Academic Partner
VIT BHOPAL

Industry Partner
ClearTrail

National CyberShield Hackathon 2025

📅 9th September 2025

📍 SGSITS, Indore

Winners to be rewarded with cash prizes and showcase their solutions at the national law enforcement summit.

Student briefing session + Q&A (Online): 📅 18th Aug'25   🕐 2:00 – 4:00 PM

Last date for registration:	Last date for entries (PPT submissions):	Selection of teams:	Doubt-clearing session for shortlisted teams:
20th Aug'25	1st Sep'25	4th Sep'25	5th Sep'25

Register Now

CIIS 2025
Advancing Investigation in the Digital Age

Main Sponsor
SBI

Academic Partner
VIT BHOPAL

Industry Partner
ClearTrail

National CyberShield Hackathon 2025

Problem Statements

- Detecting drug sales on encrypted platforms

- Tracking hoax bomb threats via digital channels

- Tracing VoIP calls via network metadata

- Mapping A-party to B-party in IPDR logs

- Detecting fake banking APKs

- Detecting anti-India campaigns on digital platforms

- Visual rule-based money laundering pattern detection across layered transactions

- Tool to automatically collect details of the adverse societal impact of social media

- AI model for flagging suspicious transactions using historical data and behaviour profiling.

Timeline & Key Milestones

Student briefing session + Q&A(online)	**18 Aug 2025**
Team members briefing session + Q&A(online)	**22 Aug 2025**
Last date for PPT submissions	**01 Sept 2025**
Selection of teams	**04 Sept 2025**
Doubt clearing session for selected teams	**05 Sept 2025**
Finale	
• SGISITS, Indore	**09 Sept 2025**
• MANIT, Bhopal	**10 Sept 2025**
• JEC, Jabalpur	**11 Sept 2025**
Winners' presentation at CIIS 2025, Bhopal	**17 Sept 2025**

Register Now

Student Police Internships at MP Police : *https://www.mppolice.gov.in/en/community-policing-1*

Cyber Shield Hackathon – CIIS 2025

Organised by Madhya Pradesh Police
Dates: 9-11 September 2025
Hackathon Locations:

- **Shri Govindram Seksaria Institute of Technology and Science (SGSITS), Indore** – 9 September 2025
- **Maulana Azad National Institute of Technology (MANIT), Bhopal** – 10 September 2025
- **Jabalpur Engineering College (JEC), Jabalpur** – 11 September 2025

About the Hackathon

As part of the lead-up to the **Cybercrime Investigation & Intelligence Summit (CIIS 2025)**, the Madhya Pradesh Police is organising the **CyberShield Hackathon – CIIS 2025** from **9-11 September 2025**.

This initiative aims to engage talented young minds in developing innovative solutions to address emerging challenges in cybercrime and digital investigations, working in close collaboration with law enforcement and federal officials.

This student-led innovation event will harness fresh ideas and technological approaches to tackle real-world cybercrime problems faced by law enforcement and prosecution agencies today.

Problem Statements
Participants will be invited to work on one or more of the following six key problem statements:

01. Detecting Drug Sales on Encrypted Platforms

Objective:
Develop a software solution to identify active Telegram, WhatsApp, and Instagram channels or bots involved in drug sales in India, and trace users through IP addresses, mobile numbers, and email IDs.

Description:

Drug traffickers are increasingly using Telegram, WhatsApp, and Instagram to promote and sell synthetic drugs such as MDMA, LSD, and Mephedrone. Many employs customised Telegram bots for automation. The challenge is to detect and track such digital drug trade, and to triangulate digital identifiers to real-world individuals.

Key Tasks:
- Analyse platform usage patterns for drug trafficking.
- Build a keyword database (slang, emojis, hashtags).
- Develop real-time monitoring and content analysis tools.
- Identify bots and automation.
- Extract metadata (IP addresses, email IDs, mobile numbers).
- Correlate identifiers to real identities.
- Design a dashboard and alert mechanism.
- Ensure compliance with Indian legal frameworks.

02. Tracking Hoax Bomb Threats via Digital Channels

Objective:

Build a system to identify and trace individuals responsible for hoax bomb threats shared via email, social media, or messaging applications.

Description:

Using data mining, NLP, and digital forensics, the system should flag suspicious language, extract sender metadata, and profile behaviours to trace and prevent threats. It must remain effective even when anonymity tools are employed.

Key Tasks:
- Study historic threat cases and linguistic markers.
- Build a threat keyword database.
- Monitor platforms in real time.
- Use NLP to detect threatening language.
- Extract IP addresses, device IDs, and metadata.
- Employ device fingerprinting.
- Create behavioural profiles.

