University of Cagliari

PhD School of Mathematics
and Computer Science

XXVI cycle

PhD course in Computer Science

Technical and legal perspectives on forensics scenario

INF/01

Author:
Fabrizio Solinas

Supervisor:
Prof. Gianni Fenu

2012-2013

Contents

Introduction

The dissertation concerns *digital forensic*. The expression digital forensic (sometimes called digital forensic science) is the science that studies the identification, storage, protection, retrieval, documentation, use, and every other form of computer data processing in order to be evaluated in a legal trial [Gup13] [Pol10] [Tak04]. Digital forensic is a branch of forensic science. First of all, digital forensic represents the extension of theories, principles and procedures that are typical and important elements of the forensic science, computer science and new technologies. From this conceptual viewpoint, the logical consideration concerns the fact that the forensic science studies the legal value of specific events in order to contrive possible sources of evidence. The branches of forensic science are: physiological sciences, social sciences, forensic criminalistics and digital forensics. Moreover, digital forensic includes few categories relating to the investigation of various types of devices, media or artefacts. These categories are:

- computer forensic: the aim is to explain the current state of a digital artefact; such as a computer system, storage medium or electronic document [YEM*03];
- mobile device forensic: the aim is to recover digital evidence or data from mobile device, such as image, log call, log sms and so on;
- network forensic: the aim is related to the monitoring and analysis of network traffic (local, WAN/Internet, UMTS, etc.) to detect intrusion more in general to find network evidence;
- forensic data analysis: the aim is examine structured data to discover evidence usually related to financial crime;
- database forensic: the aim is related to databases and their metadata [Oli09].

The origin and historical development of the discipline of study and research of digital forensic are closely related to progress in information and communication technology in the modern era. In parallel with the changes

in society due to new technologies and, in particular, the advent of the computer and electronic networks, there has been a change in the mode of collection, management and analysis of evidence. Indeed, in addition to the more traditional, natural and physical elements, the procedures have included further evidence that although equally capable of identifying an occurrence, they are inextricably related to a computer or a computer network or electronic means. The birth of computer forensics can be traced back to 1984, when the FBI and other American investigative agencies have began to use software for the extraction and analysis of data on a personal computer. At the beginning of the 80s, the CART(Computer Analysis and Response Team) was created within the FBI, with the express purpose of seeking the so-called *digital evidence*. This term is used to denote all the information stored or transmitted in digital form that may have some probative value. While the term evidence, more precisely, constitutes the judicial nature of digital data, the term forensic emphasizes the procedural nature of matter, literally, "to be presented to the Court". Digital forensic have a huge variety of applications. The most common applications are related to crime or cybercrime. Cybercrime is a growing problem for government, business and private [Arm12].

- Government: security of the country (terrorism, espionage, etc.) or social problems (child pornography, child trafficking and so on).
- Business: purely economic problems, for example industrial espionage.
- Private: personal safety and possessions, for example phishing, identity theft.

Often many techniques, used in digital forensics, are not formally defined and the relation between the technical procedure and the law is not frequently taken into consideration. From this conceptual perspective, the research work intends to define and optimize the procedures and methodologies of digital forensic in relation to Italian regulation, testing, analysing and defining the best practice, if they are not defined, concerning common software. The research questions are:

1. The problem of cybercrime is becoming increasingly significant for governments, businesses and citizens.
    - In relation to governments, cybercrime involves problems concerning national security, such as terrorism and espionage, and social questions, such as trafficking in children and child pornography.
    - In relation to businesses, cybercrime entails problems concerning mainly economic issues, such as industrial espionage.

- In relation to citizens, cybercrime involves problems concerning personal security, such as identity thefts and fraud.

2. Many techniques, used within the digital forensic, are not formally defined.

3. The relation between procedures and legislation are not always applied and taken into consideration.

The thesis has the following structure:

1. Literature review

2. Criminal investigation steps on digital investigation

3. Live digital forensic

4. Conclusions.

The literature review chapter 1 analyses the evolution of the concept of forensic science, digital forensic, computer crime, computer crime related to economic problem and how the European Union intends to deal with these problems.
The Criminal investigation steps on digital investigation2 concerns the description and analysis of models related to the correct way to conduct an investigation. Moreover, this chapter emphasizes the lack of a contextualisation in relation to the legal system in which the model could be applied. From this conceptual perspective, a model for non-volatile memory is defined and contextualised in relation to the Italian legal system.
The Live digital forensic 3 analyses how it is possible to trace evidence to the RAM of personal computer. In particular, some applications on Windows XP and Windows 7 operating systems, which represent the most used, are compared. The last, chapter 4, analyses the conclusive aspects concerning the research work. Moreover, it proposes some recommendations related to the discussed case study and the literature it is based on.
In conclusion, the aim of this thesis is to analyse some problems that cybercrime entails for police during investigations. Among these problems,the research work studied the analysis of both volatile and non-volatile memory. Moreover, not only is the analysis from the computer science viewpoint, but also from the legal system perspective, respecting the Italian legislation.

Chapter 1

Literature review

The frequency of cyber attacks is constantly increasing and cybercrime represents the principal cause of the these attacks. The term cybercrime concerns crimes that are committed through the Internet, including different types of crimes, such as, child pornography, the development and diffusion of virus, identity theft and industrial espionage. Indeed, according to Interpol, cyebercrime represents one of the areas that show a grater growth at international level, becoming one of the principal prerogative of organised crime.
From this conceptual viewpoint, this chapter aims to define the research context. The chapter is structured in four sections. In the first 1.1, the evolution of forensic science concept is analysed. In the second paragraph 1.2 the concept of digital forensic is defined with its major applications and in relation to cybercrime. The third 1.3 highlights the economic problems of cybercrime. The last paragraph 1.4 concerns the European Union's influences in relation to this important question,cybercrime and how to contrast that.

1.1 The evolution of concept of forensic science

Forensic science derives from diverse disciplines, such as geology, physics, chemistry, biology, and mathematics, in order to study physical evidence related to crime. If it is suspected that a person has died from poisoning, for example, a toxicologist, who specializes in identifying poisons and their physiological effects on humans and animals, can assist the forensic expert in the investigation. Experts in other areas, such as botany, forensic pathology, entomology, and archaeology, may also provide helpful information to criminal investigators. Overall forensic science is a scientific method

of gathering and examining evidence [BPW06]. Moreover, criminal case is solved with the use of pathological examinations that gather fingerprints, palm prints, footprints, tooth bite prints, blood, hair and fiber samples. In addition, samples of handwriting and typewriting are studied, including all ink, paper, and typography. Ballistics techniques are used to identify weapons as well as voice identification techniques are used to identify criminals [JJN05].
The first official application of specific scientific branch in the solution of a crime was represented by the use of medical knowledge. In the 1248, in the Chinese book Hsi DuanYu or the Washing Away of Wrongs, ways to distinguish between death by drowning or death by strangulation were described [Ben01]. On the other hand, an Italian doctor, Fortunatus Fidelis is considered as the first person to practice modern forensic medicine, beginning in 1598. From this perspective, forensic medicine is the "application of medical knowledge to legal questions." It became a recognized branch of medicine in the early 19th century, when it was observed that contact between someone's hands and a surface left barely visible marks called fingerprints [JJN05]. As a result, fine powder (dusting) was used to make the marks more visible.
On the other hand, modern fingerprint identification dated at 1880, when the British scientific journal, named Nature, published letters by the Englishmen Henry Faulds and William James Herschel described the uniqueness and permanence of fingerprints [Ben01]. Their hypothesis were verified by the English scientist Sir Francis Galton, who developed the first elementary system for classifying fingerprints based on grouping the patterns into arches, loops, and whorls. Galtonś system was improved by London police commissioner, Sir Edward R. Henry. The Galton-Henry system of fingerprint classification was published in June 1900, and officially introduced at Scotland Yard in 1901 [Ben01]. It is the most widely used method of fingerprinting.

1.2 Digital forensics and computer crime

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 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 analysed 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 above-mentioned branches. Indeed, for example, digital forensic branches are: computer forensics, forensic data analysis, database forensics, mobile device forensics, network forensics, forensic video and forensic audio [Cas11]. From this conceptual perspective, after this clarification, it is important to highlight that all discovered evidences should be convincing and sufficiently reliable to stand up in court. Sivaprasad and Jangale [SJ12a], in our definition, support these theses. 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 [SJ12b] [SJ12a]. The digital evidence can be found in computer (hard disks, RAMs or graphics cardś RAM), mobile phones, iPods, pen drives, digital cameras, CDs, DVDs, floppies, computer networks, the Internet etc. [Vac05] 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 [Ben01]. As a consequence, the digital forensics focuses on finding digital evidences after a breach of computer security has occurred. It consists in the analysis of information that are 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 commit 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 subjected to the main body of the law, and must be executed in accordance with the manner required by law and procedures [XCY11].

Whichever organization, businesses or government, is actually making an effort to contrast cybercrime, which is whichever crime that involves any computer, tablet, smartphone or digital device and network [Moo06]. 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 activities have entailed both a new type of economic crime and new vectors to facilitate existing economic crimes [KC12].
Today, cybercrime relates to governments, businesses and private citizens for different issues. First of all, governments has faced this issue because it represents a social problem [ZMLJ11] (child trafficking, child pornography[1], terrorism [San11], etc.) and, at the same time, a security challenge (espionage, terrorism, etc.). Secondly, in this specific field, business risks 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 periods, the threat landscape, once dominated by worms and viruses created by irresponsible hackers, is now ruled by a new type of criminals. 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 [Mer10].
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 [PL12]. 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, juvenile

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

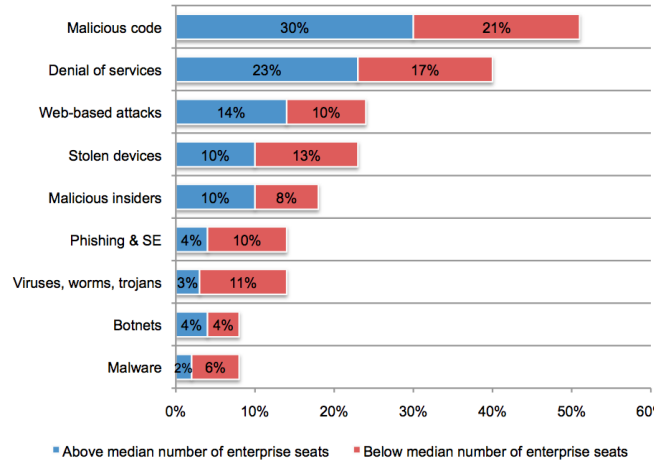

Figure 1.1: *The cost mix of attacks by organizational size [Ins12].*

pornography[2] .

