ABSTRACT

In the recent years, analysing a computer or a digital device has become a necessity in the field of criminal investigations. However, during the forensic analysis some ordinary mistakes are often made. This paper aims at defining a new approach to the problem of evidence examination, studying the practical experience of a case study within the Italian legal system concerning techniques of forensic computer analysis based on command line. The user of this type of approaches has to guarantee efficient level of both technical skills and highly qualified and specialized legal competences in order to analyse digital systems in conformity with international best practices, and national and European regulations. Moreover, although many specific hardware and software are adopted in the forensic tests, one of the main objectives of this research has been the only use of the personal computer in order to prove the possibility to obtain the same results minimizing the costs. The case study has focused on forensic analysis of various magnetic and optical devices (mass memory), such as hard disk, pen drives, cards and CD / DVD.

KEYWORDS

Digital forensic, computer forensic model, computer forensic investigation, cyber law, digital device.

1 INTRODUCTION

Globally, businesses and governments 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 for keeping up with the risks of introducing and using new technology. Cyber activity has provided both a new type of economic crime and new vectors to facilitate existing economic crimes [1]. Today, citizens of the Information Society use a new document type that has now got the upper hand: "the digital document". The digital data (files) are the most valuable assets and the most strategic resources of every company, whether private or public. The Computer Forensics is the correct solution in order to be able to prevent data theft, industrial espionage, unauthorized access to computer systems company, damage information and to answer any potential litigation.

All over the world, developed or not, governments and businesses are increasingly being targeted by waves of attacks from criminals and country 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. The lack of an Internet-wide view within the organisation makes the problem worst.

In addition, although computer security is increasingly become 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 scenario, 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\textsuperscript{1}, juvenile pornography\textsuperscript{2}.

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

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

2 DIGITAL FORENSICS

Digital forensics or digital forensic science concerns evidences from computers that should be convincing and sufficiently reliable to stand up in court. Digital forensics 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 evidence \textsuperscript{[2]}. The digital evidence can be found in computer (hard disks or RAMs), cell phones, iPods, pen drives, digital cameras, CDs, DVDs, floppies, computer networks, the Internet etc\textsuperscript{[3]} 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 on-line share trading fraud, source code theft, on-line banking frauds, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, murder cases, organized crime, terrorist operations, defamation, pornography, extortion, smuggling and so on. As a consequence, the digital forensics focuses on finding the digital evidence after a computer security breach has occurred. It is the analysis of information that is contained and created with computer systems and computing devices, typically in the interest of figuring out what happened, when it happened, how it happened and who was 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 digital device capable of digital investigations could have three distinct roles within the computer crime.

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

Computer forensics is a process to recognize, protect, extract and archive electronic evidences that exist on the computer and on the related peripherals. Moreover, these evidences have to be sufficiently reliable and persuasive in order to be accepted by the court. Judicial forensics must be subject to the main body of the law, and must be executed in accordance with the manner required by law and procedures \textsuperscript{[4]}.

\textsuperscript{1} Pornography is the sexual act performance of prepubescent age individuals
\textsuperscript{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.
2 COMPUTER CRIME: AN OVERVIEW
Since 2009, the perception of the level of economic crime that is likely to impact organisations in the future has increased. A business only becomes aware of a fraud when it is uncovered, making it difficult for many organisations to determine their fraud risk exposure. But over time, as more businesses mature in their ability to detect fraud and as more high profile cases appear in the media, businesses will become more aware of fraud as a critical issue. Long standing fraud types such as asset misappropriation, accounting fraud and bribery and corruption remain high on the list of economic crimes.
However, new risks, such as cybercrime and sustainability fraud, are rising rapidly [1]. For instance, Bank robbers steal approximately $100 million per year in the US [5]. The estimates of losses to cybercrime vary widely. In 2010, Internet crime loss by individuals totaled $560 million. Phishing alone resulted in $120 million per quarter [6]. A single botnet ring took $100 million before the FBI managed to stop it [7].
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 asked about the various activities that they do online. The vast majority of internet users across the EU use email (85%) and most respondents say that they read news online (64%). In addition, around half of internet users say they buy goods or services (53%), use social networking sites (52%), or do online banking (48%). Around a quarter (27%) play games online, while 20% sell goods or services. From this context, it is clear as the cybercrime is relevant to modern society[8].

