LAKIREDDY BALI REDDY COLLEGE OF ENGINEERING
(An Autonomous Institution since 2010)
Accredited by NAAC with 'A' Grade & NBA (Under Tier - I),
An ISO 21001:2018, 14001:2015, 50001:2018 Certified Institution
Approved by AICTE, New Delhi and Affiliated to JNTUK, Kakinada
L.B. REDDY NAGAR, MYLAVARAM, NTR DIST., A.P.-521 230.
hodcse@lbrce.ac.in, cseoffice@lbrce.ac.in, Phone: 08659-222 933, Fax: 08659-222931
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Date: 26-03-2025

Report on One-Day Guest lecture
on
Digital Forensics and Block chain in Cryptography

Event Type : One Day Guest lecture
Date : 26-03-2025
Time : 6:30 PM to 8:30PM
Mode : Online
Organized By : Dept. of CSE, LBRCE, Mylavaram, India
Resource person : Mr.T. Ram Kumar, Project Manager, Aditi Software, Hyd.
Convener : Dr.D.Veeraiah, Professor and HOD of CSE
Coordinators : T N V S Praveen, Ch. Srinivasa Rao, M. Swathi
Target : VI-Sem Students (CSE)]
Total Number of students: 210

1.Objective:

The primary objective of this guest lecture is to provide participants with a comprehensive understanding of digital forensics and cybersecurity within the realm of blockchain technology. The session aims to introduce key concepts such as blockchain architecture, security vulnerabilities, forensic investigation techniques, and the legal aspects of cybercrime related to blockchain. Participants will learn how digital forensic methodologies are applied to investigate fraudulent transactions, detect cyber threats, and ensure the integrity and security of blockchain-based systems. Additionally, the lecture will highlight the role of forensic experts in tracing illicit activities such as money laundering, ransomware attacks, and smart contract exploits.

Goal:

The goal of this lecture is to equip attendees with the fundamental knowledge and skills necessary to analyze, detect, and prevent cyber threats targeting blockchain technology. By understanding the principles of blockchain security and digital forensics, participants will be better prepared to handle forensic investigations involving cryptocurrencies, decentralized applications (DApps), and smart contracts. The session will also introduce best practices for securing blockchain networks, mitigating risks, and ensuring compliance with regulatory frameworks. Through real-world case studies, the lecture will provide insights into common cyber threats such as double-spending attacks, private key compromises, and cryptographic vulnerabilities.

2.Outcome of the Event:

By the end of the lecture, participants will:

- Have a clear understanding of the intersection between digital forensics and blockchain cybersecurity.
- Gain knowledge of various security threats, vulnerabilities, and forensic techniques used in blockchain investigations.
- Be familiar with forensic tools and methodologies for tracing blockchain transactions and detecting illicit activities.
- Understand the challenges associated with forensic analysis in decentralized and anonymous blockchain environments.
- Learn about real-world case studies of cyberattacks and forensic investigations related to blockchain technology.
- Acquire practical insights into security best practices, compliance requirements, and risk mitigation strategies for blockchain-based systems.

3.Description of the event:

On 26-03-2025, the CSE department, LBRCE hosted a highly anticipated guest lecture titled **"Digital Forensics and Cybersecurity in Blockchain"**. The session provided a platform to discuss real-world cyber threats, forensic challenges in decentralized systems, and effective security measures for blockchain-based applications.

Key Highlights of the Lecture:

1. **Introduction to Blockchain Technology and Security Concerns:**
    - Mr. T. Ram Kumar began the session with an **overview of blockchain fundamentals**, explaining **its structure, consensus mechanisms, cryptographic principles, and decentralized nature**.
    - He emphasized how **immutability, transparency, and decentralization** make blockchain secure but also introduce **new security challenges**.
2. **Digital Forensics in Blockchain:**
    - The speaker introduced the audience to **digital forensics principles** and their application in blockchain investigations.
    - He explained **how forensic experts trace transactions, detect fraud, and analyze cybercrimes** involving blockchain networks.
    - Common forensic tools used for tracking illicit transactions in cryptocurrencies were discussed.
3. **Cyber Threats and Attack Vectors in Blockchain:**
    - The session covered **various security vulnerabilities** in blockchain systems, including:
        - **51% Attacks** – when a single entity gains majority control over a blockchain network.
        - **Smart Contract Exploits** – security flaws leading to attacks like **reentrancy vulnerabilities**.

