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

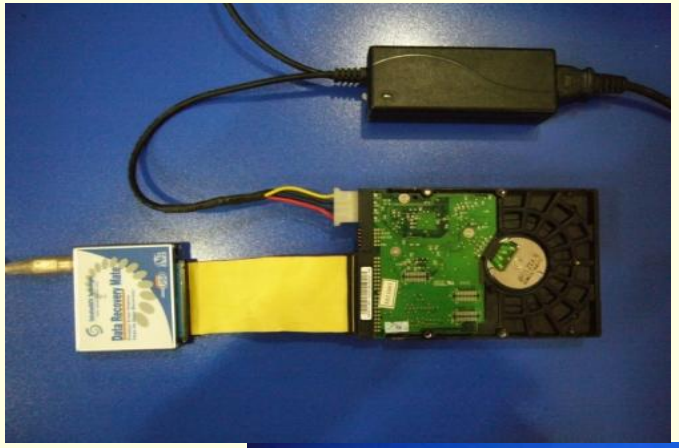
La scelta di un write blocker software è indubbiamente economica, perché non richiede l'acquisto di particolari dispositivi.

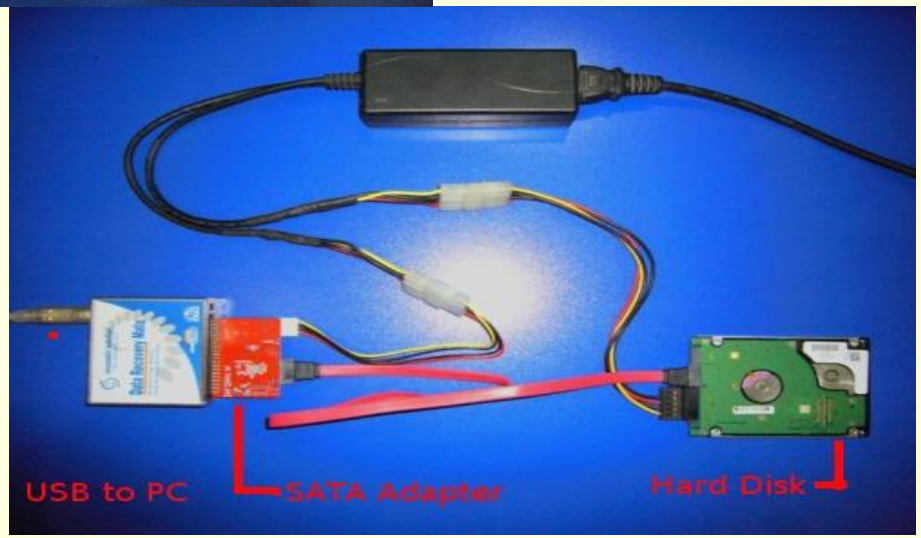
Ovviamente il digital forenser deve testare costantemente la validità di questa metodologia con la nascita e lo sviluppo dei nuovi standard di connessione.

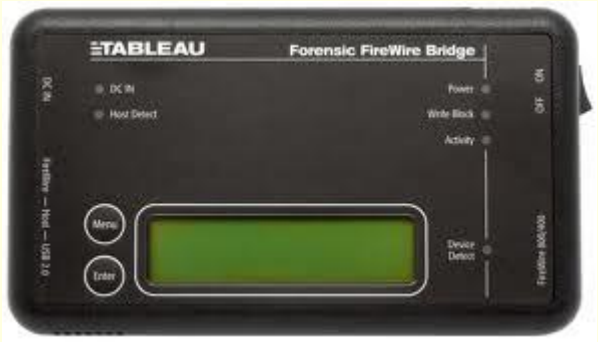
Write Blocker Hardware

- 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



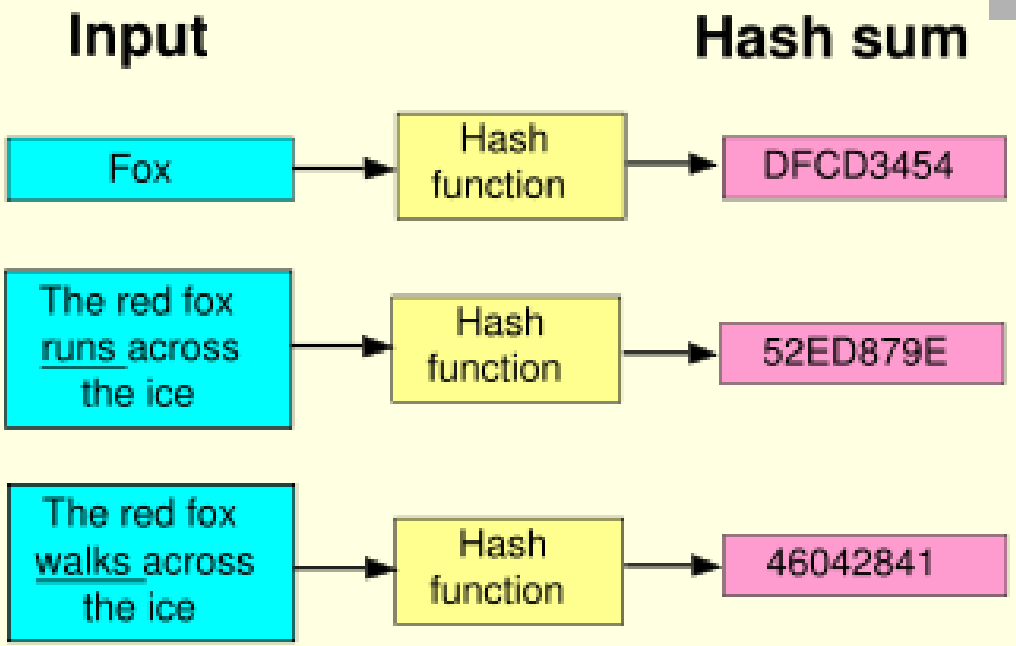




Verifica

- 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.

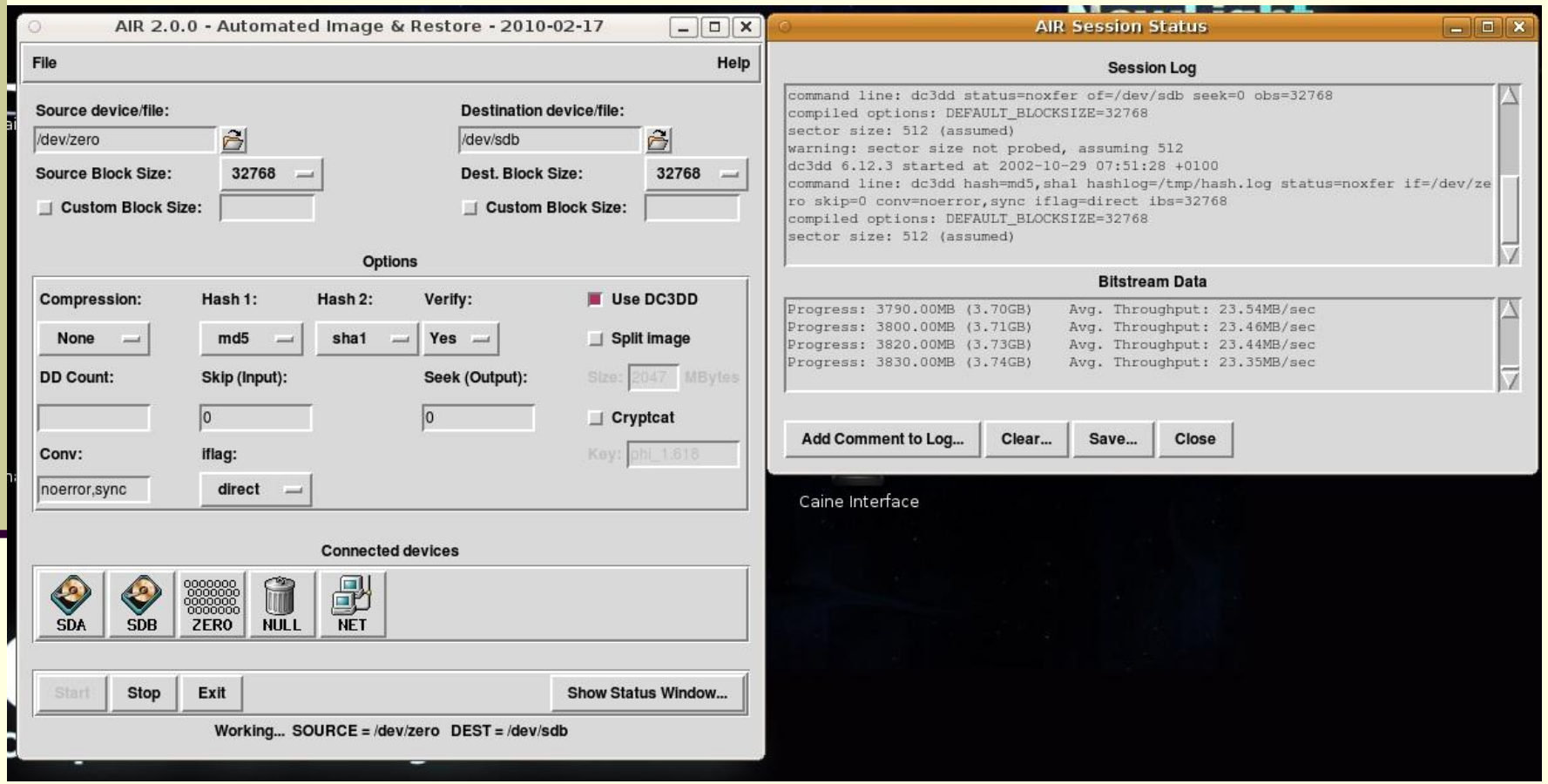
Indice - Parte II

- 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

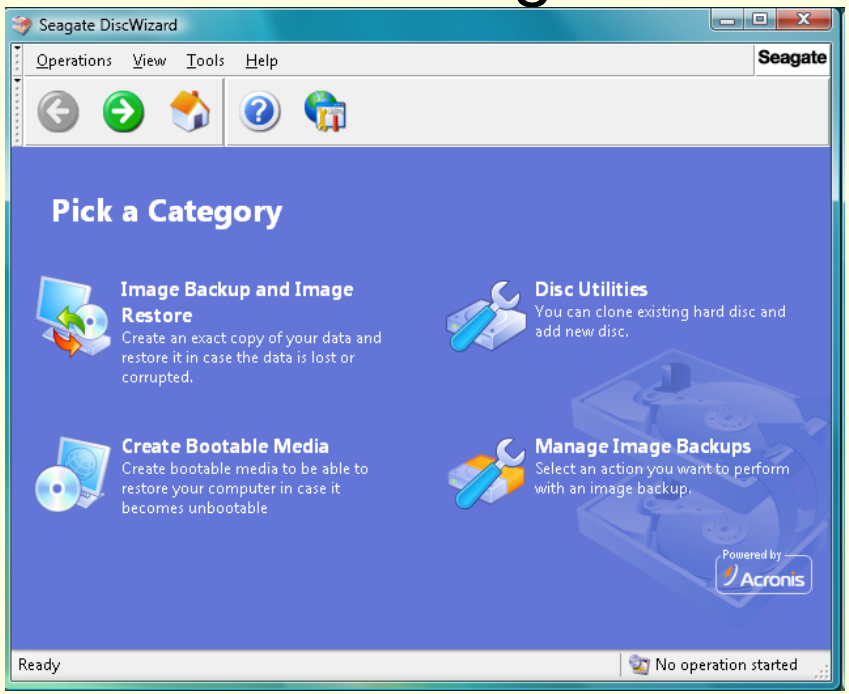


Attività dell'indagato: Software utilizzati

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

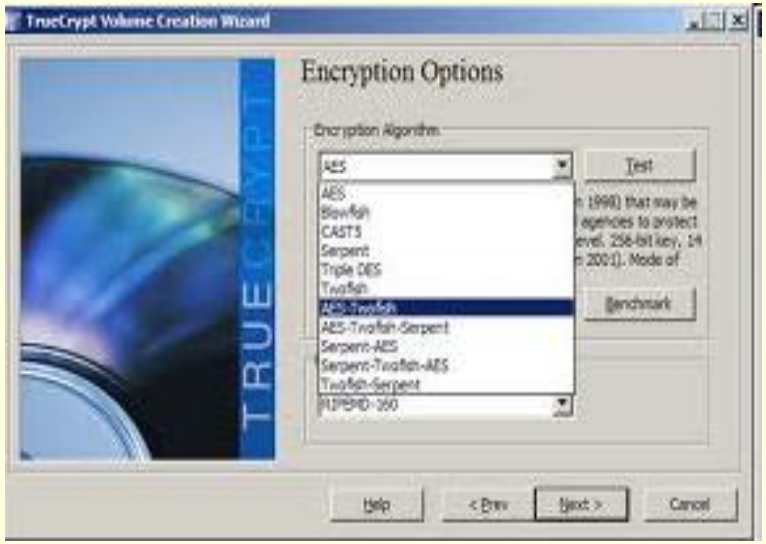
Seagate DiscWizard

- 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:

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

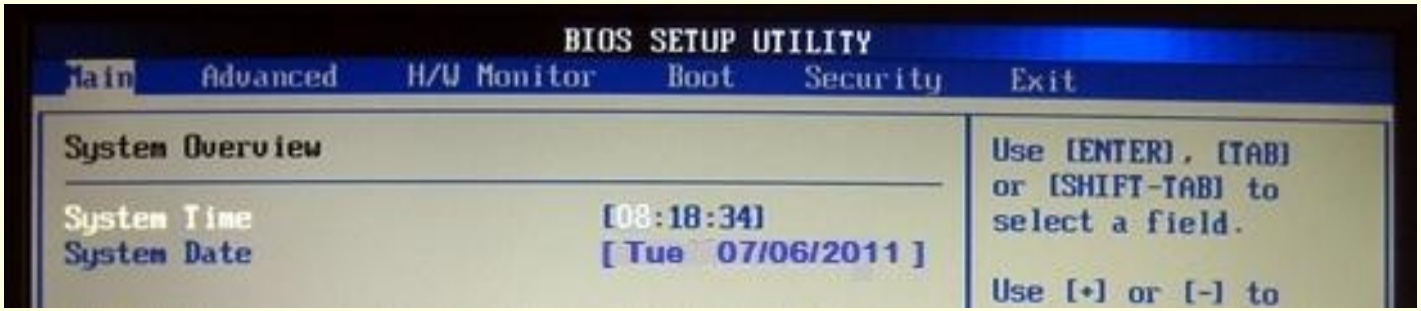
- Abbiamo sequestrato un hard disk (S/N WMA6K3300935)

