



Cybercrimes.it

Computer Forensics & Crime Informatico

Denis Frati

FCCU v.11.0

L'attenzione che fuori Italia si dedica alle problematiche legate al cyber crime è tanto maggiore, quanto maggiore è l'impegno degli organismi delegati a contrastarlo, non solo nell'attività operativa, ma anche nello sviluppo di nuovi metodi e strumenti utili alla lotta. In questo panorama lo sviluppo dell' "FCCU linux live-cd" è dimostrazione dell'attenzione volta dalla Federal Computer Crime Unit della Polizia Belga alle necessità degli operatori, al fine di consentir loro di operare con tools il più possibile aderenti alle specifiche esigenze ed ai propri profili e protocolli operativi.

Il cd è basato sul collaudato Knoppix live-cd, qui nella versione 5.01 con kernel 2.6.17.

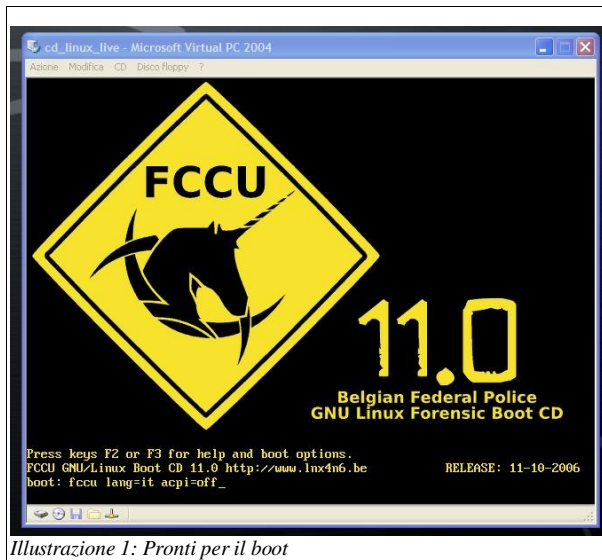


Illustrazione 1: Pronti per il boot

Ciò che colpisce, rispetto ad altre distribuzioni analoghe, è il ricorso quasi esclusivo a tools a riga di comando. Infatti, sebbene l'utente possa usufruire del classico windows manager Kde, il sistema si avvia con runlevel 3 presentando all'utente il prompt della shell.

La scelta, finalizzata a consentire una più ampia compatibilità hardware, (particolarmente utile nell'utilizzo su laptop con schede video non sempre supportate) giustifica quindi l'implementazione di tools privi di interfaccia grafica.

Nella fase di boot è possibile selezionare il layout della tastiera, tenendo presente che

quello di default è il belga. Se ci si scorda di questa opzione di configurazione si può intervenire successivamente dal prompt della shell con il comando `loadkeys it,us,ecc...` FCCU viene immediatamente in aiuto dell'operatore, procedendo, al termine della fase di boot, all'individuazione automatica dell'eventuale presenza di Host Protected Area (HPA) sull'hard disk della macchina in cui è in esecuzione.

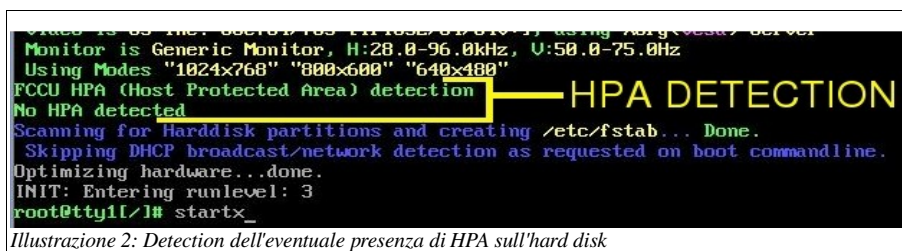


Illustrazione 2: Detection dell'eventuale presenza di HPA sull'hard disk

A differenza di altre distribuzioni linux live, l'utente è immediatamente loggato con i diritti di root, necessari per compiere gran parte delle operazioni utili all'attività forense, si tratti di acquisizione di immagini dei media, o di analisi vera e propria.

L'utente può usufruire della connettività di rete in modo estremamente semplice.

La presenza di una connessione di rete ethernet viene immediatamente riconosciuta e la scheda configurata, così come avviene per connessioni wireless ad access point non protetti da wep/wpa.

Bisogna tuttavia ammettere che il supporto alle schede ethernet più datate, o wi-fi integrate nei laptop, non è assoluto.

Esaminando l'elenco dei tools disponibili appare immediatamente evidente che ogni aspetto della forensics è stato preso in considerazione, sia per quanto riguarda i media che le reti.

