 0 - 4885759
 - Total Sector Range: 0 - 39086080

The Windows taskbar at the bottom shows the system tray with the date and time: "Mon Jun 13, 6:33 PM".

Time Line Autopsy

- Analisi delle operazioni effettuate dall'indagato;
- Web e locali;
- Analisi di parte dei dati presenti nel HD;
- Visione dettagliate degli orari e dei giorni di accesso ai files ed alle pagine web;

La verifica dei programmi installati

■ Avira antivir	03/06/2011	11:36:31
■ Acrobat	03/06/2011	11:56:38
■ TrueCrypt	06/06/2011	15:19:26
■ OpenOffice	03/06/2011	14:45:50
■ TrueImage	03/06/2011	09:38:46
■ DiskWizard	03/06/2011	09:43:01

Il registro di sistema, per qualche motivo, non memorizzava le informazioni sull'installazione di Truecrypt e Antivir. E' stato possibile ritrovarle tramite la Timeline di Autopsy.

Files individuati

- 1852 file .jpg e 1432 file .gif, la maggior parte tratti da visite di profili facebook e ricerche on-line;
- 15 file .pdf, di cui uno visitato on-line;
- 15 file .doc, di cui uno di realizzazione nostra (dell'indagato);
- 12 file .avi, filmati dimostrativi di windows e altri da noi caricati di cui due cifrati con windows.

Strumenti utilizzati

- **Autopsy Forensic Browser**
 - Timeline dell'attività del sistema;
 - Navigazione dell'immagine dell'hdd e ricerca files per estensioni.
- **OphCrack**
 - Crack delle password di amministratore del sistema.
- **Pasco**
 - Estrazione delle informazioni di navigazione.
- **LiveView e tools di Nirsoft**
 - Ricerca delle password di completamento memorizzate dal browser.
- **RegLookup e MiTeC Windows Registry Recovery**
 - Estrazione delle informazioni dal registro di sistema.
- **Tchunt/TCDDiscover e Passware kit enterprise**
 - Ricerca\Decifrazione di una partizione cifrata con TrueCrypt.

Tecniche per la ricerca dell'evidenza: OphCrack

- E' un cracker delle password di Windows basato sulla tecnica delle Rainbow Tables;
- Cracca hash LM NTLM;
- Permette di estrarre le password dell'amministratore di sistema lunghe massimo 16 caratteri con probabilità 96%;
- Estrae le password da file SAM (Security Account Manager);

OphCrack: Interfaccia grafica

The screenshot displays the OphCrack application interface. At the top, there is a toolbar with icons for Load, Delete, Save, Tables, Stop, Help, and Exit, along with an 'OS' logo and an 'About' button. Below the toolbar are three tabs: 'Progress' (selected), 'Statistics', and 'Preferences'.

The main window is divided into two primary sections. The upper section is a table listing system users and their associated hashes and passwords.

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
ISupervisor...		31D6CFE0...			empty
toto		1EF82030F...			
Administrator	9d483a84a...	33cc539403...	GUESSME	001	GuessMe001
Phillippe	b906f7976d...	b91e46819...	MAISON2	empty	maison2
Guest	3b5d42642...	fff23d5f2a0...	ZF2Y11P	5PKMWP4	zf2Y11p5PKMwP4
	eaef446f97...	ac051662cd...	TR3	empty	tr3
	ce304571fc...	db129418a...	!#%	empty	!#%
		da7e06bcb...			o*
	a13aa0bf3a...	f01d6862af...			
	3e645334fd	535f3de7eh			

The lower section is a table showing the progress of the cracking process for different tables and directories.

Table	Directory	Status	Progress
XP free fast	/mnt/ext3/ta...	36% in RAM	[Progress bar]
table0		36% in RAM	[Progress bar]
table1		36% in RAM	[Progress bar]
table2		36% in RAM	[Progress bar]
table3		36% in RAM	[Progress bar]
Vista free	/mnt/ext3/ta...	22% in RAM	[Progress bar]
table1		43% in RAM	[Progress bar]
table3		43% in RAM	[Progress bar]
XP	/mnt/ext3/ta...	10% in RAM	[Progress bar]

At the bottom of the interface, there are four status indicators: 'Preload: done', 'Brute force: done', 'Pwd found: 9/29', and 'Time elapsed: 0h 2m 38s'.

Strumenti utilizzati

- **Autopsy Forensic Browser**
 - Timeline dell'attività del sistema;
 - Navigazione dell'immagine dell'hdd e ricerca files per estensioni.
- **OphCrack**
 - Crack delle password di amministratore del sistema.
- **Pasco**
 - Estrazione delle informazioni di navigazione.
- **LiveView e tools di Nirsoft**
 - Ricerca delle password di completamento memorizzate dal browser.
- **RegLookup e MiTeC Windows Registry Recovery**
 - Estrazione delle informazioni dal registro di sistema.
- **Tchunt/TCDDiscover e Passware kit enterprise**
 - Ricerca\Decifrazione di una partizione cifrata con TrueCrypt.

Tecniche per la ricerca dell'evidenza: Pasco (1)

- Tool forense per l'analisi dell'attività su web dell'utente
- Fornisce informazioni su: cronologia, cookies, e history.
- I risultati sono presentati in modo da poter essere importati su un programma di gestione di fogli elettronici (Access)

Tecniche per la ricerca dell'evidenza: Pasco (2)

- I file su cui lavorare sono gli index.dat contenuti in:
 - C:\Documents and Settings\User\Cookies
 - C:\Documents and Settings\User\Impostazioni Locali\Cronologia\History.ie5
 - C:\Documents and Settings\User\Impostazioni Locali\Temporary Internet File\Content.ie5

Tecniche per la ricerca dell'evidenza: Pasco – History Files

Microsoft Access - [Index : Tabella]

File Modifica Visualizza Inserisci Formato Record Strumenti Finestra 2

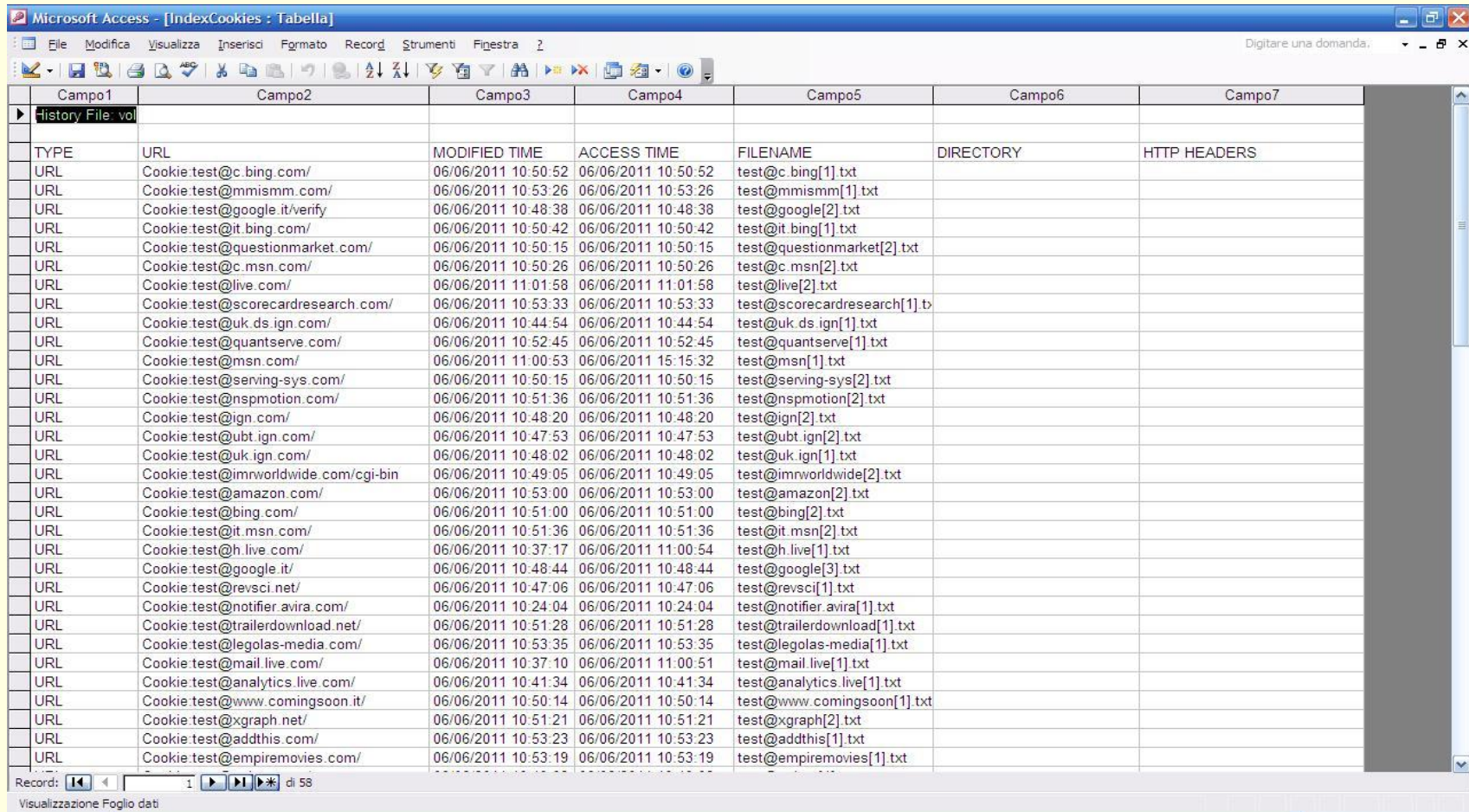
Digitare una domanda.