Indice - Parte II

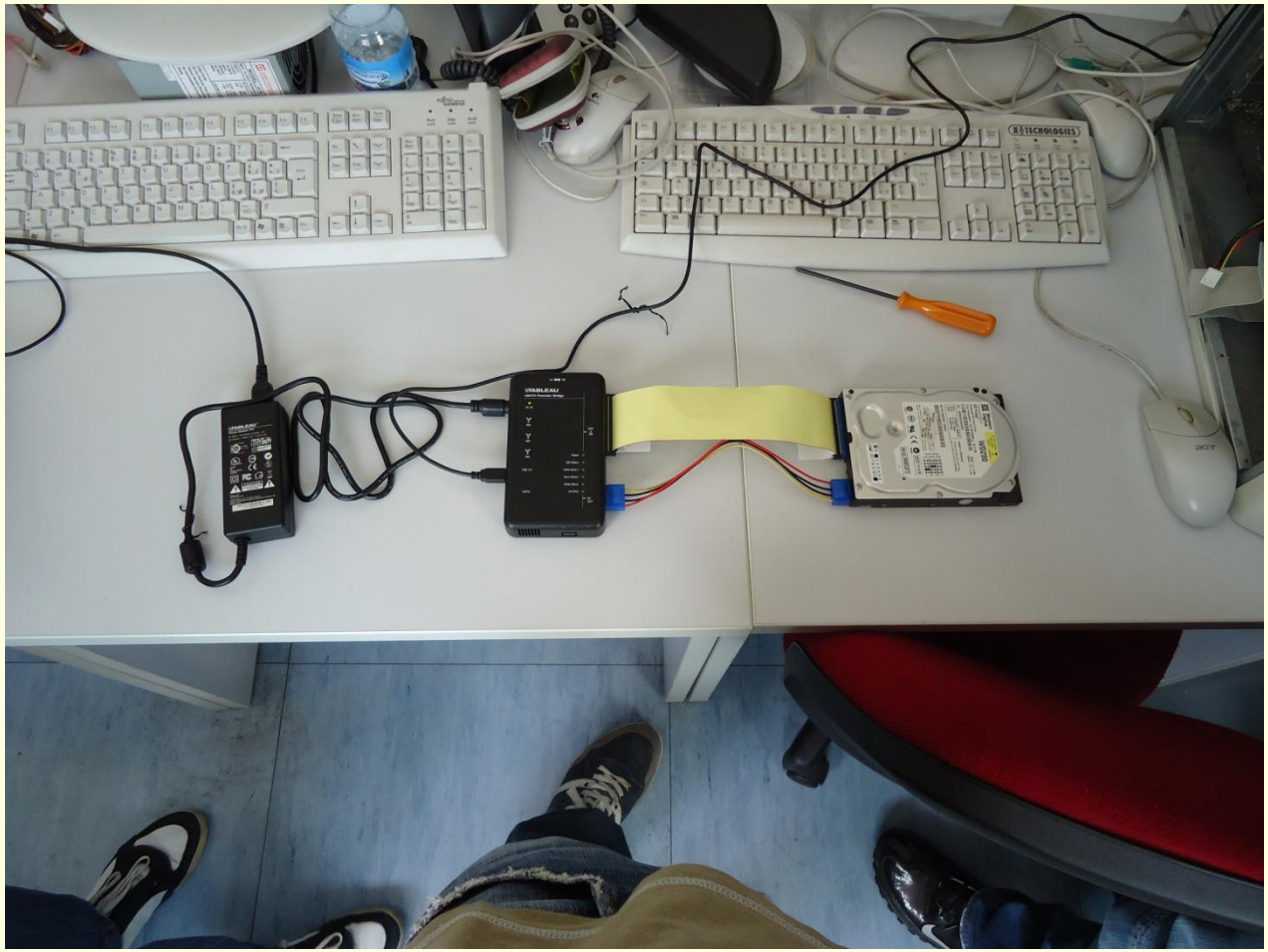
- Ambiente Hardware ed Attività dell'indagato
  - Ambiente hardware/software
  - Attività dell'indagato
- Identificazione
  - Il nostro caso
- Conservazione
  - Conservazione tramite Write Blocker
  - Write Blocker Tableau
  - GuyMager
  - Air 2.0
  - Duplicazione su supporto ottico
- Analisi
  - Attività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

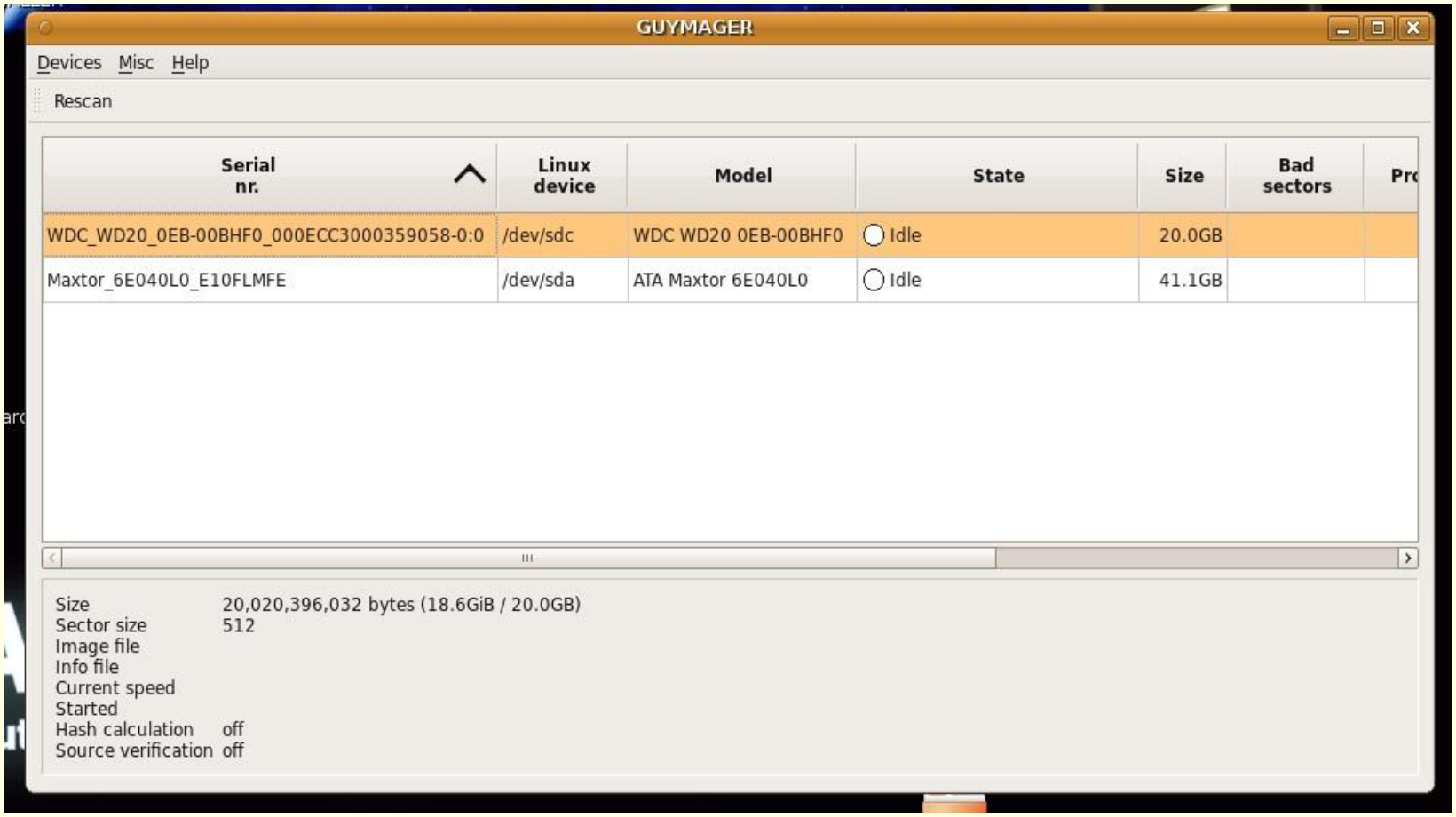
Serial nr.	Linux device	Model	State	Size	Bad sectors	Pro
WDC_WD20_0EB-00BHF0_000ECC3000359058-0:0	/dev/sdc	WDC WD20 0EB-00BHF0	Idle	20.0GB		

- 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

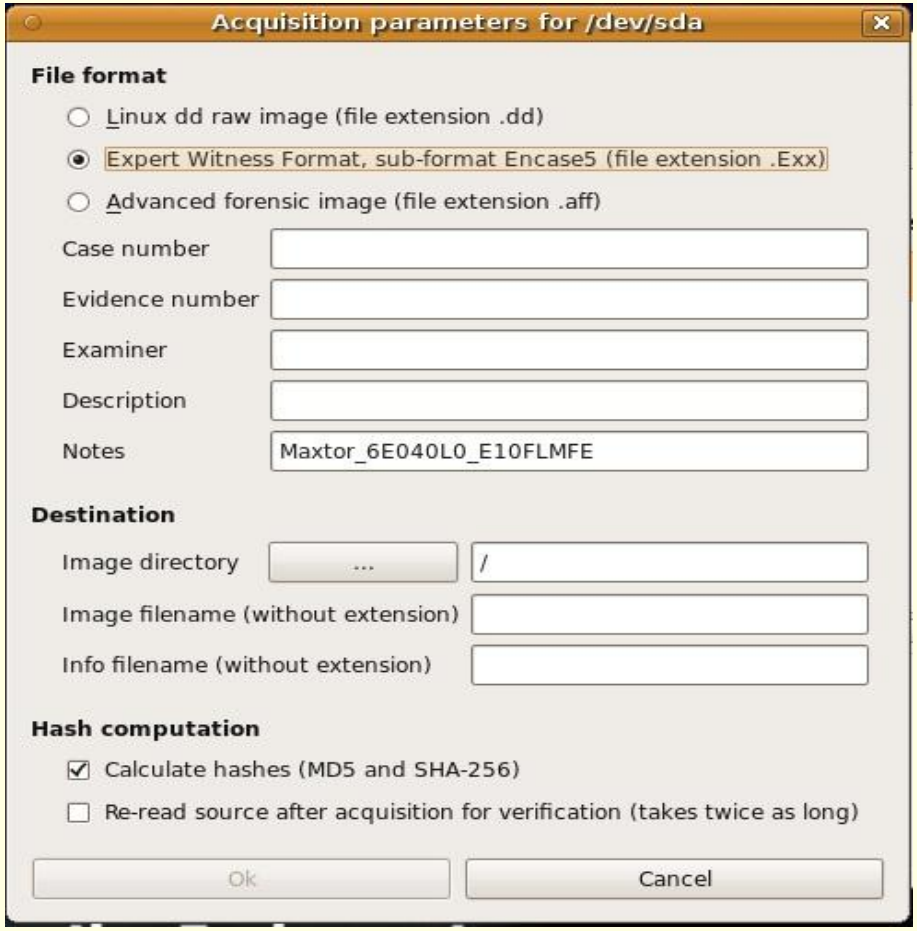
Guymager: Selezione dei dispositivi



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.

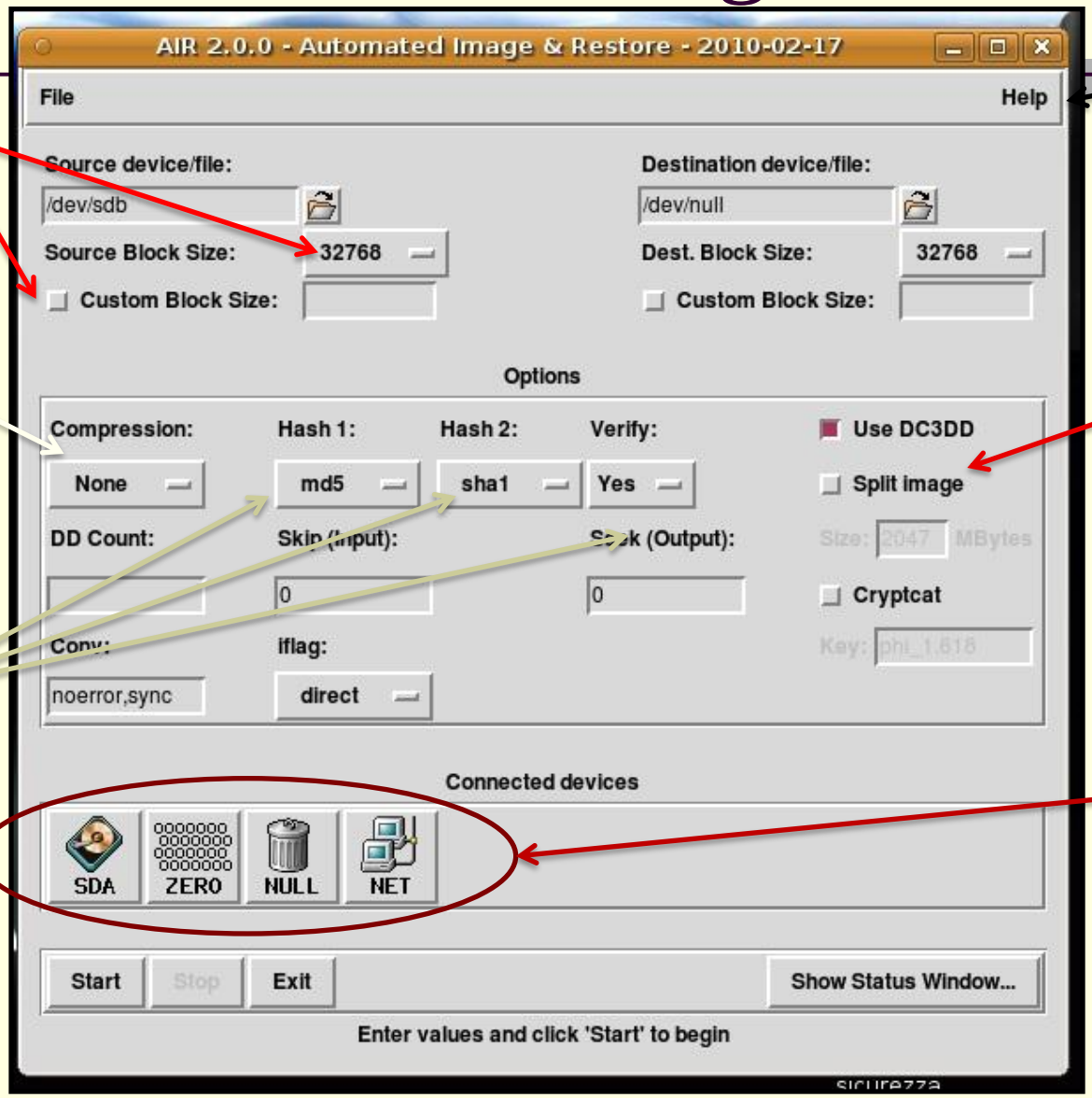
Guymager: Schermata di acquisizione



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 | ai
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=n

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

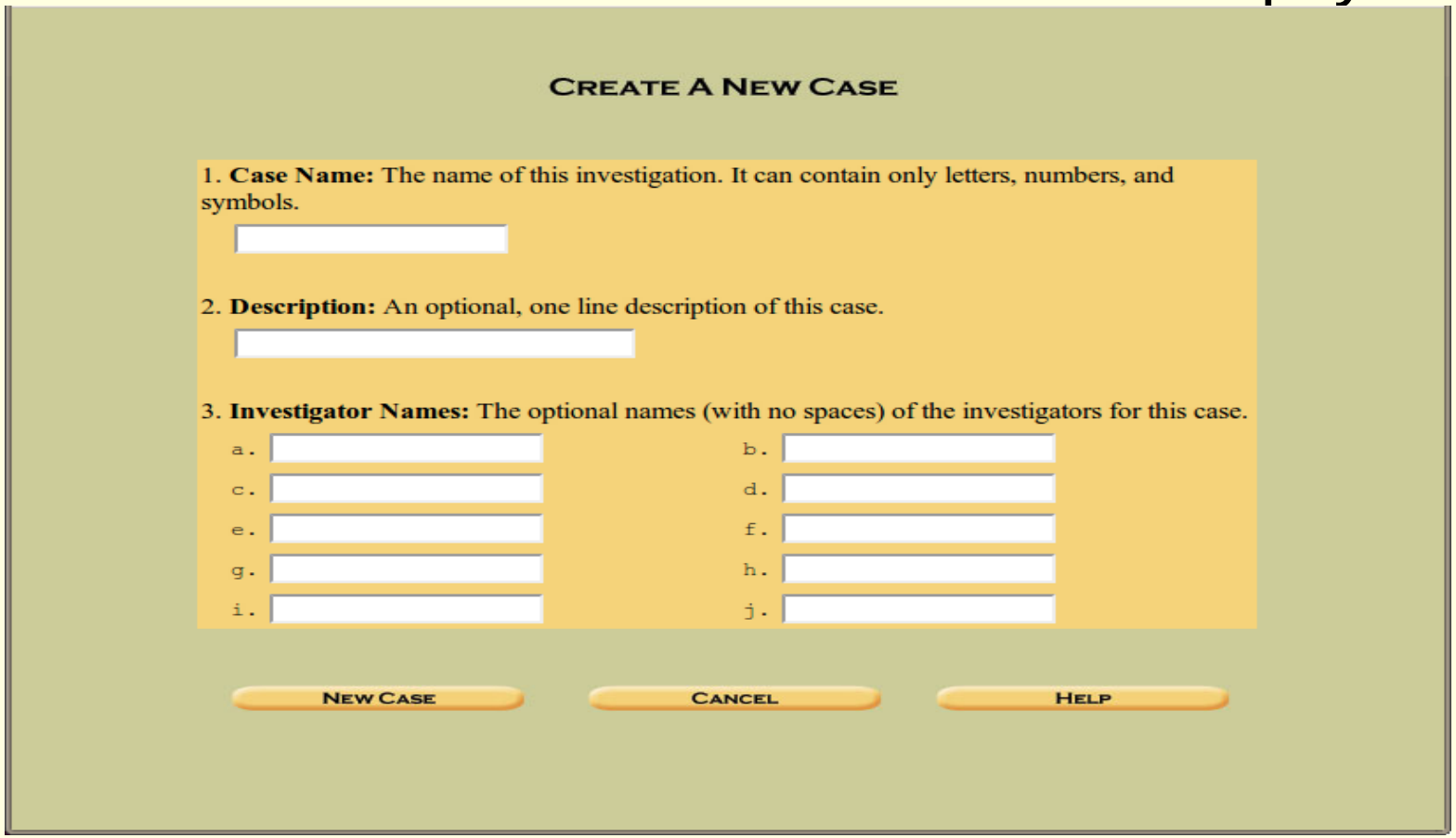
- Tramite l'opzione split di Air;
- Copia su 5 dvd;
- Calcolo dell'hash md5 su ogni split per verificarne la correttezza;
  - Infatti un dvd è risultato corrotto!
- Lavoro sulla copia;

