Digital forensics con open source e freeware

Di
Nanni Bassetti

https://nannibassetti.com

CHI SONO

- Mi occupo di digital forensics (informatica forense) dal 2005/2006, project manager di **CAINE** (distro usata in tutto il mondo)

- Fondatore di **CFI** (Computer Forensics Italy)
- Scrittore di parecchi articoli scientifici e software free/open source per la D.F.
- Membro fondatore e **Segretario di ONIF** (Osservatorio Nazionale Informatica Forense).
- Coinvolto in casi di rilevanza nazionale come:

- * Consulente tecnico informatico di parte civile nel caso del transessuale "Brenda" (caso Brenda-Marrazzo).
- * Consulente tecnico informatico di parte civile nel caso della scomparsa di Roberto Straccia
- * Consulente tecnico informatico di parte civile nel caso della scomparsa della piccola Angela Celentano
- * Consulente di parte per Massimo Bossetti nel caso di Yara Gambirasio.
- Ecc. ecc. :)

CHI SONO

CASI “MEDIATICI”

E TANTA FORMAZIONE

CHI SONO

2005/2006

primi vagiti online sulla computer forensics

2007

Tanti articoli dal 2007 ad oggi

2008

Creazione di CFI e pubblicazione di SFDumper

2009 - 2014

Classificato nella DC3 Challenge

2009

Alcuni miei scripts per la forensics

2009

Sviluppo CAINE Gnu/Linux

2013

Nel comitato di redazione di S&G

2015

Segretario e membro fondatore ONIF

Introduzione

Ormai nel panorama dei tool (software) di digital forensics, campeggiano molti strumenti commerciali veramente efficienti e comodi, ma spesso anche costosi.
Tra hardware e software si può creare un laboratorio forense per le fasi d'acquisizione ed analisi di tutto rispetto e con la comodità ed efficienza fornita dalla facilità d'uso dei suddetti tool commerciali.
In queste slide mostrarò un piccolo percorso d'acquisizione ed analisi effettuato tutto con strumenti FLOSS (Free Libre Open Source Software), su sistemi operativi Gnu/Linux e Windows, sicuramente non sarà comodo come premere un unico tasto, ma forse più affascinante e più "intimo" con l'informatica ed I dati.
Iniziamo con la fase d'acquisizione.

Acquisizione

- Acquisizione:

CAINE

1) Guymager
2) dd o dc3dd:

```
sudo dc3dd if=/dev/sda of=/media/sdb1 hash=md5,sha256
log=/media/sdb1/mylog.txt
```

3) Via rete:

```
dd if=/dev/sdb BS=1M conv=sync,noerror | netcat 192.168.1.105 2000
```

