SIX-WEEK SUMMER INTERNSHIP TRAINING PROGRAM | CYBER SECURITY & DIGITAL FORENSICS

Cyber Forensics Research Centre | Dept. of CSE, MMMUT Gorakhpur | In collaboration with Cyint Technologies, New Delhi | 11 June – 21 July 2026

Mode: Offline (On-Campus) | Classes: Monday to Friday

Programme Dates : 11-06-2026 to 21-07-2026 | Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT

Daily Session Timings (fill once – applies to all 30 days):

CYBER SECURITY & DIGITAL FORENSICS | MMMUT Gorakhpur | 11 June – 21 July 2026

Mode: Offline (On-Campus) | Classes: Monday to Friday

DAY - 01

The first day of the Six-Week Summer Internship Training Program focused on introducing participants to advanced multimedia analysis tools, specifically MD-Video and Voice Inspector powered by Phonexia technology. The session emphasized the growing significance of audio-video forensics in cyber investigations and digital evidence analysis. Participants were familiarized with the capabilities, applications, and practical relevance of these tools in modern forensic workflows. The primary objective of the session was to establish a strong foundation in multimedia forensic analysis and prepare participants for the advanced topics and hands-on exercises scheduled in the subsequent weeks of the program.

The inaugural session was graced by distinguished dignitaries, including **Prof. Anupama Kaushik Sharma**, **Vice-chancellor (VC), Shri Chandra Prakash Priyadarshi**, Registrar, Madan Mohan Malaviya University of Technology (MMMUT), Gorakhpur, and **Dr. Rakesh Kumar**, Head and Professor, Department of Computer Science & Engineering. The esteemed guests shared valuable insights into the growing role of **Technology, cyber security, and digital forensics** in addressing modern challenges and enhancing investigative capabilities. The program was effectively coordinated by **Dr. B.K.Sharma**, Associate Professor, and **Dr. Vimal Kumar**, Assistant Professor, whose dedicated efforts ensured the smooth planning, organization, and successful execution of the training program.The technical sessions were conducted by **Mr. Naveen Singh** and **Mr. Aniket Sahu**, who provided expert guidance, practical demonstrations, and hands-on training throughout the day. Their sessions enabled participants to gain a comprehensive understanding of **Advanced multimedia forensic tools** and their applications in **Cyber investigations** and **Digital Evidence Analysis**.










CYBER SECURITY &
DIGITAL FORENSICS



DAY -01

WORKSHOP: FUNDAMENTALS OF DIGITAL FORENSICS

Introduction

A focused training session on Fundamentals of Digital Forensics was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Fundamentals of Digital Forensics.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Fundamentals of Digital Forensics
- Date: 11 Jun (Thu)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Fundamentals of Digital Forensics. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Fundamentals of Digital Forensics, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Fundamentals of Digital Forensics.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

The session strengthened participants' understanding of Fundamentals of Digital Forensics and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on Fundamentals of Digital Forensics was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.





DAY -02

WORKSHOP: EVIDENCE LIFECYCLE & FORENSIC PRINCIPLES

Introduction

A focused training session on Evidence Lifecycle & Forensic Principles was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Evidence Lifecycle & Forensic Principles.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Evidence Lifecycle & Forensic Principles
- Date: 12 Jun (Fri)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Evidence Lifecycle & Forensic Principles. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Evidence Lifecycle & Forensic Principles, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Evidence Lifecycle & Forensic Principles.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

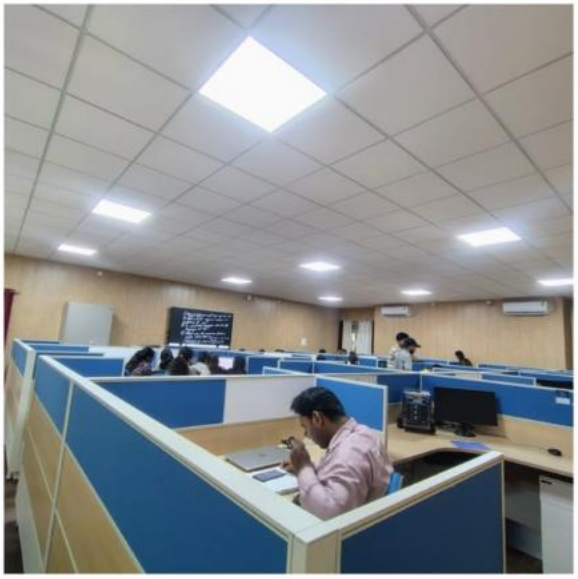
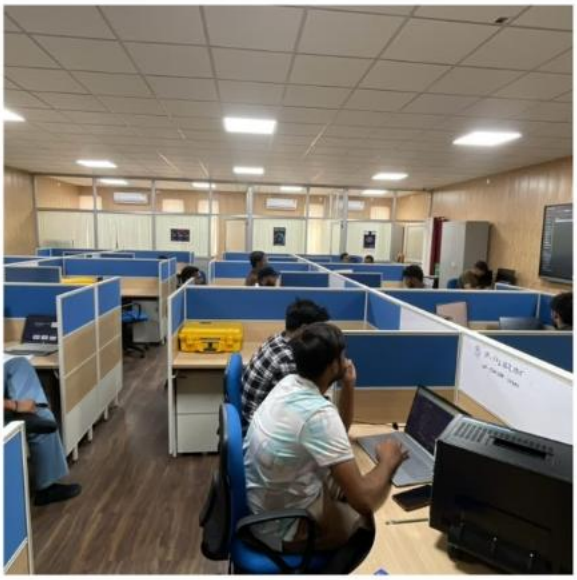
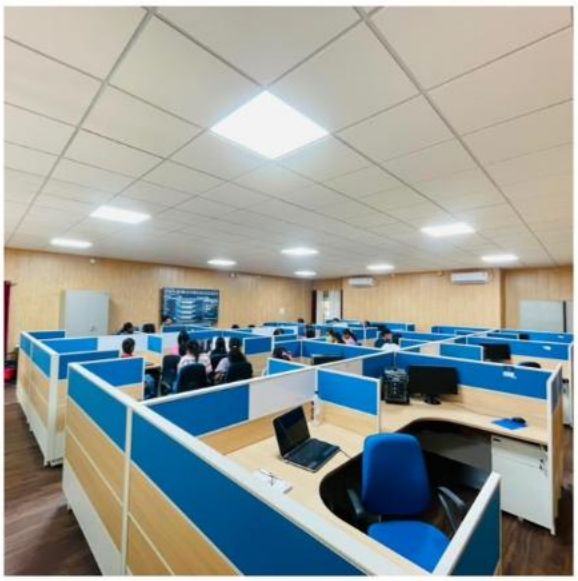
The session strengthened participants' understanding of Evidence Lifecycle & Forensic Principles and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on Evidence Lifecycle & Forensic Principles was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience


DAY -03

WORKSHOP: FORENSIC INVESTIGATION METHODOLOGY

Introduction

A focused training session on Forensic Investigation Methodology was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Forensic Investigation Methodology.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Forensic Investigation Methodology
- Date: 15 Jun (Mon)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Forensic Investigation Methodology. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Forensic Investigation Methodology, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Forensic Investigation Methodology.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

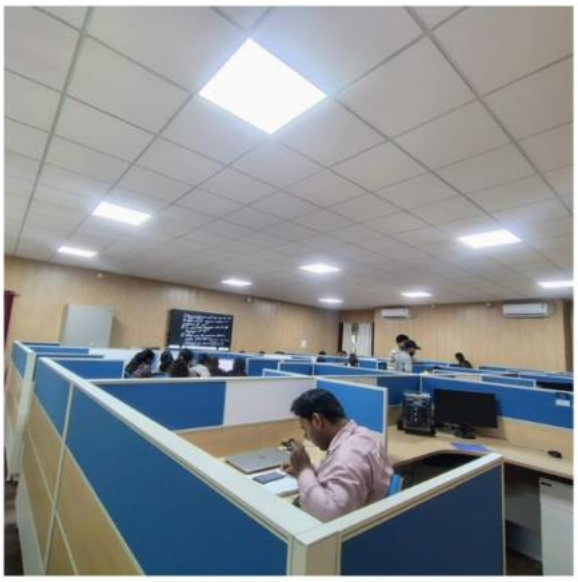
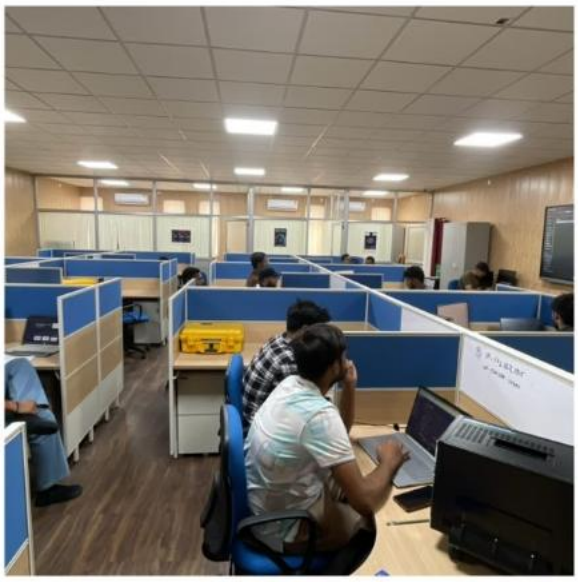
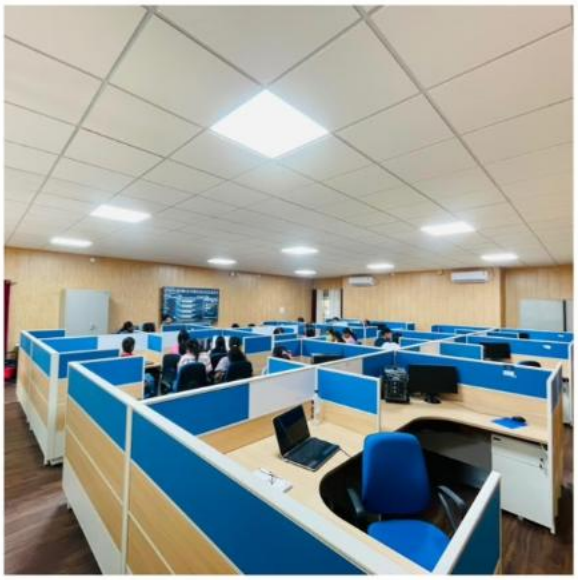
The session strengthened participants' understanding of Forensic Investigation Methodology and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on Forensic Investigation Methodology was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.


DAY -04

WORKSHOP: TYPES OF CYBERCRIME & FORENSIC DOMAINS

Introduction

A focused training session on Types of Cybercrime & Forensic Domains was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Types of Cybercrime & Forensic Domains.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Types of Cybercrime & Forensic Domains
- Date: 16 Jun (Tue)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Types of Cybercrime & Forensic Domains. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Types of Cybercrime & Forensic Domains, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Types of Cybercrime & Forensic Domains.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

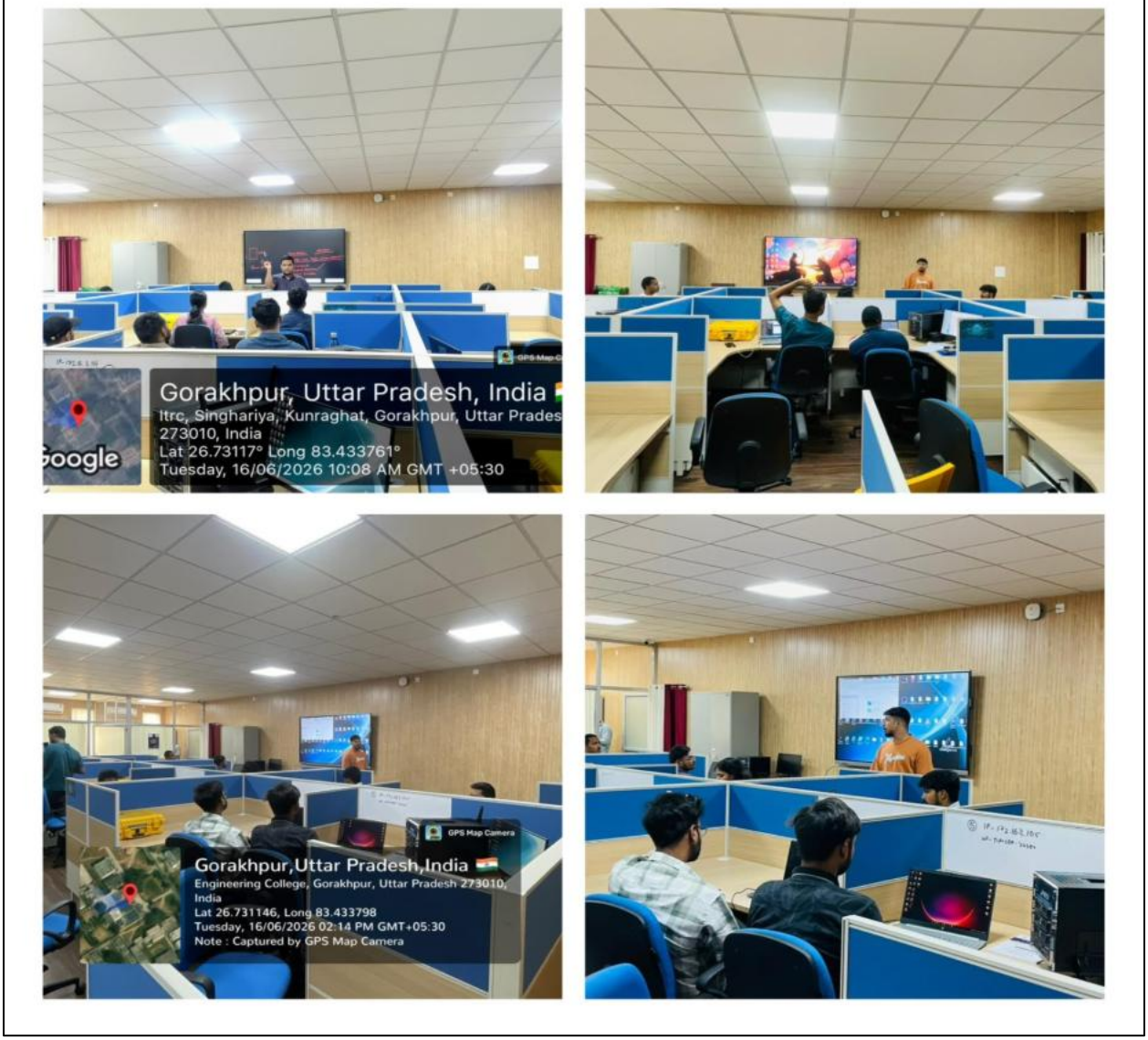
The session strengthened participants' understanding of Types of Cybercrime & Forensic Domains and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on Types of Cybercrime & Forensic Domains was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.