        - **Private Key Compromise** – the risks associated with weak private key management.
        - **Ransomware and Money Laundering** – how cybercriminals use cryptocurrencies to evade law enforcement.
4. **Forensic Investigation Techniques:**
    - Mr. Ram Kumar demonstrated how **investigators analyze blockchain transactions** using forensic tools such as **Chainalysis, Elliptic, and Blockchain Explorer**.
    - He explained methods for **tracking stolen or illegal cryptocurrency transactions** and discussed case studies involving **cryptocurrency frauds and dark web transactions**.
5. **Legal and Compliance Aspects:**
    - The discussion included **global regulations and compliance frameworks** governing blockchain and digital forensics.
    - Mr. Ram Kumar highlighted the importance of **GDPR, FATF guidelines, and government policies** in ensuring ethical blockchain forensics practices.
6. **Future Trends in Blockchain Security and Digital Forensics:**
    - The session concluded with an engaging discussion on **emerging cybersecurity trends**, including:
        - The role of **Artificial Intelligence (AI) and Machine Learning** in blockchain security.
        - The **future of quantum-resistant cryptography** in securing blockchain transactions.
        - The **integration of Zero-Knowledge Proofs (ZKPs) for privacy protection**.

4.Impact Analysis:

The guest lecture on **"Introduction to Digital Forensics and Cybersecurity in Blockchain"** had a profound impact on the attendees, particularly students and faculty members interested in blockchain security, forensic investigation, and cybersecurity practices.

The session provided a **comprehensive overview of digital forensics principles** in the context of blockchain technology, enabling participants to understand **how forensic experts track and analyze transactions in decentralized networks**. The emphasis on real-world cyber threats, including **51% attacks, smart contract vulnerabilities, and private key compromises**, helped attendees recognize the risks associated with blockchain-based applications.

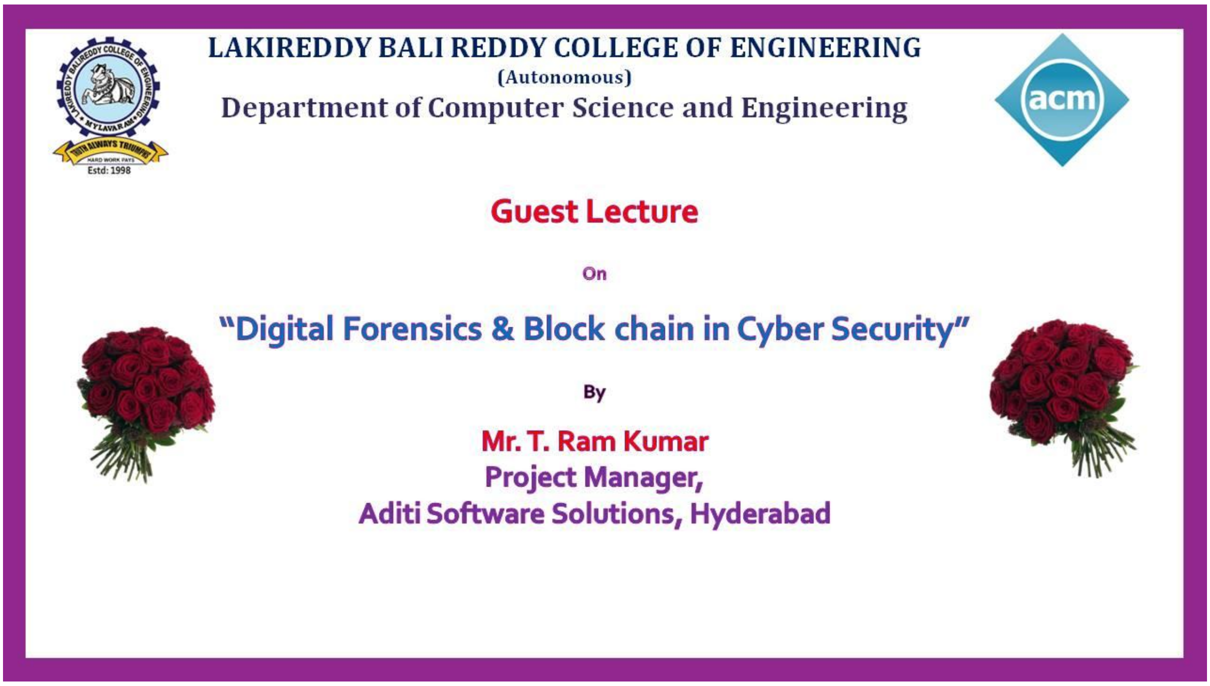
Additionally, the discussion on **forensic investigation techniques using specialized tools like Chainalysis and Elliptic** was particularly valuable for those aspiring to work in the field of blockchain security. The lecture bridged the gap between academic knowledge and industry practices, inspiring many students to consider further research and career opportunities in digital forensics, cybersecurity, and blockchain analytics.

