- Key Note -
Digital Forensics:
Experiences from the Past,
Issues from the Present
and
Challenges for the Future

Raoul “Nobody” Chiesa

United Nations Independent Advisor on Cybercrime @ UNICRI
European Network & Information Security Agency (ENISA) PSG Member
Founder, President, The Security Brokers

The International Conference on Digital Forensics
and Investigation (ICDFI) 2012.

September 22nd, 2012 - Beijing, China
Agenda

• Introductions: who am I, where I work at?
• Entering the Digital Forensics age
• The past
• The present
• The Future
• Conclusions
• Contacts, Q&A
Disclaimer

• The views expressed are those of the author and speaker and do not necessarily reflect the views of UNICRI, ENISA and its PSG, neither those companies and security communities I’m working at and/or supporting.

• Registered brands belong to the owners.

• This presentation will not endorse any commercial products, while it may give out comments and feedbacks on some of them.
Introductions
Who am I?

Raoul Chiesa

- Founder, Partner, The Security Brokers
- Principal, CyberDefcon UK
- Senior Advisor on Cybercrime at UNICRI (United Nations Interregional Crime & Justice Research Institute)
- PSG Member, ENISA (Permanent Stakeholders Group, European Network & Information Security Agency)
- Founder, Member of the Steering Committee and Technical Board, CLUSIT (Italian Information Security Association)
- Steering Committee, AIP/OPSI, Privacy & Security Observatory
- Board of Directors, ISECOM
- Board of Directors, OWASP Italian Chapter
- Founder, Owner, @ Mediaservice.net
Some books I wrote, co-authored or helped out
About UNICRI

What is UNICRI?

United Nations Interregional Crime & Justice Research Institute

UNICRI was established in 1967 and opened in 1968: it is one of the 5 global Research and Training Institutes of the United Nations which report to the UN Secretary General (UNICRI, INSTRAW, UNRISD, UNITAR, UNIDIR).

UNICRI’s goal is to support countries worldwide in crime prevention and criminal justice.

UNICRI carries out applied research, training, technical cooperation and documentation / information activities

UNICRI disseminates information and maintains contacts with professionals and experts worldwide

Emerging Crimes Unit (ECU): Organized Crime and Corruption, Counterfeiting, Cybercrimes, Trafficking in Human Beings, Youth, Drugs, Eco-Crime
United Nations Training Campus in Turin, Italy
**About ENISA**

**What is ENISA?**

- **European Network & Information Security Agency**
- ENISA is the **EU’s response to security issues** of the European Union
- “Securing Europe's Information Society” is our motto (27 Member States)
- In order to accomplish our mission, we work with EU Institutions and Member States
- ENISA came into being following the adoption of Regulation (EC) No 460/2004 of the European Parliament and of the Council on 10 March 2004. Operations started on September 2005, after moving from Brussels to Crete, and with the arrival of staff that were recruited through **EU25-wide competitions** with candidates coming from all over Europe.
- ENISA is helping the European Commission, the Member States and the business community to address, respond and especially to prevent Network and Information Security problems.
- The Agency also assists the European Commission in the technical preparatory work for updating and developing Community legislation in the field of Network and Information Security.
- I’m a Member of ENISA’s PSG – **Permanent Stakeholders Group**.
Entering the Digital Forensics age
What is Digital Forensics?

Digital Forensics is the science about how to obtain, preserve, analyze and document digital evidences from electronic devices such as: Servers and PCs, Tablets, PDAs, fax machines, digital cameras, iPods, Smartphones (Mobile Forensics) and all of those storage devices.
DF Key Phases

Computer Forensics phases:

- **Identification, Collection** and **Acquisition**;
- **Preservation** (Chain of Custody);
- **Analysis**: extracting those data significant to the investigation;
- **Evidence Presentation**: it’s the final and the most important phase, during which not-experts are capable as well to understand the job which has been done (think about Lawyers, Prosecutors, Judges, etc...). It’s a good practice to write down a document (Report) in which all of the gained data and its extracted results are analyzed and explained, step by step.
DF Expert skills

• Very often people ask me “which skills a Digital Forensics Expert should have?”

