DIGITAL FORENSICS

Corso di Sicurezza II

Dipartimento dI Informatica

Paolo Dal Checco

CHI SONO

- **Dottorato in Informatica**, gruppo di Sicurezza, @unito
- Per alcuni anni ricerca, poi **CTO** in ambito **crittografia**
- Ora **consulente Informatico Forense** per Procure, Tribunali, Aziende e Privati in ambito penale e civile
- Esperto di aspetti investigativi delle criptomonete, ransomware, computer/mobile/web/network forensics, perizie audio e video
- Tra i fondatori dell'Osservatorio Nazionale di Informatica Forense (**ONIF**), sviluppatore DEFT Linux fino al 2018
- Socio Tech & Law, Clusit, AIP, AssobIT
- paolo@dalchecco.it - @forensico
- dalchecco.it, bitcoinforensics.it, ransomware.it

PROGRAMMA 4 GIORNATA

- Ricostruzione delle attività tramite timeline e supertimeline
- Rilevamento di compromissioni
- Analisi delle periferiche USB utilizzate
- Analisi dei documenti aperti e utilizzati
- Estrazione di evidenze tramite Bulk Extractor e Autopsy
- Riepilogo degli argomenti
- Domande e Risposte

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

TIMELINE

- Una timeline è una rappresentazione di eventi ordinati cronologicamente
- Gli eventi possono provenire da un'unica fonte o da una più fonti
- Metodo rapido e intuitivo per rendersi conto di quanto è accaduto in un sistema in un determinato arco temporale

SUPER TIMELINE

- La super timeline si intende la creazione di un file in cui sono memorizzate su scala temporale analogamente a quanto descritto per la timeline tradizionale
- Consente di restituire in risultato molto più esaustivo ed accurato facendo uso dei metadati

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

USI DELLA TIMELINE E SUPER TIMELINE

- Ricostruire le attività di un utente
- Ricostruire le fasi di un attacco o l'analisi di un malware
- Individuare le cause di un incidente informatico
- Evidenziare incongruenze che siano sintomo di attività illecite o tentativi di occultamento tracce
- Per avere una rappresentazione lineare della creazione di file, chiavi di registro, installazione di servizi, ecc.

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

VERIFICA DELLE FONTI TEMPORALI

E' molto importante individuare la fonte dei riferimenti temporali:

- Locale (orologio CMOS)
    - La data locale è corretta?
- Esterna (NTP)
    - Configurazione Timezone
    - Frequenza di aggiornamento
    - Ultimo aggiornamento
- L'applicazione che ha registrato l'evento usa un timestamp particolare?

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

DOVE TROVIAMO I RIFERIMENTI TEMPORALI

- Nel filesystem guardando gli attributi MAC(B) di ogni file e cartella
- File di log e registro eventi del sistema operativo
- Registro di Windows
- Feature proprie del sistema operativo (Prefetch, Restore Points, Link, Cestino, thumbs.db, ShellBag, Volume Shadow Copy)
- Cronologia, Cache e Cookies dei browser
- Cache e database applicativi
- Metadati interni ai documenti (Office, Mail, dati EXIF, ecc.)
- Eventi temporali recuperabili tramite carving da aree deallocate, slack space, dump di memoria, partizioni di swap, file di ibernazione (record $MFT, chiavi di registro, chat, password)

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

MAC(B)

- In un filesystem gli attributi riguardano gli eventi:
  - **M**odified (modifica dei dati)
  - **A**ccessed (lettura dei dati)
  - **C**hanged (modifica dei metadati)
  - **B**irth (creazione del file)
- Non tutti i filesystem registrano le stesse informazioni
- Non tutti i sistemi operativi sfruttano le possibilità del filesystem

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

Significato degli attributi MAC(B) per i vari filesystem:

Tipo FS	Modified	Accessed	Changed	Birth
Ext2/3	Modified	Accessed	Changed	-
Ext4	Modified	Accessed	Changed	Created
FAT	Written	Accessed	N/A	Created
NTFS	File Modified	Accessed	MFT Modified	Created
HFS	Modified	Accessed	Changed	-

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

FILESYSEM E OS

- **FAT** registra gli attributi MAC in localtime
- **NTFS** registra 2 serie di attributi MACB in UTC
- In Windows l'aggiornamento dell'attributo **Access** è gestito tramite la chiave di registro:
    - **HKLM\SYSTEM\CurrentSet\Control\FileSystem\NtfsDisableLastAccessUpdate**

  Il valore **1**: aggiornamento del tempo di accesso è disattivato (default da Win Vista +)
  Il valore **0**: aggiornamento del tempo di accesso è attivato (default Win XP e prec.)
- Linux registra in **Unix time** (secondi trascorsi dal 1/1/1970 00:00:00 UTC) gli attributi MAC su Ext2/3. Con l'avvento di Ext4 viene introdotto l'attributo **Birth**
- In Linux l'aggiornamento degli attributi può essere inibito in fase di mount (**noatime**)
- HFS+ registra i secondi trascorsi da 1/1/1904 00:00:00 GMT

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

WINDOWS: ACCESS TIME DISABILITATO

Quando disabilitato, l'attributo di **Accesso**, viene solitamente

Condizione	Modified	Accessed	Changed
Rinomina file	Attrib. conservato	Attrib. conservato	Attrib. conservato
Spostamento file tra cartelle	Attrib. conservato	Attrib. conservato	Attrib. conservato
Spostamento di file tra partizioni o dischi	Attrib. conservato	Data spostamento	Attrib. conservato
Copia file	Attrib. conservato	Data copia	Data copia
Creazione nuovo file	Data creazione	Data creazione	Data creazione
Modifica file esistente	Data modifica	Attrib. conservato	Attrib. conservato
Accesso file esisitente	Attrib. conservato	Aggiornato entro un'ora se abilitato, altrimenti conservato	Attrib. conservato