1.3 Economic problem related to computer crime

Cyber-attacks are growing, as well as necessary economic costs to contrast them [FAS12]. 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", [Ins12], 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 1.1, 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. In according to the survey, information theft and disruption continue to represent the highest external

[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.

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 totalled 30 percent of the external costs, increasing by 1 percent compared to 2011. The average time that is necessary to definitely suppress 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 last year estimated average cost, or $ 415,748 in a 18 days period. In support of this study, bank robbers steal approximately $100 million per year in the US [Les11]. Phishing alone resulted in $120 million per quarter [XCY11]. A single botnet ring took $100 million before the FBI managed to stop it [DB11].
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 [Soc12].
Finally the evolution of computer security software and other defences 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 those of simpler attacks on Windows and applications, the impact of these complex attacks can be far more devastating.

1.4 European Union's influences

The extraordinary development of information technology leads to obvious consequences for organized "traditional" crime. The use of systems and computer networks is an undeniable step forward for the company, but it makes it more vulnerable. Terrorist groups, networks related to pornography or paedophilia, trafficking in arms, drugs, human beings, money laun-

dering and cyber criminals, exploit this vulnerability and the development of these new media to increase their illegal activities. The Budapest Convention [bud01], made by a committee of experts in approximately 4 years of work, is in fact the first international agreement to frame the crimes related to the Internet and computer network. In particular, one of the principal aims is to extend the scope of computer crime to all crimes, committed in any way, through a computer system, even in the case in which the proof of the offense is in electronic form [bud01].
The Budapest Convention, signed in 2001 and divided into 4 chapters [bud01], entered into force on July 1st 2004 in Italy, and it is the only international binding treaty that exists today for this scope. The treaty establishes guidelines for all states that wish to develop a comprehensive national legislation against cybercrime. It shall be open for signature by non-European states, providing the framework for international cooperation in this field [bud01]. The treaty is supplemented by an additional protocol concerning the criminalization of racist and xenophobic nature acts committed through information systems [bud01]. Although, establishing effective rules in relation to a place where all people have access but it does not belong to anyone, it is a very daunting task, it is necessary to have standards to maximize freedom reducing to a minimum the risks of navigation on cyberspace.
In more detail, the convention aim is to harmonize the criminal offenses related to computer crime. Moreover, it provides, to the signatory countries, the appropriate tools to investigation and prosecution of crimes related to the computer and finally, to build an effective system of international cooperation, which must be: a) provided the greatest extent possible, b) extended to all offenses relating to systems and computerized data, c) consistent with international agreements [bud01]. In view of the fact that the technologies are evolving faster than legal solutions to solve problems, it is necessary to constantly face new challenges. They are often related to data protection issues, such as access and exchange of data beyond borders between the police forces and information sharing and between the public and private sectors. In accordance with the Convention, member states must make important changes to the offenses under the criminal code. These modifications are related to: illegal and intentional access, without right, to an information system entirely or partially; the illegal wiretapping that are intentional and unlawful interceptions of computer data, carried out through technical means, during non-public transmissions; the aggression on the integrity of the data (damaging, deletion, deterioration, alteration or suppression of computer data) done intentionally without authorization; the attack to integrity of the systems that is translated into a serious impediment to the functioning of an information system, carried out intentionally without right through the damaging, deleting deterioration, alteration, suppression of computer data; intentional abuse without authorization of

devices (that is the production, sale, procurement for use, the importation, distribution and other forms of provision) including computer software, designed to allow the commission of the crimes listed above, as well as keyword (password) or access codes or similar systems that permit entire or partial access to information system [bud01]. Although many of these issues, such as computer fraud, unauthorized access to computer systems, child pornography, the interception of telematics data, are largely covered by the Italian law, important changes have been introduced in relation to administrative responsibility of legal persons and to the privacy law. Indeed, stricter dispositions, concerning administrative responsibilities related to cybercrime, are introduced. In addition, companies that do not implement measures to prevent cyber crimes, committed by their staff, will face severe penalties for patrimonial responsibility. Moreover, the Convention provides a power extension to police force to obtain the data from the operators. They may be forced to conserve and protect the data relating to ITC traffic for 6 months and they are required to the immediate release of the information and to the maintenance of secrecy on orders under penalty of imprisonment up to 3 years. The achieved results and challenges were discussed at the annual conference of the Council of Europe Convention on Cybercrime, held on 21 and 22 November in Strasbourg that was followed by a special meeting to celebrate the 10th anniversary of the Convention, November 23, 2011.

Chapter 2

Criminal investigation steps on digital investigation

This chapter 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 [GL07], 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 work was presented at the Cybersec2013 [FS13b] and in an article on International Journal of Cyber-Security and Digital Forensics (IJCSDF) [FS13a].
This chapter is composed of five parts. The Section 2.1 presents an overview of current models. The Section 2.2 concerns an overview of the Italian legal system into the computer forensics scope. The Section 2.3 illustrates the proposed model in a detailed way and its contribution to the state of the art. The Section 2.4 presents the novel model limitations and the last part 2.5 completes the chapter through the improvements and future works.

2.1 Overview

In 2001 Kruse and Heise [Per09] developed one of the first model in digital forensic. The process showed in Figure 2.1 is essential. Indeed, it consists

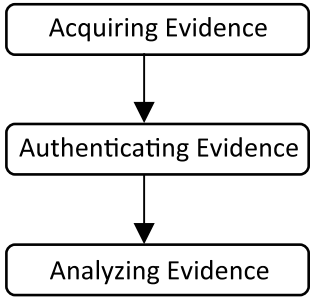

Figure 2.1: *Kruse & Heiser Model [Per09].*

in 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.

Moreover, different models have been developed [Pol07a] [YYH11] [SPRT13]. Table 2.1 shows a complete list of digital forensic investigation models based on chronological order.

Table 2.1: *List of complete digital forensic investigation model*

Model Name	Inventers	Years	Number of phases
Computer Forensic Investigative Process [M.M95] [Pol07b]	M.Pollitt	1995	4 Phases
DFRWS Investigative Model (Generic Investigation Process) [Pal01]	Palmer	2001	6 Phases
Scientific Crime Scene Investigation Model (SCSI) [Cia04]	Ciardhuain	2001	4 Phases
Abstract Model of the Digital Forensic Procedures (ADFM) [MR02]	Reith ,Carr and Gunsh	2002	9 Phases
Integrated Digital Investigation Process (IDIP) [Car09]	Carrier and Spafford	2003	5 Phases
End To End Digital Investigation [Ste03]	Stephenson	2003	6 Phases
Enhance Integrated Digital Investigation Process (EDIP) [Tus04]	Baryamureeba and Tushabe	2004	5 Phases
Extended Model of Cyber Crime Investigation [Cia04]	Ciardhuain	2004	13 Phases
A hierarchical, Objective Based Framework for the Digital Investigations Process [Bee04]	Beebe and Clark	2004	6 Stages
Event Based Digital Forensic Investigation Framework [CS04]	Carrier and Spafford	2004	16 Phases
Forensic Process [KCGD06]	Kent K, Chevalier, Grance and Dang	2006	4 Phases
Framework for a Digital Forensic Investigation [KOE06]	Kohn , Eloff and Oliver	2006	3 Phases
Computer Forensic Field Triage Process Model (CFFTPM) [RGM*06]	K.Roger, Goldman, Mislan, Wedge and Debtota	2006	12 Phases
Investigation Process model [FS07]	Freiling and Schwittay	2007	4 Phases
Dual Data Analysis Process [BH07]	Bem and Huebner	2007	4 Phases
Digital Forensic Model based on Malaysian Investigation Process (DFMMIP) [Per09]	Perumal S.	2009	7 Phases
Network Forensic Generic Process model [PJN10]	Pilli, Joshi and Niyogi	2010	9 Phases
Systematic Digital Forensic Investigation Model [AA11]	Ankit Agarwal, Megha Gupta, Saurabh Gupta and Prof (Dr.) S.C. Gupta	2011	11 Phases

2.2 The Italian legal system within computer forensic scenario

Due its nature, the Internet cannot be within a single jurisdiction, so consequently the computer forensics is closely related to this concept [Bro04] [MD09]. For this reason, this section aims at providing an overview of how the crimes are handled by the Italian legislation within the computer crime. 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 devices. The analysis could concern:

- Offences within 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 Convention is supplemented by an additional protocol concerning the criminalization of racist and xenophobic nature acts, committed through electronic systems. Italy, thanks to law 18 March 2008 no. 48 [rat08], has ratified the Council of Europe on Cybercrime, signed in Budapest on 23 November 2001. This law, among the numerous 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 distortions." [pro08];
- Article no. 247, after paragraph 1 it is inserted as follows: "1-bis. When there is a reason for believing 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 distortions. " [pro08];
- 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" [pro08];

- Article no. 254 has entailed the following changes:

  a) Paragraph 1 is replaced by the following: "1. Who provides postal, telegraphic, electronic or telecommunication service is allowed to proceed to the seizure of letters, fold, parcels, values, telegrams and other items of correspondence, even if submitted electronically, and 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." [pro08];

- 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." [pro08];

- 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." [pro08];

- Article no. 259, paragraph 2, after the first sentence 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." [pro08];

- 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." [pro08] 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 allows 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[1]) 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[2] 11th February 2005 no. 68 (in the field of PEC[3]).

