

Live Forensics

*Fabio Fulgido
Gaetano Rocco
Mario Fiore Vitale*

Sommario

- Computer Forensics
 - Metodologie forensi
 - Live forensics
- Distribuzioni
 - DEFT
 - Helix
 - CAINE
- Analisi Forense dei dati volatili
 - Tipologie di dump
 - Dump tool
 - Process analysis tool
 - Clipboard tool
- Caso di studio
 - Ambiente di lavoro
 - Risultati
- Riferimenti

Computer Forensics

«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.»

[1] «Wikipedia,» [Online]. Available: http://it.wikipedia.org/wiki/Informatica_forense.

[2] M. Epifani, 2011. [Online]. Available: www.associazionearchimede.it/Unisa/phocadownload/ssi2011.pdf.

Metodologie forensi

- Analisi post mortem
 - Analisi di un computer dopo il suo spegnimento
 - Analisi ripetibile
 - Perdita dei dati “live” in RAM
- Analisi live
 - Acquisire RAM
 - Conoscere processi in esecuzione
 - Conoscere attività di rete e IP della macchina
 - Minimizzare l'impatto sul sistema
 - Analisi non ripetibile

Live Forensics: irripetibilità

- di natura tecnica: non esiste infatti possibilità di realizzare analisi e acquisizione dati live senza modificare almeno una parte della memoria del sistema;
- di natura temporale: la situazione della macchina (stato) all'atto dell'attività è frutto del momento e la sua complessità è tale da non poter sicuramente essere riprodotta;

Forensics Volatility

- Non tutti i dati hanno la stessa volatilità
 - Attribuzione di priorità alla volatilità dei dispositivi
- Ordine di priorità
 1. Memoria RAM
 2. File di Swap
 3. Processi di rete
 4. Processi di sistema
 5. Informazioni del file system
 6. Blocchi del disco

[3] M. McDougal, «Live Forensics on Windows System using Windows Forensic Toolchest,» 2003-2006. [Online].

Available: http://www.foolmoon.net/downloads/Live_Forensics_Using_WFT.pdf.

Sommario

- Computer Forensics
 - Metodologie forensi
 - Live forensics
- Distribuzioni
 - DEFT
 - Helix
 - CAINE
- Analisi Forense dei dati volatili
 - Tipologie di dump
 - Dump tool
 - Process analysis tool
 - Clipboard tool
- Caso di studio
 - Ambiente di lavoro
 - Risultati
- Riferimenti

Distribuzioni Forensi

- Quattro distribuzioni basate su Linux
 - DEFT 6
 - CAINE 2.0
 - Helix 2008
 - Backtrack
- Tre distribuzioni presentano un eseguibile per live forensics
 - DEFT 6: Deft Extra 3.0
 - CAINE 2.0: WinTaylor
 - Helix 2008: Helix v.2.0

DEFT

- Acronimo di Digital Evidence & Forensic Toolkit
- Progetto 100% made in Italy, nato in collaborazione con il corso di Informatica Forense dell' Università degli Studi di Bologna verso la fine del 2005...
- ... evolutosi nel 2007 come progetto indipendente mantenendo collaborazioni con l'Università di Bologna e IISFA Italian Chapter
- Basata su Kubuntu
 - Attualmente alla versione 6.1.1
 - Data rilascio: 28 Ottobre 2011

[4] S. R. Stefano Fratepietro, «DEFT Manuale d'uso,» 2011. [Online]. Available: [http://www.deftlinux.net/doc/\[it\]deft_manuale_full.pdf](http://www.deftlinux.net/doc/[it]deft_manuale_full.pdf).



Helix

- Una delle più note nella computer forensic
- Basata su Knoppix
- Versione Free: Helix2008
- Versioni successive a pagamento
 - Attualmente alla versione 3Pro 2009 R3
 - Data rilascio: 23 Dicembre 2009



CAINE

- Acronimo di Computer Aided INvestigative Environment
- Sviluppata in Italia
- Offre un ambiente forense molto ampio in grado di supportare l' investigatore durante le fasi dell'analisi digitale
- Basata su Ubuntu
 - Attualmente alla versione 2.5.1 (Supernova)

Sommario

- Computer Forensics
 - Metodologie forensi
 - Live forensics
- Distribuzioni
 - DEFT
 - Helix
 - CAINE
- Analisi Forense dei dati volatili
 - Tipologie di dump
 - Dump tool
 - Process analysis tool
 - Clipboard tool
- Caso di studio
 - Ambiente di lavoro
 - Risultati
- Riferimenti

Tool utilizzati

- Strumenti per il dump e/o analisi
 - Win32dd/Win64dd
 - Winen
 - MDD
 - FTKImager
- Strumenti per il monitoraggio dei processi
 - VmMap
 - FileMonitor
- Strumenti per l'analisi della clipboard
 - InsideClipboard

[5] AccessData, «Forensic ToolKit User Guide,» 22 Maggio 2008. [Online]. Available: http://accessdata.com/downloads/media/FTK_1.80_Manual.pdf.

Dump RAM: Tipologie

- Dump di tipo RAW
 - Pro: copia esatta, simile al dd per device
 - Contro: non contiene lo stato del processore
- Dump di tipo crash
 - Pro:
 - dump completo delle pagine del Windows Memory Manager
 - include user e kernel land
 - Contro:
 - non è avviabile sui sistemi a 32 bit
 - Non acquisisce le pagini iniziali (password di autenticazione)
- Hibernation file
 - Pro:
 - Coinvolge i sistemi operativi Windows da 98 fino a Vista
 - Salva lo stato del processore, dei registri e della memoria nel file *hiberfil.sys*
 - Contro:
 - Viene eseguita solo quando l'utente richiede l'ibernazione

[6] M. Suiche, «Challenges of Windows physical memory acquisition and exploitation,» Giugno 2009. [Online]. Available: <http://shakacon.org/talks/NFI-Shakacon-win32dd0.3.pdf>.

Dump RAM

Memory Imaging

Windows

*Crash
Dump
(BSoD)*

Hibernation
File

External Tool

Win32dd

Winen, FTK
Imager,
MDD

Raw Dump

Crash Dump
(no BSoD)

Raw Dump

Dump: Win32dd

- Tool per il dump della RAM da shell di Windows
- Opzioni:
 - -f <filename> *file di output*
 - -r *RAW dump (default)*
 - -d *crash dump*
 - -s <value> *funzione hash*
 - 0 Nessun algoritmo
 - 1 SHA1
 - 2 MD5
 - 3 SHA-256

Win32dd - 1

```
C:\Documents and Settings\Gaetano\Documenti\Download\deft_6.1\deftwin\moonsols>win32dd -r -f C:\dump
win32dd - 1.3.1.20100417 - (Community Edition)
Kernel land physical memory acquisition
Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2009 - 2010, MoonSols <http://www.moonsols.com>

      Name          Value
      ----
File type:        Raw memory dump file
Acquisition method: PFN Mapping
Content:          Memory manager physical memory block
Destination path: C:\dump
O.S. Version:    Microsoft Windows XP Home Edition Service Pack 3
(build 2600)
Computer name:   CASA

Physical memory in use:      61%
Physical memory size:       1038700 Kb (< 1014 Mb)
Physical memory available:  403772 Kb (< 394 Mb)

Paging file size:          2503376 Kb (< 2444 Mb)
Paging file available:     1892080 Kb (< 1847 Mb)

Virtual memory size:       2097024 Kb (< 2047 Mb)
Virtual memory available:  2083128 Kb (< 2034 Mb)

Extented memory available:  0 Kb (< 0 Mb)

Physical page size:        4096 bytes
Minimum physical address:  0x0000000000003000
Maximum physical address:  0x000000003F6CF000

Address space size:        1064108032 bytes (1039168 Kb)

--> Are you sure you want to continue? [y/n]
```

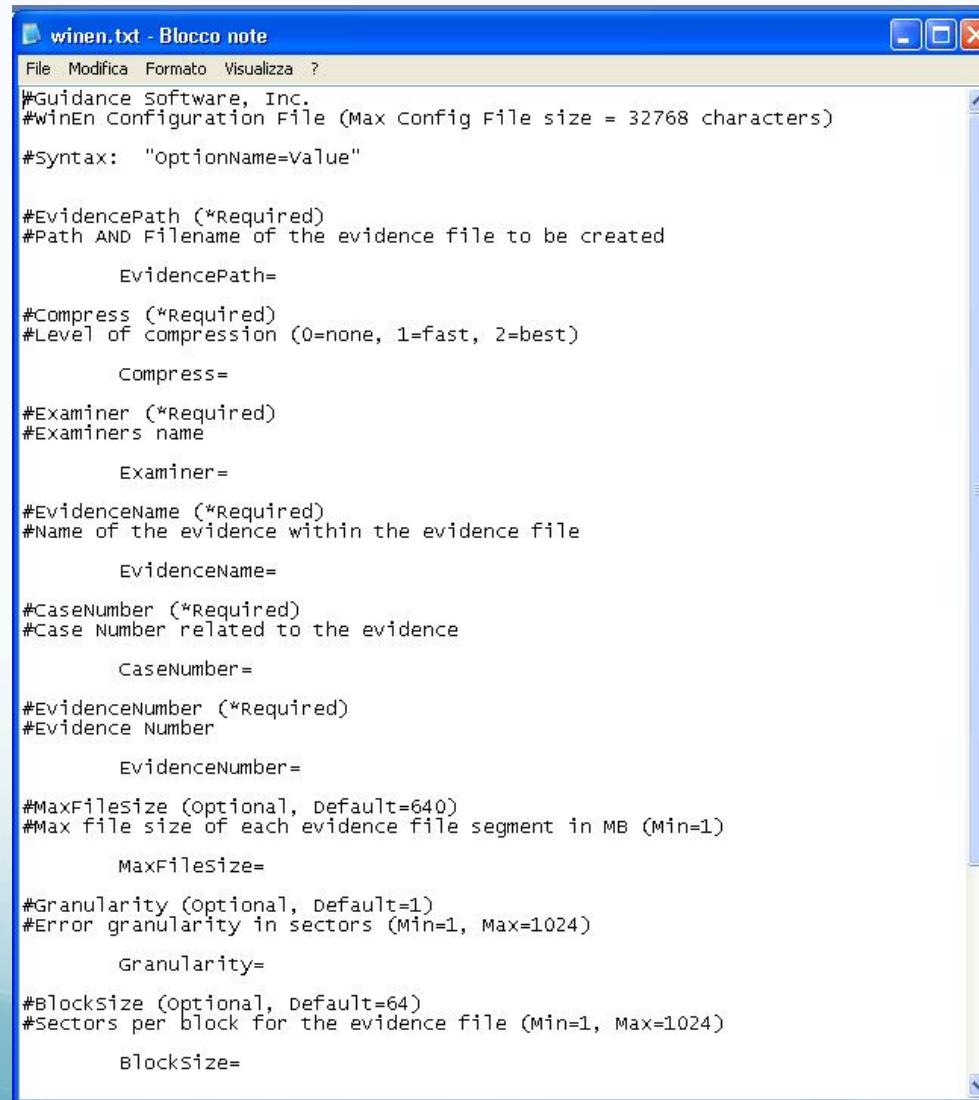
Win32dd – 2

```
--> Are you sure you want to continue? [y/n] y
Acquisition started at: [17/5/2011 <DD/MM/YYYY> 13:38:0 <UTC>]
Processing....Done.
Acquisition finished at: [2011-05-17 <YYYY-MM-DD> 13:38:19 <UTC>]
Time elapsed: 0:19 minutes:seconds (19 secs)
Created file size: 1064108032 bytes (< 1014 Mb)
NtStatus <troubleshooting>: 0x00000000
Total of written pages: 259693
Total of inaccessible pages: 0
Total of accessible pages: 259693
Physical memory in use: 62%
Physical memory size: 1038700 Kb (< 1014 Mb)
Physical memory available: 391828 Kb (< 382 Mb)
Paging file size: 2503376 Kb (< 2444 Mb)
Paging file available: 1887480 Kb (< 1843 Mb)
Virtual memory size: 2097024 Kb (< 2047 Mb)
Virtual memory available: 2083128 Kb (< 2034 Mb)
Extented memory available: 0 Kb (< 0 Mb)
Physical page size: 4096 bytes
Minimum physical address: 0x0000000000003000
Maximum physical address: 0x000000003F6CF000
Address space size: 1064108032 bytes (1039168 Kb)
```