DAY -05

WORKSHOP: LAB SETUP & EVIDENCE HANDLING SOPS

Introduction

A focused training session on Lab Setup & Evidence Handling SOPs was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Lab Setup & Evidence Handling SOPs.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Lab Setup & Evidence Handling SOPs
- Date: 17 Jun (Wed)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Lab Setup & Evidence Handling SOPs. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Lab Setup & Evidence Handling SOPs, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Lab Setup & Evidence Handling SOPs.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

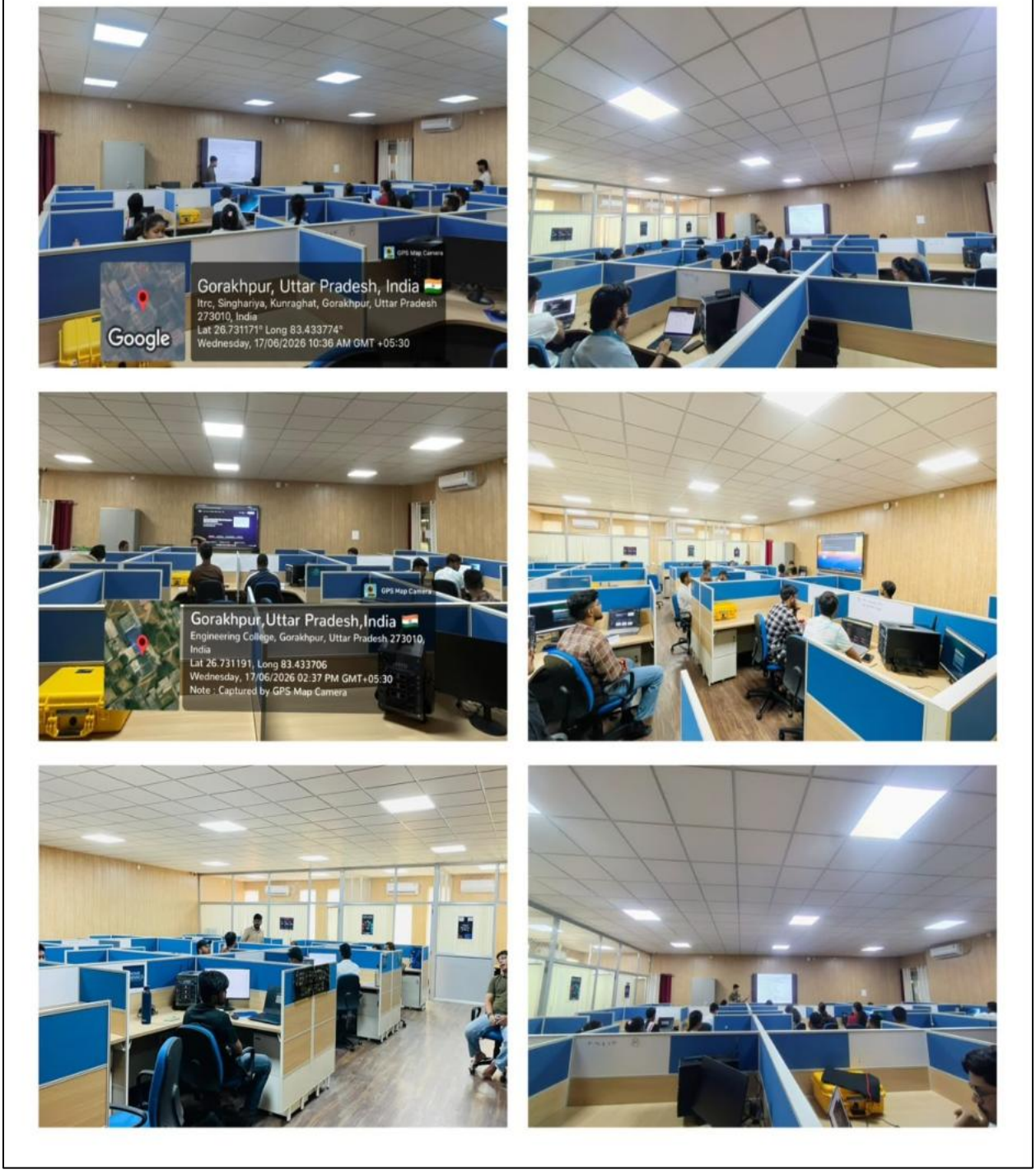
The session strengthened participants' understanding of Lab Setup & Evidence Handling SOPs and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on Lab Setup & Evidence Handling SOPs was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.



DAY -06

WORKSHOP: CHAIN OF CUSTODY & DOCUMENTATION

Introduction

A focused training session on Chain of Custody & Documentation was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Chain of Custody & Documentation.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Chain of Custody & Documentation
- Date: 18 Jun (Thu)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Chain of Custody & Documentation. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Chain of Custody & Documentation, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Chain of Custody & Documentation.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

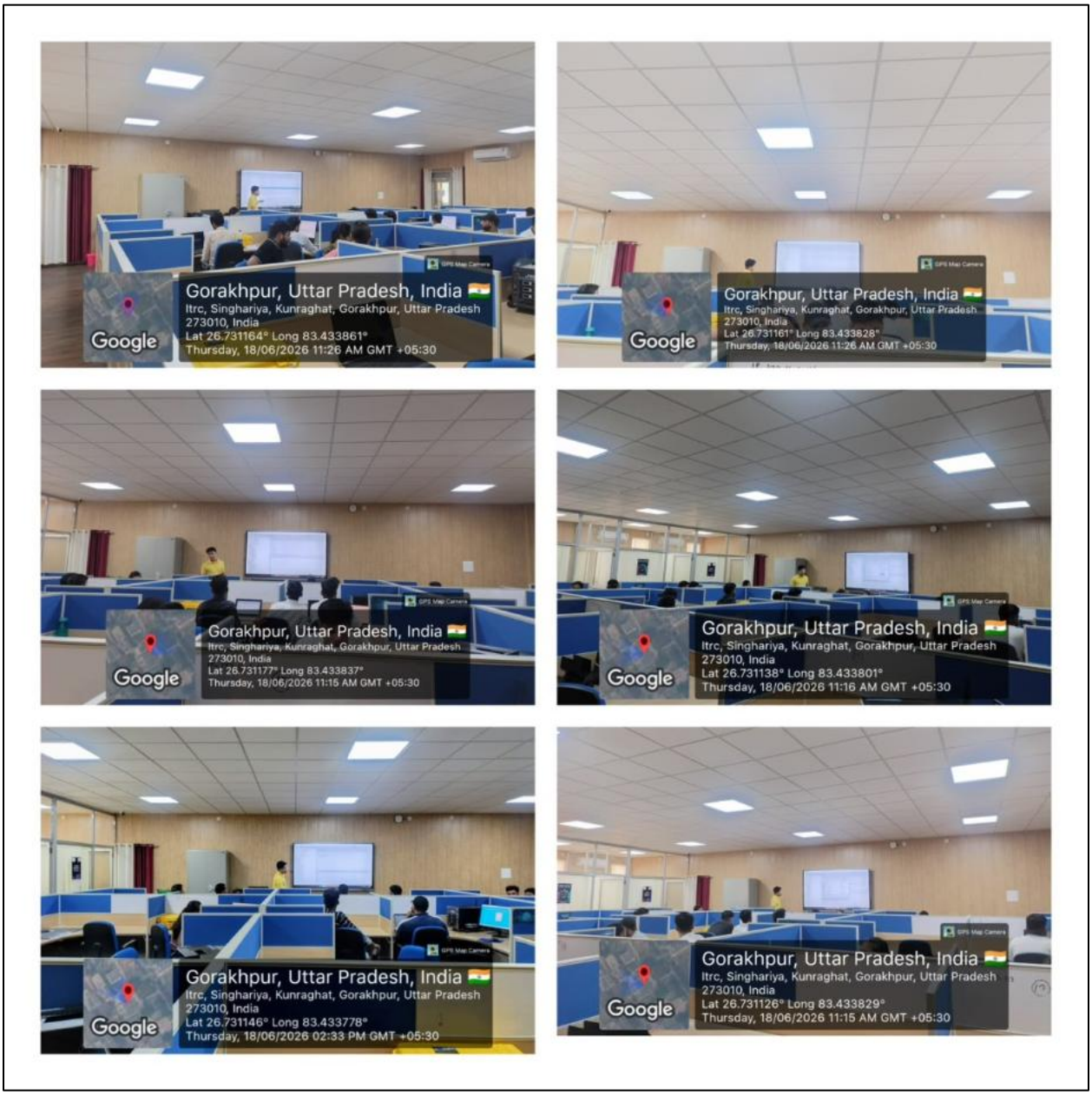
The session strengthened participants' understanding of Chain of Custody & Documentation and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on Chain of Custody & Documentation was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.



DAY -07

WORKSHOP: EVIDENCE PRESERVATION & STORAGE

Introduction

A focused training session on Evidence Preservation & Storage was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Evidence Preservation & Storage.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Evidence Preservation & Storage
- Date: 19 Jun (Fri)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Evidence Preservation & Storage. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Evidence Preservation & Storage, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Evidence Preservation & Storage.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

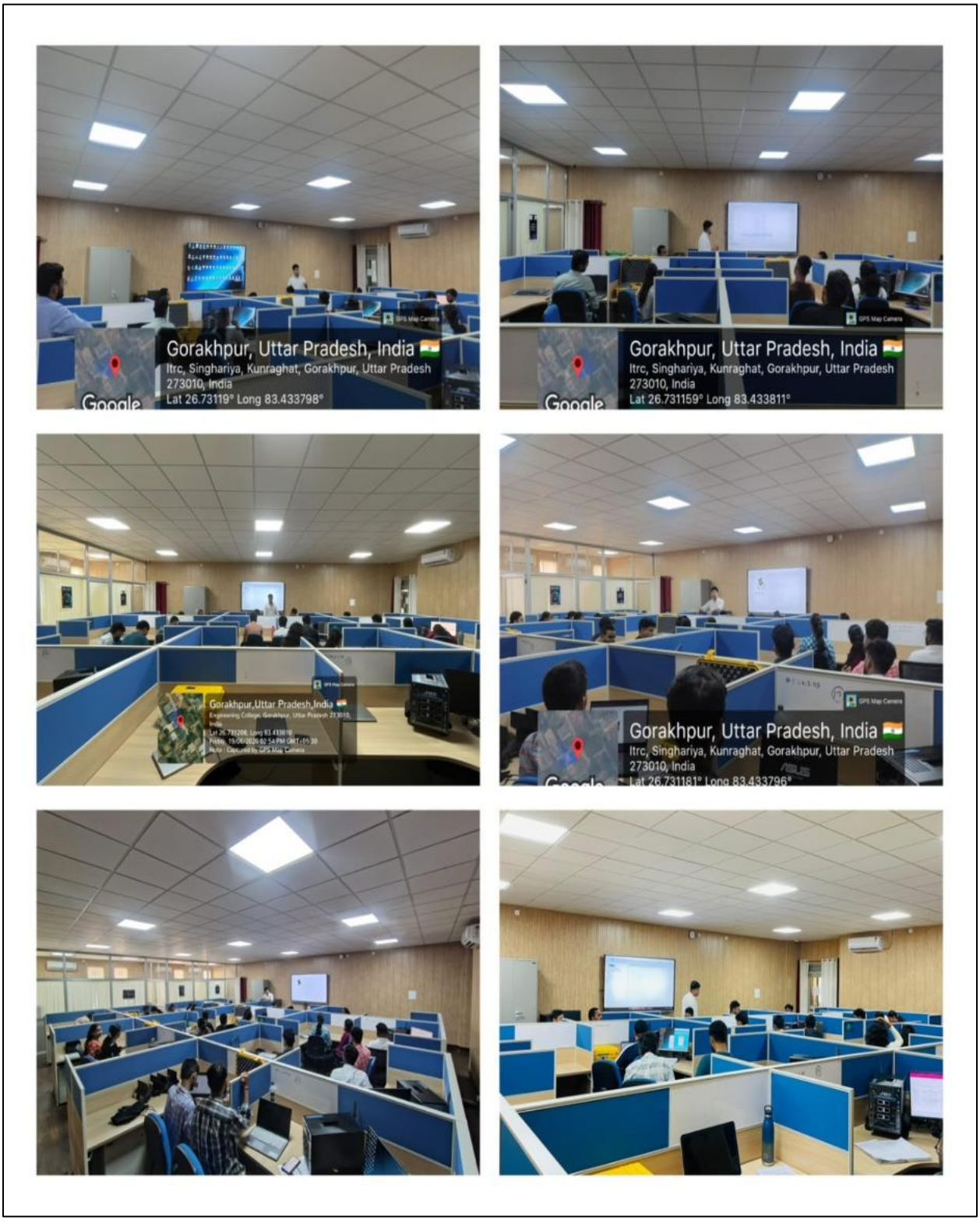
The session strengthened participants' understanding of Evidence Preservation & Storage and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on Evidence Preservation & Storage was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.



