Sleuth kit & Autopsy

Un’alternativa open source per l’analisi dei filesystem

OSD Udine 2014 - Luigi Ranzato luigi.ranzato@gmail.com

Sleuth Kit e Autopsy

- Sleuthkit – deriva da TCT (The coroner's toolkit 2000)
- Set di tool da linea di comando per l'analisi di raw images e memorie contenenti file systems
- E' strutturato a livelli (file system, metadati, filename …)
- Autopsy - Interfaccia Grafica (WEB) per i tool TSK
- Autopsy 3.X – Front end Windows
- Creato da Brian Carrier (www.sleuthkit.org)
- IBM Public Licence, Common Public License

SleuthKit e Autopsy

- Adatto per immagini raw .DD, .E01 e AFF contenenti file systems

Testato su:

- Linux
- Mac OS X
- Windows
- CYGWIN
- Open & FreeBSD
- Solaris

Supporta i seguenti file systems:

- NTFS
- FAT
- UFS 1, UFS 2
- EXT2FS, EXT3FS, Ext4
- HFS
- ISO 9660
- YAFFS2

Sleuth Kit e Autopsy

Index of /sleuthkit/man

Name	Last modified	Size	Description
Parent Directory		-	
blkcalc.html	03-Nov-2014 09:20	3.6K	
blkcat.html	03-Nov-2014 09:20	3.9K	
blkls.html	03-Nov-2014 09:20	3.3K	
blkstat.html	03-Nov-2014 09:20	2.5K	
fcat.html	03-Nov-2014 09:20	2.9K	
ffind.html	03-Nov-2014 09:20	3.1K	
fls.html	03-Nov-2014 09:20	5.6K	
fsstat.html	03-Nov-2014 09:20	2.8K	
hfind.html	03-Nov-2014 09:20	7.0K	
icat.html	03-Nov-2014 09:20	3.2K	
ifind.html	03-Nov-2014 09:20	3.7K	
ils.html	03-Nov-2014 09:20	5.8K	
img_cat.html	03-Nov-2014 09:20	2.4K	
img_stat.html	03-Nov-2014 09:20	2.2K	
istat.html	03-Nov-2014 09:20	3.0K	
jcat.html	03-Nov-2014 09:20	2.8K	
jls.html	03-Nov-2014 09:20	2.4K	
mactime.html	03-Nov-2014 09:20	3.9K	
mmcat.html	03-Nov-2014 09:20	2.6K	
mmls.html	03-Nov-2014 09:20	4.4K	
mmstat.html	03-Nov-2014 09:20	2.5K	
sigfind.html	03-Nov-2014 09:20	2.3K	
sorter.html	03-Nov-2014 09:20	15K	
tsk_comparedir.html	03-Nov-2014 09:20	3.0K	
tsk_gettimes.html	03-Nov-2014 09:20	3.2K	
tsk_loaddb.html	03-Nov-2014 09:20	3.0K	
tsk_recover.html	03-Nov-2014 09:20	3.1K	

www.sleuthkit.org/sleuthkit/man

SleuthKit e Autopsy –- Comandi

File system layer tools

- `fsstat` – Restituisce informazioni sul volume - partizione

File name layer tools

- `ffind` – Restituisce il path del file indicato in un inode
- `fls` – Restituisce l'elenco dei file allocati o cancellati, e non solo

http://www.forensicswiki.org/

SleuthKit e Autopsy – IV - Comandi

Meta data tools

- `icat` – Estrae un file a partire dal suo inode
- `ifind` – Restituisce l'inode passandogli l'offset di un cluster
- `ils` – Restituisce l'elenco degli inode separati da una pipe |
- `istat` – Restituisce i metadati relativi a un certo inode

Volume system tools

- `mmls` – Restituisce informazioni sul partizionamento
- `mmstat` – Restituisce informazioni sul volume
- `mmcat` – Estrae il contenuto di un volume specificato

http://www.forensicswiki.org/

SleuthKit e Autopsy – V - Comandi

- Data unit layer tools
  - `blkcat` – Estrae contenuti da uno specifico volume
  - `blkls` – Estrae lo spazio non allocato da uno specifico volume
  - `blkstat` – Mostra i dettagli relativi a uno specifico volume
  - `blkcalc` – Calcola dove si trova un determinato cluster in uno spazio non allocato
- File System Journal Tools
  - `jcat –` Restituisce il contenuto di uno specifico journal block.
  - `jls` – Mostra la lista delle entries del file system journal.

http://www.forensicswiki.org/

SleuthKit e Autopsy – VI - Comandi

- Automated tools
  - `tsk_comparedir` - Comparatore di directory
  - `tsk_gettimes` - Estrae metadati temporali per la creazione di timeline
  - `tsk_loaddb` - Carica i metadati di una raw image in un DB SQLite
  - `tsk_recover` - Estrae contenuti allocati o non, da un raw disk in una directory locale