Article 44 of CAD[4] 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, 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.

[1]Corresponding to statutory instrument.
[2]Decree by President of Italian Republic.
[3]Certified web mail.
[4]Italian code for digital administration

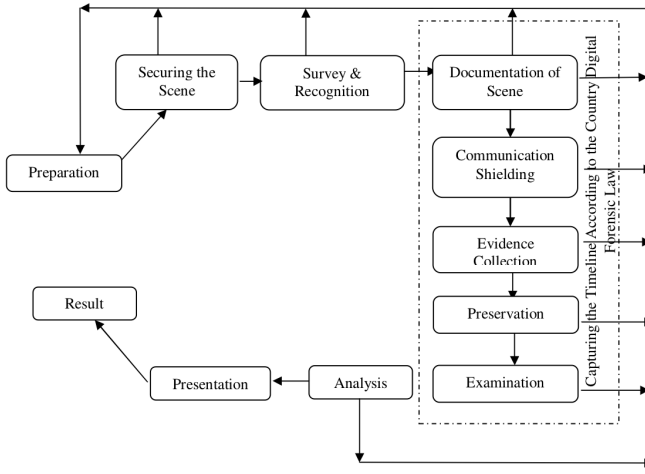

Figure 2.2: *Phases of Systematic Digital Forensic Investigation Model (SRDFIM) [AA11].*

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 have to 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 devise that 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 defence investigations. Indeed, for example, when the "computer forensic expert" is nominated by the prosecutor, he obtains the status of public official, and his statements are true until proved otherwise. In conclusion in this paragraph the Italian legislation in relation to this field is analysed in order to underline how it is continuously evolving.

2.3 The novel model to satisfy the legal system

In relation to the Table 2.1, first of all, the research analyses the last model "Systematic Digital Forensic Investigation Model" that is showed in Figure 2.2 and it consists of eleven steps [AA11].

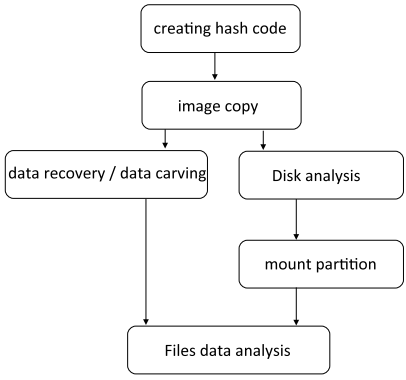

Figure 2.3: *Phases of Examination's SRDFIM phase [FS13b].*

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 time-line 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 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 research analyses in detail only the eighth phase called "Examination" related to the non-Volatile evidence. As a result, the study 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 [KGR06].
The development of the "Examination" phase is led to create a list of steps that are summarized in Figure 2.3.

In relation to the chart, the first step is to create the hash code of the 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 to each other. 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 case studies 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, where the majority of additional tools are free and also open source. The last aspect is extremely important, indeed it is possible to know what happens "under the hood" and if they are used in correct way. As a consequence, 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 does 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 research, there are not references to Sleuth Kit toolkit[5] tools while Autopsy[6], which is a graphical interface to the digital investigation tools in the Sleuth Kit. 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.

2.3.1 Creating hash code phase

The first step is "creating hash code". This phase concerns the creation of hash[7] code, usually MD5 or SHA, of drive. In relation of this step, it

[5]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.

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

[7]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

is extremely important to know that in 2005, Xiaoyun Wang and Hongbo Yu proved how breaking MD5 and Other Hash Functions [WY05]. 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 present 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.

2.3.2 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 files and directory structures. The majority of the tools, used to analyse 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 synthesized in Figure 2.4.

various points during the investigation in order to ensure that the examination process does not modify the examined image [RMB11].

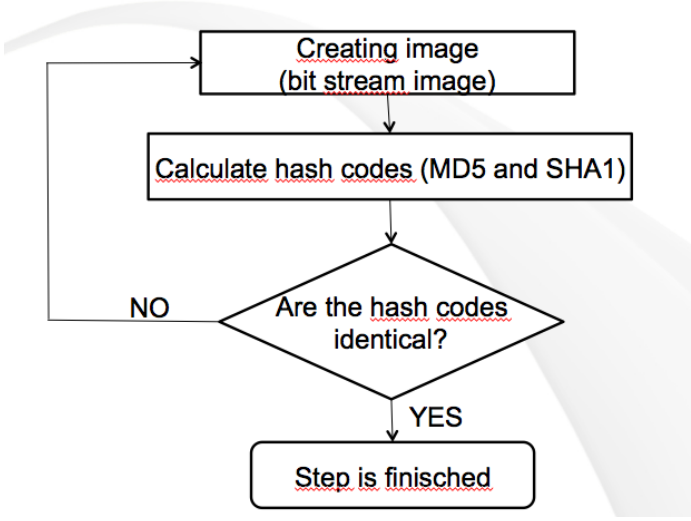

Figure 2.4: *Flow chart of image copy phase.*

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.

2.3.3 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[8] 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 requirements. 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.

2.3.4 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.
First of all, partition recognition aims at identifying the partition of the device. The mass memory could have more than one partition, such as primary partitions, extended partition and 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.
Secondly, 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 are 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

[8]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.

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 mass memory 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.

2.3.5 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, in each part of the world, it is essential that all procedures can be done again and the data are not modified or distorted. The mount command allows connecting a file system to a system folder. In relation to the steps in Figure 2.3, the mount is not directly within 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 does not change;
- noexec option, so running file is not permitted.

2.3.6 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 described 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, an 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 [Car05]. 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 tool is 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 they 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.

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 analysis 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, in relation to these programs, all

the personal information 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 analysis 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 all the items identified in a single window . All these information are relevant in a crime investigation, and they can be got only analysing the S.O.

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 wit respect to 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.

2.4 Limitations and known issues

The chapter 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

despite the Budapest Convention. As a consequence, the model should be analysed in relation to the laws of the country in which it should be applied. 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 research 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.

2.5 Improvements and future works

The presented research focuses on Italian legislation, for this reason, one of the possible developments of this work is precisely the analysis in reference to other jurisdictions. The necessary work to match the model to other jurisdictions should not be complicated if the analysed state has rectified the Budapest Convention.
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 the Sleuth Kit Hadoop, which incorporates the Sleuth Kit into a Hadoop cluster, in order to make the analysis faster. In addition there are other scalable software such as the tool described on [Rou11]. 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 upgrades in relation to cloud computing. This new challenge that is borderline between computer forensic and 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 [Man12]. Cloud consumers and providers are investigating on cloud, providing secure communication and services [Man12].

Chapter 3

Live digital forensic

This chapter presents a case study of Live Digital Forensics (LDF) on the two most popular operating systems: Windows XP and Windows Seven [GS13]. More in detail it describes the research activity branch regarding the live digital forensic on Windows systems. The case study focuses on some common applications running on these systems. Additionally, as many types of applications rely on commercial software, one of the main goals of this work is to restrict to the use of free software, in order to prove that the same results can be achieved while minimizing costs. The rest of this chapter is organized as follows. Section 3.1 discusses what live digital forensic is, in order to provide a clear and comprehensive definition of this concept. The second part (Section 3.2) describes the main differences between Windows XP and Windows 7 while the third part (Section 3.3) will present some tests. Section 3.4 will discuss the tests limitations and, finally, Section 3.5 will go through improvements and future works.

3.1 Overview

Over the last few years, analysing a computer or a digital device has become a necessity in the field of criminal investigations [OS11a]. Traditional digital forensics analysis includes static analysis, which concerns data that are permanently stored in devices, and live analysis, which regards data that are temporarily stored in equipment or that transit in networks. Whichever organization, businesses or governments, are actually making efforts to contrast cybercrime.
Moreover, although digital forensics has recently faced new challenges [Cal09], it still remains the main way to investigate digital evidences and to answer questions in relation to previous digital states and events [Car09]. Indeed, the Internet is one of the main means to attack an organisation. Nowadays,

governments and organisations are increasingly reinforcing their reliance on cyber technologies, such as cloud computing, on-line banking and social networks. In tandem, the rate of innovation in new technologies is expanded and organisations are struggling to keep up with the risks of introducing and using new technologies. Cyber activities have provided both a new type of economic crimes and new vectors to facilitate existing ones [CH12].
Nowadays, cybercrime has interested 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 concerns 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 periods, 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 that is 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 [Mer10].
In this scenario, computer security and digital forensics analysis are both correct solutions in order to prevent and to search evidences in relation to: data theft, industrial espionage, unauthorized access to computer systems company, damage to 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 risk 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 forensics is increasingly becoming important for 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 on-line banking fraud, terrorist operations, phishing or child pornography , juvenile pornography.
From this conceptual framework, the research work describes a case study of LDF on the two most popular operating systems: Windows XP and Windows 7. For the last several months, Microsoft has emphasized the importance of migrating from Windows XP to Windows 7, but even now more than 30 percent of computers are equipped with this OS (Figure 3.1 [neta]).