sul target:

```
netcat -l -p 2000 | dd of=/home/caine/disk1.dd
```

OS: CAINE (gnu/linux), Windows
Strumenti: fdisk, mounter, Guymager, FTK Imager

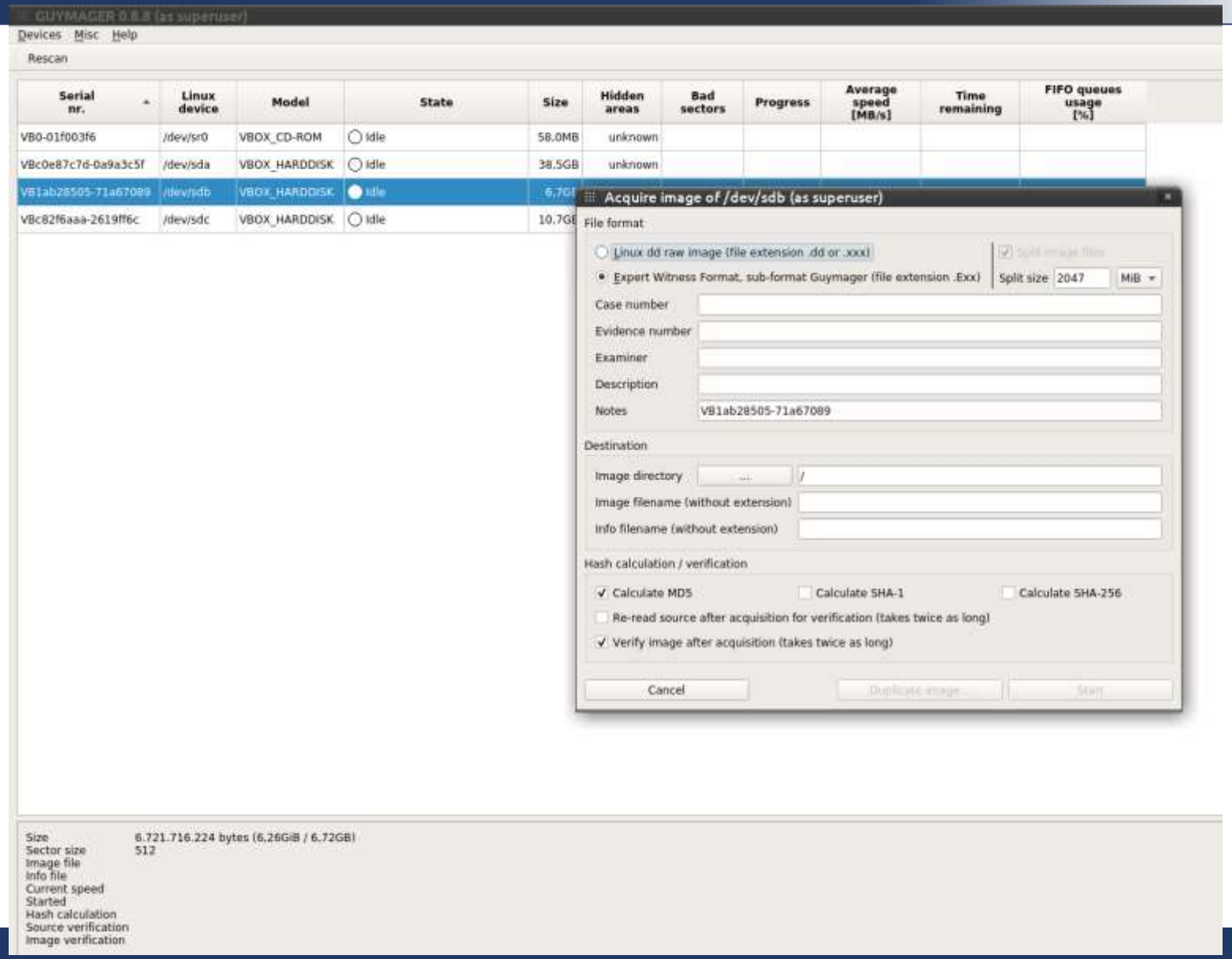
Colleghiamo il disco sorgente ad un computer sul quale vi è installato CAINE oppure effettuiamo il boot con la live distro sulla macchina contenente il disco da acquisire.

Tramite **fdisk -lu** oppure tramite il click sull'applicazione "**mounter**", individuiamo il disco sorgente, es. /dev/sdb ed il disco destinazione, dove andremo a scrivere il file immagine, es. /dev/sdc, infine montiamo in scrittura il disco destinazione e non facciamo niente sul disco sorgente.

Adesso lanciamo **GuyMager** per effettuare la copia forense, scegliendo gli algoritmi di hash ed il formato d'uscita, raw (dd) o EWF (Exper Witness Format), il primo è una copia bit a bit senza compressione, il secondo formato effettua una compressione e fa risparmiare spazio sul disco destinazione.

- Acquisizione:

GUYMAGER



- ANALISI

Recupero file cancellati:

1) XALL

2) Data Carving

ANALISI

OS: Caine
Strumenti: TSK, XALL, Photorec, XMOUNT.

