Digital Forensics Techniques in Computer Crime Control

Giuseppe Mastronardi [1,2]
[1]DEE (Dipartimento di Elettrotecnica ed Elettronica), Politecnico di Bari,
Via Orabona, 4 - Bari, Italy
[2]eBIS (electronic Business In Security), Spin-Off del Politecnico di Bari
Via Giulio Petroni, 25 – Bari, Italy
mastrona@poliba.it

Abstract — **The computer crime remains a burning issue, which could affect not just the success of the net economy. Let's take a closer look to the new investigative technologies and the Italian laws in full concordance with the European advices.**

Keywords: Computer Crime, Digital Forensics, Legal Issues

I. Introduction

With the proliferation of multimedia data on the web, surveillance cameras in cities, and mobile phones in everyday life we see an enormous expansion in multimedia data that needs to be secured to prevent illegal use, to be analyzed by forensic investigators to detect and reconstruct illegal activities, or be used as source of intelligence. The sheer volume of such datasets makes traditional inspection of all data impossible. In recent years the multimedia community has developed new technologies and interesting solutions for management of large collections of multimedia contents (video, images and audio), knowledge extraction, categorization and pattern recognition, indexing, retrieval and searching, browsing and visualization, modeling and simulation in various domains. But, due to the inherent complexity and the objective ambiguity of these data, the application of those techniques are not simple. However, the time is ripe to adopt these results for forensics and intelligence applications, and to grow security and control.

With the increase of computer crimes and, especially, with a realization by companies that have finally begun to denounce the crimes of which they are victims, it calls for a full implementation of this discipline, formed in 1980 by the FBI laboratory technicians.

The digital forensics is often mistakenly identified as a new "branch" of computer security, and it seems not without continuous changes. Undoubtedly, the computer forensics is most known respect to the digital forensics, but this one is a broader science which studies the identification, preservation, protection, retrieval, documentation, and uses any other form of computer data processing in order to be used in the legal process. A typical example is the so-called "trial court" which employs computers to rebuild a scene or an event using virtual reality techniques, so that we speak of "computer generated evidence" [1].

II. Transnational Laws

The Recommendation R (89)9 (September 9, 1989 of the European Council), introduced the indictable offenses into four main categories:

- unauthorized access to computer systems (Article 615 ter);
- defamation by Internet;
- possession and distribution of illegal content (protected material or pedo-pornographic content);
- violation of copyrights by Internet.

In July 2004 came into force the European Convention on cyber crime, signed in Budapest in November 2001, in order to effectively combat these crimes, whose spread is putting in crisis the economic, financial, industrial and political balance of the States. Now, in Italy, the reference law that defines to use the results of a forensic analysis in court, is the Law n.48/2008, known as the "Ratification Law of the Budapest Convention".

In particular, national laws to address cyber crime, are used to articulate the types of offenses in the following conduct:

Unauthorized access: as no access right to a system or a computer network in violation of security rules.

Unauthorized interception: as interception of communications from or within a system or computer network, by technical means and without any rights.

Damage to computer and attacks on the integrity of systems: as deletion, damage, deterioration or suppression of data or computer programs, without the right.

Computer sabotage: as input, alteration, deletion or suppression of computer data or programs or interference with computer systems, with the intention of impeding the operation of a computer system or a telecommunications system.

False information (spoofing or false identity): as input, alteration, deletion or suppression of data or computer programs, or any other interference in information processing, carried out in a manner or under such conditions as to constitute, under national law, an offense of false when the facts themselves were committed in respect of one of the objects of this traditional type of infringement.

Computer fraud: as input, alteration, deletion or suppression of data or computer programs, or any other interference in computer processing that influences the result and leads to economic or property damage to another person, made with the intention of obtaining an illegitimate economic advantage for himself or for others (i.e. phishing: user-id and password intercepted by fraudulent email).

Pedo-pornographic images and personal information: as exploitation of children for profit by the disclosure of compelling images and personal information on Internet.

Unauthorized copy of a protected computer program: as reproduction, distribution or public communication of a computer program protected by law, without right.

Unauthorized copy of a topography: as reproduction without right of a semiconductor topography protected by the law, importation or commercial exploitation of a design or a product manufactured with the help of a topography protected by law.

Under this law, in Italy, the Polizia Postale (as Telecommunication Police), in ongoing consultation with the relevant law enforcement agencies in the other states, carry out a constant and delocalized investigation on the network.

The issue of crime delocalization was simply solved with the criminal persecution by the state of his nationality, regardless of where the crime was committed (an Italian criminal by the Italian law).

III. Operative Tools

These operations of intelligence require smart tools to enable the acquisition of the evidence without modifications. In fact, altering the date of file creation or date and hour of last changing or access, to be unable to obtain useful information from data recorded for forensic purposes.