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

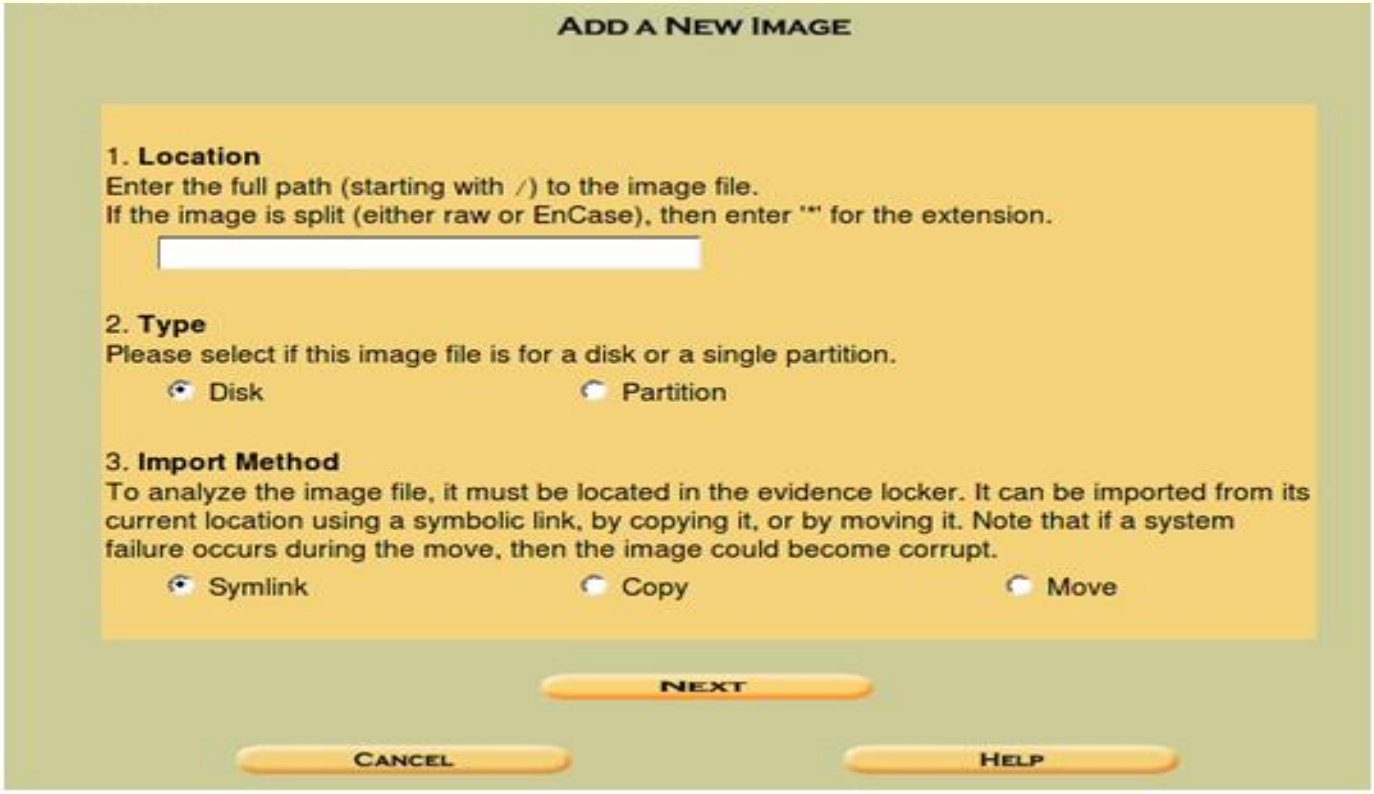
Attività di analisi

- Creazione di un nuovo caso con Autopsy



Attività di analisi

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



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.

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

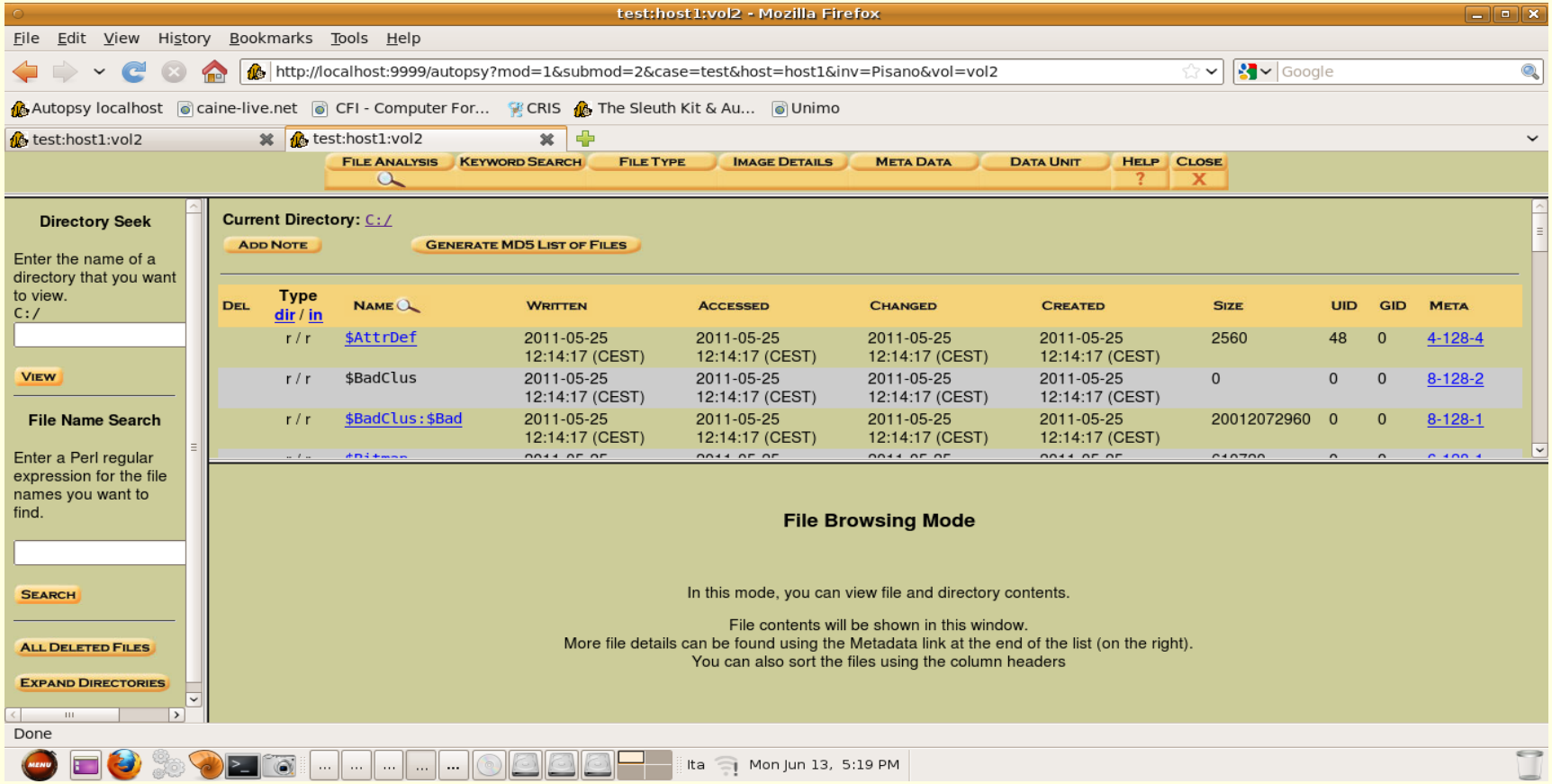
- Autopsy Forensic Browser
  - Timeline dell'attività del sistema;
  - Navigazione dell'immagine dell'hdd e ricerca files per estensioni.
- OphCrack
  - Crack delle password di amministratore del sistema.
- Pasco
  - Estrazione delle informazioni di navigazione.
- LiveView e tools di Nirsoft
  - Ricerca delle password di completamento memorizzate dal browser.
- RegLookup e MiTeC Windows Registry Recovery
  - Estrazione delle informazioni dal registro di sistema.
- Tchunt/TCDiscover 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.

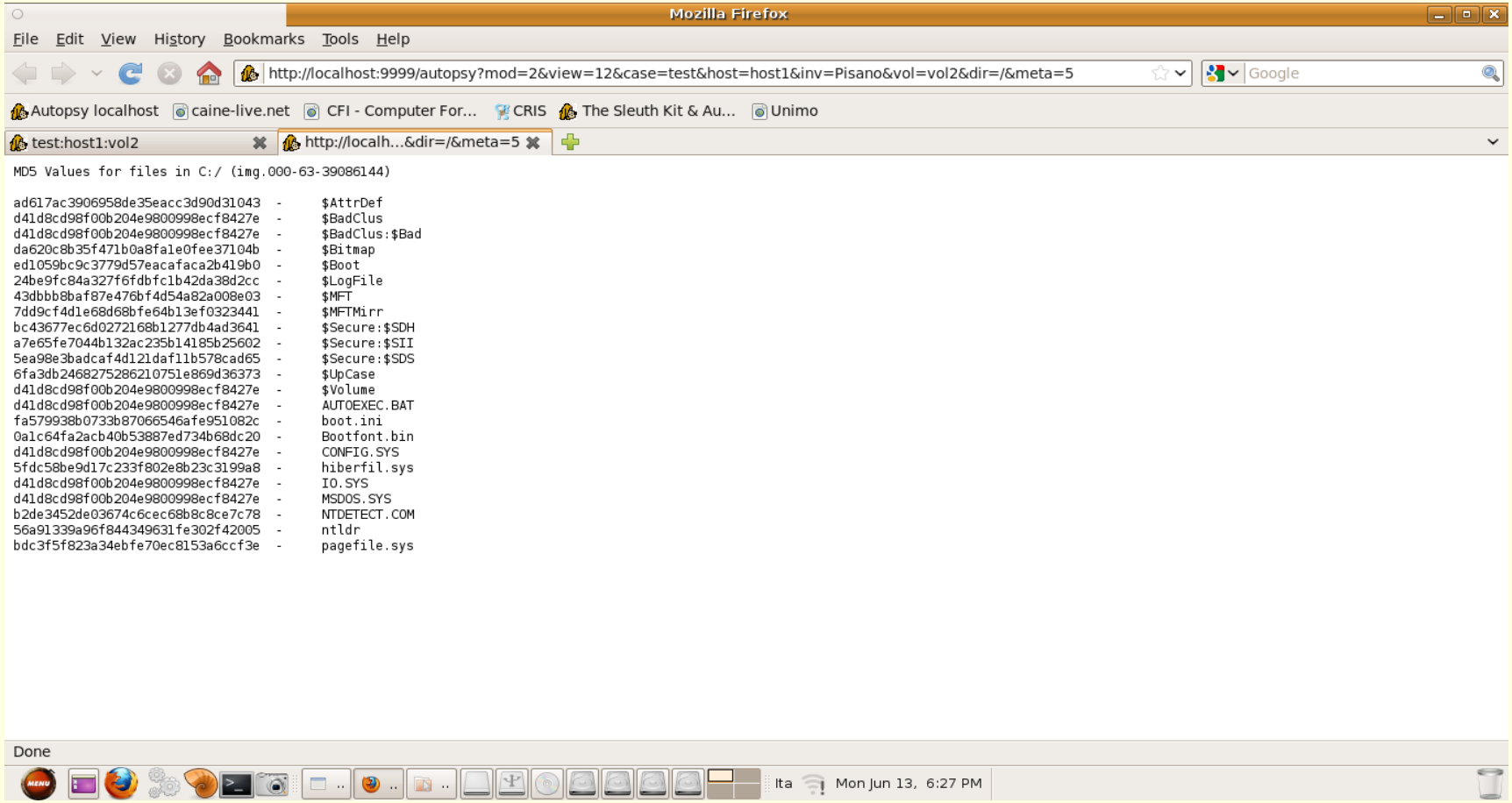
Tecniche per la ricerca dell'evidenza: Autopsy (1)

- File Analysis



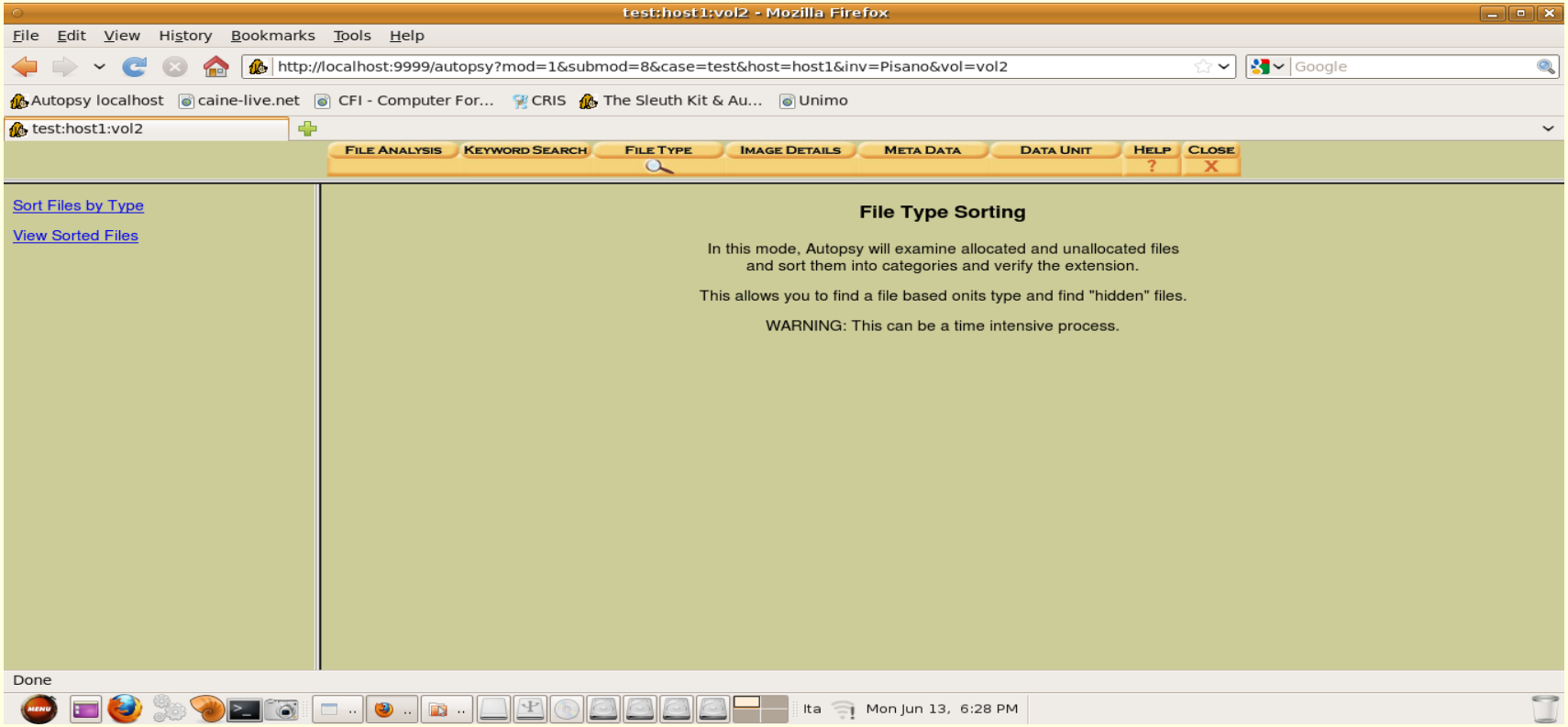
Tecniche per la ricerca dell'evidenza: Autopsy (2)