Controllo delle PARTIZIONI

Utilizziamo lo strumento **MMLS** dello Sleuthkit, il disco è così partizionato:

$ **mmls MDT1D25xxx.dd**
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

	Slot	Start	End	Length	Description
000:	Meta	0000000000	0000000000	0000000001	Primary Table (#0)
001:	-------	0000000000	0000000062	0000000063	Unallocated
002:	000:000	0000000063	0000240974	0000240912	Dell Utilities FAT (0xde)
003:	-------	0000240975	0000241663	0000000689	Unallocated
004:	000:001	0000**241664**	**0006533119**	0006291456	NTFS / exFAT (0x07)
005:	000:002	000**6533120**	**0975697919**	0969164800	NTFS / exFAT (0x07)
006:	-------	0975697920	0975699967	0000002048	Unallocated

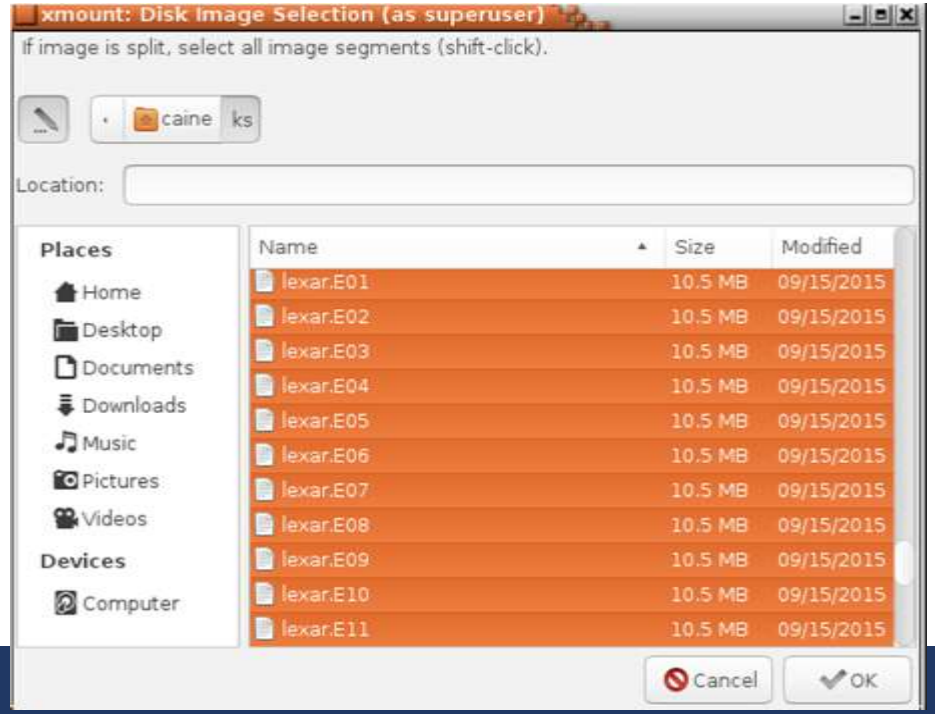
Tramite **XALL**, presente nella distribuzione Gnu/Linux CAINE 8.0 e scaricabile da:
https://github.com/nannib, possiamo decidere se estrarre dal file immagine i file allocati, quelli cancellati, fare il data carving ed estrarre lo slackspace, il risultato finale sarà una directory contenente i file che abbiamo deciso di estrarre, raggruppati nelle sotto-directory Allocati, Cancellati, Freespace e Slackspace.
XALL è un bash script che sfrutta: **TSK** (The SleuthKit), **Photorec**.

Data carving

Photorec (data carving) solo su freespace (spazio non allocato) lavora sul file immagine in formato RAW (dd), che possiamo ottenere tramite XMOUNT dal file EWF originale.

photorec lexar.dd

Possiamo personalizzare la ricerca selezionando solo di lavorare sul freespace ed eliminati i formati che potrebbero non interessarci come per esempio gli .exe, le dll, ecc.. Infine scegliamo anche su quali partizioni agire.



