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

Sanitized Release
Public

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 - Bejing, China

SecurityBrokers
Global Cybersecurity Defense Services

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 necessary 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.

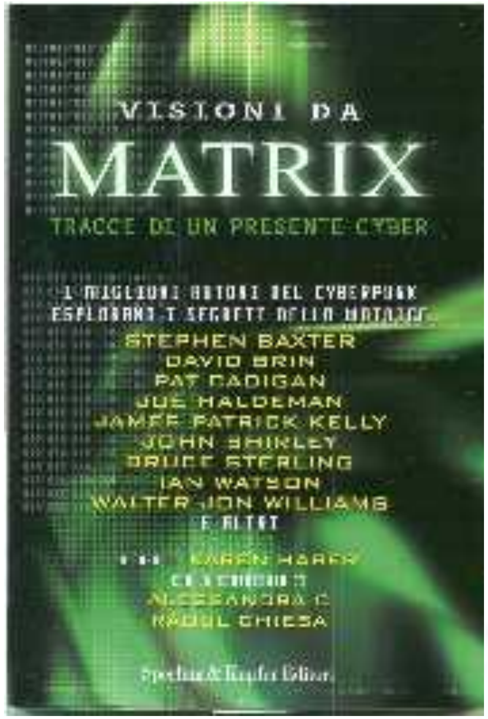
Introductions

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

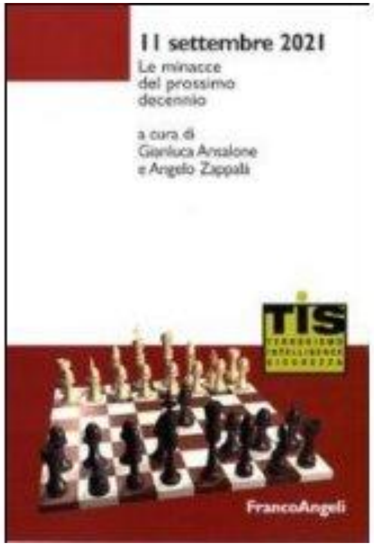


VISIONI DA
MATRIX
TRACCE DI UN PRESENTE CYBER

I MIGLIORI AUTORI DEL CYBERPUNK
ESPLORANO I SEGRETI DELLA MATRICE
STEPHEN BAXTER
DAVID BRIN
PAT CADIGAN
JOE HALDEMAN
JAMES PATRICK KELLY
JOHN SHIRLEY
BRUCE STERLING
IAN WATSON
WALTER JON WILLIAMS
E ALTRI

[illegible] KAREN HABER
[illegible]
ALESSANDRA C
RAOUL CHIESA

Sperling & Kupfer Editori

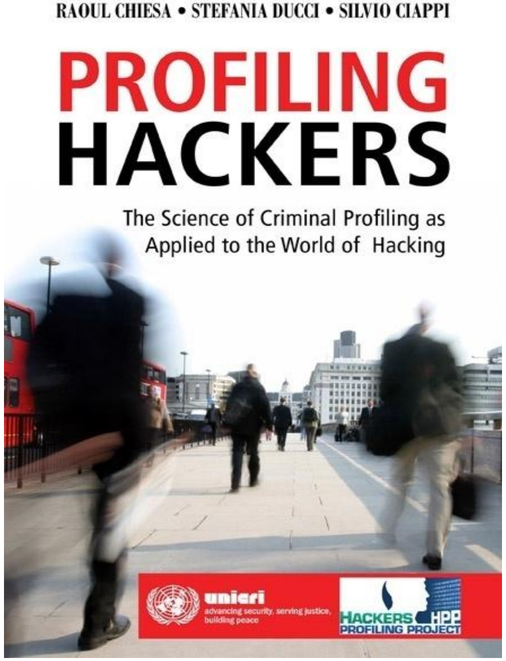


11 settembre 2021
Le minacce
del prossimo
decennio

a cura di
Gianluca Ansalone
e Angelo Zappalà

TIS

FrancoAngeli



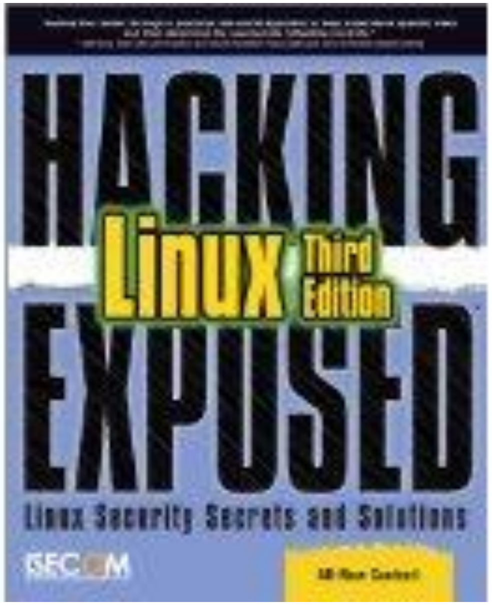
RAOUL CHIESA • STEFANIA DUCCI • SILVIO CIAPPI

PROFILING
HACKERS

The Science of Criminal Profiling as
Applied to the World of Hacking

unicri
advancing security, serving justice, building peace

HACKERS PROFILING PROJECT HPP



[illegible]