• The answer is not just a single one!

• A DF **real** expert should be a mix of:
  – Academic background
  – System Administrator (on different Operating Systems: Microsoft Windows, Apple IOS, *NIX, *BSD, legacy systems – and as many Filesystems as you can!)
  – Network Security Expert
  – Law Enforcement Officer/Investigator
  – Incident Handling Expert
  – Hacker (Ethical!)
  – Curious
  – (sometimes) be a **lucky man**... (you’ll see this later)
  – Possibly not married 😊
Digital Forensics in the Past

- Learn from the past
- Live in the present
- Believe in the future
The origins

• In the past (‘80s, ‘90s), DF was nearly an unknown science.
• The reason was very simple: computer “incidents” (anomalies, frauds, hacks) were just not so common!
• Among the very first DF analysis we can find the world-famous one by Clifford Stoll as reported in the book The Cuckoo’s Egg (1989)
Common issues (general view)

1. Lack of knowledge
2. Law Enforcement behaviors
3. Costs
4. Lack of resources & Being “alone”
5. A case study from 1995
Common issues: lack of knowledge

• As described in the book, among the main issues, we can find out:
  – Lack of **methodologies** and standard approaches
  – Lack of **tools** (hardware, software)
  – **Evolution of the hardware** VS the available investigative resources at that time (i.e. modem interception and devices speed/baudrate)
  – Lack of **experts**!
Common issues: Law Enforcement

• Seizes
  – Mousepads & monitors ?!?  
  – Chain of Custody
• Lawyers, Public Prosecutors and Judges
  – How’s the know-how of these actors in China nowadays?
• DF seen only on "computer crimes" cases (i.e. hacking)
  – Today DF can be applied to murders, kidnappings, child pornography, financial frauds, hacking incidents, insider trading, etc..
• No understanding of the basic terms (i.e. "hard drive", network, “Internet”…)
  – Nowadays (at least!) most people know what these words means (or they should…).
Common issues: costs

• The costs have always been one of the main issues when dealing with DF.
  – HW devices and SW solutions were definitely not “cheap” (this is still a problem, tough)
  – Forensics Experts costs VS Court Trial salaries
    • In Italy the fee defined by the Law Court for a DF Expert is equal to EUR 30 per day – *travel expenses included!!* (1 EUR = 8.2 RMB -> 246 RMB)
    • Well.. We do not pretend to “become rich”, right? ....While not even to loose money while working 😞
Common issues: being alone

• Ahead of the Internet boom, there were no “forums” or “boards” where somebody could ask for help.

• DF experts were very few ones...
  – Each one with its own “little garden” (*not loving* to share knowledge and experiences)

• The main issue here was the lack of people with whom *compare experiences and troubles*
  – Not even speaking about tools and shell scripts sharing!
Common issues: a case study (1995)

• On December 13\textsuperscript{th}, 1995, the SCO (Central Operative Section of the National Police of Italy) entered at 6AM into an apartment in Turin, Italy.

• Since SCO’s experience was related to Organized Crime (Mafia) and murders only, their knowledge of DF was equal to zero 🙁
Common issues: a case study (1995)

• They sized **everything**:  
  – Personal Computers (OK)  
  – Floppy disks (OK)  
  – CD-ROMS (OK)  
  – General HW: modems, cell phones (not OK, OK)  
  – Paper agendas, notepads (OK)  
  – Printouts (OK)  
  – Mouse (not OK)  
  – Mousepads (not OK!!)
Common issues: a case study (1995)

