Stato dell'arte della Computer Forensic internazionale made in Linux

Stefano Fratepietro

ERLUG

Whoami

IT Security Specialist per il CSE (Consorzio Servizi Bancari)

Consulente di Informatica Forense per le procure della Repubblica Italiana, forze dell'ordine e privati

- Telecom Italia – Ghioni
- Buongiorno! Vitaminic

DEFT Linux project leader

www.deftlinux.net

Argomenti

- Introduzione all' Informatica Forense
- Software commerciale, software free e software open
- Gli strumenti made in Linux
- Il progetto DEFT
- Casi di successo

Informatica Forense

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 al fine di essere valutato in un processo giuridico e studia, ai fini probatori, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici.

(Wikipedia)

Le specializzazioni

- Disk Forensic
  - Accertamenti tecnici su memorie di massa, generalmente hard disk, memorie esterne, penne usb ecc...
- Mobile Forensic
  - Accertamenti tecnici su cellulari, smarthphone, palmari, lettori mp3 (Ipod e simili)
- Network Forensic
  - Accertamenti tecnici su reti informatiche

Le fasi dell'accertamento tecnico

- Individuazione
- Preservazione
- Acquisizione
- Analisi
- Presentazione delle risultanze
- Catena di custodia dei reperti

Cosa uso?

Software commerciali – Da 900 € a più di 5000 € a licenza

- Encase
- FTK, Guidance Software
- Xway Forensic
- Paraben Device Seizure
- Altri...

Software non commerciali

- Software open source o freeware, specializzati in singole funzionalità
- Alcune sistemi live cd Linux che raccolgono software per la Computer Forensic

Perchè tutto questo successo?

- Costi elevati delle licenze d'uso
- Fondi sempre più scarsi in tutti i corpi di polizia e forze dell'ordine, sia in Italia che all'estero
- Possibilità di eseguire alcuni tipi di operazioni che nessun software commerciale può eseguire
  - Esempio: acquisizione di dischi in raid 5 con controller proprietario

Casi di successo - The Sleuth Kit

- Creata nel 2003 da Brian Carrier, GPL
- Collezione di librerie e applicativi a linea di comando per l'esecuzione di operazioni informatico forensi
- Utilizzabile anche mediante una interfaccia grafica chiamata Autopsy

  Consente di eseguire operazioni come
- Analizzare dischi e immagini in formato raw, aff ed encase
- Supporta ext2/3/4, fat, ntfs, iso9660 e UFS
- Recupero dati
- Creazione di time line
- Ricerca di contenuti
- Analisi dei metadata

Casi di successo – Time line

- Per time line si intende una fotografia di tutti gli eventi di creazione, ultimo accesso ed ultima modifica a file o directory contenuti all'interno di una memoria informatica di un determinato sistema
- La time line viene creata mettendo in ordine cronologico tutti gli eventi successi in un determinato tempo di vita delle memorie del sistema posto ad analisi
- Metaforicamente parlando, una time line ci permette di viaggiare nel tempo potendo così risalire ad ogni singola azione avvenuta in un arco di tempo definito dall'analista creatore della time line

Casi di successo – Carving

Recupero di file ricercando header e footer, cioè le stringhe che caratterizzano l'inizio e la fine di uno specifico tipo di file

