Course on

Cyber Security and Cyber Crime Investigations

(15 to 17 Sep, 2025)

nicfs

National Forensic Science University
लोक नायक जयप्रकाश नारायण राष्ट्रीय अपराध शास्त्र एवं विधि विज्ञान संस्थान
LNJN NATIONAL INSTITUTE OF CRIMINOLOGY AND FORENSIC SCIENCE
(NFSU Delhi Campus)

About the Course

The rise of Information Communication Technology and the vast reservoirs of knowledge disseminated through the interconnected web have enticed the tech-savvy youth to embark on the treacherous path of cyber-crime. Within the realm of Cyber Space, its delicate IT infrastructure teeters on the precipice, vulnerable to a multitude of perils emanating from both tangible and intangible threats. As cyber-crime traverses borders effortlessly and demands delicate handling, it necessitates the employ of specialized tools and technologies to meticulously gather and safeguard digital evidence, shielding it from any trace of harm. To ensure the irrefutable admission of such digital evidence in the hallowed halls of justice, it must be handled with utmost care, guaranteeing its pristine state untarnished by tampering. Thus, those entrusted with the arduous task of investigation and forensic analysis must immerse themselves in the principles and methodologies of the enigmatic realm known as Cyber Forensics.

Cybersecurity has become an increasingly critical aspect of our digital world, as technology continues to advance and shape our lives. With the proliferation of Information Communication Technology (ICT) and the widespread use of the internet, individuals and organizations are now more interconnected than ever before. However, this interconnectedness also brings about new risks and vulnerabilities that can be exploited by cybercriminals.

Cybercrime encompasses a broad range of illegal activities conducted in the digital realm. These activities can include hacking, identity theft, phishing, malware attacks, data breaches, ransomware, and various forms of online fraud. The motivations behind cybercrime can vary, ranging from financial gain to espionage, activism, or even personal amusement.

Course Objectives

1. To cover all the relevant topics from different domains of Cyber Forensics so that the participant can use and implement them at various situations of Crime Investigation.
2. To provide the participants with the basic knowledge of all the different branches of Cyber Forensics including Social Media Forensics, Digital Forensics, and use of Artificial intelligence in cyber forensics etc.
3. To provide them the practical knowledge of the various tools and techniques adopted in Cyber Forensics pertaining to collection, examination and analysis of digital evidence for the investigation of different types of cyber-crimes.
4. To provide the participants with a demonstration of examination and analysis of digital exhibits and evidence using various digital forensic tools.
5. To enable the participants, appreciate, evaluate and interpret the case laws with reference to the IT Act.

Course Content

1. **Cyber Security and Its Applications in Crime Investigation**
    - Introduction to Cyber Security
    - Principles of Cyber security
    - Overview of Cyber Crime & its Challenges
    - Use case on Cyber Crime Investigations
    - IT Act 2000: An Overview
    - Preparation, admissibility of Digital Evidence and Discussion of live case
2. **Application of Network Security in Forensics**
    - Overview of Network Security Forensics
    - Collection & Preservation of Volatile and Non-volatile data- SOPs under CIA triads
    - Introduction to open-source tool for Network Forensics
    - Use case cyber forensics in real-time (Social Network Analysis using open-Source Tools)
    - Ransomware Forensics
3. **When Cyber Security meets Biometric**
    - Introduction to AI, ML, and DL
    - Introduction to biometric
    - Application of biometric cyber security
    - Challenges in biometric applications
4. **Practical Demonstration of Tools and Techniques**
    - Collection of volatile and non-volatile data
    - Storing of digital data for analysis
    - Demonstrate the working of various tools available for collection and preservation of volatile and non-volatile data
    - Tools used for Imaging and Acquisition of Digital Evidence
    - Different open-source and pro-prietary tools for analysis and discovery of various artifacts

*****