AN AUDIT: DIGITAL FORENSICS RESEARCH

[1]SANDEEPAK BHANDARI, [2]VACIUS JUSAS

[1,2]Software Engineering Department Kaunas University of Technology Lithuania
E-mail: [1]sandeepak.bhandari@ktu.edu, [2]vacius.jusas@ktu.lt

Abstract- As explosive growth of internet and its users, production and use of electronic and innovation in technologies increase the importance of digital forensic science. Digital forensic involves collection, examination, analysis and reporting of digital evidences from digital devices that not only assesses the damage of electronic attack but also to recover lost information from such a system to prosecute a criminal. With the growing of importance of digital security today, the digital investigators need to understand how digital forensic is using and its importance in digital era to solve the digital crime case. In this paper, we provide acomprehensive review over digital forensic, its importance, digital forensic process, challenges and their overcome and future research areas in digital forensic field.

Keywords- Computer Forensics, Digital Forensics,Digital Evidence, Digital Forensics Process and User data.

I. INTRODUCTION

Computer forensics, also known as 'digital forensics,'is a term used to describe a new field that involves the intersection of digital evidence and the law. Computer forensics is the process of identifying, preserving, and analyzing data and technical items for evidence that will be used in court.Forensic examiners typically analyze data from personal computers, laptops, personal digital assistants, cell phones, servers, tapes, and any other type of media. This process can involve anything from breaking encryption, to executing search warrants with a law enforcement team, to recovering and analyzing files from hard drives that will be critical evidence in the most serious civil and criminal cases.The forensic examination of computers, and data storage media, is a complicated and highly specialized process. The results of forensic examinations are compiled and included in reports. In many cases, examiners testify to their findings, where their skills and abilities are put to ultimate scrutiny.

In late 1990s and early 2000 the digital forensics developed as an independent field when computer based crime sterted growing with the growth of use of computer systems and internet.In early days,it was called computer forensics because the collection of digital evidence restricted to computer system.However nowadays due to technology development, use of electoronic devices there is no such kind of restriction.

Moreover it is difficult to pinpointexactly when computer forensics history began. Most experts agree that the field of computer forensics began to evolve more than 30 years ago. The field began in the United States, in large part, when law enforcement and military investigators started seeing criminals get technical. Government personnel charged with protecting important, confidential, and certainly secret information conducted forensic examinations in response to potential security breaches to not only investigate the particular breach, but to learn how to prevent future potential breaches. Ultimately, the fields of information security, which focuses on protecting information and assets, and computer forensics, which focuses on the response to hi-tech offenses, started to intertwine.

Over the next decades, and up to today, the field has exploded. Law enforcement and the military continue to have a large presence in the information security and computer forensic field at the local, state, and federal level. Private organizations and corporations have followed suit – employing internal information security and computer forensic professionals or contracting such professionals or firms on an as-needed basis. Significantly, the private legal industry has more recently seen the need for computer forensic examinations in civil legal disputes, causing an explosion in the e-discovery field.
The computer forensic field continues to grow on a daily basis. More and more large forensic firms, boutique firms, and private investigators are gaining knowledge and experience in the field. Software companies continue to produce newer and more robust forensic software programs. And law enforcement and the military continue to identify and train more and more of their personnel in the response to crimes involving technology

Digital forensic can be divided into five braches are as follows:

- Computer Forensics
- Network Forensics
- Mobile Device Forensic
- Memory Forensics
- Email Forensics

Computer forencics refers to the collecting and extracting the various files on the systems, reading the hard disk and finding the information from computer to collect digital evidences. Organizations and persons of all types rely heavily on email

communications, making it a crucial factor in every litigation. The number of worldwide email accounts continuing to grow from 4.1 billion in 2014 to 5.2 billion by the end of 2018 [17]. Deleted emails can often be recovered, even if they are erased intentionally. Metadata, such as email full header information, time stamps, etc., can all be very useful in an investigation if the authenticity of an email is ever brought into question. Email clients and servers are often full database applications, complete with document sources, contact managers, time managers, calendars, and many other features, all of which might be accessed forensically. Erasing or deleting an email does not necessarily mean that it is gone forever. Oftentimes, emails can be forensically extracted even after deletion.

