Digital forensics a costo zero

Date : 17 febbraio 2017

Simuliamo una piccola indagine informatica, sfruttando solo strumenti software freeware ed open source gratuiti, per dimostrare come tutto si può fare senza grandi spese o macchine potentissime, cogliendo anche il fascino della ricerca degli strumento e della diversificazione degli stessi. In questo percorso si evidenzierà anche che così operando si impara e si approfondiscono le conoscenze informatiche.

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 quest'articolo vorrei mostrare un piccolo percorso d'acquisizione ed analisi effettuato tutto con strumenti gratuiti o molto economici ed open source, 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.

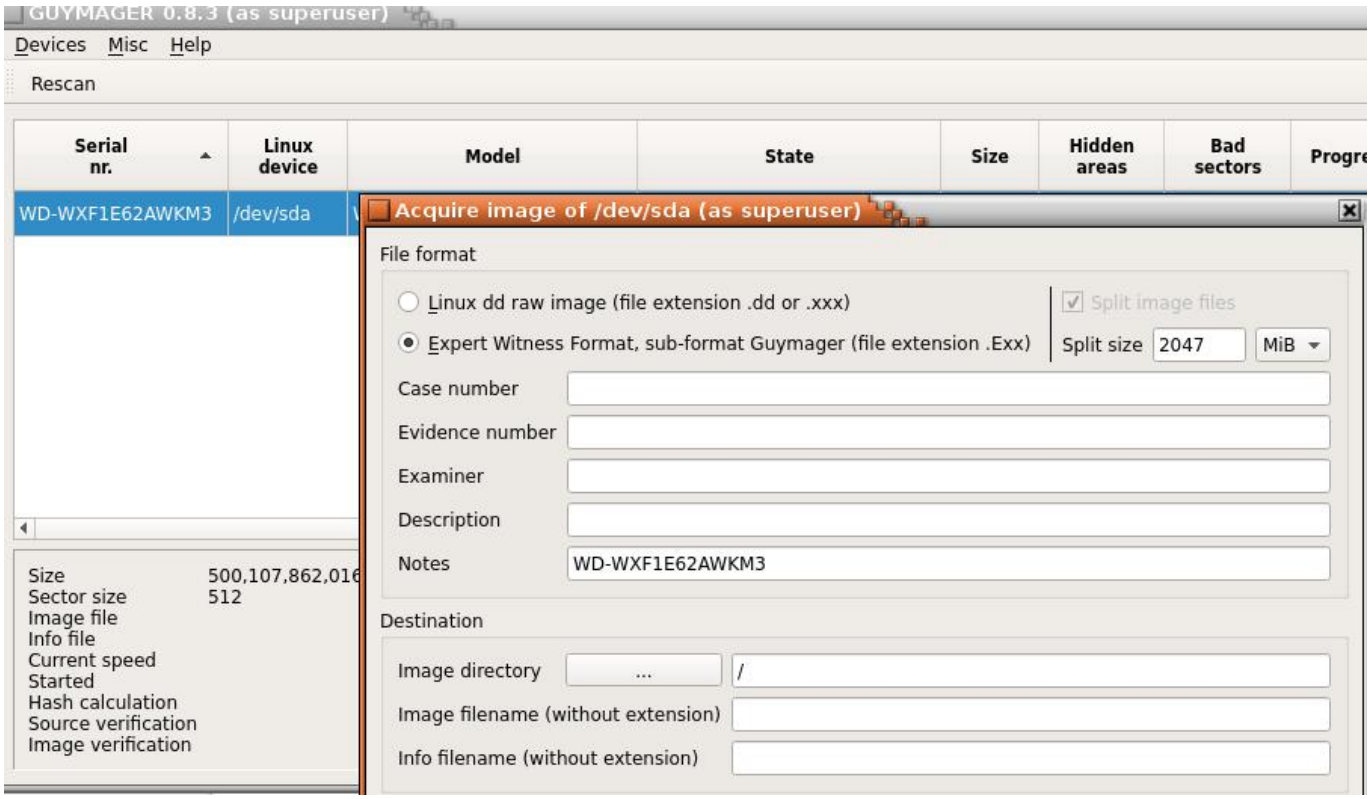
ACQUISIZIONE

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.