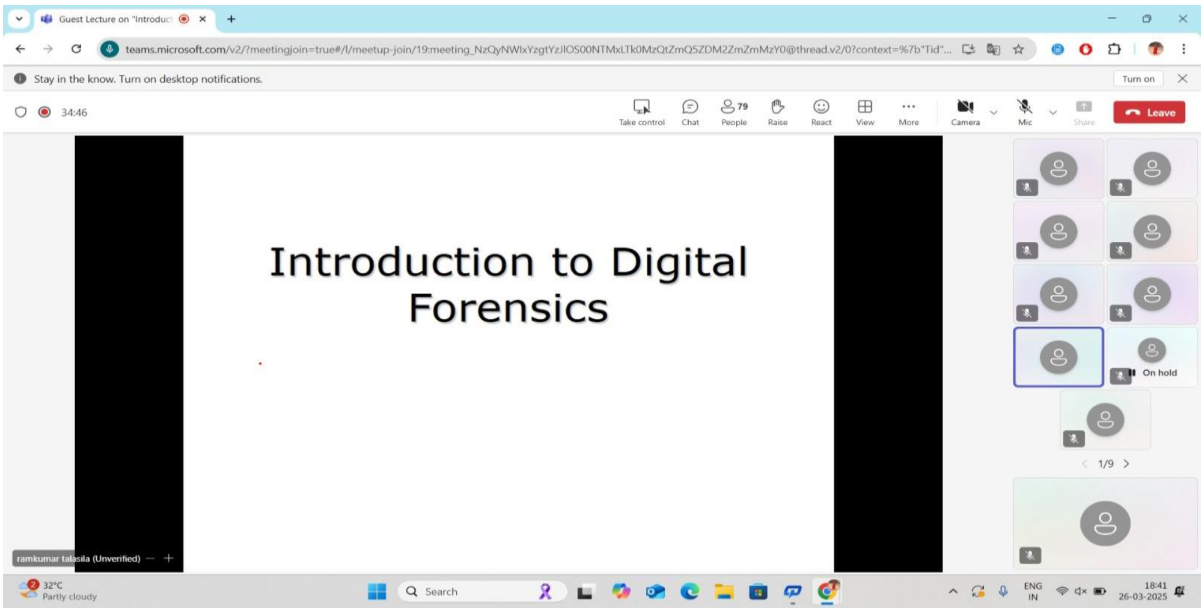
5.Feedback and Suggestions:

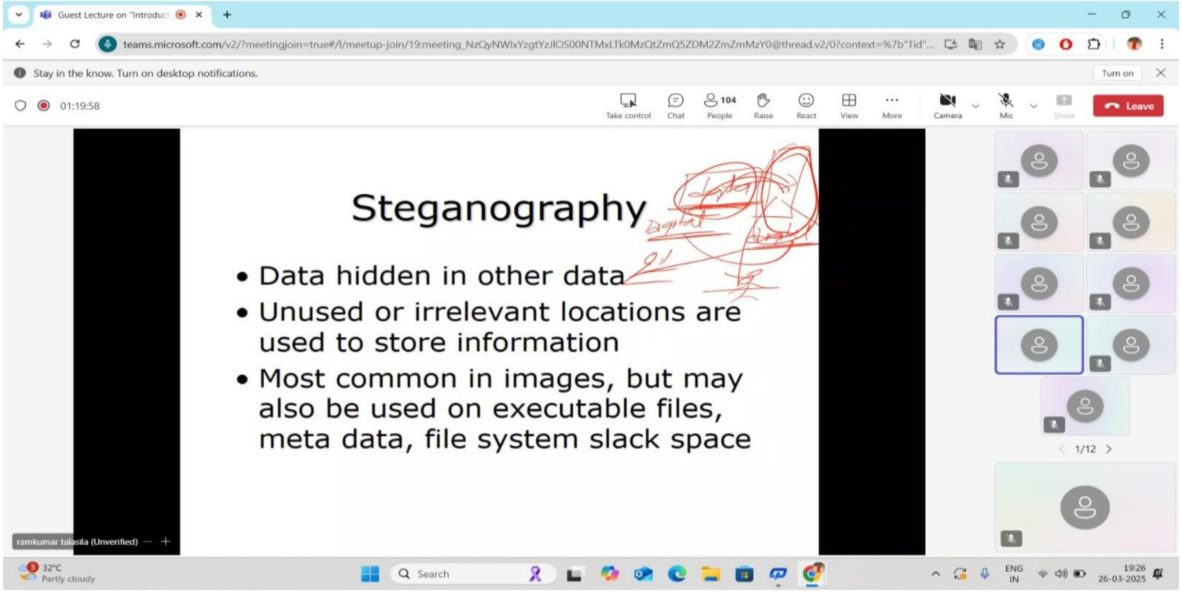
The guest lecture received **overwhelmingly positive feedback** from students, faculty, and research scholars, who appreciated the **depth and clarity** with which the speaker, **Mr. T. Ram Kumar**, explained complex topics. Many students mentioned that the session was **highly engaging and**

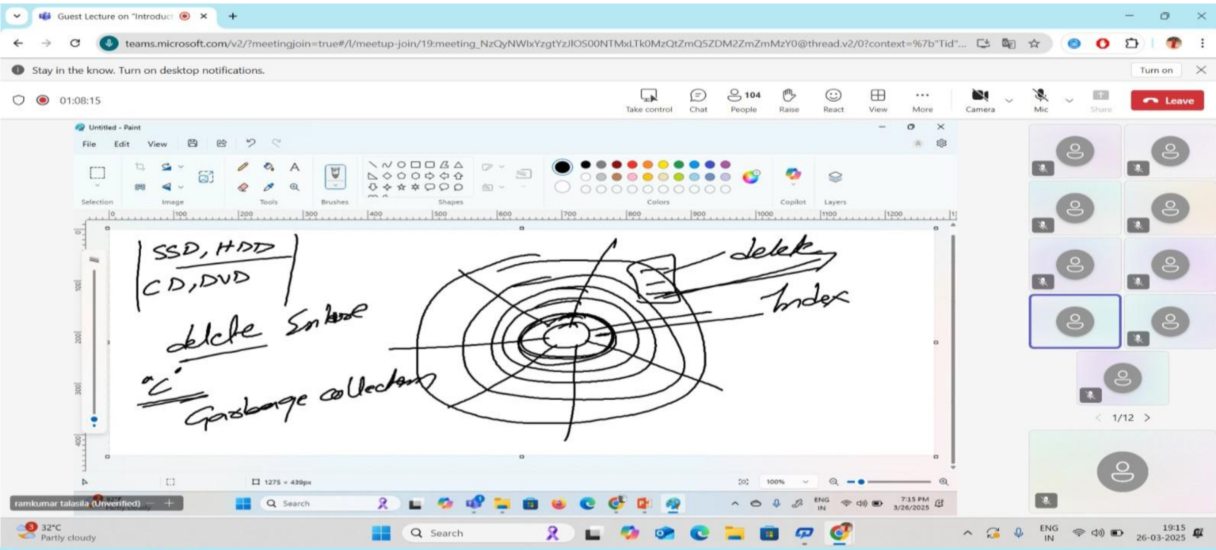
informative, as it not only covered fundamental concepts but also provided **practical applications and real-world case studies** related to blockchain forensics.