SHADOWS COPIES

OS: Linux, Windows
Strumenti: VSHADOWINFO, VSHADOWMOUNT, ARSENAL IMAGE MOUNTER, ShadowCopyView

In alcuni sistemi Windows può essere importante dare un'occhiata alle shadows copies, vediamo come poterle consultare in ambiente Gnu/Linux:

Scegliamo la partizione da esaminare e utilizziamo **VSHADOWINFO** e **VSHADOWMOUNT**:

vshadowinfo -o $((6533120*512)) MDT1D25xxx.dd

Estrazione dei VSS in formato raw

sudo vshadowmount -o $((6533120*512)) MDT1D25xxx.dd /media/sdb1/5-DISCOC

Questo genera un file binario chiamato VSS1, che possiamo montare come un normale dispositivo a blocchi:

sudo losetup -f /media/sdb1/5-discoc/vss1
sudo mount -o ro /dev/loop1 /tmp/5/vss1

Se invece si vuole utilizzare Windows, possiamo lanciare **ARSENAL IMAGE MOUNTER** per montare le partizioni presenti nel file immagine e **ShadowCopyView** della Nirsoft per consultarle ed esportare alcuni dati.

ANALISI

- ANALISI

Ricerca stringhe:

1) Grep –iaob file.xxx "stringa"