MONTH	WINDOWS 7	WINDOWS XP	WINDOWS VISTA	WINDOWS 8	MAC OS X 10.8	OTHER
June, 2012	41.59%	43.61%	6.72%	0.18%	0.03%	7.87%
July, 2012	42.21%	42.86%	6.60%	0.20%	0.28%	7.86%
August, 2012	42.76%	42.52%	6.15%	0.23%	1.41%	6.93%
September, 2012	44.04%	41.23%	6.05%	0.30%	1.60%	6.79%
October, 2012	44.69%	40.66%	5.80%	0.41%	1.85%	6.59%
November, 2012	44.71%	39.82%	5.70%	1.09%	2.14%	6.54%
December, 2012	45.11%	39.08%	5.67%	1.72%	2.27%	6.15%
January, 2013	44.48%	39.51%	5.24%	2.26%	2.44%	6.06%
February, 2013	44.55%	38.99%	5.17%	2.67%	2.61%	6.01%
March, 2013	44.73%	38.73%	4.99%	3.17%	2.65%	5.73%
April, 2013	44.72%	38.31%	4.75%	3.82%	2.82%	5.59%

Figure 3.1: *Desktop Top Operating System Share Trend (June, 2012 to April, 2013) [neta].*

LDF is the branch that focuses on the analysis of volatile memory [SETB08]. Volatile memory is the work memory and it requires power to maintain the stored information, in other words it needs power to reach the computer memory. Hence the analysis of this memory is extremely sensitive to whatever happens [OS11b]. The idea is to make a dump of a volatile memory for off-line analysis [HBN09].
An investigator can then build the case through the analysis of the memory dump in an isolated environment that does not alter original evidences. This approach addresses some of the issues to live digital forensics analysis [N.11]. First of all, this approach limits impact on the compromised system. Secondly, the analysis is repeatable and it is possible to ask new questions later. In addition, off-line volatile memory analysis does not allow to compromise machine on operating system. This enables detection of hidden processes through installation of rootkit or a similar tool [Wea08].
Few years ago, copying memory from an external storage device without modifying the memory's contents was possible thanks to a special preinstalled hardware [CG04]. Today, different tools for memory analysis are proposed such as FATKit [JWFA06], Volatools [WJ07], FACE [CCM*08] and bodySnatcher [Sch07].

3.2 Overview of main differences between Windows XP and Windows 7

Windows XP has represented a crucial point in the successful period of economic and technological expansion of Windows. After Windows XP, different operating systems have alternated in the international scenario

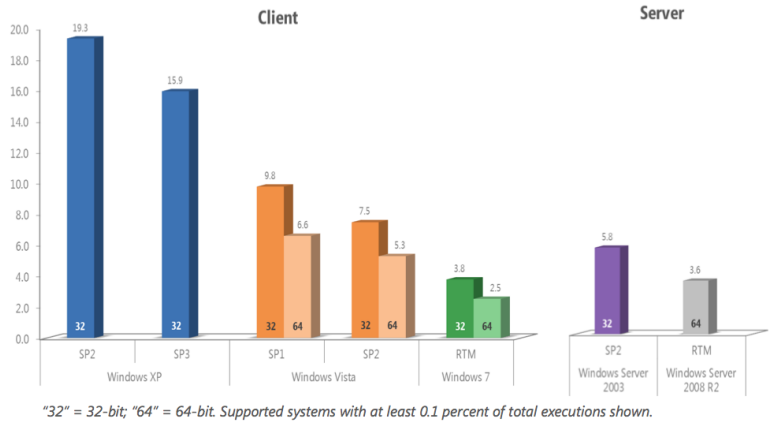

Figure 3.2: *Average quarterly infection rate (CCM) by operating system and service pack in 2010 [DC10].*

such as Windows Vista and, most recently, Windows 7 and Windows 8. Each operating system is unique in its own way [Car07]. Windows XP was released the 31 of December of 2001. In May 2012, XP still had a 44.26% share of the entire operating system market [urlc] whereas in April 2013 XP had 38.31 % and 7 44.72% [urlb]. Many users think that Windows XP is still sufficient for their needs and they do not understand the value of upgrading to a more recent system. However, Windows 7 is four to five times less vulnerable to malware infections than Windows XP [DC10]. Overall, as the figure 3.2 shows, the study has emphasized how the more recent Microsoft operating systems, which have the latest service packs, have a lower infection rates in relation to the older ones. Indeed, Windows 7 and Windows Server 2008 R2 have the highest marks for security [DC10]. On the other hand, XP still has an important slice of trade and for this reason Microsoft is going to continue supporting it until April 2014, though XP can no longer be purchased.

In relation to XP, Microsoft has introduced many new features and improvements. Some of these are improvements in security and overall performance, other ameliorations are connected with better compatibility with other programs. However, despite these improvements, different reasons should make upgrading to Window 7 tempting. First of all, Microsoft Windows 7 aims at accommodating the new emerging trends, such as the constant development of hardware (monitor touch, spread of 64-bit processors, solid state drives, multicore processors, etc..), the increasing popularity of mobile computing devices (Netbook, Tablet, Smart Phone), the use of home networks and the deployment of Media Center. Logically, all these functionalities need higher minimum requirements. Indeed, for supporting Windows

7 a machine should be equipped at least with

- a 1Ghz 32 bit processor;
- 1 GB of RAM (32-bit version) or 2GB of RAM (64-bit version);
- 16 GB of Hard Drive (32-bit version) or 20 GB (64-bit version).

The main new features of the operating system are:

- New Taskbar: in Windows 7 taskbar running programs are grouped under a single icon that is smaller than in Windows XP. In this way, Windows 7 saves space. Moving the mouse over the icon, the operating system provides a preview of the content and the possibility to access more quickly to the desired window;
- Home and Remote Media Streaming: it allows to use personal computer as a multimedia container file (images. music, video) in order to access files from external computers in a quickly way or to send playback to compatible devices (eg TV);
- Windows Touch: it allows the user to interact with the operating system directly using her own hands, through a touch system;
- Windows XP mode: it allows to run the applications that have been developed for Windows XP in a special virtualized environment;
- Windows Firewall and Windows Defender: the operating system is integrated with the new versions of Microsoft programs for the protection of PCs against intruders and malware or spyware;
- BitLocker: the operating system natively provides a tool to encrypt and decrypt the entire content of the hard disk;
- Jump Lists: right click on one of the icons in the taskbar opens a menu that contains the typical operations performed by the program and the list of recently opened documents. Jump Lists are created automatically by the operating system, but it is possible to create a software customizations for the user and for the developer . The presence of recently opened documents in the new Jump Lists makes this tool very interesting from the point of view of the forensic analysis.
- Troubleshooting Center: a new tool is accessible from the Control Panel that gives you a report of problems on your computer (e.g. connectivity failures, configuration of hardware devices and drivers, problems with application software) and it suggests possible solutions;

- New User Access Control: the User Access Control is a feature of Windows 7 that stops the execution of applications that are considered dangerous. In Windows Vista, this feature could only be turned on or off, while in Windows 7, one can set four levels of granularity;
- New Parental Control: The Parental Control is the feature that allows parents to protect and restrict the use of computers to children. In particular, you can limit the time access, you can block a certain game and you can prevent access to certain applications.

Overall, Windows 7 is faster than Windows XP. Networking computers together is easier and more streamlined than in XP or Vista. Moreover, in Windows 7 the upload and download speeds for data are improved. This includes increased speeds for browsing the internet and downloading files. XP has never been known for having good security. Indeed, User Account Control (UAC) has been introduced with Vista and later it has been kept in Windows 7 but with additional controls and improved functionalities. UAC is simply a security feature that helps to block viruses and malware. Although, it is not infallible, it certainly limits the damages that certain types of malware can do to a PC. In addition, even if XP performs well, playing computer games in Windows 7 takes gaming to a new level. Microsoft's DirectX 10 technology offers better graphics and sound. Additionally, it provides better performance even with a mid-range PC.
However, in order to ease the transition to Windows 7, Microsoft has included what it is well-known as "XP Mode". This feature is available with the Professional, Enterprise, and Ultimate versions of Windows 7. XP Mode is a way of installing and running programs that are not compatible with 7. It is a great yet cost effective tool that can allow one to go back and forth between XP and 7. In addition, Microsoft is also suggesting that organizations can save money by moving from Windows XP to Windows 7 [AG12]. Microsoft clearly wants to wrest the venerable 10-year-old Windows XP from the grip of organizations that have depended on it. Windows XP has been embraced by the commercial world in a surprising way. IDC's report, "Mitigating Risk: Why Sticking With Windows XP Is a Bad Idea," [AG12] is a financial analysis based on interviews with nine "large" organizations (an average of 3,680 employees). This study quantified the costs associated with staying on Windows XP, including lost user productivity time, as well as IT support and help desk costs. On the other hand, the study does not analyse an important and fundamental factor that is represented by the costs associated with updating applications to run on Windows 7. Of course, security should be a principal concern for those organizations that still use Windows XP. Indeed, the OS is going to lose security-patch support by April 8, 2014 in accordance with Microsoft's product life cycle schedule. Windows XP is moving out of its "extended support" phase, which means "the end of security updates, (paid) hot fix agreement support, and per-incident support

services," according to IDC's report [AG12]. An alternative option for organizations might be to pay Microsoft for "customized support," but this can be an expensive option. According to an IDC study, that the annual cost for organizations to maintain a Windows XP-based PC is $870. The same cost for a Windows 7-based PC is $168. As a consequence, organizations potentially can save about $701 per PC per year by moving to Microsoft's newer OS, according to the report. The report breaks down Windows XP user productivity costs into six categories, including time lost to malware, time taken to reimage a PC, reboot waits, downtime and time waiting for help desk support. Reboots and malware constitute the top two productivity time drainers among users. Finally, according to the report: "Moving to Windows 7 will reduce the time invested in patch management by 82%," [AG12].

3.3 The case studies on Microsoft Windows system

The research analysis has been conducted in different virtual machines. In these types of test, the use of virtual machines is fundamental. Indeed, in order to repeat test, and therefore to insert data into table, it is necessary that test could be replicable and results of each test do not vary in relation to unpredictable causes. From this perspective, the test, mentioned below, has been repeated for seven times in order to obtain the certainty of data. Moreover, in order to make the study more detailed, it has been conducted tests on systems, different from virtual machine, that have validated the obtained results. However, these tests have not been taken into consideration due to the impossibility to repeat them and, as a consequence, the invalidity of the scientific data. First of all, it is necessary to explain the configuration of the host systems and secondly the configuration of the virtual machines. The host system configuration is a MacBook Pro 15-inch, late 2008 with OS X Lion 10.7.5 equipped with:

- Processor: 2.93 GHz Intel Core 2 Duo;
- Memory (RAM): 8GB of RAM;
- Graphics: NVIDIA GeForce 9400M 256MB.