Le regole sulla modifica o preservazione dei timestamp nel casi di copia e spostamento di file che risiedono su filesystem **FAT** e **NTFS** sono riportate alla seguente pagina web:

http://support.microsoft.com/kb/299648/en-us

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ATTENZIONE

Singole applicazioni possono adottare timestamp alternativi:

- Nel registro di Windows, i valori FILETIME riportano il numero di intervalli da 100 nanosecondi trascorsi dal 1/1/1601 00:00:00 UTC

- da Mac OS X v10 le applicazioni (es. Safari) possono usare il Mac Absolute Time, o CFDate: secondi trascorsi dal 1/1/2001 00:00:00 GMT

Pertanto è necessario verificare ogni fonte e uniformare tra loro i diversi timestamp

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

UNIFORMARE I TIMESTAMP

- Conversione del fuso orario
- Compensazione eventuali discrepanze temporali
- Normalizzazione del formato data-ora
- Ricorso a formati standardizzati:
  - Body file
  - TLN

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

INFORMAZIONI DAL REGISTRO

Prima di procedere con la creazione della (super)timeline possiamo estrarre alcune informazioni utili dal registro di sistema:

- Versione del sistema operativo
- Time zone

Per recuperare queste informazioni, dopo aver montato in R/O il disco, facciamo uso del tool registry ripper presente in DEFT:

```
# cd /opt/regripper
# rip -r /mnt/C/Windows/system32/config/software -p winver
# rip -r /mnt/C/Windows/system32/config/system -p timezone
```

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

STRUMENTI

- Useremo i tool fls/mactime della suite TSK, The Sleuth Kit e log2timeline.
- Esistono diverse alternative, più o meno scomode, open/gratuite/commerciali
- fls è la più usata, anche perchè utilizzata dal frontend Autopsy

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

STRUMENTI ALTERNATIVI MA SCOMODI

- FTK Imager (AccessData)
- NTFSwalk (TzWorks)
- AnalyzeMFT
- mft.pl
- MFTView
- Encase
- X-Ways Forensics

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE TIMELINE CON DAILY SUMMARY

- Suite TSK, con fls credo file in formato bodyfile
- Converto il bodyfile in CSV
- Creo daily summary con attività giornaliera

fls -o 63 -r -m C: /mnt/raw/image.dd > c-timeline.body

mactime -y -m -d -i day c-timeline-daily.csv -z Europe/Rome -b c-timeline.body > c-timeline.csv

oppure

mactime -y -m -d -i hour c-timeline-hourly.csv -z Europe/Rome -b c-timeline.body > c-timeline.csv

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE TIMELINE CON DAILY SUMMARY

- Il daily summary serve per rilevare anomalie sui giorni
- Nell'esempio, cominceremo ad esaminare il giorno 4 marzo 2010, dove rileviamo 62.239 movimentazioni di file
- Possibile anche hourly summary, con analisi oraria, nell'esempio rileviamo pesante attività tra le ore 11 e 12

```
Tue 03 02 2010, 6616
Wed 03 03 2010, 3990
Thu 03 04 2010, 62239
Fri 03 05 2010, 315
Sat 03 06 2010, 5
Sun 03 07 2010, 178
```

```
Wed 03 03 2010 17:00:00, 63
Wed 03 03 2010 18:00:00, 94
Thu 03 04 2010 01:00:00, 2
Thu 03 04 2010 02:00:00, 1
Thu 03 04 2010 09:00:00, 294
Thu 03 04 2010 10:00:00, 46
Thu 03 04 2010 11:00:00, 13874
Thu 03 04 2010 12:00:00, 44408
Thu 03 04 2010 13:00:00, 3478
Thu 03 04 2010 16:00:00, 3
Thu 03 04 2010 17:00:00, 98
Thu 03 04 2010 18:00:00, 1
Thu 03 04 2010 19:00:00, 2
Thu 03 04 2010 20:00:00, 3
Thu 03 04 2010 23:00:00, 29
Fri 03 05 2010 01:00:00, 6
Fri 03 05 2010 06:00:00, 1
Fri 03 05 2010 08:00:00, 10
```

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE TIMELINE CON DAILY SUMMARY