- Foremost
- Scalpel

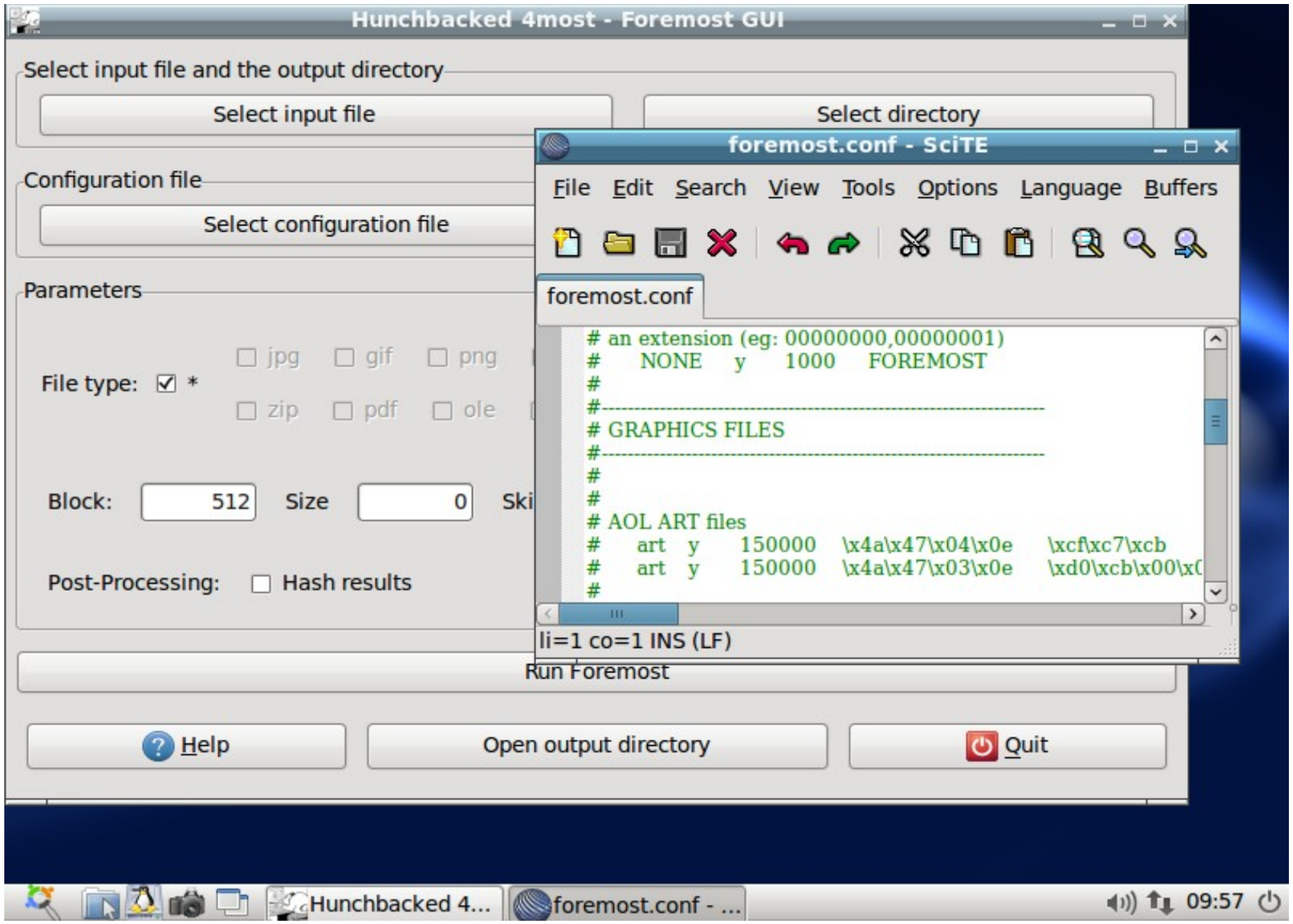
```
# GIF and JPG files
# gif y 155000000 \x47\x49\x46\x38\x37\x61 \x00\x3b
#   gif y  155000000 \x47\x49\x46\x38\x39\x61 \x00\x00\x3b
#  jpg y 200000000 \xff\xd8\xff\xe0\x00\x10     \xff\xd9
```

I valori di header e footer sono in esadecimale

Il campo size rappresenta il massimo numero di byte che foremost recupera se non trova il footer

Casi di successo – Hunchbacked 4most

Creazione di una interfaccia grafica che permetta l'esecuzione di operazione di carving anche a chi non è esperto



Casi di successo – AFF

Advanced Forensics Format (AFF)

- Sviluppato da Simson L. Garfinkel, GPL
- Creazione di un file contenente la memoria di massa acquisita, comprimendo il contenuto e salvando informazioni di interesse al suo interno come riferimenti temporali di interesse e valori di hash della memoria
- Sin dal 2006 è possibile usare The Sleuth Kit per leggere i file creati in formato aff
- Dal 2010 AFF è ufficialmente supportato anche dai software commerciali come FTK

