Digital Forensics: Development of a Forensics Appliance–Analysis and Recommendations

Yassine El Bahlouli, Nabil Hmina

Abstract: ***In the context of IT development, and with the growth of cyber crime, the IT experts still looking to improve techniques and investigative tools to defend against cyber crime. To achieve our objectives and in order to produce a better solution dedicated to make the forensics techniques and tools accessible to everyone to defend well against cyber crime, we will first present the world of forensics, define the steps necessary for an investigation, examine tow of the most popular solution SIFT and DEFT, model the process they use, and set a benchmark to produce our solution. The proposed solution is in the direction of specialization and is designed to facilitate access to these techniques and tools to improve the methodology used in the investigation to defend against cyber crime.***

Keywords: Forensics, Digital Forensics, Forensic Appliance, Forensics tools, Forensics Techniques.

I. INTRODUCTION

Over the past years, the number of crimes involving computers has increased, which caused an increase in companies and products that plan to assist law enforcement by using digital evidence to figure the who, what, where, when, and how for crimes. As a result, computer forensics has expanded to ensure proper presentation of digital evidence in court. in order to achieve this goal, the computer forensics has provided many tools and techniques in the context of criminal investigations and computer security incident handling, these tools and techniques are used to respond to an investigation by investigating suspect systems, gathering and preserving evidence, reconstructing events, and assessing the current state of an event. [6]

After many research we found that the major problems that face the investigators every time can be reflected in, which forensic tools are necessary to perform a digital forensics, where they can find these tools, how to install it and how to use it. Besides that, they must use every tool alone and sometimes they have to move the results provided by a tool to another system for review by another tool, which means waste a lot of time and it is not professional at all.

This paper is organized as follows: Section II presents the world of forensics. Then section III presents some existing solutions and their disadvantages. Then in section IV, we will propose a solution that fulfills our objective. Finally, in section V we will propose some forensics recommendations for a better result.

Revised Version Manuscript Received on 25 January, 2019.

Yassine ElBahlouli, Forensics and Cyber-security Researcher in "Systems Engineering Laboratory, Data Analysis and Security Team". National School of Applied Sciences, University Ibn Tofail, B.P 241, Kénitra 14000, Morocco.

Nabil Hmina, Researcher and Director of "Systems Engineering Laboratory, Data Analysis and Security Team". National School of Applied Sciences, University Ibn Tofail, B.P 241, Kénitra 14000, Morocco.

II. DIGITALFORENSICS

2.1. Definition

Digital Forensics also known as computer forensics generally defined as the application of the science of identification, collection, examination, analysis of data and the production of digital evidence, while preserving the integrity of the data. [1]

Data refers to specific items of digital information that have been formatted in a specific way. For example, data can be stored or transferred by standard computer systems, network equipment, personal digital assistants (PDAs), and various types of media, among other sources.(PDAs).

2.2. Forensics process

Digital Forensics also known as computer forensics generally defined as the application of the science of identification, collection, examination, analysis of data and the production of digital evidence, while preserving the integrity of the data. [1]

Data refers to specific items of digital information that have been formatted in a specific way. For example, data can be stored or transferred by standard computer systems, network equipment, personal digital assistants (PDAs), and various types of media, among other sources.Fig.1".

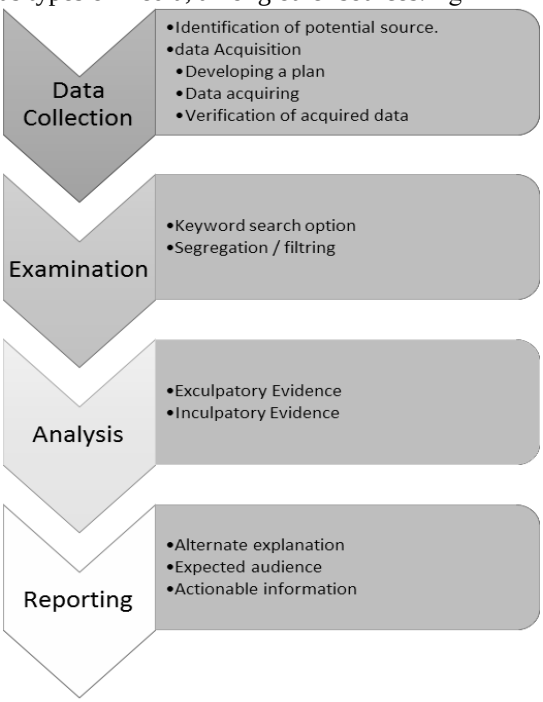

Fig.1. Forensics Process [2]

Collection, Examination, Analysis and Reporting, defined as follows:

Data Collection: identification, labeling, registration and acquisition of data from all possible sources of relevant data, while following procedures that maintain the integrity of the data. [3]
Examination: processing data using a combination of automated and manual methods, beside the assessment and data extraction of particular interest, while preserving data integrity. [3]
Analysis: analyzing the results of the examination, using methods, legal and justifiable techniques to obtain useful information that addresses issues that motivate to complete the collection and examination. [3]
Reporting: presenting the results of the analysis, which may include the description of the actions used, explaining how tools and procedures have been selected, determine what other actions should be, and provide recommendations for improving policies, procedures, tools and other aspects of the judicial process. [3]

III. RELATEDWORK

There are many similar solutions for our problem. However, analyzing these solutions can give us an idea about their advantages and disadvantages that will help us to determine the needs of potential users. Among these solutions, we have: SIFT and DEFT.