3 OVERVIEW OF THE ITALIAN LEGAL SYSTEM ABOUT COMPUTER FORENSICS
By its nature, the Internet can not be within a single jurisdiction, so that consequently the computer forensics is closely related with this concept. For this reason, this section aims at providing an overview of how the crimes within the computer crime are handled by the Italian legislation.
Nowadays, citizens of Information Society use a new type of document which has got the upper hand: the digital document. A great revolution started with Computers: they give the possibility of converting any kind of data, text, picture or sound into a long binary sequence. This sequence can be transferred into a several filing devices that are in constant evolution. In fact, a digital document exists regardless of the device that contains it because in the age of Homo Digitalis - at the same instant that someone keys in - it is possible to transmit amazing knowledge and information through the open-ended limits of "cyberspace". The digital document has changed and affected traditional concepts of original and copy, signing and traceability. Therefore, it represents a document that changes and becomes legally significant to companies and Public Administrations. As a consequence, the document must be properly written, it must be transmitted with security, filed and preserved with new techniques and methods in order to guarantee the digital storage durability.
Nowadays, computer document has represented the computer representation ("undersigned" or "not undersigned") of acts, facts or information that are legally relevant3. In other words, a relevant digital document/information concerns texts, pictures, data structures, designs, programs, movies that are

3 The concept of document has changed after the ratification of Budapest Convention of cybercrimes (law 18 of march 2008 no.48). As a result, the concept of digital document, expressed in the art. 491 bis penal code (a digital document is whether a data storage device that contains data/information with evidential effectiveness or a software that permits the process and the management of a digital document) has been annulled.
made up of a binary physical quantity, obtained by means of electronic processing with an acquainted source (article no.1 paragraph d) D.M.E.F\textsuperscript{4} 23th of January 2004.

From this conceptual framework, the Latin maxim "verba volant, scripta manent" has to be reinterpreted in a digital context, where every information (independently from the way in which the document it is written) can be certainly ascribable to someone. Moreover, information can be stored during the time through the use of accurate methods of computer security and of storage of the relevant information, with respect to the Italian legislation.

In relation to creation, transmission and preservation of digital documents, the aim of the current Italian regulation is to set techniques used for producing relevant digital documents that are protected and reliable. From a fiscal and civil point of view, the main laws 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\textsuperscript{5}) 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\textsuperscript{6} 11th February 2005 no. 68 (in the field of PEC\textsuperscript{7}).

Article 44 of CAD\textsuperscript{8} 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, n. 196, the technical specification in Annex B of this decree.

Nowadays, companies and public administration can "dematerialize" or, to be more precise, "digitalize" their "information of quality" (from contractual and accounting documents to sensible information, such as internet log-files, video surveillance system data, privacy documents, e-mail and so on). For this purpose, it is indispensable to act as by law enacted, according to proper methods and tools for the creation, stabilization and the preservation of important data.

Moreover, a proper management of information is important not only in terms of economic and

\begin{itemize}
  \item Finance Minister Decree
  \item Corresponding to statutory instrument.
\end{itemize}

\textsuperscript{6} Decree by President of Italian Republic.

\textsuperscript{7} Certified web mail.

\textsuperscript{8} Italian code for digital administration.
security advantage but also because in the lawsuit, the digital document could be considered invalid and irrelevant if it is not created and preserved properly. Nowadays, any company or any local authority cannot lose relevant information that could be used in a lawsuit.

