COMPUTER FORENSICS BETWEEN THE ITALIAN LEGISLATION AND PRAGMATIC QUESTIONS

Gianni Fenu and Fabrizio Solinas
University of Cagliari, Dept. of Computer Science Cagliari, Italy
fenu@unica.it and fabrizio.solinas@unica.it

ABSTRACT

Over the last few years, analysing a computer or a digital device has become a necessity in the field of criminal investigations. However, during the forensic analysis, some ordinary mistakes are often made. The aim of this paper is to define a new approach to the problem of evidence examination, analysing and studying practical experiences of case studies within the Italian legal system concerning techniques of computer forensic and forensic data analysis. The user of this type of approaches has to guarantee efficient level of both specialized legal competences and technical skills and highly qualified technical skill in order to analyse digital systems in conformity with the best practices, and national and European regulations. In addition, although many types of software are not free and particular hardware could be adopted in this presented work, one of the main objectives has been the only use of the personal computer in order to prove the possibility to obtain the same results minimizing the costs. The cases studies have focused on computer forensic of various magnetic and optical devices (mass memory), such as hard disk, usb flash, memory and cards.

KEYWORDS

Digital forensic, computer forensic model, forensic data analysis, computer forensic investigation, cybercrime, digital device.

1 INTRODUCTION

Whichever organization, businesses or government, is actually making an effort to contrast cybercrime. Indeed, the Internet is one of the main means to attack an organization. Initially they are increasing their reliance on cyber technologies, such as cloud computing, on-line banking and social networks. In tandem, the rate of innovation in new technology is expanded and organisations are struggling to keep up with the risks of introducing and using new technologies. Cyber activity has provided both a new type of economic crime and new vectors to facilitate existing economic crimes [1].

Today, cybercrime relates to governments, business and private citizens for different issues. First of all, governments has faced this issue because it represents a social problem (child trafficking, child pornography, etc.) and, at the same time, a security challenge (espionage, terrorism, etc.). Subsequently, in this specific field, business risk concern business espionage and therefore financial problems. Finally citizens risk theft identity, frauds and so on. In addition, Symantec (2010) argues that during the 2008-2010 reference period, the threat landscape, once dominated by worms and viruses created by irresponsible hackers, is now ruled by a new type of criminal. The cybercrime is typically a scam perpetrated by bogus emails, sent by "phishers", which are designed to steal confidential information. Moreover, in the black market, different tools are used for attacks, such as the so-called crime ware programs: bots, Trojan horses, and spyware[2].

In this scenario, computer security and digital forensics are the correct solution in order to prevent and to search evidence in relation to: data theft, industrial espionage, unauthorized access to computer systems company, damage information and to answer any potential litigation.

All governments and businesses are increasingly being targeted by waves of attacks from criminals and countries, looking for an economic or military benefit. So numerous and advanced are the attacks that many organizations are tackling problematic issues, such as the identification of the greatest risks in terms of threats and vulnerabilities and the allocation of resources in order to stop the most probable and damaging attacks in advanced.

In addition, although digital forensic is increasingly becoming important to society and in the scientific debate, the regulations that govern this type of crime are constantly evolving, representing a new field in the legislative scenarios. Moreover, not only does the legislature often fail in dealing with this kind of crimes, but these violations also involve several countries with different legal systems. In this reference context, it is necessary to consider the offences that every citizen commits. They go from tax evasion to online banking fraud, terrorist operations, phishing or child pornography[1], juvenile pornography[2].

From conceptual framework, this work describes a methodology that should be used when it is necessary to analyse devices with NON-volatile memory with particular attention to the phase "Examination", which is explained later on. In addition, a whole series of specific tools, used in computer forensics under Linux distribution, has been tested for each phase. Despite the existence of various tools and devices to investigate the evidence, the research intends to use only open software with only a common personal computer. Although, this methodology should be always followed, its use is fundamental in relation to the legal system, because working in this field entails implications for computer experts when they make mistakes.

This paper is composed of five parts. The first discusses what digital forensics is in order to provide a clear a comprehensive definition of this concept. The second section describes the economic impacts on governments, businesses and private citizens in relation to computer crime in order to highlight why it is important. The third presents an overview of the Italian legal system into the computer forensics scope. The fourth section presents the proposed model in a detailed way and its contribution to the state of the art. Finally, the last part completes the paper through conclusion and future works.

2 DIGITAL FORENSICS

Digital forensics or digital forensic science concerns evidences from any digital device. First of all, it is extremely important to highlight the difference between digital forensic and computer security. The first starts after the fact happened. Indeed, it is the science of locating, extracting and analysing types of data from different devices, which are interpreted by specialists in order to be used as legal evidences. At the contrary, the second follows the common saying “prevention is better than a cure”. This concept concerns covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized accesses, changes or destructions. This science could be split in many branches in relation to the analaysed device. It is extremely important to know and to understand this difference because the scenario is extremely wide and the research focuses on only one of the following branches. Indeed, digital forensic branches are: computer forensics, forensic data analysis, database forensics, mobile device forensics, network forensics, forensic video and forensic audio.

[1] Pornography is the sexual act performance of prepubescent age individuals

[2] Juvenile pornography is the sexual act performance of individuals who are not adult but they have already undergone some physical and mental changes from a child to an adult.