COPIA TRAMITE RETE

Se per qualche ragione abbiamo necessità di creare il file immagine su un computer in rete LAN, potremmo anche usare il montaggio del disco in rete tramite **vbladed** e **aoe** (ATA OVER ETHERNET). Oltre il classico **dd** e **netcat**.

sul server (OS: CAINE)

```
sudo blockdev --setrw /dev/sdb  sudo modprobe aoe  sudo vbladed 0 1 eth0 /dev/sdb1
```

sul client (OS: CAINE)

```
sudo modprobe aoe  sudo aoe-stat  sudo blockdev --report  sudo blockdev --setrw /dev/etherd/e0.1  sudo mount -o rw /dev/etherd/e0.1 /media/disco
```

Vediamo DD e NETCAT in azione.

Sulla macchina da acquisire:

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

DD invia i bytes di /dev/sdb all'indirizzo IP della macchina destinazione in ascolto sulla porta 2000, tramite netcat.

Sulla macchina destinazione:

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

In ambiente Windows si consiglia FTK Imager + write blocker hardware per le copie forensi e per le preview o il dump della RAM.

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

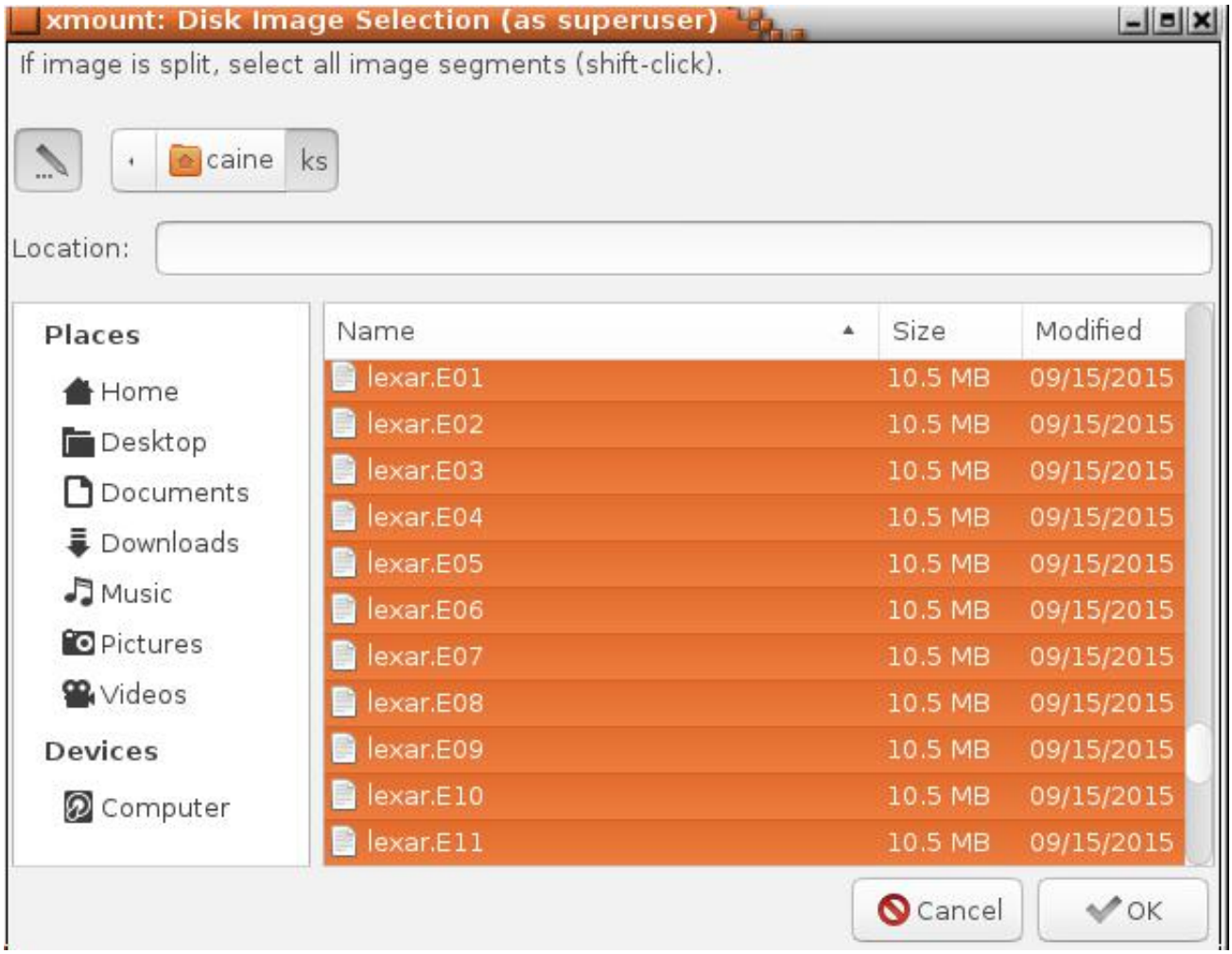
004: 000:001	0000241664	0006533119	0006291456	NTFS / exFAT (0x07)
005: 000:002	0006533120	0975697919	0969164800	NTFS / exFAT (0x07)
006: -------	0975697920	0975699967	0000002048	Unallocated