- MD5 list



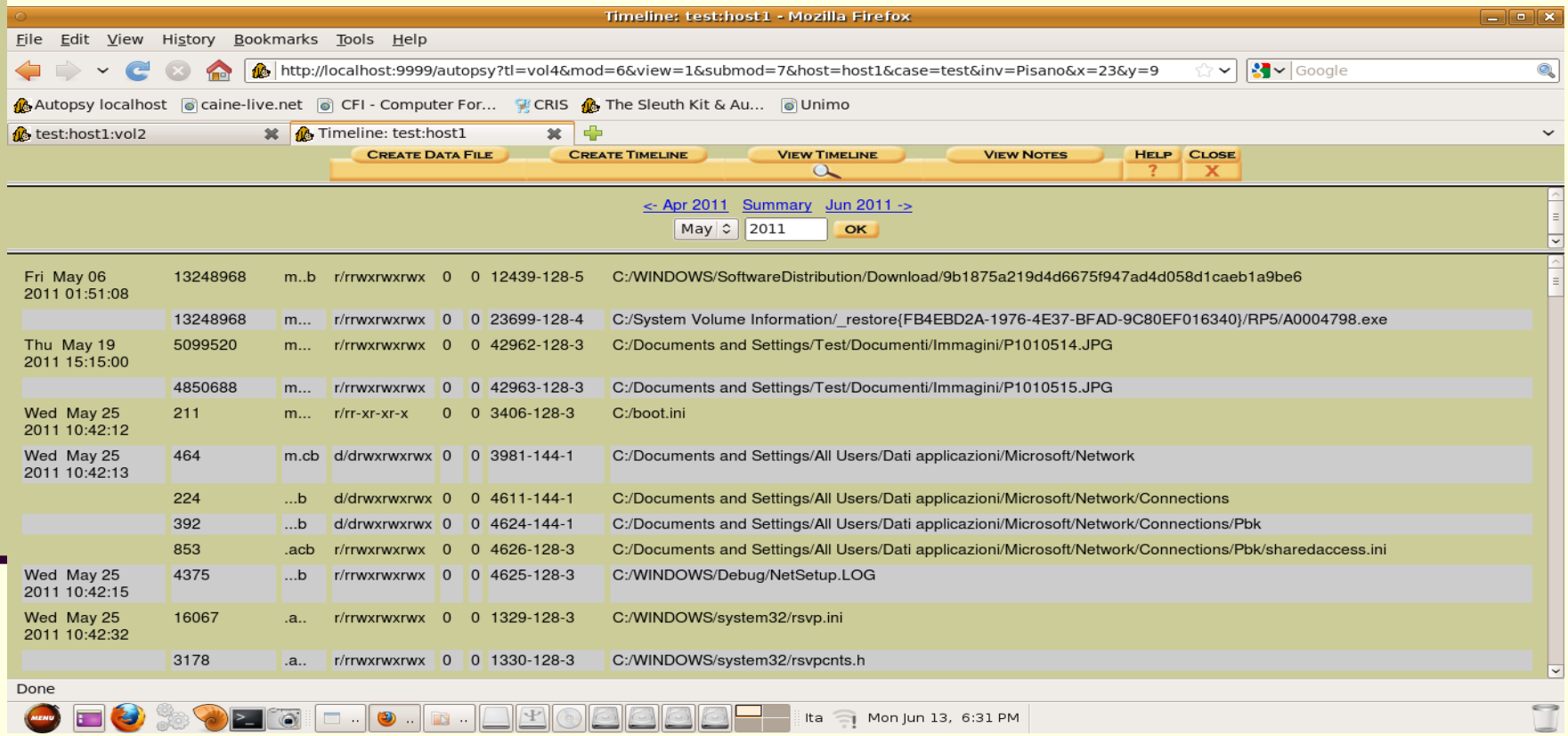
Tecniche per la ricerca dell'evidenza: Autopsy (3)

- File Type Sorting



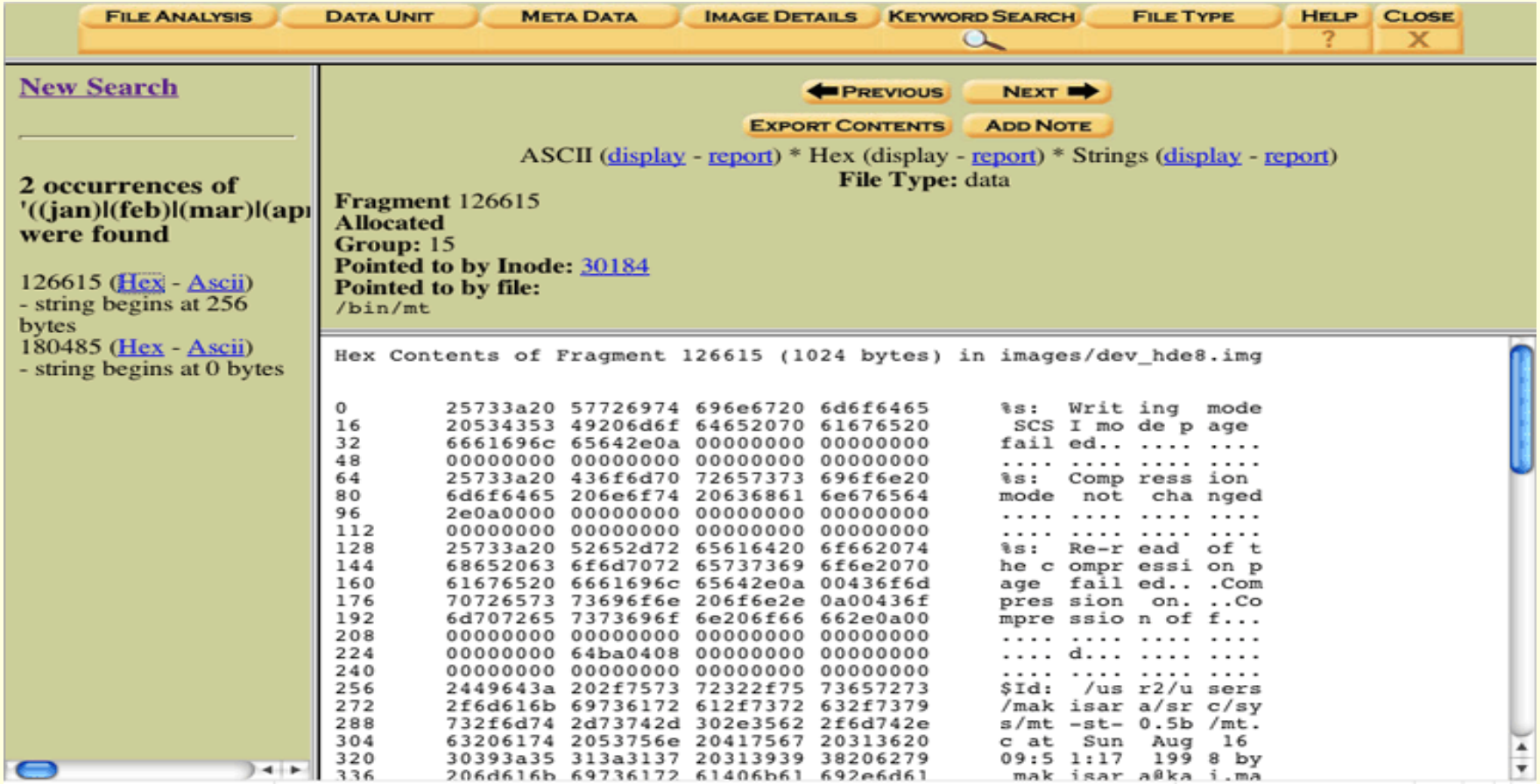
Tecniche per la ricerca dell'evidenza: Autopsy (4)

- Timeline of File Activity



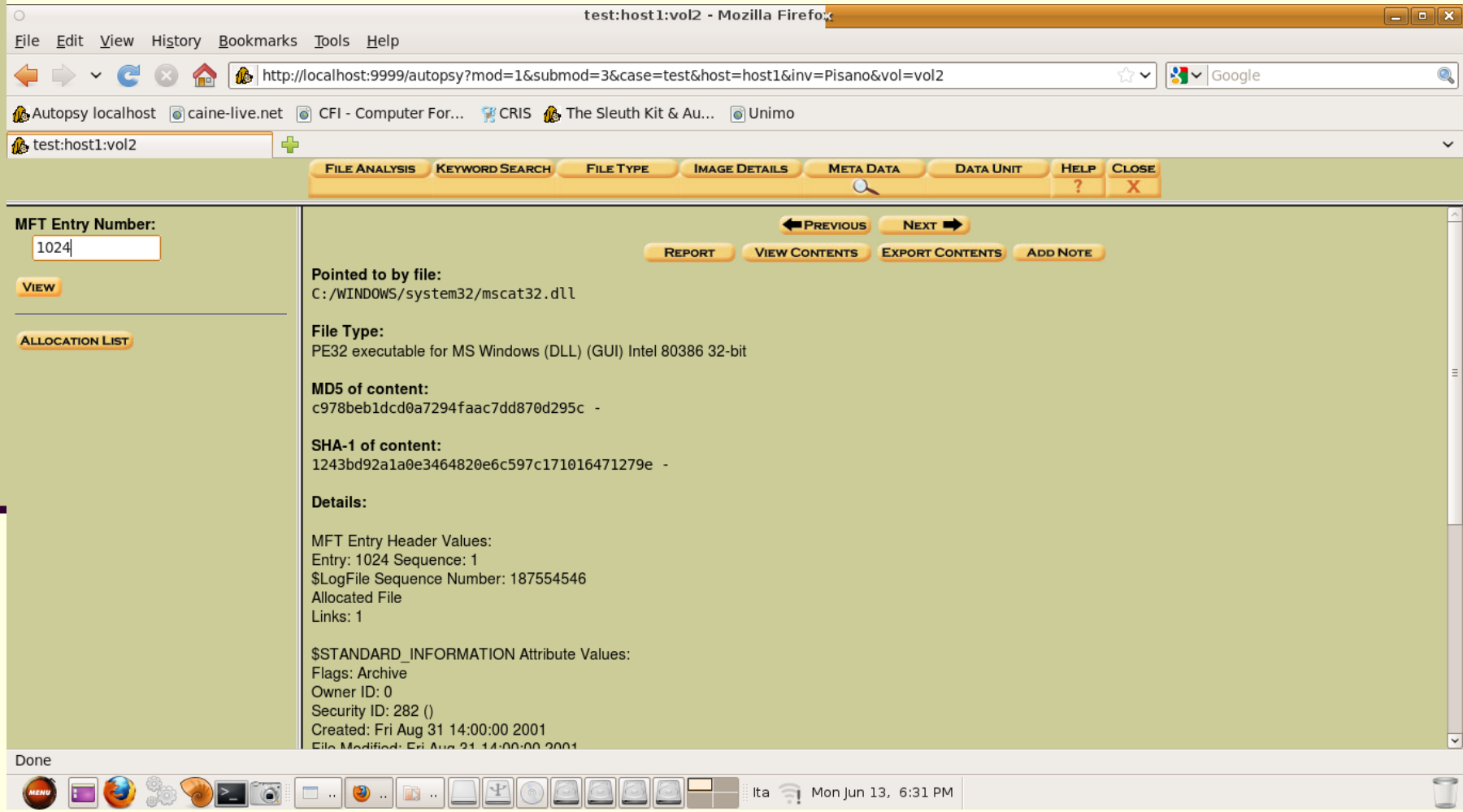
Tecniche per la ricerca dell'evidenza: Autopsy (5)

- Keyword Search



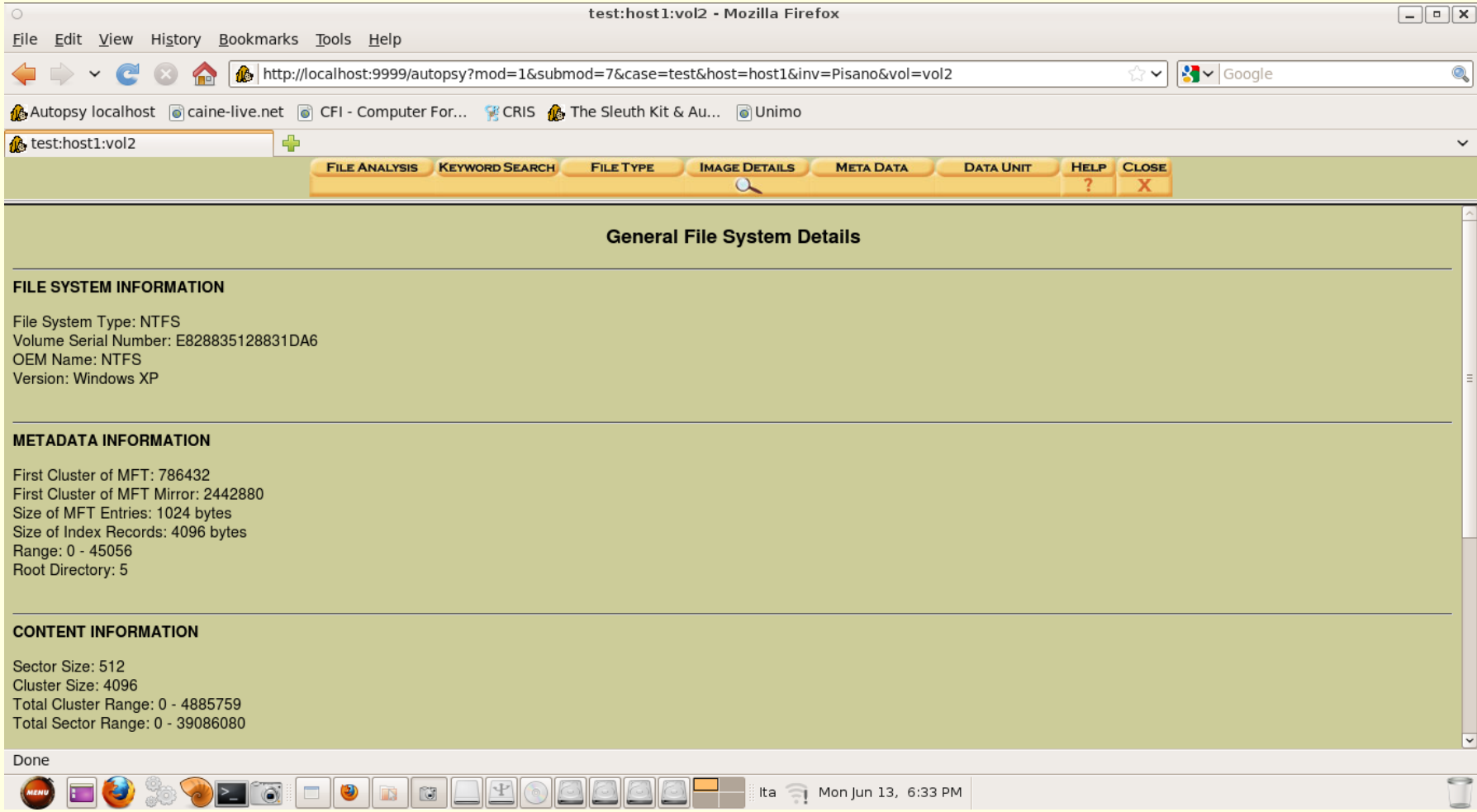
Tecniche per la ricerca dell'evidenza: Autopsy (6)

- Meta Data Analysis



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

- Image Details



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.