All evidence discovered should be convincing and sufficiently reliable to stand up in court. Sivaprasad and Jangale (2012) in our definition support these thesis. Indeed, they define digital forensics as the science of locating; extracting and analysing types of data from different devices, which are interpreted by specialists in order to be used as legal evidence [3]. The digital evidence can be found in computer (hard disks, RAMs or graphics card's RAM), mobile phones, iPods, pen drives, digital cameras, CDs, DVDs, floppies, computer networks, the Internet etc.[4] or it can be hidden in pictures (Steganography), deleted files, formatted hard disks, deleted emails, encrypted files, chat transcripts, password protected files and so on. In a nutshell, the digital evidence is information, stored or transmitted in binary form, which has to be reliable in court. It can relate to source code theft, on-line banking frauds, on-line share trading fraud, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, murder cases, organized crime, terrorist operations, defamation, pornography, extortion, smuggling and so on. As a consequence, the digital forensics focuses on finding digital evidences after a computer security breach has occurred. It consist in the analysis of information that is contained and created with computer systems and computing devices, typically in the interest of figuring out what happens, when it happens, how it happens and who is involved. Digital forensics is the process of investigating a computer system to determine the cause of the incident. A calculator or more in general a capable digital device for digital investigations could have three distinct roles within the computer crime:

- A computer can be the aim of the crime.
- It can be the means by which you make the crime.
- It can serve as evidence repository storing of information that contain criminal acts.

Computer forensics is a process to recognize, protect, extract and archive electronic evidences that exist on the computer and on the related peripherals. Moreover, these evidences have to be sufficiently reliable and persuasive in order to be accepted by the court. As a consequence, judicial forensics must be subject to the main body of the law, and must be executed in accordance with the manner required by law and procedures [5].

2 ECONOMIC PROBLEM RELATED TO COMPUTER CRIME

Cyber attacks are growing, as well as necessary economic costs to contrast them. This is sustained by a study, commissioned by HP (Hewlett Packard) and conducted by the Ponemon Institute on a sample of U.S. companies. According to the survey titled “2012 Cost of Cyber Crime Study” [6], the frequency of attacks has more than doubled in three years, while their economic impact has increased by almost 40 percent. In 2012, the average annual cost of cybercrime, which the interviewed companies paid for the research, was $ 8.9 million, increasing by 6 percent and 38 percent compared to the average cost of 2011 and 2010 respectively. The 2012 survey also showed a 42 percent growth in the number of crimes, identifying an average of 102 successful attacks against the company each week, compared to 72 and 50 attacks in 2011 and in 2010 respectively. As showed in **Fig. 1**, the most expensive cybercrimes are caused by "malware", Denial of Service (DoS), theft or misappropriation of devices and damages provoked by internal staff. The set generates more than 78 percent of the annual costs related to computer crime suffered by businesses.

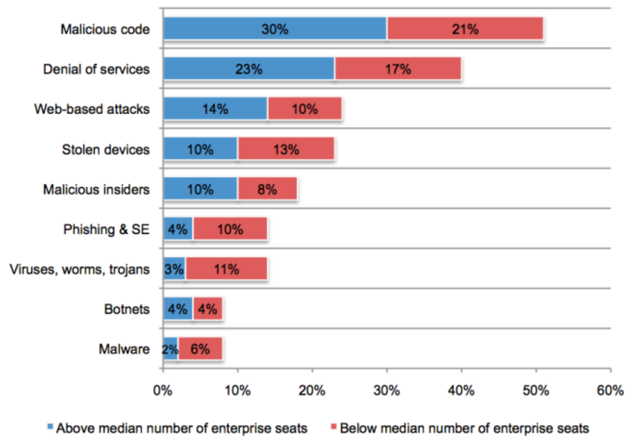

Fig. 1 The cost mix of attacks by organizational size.

In according to the survey, information theft and disruption continue to represent the highest external costs. Indeed, on an annual basis, in 2012 information theft represented 44 percent of the total external costs, increasing by 4 percent compared to 2011. Meanwhile, the business interruption, or loss of productivity totaled 30 percent of the external costs, increasing by 1 percent compared to 2011. The average time that is necessary to suppress definitely a cyber attack is 24 days. However, according to the study the estimated time is 50 days. From these considerations, the average cost paid by companies during 24-days period was $ 591.780, representing an increase of 42 percent compared to the estimated average cost last year, or $ 415,748 for a period of 18 days.

In support of this study, bank robbers steal approximately $100 million per year in the US [7]. Phishing alone resulted in $120 million per quarter [5]. A single botnet ring took $100 million before the FBI managed to stop it [9].

Moreover, a survey was carried out by TNS Opinion & Social network in the 27 Member States of the European Union between 10th and the 25th of March 2012. Around 26 thousand respondents from different social and demographic groups were interviewed face-to-face at home in their mother tongue on behalf of Directorate General Home Affairs. Internet users were questioned on the various activities that they do online. The vast majority of internet users across the EU uses email (85 percent) and many respondents say that they read news online (64 percent). In addition, around half of internet users say that they buy goods or services (53 percent), they use social networking sites (52 percent), or they do online banking (48 percent). Around a quarter (27 percent) play games online, while 20 percent sells goods or services. From this context, it is clear as the cybercrime is relevant to modern society[10].

Finally the evolution of computer security software and other defenses on client endpoints is driving threats into different areas of the operating system (S.O.) stack, especially for covert and persistent attackers. The frequency of threats attacking Microsoft Windows below the kernel are increasing. Some of the critical assets targeted include the BIOS, master boot record (MBR), volume boot record (VBR), GUID Partition Table (GPT), and NTLoader. Although the volume of these threats is unlikely to approach that of simpler attacks on Windows and applications, the impact of these complex attacks can be far more devastating.

3 THE ITALIAN LEGAL SYSTEM INTO COMPUTER FORENSICS SCENARIO

By its nature, the Internet cannot be within a single jurisdiction, so that consequently the computer forensics is closely related with this concept. For this reason, this section aims at providing an overview of how the crimes within the computer crime are handled by the Italian legislation.

