One-Week Training Program on Cyber Forensics Tools for Police Officers

Organized by: Cyber Forensic Research Center, Department of Computer Science & Engineering, MMMUT, Gorakhpur
In Collaboration with Gorakhpur Zone Police, Gorakhpur

Topic: MD-Video and Voice Inspector (Phonexia)

DAY (01) ; MONDAY Date: 04/05/2026

The first day of the one-week training program focused on introducing police officers to advanced multimedia analysis tools, specifically MD-Video and Voice Inspector 4powered by Phonexia technology. The objective was to familiarize participants with the importance of audio-video forensics in modern investigations and to build foundational knowledge for upcoming sessions.

The session was graced by distinguished guests, **Shri Dinesh Godara**, **ASP**, Gorakhpur, and **Dr. Rakesh Kumar, Head & Professor**, Computer Science & Engineering, who shared valuable insights into the role of technology in modern policing. The program was effectively coordinated by **Dr. B. K. Sharma, Associate Professor, and Dr. Vimal Kumar, Assistant Professor**, whose efforts ensured the smooth organization and execution of the training. The technical sessions were conducted by **Mr. Naveen Singh** and **Mr. Mani Bharti,** who provided expert guidance and hands-on training throughout the day.

Training Objectives

- To provide an overview of MD-Video analysis tools
- To introduce Voice Inspector (Phonexia) and its capabilities
- To highlight the role of audio and video evidence in criminal investigations
- To ensure participants understand system setup and interface navigation

The training commenced with an inaugural session in which the guests addressed the participants:

- Shri Dinesh Godara, ASP, Gorakhpur, emphasized the growing importance of digital evidence in crime investigation and the need for officers to adopt advanced forensic tools.
- Dr. Rakesh Kumar highlighted the technical aspects of multimedia forensics and encouraged participants to actively engage in the training.

Introduction to MD-Video

The session was delivered by Mr. Naveen Singh and Mr. Mani Bharti, who demonstrated the practical applications of the software.

Participants were introduced to MD-Video software, including:

Key features and functionalities

- Video enhancement and analysis techniques
- Frame-by-frame examination

Introduction to Voice Inspector (Phonexia)

The session continued with an introduction to Voice Inspector, focusing on:

- Basics of voice biometrics
- Speaker identification and verification
- Audio enhancement and noise reduction
- Practical applications in forensic investigations

Real-world case examples were discussed to illustrate the effectiveness of voice analysis tools.

Hands-On Familiarization

Participants engaged in initial hands-on activities, including:

- Navigating software interfaces
- Uploading and reviewing sample audio-video files
- Understanding basic controls and workflows
- Understanding the significance of multimedia evidence in policing
- Basic operation of MD-Video and Voice Inspector tools
- Awareness of forensic audio-video analysis techniques
- Importance of accuracy and integrity in digital evidence handling

Challenges Faced

- Initial difficulty in understanding technical terminology
- Limited familiarity with advanced forensic software among some participants

These challenges were addressed through guided demonstrations and interactive support.

Conclusion

The first day of training successfully established a strong foundation for the participants. Officers gained essential knowledge of MD-Video and Voice Inspector tools, preparing them for more advanced topics in upcoming sessions. The guidance provided by esteemed guests, trainers, and coordinators contributed significantly to the success of the program.

Recommendations

- Provide additional practice sessions for beginners
- Share reference materials for self-study

दिनांकः 05.05.2026 समाचार –पत्र : हिन्दुस्तान पेज न0 : 06

पुलिस ने सीखी साइबर फॉरेंसिक की बारीकी

एमएमएमयूटी

गोरखपुर, कार्यालय संवाददाता। एमएमएमयूटी के कंप्यूटर साइंस एवं इंजीनियरिंग विभाग ने गोरखपुर जोन पुलिस के बीच करार हुआ है। इस करार के तहत साइंस टेक्नोलॉजीज, नई दिल्ली के सहयोग से पुलिस अधिकारियों को साइबर फॉरेंसिक टूल्स पर एक सप्ताह का प्रशिक्षण दिया जाएगा। सोमवार से इसकी शुरुआत कुलपति प्रो. जेपी सैनी एवं अतिरिक्त पुलिस महानिदेशक मुथा अशोक जैन के मार्गदर्शन में की गई।

कार्यक्रम का शुभारंभ मुख्य अंतिथि एएसपी दिनेश गोदारा ने करते हुए कहा कि वर्तमान डिजिटल युग में बढ़ते साइबर अपराधों से प्रभावी ढंग से निपटने के लिए तकनीकी दक्षता आवश्यक है। कार्यक्रम का उद्देश्य प्रतिभागियों को साइबर फॉरेंसिक टूल्स, जांच तकनीकों, साक्ष्य प्रबंधन तथा विधिक अनुपालन का व्यावहारिक प्रशिक्षण प्रदान करना है, जिससे वे वास्तविक मामलों में इन कौशलों का प्रभावी उपयोग कर सकें। कार्यक्रम में गोरखपुर, देवरिया, महराजगंज एवं कुशीनगर जनपदों से कुल 25 पुलिस अधिकारी प्रतिभाग कर रहे हैं।



एमएमएमयूटी में आयोजित फॉरेंसिक कार्यशाला में जानकारी लेते पुलिस अधिकारी।

विभागाध्यक्ष प्रो. राकेश कुमार ने प्रतिभागियों का स्वागत किया। कार्यक्रम के समन्वयक डॉ. बीके शर्मा एवं डॉ. विमल कुमार हैं। नवीन सिंह एवं मणि भारती ने प्रतिभागियों को डिस्क एवं मोबाइल फॉरेंसिक्स, ऑडियो फॉरेंसिक्स मैलवेयर विश्लेषण, ड्रोन फॉरेंसिक्स, वीडियो फॉरेंसिक्स, स्टेगनोग्राफी, नेटवर्क फॉरेंसिक्स, सोशल मीडिया जांच, एन्क्रिप्टेड डेटा विश्लेषण, क्रिप्टोकरेंसी ट्रेसिंग तथा न्यायालयीन मामलों हेतु रिपोर्ट लेखन जैसे विषयों पर व्यावहारिक ज्ञान प्रदान करेंगे। समापन डॉ. बीके शर्मा ने धन्यवाद ज्ञापन किया।