DAY -08

WORKSHOP: DISK FORENSICS – IMAGING & HASHING

Introduction

A focused training session on Disk Forensics – Imaging & Hashing was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Disk Forensics – Imaging & Hashing.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Disk Forensics – Imaging & Hashing
- Date: 22 Jun (Mon)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Disk Forensics – Imaging & Hashing. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Disk Forensics – Imaging & Hashing, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Disk Forensics – Imaging & Hashing.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

The session strengthened participants' understanding of Disk Forensics – Imaging & Hashing and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

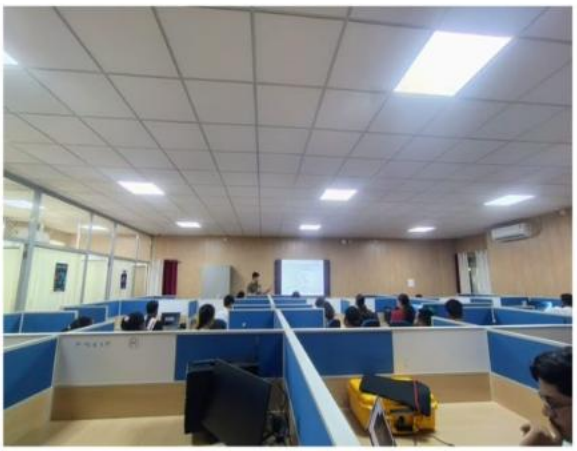
Conclusion

The session on Disk Forensics – Imaging & Hashing was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.





DAY -09

WORKSHOP: FILE SYSTEM ANALYSIS & ARTIFACT RECOVERY

Introduction

A focused training session on File System Analysis & Artifact Recovery was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of File System Analysis & Artifact Recovery.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: File System Analysis & Artifact Recovery
- Date: 23 Jun (Tue)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of File System Analysis & Artifact Recovery. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to File System Analysis & Artifact Recovery, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of File System Analysis & Artifact Recovery.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

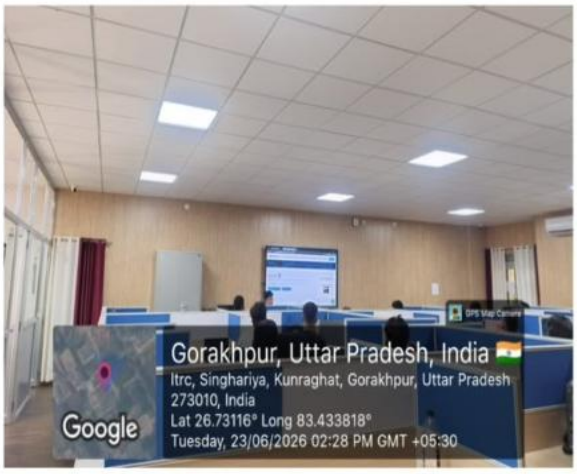
The session strengthened participants' understanding of File System Analysis & Artifact Recovery and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

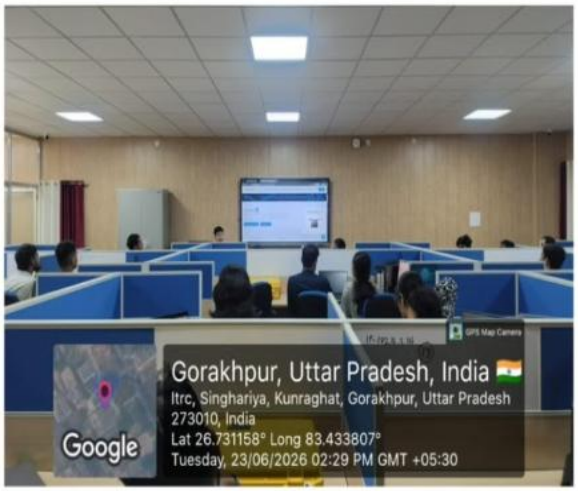
Conclusion

The session on File System Analysis & Artifact Recovery was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

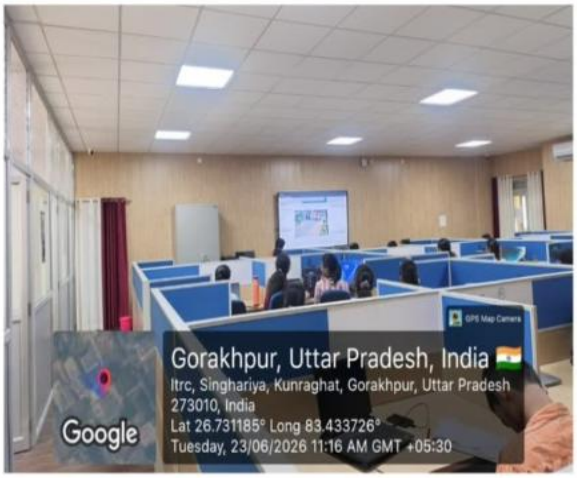
I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience

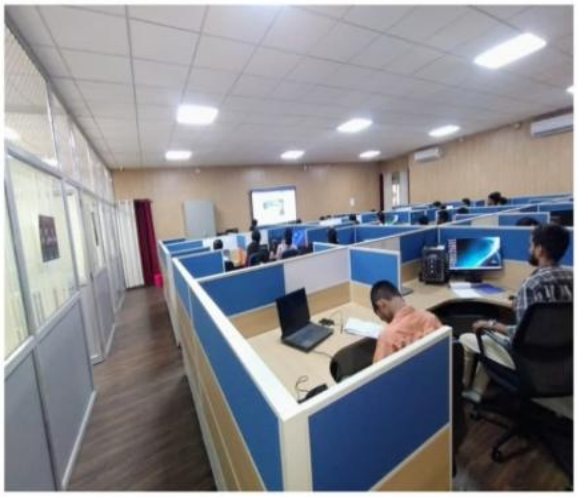












.

DAY -10

WORKSHOP: ENCRYPTED DRIVES & ANTI-FORENSICS

Introduction

A focused training session on Encrypted Drives & Anti-Forensics was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Encrypted Drives & Anti-Forensics.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Encrypted Drives & Anti-Forensics
- Date: 24 Jun (Wed)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Encrypted Drives & Anti-Forensics. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Encrypted Drives & Anti-Forensics, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Encrypted Drives & Anti-Forensics.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

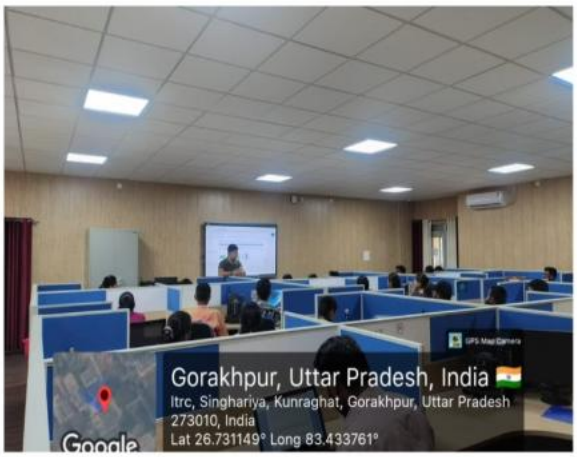
The session strengthened participants' understanding of Encrypted Drives & Anti-Forensics and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

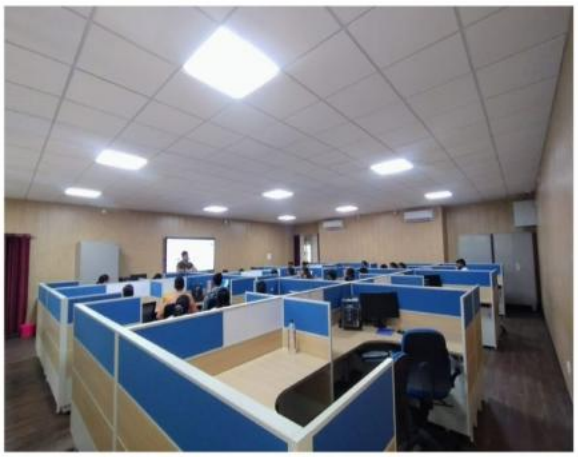
Conclusion

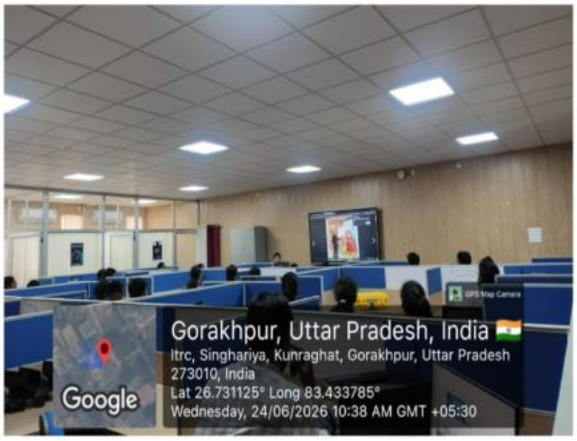
The session on Encrypted Drives & Anti-Forensics was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.

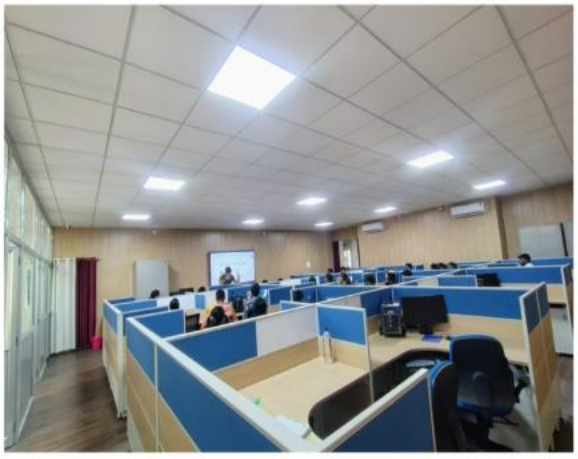












DAY -11

WORKSHOP: COMPUTER FORENSICS – CASE STUDY & REVIEW

Introduction

A focused training session on Computer Forensics – Case Study & Review was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Computer Forensics – Case Study & Review.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Computer Forensics – Case Study & Review
- Date: 25 Jun (Thu)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Computer Forensics – Case Study & Review. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Computer Forensics – Case Study & Review, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Computer Forensics – Case Study & Review.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

The session strengthened participants' understanding of Computer Forensics – Case Study & Review and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on Computer Forensics – Case Study & Review was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.



DAY -12

WORKSHOP: MOBILE FORENSICS – FUNDAMENTALS & ACQUISITION

Introduction

A focused training session on Mobile Forensics – Fundamentals & Acquisition was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Mobile Forensics – Fundamentals & Acquisition.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Mobile Forensics – Fundamentals & Acquisition
- Date: 26 Jun (Fri)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Mobile Forensics – Fundamentals & Acquisition. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Mobile Forensics – Fundamentals & Acquisition, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Mobile Forensics – Fundamentals & Acquisition.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

The session strengthened participants' understanding of Mobile Forensics – Fundamentals & Acquisition and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on Mobile Forensics – Fundamentals & Acquisition was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.



DAY -13

WORKSHOP: SIM, MEMORY & APP DATA ANALYSIS

Introduction

A focused training session on SIM, Memory & App Data Analysis was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of SIM, Memory & App Data Analysis.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: SIM, Memory & App Data Analysis
- Date: 29 Jun (Mon)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of SIM, Memory & App Data Analysis. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to SIM, Memory & App Data Analysis, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of SIM, Memory & App Data Analysis.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

The session strengthened participants' understanding of SIM, Memory & App Data Analysis and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on SIM, Memory & App Data Analysis was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

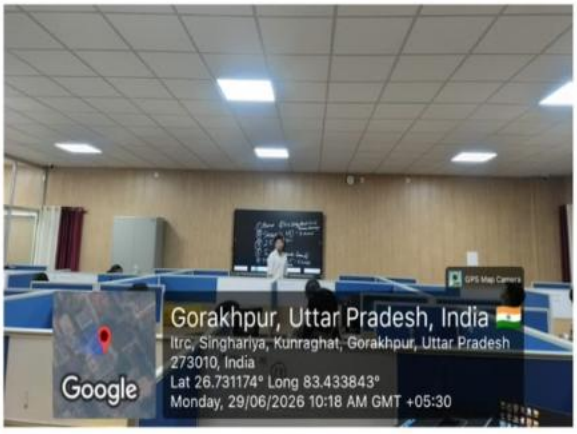
Acknowledgment

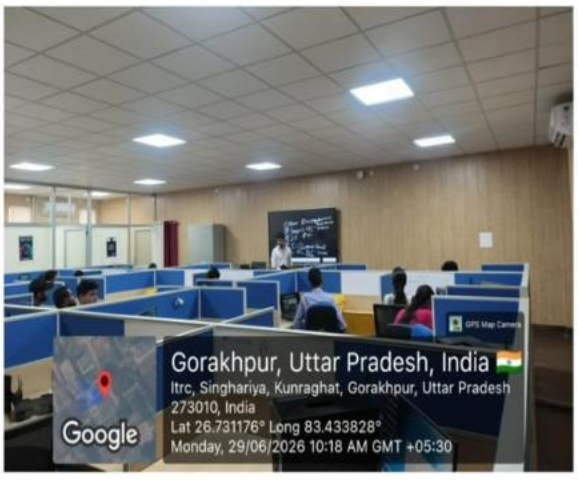
I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.

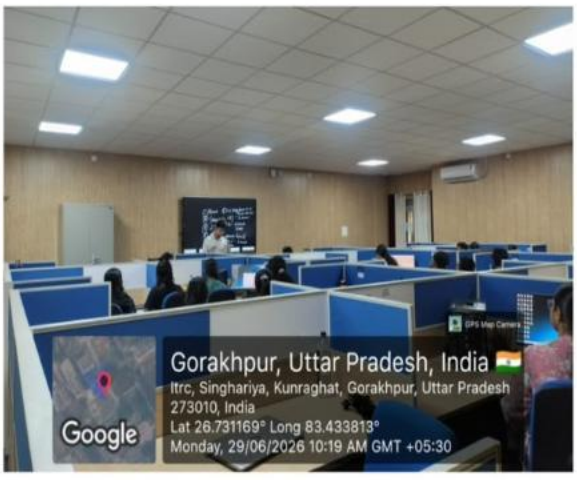












DAY -14

WORKSHOP: MOBILE FORENSICS – ADVANCED & CASE REVIEW

Introduction

A focused training session on Mobile Forensics – Advanced & Case Review was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Mobile Forensics – Advanced & Case Review.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Mobile Forensics – Advanced & Case Review
- Date: 30 Jun (Tue)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Mobile Forensics – Advanced & Case Review. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Mobile Forensics – Advanced & Case Review, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Mobile Forensics – Advanced & Case Review.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

The session strengthened participants' understanding of Mobile Forensics – Advanced & Case Review and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on Mobile Forensics – Advanced & Case Review was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

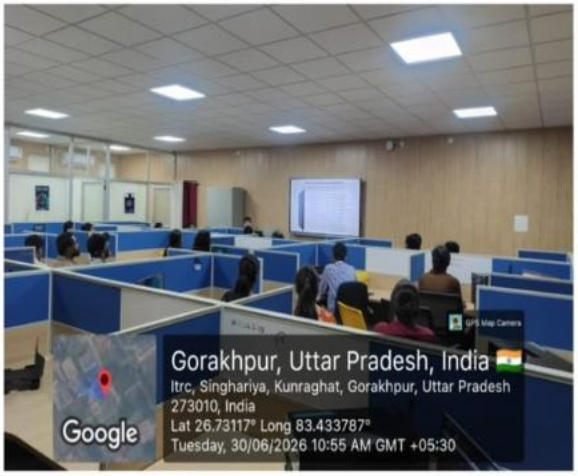
I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.

