 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

Digital Forensics

Avneet Kaur
Dept. of Computer Science, SGHCMT, Raipur, Bahadurgarh, Patiala, Punjab, India

Abstract
Crimes committed within electronic or digital domains, particularly within cyberspace, have become common. Criminals are using technology to commit their offenses and create new challenges for law enforcement agents, attorneys, judges, military, and security professionals. Digital forensics has become an important instrument in identifying and solving computer-based and computer-assisted crime. This paper provides a brief introduction to digital forensics.

Keywords
Digital Forensics, Digital Forensic Science, Computer Forensics, Network Forensics.

I. Introduction

Digital devices such as cell phones, tablets, gaming consoles, laptop and desktop computers have become indispensable part of the modern society. With the proliferation of these devices in our everyday lives, there is the tendency to use information derived from them for criminal activities. Crimes such as fraud, drug trafficking, homicide, hacking, forgery, and terrorism often involve computers. To fight computer crimes, digital forensics (DF) originated in law enforcement, computer security, and national defence. Law enforcement agencies, financial institutions, and investment firms are incorporating digital forensics into their infrastructure [1]. Digital forensics is used to help investigate cybercrime or identify direct evidence of a computer-assisted crime. The concept of digital forensics dates back to late 1990s and early 2000s when it was considered as computer forensics. The legal profession, law enforcement, policy makers, the business community, education, and government all have a vested interest in DF. Digital forensics is often used in both criminal law and private investigation. It has been traditionally associated with criminal law. It requires rigorous standards to stand up to cross examination in court.

II. Characteristics of DF

Digital forensics is usually associated with the detection and prevention of cybercrime. It is related to digital security in that both are focused on digital incidents. While digital security focuses on preventative measures, digital forensics focuses on reactive measures. Digital forensics can be split up into five branches [2]: computer forensics, network forensics, mobile device forensic, memory forensics, email forensics. Peer-to-peer file sharing is the soft area targeted by the criminals. Mobile device forensics is a newly developing branch of digital forensics relating to recovery of digital evidence from a mobile device. The digital medium has become the key area for email hacking.

III. Principles of DF

DF is derived as a synonym for computer forensics, but its definition has expanded to include the forensics of all digital technologies [3]. A digital forensic investigation can be broadly divided into three stages: preservation of evidence, analysis and presentation/reporting. Digital evidence exists in open computer systems, communication systems, and embedded computer systems. Digital evidence can be duplicated exactly and it is difficult to destroy [4]. It can be found in hard drive, flash drive, phones, mobile devices, routers, tablets, and instruments such as GPS. To be admissible in a court of law, evidence must be both relevant and reliable. To date, there have been few legal challenges to digital evidence. Forensic analysis identifies the puzzle pieces that solve the computer crime. It requires using efficient tools. A number of software tools that are now available for trained forensic investigators to use. Analysts conduct investigations using various techniques following the principles of forensic science. The presentation of evidence involves preparing a report to present the findings to all stakeholders including the judge, jury, accused, lawyers, and prosecutors. The report must be prepared in such a way that it is suitable to be presented in a court of law.

IV. Challenges

The exponential growth and advancements in the field of computing and network technologies have made existing digital forensics tools and techniques ineffective. The swift development in digital forensics resulted in a lack of standardization and training. Since every investigation is unique, it is hard to create standard procedure for every forensic analysis. However, to meet the need for standardization, various organizations such as the National Institute of Standards and Technology (NIST) have published guidelines for digital forensics. To respond to the need for training, some companies began to offer certification programs [5]. Law enforcement agencies are compelled to train officers to collect digital evidence and keep up with rapidly evolving technologies. Analyzing evidence stored on a digital computer is one of the greatest forensic challenges facing law enforcement. Laws may restrict the abilities of analysts to undertake investigations since national and international legislations can hinder how much information can be seized. Another main challenge in digital forensics is the increasing volume of data that needs to be analyzed. With the emergence of big data, the way digital forensics investigations are carried out must change. Big data is regarded as datasets that are too big and is characterized by the volume, velocity, variety and variability of data [6]. The principal future challenges include cloud computing, metadata, anti-forensics (preventing forensics analysis), encryption, social networking, Internet of things, and wireless networks. Anti-forensic (or counter-forensic) techniques are becoming a formidable obstacle for the digital forensic community. They are designed to hinder or circumvent forensic analysis. They are any attempts to compromise the availability or usefulness of evidence to the forensics process. People use anti-forensics to frustrate forensic tools, investigations, and investigators [7].