Dump: Winen

- Standalone o incluso in EnCase
- Tool che permette anche la specifica dei parametri dell'evidenza
- Utilizzo:
 - `winen <-f nome_file_conf>`
 - Senza l'opzione il programma chiederà le credenziali del caso
 - Con l'opzione basta specificare un file di configurazione contenente le credenziali

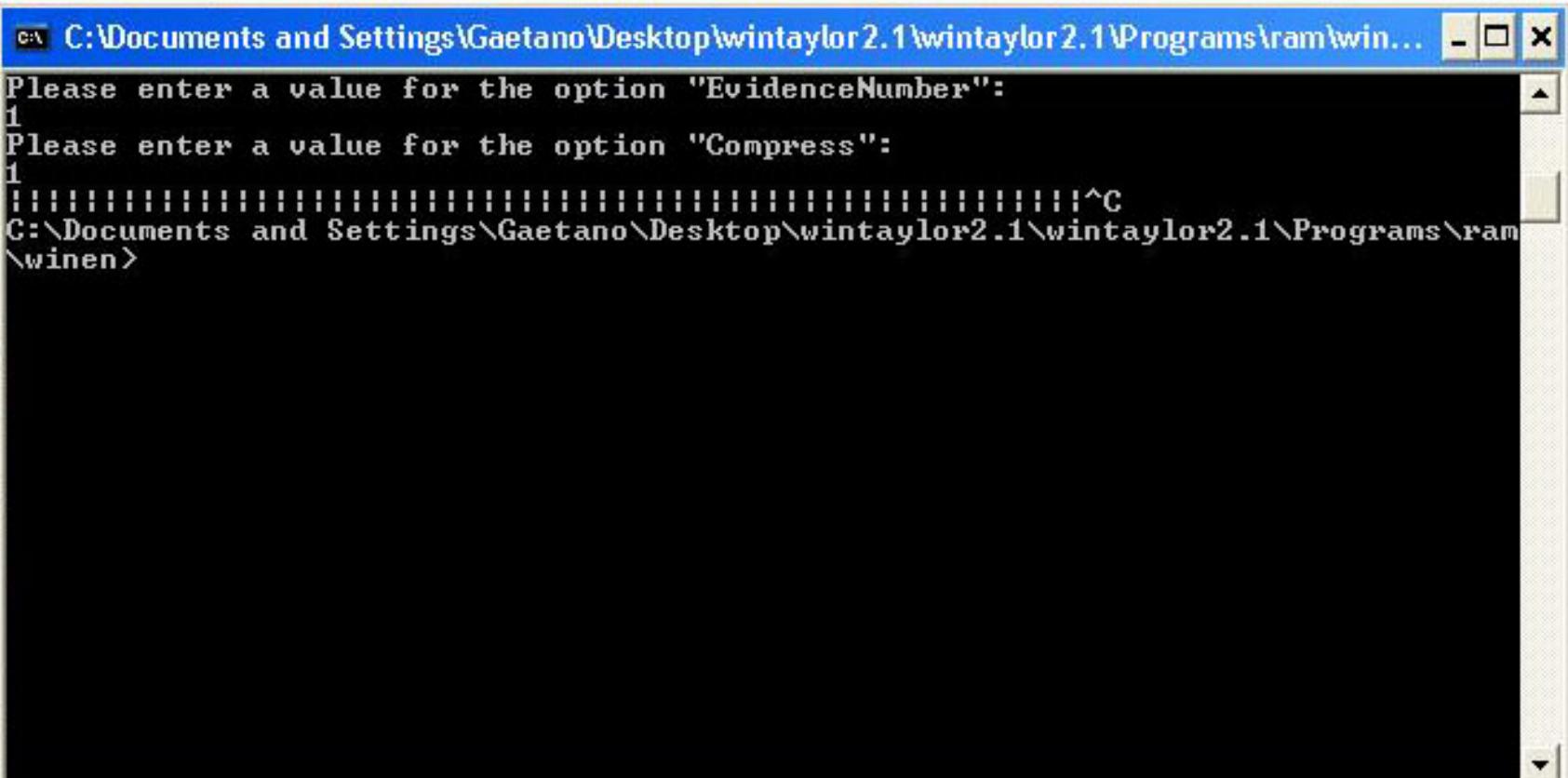
Winen: File di Config



The screenshot shows a Windows Notepad window with the title bar 'winen.txt - Blocco note'. The window contains a configuration file with the following content:

```
#Guidance Software, Inc.  
#winEn Configuration File (Max Config File size = 32768 characters)  
  
#Syntax: "OptionName=Value"  
  
#EvidencePath (*Required)  
#Path AND Filename of the evidence file to be created  
EvidencePath=  
  
#Compress (*Required)  
#Level of compression (0=none, 1=fast, 2=best)  
Compress=  
  
#Examiner (*Required)  
#Examiners name  
Examiner=  
  
#EvidenceName (*Required)  
#Name of the evidence within the evidence file  
EvidenceName=  
  
#CaseNumber (*Required)  
#Case Number related to the evidence  
CaseNumber=  
  
#EvidenceNumber (*Required)  
#Evidence Number  
EvidenceNumber=  
  
#MaxFilesize (Optional, Default=640)  
#Max file size of each evidence file segment in MB (Min=1)  
MaxFilesize=  
  
#Granularity (Optional, Default=1)  
#Error granularity in sectors (Min=1, Max=1024)  
Granularity=  
  
#Blocksize (Optional, Default=64)  
#Sectors per block for the evidence file (Min=1, Max=1024)  
Blocksize=
```

Winen senza config



```
C:\Documents and Settings\Gaetano\Desktop\wintaylor2.1\wintaylor2.1\Programs\ram\win...
Please enter a value for the option "EvidenceNumber":  
1  
Please enter a value for the option "Compress":  
1  
|||||  
C:\Documents and Settings\Gaetano\Desktop\wintaylor2.1\wintaylor2.1\Programs\ram\winen>
```

Dump: MemoryDD

- Tool per l'acquisizione della memoria in Windows
- Attualmente non è più in sviluppo
- Utilizzo:
 - mdd <opzioni>
 - -o *filename* - richiesto
 - -w - informazioni di licenza
 - -v - verbose

MemoryDD - 1

```
C:\Documents and Settings\Gaetano\Desktop\wintaylor2.1\wintaylor2.1\Programs\ram\mdd... □ X

C:\Documents and Settings\Gaetano\Desktop\wintaylor2.1\wintaylor2.1\Programs\ram\mdd>mdd -o c:\prova
-> mdd
-> ManTech Physical Memory Dump Utility
    Copyright (C) 2008 ManTech Security & Mission Assurance
-> This program comes with ABSOLUTELY NO WARRANTY; for details use option '-w'
    This is free software, and you are welcome to redistribute it
    under certain conditions; use option '-c' for details.
-> Dumping 1535.23 MB of physical memory to file 'c:\prova'.

393020 map operations succeeded (1.00)
0 map operations failed

took 40 seconds to write
MD5 is: 3bcd02163ed1815d2e5f85d709975c69

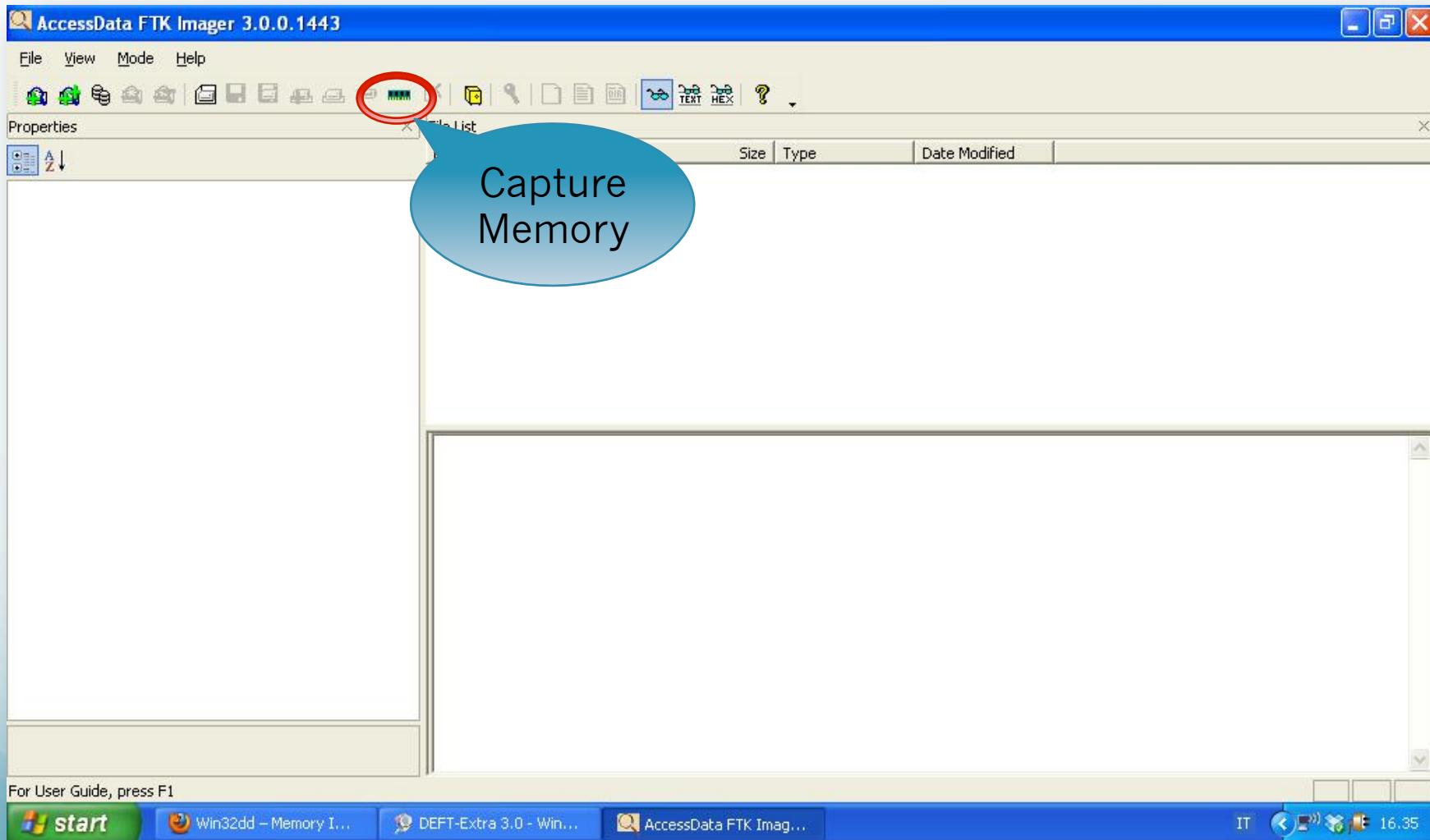
C:\Documents and Settings\Gaetano\Desktop\wintaylor2.1\wintaylor2.1\Programs\ram\mdd>
```

Dump/Analisi: FTKImager

- FTKImager viene utilizzato per
 - Creare immagini forensi di
 - Hard drive
 - Floppy
 - CD e DVD
 - RAM
 - Mostrare i contenuti di
 - dischi locali
 - periferiche locali con storage
 - Mostra i contenuti dei dump effettuati
 - Ultima versione: 3.4.1 del 24 Agosto 2011