These assumptions have been strengthened by the Italian ratification of Budapest Convention\(^9\). This ratification entails that computer crimes are a liability of local authorities and companies. As a consequence, any corporate body has to manage and organise properly the relevant information within a well-established framework of roles and responsibilities in relation to their structure and with respect to external relations. In addition, methods and procedures could be indispensable in order to avoid the loss, the modification and the corruption of important data and information. Moreover, it is necessary that the local authorities and the companies arrange a system of rules that permits to keep the integrity of a document and to determine easily the link between body corporate and relevant information. These procedures have to set within the Italian regulation with respect to the use of personal data and to the creation and the preservation of digital documents. It is not easy to implement these procedures especially when the clarification of some ambiguities and the definition of rules are inconvenient for a company. Therefore, a strategic solution is to delegate the security and the management of digital archive to another company (outsourcing). For these reasons, in the Digital Society foreseeable future, it is necessary to have a third party that assures:

- the authorship and immutability of relevant information (account and fiscal data, log files generated by electronic communications, electronic transaction, etc.);
- their proper transmission;
- their preservation in the course of time in relation to procedures that are assured and certificated by the current regulations.

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

4 THE PROPOSED MODEL

In computer forensics, one of the first methodological approaches was composed of three base components. This method was developed by Kruse and Heise[9] in 2001. The components were:

![Fig. 1 Kruse & Heiser Model](image)

- Acquiring data. While the data are collecting, their integrity should be preserved.

---

\(^9\) Italy ratified the agreement of the European council on the cybercrime, which was established at Budapest the 23th November 2001 by means of the law 18th of March 2008, no. 48.
- Authenticating the validity of the extracted data. This phase involves making sure that it is as valid as the original.
- Analysing the data, keeping its integrity.

Table 1 shows a complete list of digital forensic investigation model based on chronological order.

<table>
<thead>
<tr>
<th>Model Name</th>
<th>Inventers</th>
<th>Years</th>
<th>Number of phases</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFRWS Investigative Model (Generic Investigation Process)[12]</td>
<td>Palmer</td>
<td>2001</td>
<td>6 Phases</td>
</tr>
<tr>
<td>End To End Digital Investigation[16]</td>
<td>Stephenson</td>
<td>2003</td>
<td>6 Phases</td>
</tr>
<tr>
<td>Enhance Integrated Digital Investigation Process (EDIP)[17]</td>
<td>Baryamur eeba and Tushabe</td>
<td>2004</td>
<td>5 Phases</td>
</tr>
<tr>
<td>Event Based Digital Forensic Investigation</td>
<td>Carrier and Spafford</td>
<td>2004</td>
<td>16 Phases</td>
</tr>
<tr>
<td>Computer Forensic Field Triage Process Model (CFFTPM)[22]</td>
<td>Freiling and Schwittay</td>
<td>2007</td>
<td>4 Phases</td>
</tr>
<tr>
<td>Investigation Process model[23]</td>
<td>Bem and Huebner</td>
<td>2007</td>
<td>4 Phases</td>
</tr>
<tr>
<td>Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)[9]</td>
<td>Perumal S.</td>
<td>2009</td>
<td>7 Phases</td>
</tr>
</tbody>
</table>

The last model on Table 1 "Systematic Digital Forensic Investigation Model" is showed on Fig. 2 and it consists of eleven steps [26].
With respect to model in Fig. 2, the paper analyses in detail only the eighth phase called "Examination". This step concerns the examination, as the name suggests, of devices that have been divided in the sixth phase, named "Evidence collection". This paper aims at developing a new approach for the examination of Non-Volatile evidence collection. First of all, Non-Volatile evidence collection are for instance hard disk and external storage in general, such as compact flash (CF) cards, memory stick, secure digital (SD) cards, MMC cards, USB memory sticks. The choice of the model SRDFIM 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, it is rightly explained for the phases 4, 5, 6, 7, 8 the concept "Capturing the timeline according to the country Digital Forensic Law". The last concept is extremely important with respect to the different legislations where this model is applicable.

The development of the "Examination" phase is led to create a list of steps that are summarized in Fig. 3.

