Indira Gandhi Delhi Technical University for Women

(Established by Govt. of Delhi vide Act 09 of 2012)
Kashmere Gate, Delhi-110006

SUTRAM 2026

Problem Statements

Theme: AI-Powered Digital Investigation and Cyber Forensics Technologies for India

Background

India is witnessing unprecedented growth in cyber-enabled crimes, including financial frauds, social media crimes, ransomware incidents, digital impersonation, deepfake-enabled offences, online radicalization, and crimes involving encrypted communication platforms. Investigating agencies and forensic laboratories are increasingly challenged by the volume, diversity, and complexity of digital evidence generated from mobile devices, cloud services, social media platforms, multimedia content, and emerging technologies.

The proposed National Hackathon aims to develop indigenous, AI-enabled cyber forensic solutions that assist Law Enforcement Agencies (LEAs), Cyber Crime Investigation Units, Forensic Science Laboratories (FSLs), and judicial stakeholders in acquisition, analysis, correlation, reconstruction, and reporting of digital evidence while maintaining forensic integrity.

28/10/26

Problem Statement 1

AI-Assisted Mobile Evidence Intelligence Platform

Problem Description

Mobile phones constitute the primary source of evidence in cybercrime investigations. Investigators are often required to examine thousands of artefacts originating from call logs, messages, application databases, browser histories, media files, geolocation records, and cloud-synchronized content.

Existing forensic solutions primarily focus on extraction, while investigators spend significant effort manually identifying relevant evidence.

Challenge

Develop an AI-powered forensic intelligence platform capable of:

- Automated parsing of mobile artefacts.
- Recovery and reconstruction of deleted activities.
- Behavioural profiling of device users.
- Automated generation of investigative leads.
- Timeline reconstruction of user activities.
- Multilingual evidence analysis.

Expected Deliverables

- Mobile artefact analysis engine.
- AI-based evidence prioritization module.
- Automated timeline reconstruction.
- Investigation summary generator.
- Forensic reporting dashboard.

28/10/25

Problem Statement 2

Multimedia Evidence Authentication, Deepfake Detection and Provenance Analysis Framework

Problem Description

The increasing use of Artificial Intelligence and Generative AI technologies has led to a rise in manipulated images, videos, and audio recordings being used for cyber fraud, digital impersonation, misinformation campaigns, online harassment, extortion, and other cyber-enabled crimes. Investigating agencies and forensic laboratories require reliable tools to authenticate multimedia evidence, detect AI-generated content, identify tampering, and establish the origin and evidentiary value of digital media.

Challenge

Develop an AI-powered Multimedia Forensics Platform capable of:

- Detecting deepfakes, synthetic media, and AI-generated images, videos, or audio recordings.
- Identifying manipulation and tampering in multimedia content.
- Verifying the authenticity and integrity of multimedia evidence.
- Performing source attribution and provenance analysis of digital media.
- Generating explainable forensic findings and investigation reports.

Expected Deliverables

The participating teams shall develop and demonstrate one or more of the following:

- Deepfake and Synthetic Media Detection Engine.
- Multimedia Authentication and Tampering Detection Framework.
- Multimedia Provenance and Source Attribution Tool.
- Explainable AI-based Multimedia Forensic Analysis Dashboard.
- Automated Multimedia Forensic Reporting System (PoC/MVP/Prototype).

28/10/26

Problem Statement 3

Digital Evidence Correlation and Crime Reconstruction Engine

Problem Description

Investigations frequently involve heterogeneous evidence originating from mobile devices, social media, CCTV footage, cloud services, financial records, emails, and network logs. Manual correlation of evidence remains labour-intensive and error-prone.

Challenge

Develop an automated evidence correlation platform capable of:

- Correlating evidence from multiple sources.
- Constructing temporal and spatial relationships.
- Identifying associations among suspects, devices, locations, and events.
- Reconstructing digital crime scenes.

Expected Deliverables

- Evidence correlation engine.
- Knowledge graph generation framework.
- Crime reconstruction dashboard.
- Automated event-sequence generator.
- Interactive visual investigation platform.

28/1/2026

Problem Statement 4

AI-Powered Cyber Fraud Investigation and Attribution System

Problem Description

Financial cyber frauds involving UPI, mule accounts, SIM swapping, phishing, investment scams, and social engineering constitute the largest category of cybercrime complaints reported through NCRP and the 1930 helpline.

Investigators must rapidly identify relationships among victims, bank accounts, devices, communication channels, and suspect entities.

Challenge

Develop a forensic investigation framework capable of:

- Entity extraction and resolution.
- Relationship discovery among fraud actors.
- Transaction flow analysis.
- Identification of mule accounts and fraud networks.
- Generation of actionable intelligence.

Expected Deliverables

- Fraud attribution engine.
- Entity-resolution framework.
- Financial evidence correlation dashboard.
- Fraud-network visualization platform.
- Investigative intelligence reports.

28/10/26

Problem Statement 5

AI-Powered Digital Investigation Assistant

Problem Description

The volume of digital evidence available in modern investigations frequently exceeds the capacity of investigators to examine and interpret information manually. Artificial Intelligence offers the potential to transform digital investigations through intelligent evidence exploration and automated reasoning.

Challenge

Develop an AI-powered Digital Investigation Assistant capable of:

- Natural language querying of forensic evidence.
- Context-aware evidence search.
- Automated case summarization.
- Identification of suspicious patterns and anomalies.
- Recommendation of investigative leads.
- Generation of draft case reports.

Expected Deliverables

- Conversational forensic assistant.
- Evidence retrieval engine.
- Automated case diary generator.
- Investigative recommendation module.
- Multilingual interface.

29/10/25

Expected National Outcomes of the Hackathon

The hackathon is expected to generate:

1. Indigenous forensic technology prototypes.
2. AI-enabled digital investigation frameworks.
3. Open datasets and benchmark artefacts.
4. Deployable proof-of-concept tools for LEAs.
5. Research publications and intellectual property.
6. Start-up and technology-transfer opportunities.
7. Capacity building of students, researchers, and practitioners in cyber forensics.

The proposed problem statements are aligned with emerging challenges in mobile forensics, multimedia forensics, AI forensics, cybercrime investigation, and digital evidence analytics.

All teams reaching the final round should be required to demonstrate:

- Working prototype,
- Source code,
- Documentation,
- Investigation dataset,
- Demonstration using a realistic cybercrime scenario,
- Potential deployment roadmap for LEAs.

(Prof. A.K. Mohapatra)
Chief Investigator
ISEA Project

28/10/25