In recent years, the demand for analysis of digital data for the purpose of investigation has been increased due to rise of felony related to digital device.

The analysis could concern:

- Offences into information technology (L. 547/93)
- Offences that are not committed by means of computer systems;

- Offences whose traces or clues are found in computer systems;
- Preservation of digital data (memory, media, etc.).

Actually, in Italy it is extremely important the ratification of Budapest Convention on cybercrimes. The Convention is currently the only binding international treaty. The Treaty establishes guidelines for all states that wish to develop a comprehensive national legislation against cybercrime. This treaty could be endorsed by Europeans and non-Europeans countries, providing as a result the framework for international cooperation in this field. In addition, the treaty is supplemented by an additional protocol concerning the criminalization of acts of a racist and xenophobic nature committed through electronic systems. Italy with law 18 March 2008 no. 48 has ratified the Council of Europe on Cybercrime, signed in Budapest on 23 November 2001. This law, among the innovations, introduced the following articles after the number 254 of the code of criminal procedure:

- Article no. 244, paragraph 2, second sentence, where the following words are added at the end: ", in relation to information or computer systems, using technical measures that aim at ensuring the preservation of the original data and prevent distortion.";
- Article no. 247, after paragraph 1 it is inserted as follows: "1-bis. When there is reason to believe that data, information, computer programs or tracks, which are relevant to offense, are in a computer system, it is necessary to adopt technical measures in order to ensure the conservation of the original data and to prevent distortion. ";
- Article no. 248, paragraph 2, first sentence, the words "records, documents and correspondence with banks" are replaced by the following:" banks records, documents and correspondence as well as data, information and software»;
- Article no. 254 has entailed the following changes:
    a) Paragraph 1 is replaced by the following: "1. At who provide postal, telegraphic, electronic or telecommunications service is allowed to proceed to the seizure of letters, fold, parcels, values, telegrams and other items of correspondence, even if submitted electronically, when the court has reasonable grounds to believe that they are sent by the accused or to him, even with different names or by someone else, or someone who may be related to the offense ";
    b) Paragraph 2, after the words "without opening" shall be inserted the following: "or alter.";
- Article no. 254-bis. - (Seizure of computer data by providers of services, telematics and telecommunications). “In case of seizure of data concerning suppliers of telematics or telecommunications services, the court may establish that their acquisition is carried out by copying them on adequate support in relation to the regular supply of such services. This process could be conducted by means of a procedure to ensure the data immutability and their reliable acquisition to the original ones. In this case, however, the service provider has the task to preserve and protect adequately the original data.";
- Article no. 256, paragraph 1, after the words: "also in original if it is so ordered" the following words are inserted: "as well as data, information

and sofware, including by copying them on adequate device. ";

- Article no. 259, paragraph 2, after the first sentence is the following text is included: "When the custody is related to data, information or software, the custodian is also warned of the obligation to prevent distortion or the access by third parties, except in the case that they are authorized by the court.";
- At the article no. 260 entails the following changes:
  a) Paragraph 1, after the words "by other means" the following sentence is added: "even of an electronic or computer nature";
  b) Paragraph 2, the following sentence is added: "When the case concerns data, information or software, the copy has to be made on suitable supports, using the procedures that ensure compliance of the copy to the original and its immutability. In such cases, the custody of the originals can be placed in different places by the registrar or by the secretary. "

From this normative framework, the mentioned changes promote the use of techniques that ensure the repeatability of the assets and in addition they require the tracking of operations that allow verification of all completed actions.

From a fiscal and civil point of view, the main laws related to cybercrime and digital device are:

- CAD (Italian code for Digital Administration) (Legislative Decree 5th march 2005, no. 82): articles. 20-23 and articles 40-44;
- The DPCM (Prime minister decree[3]) 13 of January 2004 "Technical norms for creation, transmission, preservation, copy, reproduction e validation, even temporal, of a digital document";
- The Finance ministry decree 23 January 2004 (DMEF) "Discharging methods of fiscal duties for the digital document reproduction on various devices;
- The CNIPA Resolution (Public administration national center for information technology) Resolution. 11/2004 19th February 2004 "Technical norms for digital document preservation and reproduction on an optical device in order to assure the perfect correspondence between the digital document and the authentic document".

The legislative decrees are also added as following:

- Legislative decree 20th February 2004 no. 52 (implementing the directive 2001/115/CE, covering electronic invoicing);
- Legislative decree 196/2003 data protection act, in particular annex B) quoted on CAD (Italian code for digital administration) article n. 44) and the DPR[4] 11th February 2005 no. 68 (in the field of PEC[5]).

Article 44 of CAD[6] defines precisely that all the preservation methods of digital documents have to guarantee:

- The precise identification of the document writer;
- The integrity/wholeness of a document;
- The readability and traceability of the documents and ID information,

[3] Corresponding to statutory instrument.

[4] Decree by President of Italian Republic.

[5] Certified web mail.

[6] Italian code for digital administration.

including the registration and the filing of pristine data;

- The observation of all the security rules established by the articles from no. 31 to no. 36 of the legislative decree, 30 June 2003, no. 196, the technical specification in Annex B of this decree.

Finally, in Italy the term "computer forensic expert" is used to identify the professional who works in the field of computer crime. The computer forensics expert must take care to preserve, to identify, to study and to analyse the contents that are stored in whatever media or storage device. Not only does the task of experts focus on all categories of computers, but it also concerns any electronic equipment with a potential for data storage, such as mobile phones, smart-phones, home automation systems, motor vehicles, and all it stores data. However, due to the heterogeneity of unsearchable media, this professional is called "digital forensic expert." In the Italian legal system, there is a difference between the possibility of investigation requested by the prosecutor and defense investigations. Indeed, for example, when the "computer forensic expert" is nominated by the prosecutor, he obtains the status of a public official, and his statements are true until proved otherwise.