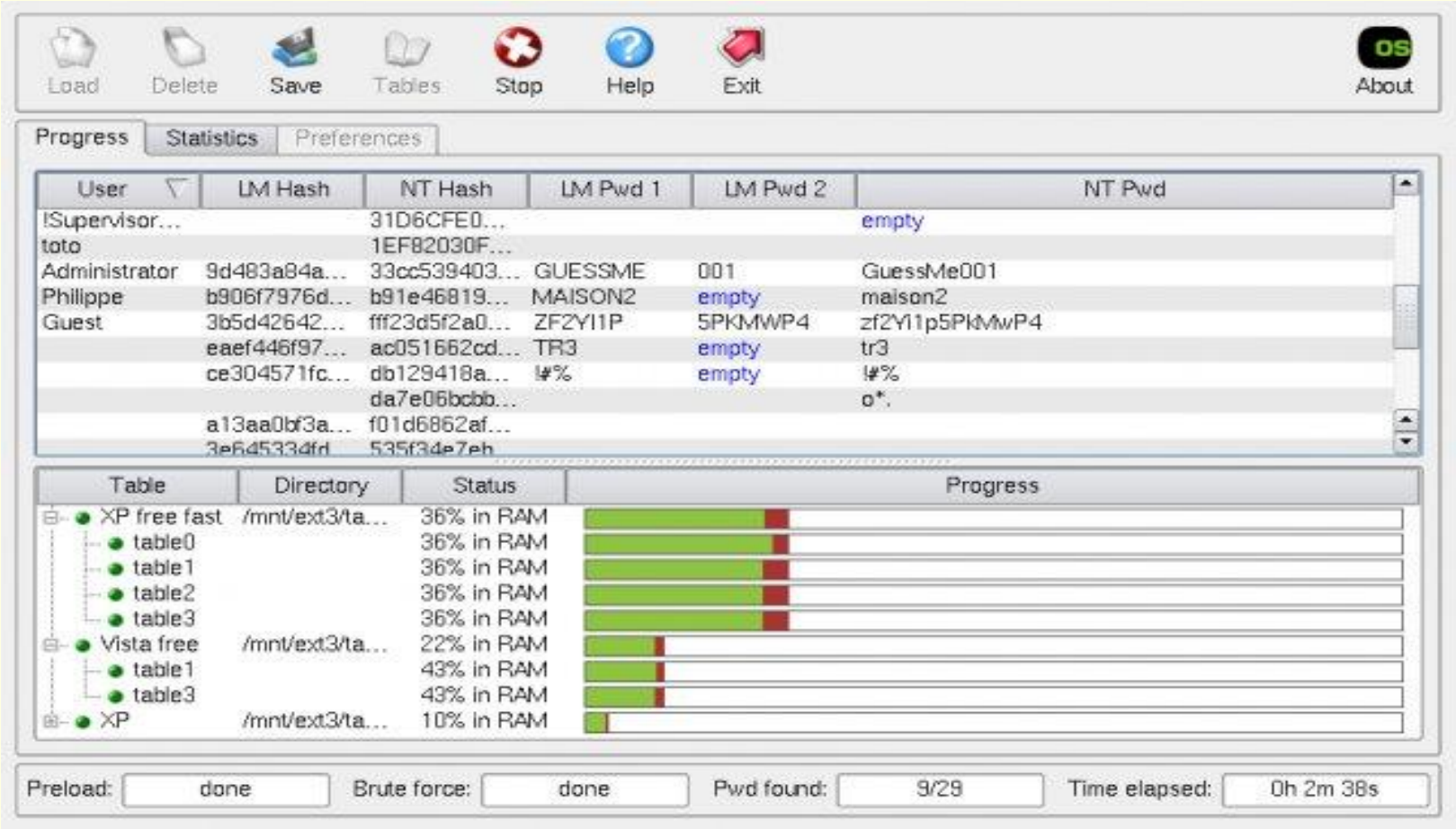
Strumenti utilizzati

- 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/TCDiscover 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



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/TCDiscover e Passware kit enterprise
  - Ricerca\Decifrazione di una partizione cifrata con TrueCrypt.

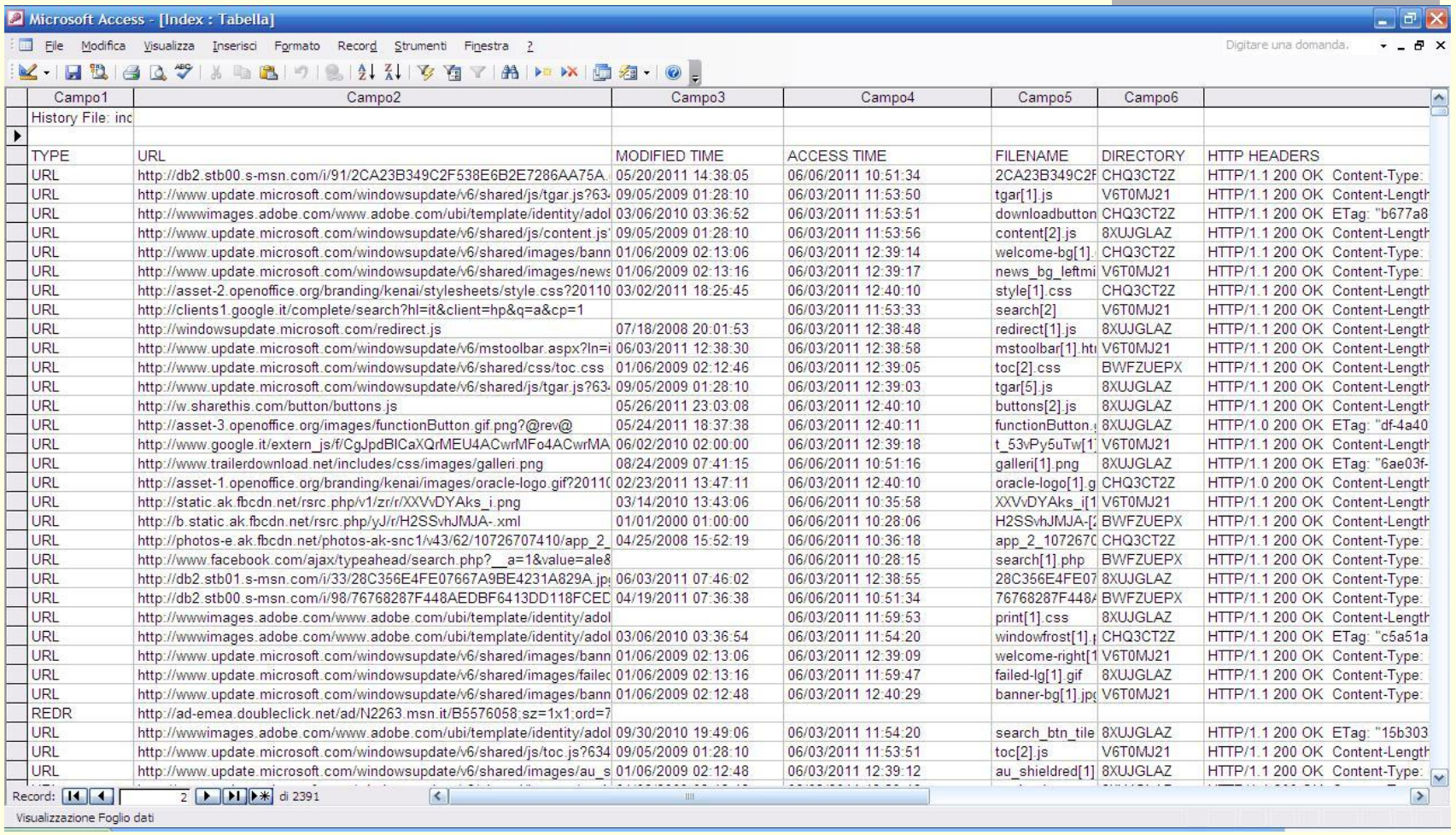
Tecniche per la ricerca dell'evidenza: Pasco (1)

- 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)

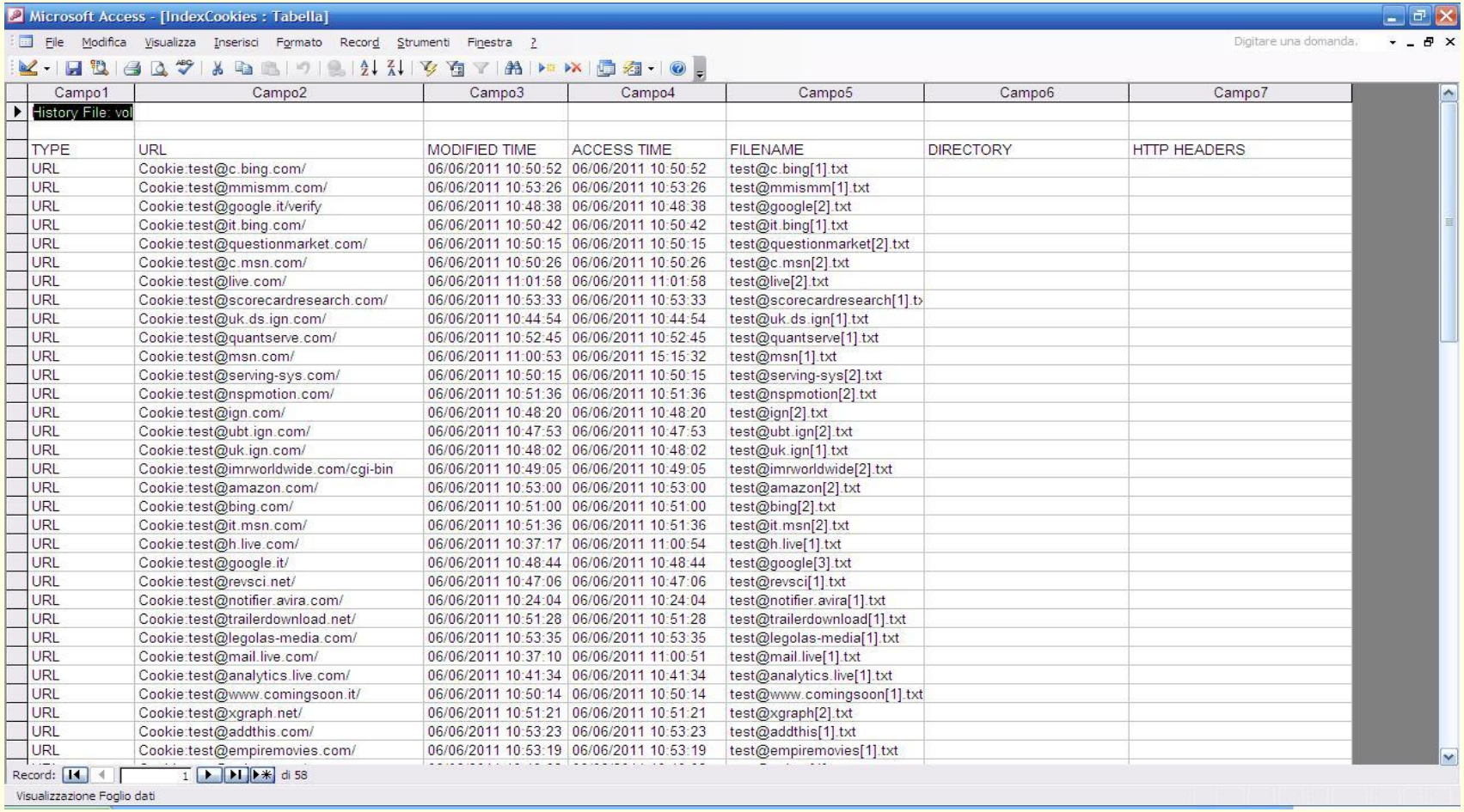
- I file su cui lavorare sono gli index.dat contenuti in:
  - C:\Documents and Settings\User\Cookies
  - C:\Documents and Settings\User\Impostazioni Locali\Cronologia\History.ie5
  - C:\Documents and Settings\User\Impostazioni Locali\Temporary Internet File\Content.ie5

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



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	2CA23B349C2F	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://wwwimages.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/bann	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-Length
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.g	8XUJGLAZ	HTTP/1.0 200 OK ETag: "df-4a40
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?2011(	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/rsrc.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/rsrc.php/yJ/r/H2SSvhJMJA-.xml	01/01/2000 01:00:00	06/06/2011 10:28:06	H2SSvhJMJA-[2	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/98/76768287F448AEDBF6413DD118FCED	04/19/2011 07:36:38	06/06/2011 10:51:34	76768287F448A	BWFZUEPX	HTTP/1.1 200 OK Content-Type:
URL	http://wwwimages.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://wwwimages.adobe.com/www.adobe.com/ubi/template/identity/adol	03/06/2010 03:36:54	06/03/2011 11:54:20	windowfrost[1].p	CHQ3CT2Z	HTTP/1.1 200 OK ETag: "c5a51a
URL	http://www.update.microsoft.com/windowsupdate/v6/shared/images/bann	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/failec	01/06/2009 02:13:16	06/03/2011 11:59:47	failed-lg[1].gif	8XUJGLAZ	HTTP/1.1 200 OK Content-Type:
URL	http://www.update.microsoft.com/windowsupdate/v6/shared/images/bann	01/06/2009 02:12:48	06/03/2011 12:40:29	banner-bg[1].jp	V6T0MJ21	HTTP/1.1 200 OK Content-Type:
REDR	http://ad-emea.doubleclick.net/ad/N2263.msn.it/B5576058;sz=1x1;ord=7					
URL	http://wwwimages.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:

Tecniche per la ricerca dell'evidenza: Pasco – Cookies



Microsoft Access - [IndexCookies : Tabella]

File Modifica Visualizza Inserisci Formato Record Strumenti Finestra ?

