

DEFT Linux 6

Digital Evidence & Forensic Toolkit

DEFT Linux
Computer Forensics Live CD



Dott. Stefano Fratepietro
stefano@deftlinux.net



Creative Commons Attribution-Non opere derivate 2.5

Milano, 22 ottobre - Smau 2010
Fiera Milano city

Obiettivi del seminario

- DEFT in pillole
- Alcune novità della release 6
- Road map di sviluppo

Dott. Stefano Fratepietro

- IT - Security specialist per il CSE Consorzio Servizi Bancari S.c.r.a.l
- Consulente di Informatica forense per tribunali, forze dell'ordine (Polizia Postale, Carabinieri e Guardia di Finanza) e privati
- Casi di importanza nazionale come Buongiorno! Vitaminic e Telecom Pirelli Ghioni
- DEFT Linux project manager

DEFT

- Acronimo di Digital Evidence & Forensic Toolkit
- Progetto 100% made in Italy, nato in collaborazione con il corso di Informatica Forense dell'Università degli Studi di Bologna verso la fine del 2005...
- ... evolutosi nel 2007 come progetto indipendente mantenendo collaborazioni con l'Università di Bologna e IISFA Italian Chapter

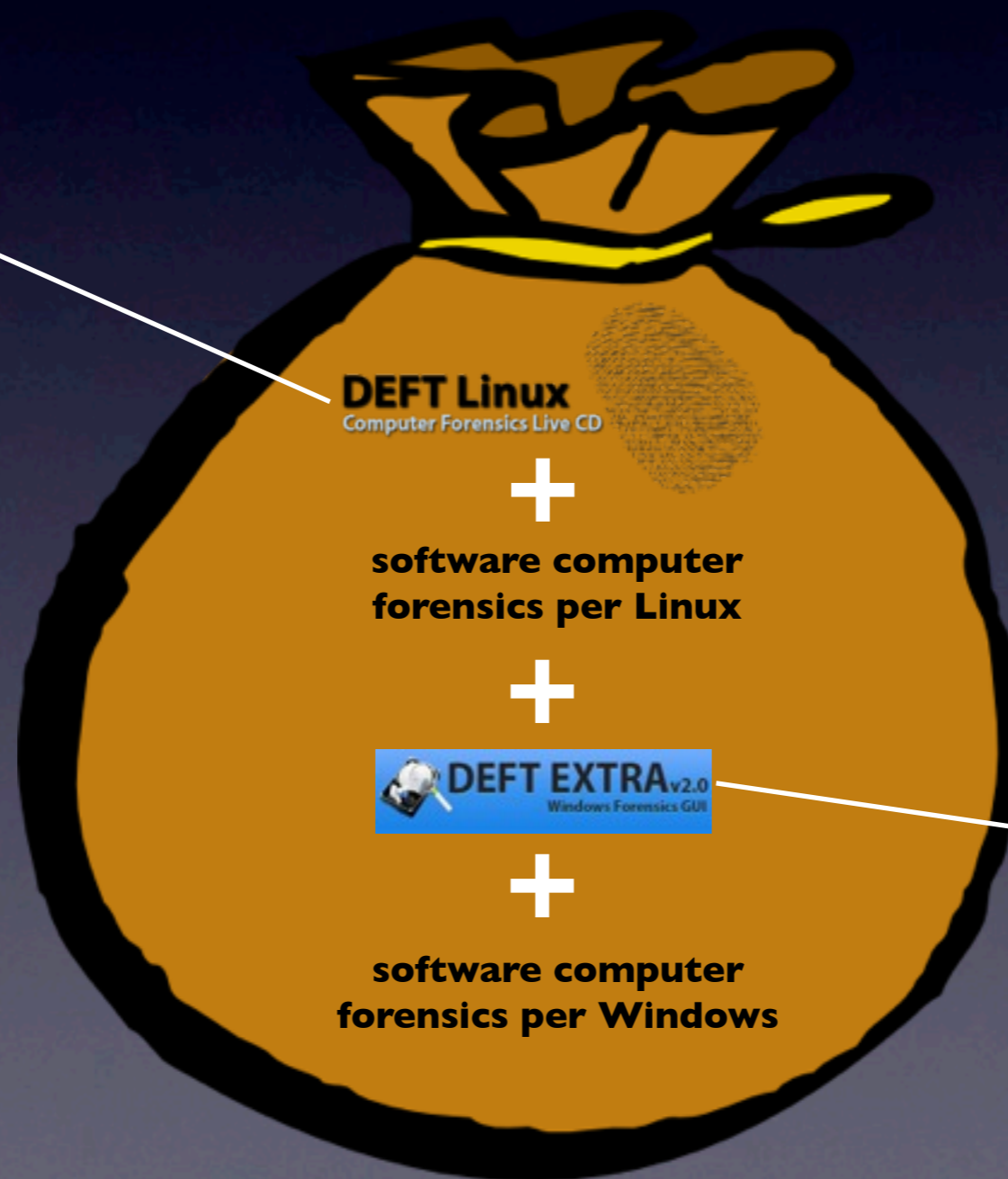
Un po di numeri...