In relation to the chart, it is evident as the first phase is preparatory to the second step. After the second phase, the process is divided into two ramifications that can be executed parallel. The first, on the left, is composed of only one step "data recovery/data carving". Meanwhile, the second, on the right, is characterized by two phases: disk analysis and mount partition. Lastly there is "files data analysis". During the Examination of Non-Volatile evidence is extremely important to disable the auto mount on the system. Moreover, the operative system usually enables this feature. As a consequence, various Linux distribution, which are expressly developed in support of computer forensics analysis, exist in order to disable the auto mount and to include all the necessary software/tools to the analysis/investigation, such as DEFT, CAINE or Helix Linux distribution. In addition, these Linux distributions, or other typical for computer forensics analysis, implement other important peculiarities as following:

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

Finally, in this paper there are references to Sleuth Kit toolkit\textsuperscript{10} while Autopsy\textsuperscript{11}, which is a graphical interface to the digital investigation tools in the Sleuth Kit, does not have any reference within this paper. Moreover, for each phase it is specified only a list of the possible tools and not a detailed description of how to use them. Indeed, reading manual is the best solution to improve knowledge with respect to a specific tool.

4.1 Creating hash code phase

The first step is "creating hash code". This phase concerns the creation of hash\textsuperscript{12} code, usually MD5 or SHA, of drive. 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.

4.2 Image copy phase

The second step "image copy" crates a copy of the device (bit stream image). On the other hand, these images must be actual bit-by-bit or "mirror" images of the originals. 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. However, it is important to not stress the device. Indeed, using the drive whenever increases the probabilities to break accidentally the evidence.

After the copy is made, it is possible to calculate the hash code of the image file. As a result, it is necessary to check if this hash is 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.

One of the possible tools to create bit stream image is Standard Linux dd command. 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, enhancing it for forensic use.
- dcfldd, fork of dd code, enhancing it for forensic use.
- ddrescue, that enhances dd program. It allows mass memory acquisition that has reading errors. As a result, there are damaged disk sectors.
- aimage, this tool is used to acquire Advanced Forensic Format (AFF) images.
- ewfacquire, this tool is used to acquire Expert Witness Format (EWF) images.

4.3 Data recovery/data carving phase

The "data recovery/data carving" step aims at recovering the removed data (files). The carving activity consists in recovering files through the files header and footer\textsuperscript{13} identification. Foremost it is probably the best recovery tools on Linux.

---

\textsuperscript{10} 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.

\textsuperscript{11} http://www.sleuthkit.org/autopsy/index.php.

\textsuperscript{12} Hash codes are large numbers, specific to each file and each drive that are mathematically computed. If a file or drive is changed, even in the smallest way, the hash code will also change. These hash codes are re-computed on the original and on its images at various points during the investigation in order to ensure that the examination process does not modify the examined image\textsuperscript{27}.

\textsuperscript{13} 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.
distribution. However, there are also photorec, scalpel and magicrescue. All these tools are valid and the choice depends on own requirement. Moreover, the mount of partition is not necessary, in order to use the above list. In addition, these tools use the file image as an input.

4.4 Disk analysis phase

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. The "Disk analysis" step has the goal to analyse the mass memory and verify the disk partitioning. It is composed of two phases: the partition recognition and the file system identification. In relation to the first, 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. As a result of these two phases, all the necessary information is obtained in order to understand which type of analysis should be conducted. For example, if there is a primary partition with file system ntfs, certainly there is a Microsoft Windows (2000, xp, vista, seven, eight) installed system. As a consequence, the analysis also concerns the system register, the internet chronology and so on. On the other hand, if there is a logical partition, the type of analysis regards exclusively present, hidden or deleted files. Moreover, it is often necessary to rebuild the disk table because the disk has been formatted. In this case, testdisk tool is perfect. Fdisk, mmls, hgparm, disk_stat and HDSentinel represent tools to analyse the disk with respect to these two phases. After that the image file is created and the partition information is obtained, it is possible to develop the first list about all existing files on the mass memory in order to create a time line. The time line is usually created through the tool mac-time. Mac-time takes as input a list, which is created by fls tool and it is completed of data that are contained into the analysed file system. On the other hand, fls takes as input a raw file that derives from the previous memory mass acquisition or directly on the device, and fls returns the list of all files, allocated and not, to be used afterwards as input in mac-time.