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
```

Il numero 6533120 è il settore d'inizio della partizione oggetto d'analisi, lo dobbiamo moltiplicare per 512 bytes (la dimensione del singolo settore), per avere l'offset in bytes d'inizio partizione.

Estrazione dei VSS in formato raw

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

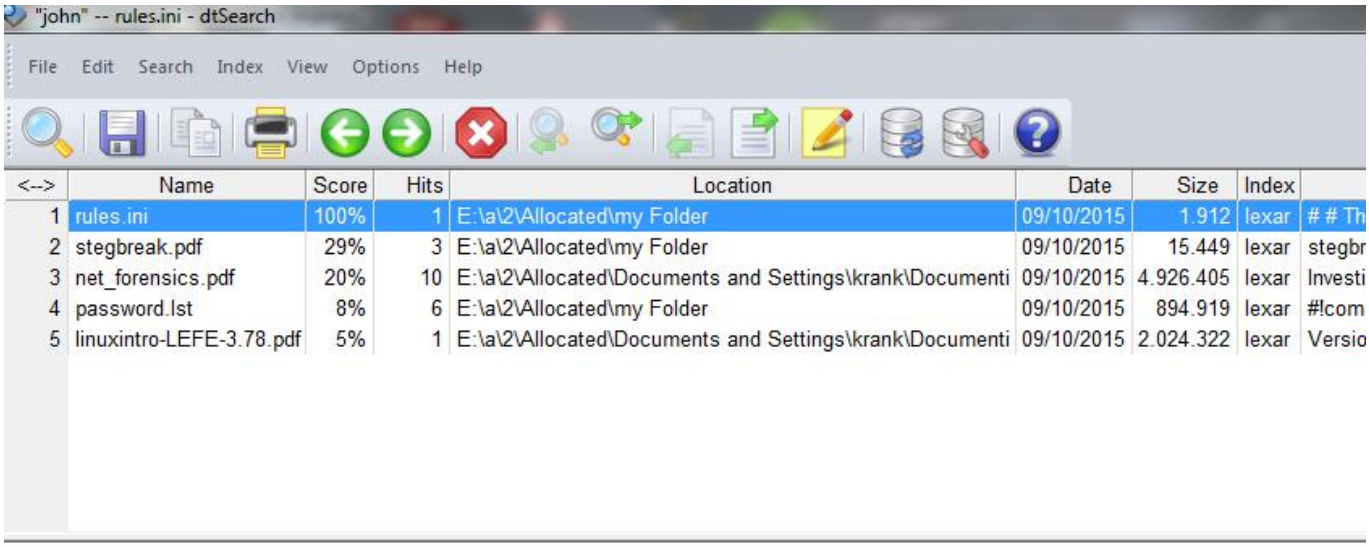
Questo genera un file binario chiamato VSS1, che possiamo montare come un normale dispositivo a blocchi:

```
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.

