

1/10/23

PA-10

Krishnay Thodear

DFI Theory Assignment 2

4/10/23

Cry
Kry

Date _____

Page _____

DFI CCA Assignment

Q.1. What is forensic science? What are the basic principles of forensic science?

→ Forensic science is a multidisciplinary field that involves the application of scientific principles and techniques to solve crimes and issues related to the criminal and civil justice systems.

★ Basic Principles:

(1) Chain of custody: maintaining a documented and unbroken chain of custody for all evidence to establish its authenticity and admissibility in court; tracing its handling and storage from time of collection to presentation.

(2) Reconstruction:

Reconstructing events or sequences of action based on the analysis of evidence to understand how a crime occurred; including the actions of the victim and the perpetrator.

(3) Accuracy and Reliability: Ensuring that forensic analysis methods and techniques are accurate, reliable, and based on sound scientific principles and the results are valid and defensible in a court of law.

Q.2. Define Modus of Operandi. What is the purpose of the offender? Why is MO required in digital crimes?

→ MO refers to a criminal's characteristic method or pattern of operation when committing a crime. It includes the specific techniques behaviours or actions an offender consistently employs to carry out criminal activities.

★ Purpose or Motives of such offenders :-

- (1) Financial Gain
- (2) Data Theft
- (3) Cyber Bullying
- (4) Ransom Attacks
- (5) Disruption and Sabotage
- (6) Espionage
- (7) Malware Distribution
- (8) Social engineering: Some people like to watch the world burn

★ Requirement of Modus Operandi

1. Pattern Recognition: In the digital realm, criminals often have characteristic patterns in how they commit crimes.
2. Evidence correlation: Analyzing cybercrime and digital evidence allow for the correlation of similar techniques.

(Q.3)

What is digital evidence? State different types of digital data used with example.

→ Digital evidence refers to any electronic data or information that is stored or transmitted in a digital form, and can be used as evidence in legal proceedings. Digital evidence is critical for establishing facts, identifying perpetrators and supporting legal cases.

(A)

Types

(1)

Documents and Text files like word files PDFs, text files, spreadsheets, presentations and emails.

(2)

Images and Photos: Examples include JPEG, PNG etc.

(3)

Databases: Examples include databases like SQL, SQLite, NoSQL databases etc.

(Q.4)

Justify importance and functions of Modus Operandi.

(a)

→ MO in criminal investigations is of utmost importance due to its role in aiding law enforcement and forensic experts in understanding. It serves several critical functions that are instrumental in law enforcement efforts.

(1) Identification of patterns and trends:

(2)

Linking Multiple crimes:

Understanding the MO helps investigators to link multiple crimes that may have been committed by the same individual or group.

(3)

Enhancing Digital Forensics

In the digital realm, understanding the modus operandi of cybercriminals aids in the development of more effective digital forensic tools and techniques.

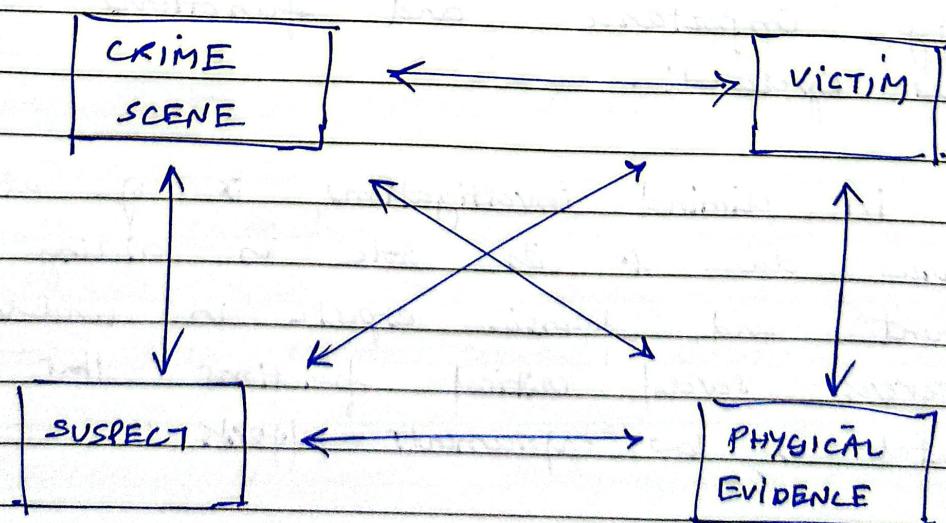
(4)

Forensic profiling and Behavioural Analysis:

Modus Operandi helps in creating offender profiles and understanding behavioural aspects.

Q.5.

Establish connection between victim, offender and crime scenes with the help of a diagram.
State the principles of digital evidence.



Victims: Victims refer to the individual entity that have suffered harm, damage or injury as a result of a crime, accident or any adverse event.

Crime scene: A crime scene is a specific location, area or place where a crime has occurred. Crime scenes are crucial to forensic analysis and investigation to gather evidence and reconstruct events.

Offenders: Offenders are groups, individuals or entities that have committed crimes. They may face legal consequences and sanctions for their actions, aiming to maintain law and order within a society.



Presuppositions of digital evidence

1.

Relevance:

Ensure that the digital evidence collected is directly related to the case at hand and has a clear connection to the alleged offence or incident being investigated.

2.

Integrity

Preserve the integrity of the digital evidence by employing proper collection, handling and storage procedures to prevent any unauthorized

Amping or corruption.

(2)

(4)

Accuracy +

Documentation:

Thoroughly document all procedures and actions taken during the handling, analysis, and preservation of digital evidence, providing a clear and complete record of the process.