CENTRAL LIBRARY
MADAN MOHAN MALAVIYA UNIVERSITY OF TECHNOLOGY
GORAKHPUR- 273010 (U.P)

दिनांकः 05.05.2026 समाचार –पत्र : दैनिक जागरण पेज न0 : 04

तकनीकी दक्षता से ही साइबर अपराधों पर लगेगी लगाम : दिनेश गोदारा

जागरण संवाददाता, गोरखपुर : एएसपी दिनेश गोदारा ने कहा है कि वर्तमान डिजिटल युग में बढ़ते साइबर अपराधों से प्रभावी ढंग से निपटने के लिए तकनीकी दक्षता अत्यंत आवश्यक है। मदन मोहन मालवीय प्रौद्योगिकी विश्वविद्यालय में पुलिस अधिकारियों के लिए आयोजित साइबर फॉरेंसिक प्रशिक्षण कार्यक्रम के उद्घाटन अवसर पर संबोधित कर रहे थे। कंप्यूटर साइंस एवं इंजीनियरिंग विभाग द्वारा आयोजित यह एक सप्ताह का प्रशिक्षण कार्यक्रम विश्वविद्यालय और गोरखपुर जोन पुलिस के बीच हुए अनुबंध के अंतर्गत आयोजित किया जा रहा है।

एएसपी ने आगे कहा कि ऐसे प्रशिक्षण कार्यक्रम पुलिस अधिकारियों की जांच क्षमता को सुदृढ़ करने में महत्वपूर्ण भूमिका निभाते हैं और साइबर अपराधियों तक पहुंचने में सहायक साबित होते हैं। उन्होंने प्रतिभागियों से प्रशिक्षण के दौरान सीखी गई तकनीकों का वास्तविक मामलों में प्रभावी उपयोग करने का आह्वान किया। उन्होंने बताया कि कार्यक्रम का उद्देश्य प्रतिभागियों को साइबर फॉरेंसिक टूल्स, जांच तकनीकों, साक्ष्य प्रबंधन और विधिक अनुपालन का व्यावहारिक प्रशिक्षण प्रदान करना है। इस प्रशिक्षण कार्यक्रम में गोरखपुर, देवरिया, महराजगंज और कुशीनगर के 25 पुलिस अधिकारी भाग ले रहे हैं। विभागाध्यक्ष प्रो. राकेश कुमार ने बताया कि डिजिटल अरेस्ट, आनलाइन ठगी, सोशल मीडिया फ्राड, साइबर स्टाकिंग और पहचान चोरी जैसे अपराध तेजी से बढ़ रहे हैं, जिनसे निपटने में साइबर फारेंसिक्स की महत्वपूर्ण भूमिका है। समन्वयक डा. बीके शर्मा और डा. विमल कुमार ने बताया कि प्रशिक्षण के दौरान मोबाइल, कंप्यूटर व नेटवर्क फारेंसिक्स, ड्रोन और वीडियो विश्लेषण, वॉयस एनालिटिक्स, स्टेगनोग्राफी और पासवर्ड विश्लेषण जैसे विषयों पर व्यावहारिक जानकारी दी जाएगी। कार्यक्रम के अंत में प्रतिभागियों को आधुनिक तकनीक का समग्र प्रशिक्षण प्राप्त होगा।



साइबर अपराध के विषय पर प्रशिक्षुओं से बात करते एएसपी दिनेश गोदारा • एमएमएमयूटी


MADAN MOHAN MALAVIYA UNIVERSITY OF TECHNOLOGY
ONE-WEEK TRAINING PROGRAM
CYBER FORENSICS TOOLS
FOR POLICE OFFICERS


MADAN MOHAN MALAVIYA UNIVERSITY OF TECHNOLOGY
Department of Computer Science & Engineering,
Cyber Forensic Research Centre
in collaboration with
CYANT TECHNOLOGIES
GORAKHPUR ZONE POLICE
Gorakhpur
ONE-WEEK TRAINING PROGRAM
on


GPS Map Camera
Gorakhpur,Uttar Pradesh,India
Engineering College, Gorakhpur, Uttar Pradesh 273010, India
Lat 26.730772, Long 83.433888
Monday, 04/05/2026 05:37 PM GMT+05:30
Note : Captured by GPS Map Camera

One-Week Training Program on Cyber Forensics Tools for Police Officers

Organized by: Cyber Forensic Research Center, Department of Computer Science & Engineering, MMMUT, Gorakhpur
In Collaboration with Gorakhpur Zone Police, Gorakhpur

Topic: Disk and File System Forensics

DAY (02) ; TUESDAY Date: 05/05/2026

The second day of the training program focused on Disk and File System Forensics, a critical component of digital investigations. The session aimed to provide police officers with a comprehensive understanding of how data is stored, retrieved, and analyzed from digital storage devices. Building upon the foundational knowledge from Day 1, the training emphasized practical approaches to handling digital evidence.

Training Objectives

- To understand the fundamentals of disk structure and storage media
- To introduce file systems and their types (FAT, NTFS, etc.)
- To demonstrate methods of data acquisition and preservation
- To develop skills in identifying, recovering, and analyzing digital evidence
- To ensure proper handling and integrity of forensic data

Overview of Disk Forensics

The session began with an introduction to disk forensics, covering:

- Types of storage devices (HDDs, SSDs, USB drives, memory cards)
- Physical vs. logical data structures
- Importance of disk imaging in forensic investigations

Participants were briefed on how digital evidence is stored and how improper handling can compromise investigations.