- Otteniamo (i dati provengono dall'$MFT) data di creazione/accesso/salvataggio/entry modified, dimensione, numero di inode e percorso sul filesystem quando disponibile
- Sappiamo se un file esisteva ma è stato cancellato e in tal caso anche se l'area disco è stata riscritta

```
2004 08 04 Wed 05:00:00,629,m..b,r/rrwxrwxrwx,0,0,1010-128-1,"C:/WINDOWS/inf/minioc.inf"
2004 08 04 Wed 05:00:00,1688,m...,r/rrwxrwxrwx,0,0,10109-128-3,"C:/WINDOWS/repair/autoexec.nt"
2004 08 04 Wed 05:00:00,673088,m..b,r/rrwxrwxrwx,0,0,1011-128-3,"C:/WINDOWS/system32/mlang.dat"
2004 08 04 Wed 05:00:00,3584,m..b,r/rrwxrwxrwx,0,0,1012-128-3,"C:/WINDOWS/system32/mll_hp.dll"
2004 08 04 Wed 05:00:00,7680,m..b,r/rrwxrwxrwx,0,0,1013-128-3,"C:/WINDOWS/system32/mll_mtf.dll"
2004 08 04 Wed 05:00:00,5632,m..b,r/rrwxrwxrwx,0,0,1014-128-3,"C:/WINDOWS/system32/mll_qic.dll"
2004 08 04 Wed 05:00:00,17135,m..b,r/rrwxrwxrwx,0,0,1015-128-3,"C:/WINDOWS/Help/mls_trb.chm"
2004 08 04 Wed 05:00:00,37298,m..b,r/rrwxrwxrwx,0,0,1016-128-3,"C:/WINDOWS/Help/mmc_dlg.hlp"
2004 08 04 Wed 05:00:00,1492,m..b,r/rrwxrwxrwx,0,0,1017-128-3,"C:/WINDOWS/system32/mmdriver.inf"
```

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

SE VOLESSIMO USARE L'INTERFACCIA GRAFICA?

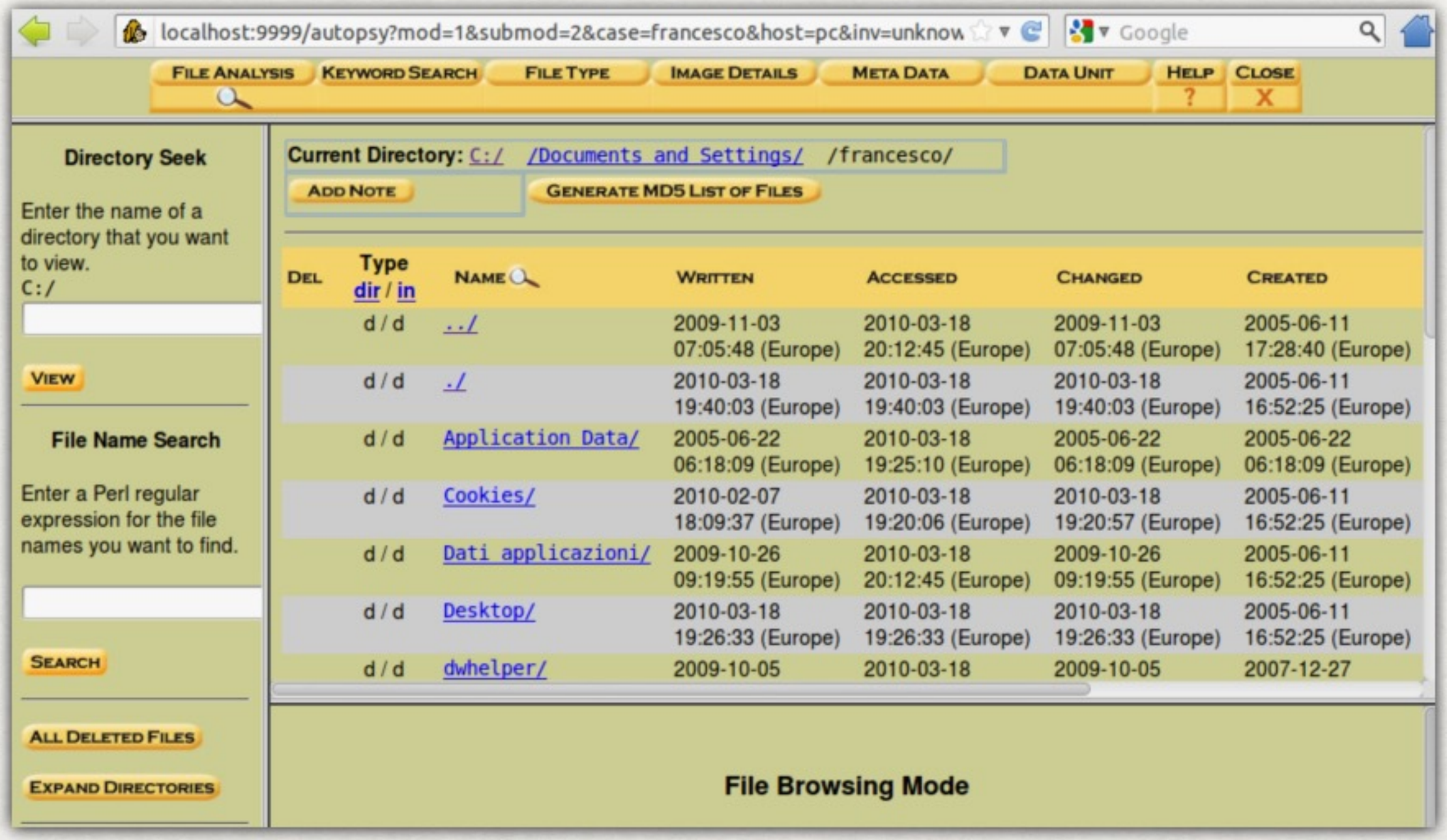
Possiamo usare Autopsy

`Menù > DEFT > Analysis Tools > Autopsy`

- Interfaccia grafica alla suite TSK
- Creo un caso, imposto timezone, inserisco immagini/dischi (/dev/sda)
- Utile per fare preview di file anche cancellati (ricavati da MFT table)
- Utile per fare keyword search su raw disk, estrazione stringhe, estrazione spazio non allocato, organizzazione file per tipo, ricupero di tutti i file cancellati (a livello MFT)
- Preview raw a livello di settore

