ICDFI 2012 White Paper, October 12th, 2012

by Prof. Raoul Chiesa

Digital Forensics: experiences from the Past, issues from the Present and challenges for the Future

Abstract

This paper aims to be a resume of my Key Note presentation held on September 22nd, 2012 at the First International Conference on Digital Forensics and Investigation (ICDFI) in Bejing, China.

After a short introduction on the key phases of Digital Forensics, I do analyze in three different chapters the past, the present and the future within the DF world, thus including a case study from a field operation against children abuse and digital pedophilia my team run a few years ago. The paper then ends up with the conclusions: a very small and quick list of axioms on DF.

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.

SUMMARY

About the author

Prof. Raoul Chiesa was born in 1973. After having been among the very first European hackers back in the idle of 80’s and 90's (1986-1995), Raoul decided to move to professional Information Security, establishing @ Mediaservice.net Srl back in 1997, a vendor-neutral and well known international security advisory company with its HQ in Turin, Italy.

Since 2003 he started its cooperation with the UN agency "UNICRI" (United Nations Interregional Crime and Justice Research Institute), working on "HPP", the Hacker’s Profiling Project run by ISECOM and UNICRI; in 2005 he has been officially recognized as a cybercrime advisor. Nowadays his role at UNICRI is that of "Independent Senior Advisor on Cybercrime".

Since February 2010, Raoul Chiesa is a Member of the European Network & Information Security Agency (ENISA) Permanent Stakeholders' Group (PSG) covering the previous two mandates, 2010-2012 and 2012-2015. The PSG is composed of 30 high-level experts who have been appointed directly by the Executive Director of ENISA to serve as a sounding board for all relevant stakeholders on issues concerning network and information security across European Union.

On March 2012 Raoul left his operating duties @ Mediaservice.net and became a Principal at Cyberdefcon Ltd, a company operating in the fight against cybercrime, mainly working on Cyber Intelligence, along with Mr. Jart Armin (founder of HostExploit).

By the end of 2012 he will officially launch "The Security Brokers", an innovative and global think-tank focused on vertical security issues, along with international networks of high-level InfoSec professionals.

Both Raoul and his associates work on research areas such as Penetration Testing, X.25 and PSDN networks, VoIP&TLC Security, malware analysis, social engineering, Digital Forensics, SCADA & industrial automation/home automation, satellite communication, mobile security, SS7 threats and much more.

Since 1999 he is a regular Speaker and Key Note at official and underground security events such as Hack in the Box (HITB), CONFidence, Hackito Ergo Sum (HES), PH-Neutral, the National Security Observatory at the Italian MoD, Chaos Communication Congress (CCC), Italian Security Summit, CCDCoE/NATO in Estonia, World Institute for Nuclear Security (WINS), India's Hacking conferences (Club Hack; C0c0n; nullcon), Italian Senate, HackCon Norway, Hacktivity Hungary, RACVIAC Croatia, Swiss Cyber Storm, Secure Poland by CERT-PL, GOV.CERT-NL, SANS, ESA (European Space Agency), ISF China (Internet Security Forum), IDC China (Internet Data Centers Conference) and many more.

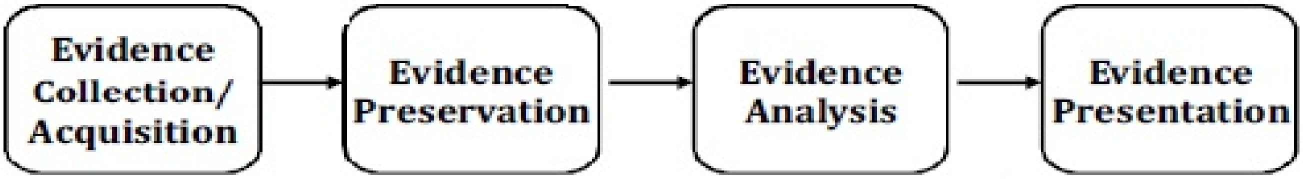
Also, Raoul publishes articles and white papers in English an Italian language as main author or contributor, and he's a regular contact for worldwide medias (newspapers, TV and bloggers) when dealing with Information Security issues and IT security incidents.

