One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(01) : Cyber Security Landscape: Emerging Threats and Attack Vectors

DAY(01): MONDAY date: 21/09/2026

The programme was designed to enhance the knowledge and practical understanding of faculty members in the areas of Cyber Security, Digital Forensics, Cybercrime Investigation, and emerging forensic technologies. It aimed to provide participants with an understanding of contemporary cyber threats, digital evidence acquisition and analysis, and modern forensic investigation techniques. The programme also focused on developing practical skills through expert lectures, demonstrations, case studies, and hands-on sessions. It further encouraged participants to apply the acquired knowledge in teaching, research, and practical cybersecurity and forensic investigations.

The programme was graced by the presence of **Hon'ble Prof. Anupama Kaushik Sharma**, Vice-Chancellor, MMMUT, as the distinguished dignitary, and **Shri Abhinav Mishra, Scientist 'D', NIELIT Gorakhpur**, as the Chief Guest. The programme was chaired by **Prof. Rakesh Kumar, Professor & Head, Department of Computer Science and Engineering, MMMUT, Gorakhpur**. The programme coordination was carried out by **Dr. B.K. Sharma, Dr. Vimal Kumar, and Dr. Pawan Kumar Mall**, who contributed to the effective planning, coordination, and smooth execution of the programme. The leaflet also identifies Prof. Anupama Kaushik Sharma as Patron and Prof. Rakesh Kumar and Shri Abhinav Mishra among the programme leadership.

Training Objective

- To enhance participants' understanding of Cyber Security and Digital Forensics.
- To familiarize participants with emerging cyber threats, attack vectors, and cybersecurity challenges.
- To develop practical knowledge of digital evidence acquisition, preservation, and analysis.
- To provide hands-on exposure to modern cybersecurity and forensic investigation tools.
- To introduce practical approaches for cybercrime investigation and digital forensic analysis.
- To strengthen participants' capabilities in applying cybersecurity and forensic knowledge in teaching, research, and practical investigations.

Introduction to Cyber Security Landscape: Emerging Threats and Attack Vectors

Cyber Security Landscape

- Introduction to the evolving cyber security landscape.
- Significance of cybersecurity in the digital environment.
- Understanding the importance of protecting digital systems and networks.

Emerging Cyber Threats

- Overview of emerging cyber threats.
- Potential impact of cyber threats on digital systems and networks.
- Awareness of changing cybersecurity challenges.

Attack Vectors

- Overview of different attack vectors.
- Understanding how attackers target information systems and network infrastructure.
- Awareness of vulnerabilities that may be exploited.

Cyber Security and Protection

- Importance of cybersecurity in protecting information, systems, networks, and digital resources.
- Basic understanding of the cyber threat environment.
- Foundation for further learning in Network Security, Cryptography, Ethical Hacking, and Digital Investigation.

Hands-on Familiarization

The session provided an overview of the evolving cyber security landscape, with emphasis on emerging cyber threats and common attack vectors. Participants were familiarized with different types of cyber threats and the ways in which attackers may target systems and networks. The hands-on familiarization helped participants connect the theoretical concepts of cyber threats and attack vectors with practical cybersecurity scenarios and understand the importance of identifying potential security risks.

Challenges Faced

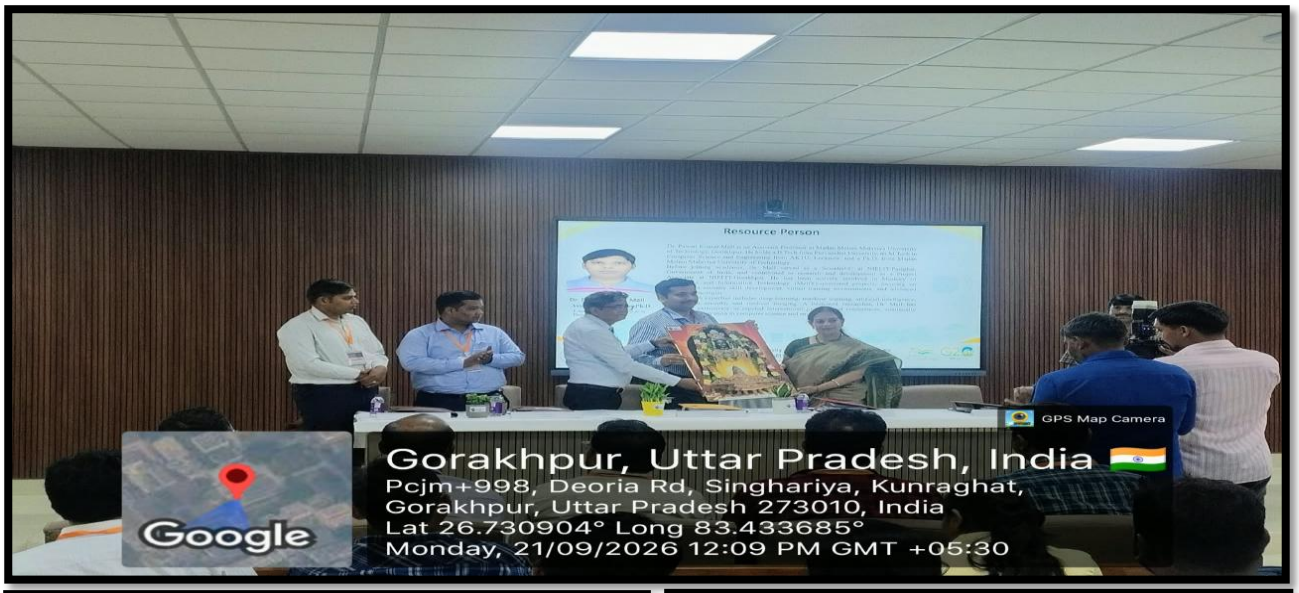
Participants faced challenges in understanding the evolving nature of cyber threats, identifying different attack vectors, relating emerging threats to security vulnerabilities and practical cybersecurity scenarios, and keeping pace with the continuously changing cybersecurity threat landscape. They also needed to understand the importance of timely identification and mitigation of potential cyber risks.

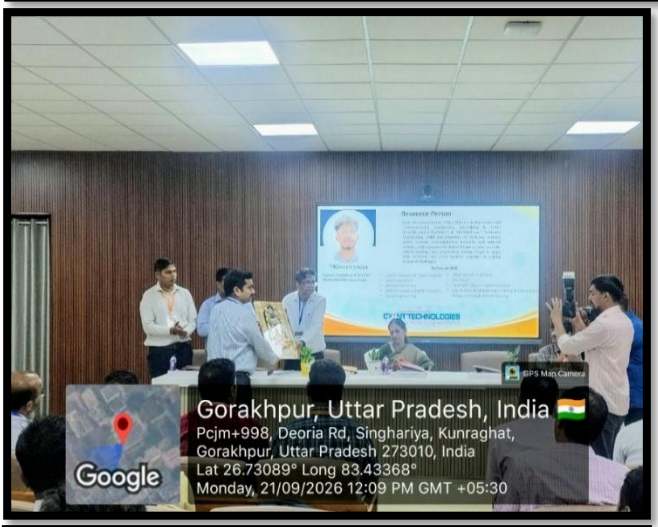
Conclusion

The session on Cyber Security Landscape: Emerging Threats and Attack Vectors provided participants with an understanding of the evolving cybersecurity environment, emerging threats, and common attack vectors. It helped participants recognize potential security risks and understand the importance of identifying and addressing cyber threats to strengthen the security of digital systems.

Recommendations

It is recommended to regularly update knowledge of emerging cyber threats and attack vectors, conduct practical cybersecurity awareness and security-testing sessions, and strengthen the ability to identify potential vulnerabilities and mitigate cyber risks. Continuous learning and practical exposure can help participants remain prepared for the changing cybersecurity landscape.

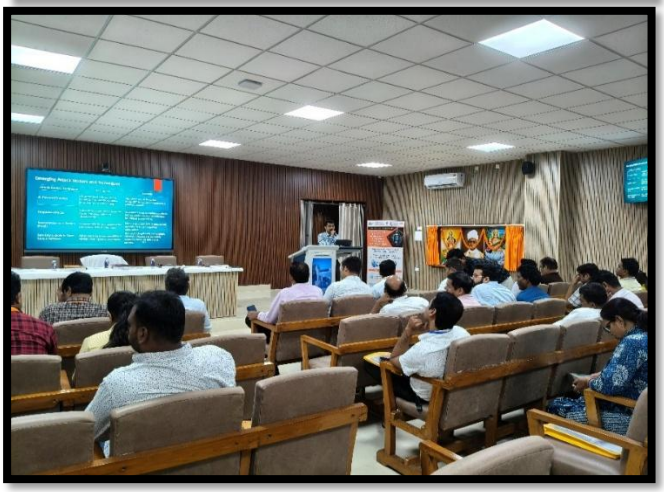

Resource Person
GPS Map Camera
Gorakhpur, Uttar Pradesh, India
Pcjm+998, Deoria Rd, Singhariya, Kunraghat,
Gorakhpur, Uttar Pradesh 273010, India
Lat 26.730904° Long 83.433685°
Monday, 21/09/2026 12:09 PM GMT +05:30
Google


GPS Map Camera
Gorakhpur, Uttar Pradesh, India
Pcjm+998, Deoria Rd, Singhariya, Kunraghat,
Gorakhpur, Uttar Pradesh 273010, India
Lat 26.73089° Long 83.43368°
Monday, 21/09/2026 12:09 PM GMT +05:30
Google


GPS Map Camera
Gorakhpur, Uttar Pradesh, India
Pcjm+8pm, Singhariya, Kunraghat, Gorakhpur, Uttar
Pradesh 273010, India
Lat 26.73087° Long 83.433669°
Monday, 21/09/2026 11:50 AM GMT +05:30
Google




Resource Person
GPS Map Camera
Gorakhpur, Uttar Pradesh, India
Pcjm+8pm, Singhariya, Kunraghat, Gorakhpur, Uttar
Pradesh 273010, India
Lat 26.730844° Long 83.433662°
Monday, 21/09/2026 11:45 AM GMT +05:30
Google





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics
Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(02) : Network Security Fundamentals: OSI & TCP/IP Security Architecture

DAY(01): MONDAY date: 21/09/2026

The session focused on developing a clear understanding of network security fundamentals and the security architecture of network communication. It introduced participants to the OSI and TCP/IP models and helped them understand how different layers contribute to secure communication and network protection. The session also provided a foundation for understanding network-level security concepts and their practical relevance.

Training Objective

The training objective was to provide participants with a basic understanding of Network Security Fundamentals and the OSI & TCP/IP Security Architecture. The session focused on understanding different network layers, their functions, and the security aspects associated with network communication. It also aimed to develop awareness of secure network architecture and network protection mechanisms.

Introduction Network Security Fundamentals: OSI & TCP/IP Security Architecture

The session introduced the fundamentals of Network Security with a focus on the OSI and TCP/IP security architecture. Participants were familiarized with the role of different network layers and the importance of securing communication across network architectures. The session provided a foundation for understanding network-level security and secure communication.

Hands-on Familiarization

The hands-on familiarization focused on understanding the practical security aspects of the OSI and TCP/IP models. Participants were familiarized with different network layers, their functions, communication flow, and the security considerations associated with network communication. The practical discussion helped participants relate network security concepts to real-world network environments.

Challenges Faced

Participants faced challenges in understanding the functions and relationships of different layers of the OSI and TCP/IP models and relating these layers to network security. Understanding the security requirements at different layers and connecting theoretical

network architecture concepts with practical security scenarios also required additional attention.

Conclusion

The session provided participants with a fundamental understanding of network security architecture based on the OSI and TCP/IP models. It helped them understand the importance of different network layers in secure communication and provided a foundation for further learning in network security and cybersecurity.

Recommendations

It is recommended to provide more practical demonstrations and network-based exercises to strengthen understanding of OSI and TCP/IP security architecture. Regular hands-on activities focusing on network communication, layer-wise security mechanisms, and practical security scenarios can further improve participants' understanding of network security concepts.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(03) : Applied Cryptography: Encryption, Hashing & Digital Signatures

DAY(01): MONDAY date: 21/09/2026

The session on Applied Cryptography: Encryption, Hashing & Digital Signatures introduced participants to the fundamental concepts of cryptography and their importance in protecting digital information. The session focused on how encryption can protect data, hashing can support data integrity, and digital signatures can support authentication and integrity in digital communication. These concepts form an important foundation for secure communication and cybersecurity applications.

Encryption, Hashing & Digital Signatures

The session explained encryption as a technique for protecting information from unauthorized access by converting readable data into an encoded form. Hashing was discussed as a method for generating a fixed-length value from data to support integrity verification. Digital signatures were introduced for verifying the authenticity and integrity of digital information. Together, these techniques provide important security mechanisms for protecting data and communications.

Hands-on Familiarization

Participants were familiarized with the practical application of encryption, hashing, and digital signatures. The hands-on exposure helped them understand how cryptographic techniques can be used for data protection, integrity verification, authentication, and secure digital communication.