- Link digital personas to real identities.
- Build a law enforcement dashboard.
- Ensure compliance with legal norms.

03. Mapping A-Party to B-Party in IPDR Logs

Objective:
Develop a smart tool to extract and identify B-party (recipient) public IP addresses or mobile numbers from IPDR logs to support investigations.

Description:
IPDR logs contain massive volumes of digital communication data. The aim is to automate the extraction of A-party to B-party relationships and present them in an investigator-friendly format.
Key Tasks:
- Understand and normalise various IPDR formats.
- Parse and clean complex log files.
- Identify and map initiator versus recipient communication.
- Filter relevant sessions.
- Visualise connections.
- Highlight anomalies or suspicious patterns.
- Develop advanced query and search features.
- Design a dashboard for investigators.
- Ensure data security and compliance.

04. Tracing VoIP Calls via Network Metadata

Objective:
Build a solution to trace VoIP calls by analysing metadata and signalling protocols (SIP, RTP), even under encryption.

Description:
Encrypted VoIP communications pose significant challenges for tracking. The goal is to detect call patterns, timings, and source/destination identifiers without accessing the call content itself.

Key Tasks:

- Study VoIP protocols (SIP, RTP).
- Build deep packet inspection tools.
- Perform traffic flow and timing analysis.
- Extract relevant metadata (IP address, duration, device information).
- Correlate findings with blacklists or known threat actors.
- Detect anomalous behaviour.
- Develop visualisation and alert tools.
- Maintain privacy and legal compliance.

05. Detecting Anti-India Campaigns on Digital Platforms

Objective:

Design a system to detect anti-India narratives through keyword tracking, user engagement analysis, and influencer detection.

Description:

Coordinated disinformation or propaganda campaigns can harm national interests. This tool should identify key actors and viral content trends to enable early intervention.

Key Tasks:

- Build and maintain a dynamic keyword/hashtag database.
- Use AI/NLP to scan platforms for flagged content.
- Analyse engagement (likes, shares, retweets).
- Detect influential users and content networks.
- Identify signs of coordination or bot-like behaviour.
- Create real-time alerts and dashboards.
- Provide actionable reports to security agencies.
- Respect free speech and legal norms.

06. Tool to Automatically Collect Details of the Adverse Societal Impact of Social Media

Objective:
Develop a tool to collate and compile online harms caused by social media.

Research Focus:
Numerous suicides, homicides, rapes, and public disturbances are linked to social media usage. For example, online friendships have led to rapes and fraud, while online games have been linked to suicides and homicides.

The tool should gather data from open sources and categorise incidents under different crime heads such as suicide, homicide, rape, and criminal intimidation. It should also collect information on mental health disorders caused by social media addiction.

Important Dates & Activities

Activity	Date	Time
Poster release and announcement	12-Aug-25	N/A
Student briefing session + Q&A (online)	18-Aug-25	2:00 – 4:00 PM
Last date for registrations	20-Aug-25	N/A
Last date for student PPT submissions	1-Sep-25	4:00 PM
Final selection of teams for finale	4-Sep-25	4:00 PM
Doubt-clearing session for selected teams	5-Sep-25	N/A
Finale	9-11 Sep 2025	N/A
Shri Govindram Seksaria Institute of Technology and Science (SGSITS), Indore	9-Sep-25	N/A
Maulana Azad National Institute of Technology (MANIT), Bhopal	10-Sep-25	N/A
Jabalpur Engineering College (JEC), Jabalpur	11-Sep-25	N/A
Winners' presentation at CIIS 2025, Bhopal	17-Sep-25	N/A

Panel Composition (3 groups each):

- Professor from VIT Bhopal
- ClearTrail VP – Engineering
- Representative from Madhya Pradesh Police

Why This Hackathon Matters

- Rising digital threats demand innovative, grassroots solutions.
- Student participation brings fresh perspectives and agility.
- Law enforcement gains valuable insight into emerging technologies and problem-solving approaches.
- Promotes academia–law enforcement collaboration on cybercrime investigation and prevention.

Opportunities for Winners

- **Showcase at CIIS 2025:** Present solutions at India's largest cybercrime investigation and intelligence summit.
- **Audience:** Senior officials from law enforcement, judiciary, and prosecution from India and abroad.
- **Exposure:** Visibility to key stakeholders influencing national security, enforcement, and digital policy.
- **Mentorship & Pre-placement Offer:** Mentorship from Mr. Chetan Kalanki, VP – Engineering, ClearTrail Technologies, and a pre-placement offer.