Understanding File Systems

The trainers explained various file systems and their significance in forensic analysis:

- File allocation methods
- Metadata and its role in investigations

Practical examples were used to illustrate how file systems organize and manage data.

Data Acquisition Techniques

A key focus of the session was on acquiring data in a forensically sound manner:

- Disk imaging techniques (live and dead acquisition)
- Use of write blockers
- Ensuring data integrity through hashing

File Recovery and Analysis

This segment covered techniques for retrieving and analyzing data:

- Recovery of deleted files
- Identification of hidden and encrypted data
- Analysis of file metadata and timestamps

Hands-on demonstrations helped participants understand how forensic tools can uncover critical evidence.

Practical Session

Participants engaged in practical exercises involving:

- Creating disk images
- Exploring file system structures
- Recovering deleted files from sample datasets

This interactive session enhanced their understanding of real-world forensic scenarios.

- Clear understanding of disk architecture and file systems
- Knowledge of forensic data acquisition methods
- Skills in recovering and analyzing digital evidence
- Awareness of maintaining data integrity and legal admissibility

Challenges Faced

- Complexity in understanding file system structures for beginners
- Difficulty in interpreting raw data and metadata

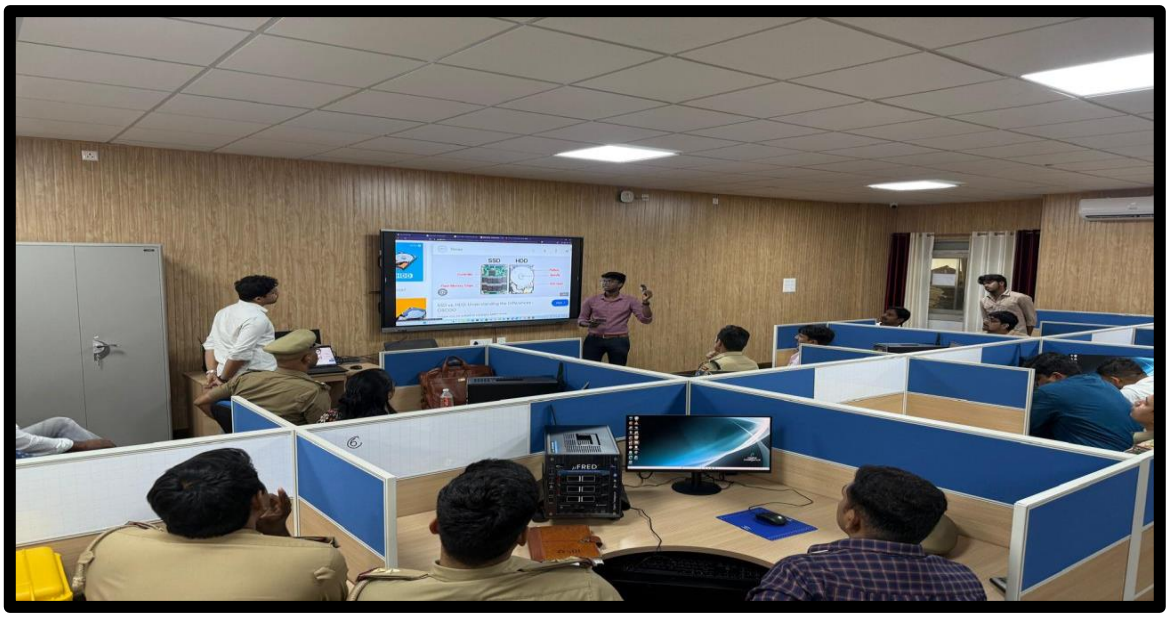
These challenges were addressed through detailed explanations and guided practice sessions.