- 5 anni di esperienza maturata sul campo
- Più di 195.000 download solo nel 2010
- Team composto da 6 persone di cui 3 sono specialisti in forza a compartimenti di Polizia Postale e Guardia di Finanza
- 447 utenti forum



DEFT come Forensic bag

Sistema Linux live che
mantiene inalterato il
contenuto delle memorie di
massa del sistema ospitante



Interfaccia grafica veloce
ed intuitiva per sistemi
Windows ideale per
l'esecuzione di attività di
pre analisi

Dove lo posso usare?

DEFT Linux: su tutte le architetture x86



DEFT Extra: su tutti i computer con Microsoft Windows

Dove non lo posso usare?



Mainframe



Architetture non x86



Cosa posso fare con DEFT?

Acquisizione di memorie di massa

Attività di analisi e pre-analisi

Recupero dati

Intercettazioni telematiche

Recupero password

Individuazione di malware e rootkit

DEFT Extra

- Interfaccia grafica per usi informatico forensi
- Raccolta di free software utili ad attività di analisi e pre analisi
- Eseguibile su tutti i sistemi Microsoft Windows a 32 bit (supporto a 64 bit non garantito al 100%)

Project manager: Salvo Tarantino

DEFT Linux 6

Principali novità

- Basata su LUbuntu 10.10 - collaborazione diretta con il maintainer del progetto
- Linux Kernel 2.6.35
- DEFT Extra 3
- Installer della distribuzione
- Wine per eseguire tool nativi Windows su Linux
- Documentazione ufficiale (FINALMENTE!)

DEFT Linux 6

Principali novità

- Xplico 0.6.1
- Dhash 2.2
- Sleuthkit 3.2
- Autopsy 2.24
- Log2TimeLine, Timescanner, Dtime e Regtimeline
- Software per la mobile forensic
- Xnview

Documentazione

- Per i primi mesi disponibile solo in Italiano
 - Traduzione in Inglese prevista entro la fine di marzo 2011
- Una serie di how-to per eseguire le principali attività informatico forensi
- Man page di tutti gli applicativi

Nel dettaglio...

DEFT installer

Requisiti minimi di sistema:

- Intel Pentium II, 64 MB ram in modalità testuale, 128 MB per la modalità grafica
- 4 GB di spazio disco

Requisiti ottimali di sistema:

- Cpu core duo, 512 MB, dischi SATA 7200rpm
- Almeno 10 GB di spazio disco

Nel dettaglio...

Wine per la CF

- ~~FTK imager 3~~
- WRR - Windows Register viewer
- Analisi della navigazione per IE, Firefox, Chrome e Opera
- Skypelog viewer
- Molti altri della suite DEFT Extra...

Nel dettaglio...

Xplico 0.6.1

- NFAT (Network Forensic Analysis Tool)
- Progetto tutto italiano, nato da un'idea di Gianluca Costa in collaborazione con DEFT Linux
- Ricostruzione completa dei contenuti intercettati usando come unica risorsa la capture eseguita
- Gestione di più casi (come Autopsy)

Nel dettaglio...

Xplico 0.6.1

- http, dns, tcp, udp - ipv4 e ipv6
- smtp, pop3 e imap
- ftp, sip
- ricostruzione di video, immagini, pagine web
- ricostruzioni in formato pdf delle stampe eseguite con stampanti di rete (protocolli IPP e PjL)
- Novità: Chat MSN

Nel dettaglio...

Xnview

- Creato da Gougelet Pierre-emmanuel
www.xnview.com
- Visualizzatore di immagini
- Supporta + di 400 formati di immagini
- Interfaccia grafica ottimizzata per la consultazione rapida o dettagliata delle immagini

Nel dettaglio...

Speciale Time Line

- Script per la creazione di time line con guida passo passo
- mactime
- log2timeline
- timescanner

Riferimenti

- <http://www.deftlinux.net>
- <http://forum.deftlinux.net>
- <http://distrowatch.com/table.php?distribution=deft>
- e-mail: info@deftlinux.net

Domande?

DEFT Linux
Computer Forensics Live CD



Dott. Stefano Fratepietro
stefano@deftlinux.net



Creative Commons Attribution-Non opere derivate 2.5

Milano, 22 ottobre - Smau 2010
Fiera Milano city