About CIIS

The **Cybercrime Investigation & Intelligence Summit (CIIS)** is India's premier platform for training and collaboration among law enforcement, judiciary, and prosecution. Organised annually by the Madhya Pradesh Police in collaboration with national and international partners, CIIS covers a wide range of subjects including digital forensics, AI, cyber law, cryptocurrency investigations, blockchain, and more.

Website: www.ciisummit.com

CIIS 2025
Advancing Investigation
in the Digital Age

info@ciisummit.com
www.ciisummit.com

Cyber Shield Hackathon – CIIS 2025

Organised by Madhya Pradesh Police
Dates: 9-11 September 2025
Hackathon Locations:

- **Shri Govindram Seksaria Institute of Technology and Science (SGSITS), Indore** – 9 September 2025
- **Maulana Azad National Institute of Technology (MANIT), Bhopal** – 10 September 2025
- **Jabalpur Engineering College (JEC), Jabalpur** – 11 September 2025

About the Hackathon

As part of the lead-up to the **Cybercrime Investigation & Intelligence Summit (CIIS 2025)**, the Madhya Pradesh Police is organising the **CyberShield Hackathon – CIIS 2025** from **9-11 September 2025**.

This initiative aims to engage talented young minds in developing innovative solutions to address emerging challenges in cybercrime and digital investigations, working in close collaboration with law enforcement and federal officials.

This student-led innovation event will harness fresh ideas and technological approaches to tackle real-world cybercrime problems faced by law enforcement and prosecution agencies today.

Problem Statements
Participants will be invited to work on one or more of the following six key problem statements:

01. Detecting Drug Sales on Encrypted Platforms

Objective:
Develop a software solution to identify active Telegram, WhatsApp, and Instagram channels or bots involved in drug sales in India, and trace users through IP addresses, mobile numbers, and email IDs.

Description:
Drug traffickers are increasingly using Telegram, WhatsApp, and Instagram to promote and sell synthetic drugs such as MDMA, LSD, and Mephedrone. Many employs customised Telegram bots for automation. The challenge is to detect and track such digital drug trade, and to triangulate digital identifiers to real-world individuals.

Key Tasks:
- Analyse platform usage patterns for drug trafficking.
- Build a keyword database (slang, emojis, hashtags).
- Develop real-time monitoring and content analysis tools.
- Identify bots and automation.
- Extract metadata (IP addresses, email IDs, mobile numbers).
- Correlate identifiers to real identities.
- Design a dashboard and alert mechanism.
- Ensure compliance with Indian legal frameworks.

02. Tracking Hoax Bomb Threats via Digital Channels

Objective:
Build a system to identify and trace individuals responsible for hoax bomb threats shared via email, social media, or messaging applications.

Description:
Using data mining, NLP, and digital forensics, the system should flag suspicious language, extract sender metadata, and profile behaviours to trace and prevent threats. It must remain effective even when anonymity tools are employed.

Key Tasks:
- Study historic threat cases and linguistic markers.
- Build a threat keyword database.
- Monitor platforms in real time.
- Use NLP to detect threatening language.
- Extract IP addresses, device IDs, and metadata.
- Employ device fingerprinting.
- Create behavioural profiles.

- Link digital personas to real identities.
- Build a law enforcement dashboard.
- Ensure compliance with legal norms.

03. Mapping A-Party to B-Party in IPDR Logs

Objective:
Develop a smart tool to extract and identify B-party (recipient) public IP addresses or mobile numbers from IPDR logs to support investigations.

Description:
IPDR logs contain massive volumes of digital communication data. The aim is to automate the extraction of A-party to B-party relationships and present them in an investigator-friendly format.
Key Tasks:
- Understand and normalise various IPDR formats.
- Parse and clean complex log files.
- Identify and map initiator versus recipient communication.
- Filter relevant sessions.
- Visualise connections.
- Highlight anomalies or suspicious patterns.
- Develop advanced query and search features.
- Design a dashboard for investigators.
- Ensure data security and compliance.

04. Tracing VoIP Calls via Network Metadata

Objective:
Build a solution to trace VoIP calls by analysing metadata and signalling protocols (SIP, RTP), even under encryption.

Description:
Encrypted VoIP communications pose significant challenges for tracking. The goal is to detect call patterns, timings, and source/destination identifiers without accessing the call content itself.

Key Tasks:

- Study VoIP protocols (SIP, RTP).
- Build deep packet inspection tools.
- Perform traffic flow and timing analysis.
- Extract relevant metadata (IP address, duration, device information).
- Correlate findings with blacklists or known threat actors.
- Detect anomalous behaviour.
- Develop visualisation and alert tools.
- Maintain privacy and legal compliance.

