

Chapter 1


A Guide to Digital Forensic “Theoretical to Software– Based Investigations”

Preeti Sharma

 <https://orcid.org/0000-0001-7530-3821>

University of Petroleum and Energy Studies, India

Manoj Kumar

 <https://orcid.org/0000-0001-5113-0639>

University of Wollongong, Dubai, UAE

Hitesh Kumar Sharma

University of Petroleum and Energy Studies, India

ABSTRACT

A branch of forensic science called “digital forensics” deals with the utilization of digital data received, maintained, and conveyed by electronic devices as evidence in inquiries and legal proceedings. It is a growing field in computing that frequently necessitates the intelligent analysis of large amounts of complex data. Rapid advancements in computer science and information technology enable the development of novel techniques and software for digital investigations. Initially, much of the analysis software was unique and proprietary, but over time, specialised analysis software for both the private and governmental sectors became available. The aim of this chapter is to deliver a comprehensive overview of digital forensics phases, applications, merits, and demerits and widely used software of the domain. The chapter also discusses legitimate and legal considerations, followed by the scope and role of artificial intelligence for solving complex problems of digital forensics.

DOI: 10.4018/978-1-6684-8218-6.ch001

1. INTRODUCTION

Across the globe, people and associations are racing to implement new advances to improve and grow in an increasingly interconnected world. The convergence of the technological progressions in informative technology, for example, cloud computing, social networking, personal devices, example, smartphones, and so forth, and the pervasive utilization of it worldwide have resulted in numerous benefits for humanity, yet it additionally gives roads to misuse and has presented new challenges for policing cybercrimes. Cyber-crimes or digital crimes have increased in frequency with the advancement and more complex techniques being deployed by individuals and groups with intricate and advanced knowledge of the working of the internet, networks, and security architectures, and who use their specialist skills for negative and crimes, normally called the Dark Side of Internet. It presents significant implications and difficulties for national and economic security (Naick and Bachalla,2016).

Many associations are at huge risk. This statement has been proved by the number of complaints received and processed for instance by the Internet Crime Complaint Centre (IC3) of the Federal Bureau of Investigation (FBI). In 2017, the total quantities of complaints received are 301,580 with reported losses of \$1,418.7 million. In this report, India is at second number in the list of top 20 victim nations with 2,819 complaints. This is significant additionally considering many personal and organizational data breaches and monetary losses go unreported in our nation and most complaints are by financial institutions like credit card organizations and banks. The list of top 20 countries by victim is depicted in figure 1 (sourced from <https://www.bankinfosecurity.com/fbi-sees-internet-enabled-crime-losses-hit-13-billion-a-10033>).”

The number of incidents of cybercrime in India is rising pointedly. An IIT Kanpur study shows that the number grew from 71,780 in 2013 to 1.49 lac in 2014 to 3 lac in addition in 2015, in this way recording a yearly increment of more than 100% from 2014 to 2015. With the advent of various digital gadgets, the internet, and social media, the environment in which digital crimes are committed has fundamentally changed. It is currently insufficient to simply examine the victim’s PC’s hard drive, as additional evidence will be required for the successful prosecution of the perpetrator and determination of the root cause of the crime (Palmer,2001). The latter is fundamental for knowing about the new methods utilized by criminals and accordingly modified the investigation as additionally the investigation of future crimes. The development of the highly technical and sophisticated nature of digital crimes has made another part of science known as Digital Forensics. Because there were few specialized digital forensic tools available in the 1980s, investigators frequently performed live examinations on media, examining computers from within

28 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/a-guide-to-digital-forensic-theoretical-to-software-based-investigations/330258

Related Content

Organizational Resilience Approaches to Cyber Security

David Gould (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1189-1199).

www.irma-international.org/chapter/organizational-resilience-approaches-to-cyber-security/228777

Hybrid Privacy Preservation Technique Using Neural Networks

R. VidyaBanuand N. Nagaveni (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 542-561).

www.irma-international.org/chapter/hybrid-privacy-preservation-technique-using-neural-networks/228744

Technological Trends and Recent Statistics of Dark Web

Kamna Solankiand Sandeep Dalal (2023). *Perspectives on Ethical Hacking and Penetration Testing* (pp. 338-359).

www.irma-international.org/chapter/technological-trends-and-recent-statistics-of-dark-web/330271

Genetic Privacy: A European Design or Default?

Elsa Supiotand Margo Bernelin (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 713-730).

www.irma-international.org/chapter/genetic-privacy/228752

Introduction to Ransomware

Qasem Abu Al-Haijaand Noor A. Jebriil (2023). *Perspectives on Ethical Hacking and Penetration Testing* (pp. 139-170).

www.irma-international.org/chapter/introduction-to-ransomware/330263