A Comparison Approach of Digital Forensics Tools

Enrique A. Torres Andino
Master of Engineering in Computer Engineering
Dr. Alfredo Cruz Triana
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— Digital forensics is an important branch in the forensics and computer science. This branch encompasses the recovery and the investigation found on digital devices, such as computers and cellphones, which typically is related to a crime. Due to the outstanding increase in technology that we are experiencing, a lot of innovative technology has been developing which are used for effective and beneficial aspects but also for malicious activities. This and the necessity to solve crimes related with computer technology has made the window to create and develop digital forensics tools that can be very helpful in a crime investigation that involves any computer technology. The proposed project is to compare a little group of forensics tools based on what they do, the basis of the Digital Forensic Investigation Process that they fulfill, and the basis of the Integrated Digital Forensics Process Model Framework that they are able to cover.*

Key Terms *— Digital Forensics Branches, Digital Forensics Investigation Process, Digital Forensics Tools, Integrated Digital Forensics Process Model.*

INTRODUCTION

Digital Forensics is a branch of the forensics discipline that cover every crime that is related or involved computer technology. When we talk about computer technology, we talked about everything that can be programmed to carry out a set of arithmetic or logical operations automatically, which lead us to desktop computers, laptops, smartphones, tables, and technology like that [1]. Digital crimes or crimes that involve computer technology begins on late 1970s and thru the pass of the years, it has been increasing exponentially [2]. The necessity to develop digital forensics tools, that analyses computer technology in order to gather data as evidence to support or refuse a hypothesis before criminal or civil courts, increase and right now there are laws and policies that guide and support digital forensics investigations. These tools are used to gather, store, analyze, examine, and report any data useful for an investigation.

The digital forensics tools are divided in several sub-branches, which are:

- Computer forensics
- Network forensics
- Mobile device forensics
- Database forensics

The computer forensics is the branch in digital forensics that covers the evidence found on computers and digital storage media and the main objectives is to identify, preserve, recover, analyze, and present the evidence gathered in the investigation [3]. The network forensics is the branch in digital forensics that is related to monitoring, gather information, and analyze computer network for the conceive purpose of gather information, legal evidence, or for intrusion detection. Mobile device forensics is the branch in digital forensics that is related to recover and gather data or evidence from a mobile device including smartphones and tablets. The database forensics is the branch in digital forensics that is related to gather information from databases and their metadata.

The fundamentals of digital forensics are to use scientifically and proven methods to preserve, validate, identify, analyze, interpret, document, and present digital evidence that are gathered from computer technology [2] [4]. During the pass of time, and the necessity to have a structure that govern the digital forensics discipline, an investigation process has been developed. Sometimes the information that a computer has is key to identify a suspect and also has hard evidence for a case, and for those reason the investigation

process is used. The digital forensics investigation process consists mainly of five steps, which are:

- Preservation
- Collection
- Examination
- Analysis
- Reporting

Figure 1, below, represent graphically what the Digital Forensics Investigation Process consists.

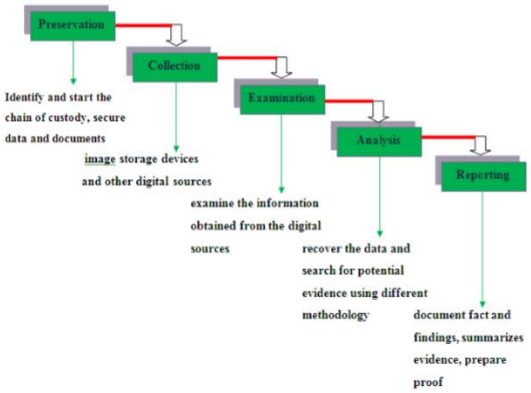

Figure 1
Digital Forensics Investigation Process [2]