HACKING
Linux Third Edition
EXPOSED
Linux Security Secrets and Solutions

ISECOM

GdL Cyber World OSN @ CASD, Centro Alti Studi per la Difesa – RAPPORTO 2012

SELEX
Sistemi Integrati
Una Società Finmeccanica

osn

CeMiSS

OSSERVATORIO PER LA SICUREZZA NAZIONALE

Gruppo di Lavoro *CyberWorld*

Sottogruppo ROSA

Aspetti Terminologici e Tecnologici

Rapporto 2012

Coordinatore: Raoul Chiesa, @ Mediaservice.net

About UNICRI

unicri
advancing security, serving justice, building peace

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

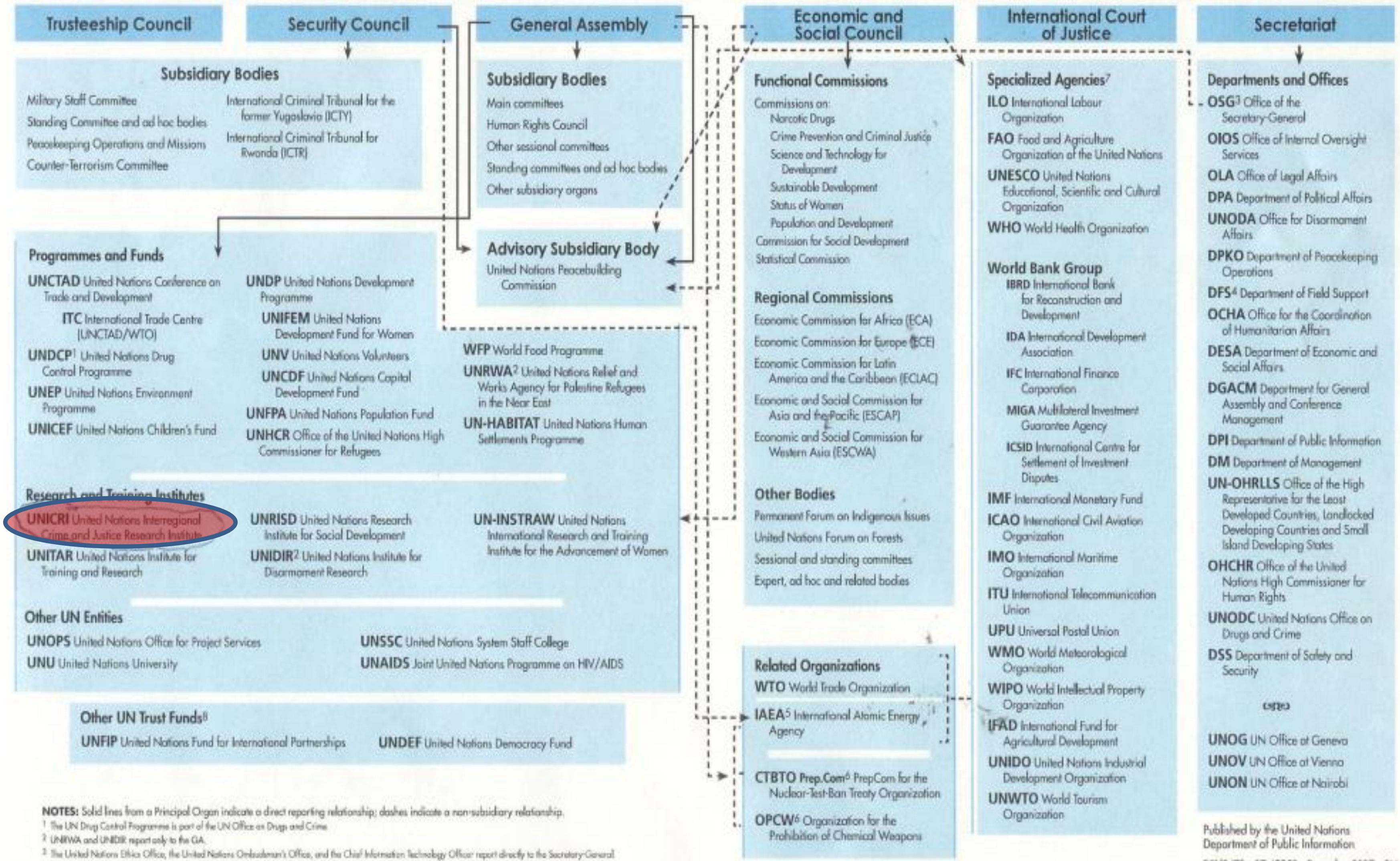
United Nations Training Campus in Turin, Italy

unicri

advancing security, serving justice, building peace

The United Nations System

Principal Organs



Trusteeship Council

Security Council

Subsidiary Bodies

Military Staff Committee
Standing Committee and ad hoc bodies
Peacekeeping Operations and Missions
Counter-Terrorism Committee
International Criminal Tribunal for the former Yugoslavia (ICTY)
International Criminal Tribunal for Rwanda (ICTR)

General Assembly

Subsidiary Bodies

Main committees
Human Rights Council
Other sessional committees
Standing committees and ad hoc bodies
Other subsidiary organs

Advisory Subsidiary Body

United Nations Peacebuilding Commission

Programmes and Funds

UNCTAD United Nations Conference on Trade and Development
ITC International Trade Centre (UNCTAD/WTO)
UNDCP[1] United Nations Drug Control Programme
UNEP United Nations Environment Programme
UNICEF United Nations Children's Fund
UNDP United Nations Development Programme
UNIFEM United Nations Development Fund for Women
UNV United Nations Volunteers
UNCDF United Nations Capital Development Fund
UNFPA United Nations Population Fund
UNHCR Office of the United Nations High Commissioner for Refugees
WFP World Food Programme
UNRWA[2] United Nations Relief and Works Agency for Palestine Refugees in the Near East
UN-HABITAT United Nations Human Settlements Programme

Research and Training Institutes

UNICRI United Nations Interregional Crime and Justice Research Institute
UNITAR United Nations Institute for Training and Research
UNRISD United Nations Research Institute for Social Development
UNIDIR[2] United Nations Institute for Disarmament Research
UN-INSTRAW United Nations International Research and Training Institute for the Advancement of Women

Other UN Entities

UNOPS United Nations Office for Project Services
UNU United Nations University
UNSSC United Nations System Staff College
UNAIDS Joint United Nations Programme on HIV/AIDS

Other UN Trust Funds[8]

UNFIP United Nations Fund for International Partnerships
UNDEF United Nations Democracy Fund

Economic and Social Council

Functional Commissions

Commissions on:
Narcotic Drugs
Crime Prevention and Criminal Justice
Science and Technology for Development
Sustainable Development
Status of Women
Population and Development
Commission for Social Development
Statistical Commission

Regional Commissions

Economic Commission for Africa (ECA)
Economic Commission for Europe (ECE)
Economic Commission for Latin America and the Caribbean (ECLAC)
Economic and Social Commission for Asia and the Pacific (ESCAP)
Economic and Social Commission for Western Asia (ESCWA)