Similarly, are of particular importance the Data Log files, in which all users movements are stored, while browsing on Intemet. The providers are not only to proceed with the identification of users at the conclusion of the contract, they shall be recorded on the log each access to the system, with the date, the time of link beginning and end, the network addresses, the subscriber identifier codes in the case of anonymous or pseudonyms use. This practice naturally responds to the needs of quality control services, access timing to the exact billing, and any verification of crime commissions, at the request of the court.

The information contained in Logs and records must be given notice to the person, together with the different purposes of treatment (accounting, marketing, quality control), in order to help user to make free and informed consent.

The need for the user consent finalized to conservation or treatment of communication traffic data, requires cancellation or anonymity when each call is finished, unless the treatment is aimed at billing or justice purposes.

Finally, the provider, as all holders of data processing, needs to ensure that appropriate security measures to minimize the risk of destruction or loss, even accidental, of data, unauthorized access or treatment not allowed or does not comply the purposes of collection, but left uncertain as they are not clearly defined what are all steps to prevent the damage, in terms of design, organization and costs. To this purpose, it must be kept in mind that the law is the mode of collection of personal data and requirements, establish the criteria against which to assess the quality of the data, which is another aspect of security (accuracy, relevance, completeness, unexcess respect to the collection purpose).

Nevertheless, special tools become increasingly necessary that help to draw useful information without affecting, especially during judicial seizure of digital supports.

As I said, part of computer forensics is a fundamental safeguard of data on storage media placed under the constraint of the seizure, and therefore not be available to the owner.

A data protection and the guarantee to the stability of the latter, the analysis of the operators in charge storage devices use certain methods to ensure and prove the exact correspondence of the content at any time of the analysis.

To make this possible must "freeze" the data, as putting in place the precautions taken to prevent technological writings (even accidental) of bit and check that later the data are the same.

To fulfill these obligations, in addition to the use of hardware or software that inhibit any writing on storage devices, algorithms are used to hash (usually MD5 or SHA1) to generate a sort of fingerprint of each file and/or of 'entire contents of the device, allowing you to check the integrity at any time after the seizure.

An hardware devices that allow access to the disk read-only mode is called write blocker: through them you can read the data on the device, removing the ones of interest or through the forensic copy. The use of write blocker necessarily require a computer and the capture rate depends on the performance of the machine used to perform the copy.

Another type of hardware tool is the copier whose purpose is to copy the disc bit to bit "suspect" (from seizure) to another disk, at the same time preserving the integrity as well as for the write blocker. The acquisition speed copiers reach very high, often touching the 5 GByte per minute and do not require the aid of a computer in order to be used.

From the software point of view, an excellent tool that prevents writing (and therefore also inadvertent modification of data on the device) is Linux: using the mount command makes it possible to mount the device read-only (not available on Windows systems instead therefore require a write blocker to access the source disk).

IV. Special Skills

The term "computer forensics expert" is used to identify the professional who lends his work in computer crime or computer crime. Since there is no single definition included within the term "forensic" computer forensics expert must look to "preserve, identify, investigate and analyze the content stored in any media or storage device."

The activities are directed not only to all categories of computers, but any electronic equipment with a potential for data storage (mobile phones, smart phones, home automation systems, vehicles and anything that contains data stored). Given the heterogeneity of media unsearchable, we prefer to call this professional, "digital forensic expert."

This expert requires special skills, in particular to conduct the following investigations:

- crime of forgery, unfair competition and false accounting reconstructed on the basis of digital documents;
- violation of the rules on the processing of personal data in the corporate;
- legal protection of corporate data base;
- contracts for the supply of services;
- damages for defects of management software;
- contracts for marketing and distributing software;
- challenge procedures, dispute resolution and reassignment of the domain name in case of unfair competition among entrepreneurs; responsibilities of the Registration Authority, the use of an inhibitory site, the provider's responsibility, liability of the maintainer;
- privacy and minimum measures of security for personal data in public and private health activities, free professional company to produce goods and/or services;
- offenses of possession and dissemination of pedo-pornography;
- offenses relating to the phenomenon of "phishing";
- terrorism.

The AICA (Italian Certification Authority for the ECDL) is now planning a new certification with European dimension on the "digital forensics", to be allocated in particular to law enforcement operators, but also to professionals experts in courts and persecutors' offices.

V. Conclusions

In this speech, I only listed several things:

- the computer crimes before and after the Budapest Convention of 2001,
- some legal solutions,
- the operational tools,
- the needed skills,

The purpose had to share the new frontiers of social life using the network in compliance with legal and Community rules.

References

Several Internet references.