Chapter 1

Cyber Forensics:
Its Importance, Cyber Forensics Techniques, and Tools

Sonali Yadav
Integral University, India

ABSTRACT

Today one of the major difficulties facing all organizations is cybercrime. Cybercrime is any crime related to computers or the internet. Cybercrimes cover a vast range, from sending fake emails to downloading and distributing copyrighted material. Cyber forensics is among one of the important branches of computer science. It deals with cybercrime investigation. In this chapter, the author provides an overview of cyber forensics. The chapter focuses on its importance and some of the techniques and tools used by cyber forensic investigators.

INTRODUCTION

Day-by-day the number of internet users is increasing and so is the Cybercrime. No one realised that internet can be used to harm mankind. Whenever an organization found that there are some loopholes in their security system, it has led to a compromise in protecting their vital data. Then the questions arise: How did this happen and how early can it be prevented from happening? This is where the role of forensics comes into play. The goal of Cyber forensics is to perform crime investigations by using evidence from digital data to find who was responsible for that particular crime said by (prabhu490730, 2015). The cyber forensic investigator collects and examines all...
the bits and pieces of information and evidence left behind the crime scene. Then the forensic investigator is liable to answer the question of who and what.

It is important to keep in mind that the area of forensics is very broad in nature as it is related to IT. It is very broad in nature, and involves many sub-specialties. Here we will focus on Cyber forensics. Cyber Forensics, Computer Forensics or Digital forensics, more or less, mean the same. In this article, we will use the term cyber forensics and computer forensics interchangeably.

**CYBER FORENSICS**

Cyber is a prefix used to describe, a person, a thing or any idea related to computers and the internet. Forensics means using some sort of scientific process for the collection, analysis, and presentation of the evidence which has been collected. Forensics deals primarily with the recovery and examination of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from blood stains to the files on a hard drive as per An Introduction to Computer Forensics-Infosec Resource. Thus, a formal definition of cyber forensics is:

*Cyber Forensics is the science of examining, analysing and reporting electronic evidence collected from computers, networks, wireless communication and storage devices.* or in other words “We define cyber forensics as the discipline that combines elements of law and computer science to collect and analyse data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law by.

Mostly, the data collected during a cyber-forensic investigation is not easily available or seen by a common computer user. This may comprise items like fragments of data that can be found in the space allocated for existing files and deleted files from the computer system, which can only be known by a cyber-forensics expert. Special skill, practice, and tools are essential for obtaining this type of evidence. In a crime scene cyber forensics is mainly concerned with three types of data and they are as follows (as said by (New York Computer Forensics).

1. **Active Data:** Active data is the data available on the computer system. This type of data is easily noticeable and can be obtained without using any restoration process. The data or information readily accessible to users includes word files, spread sheets, images, databases, email-messages, program files, system files or files used by the operating system. This is the easiest type of data.
Cognitive Radio Network-Based Design and Security Challenges in 5G Communication
Arvind Dhaka, Amita Nandal and Rahul Dixit (2020). Forensic Investigations and Risk Management in Mobile and Wireless Communications (pp. 221-241).
www.igi-global.com/chapter/cognitive-radio-network-based-design-and-security-challenges-in-5g-communication/234079?camid=4v1a