Raoul authored and co-authored books such as: “Visioni da Matrix”, featuring Bruce Sterling (Sperling&Kupfler), “Hacking Linux Exposed – ISECOM edition” (McGrawHill), “Profiling Hackers: the science of criminal profiling as applied to the world of hacking” (CRC Press/Taylor&Francis Group), “11 Settembre 2021” (Franco Angeli Editore), the “2012 Report on ICT security in Italy” (CLUSIT, Italian Information Security Association”, the “2012 Report from the Italian MoD National Security Observatory” (Hoepli Editore); furthermore he supervised the Italian editions of books such as “The Art of Hacking”, “Kingpin” and many more.

1. Entering the Digital Forensics age

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*. This means that the digital evidences we are looking for cannot just be found on hard drives, but instead on memory cards (MMC, SD, mini, USB sticks, etc) as well as into any kind of storage devices, both proprietary or standard ones.

The key phases of Digital Forensics (from now, "DF") are the following:



The first phase is definitely a mandatory one, which enables the DF experts to identify, collect and run acquisition from digital evidences. As an immediate next step we then find the preservation phase, which is essential in order to keep the evidences free from alterations and/or modifications: this is possible thanks to the so-called "Chain of Custody", which should preserve the found data itself. As a third phase we have the analysis of evidence, which would allow the DF expert to extract those data significant to the investigation.
Fourth and last phase is the evidence presentation: while many DF experts think this is among the easiest phases, it is definitely not. In fact very often it is real difficult to let non-technical people have a proper understanding of what has been done and how, from a DF point of view. We may define this phase as 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. At the same time, DF expert should *not* give any kind of personal judgments about the investigated subject(s) and he/she should only analyze the given evidence and focus on what into its hands and *not* on theorical thoughts or personal ideas and views.

Giving the above, very often people ask me questions like "Which skills a DF expert should have?" On my opinion there is not just a single answer. After more than ten years (I began in 2001) onto Digital Forensics, I come to the opinion that a real DF 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
- ✓ (Ethical) Hacker
- ✓ Curious personality
- ✓ (sometimes) be a **lucky man**… (you'll see this later)
- ✓ Possibly not married ☺

The last one is of course ironic: it simply means that the average effort of a DF expert, especially during seizure operations, is quite a lot, and this doesn't leave a lot of time for the family and the personal, "free" time.

2. The past

The origins of DF are pretty hard to find; in fact during the 80's and 90's DF was nearly an unknown science. Definitely, DF is called into the scene when a computer incident appears.

That said, the reason why DF was kind of unknown was very simple: computer "incidents" (anomalies, frauds, hacks) were just not so common! Nevertheless, a long time ago I was reading a wonderful book, "The Cuckoo's Egg: tracking a spy through the maze of computer espionage" by Clifford Stoll. While reading this book I realized that one of the very first computer and network's forensics I've ever heard about had been run by the author himself, "Cliff", while trying to identify unknown attackers who took advantage of some UNIX accounts at the servers he was a System Administrator at that time.

Recalling back those old times very good, I've been able to list out a series of common, interesting issues we could find at that time when dealing with and working on DF:

a) a general lack of knowledge;
b) the Law Enforcement;
c) the costs;
d) lack of DF resources and the feeling of "being alone".