Campo1	Campo2	Campo3	Campo4	Campo5	Campo6	
History File: inc						
TYPE	URL	MODIFIED TIME	ACCESS TIME	FILENAME	DIRECTORY	HTTP HEADERS
URL	http://db2.stb00.s-msn.com/i/91/2CA23B349C2F538E6B2E7286AA75A	05/20/2011 14:38:05	06/06/2011 10:51:34	2CA23B349C2F538E6B2E7286AA75A	CHQ3CT2Z	HTTP/1.1 200 OK Content-Type:...
URL	http://www.update.microsoft.com/windowsupdate/v6/shared/js/tgar.js?63	09/05/2009 01:28:10	06/03/2011 11:53:50	tgar[1].js	V6T0MJ21	HTTP/1.1 200 OK Content-Length:...
URL	http://www.images.adobe.com/www.adobe.com/ubi/template/identity/adol	03/06/2010 03:36:52	06/03/2011 11:53:51	downloadbutton	CHQ3CT2Z	HTTP/1.1 200 OK ETag: "b677a8"
URL	http://www.update.microsoft.com/windowsupdate/v6/shared/js/content.js	09/05/2009 01:28:10	06/03/2011 11:53:56	content[2].js	8XUJGLAZ	HTTP/1.1 200 OK Content-Length:...
URL	http://www.update.microsoft.com/windowsupdate/v6/shared/images/banner	01/06/2009 02:13:06	06/03/2011 12:39:14	welcome-bg[1].	CHQ3CT2Z	HTTP/1.1 200 OK Content-Type:...
URL	http://www.update.microsoft.com/windowsupdate/v6/shared/images/news	01/06/2009 02:13:16	06/03/2011 12:39:17	news_bg_leftmi	V6T0MJ21	HTTP/1.1 200 OK Content-Type:...
URL	http://asset-2.openoffice.org/branding/kenai/stylesheets/style.css?20110	03/02/2011 18:25:45	06/03/2011 12:40:10	style[1].css	CHQ3CT2Z	HTTP/1.1 200 OK Content-Length:...
URL	http://clients1.google.it/complete/search?hl=it&client=hp&q=a&cp=1		06/03/2011 11:53:33	search[2]	V6T0MJ21	HTTP/1.1 200 OK Content-Length:...
URL	http://windowsupdate.microsoft.com/redirect.js	07/18/2008 20:01:53	06/03/2011 12:38:48	redirect[1].js	8XUJGLAZ	HTTP/1.1 200 OK Content-Length:...
URL	http://www.update.microsoft.com/windowsupdate/v6/mstoolbar.aspx?ln=i	06/03/2011 12:38:30	06/03/2011 12:38:58	mstoolbar[1].ht	V6T0MJ21	HTTP/1.1 200 OK Content-Type:...
URL	http://www.update.microsoft.com/windowsupdate/v6/shared/css/toc.css	01/06/2009 02:12:46	06/03/2011 12:39:05	toc[2].css	BWFZUEPX	HTTP/1.1 200 OK Content-Length:...
URL	http://www.update.microsoft.com/windowsupdate/v6/shared/js/tgar.js?63	09/05/2009 01:28:10	06/03/2011 12:39:03	tgar[5].js	8XUJGLAZ	HTTP/1.1 200 OK Content-Length:...
URL	http://w.sharethis.com/button/buttons.js	05/26/2011 23:03:08	06/03/2011 12:40:10	buttons[2].js	8XUJGLAZ	HTTP/1.1 200 OK Content-Length:...
URL	http://asset-3.openoffice.org/images/functionButton.gif.png?@rev@	05/24/2011 18:37:38	06/03/2011 12:40:11	functionButton.	8XUJGLAZ	HTTP/1.0 200 OK ETag: "df4a40"
URL	http://www.google.it/extern_js/f/CgJpdBICaXQrMEU4ACwrMfo4ACwrMA	06/02/2010 02:00:00	06/03/2011 12:39:18	t_53vPy5uTw[1]	V6T0MJ21	HTTP/1.1 200 OK Content-Length:...
URL	http://www.trailerdownload.net/includes/css/images/galleri.png	08/24/2009 07:41:15	06/06/2011 10:51:16	galleri[1].png	8XUJGLAZ	HTTP/1.1 200 OK ETag: "6ae03f"
URL	http://asset-1.openoffice.org/branding/kenai/images/oracle-logo.gif?20110	02/23/2011 13:47:11	06/03/2011 12:40:10	oracle-logo[1].g	CHQ3CT2Z	HTTP/1.0 200 OK Content-Length:...
URL	http://static.ak.fbcdn.net/rsrsrc.php/v1/zr/r/XXVvDYAks_i.png	03/14/2010 13:43:06	06/06/2011 10:35:58	XXVvDYAks_i[1]	V6T0MJ21	HTTP/1.1 200 OK Content-Length:...
URL	http://b.static.ak.fbcdn.net/rsrsrc.php/v1/r/H2SSvhJMA-.xml	01/01/2000 01:00:00	06/06/2011 10:28:06	H2SSvhJMA-;	BWFZUEPX	HTTP/1.1 200 OK Content-Length:...
URL	http://photos-e.ak.fbcdn.net/photos-ak-snc1/v43/62/10726707410/app_2	04/25/2008 15:52:19	06/06/2011 10:36:18	app_2_1072670	CHQ3CT2Z	HTTP/1.1 200 OK Content-Type:...
URL	http://www.facebook.com/ajax/typeahead/search.php?_a=1&value=ale8		06/06/2011 10:28:15	search[1].php	BWFZUEPX	HTTP/1.1 200 OK Content-Type:...
URL	http://db2.stb01.s-msn.com/i/33/28C356E4FE07667A9BE4231A829A.jp	06/03/2011 07:46:02	06/03/2011 12:38:55	28C356E4FE07	8XUJGLAZ	HTTP/1.1 200 OK Content-Type:...
URL	http://db2.stb00.s-msn.com/i/98/76768287F448AEDBF6413DD118FCEC	04/19/2011 07:36:38	06/06/2011 10:51:34	76768287F448	BWFZUEPX	HTTP/1.1 200 OK Content-Type:...
URL	http://www.images.adobe.com/www.adobe.com/ubi/template/identity/adol		06/03/2011 11:59:53	print[1].css	8XUJGLAZ	HTTP/1.1 200 OK Content-Length:...
URL	http://www.images.adobe.com/www.adobe.com/ubi/template/identity/adol	03/06/2010 03:36:54	06/03/2011 11:54:20	windowfrost[1].	CHQ3CT2Z	HTTP/1.1 200 OK ETag: "c5a51a"
URL	http://www.update.microsoft.com/windowsupdate/v6/shared/images/banner	01/06/2009 02:13:06	06/03/2011 12:39:09	welcome-right[1]	V6T0MJ21	HTTP/1.1 200 OK Content-Type:...
URL	http://www.update.microsoft.com/windowsupdate/v6/shared/images/failed	01/06/2009 02:13:16	06/03/2011 11:59:47	failed-ig[1].gif	8XUJGLAZ	HTTP/1.1 200 OK Content-Type:...
URL	http://www.update.microsoft.com/windowsupdate/v6/shared/images/banner	01/06/2009 02:12:48	06/03/2011 12:40:29	banner-bg[1].jpg	V6T0MJ21	HTTP/1.1 200 OK Content-Type:...
REDR	http://ad-emea.doubleclick.net/ad/N2263.msn.it/B5576058.sz=1x1:ord=7			search_btn_tile	8XUJGLAZ	HTTP/1.1 200 OK ETag: "15b303"
URL	http://www.images.adobe.com/www.adobe.com/ubi/template/identity/adol	09/30/2010 19:49:06	06/03/2011 11:54:20	search_btn_tile	8XUJGLAZ	HTTP/1.1 200 OK ETag: "15b303"
URL	http://www.update.microsoft.com/windowsupdate/v6/shared/js/toc.js?634	09/05/2009 01:28:10	06/03/2011 11:53:51	toc[2].js	V6T0MJ21	HTTP/1.1 200 OK Content-Length:...
URL	http://www.update.microsoft.com/windowsupdate/v6/shared/images/au_s	01/06/2009 02:12:48	06/03/2011 12:39:12	au_shieldred[1]	8XUJGLAZ	HTTP/1.1 200 OK Content-Type:...

Record: 2 di 2391

Visualizzazione Foglio dati

Tecniche per la ricerca dell'evidenza: Pasco – Cookies



Microsoft Access - [IndexCookies : Tabella]

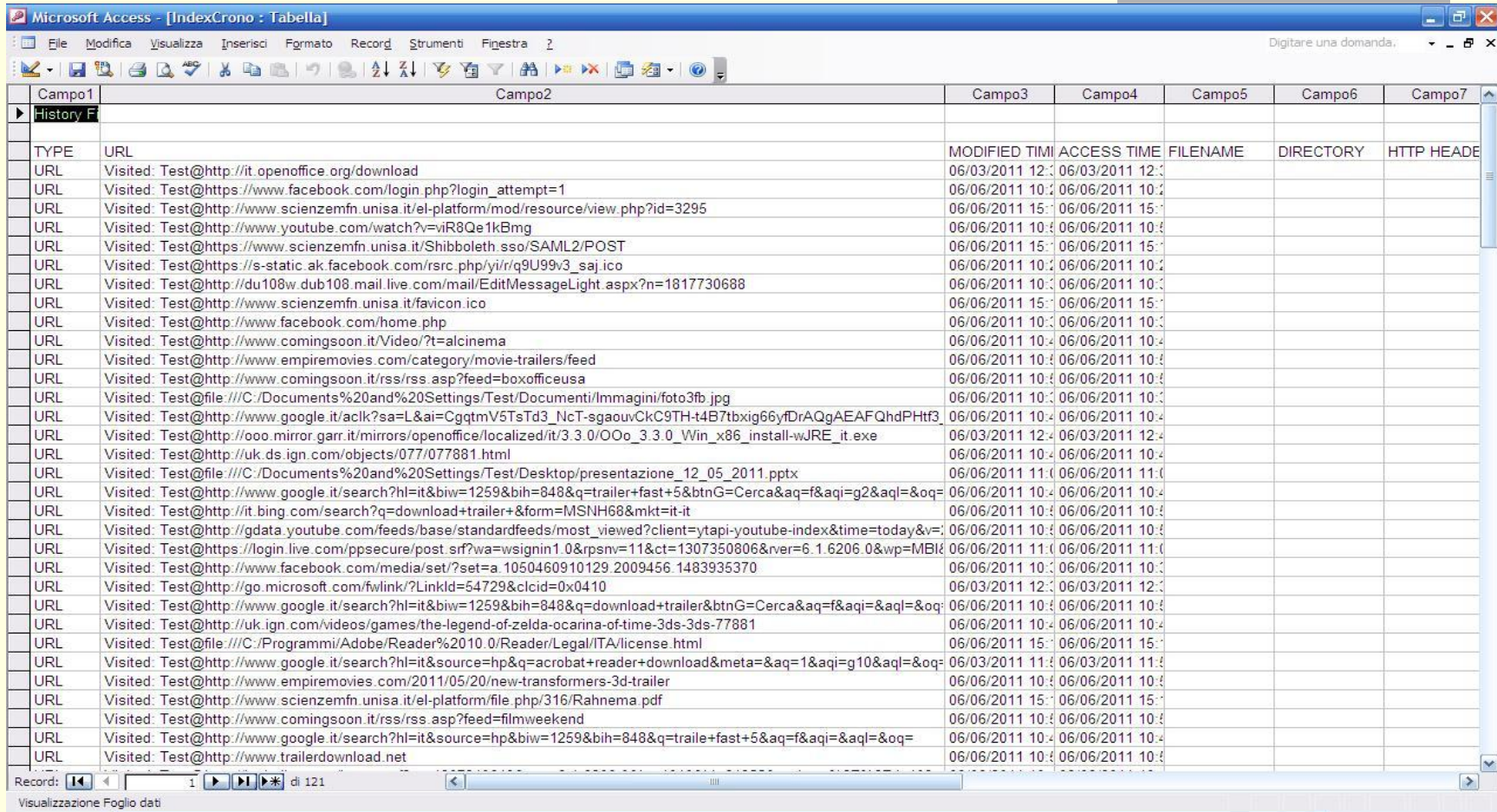
Digitare una domanda.

