CSDFC
CYBER SECURITY AND DIGITAL FORENSICS CENTRE
CHANAKYA NATIONAL LAW UNIVERSITY (CNLU), PATNA

CHANAKYA NATIONAL LAW UNIVERSITY , PATNA

PRESENTS

THREE-DAY CERTIFICATE COURSE ON

CYBER CRIMES INVESTIGATION & DIGITAL FORENSICS USING OSINT TOOLS AND TECHNIQUES

IN BLENDED* MODE **(ONLINE OR IN-PERSON)**

REGISTER TODAY

Course Fee: ***Rs. 10,000/- (INR)***
Eligibility: ***Candidates who are pursuing graduation or have graduated are eligible to register.***
Programme Dates: ***March 13–15, 2026 (3 Days)***
Last date to apply: 9 ***March 2026***
Intake: ***45 per batch***
Note: ***Admission will be first come first served basis.***

SCAN TO APPLY

***Blended mode indicates that participants have the option to attend the course either online by joining meeting-links virtually or in person (Physical) at the CNLU Patna campus.**

(A PRACTICAL ORIENTED, HANDS-ON, SKILL DEVELOPMENT PROGRAM)

ABOUT CNLU

Established on 15 July 2006 under the Chanakya National Law University Act, 2006 and recognised under Sections 2(f) and 12(B) of the UGC Act, CNLU stands as a premier institution committed to academic excellence, constitutional values, and community service. Located on an 18-acre green campus at Nyaya Nagar, Mithapur, Patna, the University provides a vibrant learning environment supported by modern infrastructure, residential facilities, IT-enabled campus, medical services, counselling support, and strong industry–judiciary engagement.

Guided by the ideals of constitutional morality, Fundamental Duties, professional ethics, social responsibility, and inclusiveness, CNLU nurtures future-ready legal professionals through rigorous academics, practical exposure, and mentorship by eminent judges, senior advocates, and distinguished academicians. The University exemplifies financial autonomy with accountability and delivers education aligned with national priorities and global standards.

ABOUT THE PROGRAMME

The three-day certificate course on “Cyber Crimes Investigation and Digital Forensics using Open Source Investigation (OSINT) Tools and Techniques” is designed to provide participants with a comprehensive understanding of cyber crime investigation frameworks, digital evidence handling, and the practical application of Open-Source Intelligence (OSINT) in cyber crime investigations. The course integrates legal principles, forensic science, and technology-driven investigative tools to bridge the gap between theory and practice.

Key Highlights

- Fundamentals of Cyber Security, cyber laws, and regulatory frameworks
- Digital Forensics techniques: evidence acquisition, preservation, analysis, and reporting
- Understanding cybercrimes, investigation workflows, and courtroom presentation of digital evidence
- Exposure to real-world case studies and tools used by investigators and legal professionals