Other Bodies

Permanent Forum on Indigenous Issues
United Nations Forum on Forests
Sessional and standing committees
Expert, ad hoc and related bodies

Related Organizations

WTO World Trade Organization
IAEA[5] International Atomic Energy Agency
CTBTO Prep.Com[6] PrepCom for the Nuclear-Test-Ban Treaty Organization
OPCW[6] Organization for the Prohibition of Chemical Weapons

International Court of Justice

Specialized Agencies[7]

ILO International Labour Organization
FAO Food and Agriculture Organization of the United Nations
UNESCO United Nations Educational, Scientific and Cultural Organization
WHO World Health Organization

World Bank Group

IBRD International Bank for Reconstruction and Development
IDA International Development Association
IFC International Finance Corporation
MIGA Multilateral Investment Guarantee Agency
ICSID International Centre for Settlement of Investment Disputes

IMF International Monetary Fund
ICAO International Civil Aviation Organization
IMO International Maritime Organization
ITU International Telecommunication Union
UPU Universal Postal Union
WMO World Meteorological Organization
WIPO World Intellectual Property Organization
IFAD International Fund for Agricultural Development
UNIDO United Nations Industrial Development Organization
UNWTO World Tourism Organization

Secretariat

Departments and Offices

OSG[3] Office of the Secretary-General
OIOS Office of Internal Oversight Services
OLA Office of Legal Affairs
DPA Department of Political Affairs
UNODA Office for Disarmament Affairs
DPKO Department of Peacekeeping Operations
DFS[4] Department of Field Support
OCHA Office for the Coordination of Humanitarian Affairs
DESA Department of Economic and Social Affairs
DGACM Department for General Assembly and Conference Management
DPI Department of Public Information
DM Department of Management
UN-OHRLLS Office of the High Representative for the Least Developed Countries, Landlocked Developing Countries and Small Island Developing States
OHCHR Office of the United Nations High Commissioner for Human Rights
UNODC United Nations Office on Drugs and Crime
DSS Department of Safety and Security

UNOG UN Office at Geneva
UNOV UN Office at Vienna
UNON UN Office at Nairobi

NOTES: Solid lines from a Principal Organ indicate a direct reporting relationship; dashes indicate a non-subsidiary relationship.

[1] The UN Drug Control Programme is part of the UN Office on Drugs and Crime
[2] UNRWA and UNIDIR report only to the GA.
[3] The United Nations Ethics Office, the United Nations Ombudsman's Office, and the Chief Information Technology Officer report directly to the Secretary-General
[4] In an exceptional arrangement, the Under-Secretary-General for Field Support reports directly to the Under-Secretary-General for Peacekeeping Operations
[5] IAEA reports to the Security Council and the General Assembly (GA)
[6] The CTBTO Prep.Com and OPCW report to the GA.
[7] Specialized agencies are autonomous organizations working with the UN and each other through the coordinating machinery of the ECOSOC at the intergovernmental level, and through the Chief Executives Board for coordination (CEB) at the inter-secretariat level.
[8] UNFIP is an autonomous trust fund operating under the leadership of the United Nations Deputy Secretary-General. UNDEF's advisory board recommends funding proposals for approval by the Secretary-General.

Published by the United Nations
Department of Public Information
DPI/2470—07-49950—December 2007—3M

About ENISA

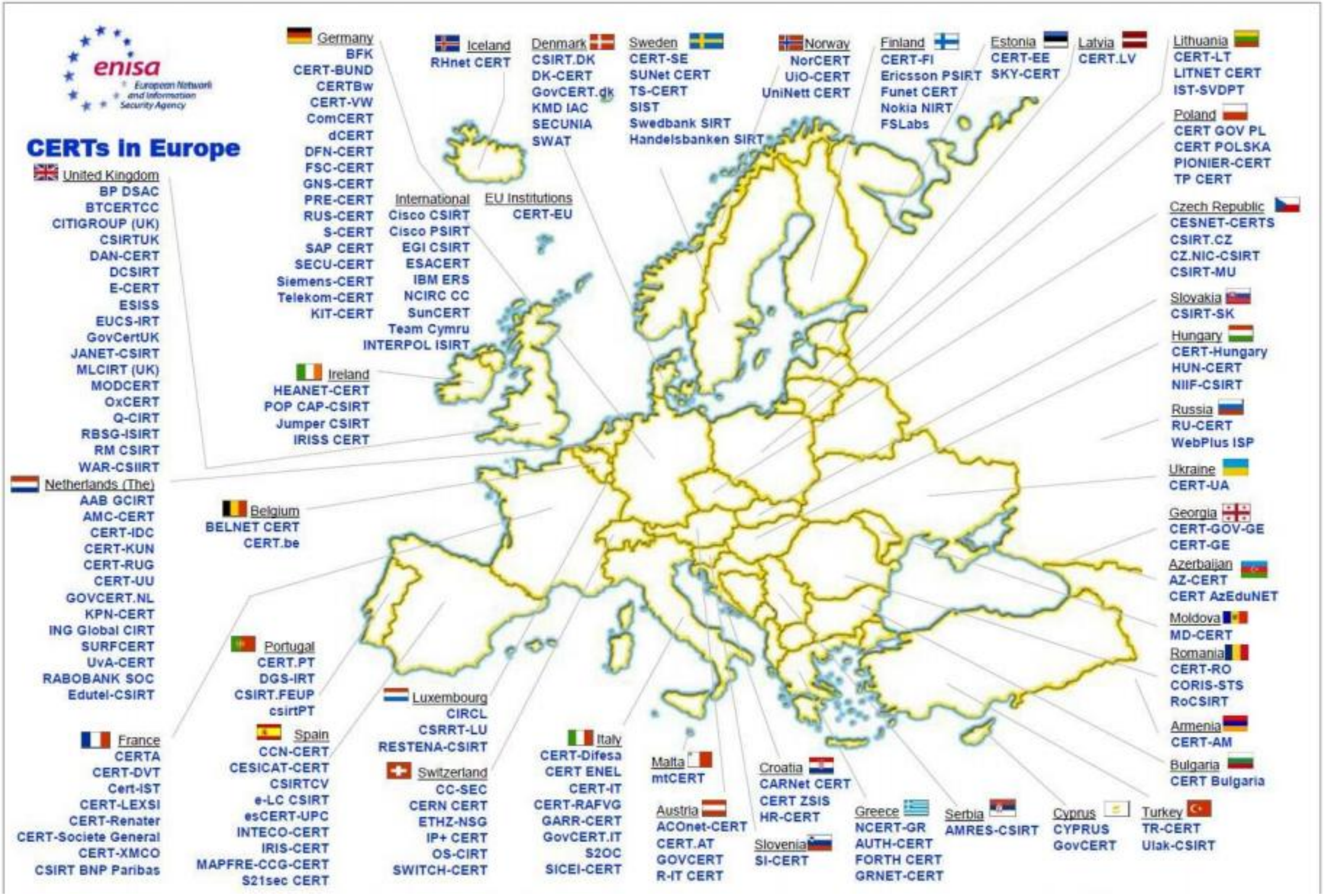
What is ENISA?