Si ha quindi a disposizione software per l'analisi dell'hardware installato sull'host in esame, per l'acquisizione di immagini secondo il classico standard dd, o, allineandosi alle nuove

```
sh-3.1# metacam /media/sda5/home/nemo/DigiKam/A CASA/2007/PICT0301.JPG
File: /media/sda5/home/nemo/DigiKam/A CASA/2007/PICT0301.JPG
Standard Fields
-----
Image Creation Date: 2007:01:03 21:25:53
Make: CAMERA
Model: 4P-939
Software Version: Ver 1.11
X Resolution: 72 Pixels/Inch
Y Resolution: 72 Pixels/Inch
Image Description: Digital StillCamera
VCbCr Positioning: Datum Point
EXIF Fields
-----
Image Capture Date: 2007:01:03 21:25:53
Image Digitized Date: 2007:01:03 21:25:53
Exposure Bias: 0 EV
Exposure Time: 1/50 Sec.
Aperture: f2.8
Exif Image Width: 1600 pixels
Exif Image Height: 1200 pixels
Exposure Program: Program Normal
Exposure Mode: Auto Exposure
White Balance: Auto White Balance
ISO Speed Rating: 10 (50)
Metering Mode: Center Weighted Average
EXIF Version: 0220
FlashPix Version: 0100
Light Source/White Balance: Automatic
Flash: Flash Fired;
Aperture Value: f2.8
Max Aperture Value: f2.8
Shutter Speed Value: 1/50 9143 Sec.
ColorSpace: sRGB
Component Configuration: YCbCr
Digital Zoom Ratio: 100/100x
35mm Focal Length: 32mm
Scene Capture Type: Standard
Gain Control: None
Contrast: Normal
Saturation: Normal
```

Illustrazione 3: Estrazione dei metadati EXIF da un'immagine jpeg

tendenze procedurali, nel formato AFF, avendo anche a disposizione per dcfldd la gui di AIR.

Non mancano tools per il recovery, sia da hardware danneggiati che da file system (ntfs, fat, ext2). Le operazioni di data carving sono possibili sia nei confronti dei formati classici (foremost), sia mirate a specifiche tipologie, quali i file immagine in formato jpeg (recoverjpeg).

Per analizzare le immagini sono disponibili diversi software che consentono, oltre al già citato recovering, la visualizzazione in console mode e l'estrazione dei metadati EXIF, modalità particolarmente comoda che, differentemente dalle GUI, permette di reindirizzare l'output su file di testo allegabili

alla documentazione.

Tra i software implementati trovano ampio spazio i tools per il dump e il cracking delle password. Oltre ai classici strumenti per operare sulle password di MS Windows NT/2x/Xp, quali "chntpw" e all'italianissimo "sumdump2",

```
sh-3.1# bkhive2
bkhive2 from Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Usage:
bkhive2 systemhive keyfile
sh-3.1# sumdump2 /media/sda1/WINDOWS/system32/config/SAM /media/sda1/WINDOWS/system32/config/system>prova2.txt
Sumdump2 ncuomo@studenti.unina.it
This product includes cryptographic software written
by Eric Young (eay@cryptsoft.com)

No password for user Administrator(500)
No password for user Guest(501)
No password for user SUPPORT_388945a0(1002)
```

Illustrazione 4: Dump delle password utenti da MS Windows XP

troviamo strumenti per crackare le password dei sistemi MS Windows 9x (pur sempre in uso), del bios, dei file criptati con gpg, degli archivi zip e password cracker generici quali "John the ripper" e "crack".

Considerando la diffusione dei sistemi e della suite per l'ufficio di Microsoft, non potevano mancare software che consentissero di analizzare, in ambiente non nativo, i file di sistema e le estensioni proprietarie della casa di Redmond.

Per l'analisi dei file di registro, FCCU non implementa "RegViewer", presente in altre note

```
Offline Registry File Parser, by Harlan Carvey
Version 1.1. 20060523

\\$$$PROTO.HIV
LastWrite time: Fri Mar 2 01:27:21 2007
\\$$$PROTO.HIV\ComputerAssociates
LastWrite time: Tue Feb 6 14:51:38 2007
\\$$$PROTO.HIV\ComputerAssociates\ISafe
LastWrite time: Tue Feb 6 14:51:38 2007
--> InterfaceDllPath; REG_SZ; C:\WINDOWS\system32\ZoneLabs\isafeif.dll
--> EngineDllPath; REG_SZ; C:\WINDOWS\system32\veted.dll
--> EngineDataPath; REG_SZ; C:\WINDOWS\system32\ZoneLabs
--> ArcLibDllPath; REG_SZ; C:\WINDOWS\system32\ZoneLabs\arclib.dll
--> Enabled; REG_DWORD; 1
```

