गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Course on Criminal Justice and Digital Forensics for Public Prosecutors

National Forensic Sciences University
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Level of Participants	**Public Prosecutor**
Duration	**05days**

ABOUT THE COURSE

The rate of technological advancement is increasing over time. Society seeks to develop easier ways of living and extend lifespans. Advances in Computers and Information Technology have revolutionized various sectors such as Communications, Business, Education, Healthcare, and the legal domain. These advancements facilitate easy access and transfer of information.However, the flip side of these technological advances is the misuse of technology for committing fraud and crimes such as money laundering, drug sales, betting, gambling, tax evasion, and casino operations. In simple terms, many traditional crimes are now aided or abetted through the use of computers and networks.Investigating these sophisticated crimes and assembling the necessary "Digital evidence," present in binary form for presentation, will become a significant responsibility of investigating officers

The dramatic increase in crime relating to the Internet and computers has caused a growing need for digital forensics. Digital forensics involves the investigation of computer-related crimes with the goal of obtaining evidence to be presented in a court of law. As a result, Criminal Justice Functioning in general and Public Prosecutors in particular are facing issues in prosecution of such cases. Afterwards, there is a dire need to sensitize Public Prosecutors to handle such cases effectively, in order to increase the conviction rate. Therefore, the Special Course on Criminal Justice and Digital Forensics for Public Prosecutors has been scheduled. The primary aim of this course is to provide participants with a comprehensive understanding of various aspects of cybercrime, digital frauds, and their associated forensic techniques.

COURSE OBJECTIVES

The course objective to equip public prosecutors with specialized knowledge and skills relevant to the intersection of criminal justice and digital forensics.Participants will:

- Develop an understanding of the role and responsibilities of Criminal Justice Functionaries in handling Cyber Crime Cases.
- Acquire familiarity with various legislative and administrative guidelines relating to cybercrime.
- Explore digital deception, including Deepfake and Deep Web phenomena, and cryptocurrency.
- Gain in-depth knowledge of tools and techniques for mobile forensics, disk forensics, collection, and preservation of volatile and non-volatile data, etc.
- Witness demonstrations of different high-end digital forensic tools like UFED, FTK, and Ant Analyzer.
- Enhance their ability to appreciate, evaluate, and interpret case laws with reference to the IT Act.

TRAINING CURRICULUM

The Special Course on Criminal Justice and Digital Forensics for Public Prosecutors offers a comprehensive program aimed at providing public prosecutors with the expertise and competencies necessary to effectively manage the complexities of digital crime investigations and prosecutions. The following topics will be extensively covered during this program:

1. Cyber Crime and Computer Frauds Challenges in Digital Forensics
   - Understanding the evolving landscape of cybercrime
   - Identifying challenges in digital forensic investigations of computer frauds

2. Digital Deception: Deepfake and Deep Web
   - Deepfake technology and its implications
   - Navigating the hidden layers of the Deep Web

3. Forensic Discovery of Digital Evidence
   - Techniques and methodologies for forensic discovery
   - Gathering and analyzing digital evidence for legal presentation

4. Mobile Phone Technology and Forensics
   - Understanding mobile phone technology and its relevance in digital forensics
   - Extracting and analyzing digital evidence from mobile devices
   - Hands-on exercises and case studies in mobile phone forensics

5. Collection and Preservation of Volatile and Non-Volatile Data
   - Best practices for collecting and preserving digital evidence
   - Legal considerations in data preservation
   - Practical exercises in data collection and preservation techniques

6. Financial Frauds: Challenges in Presentation of Digital Evidence
   - Addressing challenges in presenting digital evidence related to financial frauds
   - Ensuring the admissibility and reliability of digital evidence in financial crime cases

7. Online Abuse on Children: Measures, Prevention, and Control
   - Understanding online abuse against children
   - Implementing measures for prevention and control

8. CCTV Analysis and Digital Image Forensics
    - Analyzing CCTV footage and digital images for forensic purposes
    - Enhancing and authenticating digital images

9. Victimization in the Digital Era
    - Exploring various forms of victimization in the digital age
    - Strategies for supporting victims and seeking legal recourse

10. Decoding Cryptocurrency
    - Understanding cryptocurrency transactions and their implications for digital forensic investigations
    - Investigating cryptocurrency-related crimes

11. IT Act 2008 &Draft Digital India Act 2023
    - Understanding the legal framework surrounding digital evidence
    - Exploring the proposed Draft Digital India Act 2023 and its implications for digital forensics

12. Preparation, Admissibility of Digital Evidence, and Standard Operating Procedures (SOPs)
    - Guidance on preparing digital evidence for legal presentation
    - Ensuring the admissibility of digital evidence in court proceedings
    - Developing SOPs for handling digital evidence effectively

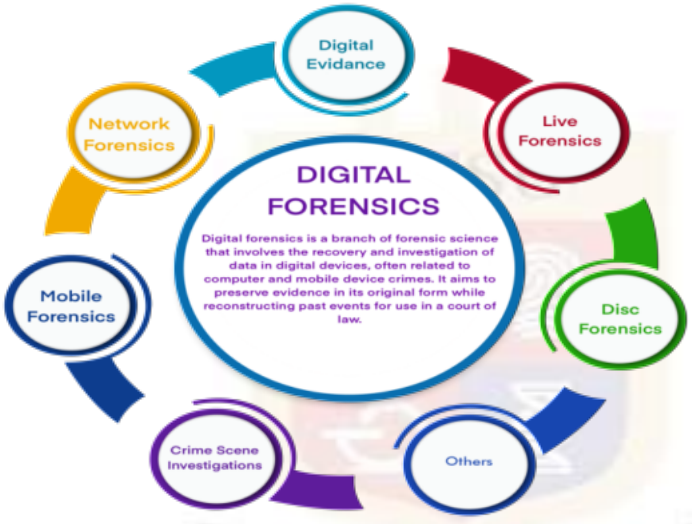

Fig 1. Digital Forensics

COURSE PROGRAMME

Day 1 addresses Financial Frauds and their challenges in presenting digital evidence, and their Forensic Discovery. It also addresses online abuse prevention measures.

Day 2 focuses on foundational topics such as Cyber Crime and Computer Frauds, Digital Deception including Deepfake and Deep Web exploration, an overview of the IT Act 2008 and an introduction to the Draft Digital India Act 2023.

Day 3 covers the new criminal laws in the digital era along with the understanding of victimization in the digital era.

Day 4 covers the critical aspects of Collection and Preservation of Volatile and Non-Volatile Data, CCTV Analysis. Participants also learn about the preparation and admissibility of digital evidence along with standard operating procedures.

Day 5 wraps up the course with deeper understanding of Mobile Phone Technology and Forensics, with practical sessions to reinforce learning.