• Furthermore, the DF analysis was executed as follows:
  – No Chain of Custody (not OK)
  – Manual signatures of the “tree” command printout (+1000 pages....) from the MS-DOS shell (not OK)
  – The “expert” hired from the Police (local University of Turin) directly connected the suspect’s hard drive (HP 5” ¼ 2 GB size) to its PC (not OK)
  – He wrote his report directly on the suspect’s hard drive (not OK)
  – Generally speaking, the whole DF analysis has been carried on in a “home-made” way -> very unprofessional!
Digital Forensics in the Present

The Present
Today’s Digital Forensics become a mix of issues and never-ending, unexpected “news”

1. Host (Intel, Motorola, Mainframes, ...), Network, Mobile, GPS Navigator’s Forensics
2. “Weird” forensics (see next)
3. Common issues (see later)
4. Forensics Labs?
5. Mobile Forensics
6. Encryption
7. A recent case study on Child Pornography & the Investigation Approach
“Weird” DF

• During my career the DF teams I worked with encountered a lot of “weird” requests
  – Sun Solaris Enterprise 10000
  – VAX/VMS
  – Sony Playstation, XBOX
  – Cloud Forensics (we’ll speak about this later)
  – Web Applications-related hacking crimes
Common issues

• There are a lot of issues when dealing with DF nowadays.
  – *Operating logistics* + geographically distributed DF teams (when executing seizure operations for/with the Law Enforcement)
  – Too many competitors VS few real experts (proofing a effective and real field experience)
  – The “Big 4” joined in (from financial fraud analysts to DF experts)
  – HW&SW cannot replace human brains (i.e. Encase won’t fix all of your problems!; you do not mandatory need a write blocker device!!)
  – Needed HW&SW is (still) too expansive 😞
Digital Forensics Lab(s)

• Building a DF lab means *technologies*, not products!

• Some people think that you *just can buy the right spare parts*. It’s like a “shopping list”:
  ✓ A PC with Encase
  ✓ “Some” Write Blockers
  ✓ “Some” Terabytes
  ✓ A software for mobile forensics + expansive CelleBrite UFED suitcase
  ✓ That’s it, ready to go!
Digital Forensics Lab(s)

• This kind of approach it’s not totally wrong, but ...
  – your operating system is your enemy
  – you are tied to the limits of your software
  – you could became an “expert” using Encase/”UTK/FTK”/whatever but you are lost outside of your “environment”
Operating system troubles

- Microsoft Windows is a desktop operating system (oh, really ?? ;)
- It tries to help you (I said “it tries”, blue screen, viruses, malware, DLLs troubles are just some “incidents”).
- It doesn’t care about “changing the evidence” (?), “reading external media”(?), “mounting read only”(??), and so on...
- If you choose Windows, your operating is your first enemy. First of all you have to defend yourself from it.
- You need specific software/hardware to do this.
Digital Forensics Lab(s)

- You could have bought the best software in the world but the possible variations are TOO MANY, not mentioning our old friend Mr. Murphy ;)
  - Exotic architecture (just a simple AS/400 is enough sometimes)
  - Strange cases (not just those “easy-to-process” child pornographic file exchanges)
  - Software “ad hoc”
  - New technologies
Digital Forensics Lab(s)

• Investigations are becoming bigger and wider

• Today’s home user’s hard drives are huge
• Sometimes you have to collect (and deeply analyze!) dozens of computers to reach the evidence of a crime
• Spreading data over dozens of external drives/server/whatever is dangerous and will slow down all your work
• Also, “some machines” linked up together won’t be enough...
Digital Forensics Lab(s)

• You must buy a back-end:
  – One or more server
  – You must upgrade your software to some sort of “enterprise edition”
  – You must choose between “having more servers but paying expensive licenses” or “saving license’s money and investing for a big server with an huge storage (SAN)”
Building a Digital Forensics Lab

• So we tried to *plan a new approach* for a computer forensics lab
• Our guidelines were:
  – Opening to every kind of digital evidence
  – Opening to raw or well documented formats
  – Opening to new technologies
  – Open Source everywhere (where possible)
  – Cheap hardware
  – Security
  – Redundancy
Building a Digital Forensics Lab