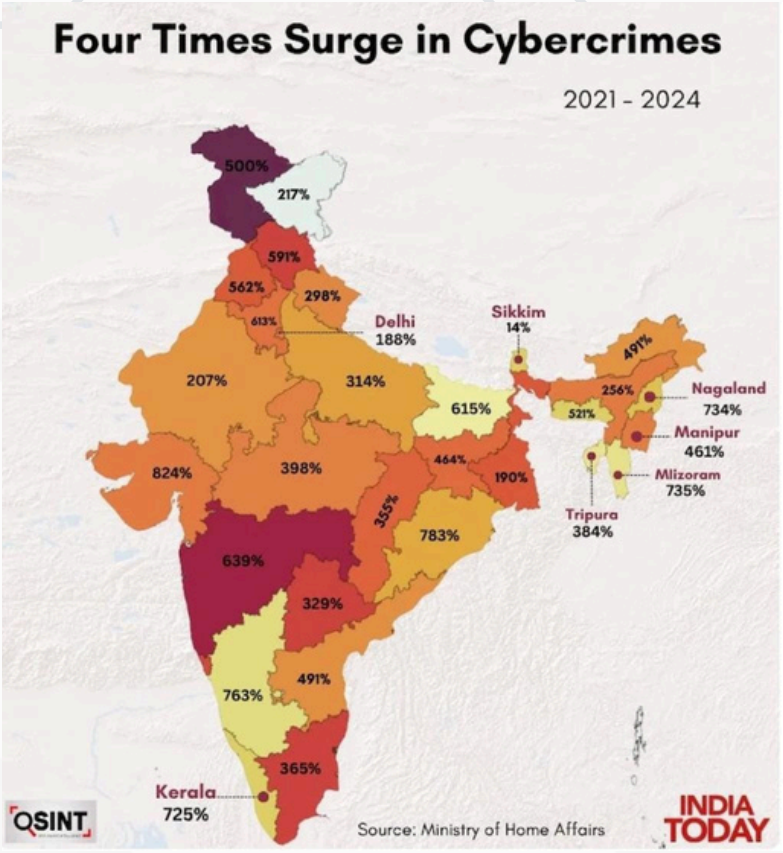
Who Should Attend

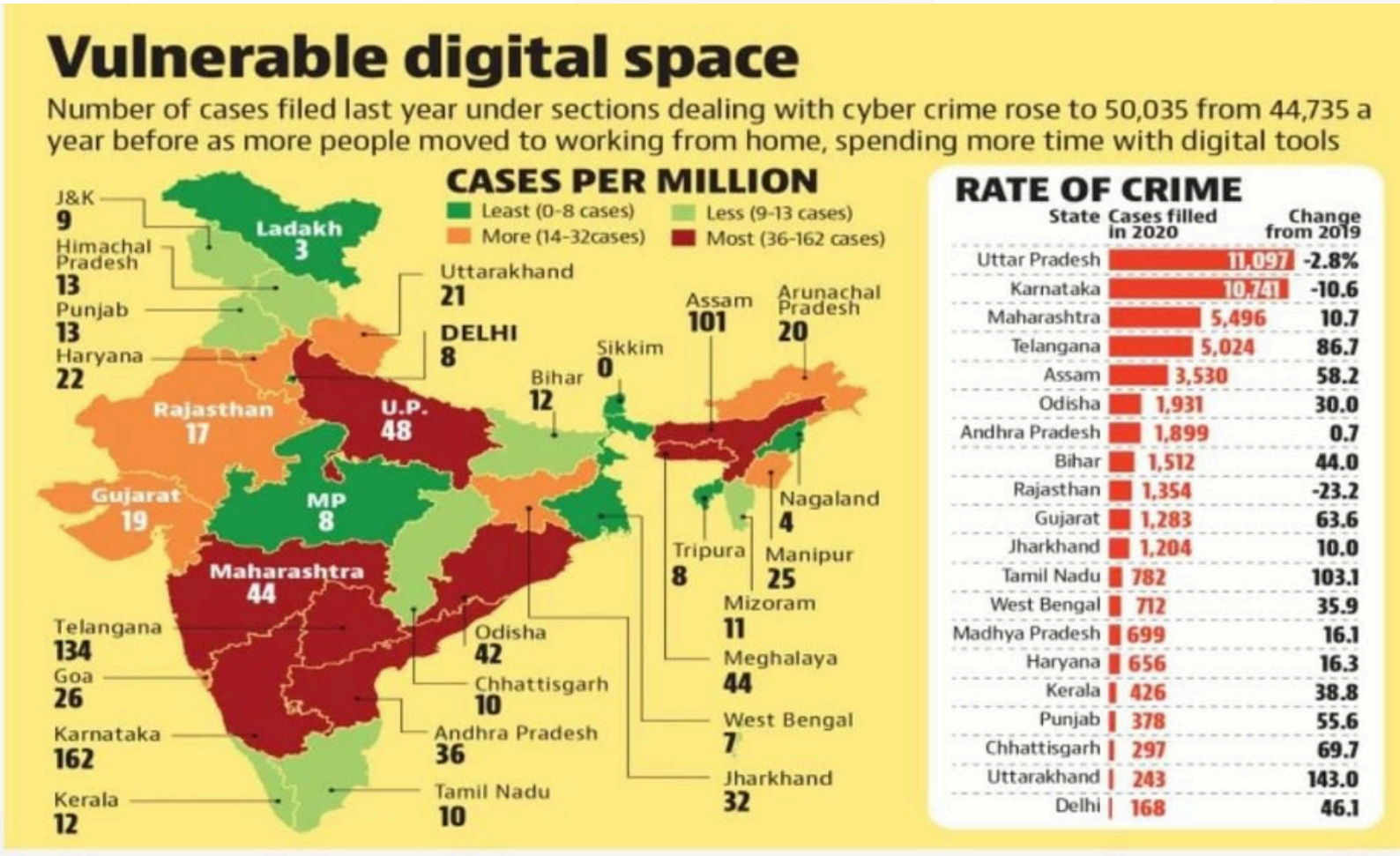
- Law students and legal practitioners
- Police and investigative officers
- IT professionals, compliance officers, and cybersecurity enthusiasts
- Academicians and researchers interested in cyber law and forensics

This programme reflects CNLU’s commitment to skill-based, contemporary legal education, empowering participants with knowledge that is immediately relevant to careers in law enforcement, legal practice, corporate compliance, and cyber investigations.