Mobile Forensics is a branch of Digital Forensics and it is about the acquisition and the analysis of mobile devices to recover digital evidences of investigative interest. here is growing need for mobile forensics due to several reasons and some of the prominent reasons such as Use of mobile phones to store and transmit personal and corporate information, Use of mobile phones in online transactions and Law enforcement, criminals and mobile phone devices
Memory forensics is a vital form of cyber investigation that allows an investigator to identify unauthorized and anomalous activity on a target computer or server.

This is usually achieved by running special software that captures the current state of the system's memory as a snapshot file, also known as a memory dump. This file can then be taken offsite and searched by the investigator.This is useful because of the way in which processes, files and programs are run in memory, and once a snapshot has been captured, many important facts can be ascertained by the investigator, such as:

- Processes running
- Executable files that are running
- Open ports, IP addresses and other networking information
- Users that are logged into the system, and from where
- Files that are open and by whom

Network forensics is capture, recording and analysis of network packets in order to determine the source of network security attacks. The major goal of network forensics is to collect evidence. It tries to analyze network traffic data, which is collected from different sites and different network equipment, such as firewalls and IDS. In addition, it monitors on the network to detect attacks and analyze the nature of attackers. Network forensics is alsothe process ofdetecting intrusion patterns, focusing on attacker activity.

II. DIGITAL FORENSIC: THE PROCESS

The digital forensic process is a recognized scientific and forensic processusedin digital forensics investigations. Digital forensics process is multi-staged beginning from identification of digital devices from the scene as potential evidence to the stage where it is presented as evidence by an expert witness in a court of law. The sequence of various phases of digital forensics process shown in above Figure 1.

The first stage of the digital forensic process is evidence identification. It involves the identification of sources of digital devices capable of storing digital data associated with the investigation. Some examples that can provide digital evidences includes hard disk on computer systems,random access memory cards, USB and other external sources of secondary storage, mobile phones, PDAs and so on. Once identified, evidence is acquired from the devices and forensically preserved.

The next stage of digital forensic process is evidence acquisition and preservation. Acquisition refer to the process of collecting binary bitwise copy of the entire contents of all digital devices that are identified and preservation mean maintain an accurate representation of the original data and maximizes its usefulness for decision makers i.e.
it is as complete as possible. To preserve the acquired digital evidences standard hash signatures like MD5 or SHA1 is used to verify integrity of the digital evidences.

In digital forensic investigation, forensic investigator deals with acquiring digital evidences for examination. Digital evidences can vary in form and types it includes digital documents on computer system, telephone contact list, history of phone calls, trace of signal strength from the base station of a mobile phone, recorded voice and video files, email conversations, network traffic patterns and virus intrusions and detections are all examples of different types of digital evidences. In short, digital evidences encompasses:

a. User data
b. Metadata associated with user data
c. Activity logs; and possibly
d. System logs

Once the digital evidences are acquired then evidences are examined using one or more digital forensic tools(such as SANS SIFT, Sleuth Kit and many more).These forensic tools generally provide some kind of file system abstraction to the digital evidence, such that their contents may be examined for trace of evidence. This stage is known as evidence examination where

