The Role of Digital Forensics in Combating Cybercrimes

Malek Harbawi and Asaf Varol
Software Engineering Department
Technology Faculty, Firat University
Elazig, Turkey
malek@firat.edu.tr, varol.asaf@gmail.com

Abstract—The recent development in Information Communication Technology (ICT) has made changes in every aspect in our life. These changes are clearly reflected in cyberspace-related areas. The positive influence of cyberspace on knowledge, trade and business, and communication is undoubtable. However, there is a dark side of cyberspace deteriorates its peaceful usage that is cybercrimes. Cybercrimes are defined as any illegal activities practiced by or done via cyberspace and its electronic environment. Unlike “traditional” crimes, cybercrimes present a real dilemma due to the fact that criminals’ identity may be hidden or fraud in virtual domain. The concept of digital forensics have come to the existence in an attempt of formulating possible ways for cybercrimes investigation and analysis process. In this paper, we deplore the concept of digital forensics in the context of cybercrimes. An investigation of the positive impact of digital forensics in combating cybercrimes is discussed and useful remarks on open research issues are provided for further investigation activities.

Keywords—cybercrime; digital forensics; cyber-attacks; digital forensics tools, technology gap

I. INTRODUCTION

Without a doubt, the last few decades are representing a major breakthrough in Information Communication Technology (ICT). The emergence of the Internet or cyberspace as a very effective communication medium has brought countless benefits. Most of our activities have been moving from the physical world to virtual world where cyberspace is the keyword. This is clearly realized in practical systems such as e-commerce, e-learning, e-banking, etc., which have tremendously facilitated and speeded-up most of transactions. We have been even observing the change in English lexiconology where a few terms are extensively used in the daily work and talk such “google it” or “email it”; which were not familiar a few decades ago [1]. Obviously, the positive impacts of cyberspace are not questionable, yet there is a very dark side within its use that is security matters. Ever since the dawn of cyberspace, cyber-attacks have been considered as a rapidly evolved trend on this complicated space. These attacks may vary from a basic e-mail stalking to very sophisticated crimes or cyber-terrorism and generally referred to as cybercrimes [2]. As a response, various security aspects have been set to ensure the safety of cyberspace.

Numerous software development companies have released computer anti-malware programs aiming to suppress and tackle any security breaches. Although, one cannot deny the positive role of anti-malware in protecting our electronic systems; yet security breach is an only one of cyber-generated concerns. Among complicated risk issues on cyberspace is the cybercrimes investigation process. Unlike “traditional” crimes, cybercrimes investigation is not straightforward, especially with the assumption of hidden or fraud identity [3]. In this regard, a relatively new concept has emerged to cope with cybercrime investigation issues along with other legislation process that is digital forensics [4].

Prior going ahead in explaining the details of digital forensics and its role in combating cybercrimes, one should imagine the huge gap between the vast evolution in the digital world and the legislation process. “Upgrading” the judicial system is not as fast and easy as its technological opponent. This is, in fact, causing a struggle in following-up with up-to-date cybercriminal activities and techniques [1, 5]. As the dependency on electronic systems is becoming more eminent, technology heavily forces the world to jump into the cyberspace where almost three billion Internet users, forming 40.4% of the world’s population, were recorded in 2014 [6]. The usage of cyberspace, though, imposes on us leaving a trail behind. This trail may be in the form of history in browsing, sent e-mails, social media interactions or perhaps the use of a credit card [7]. The exponential growing in digital data in the world confirms the previous fact. According to some reports, the amount of digital data in the world in 2014 was 4.4 zettabyte (one zettabyte is equal to a trillion gigabyte). This figure will grow to become 44 zettabyte or in other words there will be 5,200 GB of data for every person on Earth [8-11]. This massive amount of digital data is finding its way to legislation as digital evidence can be extracted from it. Nevertheless, the judicial system is yet to be qualified for this purpose [1, 11]. This is simply resulting from the fact that a considerable number of law-enforcement personnel does not really have the interest in technology and some of whom do not even care to surf the Web. Unfortunately, cybercriminals have advanced levels equal, if not surpassing, the skills law-abiding technology professionals own. These criminals may use variety of methods and tools to reach their goals and perhaps leaving little of null tracing behind.
Scientists and researchers proposed digital forensics concept to help in extracting the right digital data from the vast amount of digital data which is generated from both law-abiding citizens as well as criminals. Digital forensics can be simply defined as the process of identifying, uncovering, preserving, retrieving and analyzing of digital evidences using scientifically proven methods, tools and formulas that facilitate the reconstruction and retrieval of these digital evidences in a way that ensures the admissibility of the retrieved evidence in the court of law; which imposes the existence of a computer-based or cyberspace-based crime scene and the needed technical investigation skillset [12-14]. Although, the concept of forensic sciences is relatively old, digital forensics field is still at its early stages and various topics should be researched, investigated, highlighted and presented to students and interested readers.

