Digital Forensics and Indian Cyber Crimes: A Critical Study into the Procedure for Investigation

Narayana, A.

Faculty of Management, Osmania University, Hyderabad, India

Abstract

The impact of Information and Communication Technology (ICT) is very profound on every one of us. However, both Society and Technology are operating in a way so as to harmonize with the pace of each other's growth. As the World is progressing, more technology is emerging with each passing day leading to more development in the society. All the facets of human life including education, health, entertainment, and communication are being impacted by the advent of ICT and is being considered as a boon. With boon goes the bane! There is an incidence of increasing number of cyber-crimes including Corporate Frauds that are executed via the means of ICT in the World today. For this, a new branch of forensic audit called Cyber Forensics Audit has emerged in the contemporary world. In this perspective, this concept paper aims to deal with Cyber Crime in all its faces and facets.

Key Words: Cyber Crime, Digital Forensics, Data Extraction; Ethical Hacking, Digital Incident Response

1. Introduction

Cyber security professionals understand the value of information and respect the fact that it can be easily compromised if not properly handled and protected. A key component of the investigative process involves the assessment of potential evidence in a cyber-crime. In order to effectively investigate potential evidence, procedures must be in place for retrieving, copying, and storing evidence within appropriate databases. The field of computer forensics investigation is growing, especially as law enforcement and legal entities realize just how valuable information technology (IT) professionals are when it comes to investigative procedures. With the emergence of acts of cyber-crime, tracking malicious online activity has become crucial for protecting public at large and private citizens. It is equally important to preserve online operations in public safety, national security, government, and law enforcement. Tracking digital activity allows investigators to connect cyber communications and digitally-stored information to physical evidence of criminal activity. Computer Forensics also allows investigators to