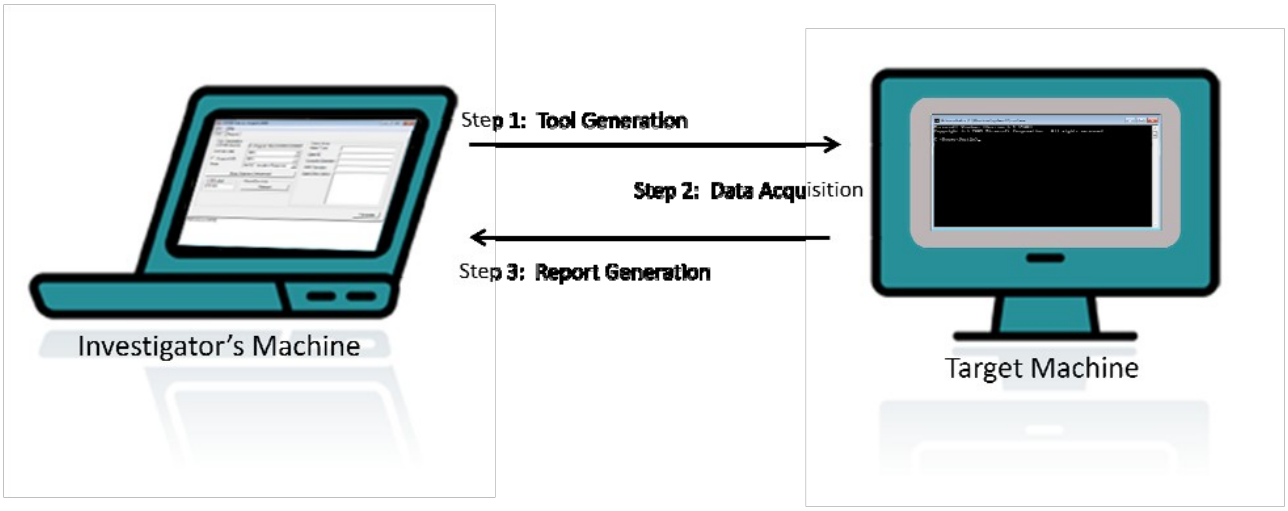
Cofee-HM (Home Made) - mini-howto

(ovvero come costruirsi il proprio Computer Online Forensic Evidence Extractor)

Augusto Scatolini (webmaster@comunecampagnano.it)
Ver. 1.0 Dicembre 2009



Computer Online Forensic Evidence Extractor (COFEE) è una chiavetta USB modificata per investigatori informatici. Questi ultimi la usano per l'estrazione veloce di dati "**forensic**" da computer basati su Windows sospettati di contenere evidenze di attività criminali.

Fonte Wikipedia in inglese

L'informatica forense *(Computer Forensics) è la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico per essere valutato in un processo giuridico e studia, ai fini probatori, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici. Si tratta di una disciplina di recente formazione, che spesso viene erroneamente identificata come una nuova "branca" della computer security.*

Fonte Wikipedia in italiano

Lo strumento, sviluppato da Microsoft, si attiva inserendolo in una porta **USB** e contiene circa **150 comandi** che possono velocizzare il reperimento di evidenze digitali tanto che, secondo Microsoft, quello che prima si faceva con 3-4 ore di tempo può ora essere fatto in circa 20 minuti.
Questi comandi offrono funzioni come la possibilità di decrittare password, verificare l'attività internet di un computer e analizzare i dati memorizzati nei dischi.
Microsoft offre gratuitamente i device Cofee e il supporto tecnico alle agenzie specializzate. Nel mese di aprile del 2009, Microsoft e **Interpol** hanno firmato un accordo per il quale quest'ultima sarà la principale distributrice internazionale di Cofee. L'**Università di Dublino** per l'investigazione di crimini informatici insieme a Interpol sviluppano programmi di formazione sull'uso di Cofee.
Il **National White Collar Crime Center** NW3C è stato autorizzato da Microsoft quale unico distributore USA di Cofee.
Nel mese di novembre 2009 alcune copie di Cofee sono arrivate nei circuiti **Torrent**.
Funzionalità similari a quelle di Cofee si possono trovare su distribuzioni specializzate di GNU/Linux come **BackTrack**, **Knoppix STD**, **PHLAK** e **nUbuntu**.
A differenza di Cofee che funziona solo su sistemi Windos, queste distribuzioni possono essere utilizzate anche su sistemi **non-windows**.