2) Bulkextractor

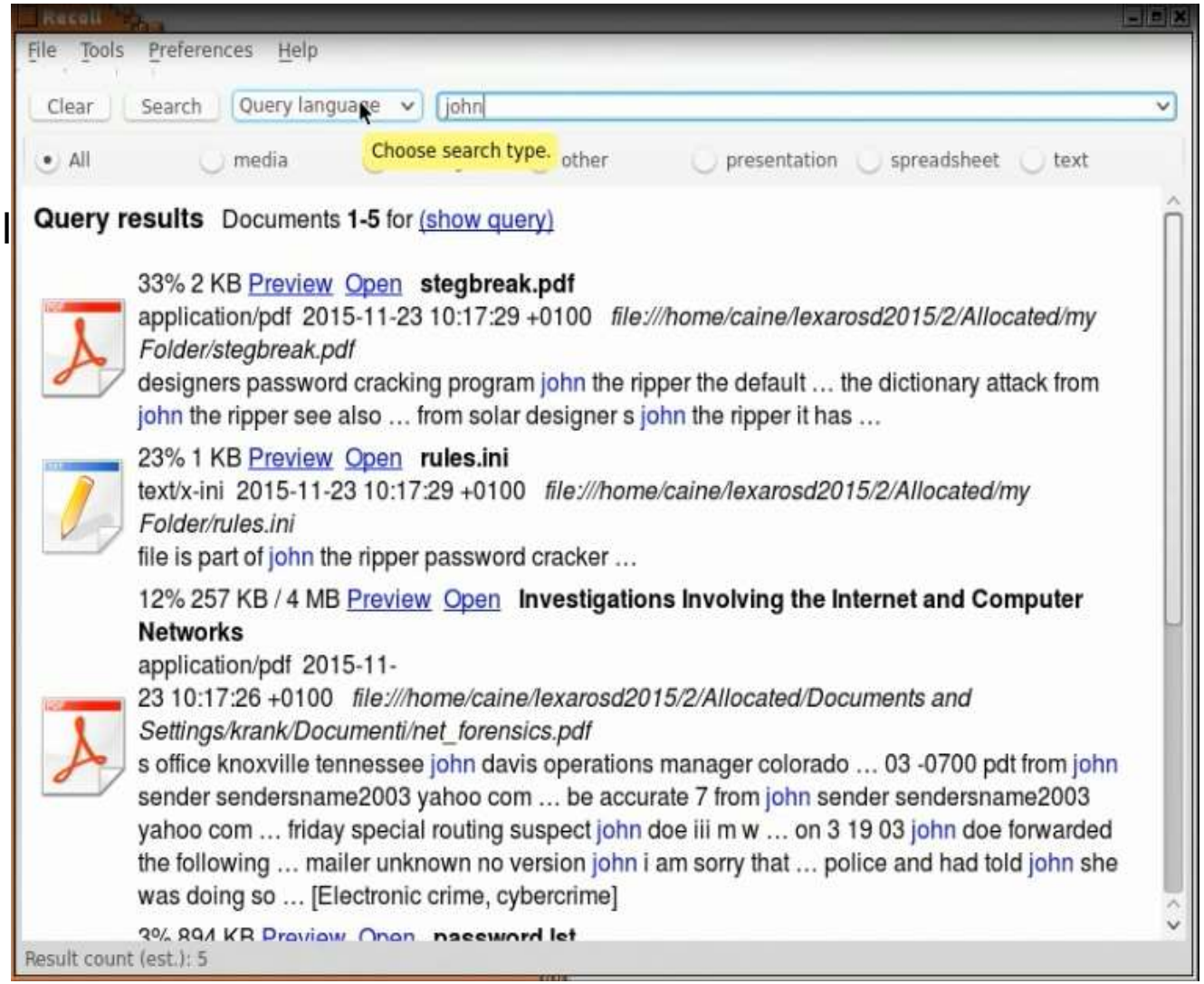
3) Recoll

4) Autopsy

INDICIZZAZIONE FILE

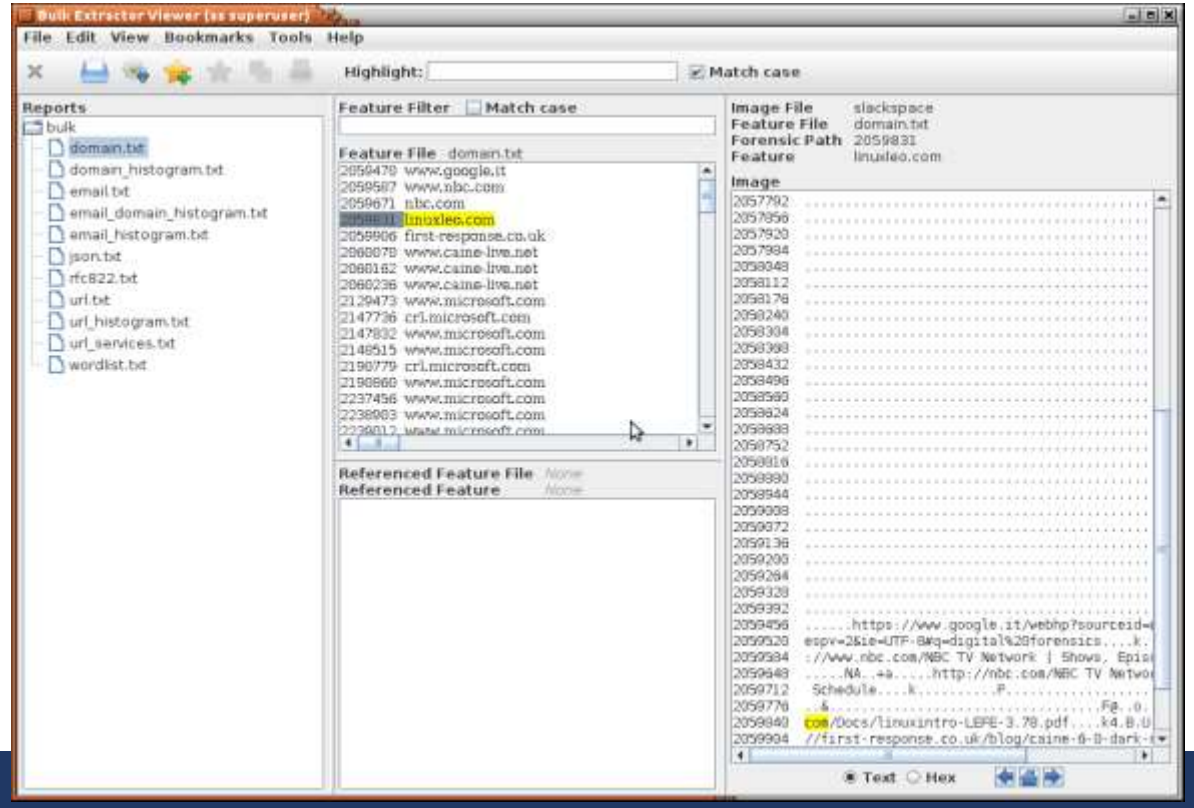
Dopo aver estratto tutti i file che ci possono interessare, conviene indicizzare e metter tutto su database, per avere un'interfaccia comoda per fare l ricerche per parole chiave.
In ambiente Linux possiamo usare RECOLL