Campo1	Campo2	Campo3	Campo4	Campo5	Campo6	Campo7
History File: voi						
TYPE	URL	MODIFIED TIME	ACCESS TIME	FILENAME	DIRECTORY	HTTP HEADERS
	URL	06/06/2011 10:50:52	06/06/2011 10:50:52	test@c.bing[1].txt		
	URL	06/06/2011 10:53:26	06/06/2011 10:53:26	test@mmismm[1].txt		
	URL	06/06/2011 10:48:38	06/06/2011 10:48:38	test@google[2].txt		
	URL	06/06/2011 10:50:42	06/06/2011 10:50:42	test@it.bing[1].txt		
	URL	06/06/2011 10:50:15	06/06/2011 10:50:15	test@questionmarket[2].txt		
	URL	06/06/2011 10:50:26	06/06/2011 10:50:26	test@c.msn[2].txt		
	URL	06/06/2011 11:01:58	06/06/2011 11:01:58	test@live[2].txt		
	URL	06/06/2011 10:53:33	06/06/2011 10:53:33	test@scorecardresearch[1].txt		
	URL	06/06/2011 10:44:54	06/06/2011 10:44:54	test@uk.ds.ign[1].txt		
	URL	06/06/2011 10:52:45	06/06/2011 10:52:45	test@quantserve[1].txt		
	URL	06/06/2011 11:00:53	06/06/2011 15:15:32	test@msn[1].txt		
	URL	06/06/2011 10:50:15	06/06/2011 10:50:15	test@erving-sys[2].txt		
	URL	06/06/2011 10:51:36	06/06/2011 10:51:36	test@nspmotion[2].txt		
	URL	06/06/2011 10:48:20	06/06/2011 10:48:20	test@ign[2].txt		
	URL	06/06/2011 10:47:53	06/06/2011 10:47:53	test@ubt.ign[2].txt		
	URL	06/06/2011 10:48:02	06/06/2011 10:48:02	test@uk.ign[1].txt		
	URL	06/06/2011 10:49:05	06/06/2011 10:49:05	test@imrworldwide[2].txt		
	URL	06/06/2011 10:53:00	06/06/2011 10:53:00	test@amazon[2].txt		
	URL	06/06/2011 10:51:00	06/06/2011 10:51:00	test@bing[2].txt		
	URL	06/06/2011 10:51:36	06/06/2011 10:51:36	test@it.msn[2].txt		
	URL	06/06/2011 10:37:17	06/06/2011 11:00:54	test@h.live[1].txt		
	URL	06/06/2011 10:48:44	06/06/2011 10:48:44	test@google[3].txt		
	URL	06/06/2011 10:47:06	06/06/2011 10:47:06	test@revsci[1].txt		
	URL	06/06/2011 10:24:04	06/06/2011 10:24:04	test@notifier.avira[1].txt		
	URL	06/06/2011 10:51:28	06/06/2011 10:51:28	test@trailerdownload[1].txt		
	URL	06/06/2011 10:53:35	06/06/2011 10:53:35	test@legolas-media[1].txt		
	URL	06/06/2011 10:37:10	06/06/2011 11:00:51	test@mail.live[1].txt		
	URL	06/06/2011 10:41:34	06/06/2011 10:41:34	test@analytics.live[1].txt		
	URL	06/06/2011 10:50:14	06/06/2011 10:50:14	test@www.comingsoon[1].txt		
	URL	06/06/2011 10:51:21	06/06/2011 10:51:21	test@xgraph[2].txt		
	URL	06/06/2011 10:53:23	06/06/2011 10:53:23	test@addthis[1].txt		
	URL	06/06/2011 10:53:19	06/06/2011 10:53:19	test@empiremovies[1].txt		

Record: 1 di 58

Visualizzazione Foglio dati

Tecniche per la ricerca dell'evidenza: Pasco – Cronologia navigazione



Microsoft Access - [IndexCrono : Tabella]

File Modifica Visualizza Inserisci Formato Record Strumenti Finestra ?

Digitare una domanda.

Campo1	Campo2	Campo3	Campo4	Campo5	Campo6	Campo7
History F						
TYPE	URL	MODIFIED TIME	ACCESS TIME	FILENAME	DIRECTORY	HTTP HEADERS
URL	Visited: Test@http://it.openoffice.org/download	06/03/2011 12:00	06/03/2011 12:00			
URL	Visited: Test@https://www.facebook.com/login.php?login_attempt=1	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@http://www.scienzemfn.unisa.it/el-platform/mod/resource/view.php?id=3295	06/06/2011 15:00	06/06/2011 15:00			
URL	Visited: Test@http://www.youtube.com/watch?v=viR8Qe1k8Bg	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@https://www.scienzemfn.unisa.it/Shibboleth.sso/SAML2/POST	06/06/2011 15:00	06/06/2011 15:00			
URL	Visited: Test@https://s-static.ak.facebook.com/rsrc.php/yiri/q9U99v3_saj.ico	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@http://du108w.dub108.mail.live.com/mail/EditMessageLight.aspx?n=1817730688	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@http://www.scienzemfn.unisa.it/favicon.ico	06/06/2011 15:00	06/06/2011 15:00			
URL	Visited: Test@http://www.facebook.com/home.php	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@http://www.comingsoon.it/Video/?t=alcinema	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@http://www.empiremovies.com/category/movie-trailers/feed	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@http://www.comingsoon.it/rss/rss.asp?feed=boxofficeusa	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@file:///C:/Documents%20and%20Settings/Test/Documents/Immagini/foto3fb.jpg	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@http://www.google.it/aclk?sa=L&ai=CgqtmV5TsTd3_NcT-sgaouvCkC9TH-t4B7tbxig66yfDrAQgAEAFQhdPHft3	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@http://ooo.mirror.garr.it/mirrors/openoffice/localized/it/3.3.0/OoO_3.3.0_Win_x86_install-wJRE_it.exe	06/03/2011 12:00	06/03/2011 12:00			
URL	Visited: Test@http://uk.ds.ign.com/objects/077/077881.html	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@file:///C:/Documents%20and%20Settings/Test/Desktop/presentazione_12_05_2011.pptx	06/06/2011 11:00	06/06/2011 11:00			
URL	Visited: Test@http://www.google.it/search?hl=it&biw=1259&bih=848&q=trailer+fast+5&btnG=Cerca&aq=f&aqi=g2&aql=&og=	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@http://it.bing.com/search?q=download+trailer+&form=MSNH68&mkt=it-it	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@http://gdata.youtube.com/feeds/base/standardfeeds/most_viewed?client=ytipi-youtube-index&time=today&v=	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsnv=11&ct=1307350806&rver=6.1.6206.0&wp=MBK&	06/06/2011 11:00	06/06/2011 11:00			
URL	Visited: Test@http://www.facebook.com/media/set/?set=a.1050460910129.2009456.1483935370	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@http://go.microsoft.com/fwlink/?LinkId=54729&clcid=0x0410	06/03/2011 12:00	06/03/2011 12:00			
URL	Visited: Test@http://www.google.it/search?hl=it&biw=1259&bih=848&q=download+trailer&btnG=Cerca&aq=f&aqi=g2&aql=&og=	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@http://uk.ign.com/videos/games/the-legend-of-zelda-ocarina-of-time-3ds-3ds-77881	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@file:///C:/Programmi/Adobe/Reader%2010.0/Reader/Legal/ITA/license.html	06/06/2011 15:00	06/06/2011 15:00			
URL	Visited: Test@http://www.google.it/search?hl=it&source=hp&q=acrobat+reader+download&meta=&aq=1&aqi=g10&aql=&og=	06/03/2011 11:00	06/03/2011 11:00			
URL	Visited: Test@http://www.empiremovies.com/2011/05/20/new-transformers-3d-trailer	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@http://www.scienzemfn.unisa.it/el-platform/file.php/316/Rahnema.pdf	06/06/2011 15:00	06/06/2011 15:00			
URL	Visited: Test@http://www.comingsoon.it/rss/rss.asp?feed=filmweekend	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@http://www.google.it/search?hl=it&source=hp&biw=1259&bih=848&q=trailer+fast+5&aq=f&aqi=g2&aql=&og=	06/06/2011 10:00	06/06/2011 10:00			
URL	Visited: Test@http://www.trailerdownload.net	06/06/2011 10:00	06/06/2011 10:00			

Record: 1 di 121

Visualizzazione Foglio dati

Strumenti utilizzati

- Autopsy Forensic Browser
 - Timeline dell'attività del sistema;
 - Navigazione dell'immagine dell'hdd e ricerca files per estensioni.
- OphCrack
 - Crack delle password di amministratore del sistema.
- Pasco
 - Estrazione delle informazioni di navigazione.
- LiveView e tools di Nirsoft
 - Ricerca delle password di completamento memorizzate dal browser.
- RegLookup e MiTeC Windows Registry Recovery
 - Estrazione delle informazioni dal registro di sistema.
- Tchunt/TCDDiscover e Passware kit enterprise
 - Ricerca\Decifrazione di una partizione cifrata con TrueCrypt.

