One-Day Demonstration Visit 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

THURSDAY, 21 MAY 2026

Program:-Training Program for Police officers

Topic:-MSAB XRY, Passware Kit Forensic, Forensic Explorer (FEX) v5, Breadcrumbs, NetworkMiner, X1 Social Discovery, MD-VIDEO, MD-DRONE, Voice Inspector, Gargoyle, StegoHunt, FRED-X 2R, UltraKit v5, microFRED, FTK Imager

Cybercrime and digital threats are rapidly increasing in today's technology-driven world, making cyber forensics and digital investigation essential for modern law enforcement agencies. To strengthen investigative capabilities, a special demonstration and training session was organized at the Cyber Forensics Research Centre (CFRC), Madan Mohan Malaviya University of Technology, in collaboration with CYINT Technologies and Gorakhpur Zone Police.
Participants were provided practical exposure to forensic hardware systems including FRED-X 2R, UltraKit v5, and microFRED, along with advanced software tools such as MSAB XRY, Passware Kit Forensic, Forensic Explorer (FEX) v5, FTK Imager, Breadcrumbs, NetworkMiner, X1 Social Discovery, MD-VIDEO, MD-DRONE, Voice Inspector, Gargoyle, and StegoHunt, covering mobile forensics, network forensics, blockchain investigation, malware analysis, and AI-powered investigation systems.
The session was graced by **Shri Dinesh Godara (ASP)**, **Shri Upendra Kumar Singh (SI)**, and **Dr. Rakesh Kumar (HoD, CSE)**, coordinated by **Dr. B.K. Sharma** and **Dr. Vimal Kumar**, with technical sessions conducted by **Mr. Naveen Singh**, Technical Expert. The program successfully enhanced awareness and technical knowledge regarding advanced cyber forensic tools and their applications in law enforcement and digital security investigations.

Objectives of the Visit / Training

The visit provided hands-on exposure to leading cyber forensic tools including MSAB XRY, Passware Kit Forensic, FEX v5, FTK Imager, Breadcrumbs, NetworkMiner, X1 Social Discovery, MD-VIDEO, MD-DRONE, Voice Inspector, Gargoyle, StegoHunt, and hardware systems FRED-X 2R, UltraKit v5, and microFRED. The program aimed to enhance officers' practical understanding of digital evidence acquisition, mobile forensics, network analysis, blockchain intelligence, and malware detection. The objective was to equip law enforcement personnel with technical knowledge and hands-on skills required for effective cybercrime investigation and digital evidence handling.

Figure 1: Cyber Forensic Tool Demonstration


AUDIO FORENSICS
GPS Map Camera
Gorakhpur,Uttar Pradesh,India
Engineering College, Gorakhpur, Uttar Pradesh 273010, India
Lat 26.731287, Long 83.433748
Thursday, 21/05/2026 05:54 PM GMT+05:30
Note : Captured by GPS Map Camera




17:52


GPS Map Camera
Gorakhpur,Uttar Pradesh,India
Engineering College, Gorakhpur, Uttar Pradesh 273010, India
Lat 26.731223, Long 83.433814
Thursday, 21/05/2026 05:52 PM GMT+05:30
Note : Captured by GPS Map Camera

Demonstrated Cyber Forensic Tools

During the demonstration visit, a total of 3 hardware systems and 12 software solutions were demonstrated covering all major domains of modern cybercrime investigation.
Hardware Systems including FRED-X 2R Forensic Workstation, UltraKit v5 Write Blocker, and microFRED Portable Forensic System were demonstrated for digital evidence acquisition and field investigations.
Software Tools including MSAB XRY, Passware Kit Forensic, Forensic Explorer (FEX) v5, FTK Imager, Breadcrumbs, NetworkMiner, X1 Social Discovery, MD-VIDEO, MD-DRONE, Voice Inspector, Gargoyle, and StegoHunt were demonstrated covering mobile forensics, disk analysis, blockchain tracing, network forensics, social media evidence preservation, surveillance video recovery, drone forensics, voice analysis, malware detection, and steganography analysis.

MSAB XRY

MSAB XRY is an advanced mobile forensic solution supporting physical and logical extraction from Android and iOS devices. It can recover deleted messages, call logs, media files, application data, and cloud data. XAMN Pro provides AI-powered analysis, timeline reconstruction, and cross-device correlation for investigations.

Passware Kit Forensic

Passware Kit Forensic is a complete password recovery and decryption solution supporting 400+ file types. It decrypts BitLocker, VeraCrypt, FileVault2, LUKS, and APFS encrypted systems using GPU-accelerated processing. It also supports live memory analysis and distributed cracking for accessing protected digital evidence.

Forensic Explorer (FEX) v5

Forensic Explorer is a professional digital forensic platform for disk imaging, file system analysis, and evidence management. It supports multiple file systems including NTFS, FAT, HFS+, APFS, and EXT4 with advanced file carving for deleted and overwritten files. It provides keyword search, registry analysis, timeline correlation, and integrated case management.