4 THE NOVEL MODEL

In 2001 Kruse and Heise[11] developed one of the first model in digital forensic. The process showed in **Fig. 2** is essential, indeed it presents only three steps. The first step is acquiring data. In this phase, data are collecting and their integrity should be preserved. Then, there is the authenticating evidence phase that involves making sure that it is as valid as the original. Finally, analysing evidence steps is the process that analyse the data, keeping its integrity.

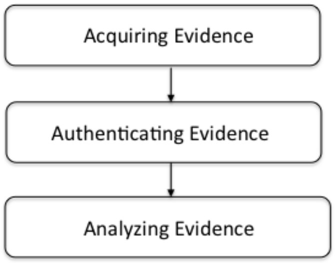

Fig. 2 Kruse & Heiser Model

Different models have been developed. **Table 1** shows a complete list of digital forensic investigation model based on chronological order.

Table 1 List of complete digital forensic investigation model

Model Name	Inventers	Years	Number of phases
Computer Forensic Investigative Process[12], [13]	M.Pollitt	1995	4 Phases
DFRWS Investigative Model (Generic Investigation Process)[14]	Palmer	2001	6 Phases
Scientific Crime Scene Investigation Model (SCSI)[15]	Ciardhua in	2001	4 Phases
Abstract Model of the Digital Forensic Procedures (ADFM)[16]	Reith ,Carr and Gunsh	2002	9 Phases
Integrated Digital Investigation Process (IDIP)[17]	Carrier and Spafford	2003	5 Phases
End To End Digital Investigation[18]	Stephens on	2003	6 Phases
Enhance Integrated Digital	Baryamu reeba	2004	5 Phases

Investigation Process (EDIP)[19]	and Tushabe		
Extended Model of Cyber Crime Investigation[15]	Ciardhuain	2004	13 Phases
A hierarchical, Objective Based Framework for the Digital Investigations Process[20]	Beebe and Clark	2004	6 Stages
Event Based Digital Forensic Investigation Framework[21]	Carrier and Spafford	2004	16 Phases
Forensic Process[22]	Kent K, Chevalier, Grance and Dang	2006	4 Phases
Framework for a Digital Forensic Investigation[23]	Kohn, Eloff and Oliver	2006	3 Phases
Computer Forensic Field Triage Process Model (CFFTPM)[24]	K.Roger, Goldman, Mislan, Wedge and Debtota	2006	12 Phases
Investigation Process model[25]	Freiling and Schwittay	2007	4 Phases
Dual Data Analysis Process[26]	Bem and Huebner	2007	4 Phases
Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)[11]	Perumal S.	2009	7 Phases
Network Forensic Generic Process model[27]	Pilli, Joshi and Niyogi	2010	9 Phases
Systematic Digital Forensic Investigation Model[28]	Ankit Agarwal, Megha Gupta, Saurabh Gupta and Prof (Dr.) S.C. Gupta	2011	11 Phases

In relation to the **Table 1**, first of all, the research analyses the last model "Systematic Digital Forensic Investigation Model" that is showed in **Fig. 3** and it consists of eleven steps [28].

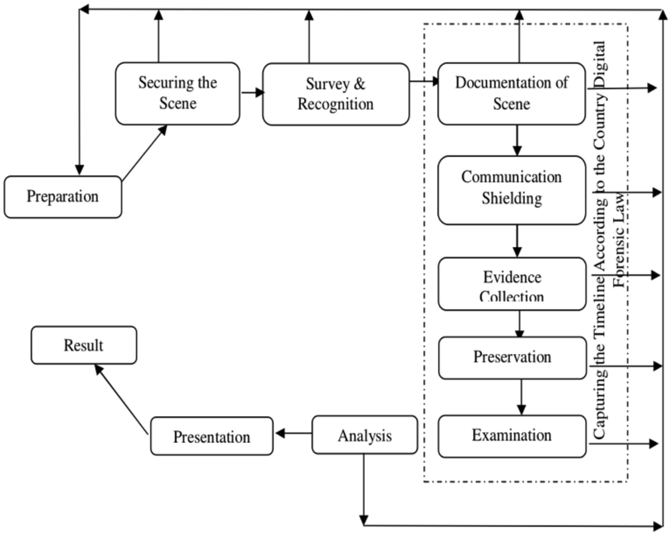

Fig. 3 Phases of Systematic Digital Forensic Investigation Model (SDFIM)

The choice of this model depends on different issues. First of all, the model allows being perfectly adapted to the modern cases. Indeed, this new approach presents a certain degree of circularity that allows repeating some steps. In addition, the concept "Capturing the timeline according to the country Digital Forensic Law" is rightly explained for the phases 4, 5, 6, 7, 8. The last concept is extremely important with respect to the different legislations where this model is applicable.

SDFIM categorizes evidence collection of the digital devices into two categories: volatile evidence collection and Non-Volatile evidence collection. This categorization is done in “evidence collection” and this research focuses on Non-Volatile evidence into the “Examination” phase. Indeed, the paper analyses in detail only the eighth phase called "Examination" related to the non-Volatile evidence. As a result, the research aims at developing a new approach for the examination of Non-Volatile evidence collection. First of all, it is useful to define what Non-Volatile evidence is. They are all devices that are able to store permanently data, for instance hard disk and external storage in general, such as compact flash (CF) cards, memory stick, secure digital (SD) cards, MMC cards, USB memory sticks.