Challenges Faced

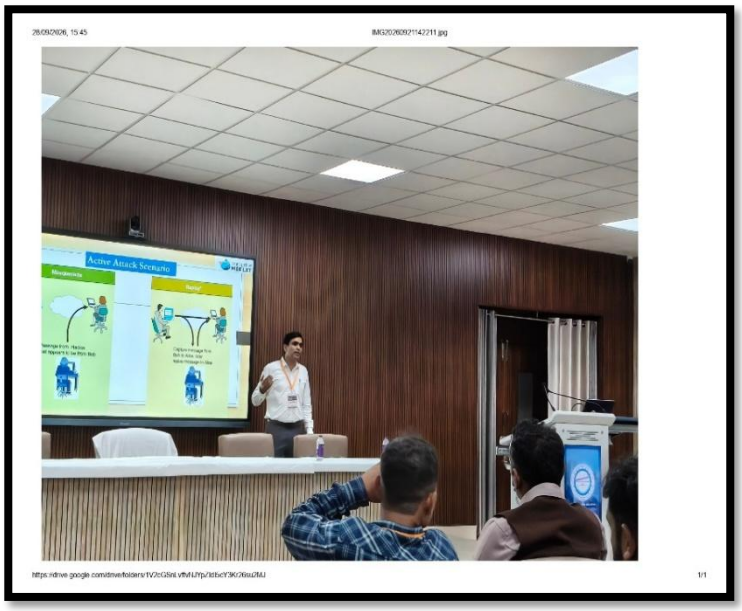
Participants faced challenges in understanding the differences between encryption, hashing, and digital signatures and in relating their theoretical concepts to practical cybersecurity applications.

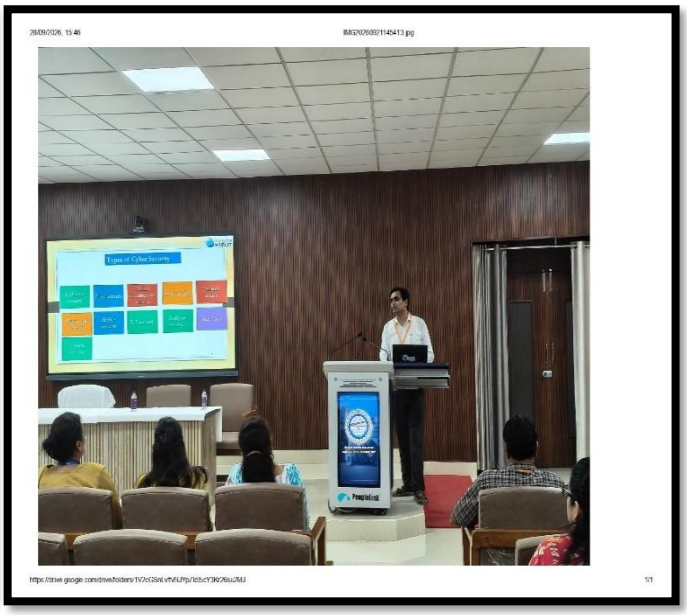
Recommendations

More practical demonstrations and real-world examples of encryption, hashing, and digital signatures can be included to strengthen participants' understanding and improve their ability to apply cryptographic concepts.

Conclusion

The session provided participants with a fundamental understanding of Encryption, Hashing, and Digital Signatures and their role in data protection, integrity, authentication, and secure digital communication. It established a strong foundation for understanding the practical applications of cryptography in cybersecurity.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(04) : Network Scanning, Enumeration, Sniffing & Man-in-the Middle Attacks

DAY(01): MONDAY date: 21/09/2026

The session focused on important concepts of network reconnaissance and security assessment, including network scanning, enumeration, network sniffing, and Man-in-the-Middle (MITM) attacks. The session helped participants understand how information about network systems can be identified and how network communication may be exposed to security threats. The topic was included in the Day 1 training schedule.

Network Scanning and Enumeration

Network scanning and enumeration were introduced as techniques for identifying systems, services, and available network information. Participants learned about their importance in understanding network infrastructure and identifying potential security weaknesses during authorized security assessments.

Network Sniffing

The session covered the concept of network sniffing, which involves observing network traffic to understand communication between systems. The discussion highlighted the importance of protecting network traffic and using appropriate security mechanisms to prevent unauthorized monitoring of sensitive communications.

Man-in-the-Middle (MITM) Attacks

The session introduced Man-in-the-Middle attacks, in which an attacker attempts to position themselves between communicating parties and potentially observe or manipulate communication. Participants were made aware of the security risks associated with such attacks and the importance of secure communication practices.

Hands-on Familiarization

The practical exposure helped participants understand the concepts of network scanning, enumeration, sniffing, and MITM attacks in a controlled learning environment. The activities connected the theoretical concepts with practical network-security scenarios.

Challenges Faced

Participants faced challenges in understanding the relationship between network scanning, enumeration, and network security assessment. Differentiating between legitimate security testing and potential attack activities, as well as understanding network traffic and MITM concepts, required careful attention.

Recommendations

It is recommended to conduct more controlled and authorized practical exercises on network scanning, traffic analysis, and network security assessment. Additional demonstrations of secure communication and network protection mechanisms can further strengthen participants' understanding.

Conclusion

The session provided participants with a fundamental understanding of network scanning, enumeration, sniffing, and Man-in-the-Middle attacks. It highlighted the importance of network visibility, secure communication, and appropriate security measures in protecting network infrastructure from potential threats.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(05) : Virtualisation Primer, Introduction to Kali Linux

DAY(01): MONDAY date: 21/09/2026

The session introduced participants to the fundamentals of virtualisation and Kali Linux and their importance in cybersecurity training. Participants learned how virtual environments provide an isolated and controlled platform for security testing and practical exercises.

Training Objective

The objective was to understand the basic concepts of virtual machines, host and guest operating systems, and to familiarize participants with the Kali Linux environment and its role in cybersecurity and ethical hacking.

Virtualisation & Kali Linux

Participants were introduced to virtual machines and their use in creating safe cybersecurity laboratories. The session covered the Kali Linux interface, terminal, basic commands, file navigation, and security tools used for practical security activities.

Hands-on Familiarization

Participants explored Kali Linux in a virtualized environment and performed basic terminal operations. The hands-on activity helped them understand the practical use of Kali Linux for subsequent cybersecurity and ethical hacking exercises.

Challenges Faced

Participants initially faced difficulties in understanding virtual machine configuration, Linux commands, and navigating the Kali Linux environment.

Recommendations

More practical exercises on Kali Linux commands, virtual machine configuration, and basic security tools can be conducted to improve participants' hands-on familiarity.

Conclusion

The session provided a basic understanding of virtualisation and Kali Linux and prepared participants for subsequent practical cybersecurity and ethical hacking sessions.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(06) : Lab Exercise / Practical Session

DAY(01): MONDAY date: 21/09/2026

The session introduced participants to virtualisation and Kali Linux as practical environments for cybersecurity training. Participants learned the basic concept of virtual machines and their importance in conducting security exercises in an isolated environment.

Virtualisation Primer

Participants were familiarized with virtual machines, host and guest operating systems, and the use of virtual environments for cybersecurity experiments and testing.

Introduction to Kali Linux

The session provided an overview of the Kali Linux operating system, its interface, terminal, basic commands, and commonly used cybersecurity tools. Participants were introduced to its role in ethical hacking and security testing.

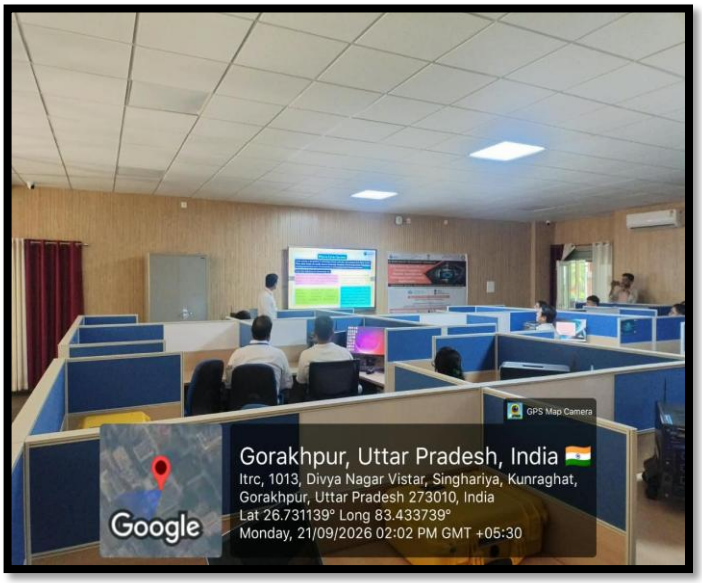
Lab Exercise / Practical Session

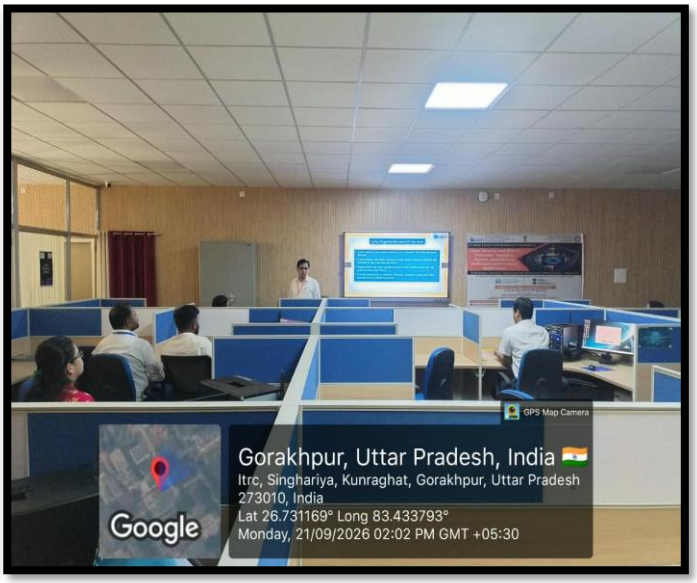
During the practical session, participants worked with a virtualized Kali Linux environment and performed basic activities such as:

- Exploring the Kali Linux desktop and terminal.
- Executing basic Linux commands.
- Navigating files and directories.
- Identifying and exploring available cybersecurity tools.
- Understanding the basic workflow of using Kali Linux for security exercises.

Conclusion

The practical session provided participants with hands-on familiarity with virtualisation and Kali Linux, establishing a foundation for further cybersecurity and ethical hacking activities. The official schedule places this practical session immediately after the Virtualisation and Kali Linux topic.


GPS Map Camera
Google
Gorakhpur, Uttar Pradesh, India
Itrc, 1013, Divya Nagar Vistar, Singhariya, Kunraghat,
Gorakhpur, Uttar Pradesh 273010, India
Lat 26.731139° Long 83.433739°
Monday, 21/09/2026 02:02 PM GMT +05:30


GPS Map Camera
Google
Gorakhpur, Uttar Pradesh, India
Itrc, Singhariya, Kunraghat, Gorakhpur, Uttar Pradesh
273010, India
Lat 26.731169° Long 83.433793°
Monday, 21/09/2026 02:02 PM GMT +05:30

One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(07) : Web Application Security, Browser Security, Burp Suite, Web Server Security, OWASP Top 10

DAY(02): TUESDAY date: 22/09/2026

The session introduced participants to the fundamentals of Web Application Security and common security risks associated with web applications, browsers, and web servers. It focused on understanding how security vulnerabilities can affect web applications and the importance of secure development and testing practices.

Web Application & Browser Security

Participants learned about common web application security concerns, including authentication, authorization, session management, input validation, and secure communication. Browser security concepts were also discussed to understand how browsers protect users and web applications from common threats.

Burp Suite

The session introduced Burp Suite as a web security testing platform. Participants were familiarized with its basic interface and its use for intercepting, inspecting, and analyzing HTTP/HTTPS requests and responses during security testing.

Web Server Security

The session covered basic web server security practices, including secure configuration, access control, software updates, proper error handling, and protection of sensitive information. Participants learned the importance of maintaining secure server environments.

OWASP Top 10

Participants were introduced to the OWASP Top 10, a widely used awareness framework for understanding major web application security risks. The discussion helped participants recognize common vulnerabilities and understand the importance of identifying and mitigating them during application development and security assessment.

