गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Special Course on Cyber Security and Cyber Crime for LEAs, Prosecution and Forensic Scientists

National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

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

ABOUT THE COURSE

In today's increasingly digital world, the rise of cybercrimes and the growing reliance on technology have made cybersecurity a critical concern for law enforcement agencies, the judiciary, and national security. Cybercrimes, ranging from data breaches and financial fraud to more serious offenses such as cyber terrorism and hacking, pose significant challenges to legal systems and law enforcement agencies. In this context, it is essential for senior officials in the police, judiciary, defence, and forensic sectors to be equipped with the knowledge, skills, and tools to address these emerging threats effectively.

The Special Course on Cybersecurity and Cyber Crime Investigation has been specifically designed for senior officials, including Additional Director Generals (ADG), Magistrates, Superintendents of Police (SP), Assistant Commissioners of Police (ACP), Defence Officers, and senior officials from Central Forensic Science Laboratories (CFSLs) and Forensic Science Laboratories (FSLs). The course aims to provide these senior officers with an advanced understanding of the evolving cyber threat landscape, cutting-edge investigative techniques, and the legal frameworks that govern cybersecurity and cybercrimes.

This intensive training program will help judicial officers and law enforcement personnel sharpen their expertise in cybercrime investigation, digital forensics, and cybersecurity, enabling them to lead investigations, manage high-stakes cybercrime cases, and formulate effective policies. With a focus on practical

applications, legal knowledge, and strategic leadership, this course empowers participants to tackle cybercrimes with confidence and proficiency, while ensuring justice and protecting critical infrastructure.

This course is a unique opportunity for senior officials to gain specialized knowledge and expertise in one of the most critical fields of modern law enforcement and judicial practice. It ensures that participants can lead cybercrime investigations**,** address challenges in handling digital evidence**,** and contribute effectively to the development of cybersecurity policies**.** As cybercrimes continue to evolve, the ability of these leaders to understand the technical, legal, and strategic aspects of cybersecurity and cybercrime investigation is paramount to safeguarding the public, national security, and critical infrastructure.

COURSE OBJECTIVES

The course objective to equip senior officers with specialized knowledge and skills relevant to the Cyber Security and Cyber Crime Investigation. Participants will:

- Enhance Knowledge of Cybersecurity Threats: Equip senior officers with a comprehensive understanding of emerging cyber threats, including ransomware, phishing, and cyber terrorism.
- Strengthen Cybercrime Investigation Skills: Provide practical training in digital forensics, including evidence collection, data recovery, and analysis to support cybercrime investigations.
- Improve Legal Understanding: Familiarize judicial officers and law enforcement leaders with cybercrime laws, data

protection regulations, and the legal processes surrounding digital evidence in court.

- Develop Incident Management Expertise: Train participants to design and lead incident response strategies for addressing major cyberattacks and cybersecurity breaches.
- Facilitate Inter-agency Coordination: Promote effective collaboration between law enforcement, defense agencies, judicial bodies, and international organizations in the fight against cybercrime.
- Enhance Leadership in Cybercrime Cases: Equip senior officials with leadership skills to manage and oversee high-profile cybercrime investigations and cybersecurity initiatives at the regional and national levels.
- Build Capacity for Handling Cybercrime Trials: Enable judicial officers to effectively manage cybercrime trials, ensuring the legal integrity of digital evidence and proper legal procedures.

TRAINING CURRICULUM

This specialized training program is designed to provide senior law enforcement, defense officers, forensic experts, and judicial officers with the knowledge and skills required to lead and oversee cybersecurity efforts, investigate cybercrimes, and manage digital evidence. The course will provide a balanced combination of technical expertise, legal knowledge, and strategic leadership in cybersecurity and cybercrime investigations.

1. OVERVIEW OF CYBERSECURITY
    - Importance of cybersecurity in the modern digital landscape.
    - Types of cyber threats: malware, ransomware, phishing, data breaches, etc.
    - Understanding the relationship between cybersecurity and cybercrime.
    - Cybercrime Types: Financial Cybercrimes, Crimes Against Individuals, Cyber Terrorism, Cyber Espionage, Hacking and Malware
    - Understanding the evolving landscape of cybercrime
    - Identifying challenges in digital forensic investigations of computer frauds

2. Digital Deception: Deepfake and Deep Web
    - Introduction of Deepfake technology
    - Social, political, legal, and psychological implications of Deepfake
    - Deepfake creation technology and Deepfake detection
    - Understanding of Dark web and Deep web
    - Dark web and Deep web investigation

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

- Data extraction from smartphones, tablets, and other mobile devices and their analysis.
- Hands-on exercises and case studies in mobile phone forensics
- Tools for mobile forensics: Cellebrite, XRY, etc.

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
    - Computer-based Evidence: Hard drives, laptops, desktops, and servers
    - Techniques for ensuring data integrity during evidence collection.
    - Understanding forensic imaging and using write blockers for evidence preservation
    - EnCase and FTK for disk imaging and evidence collection
    - Techniques for ensuring data integrity during evidence collection.
    - Understanding forensic imaging and using write blockers for evidence preservation

6. Cloud Forenscis: Collecting Evidence from cloud
    - Overview of Cloud Computing
    - Key Challenges in collecting evidence from cloud environments: Jurisdiction, data residency, and multi-tenancy
    - Data Collection Techniques in Cloud Environments
    - Cloud Forensics Process and Emerging Trends in Cloud Forensics
    - Investigating data stored in the cloud and navigating legal challenges.

7. Online Abuse on Children: Measures, Prevention, and Control
    - Definition and scope of online abuse: Cyberbullying, online grooming, sexting, exploitation, and trafficking
    - Understanding the digital landscape and how children are targeted online

- Statistics and trends: Global and regional prevalence of online child abuse
- Impact of online abuse on children: Psychological, emotional, and social consequences
- Common platforms and technologies where children are exposed to online abuse (social media, gaming, chat rooms, etc.)
- Legal Framework and Protection Mechanisms
- Implementing measures for prevention and control

8. CCTV Analysis and Digital Image Forensics
    - Overview of CCTV systems: Types of cameras (analog vs. digital, IP cameras, PTZ cameras)
    - Key components of a CCTV system: Cameras, recording devices, storage systems, monitors
    - Role of CCTV in law enforcement and criminal investigations
    - Introduction to digital image forensics: Definition and significance
    - Digital evidence: Types of digital images, video files, and metadata
    - Tools for video analysis like Amped FIVE
    - Techniques for video enhancement: Noise reduction, sharpness, color correction
    - Techniques for identifying faces, license plates, and other key objects in video

9. Investigating Financial Cybercrime
    - Definition of financial cybercrime: Overview of key types (fraud, money laundering, identity theft, cyber theft)
    - Impact of financial cybercrime on businesses, individuals, and economies
    - The evolution of financial cybercrime in the digital age
    - Understanding criminal motivations: Financial gain, espionage, extortion
    - Types of financial fraud: Securities fraud, insurance fraud, loan fraud, Ponzi schemes, insider trading
    - Common techniques used in financial fraud: Document falsification, fraudulent transactions, forgery, misrepresentation
    - Indicators and red flags of financial fraud

- Implementing fraud prevention systems and controls (e.g., two-factor authentication, encryption)
- Techniques for tracking digital money trails.
- Anti-money laundering (AML) measures in cybercrime investigations

10. Legal Framework for Cybercrime
    - Information Technology Act, 2000 (IT Act) and its amendments.
    - Indian Penal Code (IPC) provisions relevant to cybercrime.
    - Data Protection Laws and Privacy issues in digital spaces.
    - Introduction of new criminal laws in digital era

11. 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