SleuthKit – test di utilizzo

- mmls

```
luigi-virtual-machine ../luigi/Desktop/6-11-14 % mmls 06.E01
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000000   0000002047   0000002048   Unallocated
02:  00:00   0000002048   0000206847   0000204800   NTFS (0x07)
03:  00:01   0000206848   0125204479   0124997632   NTFS (0x07)
04:  -----   0125204480   0125206527   0000002048   Unallocated
```

SleuthKit – test di utilizzo

fsstat

#fsstat –i ewf –o 206848 06.E01

```
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: 44D2FC32D2FC29B6
OEM Name: NTFS
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
First Cluster of MFT: 786432
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 146944
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 15624702
Total Sector Range: 0 - 124997630
```

SleuthKit – test di utilizzo

- fls

#fls –r –p -o 206848 -u –i ewf 06.E01 > allocatedfile.txt

#fls –r –p -o 206848 -d -i ewf 06.E01 > deletedfile.txt

SleuthKit – test di utilizzo

FLS e le TimeLine

#fls –r -o 206848 -z gmt-s 0 -m C: -f ntfs 06.E01 > timeline.bodyfile

```
0|C:/($FILE_NAME)|273-48-2|d/d-wx-wx-wx|0|0|104|1413217603|1413217603|1413217603|1413217603
0|C:/($FILE_NAME)|273-144-6|d/d-wx-wx-wx|0|0|192|1415220618|1415220618|1415220618|1247541608
0|C:/($FILE_NAME)|312-48-2|d/drwxrwxrwx|0|0|106|1413217603|1413217603|1413217603|1413217603
0|C:/($FILE_NAME)|312-144-1|d/drwxrwxrwx|0|0|256|1247549558|1247549558|1413218447|1247549558
0|C:/($FILE_NAME)|313-48-2|d/drwxrwxrwx|0|0|84|1413217603|1413217603|1413217603|1413217603
```

#mactime –b timeline.bodyfile -z gmt -d > timeline.csv

```
Wed Nov 05 2014 21:50:59,22528,..cb,r/rrwxrwxrwx,0,0,1458-128-1,"C:/Users/misterx/Desktop/Altri file/12345678910.doc”
Wed Nov 05 2014 21:50:59,96,macb,r/rrwxrwxrwx,0,0,1458-48-2,"C:/Users/misterx/Desktop/Altri file/12345678910.doc ($FILE_NAME)”
Wed Nov 05 2014 21:55:29,1,.acb,r/rrwxrwxrwx,0,0,1223-128-1,"C:/Users/misterx/Desktop/Altri file/known good or bad.txt”
Wed Nov 05 2014 21:55:29,108,macb,r/rrwxrwxrwx,0,0,1223-48-2,"C:/Users/misterx/Desktop/Altri file/known good or bad.txt ($FILE_NAME)”
Wed Nov 05 2014 21:57:38,82,macb,r/rrwxrwxrwx,0,0,1579-48-2,"C:/Users/misterx/Desktop/Altri file/Help.pdf ($FILE_NAME)”
Wed Nov 05 2014 22:02:41,22528,.ac.,r/rrwxrwxrwx,0,0,15775-128-1,"C:/Users/misterx/Desktop/Altri file/Catch me.doc”
Wed Nov 05 2014 22:02:41,90,macb,r/rrwxrwxrwx,0,0,15775-48-2,"C:/Users/misterx/Desktop/Altri file/Catch me.doc ($FILE_NAME)"
```

SleuthKit – test di utilizzo – Estrazione indici $i30

09 000009.jpg	21 novembre 2014 14:09
10 000008.jpg	21 novembre 2014 14:09
31 000004.jpg	21 novembre 2014 14:09
32 000004.jpg	21 novembre 2014 14:09

Nome di File che non esiste nella directory, ma rimasto nell'indice

istat –o 2048 pendrive.E01 43

icat –o 2048 pendrive.E01 43-160-5 | xxd | less

```
0002870: 0d01 3100 3400 2000 3000 3000 3000 3000  ..1.4. .0.0.0.0.
0002880: 3100 3300 2e00 6a00 7000 6700 0000 0000  1.3...j.p.g.....
0002890: 3800 0000 0000 0300 7000 5a00 0000 0000  8.......p.Z.....
00028a0: 2b00 0000 0000 0300 1bbf ef65 ef08 d001  +..........e....
00028b0: 17cd cd57 8c05 d001 e28e 813a f008 d001  ...W.......:....
00028c0: 1bbf ef65 ef08 d001 0020 0000 0000 0000  ...e..... ......
00028d0: 5416 0000 0000 0000 2000 0000 0000 0000  T.......  .......
```

https://github.com/williballenthin/INDXParse

SleuthKit – test di utilizzo – Individuazione NTFS Change Journal (USN)

fls -o 206848 06.E01 11

```
luigi-virtual-machine ../luigi/Desktop/6-11-14 % fls -o 206848 06.E01 11
r/r 25-144-5:    $ObjId:$O
r/r 24-144-3:    $Quota:$O
r/r 24-144-2:    $Quota:$Q
r/r 26-144-5:    $Reparse:$R
d/d 27-144-2:    $RmMetadata
r/r 57607-128-3:         $UsnJrnl:$J
r/r 57607-128-5:         $UsnJrnl:$Max
```