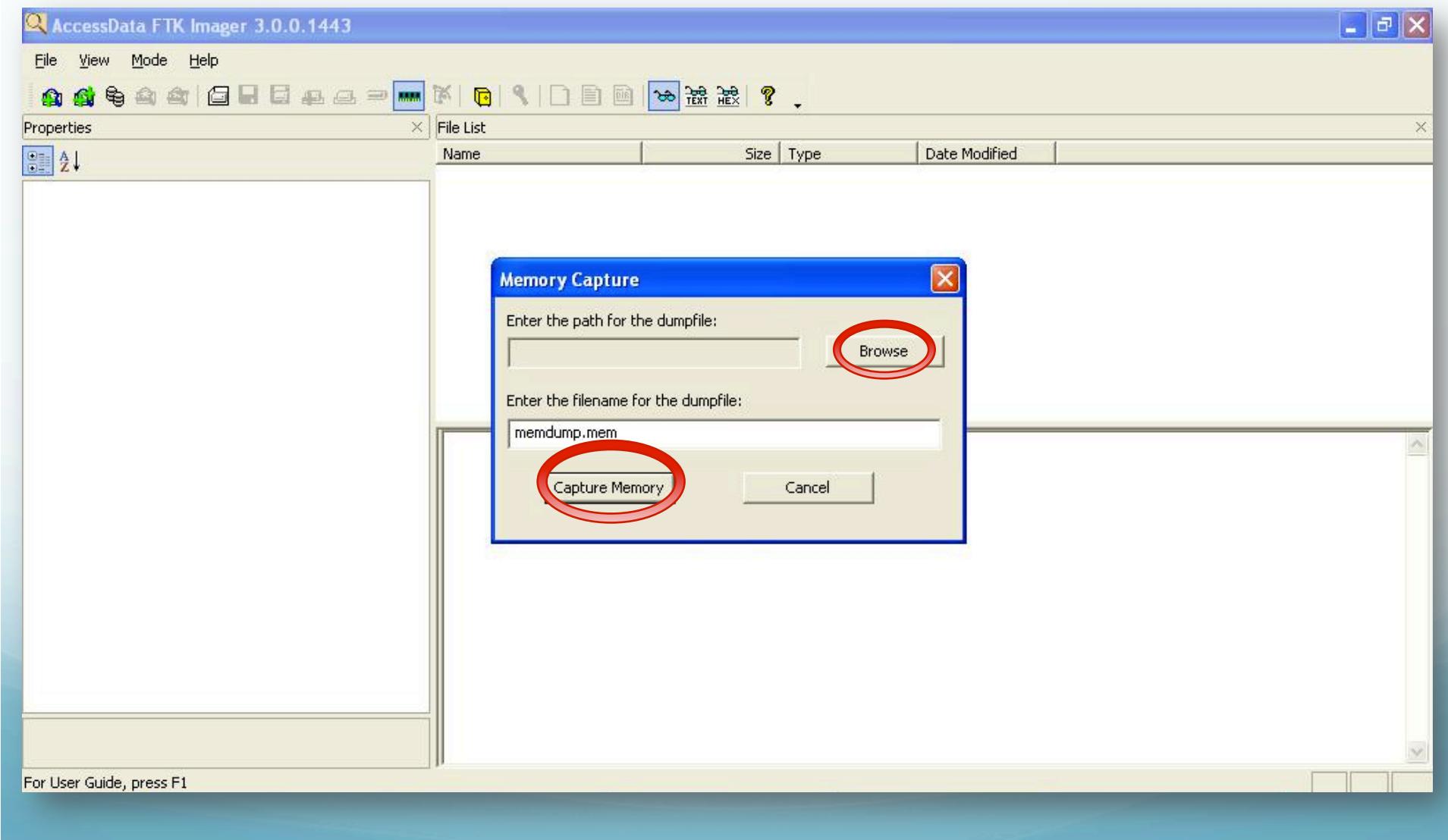
FTKImager – 1:

Acquisizione

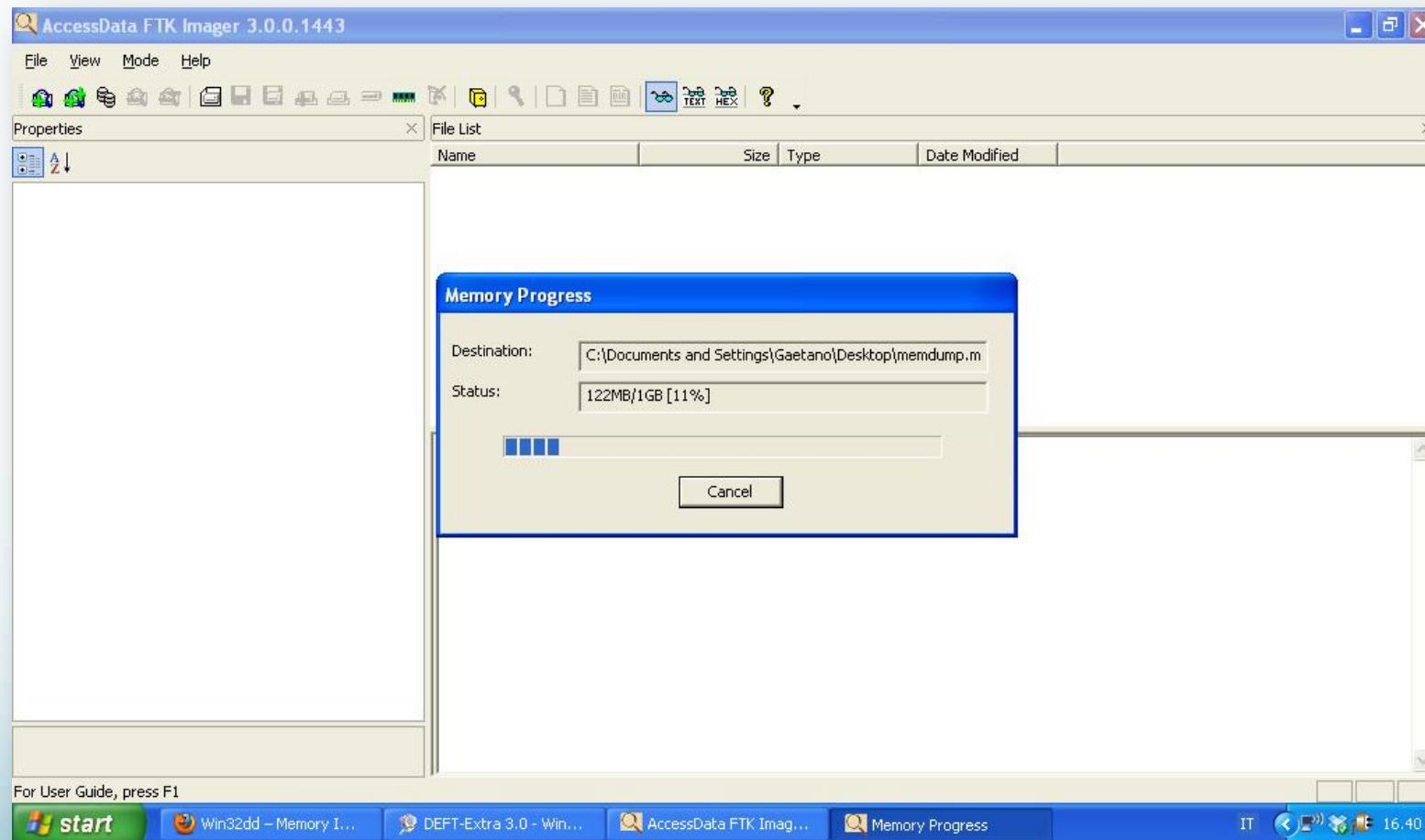


FTKImager – 2:

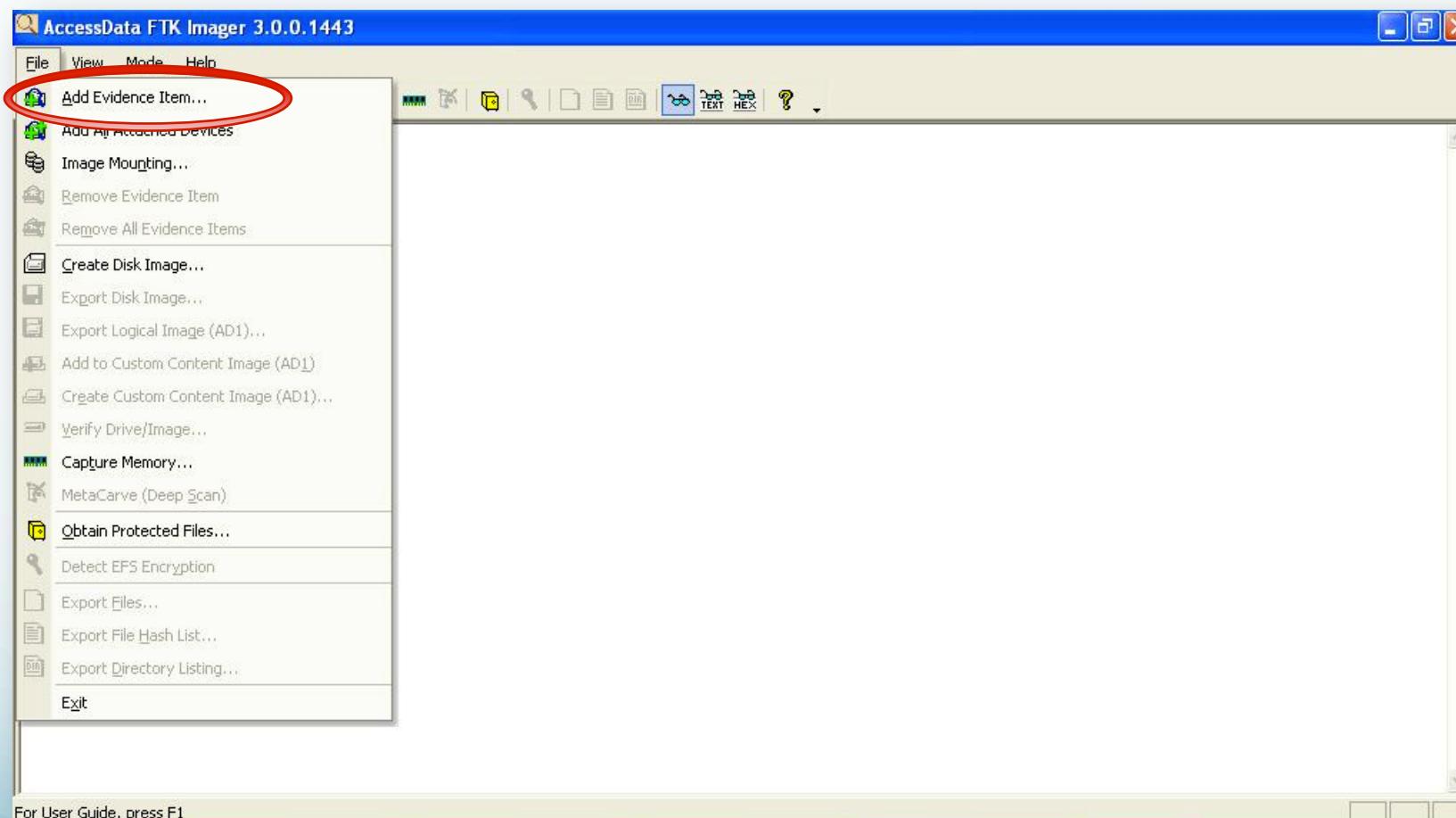
Acquisizione



FTKImager – 3: Acquisizione

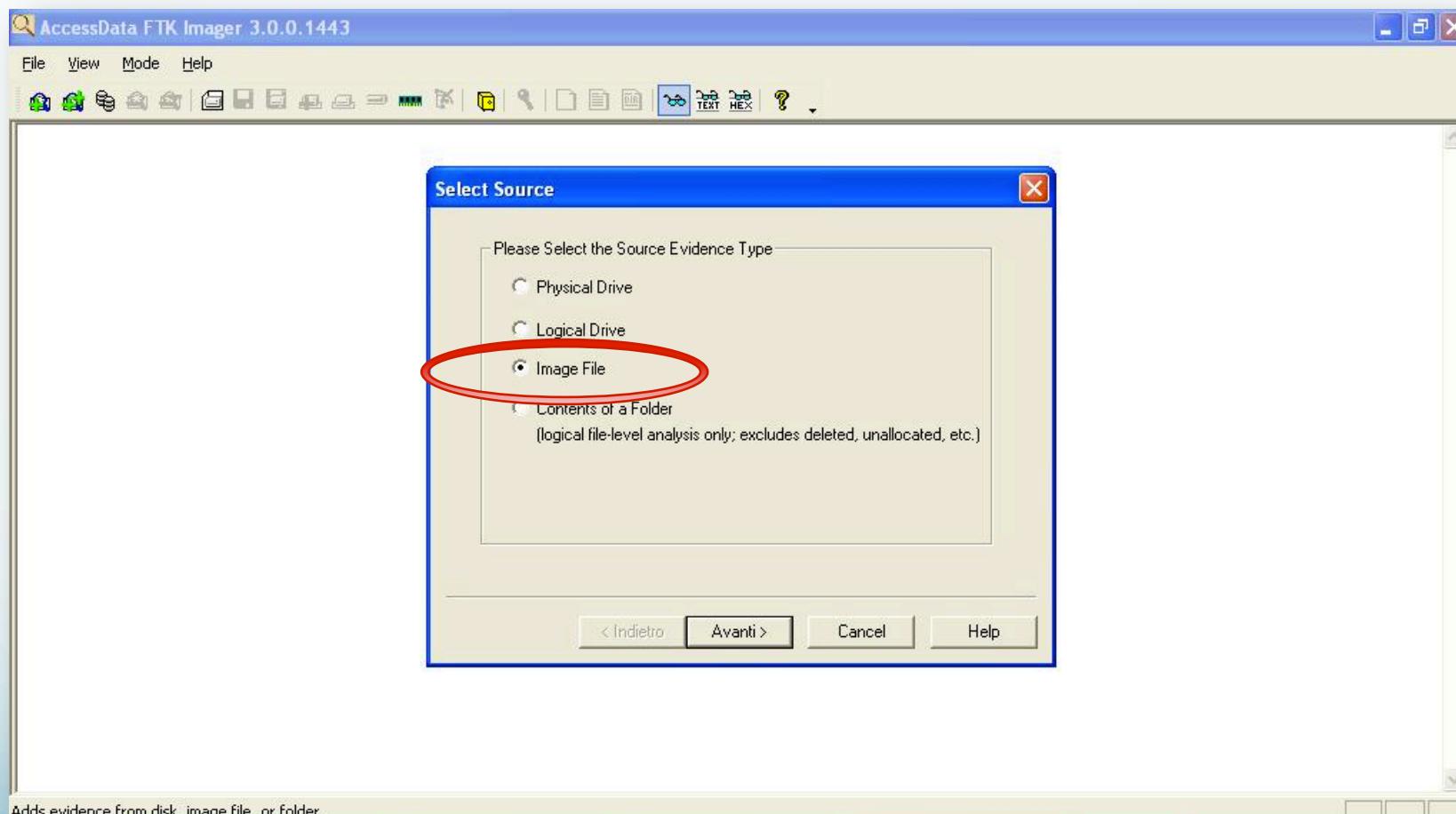


FTKImager – 4: Analisi



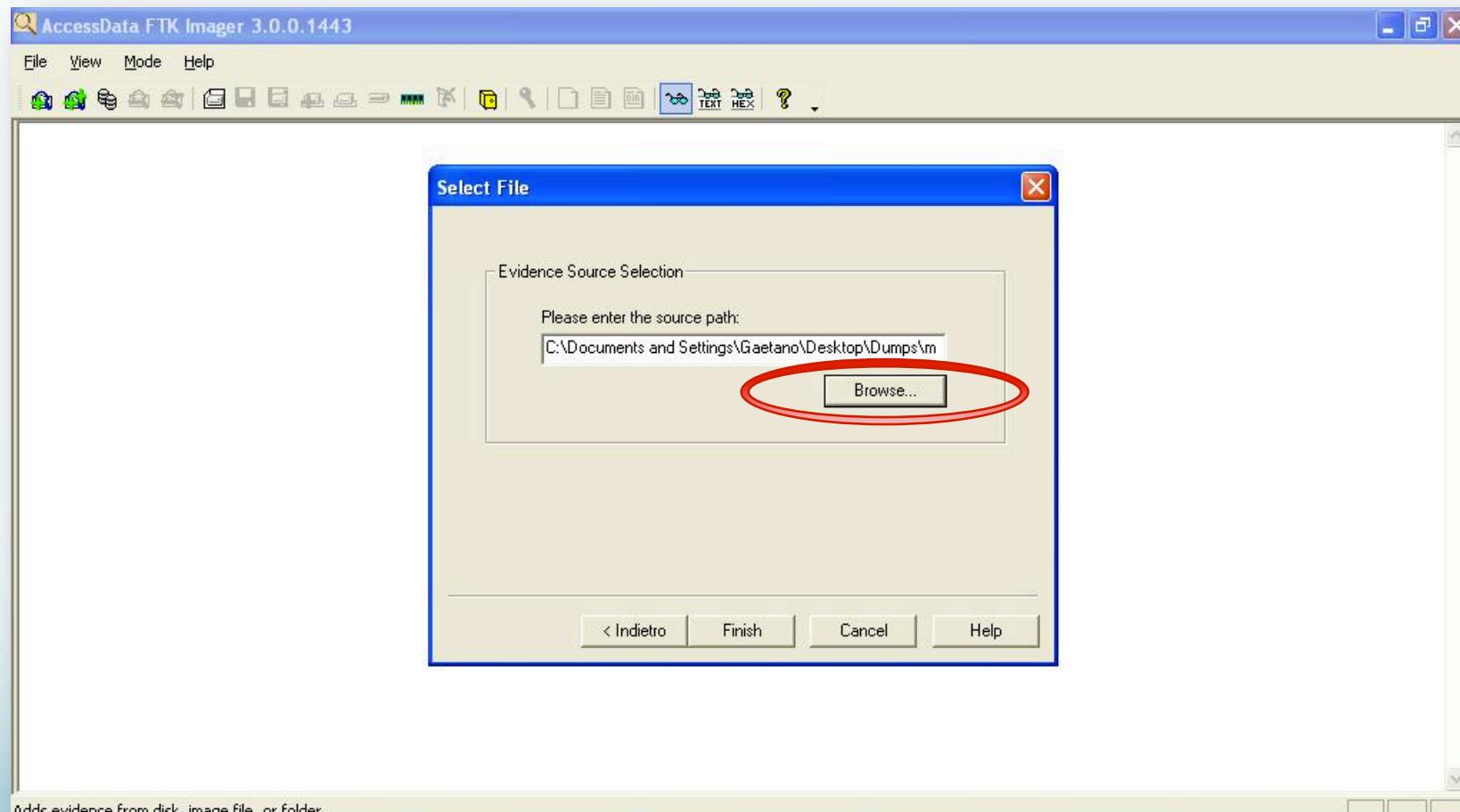
For User Guide, press F1

FTKImager – 5: Analisi



FTK Imager – 6:

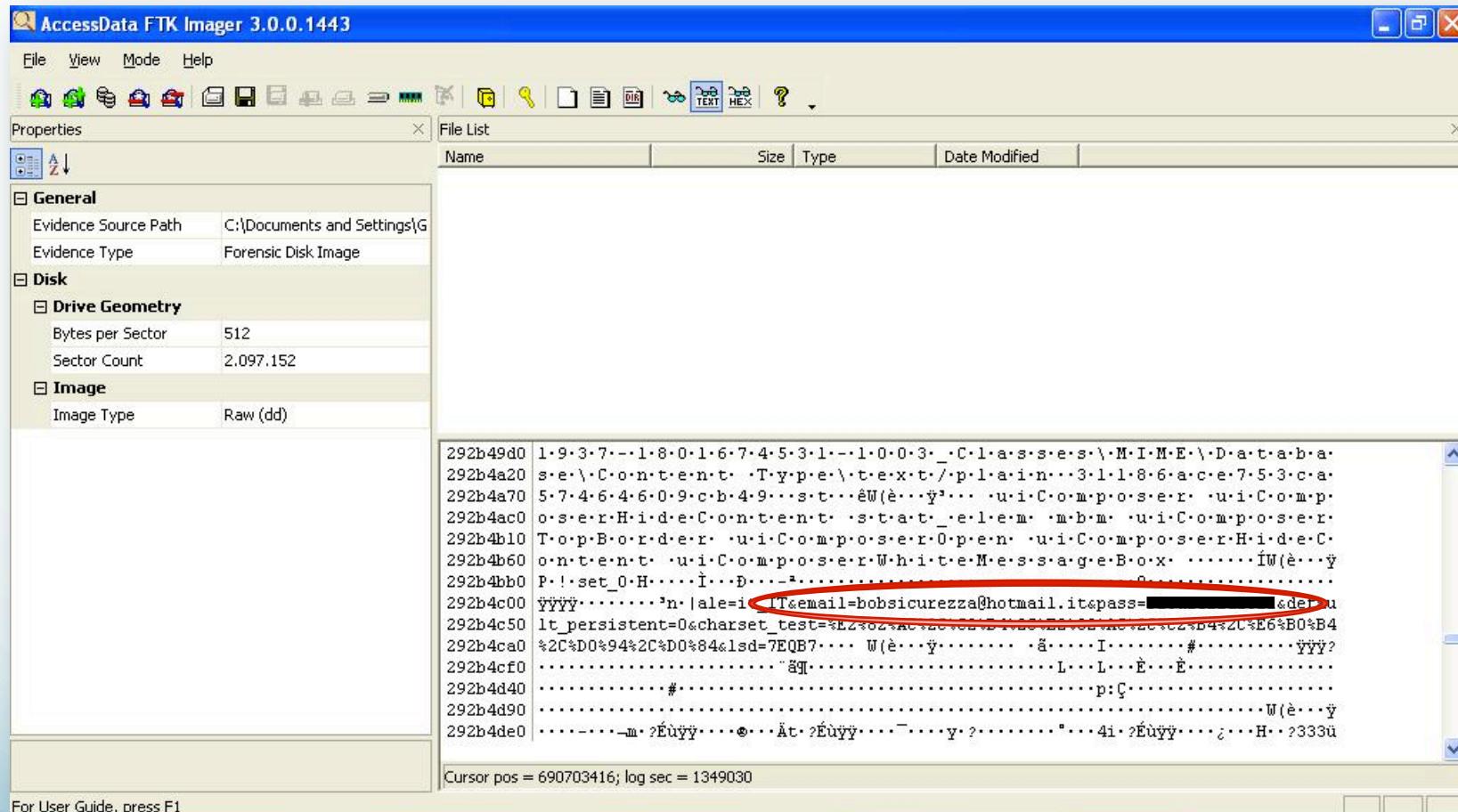
Acquisizione



Adds evidence from disk, image file, or folder

FTK Imager – 7:

Ricerca Evidenze



For User Guide, press F1

Win32dd vs Winen vs MDD vs FTKImager

	Win32dd	Winen	MDD	FTKImager
Acquisizione /Analisi	acquisizione	acquisizione	acquisizione	Acquisizione /analisi
Tipo Dump	Crash/RAW	RAW	RAW	RAW
GUI/Shell	Shell	Shell	Shell	GUI
Dettagli sul caso	NO	SI	NO	NO

Dettagli sul caso: esaminatore, id dell'evidenza, tipo di compressione, etc.