LiveView e VMWare Server

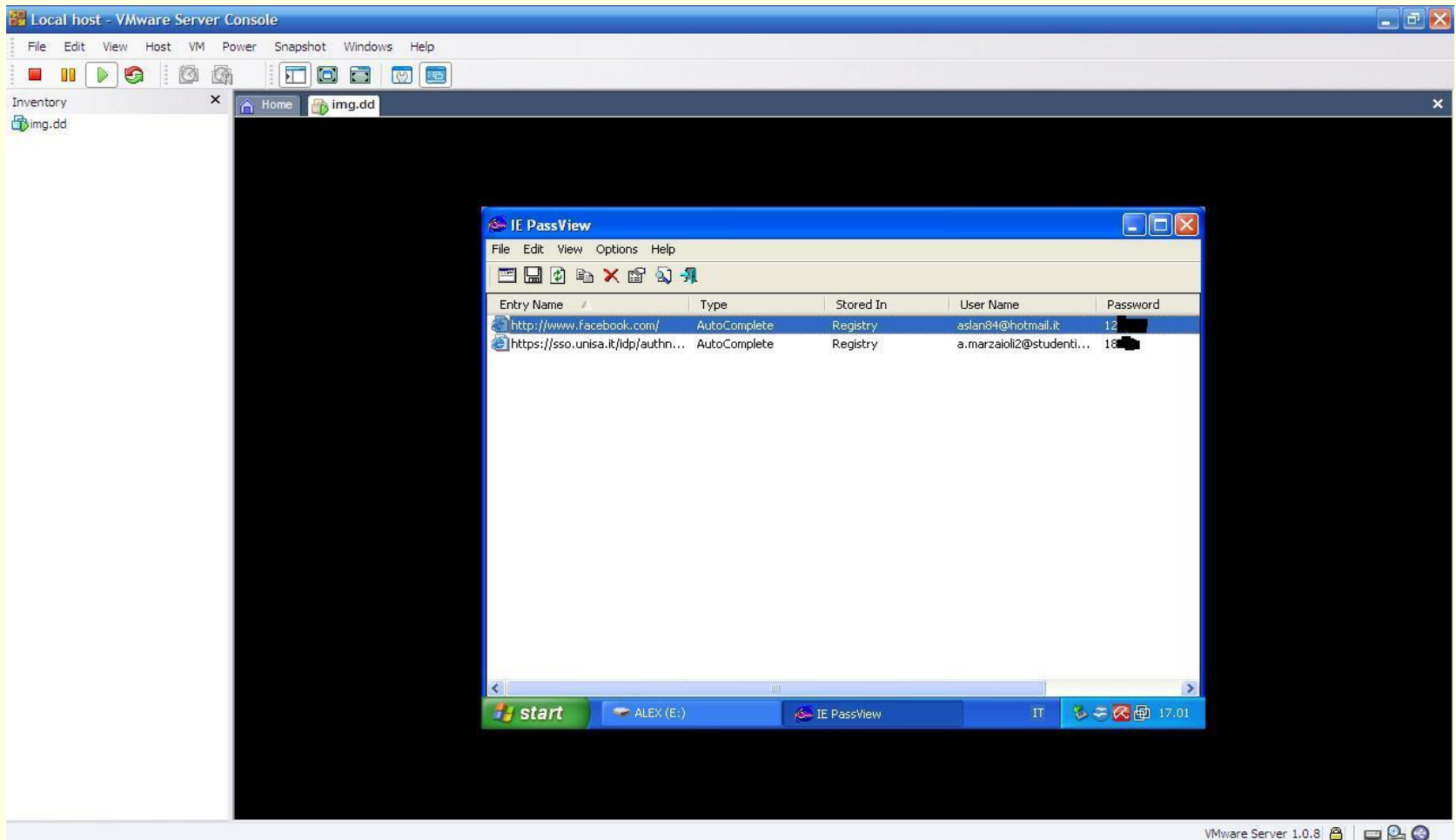
■ LiveView:

- Sviluppato dal CERT Software Engineering Institute
- E' un tool grafico basato su Java che permette di creare una macchina virtuale da un'immagine di un disco (dd)
- Supporta varie versioni di Windows (fino a Vista) ed in modo limitato Linux
- Il tutto... Senza modificare l'immagine originale

I tools di Nirsoft per analisi forense

- Numero elevato di tools che permettono di:
 - Recuperare le password;
 - Monitorare la rete;
 - Prelevare informazioni dal browser;
 - Visualizzare informazioni dal disco.
- Abbiamo utilizzato in particolare: IE Pass View, IE Cache View, IE History View ed IE Cookies View.

LiveView&IE Pass View: Password memorizzate dal browser



Ricostruzione navigazione web

	A	B	C	D
2	http://www.google.it	03/06/2011	11.51.06	Home Page
3	notifier.avira.com	03/06/2011	11.51.42	Download Antivir
4	http://www.google.it	03/06/2011	11.53.38	Ricerca Adobe Acrobat Reader
5	http://get.adobe.com/it/reader	03/06/2011	11.53.51	Download Acrobat Reader
6	http://www.google.it	03/06/2011	12.39.27	Ricerca OpenOffice
7	http://it.openoffice.org/download/3.3.0/download330.html	03/06/2011	12.40.11	Download OpenOffice 3.3.0
8	http://www.facebook.com	06/06/2011	10.26.01	Facebook
9	file:///C:/Documents%20and%20Settings/Test/Documents/Immagine/foto1fb.jpg	06/06/2011	10.30.34	Foto su PC
10	file:///C:/Documents%20and%20Settings/Test/Documents/Immagine/foto2fb.jpg	06/06/2011	10.30.59	Foto su PC
11	file:///C:/Documents%20and%20Settings/Test/Documents/Immagine/foto3fb.jpg	06/06/2011	10.32.08	Foto su PC
12	http://www.facebook.com/media/set/?set=a.2067549416706.2129797.1483935370	06/06/2011	10.32.52	Album "La mia prima laurea" - Alessio Marzaioli
13	http://www.facebook.com/media/set/?set=a.1050460910129.2009456.1483935370	06/06/2011	10.35.41	Album "Varie" - Francesco Pisano
14	http://www.facebook.com/aslan84?cropsuccess	06/06/2011	10.36.12	Profilo Francesco Pisano
15	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1307349369&nver=6.1.6206.0&wp=MBI&wreply=http:%2F%	06/06/2011	10.36.44	Accesso Hotmail
16	http://du108w.dub108.mail.live.com/mail/EditMessageLight.aspx?n=1817730688	06/06/2011	10.38.55	Editor Hotmail - aslan84@hotmail.it
17	http://du108w.dub108.mail.live.com/mail/SendMessageLight.aspx?_ec=1&n=1178752375	06/06/2011	10.39.50	Invio Mail - aslan84@hotmail.it
18	http://uk.ign.com	06/06/2011	10.43.03	Ign.com - Videogames
19	http://uk.ds.ign.com/index/top-reviewed.html	06/06/2011	10.43.47	Nintendo DS & DSi Reviews. The Best DS Games - Top Review
20	http://uk.ds.ign.com/index/upcoming.html	06/06/2011	10.44.58	New Nintendo DS & DSi Games. The Best DS Games
21	http://uk.ign.com/videos/2011/05/26/the-legend-of-zelda-ocarina-of-time-3d-epic-quest-trailer?objectid=77881	06/06/2011	10.46.55	Zelda: Ocarina of Time - 3D Epic Quest Trailer Video -
22	http://www.google.it	06/06/2011	10.48.38	traile fast 5 - Cerca con Google
23	http://www.comingsoon.it/Film/Scheda/Video/?key=47869	06/06/2011	10.49.51	Trailer - Fast & Furious 5 - Nuovo trailer italiano del film - Film (2
24	http://it.bing.com/search?q=download+trailer+&form=MSNH68&mkt=it-it	06/06/2011	10.50.44	download trailer - Bing
25	http://www.trailerdownload.net/movie/x-men-first-class/trailers/trailer-6049.html	06/06/2011	10.51.17	X-Men: First Class Movie Trailer - Trailerdownload.net
26	http://www.empiremovies.com/2011/05/20/new-transformers-3d-trailer/feed	06/06/2011	10.53.11	Empire Movies » New Transformers 3D Trailer Comments Feed
27	www.youtube.com	06/06/2011	10.53.49	
28	http://gdata.youtube.com/feeds/base/videos?q=trailer+transformers+3+ita&alt=rss&client=ytipi-youtube-search&v=2	06/06/2011	10.54.38	YouTube - trailer transformers 3 ita
29	http://www.macromedia.com/software/flash/about/installerRedirect.html	06/06/2011	10.55.09	Macromedia - Flash Player
30	http://www.youtube.com/watch?v=vR8Qe1kBgmg	06/06/2011	10.55.12	YouTube - Transformers 3 - The Dark of the Moon 3D
31	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1307350806&nver=6.1.6206.0&wp=MBI&wreply=http:%2F%	06/06/2011	11.00.39	Hotmail Accedi
32	file:///C:/Documents%20and%20Settings/Test/Desktop/presentazione_12_05_2011.pptx	06/06/2011	11.01.52	Visualizzazione di una presentazione powerpoint
33	file:///C:/Documents%20and%20Settings/Test/Documents/Lettera.doc	06/06/2011	15.14.51	Visualizzazione di un documento word
34	http://www3.unisa.it/facolta/scienze_mmffnn/index	06/06/2011	15.16.28	Scienze MM.FF.NN.
35	https://sso.unisa.it/idp/Authn/UserPassword	06/06/2011	15.17.10	Unisa Identity & access Management [lam@Unisa]
36	http://www.scienzefn.unisa.it/el-platform/course/view.php?id=316	06/06/2011	15.17.27	Corso: Reti di Calcolatori II - A.A. 2010/2011
37	http://www.scienzefn.unisa.it/el-platform/file.php/316/Rahnema.pdf	06/06/2011	15.17.30	

Strumenti utilizzati

- Autopsy Forensic Browser
 - Timeline dell'attività del sistema;
 - Navigazione dell'immagine dell'hdd e ricerca files per estensioni.
- OphCrack
 - Crack delle password di amministratore del sistema.
- Pasco
 - Estrazione delle informazioni di navigazione.
- LiveView e tools di Nirsoft
 - Ricerca delle password di completamento memorizzate dal browser.
- RegLookup e MiTeC Windows Registry Recovery
 - Estrazione delle informazioni dal registro di sistema.
- Tchunt/TCDDiscover e Passware kit enterprise
 - Ricerca\Decifrazione di una partizione cifrata con TrueCrypt.