2.1 Lack of knowledge

Just as it has been described in The Cuckoo's Egg book, among those main issues related to DF in the past, we can definitely list out:

- Lack of **methodologies** and standard approaches.
  This was the time were terminologies such as "Chain of Custody" were mainly unknown and where there was a real, deep lack of methodologies and standardized, worldwide accepted procedures.
- Lack of **tools.**
  The very same thing was happening with the DF tools, being them hardware (mainly) rather than software. The boom age for DF tools still had to pop up, as we've seen and observed from the fall of the 90's and during the last decade.
- **Evolution of the hardware** VS the available investigative resources at that time.
  Speaking about DF hardware devices, I do remember a special apparel, the "Telemonitor 40" (TM40), a product made in Germany that allowed Law Enforcement to intercept the modem communication of a given subject. In 1995 that device was really expensive (we're speaking about something like 15.000 EUR at that time), while the financial resources available to the investigators from the Law Enforcement agencies could not often afford more than one or two of those devices, for the entire country. The TM40 was able to intercept modem speeds only up to 9.6K tough… In the case study from 1995 I will analyze later in this chapter, the subject bought a new modem, the US Robotics 14.4K Courier, with HST compression, resulting in the fact that Italian Police had to send the TM40 back to the German's factory, asking for a product upgrade, then allowing the device to capture also communication at the speed of 14.4K/sec and HST compression.
- Lack of **experts**!
  A few DF expertise was available all around the world. The very first ones come from USA and UK, then encompassing the Netherlands, France, Italy, Spain, Belgium, South Africa, Hong Kong and Singapore. Basically, experts were in those countries were the local IT market was rich, allowing to customers such as banks, industry and multinationals to investigate computer intrusions and network attacks. Also, the very first DF experts were coming from Government and Military experiences (think about the US DoD and NCIS), which moved to the private industry after some years.

2.2 The Law Enforcement

Law Enforcement was definitely a big issue during the early years of DF's adoption. Better to say, the behaviors of the Law Enforcement officers! Giving very poor (if any) trainings on the DF topic, LEOs used to "made on their own" when dealing with computer crime investigations. Books such as "Underground" from Suelette Dreyfuss (1997), featuring a very young Julian Assange (under the nickname "Mendax") would allow the readers to better understand what we're talking about. LEOs at that time did not belong to special "Computer Crimes Unit" as it happens today, just because those units didn't exist at all.
When executing Police operations and raids, LEOs used to seize as well mousepads and monitors, bringing them back to the Court as some sort of "evidence", which nowadays we know it's completely useless.
On the other hand, a very few Police Officers on those years they used to have the knowledge of a Chain of Custody, resulting in tons of trials were the evidences have been acquired in a way which, these days, would have been rejected by the Judge or, at least, would allow the defendant's lawyer to make not ammissible those evidences themselves.

The problem tough was not just related to the LEOs: Lawyers, Public Prosecutors and Judges didn't have any kind of know-how about computer crimes, meaning that in Court words such as "Hard Drive" and "Internet" called for a detailed explanation in order to allow the different actors to properly understand what was the real subject of the crime.

As a last point, whenever the concept of computer crimes itself was clear to those actors, in the mind of the Judges and Public Prosecutors, as well as for Lawyers, the DF could be only applied to computer crime cases ("hacking") but not to different type of crimes. This meant a huge lost of culture, education and probably the loss of chances to prosecute criminals for different illegal actions and crimes. Just like we know today in fact, DF can be used as a very effective support analysis to crimes which involve murders, kidnappings, child pornography, industrial espionage, financial frauds, insider trading and, of course, hacking-related incidents.

2.3 The Costs

Costs have always represented one of the main issues in DF. Still nowadays, a large part of LEAs from poor or emerging countries (think about most of Africa, as well as countries such as India, Philippines, etc..) have financial constrains that do not allow them to have a proper budget in order to buy the needed hardware and software tools, rather then setting up DF labs. This lack of economic resources impacts as well on specialized trainings, resulting in the de-facto success of DF software tools such as "Encase", which is actually a "point-and-click" tool, it has average affordable cost, but does not allow the investigators to really deal with no-standard and unconventional police cases (think about running DF analysis on filesystems different from Microsoft Windows' ones, rather than on hardware such as Sun SPARC, DEC VAX/AXP and so on).

Encase in fact was able, having been one of the very first DF products to jump in the market, to fill the void left by the totally inaccessible prices of its competitors at that time, enabling the age of "cheap" DF software available both for the Law Enforcement and the DF experts.