SleuthKit – test di utilizzo – Estrazione USN Journal - $J

istat -o 206848 06.E01 57607

```
Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-1)   Name: N/A   Resident   size: 82
Type: $DATA (128-3)   Name: $J   Non-Resident, Sparse   size: 365351632  init
_size: 365351632
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
```

icat -o 206848 06.E01 57607-128-3 > exported-usn-journal.jrnl

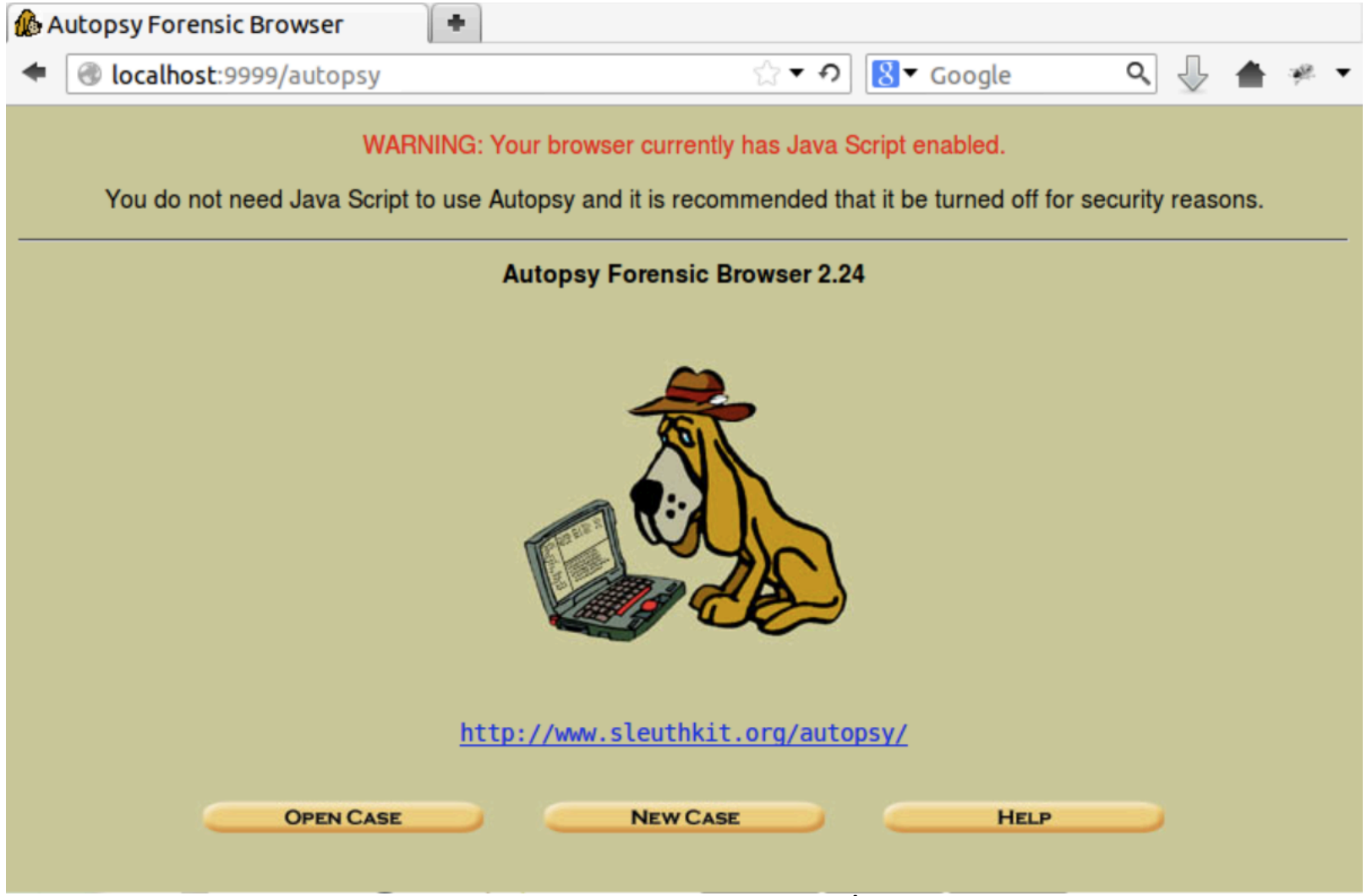
Parser USN Journal in Python

http://www.propheciesintothepast.name/2014/03/10/usnjrnlj/

https://code.google.com/p/parser-usnjrnl/downloads/list

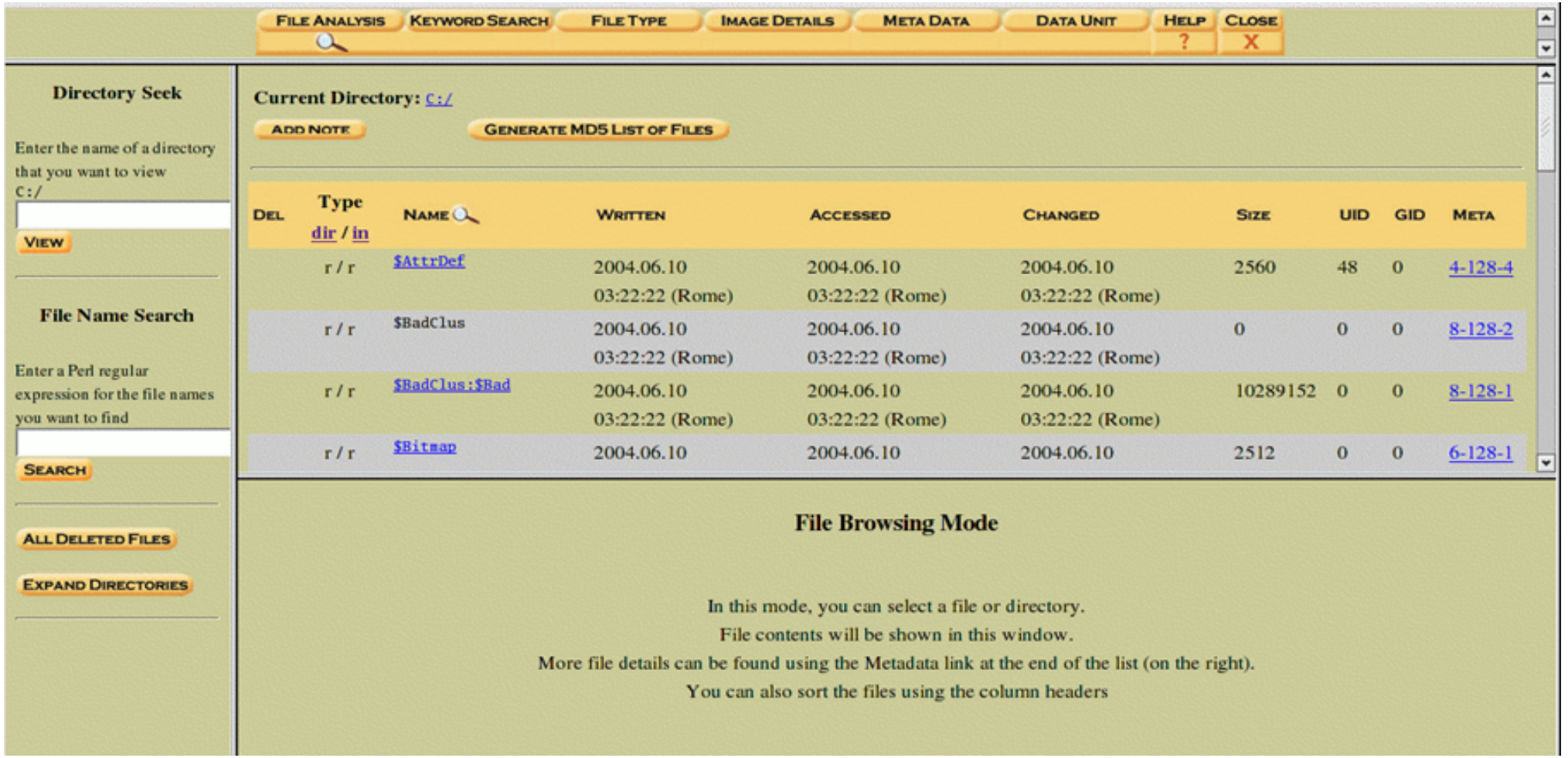
SleuthKit e Autopsy - I

Autopsy – Interfaccia WEB



SleuthKit e Autopsy - I

Autopsy – Interfaccia WEB – File analysis



SleuthKit e Autopsy

Autopsy – Interfaccia WEB – Key word Search

Keyword Search of Allocated and Unallocated Space

Enter the keyword string or expression to search for:

Unicode

grep Regular Expression

SEARCH

EXRACT UNALLOCATED

xpression Cheat Sheet

search runs grep on the image.
at will not be found is available here.

Extract Strings of Entire Volume

Extracting the ASCII and Unicode strings from a file system will make keyword searching faster.

Generate MD5?

ASCII: Unicode:

EXTRACT STRINGS

Extract Unallocated Clusters

Extracting the unallocated data in a file system allows more focused keyword searches and data recovery.

(Note: This Does Not Include Slack Space)
Generate MD5?