https://www.lesbonscomptes.com/recoll/



Bulk_Extractor/BEViewer è un altro potente strumento sia per Windows che per Linux è Bulk_Extractor, che lo si può definire un data carver per espressioni regolari al fine di identificare stringhe particolari definite da pattern, per esempio le e-mail sono fatte da: [lettere_e_numeri]@[lettere_e_numeri].[lettere] (esempio semplificato per rendere l'idea).

Bulk_Extractor non lavora a livello file system, può analizzare qualunque oggetto binario, poi i risultati saranno identificati dalla posizione (byte offset) che una certa stringa occupa nel file in analisi.



- Timeline

NBTempo e NBTempoW

Log2Timeline

Autopsy

NBTEMPO (presente in CAINE e qui https://github.com/nannib) che sfrutta i tool dello SLEUTHKIT **Tsk_times** e **mactime**, al fine di generare un file CSV (consultabile con uno spreadsheet tipo EXCEL).
Può essere utile anche **Log2Timeline,** che permette una timeline basata non solo su i timestamps di file system, ma anche su quelli dei metadati.
Esempio:
Utilizzo di log2timeline per la web history :

```
sudo log2timeline.py --parsers webhist url.dmp disk.E01
```

`pinfo.py url.dmp` (informazioni sull'elaborato da log2timeline) si può anche riderezionarlo con l'operatore ">" su un file .txt

`psort.py -w url.csv url.dmp` (crea il file excel con la history di tutto)

Poi si può interrogare anche solo per un intervallo di tempo:

```
psort.py -q url.dmp "date < '2004-09-20 16:20:00' and date > '2004-09-20 16:10:00'"
```

Manuale: http://plaso.readthedocs.org/en/latest/Using-psort/

SOLO FILESYSTEM

```
log2timeline.py --parsers filestat pippo.plaso disco.dd
psort.py pippo.plaso -o l2tcsv -w disco.csv
```

VIRTUAL MACHINE

Tramite **XMOUNT** possiamo generare “al volo” un file VDI (formato per VirtualBox) o VMDK (VMWare) senza doverlo realmente creare tramite conversione da EWF a VDI, con conseguente perdita di tempo e spazio su disco.