WHY THIS COURSE

Cybercrime conviction rates remain strikingly low worldwide, and particularly in India, often falling below 5%. This is largely due to challenges such as complex digital evidence, jurisdictional hurdles, and the fact that many offenses are bailable. In India, conviction rates have at times been reported around 27.6%, yet experts argue the real figure is closer to under 1%, as smaller frauds often go unprosecuted and forensic capabilities remain weak—even as cybercrime incidents continue to rise. Although broader court statistics sometimes show higher conviction percentages (for example, 54.2% in 2022 across all cases), these numbers reflect general judicial efficiency rather than cybercrime specifically. In reality, cybercrime convictions remain critically low, with only a small fraction of cases resulting in final punishment.





LEARNING OUTCOMES

After completing this course, participants shall be able to

- To provide foundational understanding of cyber crimes by familiarizing participants with the nature, typologies, and evolving trends of cyber offences and their impact on individuals, institutions, and the criminal justice system.
- To introduce the principles and processes of digital forensics, including identification, preservation, collection, examination, analysis, and reporting of digital evidence in accordance with legal and procedural standards.
- To develop awareness of the legal and ethical framework governing cyber crime investigation, digital evidence handling, and the admissibility of electronic evidence under Indian cyber laws.
- To impart practical knowledge of Open Source Intelligence (OSINT) and its role in cyber crime investigation, intelligence gathering, and evidence correlation.
- To train participants in the use of OSINT tools and techniques for investigating cyber crimes related to social media, email, websites, financial frauds, and online identities.
- To integrate OSINT findings with digital forensic analysis for effective reconstruction of cyber crime incidents and attribution of online activities to individuals or entities.
- To familiarize participants with network, email, and social media forensics, enabling them to analyze communication trails, identify spoofing/phishing attempts, and trace digital footprints.
- To enhance investigative skills through hands-on exercises and case studies, simulating real-world cyber crime scenarios and multidisciplinary investigative approaches.
- To develop competency in digital forensic and OSINT-based reporting, including preparation of investigation reports suitable for legal scrutiny and court proceedings.
- To sensitize participants to emerging challenges and future trends such as dark web crimes, cryptocurrency misuse, deepfakes, and advanced cyber fraud techniques.

TOPICS COVERED

- Cyber Crimes: Concepts and Legal Framework
- Digital Evidence and Forensic Principles along with Digital Forensics Investigation Process
- Understanding Computer Forensics, Network Forensics, Email Forensics, Web Browser Forensics, Mobile Device and Application Forensics, Cloud Forensics Etc
- Introduction to Open-Source Intelligence (OSINT) Tools and Techniques
- Social Media and Web Investigation-(SOCMINT)
- Image, Video, and Multimedia Investigation
- Dark Web and Emerging Cyber Threats
- OSINT in Financial and Online Fraud Investigation
- Electronic / Digital Evidence chain of custody, legal admissibility, Reporting and Courtroom Presentation

SESSION WISE PRACTICAL, HANDS ON TECHNOLOGICAL CONCEPTS DEMONSTRATED IN THE THREE DAYS PROGRAM ARE AS FOLLOWS: -

DAY 1: Fundamentals of Cyber Crime Investigation & Open-Source Intelligence (OSINT)

Session 1: Cyber Crimes Landscape & Legal Framework

·Evolution and typology of cyber crimes
·Financial frauds, social media crimes, cyber stalking
·Legal provisions:
- o Information Technology Act, 2000
- o Bharatiya Nyaya Sanhita & Bharatiya Sakshya Adhiniyam (overview)

·Role of investigators, courts, and forensic experts

Session 2: Digital Evidence & Forensic Investigation Process

·Types and sources of digital evidence
·Locard's Exchange Principle (Digital Context)
·Digital Forensics Lifecycle:
- o Identification
- o Preservation
- o Collection
- o Examination
- o Analysis
- o Reporting