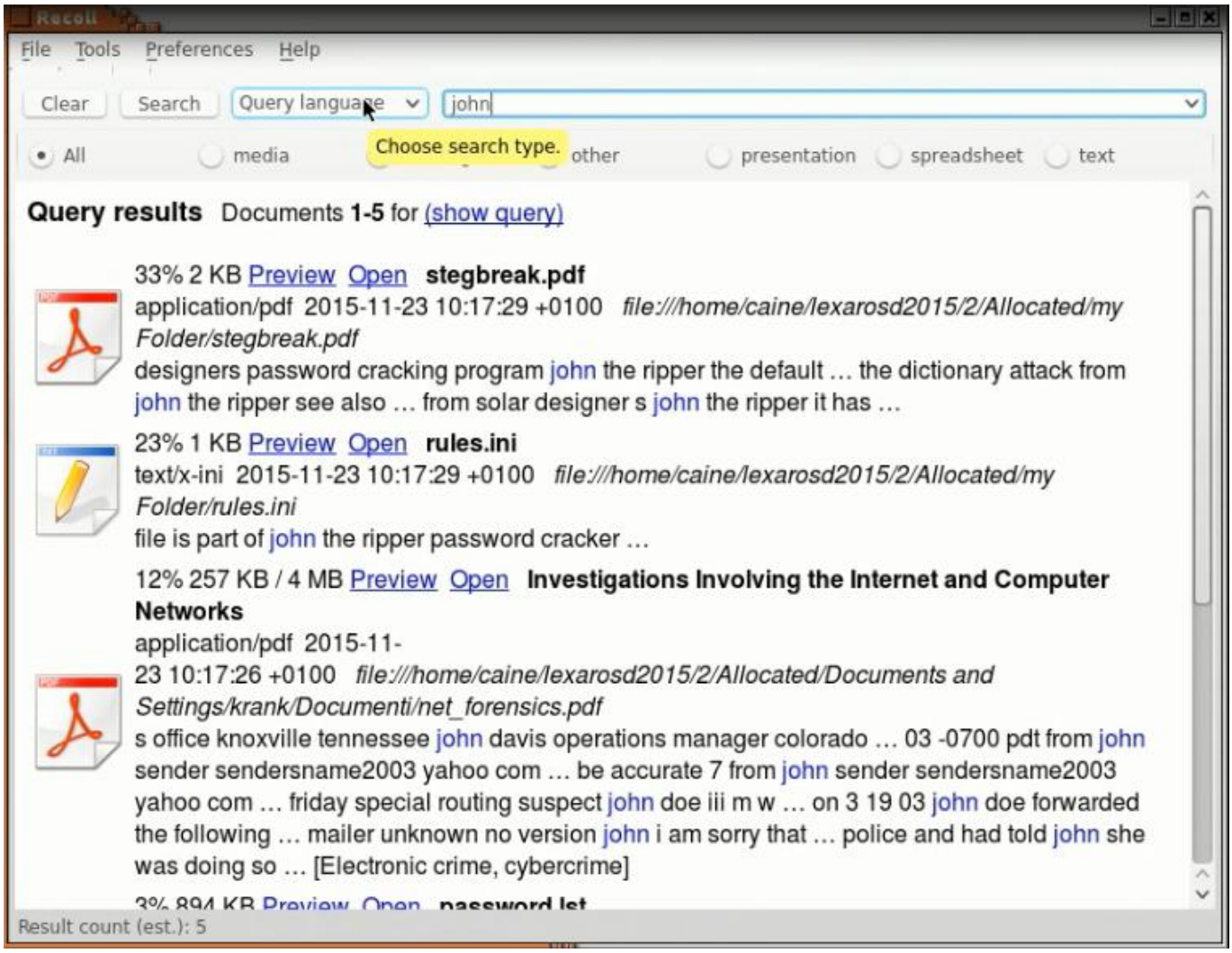
INDICIZZAZIONE FILE

Dopo aver estratto tutti i file che ci possono interessare, conviene indicizzare e metter tutto su database, per avere un'interfaccia agevole per fare le ricerche per parole chiave.
In ambiente Windows possiamo usare DTSearch (non ha costi proibitivi).




```
#
# This file is part of John the Ripper password cracker,
# Copyright (c) 1996-98 by Solar Designer
#
# Wordlist mode rules
[List.Rules:Wordlist]
# Try words as they are
```

In ambiente Linux possiamo usare RECOLL:



TIMELINE

Possiamo generare una timeline tramite lo script **NBTEMPO** (presente in CAINE 8.0 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 urls.dmp disk.E01
```

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

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

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