The development of the "Examination" phase is led to create a list of steps that are summarized in **Fig. 4**.

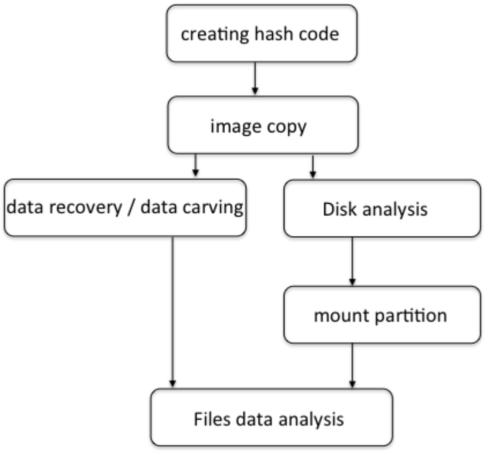

Fig. 4 Phases of Examination's SRDFIM phase

In relation to the chart, the first step is to create the hash code of device. In the second phase, the correct image copy is done. After the second phase, the process is divided into two ramifications that can be executed parallel. The first, on the left, is composed of only one step "data recovery/data carving". Meanwhile, the second, on the right, is characterized by two phases: disk analysis and mount partition. Lastly, there is "files data analysis". During tests of cases study where this approach was tested only a simple personal computer and some other devices such as box external, usb cable, SD card adapter was used. In addition, no software was bought. Indeed, the preliminary phase was to study the different Linux distributions, which have been developed in relation to digital investigation such as DEFT, CAINE, HELIX or BACKTRACK. Not only, the choice of a specific Linux distribution is related to the fact that it is free, but also it concerns several reasons. First of all, it is implemented the first best practice into computer forensic of Non-Volatile memory, that is: auto mount disabled. In addition, it is a flexible environment, the most of additional tools are free and also open source. The last aspect is extremely important, indeed it can know what happens "under the hood" and if they are used in correct way, they could be brought in the court.

In conclusion, these Linux distributions, or other typical for computer forensics analysis, implement other important peculiarities as following:

- At the boot, the system do not use swap partition of the system that is subjected to the analysis;
- During the activity of analysis, there are not automatisms, by doing so, the user is the owner of the device and he must be conscious of the command that he is going to run;
- All mass memory acquisition tools do not modify the data originality.

Finally, in this paper there are references to Sleuth Kit toolkit[7] tools while Autopsy[8], which is a graphical interface to the digital

[7] The Sleuth Kit is written by Brian Carrier and maintained at http://www.sleuthkit.org/sleuthkit/index.php. It is partially based on The Coroner's Toolkit (TCT) originally written by Dan Farmer and Wietse Venema.

[8] http://www.sleuthkit.org/autopsy/index.php.

investigation tools in the Sleuth Kit, does not have any reference within this paper. Moreover, for each phase it is specified only a list of the possible tools and not a detailed description of how to use them. Indeed, reading manual is the best solution to improve knowledge with respect to a specific tool.

4.1 Creating hash code phase

The first step is "creating hash code". This phase concerns the creation of hash[9] code, usually MD5 or SHA, of drive. In relation of this step, it is extremely important to know that in 2005, Xiaoyun Wang and Hongbo Yu proved how breaking MD5 and Other Hash Functions[29]. In this perspective, in this step it is necessary to calculate MD5 and SHA of device. As a consequence, it is clear that after the second phase the image copy is effectively a copy that could be brought to the court. In this step, it is impossible to create the hash code for each file that is presented into the device. Indeed, there is not knowledge about files inside the drive. Moreover, within Linux distribution, there are many tools to calculate hash code, for instance md5sum and sha1sum.

4.2 Image copy phase

Before starting with this step, when the mass memory is connected to the personal computer, it is useful to see the log message whose path is /var/log/messages in Linux distribution. This operation is made through a tool called tail. In this way, it can know the identification that the operating system has got to the device. The aim is to create a reliable copy of the device (bit stream image) that, as a consequence, could be brought to the court. On the other hand, a bit-stream image is a sector-by-sector / bit-by-bit copy of a hard drive. A bit-stream image is actually a set of files that can be used to create an exact copy of a hard drive, preserving all latent data in addition to the files and directory structures. The majority of the tools, used to analyze the hard drive, can read a bit-stream image. This mirror is the only way to have got a reliable copy. Indeed, the simple copies of data do not allow protecting the original data from inadvertent alterations. Acquiring these kinds of exact copies requires the use of specialized forensics techniques. This copy, usually in raw format, is a file image of the analysed drive. It is possible to create more files image of the same device. Each of them is a part of the whole image file. Moreover, it is good practice to create one copy of backup and all the copies that are necessary to work well. Indeed, it is important to not stress the device. Using the drive whenever the probabilities to break accidentally the evidence increase.

After the copy is made, it is possible to calculate the hash code of the image file. Type of hash code must be the same in the previous step. For instance, if in the previous step are used MD5 and SHA, at the same way in this sub-step it is necessary to calculate the same. As a result, it is necessary to check if these hash codes are different with respect to the original hash. From this perspective, if the hash codes are different, it is mandatory to create a new file image, deleting the previous one. This process has to be reset until the hash code and the image file are identical. All this process is synthetized in **Fig. 5**.

[9] Hash codes are large numbers, specific to each file and each drive that are mathematically computed. If a file or drive is changed, even in the smallest way, the hash code will also change. These hash codes are re-computed on the original and on its images at various points during the investigation in order to ensure that the examination process does not modify the examined image[30].