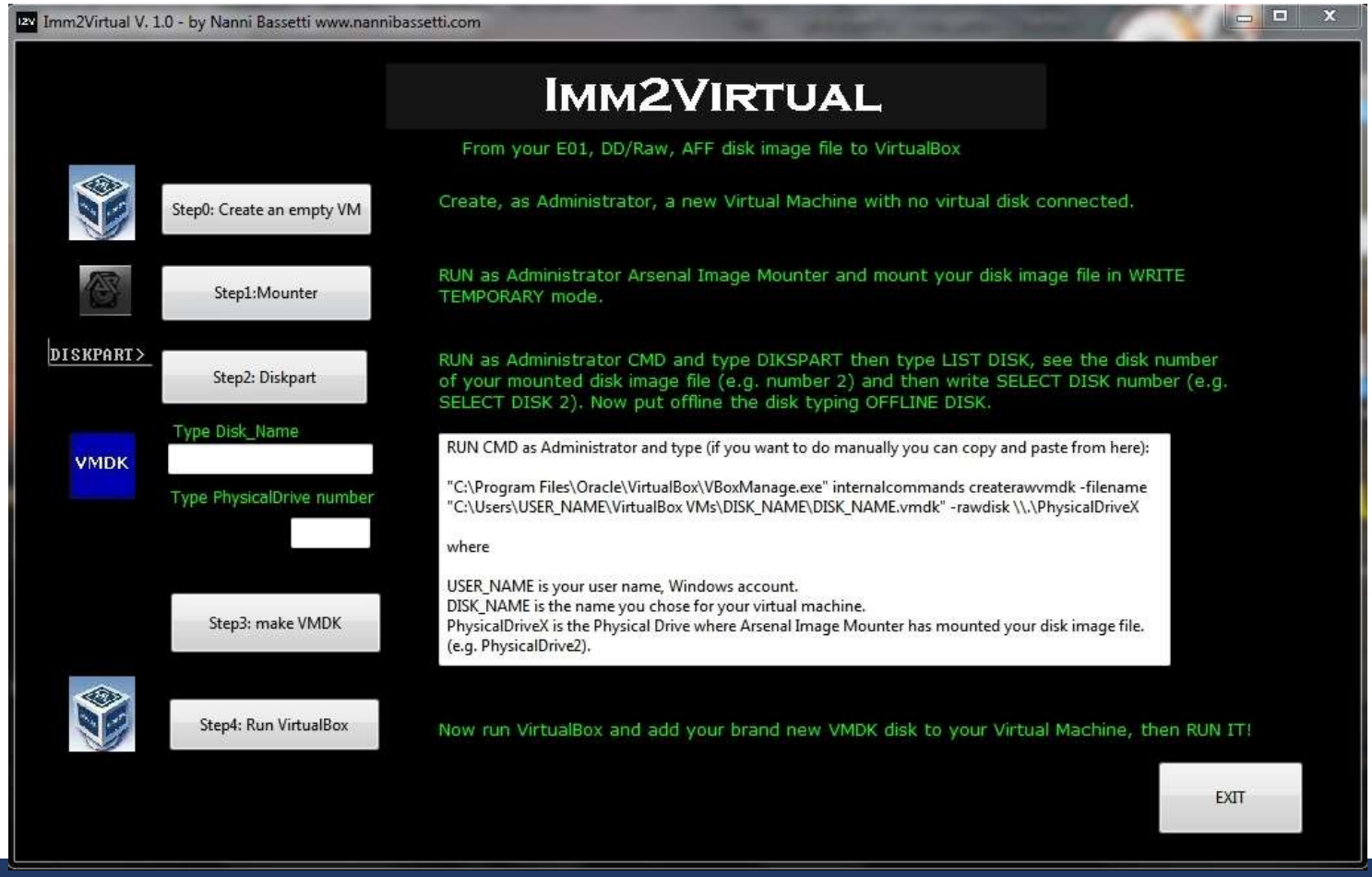
Poi lanciamo **VirtualBox** e virtualizziamo il sistema presente sul file immagine del disco in analisi, al fine di poter utilizzare un computer virtuale che riproduca lo stesso ambiente di lavoro del computer sul quale era montato il disco rigido avere la possibilità di usare tutti gli strumenti free (es. Nirsoft, Sysinternals, ecc.) sul sistema in running ed anche vedere meglio il tutto.
Se vogliamo poi esportare la macchina virtuale possiamo anche creare il file in formato **OVA**, utilizzando **VirtualBox**, così da poterlo lavorare su altri sistemi dove abbiamo Virtual Machine Players.