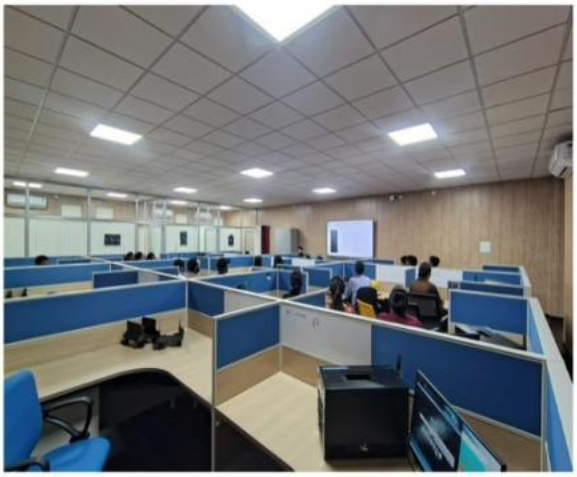












DAY -15

WORKSHOP: MULTIMEDIA FORENSICS – IMAGE & VIDEO ANALYSIS

Introduction

A focused training session on Multimedia Forensics – Image & Video Analysis was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Multimedia Forensics – Image & Video Analysis.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Multimedia Forensics – Image & Video Analysis
- Date: 01 Jul (Wed)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Multimedia Forensics – Image & Video Analysis. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Multimedia Forensics – Image & Video Analysis, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Multimedia Forensics – Image & Video Analysis.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

The session strengthened participants' understanding of Multimedia Forensics – Image & Video Analysis and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

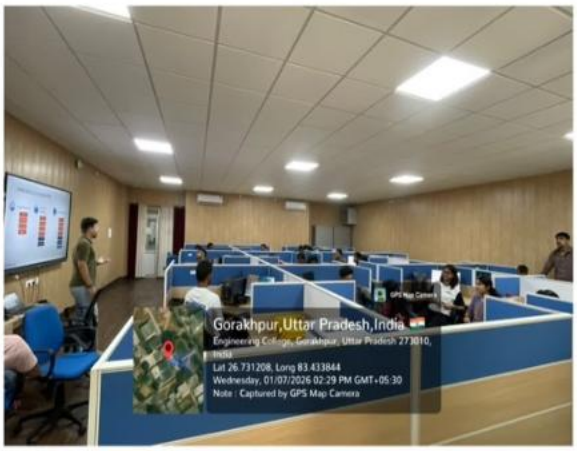
Conclusion

The session on Multimedia Forensics – Image & Video Analysis was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.









DAY -16

WORKSHOP: STEGANOGRAPHY DETECTION & AUDIO FORENSICS

Introduction

A focused training session on Steganography Detection & Audio Forensics was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Steganography Detection & Audio Forensics.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Steganography Detection & Audio Forensics
- Date: 02 Jul (Thu)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Steganography Detection & Audio Forensics. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Steganography Detection & Audio Forensics, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Steganography Detection & Audio Forensics.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

The session strengthened participants' understanding of Steganography Detection & Audio Forensics and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

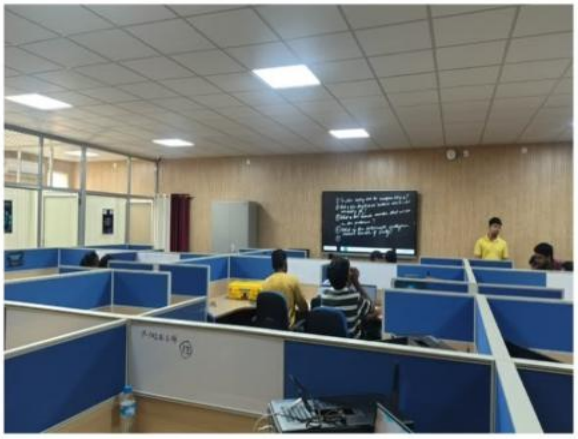
The session on Steganography Detection & Audio Forensics was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

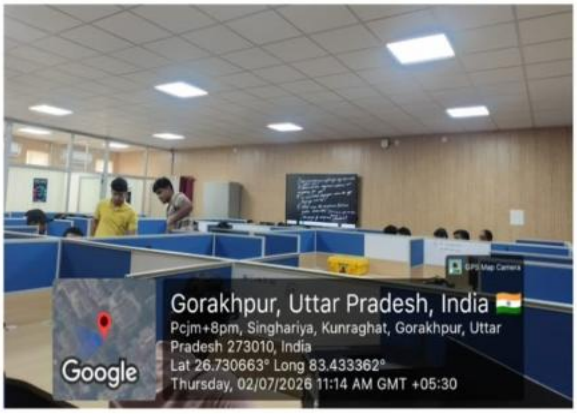
Acknowledgment

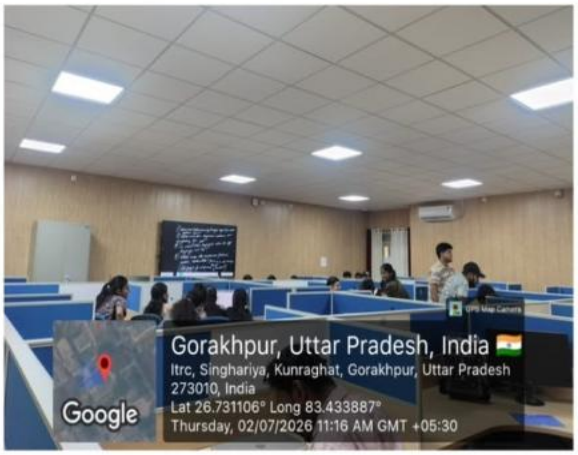
I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.

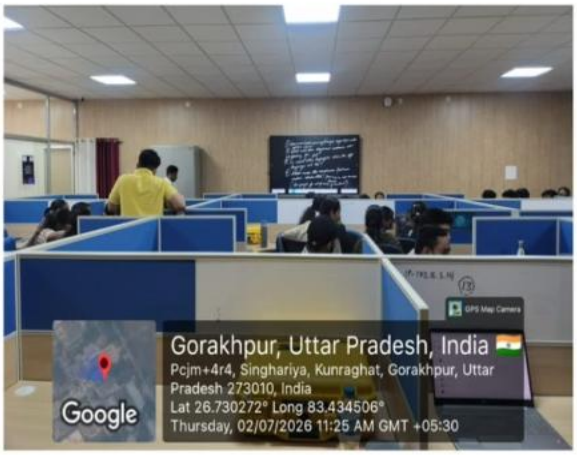












DAY -17

WORKSHOP: MULTIMEDIA EVIDENCE – CASE REVIEW & REPORTING

Introduction

A focused training session on Multimedia Evidence – Case Review & Reporting was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Multimedia Evidence – Case Review & Reporting.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Multimedia Evidence – Case Review & Reporting
- Date: 03 Jul (Fri)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Multimedia Evidence – Case Review & Reporting. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Multimedia Evidence – Case Review & Reporting, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Multimedia Evidence – Case Review & Reporting.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

The session strengthened participants' understanding of Multimedia Evidence – Case Review & Reporting and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

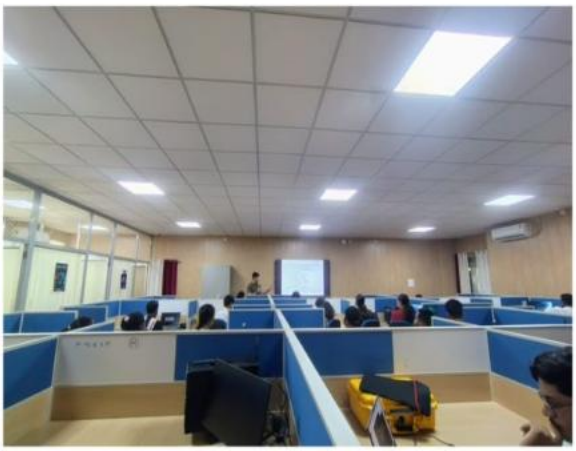
Conclusion

The session on Multimedia Evidence – Case Review & Reporting was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.





DAY -18

WORKSHOP: NETWORK FORENSICS – LOGS & PACKET CAPTURE

Introduction

A focused training session on Network Forensics – Logs & Packet Capture was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Network Forensics – Logs & Packet Capture.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Network Forensics – Logs & Packet Capture
- Date: 06 Jul (Mon)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Network Forensics – Logs & Packet Capture. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Network Forensics – Logs & Packet Capture, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Network Forensics – Logs & Packet Capture.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

The session strengthened participants' understanding of Network Forensics – Logs & Packet Capture and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on Network Forensics – Logs & Packet Capture was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.













DAY -19

WORKSHOP: SOCIAL MEDIA FORENSICS & OSINT

Introduction

A focused training session on Social Media Forensics & OSINT was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Social Media Forensics & OSINT.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Social Media Forensics & OSINT
- Date: 07 Jul (Tue)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Social Media Forensics & OSINT. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Social Media Forensics & OSINT, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Social Media Forensics & OSINT.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

The session strengthened participants' understanding of Social Media Forensics & OSINT and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on Social Media Forensics & OSINT was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.





DAY -20

WORKSHOP: NETWORK & SOCIAL MEDIA – INTEGRATED CASE

Introduction

A focused training session on Network & Social Media – Integrated Case was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Network & Social Media – Integrated Case.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Network & Social Media – Integrated Case
- Date: 08 Jul (Wed)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Network & Social Media – Integrated Case. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Network & Social Media – Integrated Case, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Network & Social Media – Integrated Case.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

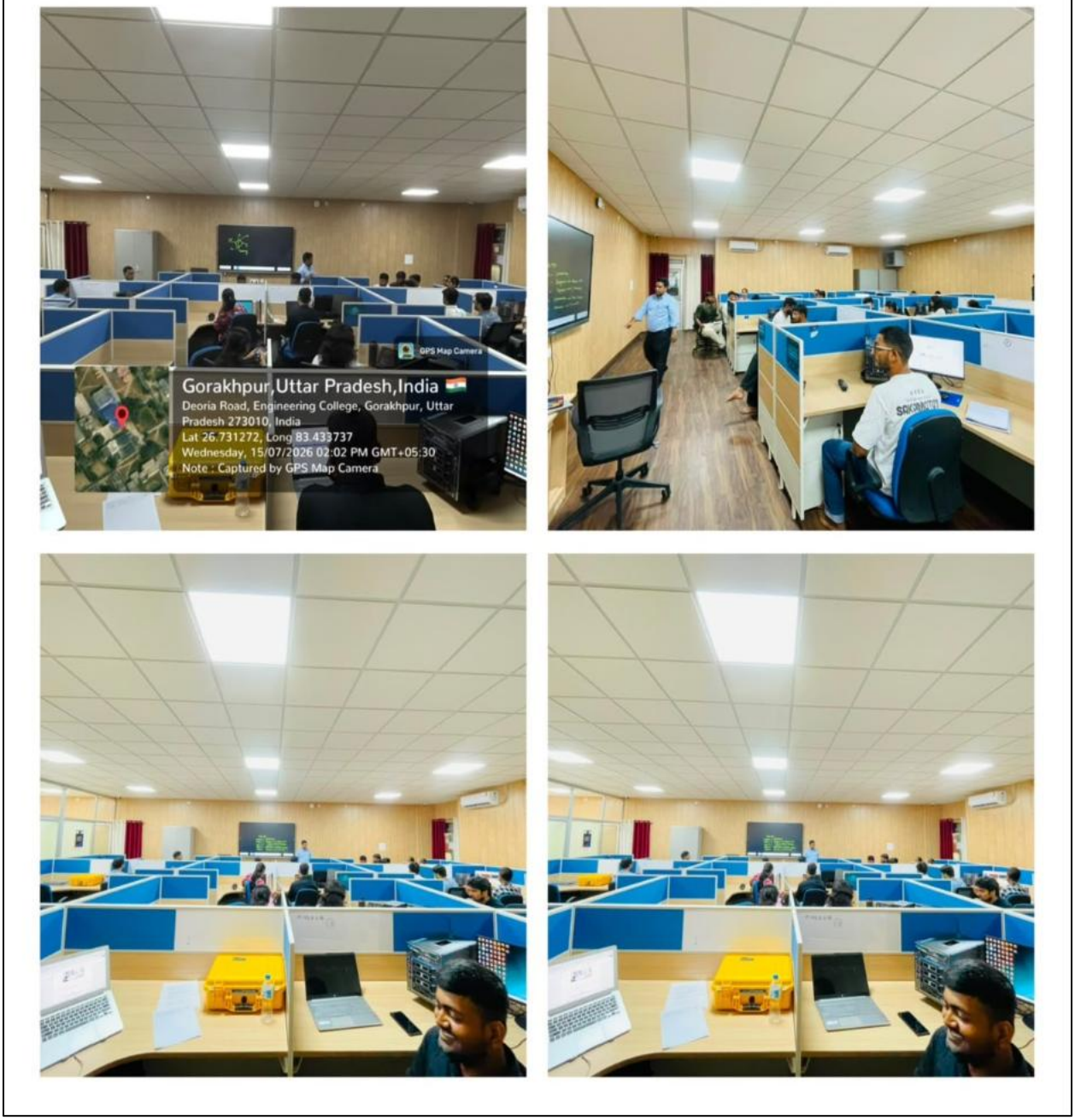
The session strengthened participants' understanding of Network & Social Media – Integrated Case and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on Network & Social Media – Integrated Case was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.