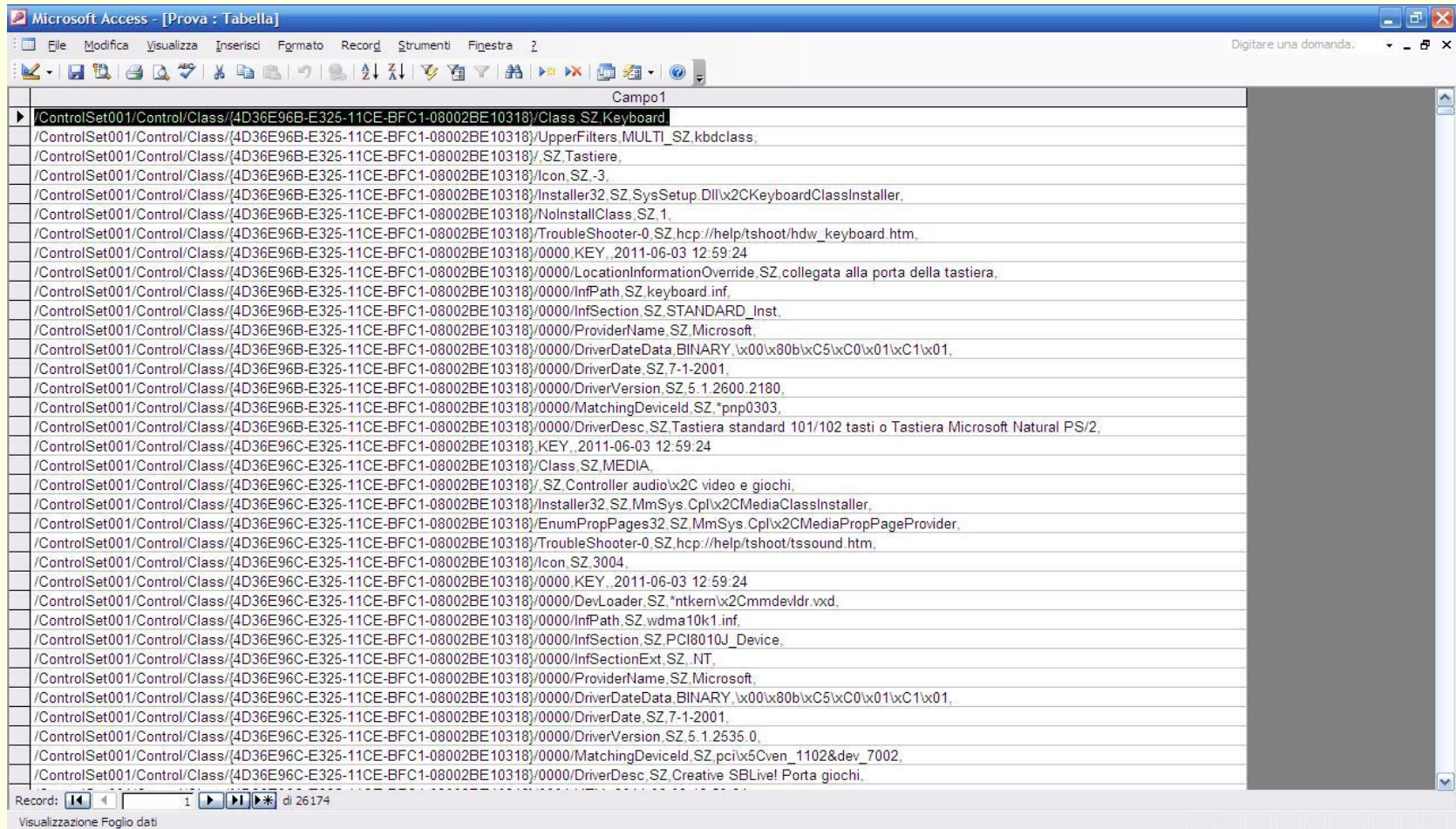
Analisi del registro del sistema

- Dove è contenuto il registro di Windows?
 - Nella cartella config di system32:
 - File “default”;
 - File “SAM”;
 - File “SECURITY”;
 - File “software”;
 - File “system”;
 - NTUSER.DAT nella cartella utente.

Tecniche per la ricerca dell'evidenza: Reglookup (1)

- Comando di linea utilizzato per leggere all'interno del registro di sistema;
- Genera un output CSV su stdout;
- Il file generato può essere importato da un programma per la gestione di fogli elettronici (Access).

Tecniche per la ricerca dell'evidenza: Reglookup (2)



The screenshot displays a Microsoft Access database window titled "Microsoft Access - [Prova : Tabella]". The window shows a table with a single column labeled "Campo 1". The table contains a list of registry paths, primarily related to keyboard drivers and hardware. The paths are listed in a single column, with the first row highlighted. The paths include:

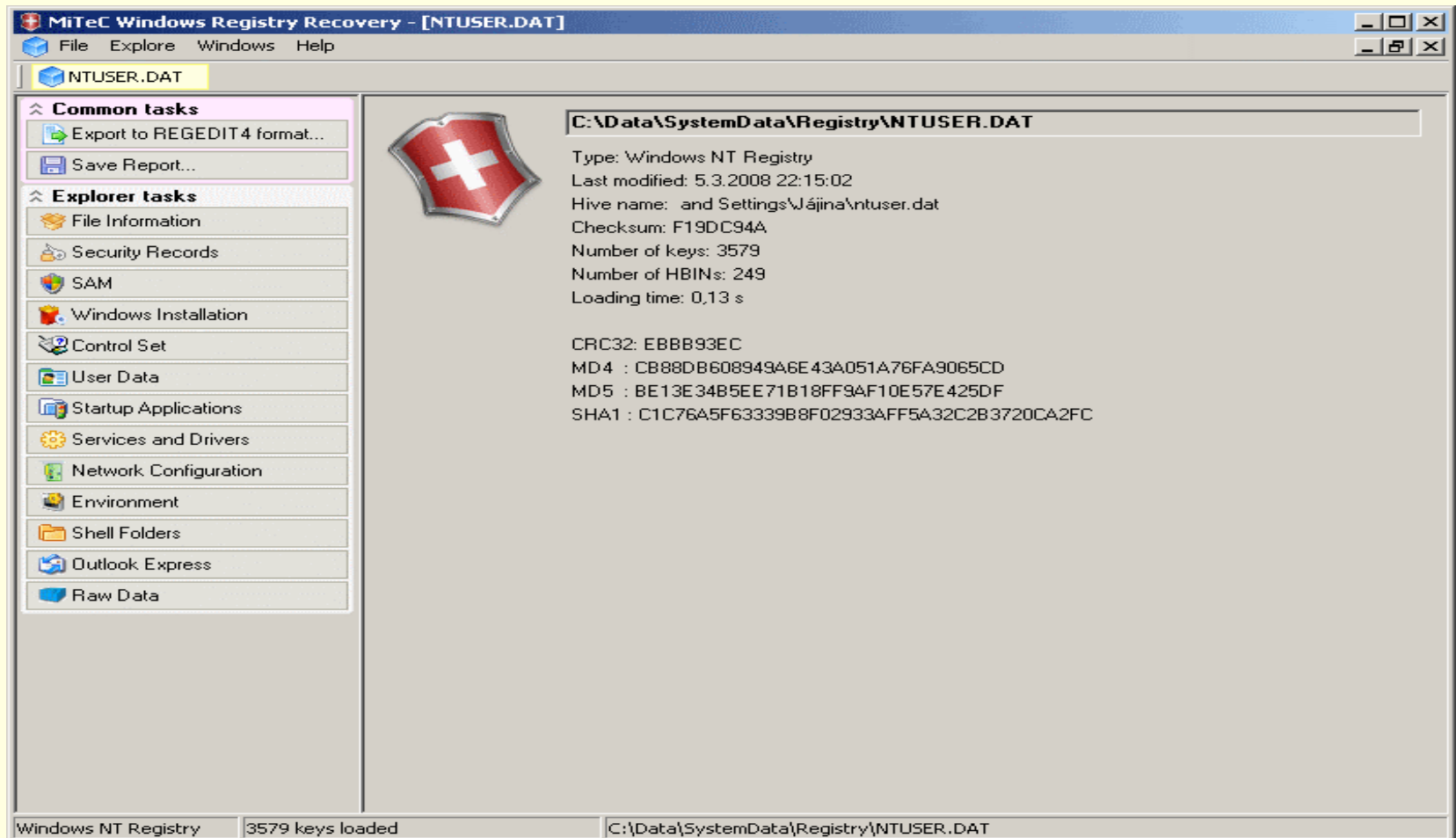
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/Class.SZ.Keyboard
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/UpperFilters.MULTI.SZ.kbdclass.
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/.SZ.Tastiere.
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/Icon.SZ.-3.
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/Installer32.SZ.SysSetup.Dllx2CKeyboardClassInstaller.
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/NoInstallClass.SZ.1.
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/TroubleShooter-0.SZ.hcp://help/tshoot/hdw_keyboard.htm.
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/0000.KEY.,2011-06-03 12:59:24
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/0000.LocationInformationOverride.SZ.collegata alla porta della tastiera.
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/0000/InfPath.SZ.keyboard.inf.
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/0000/InfSection.SZ.STANDARD_Inst.
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/0000/ProviderName.SZ.Microsoft.
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/0000/DriverDateData.BINARY.\x00\x80bxC5\xC0\x01\xC1\x01.
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/0000/DriverDate.SZ.7-1-2001.
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/0000/DriverVersion.SZ.5.1.2600.2180.
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/0000/MatchingDeviceId.SZ.*pnp0303.
- /ControlSet001/Control/Class/{4D36E96B-E325-11CE-BFC1-08002BE10318}/0000/DriverDesc.SZ.Tastiera standard 101/102 tasti o Tastiera Microsoft Natural PS/2.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/KEY.,2011-06-03 12:59:24
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/Class.SZ.MEDIA.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/.SZ.Controller audio\x2C video e giochi.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/Installer32.SZ.MmSys.Cpl\x2CMediaClassInstaller.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/EnumPropPages32.SZ.MmSys.Cpl\x2CMediaPropPageProvider.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/TroubleShooter-0.SZ.hcp://help/tshoot/tssound.htm.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/Icon.SZ.3004.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/0000.KEY.,2011-06-03 12:59:24
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/0000/DevLoader.SZ.*ntkern\x2Cmmdevldr.vxd.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/0000/InfPath.SZ.wdma10k1.inf.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/0000/InfSection.SZ.PCI8010J_Device.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/0000/InfSectionExt.SZ._NT.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/0000/ProviderName.SZ.Microsoft.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/0000/DriverDateData.BINARY.\x00\x80bxC5\xC0\x01\xC1\x01.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/0000/DriverDate.SZ.7-1-2001.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/0000/DriverVersion.SZ.5.1.2535.0.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/0000/MatchingDeviceId.SZ.pci\x5Cven_1102&dev_7002.
- /ControlSet001/Control/Class/{4D36E96C-E325-11CE-BFC1-08002BE10318}/0000/DriverDesc.SZ.Creative.SBLive! Porta giochi.