05. Detecting Anti-India Campaigns on Digital Platforms

Objective:
Design a system to detect anti-India narratives through keyword tracking, user engagement analysis, and influencer detection.

Description:
Coordinated disinformation or propaganda campaigns can harm national interests. This tool should identify key actors and viral content trends to enable early intervention.

Key Tasks:

- Build and maintain a dynamic keyword/hashtag database.
- Use AI/NLP to scan platforms for flagged content.
- Analyse engagement (likes, shares, retweets).
- Detect influential users and content networks.
- Identify signs of coordination or bot-like behaviour.
- Create real-time alerts and dashboards.
- Provide actionable reports to security agencies.
- Respect free speech and legal norms.

06. Tool to Automatically Collect Details of the Adverse Societal Impact of Social Media

Objective:
Develop a tool to collate and compile online harms caused by social media.

Research Focus:
Numerous suicides, homicides, rapes, and public disturbances are linked to social media usage. For example, online friendships have led to rapes and fraud, while online games have been linked to suicides and homicides.

The tool should gather data from open sources and categorise incidents under different crime heads such as suicide, homicide, rape, and criminal intimidation. It should also collect information on mental health disorders caused by social media addiction.

Important Dates & Activities

Activity	Date	Time
Poster release and announcement	12-Aug-25	N/A
Student briefing session + Q&A (online)	18-Aug-25	2:00 – 4:00 PM
Last date for registrations	20-Aug-25	N/A
Last date for student PPT submissions	1-Sep-25	4:00 PM
Final selection of teams for finale	4-Sep-25	4:00 PM
Doubt-clearing session for selected teams	5-Sep-25	N/A
Finale	9-11 Sep 2025	N/A
Shri Govindram Seksaria Institute of Technology and Science (SGSITS), Indore	9-Sep-25	N/A
Maulana Azad National Institute of Technology (MANIT), Bhopal	10-Sep-25	N/A
Jabalpur Engineering College (JEC), Jabalpur	11-Sep-25	N/A
Winners' presentation at CIIS 2025, Bhopal	17-Sep-25	N/A

Panel Composition (3 groups each):

- Professor from VIT Bhopal
- ClearTrail VP – Engineering
- Representative from Madhya Pradesh Police

Why This Hackathon Matters

- Rising digital threats demand innovative, grassroots solutions.
- Student participation brings fresh perspectives and agility.
- Law enforcement gains valuable insight into emerging technologies and problem-solving approaches.
- Promotes academia–law enforcement collaboration on cybercrime investigation and prevention.

Opportunities for Winners

- **Showcase at CIIS 2025:** Present solutions at India's largest cybercrime investigation and intelligence summit.
- **Audience:** Senior officials from law enforcement, judiciary, and prosecution from India and abroad.
- **Exposure:** Visibility to key stakeholders influencing national security, enforcement, and digital policy.
- **Mentorship & Pre-placement Offer:** Mentorship from Mr. Chetan Kalanki, VP – Engineering, ClearTrail Technologies, and a pre-placement offer.

About CIIS

The **Cybercrime Investigation & Intelligence Summit (CIIS)** is India's premier platform for training and collaboration among law enforcement, judiciary, and prosecution. Organised annually by the Madhya Pradesh Police in collaboration with national and international partners, CIIS covers a wide range of subjects including digital forensics, AI, cyber law, cryptocurrency investigations, blockchain, and more.

Website: www.ciisummit.com

About CIIS

- The **Cybercrime Investigation & Intelligence Summit (CIIS)** is India's premier platform for training and collaboration among law enforcement, judiciary, and prosecution.

- Organized annually by the Madhya Pradesh Police in collaboration with national and international partners.

- Covers a wide range of subjects including digital forensics, AI, cyber law, cryptocurrency investigations, blockchain, and more

About Hackathon

- **As a lead-up** to the Cybercrime Investigation & Intelligence Summit (CIIS 2025), the Madhya Pradesh Police is organizing a Cyber Shield Hackathon - CIIS 2025 on 9-11 September 2025.

- This initiative is designed to engage bright young minds in solving emerging cybercrime and digital investigation challenges, in collaboration with law enforcement and federal officials.

Date & Venue

9 September – SGSITS Indore
10 September – MANIT Bhopal
11 September – JEC Jabalpur

Sponsor

Academic Partner

Industry Partners

CIIS 2025
Advancing Investigation
in the Digital Age

Why Hackathon?