Fonte Wikipedia in inglese

Dopo aver letto queste notizie che riguardano l'Interpol, l'NW3C, l'Università di Dublino ecc. si potrebbe rimanere impressionati da questo tool *microsoft-miracoloso*.
Da alcuni giorni, inoltre, circolano in rete le precisazioni di Microsoft che minaccia i siti torrent di rimuovere i link per il download di Cofee in quanto "azione illegale" e illegale sarebbe perfino (e solo) usarlo, a prescindere dall'origine, perché è illegale violare i computer altrui.

Questo dimostra soltanto l'abilità di Microsoft, questa sì miracolosa, di saper **vendere i tappeti bucati**, e bene.

Cofee altro non è se non un'interfaccia grafica per una serie di comunissimi comandi dos, sì il vecchio dos, che

- prima copia i comandi (programmi) sulla chiavetta USB
- che poi, grazie alla funzione Autorun (se attiva), vanno in esecuzione automaticamente, re-direzionano l'output su file (mi sembra xml)
- infine genera un report sulla base delle informazioni contenute nei file collezionati dai comandi dos

C'era bisogno di fare cotanto fumo per un arrosto così misero?

A parte che come citato prima ci sono molte distribuzioni Linux che

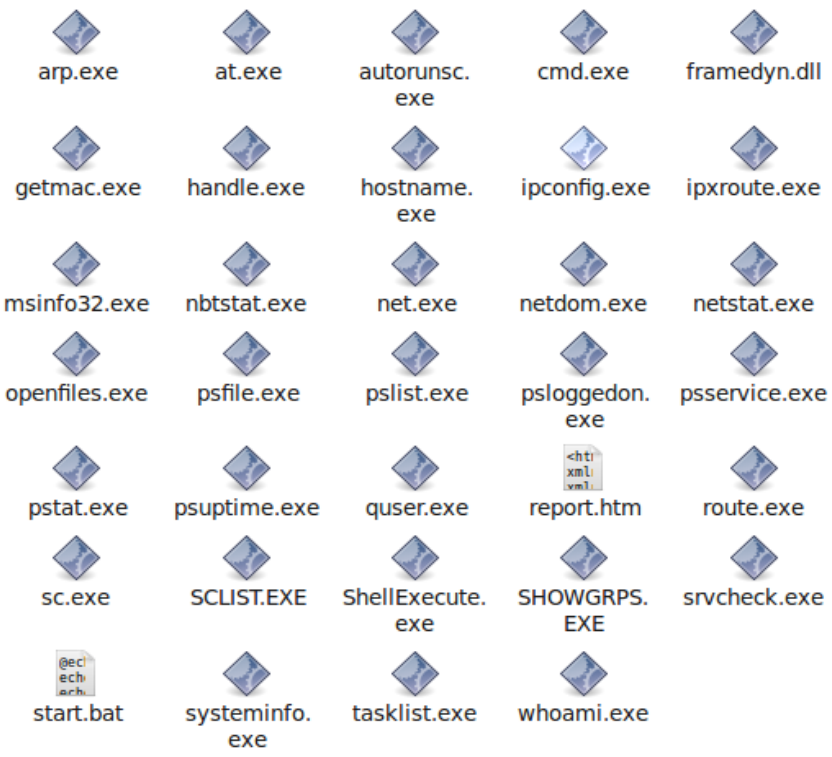
- non solo fanno le stesse cose (sicuramente meglio) ma
- le fanno anche su macchine non-windows e
- dato che sono della famiglia GNU ovvero a codice aperto non c'é nessunissimo problema legale a procurarsele via internet

A parte che questi tools possono essere usati legittimamente

- per controllare la propria macchina per verificarne l'integrità o
- per controllare la macchina di un amico in difficoltà o
- per controllare la macchina di un cliente (attività commerciale) o
- per controllare l'integrità delle macchine di una rete lan da parte di un amministratore

Siamo sicuri che non possiamo farci un Cofee fatto in casa in un paio d'ore?

A mero titolo dimostrativo, ci procuriamo un certo numero di comandi/programmi dos che fanno parte del proprio sistema oprativo Windows + qualche comando/programma pubblico da Sysinternal + il programma/(comando shellexecute + un compilatore di file batch



Ci costruiamo un file batch che manda in esecuzione tutti i comandi con più opzioni e re-direzioniamo i risultati su una serie di file ASCII numerati 01.txt, 02.txt, ecc

