गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

2nd Special Course on Digital Forensic and Cyber Security for Judiciary officers & Public Prosecutors

National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

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

Special Course on Digital Forensics and Cyber Security for Judiciary Officers & Public Prosecutors

ABOUT THE COURSE

The rate of technological progress continues to accelerate at an exponential pace, shaping and transforming nearly every aspect of human life. Society, in its relentless pursuit of improving quality of life and extending human lifespans, consistently looks for innovative solutions to make living easier and more efficient. The rapid advancements in computers and information technology have had a profound impact on numerous sectors, including communications, business, education, healthcare, and the legal domain. These technological innovations have made accessing and sharing information simpler and faster than ever before, revolutionizing the way society operates and interacts.

However, this technological evolution comes with a darker side. The same tools that have empowered positive change are also being exploited for nefarious purposes. Technology has become a vehicle for committing a wide array of fraudulent and criminal activities, including money laundering, illicit drug sales, illegal betting, gambling, tax evasion, and the operations of unregulated online casinos. In essence, many traditional crimes that once relied on physical presence or manual operations are now carried out with the help of computers, digital networks, and the internet, making the crimes more sophisticated and difficult to trace. As these crimes become increasingly digital in nature, the task of investigating and uncovering the digital evidence hidden in binary code becomes ever more complex. This responsibility to investigate, collect, and present digital evidence will become a critical role for law enforcement officers as they tackle these high-tech criminal activities.

The surge in internet and computer-related crimes has given rise to a growing and urgent need for digital forensics. Digital forensics is the field dedicated to investigating computer crimes, with the goal of uncovering, analyzing, and presenting evidence in a court of law. As cybercrime continues to escalate, the criminal justice system, and particularly public prosecutors, are facing significant challenges in effectively prosecuting such cases. There is an increasing demand for specialized knowledge and skills to navigate these cases, as traditional legal practices are often ill-equipped to handle the complexities of digital evidence. In response, there is an urgent need to equip public prosecutors with the expertise necessary to handle digital forensics cases effectively, ensuring that justice is served and that the conviction rate for these crimes increases. To address this gap, a specialized course on Criminal Justice and Digital Forensics for Public Prosecutors has been designed. The course aims to provide participants with a deep and comprehensive understanding of cybercrime, digital frauds, and the forensic techniques required to investigate and prosecute these high-tech offenses, ultimately ensuring that the criminal justice system remains capable of addressing the challenges posed by modern digital crimes.

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 Distinct Course on Criminal Justice and Digital Forensics for Public Prosecutors is a meticulously designed, comprehensive training program personalised to equip public prosecutors with the essential expertise, skills, and competencies required to navigate and manage the intricate challenges of digital crime investigations and prosecutions. This program provides participants with an in-depth understanding of the rapidly evolving landscape of cybercrime and digital forensics, offering them the tools needed to effectively handle complex, technology-driven criminal cases. Prosecutors will gain valuable insights into how digital evidence is collected, preserved, analyzed, and presented in court, all while staying abreast of emerging trends and threats in the cybercrime space. Through this specialized training, participants will be empowered to confidently prosecute cybercrimes, understand digital fraud mechanisms, and apply cutting-edge forensic techniques in the judicial process. The following critical topics will be thoroughly explored and extensively covered throughout the program:

1. Computer Frauds Issues and Challenges (Case Analysis):

- Gain a deep understanding of the ever-evolving landscape of cybercrime, specifically in the realm of computer frauds, and explore how technological advancements impact criminal activity.
- Identify and analyze the unique challenges that arise during digital forensic investigations of computer frauds, including the complexities of tracing digital footprints, dealing with encrypted data, and ensuring the integrity of evidence throughout the investigation process.

2. Digital Deception: Deepfake and Deep Web:

- Examine the implications of Deepfake technology, understanding how it can be used to deceive, manipulate, and commit fraud, and learn about the challenges in detecting such advanced forms of digital deception.
- Navigate the hidden layers of the Deep Web, understanding its role in facilitating illicit activities, and learn the methodologies to investigate criminal activities that occur in this often anonymous and inaccessible part of the internet.

3. Understanding of Digital Evidence:

- Explore the latest techniques and methodologies used in the forensic discovery of digital evidence, including the tools and processes required for successful data retrieval.
- Understand how to effectively gather, analyze, and interpret digital evidence, ensuring it is legally viable for presentation in court while maintaining the integrity of the investigation.

4. Mobile Phone Technology and Forensics:

- Gain a thorough understanding of mobile phone technology and its critical relevance in digital forensics, including how mobile devices store and transmit data that can be crucial in criminal investigations.
- Learn how to extract and analyze digital evidence from mobile phones, including texts, images, call logs, and location data.
- Participate in hands-on exercises and case studies that allow participants to gain practical experience in mobile phone forensics and build confidence in handling real-world forensic scenarios.

5. Collection and Preservation of digital evidence:

- Learn best practices for the collection and preservation of both volatile (temporary) and non-volatile (permanent) digital evidence, ensuring its reliability and integrity during forensic investigations.
- Understand the legal considerations involved in data preservation, such as maintaining a proper chain of custody, ensuring compliance with legal standards, and preventing evidence tampering.
- Engage in practical exercises that allow participants to apply these best practices in simulated forensic environments.

6. Cloud Computing and Forensics:

- Address the unique challenges involved in collecting evidence from cloud storage systems, including issues of data ownership, jurisdiction, and cross-border legal considerations.
- Gain an in-depth understanding of the cloud forensics process, including the methodologies for accessing cloud data, preserving evidence, and investigating crimes involving cloud-based services.
- Explore emerging trends in cloud forensics and understand how the shift towards cloud-based data storage impacts digital forensics investigations.

7. Measures, Prevention, and Control for Online Child Abuse:

- Develop a thorough understanding of the nature and scope of online abuse against children, including the use of digital platforms for exploitation, trafficking, and other forms of abuse.
- Learn about the strategies and measures used for the prevention and control of online child abuse, including the identification of grooming behaviors, legal measures, and the role of technology in protecting children from online harm.

8. Photography and Videography of crime scene

- The role of video recordings in crime scene documentation
- Advantages and limitations of using videography compared to photography
- Types of video cameras and accessories for crime scene work
- Basic principles of videography: Framing, focus, and stability

9. CCTV Analysis and Digital Image Forensics:

- Learn how to analyze CCTV footage and digital images for forensic purposes, including identifying critical moments, detecting tampering, and improving image quality for clarity in criminal investigations.
- Gain expertise in digital image forensics, including techniques to authenticate, enhance, and validate the integrity of digital images and videos to ensure they are admissible in court as reliable evidence.

10. National and International Cyber Laws:

- Obtain a comprehensive overview of the Information Technology (IT) Act of 2008, exploring its key provisions and its role in governing digital evidence and cybercrime investigations in India.
- Discussions on new cyber laws and data protection bill
- Analysis of landmark cybercrime cases and their legal implications
- Key treaties and conventions related to cybercrimes
- Introduction to new criminal laws in digital era

11. Admissibility of digital evidence and Legal challenges in cybercrime investigation:

- Gain practical guidance on how to prepare digital evidence for legal presentation, ensuring it meets the standards required for admissibility in court.
- Learn the essential steps to verify the authenticity and integrity of digital evidence, from its collection to its presentation in legal proceedings, ensuring it is accepted by judges and juries.
- Learn the Standard Operating Procedures (SOPs) for handling, processing, and presenting digital evidence to boost the credibility and success of digital crime prosecutions.
- Legal challenges like jurisdiction issues and admissibility of digital evidence in cybercrime investigation.