The virtualization system is VMware Fusion Professional 5.0.3. Two different virtual machines are used to run tests. The first is equipped as follows: Windows XP Professional service pack 2 with 512 MB and 15 GB of HD, while the second is equipped with Windows 7 Professional 32 bit with 1 GB of RAM and 15 GB of HD. In both systems, the following software is installed: Skype 6.0.0.126, Google Talk 3.7.1.9330, Internet Explorer 8.0.7600.16385 (IE). Moreover, the following accounts are created

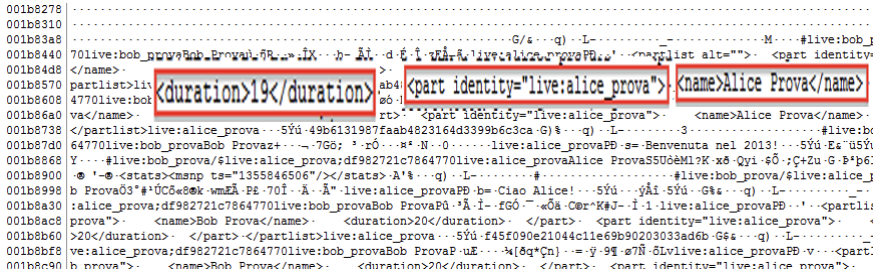

Figure 3.3: *Dump RAM: Skype focus.*

to make the use of this software possible: two Facebook accounts (Alice Prova, Bob Prova), two Hotmail accounts (alice_prova@hotmail.com, bob_prova@hotmail.com), two Gmail accounts (alice.prova.0gmail.com, bob.prova.0gma one Yahoo account (alice_prova@yahoo.it). Google Talk needs the use of the Gmail account, while Skype requires the use of Hotmail account. Indeed, Windows Live Messenger accounts are switched into Skype account in April 2013. The tests are divided into steps, which are:

- Starting up the virtual machine;
- Use of the analysed service;
- Acquisition of the dump;
- Dump analysis.

The software FTK Imager [Sof12] is used to do the acquisition. FTK Imager is present, by default, on the live CD of DEFT. The Dump is saved in an external drive, connected by the USB.

3.3.1 Skype's RAM analysis

After the starting up, in each virtual machine Skype runs. As a consequence, it is logged with alice_prova and it is added Bob's account (bob_prova). After that bob_prova is showed in contact list, first of all a chat starts and then a skype call, secondly Alice signs out from the Skype. Nothing about the history of Skype account will be saved because it is setted. The fourth step is showed in the figure 3.3, where through the dump analysis it is possible to find information about the chat, the source's account and destination's account. Therefore, by the RAM's dump it is possible to find all the communications of Skype activities.

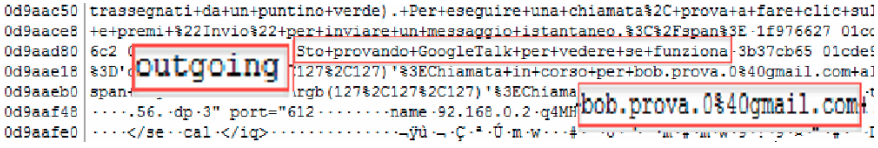

Figure 3.4: *Dump RAM: Google Talk focus.*

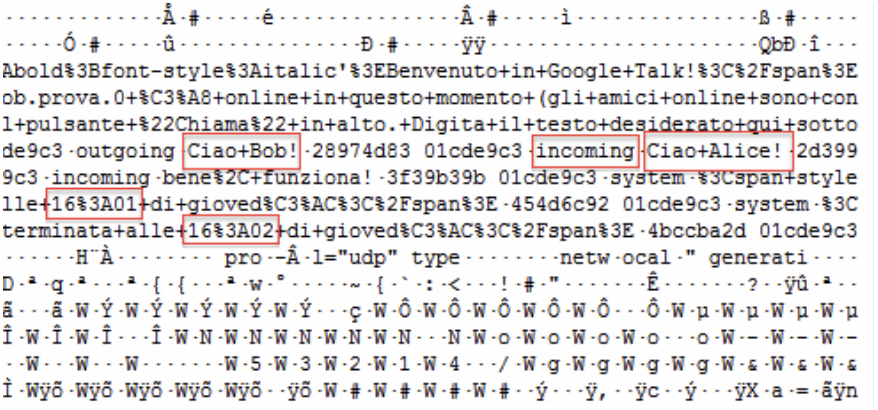

Figure 3.5: *Dump RAM: Google Talk focus.*

3.3.2 Google Talk's RAM analysis

After the preliminary operation of starting up (run VM and run Google Talk), from the account alice_prova.0@gmail.com it is added bob_prova.0@gmail.com After the presence of bob_prova.0@gmail.com on the list of contacts, a chat starts and after this a call of few seconds. From the analysis, it is possible to find evidences in relation to both actions. First of all, it has been recovered the entire chat conversation and information about the start date and end date of the conversation. However, the two considered operating systems do not show significant differences. In the pictures 3.4 and 3.5 some frames of chat and the date of the start and of the end of a brief conversation are highlighted.

3.3.3 Internet Explorer's RAM analysis

IE is tested on Facebook, Gmail, hotmail and Yahoo. The choice of this browser is related to the fact that it is the more used browser in the web (Figure 3.6). For each of the virtual machines, Windows XP and Windows 7, the browser applications have been verified using the portals Facebook, Yahoo, Hotmail and Gmail, which are some of the most used in the world. The tests are made using Internet Explorer in two ways: normal mode and

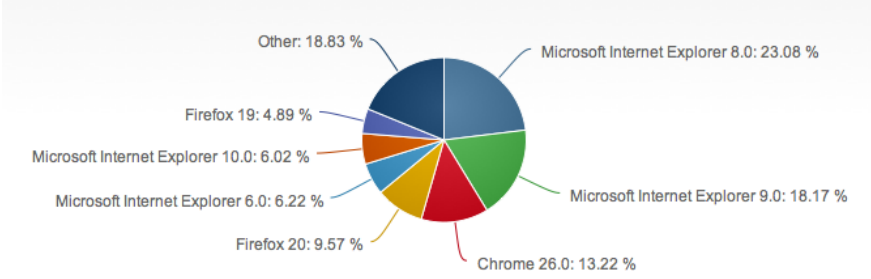

Figure 3.6: *Desktop top browser share trend [urla].*

private mode. The second does not record your browsing history, and, at least in theory, it should not leave traces on your computer, in the form of cookies, when you close the window or Tab[1].

The scenario for each sub-section is the same. For each VM, first of all, after the system is ready, Internet Explorer runs. By default, IE opens www.google.it web page, the correct url is typed and logged to web portal with alice_prova account. In the case of tests in private mode, after IE runs it is necessary to start the private mode and to type the correct url. Dump of RAM is done for each single test. When the browser is opened, it is necessary to logout first and then to do the dump.

Facebook

The Facebook tests focus on the chat activities. After alice_prova is logged, bob_prova account is added to the list of friends and after the friend acceptance, a chat starts. The chat lasts for 5 minutes. The tests are split in chat with browser in normal mode a private mode and, as a result, the RAM dump is done in the two cases: closed and opened browser. However, in those cases the logout is always done. As it can be seen on Table 3.1 and Table 3.2, there is only one different result between XP and 7. This concerns the case in which the browser works in normal mode and when the browser is opened during the dump. Logically, the logout from Facebook is guaranteed. In this specific case on the Windows XP, it is possible to find the no encrypted account's password; whereas on Windows 7 the password is not present in the dump. The research keywords used on the dump are: *Facebook*, *_prova*, *alice*, *bob*.

[1]In the area of graphical user interfaces (GUI), a tabbed document interface (TDI) or a Tab is one that allows multiple documents to be contained within a single window, using tabs as a navigational widget for switching between sets of documents. It is an interface style most commonly associated with web browsers, web applications, text editors, and preference panes.

Yahoo,Hotmail and gmail

The Yahoo and Hotmail tests focus on the mail activities. The results are identical, therefore they are analysed in the same section. The scenario of tests is login on the web mail with the browser in normal or private mode at the url https://login.yahoo.com for Yahoo and https://login.live.com/ for Hotmail. After that an email is composed, it is sent from the alice_prova@yahoo.it or alice_prova@hotmail.it to bob_prova@hotmail.it. Finally, logout from the web mail and the RAM dump can start. The same operation is repeated changing surfing mode (normal or private) or operating system. However in these cases, there are not differences in relation to the variables: OS, browser in private or normal mode and browser open or close during dump. The research keywords used on the dump are: *%40hotmail.it*, *hotmail.it*, *_prova*, *alice*, *bob*, *%40gmail.it*, *gmail.it*, *%40yahoo.it*.

3.3.4 Summarized of Internet Explorer tests

The table 3.1 summarizes the Internet Explorer tests on Windows XP, whereas the table 3.2 sums up the tests on Window 7.

As the tables show, there is not significant difference; however some details are evident. First of all, in the first row of both tables, it is possible to recognize a dissonance in relation to Yahoo and Hotmail. Indeed, in XP it is possible discover sender and recipient that are not feasible in 7. Looking the second row, when the browser is opened, there is only one but extremely important difference: the account's password is decrypted, as well as the chat. In the third row, the email recipient is identifiable on XP and in relation to Yahoo and Hotmail, meanwhile in the other cases it is not possible. Finally in the last row, still in Yahoo and Hotmail web site, there is a difference. This is the only case in which Windows 7 provides more information than XP. Indeed, the sender's user-name can be discovered.