Preservation is the first step in the investigation process that preserve digital evidence in order to avoid alteration or damage in the evidence and to increase the chances of having a successful investigation, litigation, or incident response. Collection is the second step in the investigation process that is related to collect all the digital information means, the equipment that contains the information, or record the information on a medium that can be used in the investigation. Examination is the third step in the investigation process that is related to examine the evidence gathered from the computer technology collected. The examination step is performed on a copy of the gathered information in order to preserve the integrity of the original evidence. Analysis is the fourth step in the digital forensics investigation process that is related to analyze the evidence gathered using a significant number of methodologies and tools, that will help with the analysis of the evidence and in addition, deleted data can be recovered [5][6]. Reporting is the final step of the investigation process that is related to report al the finding obtained from the analysis of the evidence in a way that a non-technical person can understand easily.

In digital forensics, there is a model that provides a logic sequence that can be followed and will guide us in a digital forensic investigation. This model name is Integrated Digital Forensics Process Model [2] [4]. This model consists on the following processes:

- Preparation – in this process a policy or procedure about how to perform a digital forensic investigation is defined and developed in order to begin working with the infrastructure and operational readiness to have all the tools needed to perform a successful investigation [4].
- Incident – this is the process in where an incident is detected, following by the assessment of an investigator in order to let know the course of the investigation based on the incident detected. In addition, the incident is confirmed by a second source before any action is taken. Following that an authorization to begin the investigation must be given, and when received the investigation is deployed [4].
- Incident response – in this process the approach strategy of the investigation is determined by the type of investigation with a very clear objective of initialize a chain of custody and a chain of evidence avoiding to damage the potential digital evidence. After the approach strategy is determined, then the search, seize, recover, preservation, transportation, and storage of evidence begins until it's gathered every piece of information [4].
- Digital forensic investigation – this is the process in where the evidence of a case in process or investigation can be collected, authenticated, examined and harvested, reduced, identified, classified, organized, compared, hypothesis, analyzed, attributed, evaluated, interpreted and reconstructed, communicated and reviewed [4].
- Presentation – this is the final process of the model in which all the finding gathered of the evidence is presented in a report and with this

report, a decision is made on the suspect to whom the incident can be attributed. Finally, the outcome of the investigation is disseminated to review the existing policies and procedures of the organization [4].

Figure 2, below, represent graphically what the Integrated Digital Forensics Process Model consists.

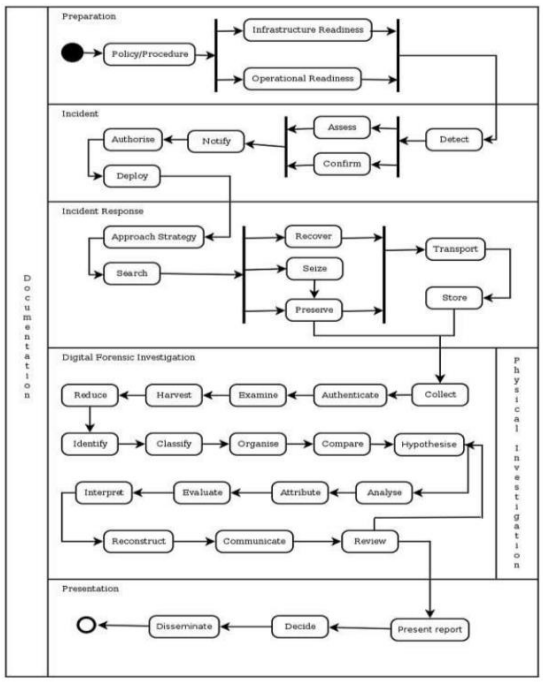

Figure 2
Integrated Digital Forensics Process Model Framework [4]

PROBLEM STATEMENT

The digital forensics tools are an essential part on the digital forensics investigation because it can help to gather hard evidence of a case that can incriminates a person of doing a crime. By this, is important to know what some digital forensics tools are capable to do based on the digital forensics investigation process and the integrated digital forensics model framework. Sometimes, the forensic investigators do not have the expertise or the knowledge about what are the capabilities of the digital forensics tools, making the gather of evidence a loss of time. The main objective of this project is to compare some of the digital forensics tools on the investigation process and in the model framework in order to know what exactly cover the compared tools. This can be helpful at the time to perform a digital forensics investigation, because it will let you know what is capable to do each of the compared tools.