V. Conclusion

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. A typical way of showing these related disciplines is shown in Figure 1 [8]. It is the process of uncovering and interpreting electronic data so as to preserve any evidence in its most original form.

Although the field of digital forensics is still young, increased awareness of DF has drawn many to this developing field. It is going through a transition from a relatively obscure tradecraft to a scientific field that needs to be continuously held to higher standards. Several next generation forensic analysis systems are under development. Colleges and universities around the world have started to offer courses in DF in the information security curriculum at undergraduate and graduate levels. The Digital Forensic Research Workshop (DFRWS) has contributed more than any other organization to research and development in digital forensics. It has organized annual open workshops devoted to digital forensics since 2001 [9].

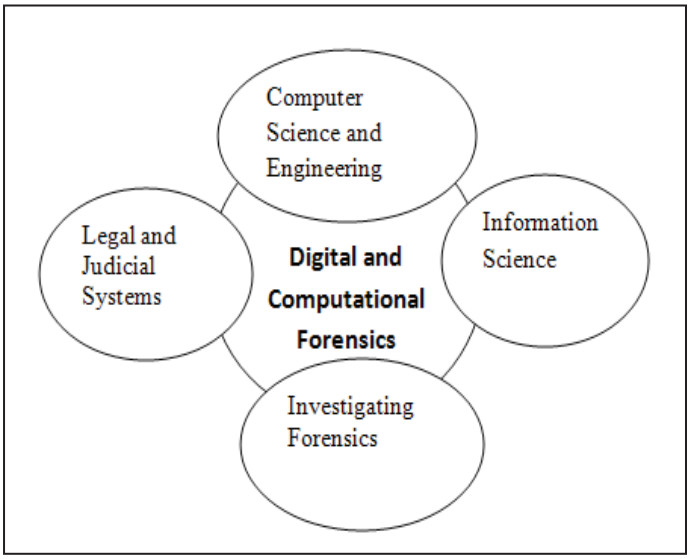

Fig. 1: Multiple Domains of Digital Forensics [8]

References

[1] I. Resendez, P. Martinez and J. Abraham, "An Introduction to Digital Forensics," June 2014, [Online] Available: https://www.researchgate.net/publication/228864187_An_Introduction_to_Digital_Forensics.

[2] N. Kumari, A. K. Mohapatra,"An insight into digital forensics branches and tools," Proceedings of the International Conference on Computational Techniques in Information and Communication Technologies, 2016.

[3] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," International Journal of Digital Evidence, Vol. 1, No. 3, Fall 2002.

[4] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. San Diego, CA: Academic Press, 3rd edition, 2011.

[5] "Digital forensics," Wikipedia, the free encyclopedia.

[6] O. M. Adedayo,"Big data and digital forensics: Rethinking digital forensics," Proceedings of IEEE International Conference on Cybercrime and Computer Forensic, 2016.

[7] N. M. Karie, H. S. Venter,"Taxonomy of challenges for digital forensics," Journal of Forensic Sciences, Vol. 60, No. 4, pp. 885-893, 2015.

[8] M. Losavio, K. C. Seigfried-Spellar, J. J. Sloan III,"Why digital forensics is not a profession and how it can become one," Criminal Justice Studies, Vol. 29, No. 2, pp. 143-162, 2016.

[9] S. L. Garfinkel,"Digital forensics research: The next 10 years," Digital Investigation, Vol. 7, pp. S64 - S73, 2010.