2.4 The lack of resources and "being alone"

In this panorama, especially ahead of the so-called "Internet boom" (1997-2002), DF experts didn't have any kind of available forums or boards were discuss about their investigations and crime cases they were onto, neither sharing information or simply ask for help and support.
While hackers all over the world were experiencing the "jump" from BBS (Bulletin Board Systems) on dialup (PSTN) phone lines upwards the Internet and TCP/IP centered online, public resources, plus enjoying readings such as Phrack and 2600 The Hacker's Quarterly, DF experts did not have a "place" to hang out at. It would

have been great to have such a place where experts could have been able to compare their own experiences and troubles, rather than speak about tools to be used, the new tools appearing on the market, and possibly sharing some scripts for MS-DOS or *NIX command line shells!

2.5 A case study from 1995

With the above descripted scenario, on December 13th, 1995, the SCO ("Sezione Centrale Operativa della Polizia di Stato – Italian State Police Central Operating Section") entered into the apartment of a hacker in Turin, northern Italy, at 6AM. Since Italy at that time didn't had the Postal & Computer Security Police Section yet (which would have been established a few years later, because of this police operation named "Ice Trap") the operation itself was lead by the SCO as I mentioned earlier.

The problem with SCO was very simple tough: they were the elite of Police investigators and Special Agents, while their key experiences were related to Mafia and international Organized Crime: they barely never seen a "hacker" before, probably neither heard the word itself, and they were used to enter into suspect's apartments helding guns and rifles, looking for drugs, weapons and first-class gangsters, which is actually very different from a teenager into its bedrooms, surrounded by computers and blinking-lights modems, while its parents are watching the TV in the living room.

Since in 1995 the knowledge related to Digital Forensics was equal to zero, the agents seized nearly everything, from the PCs, floppy disks and CD-ROMs (which is OK) 'till generic hardware such as modems and cell phones, paper agendas and notepads, printouts….. while they gave their very best (from a ironic point of view) when seizing the suspect's mouse and its mousepad!

From a legal framework point of view tough, this case study would be a very embarrassing one (for the Court and the LEA involved) if it'd be analyzed nowadays. In fact the DF analysis was executed by a University Professor, who should actually know its stuff very good, isn't it? Instead, the academic professor didn't follow neither respect any kind of Chain of Custody; furthermore, he printed out onto more than 1.000 pages the full "tree" command output from a MS-DOS prompt, run directly on the suspect's PC and hard drive (!). This "expert" hired by the Police from the local Polytechnic of Turin he directly connected the suspect's hard drive (a HP 5" ¼ hard drive, 2 GB size) to its PC (!!), and a last "touch of class", he wrote the report for the Court directly onto the hard drive of the suspect…

So generally speaking, we can definitely state, without any kind of doubts, that the DF analysis has been carried out in a very "home-made" way, with a totally unprofessional approach which was, indeed and sadly, much common on those years.

3. The present

Before we start his section, some remarks are noticeable. First of all, Computer Forensics – thus becoming Digital Forensics – is a *scientific Police discipline*. As I have stated earlier, the myth for which DF is only useful on "those weird computer crimes" is not true: DF is very useful when combined with those evidences gathered from the real world, as I will detail while analyzing the FDB investigation. And, DF is in our every day's life: criminals use technology. It can be a cellular phone, a PC, an "home" server, a PDA, a Skype phone call…our evidences, in all of these examples, *could be found there as well.*

Today's DF thus become a mix of issues and never ending, unexpected news.

One of the most common issues when dealing with DF are related with those very weird requests which the DF experts may receive from the Public Prosecutors or District Attorney, rather than the Judges themselves. Once upon a time my team has been asked to "seize" a Sun Solaris Enterprise 10000, which couldn't even physically fit into the apartment I was living in at the time I was a single…I had tough times explaining to the Judge that we simply could not go there and "load in our cars" that Sun Enterprise 10000!