DAY -21

WORKSHOP: DRONE/UAV FORENSICS – FUNDAMENTALS

Introduction

A focused training session on Drone/UAV Forensics – Fundamentals was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Drone/UAV Forensics – Fundamentals.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Drone/UAV Forensics – Fundamentals
- Date: 09 Jul (Thu)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Drone/UAV Forensics – Fundamentals. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Drone/UAV Forensics – Fundamentals, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Drone/UAV Forensics – Fundamentals.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

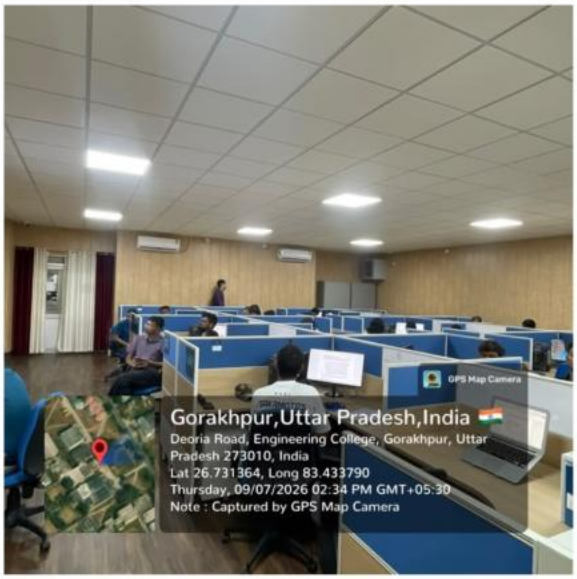
The session strengthened participants' understanding of Drone/UAV Forensics – Fundamentals and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

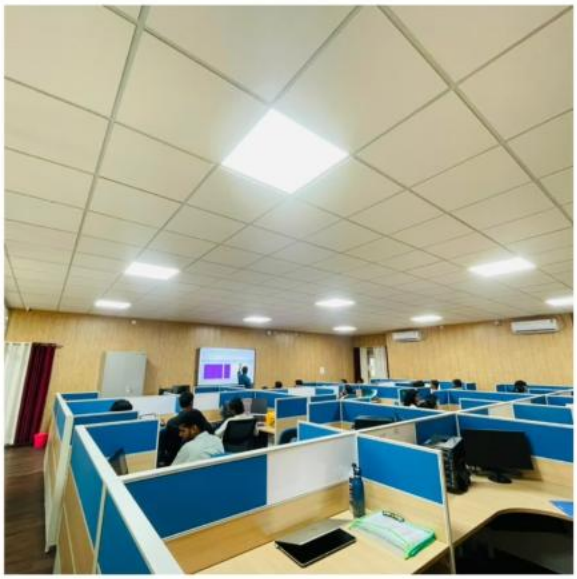
Conclusion

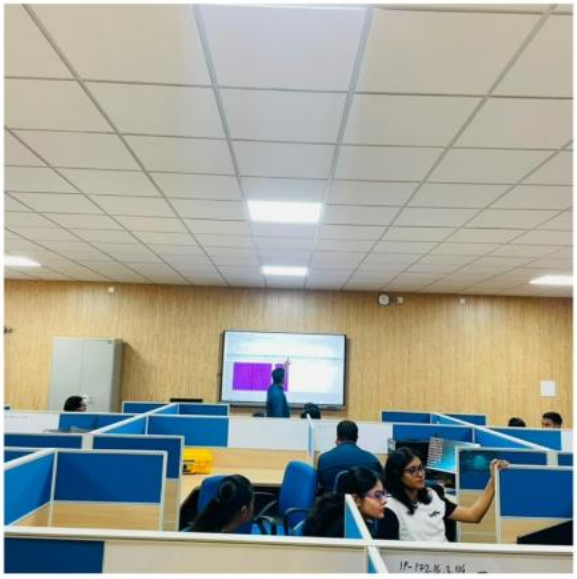
The session on Drone/UAV Forensics – Fundamentals was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

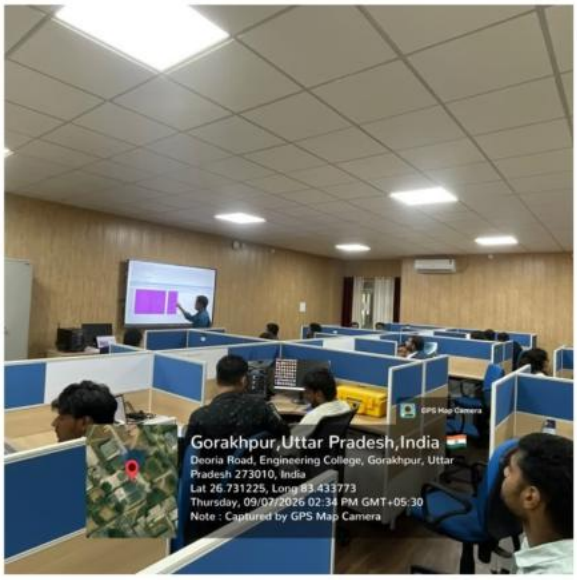
Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.









DAY -22

WORKSHOP: DRONE/UAV FORENSICS – ADVANCED & CASE STUDY

Introduction

A focused training session on Drone/UAV Forensics – Advanced & Case Study was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Drone/UAV Forensics – Advanced & Case Study.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Drone/UAV Forensics – Advanced & Case Study
- Date: 10 Jul (Fri)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Drone/UAV Forensics – Advanced & Case Study. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Drone/UAV Forensics – Advanced & Case Study, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Drone/UAV Forensics – Advanced & Case Study.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

The session strengthened participants' understanding of Drone/UAV Forensics – Advanced & Case Study and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on Drone/UAV Forensics – Advanced & Case Study was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.



DAY -23

WORKSHOP: CRYPTOCURRENCY FORENSICS

Introduction

A focused training session on Cryptocurrency Forensics was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Cryptocurrency Forensics.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Cryptocurrency Forensics
- Date: 13 Jul (Mon)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Cryptocurrency Forensics. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Cryptocurrency Forensics, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Cryptocurrency Forensics.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

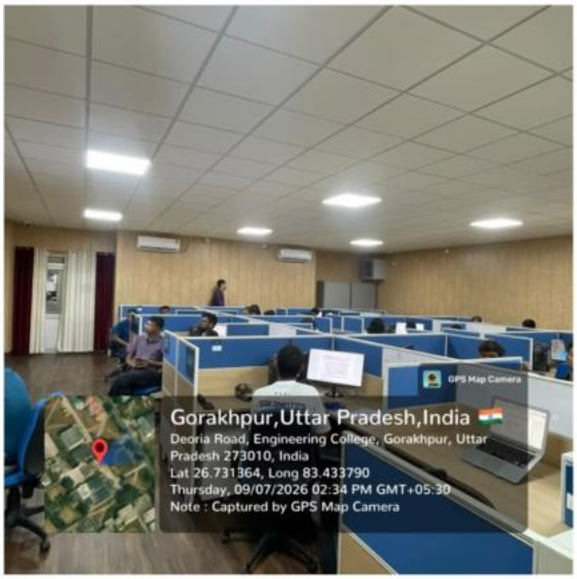
The session strengthened participants' understanding of Cryptocurrency Forensics and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

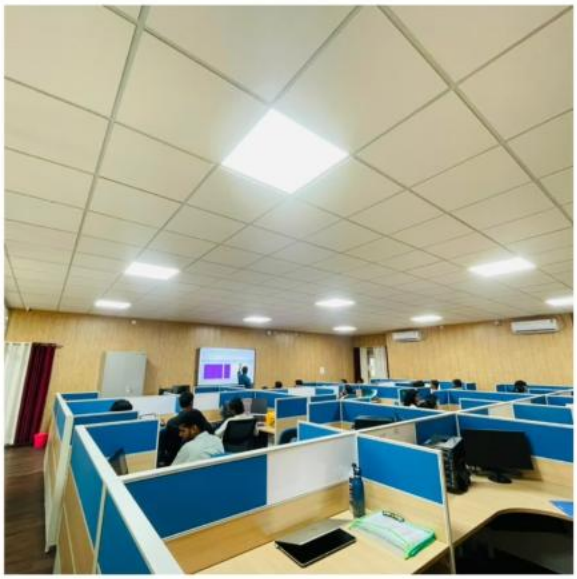
Conclusion

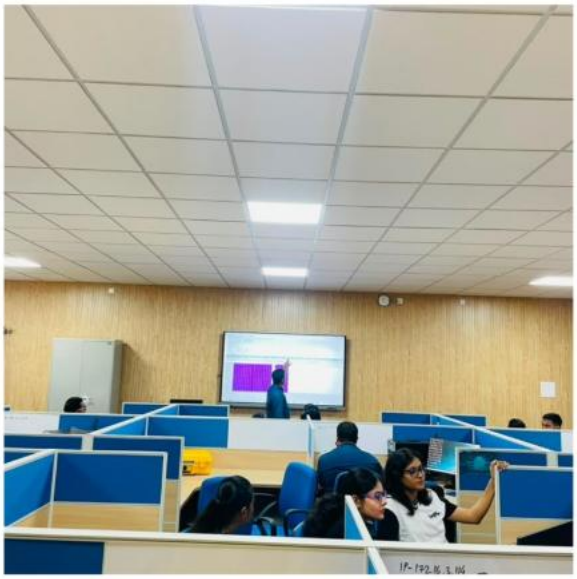
The session on Cryptocurrency Forensics was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

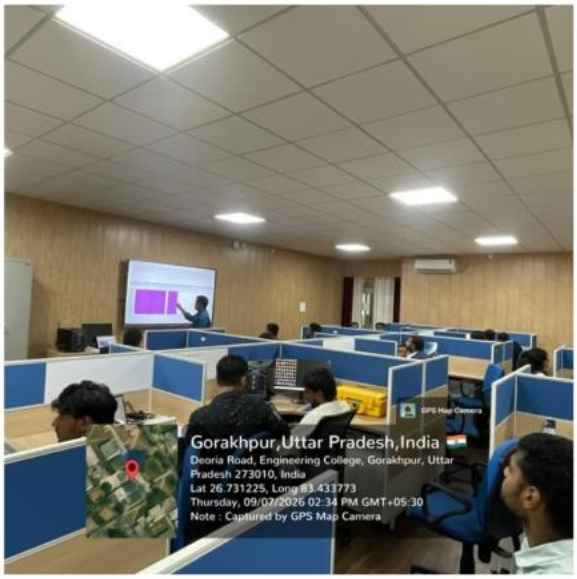
Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.









DAY -24

WORKSHOP: MALWARE ANALYSIS & ENCRYPTED DATA

Introduction

A focused training session on Malware Analysis & Encrypted Data was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Malware Analysis & Encrypted Data.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Malware Analysis & Encrypted Data
- Date: 14 Jul (Tue)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Malware Analysis & Encrypted Data. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Malware Analysis & Encrypted Data, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Malware Analysis & Encrypted Data.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

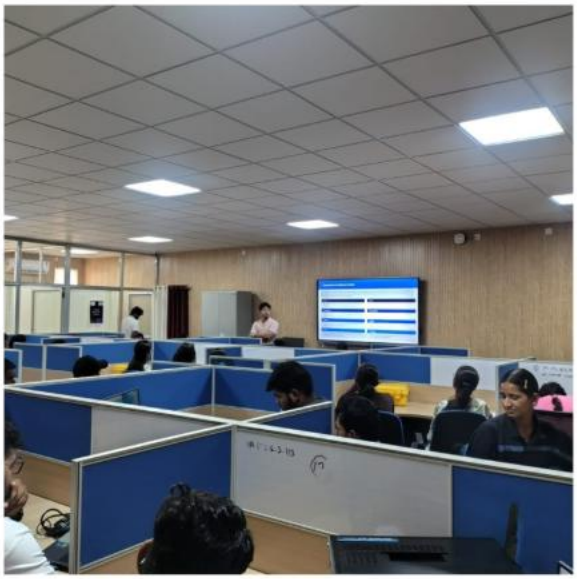
The session strengthened participants' understanding of Malware Analysis & Encrypted Data and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

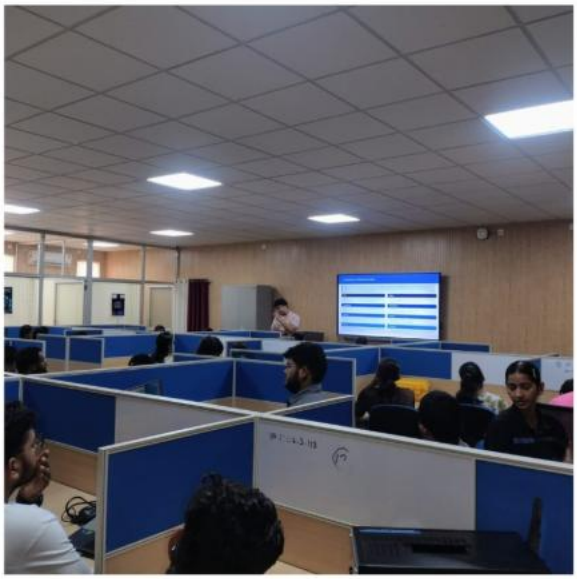
Conclusion

The session on Malware Analysis & Encrypted Data was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

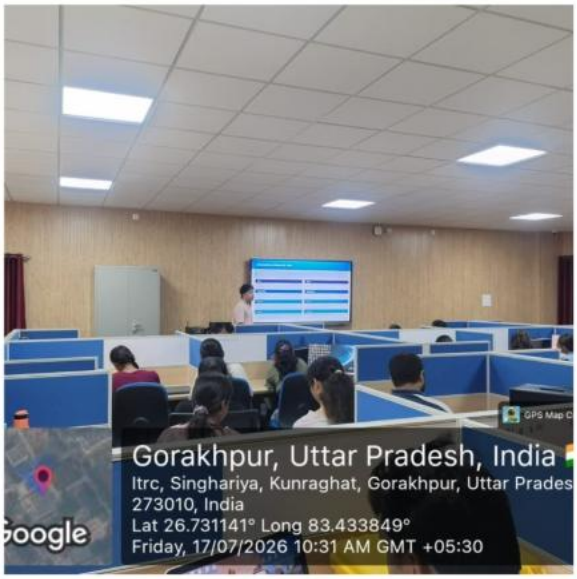
Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.