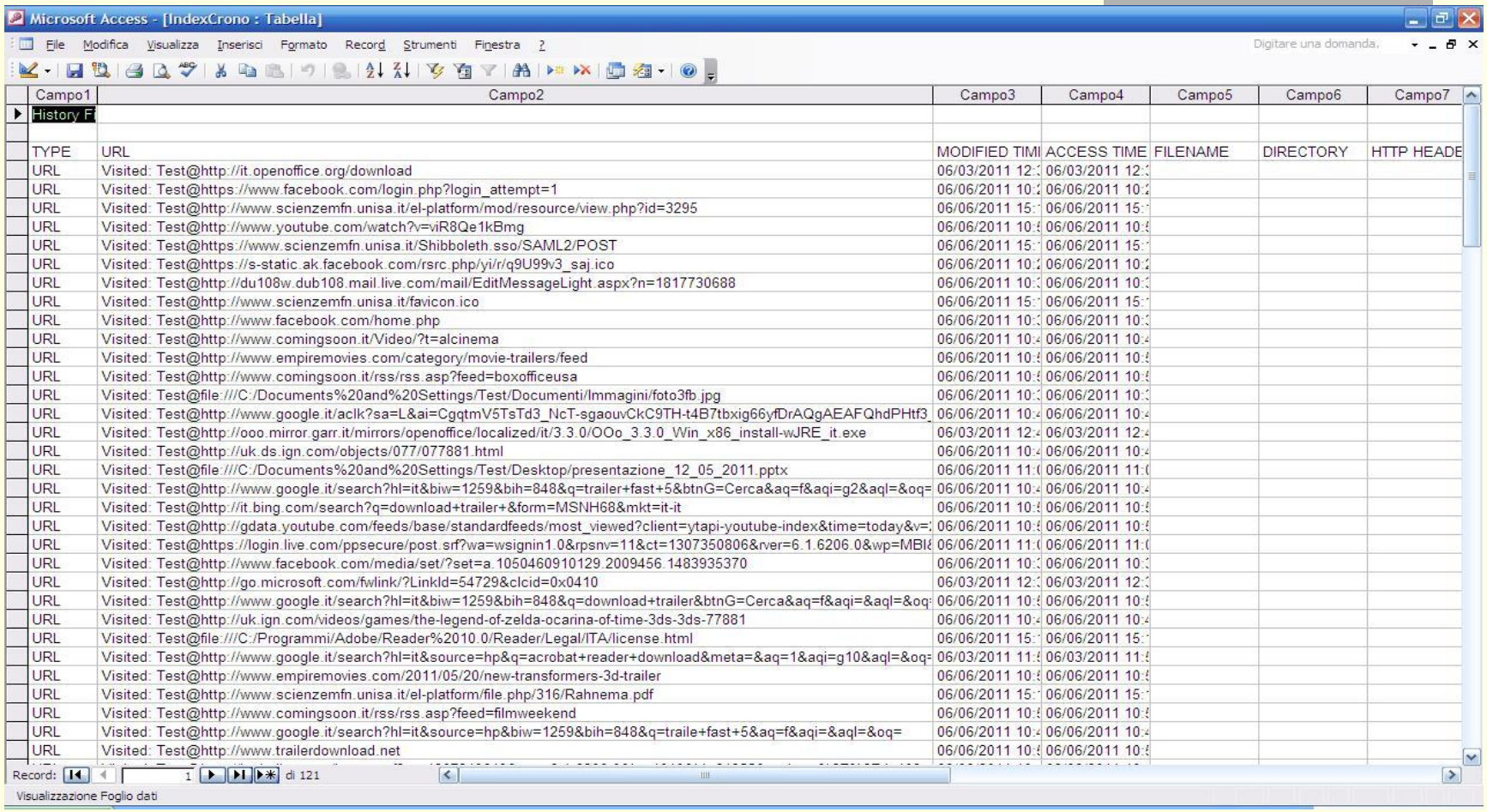
Digitare una domanda.

Campo1	Campo2	Campo3	Campo4	Campo5	Campo6	Campo7
History File: vol						
TYPE	URL	MODIFIED TIME	ACCESS TIME	FILENAME	DIRECTORY	HTTP HEADERS
URL	Cookie:test@c.bing.com/	06/06/2011 10:50:52	06/06/2011 10:50:52	test@c.bing[1].txt		
URL	Cookie:test@mmismm.com/	06/06/2011 10:53:26	06/06/2011 10:53:26	test@mmismm[1].txt		
URL	Cookie:test@google.it/verify	06/06/2011 10:48:38	06/06/2011 10:48:38	test@google[2].txt		
URL	Cookie:test@it.bing.com/	06/06/2011 10:50:42	06/06/2011 10:50:42	test@it.bing[1].txt		
URL	Cookie:test@questionmarket.com/	06/06/2011 10:50:15	06/06/2011 10:50:15	test@questionmarket[2].txt		
URL	Cookie:test@c.msn.com/	06/06/2011 10:50:26	06/06/2011 10:50:26	test@c.msn[2].txt		
URL	Cookie:test@live.com/	06/06/2011 11:01:58	06/06/2011 11:01:58	test@live[2].txt		
URL	Cookie:test@scorecardresearch.com/	06/06/2011 10:53:33	06/06/2011 10:53:33	test@scorecardresearch[1].tx		
URL	Cookie:test@uk.ds.ign.com/	06/06/2011 10:44:54	06/06/2011 10:44:54	test@uk.ds.ign[1].txt		
URL	Cookie:test@quantserve.com/	06/06/2011 10:52:45	06/06/2011 10:52:45	test@quantserve[1].txt		
URL	Cookie:test@msn.com/	06/06/2011 11:00:53	06/06/2011 15:15:32	test@msn[1].txt		
URL	Cookie:test@serving-sys.com/	06/06/2011 10:50:15	06/06/2011 10:50:15	test@serving-sys[2].txt		
URL	Cookie:test@nspmotion.com/	06/06/2011 10:51:36	06/06/2011 10:51:36	test@nspmotion[2].txt		
URL	Cookie:test@ign.com/	06/06/2011 10:48:20	06/06/2011 10:48:20	test@ign[2].txt		
URL	Cookie:test@ubt.ign.com/	06/06/2011 10:47:53	06/06/2011 10:47:53	test@ubt.ign[2].txt		
URL	Cookie:test@uk.ign.com/	06/06/2011 10:48:02	06/06/2011 10:48:02	test@uk.ign[1].txt		
URL	Cookie:test@imrworldwide.com/cgi-bin	06/06/2011 10:49:05	06/06/2011 10:49:05	test@imrworldwide[2].txt		
URL	Cookie:test@amazon.com/	06/06/2011 10:53:00	06/06/2011 10:53:00	test@amazon[2].txt		
URL	Cookie:test@bing.com/	06/06/2011 10:51:00	06/06/2011 10:51:00	test@bing[2].txt		
URL	Cookie:test@it.msn.com/	06/06/2011 10:51:36	06/06/2011 10:51:36	test@it.msn[2].txt		
URL	Cookie:test@h.live.com/	06/06/2011 10:37:17	06/06/2011 11:00:54	test@h.live[1].txt		
URL	Cookie:test@google.it/	06/06/2011 10:48:44	06/06/2011 10:48:44	test@google[3].txt		
URL	Cookie:test@revsci.net/	06/06/2011 10:47:06	06/06/2011 10:47:06	test@revsci[1].txt		
URL	Cookie:test@notifier.avira.com/	06/06/2011 10:24:04	06/06/2011 10:24:04	test@notifier.avira[1].txt		
URL	Cookie:test@trailerdownload.net/	06/06/2011 10:51:28	06/06/2011 10:51:28	test@trailerdownload[1].txt		
URL	Cookie:test@legolas-media.com/	06/06/2011 10:53:35	06/06/2011 10:53:35	test@legolas-media[1].txt		
URL	Cookie:test@mail.live.com/	06/06/2011 10:37:10	06/06/2011 11:00:51	test@mail.live[1].txt		
URL	Cookie:test@analytics.live.com/	06/06/2011 10:41:34	06/06/2011 10:41:34	test@analytics.live[1].txt		
URL	Cookie:test@www.comingsoon.it/	06/06/2011 10:50:14	06/06/2011 10:50:14	test@www.comingsoon[1].txt		
URL	Cookie:test@xgraph.net/	06/06/2011 10:51:21	06/06/2011 10:51:21	test@xgraph[2].txt		
URL	Cookie:test@addthis.com/	06/06/2011 10:53:23	06/06/2011 10:53:23	test@addthis[1].txt		
URL	Cookie:test@empiremovies.com/	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 TIMI	ACCESS TIME	FILENAME	DIRECTORY	HTTP HEADE
URL	Visited: Test@http://it.openoffice.org/download	06/03/2011 12:3	06/03/2011 12:3			
URL	Visited: Test@https://www.facebook.com/login.php?login_attempt=1	06/06/2011 10:2	06/06/2011 10:2			
URL	Visited: Test@http://www.scienzemfn.unisa.it/el-platform/mod/resource/view.php?id=3295	06/06/2011 15:1	06/06/2011 15:1			
URL	Visited: Test@http://www.youtube.com/watch?v=viR8Qe1kBmg	06/06/2011 10:5	06/06/2011 10:5			
URL	Visited: Test@https://www.scienzemfn.unisa.it/Shibboleth.sso/SAML2/POST	06/06/2011 15:1	06/06/2011 15:1			
URL	Visited: Test@https://s-static.ak.facebook.com/rsrc.php/yi/r/q9U99v3_saj.ico	06/06/2011 10:2	06/06/2011 10:2			
URL	Visited: Test@http://du108w.dub108.mail.live.com/mail/EditMessageLight.aspx?n=1817730688	06/06/2011 10:3	06/06/2011 10:3			
URL	Visited: Test@http://www.scienzemfn.unisa.it/favicon.ico	06/06/2011 15:1	06/06/2011 15:1			
URL	Visited: Test@http://www.facebook.com/home.php	06/06/2011 10:3	06/06/2011 10:3			
URL	Visited: Test@http://www.comingsoon.it/Video/?t=alcinema	06/06/2011 10:4	06/06/2011 10:4			
URL	Visited: Test@http://www.empiremovies.com/category/movie-trailers/feed	06/06/2011 10:5	06/06/2011 10:5			
URL	Visited: Test@http://www.comingsoon.it/rss/rss.asp?feed=boxofficeusa	06/06/2011 10:5	06/06/2011 10:5			
URL	Visited: Test@file:///C:/Documents%20and%20Settings/Test/Documenti/Immagini/foto3fb.jpg	06/06/2011 10:3	06/06/2011 10:3			
URL	Visited: Test@http://www.google.it/aclk?sa=L&ai=CgqtmV5TsTd3_NcT-sgaouvCkC9TH-t4B7tbxig66yfDrAQgAEAFQhdPHtf3_	06/06/2011 10:4	06/06/2011 10:4			
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 12:4	06/03/2011 12:4			
URL	Visited: Test@http://uk.ds.ign.com/objects/077/077881.html	06/06/2011 10:4	06/06/2011 10:4			
URL	Visited: Test@file:///C:/Documents%20and%20Settings/Test/Desktop/presentazione_12_05_2011.pptx	06/06/2011 11:0	06/06/2011 11:0			
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=&oq=	06/06/2011 10:4	06/06/2011 10:4			
URL	Visited: Test@http://it.bing.com/search?q=download+trailer+&form=MSNH68&mkt=it-it	06/06/2011 10:5	06/06/2011 10:5			
URL	Visited: Test@http://gdata.youtube.com/feeds/base/standardfeeds/most_viewed?client=ytapi-youtube-index&time=today&v=2	06/06/2011 10:5	06/06/2011 10:5			
URL	Visited: Test@https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsnv=11&ct=1307350806&rver=6.1.6206.0&wp=MBI8	06/06/2011 11:0	06/06/2011 11:0			
URL	Visited: Test@http://www.facebook.com/media/set/?set=a.1050460910129.2009456.1483935370	06/06/2011 10:3	06/06/2011 10:3			
URL	Visited: Test@http://go.microsoft.com/fwlink/?LinkId=54729&clcid=0x0410	06/03/2011 12:3	06/03/2011 12:3			
URL	Visited: Test@http://www.google.it/search?hl=it&biw=1259&bih=848&q=download+trailer&btnG=Cerca&aq=f&aqi=&aql=&oq=	06/06/2011 10:5	06/06/2011 10:5			
URL	Visited: Test@http://uk.ign.com/videos/games/the-legend-of-zelda-ocarina-of-time-3ds-3ds-77881	06/06/2011 10:4	06/06/2011 10:4			
URL	Visited: Test@file:///C:/Programmi/Adobe/Reader%2010.0/Reader/Legal/ITA/license.html	06/06/2011 15:1	06/06/2011 15:1			
URL	Visited: Test@http://www.google.it/search?hl=it&source=hp&q=acrobat+reader+download&meta=&aq=1&aqi=g10&aql=&oq=	06/03/2011 11:5	06/03/2011 11:5			
URL	Visited: Test@http://www.empiremovies.com/2011/05/20/new-transformers-3d-trailer	06/06/2011 10:5	06/06/2011 10:5			
URL	Visited: Test@http://www.scienzemfn.unisa.it/el-platform/file.php/316/Rahnema.pdf	06/06/2011 15:1	06/06/2011 15:1			
URL	Visited: Test@http://www.comingsoon.it/rss/rss.asp?feed=filmweekend	06/06/2011 10:5	06/06/2011 10:5			
URL	Visited: Test@http://www.google.it/search?hl=it&source=hp&biw=1259&bih=848&q=traile+fast+5&aq=f&aqi=&aql=&oq=	06/06/2011 10:4	06/06/2011 10:4			
URL	Visited: Test@http://www.trailerdownload.net	06/06/2011 10:5	06/06/2011 10:5			

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/TCDiscover e Passware kit enterprise
  - Ricerca\Decifrazione di una partizione cifrata con TrueCrypt.