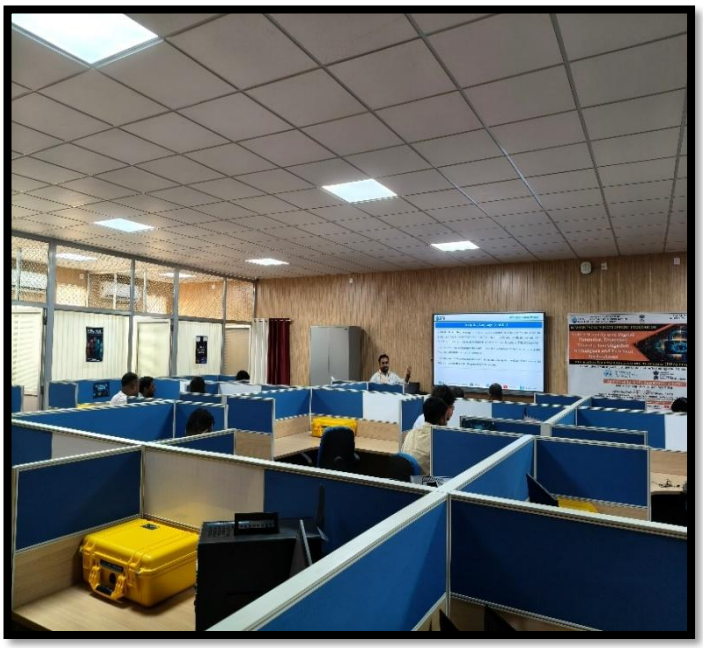
Hands-on Familiarization

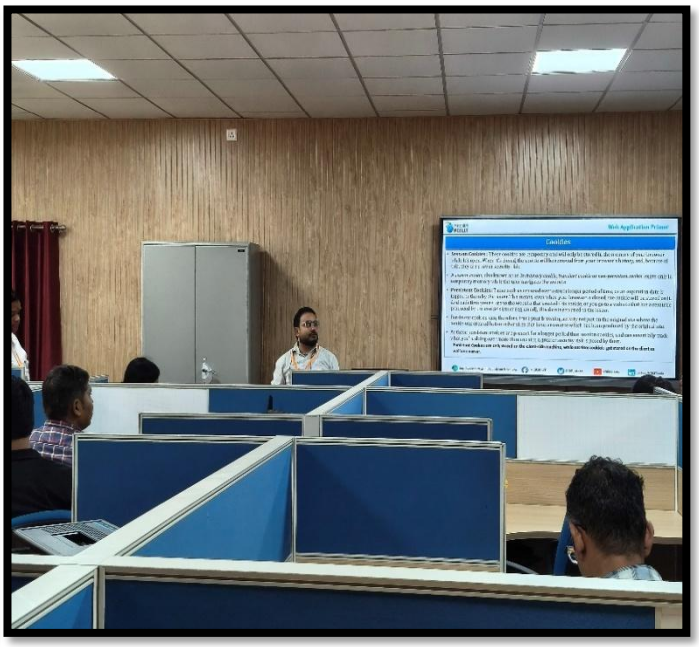
Participants explored basic web security testing concepts using Burp Suite and examined web

requests and responses in a controlled environment. The practical activity helped them understand how web application security assessment is performed.

Conclusion

The session provided participants with a foundational understanding of web application security, browser security, Burp Suite, web server security, and OWASP Top 10, preparing them for further practical cybersecurity and web security activities.
This matches the official Day 2 schedule, where Session 07 covers Web Application Security, Browser Security, Burp Suite, Web Server Security, and OWASP Top 10.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(08) : AI/LLM Threats and Security Testing: Prompt Injection and Red Teaming, OSINT

DAY(02): TUESDAY date: 22/09/2026

The session introduced participants to emerging AI and Large Language Model (LLM) security threats and the importance of security testing. It focused on understanding potential risks associated with AI-based systems and the role of security assessment in identifying vulnerabilities.

AI/LLM Threats

Participants were introduced to common security concerns related to AI/LLM systems, including misuse of AI systems, malicious inputs, information leakage, and unsafe or unintended model responses. The session highlighted the importance of responsible and secure use of AI technologies.

Prompt Injection

The session explained prompt injection as a security concern in which specially crafted inputs can influence an AI system to produce unintended responses or bypass expected instructions. Participants learned the importance of identifying and mitigating such risks during AI security testing.

Red Teaming

Participants were introduced to AI security red teaming, which involves controlled testing of AI systems to identify weaknesses, unexpected behaviours, and potential security risks. The approach helps improve the robustness and security of AI-enabled applications.

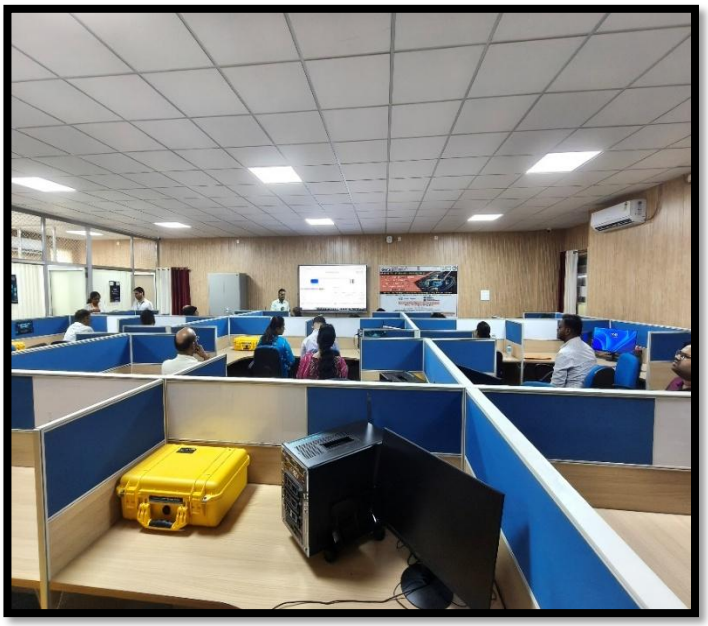
OSINT

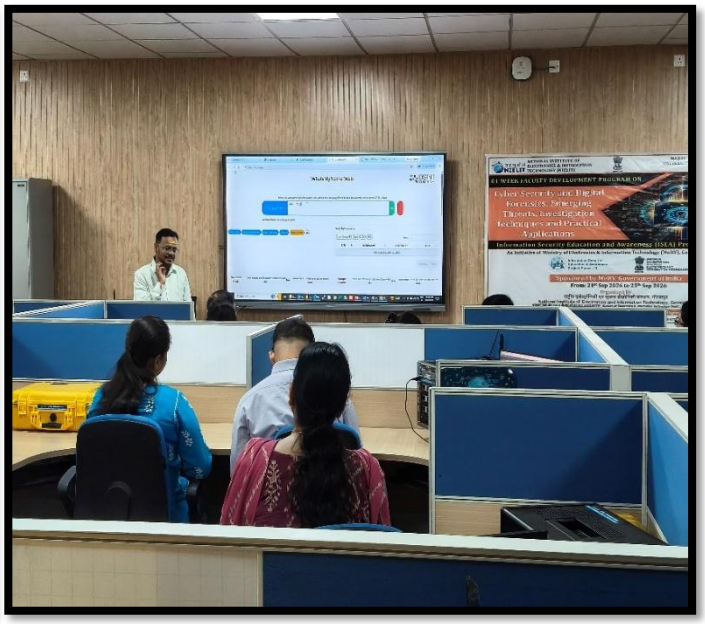
The session also covered Open-Source Intelligence (OSINT) and its role in security investigation. Participants learned how publicly available information can be collected, analysed, and correlated to support cybersecurity assessment and investigation.

Conclusion

The session provided participants with an understanding of AI/LLM security threats, prompt

injection, red teaming, and OSINT, highlighting their importance in modern cybersecurity testing and investigation.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(09) : API Security: Threats, Testing & Protection

DAY(02): TUESDAY date: 22/09/2026

The session introduced participants to the fundamentals of API Security and the security risks associated with Application Programming Interfaces. It focused on understanding how APIs communicate between applications and why proper security controls are required to protect data and services.

API Security Threats

Participants were familiarized with common API security concerns such as unauthorized access, weak authentication, improper authorization, insecure data exposure, and improper input validation. The session highlighted the importance of identifying security weaknesses in API-based applications.

API Security Testing

The session covered the basic approach to API security testing, including examining API requests and responses, checking authentication and authorization mechanisms, and identifying potential security weaknesses in a controlled testing environment.

API Protection

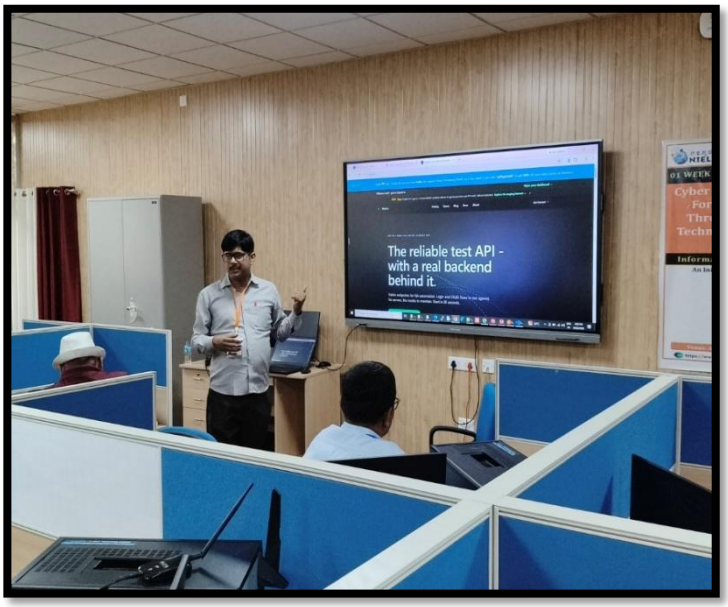
Participants learned about basic API protection measures such as strong authentication, proper authorization, input validation, secure communication, access control, and appropriate error handling. These practices help protect APIs from unauthorized access and misuse.

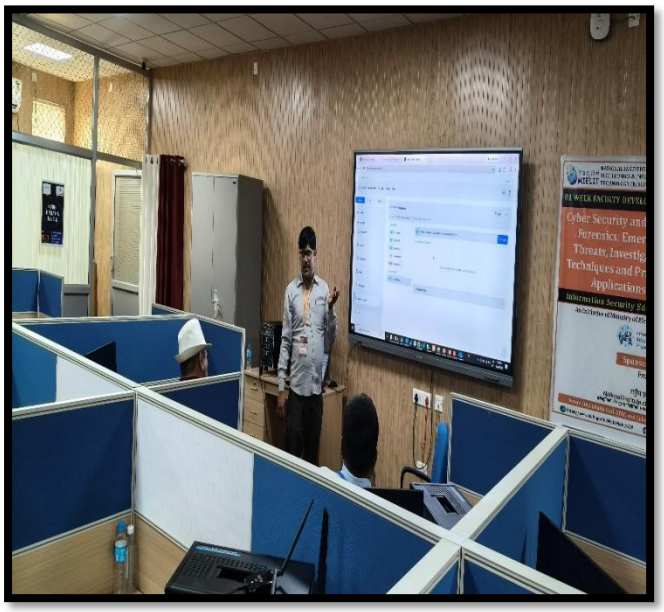
Hands-on Familiarization

The practical discussion helped participants understand the basic process of analysing API endpoints and applying security controls during API development and testing.

Conclusion

The session provided participants with a foundational understanding of API threats, security testing, and protection mechanisms, helping them recognize the importance of securing APIs in modern web and software applications.


The reliable test API -
with a real backend
behind it.



One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(10) : Lab Exercise / Practical Session

DAY(02): TUESDAY date: 22/09/2026

The session introduced participants to the fundamentals of API Security and the importance of protecting APIs that enable communication between different applications and services.

API Security Threats

Participants learned about common API security concerns such as unauthorized access, weak authentication, improper authorization, insecure data exposure, and inadequate input validation.

API Security Testing

The session covered basic API testing concepts, including examining API endpoints, requests and responses, authentication mechanisms, and access controls to identify potential security weaknesses.

API Protection

Participants were introduced to security measures such as strong authentication, proper authorization, input validation, access control, secure communication, and appropriate error handling for protecting APIs.

Lab Exercise / Practical Session

During the practical session, participants performed basic API security testing in a controlled environment. They explored API endpoints, analysed requests and responses, examined authentication and authorization mechanisms, and identified potential security issues.

Conclusion

The session provided participants with practical understanding of API threats, testing techniques, and protection mechanisms, strengthening their ability to assess and secure API-based applications.
The official schedule lists Session 09 as “API Security: Threats, Testing & Protection” followed by Session 10 “Lab Exercise / Practical Session.”


SECURITY MOVES UPSTREAM
IN API DESIGN


SECURITY ANATOMY OF AN API REQUEST

One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(11) : Cloud Security

DAY(02): TUESDAY date: 22/09/2026

The session introduced participants to the fundamentals of Cloud Security and the importance of protecting data, applications, and services hosted in cloud environments.

Cloud Security Concepts

Participants were familiarized with basic cloud security concepts, including data protection, access control, authentication, and secure cloud resource management. The session highlighted the need for appropriate security measures while using cloud-based services.