- 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**.

enisa
European Network
and Information
Security Agency

http://www.enisa.europa.eu/media/news-items/enisa-has-held-the-first-meeting-of-its-new-permanent-stakeholders2019-group-on-thursday-13th-september-2012

enisa
European Network and Information Security Agency



enisa
European Network and Information Security Agency

CERTs in Europe

United Kingdom
BP DSAC
BTCERTCC
CITIGROUP (UK)
CSIRTUK
DAN-CERT
DCSIRT
E-CERT
ESISS
EUCS-IRT
GovCertUK
JANET-CSIRT
MLCIRT (UK)
MODCERT
OxCERT
Q-CIRT
RBSG-ISIRT
RM CSIRT
WAR-CSIIRT

Netherlands (The)
AAB GCIRT
AMC-CERT
CERT-IDC
CERT-KUN
CERT-RUG
CERT-UU
GOVCERT.NL
KPN-CERT
ING Global CIRT
SURFCERT
UvA-CERT
RABOBANK SOC
Edutel-CSIRT

France
CERTA
CERT-DVT
Cert-IST
CERT-LEXSI
CERT-Renater
CERT-Societe General
CERT-XMCO
CSIRT BNP Paribas

Germany
BFK
CERT-BUND
CERTBw
CERT-VW
ComCERT
dCERT
DFN-CERT
FSC-CERT
GNS-CERT
PRE-CERT
RUS-CERT
S-CERT
SAP CERT
SECU-CERT
Siemens-CERT
Telekom-CERT
KIT-CERT

Ireland
HEANET-CERT
POP CAP-CSIRT
Jumper CSIRT
IRISS CERT

Belgium
BELNET CERT
CERT.be

Portugal
CERT.PT
DGS-IRT
CSIRT.FEUP
csirtPT

Spain
CCN-CERT
CESICAT-CERT
CSIRTCV
e-LC CSIRT
esCERT-UPC
INTECO-CERT
IRIS-CERT
MAPFRE-CCG-CERT
S21sec CERT

Iceland
RHnet CERT

International
Cisco CSIRT
Cisco PSIRT
EGI CSIRT
ESACERT
IBM ERS
NCIRC CC
SunCERT
Team Cymru
INTERPOL ISIRT

EU Institutions
CERT-EU

Luxembourg
CIRCL
CSRRT-LU
RESTENA-CSIRT

Switzerland
CC-SEC
CERN CERT
ETHZ-NSG
IP+ CERT
OS-CIRT
SWITCH-CERT

Denmark
CSIRT.DK
DK-CERT
GovCERT.dk
KMD IAC
SECUNIA
SWAT

Sweden
CERT-SE
SUNet CERT
TS-CERT
SIST
Swedbank SIRT
Handelsbanken SIRT

Norway
NorCERT
UiO-CERT
UniNett CERT

Finland
CERT-FI
Ericsson PSIRT
Funet CERT
Nokia NIRT
FSLabs

Estonia
CERT-EE
SKY-CERT

Latvia
CERT.LV

Lithuania
CERT-LT
LITNET CERT
IST-SVDPT

Poland
CERT GOV PL
CERT POLSKA
PIONIER-CERT
TP CERT

Czech Republic
CESNET-CERTS
CSIRT.CZ
CZ.NIC-CSIRT
CSIRT-MU

Slovakia
CSIRT-SK

Hungary
CERT-Hungary
HUN-CERT
NIIF-CSIRT

Russia
RU-CERT
WebPlus ISP

Ukraine
CERT-UA

Georgia
CERT-GOV-GE
CERT-GE

Azerbaijan
AZ-CERT
CERT AzEduNET

Moldova
MD-CERT

Romania
CERT-RO
CORIS-STS
RoCSIRT

Armenia
CERT-AM

Bulgaria
CERT Bulgaria

Italy
CERT-Difesa
CERT ENEL
CERT-IT
CERT-RAFVG
GARR-CERT
GovCERT.IT
S2OC
SICEI-CERT

Malta
mtCERT

Austria
ACOnet-CERT
CERT.AT
GOVCERT
R-IT CERT

Croatia
CARNet CERT
CERT ZSIS
HR-CERT

Slovenia
SI-CERT

Greece
NCERT-GR
AUTH-CERT
FORTH CERT
GRNET-CERT

Serbia
AMRES-CSIRT

Cyprus
CYPRUS
GovCERT

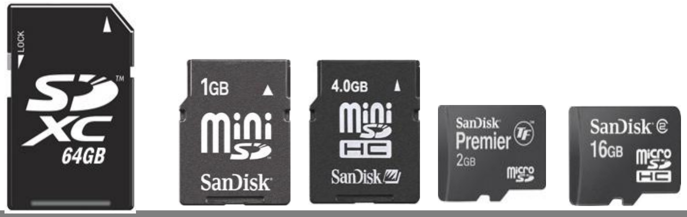
Turkey
TR-CERT
Ulak-CSIRT

http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Entering the Digital Forensics age

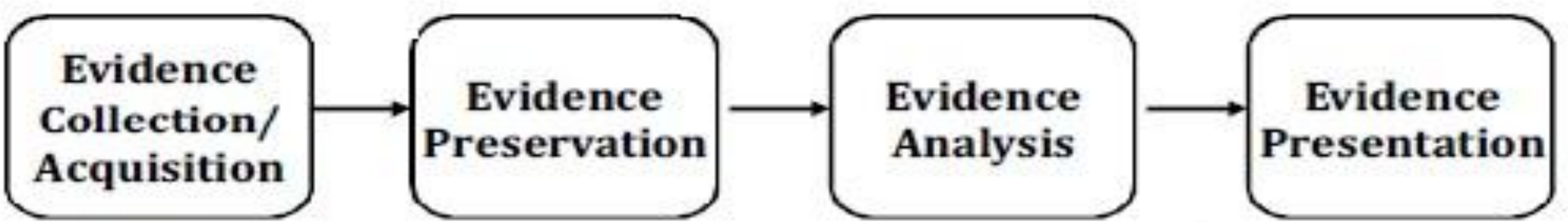
What is Digital Forensics?