METHODOLOGY

The methodology to be used in this project is simple, and will be generally the same, with the slight difference of the environment in were each forensic tool is working on. There are several steps in the methodology used for this project. One step in the methodology is to select the tools to be considered in this project for comparison. The tools selected are:

- MOBILedit! Forensics
- Forensic Toolkit (FTK) Imager
- Digital Forensics Framework (DFF)
- Autopsy
- WinHex

Once these tools are selected, then it was started with the environment preparation for them. The tool selected to be considered work in two different operating systems (OS) which are:

- Windows
- Linux

It was prepared two computers with the operating systems needed to run the tools selected. The computer that have the Windows operating system have the following specifications:

- Processor: AMD FX-8350 Eight-Core Processor 4.00 GHz
- RAM: 32.0 GB
- OS: Windows 10 Pro 64-bit

The computer that is prepared with the Linux operating system have the following specifications:

- Processor: AMD Athlon Quad-Core Processor 1.4 GHz
- RAM: 8.0 GB
- OS: Kali Linux 2016.1 64-bit

The next step is to have the necessary components to test the tools. Is important to remark that only will be tested what these tools do and nothing else, making clear that is not tested the

performance of the tools. For each tool a test case of functionality will be done, in order to show what the tools can do. Saying this, we will see 5 test cases. For each of the test cases we will need different materials. In Table 1, is detailed the materials that we need for the test cases.

Table 1
Materials Used on Test Cases

Test Cases	**Materials Used**
Test Case 1: MOBILedit! Forensics	• Cell Phone • Cable to connect cell phone with computer • Computer with Windows OS • Forensic Tool: MOBILedit! Forensics
Test Case 2: Forensic Toolkit (FTK) Imager	• Computer with Windows OS • Storage Medium (HDD, USB Drive, etc.) • Forensic Tool: Forensic Toolkit (FTK) Imager
Test Case 3: Digital Forensics Framework (DFF)	• Computer with Linux OS • Storage Medium (HDD, USB Drive, etc.) • Forensic Tool: DFF
Test Case 4: Autopsy	• Computer with Linux OS • Storage Medium Image (HDD, USB Drive, etc.) • Forensic Tool: Autopsy
Test Case 5: WinHex	• Computer with Windows OS • Storage Medium (HDD, USB Drive, etc.) • Forensic Tool: WinHex

Test Case 1: MOBILedit! Forensics

In this test case, the functionality of the tool MOBILedit! Forensics is tested, in order to see what this tool can do. This tool is focused on mobile device forensics and is capable of gather information of smartphones, including Android, Windows phone, and IOS phones. This tool runs in a Windows OS environment only. The tool is capable to collect the information of the phone and preserve it in order to analyze it for the case investigation. Also the same tool is able to segregate the information into different popular segments that will be useful in an investigation. The popular segments in were the tool segregate the information are phonebook, call logs, messages, applications, application data, files, media, user files, and calendar. In addition, the tool is capable of analyzing data in its logical and physical form and important information can be gathered, see Figure 3, and dumped in a file as evidence.