Processi in esecuzione: VmMap

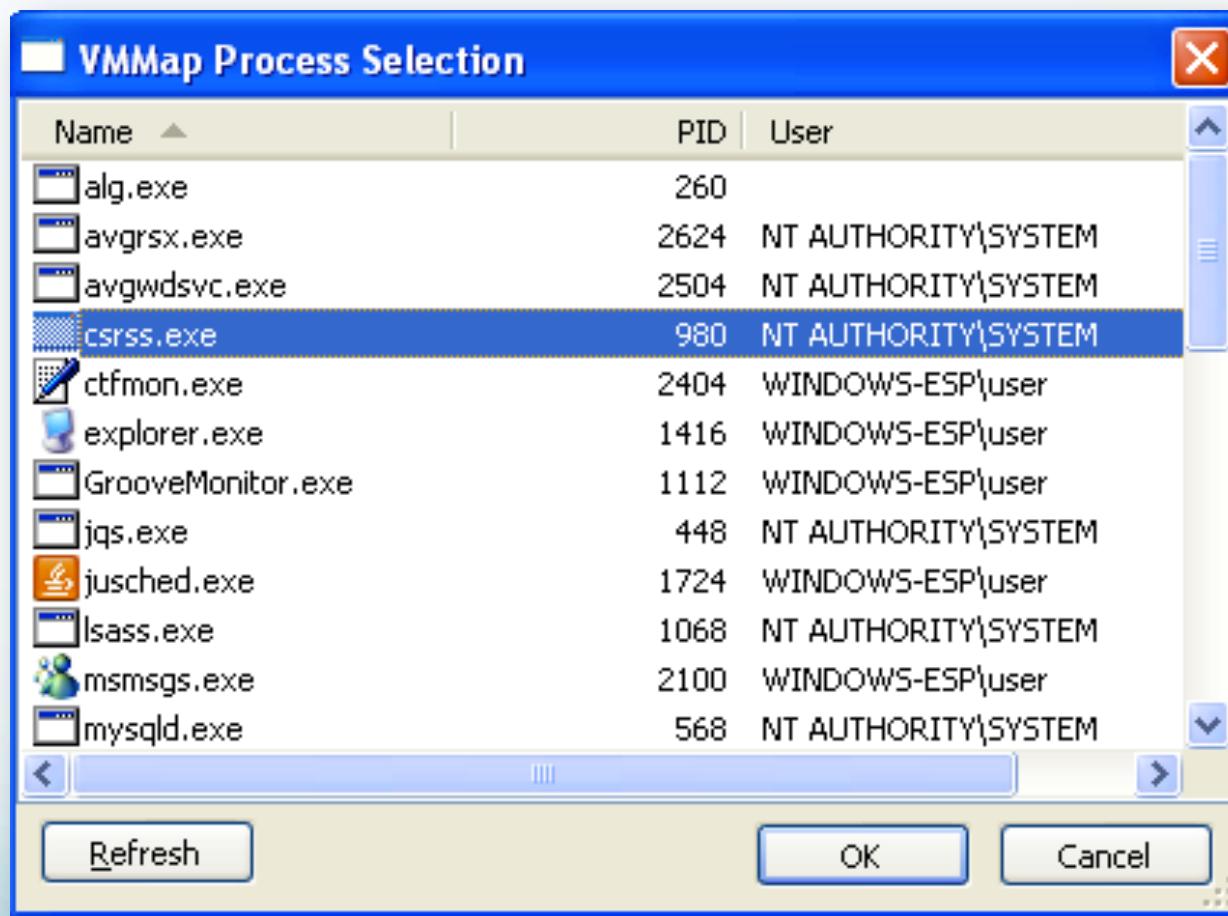
- Tool per analizzare la memoria
 - Fisica e virtuale
 - Scelta processo da analizzare
 - Analisi real-time

Sviluppato da Mark Russinovich and Bryce Cogswell

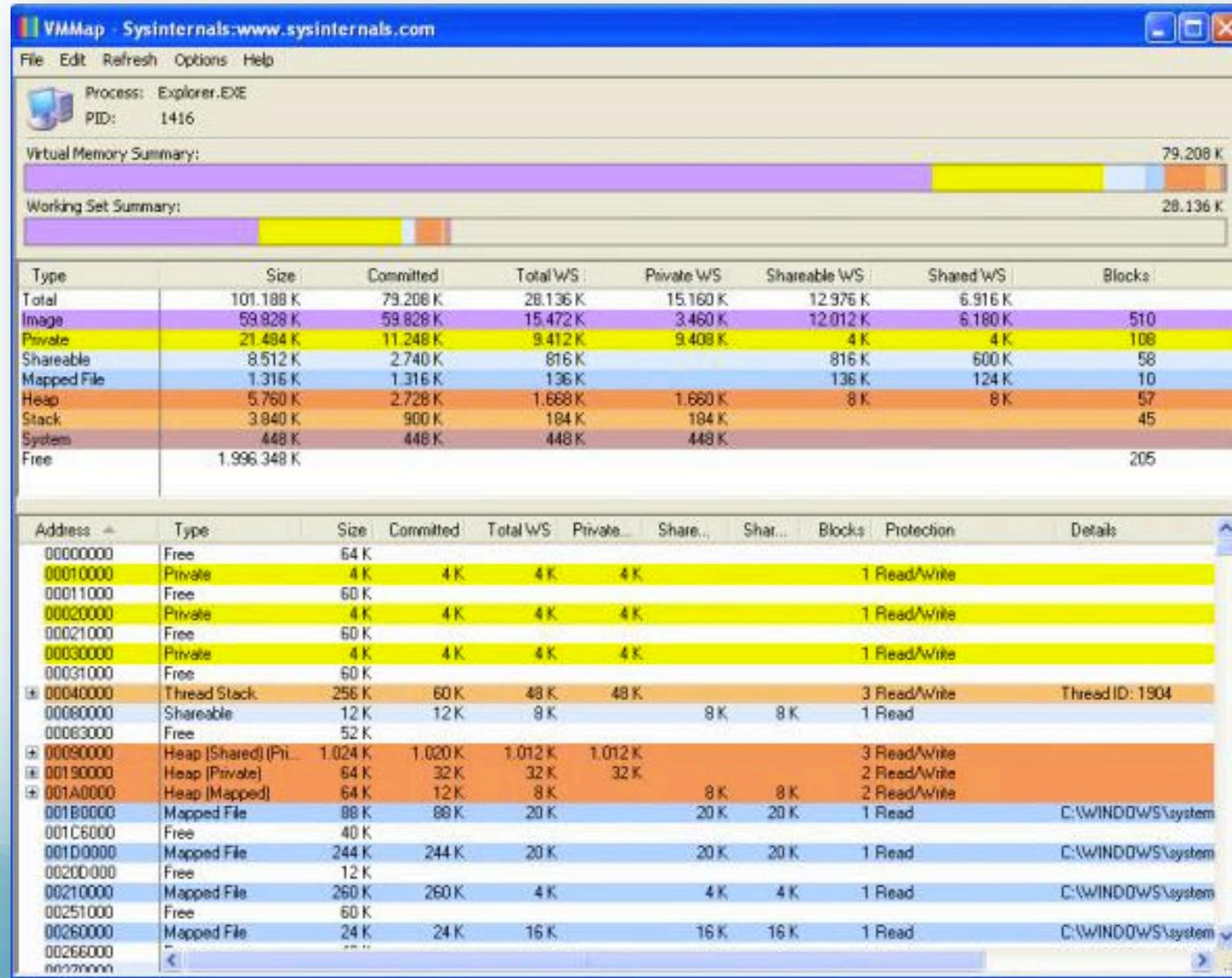


VmMap:

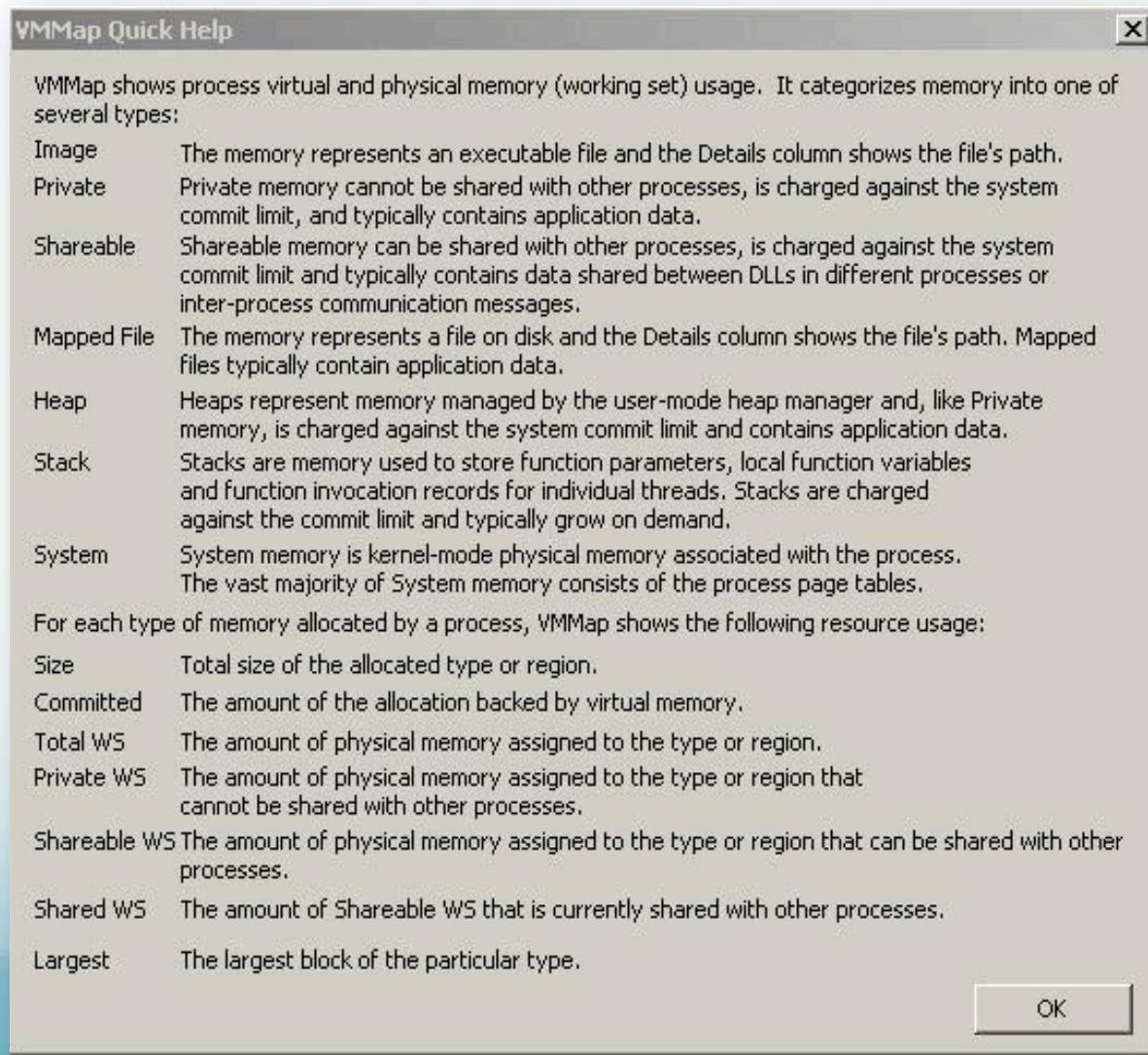
scelta processo



VmMap: visualizzazione



VmMap



Processi in esecuzione: FileMonitor

- FileMonitor permette di visualizzare l'attività del sistema in tempo reale.
- Le sue funzionalità lo rendono semplice da usare e allo stesso modo uno strumento potente per esplorare il modo in cui Windows funziona.

