Digital Forensics: A Step towards the Digital Investigation & its Legal Implications in India

Dr. O. Gambhir Singh

Professor, Forensic Medicine Department, SRM Medical College & Research Centre, Potheri, Tamil Nadu-603203, India
E-mail: *drgambhirsingh[at]gmail.com*
Mobile No.9629047798

Abstract: ***Digital forensics is the branch of forensic science that is concerned with the identification, examination, analysis, and preservation of digital evidence by using scientific methods in cases of cybercrime, a crime that involves a computer and a network. It deals with the science of finding evidence from digital media like mobile phones, computers, laptops, servers, or networks. So, this branch helps in the prevention and solving of legal cases involving cybercrimes. Though it is a newer branch of forensic science, it is gaining momentum as the whole world is heading towards a digital era. The main aim of this review article is to examine and discuss an overview of this branch of forensic science in the Indian scenario.***

Keywords: Digital forensics, Forensic Investigation, Crime reconstruction, Information & Technology Act, Digital media

1. Introduction

In this era of computer science and the internet, we are moving towards a digital world, almost all important documents and sensitive information are digitalized and preserved in the form of electronic data.[1]Electronic gadgets such as computers, laptops, mobile phones, etc. become inseparable in our life and we store almost all our information & documents in them. Internet and computers are extensively used by many government departments, agencies, and business companies in different forms of transactions. Modern criminal activities involve thus digitally stored information. This gives rise to the new crime that is known as Cybercrime.[2]Digital forensics or Digital Forensic Science is a branch of forensic science that helps in the investigation of such crimes involving electronic evidence. It is a newer branch of forensic sciences. It focuses on identifying, acquiring, processing, analyzing, and reporting on data during the course of the investigation. The main aim of digital forensics is to extract data from electronic evidence and process it into actionable intelligence findings admissible in and outside the court of law.

For convenience, we may divide digital forensics into the following five branches:-[2,3,4]

1) Computer Digital Forensics: It is the branch of digital forensic science that deals with evidence found in computers and digital storage media. The main aim is to examine digital data for the purpose of identification, recovering, analyzing, and presenting facts.
2) Mobile Device Digital Forensics: It is the branch of digital forensics that focus on the recovery of digital evidence from a mobile phone or any other devices that have internal memory such as Tablets, PDA, and GPS.
3) Network Digital Forensics: It is the branch of digital forensics that focuses on monitoring and analyzing computer networks for information gathering, intrusion detection, etc. It has two main uses (a) Monitoring the network for any anomalous traffic and identifying intrusion and (b) Analysis of captured network traffic as a part of a criminal investigation.
4) Forensic Data Analysis: It is the branch of digital forensics that examines structured data to discover and analyze patterns of fraudulent activities.
5) Database Forensics: It is the branch of digital forensics related to databases.

History of Digital Forensics: [1,3,4,5,6]
Before the 1970s there was no separate law for cybercrime. Historically the first cybercrime was recognized legally in the 1978 Florida Computer Crimes Act which included legislation against the unauthorized modification or deletion of data. Later on, the Florida state government passed laws to deal with misuse of copyright, privacy, child pornography, etc. The growth of cybercrime during the 1980s and 1990s gave rise to the establishment of various specialized groups at the national level for better investigation.

The FBI launched a Computer Analysis and Response Team in 1984 and one year later the British Metropolitan Police fraud squat launched a Computer Crime Department. A great turning point in the history of digital forensics was seen during the 1990s as there was high demand for digital forensic experts.

Since 2000 many agencies published guidelines as there was a need for a common standardization. In the year 2001, the British National Hi-Tech Crime Unit was set up to provide a national infrastructure for computer crime. One year later in 2002, the Scientific Working Group on Digital Evidence produced best practices for Computer Forensics.

The treaty of the Convention on Cybercrime came into existence in 2004 with the aim of reconciling national computer crime laws, investigation techniques, and worldwide cooperation. In 2005, an ISO standard for digital forensics was released.

Advantages of Digital Forensics:[7,8,9]

1) To ensure the integrity of the computer system

2) To help government organizations or companies to recapture important information if their network or computer system is hacked.
3) To track down cybercrimes from anywhere in the world.
4) To collect and produce evidence in a court of law.

Disadvantages of Digital Forensics:[7,8,9]

1) Legal practitioners must have good knowledge of computers.
2) All investigating officers also should have good knowledge of computers.
3) Producing electronic records and storing them is very costly.
4) Digital evidence is accepted in a court of law only when it is proved that there is no tampering.