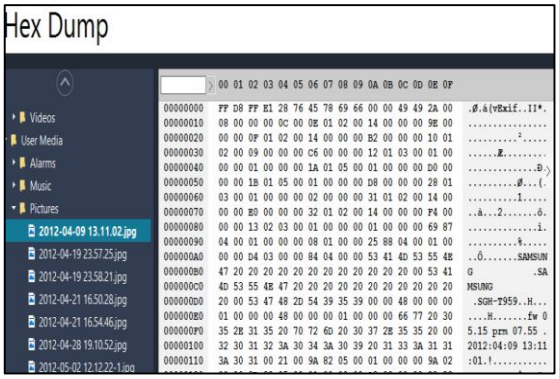

Figure 3
Logical and Physical Analysis of a Picture in the Phone

In Figure 3, a picture gathered from the phone used on the test case is being analyzed. As shown, the physical data of the picture is in the hexadecimal, and at the right side, it interpretation is presented. In here we can see metadata of the picture such as the device model and manufacturer and the date in where the picture was taken. The tool also is capable of generate different formats of reports, such as Excel, HTML, and RTF. The report can be generated as full report, or just a specific part of the information gathered. This tool is also capable of analyze the data gathered from the phone. In addition is capable of make a copy of the SIM card that have the cell phone in order to gather other information, such as contacts and text messages [7]. In general, this tool is very useful, complete, and independent at the moment to make a forensic investigation.

Test Case 2: Forensics Toolkit (FTK) Imager

In this test case, the functionality of the tool Forensics Toolkit (FTK) Imager is tested, in order to see what this tool can do. This forensics tool is the free version of the popular Forensic Toolkit or FTK, and it does almost everything that the commercial

version does. Forensics Toolkit Imager runs in a Windows OS environment and is more focused on computer forensics. Forensic Toolkit Imager is capable of collect the data of a storage medium by the method of creating an image of it. This image is preserved intact and can be used for further analysis. This tool is also capable of analyze the image in the physical and logical spectrum, making it a useful tool at the moment to examine evidence. In Figure 4, is shown the capability of analysis that FTK Imager has.

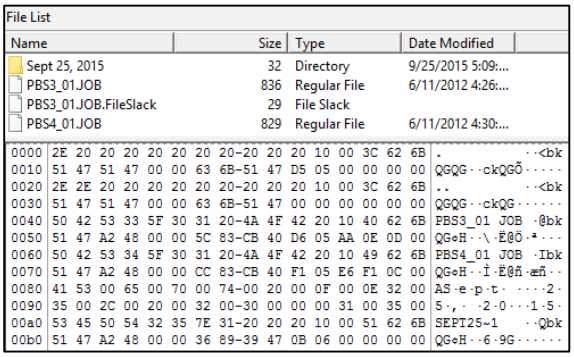

Figure 4
Logical and Physical Analysis of a File in FTK Imager

In Figure 4, at the top, can be seen the logical structure of a file in the image created for this test case, which contain two regular files and a directory. Below of the logical structure, the physical structure of the file can be analyzed on hexadecimal form, and in addition a human readable translation of every hexadecimal line can be found on the left side of the physical structure. As can be notice, this human readable translation has the names of the two regular files and the directory. The tool can mount the image in the computer, and this is needed for an easy analysis and investigation. The tool is capable of generate a report of the image investigated in order to be used in a case. Also it has the ability of organize the evidence in a case file for investigation purposes [8]. In general, Forensics Toolkit Imager can be considered a complete tool that can be used in when a digital forensics investigation comes, and the best part of it is that is free.

Test Case 3: Digital Forensics Framework (DFF)

In this test case, the functionality of the tool Digital Forensics Framework (DFF) is tested, in order to see what this tool can do. This tool is focused on computer forensics. Digital Forensics Framework (DFF) is a commercial license software that runs on Linux OS environment, but also can run on Windows OS. This forensics tool is based on a command lines, so it runs on a terminal, but in addition it has a graphical user interface which permits a better interaction with it. This software is capable of preserve the data of a storage medium image. This tool can calculate the cryptographic hash number of the image created in order to corroborate the integrity of the files, which is of sum importance in the digital forensics environment and ensure the preservation of the evidence. In addition, this tool is compatible with the Raw, EWF, and AFF image format able it to be used with various forensics tools in conjunction. Also, this tool is able to reconstruct volumes and file systems in order to analyze it, in order to perform several analyses. In the analysis, metadata can be extracted, and other information such as the registry information and memory analysis. This tool permits the investigator to perform logical and physical analysis of the files in an image. Below, in Figure 5, is an example of a physical and logical examination of an image used for this test case.