- Rising digital threats demand innovative grassroots solutions.

- Student participation brings fresh perspectives and agility.

- Law enforcement gains insight into emerging technologies and problem-solving approaches.

- Promotes academia–law enforcement collaboration on cybercrime investigation and prevention
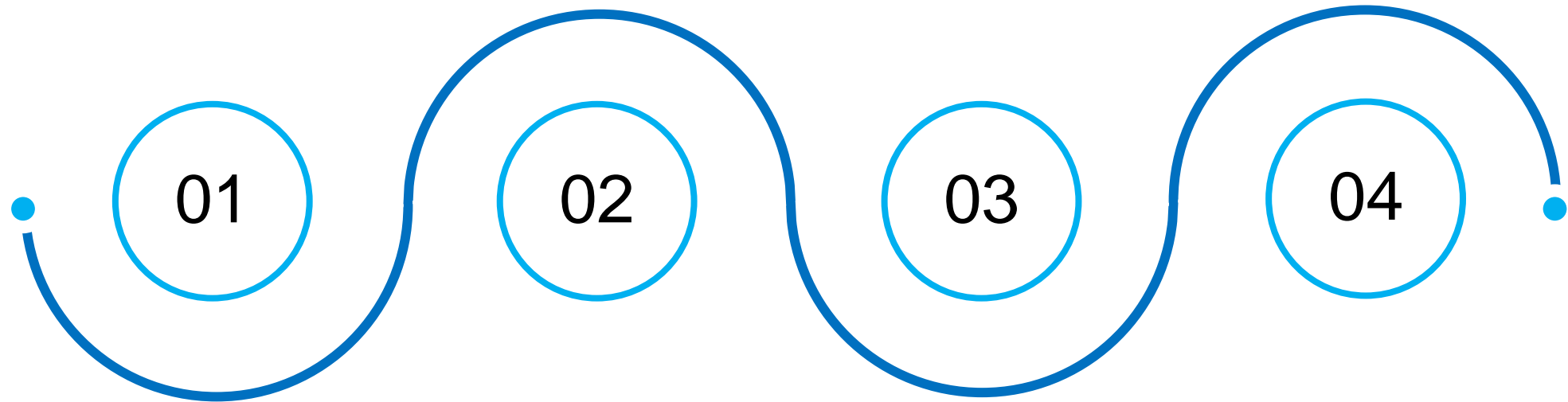
Participation Format

- Expected Teams: 9–12 multidisciplinary student teams

- Structure: 24-hour hackathon

- Deliverables: Tech prototype, solution brief, and presentation

- Evaluation Criteria: Innovation, relevance, scalability, and alignment with law enforcement needs

Process

01   02   03   04

REGISTRATION

Teams of 3-5 students with minimum 1 female participant in each team

SCREENING

1 team from each institute will go for the competition

ROUND 1

Case Review - PPT submitted

FINAL ROUND

Interactive Session/ Presentation Round

Schedule

Poster release and announcement	**12-Aug-25**
Student briefing session + Q&A (online)	18-Aug-25
Last date for registrations	20-Aug-25
Student briefing session + Q&A (online) - Open house for the registered team members	22-Aug-25
Last date for student PPT submissions	1-Sep-25
Selection of teams	4-Sep-25
Doubt-clearing session for selected teams	5-Sep-25
Finale	**9–11 Sep 2025**
Shri Govindram Seksaria Institute of Technology and Science (SGSITS), Indore	9-Sep-25
Maulana Azad National Institute of Technology (MANIT), Bhopal	10-Sep-25
Jabalpur Engineering College (JEC), Jabalpur	11-Sep-25
Winners' presentation at CIIS 2025, Bhopal	17-Sep-25

Problem Statements

1. Detecting Drug Sales on Encrypted Platforms

2. Tracking Hoax Bomb Threats via Digital Channels

3. Mapping A-Party to B-Party in IPDR Logs

4. Tracing VoIP Calls via Network Metadata

5. Detecting Anti-India Campaigns on Digital Platforms

6. Tool to Automatically Collect Details of the Adverse Societal Impact of Social Media

Winner Rewards

- **Prizes for the Winners:** Great Cash Prizes from Sponsors and a Pre-Placement Offer from ClearTrail Technologies.

- **Showcase at CIIS 2025:** Present solutions at India's largest cybercrime investigation and intelligence summit.

- **Audience:** Senior officials from law enforcement, judiciary, and prosecution from India and abroad.

- **Mentorship & Recognition:** Opportunities for further development, incubation, and collaboration.

Thanks