The bottom of the window shows a record navigation bar with "Record: 1 di 26174" and a "Visualizzazione Foglio dati" button.

MiTeC Windows Registry Recovery

- Freeware;
- Tool grafico che mostra informazioni del sistema organizzando i dati del registro;
- Funziona su piattaforma Windows;
- Non c'è bisogno di installazione;
- Funziona su dati offline (molto adatto all'analisi forense);
- Consigliato da Andrea Ghirardini e Gabriele Faggioli (Computer Forensics – Apogeo).

MiTeC Windows Registry Recovery: Schermata iniziale



Strumenti utilizzati

- Autopsy Forensic Browser
 - Timeline dell'attività del sistema;
 - Navigazione dell'immagine dell'hdd e ricerca files per estensioni.
- OphCrack
 - Crack delle password di amministratore del sistema.
- Pasco
 - Estrazione delle informazioni di navigazione.
- LiveView e tools di Nirsoft
 - Ricerca delle password di completamento memorizzate dal browser.
- RegLookup e MiTeC Windows Registry Recovery
 - Estrazione delle informazioni dal registro di sistema.
- Tchunt/TCDDiscover e Passware kit enterprise
 - Ricerca\Decifrazione di una partizione cifrata con TrueCrypt.

Ricerca di una partizione o file cifrata con TrueCrypt

- Cos'è TrueCrypt?
 - Software Open Source per cifrare dischi
 - Crea un disco virtuale cifrato e permette di montarlo come se fosse un disco fisico;
 - Permette di cifrare una partizione o un disco su cui è installato Windows;
 - Permette di cifrare interi dischi o dispositivi USB.

<http://www.truecrypt.org/>

Tracce di utilizzo di TrueCrypt

- TrueCrypt può essere utilizzato in modalità portable -> senza installazione;
- Un volume di TrueCrypt va montato per essere utilizzato;
- Il registro di Windows memorizza tutti i dispositivi montati sul sistema;
 - Nell'entry del registro di sistema: MountedDevices

Ricerca di una partizione o file cifrato con TrueCrypt

- Primo problema:
 - I dati cifrati appaiono come una sequenza pseudo-random -> difficoltà ad individuare una partizione virtuale cifrata!
- Soluzione:
 - Un software in grado di discriminare una partizione cifrata di TrueCrypt in funzione di alcune sue caratteristiche -> tchunt

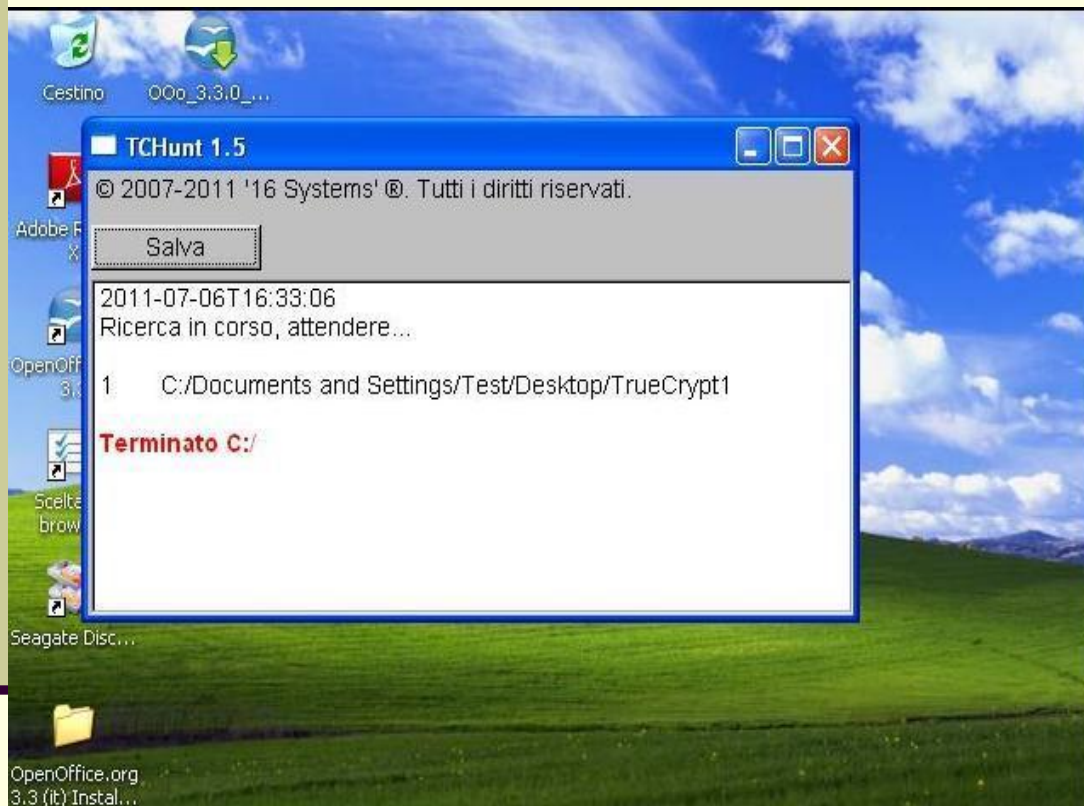
Tchunt e TCDDiscover

- Software Freeware che ricerca dei files che abbiano determinate caratteristiche:
 - La dimensione del file modulo 512 è 0;
 - La dimensione del file è almeno di 19KB;
 - Il contenuto del file sospetto deve superare un test chi-quadro;
 - Il file sospetto non contiene un file header comune.
- Tchunt lavora su un classico disco, TCDDiscover lavora su un'immagine dd.

<http://16s.us/TCHunt/faq/>

Tchunt

- Il software individua un certo numero di falsi positivi che però è abbastanza semplice riuscire a scartare
- Non è in grado di distinguere tra dati cifrati o dati random



Trovata la partizione... E poi?

- Una volta individuata una possibile partizione cifrata con Truecrypt si può:
 - Provare ad individuare la password;
 - Provare a decifrare il contenuto della partizione;

Individuazione della password: Software Free vs Software a pagamento

- Passware kit enterprise 10.0
 - Permette di provare un attacco brute force
 - Una password solo alfabetica di 7 caratteri in inglese in circa 4 ore.
- AccessData DNA e Tableau TACC1441
 - Permette un attacco distribuito tra tutte le macchine che dispongono del software installato con aggiunta di acceleratore hardware (5315 \$).
- TCBrute 2.7 (freeware)
 - Permette un attacco a forza bruta ad una partizione truecrypt con utilizzo di una wordlist preconfezionata con altri software in base ad una minima conoscenza della password utente (non un vero e proprio attacco su tutte le keywords disponibili).

Software free Vs Software a pagamento

- Passware kit enterprise 10.5
 - Un kit a pagamento, ma dal prezzo accessibile a tutti (795 \$).
 - Promette di:
 - Decifrare un volume Truecrypt in pochi minuti.
 - In realtà:
 - Può farlo solo se si riesce ad avere un'immagine della memoria quando il volume è ancora montato (live analysis);
 - Se trova qualcosa nel file hiberfill.sys.

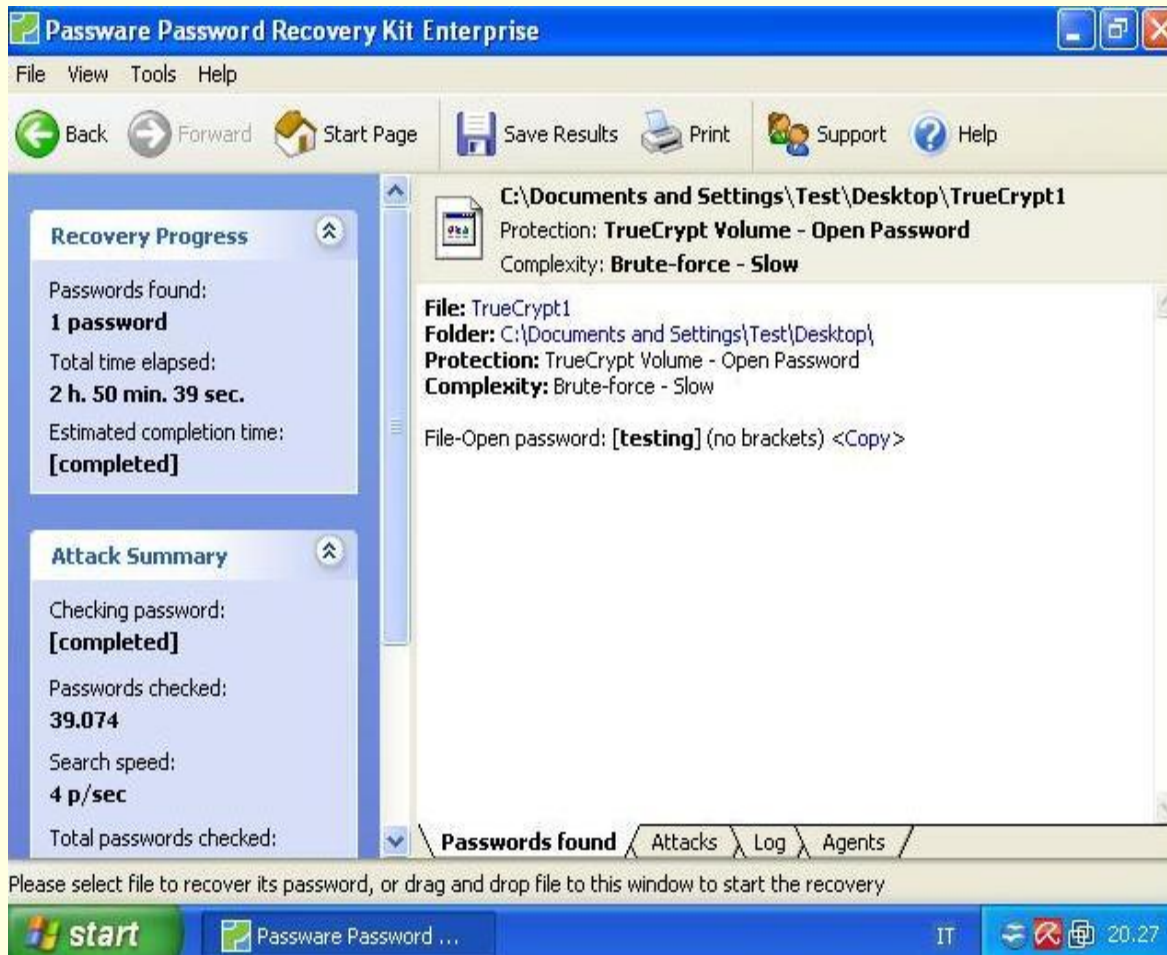
Passware kit enterprise 10.0

- Non fornisce la password inserita dall'utente;
- Si ipotizza che possa lavorare sulle chiavi di round generate dall'algoritmo di crittografia;
- Tali chiavi sono memorizzate in RAM e sono utilizzate per cifrare il disco;
- Individuate tali chiavi è possibile decifrare il disco senza per forza conoscere la password iniziale.