Casi di successo – Lib EWF

- Creata nel 2006 da Joachim Metz, GPL
- Libreria che permette l'utilizzo delle memorie di massa acquisite in formato Encase
- Ad oggi usata da TSK e altri software open

Casi di successo - Xplico

- Creata da Gianluca Costa e Andrea De Franceschi, GPL
  - In collaborazione con DEFT Linux
- E' un Internet Traffic Decoder
- Dato un file pcap è in grado di ricostruire il traffico IP
  - Siti web visitati
  - Posta elettronica
  - Web mail
  - File transfer FTP
  - Stampe
  - Sessioni telnet
  - VoIP SIP
  - Facebook chat

Casi di successo - Xplico

Xplico Interface — User: deft

Help Logout

Cases
Sols
Email
Sip
Web
Images
Printer
Ftp
Mms
GeoMap

For a complete wiew of html page set your browser to use Proxy, and point it to Web server.

Web URLs: Html Image Flash Video Audio All Go

Date	Url	Size	Method	Info
2007-08-14 11:13:58	www.google.it/	1521	GET	info.xml
2007-08-14 11:13:33	track3.mybloglog.com/tr/urltrk.php?i=2007011710424247&t=1&u=http%3A//www.aphotoac	105	GET	info.xml
2007-08-14 11:13:32	track3.mybloglog.com/js/jsserv.php?mblID=2007011710424247	5276	GET	info.xml
2007-08-14 11:13:25	track3.mybloglog.com/tr/urltrk.php?i=2007011710424247&t=1&u=http%3A//www.aphotoac	105	GET	info.xml
2007-08-14 11:13:24	track3.mybloglog.com/js/jsserv.php?mblID=2007011710424247	5274	GET	info.xml
2007-08-14 11:13:23	rcm.amazon.com/e/cm?t=ap06-20&o=1&p=20&l=qs1&f=ifr	2669	GET	info.xml
2007-08-14 11:13:10	rcm.amazon.com/e/cm?t=ap06-20&o=1&p=20&l=qs1&f=ifr	2669	GET	info.xml
2007-08-14 11:13:04	www.aphotoaday.org/fronts.html	850	GET	info.xml
2007-08-14 11:12:37	www.aphotoaday.org/apadnews/	3793	GET	info.xml
2007-08-14 11:12:26	c14.statcounter.com/text.php?sc_project=1435373&resolution=1280&camefrom=http%3A	25	GET	info.xml
2007-08-14 11:12:23	www.aphotoaday.org/favicon.ico	320	GET	info.xml
2007-08-14 11:12:08	www.aphotoaday.org/favicon.ico	320	GET	info.xml
2007-08-14 11:12:08	www.aladingenius.com/theMagicLamp/	6775	GET	info.xml
2007-08-14 11:12:07	www.aphotoaday.org/bestof2006/	604	GET	info.xml
2007-08-14 11:12:07	www.aphotoaday.org/	1390	GET	info.xml
2007-08-14 11:12:02	www.photoblogdirectory.org/buttons/photoblogdirectory_bw.gif	1606	GET	info.xml
2007-08-14 11:11:52	www.aladingenius.com/templates/themagiclamp_2006/img/back.gif	238	GET	info.xml
2007-08-14 11:11:51	www.aladingenius.com/theMagicLamp/index.php?x=browse&pagenum=1	14029	GET	info.xml
2007-08-14 11:11:47	www.aladingenius.com/templates/themagiclamp_2006/img/back.gif	238	GET	info.xml
2007-08-14 11:11:42	www.aladingenius.com/favicon.ico	209	GET	info.xml

Casi di insuccesso – Mobile forensic

- Scarsa implementazione di tool per l'esecuzione di accertamenti tecnici su cellulari
  - Dovuta al fatto che ogni cellulare ha una architettura proprietaria, spesso scarsamente documentata e con sistema operativo sempre differente
- Inesistenza di tool per l'acquisizione e l'analisi avanzata di iPad e iPhone
  - Ad eccezione dei Sql lite client per la lettura dei database

Anche se...

