Chapter 12
Advancing Digital Forensics Education With Generative AI for Sustainable Development Goals

Naziya Hussain
https://orcid.org/0000-0002-4852-6314
School of Computers, IPS Academy, Indore, India

V. Dankan Gowda
https://orcid.org/0000-0003-0724-0333
Department of Electronics and Communication Engineering, BMS Institute of Technology and Management, Bangalore, India

K. R. Swetha
Department of Computer Science and Engineering, BGS Institute of Technology, Adichunchanagiri University, Mandya, India

Aparna Atul Junnarkar
Department of Information Technology, Vishwakarma Institute of Information Technology (VIIT), Pune, India

Sheetalrani R. Kawale
https://orcid.org/0000-0001-7887-0346
Department of Computer Science, Karnataka State Akkamahadevi Women University, Vijayapura, India

ABSTRACT

The term "forensics" refers to a broad range of activities that involve gathering, analyzing, and presenting evidence that is admissible in a court of law and are intended to investigate potential entities. In particular, network and computer forensics examine a wide range of data in order to find evidence that can be used in court. During the forensic process, the examination and auditing of computer and network data is essential for gathering data, identifying breaches, and presenting legal evidence. In computer and network forensics, evidence relating to cybercrime is identified, acquired, extracted, examined, analyzed, interpreted, documented, and presented using a methodical, scientific approach. The field of network and computer forensics is constantly expanding, and as crimes move beyond computers and into networks, clouds, and social networks, it is essential to stay current with the newest tools and techniques. The goal of this chapter is to study and explore the methods and tools used in network and computer forensics.

DOI: 10.4018/979-8-3693-2440-0.ch012

INTRODUCTION

Penetration of Information and Communication Technology (ICT) in the modern society, has led to expansion of the crime domain to Network and Computer related crimes across cyberspace. The spreading domain of cybercrime is a severe concern for forensic analysis. Thus, presenting admissible, well defined and documented evidence in a court of law is the goal of cyber forensics (G. Shrivastava and B. B. Gupta. 2014). Computer forensics is also known as cyber forensics that consists of acquiring, retrieving, preserving and preparing data, in forensic labs for presentation, that is electronically processed and stored on digital media. Cybercrime (computer-related crime, e-crime or digital technology, crime) is an unlawful act committed with the help of a network node (computer, laptop, and mobile) to target other resources. Cybercrime leads to intrusion, disruption or downgrading of the target node. In the last decade, the modern cybercrime techniques have become more sophisticated and commercialized. Criminals have been using high speed, readily available and anonymous technologies to run syndicate as professionals (Easwaran et al., 2022; Mijwil et al., 2022).

In addition to revolutionary advancements and increased connectivity, the advent of the digital age also marked the beginning of a new era in criminal activities. Cybercrimes including identity fraud; state sponsored attacks which arise from the migration of personal and business activities online have become quite a big problem. These emerging hardships demanded a new discipline that could combine interconnectedness of vital investigation strategies with continuously developing digital danger zone. The discipline of digital forensic came into existence as an indispensable tool in a war against cybercrime.

By its way, digital forensics was a science specially designed whose main fields were restricted to seeking lost files on floppy disks and tracing their indications. Though the degree of the cyber crimes has reached the complexity, as the world is exposed to the extensive digital interdependence. An mechnical race of arms between cyber criminals and the law enforcement agencies is the result of this growth. Unlike in the past, when forensics experts kept an eye on hard drives of computers, digital forensics today covers a wide range of subjects: for example, cloud databases, huge corporate networks, and telephone stories.

Also, the spread of the IoT can be regarded as an extra dimension of complexity. Refrigerators, webcams and thermostats which are commonly used at home formerly became part of the cyber court having a capacity to say something important.

Mental and physical elements together form the basic principle of law against the criminal offense. Mens rea and actusreus are the elements of any crime as shown in Figure.1. The act that leads to crime is the actusreus and the mental state, in which the person knowingly does a crime, is referred as Mens rea. Actusreus alone is not a crime. Problem with cybercrime is that it's hard to prove both elements (Choubisa et al., 2022; Patel et al., 2022). In cybercrime, the person's act in cyberspace, which laws look to prevent, are actusreus of cybercrime. Suppose a person sends SMS text message and recipient respond with positive response, it's not crime. But if recipient feels offended and is harassed, it would be a crime (M. H. Mate and S. R. Kapse. 2015). In the current scenario, actusreus is 'sending the message text' and 'intension behind stalking' is mens rea.

Types of Crimes

Steven Furnell classifies cybercrime in two categories namely cyber-enabled and cyber-dependent crimes. Cyber-enabled is a traditional crime whose scalability has exponential growth, with or without the use of any Information and Communication Technology (ICT), such as frauds, thefts, and defamation. Whereas,