Nel nostro caso

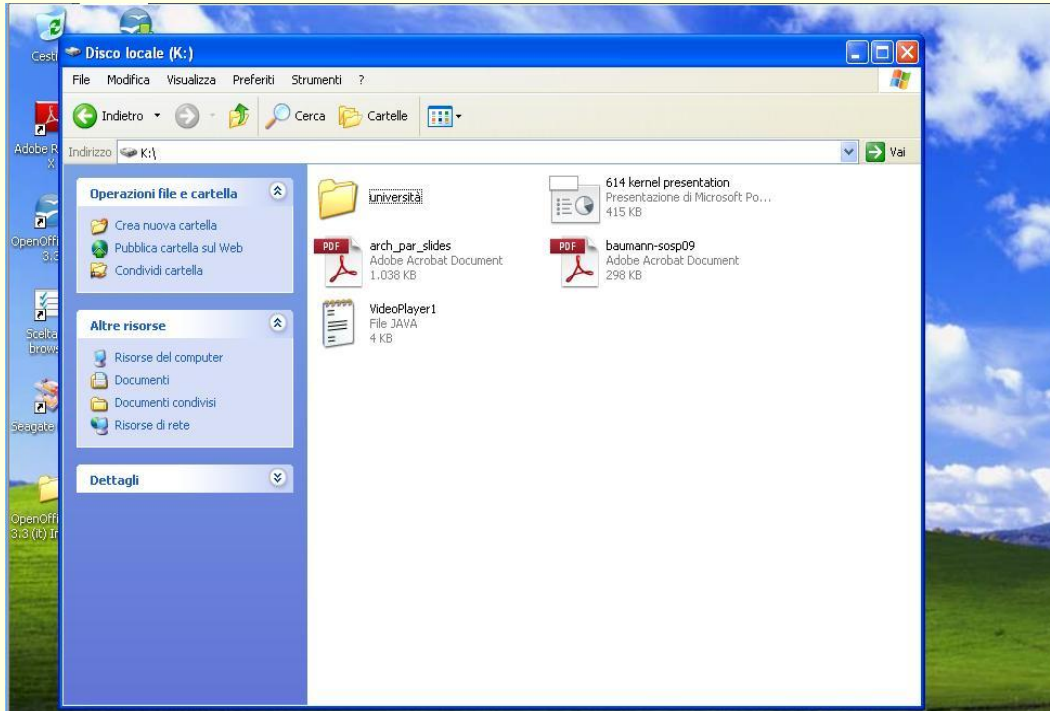
- Niente dump della memoria con partizione montata;
- Niente file hiberfill.sys;
- Attacco a dizionario con Passware kit su un range di chiavi di lunghezza tra 5 e 8 caratteri in lingua inglese (Password di un utente non molto scaltro..).

Nel nostro caso... 2



- Password trovata!
- Tempo impiegato: 2h e 50 min;
- In funzione su macchina virtuale (può fare di meglio).

Nel nostro caso... 3



- Contenuto della partizione cifrata:
 - Due files .pdf;
 - Una presentazione .ppt;
 - Un file Java;
 - Una cartella vuota.

Indice - Parte II

- Ambiente Hardware ed Attività dell'indagato
 - Ambiente hardware/software
 - Attività dell'indagato
- Identificazione
 - Il nostro caso
- Conservazione
 - Conservazione tramite Write Blocker
 - Write Blocker Tableau
 - GuyMager
 - Air 2.0
 - Duplicazione su supporto ottico
- Analisi
 - Attività di analisi
 - Strumenti utilizzati
- Incidenti di percorso
- Conclusioni

. . . Incidenti di percorso . . .(1)

- Problematiche di natura tecnica:
 - Fondamentale è procurarsi hw con gli ultimi standard in termini di velocità
 - Un DD di un HDD di 20 Gb con verifica hash completato in 6h e 30min con collegamento USB 1.0;
 - Prima configurazione di macchina forense con processore 333 MHz e 256 Mb di RAM, fallita.

. . . Incidenti di percorso . . . (2)

- Problematiche di natura software
 - Installazione della distribuzione forense
 - Provate varie distribuzioni live di CAINE su DVD, CD e chiavetta USB.

Indice - Parte II

- Ambiente Hardware ed Attività dell'indagato
 - Ambiente hardware/software
 - Attività dell'indagato
- Identificazione
 - Il nostro caso
- Conservazione
 - Conservazione tramite Write Blocker
 - Write Blocker Tableau
 - GuyMager
 - Air 2.0
 - Duplicazione su supporto ottico
- Analisi
 - Attività di analisi
 - Strumenti utilizzati
- Incidenti di percorso
- Conclusioni

Conclusioni...1

- Informazioni principali sull'utente
 - Owner: **Test**
 - Product ID: **55274-641-3126376-23064**
 - Product Key: **BHFBH-*****_*****_*****_*******
 - Installed Date: **25/05/2011 9.09.57**
 - System Root: **C:\WINDOWS**
- Dati dell' utente
 - Password amministratore (OphCrack) **Test**
 - Password di completamento browser :
 - aslan84@hotmail.it **12******
 - a.marzaioli2@studenti.unisa.it **18******
 - Volume TrueCrypt Individuato:
 - **C:/Documents and Settings/Test/Desktop/TrueCrypt1**
 - Password Volume TrueCrypt : **testing**

Conclusioni..2

■ Hardware

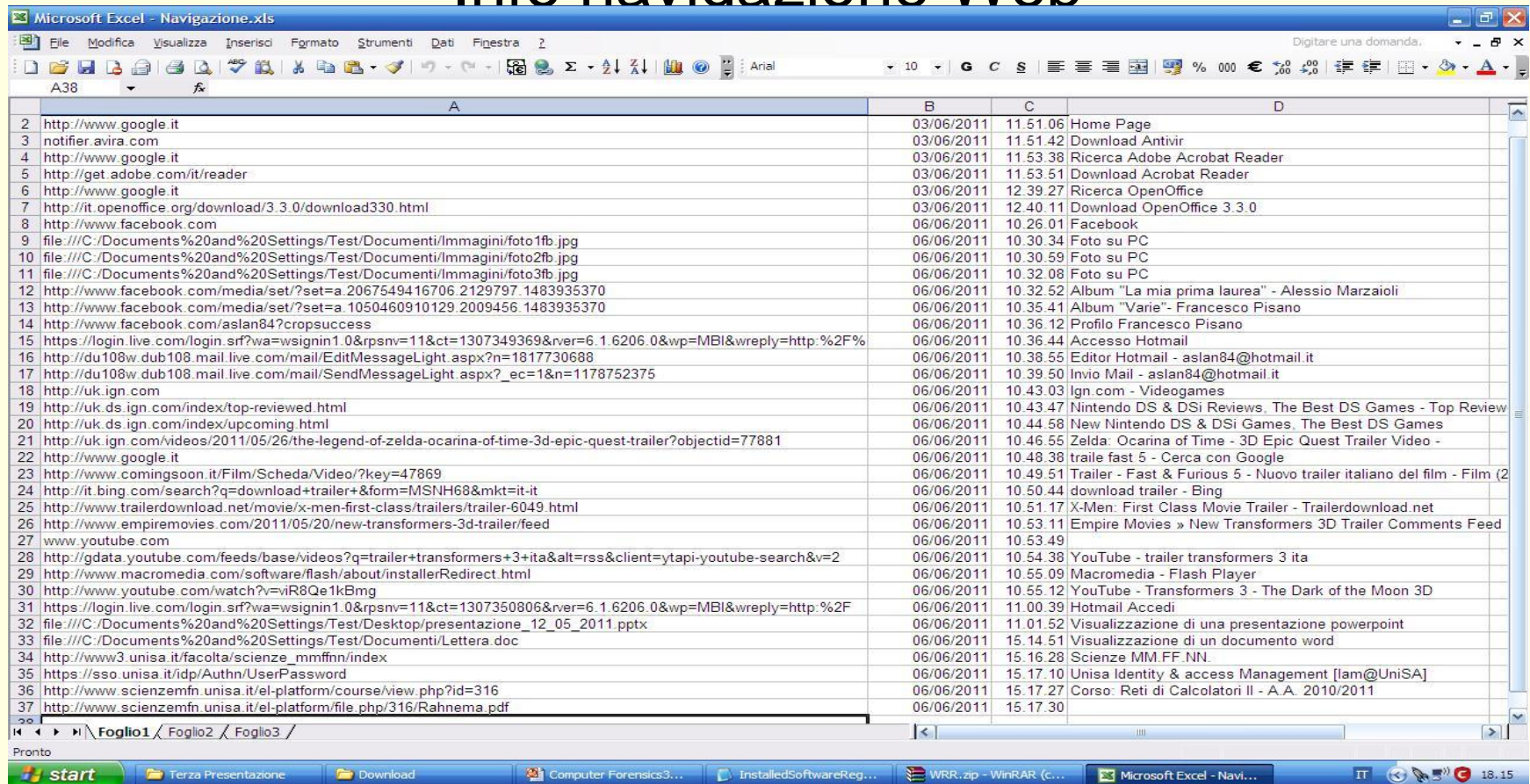
- CPU: AMD Athlon
- Monitor: AcerAL707
- Graphics: NVIDIA GeForce4 MMX 440
- Sound: Creative SBLive!
- Network: NIC Fast Ethernet PCI Realtek RTL8139 Family

■ Network

- IPAddress: 172.**.**.***
- SubnetMask: 255.***.***.***
- DefaultGateway: 172.**.**.***
- NameServer: 193.***.***.*

Conclusioni...3

Info navigazione Web



The screenshot shows a Microsoft Excel spreadsheet titled "Microsoft Excel - Navigazione.xls". The spreadsheet contains a list of web navigation events, with columns for date, time, and description. The data is organized into four columns: A (URL), B (Date), C (Time), and D (Description). The table lists various activities such as visiting Google, downloading software, and accessing social media.