• First, we looked for the technologies:
  – GNU/Linux
  – OpenAFS
  – Live-CD Linux distributions (i.e. DEFT from Italy, with a Chinese-language installation guide: download it!!! - http://www.deftlinux.net/)
  – Cheap Hardware
Building a Digital Forensics Lab

• GNU/Linux:
  – It’s Unix: it’s stable, it does what YOU want and not what *it wants*, it doesn’t have wizards, witches, goblins or so on...
  – It has the best filesystem support all over the world: it can mount more than 40 different filesystems, it supports more than 18 partition schemas
  – It has the widest hardware support in the world, a very good one
  – Oh, *it’s free!*
Building a Digital Forensics Lab

• It’s true: you can’t build a (real) computer forensics lab without a huge repository

• You have some choices
  ✓ A big server with a SAN connected through a Fiber Channel or iSCSI
  ✓ Some different servers
Building a Digital Forensics Lab

• One big server with a SAN it’s a good solution but has some drawbacks:
  – You have only one machine. If you need to work on many cases you can exhaust its resources if you are working “server side”
  – On the other hand if you work client side, you could get old while waiting for the files to transit on cable
Building a Digital Forensics Lab

• The best solution should be having *some application servers* in the back-end *working directly on the data* (motherboard’s bus are faster than networks)

• But there are some troubles:
  – If you split data on various server *it’s hard to find* everything you need
  – It’s hard to find *sharing protocol smart enough*...

  • NFS is horrible: it’s too server oriented, it hasn’t good security (NFS stands for “Not For Security” as I often love to remind to my collagues ;)
  • SaMBa is too complex to administer, it has security problems, it doesn’t scale up well, it’s too tied up with Microsoft’s humors...

• So, we went hunting for something that would eventually fit our (weird, very specific) needs 😊
Building a Digital Forensics Lab

• OpenAFS is an amazing technology!

• It’s a unique network filesystem
  – It was born as academic project (1989!)
  – IBM owned it for 10 years
  – It’s Open Source since 2001
  – It’s used worldwide... Fortune 500, IBM, CERN, IHEPs, Universities... more than 250 public cells on the Internet...
Building a Digital Forensics Lab

- OpenAFS is a global, federated, location independent open source storage system that provides pervasive data access from a broad range of heterogeneous devices scaling from handsets to super computers.
Building a Digital Forensics Lab

- Broad platform support
  - UNIX
    - MacOS 10.3-10.8, Solaris (Sparc and x86) 7-11 and OpenSolaris
    - AIX 5.1-5.3; HPUX 11.0, 11i, 11i v2, 11i v3; IRIX 6.5;
    - NetBSD, FreeBSD and OpenBSD (server only)
    - Linux 2.4 and 2.6 (through .24) kernels
    - Fedora Core 3-7, RHEL3-5, Debian and others
    - Microsoft Windows
  - 250 Public Cells (and an increasing number of known private cells)
  - Growing number of developers
  - Partnerships with academic CS departments
Building a Digital Forensics Lab

• **OpenAFS Strengths**
  – Unified named space (like “CIFS”: but it works ;-)P)
  – WAN friendly
  – NAT capable
  – Authentication, Authorization, and Auditing
  – Change notifications
  – Distributed administration
  – High availability
  – Maintenance without downtime
  – Data consistency
# Building a Digital Forensics Lab

- A simple comparison (from 2009)