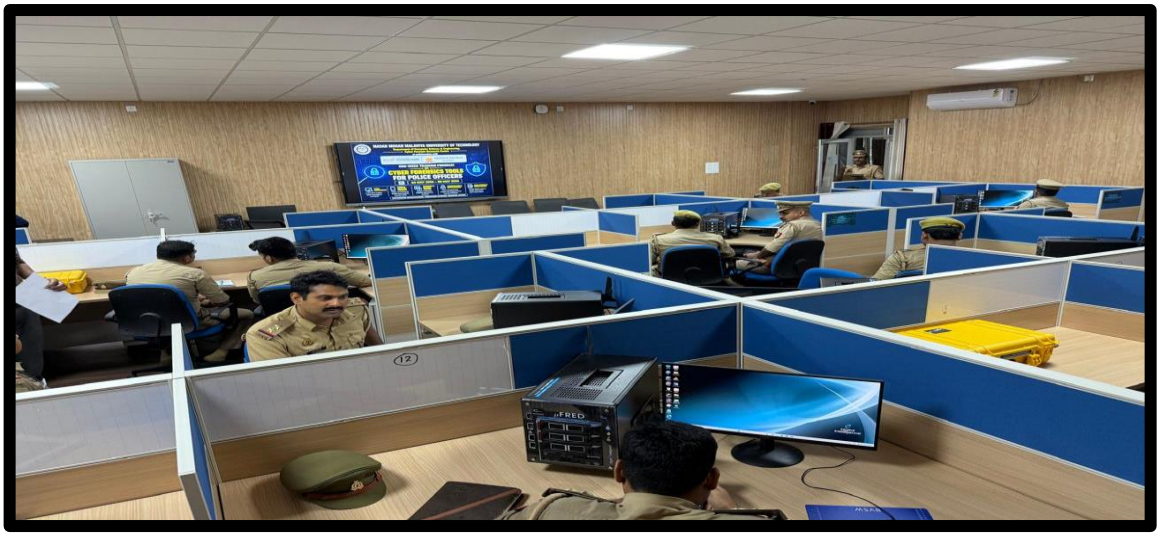
Conclusion

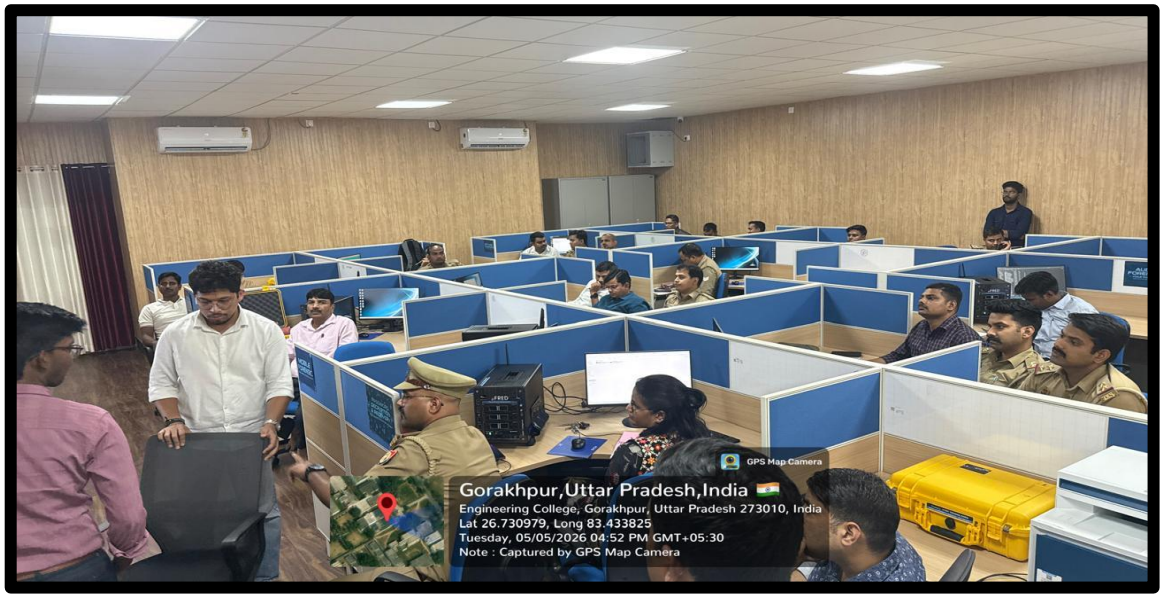
Day 2 of the training program significantly enhanced the participants' knowledge of disk and file system forensics. The combination of theoretical concepts and practical exercises enabled officers to develop essential skills required for handling digital evidence effectively. The session laid a strong foundation for advanced forensic analysis in the upcoming days.

Recommendations

- Provide additional hands-on exercises for deeper understanding
- Share sample datasets for independent practice






GPS Map Camera
Gorakhpur,Uttar Pradesh,India
Engineering College, Gorakhpur, Uttar Pradesh 273010, India
Lat 26.730979, Long 83.433825
Tuesday, 05/05/2026 04:52 PM GMT+05:30
Note : Captured by GPS Map Camera

One-Week Training Program on Cyber Forensics Tools for Police Officers

Organized by: Cyber Forensic Research Center, Department of Computer Science & Engineering, MMMUT, Gorakhpur
In Collaboration with Gorakhpur Zone Police, Gorakhpur

Topic: Mobile IoT and Password Recovery Forensics

DAY (3) ; WEDNESDAY Date: 06/05/2026

The third day of the one-week training program focused on advanced forensic investigation techniques related to Mobile IoT and Password Recovery Forensics. The session emphasized practical investigation of workflows, encrypted evidence analysis, mobile application examination, and secure digital evidence management.

Participants received hands-on exposure to forensic tools including MSAB XRY Office, XAMN Pro Software, OffGrid Faraday Bags, Passware Kit Forensic, and Passware Kit Mobile. The training aimed to strengthen participants' understanding of forensic extraction, password recovery, and evidence analysis in real-world investigation scenarios.

The technical sessions were conducted by expert trainers who guided participants through advanced forensic methodologies and practical demonstrations.

Training Objectives

The objectives of Day 3 training were:

- To provide advanced knowledge of mobile forensic investigations
- To demonstrate encrypted data analysis techniques
- To explain password recovery workflows in forensic investigations
- To provide practical exposure to forensic evidence analysis
- To enhance understanding of secure evidence preservation methods
- To strengthen investigation and reporting skills

Session Overview

Advanced Mobile Forensic Investigation

The day began with an advanced session on mobile forensic investigations.

Participants learned about:

- File system and physical extraction methods
- Recovery of deleted mobile data
- Mobile application forensic analysis
- Extraction of browser and communication history

- Analysis of multimedia and location data

Practical Demonstration using MSAB XRY Office

A detailed practical session was conducted using **MSAB XRY Office**.

The demonstrations included:

- Connecting mobile devices for forensic extraction
- Logical and physical acquisition processes
- Recovery of deleted chats and call records
- Extraction of application databases
- Evidence verification and reporting procedures

Participants observed how MSAB XRY Office assists investigators in collecting reliable digital evidence while maintaining forensic integrity.

Evidence Analysis using XAMN Pro Software

The next session focused on advanced forensic analysis using **XAMN Pro Software**.

Participants explored:

- Timeline reconstruction of activities
- Chat and social media analysis
- Visualization of communication patterns
- Filtering and categorization of forensic data
- Multimedia evidence examination

Practical exercises demonstrated how XAMN Pro improves investigation efficiency and helps investigators identify relevant evidence quickly.

Secure Evidence Handling using OffGrid Faraday Bags

The trainers demonstrated the role of **OffGrid Faraday Bags** in protecting seized digital devices.

Topics discussed included:

- Prevention of remote wiping attacks
- Isolation of devices from wireless networks
- Blocking Wi-Fi, Bluetooth, GPS, and cellular signals
- Secure transportation and storage of forensic evidence

Participants understood the importance of preserving evidence immediately after device seizure.

Password Recovery using Passware Kit Forensic

The session continued with practical demonstrations of **Passware Kit Forensic**.