Still speaking about unexpected news, thus recalling the comments I have made ahead and related to the Encase software, it has happened to us (quite often, I must say) to work on different hardware architectures for Host-based DFs jobs, such as Motorola, SPARC and different mainframes, while obviously working with Intel chipsets as well. We ran DF on network and mobile environments as well, even including GPS navigator's forensics. But we had also DF on VAX/VMS and AXP (Alpha) OpenVMS, Sony Playstation, Microsoft Xbox, and lately cloud forensics; as a last note of unconventional DF requests, we've very often dealt with web applications forensics, 90% of the times related to hacking incidents, which lead to economic crimes and financial frauds.

Jumping back to my presentation at ICDFI 2012, I explained those common issues when dealing with DF at the present time, including:
- operation logistics
- real experts VS competition
- the "Big 4"
- HW&SW VS the human brain
- (still too high) prices for DF tools

Getting the last point as a good example in order to start, I then detailed the experiences of my team when designing and setting up a Digital Forensics Lab, then speaking about Mobile Forensics and those issues DF experts may find out when dealing with encryption.

Unfortunately I do not have space enough here to report to the readers all the details of what I've said during my Key Note, so I do prefer to fill in the remaining text space for the FDB investigation case.

3.1 Case study: Child Pornography (and the Investigation Approach)

This case we will analyze concerns Mr. "FDB", an investigation carried out by the Italian Postal Police (Polizia Postale e delle Telecomunicazioni) and focused on Sexual Tourism and Child Abuse crimes.

"FDB" is a 55 years old man, actually jailed in an Italian state prison, waiting for the sentence. The Attorney General asked for a grand-total of 14 years of jail. "FDB" was accused of the following crimes:

- ✓ Children abuse
- ✓ Sexual Tourism (Italian Law n.° 28/2006)
- ✓ Possession, Diffusion and Creation of Child Pornography material

The investigation technically started when a covered Police Agent online met, then started trading child-pornography images with FDB.

Police began the wiretap procedure for FDB ADSL line. A.G. goals were to focus on chat, email, IM evidences: we started gathering and analyzing all the kind of outgoing communication. During the next month of wiretapping, we realized that a certain "Mr. W" was the most active commercial trader in Europe, and "FDB" was one of his active contacts. The economical gain of Mr. W was coming from Web sites wasn't even a small one, thus motivating the DA to urgently proceed on the investigation path we had about "FBD".

At this point our goal, from a DF expert point of view, mainly was to track the "FDB" IP address; this was done by mixing and comparing the data from the IM logs and the intercepted email headers. "FDB" didn't had an Internet link at his home (maybe he was feeling more safe in this way), since he was (ab)using his office connection.

When Police went to pick him up at work, they found him sharing child-pornography data via the P2P network, using E-Mule. Police caught him while committing a crime…

a. Size (and Analyze!)

When Police came back to our labs, they sized the following:

From his office

- One PC
- 3 Hard Drives

From his home

- One PC
- 2 Hard Drives
- 1.500 CDs and DVDs

Analyzing the data hereby contained in the seized material produced something like 1.500.000 child pornography images, along with more than 300 videos.

b. Working with images & videos

Many of the images we found included a man interacting with many teen girls and boys, but his face covered by black paint via a graphic program (it looked as "Paint" from Microsoft). We were kind of sure the guy was "FDB"; of course we needed evidences in order to proof our theory…

We found also 10 different video clips, where a guy – wearing a mask like in the movie "Scary Movie", was raping little girls, aged in the 5 to 15 years old range. All of these videos were filmed by a third person, present on the crime scene. All of the 10 videos were shot in 2 locations only.

We thought we had enough good starting points, but yet we needed full effective proofs. In the meanwhile, the DA told us the case must be closed by 6 months…

c. A smart DA makes the difference!

DA then decided to close the active investigation and open a **new one**, allowing in this way the needed time we were asking for. As all of us we know, IT investigations depends on so many aspects and issues – not always directly depending on yourself, your skills, your team or your Police Unit – and we always have to fight with the given time. The DA strategy was the following:

- FDB was indicted only for possession and distribution of child pornography material (a minor accuse);
- in this way, FDB felt relaxed, thinking that, at the worst, he would have been condemned for two minor crimes.

d. One step ahead

We won in getting our "extra" investigation time. Our goal was to obtain evidences that FDB abused minors in Thailand, Laos and Cambodia.

