

Chapter 1

Forensic Methodologies in the Digital Age

ABSTRACT

The advent of sophisticated Information and Communication Technologies and exponential growth in the usage of internet has enabled the cybercriminals to exploit the vulnerabilities of digital systems and networks, to perform crimes like hacking, phishing, identity theft, ransom ware, cyber espionage, cyber terrorism and cyber warfare. These Cybercrimes can cause significant financial losses, reputational damage, operational disruption, legal liability and national security risks. Today almost all criminal activity has a digital forensics footprint, and digital forensics experts can provide critical assistance to case investigations by identifying, acquiring, and analyzing electronic evidence. Digital evidence ranges from emails, images of child sexual exploitation, messages, to the location of a mobile phone. Digital forensics plays an important role in identifying, mitigating, and eradicating cyber threats and is also useful in the aftermath of an attack, to provide information required by auditors, legal teams, or law enforcement.

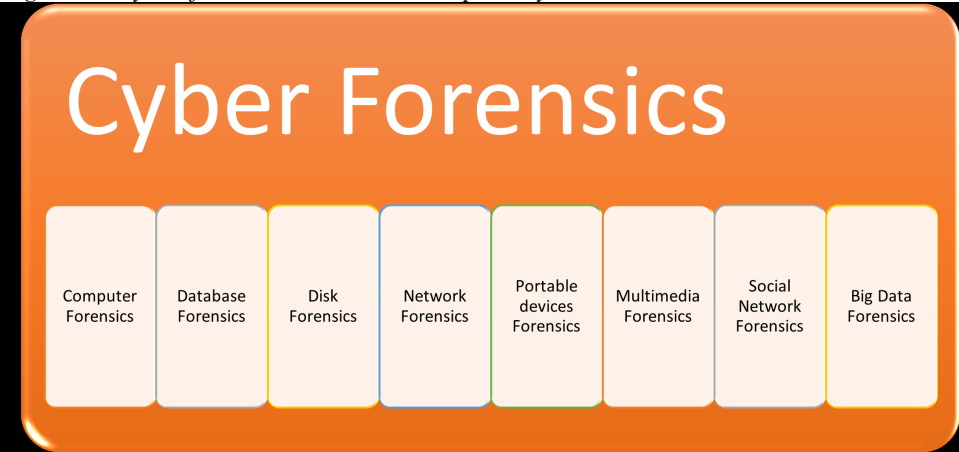
1. INTRODUCTION

The advent of sophisticated Information and Communication Technologies and exponential growth in the usage of internet has enabled the cybercriminals to exploit the vulnerabilities of digital systems and networks, to perform crimes like hacking, phishing, identity theft, ransom ware, cyber espionage, cyber terrorism and cyber warfare. These Cybercrimes can cause significant financial losses, reputational damage, operational disruption, legal liability and national security risks. Today almost all criminal activity has a digital forensics footprint, and digital forensics experts can provide critical assistance to case investigations by identifying, acquiring, and analyzing electronic evidence. Digital evidence ranges from emails, images of child

DOI: 10.4018/979-8-3693-2960-3.ch001

sexual exploitation, messages, to the location of a mobile phone. Digital forensics plays an important role in identifying, mitigating, and eradicating cyber threats and is also useful in the aftermath of an attack, to provide information required by auditors, legal teams, or law enforcement. For analysis purposes, various computerized systems can be used to acquire digital evidence like computers, portable or mobile devices, remote storage devices, wearable devices, internet of things (IoT) devices. Digital forensics includes many other subdomains as mentioned in Figure 1.

Figure 1. Cyber forensics: An interdisciplinary science



This chapter explores the evolution of cyber forensic over the years and various forensic methodologies employed in the digital age, examining their challenges, and the crucial role they play in modern law enforcement. With a focus on real-world case studies, enriched by current facts and figures, this exploration aims to illuminate the multifaceted landscape of digital forensics.

2. EVOLUTION OF CYBER FORENSICS

Cyber forensics, also known as digital forensics or computer forensics, has evolved significantly since its inception. Initially focused on computer-based crimes, it has expanded to encompass a broad spectrum of digital devices, including smartphones, tablets, and IoT devices (Husain & Khan, 2019). The evolution is driven by the surge in cybercrimes and the increasing complexity of digital systems.

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/forensic-methodologies-in-the-digital-age/370606

Related Content

Emergency Response to Mumbai Terror Attacks: An Activity Theory Analysis

Divya Shankar, Manish Agrawal and H. Raghav Rao (2011). *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives* (pp. 46-58).

www.irma-international.org/chapter/emergency-response-mumbai-terror-attacks/50713

Network Forensics: A Practical Introduction

Michael I. Cohen (2010). *Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions* (pp. 279-306).

www.irma-international.org/chapter/network-forensics-practical-introduction/39222

Internet of Things: The Argument for Smart Forensics

Edewede Oriwohand Geraint Williams (2015). *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (pp. 407-423).

www.irma-international.org/chapter/internet-of-things/115772

An Approach for Hand Vein Representation and Indexing

D S. Guru, K B. Nagasundara, S Manjunath and R Dinesh (2011). *International Journal of Digital Crime and Forensics* (pp. 1-15).

www.irma-international.org/article/approach-hand-vein-representation-indexing/55499

Dangerous Objects Detection Using Deep Learning and First Responder Drone

Zeyad AlJundi, Saad Alsubaie, Muhammad H. Faheem, Raha Mosleh Almarashi, Emad-ul-Haq Qazi and Jong Hyuk Kim (2024). *International Journal of Digital Crime and Forensics* (pp. 1-18).

www.irma-international.org/article/dangerous-objects-detection-using-deep-learning-and-first-responder-drone/367034