DAY -25

WORKSHOP: EMERGING TECH – IOT, CLOUD & AI FORENSICS

Introduction

A focused training session on Emerging Tech – IoT, Cloud & AI Forensics was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Emerging Tech – IoT, Cloud & AI Forensics.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Emerging Tech – IoT, Cloud & AI Forensics
- Date: 15 Jul (Wed)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Emerging Tech – IoT, Cloud & AI Forensics. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Emerging Tech – IoT, Cloud & AI Forensics, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Emerging Tech – IoT, Cloud & AI Forensics.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

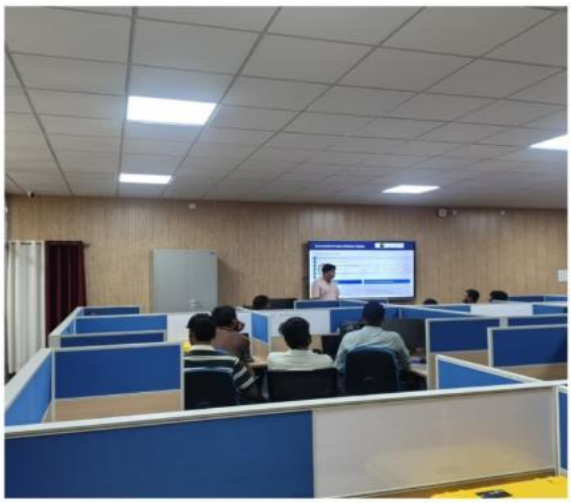
The session strengthened participants' understanding of Emerging Tech – IoT, Cloud & AI Forensics and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

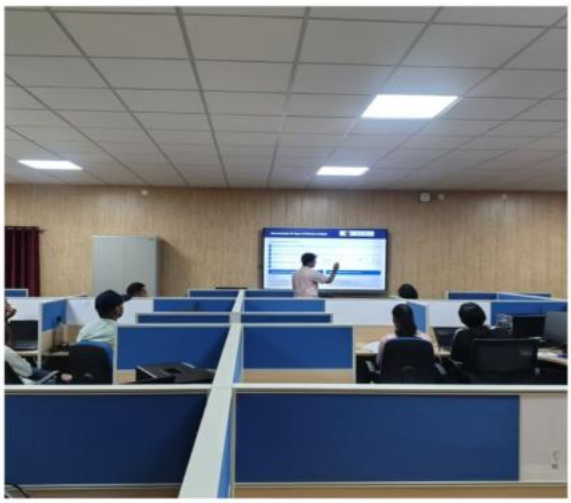
Conclusion

The session on Emerging Tech – IoT, Cloud & AI Forensics was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

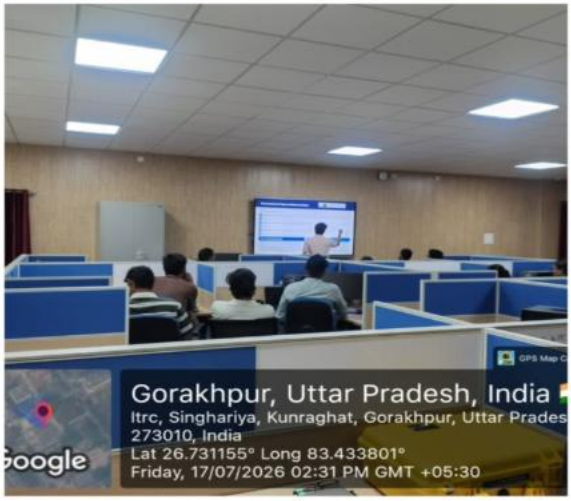
Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.









DAY -26

WORKSHOP: LEGAL FRAMEWORK – IT ACT & CYBERCRIME LAW

Introduction

A focused training session on Legal Framework – IT Act & Cybercrime Law was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Legal Framework – IT Act & Cybercrime Law.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Legal Framework – IT Act & Cybercrime Law
- Date: 16 Jul (Thu)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Legal Framework – IT Act & Cybercrime Law. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Legal Framework – IT Act & Cybercrime Law, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Legal Framework – IT Act & Cybercrime Law.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

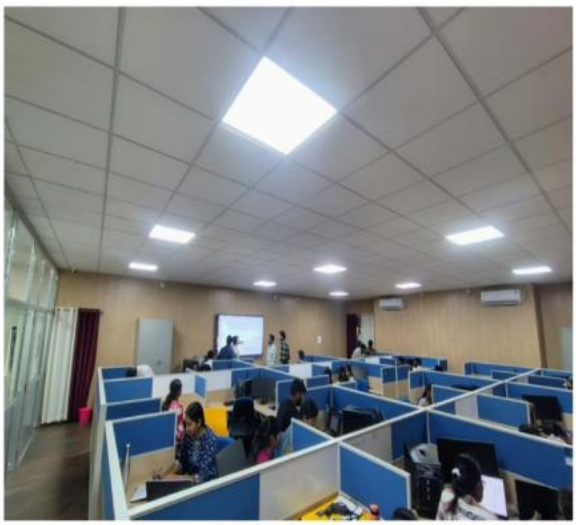
The session strengthened participants' understanding of Legal Framework – IT Act & Cybercrime Law and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

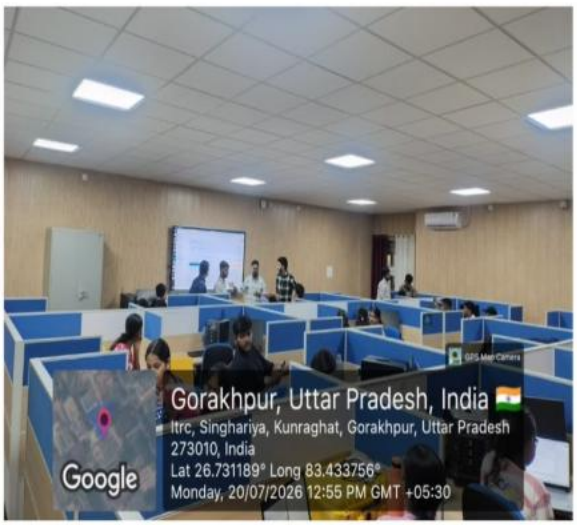
Conclusion

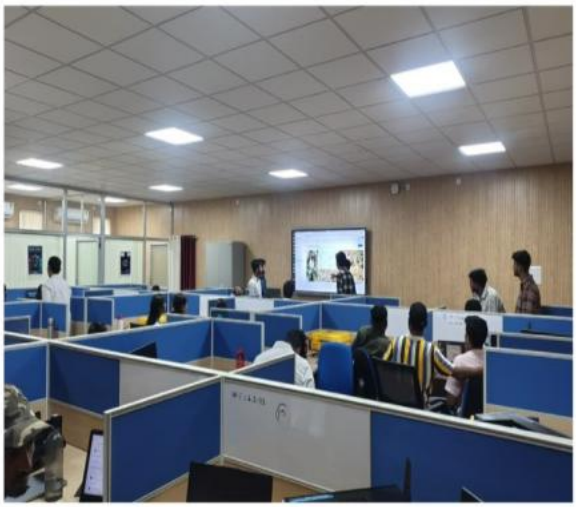
The session on Legal Framework – IT Act & Cybercrime Law was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.

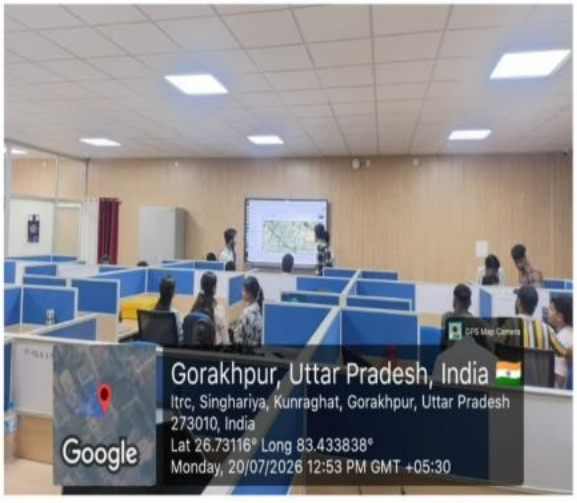












DAY -27

WORKSHOP: FORENSIC REPORT WRITING

Introduction

A focused training session on Forensic Report Writing was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Forensic Report Writing.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Forensic Report Writing
- Date: 17 Jul (Fri)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Forensic Report Writing. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Forensic Report Writing, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Forensic Report Writing.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

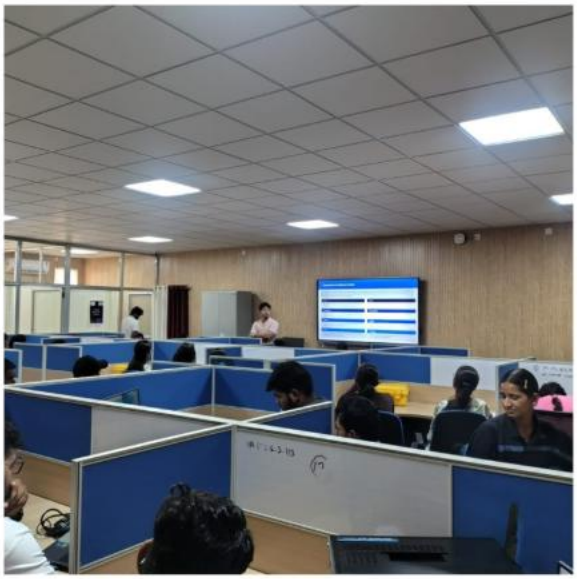
The session strengthened participants' understanding of Forensic Report Writing and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

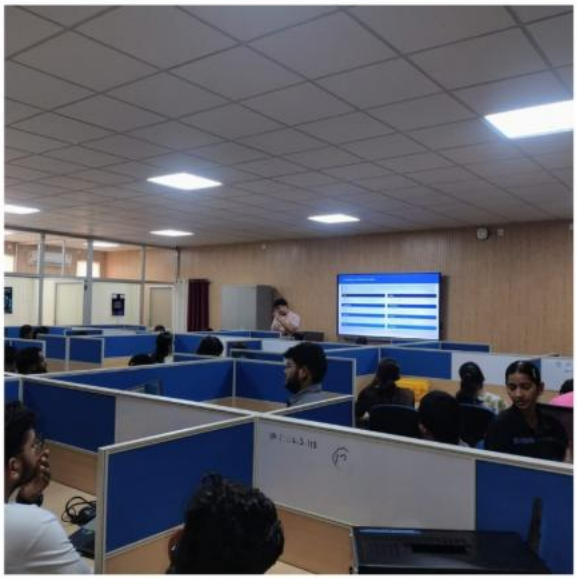
Conclusion

The session on Forensic Report Writing was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

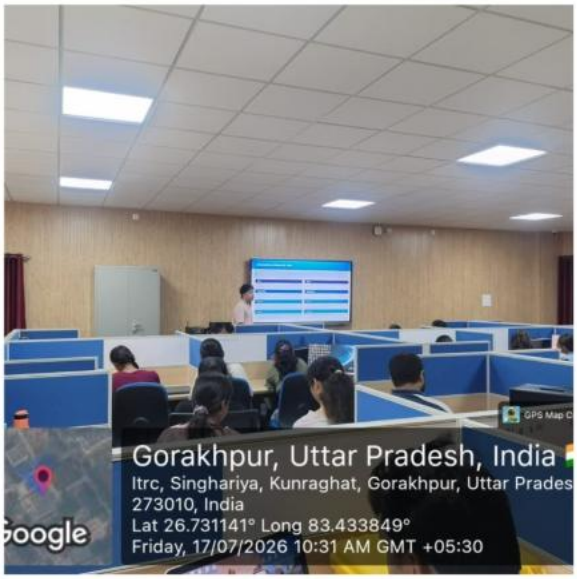
Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.









DAY -28

WORKSHOP: CAPSTONE PROJECT – FINAL PRESENTATION PREPARATION

Introduction

A focused training session on Capstone Project – Final Presentation Preparation was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Capstone Project – Final Presentation Preparation.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Capstone Project – Final Presentation Preparation
- Date: 20 Jul (Mon)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Capstone Project – Final Presentation Preparation. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Capstone Project – Final Presentation Preparation, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Capstone Project – Final Presentation Preparation.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

The session strengthened participants' understanding of Capstone Project – Final Presentation Preparation and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

The session on Capstone Project – Final Presentation Preparation was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.



DAY -29

WORKSHOP: CAPSTONE PROJECT – FINAL PRESENTATIONS & GRADUATION

Introduction

A focused training session on Capstone Project – Final Presentations & Graduation was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Capstone Project – Final Presentations & Graduation.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Capstone Project – Final Presentations & Graduation
- Date: 21 Jul (Tue)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Capstone Project – Final Presentations & Graduation. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Capstone Project – Final Presentations & Graduation, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Capstone Project – Final Presentations & Graduation.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

The session strengthened participants' understanding of Capstone Project – Final Presentations & Graduation and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

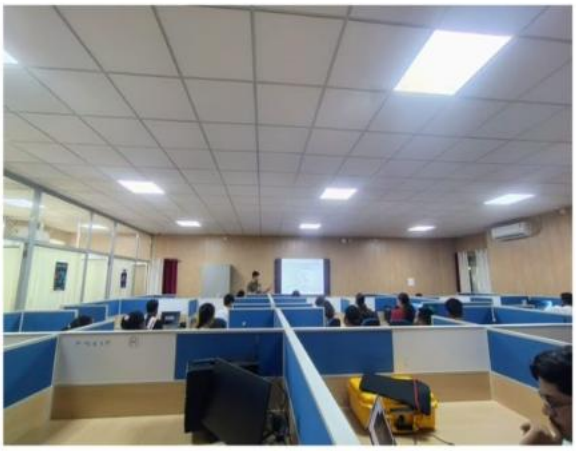
The session on Capstone Project – Final Presentations & Graduation was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic

investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.