FileMonitor

#	Time	Process	Request	Path	Result	Other
1	17:00:23	svchost.ex...	QUERY INFORMATION	C:\WINDOWS\TEMP\ZLT02C70.TMP	NOT FOUND	Attributes: Error
2	17:00:23	svchost.ex...	QUERY INFORMATION	C:\WINDOWS\TEMP\ZLT06EC9.TMP	SUCCESS	Attributes: TA
933	17:06:56	winlogon.e...	CREATE	C:\WINDOWS\TEMP\win2.tmp	SUCCESS	Options: Create Access: All
934	17:06:56	winlogon.e...	QUERY INFORMATION	C:\WINDOWS\TEMP\win2.tmp	SUCCESS	FileNameInformation
935	17:06:56	winlogon.e...	QUERY INFORMATION	C:\WINDOWS\TEMP\win2.tmp	SUCCESS	FileNameInformation
936	17:06:56	winlogon.e...	DIRECTORY	C:\WINDOWS\Temp\	SUCCESS	FileBothDirectoryInformation:...
937	17:06:56	winlogon.e...	CLOSE	C:\WINDOWS\TEMP\win2.tmp	SUCCESS	
938	17:08:56	winlogon.e...	CREATE	C:\WINDOWS\TEMP\win3.tmp	SUCCESS	Options: Create Access: All
939	17:08:56	winlogon.e...	QUERY INFORMATION	C:\WINDOWS\TEMP\win3.tmp	SUCCESS	FileNameInformation
940	17:08:56	winlogon.e...	QUERY INFORMATION	C:\WINDOWS\TEMP\win3.tmp	SUCCESS	FileNameInformation
941	17:08:56	winlogon.e...	DIRECTORY	C:\WINDOWS\Temp\	SUCCESS	FileBothDirectoryInformation:...
942	17:08:56	winlogon.e...	CLOSE	C:\WINDOWS\TEMP\win3.tmp	SUCCESS	
943	17:10:57	winlogon.e...	CREATE	C:\WINDOWS\TEMP\win4.tmp	SUCCESS	Options: Create Access: All
944	17:10:57	winlogon.e...	QUERY INFORMATION	C:\WINDOWS\TEMP\win4.tmp	SUCCESS	FileNameInformation
945	17:10:57	winlogon.e...	QUERY INFORMATION	C:\WINDOWS\TEMP\win4.tmp	SUCCESS	FileNameInformation
946	17:10:57	winlogon.e...	DIRECTORY	C:\WINDOWS\Temp\	SUCCESS	FileBothDirectoryInformation:...
947	17:10:57	winlogon.e...	CLOSE	C:\WINDOWS\TEMP\win4.tmp	SUCCESS	
948	17:12:57	winlogon.e...	CREATE	C:\WINDOWS\TEMP\win5.tmp	SUCCESS	Options: Create Access: All
949	17:12:57	winlogon.e...	QUERY INFORMATION	C:\WINDOWS\TEMP\win5.tmp	SUCCESS	FileNameInformation
950	17:12:57	winlogon.e...	QUERY INFORMATION	C:\WINDOWS\TEMP\win5.tmp	SUCCESS	FileNameInformation
951	17:12:57	winlogon.e...	DIRECTORY	C:\WINDOWS\Temp\	SUCCESS	FileBothDirectoryInformation:...
952	17:12:57	winlogon.e...	CLOSE	C:\WINDOWS\TEMP\win5.tmp	SUCCESS	
953	17:14:57	winlogon.e...	CREATE	C:\WINDOWS\TEMP\win6.tmp	SUCCESS	Options: Create Access: All
954	17:14:57	winlogon.e...	QUERY INFORMATION	C:\WINDOWS\TEMP\win6.tmp	SUCCESS	FileNameInformation
955	17:14:57	winlogon.e...	QUERY INFORMATION	C:\WINDOWS\TEMP\win6.tmp	SUCCESS	FileNameInformation
956	17:14:57	winlogon.e...	DIRECTORY	C:\WINDOWS\Temp\	SUCCESS	FileBothDirectoryInformation:...
957	17:14:57	winlogon.e...	CLOSE	C:\WINDOWS\TEMP\win6.tmp	SUCCESS	

Analisi Clipboard: InsideClipboard

- Tool prodotto dalla **NirSoft** che permette di visualizzare i dati contenuti nella clipboard di windows
- L'utility permette di visualizzare tutti i formati presenti attualmente nella clipboard visualizzandoli in formato ASCII(formato RTF o HTML) o come dump esadecimale
- Non necessita di installazione o file aggiuntivi per poterlo eseguire

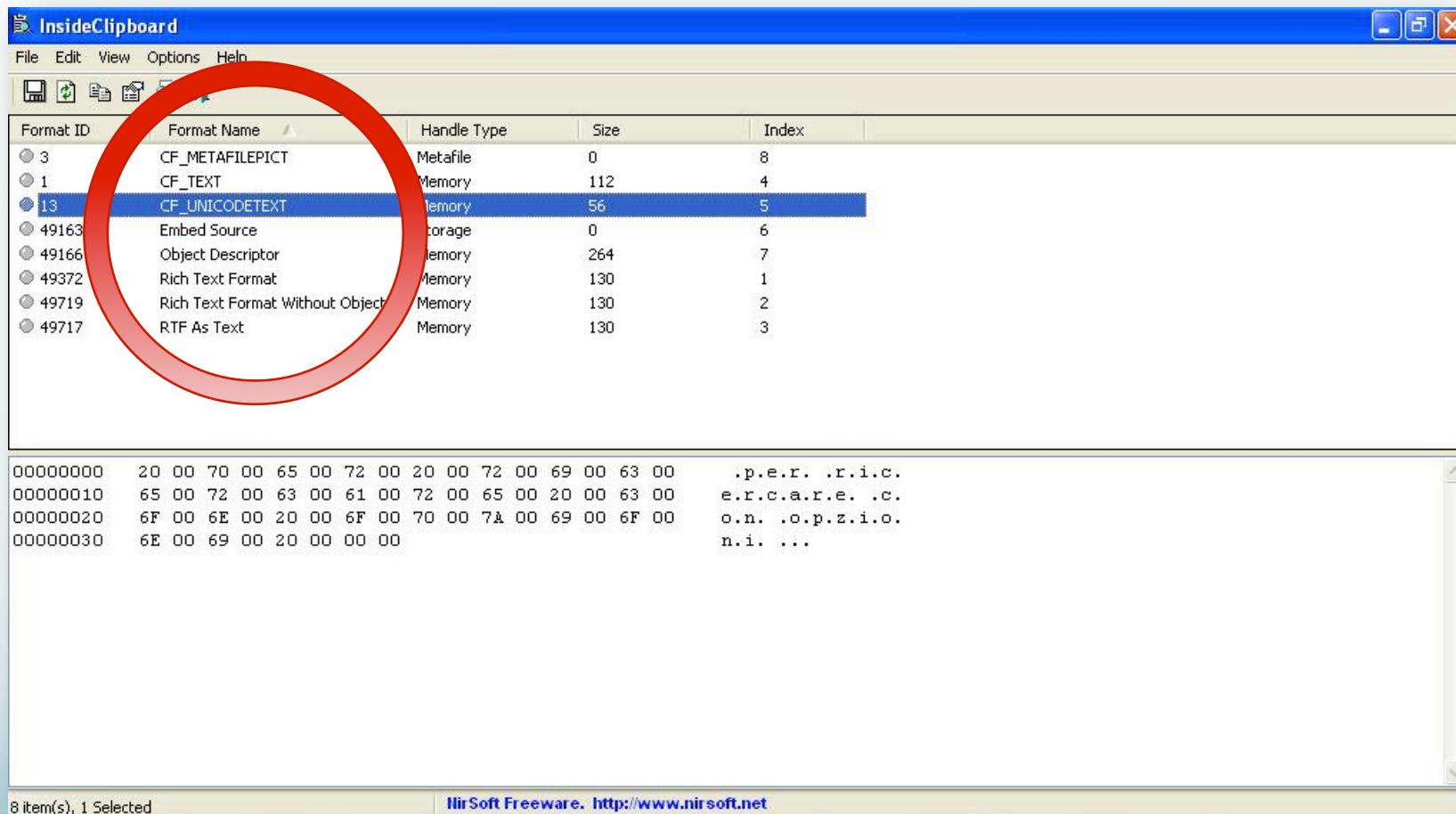
InsideClipboard di un file

The screenshot shows the InsideClipboard application interface. At the top is a menu bar with File, Edit, View, Options, and Help. Below the menu is a toolbar with icons for opening files, saving, and clipboard operations. The main window contains two tables. The top table lists clipboard formats with columns for Format ID, Format Name, Handle Type, Size, and Index. A red circle highlights the row for CF_HDROP. The bottom table displays binary data in hex and ASCII format.

Format ID	Format Name	Handle Type	Size	Index
15	CF_HDROP	Memory	1.760	2
49158	FileName	Memory	54	5
49159	FileNameW	Memory	136	6
49336	Preferred DropEffect	Memory	4	3
49268	Shell IDList Array	Memory	1.034	1
49327	Shell Object Offsets	Memory	104	4

00000000	14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000010	01 00 00 00 43 00 3A 00 5C 00 44 00 6F 00 63 00C...\.D.o.c.
00000020	75 00 6D 00 65 00 6E 00 74 00 73 00 20 00 61 00	u.m.e.n.t.s. .a.
00000030	6E 00 64 00 20 00 53 00 65 00 74 00 74 00 69 00	n.d. .S.e.t.t.i.
00000040	6E 00 67 00 73 00 5C 00 47 00 61 00 65 00 74 00	n.g.s.\.G.a.e.t.
00000050	61 00 6E 00 6F 00 5C 00 44 00 6F 00 63 00 75 00	a.n.o.\.D.o.c.u.
00000060	6D 00 65 00 6E 00 74 00 69 00 5C 00 44 00 6F 00	m.e.n.t.i.\.D.o.
00000070	77 00 6E 00 6C 00 6F 00 61 00 64 00 5C 00 64 00	w.n.l.o.a.d.\.d.
00000080	65 00 66 00 74 00 5F 00 36 00 2E 00 31 00 5C 00	e.f.t._.6...1\.
00000090	2E 00 64 00 69 00 73 00 6B 00 00 00 43 00 3A 00	..d.i.s.k...C...\\
000000A0	5C 00 44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00	\.D.o.c.u.m.e.n.
000000B0	74 00 73 00 20 00 61 00 6E 00 64 00 20 00 53 00	t.s. .a.n.d. .S.
000000C0	65 00 74 00 74 00 69 00 6E 00 67 00 73 00 5C 00	e.t.t.i.n.g.s.\.
000000D0	47 00 61 00 65 00 74 00 61 00 6E 00 6F 00 5C 00	G.a.e.t.a.n.o.\.

InsideClipboard di un testo



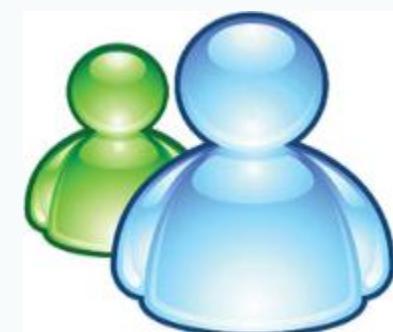
Sommario

- Computer Forensics
 - Metodologie forensi
 - Live forensics
- Distribuzioni
 - DEFT
 - Helix
 - CAINE
- Analisi Forense dei dati volatili
 - Tipologie di dump
 - Dump tool
 - Process analysis tool
 - Clipboard tool
- Caso di studio
 - Ambiente di lavoro
 - Risultati
- Riferimenti

Caso di studio

Individuare eventuali tracce di «attività» recenti su

- Facebook
- Windows Live Messenger
- Windows Hotmail
- Skype
- Gmail



Perché la webmail

- Utilizzata per scambiare informazioni in modo sicuro

Come ?

