Resurse Open Source în Computer Forensic

18 Mai 2007

Cezar Spatariu Neagu

Agendă

- Cine sînt eu?
- Ce este Computer Forensic?
- De ce Computer Forensic cu ajutorul tool-urilor Open Source?
- Distribuții, tool-uri şi resurse.
- Implicații legale.
- Întrebări, răspunsuri, discuții.

Ce este computer forensic?

Computer forensic is application of the scientific methods to digital media in order to establish **factual** information for juridical review.

- Fapte penale:
  - Îndreptate împotriva unui calculator.
  - Unde calculatorul conține probe.
  - Unde calculatorul este instrument în comiterea infracțiunii.

De ce computer forensic?

- Cine sînt tipii răi?
- Ce s-a intîmplat şi cînd?
- De ce s-a intîmplat?
- **Ce putem face să nu se mai întîmple?**

De ce open source ?

One of the questions I hear most often is: “why should I use Linux when I already have [insert Windows GUI forensic tool here]?” There are many reasons why Linux is quickly gaining ground as a forensic platform. I’m hoping this document will illustrate some of those attributes.

- Control – not just over your forensic software, but the whole OS and attached hardware.
- Flexibility – boot from a CD (to a complete OS), file system support, platform support, etc.
- Power – A Linux distribution is a forensic tool.

“The Law Enforcement and Forensic Examiner's Introduction to Linux A Beginner's Guide” NASA

Computer Forensic înseamnă:

- Prelevarea datelor.
- Analiza probelor.
- **Documentarea întregului proces.**

Probleme

- *‚To pull or not the cable?‘. This is the question.*

- Offline Forensic
- Online Forensic
  - Root-kit-uri, criptoviruşi, malware (memory resident),
  - Medii criptate.
  - Sisteme ce nu pot fi oprite.

Starea sistemului este modificată.DOCUMENTEAZĂ!

Proprietăți

- O distribuție (LiveCD) poate fi folosită dacă:
  - NU modifică sistemul de unde se prelevează.TESTEAZĂ!(vezi Knoppix)
  - Suportă un spectru larg de controlere.
  - Oferă programe (shell-uri şi binaries) pentru prelevare de probe online.
  - Oferă sisteme de logging pentru documentarea procesului de forensic.

Tool pentru prelevare

- nc, hdparm, fdisk, mmls, lshw, cat /proc/…
- dd if=/dev/victimaHDD_MEM of=/media/caseNr.dd
- dclfdd if=/dev/victimaHDD_MEM of=/media/caseNr hash=sha1sum hashlog=/media/CaseNr/image.hash
- sha1sum ori md5sum?
- aimage (AFT Tools)
- ☹linen (*EnCase Image Acquisition Tool*)

Tool-uri pentru analiză

- **file, strings, scalpel,foremost** (reconstituie fisiere)
- **Autopsy** (integrare cu NSRL), **PyFLAG** (case management)
- **Sleuthkit ,Faust** (analiza binary si shell script-uri)
- **Antivirus** (ClamAV. F-Prot)
- **Rootkit detector** (chkrootkit, rkhunter)
- **Stego** (Outguess, Stegdetect)
- **libewf** Expert Witness Library - Encase

Windows World

- **Regviewer** – Registry Viewer
  - (share-uri accesate, device-uri conectate, timeline, useri)
- **GroKEVT** – analiza Windows Event View
- **Rifiuti** – analiza Recycle BIN
- **fcrackzip**
- Internet Explorer
  - **pasco** index.dat
  - **galleta** cookie
- Firefox
  - **mork.pl**

Live CD-uri

- HELIX (http://www.e-fense.com/helix/)
  - Windows, Linux, (Solaris☹) online forensic
  - Live CD
- FCCU GNU/Linux Forensic Boot CD
  - Live si analiza CD
- DEFT (http://www.stevelab.net/deft/)
- ASRData (http://www.asrdata.com)

Şi nu uita-ți de optiunea „noswap“ în grub!!

Implicații Legale

- Orice caz trebuie tratat corespunzător.
- Legislație ??? (Ministerul de Justiție, Interne)
- Competența examinatorului (certificări)
  - SANS
  - International Association of Computer Investigative Specialists (IACIS)
  - The International Society of Forensic Computer Examiners - ISFCE
  - etc.

Resurse

Documentații şi proiecte

- Open Sourse Digital Forensic http://www.opensourceforensics.org
- Honeynet Project http://www.honeynet.org
- ForensicWiki http://www.forensicswiki.org
- **Computer Forensics Tool Testing** http://www.cftt.nist.gov/

Live CD-uri

- Helix http://www.e-fense.com/helix
- FCCU http://www.lnx4n6.be/

Informații

- Prezentare va fi disponibilă pe site-ul:
  - http://eliberatica.ro
  - http://securityaspects.wordpress.com
- Contact

  cezar (.) spatariu (at) gmail (.)com
- Şi nu uitați:

Not all „BAD GUYS“ are from ROMANIA☺