4.5 Mount partition phase

After the disk analysis, there is a tricky step. This is very important to avoid that files or everything into the partition could be distorted. The mount command allows connecting a file system to a system folder. In relation to the steps in Fig. 3, the mount is not directly on the device, but it is on the bit stream image. This approach obeys the best practice on computer forensics. The best practice strongly recommends not to work on the original mass memory but always on its copy. The bit stream image can have various format and the more common are:

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

In addition the mount command must ensure:

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

4.6 Files system analysis

Finally, there is the core of the analysis that needs more time with respect to the other phases. After recovering data or entering into the file system in safe way, as describe previously, the phase of finding the evidence starts. This step could have two sub steps. The first, called system operation analysis, is conducted only if the analysis regards a primary partition.
this case, as a result, a systems operation, such as Microsoft Windows, IOS, Linux and so on, is always installed. On the other hand, the second phase, called files data analysis, is always developed. Indeed, there are almost always some personal files into a partition or unallocated space. Useful command line tools are find, locate, grep and its different version like egrep, fgrep or rgrep. All of them are useful for both sub phases and probably without them it is impossible to proceed the analysis. For example, find e locate are dedicated to search activity.

4.6.1 System operation analysis

This phase concerns a wide argument. Indeed, first of all, there are different types of operation system. 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 operation and the most useful tools on Linux distribution to resolve the problems. Moreover, the first thing to do is to analyse the 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: IE Cache View, IE Cookie View, IE History view and IE PassView. Important programs, such as Messenger, Skype and email management, are installed within the S.O. As a consequence, all the personal information in relation to these programs is obviously stored within the system. Therefore, programs to find account info (user and password), such asMail PassView, Live Contacts View, PSTPassword, MessenPass, and Protected Pass View, exist. All these information are relevant in a crime investigation, and they can be got only analysing the S.O.

4.6.2 Files data analysis

This phase can take really long time, it is extremely ticklish because it can waste time to analyse and view useless file for own crime investigation. Thus, it is very important to have some key words to search only files that should be relevant to own aim. 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. In this phase, the computer forensic expert is usually not alone, but he needs the help of who knows if the files are relevant with respect to the investigation.

5 CONCLUSIONS AND FUTURE WORK

In this paper, a novel model is analysed in order to examine the mass memory. Moreover, for each phase there are specific references to Linux tools. In addition, the model satisfies the Italian legislation and probably could be used also in other countries. This argue is a probably suggestions for future work. Indeed, the team is interested to match the same model for two or more legislations. Unfortunately the Italian legislation, as the world's legislation, is in continuous evolution to better contrast the crime. However, the presented model should be unchanged in relation to normal improvements
that could be made to the Italian legal system in the field of cybercrime and computer forensics due to its flexible nature. In addition, the Linux tools with respect to each phase are limited to a brief description or mention only because their complex nature, characterized by various options, is well explained by many guides or manuals. Nevertheless, the paper provides a complete list of them and hence the way to do the analysis at low cost. The cybercrime, as explained in the previous paragraphs, is constantly expanded due to a wide range of applications. In this paper the forensic analysis focuses on non volatile memory. The future work concerns the normalization of the model to the other legislations, defining e new model in relation to different types of media such as mobile phone, tablet and volatile memory and into a cloud computing. The last aspect could be the new challenge of the computer forensics. Finally, the future works could also contribute to the Sleuth Kit Hadoop, which incorporates the Sleuth Kit into a Hadoop cluster, so the analysis could be faster.

6 REFERENCES


cybersecurity-coreflood-idUSTRE73C7NQ20110413 [Accessed: 13 October 2012].