ABSTRACT

The digital age has undoubtedly revolutionized the life and work of people. However, this sheen of digital technology remains challenged by the spate of cybercrimes that imperil the privacy and data of the end-users. The alarming rise in cybercrimes has become a major concern for cyber specialists. In this grim context, digital forensics has emerged as a boon for cyber specialists because it has proven to be an effective means for investigating cyber-attacks. This chapter reviews the existing tools and approaches in the field of digital forensics in cybersecurity. This chapter also discusses the current challenges and problems that are faced by a forensic investigator. In addition, it enlists the different categories of digital forensics. The study concludes by underlining the importance and the need for extensive research in digital forensic tools.

DOI: 10.4018/978-1-7998-1558-7.ch003
INTRODUCTION

The use of computers in business, home, office and many other places is very popular and necessary nowadays. The world of the digital era is expanding rapidly as more and more users become a part of the cyber world and benefit from it. However, not all the users of internet adhere to the standard and valid use of computers. This era has witnessed a steep increase in what is termed as negative computing which is the use of computers and the internet for illegal and unauthorized work. The negative use of computers creates many subdomains that must be prevented. Digital forensics plays an important role in detecting and examining these subdomains and thus becomes a deterrent in containing cyber attacks. Digital forensics techniques and tools are being used by cyber specialists to collect and relate digital evidence to find the truth behind any cybercrime.

A survey by India Times in early 2019 stated that “58% of data breach victims are the persons or organizations who have a small type of business at very low or medium-level” (C.R. Srinivasan, 2019). Moreover, with the voluminous increase in the use of mobile devices, tabs, laptops, etc., the implementation of cyber-attacks is very easy for the attackers. Hence, the examination and analysis of cyber-attacks and security exploits have become imperative. In this paper, the first section is about different perspectives of digital forensics and their examination tools. In the second section, the authors discuss different challenges & issues and their importance. Then the paper talks about future research topics in digital forensic. The final section profiles the recommendations and the conclusion.

DIGITAL FORENSICS IN DIFFERENT PERSPECTIVE

Digital forensic has different domains and types for a different kind of analysis and identification procedure. Some are described below:-

Data Forensics

It deals with digital data. Data forensic is about the process of how to use the data or Metadata for investigation and find real evidence or truth. Data carving is a technique that is used in data forensic. Data carving is a process of retrieving data or files from the raw fragments. (Nadeem Alherbawi, 2013) Gave a detailed description of data carving and proposed a method of data carving to handle the fragmentation issue in the examination of data. Some standard tools for data forensics are shown in figure 1.
Related Content

Financial Statement Fraud Detection and Investigation in Digital Environment

Current Challenges of Digital Forensics in Cyber Security

Forensic Case Studies
[www.igi-global.com/chapter/forensic-case-studies/247297?camid=4v1a](www.igi-global.com/chapter/forensic-case-studies/247297?camid=4v1a)
Communiqué Issues in MANET and VANET Protocols With Network Security Disquiet
Mamata Rath, Bibudhendu Pati and Jhum Swain (2020). Forensic Investigations and Risk Management in Mobile and Wireless Communications (pp. 195-220).
www.igi-global.com/chapter/communiqu-issues-in-manet-and-vanet-protocols-with-network-security-disquiet/234078?camid=4v1a