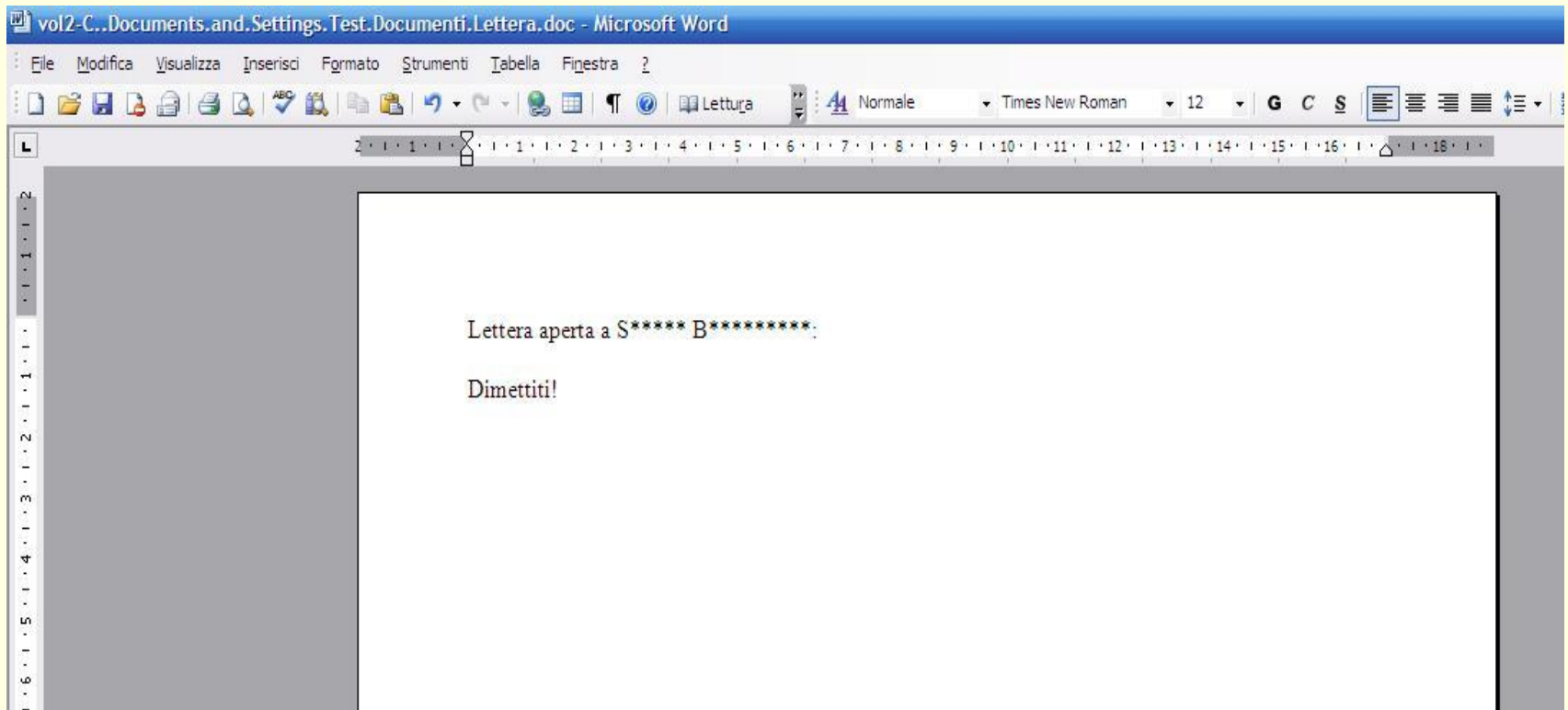
	A	B	C	D
2	http://www.google.it	03/06/2011	11 51.06	Home Page
3	notifier.avira.com	03/06/2011	11 51.42	Download Antivir
4	http://www.google.it	03/06/2011	11 53.38	Ricerca Adobe Acrobat Reader
5	http://get.adobe.com/it/reader	03/06/2011	11 53.51	Download Acrobat Reader
6	http://www.google.it	03/06/2011	12 39.27	Ricerca OpenOffice
7	http://it.openoffice.org/download/3.3.0/download330.html	03/06/2011	12 40.11	Download OpenOffice 3.3.0
8	http://www.facebook.com	06/06/2011	10 26.01	Facebook
9	file:///C:/Documents%20and%20Settings/Test/Documents/immagini/foto1fb.jpg	06/06/2011	10 30.34	Foto su PC
10	file:///C:/Documents%20and%20Settings/Test/Documents/immagini/foto2fb.jpg	06/06/2011	10 30.59	Foto su PC
11	file:///C:/Documents%20and%20Settings/Test/Documents/immagini/foto3fb.jpg	06/06/2011	10 32.08	Foto su PC
12	http://www.facebook.com/media/set/?set=a.2067549416706.2129797.1483935370	06/06/2011	10 32.52	Album "La mia prima laurea" - Alessio Marzaioli
13	http://www.facebook.com/media/set/?set=a.1050460910129.2009456.1483935370	06/06/2011	10 35.41	Album "Varie" - Francesco Pisano
14	http://www.facebook.com/aslan84?cropssuccess	06/06/2011	10 36.12	Profilo Francesco Pisano
15	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1307349369&rver=6.1.6206.0&wp=MBI&wreply=http:%2F%2Fdu108w.dub108.mail.live.com/mail/EditMessageLight.aspx?n=1817730688	06/06/2011	10 36.44	Accesso Hotmail
16	http://du108w.dub108.mail.live.com/mail/EditMessageLight.aspx?n=1817730688	06/06/2011	10 38.55	Editor Hotmail - aslan84@hotmail.it
17	http://du108w.dub108.mail.live.com/mail/SendMessageLight.aspx?_ec=1&n=1178752375	06/06/2011	10 39.50	Invio Mail - aslan84@hotmail.it
18	http://uk.ign.com	06/06/2011	10 43.03	Ign.com - Videogames
19	http://uk.ds.ign.com/index/top-reviewed.html	06/06/2011	10 43.47	Nintendo DS & DSi Reviews, The Best DS Games - Top Review
20	http://uk.ds.ign.com/index/upcoming.html	06/06/2011	10 44.58	New Nintendo DS & DSi Games, The Best DS Games
21	http://uk.ign.com/videos/2011/05/26/the-legend-of-zelda-ocarina-of-time-3d-epic-quest-trailer?objectid=77881	06/06/2011	10 46.55	Zelda: Ocarina of Time - 3D Epic Quest Trailer Video -
22	http://www.google.it	06/06/2011	10 48.38	traile fast 5 - Cerca con Google
23	http://www.comingsoon.it/Film/Scheda/Video/?key=47869	06/06/2011	10 49.51	Trailer - Fast & Furious 5 - Nuovo trailer italiano del film - Film (2
24	http://it.bing.com/search?q=download+trailer+&form=MSNH68&mkt=it-it	06/06/2011	10 50.44	download trailer - Bing
25	http://www.trailerdownload.net/movie/x-men-first-class/trailers/trailer-6049.html	06/06/2011	10 51.17	X-Men: First Class Movie Trailer - Trailerdownload.net
26	http://www.empiremovies.com/2011/05/20/new-transformers-3d-trailer/feed	06/06/2011	10 53.11	Empire Movies » New Transformers 3D Trailer Comments Feed
27	www.youtube.com	06/06/2011	10 53.49	
28	http://gdata.youtube.com/feeds/base/videos?q=trailer+transformers+3+ita&alt=rss&client=ytapi-youtube-search&v=2	06/06/2011	10 54.38	YouTube - trailer transformers 3 ita
29	http://www.macromedia.com/software/flash/about/installerRedirect.html	06/06/2011	10 55.09	Macromedia - Flash Player
30	http://www.youtube.com/watch?v=viR8Qe1kBmg	06/06/2011	10 55.12	YouTube - Transformers 3 - The Dark of the Moon 3D
31	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1307350806&rver=6.1.6206.0&wp=MBI&wreply=http:%2F%2Ffile:///C:/Documents%20and%20Settings/Test/Desktop/presentazione_12_05_2011.pptx	06/06/2011	11 00.39	Hotmail Accedi
32	file:///C:/Documents%20and%20Settings/Test/Desktop/presentazione_12_05_2011.pptx	06/06/2011	11 01.52	Visualizzazione di una presentazione powerpoint
33	file:///C:/Documents%20and%20Settings/Test/Documents/Lettera.doc	06/06/2011	15 14.51	Visualizzazione di un documento word
34	http://www3.unisa.it/facolta/scienze_mmffnn/index	06/06/2011	15 16.28	Scienze MM FF NN.
35	https://sso.unisa.it/idp/Authn/UserPassword	06/06/2011	15 17.10	Unisa Identity & access Management [lam@Unisa]
36	http://www.scienzefmh.unisa.it/el-platform/course/view.php?id=316	06/06/2011	15 17.27	Corso: Reti di Calcolatori II - A.A. 2010/2011
37	http://www.scienzefmh.unisa.it/el-platform/file.php/316/Rahnema.pdf	06/06/2011	15 17.30	

Conclusioni... 4

- Circa 30 Immagini visualizzate dal Social Network Facebook (risoluzione 720x540 o 540x720)
 - File immagine visitata su facebook
40388_1602529067536_1365368633_1604237_2321885_a
[1].jpg visitato 2 volte, la prima risale al 06/06/2011 ore
10:29:53;
 - File immagine visitata su facebook
40980_1602526667476_1365368633_1604204_6913637_n
[1].jpg visitato 2 volte, la prima risale al 06/06/2011 ore
10:29:34;
 - File immagine visitata su facebook
44638_1602527227490_1365368633_1604211_6127116_n
[1].jpg visitato 2 volte, la prima risale al 06/06/2011 ore
10:29:50;
- 3 files sono stati scaricati nella cartella C:\Documents and Settings\Test\Documenti\Immagini in cui si trovano ulteriori 2 immagini.

Conclusioni... 5

- File lettera.doc visitato 5 volte, la prima risale al 06/06/2011 ore 15:14:45



Conclusioni... 6

- Documenti Pdf visualizzati dall' utente online;
- File Rahnema.pdf visitata on-line, una sola volta il 06/06/2011 alle ore 15:17:30;
- File TrueCrypt User Guide.pdf visitato on-line, una sola volta il 06/06/2011 alle ore 15:26:04.

Conclusioni... 7

- 2 Video Avi cifrati con Windows in C:\Documents and Settings\All Users\Documenti\Video\Video
 - MOV00038.avi
 - video_laurea.avi
- Prelevati e visualizzati tranquillamente dalla macchina virtuale (l'accesso è dell'utente e quindi i file sono disponibili)

Beccato! (Grazie)