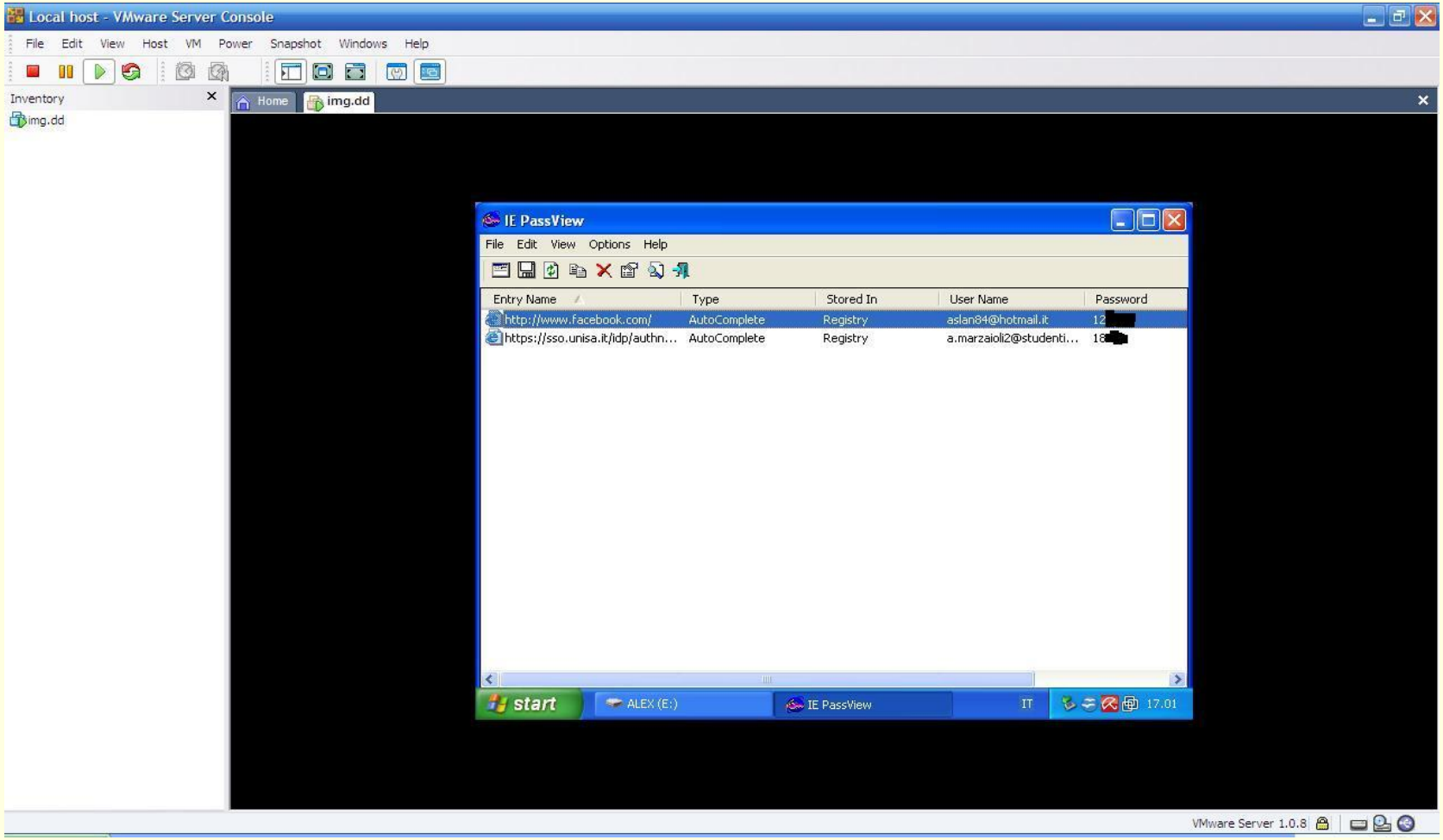
LiveView e VMWare Server

- 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

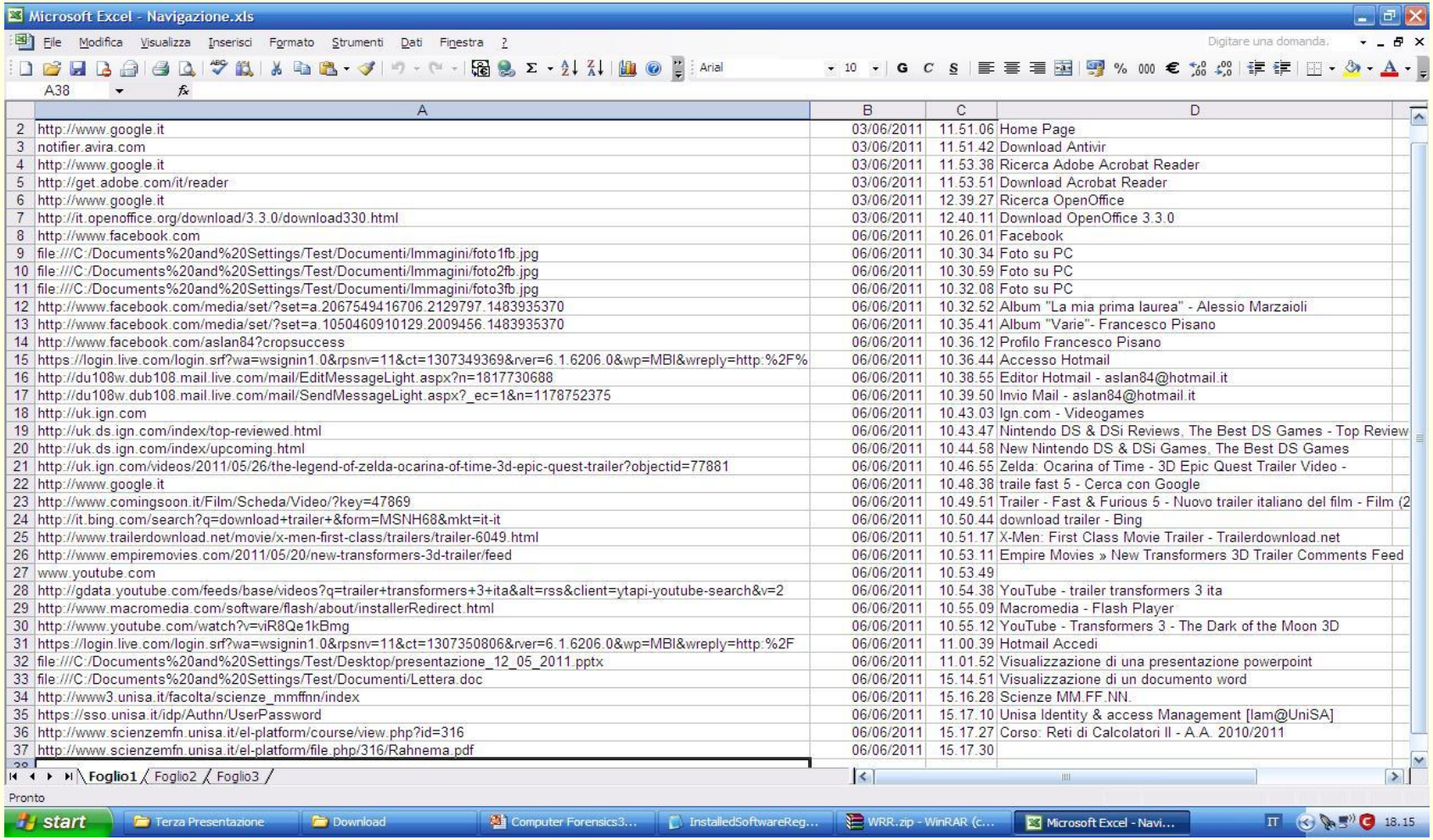
I tools di Nirsoft per analisi forense

- 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/Documenti/Immagini/foto1fb.jpg	06/06/2011	10.30.34	Foto su PC
10	file:///C:/Documents%20and%20Settings/Test/Documenti/Immagini/foto2fb.jpg	06/06/2011	10.30.59	Foto su PC
11	file:///C:/Documents%20and%20Settings/Test/Documenti/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?cropsuccess	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%	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	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/Documenti/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 [Iam@UniSA]
36	http://www.scienzemfn.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.scienzemfn.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/TCDiscover e Passware kit enterprise
  - Ricerca\Decifrazione di una partizione cifrata con TrueCrypt.

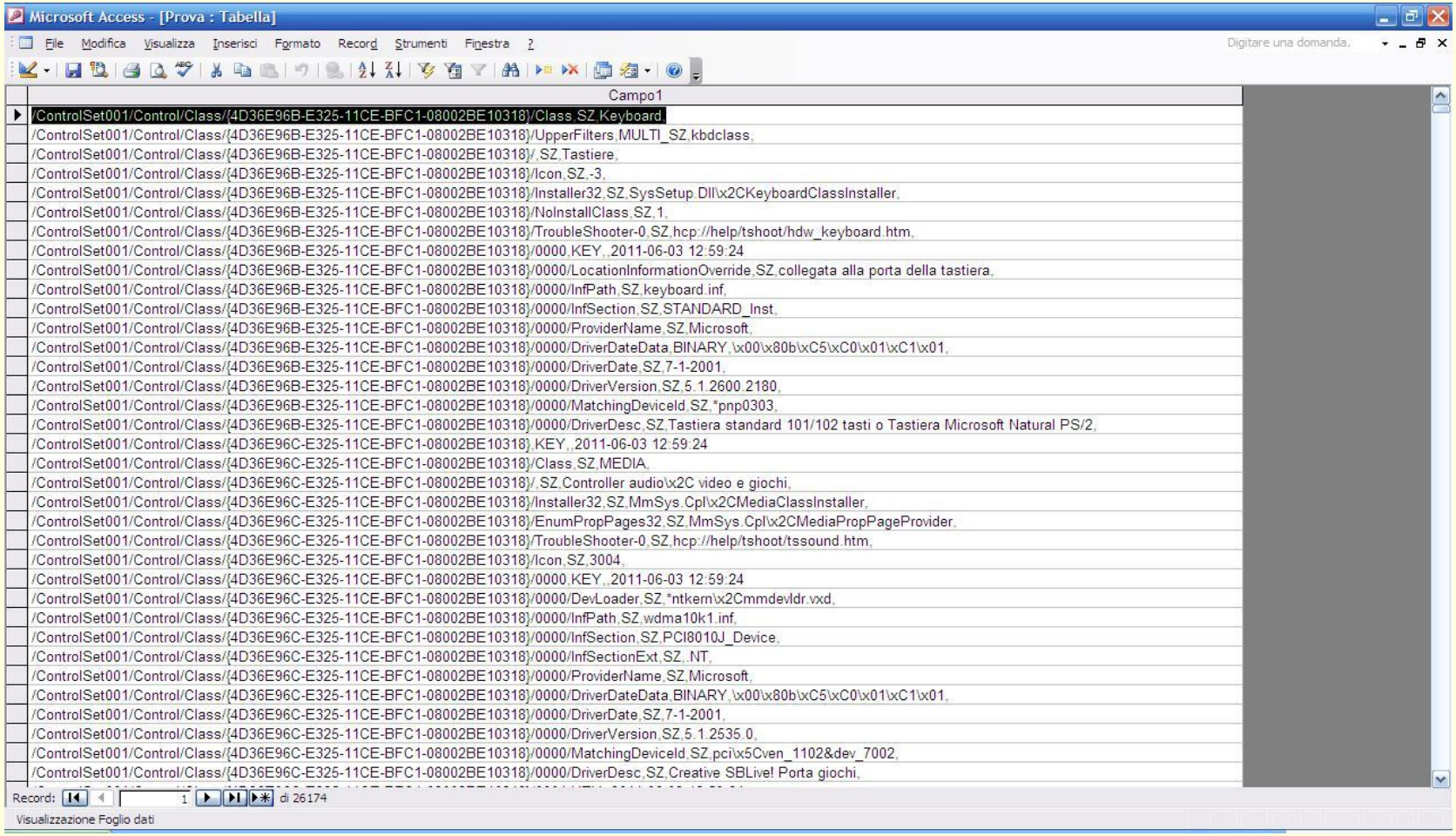
Analisi del registro del sistema

- 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).

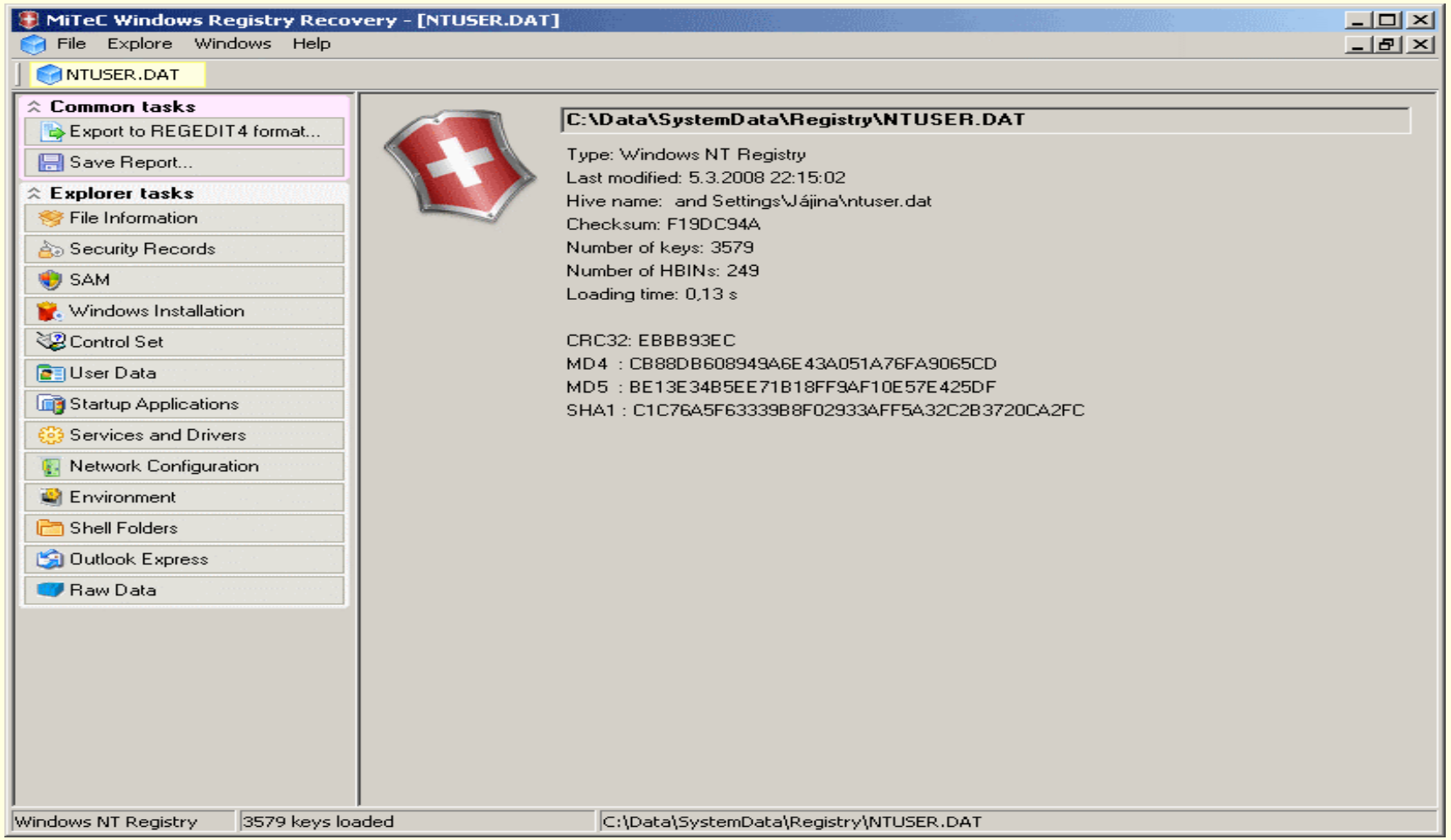
Tecniche per la ricerca dell'evidenza: Reglookup (2)



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/TCDiscover 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

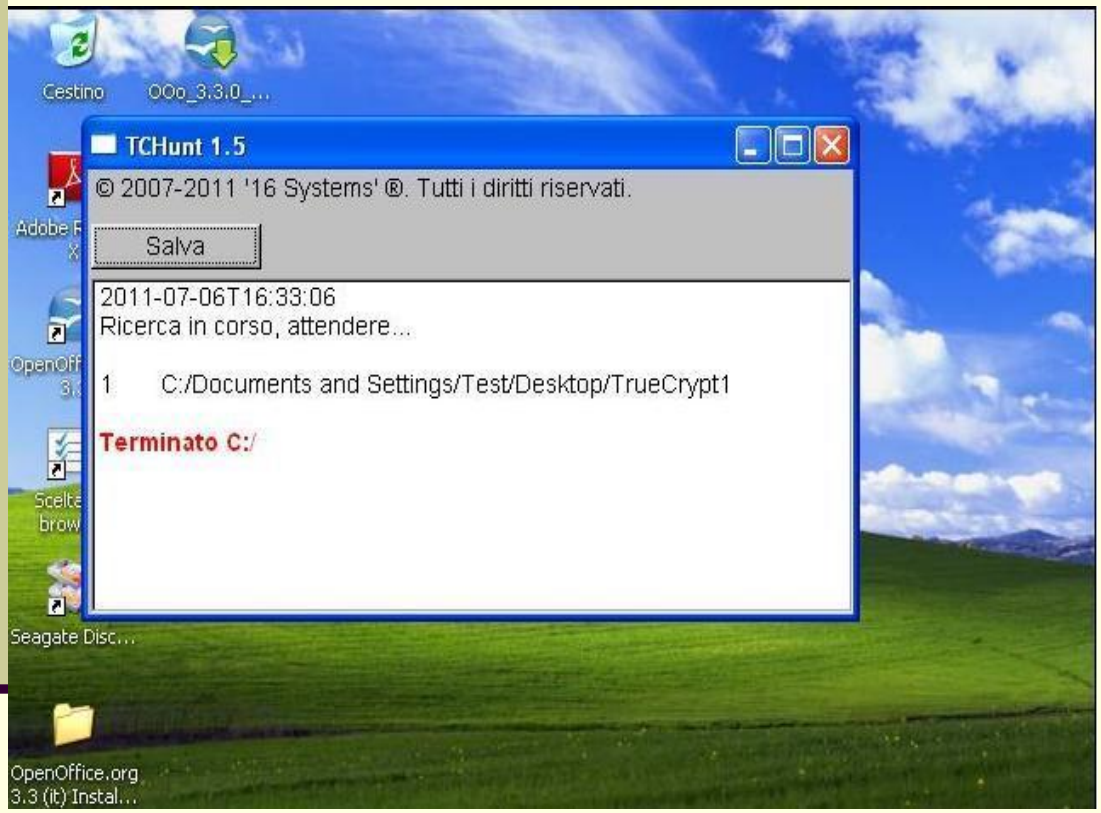
- Primo problema:
  - I dati cifrati appaiono come una sequenza pseudo-random -> difficoltà ad individuare una partizione virtuale cifrata!
- Soluzione:
  - Un software in grado di discriminare una partizione cifrata di TrueCrypt in funzione di alcune sue caratteristiche -> tchunt

Tchunt e TCDiscover

- 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,TCDiscover 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.