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 wich 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?”

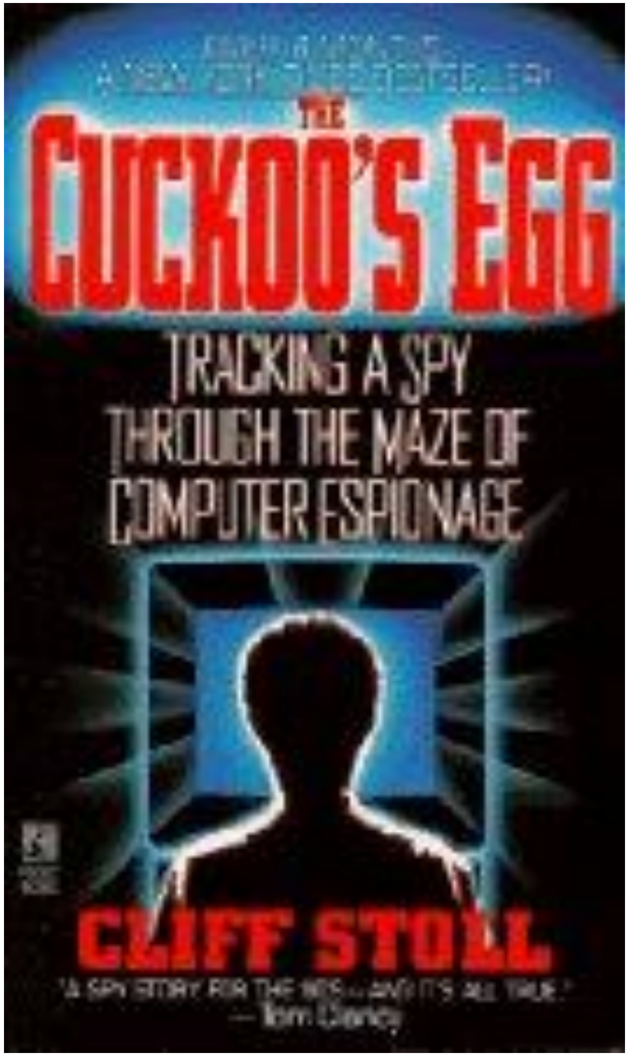
- The answer is not just a single one!

- A DF **real** expert should be a mix of:
  - Academic background
  - System Administrator (on <u>different</u> 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

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 13th, 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!

LEARN from the past
LIVE in the present
BELIEVE in the future

Digital Forensics in the Present

DF today

- 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”

Digital Forensics Lab(s)

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

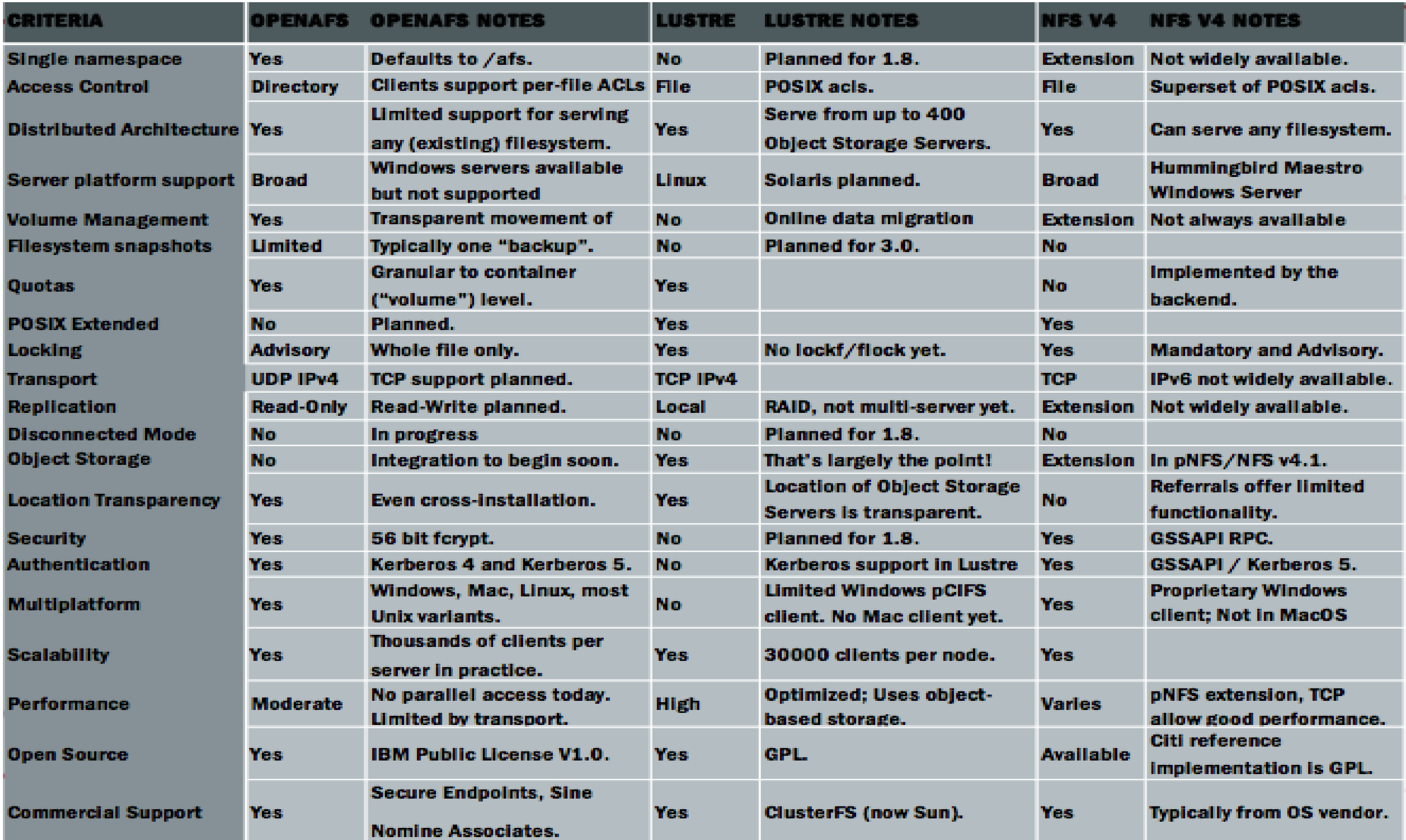
- Broad platform support
- UNIX
  - MacOS 10.3-10.8, Solaris (Sparc and x86) 7-11 and OpenSolaris
  - AIX 5.1-5.3; HPUX 11.0, 11i, 11i v2, 11i v3; IRIX 6.5;
  - NetBSD, FreeBSD and OpenBSD (server only)
  - Linux 2.4 and 2.6 (through .24) kernels
  - Fedora Core 3-7, RHEL3-5, Debian and others
  - Microsoft Windows
    - 2000, XP, Server 2003, Vista, Server 2008 (32-bit and 64-bit)
- 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 comparision (from 2009)