Cloud Security Threats

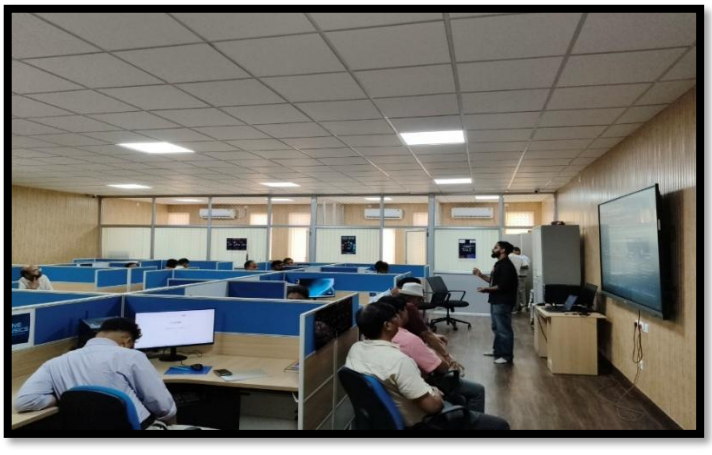
The session discussed common security concerns in cloud environments, such as unauthorized access, data exposure, insecure configurations, and improper access permissions. Participants learned the importance of identifying and managing these risks.

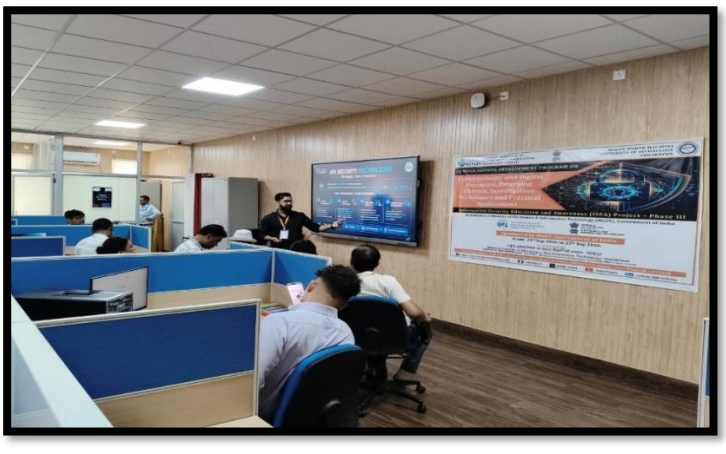
Security Measures

Participants were introduced to basic protection mechanisms such as strong authentication, proper access control, data protection, secure configuration, and continuous monitoring to improve cloud security.

Conclusion

The session provided participants with a basic understanding of cloud security, associated threats, and essential protection measures, helping them recognize the importance of securing cloud-based infrastructure and services.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(12) : Lab Exercise / Practical Session

DAY(02): TUESDAY date: 22/09/2026

The session introduced participants to the fundamentals of Cloud Security and the importance of protecting cloud-based data, applications, and services.

Cloud Security

Participants were familiarized with key concepts such as access control, authentication, data protection, secure configuration, and cloud resource management. The session also highlighted common risks associated with cloud environments, including unauthorized access and insecure configurations.

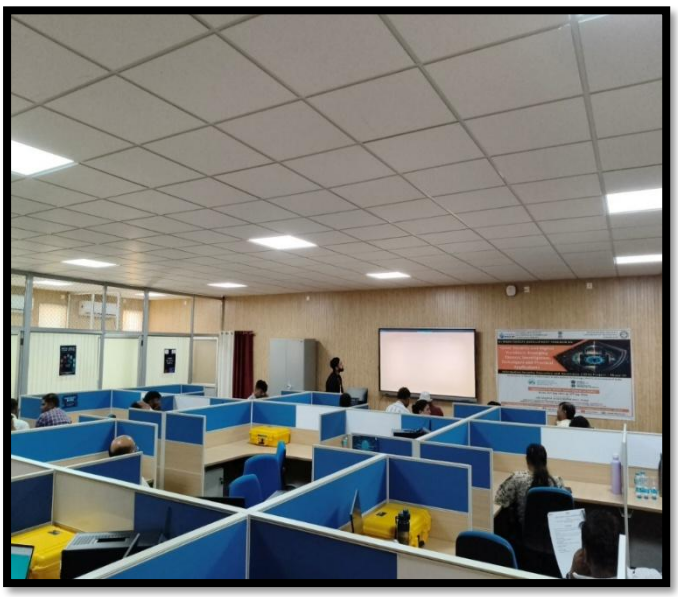
Lab Exercise / Practical Session

During the practical session, participants explored basic cloud security configurations and access-control mechanisms in a controlled environment. The activity helped participants understand how security controls can be applied to protect cloud resources and data.

Conclusion

The session provided participants with practical exposure to cloud security concepts and protection mechanisms, strengthening their understanding of securing cloud-based environments.


Cybersecurity and Digital Forensics, Emerging Threats, Investigation Techniques and Practical Applications
Information Security Education and Awareness (ISEA) Project – Phase III



One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(13) : Digital Forensics for Cybercrime Investigation: Emerging Threats, Modern Techniques and Practical Applications

DAY(03): WEDNESDAY date: 23/09/2026

The session introduced participants to Digital Forensics and its role in investigating cybercrime. It focused on understanding emerging cyber threats and the application of modern forensic techniques for examining digital evidence.

Digital Forensics in Cybercrime Investigation

Participants learned about the importance of digital evidence identification, collection, preservation, examination, and analysis during cybercrime investigations. The session highlighted the need to maintain the integrity and reliability of digital evidence.

Emerging Threats

The session discussed the changing nature of cybercrime and the challenges involved in investigating incidents involving digital devices, online activities, and evolving technologies.

Modern Forensic Techniques

Participants were introduced to modern approaches used in digital investigations, including evidence acquisition, forensic examination, analysis of digital artifacts, and documentation of investigation findings.

Practical Applications

The session highlighted the practical application of digital forensics in cybercrime investigation, evidence analysis, incident investigation, and supporting investigative findings.

Conclusion

The session provided participants with a foundational understanding of digital forensics, emerging cyber threats, modern investigation techniques, and their practical applications in cybercrime investigations.


ULTY DEVELOPMENT PROGRAM ON
Security and
al Forensics:
ging Threats,
estigation
niques and
l Applications
Project Phase -III)
lan Mohan Malaviya University of
chnology (MMMUT), Gorakhpur
&
tional Institute of Electronics &
tion Technology (NIELIT), Gorakhpur
NIELIT
21st Sep, 2026 to 25th Sep, 2026
Sponsored by



One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(14) : Advanced Search & Google Dorking for Security Investigation, Dark Web Intelligence: Concepts, Risks & Investigative Approaches

DAY(03): WEDNESDAY date: 23/09/2026

The session introduced participants to advanced search techniques, Google Dorking, and Dark Web Intelligence for cybersecurity and security investigations.

Advanced Search & Google Dorking

Participants learned how advanced search techniques can help in finding and analysing publicly available information relevant to security investigations. Google Dorking was introduced as a technique for refining search queries to locate specific information available through search engines.

Dark Web Intelligence

The session provided an overview of Dark Web Intelligence, including its concepts, characteristics, and relevance to cybersecurity investigations. Participants learned about the challenges associated with gathering and analysing information from dark web sources.

Risks & Investigative Approaches

The session discussed potential security, privacy, and investigative risks associated with dark web activities. Participants were introduced to structured approaches for collecting, analysing, and documenting relevant intelligence while maintaining ethical and legal considerations.

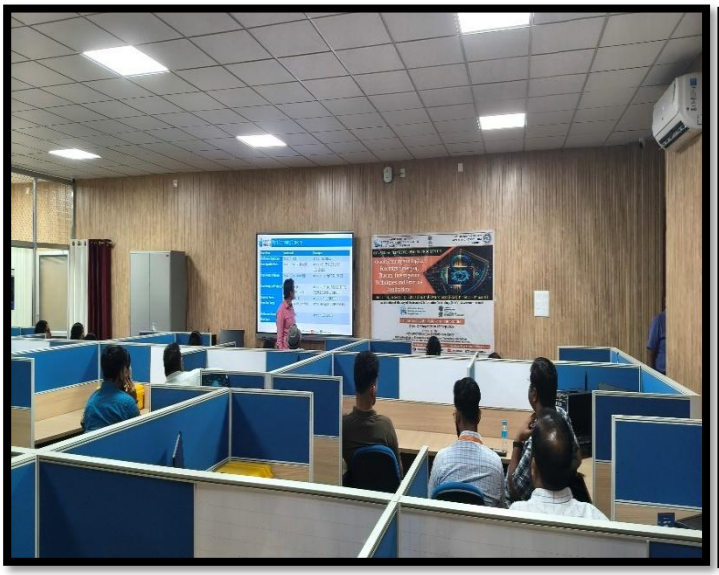
Practical Applications

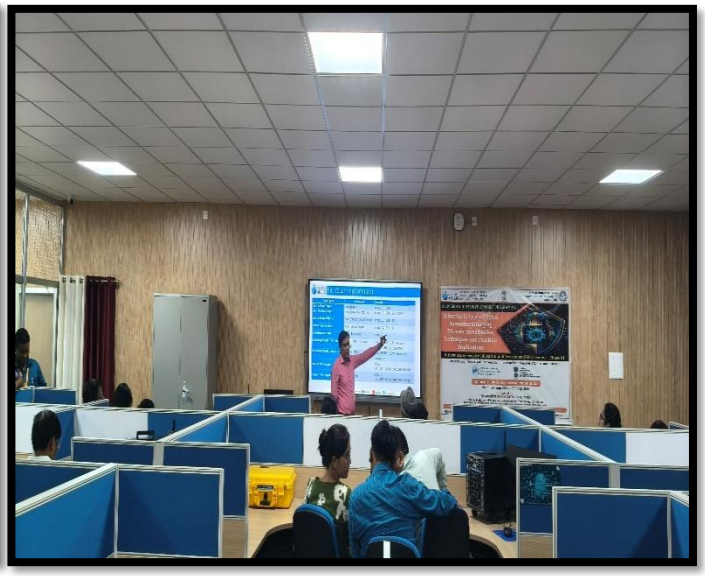
The concepts were related to cybercrime investigation, information gathering, threat intelligence, and security analysis, demonstrating how publicly available information can support investigative activities.

Conclusion

The session provided participants with an understanding of advanced search, Google Dorking,

Dark Web Intelligence, associated risks, and investigative approaches, strengthening their information-gathering and security investigation skills.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(15) : Infrastructure Security Hardening, Patch Management & Monitoring SIEM Fundamentals: Log Management, Event Correlation & Threat Detection 'Wazuh SIEM: Security Monitoring, Threat Detection & Incident Analysis Hands-on Lab: Security Monitoring & Threat Detection using Wazuh

DAY(03): WEDNESDAY date: 23/09/2026

The session focused on infrastructure security hardening, patch management, monitoring, and SIEM-based security operations. Participants learned how security controls and continuous monitoring help in identifying and responding to security events.

Infrastructure Security Hardening & Patch Management

Participants were introduced to security hardening techniques, patch management, and system monitoring. The session highlighted the importance of maintaining secure configurations and keeping systems updated to reduce security risks.

SIEM Fundamentals

The session covered Security Information and Event Management (SIEM) concepts, including log management, event correlation, and threat detection. Participants learned how security logs can be collected and analysed to identify suspicious activities.

Wazuh SIEM

Participants were introduced to Wazuh for security monitoring, threat detection, and incident analysis. The session demonstrated how security events and system activities can be monitored through a SIEM platform.

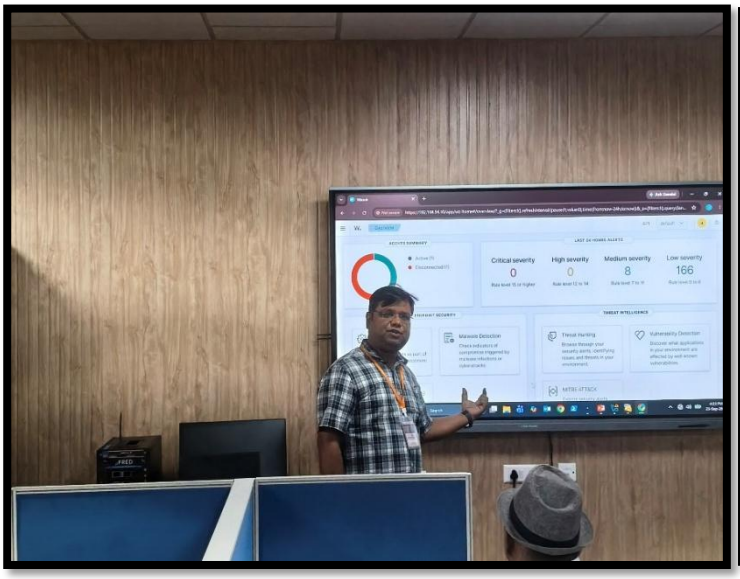
Hands-on Lab

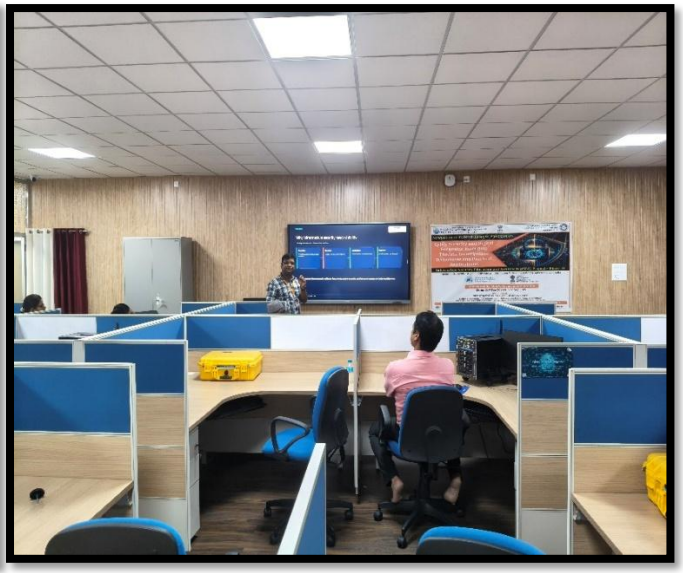
The practical session provided hands-on exposure to security monitoring and threat detection using Wazuh. Participants explored security logs, monitored events, and understood the basic process of analysing detected security activities.