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

TIMELINE CON AUTOPSY



RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE DI UNA SUPERTIMELINE

- Creando la STL aggiungiamo ai timestamp del filesystem anche i metadati contenuti nei file per creare la nostra linea temporale
- Utilizzeremo il tool open source **log2timeline**
  - Framework composto da 4 moduli: front-end, librerie condivise, modulo input e modulo output
  - Include diversi plugin

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE DI UNA SUPERTIMELINE: PLUGIN

- **altiris** Parse the content of an XeXAMInventory or AeXProcessList log file
- **analog_cache** Parse the content of an Analog cache file
- **apache2_access** Parse the content of a Apache2 access log file
- **apache2_error** Parse the content of a Apache2 error log file
- **chrome** Parse the content of a Chrome history file
- **encase_dirlisting** Parse the content of a CSV file that is exported from Encase (dirlist)
- **evt** Parse the content of a Windows 2k/XP/2k3 Event Log
- **evtx** Parse the content of a Windows Event Log File (EVTX)
- **exif** Extract metadata information from files using ExifTool
- **ff_bookmark** Parse the content of a Firefox bookmark file
- **ff_cache** Parse the content of a Firefox _CACHE_00[123]_ file
- **firefox2** Parse the content of a Firefox 2 browser history
- **firefox3** Parse the content of a Firefox 3 history file
- **ftk_dirlisting** Parse the content of a CSV file that is exported from FTK Imager (dirlist)
- **generic_linux** Parse content of Generic Linux logs that start with MMM DD HH:MM:SS

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE DI UNA SUPERTIMELINE: PLUGIN

- **iehistory** Parse the content of an index.dat file containg IE history
- **iis** Parse the content of a IIS W3C log file
- **ibsatxt** Parse the content of a ISA text export log file
- **jp_ntfs_change** Parse the content of a CSV output file from JP (NTFS Change log)
- **l2t_csv** Parse the content of a body file in the l2t CSV format
- **mactime** Parse the content of a body file in the mactime format
- **mcafee** Parse the content of log files from McAfee AV engine
- **mcafeefireup** Parse the content of an XeXAMInventory or AeXProcessList log file
- **mcafeehel** Parse the content of a McAfee HIPS event.log file
- **mcafeehs** Parse the content of a McAfee HIPShield log file
- **mft** Parse the content of a NTFS MFT file
- **mssql_errlog** Parse the content of an ERRORLOG file produced by MS SQL server
- **ntuser** Parse the NTUSER.DAT registry file
- **openvpn** Parse the content of an openVPN log file
- **opera** Parse the content of an Opera's global history file

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE DI UNA SUPERTIMELINE: PLUGIN

- **oxml** Parse the content of an OpenXML document (Office 2007 documents)
- **pcap** Parse the content of a PCAP file
- **pdf** Parse some of the available PDF document metadata
- **prefetch** Parse the content of the Prefetch directory
- **proftpd_xferlog** Parse the content of a ProFTPd xferlog log file
- **recycler** Parse the content of the recycle bin directory
- **restore** Parse the content of the restore point directory
- **safari** Parse the contents of a Safari History.plist file
- **sam** Parses the SAM registry file
- **security** Parses the SECURITY registry file
- **setupapi** Parse the content of the SetupAPI log file in Windows XP
- **skype_sql** Parse the content of a Skype database
- **software** Parse the SOFTWARE registry file
- **sol** Parse the content of a .sol (LSO) or a Flash cookie file

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE DI UNA SUPERTIMELINE: PLUGIN

- **squid** Parse the content of a Squid access log (http_emulate off)
- **symantec** Parse the content of a Symantec log file
- **syslog** Parse the content of a Linux Syslog log file
- **system** Parse the SYSTEM registry file
- **tln** Parse the content of a body file in the TLN format
- **volatility** Parse the content of a Volatility output files (psscan2, sockscan2, ...)
- **win_link** Parse the content of a Windows shortcut file (or a link file)
- **wmiprov** Parse the content of the wmiprov log file
- **xpfirewall** Parse the content of a XP Firewall log

Nuovi plugin o aggiornamenti vengono introdotti nelle più recenti release…

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE DI UNA SUPERTIMELINE: MODULI E LISTE

List Name	Modules Included
linux	apache2_access, apache2_error, pcap, syslog, generic_linux,
web	chrome, firefox3, firefox2, ff_bookmark, opera, iehistory, iis, safari,
webhist	chrome, firefox3, firefox2, ff_bookmark, opera, iehistory, iis, safari, sol,
win7	chrome, evt, exif, ff_bookmark, firefox3, iehistory, iis, mcafee, opera, oxml, pdf, prefetch, recycler, restore, sol, win_link, xpfirewall, wmiprov, ntuser, software, system,
win7_no_reg	chrome, evt, exif, ff_bookmark, firefox3, iehistory, iis, mcafee, opera, oxml, pdf, prefetch, recycler, restore, sol, ntuser, win_link, xpfirewall, wmiprov,
winvista	chrome, evt, exif, ff_bookmark, firefox3, iehistory, iis, mcafee, opera, oxml, pdf, prefetch, recycler, restore, sol, userassist, win_link, xpfirewall, wmiprov,
winxp	chrome, evt, exif, ff_bookmark, firefox3, iehistory, iis, mcafee, opera, oxml, pdf, prefetch, recycler, restore, setupapi, sol, win_link, xpfirewall, wmiprov, ntuser, software, system,
winxp_no_reg	chrome, evt, exif, ff_bookmark, firefox3, iehistory, iis, mcafee, opera, oxml, pdf, prefetch, recycler, restore, setupapi, sol, ntuser, win_link, xpfirewall, wmiprov,