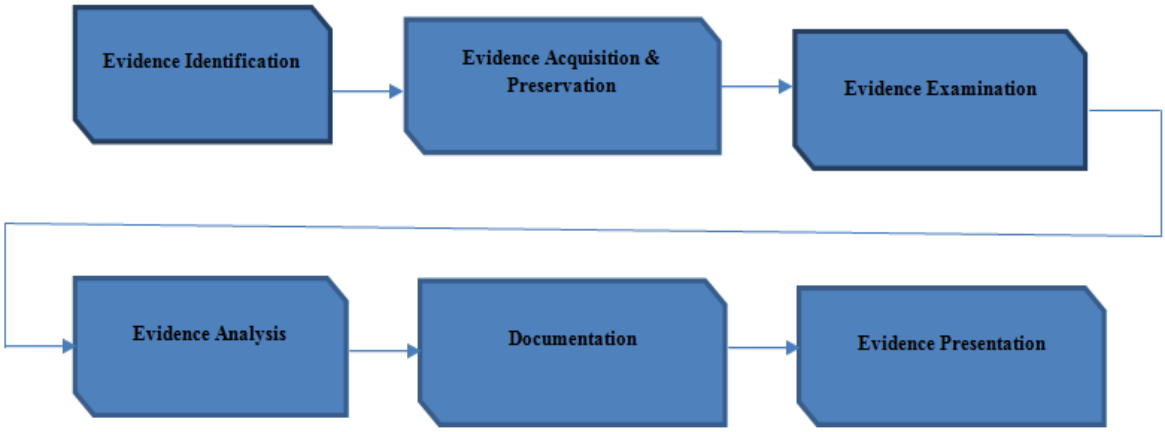


Fig.1. Digital Forensic Process

the digital evidence sources are examined for their contents and possibly indexed for conducting searches.

Casey [16] defines forensic examination as the process of extracting information from digital evidence and making it available for analysis. Afterexamination and discovery of evidences, analysis of digital evidences begins. Analysis refers to determine the sequence of events leadingtothereportedcrimeunderinvestigation.Casey[16] defines forensic analysis as the application of scientific methods and critical thinking to address the fundamental questions in an investigation: what, who, why, how, when andwhere.Each stage is thoroughly documented, and this documentation is presented in a court of law. Oftentimes, the presentation of digital evidence in court may be accompanied by an expert witness for testifying.

III. CLASSIFICATION OF LITERATURE REVIEW

In this section we review the immense area of digital forensics, to inform the state of the digital forensics, its development from beginning to still, innovation and current challenges faced by this field.

The term “forensics” derives from Latin “forensis”, which depicts “in open court or public” from Hong et al. [8].Mark[4] review and depicts complete history of digital forensic begins in late 1995 and still progress. Although there is tremendous advancement and innovation in digital investigation field, but all approaches based on four pillars it includes collection, examination, analysis and reporting.

Digital forensics is a multi-disciplinary and inter-disciplinary field encompassing diverse disciplines such as criminology, law, ethics, computer engineering, and information and communication technology (ICT), computer science, and forensic science by Roussev et al. [6].Various digital forensics branches such as computer forensics, network forensics and many other and their corresponding tools are reviewed which will help investigator to begin the blind case Noble and A.K [11].Each device is considered as digital crime scene which is included in the physical crime scene where it is located. The investigation includes the preservation of the system, the search, collection and interpretation for digital evidences, and the reconstruction of digital events. The aim of the investigation is on the reconstruction of events using evidence so that hypotheses can be developed and teste by Brian and Eugene [12].The taxonomy of digital forensic research can be split into four main streams digital forensic process modelling, acquisition and modelling, examination and discovery and digital forensic analysis Sriram [15].

Oluwasola [1], stated that one of main challenge faced by digital forensic is continuously increase volume of data that need to be analyzed. Based on this problem author suggest that there is change required in the system of digital forensic investigation which can handle this big data and future challenges. For this author proposed a digital forensics analysis framework, which can reassess the various phases of digital forensic investigation process and introduce into each phase the needed techniques to improve better digital evidence collection, analysis, preservation and presentation to overcome big data and other challenges facing by digital forensics.

Nowadays by explosive growth of internet and use of electronic devices, digital forensic get more important. The huge amount of multimedia data from different codecs and formats and limited amount of time to investigate it is one of the huge challenges by Rainer and Simon [2]. Nordiana et al. [5], provide three main issues and challenges such as technical and procedure, digital forensicand legal enforcement issues. Moreover, authors suggest that knowledge and skill in managing the digital evidence is an important criterion should be Considered and it can be implemented by put digital forensic module in syllabus of university and colleges.

