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.

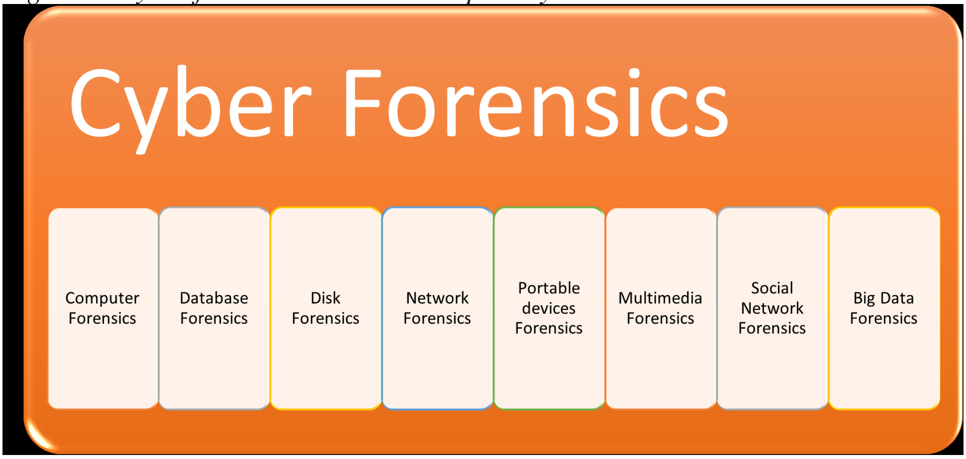
1. INTRODUCTION

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.