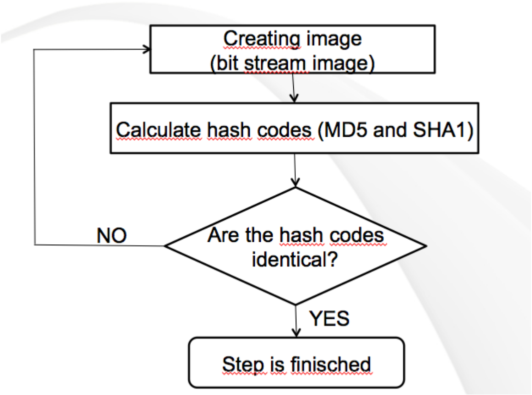
Creating image
(bit stream image)
Calculate hash codes (MD5 and SHA1)
Are the hash codes identical?
NO
YES
Step is finisched

Fig. 5 flow chart of image copy phase

One of the possible tools to create bit stream image is GNU dd command shell. It is robust, well tested, and it has a proven track record. However, several forensic specific tools exist, as following:

- dc3dd, based on dd code, is a patched version of it with added features for computer forensics. The main feature is that on a partial read, the whole block is wiped with zeros. This allows for repeatable reads/hashes of a drive with errors.
- dcfldd, fork of dd code, enhances it for forensic use. It was developed by the Department of Defense Computer Forensics Lab in U.S.A.
- ddrescue enhances dd program. It allows mass memory acquisition that has reading errors, indeed it has intelligent error recovery.
- aimage, this tool is used to acquire Advanced Forensic Format (AFF) images.
- ewfacquire, this tool is used to acquire Expert Witness Format (EWF) images. It is one of tools that are included into libewf package that is a library to access the EWF Format.

After this phase, all operations will be done only on image files, created from the first image.

4.3 Data recovery/data carving phase

The "data recovery/data carving" step aims at recovering the removed data (files). The carving activity consists in recovering files through the files header and footer[10] identification. Indeed, when data carving tool encounters a coincident sequence of bytes with one of the header stored in its configuration file, it starts the extraction of bytes from that header until the first occurrence of bytes coincident with the known footer. If a particular file should not be equipped with the footer carver, it stops after a number of bytes arbitrarily predefined by the user in the configuration file. Obviously, this number must have a reasonable size, preferably oversized compared to the size of the file to recover. As a result, the excess bytes may, in principle, be removed manually. Foremost it is probably the best recovery tools on Linux distribution. However, there are also photorec, scalpel and magicrescue. All these tools are valid and the choice depends on own requirement. Moreover, the mount of partitions is not necessary in order to use the above list. In addition, these tools use the file image as an input.

4.4 Disk analysis phase

The "Disk analysis" step has the goal to analyse the mass memory and to verify the disk partitioning. This phase is complex, and for this reason, it is composed of two sub-phases: the partition recognition and the file system identification.

Partition recognition aims at identifying the partition on the device. The mass memory could have more than one partition, such as primary partitions, extended partition and

[10] Header and footer are signs that detect the start and the end of the specific type file; in particular, they concern a group of consecutive octal or hexadecimal values that are always in a particular position of a determinate file at the start or at the end of this file.

logical partition. In addition, it could have some unallocated disk space. Moreover, it is often necessary to rebuild the disk table because the disk has been formatted or could be corrupted. In this case, testdisk tool is perfect.

The aim of file system identification is to identify the file system of each partition that has been recognized in the preview sub-steps.

As a result of these two phases, all the necessary information is obtained in order to understand which type of analysis should be conducted. For example, if there is a primary partition with file system ntfs, certainly there is a Microsoft Windows (2000, xp, vista, seven, eight) installed system. As a consequence, the analysis also concerns the system register, the Internet chronology, emails, chat and so on. On the other hand, if there is a logical partition, the type of analysis regards exclusively present, hidden or deleted files. Fdisk, Mmls, Hgparm, Disk_stat and HDSentinel represent tools to analyse the disk with respect to these two phases. After that it is possible to develop the first list about all existing files on the mass memory in order to create a time line. The time line is usually created through the tool mac-time. Mac-time takes as input a list, which is created by Fls tool and it is completed of data that are contained into the analysed file system. On the other hand, Fls takes as input a raw file that derives from the previous memory mass acquisition or directly on the device, and Fls returns the list of all files, allocated and not, to be used afterwards as input in mac-time.

4.5 Mount partition phase

The mount partition phase is a tricky step. Indeed, it is very important to avoid that files or everything into the partition could be distorted. In each court on the world it is essential that all procedures can be done again and the data are not modified o distorted. The mount command allows connecting a file system to a system folder. In relation to the steps in **Fig. 4**, the mount is not directly on the device, but it is on the bit stream image. This approach obeys the best practice on computer forensics. The best practice strongly recommends not to work on the original mass memory but always on its copy and following this new presented model after the second phase the device is never used.

The bit stream image can have various formats and the more common are:

- bit stream image, better known as format dd or raw;
- encase, better known as format ewf;
- advanced forensic format, better known as format aff.

In addition the mount command must ensure:

- read-only option, so there are not problem to possible files change;
- noatime option, so the date of last access to the files do not change;
- noexec option, so running file is not permitted.

4.6 Files system analysis

Finally, there is the core of the analysis that needs more time with respect to the other phases. After recovering data or entering into the file system in safe way, as describe previously, the phase of finding the evidence starts.