Legal Aspects in India:[1,10]

Recently there is a development in the field of digitalization and cyber technology in India. The government of India has launched national policies like National E-Governance Plan (NeGP), Digital India, etc. It is extensively used in various fields of science and technology, national health policies, transport & communications, banking & other commercial transactions, and education sectors so on and so forth. Unfortunately, these newer technologies also bring forth newer crimes with them. Any criminal activity that involves a computer, networked device, or a network may be defined as a Cybercrime. E-mail & internet fraud, card payment data fraud, personal information stolen fraud, etc. are some examples of cybercrime. To prevent cybercrime, the government of India passed Information Technology Act, 2000 (ITA-2000) which is popularly known as IT Act on 17 October 2000. With this India became the 12th country to enable cyber law. This act is the primary law in India dealing with cybercrime & electronic commerce. Subordinate legislation to the ITA-2000 includes the Intermediary Guidelines Rules 2011 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Cybercrime law enforcement may also occur on the basis of the Copyright Act of 1957. Depending on the situation, other laws such as the Indian Penal Code, 1860, the Code of Criminal Procedure, 1973, the Indian Telegraph Act, 1885, the Companies Act, 1956, the Copyright Act, 1957, the Patents Act, 1970, and the Consumer Protection Act, 2019, etc. may also apply. CERT-In is the nodal agency for regulating cyber security as per provisions of Section 70B of the Information Technology Act, 2000 (IT Act).[10]

Some frequently encountered cybercrimes and the corresponding penalties are listed below:-

1) Tampering with computer source documents - Imprisonment up to three years, or/and with a fine up to Rs.200,000/- (u/s 65, ITA-2000).
2) Hacking with a computer system - Imprisonment for up to three years, or/and with a fine up to Rs.500,000/-(u/s 66, ITA-2000).
3) Receiving a stolen computer or communication device – Imprisonment for up to three years, or/and with a fine up to Rs.100,000/- (u/s 66B, ITA-2000).
4) Using password of another person - Imprisonment up to three years, or/and with fine up to Rs.100,000/- (u/s 66C, ITA-2000).
5) Publishing private images of others - Imprisonment up to three years, or/and with fine up to Rs.200,000/- (u/s 66E, ITA-2000).
6) Failure to maintain records - Imprisonment up to three years, or/and with fine. (u/s 67C, ITA-2000).
7) Securing access or attempting to secure access to a protected system - Imprisonment up to ten years, or/and with fine. (u/s 70 C, ITA-2000).
8) Breach of confidentiality and privacy - Imprisonment up to 2 years, or/and with fine up to Rs.100,000/- (u/s 72, ITA-2000).
9) Disclosure of information in breach of lawful contract - Imprisonment up to 3 years, or/and with fine up to Rs.500,000/- (u/s 72 A, ITA-2000).
10) Publishing electronic signature certificate false in certain particulars - Imprisonment up to 2 years, or/and with fine up to Rs. 100,000/- (u/s 73, ITA-2000).

2. Conclusion

With the emergence of science and technology, digital forensics has played a very important role in solving cybercrimes. The future of digital forensics is limitless. With the expansion of technology, the field will also continue to expand along it its benefits and barriers. Only use tools and methods that have been tested and evaluated to validate their accuracy and reliability. The evidence so collected by the specialist has to be handled and preserved in an appropriate manner so that it can be produced before the court in its exact manner.

References

[1] Shuvangi. Future Of Digital Forensics In India: An Analysis. Legal Service India E-journal [Internet] [Cited 2022 Jan 21] Available from: https://www.legalserviceindia.com/legal/article-4896-future-of-digital-forensics-in-india-an-analysis.html.

[2] William L. What is Digital Forensics? History, Process, Types, Challenges. [Internet] Updated 2022 Jul'9[Cited 2022 Jul' 19]. Available from: https://www.guru99.com/digital-forensics.html.

[3] Horsman G. The different types of reports produced in digital forensic investigations. Sci Justice. 2021 Sep;61(5):627-634.

[4] Sunde N. What does a digital forensics opinion look like? A comparative study of digital forensics and forensic science reporting practices. Sci Justice. 2021 Sep;61(5):586-596.

[5] Bulbul HI, Yavuzcan HG, Ozel M. Digital forensics: an analytical crime scene procedure model (ACSPM). Forensic Sci Int. 2013 Dec 10;233(1-3):244-56.

[6] Luzton DD, Lexcen FJ, McIntyre KA. Forensic Competency Assessment with Digital Technologies. Curr Psychiatry Rep. 2019 Jun 20;21(7):60.

[7] Horsman G, Mammen AB. A glance at digital forensic academic research demographics. Sci Justice. 2020 Sep;60(5):399-402.

[8] Page H, Horsman G, Sarna A, Foster J. A review of quality procedures in the UK forensic sciences: What

can the field of digital forensics learn? Sci Justice. 2019 Jan;59(1):83-92.

[9] Reedy P. Interpol review of digital evidence 2016 – 2019. Forensic SciIntSynerg. 2020 Mar 19;2:489-520.

[10] Bhardwaj N. Why Are Industry Players Unhappy with India’s New Cybersecurity Directives? [Internet] Updated 2022 Jul’1[Cited 2022 Jul’23]. Available from: https://www.india-briefing.com/news/indias-new-cybersecurity-directives-what-are-they-and-why-are-industry-players-unhappy-25006.html/.

[11] Wikipedia. Information Technology Act, 2000.[Internet] [Cited 2022 Jul’26]. Available from: https://en.wikipedia.org/wiki/Information_Technology_Act,_2000#Amendments.