Luca et al. [7], concluded the new generation of forensics tools should be developed to support heterogeneous investigations, preserve privacy, and offer scalability.For ensuring investigation of request timely, signature-based methods for automated action instance approximation to automatically reconstruct past user activities within a compromised or suspect system proposed by Joshua and Pavel [9].Many solutions have been proposed from data mining, data reduction, increased processing power, distributed processing, artificial intelligence and many other to overcome volume of data challenges in digital forensics by Darren and Kim [10].

Nicole [3], mention four key research themes in digital forensic investigation field for substantial effort such as (i)volume and scalability challenges, (ii) intelligent analytical approaches, (iii) digital forensics in and of non-standard computing environments, and (iv) forensic tool development. Digital forensics need to adopt standards and modular approaches for data representation and forensic processing by Simson [13] for transparency among researcher and better innovation.
David et al. [14], discuss the future research areas in digital forensics it includes Distributed Processing, HPC and Parallel Processing, GPU-Powered Multi-threading, Digital Forensics as a Service (DFaaS), Field-programmable Gate Arrays and Applying Complementary Cutting-Edge Research to Forensics.

IV. CHALLENGES

Digital investigator working with digital devices for identifying, analyzing and examination of digital evidences. Digital evidences can be in various forms and types. According to Raghavan [1], digital evidences can be in the form of pictures, audio, documents on computer, telephone contacts, video files, email conversations, encrypted data, instant messenger conversation and network traffic patterns. Due to advancement in technology and explosive growth of internet and its users had bring various challenges in this field. The presence of set of hybrid technologies are not only the factor increasing the complexity of problem space to be faced when performing digital investigations. The digital forensics faces many challenges from both ethical and technological viewpoints:

- High speed and volumes

The using of gigabit class links and multimedia-rich contents accounts for an explosive growth in the volume of data to be stored, processed and analyzed for collecting clues and evidence or detecting incidents. This is of particular relevance in the case of live network forensic analysis, as the investigator might not be able to capture and store all the necessary traffic. Nevertheless, issues related to acquiring, storing, and processing large amounts of data for forensic purposes have been causing problems for at least a decadeand are now exacerbated by the ubiquitous availability and massification of digital information.

- Explosion of complexity

The innovative advances in and expansion of novel services account for a sensational increase in the complexity that forensics professionals must manage. In particular, evidence is no longer confined within a single host but, rather, is scattered among different physical or virtual locations, such as online social networks, cryptocurrency wallets, CaaS machinery, cloud resources, and personal network–attached storage units. For this reason, more expertise, digital forensic tools, and time are needed to completely and correctly reconstruct evidence from digital devices. This explosion in complexity also effects the length of digital investigations, including the degree of occupancy of resources involved (such as the manpower of forensics experts or third parties, including specialized professionals hired by LEAs). Such issues could be partially solved by automating some tasks.However, this has been exceedingly criticized by the digital investigation community, since it could rapidly deteriorate both the quality of the investigation and the information of crime scene investigation specialists

- Development of standards

As mentioned earlier, digital forensics need the ability to handle various hardware and software entities, ranging from RAM to USB solid-state mass storage. Although technological advances, files are still the most popular digital artifacts to be collected, categorized, and analyzed for digital evidences. Thus, the research community has tried to agree on standard formats, schema, and ontologies—but without much success.Investigations of cutting-edge cybercrimes might require processing and interpreting information in a collaborative manner or using outsourced storage and computation. Therefore, a core step for the digital forensic community will be the development of proper standard formats and abstractions.

- Privacy-preserving investigations

Today, people bring into cyberspace various aspects of their lives, mainly through online social networks or social media sites. Unfortunately, collecting information to reconstruct and locate an attack can severely violate privacy of users and is linked to other hurdles when cloud computing is involved.

- Rise of antiforensics techniques

As defensive measures become increasingly efficient, more aggressive deployment of anti-forensics methods can be envisioned. These encompass encryption, obfuscation, and cloaking techniques, including information hiding. For example, a challenge for filesystem analysis is steganographic configurations, which allow hiding information in

unused areas of the hard disk or in metadata, such as timestamps. With the exception of binary obfuscation, such mechanisms aren't yet widespread, but they could become relevant for digital forensics investigation in the mid-term future.