Smarthphone Android, se con accesso di root, è possibile eseguire una accurata perizia... ma non per tutti i modelli!

- Produttori applicano modifiche fuori standard Android, come ad esempio Samsung usa RFS

Pubblicazione su IISFA Memberbook 2012, Stefano Fratepietro e Alessandro Rossetti per l'analisi di un Samsung Galaxy S

Tanti tool sparsi qua e la... la soluzione?

Raccogliere tutti gli applicativi in un unico sistema ottimizzato per l'esecuzione di attività informatico forensic

- Nel 2003 nase F.I.R.E boot cd, prima distribuzione nel suo genere, progetto che muore verso la fine del 2004
- Nel 2005 nasce Helix, che diventa commerciale nel 2009 perdendo popolarità
- Verso la fine del 2005 nasce FCCU, prima distribuzione Linux per usi informatico forensi creata da un copro di polizia (belga); il progetto muore nel 2009
- Nel 2006 nasce DEFT Linux, 100% made in Italy, primo sistema di computer forensic basato sul progetto *ubuntu
- Verso la fine del 2008 nasce CAINE, italiana
- Nel 2008 nasce anche ForLex, italiana

DEFT Linux – www.deftlinux.net

- Acronimo di Digital Evidence Forensic Toolkit
- Nato nel 2005 in collaborazione con la cattedra del corso di Informatica Forense dell'Università degli studi di Bologna; dal 2007 è un progetto indipendente
- Staff di 6 persone di cui 3 appartenenti alle forze dell'ordine
- Soluzioni sia per attività informatico forensi che per Incident Response
- Due sotto sistemi
  - Linux live cd/usb basato su Lubuntu
  - GUI Windows
- Documentazione, italiano ed inglese
- Community Facebook e forum di supporto

DEFT Linux - caratteristiche

- Kernel 2.6.35
- USB 3 ready
- DEFT Extra, Windows Forensic GUI con binari dei principali sistemi operativi
- LXDE
- Supporto ai principali file system in uso
- Wine

Requisiti minimi di sistema

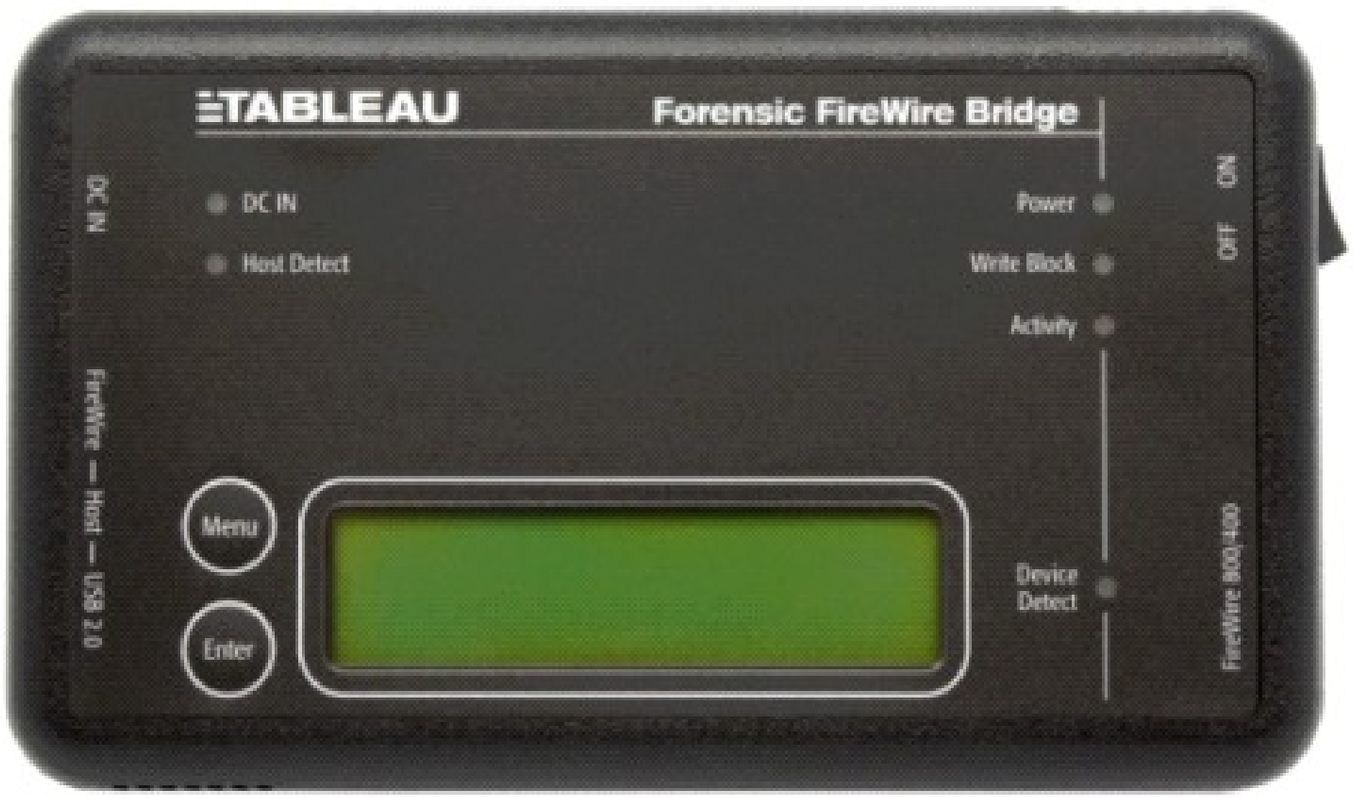
- Pentium II
- 64MB di ramparte testuale, 128 MB di ram per la parte grafica