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE DI UNA SUPERTIMELINE: OUTPUT

Name	Description
beedocs	tab-delimited file to import into BeeDocs
cef	ArcSight Commen Event Format (CEF)
cftl	Output timeline in a XML format that can be read by CFTL
csv	CSV (Comma Separated Value) file
mactime	mactime format
mactime_l	legacy version of the mactime format (version 1.x and 2.x)
simile	Output timeline in a XML format that can be read by a SIMILE widget
sqlite	Output timeline into a SQLite database
tab	TDV (Tab Delimited Value) file
tln	H. Carvey's TLN format
tlnx	H. Carvey's TLN format in XML

Useremo CSV perché veloce da gestire ed ideale per integrare le diverse fonti di dati/metadat

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE DI UNA SUPERTIMELINE

- Monto il disco in modalità read only come visto in precedenza

```
mount -o ro,loop,
show_sys_files,streams_interface=windows,
offset=$((512*63)) /mnt/image.dd /mnt/c
```

- Importanti i parametri speciali per file di sistema e ADS:
  - show_sys_files
  - streams_interface=windows
- Il valore 63 relativo all'offset indica il settore di partenza della partizione da montare

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE DI UNA SUPERTIMELINE

- Possibile operare anche su dischi fisici **(prendendo le dovute precauzioni)**
- Si possono montare tutti i tipi di immagini usati nella computer forensics o i dischi tramite i seguenti tool:
  - affuse (raw, split raw)
  - xmount (raw, split raw, aff, ewf)
  - mount [-o loop] (raw)
  - ewfmount [ewf]

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE DI UNA SUPERTIMELINE: FILE PARTICOLARI

- Si notano alcuni file di metadati NTFS ($Boot, $MFTMirr, ecc.)
- Alcuni metafile non si vedono ma si possono accedere direttamente ($MFT, $UsnJrnl:$J) e potranno servirci

```
deft ~ % mount -o ro,show_sys_files,streams_interface=windows /dev/sda1 /mnt/c
deft ~ % ls -al /mnt/c
totale 853110
drwxrwxrwx 1 root root      8192 2010-03-18 17:45 .
drwxr-xr-x 3 root root        60 2012-03-20 23:11 ..
drwxrwxrwx 1 root root     16384 2009-08-08 01:12 4928cbe0584148074357
-rwxrwxrwx 1 root root      2560 2005-06-11 18:23 $AttrDef
-rwxrwxrwx 1 root root         0 2005-06-11 16:46 AUTOEXEC.BAT
-rwxrwxrwx 1 root root         0 2005-06-11 18:23 $BadClus
-rwxrwxrwx 1 root root    435512 2005-06-11 18:23 $Bitmap
-rwxrwxrwx 1 root root      8192 2005-06-11 18:23 $Boot
-rwxrwxrwx 1 root root      4952 2001-08-31 11:00 Bootfont.bin
-rwxrwxrwx 1 root root       211 2005-06-11 17:28 boot.ini
```

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE DI UNA SUPERTIMELINE

- A volte utile usare parametri “-p” e “-f winxp”
- l2t_process può filtrare per keyword (blacklist/whitelist), timestamping (MFT con millisecondi a 0), date o evidenziare scostamenti time/number MFT tramite scatter plot della cartella /windows/system32

```
log2timeline -r -z Europe/Rome /mnt/c/ -m C: -w c-log2t.csv

cat c-log2t.csv > supertimeline-unsorted.csv
l2t_process -i -b supertimeline-unsorted.csv -y > supertimeline.csv
```

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ESPORTO $MFT PER L'ANALISI LABORATORIO

- Utile se non si ha tempo di fare timeline/supertimeline
- log2timeline lo elabora in automatico
- Si può elaborare in laboratorio con diversi tool, compreso log2timeline
- Se non si ha tempo di usare fls/autopsy, acquisire MFT e parsificare in laboratorio

```
cat -c /mnt/c/\$MFT > mft.bin
(oppure)
icat -o 63 /dev/sda 0 > mft.bin
```

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ESPORTAZIONE DEL JOURNAL NTFS

- Se il journaling è attivo, il file contiene timestamp di creazione, modifica e cancellazione dei file presenti sul disco
- Si può elaborare in laboratorio con diversi tool, commerciali e non e integrare tramite apposito plugin nella super timeline

```
cat /mnt/c/\$Extend/\$UsnJrnl:\$J > usnjrnl.bin
```

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

INTEGRAZIONE DI FILE RECUPERATI NELLA SUPERTIMELINE

- Prassi poco nota ma dagli ottimi risultati
- Estrarre tramite carving e applicare log2timeline su quanto ricuperato
- Verranno parsificati registro, eventi, immagini, documenti, link, navigazione Internet e molti altri metadati che altrimenti non sarebbero stati inclusi nella supertimeline

```
log2timeline -r -z Europe/Rome ./carving -m C: -w c-log2t-
carve.csv
cat *.csv > supertimeline-unsorted.csv
l2t_process -i -b supertimeline-unsorted.csv -y >
supertimeline.csv
```

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ESEMPIO: NAVIGAZIONE WEB

- 10/20/2014,15:42:24,PST8PDT,.ACB,WEBHIST,**Internet Explorer**,time1,Administrator,-,visited http://www.google.com/search?hl=en&**q=pidgin**&aq=f [...]