CRITERIA	OPENAFS	OPENAFS NOTES	LUSTRE	LUSTRE NOTES	NFS V4	NFS V4 NOTES
Single namespace	Yes	Defaults to /afs.	No	Planned for 1.8.	Extension	Not widely available.
Access Control	Directory	Clients support per-file ACLs	File	POSIX acls.	File	Superset of POSIX acls.
Distributed Architecture	Yes	Limited support for serving any (existing) filesystem.	Yes	Serve from up to 400 Object Storage Servers.	Yes	Can serve any filesystem.
Server platform support	Broad	Windows servers available but not supported	Linux	Solaris planned.	Broad	Hummingbird Maestro Windows Server
Volume Management	Yes	Transparent movement of	No	Online data migration	Extension	Not always available
Filesystem snapshots	Limited	Typically one "backup".	No	Planned for 3.0.	No	
Quotas	Yes	Granular to container ("volume") level.	Yes		No	Implemented by the backend.
POSIX Extended	No	Planned.	Yes		Yes	
Locking	Advisory	Whole file only.	Yes	No lockf/flock yet.	Yes	Mandatory and Advisory.
Transport	UDP IPv4	TCP support planned.	TCP IPv4		TCP	IPv6 not widely available.
Replication	Read-Only	Read-Write planned.	Local	RAID, not multi-server yet.	Extension	Not widely available.
Disconnected Mode	No	In progress	No	Planned for 1.8.	No	
Object Storage	No	Integration to begin soon.	Yes	That's largely the point!	Extension	In pNFS/NFS v4.1.
Location Transparency	Yes	Even cross-installation.	Yes	Location of Object Storage Servers is transparent.	No	Referrals offer limited functionality.
Security	Yes	56 bit fcrypt.	No	Planned for 1.8.	Yes	GSSAPI RPC.
Authentication	Yes	Kerberos 4 and Kerberos 5.	No	Kerberos support in Lustre	Yes	GSSAPI / Kerberos 5.
Multiplatform	Yes	Windows, Mac, Linux, most Unix variants.	No	Limited Windows pCIFS client. No Mac client yet.	Yes	Proprietary Windows client; Not in MacOS
Scalability	Yes	Thousands of clients per server in practice.	Yes	30000 clients per node.	Yes	
Performance	Moderate	No parallel access today. Limited by transport.	High	Optimized; Uses object-based storage.	Varies	pNFS extension, TCP allow good performance.
Open Source	Yes	IBM Public License V1.0.	Yes	GPL.	Available	Citi reference implementation is GPL.
Commercial Support	Yes	Secure Endpoints, Sine Nomine Associates.	Yes	ClusterFS (now Sun).	Yes	Typically from OS vendor.

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 an 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
    - ……