<table>
<thead>
<tr>
<th>CRITERIA</th>
<th>OPENAFS</th>
<th>OPENAFS NOTES</th>
<th>LUSTRE</th>
<th>LUSTRE NOTES</th>
<th>NFS V4</th>
<th>NFS V4 NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single namespace</td>
<td>Yes</td>
<td>Defaults to /afs.</td>
<td>No</td>
<td>Planned for 1.8.</td>
<td>Extension</td>
<td>Not widely available.</td>
</tr>
<tr>
<td>Access Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>File</td>
<td>Superset of POSIX acls.</td>
</tr>
<tr>
<td>Distributed Architecture</td>
<td>Yes</td>
<td>Limited support for serving any (existing) filesystem.</td>
<td>Yes</td>
<td>Serve from up to 400 Object Storage Servers.</td>
<td>Yes</td>
<td>Can serve any filesystem.</td>
</tr>
<tr>
<td>Server platform support</td>
<td>Broad</td>
<td>Windows servers available but not supported</td>
<td>Linux</td>
<td>Solaris planned.</td>
<td>Broad</td>
<td>Hummingbird Maestro Windows Server</td>
</tr>
<tr>
<td>Volume Management</td>
<td>Yes</td>
<td>Transparent movement of</td>
<td>No</td>
<td>Online data migration</td>
<td>Extension</td>
<td>Not always available</td>
</tr>
<tr>
<td>Filesystem snapshots</td>
<td>Limited</td>
<td>Typically one “backup”.</td>
<td>No</td>
<td>Planned for 3.0.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Quotas</td>
<td>Yes</td>
<td>Granular to container (“volume”) level.</td>
<td>Yes</td>
<td></td>
<td>No</td>
<td>Implemented by the backend.</td>
</tr>
<tr>
<td>POSIX Extended Locking</td>
<td>No</td>
<td>Planned.</td>
<td>Yes</td>
<td>No lockf/flock yet.</td>
<td>Yes</td>
<td>Mandatory and Advisory.</td>
</tr>
<tr>
<td>Transport</td>
<td>Advisory</td>
<td>Whole file only.</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Replication</td>
<td>UDP IPv4</td>
<td>TCP support planned.</td>
<td>TCP IPv4</td>
<td>TCP</td>
<td>IPv6 not widely available.</td>
<td></td>
</tr>
<tr>
<td>Disconnected Mode</td>
<td>Yes</td>
<td>Read-Write planned.</td>
<td>Local</td>
<td>RAID, not multi-server yet.</td>
<td>Extension</td>
<td>Not widely available.</td>
</tr>
<tr>
<td>Object Storage</td>
<td>No</td>
<td>In progress</td>
<td>No</td>
<td>Planned for 1.8.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Location Transparency</td>
<td>Yes</td>
<td>Even cross-installation.</td>
<td>Yes</td>
<td>Location of Object Storage Servers is transparent.</td>
<td>No</td>
<td>Referrals offer limited functionality.</td>
</tr>
<tr>
<td>Security</td>
<td>Yes</td>
<td>56 bit crypt.</td>
<td>No</td>
<td>Planned for 1.8.</td>
<td>Yes</td>
<td>GSSAPI RPC.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Yes</td>
<td>Kerberos 4 and Kerberos 5.</td>
<td>No</td>
<td>Kerberos support in Lustre</td>
<td>Yes</td>
<td>GSSAPI / Kerberos 5.</td>
</tr>
<tr>
<td>Multiplatform</td>
<td>Yes</td>
<td>Windows, Mac, Linux, most Unix variants.</td>
<td>No</td>
<td>Limited Windows pCIFS client. No Mac client yet.</td>
<td>Yes</td>
<td>Proprietary Windows client; Not in MacOS</td>
</tr>
<tr>
<td>Scalability</td>
<td>Yes</td>
<td>Thousands of clients per server in practice.</td>
<td>Yes</td>
<td>30000 clients per node.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Open Source</td>
<td>Yes</td>
<td>IBM Public License V1.0.</td>
<td>Yes</td>
<td>GPL.</td>
<td>Available</td>
<td>Citi reference implementation is GPL.</td>
</tr>
</tbody>
</table>
Building a Digital Forensics Lab

• From a DF point of view:
  ✓ Building an HUGE repository with common hardware
  ✓ Easy to find everything
  ✓ Secure!
  ✓ No downtime
  ✓ Replication (see above)
  ✓ Works well with BIG files
  ✓ Works well with various architectures
Building a Digital Forensics Lab

• We built **two different Labs** with OpenAFS:
  – Every single machine works both as a *OpenAFS node* and as an *analysis workstation*
  – Every single computer is reachable through **SSH**, also with graphics (X-Window)
  – *FreeNX* is another interesting technology:
    • Works well with low bandwidth
    • It has the concept of “suspension” and “detached session”, like *screen*
Mobile Forensics

• As previously stated, Mobile Forensics is (already) the new DF’s frontier.