Listato del file start.bat

```
@echo off
echo "======================================================================"
echo "============       INIZIO RACCOLTA INFORMAZIONI       ================="
echo "======================================================================"
echo "A T T E N D E R E ..........."
arp.exe /a › 01.txt
autorunsc.exe › 02.txt
at.exe › 03.txt
getmac.exe › 04.txt
handle.exe /a › 05.txt
hostname.exe › 06.txt
ipconfig.exe /all › 07.txt
msinfo32.exe /report 08.txt
net.exe group › 09.txt
net.exe accounts › 10.txt
net.exe localgroup › 11.txt
net.exe use › 12.txt
net.exe user › 13.txt
net.exe Session › 14.txt
net.exe start › 15.txt
net.exe file › 16.txt
net.exe view › 17.txt
net.exe localgroup administrators › 18.txt
net.exe localgroup administrators /domain › 19.txt
net.exe share › 20.txt
netstat.exe /ao › 21.txt
netstat.exe /no › 22.txt
netdom.exe query DC › 23.txt
nbtstat.exe /n › 24.txt
nbtstat.exe /c › 25.txt
nbtstat.exe /S › 26.txt
nbtstat.exe /A 127.0.0.1 › 27.txt
openfiles.exe /query /v › 28.txt
pslist.exe › 29.txt
pslist.exe /t › 30.txt
psfile.exe › 31.txt
psuptime.exe › 32.txt
psloggedon.exe › 33.txt
pstat.exe › 34.txt
psservice.exe › 35.txt
quser.exe › 36.txt
route.exe print › 37.txt
srvcheck \\127.0.0.1 › 38.txt
showgrps.exe › 39.txt
systeminfo.exe › 40.txt
sclist.exe › 41.txt
sc.exe queryex › 42.txt
sc.exe query › 43.txt
tasklist.exe /svc › 44.txt
whoami.exe › 45.txt
echo "======================================================================"
echo "==============     RACCOLTA INFORMAZIONI COMPLETATA      ================"
echo "======================================================================"
echo ""
echo " premi un tasto vedere il REPORT"
echo ""
pause
shellexecute.exe /f:report.htm
```

in questo modo il comando start.bat eseguirà tutti i comandi in sequenza, ogni comando creerà il relativo file numerato con estensione txt (in totale 45 file, in questo esempio) il comando nell'ultima riga serve per aprire automaticamente una pagina HTML che contiene dei semplici link ai 45 file txt. Abbiamo creato un **Cofee Home Made**

anteprima del file HTML che spiega i comandi e linka i risultati

Computer Online Forensic Evidence Extractor (COFEE) Home Mad				
1	1	arp.exe	/a	Mostra le attuali entrate del protocollo A
2	2	autorunsc.exe		Mostra i programmi che vanno in esecuz fase di boot
3	3	at.exe		Mostra gli eventi schedulati
4	4	getmac.exe		Mostra l'indirizzo MAC della scheda di re
5	5	handle.exe	/a	Handle è un comando specifico per ricer
6	6	hostname.exe		Elenca i nomi degli Host del Computer
7	7	ipconfig.exe	/all	Mostra la configurazione delle schede di
8	8	msinfo32.exe	/report %OUTFILE%	Elenca una serie interminabile di inform
9	9	net.exe	group	Mostra i gruppi di rete
	10	net.exe	accounts	Mostra gli account di rete
	11	net.exe	localgroup	Mostra i gruppi locali
	12	net.exe	use	Mostra informazioni sulle connessioni
	13	net.exe	user	Mostra l'utente del computer and/o dom
	14	net.exe	Session	Mostra tutte le sessioni connesse al com
	15	net.exe	start	Mostra la lista dei servizi attivi
	16	net.exe	file	Mostra i file condivisi aperti
	17	net.exe	view	Mostra la lista die computer Displays a l specified workgroup or the shared resou

Amenità:

una volta scaricato il file compresso ed estratto il contenuto si otterranno tre file e una cartella contenete tutta l'applicazione:

se si mette tutto il contenuto in una **pen drive USB** e si inserisce in una porta USB di un Computer, il file autorun.inf (se l'autorun è attivato) eseguirà il file start.exe che altro non è che un file batch compilato (con **quick batch file compiler**) che cambia directory e manda in esecuzione il file start.bat

file autorun.inf

```
[autorun]
open=start.exe
action=Execute start.exe
```

Il file report.bat del quale segue il contenuto

```
@echo off
cd cofee_hm
shellexecute.exe /f:report.htm
```

permette di riaprire il report (report.htm) in un secondo momento

** **attenzione**, per eseguire una nuova scansione su un 'altro PC si devono archiviare i 45 file ASCII contenuti nella cartella cofee_HM, se si vogliono conservare, questo perché ogni nuova scansione **sovrascrive** tutti i file

Download: http://www.adrive.com/public/5a3c90b02c330fb6109474b3c1e6ef049fe62d287c780629cb8a5466fb58b546.html

FINE

altre miniguide
http://www.comunecampagnano.it/gnu/miniguide.htm

il font Traveling_Typewriter è scaricabile da http://img.dafont.com/dl/?f=traveling_typewrite