- 10/20/2014,15:42:55,PST8PDT,M...,WEBHIST,**Internet Explorer**,time2,Administrator,-,visited http://sourceforge.net/project/downloading.php?groupname=pidgin&filename=**pidgin-2.5.2.exe**&use_mirror=internap [...]

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ESEMPIO: FILESYSTEM

- 10/21/2014,11:13:04,PST8PDT,.A..,FILE,NTFS $MFT,$FN [.**A**..] time,-,-,C:/Documents and Settings/All Users/Documents/**pidgin-2.5.2.exe** [...]

- 10/21/2014,11:04:08,PST8PDT,.A..,FILE,NTFS $MFT,$FN [.**A**..] time,-,-,C:/Documents and Settings/All Users/Documents/**Thunderbird Setup 2.0.0.17.exe** [...]

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ESEMPIO: ESECUZIONE PROGRAMMI

- 10/29/2014,19:44:34,,MACB,REG,UserAssist key,Time of Launch,domex2,REALISTIC_XP,UEME_RUNPATH:C:/Program Files/Mozilla Thunderbird/**thunderbird.exe**, [**Count: 2**] [...]

- 10/30/2014,00:50:43,PST8PDT,MACB,PRE,XP Prefetch,Last run,-,REALISTIC_XP,AIM6.EXE-34DC5725.pf: AIM6.EXE was executed,**AIM6.EXE-34DC5725.pf** - [AIM6.EXE] was executed - run **count [5]** [...]

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ESEMPIO: AVVIO E SPEGNIMENTO PC

- 10/29/2014,19:44:34,,MACB,REG,UserAssist key,Time of Launch,domex2,REALISTIC_XP,UEME_RUNPATH:C:/Program Files/Mozilla Thunderbird/**thunderbird.exe**, [**Count: 2**] [...]

- 10/30/2014,00:50:43,PST8PDT,MACB,PRE,XP Prefetch,Last run,-,REALISTIC_XP,AIM6.EXE-34DC5725.pf: AIM6.EXE was executed,**AIM6.EXE-34DC5725.pf** - [AIM6.EXE] was executed - run **count [5]** [...]

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ESEMPIO: AVVIO E SPEGNIMENTO PC

```
03/16/2010,07:42:40,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FRAPC,EventLo
g/6009;Info;5.01. - 2600 - Service Pack 3 - Uniprocessor Free,EventLog/6009;Info;5.01. -
2600 - Service Pack 3 - Uniprocessor Free,2,/mnt/c/WINDOWS/system32/config//SysEvent.Evt,
3266,URL: http://eventid.net/display.asp?eventid=6009&source=EventLog,Log2t::input::evt,u
id: unknown size: 524288
03/16/2010,07:42:40,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FRAPC,EventLo
g/6005;Info;,EventLog/6005;Info;,2,/mnt/c/WINDOWS/system32/config//SysEvent.Evt,3266,URL:
 http://eventid.net/display.asp?eventid=6005&source=EventLog,Log2t::input::evt,uid: unkno
wn size: 524288
03/16/2010,10:55:43,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FRAPC,EventLo
g/6006;Info;,EventLog/6006;Info;,2,/mnt/c/WINDOWS/system32/config//SysEvent.Evt,3266,URL:
 http://eventid.net/display.asp?eventid=6006&source=EventLog,Log2t::input::evt,uid: unkno
wn size: 524288
03/16/2010,10:56:53,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FRAPC,EventLo
g/6009;Info;5.01. - 2600 - Service Pack 3 - Uniprocessor Free,EventLog/6009;Info;5.01. -
2600 - Service Pack 3 - Uniprocessor Free,2,/mnt/c/WINDOWS/system32/config//SysEvent.Evt,
3266,URL: http://eventid.net/display.asp?eventid=6009&source=EventLog,Log2t::input::evt,u
id: unknown size: 524288
03/16/2010,10:56:53,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FRAPC,EventLo
g/6005;Info;,EventLog/6005;Info;,2,/mnt/c/WINDOWS/system32/config//SysEvent.Evt,3266,URL:
 http://eventid.net/display.asp?eventid=6005&source=EventLog,Log2t::input::evt,uid: unkno
wn size: 524288
03/16/2010,11:54:36,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FRAPC,EventLo
g/6005;Info;,EventLog/6005;Info;,2,/mnt/c/WINDOWS/system32/config//SysEvent.Evt,3266,URL:
 http://eventid.net/display.asp?eventid=6005&source=EventLog,Log2t::input::evt,uid: unkno
wn size: 524288
```

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ELABORAZIONE TIMELINE SUPER TIMELINE

Una volta creata la (super)timeline, per visionarla, filtrarla o fare ricerche, si consiglia l'uso di un foglio di calcolo o eventualmente un DBMS

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

POSSIBILI PROBLEMATICHE

- Programmi che eseguono scansioni di file (antivirus, antispyware), software di indicizzazione, deframmentazione, ecc. spesso alterano la data di accesso, rendendo l'informazione poco significativa

- Alcuni antivirus ci vengono incontro a tal proposito (es. “Preserve Filetime" in Norton Anti Virus Corporate)

RILEVAMENTO DI COMPROMISSIONI

Per verificare se un sistema è stato compromesso o se c'è stato un utilizzo non autorizzato, possiamo effettuare questi controlli:

- Creazione (super)timeline
- Registro di sistema
    - Verifica orari accensione/spegnimento del sistema
    - Verifica dei file recenti (recents su filesystem o da registro)
        - Verifica file recenti all'interno delle varie applicazioni
        - Verifica connessione dispositivi USB
        - Verifica comandi eseguiti
- Verifica processi attivi
- Registro eventi
- …

RILEVAMENTO DI COMPROMISSIONI

Una vasta serie di informazioni la possiamo estrarre dal registro di Windows utilizzando **regripper**. Regripper funziona sia in ambiente Linux ma è possibile eseguirlo anche da Windows.