Conclusion

The session provided participants with practical knowledge of infrastructure hardening, patch management, SIEM, Wazuh-based monitoring, threat detection, and incident analysis,

strengthening their understanding of modern security monitoring practices.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(16) : Web Application Attacks and Security, Lab

DAY(03): WEDNESDAY date: 23/09/2026

The session focused on web application attacks and security and provided participants with an understanding of common security issues affecting web applications.

Web Application Attacks

Participants were introduced to common web application security threats and the basic techniques used to identify vulnerabilities during security assessment. The session emphasized understanding how insecure web applications can be exploited.

Web Application Security

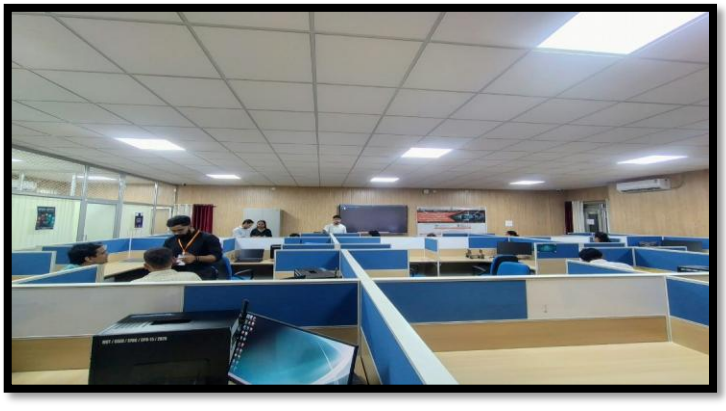
The session discussed important security practices for protecting web applications, including secure configuration, input validation, authentication, authorization, and access control.

Lab / Practical Session

During the practical session, participants explored web application security in a controlled laboratory environment. They examined common security weaknesses and learned the basic process of identifying and analysing vulnerabilities in web applications.

Conclusion

The session provided participants with practical exposure to web application attacks and security assessment, helping them understand common vulnerabilities and the importance of implementing appropriate security controls.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(17) : Steganography

DAY(03): WEDNESDAY date: 23/09/2026

The session introduced participants to Steganography, a technique concerned with concealing information within digital media. The topic was discussed from a digital forensics and cybersecurity perspective.

Concept of Steganography

Participants learned the basic concept of hiding secret information within digital files such as images, audio, video, or other media so that the presence of the hidden information is not immediately apparent.

Role in Digital Forensics

The session highlighted the importance of identifying and analysing steganographic content during digital investigations. Participants were introduced to the challenges involved in detecting hidden information within digital evidence.

Forensic Analysis

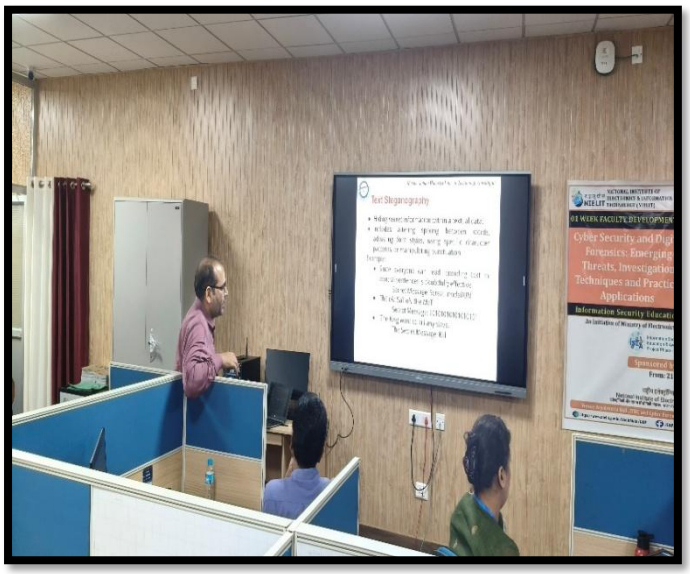
The session focused on the basic approach to examining suspected files, identifying possible hidden data, and analysing digital artifacts as part of a forensic investigation.

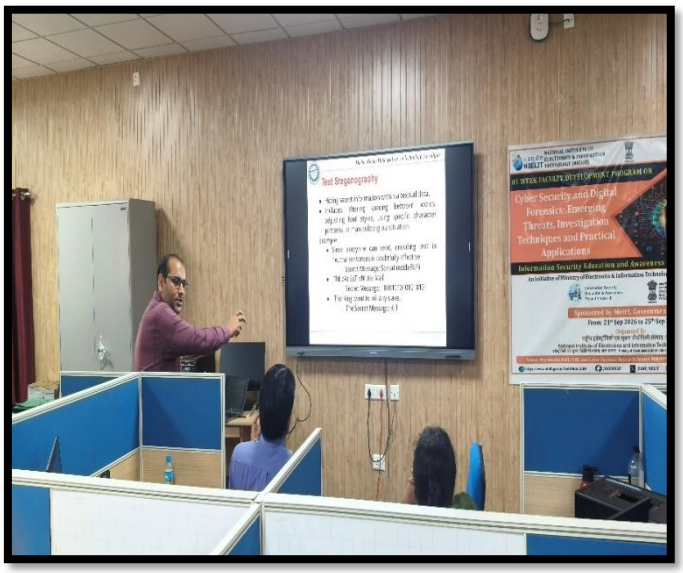
Practical Relevance

Understanding steganography helps investigators recognise potential methods of concealing digital information and supports the examination of suspicious multimedia files during cybercrime investigations.

Conclusion

The session provided participants with a foundational understanding of steganography and its relevance to digital forensics, particularly in identifying and analysing potentially concealed information.


Text Steganography
Cyber Security and Digital Forensics: Emerging Threats, Investigation Techniques and Practical Applications


Text Steganography
Cyber Security and Digital Forensics: Emerging Threats, Investigation Techniques and Practical Applications

One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(18,19) : Hands-on Session on Disk and File System Forensics using Forensic Explorer

DAY(03): WEDNESDAY date: 23/09/2026

The session provided participants with practical exposure to Disk and File System Forensics using Forensic Explorer. The focus was on understanding digital evidence stored on forensic disk images and file systems.

Disk & File System Forensics

Participants learned the basic process of examining digital storage media, file systems, files, folders, and associated digital artifacts during a forensic investigation.

Forensic Explorer

The session demonstrated the use of Forensic Explorer (FEX) for forensic examination and analysis. Participants were familiarized with exploring forensic evidence and examining relevant files and artifacts.

Hands-on Practical

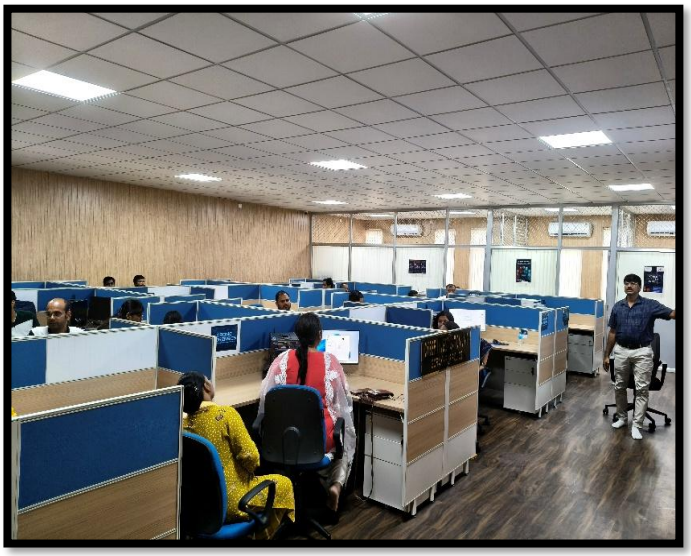
During the practical session, participants worked with forensic data and explored techniques for examining files, directories, file-system information, and digital artifacts using Forensic Explorer.

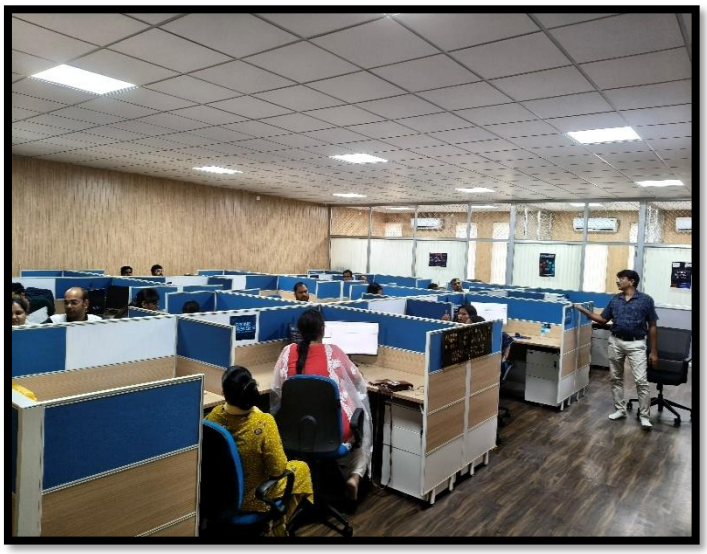
Forensic Analysis

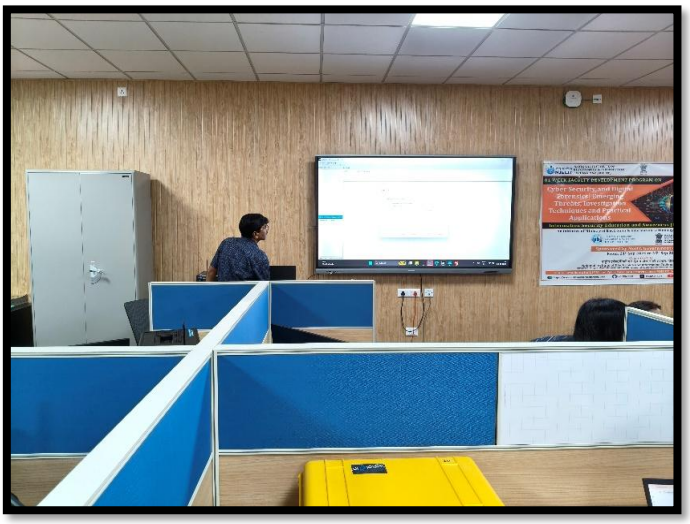
The practical activity highlighted the importance of systematic examination and documentation of digital evidence while conducting a forensic investigation.

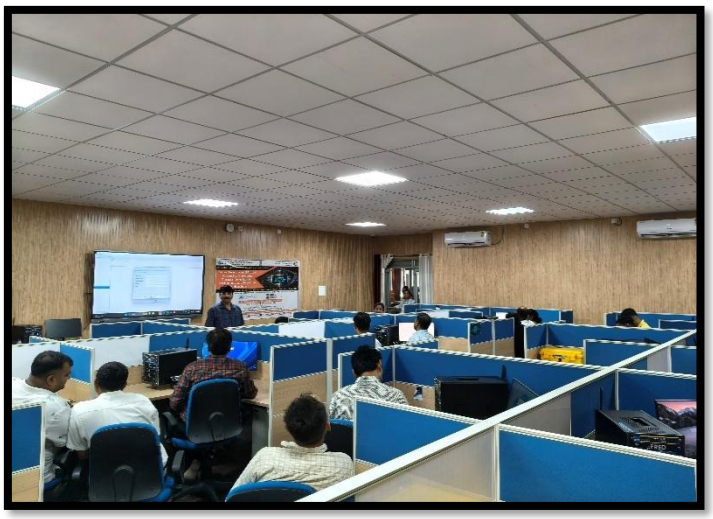
Conclusion

The session provided participants with hands-on understanding of disk and file system forensics using Forensic Explorer, strengthening their practical skills in digital evidence examination and forensic analysis.