Breadcrumbs Blockchain Intelligence

Breadcrumbs is a blockchain forensic and cryptocurrency investigation platform supporting Bitcoin, Ethereum, Tron, XRP, and 20+ networks. It provides visual graph-based transaction mapping, automated risk scoring, and sanctions screening. It is widely used for tracing ransomware payments, cryptocurrency fraud, and dark web financial intelligence.

NetworkMiner Professional

NetworkMiner Professional is a network forensic tool by Netresec for analyzing PCAP files and network traffic. It passively captures packets, reassembles TCP sessions, extracts **files** and credentials, and identifies all network hosts with OS fingerprinting. It is used for incident response, data exfiltration detection, and malware communication analysis.

X1 Social Discovery

X1 Social Discovery is a social media evidence collection and preservation platform. It captures and archives content from Facebook, Instagram, Twitter/X, TikTok, LinkedIn, and other platforms with tamper-evident hash verification. It produces court-admissible exports with complete chain-of-custody documentation for legal investigations.

MD-VIDEO

MD-VIDEO AI is a forensic video recovery and analysis tool by GMDSOFT supporting 300+ DVR/NVR manufacturers. It recovers deleted or corrupted CCTV footage using AI-based reconstruction and provides frame-by-frame enhancement for facial recognition and license plate analysis. Output is court-admissible with SHA-256 hash verification.

MD-DRONE

MD-DRONE is a drone forensic investigation tool by GMDSOFT supporting 50+ drone brands including DJI, Parrot, and Autel. It extracts flight logs, GPS routes, telemetry data, deleted images, and videos from drone storage. It reconstructs 3D flight paths for courtroom visualization and identifies drone operators from encrypted flight data.

Phonexia Voice Inspector

Phonexia Voice Inspector is an AI-powered voice forensic tool for speaker identification and verification. It uses deep neural network voice biometrics to compare voice samples from calls, recordings, and social media with 99%+ accuracy. It is used for ransom call investigations, organized crime wiretap analysis, and fraud detection.

Gargoyle DFIR

Gargoyle DFIR by Wetstone Labs is a deep static malware analysis tool for digital forensic investigations. It scans entire drives for known and unknown malware including RATs, keyloggers, rootkits, and exploit kits without executing malicious code. It contains 10,000+ hacker tool signatures and generates comprehensive forensic reports.

StegoHunt

StegoHunt by Wetstone Labs is a steganography detection tool that identifies hidden data concealed within images, audio, video, and documents. It detects 30+ steganography tools using signature-based and statistical anomaly analysis. It is critical for terrorism, espionage, and cybercrime investigations involving covert communication channels.

FRED-X 2R Forensic Workstation

FRED-X 2R is a high-performance rack-mount forensic workstation by Digital Intelligence. It supports dual-boot Windows and Linux, NVMe, SATA, and SAS drives with hardware write-block interfaces. It is widely used for disk imaging, data recovery, and large-scale forensic analysis in laboratory environments.

UltraKit v5 Write Blocker

UltraKit v5 is a portable forensic write-blocker kit supporting HDD, SSD, USB, SD, CF, and mSATA devices. It enforces read-only access at hardware level to prevent modification of original evidence during data extraction. It is ideal for field investigations and forensic imaging operations.

microFRED Portable Forensic System

microFRED is an ultra-compact portable forensic system supporting Intel Core i9 processor with dual display capability. It provides full-size I/O in a compact form factor with integrated write-block support. It is commonly used for on-site digital evidence analysis and courtroom presentations.

FTK Imager

FTK Imager is a forensic imaging and data preview tool by Exterro. It creates forensic images of storage devices in E01, DD, and AFF formats while maintaining evidence integrity through hash verification. It is widely used for disk imaging, evidence preview, and data acquisition in digital investigations.

Key Learnings and Outcomes

The training program provided valuable hands-on knowledge of advanced cyber forensic tools including MSAB XRY, Passware Kit Forensic, FEX v5, FTK Imager, Breadcrumbs, NetworkMiner, X1 Social Discovery, MD-VIDEO, MD-DRONE, Voice Inspector, Gargoyle, StegoHunt, and hardware systems FRED-X 2R, UltraKit v5, and microFRED. Officers gained practical understanding of mobile forensics, network analysis, blockchain intelligence, malware detection, surveillance video recovery, drone forensics, and digital evidence preservation techniques. The program successfully strengthened technical capabilities and investigative skills of law enforcement personnel for effective cybercrime prevention and digital forensic analysis.

Conclusion

The demonstration visit successfully provided law enforcement officers practical exposure to advanced cyber forensic tools, strengthening their investigative capabilities in mobile forensics, network analysis, blockchain intelligence, and digital evidence preservation for effective cybercrime prevention.