```
psort.py -q urls.dmp "date  '2016-09-20 16:10:00'"
```

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

VIRTUAL MACHINE

Tramite **XMOUNT-GUI** 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.

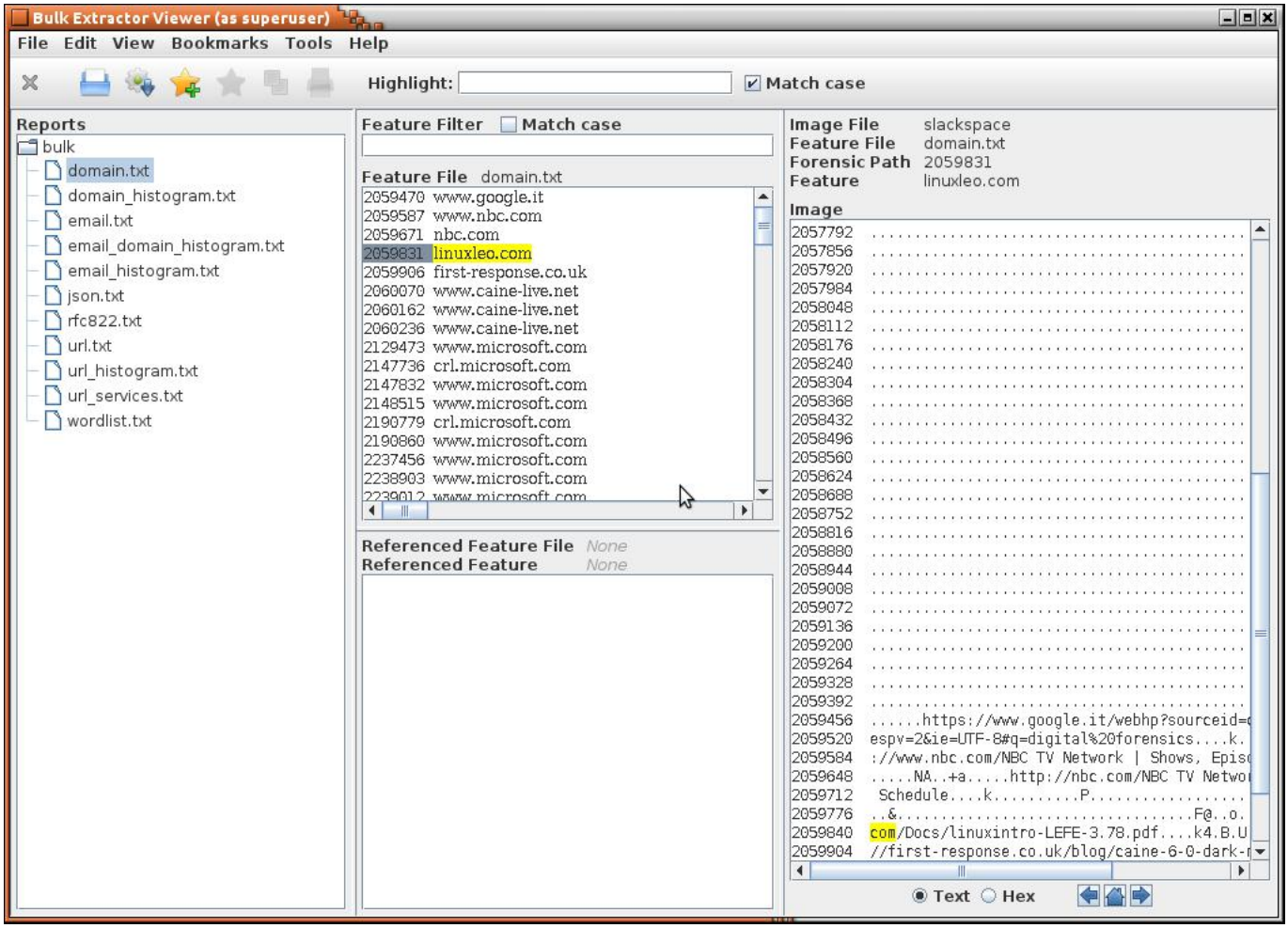
Poi lanciamo **VirtualBox** e virtualizziamo il sistema presente sul file immagine del disco in analisi, al fine di poter utilizzare un computer virtuale che riproduca lo stesso ambiente di lavoro del computer sul quale era montato il disco rigido ed avere la possibilità di usare tutti gli strumenti free (es. Nirsoft, Sysinternals, ecc.) sul sistema in running ed anche vedere più comodamente 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.

Per l’analisi dei registri sia in ambiente Windows sia in Linux c’è il buon RegRipper.

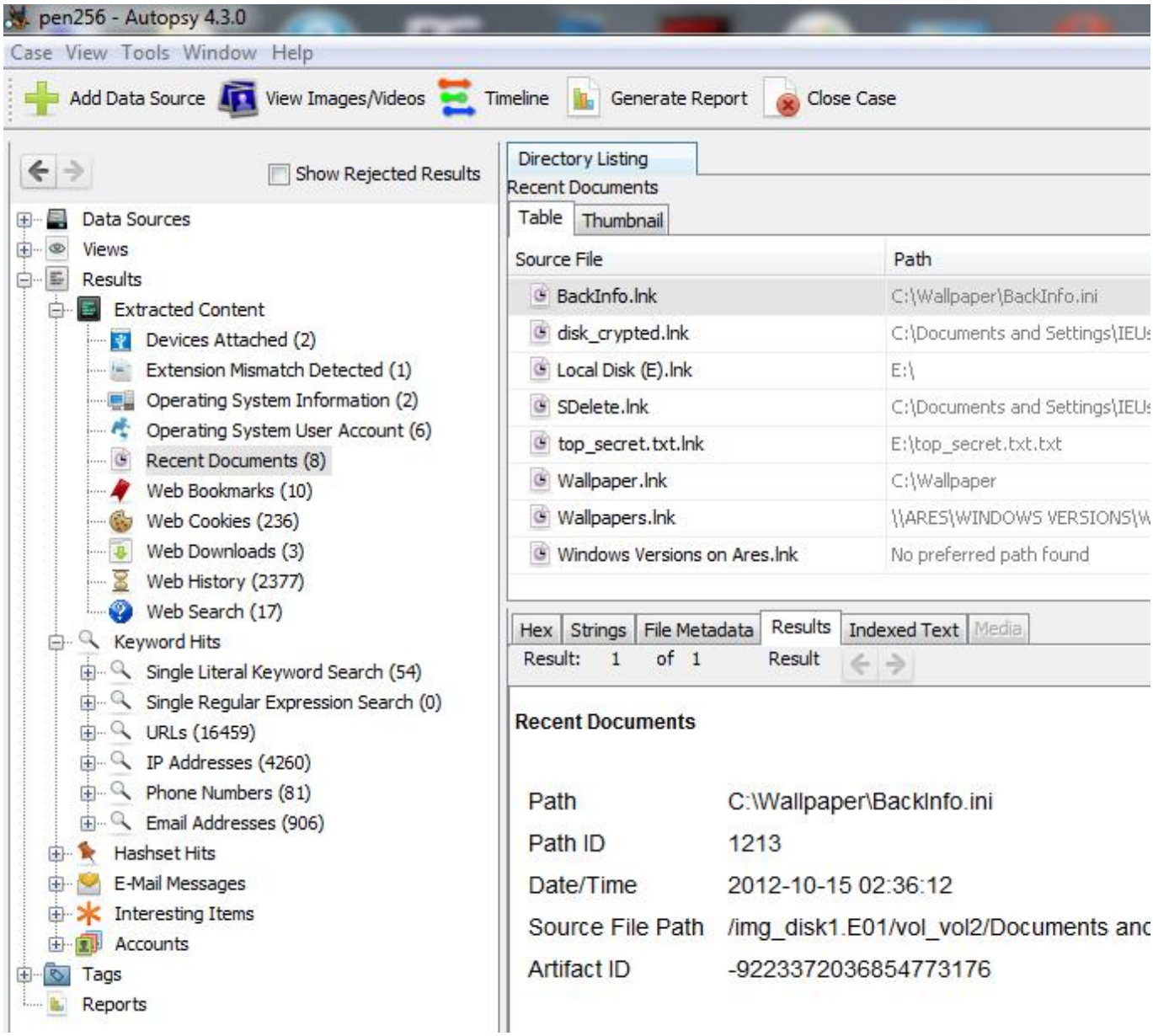
Infine un altro potente strumento sia per Windows che per Linux è Bulk Extractor, che lo si può definire un data carver per espressioni regolari al fine di identificare stringhe particolari definite da

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.



AUTOPSY