In this paper, we present the role of digital forensics in context of cybercrimes and how this field of knowledge can assist in law-enforcement in cyberspace community. The paper is organized as follows: A brief introduction is presented in section I followed by an insight on digital forensics in the context of cybercrime in section II. In section III, an overview of some tools used for digital forensics investigation in cybercrimes. A general consideration for challenging contemporary research ideas in the field of digital forensics is highlighted and reviewed in section IV. Finally, the paper is concluded with authors’ remarks and directions for further investigation in section V.

II. DIGITAL FORENSICS IN THE CONTEXT OF CYBERCRIME

A. Digital Evidence

As briefly presented in section I, the idea of digital forensic sciences is based on an electronic environment and/or cyberspace crime scene. In this regard, it is likely to need the know-how to be able to analyze the crime scene. This analysis aims at identifying the puzzle pieces that solve the electronic crime. Therefore, the first thing should be considered is the evidence which in this case is likely to be in the digital form. Digital evidence can be defined as any form of data that moved from/to an electronic system; which could be a document, an audio, a video, browsing history, social media activities, logs, e-banking and credit card transactions [15, 16]. In fact, the digital evidence may be also in the form of e-signature, online shopping or appointment [17].

Currently, the ubiquity of computer systems, dependency on electronic devices as well as cyberspace create variety of forms and lots of digital evidences that can be traced. It is essential to present the sources of digital evidence to enhance the understanding of the reader and to increase the awareness of both law-makers and researchers. Digital evidence may generated by [7]:

- Open computer systems: Including any internal or external storage, input and output devices, and any peripheral devices.
- Communication systems: Including traditional and mobile phones, wireless devices, routers, cyberspace, and any network in general.

- Embedded computer systems: Including portable devices, smart cards, tablets, MP4, PDA and any other device with an embedded computer.

These sources of digital evidence are generally used by criminals as well as law-abide citizens. The generated evidence, for instance an e-mail message, includes vital information in its header as well as its content. It is also important to note that e-mail messages provide the date and time they were sent, via which ISP (Internet Service Provider) they came through and who likely they are sent from. Even though these vital pieces of information are presented in only one type of digital evidence, they can be confused, overlooked and even disregarded due to the lack of the technical experience needed for analyzing them. In addition, the content provided by digital evidence may become confusing and misleading if not properly investigated and analyzed.

The issue of digital evidence awareness is extremely important and it should be re-evaluated and considered by researchers in their studies. A number of researchers have attempted to investigate and highlight this issue; for example, a team from the Advanced System Security Education, Research, and Training (ASSERT) Center, University of Alaska, had conducted a practical education program in promoting digital forensics awareness targeted K-12 students, K-12 teachers, business personnel, community members, and higher education audiences [18]. The training program aimed at presenting digital forensics (including digital evidence) in forums and also the safe use of computer systems in daily activities. Although the program was an important initiative yet it is not enough by itself to ensure the awareness of investigators, especially lawmakers, on the importance of digital evidence and the proper way to analyze it. Apart from this work, a more extensive research was conducted in [19] where the author attempted to address judges’ awareness of digital evidence. The study was the first to be known in the US and it concluded that although judges recognized the importance of digital evidences and how carefully it should be dealt with. Yet, they indicated that they should be provided with specialized training to increase their knowledge in digital forensics field. For further information on the same aspect, the reader is advised to check [20-23].

