गृह मंत्रालय
MINISTRY OF
**HOME AFFAIRS**

# Special Course on Digital Forensics for BSF Personnel (22nd April to 31st May, 2025)

National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

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

# Special Course on Digital Forensics for BSF Personnel (22nd April to 31st May, 2025)

## ABOUT THE COURSE

Digital forensics is an essential field in cybersecurity and criminal investigations, focusing on identifying, preserving, and analyzing digital evidence to uncover cybercrimes, security breaches, and digital fraud. This comprehensive course provides an in-depth exploration of digital forensic methodologies across multiple domains, with a primary focus on Drone Forensics. Participants will gain expertise in computer forensics, social media analysis, network forensics, mobile forensics, IoT forensics, and the specialized field of drone forensics.

For Border Security Force (BSF) personnel, this course offers essential skills to combat modern security threats involving digital devices and unmanned aerial vehicles (UAVs). With the increasing use of drones for surveillance, smuggling, and border intrusions, BSF officers must be well-versed in drone forensics to track, analyze, and neutralize threats. The course provides hands-on training on extracting flight logs, geolocation tracking, and analyzing drone communications, enabling personnel to counter unauthorized drone activities effectively. Furthermore, the inclusion of computer, mobile, and network forensics ensures that BSF personnel can investigate cyber threats, track digital footprints, and safeguard national security interests.

By equipping BSF personnel with state-of-the-art forensic tools and techniques, this course enhances their operational capabilities in digital intelligence gathering and counter-terrorism efforts. Officers will gain proficiency in using industry-standard tools such as Autopsy, FTK Imager, FTK Tool kit, Encase, Cellebrite UFED 4PC, MOBILedit, Wireshark, Burp Suite and Maltego, which are crucial for forensic investigations. The knowledge acquired will empower them to intercept illegal digital activities, identify security vulnerabilities, and strengthen border surveillance mechanisms. With real-world case studies and practical exercises, the officers will be better prepared to handle forensic investigations efficiently, making this course a valuable asset for national defense and law enforcement operations.

## COURSE OBJECTIVES

- **Understand Digital Forensics Fundamentals** – Learn the principles, methodologies, and best practices for identifying, collecting, and analyzing digital evidence.
- **Develop Expertise in Drone Forensics** – Gain skills in extracting flight logs, tracking geolocation, and analyzing drone communications to counter unauthorized UAV activities.
- **Enhance Computer and Mobile Forensics Skills** – Learn to recover and analyze digital evidence from computers, mobile devices, and storage media using industry-standard tools.
- **Strengthen Network and Cybercrime Investigations** – Acquire knowledge in network traffic analysis, intrusion detection, and cyber threat investigations using forensic techniques.
- **Investigate Social Media and IoT Forensics** – Understand methods for tracking digital footprints across social media platforms and IoT devices for intelligence gathering.
- **Utilize Advanced Forensic Tools** – Gain hands-on experience with forensic tools such as Autopsy, FTK Imager, FTK Tool kit, Encase, Cellebrite UFED 4PC, MOBILedit, Wireshark, Burp Suite and Maltego for comprehensive investigations.
- **Ensure Legal and Ethical Compliance in Forensic Investigations** – Understand cyber laws, privacy regulations, and legal procedures for collecting and presenting digital evidence in court.

OBJECTIVES
STRATEGIC
VALUE
STATEMENT
MISSION
INTEGRITY
CONDUCT
STATEMENT
COMPANY
PRINCIPLES
PLAN
IDEOLOGY
INNOVATION
CUSTOMER
OBJECTIVES
MARKET
ACCOUNT
VISION
EMPLOYEES
EXPENSE
PRICE
FINANCE
RULE
GUIDING
VISION
COMMERCE
GOALS
EXCELLENCE

# TRAINING CURRICULUM

**Module 1: Fundamentals of Digital Forensics**

- Introduction to Digital Forensics and Cybercrime Investigations
- Legal and Ethical Considerations in Forensic Investigations
- Evidence Collection, Chain of Custody, and Data Integrity
- Forensic Imaging and Data Acquisition Techniques

**Module 2: Computer Forensics**

- Hard Drive and File System Analysis
- Recovering Deleted Files and Analyzing Metadata
- Detecting Unauthorized Access and Malware Investigations
- Hands-on Training with Autopsy, FTK Imager, and EnCase

**Module 3: Drone Forensics and UAV Investigations**

- Understanding Drone Technology and Communication Protocols (Wi-Fi, GPS, RF Signals)
- Extracting and Analyzing Flight Logs, GPS Metadata, and Telemetry Data
- Investigating Drone-Captured Images, SD Card Data, and Cloud Storage
- Reverse Engineering and Firmware Analysis of Drones
- Identifying Hacked, Tampered, or Weaponized UAVs
- Countering Anti-Forensic Techniques Used by Criminals
- Hands-on Training with Drone Forensic Tools and Case Studies

**Module 4: Mobile Forensics**

- Data Extraction from Smartphones and Tablets
- GPS Tracking and Call Log Analysis
- Bypassing Encryption and Recovering Deleted Messages
- Practical Exercises Using Cellebrite UFED 4PC and MOBILedit

**Module 5: Network Forensics and Cyber Threat Investigation**

- Packet Capture and Traffic Analysis with Wireshark
- Intrusion Detection and Incident Response
- Tracing Cyberattacks and Digital Footprints
- Hands-on Training in Wireshark, Snort and Maltego for Network Investigations

**Module 6: IoT Forensics and Social Media Analysis**

- Investigating Smart Devices and Industrial IoT Systems

- Extracting Logs, Network Traffic, and Cloud-Based Data
- Social Media Intelligence (SOCMINT) and Digital Profiling
- Countering Misinformation and Cyber Threats in Open-Source Investigations