- Alice e Bob si incontrano e si scambiano le credenziali di accesso
- Alice:
 - Effettua il login nella webmail
 - Scrive un messaggio in bozza
 - Effettua il logout dalla webmail
- Bob:
 - Effettua il login nella webmail
 - Legge il messaggio
 - Effettua il logout



Ambiente di lavoro -1

- Macchine Virtuali eseguite su VMWare Player:
 - Macchina 1:
 - Windows XP SP3
 - 1GB di Ram
 - Macchina 2:
 - Windows 7 Professional
 - 1GB di Ram
- Software installati:
 - Skype 5.3.0.111
 - Windows Live Messenger – versione 2009 (Build 14.0.8117.416)
 - Internet Explorer 8.0.6001.18702IC
 - Chrome 11.0.696.60

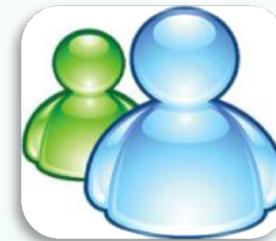
Ambiente di lavoro -2

- Account creati:
 - Hotmail
 - alicesicurezza@hotmail.it
 - bobsicurezza@hotmail.it
 - Facebook
 - Alice Sicurezza
 - Bob Sicurezza
 - Skype
 - alice.sicurezza
 - bob.sicurezza
 - Gmail
 - alicesicurezza@gmail.com



Risultati - 1

- Facebook
 - Password
 - Messaggi chat
- Windows Live Messenger
 - Messaggi chat
 - Trasferimento file
- Skype
 - Durata conversazione
- Hotmail
 - Password
 - Informazioni su bozze
- Gmail
 - Account accesso
 - Informazioni su bozze



Risultati - 2

- Test durabilità dei dati
 - Esecuzione del gioco NeverWinterNight 2
 - Sessione di 30 minuti di gioco
 - Informazioni assenti
- Test su Windows 7
 - Risultati identici
 - Chrome non memorizza in RAM le credenziali di accesso a Facebook
- Acquisizione RAM video
 - Nessuna informazione né software in rete
- Chrome in modalità incognito
 - Evidenze comunque presenti

Metodologie di ricerca

- Facebook
 - Password
 - Messaggi chat
- Windows Live Messenger
 - Messaggi chat
 - Trasferimento file
- Skype
 - Durata Conversazione
- Hotmail
 - Password
 - Informazioni su bozze
- Gmail
 - Account accesso (NO password)
 - Informazioni su bozze

Facebook: password

Facebook: password

- Pattern trovato
 - *email=nomeutente&pass=password*
- Testo da ricercare
 - email=
 - &pass=
- Possibile espressione regolare
 - *email=.*&pass=.*&*

Facebook: chat

06386390
063863e0FILE0...P...].....8.....(.....eU..
06386430	..";.....H.....D·Á2·í..D·Á2·í..D·Á2·í..D·Á2·í..
063864800...x.....Z.....@M.....D·Á2·í..D·Á2·í..D·Á2·í..
063864d0	D·Á2·í.....P_..1..0..0..0..~..4..T·X·T·2..7..2..0.....
06386520	x.....@M.....D·Á2·í..D·Á2·í..D·Á2·í..D·Á2·í.....p_..1..
06386570	0..0..0..0..2..3..3..4..2..7..2..5..7..=..1..2..[..1..]..t..x..t.....f.....for (();
063865c0	;{"t":"msg","c":"p_100002333427257","s":13,"ms":[{"msg":{"text .. "grazie mille :D
06386610	","time":1304606569424,"clientTime":1304606568299,"msgID":"86610147"}, "from":100
06386660	002363967130,"to":100002333427257,"from_name":"Alice Sicurezza","from_first_name
063866b0	":"Alice","from_gender":1,"f1":1,"to_name":"Bob Sicurezza","to_first_name":"Bob"
06386700	,"to_gender":2,"type":"msg"}]} .. YYYY.yG.....
06386750
063867a0
063867f0FILE0...zS].....8..8.....fU.....`..
06386840H.....Zé Ņ2·í..Zé Ņ2·í..Zé Ņ2·í..Zé Ņ2·í..
063868900...x.....Z.....M.....Zé Ņ2·í..Zé Ņ2·í..Zé Ņ2·í..
063868e0B..9..B..5..R..P..~..1..P..N..G..1..]..0.....f.....M.....
06386930	Zé Ņ2·í..Zé Ņ2·í..Zé Ņ2·í..Zé Ņ2·í.....b..9..B..5..r..P..7..C..Z..U..J..
06386980	[..1..]..p..n..g.....PNG.....IHDR.....2Í¾..KIDA
063869d0	TxÚ·Í;..DQ·"iÑ‰·Ã·utÃr···'‰<q)"@D·E·udh·f·üÖFkøÁö·ë·3PYXYØYh, ..>u-/y³N'
06386a20	···IEND@B`.....YYYY.yG.....
06386a70

Facebook: chat

- Pattern trovato
 - `[{"msg":{"text":"testodelmessaggio","time":timestamp,"clientTime":...}}`
- Testo da ricercare
 - `[{"msg":{"text":`
- Possibile espressione regolare
 - `for (;;) {"t":"msg",.*time"`

Messenger: chat

2c4cb220
2c4cb270
2c4cb2c0
2c4cb310
2c4cb360 F
2c4cb3b0
2c4cb400(.....
2c4cb450'üy Non·fornire·mai·informazio·
2c4cb4a0	n·i··quali·la·passw·ord·o·il·numero·della·c·
2c4cb4f0	arta·di·credi·to·in·un·messag·gio·istant·an·
2c4cb540	e·o·üy ·Bob·scrive··üyCiao·Alice·üy·Alice·s·
2c4cb590	cri·ve··üyciao·bob··üycome·stai?··üyd·a·quanto·
2c4cb5e0	tempo·Bob·scrive··üytutt·o·ben·e··üystavo·pre·
2c4cb630	parando·l'e·same·di·sicurezza!·Bob·invia··
2c4cb680	üy·Annul·la·(Alt+Q)··üy··üy·Trasferim·ento·de·
2c4cb6d0	l·file··"·Tramonto·jAnnul·la·(Alt+Q)··üy··üy·Tr·
2c4cb720	a·sferim·ento·del·file·"·Tramonto·jpq"·comp·
2c4cb770	letato··üy!·ä·p.....
2c4cb7c0(.....
2c4cb8104.....
2c4cb860!.....ð·ä·ð·ä.....

Messenger: chat

- Pattern trovato
 - *nomeUtente* scrive: *messaggio*
 - Trasferimento del file
- Testo da ricercare
 - scrive:
- Possibile espressione regolare
 - scrive:

Skype: durata chiamata

073b96e0 | ð · · · · 0 · > · 10iÔ»È, è, É: \ge. öL"zÓöI · iT · 2WÒ · ÉZ^W ·) · Èq · · y=® · ø¶ · ýS · ~ · b<ó (èJYU «ö- · { ·
073b9730 | ù · INéD · · · fç · ID · à · 9 · ~ · 8YVÖ · u · · +òø · %Ñl« · · (· « · ¥r^ · xP · Äý «r · FQ^- · «fR · · @^ · É · Ýg!± ·
073b9780 | I · i#qÛx+ · Ó · d · · "xü@ · F · · °Y · Õ · H\$' · , · à · · =w*xñÈý · u · /aLÎ"] · pé · Eß · É · è · çÎ · ó · ÉÈ ·) !% · ö< · oÜ ·
073b97d0 | \$< · áWò · ;+;âP · I · iXi · ê · , · VIZÔ» · · o · vP · 8o» · 1È, äxÖ{óÈ} · · È · N-¾ · H · <á · ý^ · Q]E^V\·oñ · @; ·
073b9820 | 6o · ð: «pÅ¹È · BOu? · @2EA · %ÄF*o · I · fâÈQ · Ùk · çá · G · + · ¾ · x(· ¾ · ï])g^@^ · · B§- · (· · nj · È[· «ù ·
073b9870 | W · · +&ö · · f§Éç_ · · " · §È · " · w · ô · · HD=q "5TDâ · · (^J^ · ðcII^ · fS · +u= · f · · D: "N%d · DIY^ · tÅ>T ·
073b98c0 | # · .;BT{i^#¥ · · ë · d · = · QÈf · qâO" · ¾ · « · · · · §+ · áQ · 9 · J · è · F%n\$üw · ö6 · ö` · o · · · · é0 · | · · · ·
073b9910 | < · / · p · a · r · t · > · · · · < · p · a · r · t · · i · d · e · n · t · i · t · y · = · " · b · o · b · · s · i · c · u · r · e · z · z · a · ·
073b9960 | > · · · · · < · n · a · m · e · > · b · o · b · · s · i · c · u · r · e · z · z · a · < · / · n · a · m · e · > · · · · · < · d · u ·
073b99b0 | r · a · t · i · o · n · > · 1 · 2 · < · / · d · u · r · a · t · i · o · n · > · · · · < · / · p · a · r · t · > · · · < · / · p · a · r · t · l · i · s ·
073b9a00 | t · > · · · · · ã · · · · o · «§ · @ · » · | · · · · < · / · p · a · r · t · > · · · · < · p · a · r · t · · i · d · e · n · t · i · t · y ·
073b9a50 | = · " · b · o · b · · s · i · c · u · r · e · z · z · a · · > · · · · < · n · a · m · e · > · b · o · b · · s · i · c · u · r · e · z ·
073b9aa0 | a · < · / · n · a · m · e · > · · · · < · d · u · r · a · t · i · o · n · > · 1 · 2 · < · / · d · u · r · a · t · i · o · n · > · · · < ·
073b9af0 | / · p · a · r · t · > · · · < · / · p · a · r · t · l · i · s · t · > · · · Ún;;+ · o · 7% · H · » · | · · · · < · / · p · a · r · t · > · ·
073b9b40 | · · < · p · a · r · t · · i · d · e · n · t · i · t · y · = · " · b · o · b · · s · i · c · u · r · e · z · z · a · · > · · · · < · n ·
073b9b90 | a · m · e · > · b · o · b · · s · i · c · u · r · e · z · z · a · < · / · n · a · m · e · > · · · · < · d · u · r · a · t · i · o · n · > · 1 ·
073b9be0 | 2 · < · / · d · u · r · a · t · i · o · n · > · · · · < · / · p · a · r · t · > · · · < · / · p · a · r · t · l · i · s · t · > · · · XÈ_bGw; Ói ·
073b9c30 |]Gx! · · \I*i · à3 · °CVZ · · xT_ · · Õî · eÈ · ; · b · G · · t+ · ;#döAñ! · Å · Úét · 6á · i · \$të · · · ë · {E · ; · yv?
073b9c80 | · · _w · · · ^hö · · · · ðo · äyü · Ç8M¥ · ÙW · m · .c · · ûÝÁG · · 8û · · =à3;u · · Õ3ò · Ý · í<bmz · · (· uôÈjHåGD
073b9cd0 | ¶ · è · · i¾a · · ¶vG¾+ · k · · Õ · ÀÈ\$ · ÙÙ@Ya| · · Õ · > · ~ · 0 · g1 Ç · · ó · 0 · · · *Bo- \$ÙXÇ_ · àñü · · · · · ãÍýøåC~ · ·
073b9d20 | bR · WLð · · ;c · Ý(· 7i7; % · c · Md · p · :FF · }gÞå0AEIZQ · % · · m@Sof · Õ · · · 5E · pI · R4\$+g · · x%ä1Ya| · 6 ·
073b9d70 | WXK& · · n* · · D · ÀGÌcLb · Ñ · ôe · @ · ?ÙÇ_ · ðë: · ò · ?è · H · 7 · · L¥w\$" · i-N · · · 0ð\ · ¶B · d¥ZkwíöÈ · · Uë[· m2

Skype: durata chiamata

- Pattern trovato
 - *<part
identity="nomeChiamante"><name>nomeChiamante</
name><duration>durataInSecondi</duration></part>*
- Testo da ricercare
 - *part identity=*
 - *<duration>*
- Possibile espressione regolare
 - *<part identity=.*></part>*