Participants learned about:

- Password recovery methodologies
- Decryption of protected files and systems
- Dictionary and brute-force attack techniques
- GPU-accelerated password recovery
- Memory analysis for credential extraction

Mobile Access Recovery using Passware Kit Mobile

The trainers introduced advanced features of **Passware Kit Mobile**.

The session covered:

- Mobile backup password recovery
- Recovery of encrypted mobile data
- Device unlocking techniques
- Authentication credential analysis
- Mobile forensic evidence accessibility

Hands-on demonstrations helped participants understand mobile password recovery workflows.

Hands-On Investigation Exercise

Participants engaged in practical forensic investigation activities including:

- Performing sample mobile extractions
- Reviewing extracted evidence datasets
- Conducting password recovery exercises
- Analyzing communication records
- Preparing preliminary forensic observations

The exercise enhanced participants' confidence in using forensic tools during investigations.

- Participants gained understanding of:
- Advanced mobile forensic investigation methods
- Password recovery and decryption techniques
- Secure evidence handling procedures
- Practical use of forensic analysis software
- Investigation workflow management
- Importance of evidence integrity and documentation

Challenges Faced

The following challenges were observed during the training:

- Complexity of encrypted mobile environments

- Difficulty understanding advanced forensic workflows
- Large volumes of extracted digital evidence
- Initial challenges in forensic data interpretation

These challenges were addressed through guided demonstrations, practical exercises, and trainer support.

Conclusion

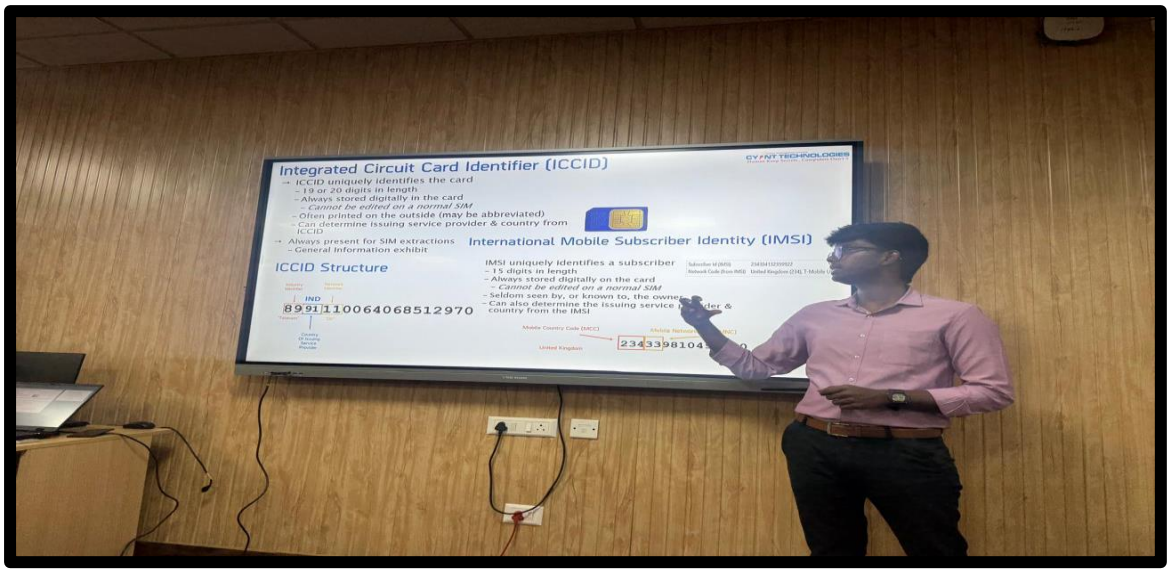
The third day of the training program successfully enhanced participants' practical understanding of Mobile IoT and Password Recovery Forensics. Officers gained valuable experience in evidence acquisition, forensic analysis, password recovery, and secure digital evidence handling.

The demonstrations and hands-on exercises using MSAB XRY Office, XAMN Pro Software, OffGrid Faraday Bags, Passware Kit Forensic, and Passware Kit Mobile provided practical exposure to real-world forensic investigation procedures.

The training significantly improved participants' technical awareness and preparedness for advanced digital forensic investigations.

Recommendations

- Increase practical hands-on investigation exercises
- Conduct advanced encrypted data analysis sessions
- Provide additional case-study-based training
- Share reference guides and forensic manuals





DATE – 06/05/2026

One Week Training Program on Cyber Forensics Tools for Police Officers

Organized by: Cyber Forensic Research Center, Department of Computer Science & Engineering, MMMUT, Gorakhpur
In Collaboration with Gorakhpur Zone Police, Gorakhpur

Topic: Anti-Forensics, Network Forensics, and Cryptocurrency Forensics

DAY (04) ; THURSDAY Date: 07/05/2026

The fourth day of the one-week training program focused on advanced cyber forensic investigation techniques related to Anti-Forensics, Network Forensics, and Cryptocurrency Forensics. The session emphasized the identification of cybercriminal activities, detection of evidence tampering techniques, network traffic analysis, and cryptocurrency transaction tracing.

Participants received practical exposure to forensic investigation of workflows, digital evidence analysis, and blockchain tracking methodologies. The training aimed to strengthen participants' understanding of modern cybercrime investigation techniques and enhance their capability to investigate complex digital crimes.

The technical sessions were conducted by expert trainers who demonstrated real-world forensic scenarios and advanced investigative methodologies.

Training Objectives

The objectives of Day 4 training were:

- To explain anti-forensics techniques used by cybercriminals
- To provide knowledge of network forensic investigation methods
- To demonstrate suspicious network traffic analysis
- To introduce cryptocurrency investigation and blockchain tracing
- To enhance practical understanding of cyber forensic tools
- To strengthen evidence collection and reporting procedures

Introduction to Anti-Forensics

The training began with a session on Anti-Forensics techniques used by attackers to hide malicious activities and destroy digital evidence.