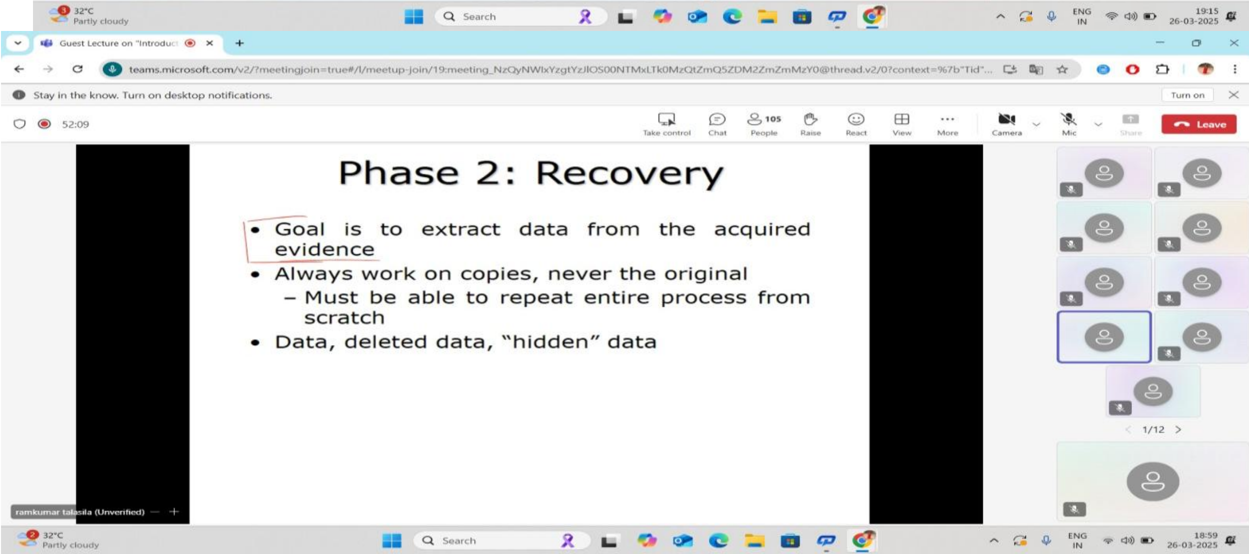
Attendees were particularly impressed by the detailed discussion on **cybercrime investigations involving cryptocurrencies, fraud detection in blockchain transactions, and forensic methodologies used to trace illicit activities**. The Q&A session was another highlight, where participants had the opportunity to interact directly with the speaker and clarify their doubts about **emerging threats, forensic techniques, and industry best practices**.