This step is characterized by two sub-steps. The first, called system operation analysis, is conducted only if the analysis regards a primary partition. In this case, as a result, a operating system, such as Microsoft Windows, IOS, Linux and so on, is always installed. On the other hand, the second phase, called files data analysis, is always developed. Indeed, there are almost always some personal files into a partition or unallocated space. Useful command line tools are Find, Locate, Grep (general regular expression print) and its different version like Egrep, Fgrep or Rgrep. This tools in extremely important to search in one or more rows of text lines that correspond to one or more specified patterns with regular expressions or literal strings. As a result, it produces a list of lines, or also of the single file names, for which correspondence was found. All them are useful for both sub phases and probably without them it is impossible to proceed the analysis. In addition, Find e Locate are also useful. In relation to the first, the tool searches in the real system. It is slower but always up-to-date and it has more options such as size, modification time and so on than Locate tool. On the other hand, Locate uses a previously built database. To update the database it is necessary to run the command “updated” on the Unix shell. The latter is much faster, but it could use an older database and in addition it searches only names or parts of them.

4.6.1 System operation analysis

This phase concerns a wide argument. Indeed, first of all, there are different types of operating systems. Secondly, distinct philosophies interpret the problem "the management of the computer" in different ways. Therefore, as done previously, it is going to define the most important operations and the most useful tools on Linux distribution to resolve the problems.
First of all, if the operating system is Microsoft, the best way to start is the analyse by WinAudit. This tool takes over every aspect of computer inventory and configuration. For each application a series of information is shown. In addition, a useful tool exists called WhatInStartup, which displays the list of all applications that are launched at the boot of Windows. Moreover, if operating system does not belong to Microsoft family, it can start with the analyse of Internet history, browser chronology and the temporary internet files. It is necessary to identify the installed browsers and their settings in order to find where this information is. A useful program is Pasco that reconstructs an individual's internet activity. Since this analysis technique is executed regularly, the structure of the data, found in Internet Explorer activity files (index.dat files), can be researched. Pasco, whose name derives from the Latin word that means "browse", was developed to examine the contents of Internet Explorer's cache files. Moreover, graphical tools to view cache, cookie, history and to find password, saved on the most important browser, such as IE, Firefox, Chorme, Safari and Opera, exist. For instance, these software are: Chrome Cache View IE Cache View, Mozilla Cache View, MUI Cache View,Opera Cache View, Video Cache View, IE Cookie View, IE History view and IE PassView. Important programs, such as Messenger, Skype and email management, are installed within the S.O. As a consequence, all the personal information in relation to these programs is obviously stored within the system. Therefore, programs to find account info (user and password), such as Mail PassView, Live Contacts View, PSTPassword, MessenPass, and Protected Pass View, SkypeLogView, SkypeHistoryViewer, LibPST exist. Finally, the analyse also concerns the system register. For instance, within Microsoft family, a tool named RegScanner is present. It is equipped with a powerful search capability that scans the registry, in order to identify the value, supplied in input from the user, and it displays in a single window all the items identified. All these information are relevant in a crime investigation, and they can be got only analysing the S.O.

4.6.2 Files data analysis

This phase can take really long time, it is extremely ticklish because it can waste time to analyse and view useless file for own crime investigation. Thus, it is very important to have some key words to search only files that should be relevant to own aims. For example, a method could be searching all file images, or searching all files that contain a specific word or words that include your term. For each of these searches, a file list should be created. In this way, it is possible to verify the relevance of the file in relation to investigation. In this step, it is useful to know the regular expression (RE) and to use Grep, Egrep, Fgrep, Find, Locate. Moreover, after the search, it is necessary to view directly the file, and to annotate the date of the last modified file and when the file was saved on the device. If the file is protected by password, it is possible to find it through some tools, such as Advanced Password Recovery or BulkExtractor. In this phase, the computer forensic expert is usually not alone, but he needs the help of who knows if the files are relevant with respect to the investigation.

5 CONCLUSIONS AND FUTURE WORK

The paper presents a new model in relation to examination phase, which is defined on SDFIM model, about Non-Volatile memory. In addition, there are specific references to the tools available in Unix like (Linux) operating system, in order to support the objectives of the research. Indeed, the research aims at not buying software, allowing the only use of free tools. Lastly, it intends to follow the Italian legislation. In fact, if the computer forensic expert follows the proposed process, he will never go against the Italian legislation. From this conceptual perspective, the research intends to mitigate the gap between the normative approach and the pragmatic questions that characterized the computer forensic field, defining a new model. However, the model is related only to the Italian legislation because, unfortunately, in computer forensic scenario each country has its own laws. As a consequence, the model should be analyzed in relation to the laws of the country in which it should be applied. For this reason, one of the possible developments of this work is precisely the analysis in reference to other jurisdictions. However, the presented model should be enough flexible to remain unchanged in relation to normal improvements that Italian legal system will do in the field of cybercrime and computer forensics. The Linux tools with respect to each phase are limited to a brief description or mention only because their complex nature, characterized by various options, is well explained by many guides or manuals. Nevertheless, the paper provides a complete list of them and hence the way to do the analysis at low cost. The cybercrime, as explained in the previous paragraphs, is constantly expanded due to a wide range of applications. In this paper the proposed model is referred to non-volatile memory into computer forensic scenario. From these perspectives, the research could be implemented through future works. First of all, one possible future development could concern the definition of a new model into computer forensic scenario, related to volatile memory. As a result, it could be possible to analyse similarities and differences between the two models. Secondly, it could be interesting to contribute to the Sleuth Kit Hadoop, which incorporates the Sleuth Kit into a Hadoop cluster, in order to make the analysis faster. During the test, much time was spent on waiting the process. Finally, in the future works it could be possible to test the model and some upgrade in relation to cloud computing. This new challenge that is borderline between computer forensic e network forensic is extremely important for future investigations. In addition, cloud computing has numerous benefits, since it is still a new technology, there are vulnerabilities that need to be addressed[31]. Cloud consumers and providers are investigating on cloud, providing secure communication and services[31].