Participants learned about:

- Data hiding and encryption techniques
- Secure file deletion methods
- Log manipulation and timestamp alteration
- Use of VPN and TOR networks
- Steganography and evidence obfuscation

The trainers explained how anti-forensic techniques complicate cybercrime investigations and how investigators can detect suspicious activities.

Practical Demonstration of Evidence Hiding Techniques

A practical session demonstrated how attackers attempt to conceal evidence from investigators.

The demonstrations included:

- Secure deletion of files
- Log cleaning methods
- Encrypted file containers
- Metadata manipulation
- Hidden partition identification

Participants observed how forensic investigators identify traces of anti-forensic activities during digital investigations.

Network Forensics Investigation

The next session focused on Network Forensics and Traffic Analysis methodologies.

Participants explored:

- Packet capture techniques
- Analysis of suspicious network traffic
- Monitoring inbound and outbound connections
- Detection of malware communication
- DNS and HTTP traffic analysis

The trainers explained the importance of network logs and packet analysis in identifying cyberattacks and unauthorized access attempts.

Practical Demonstration using Wireshark

A detailed practical demonstration was conducted using Wireshark.

The session covered:

- Capturing live network packets
- Filtering suspicious traffic
- Identifying malicious IP addresses
- Protocol analysis
- Investigation of suspicious communication patterns

Participants learned how investigators analyze captured network data to identify cyber threats and evidence of compromise.

Cryptocurrency Forensics Investigation

The session continued with Cryptocurrency Forensics and blockchain investigation techniques.

Participants learned about:

- Basics of blockchain technology
- Cryptocurrency wallet analysis
- Bitcoin and Ethereum transaction tracing
- Identification of suspicious wallet activity
- Cryptocurrency laundering methods

Blockchain Transaction Analysis

The trainers demonstrated blockchain investigation techniques using blockchain explorer tools.

The demonstrations included:

- Tracking cryptocurrency transactions
- Identifying wallet interactions
- Transaction timeline analysis
- Detection of mixer services
- Exchange transaction tracing

Participants observed how investigators trace digital currency movements during financial cybercrime investigations.

Hands-On Investigation Exercise

Participants engaged in practical forensic investigation exercises including:

- Capturing and analyzing network packets
- Detecting suspicious traffic patterns
- Identifying anti-forensic indicators
- Tracing sample cryptocurrency transactions
- Preparing preliminary investigation findings

The practical exercises enhanced participants' confidence in conducting cyber forensic investigations.

- Participants gained understanding of:
- Anti-forensics detection techniques
- Network traffic analysis procedures
- Cryptocurrency transaction tracing methods
- Practical use of network forensic tools
- Cyber investigation workflow management
- Importance of evidence integrity and preservation

Challenges Faced

The following challenges were observed during the training:

- Complexity of encrypted communications
- Difficulty understanding blockchain transactions
- Large volume of network traffic data
- Identification of hidden anti-forensic activities

These challenges were addressed through guided demonstrations, practical exercises, and trainer support.

Conclusion

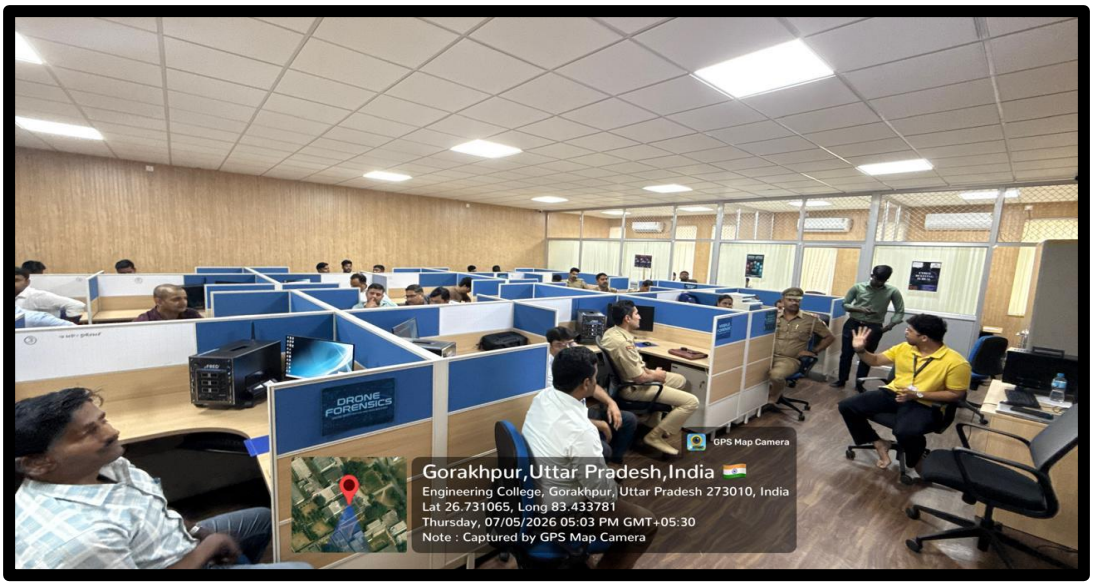
The fourth day of the training program successfully enhanced participants' understanding of Anti-Forensics, Network Forensics, and Cryptocurrency Forensics. Officers gained valuable practical exposure to digital evidence analysis, suspicious network investigation, and blockchain transaction tracing.

The demonstrations and hands-on exercises using forensic investigation tools significantly improved participants' technical awareness and investigative capabilities in handling modern cybercrime cases.

The training contributed to strengthening participants' preparedness for advanced cyber forensic investigations and digital evidence handling procedures.