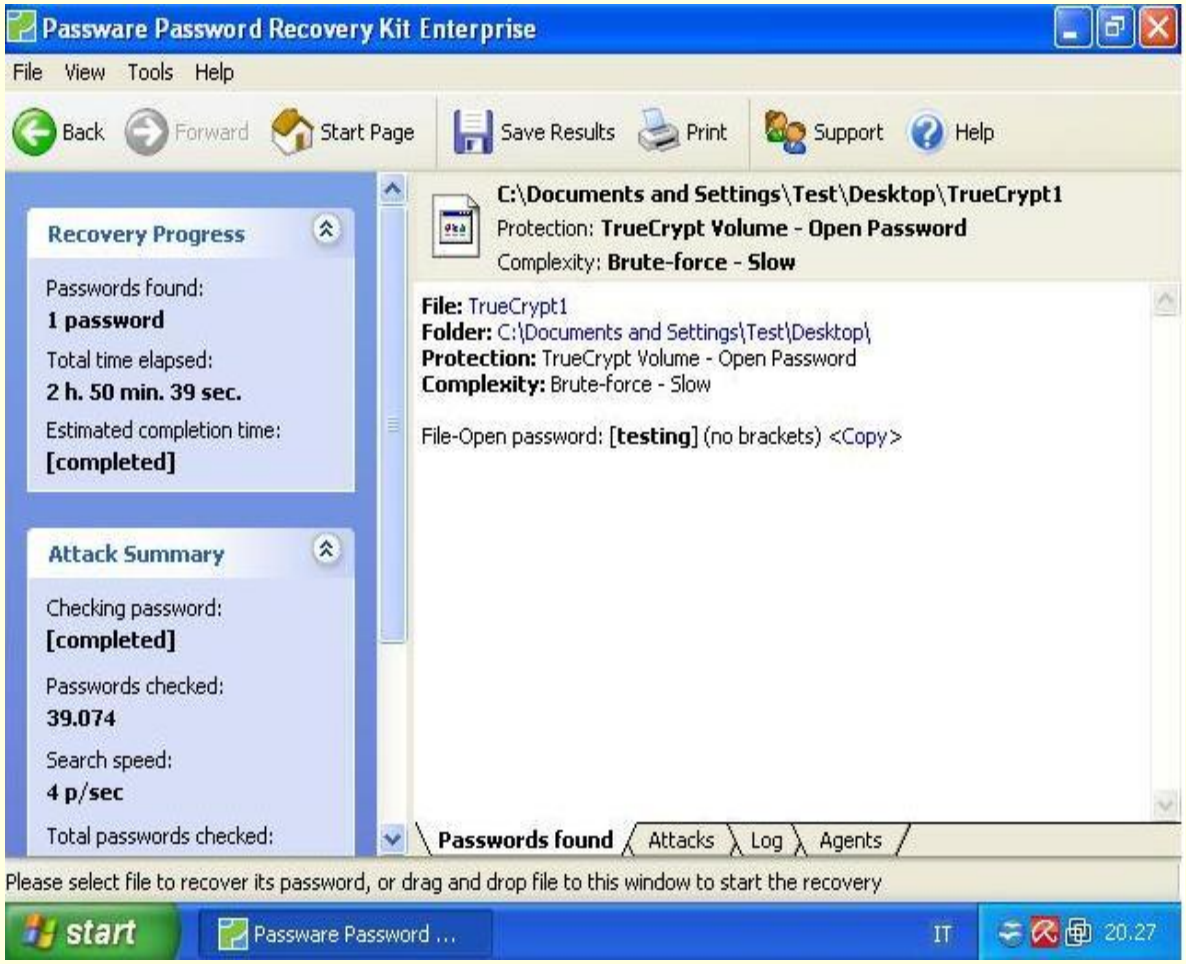
Passware kit enterprise 10.0

- 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

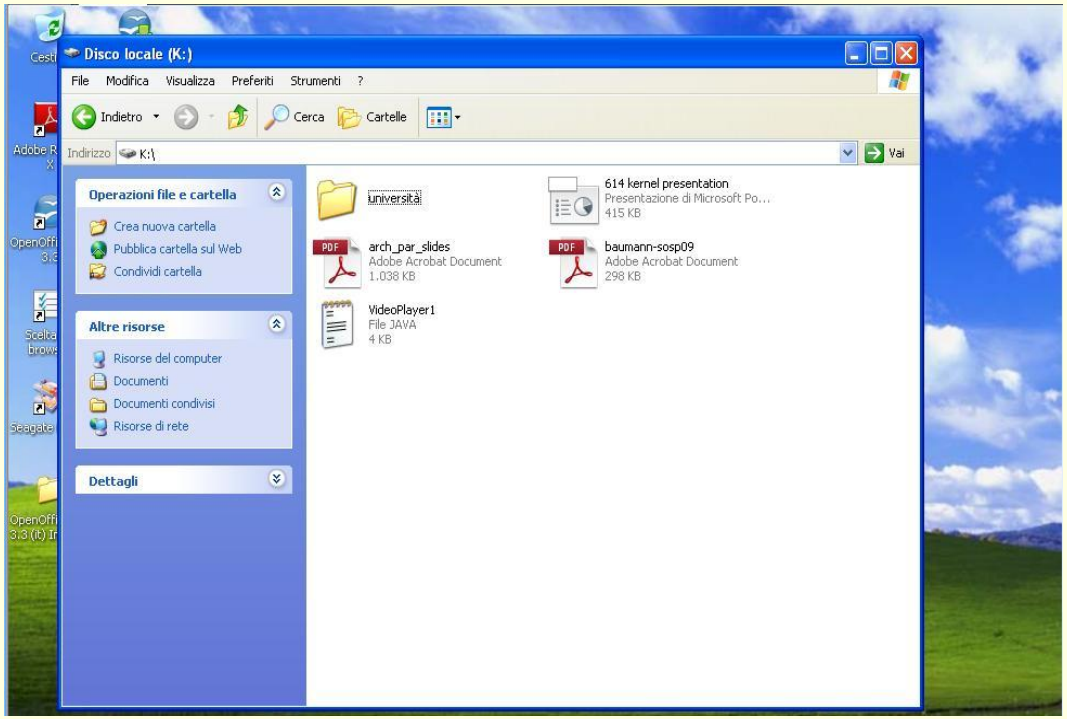
- Niente dump della memoria con partizione montata;
- Niente file hiberfill.sys;
- Attacco a dizionario con Passware kit su un range di chiavi di lunghezza tra 5 e 8 caratteri in lingua inglese (Password di un utente non molto scaltro..).

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

Conclusioni...1

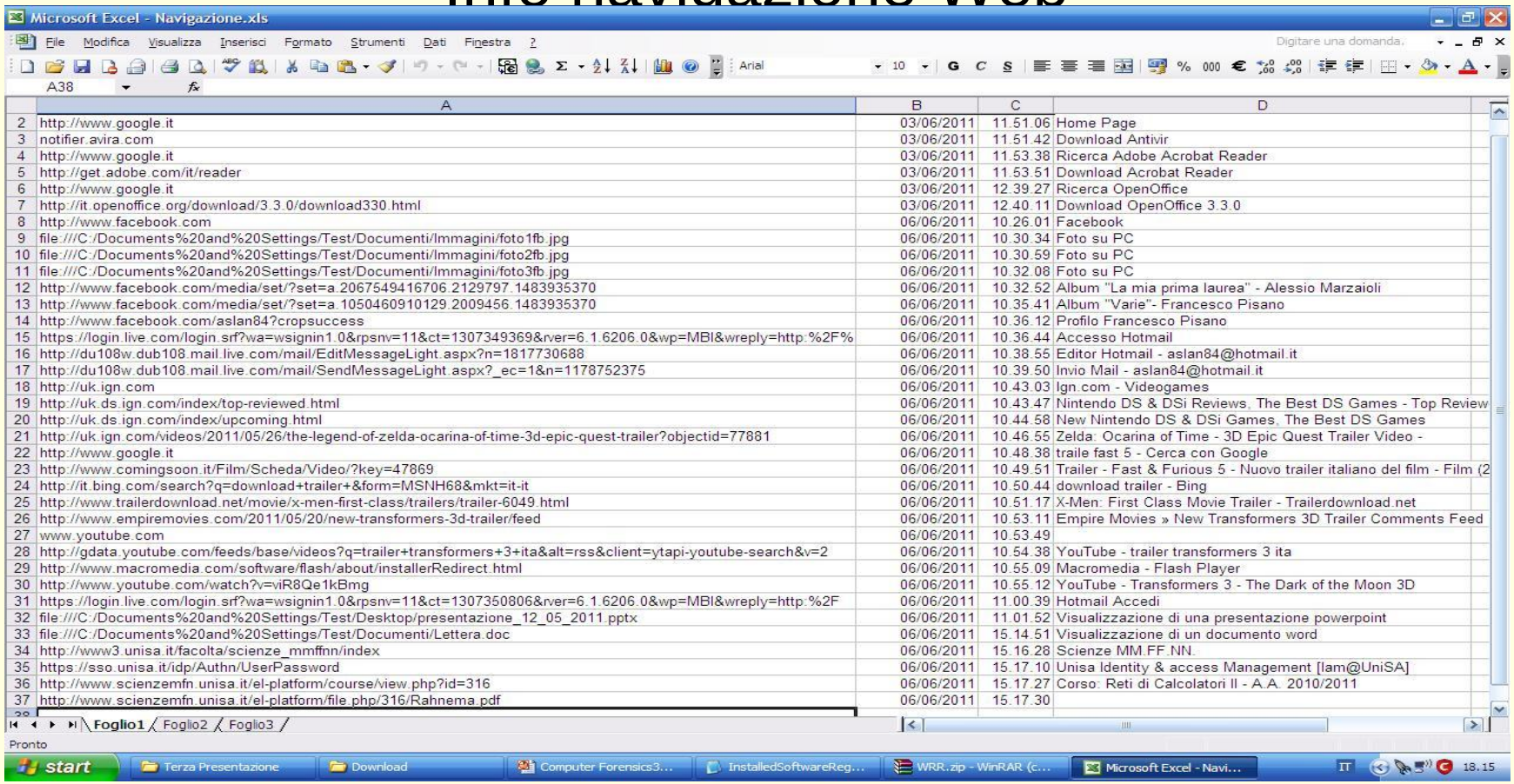
- Informazioni principali sull'utente
  - Owner: Test
  - Product ID: 55274-641-3126376-23064
  - Product Key: BHFBH-*****-*****-*****-*****
  - Installed Date: 25/05/2011 9.09.57
  - System Root: C:\WINDOWS
- Dati dell' utente
  - Password amministratore (OphCrack) Test
  - Password di completamento 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



Microsoft Excel - Navigazione.xls

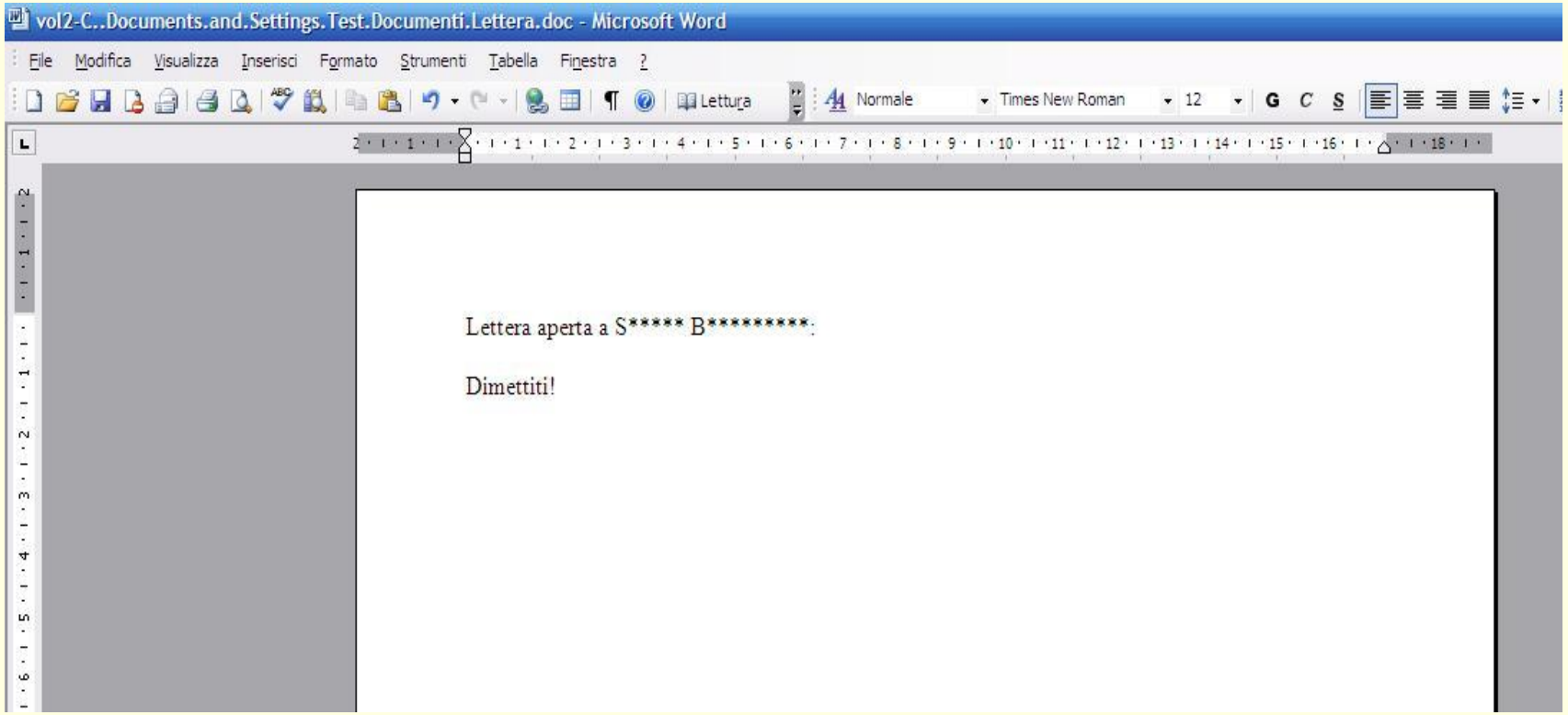
	A	B	C	D
2	http://www.google.it	03/06/2011	11.51.06	Home Page
3	notifier.avira.com	03/06/2011	11.51.42	Download Antivir
4	http://www.google.it	03/06/2011	11.53.38	Ricerca Adobe Acrobat Reader
5	http://get.adobe.com/it/reader	03/06/2011	11.53.51	Download Acrobat Reader
6	http://www.google.it	03/06/2011	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/Documenti/Immagini/foto1fb.jpg	06/06/2011	10.30.34	Foto su PC
10	file:///C:/Documents%20and%20Settings/Test/Documenti/Immagini/foto2fb.jpg	06/06/2011	10.30.59	Foto su PC
11	file:///C:/Documents%20and%20Settings/Test/Documenti/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?cropsuccess	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%	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	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/Documenti/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 [Iam@UniSA]
36	http://www.scienzemfn.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.scienzemfn.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)