EXRACT UNALLOCATED

SleuthKit e Autopsy

Autopsy – Interfaccia WEB – Sorted file by type

Sort Files by Type

View Sorted Files

- /root/evidence/test1/host1/images/8-jpeg-search.dd

Files (45)

Files Skipped (11)

- Non-Files (11)
- Reallocated Name Files (0)
- 'ignore' category (0)

Extensions

- Extension Mismatches (5)

Categories (34)

- archive (2)
- audio (0)
- compress (1)
- crypto (0)
- data (13)
- disk (1)
- documents (1)

SleuthKit e Autopsy

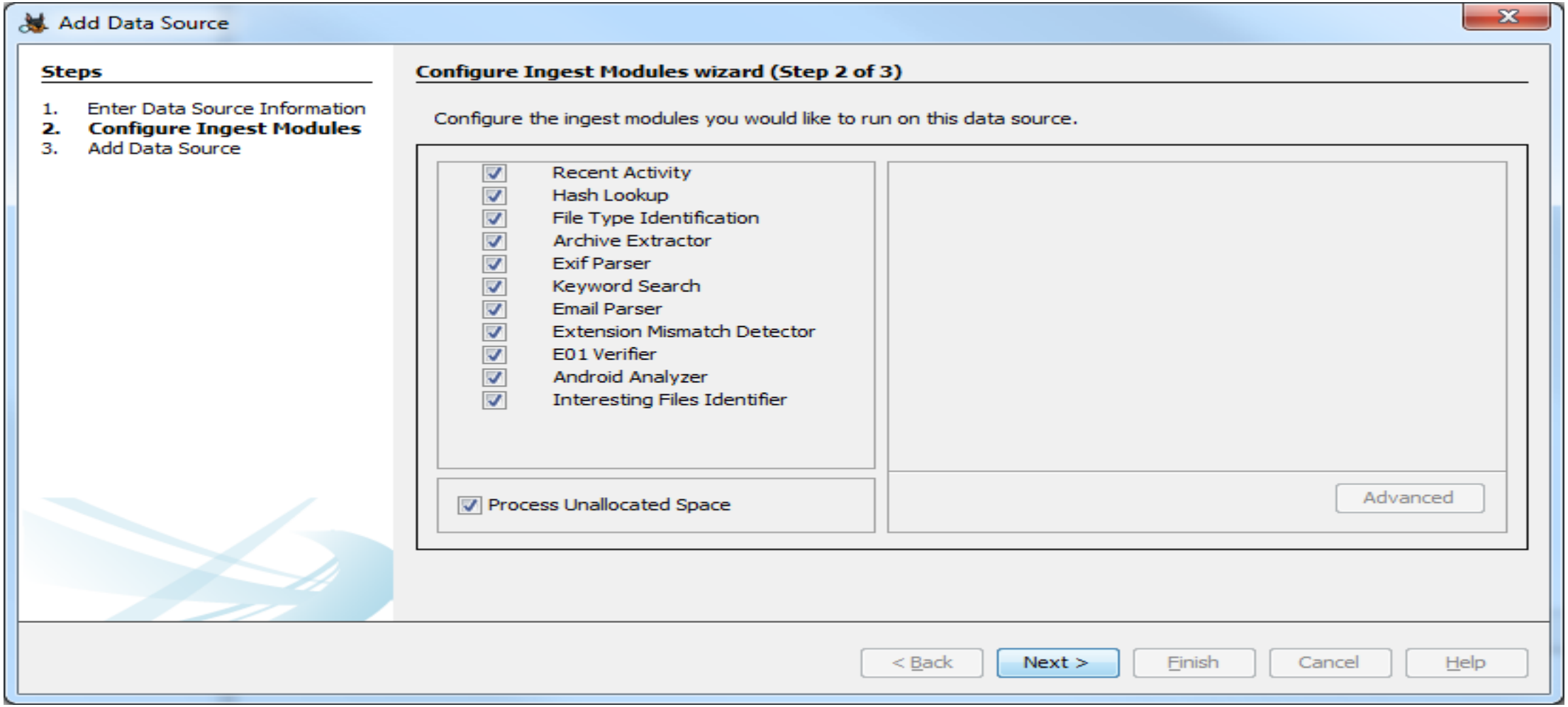
Autopsy 3.x per Windows

- Lo sviluppo inizia nel 2010 e a settembre 2012 viene rilasciata la versione 3.0.0
- Sovvenzionato in parte da US Army
- Implementati automatismi che si possono trovare in applicazioni commerciali di ottimo livello

- E' un'applicazione versatile ed estensibile con appositi plugin
- Interfaccia utente estremamente semplice da utilizzare ed intuitiva
- I risultati post elaborazione vengono istantaneamente messi a disposizione dell'utilizzatore / analista
- Completamente gratuito

