गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Course on Cyber Crime Investigation: SOPS for Collection, Preservation and Transport of Digital Evidence to Forensic Laboratory (09 to 13 June, 2025) -05 days

National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Level of Participants	**Judges/Magistrates, Dy. SP/ACP/AC, and above , Prosecutions Officials, Defence Officers, Govt. Medical Officers and SSO and above from CFSL/FSL**
Duration	**05days**

ABOUT THE COURSE

Cyber-crimes have become not only numerous and diverse but also more damaging and disruptive. Digital evidence, which constitute an essential part of cyber-crime, is any piece of information of probative value stored or transmitted in digital form. It is fragile and delicate in nature and needs to be handled carefully to preserve its integrity. The sources of digital evidence can vary from computers and laptops to mobile phones and online social media. As collection of digital evidences from the scene of crime effectively is a complex undertaking, it is necessary to follow standard principles and best practices while acquiring them from the crime scene. Establishing clear procedures for the search, collection and preservation of digital evidence is critical, so as to maintain the Chain-of-Custody and ensure their admissibility in the court of Law.

This course has been designed with the objective of providing the participants with the basic knowledge of collecting digital evidences from a variety of sources at the scene of crime. It will establish the importance of digital evidences in the present-day crime scenario, thus, enlightening them about the principles and best practices that need to be followed for their collection. This course will also provide much insight on the search, collection, handling and preservation of both volatile and non-volatile data at the crime scene in a forensically sound manner so as to preserve their

integrity. Not only desktops and laptops, but the course will also cover the potential evidences found in mobile phones and online social media and the procedure for acquiring them. There will be a demonstration of various open-source and proprietary tools and techniques that are used for the collection of digital evidence from computers, mobile phones and online social media.

COURSE OBJECTIVES

1. To understand the importance of digital evidences in the present-day crime scenario.
2. To provide the participants with the basic knowledge of the principles and best practices that should be followed while search, collection, preservation and handling of digital evidences at the crime scene.
3. To enrich their knowledge regarding the various sources of volatile and non-volatile evidences and techniques for collecting the same.
4. To enlighten the participants about the procedure for the acquisition of evidences from mobile phones and different social media platforms.
5. To show demonstration of different open-source and proprietary tools that can be used for collecting evidences from various electronic devices found at the crime scene.

COURSE CONTENT

1. **Importance of Digital Evidence.**
    - Different types of cyber-crimes and digital evidences involved.
    - The fragile and delicate nature of digital evidence.
    - Challenges faced by the LEA in collection and preservation of digital evidences from the crime scene.
2. **Principles and Best Practices for the Collection of Digital Evidences**
    - The principle and methodology for the collection and handling of digital evidences.
    - Guidelines that need to be followed at the scene of crime.
    - Preservation of digital evidence without destroying or corruption.
3. **Search, Collection, and Handling of Digital Evidences**
    - Collection of volatile and non-volatile data and preservation for further analysis.
    - Various tools and techniques available for handling and preservation of digital evidences.
4. **Forensic Discovery of Digital Evidences**
    - Different sources of digital evidences in an electronic device.
    - Practical demonstration of various tools available for collection and preservation of volatile and non-volatile data.
5. **Collection of Data from Mobile Phones and Online Social Media**
    - Collection and analysis of evidence from mobile phones.
    - Collection and Preservation of Evidence from Social Media.
    - Practical demonstration of different tools for collecting evidence from mobile phones and social media platforms.