E' un programma che funziona tramite l'ausilio di plugin e di conseguenza le sue potenzialità sono espandibili.

I file di registro che andremo a leggere si trovano in:

- /Users/NOME-Utente/**NTUSER.DAT**
- /Windows/System32/config/**SOFTWARE**
- /Windows/System32/config/**SAM**
- /Windows/System32/config/**SECURITY**
- /Windows/System32/config/**SYSTEM**

RILEVAMENTO DI COMPROMISSIONI

I plugin di regripper sono contenuti all'interno della cartella **plugins** di regripper ed essendo in formato testuale, possono essere letti per avere una descrizione sul plugin e soprattutto per comprendere quale chiave di registro utilizzare come file di input.

ANALISI DELLE PERIFERICHE USB UTILIZZATE

Il collegamento di periferiche USB viene tracciato nel registro di sistema di Windows, pertanto estraiamo tali informazioni tramite regripper:

- **# rip -r /mnt/c/Windows/system32/config/system -p usbstor2**

- PC-402,Disk&Ven_&Prod_USB_DISK&Rev_1.04,**0738015025AC&0**,1127776426,USB DISK USB Device,7&2713a8a1&0,\DosDevices\H:

Dove i vari paramentri sono:

- Nome del sistema
- ID classe dispositivo
- Numero di serie
- Ultima scrittura nel registro (inserimento usb), 'normalizzato' in Unix time
- Nome dispositivo
- ID dispositivo
- Lettera dell'unità

ANALISI DEI DOCUMENTI APERTI E UTILIZZATI

- Per effettuare un controllo sui file aperti di recente, oltre a fare riferimento alle informazioni presenti nel registro di sistema, è possibile analizzare i file nella cartella dei dati recenti.

- Tale cartella contiene dei link ai documenti recenti pertanto utilizzando il software **lnkinfo** (link info), possiamo ottenere informazioni dettagliate relative a quel link.

- Tra queste informazioni ricordiamo:

- Data di creazione

- Data apertura

- Percorso sorgente

ESTRAZIONE DI EVIDENZE TRAMITE BULK EXTRACTOR E AUTOPSY

BULK EXTRACTOR

Bulk Extractor è un software scritto da Simson Garfinkel l'autore di AffLib

- Parsifica il disco a livello raw estraendo:
  - numeri di carte di credito
  - indirizzi
  - telefoni
  - email
  - url
  - ricerche su Google
  - indirizzi IP
  - zip file
  - ecc.