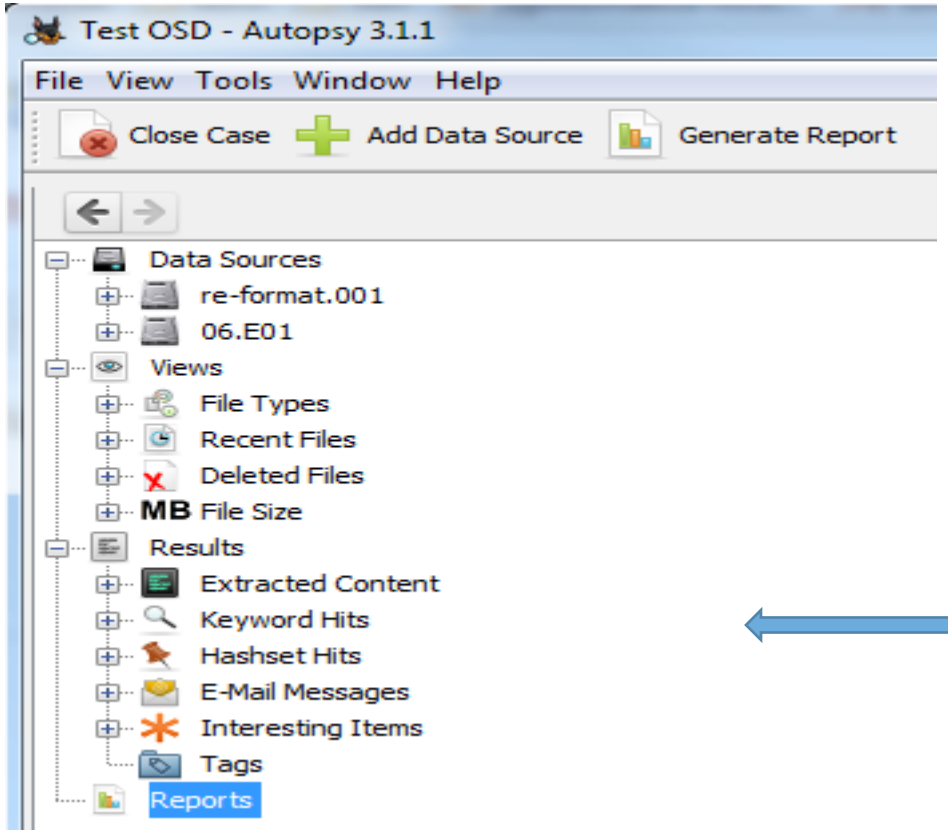
SleuthKit e Autopsy

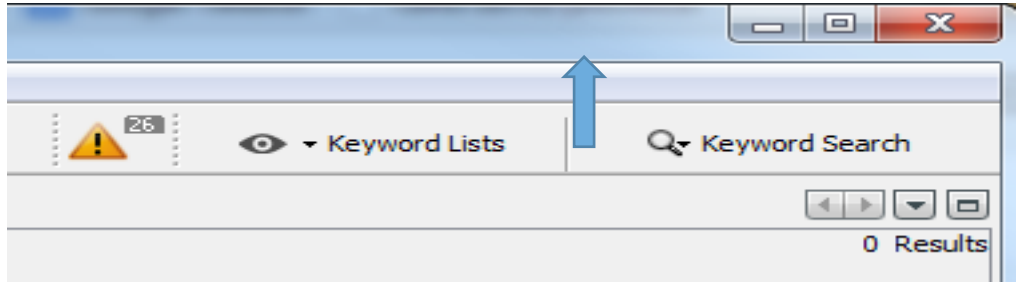
Autopsy 3.x per Windows



SleuthKit e Autopsy

Autopsy 3.x per Windows

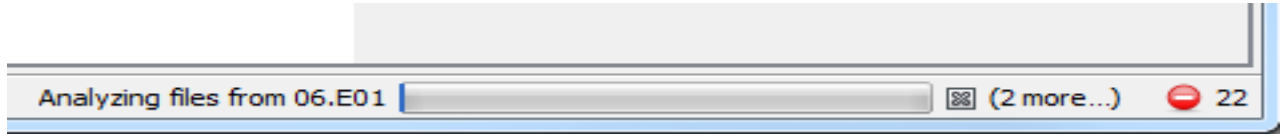




Ricerche veloci per keyword all'interno del caso

Raggruppamento delle informazioni estratte per tipologia

Barra di avanzamento per la verifica delle operazioni in corso



SleuthKit e Autopsy

Autopsy 3.x per Windows

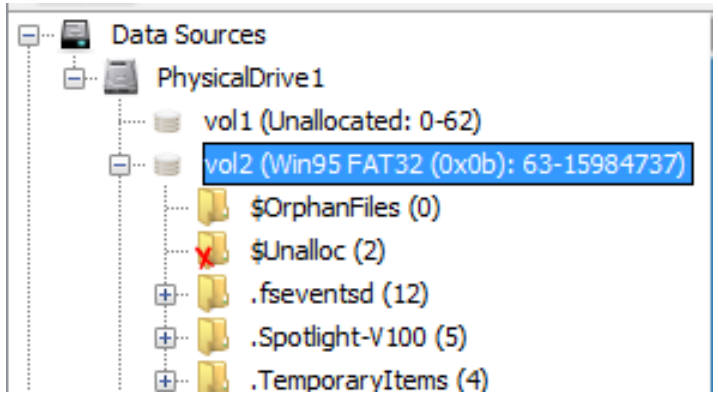
Attività eseguite automaticamente al caricamento della evidence