3.4 Limitations and known issues

This chapter has highlighted the differences, in live digital forensics, between Windows XP and Windows 7 in a few, but extremely permeated, software. The research shows that there are no important differences between Windows XP and Windows 7 during live forensic analysis. The only one is due to the use of Facebook. Indeed using Facebook by IE in normal mode and leaving the browser opened, though logout is done, in Windows XP it is possible to find the not encrypted password, whereas in Windows 7 the password cannot be found. Probably Microsoft does not implement any function to remove evidences from the RAM, and this task could be implemented by each installed software. Certainly, this is good in relation to the investigation of police, but the private and public organizations probably

Table 3.1: *Summarized of Internet Explorer tests on Windows XP*

Type of surfing	**Dump with browser closed/ opened**	**Facebook (Chat)**	**Yahoo (Mail)**	**Hotmail (Mail)**	**Gmail (Mail)**
Normal mode	Closed	Username (sender and recipient) and chat's body	Username (sender and recipient), subject and email's body	Username (sender and recipient), subject and email's body	Username of sender, sender, recipient, subject and email's body
Normal mode	Opened	Username (sender and recipient), account's password not encrypted and chat	Username (sender and recipient), subject and email's body	Username (sender and recipient), subject and email's body	Username of sender, sender, recipient, subject and email's body
In Private Browsing	Closed	Nothing	Username (sender and recipient), Subject and email's body	Username (sender and recipient), Subject and email's body	Username of sender, sender, recipient, subject and email's body
In Private Browsing	Opened	Username (sender and recipient) and chat's body	Subject and email's body	Subject and email's body	Username of sender, sender, recipient, subject and email's body

Table 3.2: *Summarized of Internet Explorer test on Windows 7*

Type of surfing	**Dump with browser closed/ opened**	**Facebook (Chat)**	**Yahoo (Mail)**	**Hotmail (Mail)**	**Gmail (Mail)**
Normal mode	Closed	Username (sender and recipient) and chat's body	Subject and email's body	Subject and email's body	Username of sender, sender, recipient, subject and email's body
Normal mode	Opened	Username (sender and recipient) and chat's body	Username of sender, sender, recipient, subject and email's body	Username of sender, sender, recipient, subject and email's body	Username of sender, sender, recipient, subject and email's body
In Private Browsing	Closed	Nothing	Username (sender), Subject and email's body	Username (sender), Subject and email's body	Username of sender, sender, recipient, subject and email's body
In Private Browsing	Opened	Username (sender and recipient) and chat's body	Username (sender), Subject and email's body	Username (sender), Subject and email's body	Username of sender, sender, recipient, subject and email's body

would not appreciate any unauthorized access on their machines. However, the dump analyses are simplified because the content of research was known a priori. In general, the work of a computer forensics investigator can be very stressful because although different information is available, only some of them are useful for investigation. From this research, it is possible to notice that Facebook use *email=user-name&pass=password*, therefore they can be used in general as keywords, whereas *["msg":"text"* is always present for the message parts. In Skype there is always *part identity=*, *name* or *duration*, the first and the second are always followed by information about account of sender or recipient, while the third is followed by the seconds of call if the evidence is a call and not a chat. Using Google Talk *incoming* and *outcoming* mean respectively an input to the sender and a message sent by the sender.

3.5 Improvements and future works

In this work, the analysis on the two common operating systems of Microsoft, Windows XP and Windows 7, has been presented. In the future, it is scheduled to complete the analysis with Widows 8, which represents the new Microsoft operating system. This is not the only possible implementation. Indeed, forensics analysis is extremely interested in knowing dissimilarities among different browsers. Moreover, it is important to notice that smart users are more likely to prefer third party browsers (e.g. Chrome, Firefox) over IE. Browsers are among the most used software for private issues (e.g. internet banking, social networking, shared documents). From this viewpoint, the work will evolve through Windows 8 and other browsers in order to complete the scenario on Windows. Moreover, the study could be completed through the correlations with other operating systems such as Mac OS X and the most common Linux distributions (Ubuntu, Red Hat). Finally, it could be interesting to compare Mac OS X and Linux distribution, as they both are unix-like, to prove that these operating systems have the same behaviour.

Chapter 4

Conclusions

The conclusion chapter aims at providing the final considerations and recommendations coming from the research work. The final chapter is composed of five paragraphs. The first 4.1 summarizes the main concepts of the thesis in order to clarify and to hammer home the key issues that the research analyses. The second paragraph 4.2 examines the implications of the results of the research in relation to the research questions, defined in the . The third section 4.3 concerns the inferences related to theories on digital forensics applied to common application on Microsoft Windows operating system. Moreover, areas of further research in relation to the results of the thesis are suggested. The fourth 4.4 regards the concluding remarks of the research. Finally, the last paragraph 4.5 summarizes the work published.

4.1 Summary of the key concepts

The research work focuses mainly on the analysis of stand-alone systems and on how different procedures, methodologies and techniques can be applied. Indeed, although digital forensic science has been analysed only from the computer science viewpoint, it represents an extremely wide topic, dealing with various questions, such as analysis of protocol in the network, stand-alone systems, interconnected systems oriented to the research of evidence. From this conceptual point of view, digital forensic science is strongly connected with cybercrime.
Nowadays, not only has cybercrime increasingly become a significant problem for every business that need to be faced with extremely attention, but it is also a serious difficulty for governments and citizens. Moreover, cybercrime can damage both small, medium and big businesses. From the business' perspective, cybercrime entails economic problems that can assume different forms, such as industrial secrets. On the other hand, from

the governments' viewpoint, cybercrime involves social problems and internal security questions. Whereas, from the citizens' point of view, cybercrime can become whether a personal problem or an economic matter.
More in general, first of all cybercrime, interpreted and analysed as whatever security problem, could be dealt with prevention and, in this case, we talk about informatics security. Secondly, it could be faced with post-crime investigations, concerning digital forensics. The former regards the adage "prevention is better than a cure". The latter starts after the crime happened.
Despite the fact that it is not very common to have information on wars among whether governments or businesses into cyberspace, they happen frequently and they are kept secret from specific interlocutors. Indeed, compared to traditional wars, those into the cyberspace are invisible and the society has the overall impression that everything is under control and everyday life is wholly peaceful. On the other hand, the implications of a lost battle into the cyberspace could have catastrophic consequences for both government and business that lose it. For example, if Samsung came into possession of sensitive data of Apple in relation to new tablet, it would cause a serious damage to Apple.
From the viewpoint of the methodological procedure analysis, after having studied and examined in depth the subject from both computer science and legal perspectives, it has been clear that its contextualization within specific jurisdiction has not been present in the literature. As a consequence, in the chapter it is defined a new methodology, applied to the Italian jurisdiction and based on the Budapest Convention that was signed before the amendment, defined by the Law 18th March 2008, no. 48 by Italy. Indeed, all models, related to the analysis of non-volatile memory, are general and non-specific to a particular reference context. From this conceptual point of view, defining a homogeneous procedure, based on the Italian legislation, seems to be indispensable and necessary. Moreover, in order to have evidence that could be used in court to prove the crime, this evidence has to be traced in relation to a series of procedures that make the evidence unexceptionable.
On the other hand, in the second chapter 3, the operation, performed by more common software in Windows environment, is studied in order to understand how the evolution of Microsoft operating systems interacts with particularly relevant problems concerning privacy. Indeed, through the analysis of the RAM, it is possible to trace different sensitive data of the single user. However, this activity could be accomplished in relation to whether worthy reason, such as the research of evidence by the side of law, or illegal aims, such as the identity thief or the theft of other sensitive data.
In conclusion, the research is linked to the idea that nowadays it is impossible to carry on without digital forensics due to the cybercrime and the significant problems that it involves. In addition, in order to perform the

task in the better way, forensic computer scientist has to know the laws in their specific reference context. Indeed, ignoring the legal procedures and laws could entail to make all the work useless to be presented in the court.

4.2 Set of conclusions with respect to the research questions

In the introduction , different research questions are identified. This paragraph aims at analysing the implications that the results of the dissertation have for the research questions, providing a set of conclusions with respect to each of them. In particular, they are:

1. How is it possible to apply the theoretical concepts of the digital forensics processes into Italian "legislation"? Does the Italian legislation deal with this problem concerning processes and procedure that make evidence usable in the court?

2. Among more common software and operating systems, does a form of control exist to remedy for a possible forensic analysis of RAM? Is it possible to trace personal information analysing RAM concerning a computer that remains in operation?

In relation to the first research question, both thesis and the literature underline how the minimum distraction could make all works useless. Indeed,conducting a forensic analysis that goes beyond an educational lessons means to take into consideration the law that regulates that specific field of analysis. However, sometimes, the law does not keep up with new techniques or methodologies. For example, some procedures are not regulated within the system of laws. As a result, therefore some normative "holes" exist. In these cases, it is appropriate to take inspiration from the best practice, which usually defines, in an empirical way, the methodologies to follow in relation to specific situations. On the other hand, in some cases, although the procedure is regulated by a specific law, it is never analysed and focused by the scholars and researchers. These particular cases are described in the section 2, where best practices concerning forensic analysis of non-volatile memory are related to the Italian legislation. In this case, as described by the figure 2.4, the process has been divided into more phases. Some of them are preparatory to other stages; others could be conducted in parallel. Moreover, the model does not contrast the Italian law no. 48/2008 that ratifies the Budapest Convention, which was signed by Italy on 23th November 2001. Considering these two dates, it is to understand how the law is "late" in relation to significant problems, such as cybercrime that has become extremely actual in the last decade. From this perspective, the struggle against cybercrime represents one of the principal reasons that have

inspired this research. Indeed, in Italy, sometimes forensics experts present to the court evidence that, from the legal viewpoint, are not valid because they do not apply the specific reference law.
In relation to the second research question, after the application of the two most common operating systems in the Microsoft environment, the RAM has been analysed, Figure 3.1. The use of the two operating systems has been delimited to some software due to simplicity reasons. On the other hand, this software are extremely thorny due to the type of information that transmits through them. Indeed, the above-mentioned software is Skype, GTalk and Internet Explorer in relation to some websites that concern extremely sensitive data (Facebbok, Gmail, Hotmail and Yahoo). As highlighted in the paragraphs 3.4 and 3.5, the differences between these two operating systems are minimal and unimportant. However, analysing the RAM, it is important to underline the possibility to retrieve username, chat's body and, in one occasion, the not-encrypted password(3.1 row teo, colums three).