- VIRTUALIZZAZIONE

Xmount-Gui + VirtualBox

In Windows

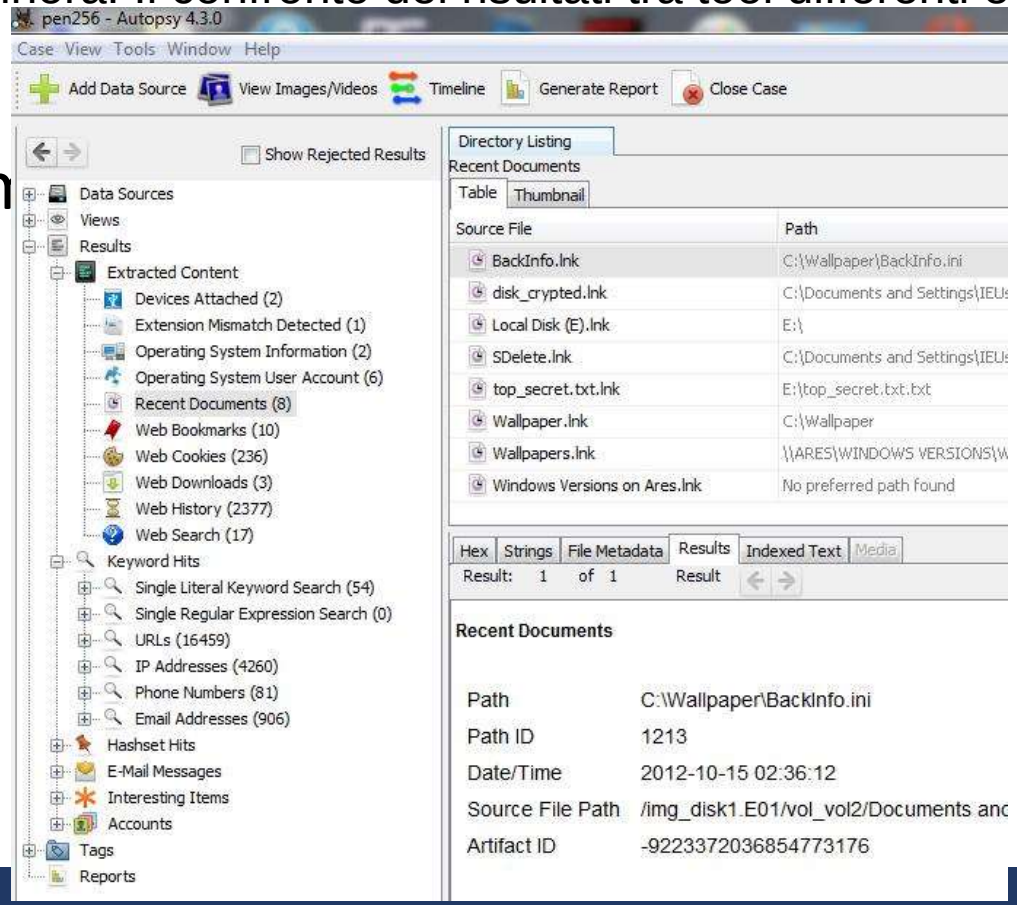
Imm2Virtual



AUTOPSY

AUTOPSY per Windows/Linux è un framework che permette una visione, analisi e classificazioni delle informazioni, in maniera visuale e confortevole, oltre che ha un motore d'indicizzazione per stringhe. Attualmente pecca di essere un po' lento, ma è in costante evoluzione, in ogni caso conviene utilizzarlo, anche per avere una panoramica complessiva di tanti dati estratti ed analizzati con tanti tool diversi, come abbiamo visto finora. Il confronto dei risultati tra tool differenti è sempre consigliabile!

Esen



https://github.com/markmckinnon/Autopsy-Plugins

https://github.com/tomvandermussele/autopsy-plugins

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

SCRCPY

- https://github.com/Genymobile/scrcpy

  Nothing is required to be installed on the device by the user: at startup, the client is responsible for executing the server on the device.

  pushed to /data/local/tmp

  Note that /data/local/tmp is readable and writable by shell, but not world-writable, so a malicious application may not replace the server just before the client executes it.