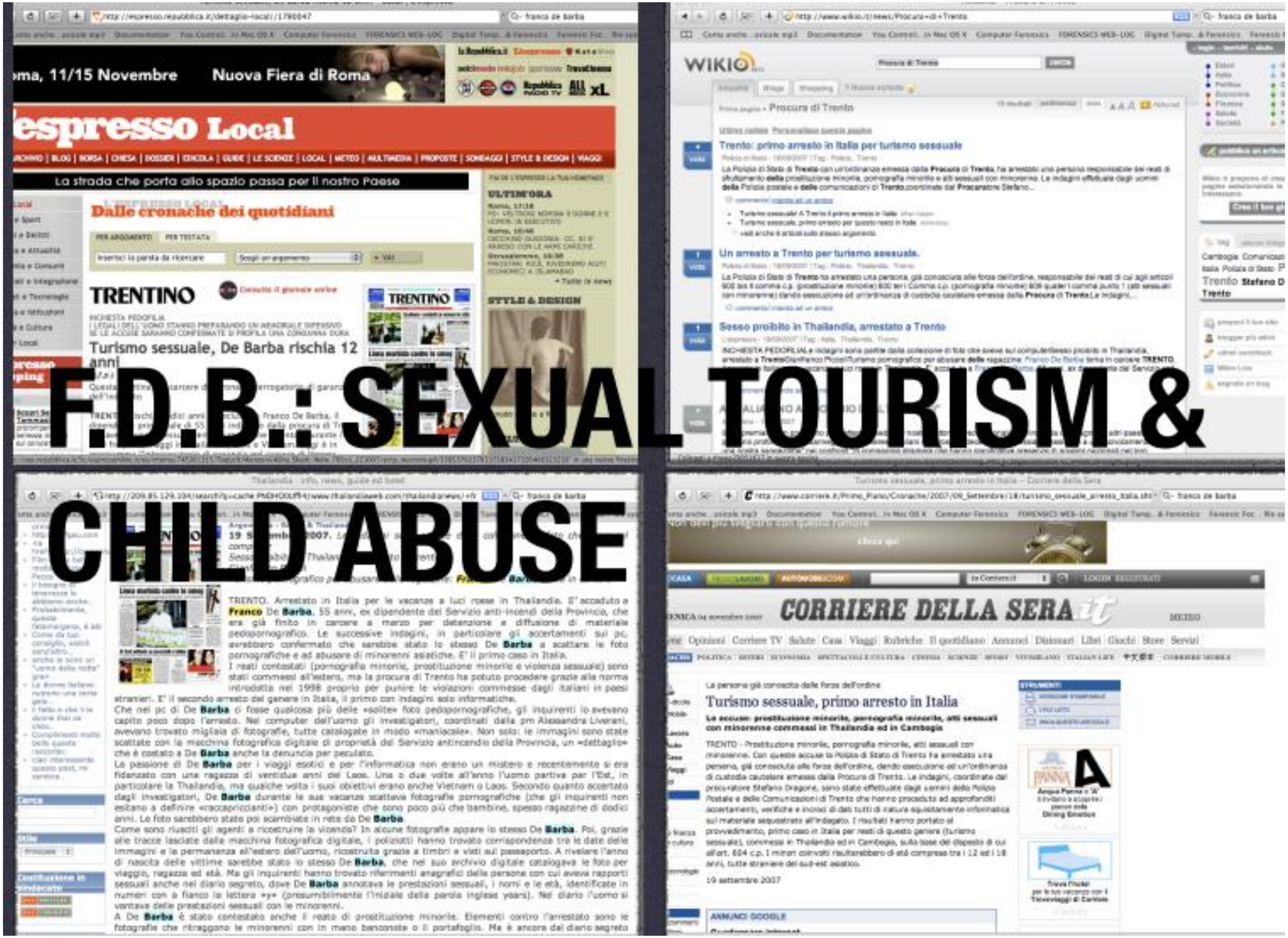
Encryption

- 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



F.D.B.: SEXUAL TOURISM & CHILD ABUSE

Turismo sessuale, De Barba rischia 12 anni

Trento: primo arresto in Italia per turismo sessuale

La Polizia di Stato di Trento con un'ordinanza emessa dalla Procura di Trento, ha arrestato una persona responsabile dei reati di sfruttamento della prostituzione minorile, pornografia minorile e atti sessuali con minorenne. Le indagini effettuate dagli uomini della Polizia postale e delle comunicazioni di Trento,coordinate dal Procuratore Stefano...

- Turismo sessuale! A Trento il primo arresto in Italia
- Turismo sessuale, primo arresto per questo reato in Italia

Un arresto a Trento per turismo sessuale.

La Polizia di Stato di Trento ha arrestato una persona, già conosciuta alle forze dell'ordine, responsabile dei reati di cui agli articoli 600 bis II comma c.p. (prostituzione minorile) 600 ter I Comma c.p. (pornografia minorile) 609 quater I comma punto 1 (atti sessuali con minorenne) dando esecuzione ad un'ordinanza di custodia cautelare emessa dalla Procura di Trento.Le indagini...

Sesso proibito in Thailandia, arrestato a Trento

INCHIESTA PEDOFILIA Le indagini sono partite dalla collezione di foto che aveva sul computer Sesso proibito in Thailandia, arrestato a Trento ... Franco De Barba torna in carcere TRENTO

TRENTO. Arrestato in Italia per le vacanze a luci rosse in Thailandia. E' accaduto a **Franco** De **Barba**, 55 anni, ex dipendente del Servizio anti-incendi della Provincia, che era già finito in carcere a marzo per detenzione e diffusione di materiale pedopornografico. Le successive indagini, in particolare gli accertamenti sul pc, avrebbero confermato che sarebbe stato lo stesso De **Barba** a scattare le foto pornografiche e ad abusare di minorenni asiatiche. E' il primo caso in Italia.

I reati contestati (pornografia minorile, prostituzione minorile e violenza sessuale) sono stati commessi all'estero, ma la procura di Trento ha potuto procedere grazie alla norma introdotta nel 1998 proprio per punire le violazioni commesse dagli italiani in paesi stranieri. E' il secondo arresto del genere in Italia, il primo con indagini solo informatiche.

Che nel pc di De **Barba** ci fosse qualcosa più delle «solite» foto pedopornografiche, gli inquirenti lo avevano capito poco dopo l'arresto. Nel computer dell'uomo gli investigatori, coordinati dalla pm Alessandra Liverani, avevano trovato migliaia di fotografie, tutte catalogate in modo «maniacale». Non solo: le immagini sono state scattate con la macchina fotografica digitale di proprietà del Servizio antincendio della Provincia, un «dettaglio» che è costato a De **Barba** anche la denuncia per peculato.

La passione di De **Barba** per i viaggi esotici e per l'informatica non erano un mistero e recentemente si era fidanzato con una ragazza di ventidue anni del Laos. Una o due volte all'anno l'uomo partiva per l'Est, in particolare la Thailandia, ma qualche volta i suoi obiettivi erano anche Vietnam o Laos. Secondo quanto accertato dagli investigatori, De **Barba** durante le sue vacanze scattava fotografie pornografiche (che gli inquirenti non esitano a definire «raccapriccianti») con protagoniste che sono poco più che bambine, spesso ragazzine di dodici anni. Le foto sarebbero state poi scambiate in rete da De **Barba**.

Come sono riusciti gli agenti a ricostruire la vicenda? In alcune fotografie appare lo stesso De **Barba**. Poi, grazie alle tracce lasciate dalla macchina fotografica digitale, i poliziotti hanno trovato corrispondenze tra le date delle immagini e la permanenza all'estero dell'uomo, ricostruita grazie a timbri e visti sul passaporto. A rivelare l'anno di nascita delle vittime sarebbe stato lo stesso De **Barba**, che nel suo archivio digitale catalogava le foto per viaggio, ragazza ed età. Ma gli inquirenti hanno trovato riferimenti anagrafici delle persone con cui aveva rapporti sessuali anche nel diario segreto, dove De **Barba** annotava le prestazioni sessuali, i nomi e le età, identificate in numeri con a fianco la lettera «y» (presumibilmente l'iniziale della parola inglese years). Nel diario l'uomo si vantava delle prestazioni sessuali con le minorenni.