One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(20) : Hands-on Session on Mobile Forensics using MSAB XRY

DAY(04): THURSDAY date: 24/09/2026

The session provided participants with practical exposure to Mobile Forensics using MSAB XRY. It focused on understanding the examination of digital evidence obtained from mobile devices during forensic investigations.

Mobile Forensics

Participants were introduced to the basic process of mobile evidence acquisition, examination, and analysis. The session highlighted the importance of systematic handling of mobile-device evidence during investigations.

MSAB XRY

The session demonstrated MSAB XRY as a mobile forensic tool and provided participants with an overview of its application in examining mobile-device data and supporting digital investigations.

Hands-on Practical

During the practical session, participants observed and explored the forensic examination process using MSAB XRY. The activity provided practical understanding of handling and analysing mobile forensic evidence in a controlled environment.

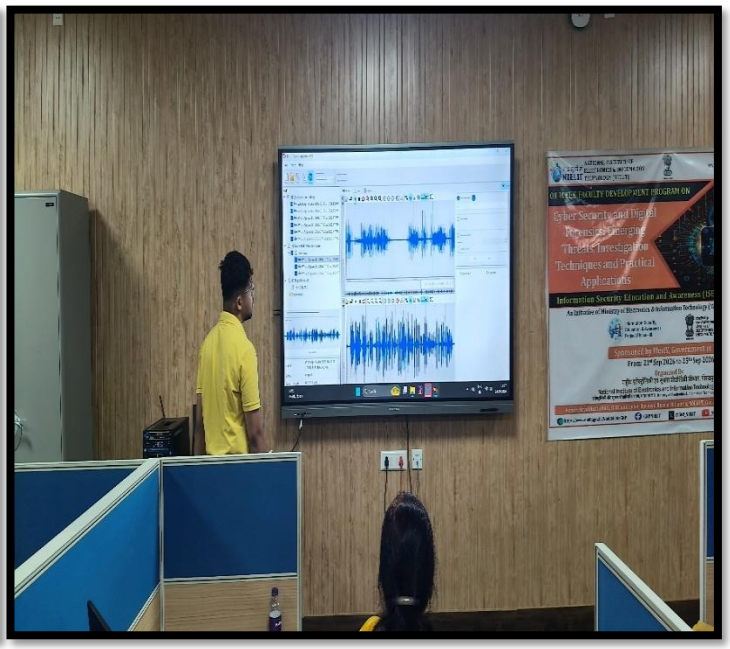
Forensic Investigation

The session emphasized proper evidence handling, examination, analysis, and documentation to support reliable findings during mobile forensic investigations.

Conclusion

The session provided participants with hands-on exposure to mobile forensics using MSAB XRY, strengthening their understanding of mobile-device evidence examination and digital investigation techniques.


Where can the Evidence be Located?
Data can be physically stored in 3 different locations
Some types of data may be found in more than one location, e.g.
Cyber Security and Digital Forensics: Emerging Threats, Investigation Techniques and Practical Applications


Cyber Security and Digital Forensics: Emerging Threats, Investigation Techniques and Practical Applications

One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(21) : Hands-on Session on Password Recovery and Decryption using Passware Tools

DAY(04): THURSDAY date: 24/09/2026

The session provided participants with practical exposure to password recovery and decryption using Passware tools. It focused on understanding the role of password recovery in digital forensic investigations.

Password Recovery & Decryption

Participants were introduced to the basic concepts of password-protected and encrypted digital evidence and the challenges involved in accessing such information during forensic examination.

Passware Tools

The session demonstrated the use of Passware tools for password recovery and decryption of supported digital files. Participants were familiarized with the forensic application of these tools in a controlled investigation environment.

Hands-on Practical

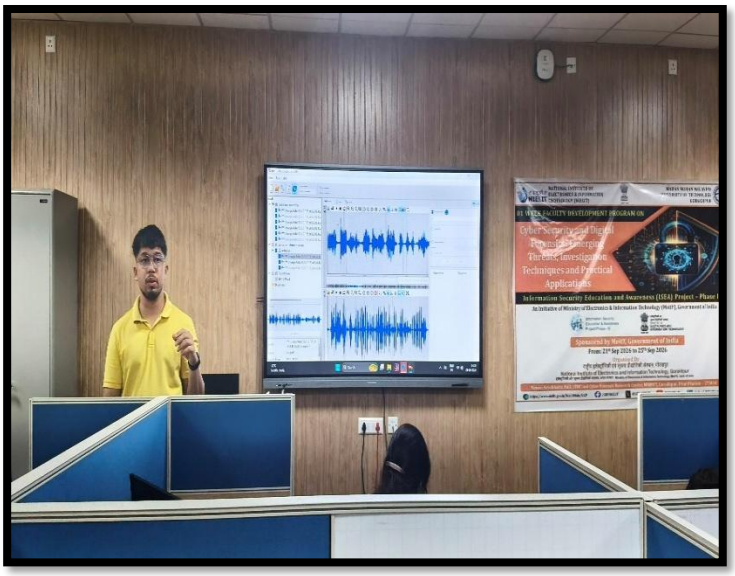
During the practical session, participants observed the process of examining protected files and understanding the workflow involved in password recovery and decryption. The activity emphasized proper handling and analysis of digital evidence.

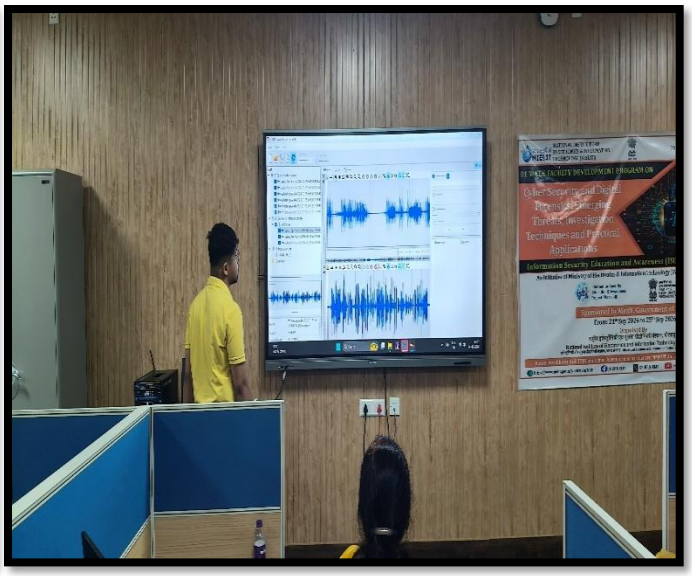
Forensic Relevance

The session highlighted how password recovery and decryption techniques can support investigators when dealing with protected or encrypted digital evidence during forensic investigations.

Conclusion

The session provided participants with practical exposure to password recovery and decryption using Passware tools, strengthening their understanding of handling protected digital evidence in forensic investigations.


Cyber Security and Digital Forensics: Emerging Threats, Investigative Techniques and Practical Applications
Information Security Education and Awareness (ISEA) Project - Phase


Cyber Security and Digital Forensics: Emerging Threats, Investigative Techniques and Practical Applications

One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(22,23) : Hands-on Session on Multimedia Forensics: Audio Forensics using Voice Inspector

DAY(04): THURSDAY date: 24/09/2026

The session provided participants with practical exposure to Multimedia Forensics, with a focus on the examination and analysis of audio evidence using Voice Inspector.

Audio Forensics

Participants were introduced to the basic concepts of audio evidence collection, examination, and analysis. The session highlighted the importance of audio analysis in digital investigations and forensic examination.

Voice Inspector

The session demonstrated Voice Inspector as a forensic tool for examining audio evidence. Participants were familiarized with the analysis of audio recordings and relevant characteristics that may support forensic investigation.

Hands-on Practical

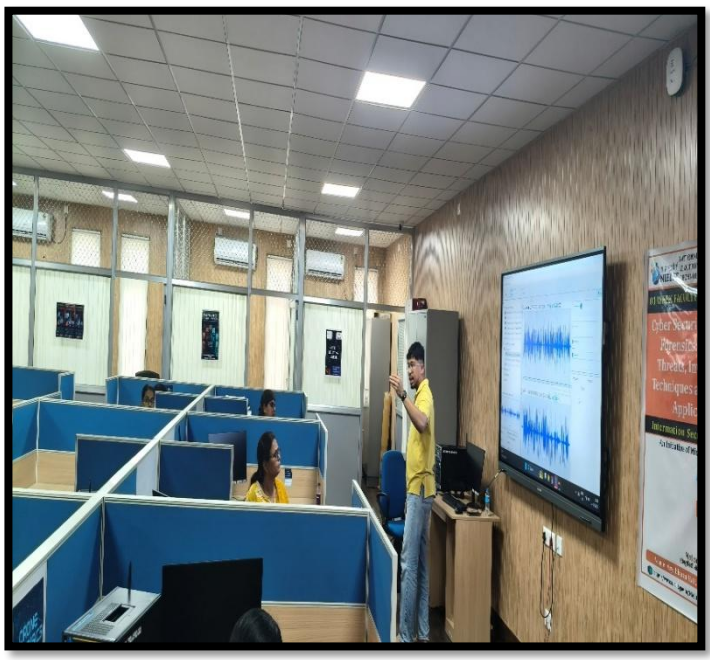
During the practical session, participants observed the workflow of audio forensic examination, including loading audio evidence, examining audio characteristics, and analysing relevant information in a controlled forensic environment.

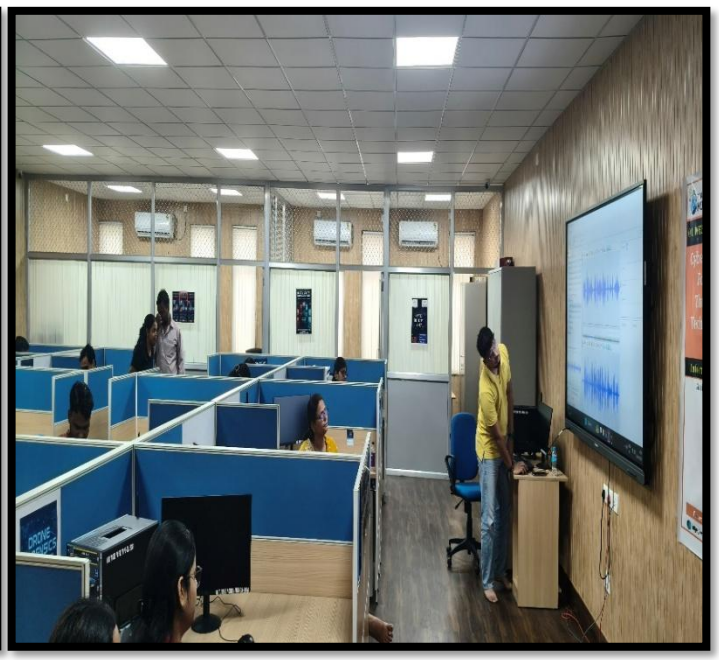
Forensic Applications

The session highlighted the use of audio forensics in digital investigations, evidence examination, and analysis of audio recordings.

Conclusion

The session provided participants with practical exposure to audio forensics using Voice Inspector, strengthening their understanding of multimedia evidence examination and forensic analysis.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(24,25) : Hands-on Session on Multimedia Forensics: Video Forensics using MD-Video

DAY(04): THURSDAY date: 24/09/2026

The session provided participants with practical exposure to Multimedia Forensics, focusing on the examination and analysis of video evidence using MD-Video.

Video Forensics

Participants were introduced to the basic concepts of video evidence examination and forensic analysis. The session highlighted the importance of analysing video material during digital investigations.

MD-Video

The session demonstrated MD-Video as a forensic tool for examining video evidence. Participants were familiarized with the forensic examination of video content and relevant information contained within video files.

Hands-on Practical

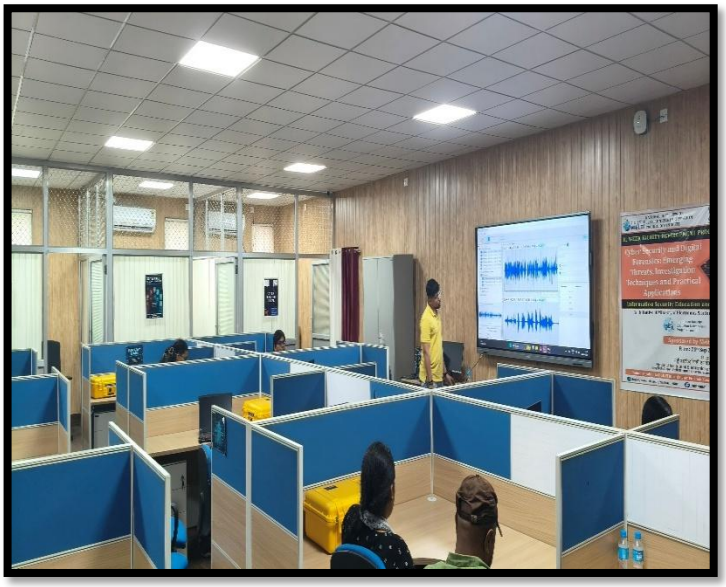
During the practical session, participants explored the basic workflow of video forensic examination, including working with video evidence and analysing relevant video information in a controlled forensic environment.