• Reasons?
  – **Everyone has got a mobile phone!** (one at least)
    • Even poor countries / emerging ones (Africa, India, Brazil, etc..)
  – Today’s mobile phones are just “fully-equipped PCs”:
    • Powerful CPUs, Internet access (broadband), Camera, “Keyboard”, Color display
  – Mobile phone users store important/critical information onto it:
    • Contacts/phone numbers
    • Personal picture/videos
    • E-banking
    • ……..
  – Cybercrime easily realized how to heavily launch attacks towards them:
    • Zeus (and all of its variants)
    • Android, iPhone, Symbian, Windows CE, Windows Mobile malwares
    • ……..
Encryption

• No matter if we’re speaking about standard PCs, tablets or Mobile Phones.... Encryption tools are (somehow) easily available to everyone.

• This is a true pain/big problem for DF experts...just like “the Cloud” (as Dr. Fred Cohen pointed out earlier)
Case study: Child Pornography (and the Investigation Approach)

- Fighting Digital Pedophilia: the “FDB” investigation case.
- This case study is very interesting and useful because:
  - It shows the power of combining digital and real-life evidences
  - It shows the power of a good investigation + Court trial strategy by the General Attorney to solve the case
  - It has been the first case in Italy where a private DF lab and the Computer Crime Police Department (Italian Postal Police) worked together side-by-side
Case study: the “FDB” investigation
WARNING

• This case study reports real-life evidences from a Digital Pedophilia investigation.
• Some slides will show images that could offend the audience’s sensibility.
• If you do not want this, please get out of the room now. Thanks.
• NOTE: this case study will not be included in the public release of this presentation
Case study: the “FDB” investigation

• “FDB” is an Italian citizen, 55 years old, male.
• At this time he is jailed in Italy. The General Attorney obtained from the Court a grand total of 14 years of jail. His crimes have been:
  – Children sexual abuse
  – Sexual Tourism (Italian law n. 28/2006)
  – Owning, spreading and creation of children pornography material
SLIDES NOT AVAILABLE IN THE PUBLIC, SANITIZED RELEASE OF THIS KEY NOTE
Digital Forensics in the Future
The Future

• The way I see the future of DF is...intriguing, while it gives me a lot to worry about!
  – IT & TLC will grow, grow ad grow up: we’re living in a Digital World, thus heavily depending on the ICT. And, this will just get worse.
  – Cybercrime has (somehow) moved towards the “end-user” (which is much easier to be exploited).
  – Security Incidents, financial frauds, hacks and IT attacks will target the so-called “new technology”.
  – (most of) these new technologies will not be designed with Security in mind!
  – DF will not always be ready on time.
  – Laws (and judges, lawyers, sometimes the law enforcement) will not be ready (always too late, very generalist approach, lack of budget, lack of trainings).
  – Just as history teach us, criminals will always be one step ahead 😞
The Future

• There’s nothing more I can state here, since I’m not Nostradamus 😊

• What I can say for sure is that DF Experts must invest their money into new technologies, keeping on to study, running security research on new scenarios, targets, actors.
Conclusions

- DF is **now** a scientific Police Enforcement discipline
- DF is **not** useful only within IT crimes
- DF is **very useful** when its results are combined with real-life evidences
- Computers (let’s say “IT”...) are everywhere
- Information & Experience’s sharing is the key for success.
Q&A time

* Thanks for your attention! *

Questions? / 有问题吗？