6 REFERENCES

1. K. Cheater and D. Harley, “Cybercrime: Out of obscurity and into reality,” *6th PwC Global Economic Crime Survey*, March 2012.

2. Marian Merritt, "Cybercrime Exposed," 2010 [Online]. Available at: http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/norton_cybercrime_exposed_booklet.pdf [Accessed: 04 March 2013].
3. A. Sivaprasad and S. Jangale,"A complete study on tools & techniques for digital forensic analysis," *Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on*, pp.881-886, 21-22 March 2012.
4. J. Vacca,"Computer Forensics: Computer Crime Scene Investigation (Networking Series) (Charles River Media Networking/Security)," May 2005.
5. R. Xu, K.P. Chow and Yang Y., "Development of Domestic and International Computer Forensics," *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011 Seventh International Conference on*, pp.388-394, 14-16 Oct. 2011.
6. Ponemon Institute, "2012 Cost of Cyber Crime Study: United States", October 2012, [Online]. Available at: http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf [Accessed: 2 March 2013].
7. M. Lesk, "Cybersecurity and Economics," *Security & Privacy, IEEE*, vol.9, no.6, pp.76-79, Nov.-Dec. 2011.
8. H. S. Newswire, "Us cybercrime losses double", March 2010 [Online]. Available at: http://www.homelandsecuritynewswire.com/us-cybercrime-losses-double [Accessed: 10 October 2012].
9. D. Bartz and J. Finkle, "U.S. shuts down massive cyber theft ring", April 2011 [Online]. Available at: http://www.reuters.com/article/2011/04/13/us-cybersecurity-coreflood-idUSTRE73C7NQ20110413 [Accessed: 13 October 2012].
10. European Commission, "Cyber security", July 2012, [Online]. Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf [Accessed: 11 October 2012].
11. P. Sundresan, "Digital forensic model based on malaysian investigation process", *International Journal of Computer Science and Networked Security*, August 2009.
12. M. M. Pollitt, "Computer forensics: An approach to evidence in cyberspace", in *Proceeding of the National Information Systems Security Conference*, Baltimore, vol. II, 1995, pp. 487-491.
13. M. M. Pollitt, "An ad hoc reviwe of digital models", in *Proceeding of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07),* Washington, USA, 2007.
14. G. Palmer, "Dtr-t001-01 technical report. a road map for digital forensic research", in *Digital Forensics Workshop*, Utica, New York, 2001.
15. S. O. Ciardhuáin, "An extended model of cybercrime investigations", *International Journal of Digital Evidence*, vol. 3, no. 1, 2004.
16. M. Reith, C. Carr and G. Gunsch, "An examination of digital forensics models", *International Journal of Digital Evidence*, vol. 1, no. 3, 2002.
17. B. Carrier, E.H. Spafford, "Getting physical with the digital investigation process", *International Journal of Digital Evidence,* vol. 2, no. 2, 2003.
18. P. Stephenson, "A comprehensive approach to digital incident investigation", *Information Security Technical Report*, vol. 8, no. 2, pp. 42-54, 2003.
19. V. Baryamureeba, and F. Tushabe, "The enhanced digital investigation process model", in *Proceeding of Digital Forensic Research Workshop*, Baltimore, MD, 2004.
20. N.L. Beebe and J.G. Clark, "A hierarchical, objectives-based framework for the digital investigations process", *Digital Investigation,* vol. 2, no.2, June 2005, pp. 147-167.
21. B.D. Carrier and E.H. Spafford, "An event-based digital forensic investigation framework", in *Proceedings of Digital Forensic Research Workshop,* 2004.
22. K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response: Recommendations of the national institute of standards and technology", *National Institute of Standards and Technology (NIST)*, Aug. 2006. [Online]. Available at: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
23. M. Kohn, M.S. Olivier and J.H.P. Eloff, "Framework for a digital forensic investigation", in *Proceedings of the ISSA 2006 from Insight to Foresight Conference,* 5-7 July 2006, Sandton, South Africa, 2006.
24. M.K. Rogers, J. Goldman, R. Mislan, T. Wedge and S. Debrota, "Computer forensics field triage process model", *Journal of Digital Forensics, Security and Law,* vol. 1, 2006, pp. 27-40.
25. F.C. Freiling and B. Schwittay, "A common process model for incident response and computer forensics," in *3rd International Conference on IT-Incident Management and IT- Forensic,* 2007.
26. D. Bem, and E. Huebner, "Computer forensic analysis in a virtual environment," *International Journal of Digital Evidence - IJDE,* vol. 6, no. 2, 2007.
27. E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," *Digital Investigation,* vol. 7, no. 1-2, pp. 14–27, Oct. 2010.

28. Agrawal, A. Gupta, M. Gupta and S. Gupta, C., “Systematic digital forensic investigation model,” *International Journal of Computer Science and Security (IJCSS)*, vol. 5, no. 1, 2011, pp. 118-131.
29. X. Wang and H. Yu, “How to break MD5 and other hash functions,” *in Proceedings of the 24th annual international conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'05)*, Ronald Cramer (Ed.). Springer-Verlag, 2005, Berlin, Heidelberg, pp. 19-35, doi=10.1007/11426639_2
30. Brown, R. and Davenport, J. "Forensic Science: Advanced Investigations," February 24, 2011.
31. S. Manavi, S. Mohammadalian, N. I. Udzir, A. Abdullah, "Secure Model for Virtualization Layer in Cloud Infrastructure", International Journal of Cyber-Security and Digital Forensics (IJCSDF), vol. 1, no. 1, pp. 32-40, 2012