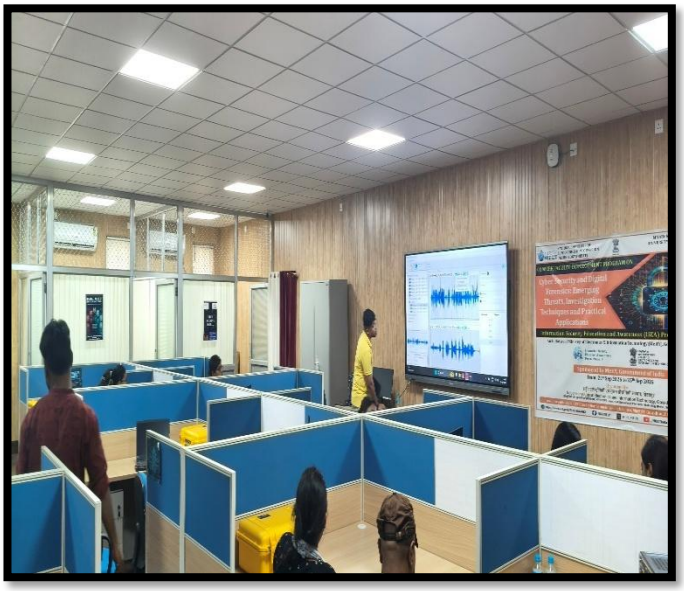
Forensic Applications

The session highlighted the application of video forensics in digital investigations, evidence examination, and analysis of multimedia evidence.

Conclusion

The session provided participants with hands-on exposure to video forensics using MD-Video, strengthening their understanding of multimedia evidence examination and forensic analysis.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(26,27) : Hands-on Session on Steganography using StegoHunt and Other Forensic Tools

DAY(04): THURSDAY date: 24/09/2026

The session provided participants with practical exposure to Steganography and digital forensic analysis using StegoHunt and other forensic tools. It focused on understanding how hidden information may be detected and examined in digital media.

Steganography

Participants learned the concept of concealing information within digital media such as images, audio, or other files. The session highlighted its relevance to digital investigations.

StegoHunt & Forensic Tools

The session demonstrated StegoHunt and other forensic tools for examining suspected files and identifying possible hidden information or steganographic content.

Hands-on Practical

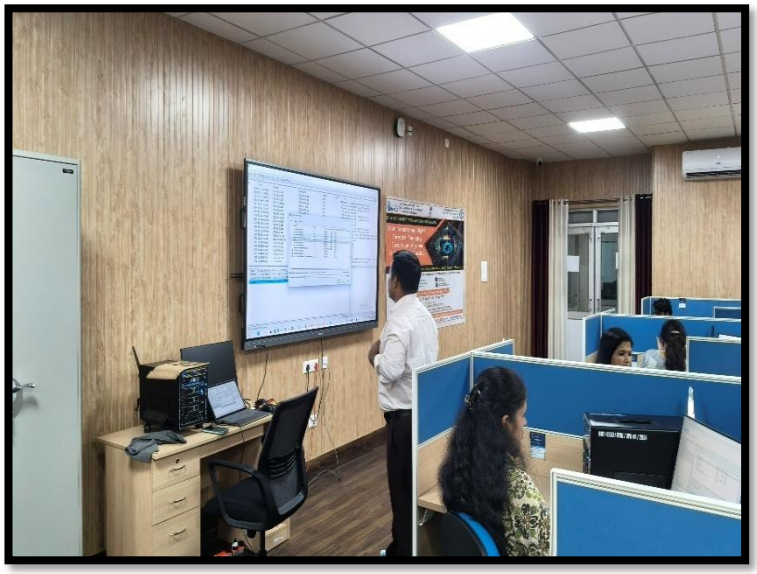
During the practical session, participants worked with sample digital files and explored the basic process of examining, detecting, and analysing potential hidden data in a controlled forensic environment.

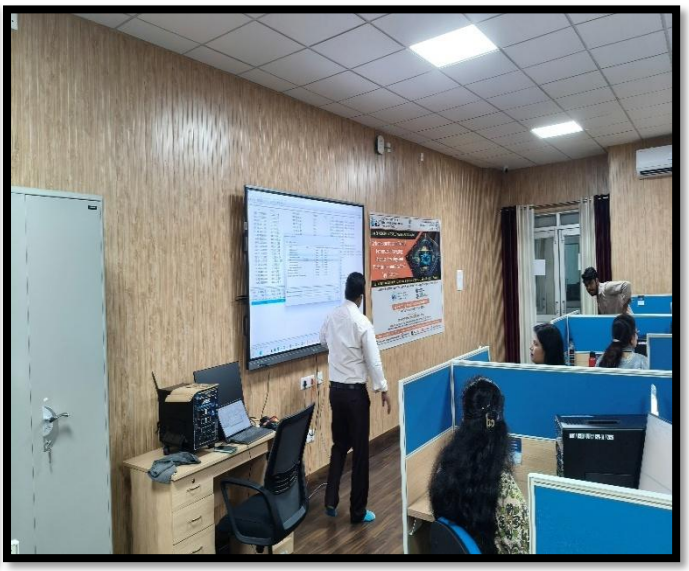
Forensic Applications

The practical activity demonstrated the relevance of steganography analysis in digital evidence examination, cybercrime investigation, and forensic analysis.

Conclusion

The session provided participants with hands-on understanding of steganography detection and analysis using StegoHunt and other forensic tools, strengthening their practical digital forensic skills.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(28,29) : Hands-on Session on Network Forensics: Demonstration Using Wireshark, Network Miner, and Other Forensic Tools

DAY(05): FRIDAY date: 25/09/2026

The session provided participants with practical exposure to Network Forensics and the examination of network-related digital evidence using forensic tools.

Network Forensics

Participants were introduced to the basic concepts of network traffic analysis, packet examination, and identification of relevant network evidence during digital investigations.

Wireshark & NetworkMiner

The session demonstrated Wireshark and NetworkMiner for examining network traffic and analysing available network information. Participants were familiarized with the role of these tools in network forensic investigations.

Hands-on Practical

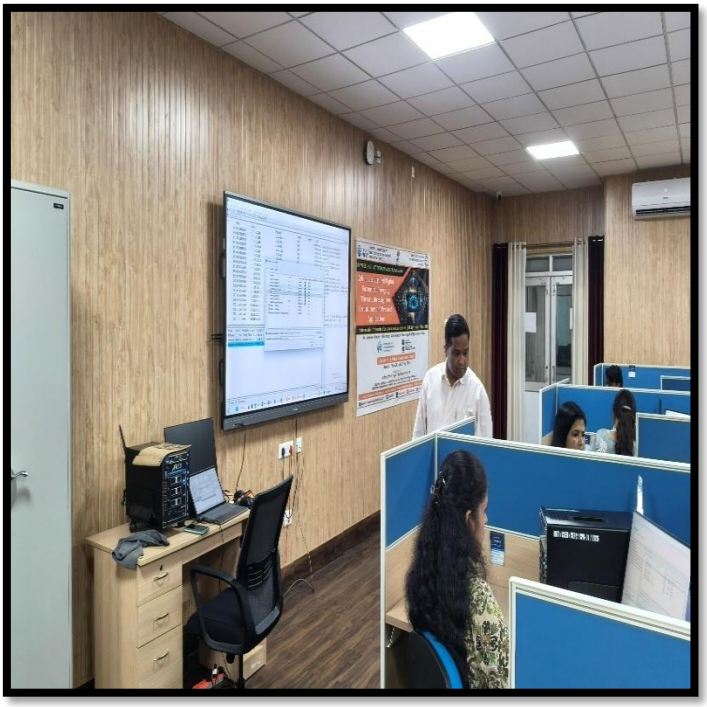
During the practical session, participants observed the process of capturing and analysing network traffic, examining packets, and identifying relevant network information using the demonstrated forensic tools.

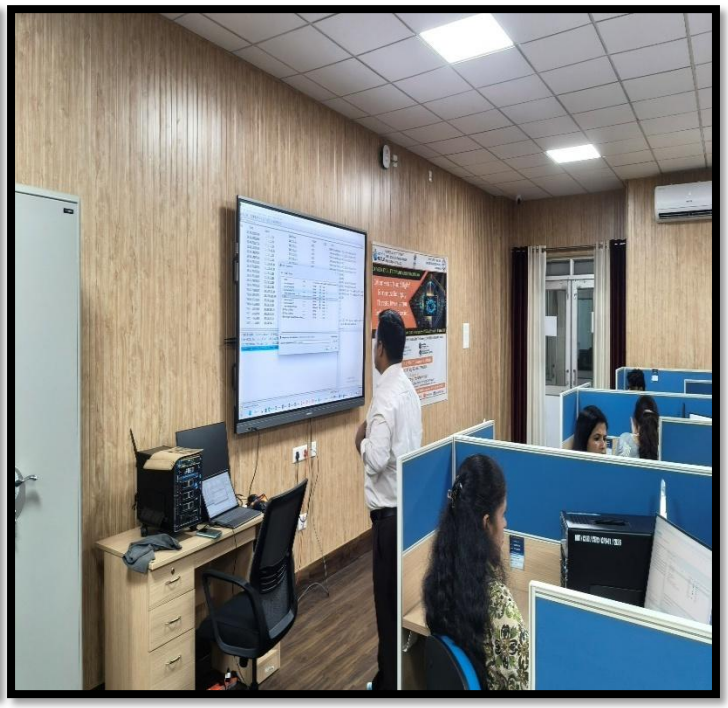
Forensic Applications

The session highlighted the application of network forensics in cybercrime investigation, incident analysis, network monitoring, and digital evidence examination.

Conclusion

The session provided participants with hands-on exposure to network forensic investigation using Wireshark, NetworkMiner, and other forensic tools, strengthening their practical understanding of network evidence analysis.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(30) : Anti-Forensics

DAY(05): FRIDAY date: 25/09/2026

The session introduced participants to the concept of Anti-Forensics and its relevance to digital investigations. It focused on understanding techniques that may affect the availability, visibility, or integrity of digital evidence.

Concept of Anti-Forensics

Participants learned how anti-forensic activities can be used to hide, alter, remove, or make digital evidence more difficult to identify and analyse during a forensic investigation.

Impact on Digital Investigation

The session highlighted the challenges investigators may face when examining digital evidence affected by anti-forensic activities. Participants learned the importance of careful examination and identification of potential evidence manipulation.

Forensic Approach

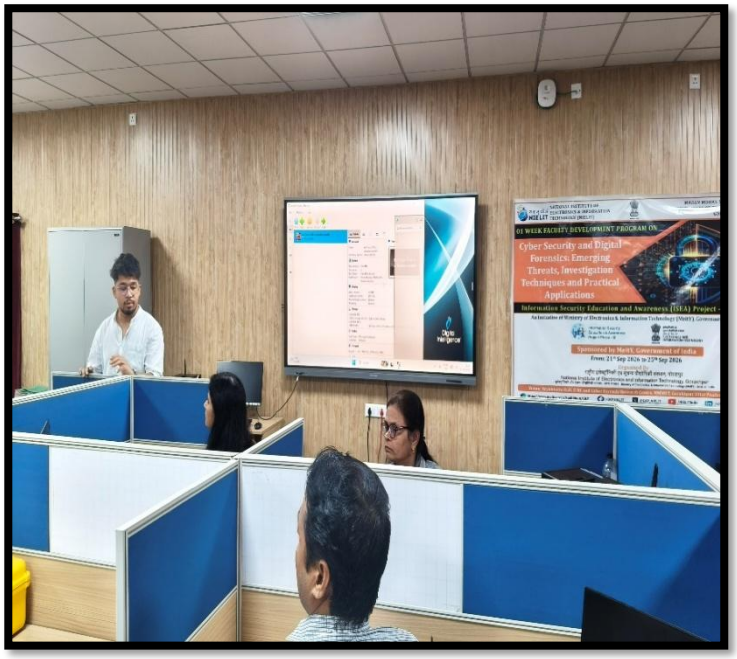
The session emphasized the need for systematic evidence examination, proper documentation, and identification of indicators of evidence alteration or concealment during forensic investigations.