B. Digital Forensics: The Concept

Digital forensics is basically represented by the application of forensic science disciplines to electronic-based crime scenes following certain legal procedures. The concept of forensic sciences has been in practice for a long while; however, its digital forensics counterpart has recently been established as a distinguished part of knowledge. This can be easily noticed by the massive number of publications related to digital forensics in the last few years. The original of digital forensics roots back to late 1999s and early 2000 where it was considered as computer forensics due to the crime and evidence nature [24]. However, in a matter of a few following years, the concept has changed as a response to ubiquity, especially over the Internet, to cover all forms of digital-based forensics. This is particularly true as we are witnessing the unusual growth in cybercrimes and terrorism. Cyberspace, has become a very fertile ground for organized criminal groups and individuals attacking variety of targets using different maneuvers. According to the Center
for Strategic and International Studies, cybercrimes cost the world approximately $400 billion [25, 26]. Thus, the choice of investigating the role of digital forensics in combating cybercrime is highly justified.

C. Digital Forensics: Tenets

The main principles of digital forensics are applied with the following areas [15, 25]:

- Identification: Prior to any investigation step, the identification of relevant digital elements that can be used for data acquisition should be done. These elements include: computers, mobile phones, PDAs, tablets, or any other electronic device may contain and store digital information, and storage devices such as hard disks, pen drives, CDs, DVDs and other peripheral device capable of storing digital data.

- Acquisition: Once the items of interest have been identified, the process of digital acquisition initiates. Here, acquisition is done by seizing electronic devices found or attached to the crime scene and forensically acquiring (copying) the data found on their memory for investigation purposes.

- Preservation: The acquired evidence should be kept the way it is acquired in the first place. This is done via a well formulated chain to ensure the preservation of the evidence from intended and unintended alteration to its contents. During forensic acquisition process, read only copies of acquired evidences should be also taken as precaution step.

- Examining and analyzing: Evidence examining is done as step in categorizing the digital evidence and the tools that can be used in analyzing it. For instance, evidence extracted from an email contains different data and metadata compared to data and metadata extract from an image. Once the evidence has been examined, the analysis step starts by identifying the methods, tools, and skills needed for extracting vital information that can be used in the court of law. This step has a very core importance and relies much on the forensic examiner’s experience and skills.

- Presentation: The final step in forensic process where the examiner should provide a report, documentation, on how the forensic process was done, what type of tools and methods were used, legal protocols and policies followed, forensics findings and relevant articulations. The report should be written in an understandable and explicit language, consistent with the findings and accurate in its presentation.

Considering these processing steps or procedures, when the forensic process is attached to a cybercrime, there should be a special care to the following key points:

- Cyberspace is, somehow, considered as an unauthorized environment where identities can be hidden or hijacked.

- Ubiquity of the cyberspace where individuals, states, organizations share the same space with more or less same techniques.

- Back tracing of any criminal activity may not be a straightforward and easy task as billions of digital data sequences get exchanged in normal daily activities.

- The diversity of criminal activities on the cyberspace. Cybercriminals have been attacking almost everything worth the trouble over the Internet. This indeed implies the diversity in cybercrime techniques and tools.

- The cost of accessing and owning the skills to attack on the cyberspace is inexpensive. There are even organized groups that train and recruit new criminals with every day passes by.

- The targets of the attack may not be expected as we are yet to discover new cyber-attacks and illegal activities on the cyberspace.

- In some cases, cybercrimes represent only information warfare which cannot be easily identified in the first place.

- The ethical aspect that is attached to the investigation process needed by digital forensics in the cyberspace.

III. TOOLS USED FOR CYBERCRIME DIGITAL FORENSICS

Due to the diversity of cybercrimes, there is a number of tools used for digital forensics in cyberspace-related crimes. The following subsections briefly discuss the most commonly used tools for this purpose.