Hotmail: password

0995e580	n·s·c·=·1·&·b·k·=·1·3·0·5·1·0·8·9·9·1·.....·h·t·t·p·s·:/·1·o·g·i·n..·l·i·v·e· 0995e5d0 .·c·o·m·/·p·p·s·e·c·u·r·e·/·p·o·s·t..·s·r·f·?·w·a·=·w·s·i·g·n·i·n·1..·0·&·r·p·s· 0995e620 n·v·=·1·1·&·c·t·=·1·3·0·5·1·0·9·0·0·7·&·r·v·e·r·=·6..·1..·6·2·0·6..·0·&·w·p·=·M· 0995e670 B·I·&·w·r·e·p·l·y·=·h·t·t·p·:/·%·2·F·%·2·F·m·a·i·l..·l·i·v·e..·c·o·m·%·2·F·d·e·f· 0995e6c0 a·u·l·t..·a·s·p·x·&·l·c·=·1·0·4·0·&·i·d·=·6·4·8·5·5·&·m·k·t·=·i·t--·i·t·&·c·b·c· 0995e710 x·t·=·m·a·i·&·s·n·s·c·=·1·&·b·k·=·1·3·0·5·1·0·8·9·9·1···ÿÿÿ·...·ÿÿÿÿÿÿÿ·..... 0995e760·n···h·t·t·p·s·:/·1·o·g·i·n..·l·i·v·e..·c·o·m·/·1·o·g·i·n· 0995e7b0 ..·s·r·f·?·w·a·=·w·s·i·g·n·i·n·1..·0·&·r·p·s·n·v·=·1·1·&·c·t·=·1·3·0·5·1·0·9·0·0· 0995e800 7·&·r·v·e·r·=·6..·1..·6·2·0·6..·0·&·w·p·=·M·B·I·&·w·r·e·p·l·y·=·h·t·t·p·:/·%·2·F· 0995e850 %·2·F·m·a·i·l..·l·i·v·e..·c·o·m·%·2·F·d·e·f·a·u·l·t..·a·s·p·x·&·l·c·=·1·0·4·0·&· 0995e8a0 i·d·=·6·4·8·5·5·&·m·k·t·=·i·t--·i·t·&·c·b·c·x·t·=·m·a·i·&·s·n·s·c·=·1·.....~..^ 0995e8f0 ý·..°·..^ý·.....·login=alicesicurezza%40hotmail.it&passwd=password 0995e940 d12345&type=11&LoginOptions=2&NewUser=1&MEST=&PPSX=PassportRN&PPFT=CS81ZLPZC3b7e 0995e990 ij1Qy97V3alRuN*XyZvPj1P8kZDDftB0Z4Rbsnevg*2I0vcWrSJ4oszG*PzcZU35qksU6RqqSBCZLaUJ 0995e9e0 SgHOTpMW%21BjYS7Hy7Mxg5shF3hwcvQGzRbxJm8soCn%21INVVB*5QTv9xCMSsWi3WBKDbDEK6%21S 0995ea30 nrakD1q0h8c*G4Thk*qzlB2W*P9MZXYTCY38Z%21bWSajs%21N2oNFra3&idsbho=1&PwdPad=&ss0=& 0995ea80 i1=&i2=1&i3=25170&i4=&i12=1 .. ;=bý·..B···a·p·p·l·i·c·a·t·i·o·n·/·x···w·w·w···f·o· 0995ead0 r·m···u·r·l·e·n·c·o·d·e·d···n···h·t·t·p·s·:/·1·o·g·i·n..·l·i·v·e..·c·o·m·/·1· 0995eb20 o·g·i·n..·s·r·f·?·w·a·=·w·s·i·g·n·i·n·1..·0·&·r·p·s·n·v·=·1·1·&·c·t·=·1·3·0·5·1· 0995eb70 0·9·0·0·7·&·r·v·e·r·=·6..·1..·6·2·0·6..·0·&·w·p·=·M·B·I·&·w·r·e·p·l·y·=·h·t·t·p·
----------	--

Hotmail: password

- Pattern trovato
 - login=loginUtente&passwd=password
- Testo da ricercare
 - login=
 - &passwd=
- Possibile espressione regolare
 - login=.*&passwd=.*

Hotmail: bozze

Odcb13a0
Odcb13f0
Odcb1440 h#
Odcb1490	Centro assistenzaCommenti e suggerimentiItaliano ..À...Á...À...À...À...È... ç...È...É...È...È...í... Windows Liveâ· Hotmail (6)MessengerOffi
Odcb14e0	ceFotoMSN à· Alice Sicurezza profilo disconnetti Hotmail Posta in arrivo (6)
Odcb1530	Cartelle Posta indesiderata Bozze (3) Posta inviata Posta eliminata Nuova cartel
Odcb15d0	la Categorie Contrassegnato Foto Documenti di Office Messenger Caricamento in co
Odcb1620	rso... Home page Contatti Calendario Nuovo Elimina Posta indesiderata Organizza
Odcb1670	à· Segna come à· Sposta in à· à· Opzioni à· Posta in arrivo Disponi per à
Odcb16c0	à· Mostra: Tutti Da leggere Da contatti Social network Da gruppi Tutti
Odcb1710	gli altri elementi À« Facebook Bob Sicurezza ha pubblicato qualcosa sulla tua B
Odcb1760	achecca.â· 05/05/2011 Facebook Torna su Facebookâ· 05/05/2011 Skype Benvenuto s
Odcb17b0	u Skypeâ· 05/05/2011 Facebook Bob Sicurezza ha accettato la tua richiesta di am
Odcb1800	icizia su Facebook...â· 05/05/2011 Facebook Benvenuti su Facebookâ· 05/05/2011
Odcb1850	Facebook Solo un altro passo per iniziare a usare Facebookâ· 05/05/2011 Team d
Odcb18a0	i Hotmail Introduzione a Windows Live Hotmailâ· 05/05/2011 Numero messaggi: 7 N
Odcb18f0	uovo Elimina Posta indesiderata Organizza à· Segna come à· Sposta in à· À®
Odcb1940	2011 MicrosoftCondizioniPrivacyInformazioni sugli annunci pubblicitariPubblicitÃ
Odcb1990	Centro assistenzaCommenti e suggerimentiItaliano ..HD.....ÈGù·aCommenti e sugg
Odcb19e0	erimentiItaliano,èE·ç·

Hotmail: bozze

- Pattern trovato
 - Cartella Posta indesiderata Bozze
 - **Pattern variabile**
- Testo da ricercare
 - Bozze
- Possibile espressione regolare
 - Bozze.*Posta inviata
 - **Pattern variabile**

Hotmail: bozze

0042c340 | d:Crm120x60_1;wt:120;ht:60;pg:WLMITC;hnegurl:http%3A%2F%2Fdu101w.dub101.mail.live.com%2FHandlers%2FAdservemsg.mvc%3Fhostdm%3Dlive.com;hstkn:pcNHiEeQTskyzizEu09kfw%3D%3D;adcctr:1F6-----http://imagesrv.adition.com/banners/200/652272/lafetrali.html·k5---W---http://js2.wlxrs.com/z0Y5z4E-Pw9vNv2ie7Ny3A/adloader.html#pgqp

0042c480 :%26PG%3DWLMIT8%26AP%3D1090%26PN%3DMSFT%26ID%3DC4344F76ABB12693FD9F9321FFFFFF%26MUID%3D92222F68E5174DB9ACE620A92D5A248F;divid:Ad160x600_0;wt:160;ht:600;pg:WLMIT8;hnegurl:http%3A%2F%2Fdu101w.dub101.mail.live.com%2FHandlers%2FAdservemsg.mvc%3Fhostdm%3Dlive.com;hstkn:pcNHiEeQTskyzizEu09kfw%3D%3D---4-----http://du101w.dub101.mail.live.com/mail/InboxLight.aspx?FolderID=00000000-0000-0000-0000-000000000004&fav=False&n=1578296223·C3---q·1http://du101w.dub101.mail.live.com/default.aspx?rru=inboxHotmail - alicesicurezza@hotmail.it - Windows LiveWindows Liveà·o Hotmail (6)MessengerOfficeFotoMSN à·ù Alice Sicurezza profilo | disconnetti Hotmail Posta in arrivo (6) Cartelle Posta indesiderata Bozze (3) Posta inviata Posta eliminata Nuova cartella Categorie Contrassegnato Foto Documenti di Office Messenger Caricamento in corso... Home page Contatti Calendario Nuovo Elimina Organizza à·ù Segna come à·ù Sposta in à·ù | à·ù Opzioni à·ù Bozze Disponi per à·ù Mostra: Tutti | Da leggere | Da contatti | Social network | Da gruppi | Tutti gli altri elementi Å« (sconosciuto) Prova Bozzaâ· 12.18 (sconosciuto) Oggetto di provaâ· 10/05/2011 (sconosciuto) Oggetto di provaâ· 10/05/2011 Numero messaggi: 3 Nuovo Elimina Organizza à·ù Segna come à·ù Sposta in à·ù | Å® 2011 MicrosoftCondizioniPrivacyInformazioni sugli annunci pubblicitariPubblicitÃ Centro assistenzaCommenti e suggerimentiItalianoc2---G---http://du101w.dub101.mail.live.com/handlers/resourcespreload.mvc?bicild=&view=Hotmail.Compose·x1---q---http://js2.wlxrs.com/z0Y5z4E-Pw9vNv2ie7Ny3A/adloader.html#pgqp:%26PG%3DWLMITC%26AP%3D1499%26SDN%3DWL4%26PN%3DMSFT%26ID%3DC4344F76ABB12693FD9F9321FFFFFF%26MUID%3D92222F68E5174

Hotmail: bozze

Hotmail: bozze

- Pattern trovato
 - <h2 class=ReadMsgSubject>oggettoDelMessaggio</h2>
 - Pattern dipendente dall'HTML
- Testo da ricercare
 - class=ReadMsgSubject>
- Possibile espressione regolare
 - class=ReadMsgSubject>

Hotmail: bozze

Hotmail: bozze

- Pattern trovato
 - Pattern dipendente dall'html
- Testo da ricercare
 - class=ReadMsgBody
- Possibile espressione regolare
 - class=ReadMsgBody

Gmail: account

```
2ff48b50 .....  
2ff48ba0 .....  
2ff48bf0 .....  
2ff48c40 .....  
2ff48c90 .....m-7-qy-https://mail.g  
2ff48ce0 oogle.com/mail/?hl=it&shva=1#composeGmail - Posta in arrivo (3) - alicesicurezza  
2ff48d30 @gmail.com:6-m-https://mail.google.com/mail/?hl=it&shva=1#inboxGmailB-5.....  
2ff48d80 https://mail.google.com/mail/?ui=2&view=bsp&ver=ohhl4rw8mbn4-4-3-https://ma  
2ff48dd0 il.google.com/mail/?ui=2&view=js&name=main,tlist&ver=YVTYHTYLT_U.it.&am!=1GS9IZn  
2ff48e20 spIa7Qv3hwtAogqz4DFIIkjyyjBR7VaT9W2NHUNnlXVO7HHkDS_y9&fri4-3-a-https://mail.go  
2ff48e70 ogle.com/mail/?hl=it&shva=1Gmailj-2-U-https://accounts.youtube.com/accounts/C  
2ff48ec0 heckConnection?pmmpo=https%3A%2F%2Fwww.google.com&v=1178808674-1-O-https://w  
2ff48f10 ww.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=  
2ff48f60 http%3A%2F%2Fmail.google.com%2Fmail%2F%3Fhl%3Dit%26ui%3Dhtml%26zy%3D1&bsv=1lyA69  
2ff48fb0 4le36z&scc=1&ltmpl=default&ltmplcache=2&hl=it&from=loginGmail: l'email di Google  
2ff49000 .....ý:....., ..I \ Ä ..ý 7 ..
```

Gmail: bozze

Gmail: bozze

- Pattern trovato
 - subject text4 oggettoDelMessaggio body textareaV messaggio
- Testo da ricercare
 - subject
- Possibile espressione regolare
 - subject.*body.*
 - Nessun delimitatore finale

Sommario

- Computer Forensics
 - Metodologie forensi
 - Live forensics
- Distribuzioni
 - DEFT
 - Helix
 - CAINE
- Analisi Forense dei dati volatili
 - Tipologie di dump
 - Dump tool
 - Process analysis tool
 - Clipboard tool
- Caso di studio
 - Ambiente di lavoro
 - Risultati
- Riferimenti

Riferimenti

- [1] «Wikipedia,» [Online]. Available: http://it.wikipedia.org/wiki/Informatica_forense.
- [2] M. Epifani, 2011. [Online]. Available: www.associazionearchimede.it/Unisa/phocadownload/ssi2011.pdf.
- [3] M. McDougal, «Live Forensics on Windows System using Windows Forensic Toolchest,» 2003-2006. [Online]. Available: http://www.foolmoon.net/downloads/Live_Forensics_Using_WFT.pdf.
- [4] S. R. Stefano Fratepietro, «DEFT Manuale d'uso,» 2011. [Online]. Available: [http://www.deftlinux.net/doc/\[it\]deft_manuale_full.pdf](http://www.deftlinux.net/doc/[it]deft_manuale_full.pdf).
- [5] AccessData, «Forensic ToolKit User Guide,» 22 Maggio 2008. [Online]. Available: http://accessdata.com/downloads/media/FTK_1.80_Manual.pdf.
- [6] M. Suiche, «Challenges of Windows physical memory acquisition and exploitation,» Giugno 2009. [Online]. Available: <http://shakacon.org/talks/NFI-Shakacon-win32dd0.3.pdf>.
- [7] R. Galati, «MSNP9, il protocollo di MSN,» 3 Gennaio 2008. [Online]. Available: <http://www.programmazione.it/index.php?entity=eitem&idItem=38198>.

[