DEFT Linux – principali usi

- Trasformazione di un qualsiasi pc x86 in un forensic duplicator
- Trasformazione di un qualsiasi pc x86 in un network sniffer
- Recupero file cancellati anche con metodologia di carving
- Ricerca di contenuti
- Analisi della navigazione Internet dei principali browser
- Analisi avanzata di immagine e filmati
- Analisi del registro di Windows
- Individuazione di rootkit e malware
- Cracking di password
- Analisi della chat di Skype
- Individuazione di immagini steganografate

Write blocker software

Mediante l'utilizzo delle opportune policy, è possibile utilizzare DEFT con le stesse funzioni di un write blocker hardware



Acquisizione di un iMac

Case study – Spionaggio industriale

- Nota azienda che produce pezzi in esclusiva per famosa casa automobilistica
- “Fuga” di progetti con relativa produzione degli stessi componenti in oriente
- L'azienda non riesce a capire dove avvenga la fuori uscita di informazioni
- Tutti i computer in azienda hanno un sistema di device controll che vieta l'utilizzo di penne usb
- Tutta la posta elettronica verso l'esterno può essere controllata
- La navigazione Internet verso siti di scambio file o webmail è disabilitata tramite proxy
- Le stampanti non sono controllate...

Case study – Spionaggio industriale

- Porta in monitoring dello switch del campus con un pc con Xplico avviato
- Richiesto pezzo di ricambio X all'azienda orientale
- Dopo sole 4 ore parte in stampa il progetto del ricambio X
  - Un genio, non potendo portarsi via fogli di plotter in formato A1, per passare inosservato stampava progetti in formato A1 in tanti fogli A4

Case study – DEFT nei paese emergenti

Creazione del toolkit per forze dell'ordine e servizi segreti partendo da DEFT

- Creazione di linee guida per l'esecuzione di attività informatico forensi mediante l'utilizzo di soli strumenti freeware
- Aggiunta di moduli nel kernel
- Inserimento di nuovi software e script sviluppati internamente
- Traduzione degli applicativi

GRAZIE PER L'ATTENZIONE

steve.deftlinux.net
twitter: stevedeft
stefano@deftlinux.net

Le slides e le riprese audio/video dell'intervento saranno disponibili su:

http://erlug.linux.it/linuxday/2011/