Recommendations

- Increase advanced network traffic analysis exercises
- Conduct practical blockchain investigation workshops
- Provide additional anti-forensics case studies
- Share forensic investigation reference materials
- Continue scenario-based cyber investigation training


DRONE FORENSICS
GPS Map Camera
Gorakhpur,Uttar Pradesh,India
Engineering College, Gorakhpur, Uttar Pradesh 273010, India
Lat 26.731065, Long 83.433781
Thursday, 07/05/2026 05:03 PM GMT+05:30
Note : Captured by GPS Map Camera


FRED

One-Week Training Program on Cyber Forensics Tools for Police Officers

Organized by: Cyber Forensic Research Center, Department of Computer Science & Engineering, MMMUT, Gorakhpur
In Collaboration with Gorakhpur Zone Police, Gorakhpur

Topic: StegoHunt , Gargoyle Investigator & MD Drone Forensics

DAY (05) ; FRIDAY Date: 08/05/2026

Digital forensic investigations increasingly require specialized tools capable of identifying hidden content, steganographic techniques, malware artifacts, suspicious files, and drone-based digital evidence. StegoHunt MP, Gargoyle Investigator MP, and MD Drone Forensics are important technologies used by cyber investigators and law enforcement agencies to detect hidden information, malware signatures, covert communication mechanisms, and drone-related evidence.

This report provides a technical overview of these forensic technologies, including their operational methodologies, detection capabilities, forensic workflows, reporting mechanisms, and practical applications in cyber investigations.

StegoHunt MP

StegoHunt MP is a forensic software application designed to identify steganography and encryption programs while detecting suspicious multimedia files that may contain hidden data. The software combines statistical analysis and signature-based detection techniques.

Core Capabilities

- Detection of hidden information within multimedia files.
- Identification of known steganography and encryption software.
- Statistical anomaly analysis for image, audio, and video formats.
- Archive extraction and scanning support.
- Generation of CSV, HTML, and PDF reports.
- Case creation and evidence preservation.

Features of StegoHunt

StegoHunt uses both signature-based and anomaly-based detection techniques. These methods identify irregular structures, hidden payloads, encrypted metadata, and known steganographic signatures.

File Type	Detection Type	Examples
JPEG	Statistical & Signature	F5, Pixelknot, Passlok
PNG	Structural & Signature	MobiStego, PocketStego
MP3	Audio & Metadata	MP3 Stego, UnderMP3Cover

WAV	Statistical	Deep Sound, Xiao Steganography

Installation and Licensing

The installation process for StegoHunt involves downloading the software package from the WetStone Technologies Customer Support Portal, executing the installer, and completing license activation using a machine-specific registration code.

Installation Steps

1. Download StegoHunt MP from the support portal.
2. Run the MSI installer with administrator privileges.
3. Generate a registration code from the application.
4. Submit the registration code through the portal.
5. Receive and activate the license file.
6. Update factory datasets regularly.

Operational Workflow

Investigators select target drives or directories and choose between Factory Dataset Scanning and Statistical Analysis Scanning. Additional scan options include archive scanning, image carving, network file scanning, and case creation.

Workflow Steps

- Select target drives or directories.
- Enable required scan types.
- Run the forensic scan.
- Review CSV, HTML, or PDF reports.

Export suspicious files into a forensic case directory.

Gargoyle Investigator MP

Gargoyle Investigator MP is a malware detection and forensic investigation tool that enables investigators to identify suspicious applications, malicious artifacts, and hidden malware using datasets, hash analysis, and YARA rules.

Key Features

- MD5 and SHA-256 hash-based malware detection.
- Custom dataset support.
- YARA rule integration.
- Global and Local Whitelisting.
- Golden Image Whitelist creation.

- HTML, CSV, and PDF reporting.

Gargoyle Features and YARA Support

Gargoyle supports YARA version 4.1.3 and allows investigators to define custom YARA rules to identify malware patterns and suspicious behaviors. YARA scanning supports live systems, files, and memory images.

YARA Capabilities

- Supports scanning of active processes.
- Supports memory image analysis.
- Allows custom malware signatures.
- Enables detection of emerging threats.

Whitelisting and Golden Image Analysis

Gargoyle Investigator MP provides flexible whitelisting capabilities. Investigators may define Global or Local Whitelists to reduce false positives and focus investigations on suspicious applications.

Whitelisting Features

- Global Whitelists exclude organization-wide trusted applications.
- Local Whitelists allow system-specific exclusions.
- Golden Image Whitelists are generated from known-clean systems.
- Whitelist entries can include application names or MD5 hashes.

Reporting and Scan Results

Both StegoHunt MP and Gargoyle Investigator MP generate professional investigation reports in HTML, CSV, and PDF formats. Reports include detailed metadata such as file hashes, timestamps, anomaly descriptions, malware categories, and scan configurations.

Report Element	Description
Case Overview	Investigator and case details
Detection Results	Suspicious files and anomalies
Hash Information	MD5 and SHA-256 values
Timestamps	Created, modified, and accessed times
Export Formats	HTML, CSV, PDF

MD Drone Forensics

MD Drone Forensics is an emerging and important field within cyber forensic investigations. With the increasing use of drones in surveillance, photography, logistics, mapping, and criminal activities,

understanding drone forensics has become essential for law enforcement personnel and cyber investigators.

The training session provided participants with practical and theoretical knowledge regarding the identification, acquisition, preservation, and analysis of forensic evidence from drone devices.

Training Objectives

- Understand the fundamentals of drone forensics.
- Identify components and storage mechanisms of MD Drones.
- Learn methods of drone data acquisition and preservation.
- Develop skills in analyzing drone flight logs and metadata.
- Understand legal and procedural considerations in drone investigations.
- Ensure integrity and admissibility of digital evidence collected from drones.

Introduction to Drone Forensics

The session began with an overview of drone technology and its role in modern investigations. Participants learned about:

- Types of drones and their applications.
- Components of drones such as cameras, GPS modules, controllers, and storage devices.
- Common criminal activities involving drones.
- Importance of drone forensics in cybercrime investigations.