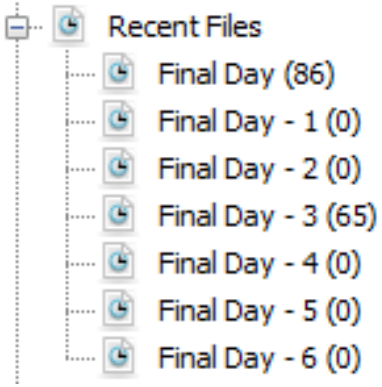
- Calcolo Hash
- Verifica hash rispetto a un database Known Good or Bad
- Estrazione exif dalle immagini
- Creazione di un indice di testo per la ricerca di keyword
- Estrazione di archivi compressi
- Analisi delle navigazioni internet
- Analisi del registro di windows (by regripper!)
- Analisi del contenuto di MBOX Thunderbird

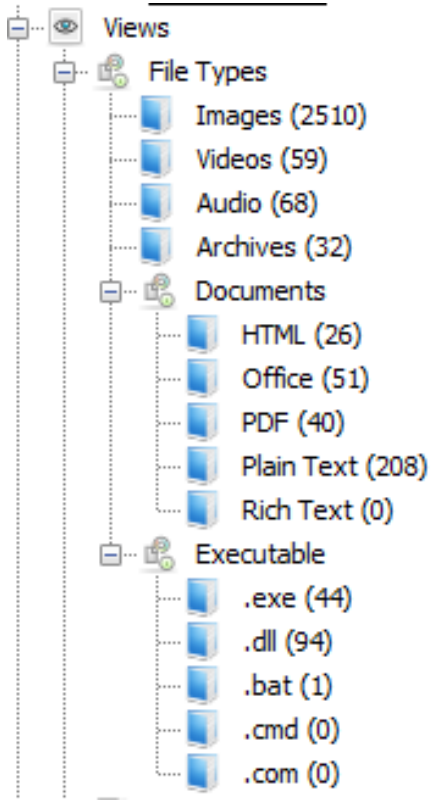
- Possibilità di aggiungere moduli ad hoc per analisi personalizzate …