4.3 Implications for theories and further research areas

The analysis on chapter 2 and on 3 underlines different aspects with some important implications for theories related to this specific area of interest. The first chapter underlines the lack of contextualisation concerning techniques and procedures, defined as best practices, in relation to the law that should regulate them. From this conceptual perspective, it could be useful to verify if the model, define in relation to the Italian legislation, could be applied to other jurisdictions. Moreover, it could be interesting to compare one jurisdiction, whose country has ratified the Budapest Convention and another one that it does not, in terms of method applicability. In this way, it could be possible to understand if the convention defines, albeit in general, some guidelines that could entail specific laws that could be homogeneous in relation to different countries. In prospect, it is expected that the model entails only secondary and negligible changes, particularly in those countries that have ratified the Budapest Convention. Moreover, from the practical and technical viewpoint, tests need considerable time. Indeed, one of the constraints, imposed by the research has been to use only common personal computer and open source software. Therefore, ad hoc tools, which could drastically reduce times, has not been used. Indeed, among this software, there are some alpha or beta versions that can operate in parallel, taking advantages of modern CPU. However, at the moment, this software can be used only for performance tests or quality tests. In this field, there are different possibilities to further researches and theories in relation to parallel codes and algorithms. Indeed, verifying whether which algorithms or which

parts of algorithms could be paralleled is an extremely interesting and stimulating research field that the thesis could develop.

The second chapter highlights how Microsoft operating systems and single software do not deal with possible evidence that remain in the RAM after the program implementation. In relation to this specific problem, having limited tests to only two operating systems Microsoft XP and Windows 7 and to some software, the research is only in an embryonic form. Indeed, it would be necessary to test more software in order to confirm if the specific software does not deal with this question. Moreover, although Windows XP and Windows 7 operating systems are more used, they are not representative only of Microsoft products. Indeed, Microsoft has a new operating system, called Windows 8, that is rising in ranking in the use of modern personal computer Table 4.1.

Table 4.1: *Windows desktop top operating system share trend [netb]*

	Windows 7	**Windows XP**	**Windows 8**	**Windows 8.1**
Sept, 2013	46.39%	31.42%	8.02%	0.87%
Oct, 2013	46.42%	31.24%	7.53%	1.72%
Nov, 2013	46.64%	31.22%	6.66%	2.64%
Dec, 2013	47.52%	28.98%	6.89%	3.60%

Therefore, from this viewpoint, the research should be implemented in relation to other operating systems, such as whether Mac OS X or Linux. In the latter, it could be possible to study and develop a tool to implement the cleanliness of RAM in case of lack of some forms of control. Moreover, it could be possible to evaluate differences, in terms of performance, between systems that have the new service and systems without the new service.

4.4 Concluding remarks

The research work has focused on two principal topics. First of all, a methodology concerning forensic analysis of non-volatile memory in relation to the Italian legislation has been defined. Secondly, the thesis has regarded the analysis of volatile memory in relation to personal computers, identifying possible situations to advantage researchers who intend to conduct this type of analysis. The first part has underlined the importance of the ratification of Budapest Convention by the side of Italy. As a consequence, who conducts forensic analysis in relation to different sectors has to deal with the reference legislation. Indeed, in the context of computer science, experts sometimes ignore the reference normative and, in this way, they make their work useless. For this reason, a methodological procedure has been defined in relation to the analysis of non-volatile memory in order

to make evidence unexceptionable before the law. The phases are synthetically defined in the Figure 2.3, in which it is possible to identify some steps that are preparatory and others that can operate in parallel because they are completely.
The second part of the research that can be consulted in the chapter 3 shows how the detailed analysis of RAM in personal computer, which is left on, makes extremely sensitive information available. However, the analysed systems are not completely thorough due to time questions. Indeed, in order to have a complete framework, it could be necessary to have more time. On the other hand, the most used and the most pervasive systems in relation to the average user have been analysed and studied. The average user is usually a user who is exposed to specific risks. Moreover, the research work has highlighted how both Microsoft and whichever software do not apply any procedure of RAM cleaning, entailing the possibility to trace sensitive data that could be useful in relation to a specific aim.
In conclusion, the research work intends to provide a contribution to both the definition of a new procedure that can be used by forensic experts in the analysis of non-volatile memory within the Italian jurisdiction, and how operating systems maintain confidential information without worrying about consequences.

4.5 Final Remarks

We published the exposed procedure and methodology on Chapter 2 at the Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (Cybersec2013) at Kuala Lampur, Malaysia - March 4-6, 2013 [FS13b] and in an article titled "Computer Forensics between the Italian Legislation and Pragmatic Questions" published by the International Journal of Cyber-Security and Digital Forensics (IJCSDF) [FS13a]. The chapter 3 published on The Second International Conference on Informatics & Applications (ICIA2013) at Lodz, Polish - Sept. 23-25, 2013 [GS13]. Finally, during the PhD, a minor publication presented at CHITALY 2011 at Alghero, Italy - Sept. 13-16 2011 [FS11].

Bibliography

[AA11] Ankit Agarwal Megha Gupta S. G. P. D. S. G.: Systematic digital forensic investigation model. *International Journal of Computer Applications, IJCSS 5*, 4 (mar-apr 2011), 118 – 131.

[AG12] Al Gillen Randy Perry N. S.: *Mitigating Risk: Why Sticking with Windows XP Is a Bad Idea*. Tech. rep., Microsoft, 2012. [Online; accessed 01-03-2013].

[Arm12] Armstrong C.: Including stakeholder perspectives in digital forensic programs. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (Jan 2012), pp. 5414–5423.

[Bee04] Beebe N. L.: A hierarchical, objectives-based framework for the digital investigations process. In *In Digital Forensics Research Workshop (DFRWS* (2004), St. Paul: West Publishing Co, pp. 147–167.

[Ben01] Benecke M.: A brief history of forensic entomology. *Forensic Science International 120* (2001), 2–14.

[BH07] Bem D., Huebner E.: Computer forensic analysis in a virtual environment. *IJDE 6*, 2 (2007).

[BPW06] Brill A. E., Pollitt M., Whitcomb C. M.: The evolution of computer forensic best practices: An update on programs and publications. *J. Digital Forensic Practice 1*, 1 (2006), 3–11.

[Bro04] Broucek V. . T.: Computer incident investigations: e-forensic insights on evidence aquisition. In *13th Annual EICAR Conference* (2004), pp. 1–15.

[bud01] Convention on cybercrime. `http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm`, 2001. [Online; accessed 04-July-2011].

[Cal09] Caloyannides M.: Forensics is so "yesterday". *Security Privacy, IEEE 7*, 2 (2009), 18–25.

[Car05] Carrier B.: *File System Forensic Analysis.* Addison Wesley, 2005.

[Car07] Carvey H.: *Windows forensic analysis : Incident response and cybercrime investigation secrets.* Syngress Publishing, 2007.

[Car09] Carrier B.: Digital forensics works. *Security Privacy, IEEE 7*, 2 (2009), 26–29.

[Cas11] Casey E.: *Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet, 3rd Edition.* Academic Press, 2011.

[CCM*08] Case A., Cristina A., Marziale L., Richard G. G., Roussev V.: Face: Automated digital evidence discovery and correlation. *Digital Investigation 5*, 0 (2008), S65 – S75.

[CG04] Carrier B. D., Grand J.: A hardware-based memory acquisition procedure for digital investigations. *Digital Investigation 1*, 1 (2004), 50 – 60.

[CH12] Cheater K., Harley D.: *Cybercrime: Out of obscurity and into reality.* Tech. rep., 6th PwC Global Economic Crime Survey, March 2012.

[Cia04] Ciardhuain S. O.: An extended model of cybercrime investigations. *IJDE 3*, 1 (2004).

[CS04] Carrier B. D., Spafford E. H.: An event-based digital forensic investigation framework. In *In Proceedings of the 2004 Digital Forensic Research Workshop* (2004).

[DB11] Diane Bartz J. F.: U.s. shuts down massive cyber theft ring @ONLINE, Apr. 2011.

[DC10] Doug Cavit J. F. e. a.: *Microsoft Security Intelligence Report.* Tech. rep., Microsoft, 2010.

[FAS12] Flores D., Angelopoulou O., Self R.: Combining digital forensic practices and database analysis as an anti-money laundering strategy for financial institutions. In *Emerging Intelligent Data and Web Technologies (EIDWT), 2012 Third International Conference on* (Sept 2012), pp. 218–224.

[FS07] Freiling F. C., Schwittay B.: A common process model for incident response and computer forensics. In *IT-Incidents Management & IT-Forensics - IMF 2007, Conference Proceedings, September 11-13, 2007, Stuttgart, Germany* (2007), Frings S., GÃ¶bel O., GÃ¼nther D., Hase H., Nedon J., Schadt D., BrÃ¶mme A., (Eds.), vol. 114 of *LNI*, GI, pp. 19–40.

[FS11] Fenu G., Solinas F.: An augmented reality application to improve real-time communication among tourists. In *CHITALY 2011, Sept. 13-16 2011* (2011).

[FS13a] Fenu G., Solinas F.: Computer forensics between the italian legislation and pragmatic questions. *International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2*, 1 (2013), 9–24.

[FS13b] Fenu G., Solinas F.: Computer forensics investigation an approach to evidence in cyberspace. In *The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (Cybersec2013), 4-6 March 2013* (2013).

[GL07] GL G.: Forensic physical memory analysis: An overview of tools and techniques. In *TKK TI 10.5290 Seminar on Network Security* (2007), pp. 305–320.