3.1. SIFT

The SANS Investigative Forensic Toolkit (“SIFT”) is a computer forensics VMware appliance completely built on an Ubuntu base with some forensics tools and capabilities that can match the modern forensic tool. SIFT is pre-configured with some necessary tools to perform a detailed digital forensic examination.
Among the disadvantages of the Appliance SIFT, we found:
- Complex Interface and not easy to manage, the interface used is the classic interface of Ubuntu itself.
- Difficulty of access to the forensics tools installed, no menu designed only for computer forensics tools.
- Lack of important tools like password cracking tools
- Size: 2.36 GB

3.2. DEFT Toolkit:

The Digital Evidence & Forensics Toolkit (“DEFT”) it is a live system with tools for computer forensics and incident response created for the Computer Forensics specialists. DEFT contains many forensics tools almost 50.

DEFT also has some disadvantages, among these disadvantages we find:
- Lack of important tools, such as:
1. Ghiro: analyzing the digital image
2. Hashcat: password hach cracking
3. Rarcrack: Archives password cracking
- Very large size: 3.08 GB

IV. PROPOSED SOLUTION

In order to facilitate any investigation for forensics experts to achieve effective results, we propose the following solution.
Indeed, we propose a development of an Appliance including major and important tools for digital forensics. In our case, this Appliance represents a "Live CD", more precisely we will modify a Linux environment and make it an environment dedicated only to computer forensics, by installing the most important computer forensics tools, and then make it a system ready to install and use.

This solution includes all the advantages and eliminates all disadvantages of previous solutions. It includes 40 tools in a special menu divided in eight categories (Analysis, Imaging, Hashing, Password Recovery, Data Recovery, Network Forensics, Mobile Forensics and Reporting Tools)”Fig. 2”. Besides that, it presents a friendly and a stable interface, which facilitates access to all these tools; in addition, some scripts are ready to use to execute the complex tools with one simple click, which make it an exceptional solution for all investigators.

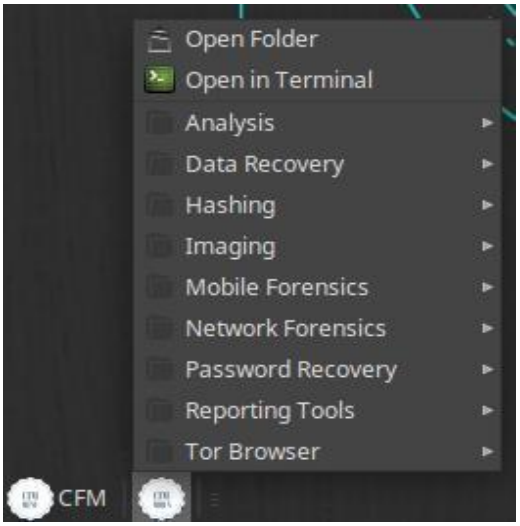

Fig.2: CFM Special Menu

V. RECOMMENDATIONS

The analysis phase is the most important phase in any investigation. So in order to succeed in your investigation you have to analyze your data correctly, so here are some valuable advices:

A. Analysts should use a methodical approach to analyze data.

The legal foundation of computer uses a systematic approach to analyze available data so that analysts can either draw appropriate conclusions based on available data, or determine that no conclusions can yet be drawn. If an evidence may be needed for legal or internal disciplinary actions, analysts should carefully document the results and the measures taken. [5]

B. Analysts should consider copies of files, not the original files.

During the collection phase, the analyst must make multiple copies of files or file systems desired, usually a master copy and a working copy.

The analyst can then work with the files of the working copy without affecting the original files or the master copy. [5]

C. Analysts should consider the loyalty and value of each data source.

Analysts should have more confidence in the original data sources than the data receive from other sources. Analysts must validate any unusual or unexpected data based on the interpretation of data, such as IDS and SEM alerts. [5]

D. Analyst smustrelyon the file headers, and no to next en sions to identify file types of content.

Because users can map a file extension to another file, analysts should not assume that the file extensions are accurate. Analysts can identify the type of data stored in many files by examining their file headers. Although people can change the file headers to hide the actual types of files, which is much less common as changing file extensions. [5].

E. Analysts genera lly should focus on the characteristics and impact of the event.

Determining the identity of an attacker and similar actions is generally difficult, and they do not help the organization to correct operational problems or vulnerabilities in their system. Establish the identity of an attacker may be important, but it must be balanced with other important goals. [5]

F. Organizations should be aware of the technical and logistical complexity of the analysis.

One event produces more information than analysts can realistically review. Tools such as SEM can assist analysts by bringing information from many data sources in one place. [5]

G. Analysts should gather data from various sources.

The analyst should examine the results of the review and analysis of individual data sources, such as data files, operating systems, and network traffic, and how the information goes together with a detailed analysis of the events related to the implementation and reconstruction of the event. [5]

VI. CONCLUSION

The general objective of this article is to develop a computer forensics appliance. The main aspects taken into account in our case are regroup the best tools for computer forensics, reorganize these tools according to their categories and finally make the appliance accessible to the world. Then we analyzed other appliances similar to our objective and we have determined disadvantages to decide the necessary improvements, remove the tools that they are not important to minimized the size of the appliance and add other tools that are very important to facilitate any investigation and get a better result.

REFERENCES

1. Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang, Guide to Integrating Forensic Techniques into Incident Response, August 2006
2. Muhammad Sharjeel Zareen, Adeela Waqar, and Baber Aslam, Digital Forensics: Latest Challenges and Response, 2013
3. Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, Common Phases of Computer Forensics Investigation Models, June 2011
4. Sabah Al-Fedaghi and Bashayer Al-Babtain, Modeling the Forensics Process, October 2012
5. Mark Pollitt, The key to forensic success: examination planning is a key determinant of efficient and effective digital forensics,
6. Advances in Digital Forensics (Mark Pollitt, February 13-16, 2005)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication