Open Source applied to Computer Forensics

Presentation by Mr. Andrea Ghirardini
United Nations
Interregional Crime and Justice Research Institute (UNICRI)
ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States (CIS) – Sofia, Bulgaria – 9 October 2008

unicri
advancing security, serving justice, building peace

Open Source: Why?

unicri
advancing security, serving justice, building peace

Open Source should be used in Computer Forensics for many different reasons:

✓ In the back-office it's useful to build an enterprise level lab with a very low investment. You may use many interesting technologies which are far better than commercial ones (AFS, for example)

✓ The above helps emerging countries and States with a low dedicated budget

✓ When you need to perform analysis you find that open source software is often updated faster than others

✓ GNU/Linux is the best Computer Forensics environment in the world, without any doubt

Open Source in the Back-office I

unicri
advancing security, serving justice, building peace

A Computer Forensics Lab has many different needs:

✓ You need HUGE storage (our lab has > 40 TB), but you don't want to spend everything in SAN/NAS/whatever

✓ You need to keep data secure but you need to give local root (or Administrator) password to every single computer forensics expert

✓ You need to work with many different platforms

✓ These needs don't coexist very well

✓ We had many troubles trying to work with these problems

✓ We tried many technologies:

- NFS
- SMB
- NFS v.4
- Coda

Open Source in the Back-office III

unicri
advancing security, serving justice, building peace

- ✓ OpenAFS solved all the troubles at once!
- ✓ It has:
  - ➢ Strong Authentication (Kerberos V)
  - ➢ Client and server for more than 20 different platforms
  - ➢ Replication
  - ➢ Surpass the concept of "file server" (cell)
  - ➢ Backup
  - ➢ Strong encryption
  - ➢ Central management
  - ➢ Works well also with low band

unicri
advancing security, serving justice, building peace

✓ With OpenAFS we work with cheap hardware and we are able to scale up without a single problem

✓ At the present we have:

- 1 Cell (lab.atpss.net)
- 10 File Servers
- > 40 Tb of data
- 1 Site

✓ In a very near future we'll able to scale up to :

- 3 Sites (1 Research Lab and 2 operating ones)
- 1 Cell
- > 100 Tb
- > 20 File Server

Everything without changing actual systems but simply adding new components to the system

Linux as Computer Forensics OS I

unicri
advancing security, serving justice, building peace

✓ GNU/Linux is unique operating system

✓ Yes, there are many other open source operating systems but only GNU/Linux has:

- Support for more than 18 types of partition schemes
- Support for more than 40 file systems

✓ GNU/Linux is also useful because it's:

- Reliable
- Affordable
- Very good hardware support

✓ And, last but not least ... it does what you are asking for (no wizards, helpers, whatsoever)

unicri
advancing security, serving justice, building peace

✓ **You have also many other interesting technologies:**

- **Loop devices**
- **Software RAID**
- **Wine**
- **Bond devices**
- **Libpcap**

unicri
advancing security, serving justice, building peace

✓ On the top of GNU/Linux and its features you'll find a world of computer forensics programs to perform (for example):

- Bitstream copy
- Hash validation
- Analysis
- Network Forensics
- Reverse engineering
- RAM Dumping
- ... many others ...

Linux as Computer Forensics OS IV

unicri
advancing security, serving justice, building peace

✓ Are you scared about all these things?

✓ Don't worry there are Computer Forensics Distributions!

✓ Helix Knoppix: recently updated (no more than 2 weeks ago), it's one of the best computer forensics distro in the world. It's a Live CD useful both to copy and inspect computer systems

✓ DEFT: A true "Italian job" by Stefano Fratepietro and Andrea Ghirardini. Ubuntu based (like the new Helix), it's a Linux Live CD with everything you need to perform forensics analysis

✓ DEEEFT: A SD-CARD distribution (by Andrea Ghirardini). With DEEEFT you can turn an eeepc in a compact forensics machine. A little lab in 1.1 Kg!

Open Source in Analysis

unicri
advancing security, serving justice, building peace

✓ **There is also profound reasons to use Open Source Software for forensics analysis:**

- **Availability: Software is always "on the net" you can find also a obsolete version years later**
- **Open Format: Open source means open formats. You always convert an open source file format in an other one... (Try to read a very old .doc file if you can...)**
- **Double check: The oppose side can check every step of your analysis if you use (and produce) open source software. This is not true if you need a many-thousand-dollar software...**
- **Transparency: Commercial software is a black box. Open source software can be checked without any problem**

unicri
advancing security, serving justice, building peace

That's all!

Any questions?

unicri
advancing security, serving justice, building peace

Do you want to contact me?

E-Mail andrea@atpss.net

Mobile: +39 392 1101101
Office: +39 011 3272100