DAY -30

WORKSHOP: TRAINING REVIEW, ASSESSMENT & CLOSING DOCUMENTATION

Introduction

A focused training session on Training Review, Assessment & Closing Documentation was conducted as part of the Six-Week Summer Internship Training Program in Cyber Security & Digital Forensics. The session was designed to provide participants with practical and conceptual understanding of the topic and its relevance to digital investigations.

Objectives

The primary objectives of the session were:

1. To understand the concepts and significance of Training Review, Assessment & Closing Documentation.
2. To learn relevant forensic procedures and evidence-handling practices.
3. To examine the role of the topic in cybercrime investigations.
4. To gain familiarity with applicable tools, techniques, and workflows.
5. To develop professional awareness of documentation, integrity, and reporting requirements.

Workshop Details

- Topic: Training Review, Assessment & Closing Documentation
- Date: 21 Jul (Tue)
- Mode: Offline (On-Campus)
- Venue: Cyber Forensics Research Lab, Ground Floor, ITRC, MMMUT
- Target Audience: Students, Researchers, IT Professionals, and Cybersecurity Enthusiasts

Sessions Covered

The session covered the fundamental concepts, investigation workflow, practical considerations, and forensic relevance of Training Review, Assessment & Closing Documentation. Participants were introduced to identification of relevant evidence, appropriate examination methods, preservation requirements, and interpretation of findings.

Practical / Technical Focus

Participants discussed and reviewed procedures applicable to Training Review, Assessment & Closing Documentation, including evidence identification, acquisition or examination, validation, documentation, and analysis. Where appropriate, examples and forensic scenarios were used to connect theoretical concepts with investigation practice.

Key Learning Outcomes

After attending the session, participants were able to:

- Explain the fundamentals of Training Review, Assessment & Closing Documentation.
- Identify relevant digital evidence and forensic indicators.
- Describe an appropriate investigation workflow.
- Recognize commonly used techniques and tools.
- Understand the importance of evidence integrity and proper documentation.

Benefits of the Session

The session strengthened participants' understanding of Training Review, Assessment & Closing Documentation and its practical importance in cyber security and digital forensic investigations. It also helped develop analytical thinking, evidence-handling awareness, and professional investigation skills.

Conclusion

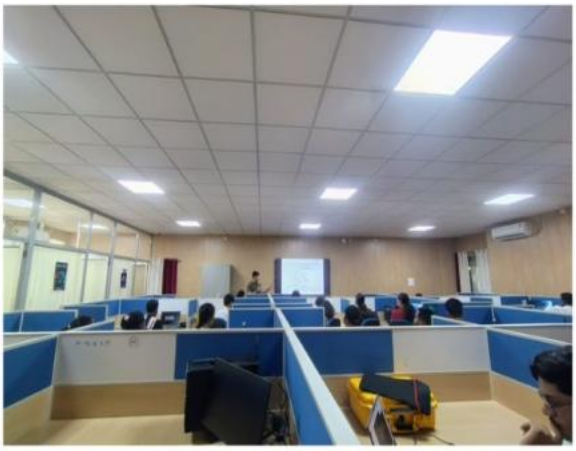
The session on Training Review, Assessment & Closing Documentation was informative and beneficial. It provided a structured understanding of the subject and demonstrated how the topic contributes to systematic digital forensic

investigations. The knowledge gained will support participants in subsequent practical sessions and the overall training program.

Acknowledgment

I express my sincere gratitude to the organizers, resource persons, instructors, and all participants for making the session successful. Their valuable guidance, demonstrations, and support contributed significantly to the learning experience.





DAY – 30

CERTIFICATE DISTRIBUTION CEREMONY

Date: 21 July 2026 (Tuesday)

Venue: Cyber Security & Digital Forensics Laboratory

Introduction

The **Certificate Distribution Ceremony** marked the successful completion of the **Six-Week Summer Internship Training Program on Cyber Security & Digital Forensics**. The ceremony celebrated the achievements of all participants who successfully completed the internship and recognized their dedication, hard work, and commitment throughout the six-week training.

The event was organized under the guidance of **Prof. Rakesh Kumar, Chairman & Head**, with the coordination of **Dr. B. K. Sharma** and **Dr. Vimal Kumar**. The ceremony was graced by the presence of **Chief Guest Shri Upendra Kumar Singh**, whose motivational address inspired participants to pursue excellence in cybersecurity. The program also acknowledged the valuable contribution of **Mr. Naveen Singh, Trainer, Cyint Technologies**, who provided practical training and industry-oriented guidance throughout the internship.

Objectives

The primary objectives of the ceremony were:

- To recognize the successful completion of the Six-Week Summer Internship Training Program.
- To distribute certificates to all eligible participants.
- To appreciate the efforts of trainers, coordinators, faculty members, and organizers.
- To motivate students towards careers in Cyber Security and Digital Forensics.
- To encourage continuous learning, innovation, and professional development.

Ceremony Details

Particular	Details

Event	Certificate Distribution Ceremony
Program	Six-Week Summer Internship Training Program
Domain	Cyber Security & Digital Forensics
Date	**21 July 2026 (Tuesday)**
Duration	Half Day
Mode	Offline
Venue	Cyber Security & Digital Forensics Laboratory
Chairman & Head	**Prof. Rakesh Kumar**
Coordinators	**Dr. B. K. Sharma & Dr. Vimal Kumar**
Chief Guest	**Shri Upendra Kumar Singh**
Industry Trainer	**Mr. Naveen Singh, Cyint Technologies**

Program Highlights

Welcome Address

The ceremony commenced with a warm welcome by the organizing committee. **Prof. Rakesh Kumar, Chairman & Head**, welcomed the distinguished guests, faculty members, trainers, and participants. He appreciated the efforts of everyone involved in making the internship program successful and emphasized the growing significance of Cyber Security and Digital Forensics in today's digital world.

Overview of the Internship Program

The coordinators, **Dr. B. K. Sharma** and **Dr. Vimal Kumar**, presented an overview of the six-week internship, highlighting the various technical modules covered during the training. The internship included both theoretical lectures and practical laboratory sessions on:

- Digital Forensics Fundamentals
- Computer & Mobile Forensics
- Network Forensics
- Malware Analysis
- Memory Forensics
- Ethical Hacking
- Penetration Testing
- Bug Bounty
- Incident Response
- Cyber Threat Intelligence
- Evidence Collection & Preservation
- Digital Investigation Techniques
- Technical Report Writing

The coordinators appreciated the active participation and dedication of all interns throughout the program.

Address by the Chief Guest

Chief Guest Shri Upendra Kumar Singh delivered an inspiring keynote address, emphasizing the increasing demand for skilled cybersecurity professionals. He encouraged participants to continuously upgrade their technical knowledge, maintain ethical standards, and contribute towards building a secure digital ecosystem. He congratulated all participants for successfully completing the internship and wished them success in their future careers.

Industry Expert Session

Mr. Naveen Singh, Trainer, Cyint Technologies, shared valuable insights into current industry practices, real-world cyber threats, and practical approaches used in Cyber Security and Digital Forensics. He highlighted the importance of hands-on learning, continuous skill development, professional certifications, and industry exposure for aspiring cybersecurity professionals.

He also appreciated the enthusiasm and commitment shown by the participants during the practical training sessions.

Certificate Distribution

The certificate distribution ceremony was conducted in the presence of **Prof. Rakesh Kumar**, **Dr. B. K. Sharma**, **Dr. Vimal Kumar**, **Shri Upendra Kumar Singh**, and **Mr. Naveen Singh**. Certificates were awarded to all participants who successfully completed the **Six-Week Summer Internship Training Program on Cyber Security & Digital Forensics**.

The dignitaries congratulated the participants and appreciated their dedication, discipline, and active involvement throughout the internship.

Participant Experience Sharing

Selected participants shared their experiences and expressed gratitude to the faculty members, coordinators, trainer, and organizers for providing excellent guidance and practical exposure. They acknowledged that the internship significantly improved their technical knowledge, analytical thinking, and practical skills in Cyber Security and Digital Forensics.

Vote of Thanks

The ceremony concluded with a formal vote of thanks delivered by the organizing committee. Heartfelt gratitude was expressed to:

- **Prof. Rakesh Kumar, Chairman & Head**
- **Dr. B. K. Sharma, Coordinator**
- **Dr. Vimal Kumar, Coordinator**
- **Chief Guest Shri Upendra Kumar Singh**
- **Mr. Naveen Singh, Trainer, Cyint Technologies**

Faculty members, technical staff, and all participants

for their valuable support and contribution towards the successful completion of the internship program.

Key Learning Outcomes

By the end of the internship, participants were able to:

- Understand the core concepts of Cyber Security and Digital Forensics.
- Apply forensic investigation methodologies.
- Perform evidence acquisition and analysis.
- Use industry-standard forensic and cybersecurity tools.
- Conduct basic vulnerability assessments and penetration testing.
- Understand ethical hacking and bug bounty methodologies.
- Prepare professional forensic reports and technical documentation.
- Follow legal and ethical practices during digital investigations.

Benefits of the Internship Program

The internship provided participants with comprehensive theoretical knowledge and extensive hands-on experience in Cyber Security and Digital Forensics. Practical laboratory sessions, expert lectures, case studies, and real-world demonstrations enhanced participants' technical competencies and industry readiness.

The program also strengthened participants' analytical thinking, teamwork, problem-solving abilities, communication skills, and professional confidence.

Conclusion

The **Certificate Distribution Ceremony** successfully marked the completion of the **Six-Week Summer Internship Training Program on Cyber Security & Digital Forensics**. The event celebrated the achievements of the participants and recognized the dedicated efforts of the faculty members, coordinators, trainer, and organizing team.

Under the leadership of **Prof. Rakesh Kumar**, the coordination of **Dr. B. K. Sharma** and **Dr. Vimal Kumar**, the inspirational presence of **Chief Guest Shri Upendra Kumar Singh**, and the practical training provided by **Mr. Naveen Singh (Cyint Technologies)**, the internship proved to be an enriching learning experience. The knowledge and practical exposure gained during the program will serve as a strong foundation for participants aspiring to build successful careers in Cyber Security, Digital Forensics, and Information Security.

Acknowledgment

I express my heartfelt gratitude to **Prof. Rakesh Kumar (Chairman & Head)** for his visionary leadership and continuous encouragement throughout the internship program. I sincerely thank **Dr. B. K. Sharma** and **Dr. Vimal Kumar**, Coordinators of the program, for their excellent guidance, planning, and support in successfully organizing the internship.

I am deeply grateful to our **Chief Guest, Shri Upendra Kumar Singh**, for his inspiring words and valuable motivation during the Certificate Distribution Ceremony. Special thanks are extended to **Mr. Naveen Singh, Trainer, Cyint Technologies**, for sharing his industry expertise and providing practical training sessions that greatly enhanced our technical knowledge.

Finally, I thank all faculty members, technical staff, organizers, and fellow participants for their cooperation and contribution, making the **Six-Week Summer Internship Training Program on Cyber Security & Digital Forensics** a memorable and enriching learning experience.


CYBER SECURITY &
DIGITAL FORENSICS
Gorakhpur, Uttar Pradesh, India
Pcjm+8pm, Singhariya, Kunraghat, Gorakhpur, Uttar Pradesh 273010, India
Lat 26.730832° Long 83.433649°
Google


CY NT TECHNOLOGIES
Gorakhpur, Uttar Pradesh, India
Pcjm+8pm, Singhariya, Kunraghat, Gorakhpur, Uttar Pradesh 273010, India
Lat 26.730838° Long 83.43365°
Google


Gorakhpur, Uttar Pradesh, India
Pcjm+998, Deoria Rd, Singhariya, Kunraghat, Gorakhpur, Uttar Pradesh 273010, India







INDUSTRIAL VISIT REPORT

Madan Mohan Malaviya University of Technology (MMMUT), Gorakhpur

Venue: Cyber Police Station (Cyber Thana), Gorakhpur

Date: 07 July 2026 (Tuesday)

Introduction

As part of the **Six-Week Summer Internship Training Program on Cyber Security & Digital Forensics**, the students of the **Cyber Security & Digital Forensics Laboratory, Madan Mohan Malaviya University of Technology (MMMUT), Gorakhpur**, visited the **Cyber Police Station (Cyber Thana), Gorakhpur** on **07 July 2026 (Tuesday)**.

Objectives

The primary objectives of the visit were:

- To understand the functioning of the Cyber Police Station.
- To observe real-world cybercrime investigation procedures.

Visit Details

Particular	Details
Event	Educational Visit to Cyber Police Station
Institution	Madan Mohan Malaviya University of Technology (MMMUT), Gorakhpur
Department	Cyber Security & Digital Forensics Laboratory
Date	**07 July 2026 (Tuesday)**
Venue	Cyber Police Station (Cyber Thana), Gorakhpur
Duration	Half Day
Participants	Internship Students, Faculty Members, Coordinators and Technical Staff

Introduction to Cyber Police Station

The visit began with an introductory session conducted by the officers of the Cyber Police Station. Students were introduced to the organizational structure, responsibilities, and day-to-day operations of the Cyber Thana. The officers explained the increasing importance of cyber policing in combating cybercrime and protecting citizens in the digital era.

2. Cybercrime Complaint Registration Process

Students learned about the complete process of handling cybercrime complaints, including:

- Online complaint registration.
- Complaint verification.

Digital Evidence Collection and Preservation

The officers demonstrated the methods used for collecting and preserving digital evidence while maintaining its integrity. Topics discussed included:

Cyber Forensic Investigation Process

The Cyber Police officials explained the standard digital forensic investigation process, including:

- Identification of digital evidence.
- Acquisition.

Demonstration of Cybercrime Investigation Tools

Students observed demonstrations of various tools and technologies used during cyber investigations, including:

- Mobile Forensic Tools
- Computer Forensic Software

Awareness on Common Cyber Frauds

The officers explained various cyber frauds frequently reported by citizens, such as:

- UPI Fraud
- QR Code Scam
- OTP Fraud

Interactive Question & Answer Session

The visit concluded with an interactive discussion where students asked questions regarding cybercrime investigations, forensic tools, legal procedures, career opportunities, and emerging cyber threats.

Key Learning Outcomes

After completing the educational visit, students were able to:

- Understand the functioning of a Cyber Police Station.
- Learn the cybercrime investigation process.