We went back to the seized material. When Police seized the material, we split the homework: Police analyzed around 1.200.000 pictures and videos, stored on DVDs, while we run a full search on 10 Hard Drives, for 1.200.000 more pictures.

We needed to find a logic link, an evidence. And this was somewhere, among the millions of pictures. So we wrote a software in order to look for all the images with EXIF data, then saving the results in a database. Our primary keys were time, date and the camera's model. Then we passed the results to the Police, in order to join the XIF infos with the trip's tickets and all the receipts from his travel. Police was able to found pictures (normal ones: on the beach, at the restaurant, etc…) shot when the suspect was on holiday in South-East Asia.

We begin to select some pictures, in order to deeply analyze them and find some evidences about the head-less man. But the pics were really orrible: underexposed, 640x480 up to 1024x768 (in the best cases!), shot during the night….

So we decided to use different image software (Kneson Imageneer Unlimited, Photozoom2, Genuin Fractals), in order to better enlarge and enhance those "beach" images.

Bingo ! We found two nevi on the left hand both between his thumb and his forefinger. **FDB had the same nevi**…

We went back to the videos again. We worked with iMove (Apple's consumers video editing program) so that we could save the Quicktime format in Bitmap sequences. The QVGA video was under low light, so we didn't had enough resolution to show nevi or some other details..

Then we found that the Scream-masked man had big spots on the skin of his face, realizing at the same time that FDB didn't had any spot…

e. Let's resume the evidences…and find a final to this tale

We sit and tried to resume the evidences:

✓ the videos were filmed in Thailand
✓ the videos showed skin spots
✓ the person's body was very very similar to FDB
✓ …but FDB didn't had any more spots at the present time….

We didn't understood where we did wrong.

Here it came the Police, suggesting us some sort of disease. Going back to analyze the evidences gathered from the Police, we found a TIFF image of a fax, sent from the Bangkok's hospital (just a week before the movies were shot), because FDB was **diabetic**.

Diabetes often leaves **large spots** on the skin, especially after a serious fit. Moreover, these spots **are not permanent**.

Luckyness was definitevily on our side, since the Police called us back: they found two handwritten pages, containing the following data:

- ✓ Girls' names
- ✓ Location
- ✓ A number in the range 1-10
- ✓ A number followed by a "y"

We got another goal. In fact, we have been able to find many photos in the directory, named as the girls in the pages were FDB and those girls (naked, sometimes with their genitals fully exposed) were in an hotel room together.

We decided to go back to other evidences, such as the IM (Instant Messaging) logs. We fired up "Belkasoft Forensic IM Extractor", in order to look for evidences in the IM logs. We did find 400 MBs of text logs, something like the last 4 years of chat activity.

Also, we did found in these IM logs that FDB used to boast himself with his friends, claiming to have had sexual intercourse with this or that "cute little girl", with names and age: these info were exactly the same notes that we found on the paper's list !

Of course, we couldn't know if these boasts were true or fake… Then, in a chat's log, we found a very long and deeply detailed description, where he stated having had a sexual relationship with his daughter when she was 10 years old. The Police called the girl (now 26 y.o.) and talked with her. Finally, she told everything to the Police, confirming every single detail that FDB wrote in the chat.

So, FDB was truthful, the boasts were real. The DA decided to pack-up everything and sent the Postal Police to pick up FDB at this home, then took him to jail.

The DA interrogated him for many hours and, at the end, FDB admitted all of his crimes.

4. The future

As I said during my Key Note at ICDFI2012, the way I see the future of DF is…intriguing, while it gives me a lot to worry about!
I've listed out those main topics of interest which I think DF experts should carefully study on and think about:

- ✓ *IT & TLC* will grow, grow and 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 ☹

Well… 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.

5. 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!