DF Lecture 1 Notes

Digital Forensics

Lecture 01 - Introduction

Instructor: Dr. Zunera Jalil
Email: zunera.jalil@au.edu.pk
Date: 11th February 2025

Course Information

- **Course Code**: CY- 334
- **Course Title**: Digital Forensics
- **Theory Instructor**: Dr. Zunera Jalil
- **Lab Instructor**: Ms. Memoona Sadaf
- **Class Time**: Every Monday, 10:40 AM - 12:30 PM
- **Google Classroom**: ge6pddu

Assessment Plan (Tentative)

Assessment Type	Count	Weightage
Quizzes	5	10%
Home Assignments	4	10%
In-Class Assignments	4	10%
Project	1	10%
Mid-semester Exam	1	25%

Assessment Type	Count	Weightage
Final Exam	1	45%

Cybercrime

- **Definition**: Cybercrime is criminal activity that either targets or uses a computer, a computer network, or a networked device.
    - *(Source: Kaspersky)*

Cyber Crimes Include:

- Phishing Attack
- Ransomware Attack
- Identity Fraud (misusing personal information)
- Theft of Financial or Card Payment Data
- Theft and Sale of Corporate Data
- Harassment
- Spreading Hate and Inciting Terrorism
- Distributing Child Pornography
- Publishing Derogatory Materials
- E-Money Laundering and Taxation
- **...and more**

Source for further details:

- Broadband Search - Alarming Cybercrime Statistics

Activity 1 [10 minutes]

ENUMERATION

- **Group A**: Visit the FBI website and find 3 interesting facts.
- **Group B**: Visit the Forensic Focus website and find 3 interesting clues.

Digital Forensics

Definition:
Digital forensics is the **preservation, identification, extraction, documentation**, and **interpretation** of computer media for evidentiary and/or root cause analysis using well-defined methodologies and procedures.

Methodology:

1. Acquire the evidence without altering or damaging the original.
2. Authenticate that the recovered evidence is the same as the original seized.
3. Analyze the data without modifying it.

Market Overview

The global Digital Forensics market size was valued at **US$ 2453.06 million** in 2022 and is expected to expand at a **CAGR of 13.38%** during the forecast period, reaching **US$ 5211.15 million** by 2031.

Digital Forensics (NIST)

The **National Institute of Standards and Technology (NIST)** defines digital forensics as:

> **"The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data."**

Activity 2 [10 minutes]

1. Form a group of three.
2. Discuss and document details about:
    - Interesting cybercrime (could be a personal experience).
    - How the investigation of the cybercrime was conducted (or how it could have been investigated).
3. Prepare to present your findings to the class.

Reading Task

Digital Forensics Framework

Links to Explore

- SANS Digital Forensics & Incident Response
- Forensic Science International - Digital Investigation
- Springer Digital Forensics
- NIST Digital Forensics Experts
- IEEE Digital Forensics Research