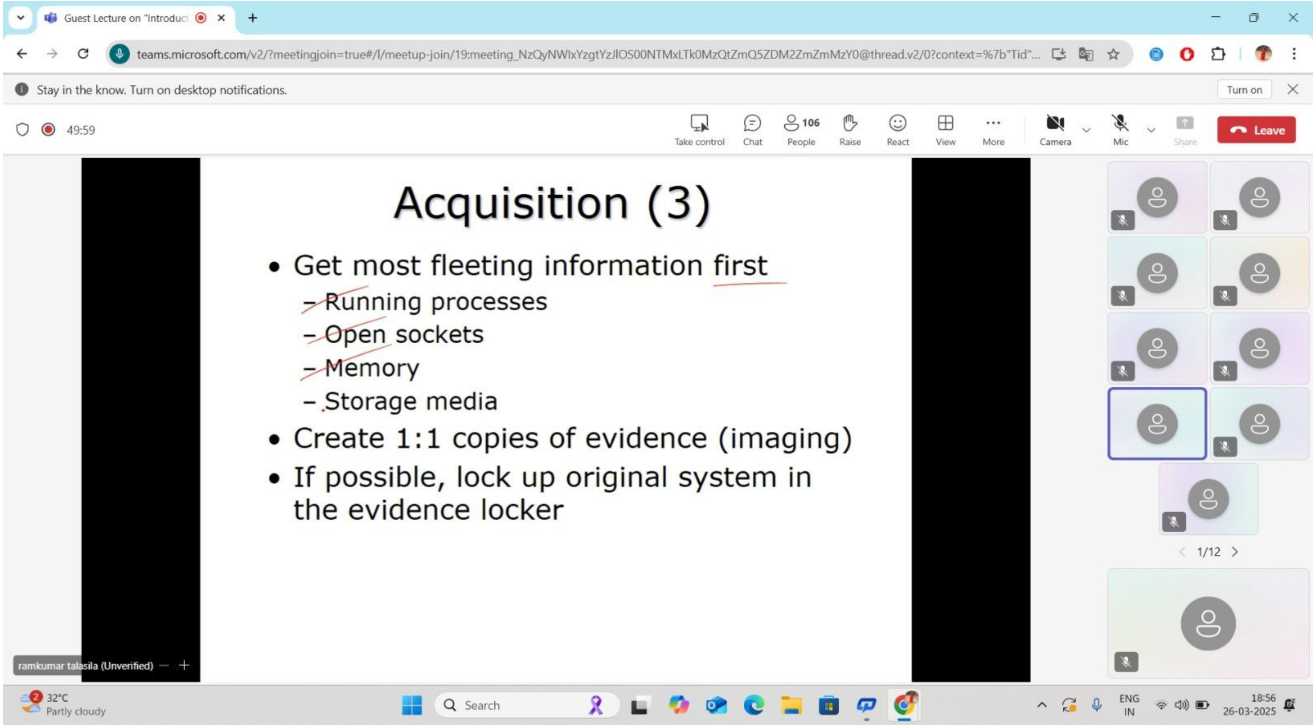





Steganography
Data hidden in other data
Unused or irrelevant locations are used to store information
Most common in images, but may also be used on executable files, meta data, file system slack space


SSD, HDD
CD, DVD
delete
Garbage collection
delete
Index


Phase 2: Recovery
Goal is to extract data from the acquired evidence
Always work on copies, never the original
– Must be able to repeat entire process from scratch
Data, deleted data, "hidden" data



Conclusion:

The guest lecture on **"Introduction to Digital Forensics and Cybersecurity in Blockchain"** was a highly insightful and engaging session that provided participants with a **strong foundation in blockchain security, forensic investigation techniques, and emerging cyber threats**. The lecture successfully bridged the gap between academic knowledge and practical applications, equipping students and faculty with **valuable insights into blockchain vulnerabilities, forensic methodologies, and security best practices**. The event fostered **intellectual curiosity, critical thinking, and professional interest** in the rapidly evolving domain of cybersecurity and digital forensics.

Coordinator	HOD
(T N V S Praveen)	(Dr.D.Veeraiah)