CONCLUSION

In this paper we present the overall scenario,to help the new researchers or scholars to understand the era of digital forensic. We reviewed and discussed the various perspective of authors and their contribution to understand digital forensic deeply. Webegin our review from the history of digital forensic, its basic fundamental such as digital forensic process and its basic four pillars namely collection, examination, analysis and reporting, classification of digital forensic (such as computer forensic, network forensic).In the paper various challenges face by digital forensic such as High speed and volumes, Explosion of complexity, Development of standards and many more and to overcome these challenges various approaches such as
to support heterogeneous investigations, preserve privacy, and offer scalability are discussed. For substantial approach for digital investigation four key research themes should be includedvolume and scalability challenges,intelligent analytical approaches,digital forensics in and of non-standard computing environments and forensic tool development.

REFERENCES

[1] O. M. Adedayo, "Rethinking Digital Forensics," 2016 IEEE Int. Conf. Cybercrime Comput. Forensic, pp. 1–7, 2016.

[2] R. Poisel and S. Tjoa, "Forensics investigations of multimedia data: A review of the state-of-the-art," Proc. - 6th Int. Conf. IT Secur. Incid. Manag. IT Forensics, IMF 2011, pp. 48–61, 2011.

[3] N. Beebe, "Digital Forensic Research: The Good, the Bad and the Unaddressed," pp. 17–36, 2009.

[4] M. M. Pollitt, "An ad hoc review of digital forensic models," Proc. - SADFE 2007 Second Int. Work. Syst. Approaches to Digit. Forensic Eng., pp. 43–52, 2007.

[5] N. Rahim, A. Wahid, M. Yamani, and M. Laiha, "Digital Forensics: An Overview of the Current Trends (PDF Download Available)," Int. J. Cryptol. Res., vol. 4, no. 2, 2014.

[6] V. Roussev, "Digital forensics," Comput. Handbook, Third Ed. Inf. Syst. Inf. Technol., no. April 2017, pp. 56-1-56–29, 2014.

[7] L. Caviglione, S. Wendzel, and W. Mazurczyk, "The Future of Digital Forensics: Challenges and the Road Ahead," IEEE Secur. Priv., vol. 15, no. 6, pp. 12–17, 2017.

[8] H. Guo, B. Jin, and D. Huang, "Research and review on computer forensics," Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng., vol. 56, pp. 224–233, 2011.

[9] J. I. James and P. Gladyshev, "Automated inference of past action instances in digital investigations," Int. J. Inf. Secur., vol. 14, no. 3, pp. 249–261, 2015.

[10] D. Quick and K. K. R. Choo, "Impacts of increasing volume of digital forensic data: A survey and future research challenges," Digit. Investig., vol. 11, no. 4, pp. 273–294, 2014.

[11] N. Kumari and A. K. Mohapatra, "An insight into digital forensics branches and tools," 2016 Int. Conf. Comput. Tech. Inf. Commun. Technol. ICCTICT 2016 - Proc., pp. 243–250, 2016.

[12] B. D. Carrier and E. H. Spafford, "An Event-Based Digital Forensic Investigation Framework," Ecol. Modell., vol. 213, no. 3–4, pp. 1–12, 2004.

[13] S. L. Garfinkel, "Digital forensics research: The next 10 years," Digit. Investig., vol. 7, no. SUPPL., 2010.

[14] D. Lillis, B. A. Becker, and M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation," 2016.

[15] S. Raghavan, "Digital forensic research: current state of the art," CSI Trans. ICT, vol. 1, no. 1, pp. 91–114, 2013

[16] E. Casey, Digital Evidance And Computer Crime. 2011.

[17] Radicati Group, Inc., "Email Statistics Report, 2014-2018",http://www.radicati.com/wp/wp-content/uploads/2014/01 EmailStatistics-Report-2014-2018-Executive-Summary.pdf

★★★