A. MemGator

As the name indicates, MemGator is a memory interrogation tool that automates the extraction of data from memory files and compiles a report on the extract data [26]. MemGator brings together a number of memory analysis tools such as the Volatility Framework and PTFinder into the one program. Data can be extracted in relation to memory details, processes, network connections, malware detection, passwords and encryption keys and the registry [28].

B. First on Scene

FoS is a scripted code written in visual basic and it works along with other tools such as LogonSessions, FPort, PromiseDetect, and FileHasher to create an evidence log report. Log report is very important for forensic investigators during the investigation process.
C. **Galleta**

Galleta tool is specialized in inspecting cookies’ files which are linked to browsing history. These files provide an idea on which websites were recently visited and where they keep their traces in the form of cookies.

D. **Ethereal**

Ethereal is network security tool used for sniffing packet traffic on the network (incoming and outgoing). Although this tool is useful; however, it is fragile against encryption codes which deteriorate its performance.

E. **Pasco**

Pasco is a tool used extensively in analyzing browsers’ contents and helps in identifying the conducted transaction based on the analyzed contents. The origin of the name comes from Latin language where Pasco means browse.

F. **Rifiuti**

This tool performs its action on recycle bin of the system to recover any recent deleted files. Rifiuti is an open source released under the liberal FreeBSD license [29].

G. **NMap**

Network Mapper or NMap is a network security tool that operates based on scanning a remote workstation for finding any open ports. NMap has the ability to hide its nature from the source workstation so that it won’t cause any alert as a malware attack [30].

There are a number of other digital forensics tools and software kits found in the literature. However, discussing them will be beyond the sections of this short paper.

IV. **CHALLENGES WITH CYBERCRIME DIGITAL FORENSICS**

One of the objectives of this paper is to present open research questions for the benefit of the reader as well as enriching the research in this interesting field. In the following sub-sections, a number of issues yet to investigated and studied.

A. **Data View Inconsistency**

It is often to discover that the visualized content over cyberspace does not always represent the same saved copy on the disk which creates a confusion and even inaccurate results in forensic analysis. This opens an area for investigation on how we can solve this issue and which protocols, tools, upgrades, etc., can be used to alleviate the impact of this scenario.

B. **Evidence-Oriented Design**

Current digital forensics tools were originally designed to analyze the digital evidence irrelevant to the circumstances. Meaning that, the examined evidence facilitates the investigation process but does not solve any issue over the cyberspace. In addition, most of these tools deal with crimes committed on a computer not against, for example, a human being [14].

C. **Object-Interpolation Mechanism**

It was discovered a few years ago that it is possible to interpolate a missing part of a JPEG file. Unfortunately, this feature is not really found in contemporary digital forensics tools.

D. **Run-Time vs. Performance**

The majority of forensic tools are running in a very slow mode performance, most of them take a relatively long time to complete its task. This may affect the outcomes of the investigation specially when the time mattes.

E. **Digital Forensic Awareness**

One of the key research areas in this field is the development of a comprehensive educational training that can be provided to both investigators as well as judges and persecutors to be enlightened on digital forensics and its application to cybercrime.

F. **Technology Gap**

There is an obvious technology gap between cybercriminals and combating tools and software kits and, unfortunately, it is in the favor of cybercriminals. This indicates the importance of researching security software techniques and tools in order to lessen this inevitable gap [31].

G. **Technology vs. Tools**

The gap between the emerging smart technologies and forensic tools. This offers a very rich area of research in developing tools that are compatible with current smart devices and can be provided for public use.

V. CONCLUSION

In this paper, an attempt to discuss the role of digital forensics in combating cybercrimes was provided. Throughout the paper, various important aspects, features and technologies were presented and uttered. It is observed that there is a considerable gap between the current available digital forensics tools and the optimal application of the digital forensics concept. This observation was investigated within the sections of this paper. Based on that, some vital considerations were highlighted to provide areas for contemporary research aiming to enhance digital forensics implementation and investigation process especially for cybercrimes. Although the current gap between the realized technology and digital forensic tools is big, it still can be lessened by supporting the research in this direction.

REFERENCES

The Role of Digital Forensics in Combating Cybercrimes