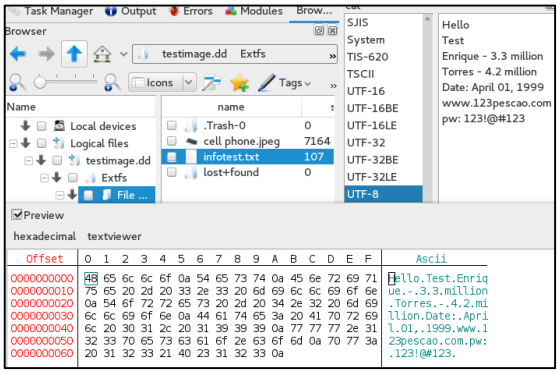

Figure 5
Physical and Logical Analysis of a File in a Storage Image

In Figure 5, can be seen that a text file is examined in its physical and logical form. As seen, the logical form of the analysis shown were the file

is located and its size. The physical form shown its hexadecimal representation, making the way to analyze the file bit by bit, and at the right side of the hexadecimal representation in the DFF tool, an ASCII representation can be observed, translating what each hexadecimal bit said in a human readable form. This tool can also analyze documents, and inclusive can retrieve or recover deleted files in order to be analyzed. In addition, this tool is capable of analyze user activities using event logs in collected in the image. Also this tool is capable of automation make it able to gather information in an automatic form and also make report of the data collected in order to be used as part of the investigation [9]. This tool is very useful at the moment to preserve and analyze data, but unfortunately it doesn't collect the data, making it dependable of other forensics tools to start the forensic investigation process.

Test Case 4: Autopsy

In this test case, the functionality of the tool Autopsy is tested, in order to see what this tool can do. Autopsy is a forensics tool that run in Linux OS, Windows OS, and is web-based. This tool is more focused on computer forensics. This tool is unable to collect data of the storage medium and convert it into an image. It needs an image in order to start to work. It web-based environment make it very useful and understandable for a forensics investigator. The user can create a case and add all the images or piece of evidence regarding the case in investigation. This tool is capable of calculate the hash numbers to verify the integrity of the image added with the original source. After adding the image to the case, Autopsy can analyze the file in the logical and physical form. It provides a user interface that can provides you the options of analyze the whole image or to analyze a file of the image. In addition, Autopsy delivers the option of adding notes to the files analyzing which can be later posted on the report of the case. In Figure 6 and 7, is shown some of the analysis that can be done in Autopsy.

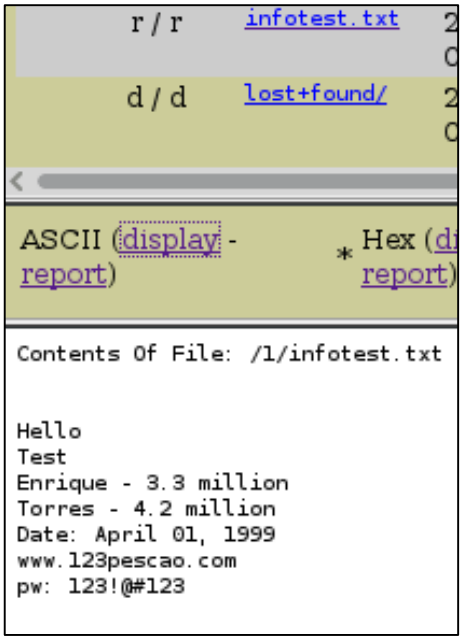

Figure 6
File ASCII Analysis

In Figure 6, the ASCII interpretation of the file infotest.txt is shown. This interpretation shows the text content that the file has, in order to clearly read what the file in analysis said.

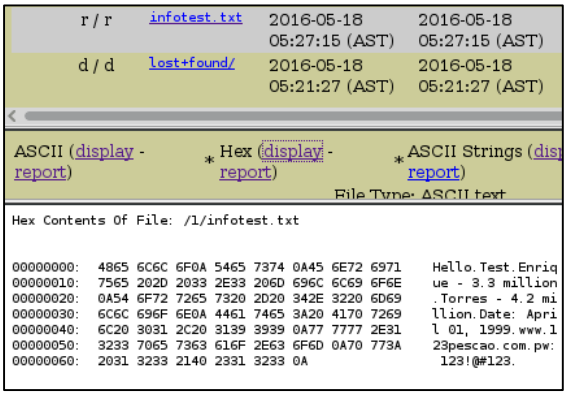

Figure 7
File Hex Analysis

In Figure 7, is shown the ability that Autopsy has to analyze the file in the raw format, which is hexadecimal. In addition, it can be noticed that at the right side of the hexadecimal interpretation can be found human readable text which translate what the files said in hexadecimal. Also, this tool is capable to provide the option of search a specific keyword in the files of the images in order to find evidence faster and more efficiently. It also provides the option to

generate a report of the image investigated with all the notes taken when analyzing [10]. In general, is a good forensic tool but is dependent of a tool that can collect the data into an image.

Test Case 5: WinHex

In this test case, the functionality of the tool WinHex is tested, in order to see what this tool can do. This tool runs on a Windows OS environment and is focused on computer forensics. WinHex is a digital forensic tool that is capable of collect and preserve data from a storage medium and create an image from it. It creates the image from the original source, and calculate the hash number in order to be able to corroborate the integrity of the image created. Also, the forensic tool is capable of analyze the physical and logical part of the image making it useful for analyze and examine a piece of evidence of a case, which is shown on Figure 8. This tool is able to recover deleted data, and also can organize all the evidence in a case infrastructure in order to be easy to read for an investigator.

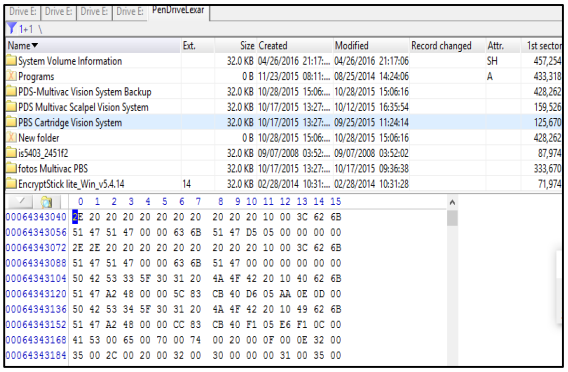

Figure 8
Logical and Physical Analysis in WinHex

In Figure 8, is shown a file selected in the logical form and below can be seen it physical interpretation of the file selected. If another file is selected, the physical interpretation will be shown. It is able to generate a report of the image analyzed with all the observations made in the analyzing process [11]. WinHex is an excellent digital forensics tool, complete, and independent in the moment to make a forensic investigation with it.

RESULTS

The five digital forensics tools selected to be considered was tested in a functionality point of view. With this tests we can gather information and results that will answer the questions made to perform this project. First let's summarize in what branch of the digital forensics environment the tools selected work. See Table 2 below.

Table 2
Branches Where Forensics Tools Considered are Focused

Forensics Tool	Dedicated Branch in Digital Forensics
MOBILedit! Forensics	Mobile Device Forensics
Forensics Toolkit (FTK) Imager	Computer Forensics
Digital Forensics Framework (DFF)	Computer Forensics
Autopsy	Computer Forensics
WinHex	Computer Forensics

In each test cases were looked for the capabilities of each tool selected in order to see what steps, in the digital forensics investigation process, they are capable to cover and also what process of the Integrated Digital Forensics Process Model framework (IDFPM) they are capable to do. Below are two tables that summarize the results for this questions. See Table 3 and 4 below.

Table 3
Comparison of the Selected Tool on the Basis of Digital Forensics Investigation Process

	Preser-vation	Collec-tion	Exami-nation	Ana-lysis	Repor-ting
MOBILedit! Forensic	YES	YES	YES	YES	YES
Forensic Toolkit (FTK) Image	YES	YES	YES	YES	YES
Digital Forensics Framework (DFF)	YES	NO	YES	YES	YES
Autopsy	NO	NO	YES	YES	YES
WinHex	YES	YES	YES	YES	YES

Table 4
Comparison of the Selected Tools on the Basis of IDFPM Framework

	Prepa-ration	Inci-dent	Inci-dent Res-ponse	Digital Forensic Investi-gation	Pre-senta-tion
MOBILedit! Forensic	YES	YES	YES	YES	YES
Forensic Toolkit (FTK) Image	YES	YES	YES	YES	YES
DFF	YES	NO	YES	YES	YES
Autopsy	YES	NO	YES	YES	YES
WinHex	YES	YES	YES	YES	YES

To analyze the results obtained in the test cases, and summarized in the tables above, three of the five digital forensics tools are capable of perform all the tasks and procedure needed to conduct a digital forensics investigation, the other two digital forensics tools can perform part of the digital forensics investigation but will need or are dependent of other tools to complete the whole process. In general, all the tools can perform the work for what they are designed without any problem, but they need to be worked in order to know what they are capable to do.

CONCLUSION

Digital forensics tools are useful tools to investigate and solve computer or cyber-crimes. Most of the tools considered in this project can collect, preserve, examine, analyze, and report; in other words, they perform the complete digital forensics investigation process, making them independent of other forensics tools. The others only perform a partial part of the forensics investigation making them dependable of other tools to complete the investigation process. To know what these tools are capable to do, the investigator must work with them to know them because they are not user-friendly at all and the person must know what they are doing to avoid errors in the investigation. To conclude, there is a lot of digital forensics tools in that are powerful and useful to perform a digital forensics investigation, but they need to be tested by investigators in order to know what they are capable to do, to be more efficient at the moment of an investigation.

ACKNOWLEDGEMENT

First of all, thanks to my God for given me the strength and the wisdom to make this possible. An acknowledgement to my advisor Dr. Alfredo Cruz Triana. Thanks for putting your confidence on me. Thanks to my wife and my daughters for all the support given to me in this and in every moment. Thanks to my family for the support.

REFERENCES

[1] G. Palmer, “A Road Map for Digital Forensic Research,” in First Digital Forensic Research Workshop, N.Y., 2001, pp. 27–30.

[2] D. Ramesh & N. Jain, “Digital Forensics Tools: A Comparative Approach,” Int. J. of Adv. Research in Sci. and Eng., vol. 4, no. 2, pp. 157-168, Feb. 2015.

[3] A. Yasinsac, R. F. Erbacher, D. G. Marks, M. M. Pollitt, "Computer forensics education," IEEE Security & Privacy, vol. 1, no. 4, pp. 15-23, Aug. 2003.

[4] M. D. Kohn, “Integrated Digital Forensics Process Model,” Ph. D. dissertation, Dept. Comp. Sci., Univ. of Pretoria, Pretoria, South Africa, 2012.

[5] M. S. Olivier, "On metadata context in Database Forensics," Digital Investigation Science Direct, vol. 5, no. 3, pp. 115-123, Mar. 2009.

[6] S. L. Garfinkel, “Digital forensics research: The next 10 years,” Digital Investigation Science Direct, vol. 7, pp. 64-73, Aug. 2010.

[7] Compelson Labs. (2015). *MOBILedit Forensic User Guide* [Online]. Available: http://www.mobiledit .com /forensic-guide.

[8] AccessData Corp. (2007). *Forensic Toolkit User Guide* [Online]. Available: http://myweb.cwpost.liu .edu/cmalinow/ftk/ftkusersguide.pdf.

[9] Digital Forensics Framework. (2016). User *Guide* [Online]. Available: http://www.arxsys.fr.

[10] Basis Technology. (2015). *Autopsy User Documentation* [Online]. Available: http://sleuthkit. org/autopsy/docs/user-docs/3.1/.

[11] X-Ways Software Technology AG. (2016). *X-Ways Forensics/WinHex Manual* [Online]. Available: http://www.x-ways.net/winhex/manual.pdf.