[GS13] Gianni F., Solinas F.: Live digital forensics: Windows xp vs windows 7. In *Informatics and Applications (ICIA),2013 Second International Conference on* (Sept 2013), pp. 1–6.

[Gup13] Gupta A.: Privacy preserving efficient digital forensic investigation framework. In *Contemporary Computing (IC3), 2013 Sixth International Conference on* (Aug 2013), pp. 387–392.

[HBN09] Hay B., Bishop M., Nance K.: Live analysis: Progress and challenges. *Security Privacy, IEEE 7*, 2 (March 2009), 30–37.

[Ins12] Institute P.: *2012 Cost of Cyber Crime Study: United States.* Tech. rep., Ponemon Institute, 2012.

[JJN05] Jon J. Nordby S. H. J.: *Forensic Science An Introduction to Scientific and Investigative Techniques 2nd Edition.* CRC Press, 2005.

[JWFA06] Jr. N. L. P., Walters A., Fraser T., Arbaugh W. A.: Fatkit: A framework for the extraction and analysis of digital forensic data from volatile system memory. *Digital Investigation 3*, 4 (2006), 197 – 210.

[KC12] Kim Cheater David Harley T. G. M. C. S. I. C. J. M. S. C. M.: *Cybercrime: Out of obscurity and into reality, 6th PwC Global Economic Crime Survey.* pwc, 2012.

[KCGD06] Kent K., Chevalier S., Grance T., Dang H.: Guide to integrating forensic techniques into incident response: Recommendations of the national institute of standards and technology. National, (Ed.), National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

[KGR06] Ksander S. L., Gillam W. B., Rogers M. K.: Ultrablock forensic card reader. *J. Digital Forensic Practice 1*, 1 (2006), 69–70.

[KOE06] Kohn M., Olivier M. S., Eloff J. H. P.: Framework for a digital forensic investigation. In *Proceedings of the ISSA 2006 from Insight to Foresight Conference, 5-7 July 2006, Balalaika Hotel, Sandton, South Africa* (2006), Eloff J. H. P., Labuschagne L., Eloff M. M., Venter H. S., (Eds.), ISSA, Pretoria, South Africa, pp. 1–7.

[Les11] Lesk M.: Cybersecurity and economics. *IEEE Security & Privacy 9*, 6 (2011), 76–79.

[Man12] Manavi S.: Secure model for virtualization layer in cloud infrastructure. *International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1*, 1 (2012).

[MD09] Manes G., Downing E.: Overview of licensing and legal issues for digital forensic investigators. *Security Privacy, IEEE 7*, 2 (March 2009), 45–48.

[Mer10] Merritt M.: Cybercrime exposed. `http://www.symantec.com/content/en/us/home_homeoffice/\media/pdf/norton_cybercrime_exposed_booklet.pdf`, 2010. [Online; accessed 04-March-2013].

[M.M95] M.M.Pollitt: Computer forensics: An approach to evidence in cyberspace. In *National Information Systems Security Conference* (1995), vol. 2, pp. 487–491.

[Moo06] Moore R.: *Cybercrime: Investigating High-Technology Computer Crime.* 2006.

[MR02] M. Reith C. C. . G. G.: An examination of digital forensics models. *International Journal of Digital Evidence 1*, 3 (2002).

[N.11] N. O. F. S.: On the identification of information extracted from windows physical memory. *International Journal for Information Security Research (JJISR) 2*, 2 (March 2011), 164–168.

[neta] Desktop top operating system share trend. `http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=11&qpcustomb=0`. [Online; accessed 04-May-2013].

[netb] Desktop top operating system share trend. `http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=11&qpcustomb=0&qpsp=176&qpnp=4&qptimeframe=M`. [Online; accessed 10-Gen-2014].

[Oli09] Olivier M. S.: On metadata context in database forensics. *Digital Investigation 5*, 3 (2009), 115–123.

[OS11a] Olajide F., Savage N.: Forensic extraction of user information in continuous block of evidence. In *Information Society (i-Society), 2011 International Conference on* (June 2011), pp. 476–481.

[OS11b] Olajide F., Savage N.: On the extraction of forensically relevant information from physical memory. In *Internet Security (WorldCIS), 2011 World Congress on* (Feb 2011), pp. 248–252.

[Pal01] Palmer G.: Dtr-t001-01 technical report. a road map for digital forensic research. In *Digital Forensics Workshop, Utica, New York* (2001).

[Per09] Perumal S.: Digital forensic model based on malaysian investigation process. *International Journal of Computer Science and Network Security 9*, 8 (2009), 38–44.

[PJN10] Pilli E. S., Joshi R. C., Niyogi R.: Network forensic frameworks: Survey and research challenges. *Digit. Investig. 7*, 1-2 (Oct. 2010), 14–27.

[PL12] Pooe A., Labuschagne L.: A conceptual model for digital forensic readiness. In *Information Security for South Africa (ISSA), 2012* (Aug 2012), pp. 1–8.

[Pol07a] Pollitt M.: An ad hoc review of digital forensic models. In *SADFE* (2007), Huang M.-Y., Frincke D. A., (Eds.), IEEE Computer Society, pp. 43–54.

[Pol07b] Pollitt M. M.: An ad hoc reviwe of digital models. In *Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07), Washington, USA* (2007).

[Pol10] Pollitt M.: A history of digital forensics. In *IFIP Int. Conf. Digital Forensics* (2010), pp. 3–15.

[pro08] Codice di procedura penale. `http://www.altalex.com/?idnot=2011`, 2008. [Online; accessed 05-July-2011].

[rat08] Ratifica. `http://legxv.camera.it/parlam/leggi/080481.htm`, 2008. [Online; accessed 05-July-2011].

[RGM*06] Rogers M. K., Goldman J., Mislan R., Wedge T., Debrota S.: Computer forensics field triage process model, 2006.

[RMB11] Rhonda M. Brown J. S. D.: *Forensic Science: Advanced Investigations*. Cengage Learning, 2011.

[Rou11] Roussev V.: Building open and scalable digital forensic tools. In *Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on* (May 2011), pp. 1–6.

[San11] Sandier T.: New frontiers of terrorism research: An introduction. *Journal of Peace Research 48*, 3 (2011), 279–286.

[Sch07] Schatz B.: Bodysnatcher: Towards reliable volatile memory acquisition by software. *Digital Investigation 4* (Sept 2007), 126–134.

[SETB08] Sutherland I., Evans J., Tryfonas T., Blyth A.: Acquiring volatile operating system data tools and techniques. *SIGOPS Oper. Syst. Rev. 42*, 3 (Apr. 2008), 65–73.

[SJ12a] Sivaprasad A., Jangale S.: A complete study on tools amp; techniques for digital forensic analysis. In *Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on* (2012), pp. 881–886.

[SJ12b] Sivaprasad A., Jangale S.: A complete study on tools amp; techniques for digital forensic analysis. In *Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on* (2012), pp. 881–886.

[Soc12] Social T. O. .: *Cyber security*. Tech. rep., European Commission, 2012.

[Sof12] Software A. D. F.: Forensic toolkit®(ftk®). `http://accessdata.com/products/computer-forensics`, 2012. [Online; accessed 04-November-2012].

[SPRT13] Shrivastava A., Payal N., Rastogi A., Tiwari A.: Digital forensic investigation development model. In *Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on* (Sept 2013), pp. 532–535.

[Ste03] Stephenson P.: A comprehensive approach to digital incident investigation. *Information Security Technical Report 8*, 2 (2003), 42 – 54.

[Tak04] Takahashi I.: Legal system and computer forensics business. In *Applications and the Internet Workshops, 2004. SAINT 2004 Workshops. 2004 International Symposium on* (Jan 2004), pp. 74–77.

[Tus04] Tushabe V. B. . F.: The enhanced digital investigation process model. In *Digital Forensic Research Workshop, Baltimore, MD* (2004).

[urla] Desktop browser version market share april, 2013. `http://marketshare.hitslink.com/browser-market-share.aspx?qprid=2&qpcustomd=0`. [Online; accessed 01-May-2013].

[urlb] Desktop operating system market share april, 2013. `http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0&qpsp=171&qpnp=1&qptimeframe=M`. [Online; accessed 01-May-2013].

[urlc] Desktop operating system market share may, 2012 to june, 2012. `http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0&qpsp=160&qpnp=2&qptimeframe=M`. [Online; accessed 01-May-2013].

[Vac05] Vacca J. R.: *Computer Forensics: Computer Crime Scene Investigation*, 2 ed. 2005.

[Wea08] Waits C., et al J. A.: *Computer Forensics: Results of Live Response Inquiry vs. Memory Image Analysis.* Tech. rep., CERT, 2008.

[WJ07] Walters A., Jr N. P.: *Volatools: integrating volatile memory forensics into the digital investigation process.* Black Hat DC, 2007.

[WY05] Wang X., Yu H.: How to break md5 and other hash functions. In *In EUROCRYPT* (2005), Springer-Verlag.

[XCY11] Xu R., Chow K. P., Yang Y.: Development of domestic and international computer forensics. In *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)* (2011), Niu X., Li M., Suzuki Y., Pan J.-S., Jain L. C., (Eds.), IEEE, pp. 388–394.

[YEM*03] Yasinsac A., Erbacher R., Marks D., Pollitt M., Sommer P.: Computer forensics education. *Security Privacy, IEEE 1*, 4 (2003), 15–23.

[YYH11] Yunus Yusoff R. I., Hassan Z.: Common phase of computer forensics investigation models. *International Journal of Computer Science & Information Technology 3*, 3 (2011).

[ZMLJ11] Zainudin N., Merabti M., Llewellyn-Jones D.: Online social networks as supporting evidence: A digital forensic investigation model and its application design. In *Research and Innovation in Information Systems (ICRIIS), 2011 International Conference on* (Nov 2011), pp. 1–6.