A De **Barba** è stato contestato anche il reato di prostituzione minorile. Elementi contro l'arrestato sono le fotografie che ritraggono le minorenni con in mano banconote o il portafoglio. Ma è ancora dal diario segreto

La persona già conosciuta dalle forze dell'ordine

Turismo sessuale, primo arresto in Italia

Le accuse: prostituzione minorile, pornografia minorile, atti sessuali con minorenne commessi in Thailandia ed in Cambogia

TRENTO - Prostituzione minorile, pornografia minorile, atti sessuali con minorenne. Con queste accuse la Polizia di Stato di Trento ha arrestato una persona, già conosciuta alle forze dell'ordine, dando esecuzione ad un'ordinanza di custodia cautelare emessa dalla Procura di Trento. Le indagini, coordinate dal procuratore Stefano Dragone, sono state effettuate dagli uomini della Polizia Postale e delle Comunicazioni di Trento che hanno proceduto ad approfonditi accertamenti, verifiche e incroci di dati tutti di natura squisitamente informatica sul materiale sequestrato all'indagato. I risultati hanno portato al provvedimento, primo caso in Italia per reati di questo genere (turismo sessuale), commessi in Thailandia ed in Cambogia, sulla base del disposto di cui all'art. 604 c.p. I minori coinvolti risulterebbero di età compresa tra i 12 ed i 18 anni, tutte straniere del sud-est asiatico.

19 settembre 2007

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 to 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

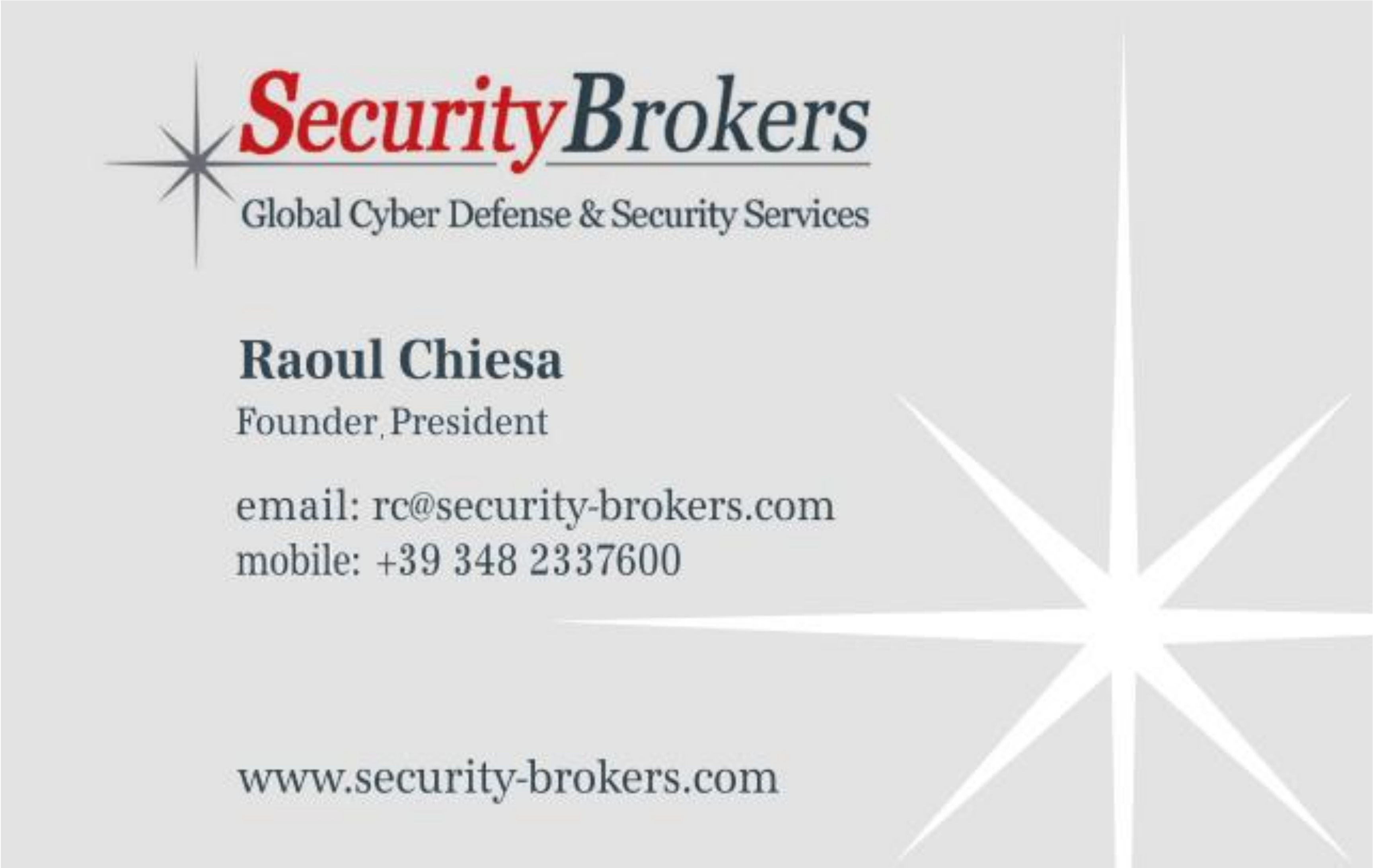
- DF is **now** a scientific Police Enforcement discipline
- DF is **not** useful only within IT crimes
- DF is **very useful** when its results are combined with real-life evidences
- Computers (let’s say “IT”…) are everywhere
- **Information & Experience’s sharing is the key for success.**

Q&A time

- Thanks for your attention!
- 谢谢! ☺

Questions? /有问题吗？

Contacts



SecurityBrokers

Global Cyber Defense & Security Services

Raoul Chiesa

Founder, President

email: rc@security-brokers.com
mobile: +39 348 2337600

www.security-brokers.com