Participants also learned that drones store important evidence such as:

- Flight history
- GPS coordinates
- Images and videos
- Telemetry data
- Metadata and timestamps

Understanding MD Drone Architecture

This segment focused on the internal structure and functioning of MD Drones, including:

- Internal and external storage systems
- Flight control systems
- GPS and telemetry data
- Communication between drone and controller

The trainers demonstrated how drone data can provide critical information regarding user activity and movement patterns.

Drone Data Acquisition Techniques

A major part of the session emphasized forensic acquisition procedures and evidence handling.

Important Acquisition Methods

- Safe handling and seizure of drone devices
- Extraction of SD cards and internal memory
- Logical and physical acquisition methods
- Use of write blockers during evidence collection
- Hash value generation for data integrity verification

Participants were informed about maintaining the chain of custody and following forensic best practices during investigations.

Flight Log and Media Analysis

The trainers demonstrated techniques used to analyze drone data, including:

- Extraction of flight logs
- GPS coordinate analysis
- Recovery of images and videos captured by drones
- Examination of timestamps and metadata
- Identification of deleted or hidden files

Participants observed how forensic tools help reconstruct drone activities and movements.

Practical Session

The practical session included hands-on exercises such as:

- Connecting and examining an MD Drone device
- Creating forensic images of drone storage media
- Recovering deleted files from sample drone datasets
- Mapping GPS coordinates from flight logs

This interactive exercise enhanced participants' understanding of real-world drone forensic investigations.

Skills and Knowledge Gained

Participants gained:

- Understanding of MD Drone architecture and storage systems
- Knowledge of drone forensic acquisition methods

- Skills in analyzing flight logs, GPS data, and metadata
- Awareness of legal procedures for handling drone evidence
- Ability to recover deleted multimedia files from drone storage

Challenges Faced

- Difficulty interpreting flight log data
- Complexity in analyzing encrypted drone information
- Limited familiarity with drone forensic tools among beginners
- Knowledge of drone forensic acquisition methods
- Skills in analyzing flight logs, GPS data, and metadata
- Awareness of legal procedures for handling drone evidence

Comparative Analysis

Feature	StegoHunt MP	Gargoyle MP	MD Drone Forensics
Primary Focus	Steganography Detection	Malware Detection	Drone Evidence Analysis
Detection Method	Statistical + Signature	Hash + YARA	Flight Log + Metadata
Media Analysis	Extensive	Limited	Drone Media & Telemetry
YARA Support	No	Yes	Limited
Evidence Recovery	Hidden Multimedia	Malware Artifacts	Drone Media & Logs
Reporting	HTML/PDF/CSV	HTML/PDF/CSV	Forensic Investigation Reports

Recommendations

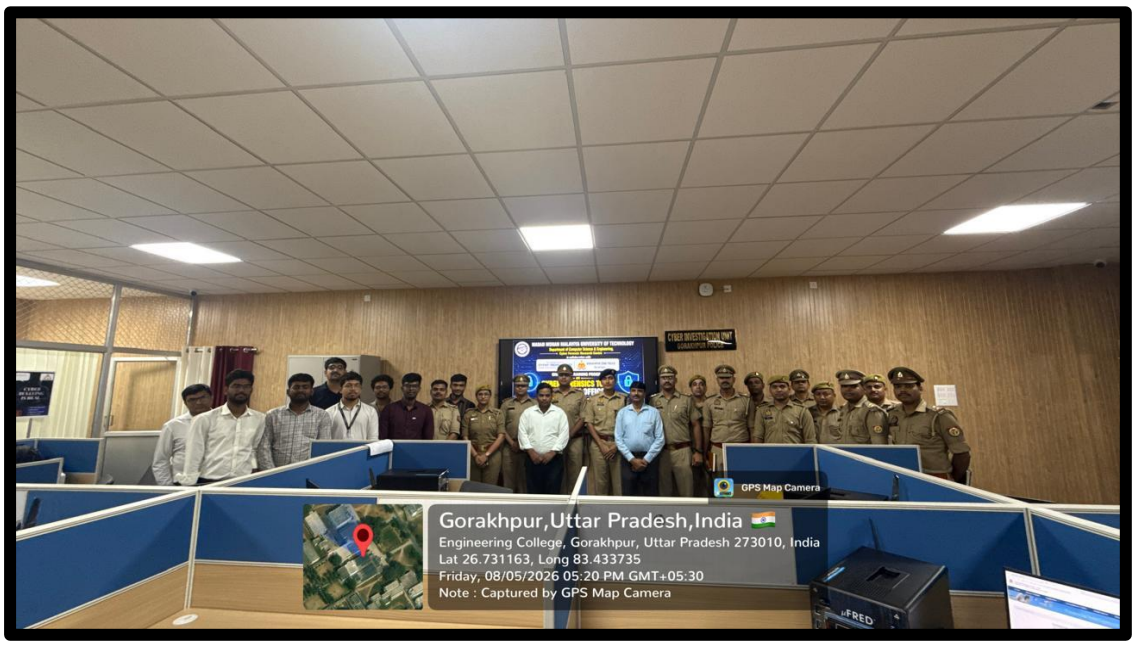
- Conduct advanced practical sessions on drone forensic tools.
- Provide additional case studies involving drone investigations.
- Share sample flight log datasets for independent practice.
- Organize refresher sessions on GPS and metadata analysis.

Conclusion

StegoHunt MP, Gargoyle Investigator MP, and MD Drone Forensics are powerful technologies that support modern cyber forensic investigations.

References

- StegoHunt MP User Manual, WetStone Technologies.
- Gargoyle Investigator MP User Manual, WetStone Technologies.


GPS Map Camera
Gorakhpur,Uttar Pradesh,India
Engineering College, Gorakhpur, Uttar Pradesh 273010, India
Lat 26.731163, Long 83.433735
Friday, 08/05/2026 05:20 PM GMT+05:30
Note : Captured by GPS Map Camera