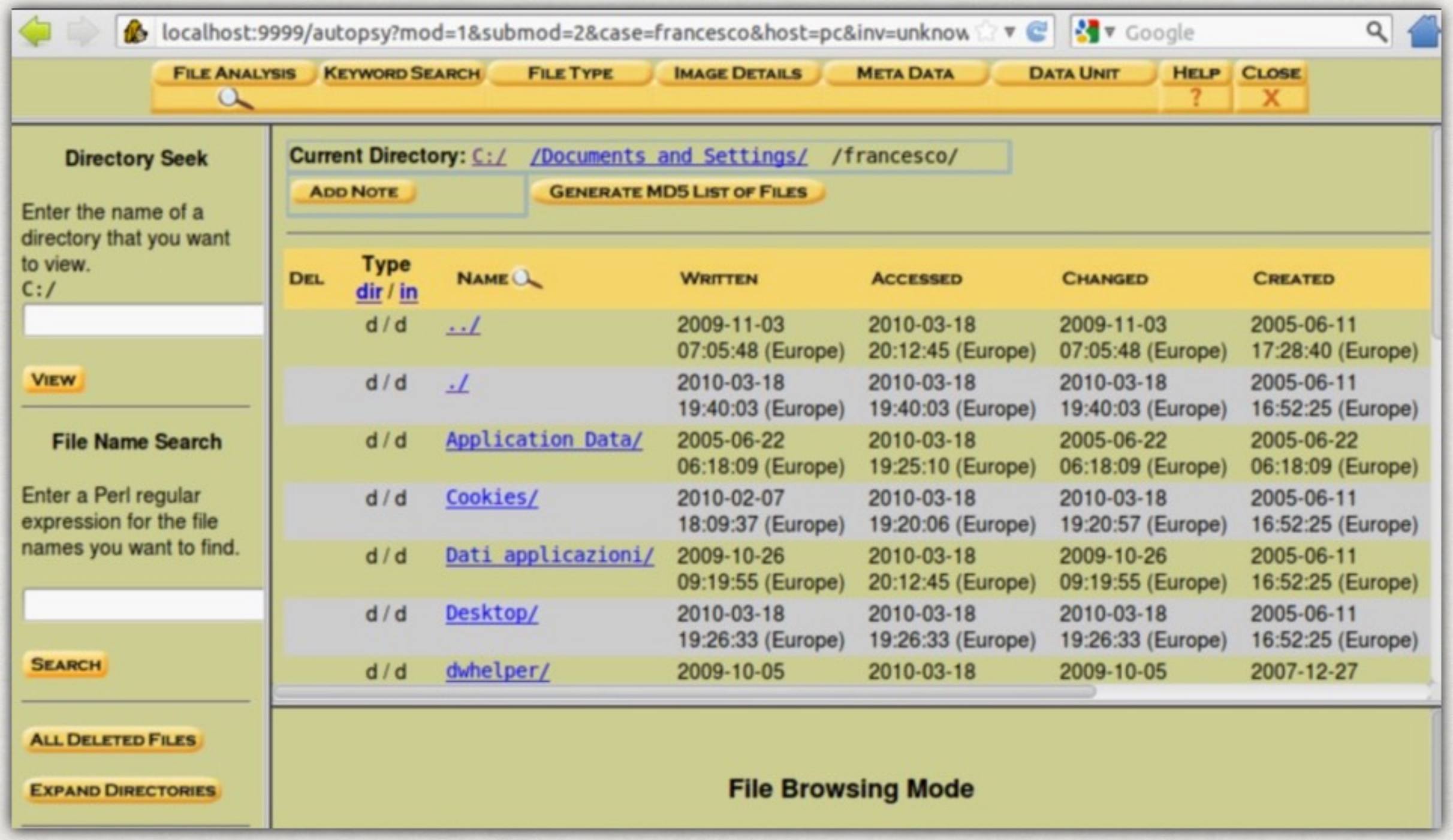
ESTRAZIONE DI EVIDENZE TRAMITE BULK EXTRACTOR E AUTOPSY

AUTOPSY

- Interfaccia grafica alla suite TSK
- Possiamo creare un caso, impostare una timezone, inserire immagini forensi e/o dischi (es. /dev/sda)
- Utile per fare preview di file anche cancellati (ricavati da MFT)
- Utile per fare ricerca di parole chiavi su raw disk, estrazione stringhe, estrazione dello spazio non allocato, organizzazione file per tipo, ricupero di tutti i file cancellati (a livello MFT)
- Preview raw a livello di settore

ESTRAZIONE DI EVIDENZE TRAMITE BULK EXTRACTOR E AUTOPSY

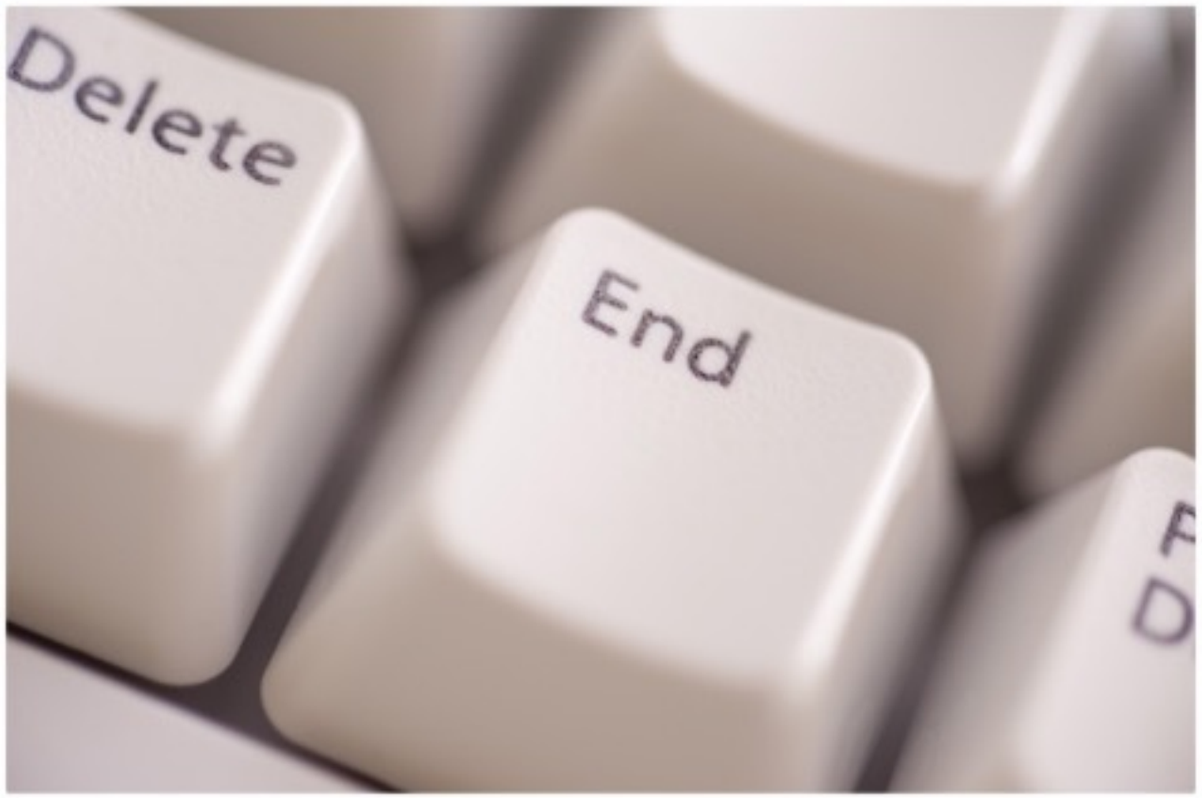
AUTOPSY



RIEPILOGO DEGLI ARGOMENTI

DOMANDE E RISPOSTE

GRAZIE PER L'ATTENZIONE



LABORATORIO