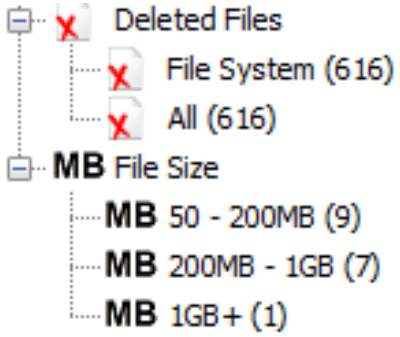
SleuthKit e Autopsy

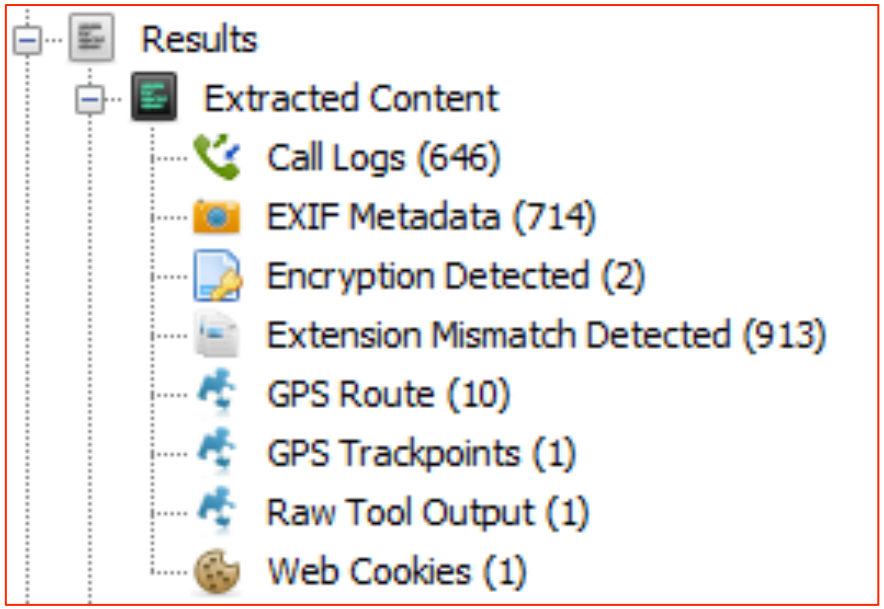
Output Autopsy 3.1.1 per Windows











SleuthKit e Autopsy

Autopsy 3.x per Windows

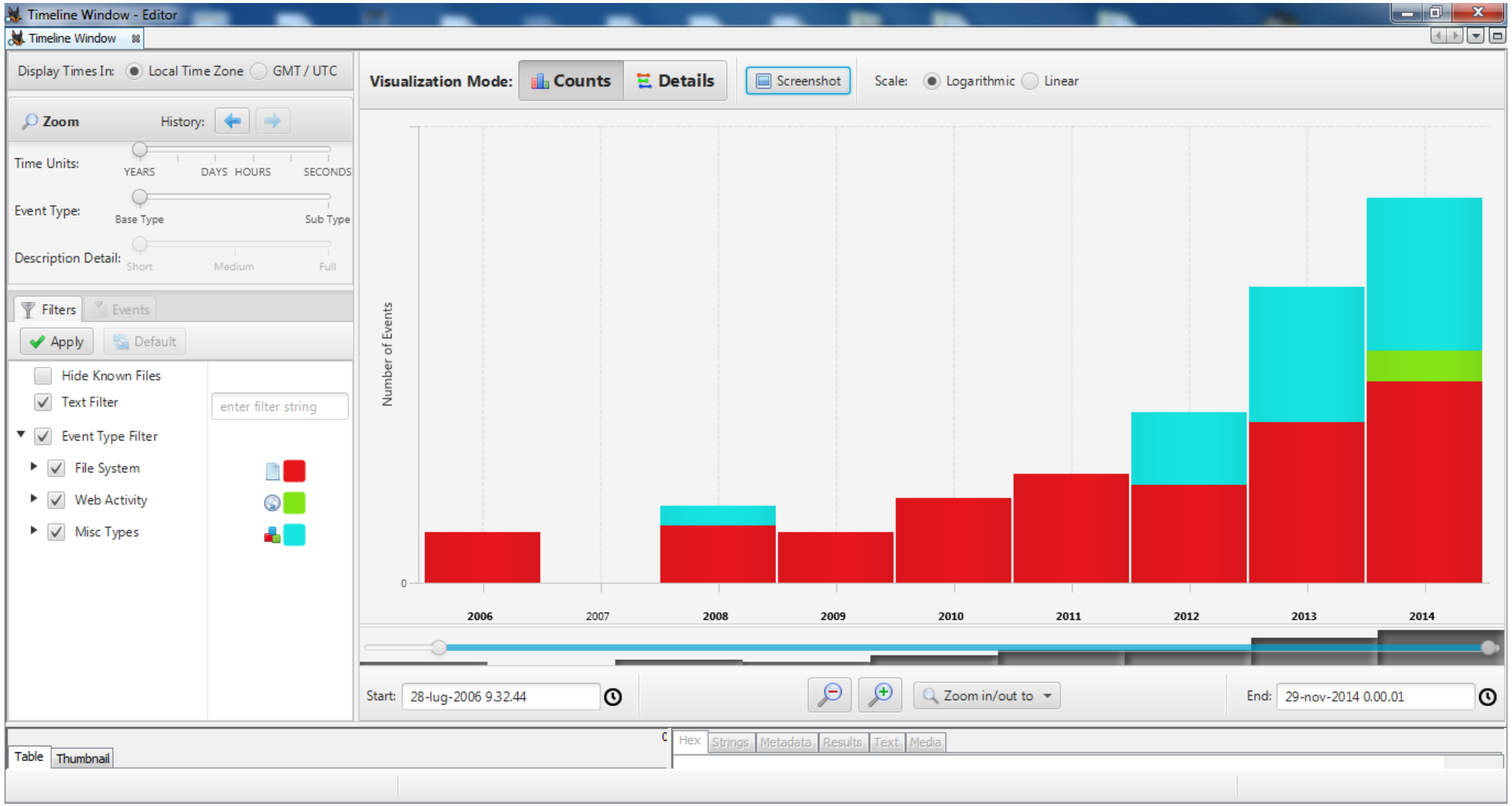
Previsione per prossime future attività di analisi automatiche

- P2P e altri formati aggiuntivi
- Antivirus, Malware
- Volume Shadow copy e Journal di sistema
- Detection di crittografia e steganografia
- Picture analysis (skin tone e object identification)

- La modularità dello strumento non pone limiti alla sua espandibilità

SleuthKit e Autopsy

Autopsy 3.1.1 per Windows - Modulo per le Time Line



SleuthKit e Autopsy

Autopsy 3.x per Windows

moduli già disponibili per il download

http://wiki.sleuthkit.org/index.php?title=Autopsy_3rd_Party_Modules

- sdhash (Autopsy AHBM) – Fuzzy HASH
- SmutDetect Module
- Windows Registry Ingest Module (di Willi Ballenthin)
- Child Exploitation Hashset Modules (database ProjectVic e C4All)
- Video Triage
- Windows Registry Content Viewer
- Multi Content Viewer (visualizzatore per numerosissimi formati)

Sleuth kit & Autopsy

Grazie