Benefits of the Visit

The educational visit provided students with valuable practical exposure to real-world cybercrime investigations and digital forensic practices.

Conclusion

The educational visit to the **Cyber Police Station (Cyber Thana), Gorakhpur**, on **07 July 2026 (Tuesday)** was highly informative and professionally enriching. It offered internship students of the **Cyber Security & Digital Forensics Laboratory, MMMUT Gorakhpur** an excellent opportunity to understand real-world cybercrime investigation procedures and digital forensic practices.

Acknowledgment

I express my sincere gratitude to the **Cyber Police Station (Cyber Thana), Gorakhpur**, for granting us the opportunity to visit and observe their cybercrime investigation facilities.

I also extend my heartfelt appreciation to **Prof. Rakesh Kumar (Chairman & Head)**, **Dr. B. K. Sharma**, and **Dr. Vimal Kumar**, Coordinators And **Mr. Naveen Singh, Trainer, Cyint Technologies** of the **Cyber Security & Digital Forensics Laboratory, MMMUT Gorakhpur**, for organizing this educational visit. Their continuous support and guidance made this industrial visit highly successful and beneficial.







साइबर अपराध थाना

WORKSHOP: CYBER SECURITY AWARENESS

By Shri Upendra Kumar Singh

Cyber Commando, Sub-Inspector, Uttar Pradesh Police

Introduction

A one-day **Cyber Security Awareness** workshop was conducted by **Shri Upendra Kumar Singh, Cyber Commando and Sub-Inspector, Uttar Pradesh Police**, to educate participants about the growing challenges of cybercrime and the importance of cyber safety in today's digital era. The workshop focused on creating awareness about online fraud, cybercrime prevention, digital safety, social engineering attacks, and legal provisions related to cyber offences.

Drawing upon his professional experience as a **Cyber Commando** with the **Uttar Pradesh Police**, Shri Upendra Kumar Singh shared practical insights into real-life cybercrime investigations, the latest cyber threats, and effective strategies for protecting individuals and organizations from cyber attacks. The session emphasized the importance of cyber awareness, responsible digital behavior, and timely reporting of cyber incidents.

Objectives

The primary objectives of the workshop were:

- To understand the fundamentals of Cyber Security and Cybercrime.
- To create awareness about online frauds and digital threats.

Workshop Details

Particular	Details
Workshop Title	Cyber Security Awareness
Resource Person	**Shri Upendra Kumar Singh**
Designation	**Cyber Commando & Sub-Inspector, Uttar Pradesh Police**
Date	**21 July 2026 (Tuesday)**
Duration	1 Day
Mode	Offline
Venue	Cyber Security & Digital Forensics Laboratory
Target Audience	Students, Faculty Members, Researchers, IT Professionals, Government Officials, and Cybersecurity Enthusiasts

Sessions Covered

Introduction to Cyber Security

The workshop began with an overview of Cyber Security and its importance in protecting digital assets, personal information, and organizational infrastructure. Participants learned about the increasing impact of cybercrime on individuals, businesses, and government institutions.

Current Cybercrime Trends

The resource person explained various cyber threats currently affecting society, including:

- Online Banking Fraud
- UPI and Digital Payment Frauds
- QR Code Scams

Real-life investigation cases from Uttar Pradesh Police were discussed to help participants understand the methods used by cybercriminals.

Social Engineering Attacks

Participants learned about different forms of social engineering attacks, including:

- Phishing
- Spear Phishing
- Impersonation Attacks

Cyber Hygiene and Digital Safety

This session focused on best practices for maintaining cyber security in daily life, including:

- Creating strong and unique passwords
- Using Multi-Factor Authentication (MFA)

Cybercrime Reporting and Legal Awareness

Shri Upendra Kumar Singh explained the legal framework governing cybercrime in India and discussed:

- Information Technology Act, 2000
- Relevant provisions of the Bharatiya Nyaya Sanhita (BNS)
- Digital evidence preservation
- National Cyber Crime Reporting Portal
- Cyber Crime Helpline Number – **1930**
- Role of Uttar Pradesh Police in cybercrime investigations

Interactive Session and Real-Life Case Studies

One of the most engaging parts of the workshop was the interactive discussion where the resource person shared actual cybercrime investigation experiences. Participants asked questions regarding cyber fraud, ethical hacking, digital investigations, and career opportunities in cybersecurity.

Key Learning Outcomes

After attending the workshop, participants were able to:

- Understand the fundamentals of Cyber Security and Cybercrime.
- Identify common online frauds and cyber attacks.
- Practice safe internet and digital payment security.

Conclusion

The **Cyber Security Awareness Workshop**, conducted by **Shri Upendra Kumar Singh, Cyber Commando and Sub-Inspector, Uttar Pradesh Police**, was highly informative and impactful. The workshop successfully highlighted the importance of cyber awareness, digital safety, cybercrime prevention, and legal compliance in today's technology-driven society.

Through practical demonstrations, real-life case studies, and interactive discussions, participants gained valuable knowledge about protecting themselves from cyber threats and contributing to a safer digital environment.

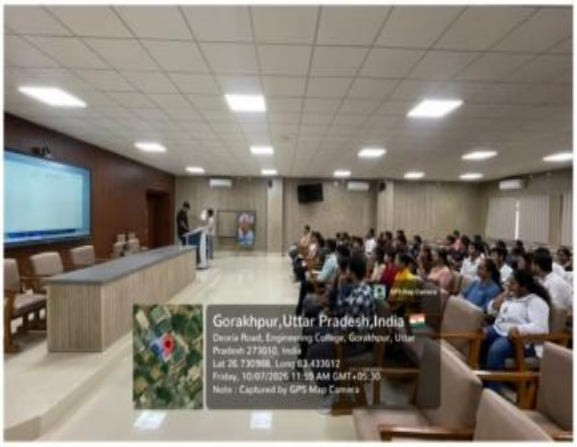
Acknowledgment

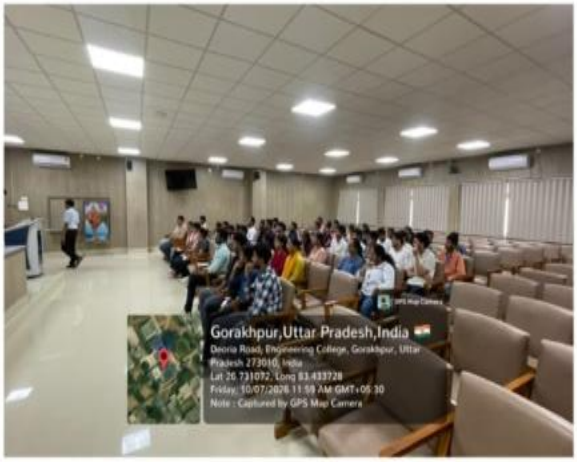
I express my sincere gratitude to **Shri Upendra Kumar Singh, Cyber Commando and Sub-Inspector, Uttar Pradesh Police**, for delivering an insightful and inspiring session on **Cyber Security Awareness**. His practical experience, real-life case studies, and expert guidance provided participants with valuable knowledge about cybercrime prevention and digital safety.








Gorakhpur,Uttar Pradesh,India
Deoria Road, Engineering College, Gorakhpur, Uttar
Pradesh 273010, India
Lat 26.730908, Long 83.433012
Friday, 10/07/2026 11:59 AM GMT+05:30
Note : Captured by GPS Map Camera


Gorakhpur,Uttar Pradesh,India
Deoria Road, Engineering College, Gorakhpur, Uttar
Pradesh 273010, India
Lat 26.731072, Long 83.433728
Friday, 10/07/2026 11:59 AM GMT+05:30
Note : Captured by GPS Map Camera



WORKSHOP : BUG BOUNTY

By Mr. Anas Ahmad

Date: 20 July 2026 (Monday)

Venue: Cyber Security Forensic Laboratory

A one-day workshop on **Bug Bounty** was conducted on **20 July 2026 (Monday)** by **Mr. Anas Ahmad** to provide participants with a comprehensive understanding of vulnerability discovery, ethical hacking practices, and responsible vulnerability disclosure. The workshop introduced participants to the fundamentals of bug bounty programs, reconnaissance methodologies, vulnerability assessment techniques, and the process of reporting security flaws responsibly. The session combined theoretical concepts with practical demonstrations, enabling participants to understand how ethical hackers identify and report vulnerabilities in real-world applications.

Objectives

The primary objectives of the workshop were:

- To understand the fundamentals of Bug Bounty programs.
- To learn the methodology of web application reconnaissance and vulnerability assessment.
- To identify common web application vulnerabilities.

Workshop Details

Particular	Details
Workshop Title	Bug Bounty
Resource Person	**Mr. Anas Ahmad**
Date	**20 July 2026 (Monday)**
Duration	1 Day
Mode	Offline
Venue	Cyber Security Forensic Laboratory
Target Audience	Students, Researchers, IT Professionals, Ethical Hackers, and Cybersecurity Enthusiasts

Introduction to Bug Bounty

The workshop began with an overview of Bug Bounty programs and their significance in today's cybersecurity landscape. Participants learned how organizations invite ethical hackers to identify and report vulnerabilities before malicious attackers can exploit them. The session also covered the evolution of bug bounty programs and their importance in strengthening organizational security.

Bug Bounty Methodology

The instructor explained the standard workflow followed by professional bug bounty hunters, including:

- Target Selection
- Scope Analysis
- Information Gathering
- Reconnaissance

Common Web Application Vulnerabilities

- The instructor discussed the most common vulnerabilities encountered in bug bounty programs, including:
- Cross-Site Scripting (XSS)
- SQL Injection (SQLi)
- Cross-Site Request Forgery (CSRF)
- Server-Side Request Forgery (SSRF)
- Insecure Direct Object Reference

Bug Bounty Tools

Participants were introduced to widely used bug bounty and penetration testing tools, including:

- Burp Suite
- Nmap
- Subfinder
- Amass

Conclusion

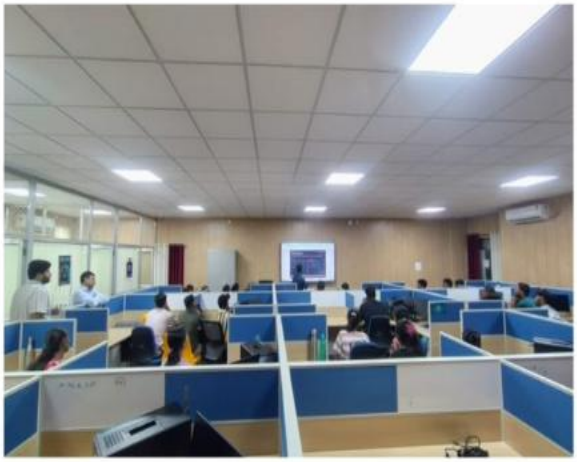
The one-day workshop on **Bug Bounty**, conducted by **Mr. Anas Ahmad** on **20 July 2026 (Monday)**, was highly informative and engaging. It successfully introduced participants to the principles of ethical hacking, reconnaissance methodologies, vulnerability assessment, and responsible disclosure. The workshop strengthened participants' understanding of modern cybersecurity practices and inspired them to further develop their skills in bug bounty hunting and penetration testing.

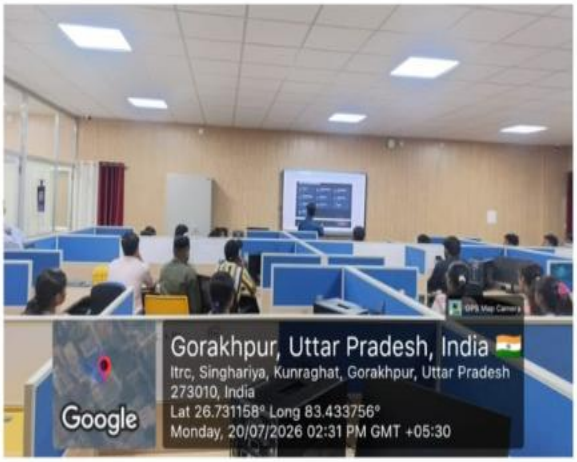
Acknowledgment

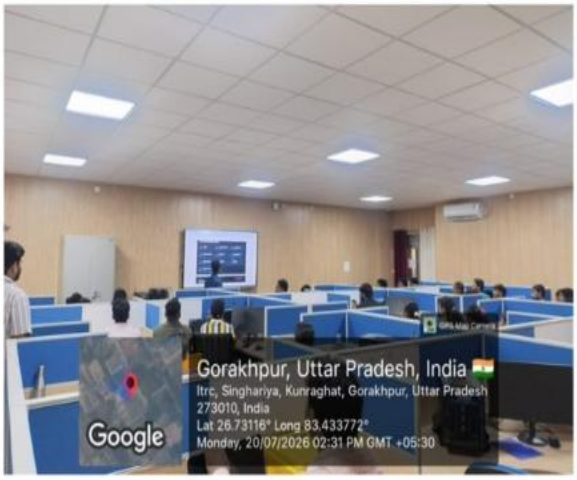
I express my sincere gratitude to **Mr. Anas Ahmad** for conducting such an informative and insightful workshop on **Bug Bounty** on **20 July 2026 (Monday)**. His expert guidance, practical demonstrations, and valuable industry experience greatly enhanced our understanding of ethical hacking and vulnerability assessment. I also extend my heartfelt thanks to the organizers, faculty members, and all participants for their support and active involvement, which contributed significantly to the success of the workshop.


Gorakhpur, Uttar Pradesh, India
Itrc, Singhariya, Kunraghat, Gorakhpur, Uttar Pradesh 273010, India
Lat 26.731157° Long 83.433781°
Monday, 20/07/2026 02:31 PM GMT +05:30
Google






Gorakhpur, Uttar Pradesh, India
Itrc, Singhariya, Kunraghat, Gorakhpur, Uttar Pradesh 273010, India
Lat 26.731158° Long 83.433756°
Monday, 20/07/2026 02:31 PM GMT +05:30
Google


Gorakhpur, Uttar Pradesh, India
Itrc, Singhariya, Kunraghat, Gorakhpur, Uttar Pradesh 273010, India
Lat 26.73116° Long 83.433772°
Monday, 20/07/2026 02:31 PM GMT +05:30
Google