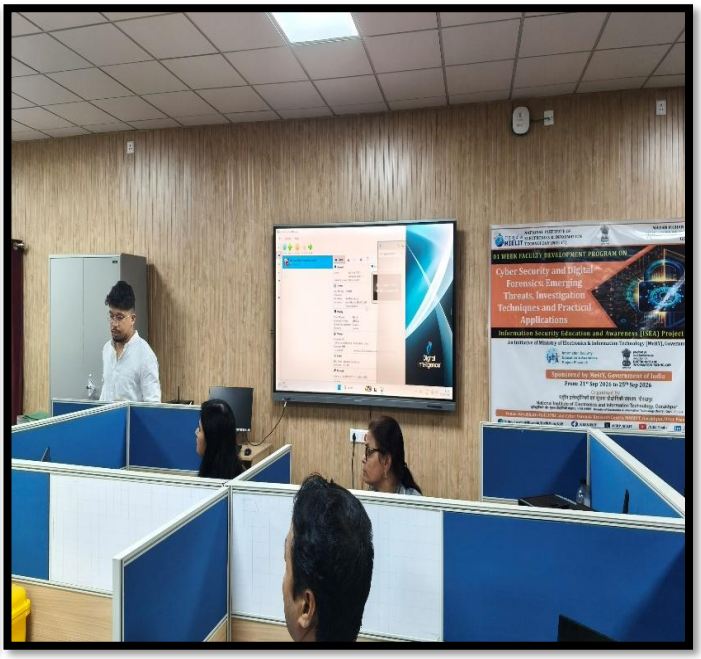
Practical Relevance

Understanding anti-forensics helps forensic investigators recognize potential attempts to conceal or manipulate digital evidence and consider such possibilities during evidence analysis.

Conclusion

The session provided participants with an understanding of anti-forensics, its impact on digital evidence, and the challenges it presents during forensic investigations.


01 WEEK FACULTY DEVELOPMENT PROGRAM ON
Cyber Security and Digital Forensics: Emerging Threats, Investigation Techniques and Practical Applications
Information Security Education and Awareness (ISEA) Project
Sponsored by MeitY, Government of India
From 21st Sep 2026 to 25th Sep 2026


01 WEEK FACULTY DEVELOPMENT PROGRAM ON
Cyber Security and Digital Forensics: Emerging Threats, Investigation Techniques and Practical Applications
Information Security Education and Awareness (ISEA) Project
Sponsored by MeitY, Government of India
From 21st Sep 2026 to 25th Sep 2026

One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(31) : Hands-on Session on Cryptocurrency Forensics and Analysis using Breadcrumbs

DAY(05): FRIDAY date: 25/09/2026

The session provided participants with practical exposure to Cryptocurrency Forensics and the analysis of cryptocurrency-related digital evidence using Breadcrumbs.
.

Cryptocurrency Forensics

Participants were introduced to the fundamentals of cryptocurrency transactions, blockchain-based evidence, and transaction analysis in the context of digital investigations.

Breadcrumbs

The session demonstrated Breadcrumbs as a blockchain intelligence and forensic analysis tool. Participants were familiarized with analysing cryptocurrency transactions and tracing relevant blockchain information.

Hands-on Practical

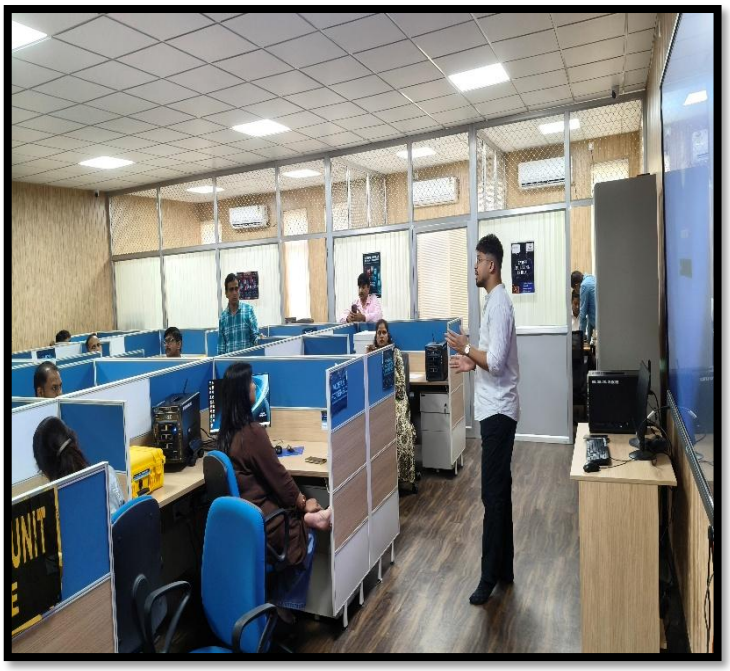
During the practical session, participants explored the basic process of examining cryptocurrency transactions, analysing blockchain data, and identifying relevant transaction information using Breadcrumbs.

Forensic Applications

The session highlighted the application of cryptocurrency forensics in cybercrime investigation, blockchain analysis, financial investigations, and digital evidence examination.

Conclusion

The session provided participants with hands-on understanding of cryptocurrency forensics and blockchain transaction analysis using Breadcrumbs, strengthening their practical skills in digital investigations.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(32) : Hands-on Session on Drone Forensics using MD- Drone

DAY(05): FRIDAY date: 25/09/2026

The session provided participants with practical exposure to Drone Forensics and the examination of drone-related digital evidence using MD-Drone.

Drone Forensics

Participants were introduced to the role of drone-related data and digital evidence in forensic investigations. The session focused on understanding the examination of information associated with drone activities.

MD-Drone

The session demonstrated MD-Drone as a forensic tool for examining drone-related evidence. Participants were familiarized with the forensic analysis process in a controlled environment.

Hands-on Practical

During the practical session, participants explored the basic workflow of drone evidence examination and analysis using MD-Drone, gaining practical understanding of handling and interpreting relevant forensic information.

Forensic Applications

The session highlighted the relevance of drone forensics in digital investigations, evidence examination, and analysis of drone-related data.

Conclusion

The session provided participants with hands-on exposure to drone forensics using MD-Drone, strengthening their understanding of emerging areas of digital forensic investigation.





One-Week Faculty Development Training Programme on Cyber Security and Digital Forensics

Organized by: Cyber Forensics Research Centre, Department of Computer Science & Engineering, (MMMUT), Gorakhpur
In Collaboration with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur

Session(33) : Hands-on Session on Social Media Forensics using X1 Social Discovery

DAY(05): FRIDAY date: 25/09/2026

The session provided participants with practical exposure to Social Media Forensics and the examination of social media-related digital evidence using X1 Social Discovery.

Social Media Forensics

Participants were introduced to the importance of collecting, examining, and analysing information from social media sources during digital investigations. The session focused on understanding social media data as a potential source of digital evidence.

X1 Social Discovery

The session demonstrated X1 Social Discovery as a forensic tool for examining and organizing social media-related information. Participants were familiarized with its use in the investigation and analysis of digital evidence.

Hands-on Practical

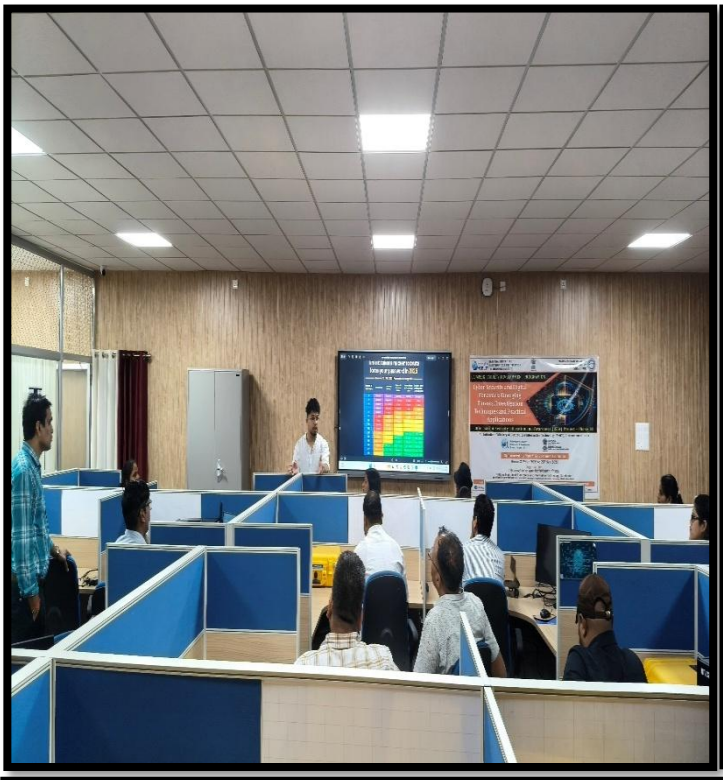
During the practical session, participants explored the basic process of collecting and analysing social media information, reviewing relevant digital content, and organizing findings for forensic examination.

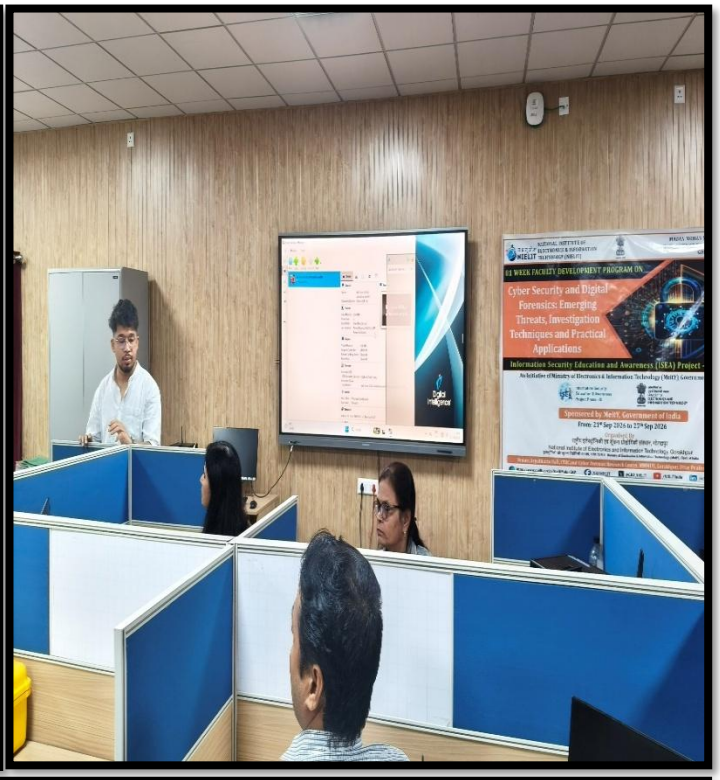
Forensic Applications

The session highlighted the application of social media forensics in cybercrime investigation, digital evidence analysis, and investigation of online activities.

Conclusion

The session provided participants with hands-on understanding of social media forensics using X1 Social Discovery, strengthening their practical skills in examining and analysing social media-related digital evidence.




01 WEEK FACULTY DEVELOPMENT PROGRAM ON
Cyber Security and Digital Forensics: Emerging Threats, Investigation Techniques and Practical Applications
Information Security Education and Awareness (ISEA) Project -
Sponsored by MeitY, Government of India
From: 23rd Sep 2024 to 27th Sep 2024


Resource Person


ONE WEEK FACULTY DEVELOPMENT PROGRAM ON
Cyber Security and Digital Forensics: Emerging Threats, Investigation Techniques and Practical Applications
Information Security Education and Awareness (ISEA) Project – Phase III


Resource Person
10+ Years of Work Experience
Networking & Infrastructure
Cyber Security
Windows Server Administration
Linux Server Administration
Infrastructure Security and Monitoring
Switches & Network Devices Management
Storage & Disaster Recovery
Troubleshooting & Documentation
Siddhant
System Ad
NIELIT Go
BCA, ME
ISEA


Resource Person
Project Associate under the ISEA Project Phase-III at NIELIT Gorakhpur, with expertise in Cyber Security, network and web application security, ethical hacking, vulnerability assessment, Cyber Security with Python and technical content development.
Responsibilities include CISO content development, ISEA-related training and project activities, and coordination and execution of various programmes such as Cyber Security Bootcamps, internship Programmes, Faculty Development Programmes (FDPs), short-term training programmes, and cybersecurity awareness initiatives.
Also involved in the development of training content, MCQs, laboratory manuals, and practical cybersecurity exercises for academic and professional training programmes.
Actively involved in B.Tech. teaching and academic activities, delivering classes and supporting students in technical and cybersecurity-related subjects.
Prashant Kumar Tripathi
M.Tech. (CSE)
NIELIT
ISEA
Information Security Education & Awareness Project Phase - III
Ministry of Electronics and Information Technology ,Government of India


01 WEEK FACULTY DEVELOPMENT PROGRAM ON
Cyber Security and Digital Forensics: Emerging Threats, Investigation Techniques and Practical Applications
Madan Mohan Malaviya University of Technology (MMMUT), Gorakhpur
&
National Institute of Electronics & Information Technology (NIELIT), Gorakhpur
NIELIT
Sponsored by
ISEA