AUTOPSY per Windows è un framework che permette una visione, analisi e classificazioni delle informazioni, in maniera semplice, organizzata 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!



Conclusioni

Tra Linux e Windows ci sono tantissimi tool freeware, open source gratuiti, che permettono una serie di analisi ed anche comparazione dei risultati.
Sicuramente bisogna cercarli, provarli, confrontarli, unire i risultati in un unico report, alcuni sono scomodi, ma ci permettono di effettuare un'analisi informatica senza necessariamente avere delle macchine potentissime e sopportare dei costi elevati, ma la cosa più importante è la versatilità, poter scegliere varie soluzioni ed approcci, il confronto, la ricerca e spesso grazie a questi strumenti si comprendono meglio anche alcuni meccanismi e sistemi informatici, questo rende l'investigatore informatico più “intimo” con quello che

sta analizzando.
Non meno importante è che l'uso dell'open source garantisce tutto il percorso del trattamento dei dati, si sa cosa entra, si sa come viene elaborato e si sa cosa esce, proprio perché il codice è aperto, quindi tutto è tracciabile, diversamente se un software commerciale fornisce alcuni risultati, non possiamo sapere che tipo di elaborazione ha fatto, dato che non siamo in possesso del codice sorgente, pertanto a livello di pura metodologia scientifica l'open source è più aderente rispetto al commerciale.
Indubbiamente, se si impara a navigare col sestante e le stelle, nulla vieta di evolversi usando un bel navigatore GPS magari in 3D su una barca di lusso, tanto se qualsiasi cosa dovesse andar storto, abbiamo sempre le competenze per tornare a terra, possiamo dire ugualmente di chi impara direttamente sulla barca di lusso?

Concludendo, sì ai software commerciali belli e performanti, anche perché senza di loro alcuni casi con grandi e diverse moli di dati, diventano ingestibili con open source e tool gratuiti, ma non dimentichiamo che, anche svolgere un caso usando tanti tool ed incastrare i risultati tra loro, sapendo che tutto può essere ripetuto da qualsiasi altro analista, perché tutto è fatto con strumenti liberi, è anche una gran bella soddisfazione.

A cura di: **Nanni Bassetti**