·Chain of custody and evidentiary integrity

Session 3: Introduction to Open Source Intelligence (OSINT) for Cyber Crime Investigation

·Concept and scope of OSINT
·OSINT vs covert intelligence
·Legal, ethical, and privacy considerations
·OSINT categories:
- o Web & search engine intelligence
- o Social media intelligence
- o Domain & IP intelligence

Session 4: OSINT Tools – Demonstration & Practical Orientation

·Advanced Google Dorking techniques
·WHOIS, DNS, and IP lookup tools
·Username and email reconnaissance
·Hands-on OSINT exercises (guided)

DAY 2: Digital, Network & Social Media Forensics with OSINT

Session 5: Computer & Browser Forensics

·File system artifacts and user activity traces
·Browser artifacts (history, cache, cookies)
·Correlation of browser artifacts with OSINT findings
·Introduction to forensic tools (FTK / Autopsy – demo)

Session 6: Mobile & Application Forensics

·Mobile device forensics overview
·App-based crimes and artifacts
·Social media and messaging application analysis
·OSINT correlation with mobile evidence

Session 7: Network & Email Forensics

·Network forensics fundamentals
·Traffic capture and analysis (Wireshark – demo)
·IP address tracing and geolocation
·Email forensics:
o Header analysis
o Spoofing and phishing detection
o OSINT-based sender profiling

Session 8: Social Media & Web Investigation

·Investigation of social media crimes
·Fake profile detection and attribution
·Timeline and activity reconstruction
·Website footprinting and metadata analysis

DAY 3: Advanced Open-Source Intelligence (OSINT), Case Studies & Reporting

Session 9: Image, Video & Multimedia Investigation

·Image and video forensics basics
·Metadata extraction
·Reverse image search techniques
·Deepfake awareness and challenges

Session 10: Dark Web & Financial Cyber Crime Investigation

·Deep & Dark Web structure (overview)
·Cyber crime marketplaces and modus operandi
·OSINT in financial frauds using Maltego :
o Phishing
o Investment scams
o UPI frauds
·Cryptocurrency tracing (introductory concepts)

Session 11: Cyber Crime Case Studies & Practical Exercise

·Real-world cyber crime investigation case studies
·End-to-end OSINT-driven investigation exercise
·Group activity: linking digital footprints across platforms

Session 12: Reporting, Courtroom Presentation & Assessment

·Digital Forensics & Investigation report writing
·Expert witness testimony and courtroom challenges
·Future trends in cyber crime investigation
·Assessment, feedback & certification

MODE OF DELIVERY

- **Mode of Delivery:** Blended (both Online and In-Person) Sessions commence at 10AM and ends at 5PM, all the three days of the course delivery.
- **Location for In-Person mode:** Cyber Forensics Lab, Cyber Security and Digital Forensics Center - CSDFC, CNLU Campus, Patna.
- **For Online**: Links for joining the course online will be sent to registered email-id.
- **Registration Process:** Submission of Online Application Form along with the requisite fee.

Course Fee: ***Rs. 10,000/- (INR)***
Eligibility: ***Candidates who are pursuing graduation or have graduated are eligible to register.***
Programme Dates: ***March 13–15, 2026 (3 Days)***
Last date to apply: 9 ***March 2026***
Intake: ***45 per batch***
Note: ***Admission will be first come first served basis.***

REGISTER TODAY

CLICK HERE TO APPLY

***Blended mode indicates that participants have the option to attend the course either online by joining meeting-links virtually or in person (Physical) at the CNLU Patna campus.**

(A PRACTICAL ORIENTED, HANDS-ON, SKILL DEVELOPMENT PROGRAM)

SPEAKERS

Prof. (Dr.) Faizan Mustafa

Mr. Ram Mohan,
SP -Cyber Crimes, AP Police

Dr. Rajesh Kumar,
I4C Expert and Digital Forensics Examiner

Mr. B .Md. Irfan,
Professor of Practice – Cyber security

Dr. Kumar Gaurav

Dr. Sadaf Fahim
Assistant Professor of Law

Mr. Rajesh Gopal,
Cyber Security Expert

(A PRACTICAL ORIENTED, HANDS-ON, SKILL DEVELOPMENT PROGRAM)