Illustrazione 5: Analisi dei file di registro

distribuzioni con le features della gui non sempre funzionanti, ma si avvale di “reglookup” e dello script in perl “regp.pl”.

```
String      : Product: GFI LANguard Network Security Scanner --
String      : (NULL)
String      : (NULL)
String      : (NULL)
---
[Header part]
Record number      : 87
Time generated     : Sat Feb 10 01:01:59 2007 local (Sat Feb 10 00:01:59
Event ID          : 11707 (no description)
Event type        : 4 (Information)
Event category     : 0 (None)
---
[Body part]
Event source      : MsiInstaller
Computer         : NAUTILUS
Sid              : S-1-5-21-2159741093-338363475-3955426747-1006 (um
---
[Strings part]
String           : Prodotto: OpenOffice.org 2.0 -- Processo di insta
String           : (NULL)
String           : (NULL)
String           : (NULL)
```

Illustrazione 6: Analisi dei file di log

Il registro degli eventi di MS Windows può essere analizzato in modo dettagliato, reindirizzando nel caso l'output della shell in file di testo, grazie ai tools “grokvt” ed “fccu.evttreader”, consentendo, per esempio, di provare l'installazione di specifici programmi o il login, in un dato momento, di un utente piuttosto che un altro.

FCCU rappresenta una piacevolissima sorpresa per l'implementazione di tools dedicati all'analisi dei files con estensioni proprietarie di Microsoft leggeri ed ottimamente funzionanti. Visionando il menù di Kde si nota immediatamente l'assenza della suite OpenOffice, recentemente implementata in parte in Helix.

FCCU non ne risente in modo eccessivo, avvalendosi di software per estrarre le immagini dalle presentazioni in MS Power Point e di anitword, tools per visualizzare nella shell il contenuto dei files di MS Word.

```
Starting a Campus Tradition
A Graduation Pledge of Responsibility

By William Ihne

Foreword

Let's just say you woke up one morning, after a night of discussing
the plight of the world's fate with folks from a wide range of
fields, and expertise. For example, your company may have included:
a marine biologist, a chemist, a pastor or rabbi or both, a
professor of philosophy and literature, a master of the violin, a
member of the Science Board for the military, and thirty young
students that have become aware of the major issues of our time;
those issues that will play out in their futures. Those students,
home schooled and otherwise, between the ages of 18-25, would
certainly have some questions. What could an older adult learn from
them? What could the violinist teach the chemist, and vice versa of
each participant? And what if upon waking, you decide that you're
going to make a commitment to one part affecting the futures of
those young people? Where would you begin?
```

Illustrazione 7: Antiword in azione, un file di MS Word visualizzato nelle shell

Troviamo, inoltre, strumenti per l'estrazione delle e-mail e degli allegati dagli archivi di posta elettronica di Outlook Express. Sebbene questi strumenti non rappresentino una novità all'interno delle distribuzioni per la computer forensics, va notato come a differenza di altre distribuzioni, quali Helix, in FCCU questi strumenti funzionino perfettamente.

Altra particolarità di cui gli sviluppatori di FCCU hanno merito è quella di aver per primi implementato strumenti di analisi per Firefox, web browser che sta trovando sempre maggior spazio tra gli internauti.

```
<?xml version="1.0" standalone="yes"?>
<cachedata>
  <autocomplete file="/media/sda5/home/nemo/.mozilla/firefox/8dqtqkut.default/formhistory.dat" time=
  "Sat Feb 09 2007 16:02:25">
    <field name="Email">
      <saved>denisfrati@... it</saved>
    </field>
    <field name="TELEFONO">
      <saved>392...</saved>
      <saved>392...</saved>
    </field>
    <field name="USR">
      <saved>denisfrati...</saved>
      <saved>denisfrati...</saved>
    </field>
    <field name="accesscode">
```

Illustrazione 8: Dump della chace di autocompletamento di Mozilla Firefox

Sono infatti presenti due script per il dump della cronologia e della cache di autocompletamento di Firefox.

Per la network forensics è disponibile un'ampia scelta di software per l'analisi, la scansione e la cattura del traffico in transito nelle reti.

Oltre ai tools più classici, quali Ethereal, Ettercap, TcpDump, Sniffit, ecc... sono presenti tools per sniffare i dati scambiati tra programmi di messaggistica istantanea e su reti wireless, per testare la sicurezza di reti wi-fi, per estrarre le immagini in transito su un'interfaccia di rete e molto altro.

Non mancano poi software per ricercare virus, rootkit e malware, in particolare strumenti per l'individuazione di questi ultimi, quali nepenthes e mwcollect (non più supportato), rappresentano una novità all'interno di distro dedicate alla forensics.

Concludendo si può affermare che FCCU rappresenta una valida alternativa a live-cd più conosciuti e rinomati.

Purtroppo sul sito di riferimento (<http://www.lnx4n6.be>) è disponibile solo una scarsa documentazione relativa allo svolgimento delle più comuni e basilari attività di forensic: wiping dei supporti di destinazione, acquisizione di un immagine con AFF, ecc....

Si sente, inoltre, la mancanza di un qualsiasi supporto, non è infatti presente né il forum, né una documentazione dettagliata riguardante i tools meno conosciuti.