Acknowledgement

he organizers sincerely express gratitude to Uttar Pradesh Police, Gorakhpur Zone, Cyber Forensics Research Centre (CFRC), Department of Computer Science & Engineering, MMMUT Gorakhpur, and CYINT Technologies for organizing this valuable training program. Special thanks to Shri Dinesh Godara (ASP), Shri Upendra Kumar Singh (SI), Dr. Rakesh Kumar (HoD), Dr. B.K. Sharma, Dr. Vimal Kumar, and Mr. Naveen Singh whose guidance and participation made the session informative and successful.

Figure 6: Police Officers Attending Cyber Awareness Presentation

Home / ब्रेकिंग न्यूज़ / मदन मोहन मालवीय प्रौद्योगिकी विश्वविद्यालय गोरखपुर में साइबर फॉरेंसिक जागरूकता कार्यक्रम का हुआ आयोजन



मदन मोहन मालवीय प्रौद्योगिकी विश्वविद्यालय गोरखपुर में साइबर फॉरेंसिक जागरूकता कार्यक्रम का हुआ आयोजन

लखनऊ। मदन मोहन मालवीय प्रौद्योगिकी विश्वविद्यालय (MMMUT), गोरखपुर के कंप्यूटर साइंस एवं इंजीनियरिंग विभाग द्वारा विश्वविद्यालय एवं गोरखपुर जोन पुलिस के मध्य हस्ताक्षरित एमओयू के अंतर्गत "नव नियुक्त प्रशिक्षु पुलिस अधिकारियों हेतु साइबर फॉरेंसिक जागरूकता कार्यक्रम (Cyber Forensics Awareness Program)" का आयोजन दिनांक 21 मई 2026 को सफलतापूर्वक किया गया। यह कार्यक्रम कुलपति प्रो. जे. पी. सैनी तथा मुथा अशोक जैन, अतिरिक्त पुलिस महानिदेशक, गोरखपुर जोन पुलिस, गोरखपुर के मार्गदर्शन में संपन्न हुआ। कार्यक्रम के प्रारंभ में डॉ. विमल कुमार द्वारा सभी अतिथियों एवं प्रशिक्षु पुलिस अधिकारियों का स्वागत किया गया। इस अवसर पर साइबर फॉरेंसिक रिसर्च सेंटर में उपलब्ध साइबर फॉरेंसिक टूल्स एवं तकनीकों की विस्तृत जानकारी प्रदान की गई। नवीन सिंह, साइंट टेक्नोलॉजीज़ (Cyint Technologies) द्वारा विभिन्न आधुनिक डिजिटल जांच उपकरणों, मोबाइल फॉरेंसिक, वीडियो फॉरेंसिक, डाटा रिकवरी, नेटवर्क फॉरेंसिक तथा डिजिटल एविडेंस एनालिसिस से संबंधित तकनीकों के उपयोग एवं महत्व पर विस्तारपूर्वक प्रकाश डाला गया। कार्यक्रम के उद्घाटन अवसर पर आयोजित सत्र में मुख्य अतिथि के रूप में दिनेश गोदारा (एएसपी) तथा विशिष्ट अतिथि के रूप में उपेन्द्र सिंह, साइबर कमांडो, गोरखपुर जोन पुलिस उपस्थित रहे। मुख्य अतिथि दिनेश गोदारा ने अपने संबोधन में कहा कि वर्तमान डिजिटल युग में बढ़ते साइबर अपराधों से प्रभावी रूप से निपटने के लिए पुलिस अधिकारियों का तकनीकी रूप से दक्ष एवं प्रशिक्षित होना अत्यंत आवश्यक है। उन्होंने मोबाइल फॉरेंसिक, वीडियो फॉरेंसिक, पासवर्ड बायपासिंग हेतु Passware, डिक्रिप्शन तकनीकों आदि के महत्व पर प्रकाश डालते हुए कहा कि इस प्रकार के प्रशिक्षण एवं जागरूकता कार्यक्रम जांच क्षमता को सुदृढ़ करने की दिशा में अत्यंत महत्वपूर्ण पहल हैं। विशिष्ट अतिथि उपेन्द्र सिंह, साइबर कमांडो, गोरखपुर जोन पुलिस ने अपने संबोधन में कहा कि साइबर जांच के दौरान Faraday Bags, UltraKit, Write Blocker, Google Activity, GPS Activity आदि आधुनिक साइबर फॉरेंसिक उपकरणों के साथ-साथ सरकारी रूप से अनुमोदित एवं समर्थित टूल्स का उपयोग करना अत्यंत आवश्यक है। इससे जांच प्रक्रिया अधिक विश्वसनीय, सुरक्षित एवं विधिसम्मत बनी रहती है। कार्यक्रम के अंत में डॉ. बी. के. शर्मा द्वारा सभी अतिथियों, प्रतिभागियों एवं आयोजकों के प्रति धन्यवाद ज्ञापित किया गया।

Figure 5: Cyber Forensic Training and Technical Demonstration Session



Figure 6: Cyber Forensics Awareness Program



Glimpses During the Visit to Cyber Forensics Research Center (CFRC)

