VERSION 2.0

ADVANCED CERTIFICATE PROGRAM

IN

CYBER THREATS, DIGITAL FORENSICS & LEGAL RESPONSE

UTTAR PRADESH
STATE INSTITUTE OF FORENSIC SCIENCE
LUCKNOW

WWW.UPSIFS.AC.IN

ABOUT US

Uttar Pradesh State Institute of Forensic Science (UPSIFS), Lucknow established by the Government of Uttar Pradesh, a newly created institute spread over fifty acres of land, is a flagship project of the Government of Uttar Pradesh, and was inaugurated by the Hon'ble Prime Minister of India in March 2024. UPSIFS is affiliated to the National Forensic Science University, Gandhinagar. The institute has built-up world-class laboratory facilities. We have successfully completed the First Batch (2023-24) of 05 programs in July, 2024. The new academic session 2024-25 has commenced from 21st August, 2024 for graduation and post-graduation degrees in fields of Forensic Science, Computer Science and Cyber Security and Legal Studies. We have introduced a new concept- "LAW with LABS" for integrating legal studies with hands-on training of law students in the fields of DNA, Fingerprint, Document Forensic, Ballistics, Cyber Security etc. so that they may understand fine nuances of science and law. UPSIFS is devoted to create “Forensic-as-a-Service” (FaaS).

INTRODUCTION TO THE PROGRAM

Advanced Certificate Program in Cyber Law and Cyber Forensics is one of the most unique programs in India, offering a seamless blend of theoretical knowledge and practical skills essential for understanding and addressing the complexities of cyber law and digital forensics after cyber attacks. As a three-credit program, it provides participants with a valuable edge for career advancement in legal, forensic, and cybersecurity domains. UPSIFS takes pride in pioneering this innovative program, which stands out for its multidisciplinary teaching approach, featuring industry experts, seasoned police personnel, and accomplished advocates. This holistic learning experience equips participants with both academic insights and practical expertise, making it a standout opportunity for those seeking to excel in this dynamic field.

The program offered by Uttar Pradesh State Institute of Forensic Science (UPSIFS), Lucknow, is an intensive program designed to meet the urgent need for skilled professionals in the field of cyber law and digital forensics. As cyber threats and digitalcrimes escalate globally, understanding both legalframeworks and forensic methods is crucial for safeguarding digital spaces and enforcing justice. This three-month program integrates foundational knowledge of cyberlaw with hands-on forensic training, making it an ideal learning experience for forensic, ethical hacker & law students, professionals, and individuals interested in cyber law, forensic and investigation. The program's hybrid format combines 50 sessions, including lectures, case studies, and practical work, ensuring participants gain both theoretical knowledge and practical experience. Participants will learn about approach of attacker, cybercrime legislation, evidencecollection, digital contracts, and data protection laws, while also mastering forensic tools like FTK Imager and Autopsy. Guided by experts from academia and law enforcement, this program promises a holistic understanding of the intersections between technology and law, equipping participants to analyze, investigate, and navigate complex cyber law scenarios confidently. Successful completion grants participants a certificate and opens doors to careers in cyber law, cybersecurity consultancy, and regulatory compliance across various sectors.

WHY THIS PROGRAM

In today's interconnected digital landscape, technology drives innovation and daily interactions—from academic research and financial transactions to governmental processes. However, this same connectivity has spawned a surge in cybercrimes such as data breaches, financial fraud, and ransomware attacks. Global incidents like the WannaCry ransomware epidemic and high-profile corporate breaches have underscored the urgent need not only to defend against these threats but also to understand the underlying mindset of cyber adversaries.

This advanced certification program is uniquely designed to bridge the gap between the attacker's perspective and the necessary defensive, forensic, and legal measures to counter these threats. By delving into the very strategies employed by cybercriminals, the program equips professionals with the insight required to not only safeguard personal and corporate data but also to collect, analyze, and legally deploy digital evidence that withstands judicial scrutiny.

" THINK LIKE AN ATTACKER. DEFEND LIKE A CHAMPION. TRANSFORM DIGITAL CHAOS INTO COURTROOM VICTORY"

TARGET AUDIENCE

This program is designed to enable legal experts to understand technical nuances and technical experts to grasp legal intricacies, ensuring they can effectively contribute to the criminal justice system. It is beneficial for:

- **Advocates and Legal Professionals**: To expand their understanding of cyber and digital forensic aspects.
- **Cyber Experts and Forensic Analysts**: To gain insights into the legal frameworks relevant to their expertise.
- **Police Personnel**: To enhance their proficiency in handling cyber-related cases.
- **Judiciary Members**: To better comprehend the technical aspects of cases they adjudicate.
- **Students of Law, Cyber technology and Forensic Sciences**: To develop an interdisciplinary skillset for a competitive edge.
- **Awakened Individuals**: Anyone interested in understanding the nuances of cyber laws and digital know-how.
- **Industry Professionals and Managers**
- **Bureaucrats and Administrator**
- **Management Professionals**

This program is a valuable resource for all those keen on bridging the gap between law and technology in the context of the criminal justice system.

PROGRAM OVERVIEW

- **Duration**: 3 Month (12 weeks)
  *[Classes to be scheduled on Fridays and Saturdays
  from 05:30 PM to 07:30 PM IST]
- **Program Format**: Lectures, Case Studies, Hands-on Practice
- **Level**: An Advanced Certificate Program (Advanced and in-depth understanding of the concepts)
- **Credit**: 3 Credit program (NEP, 2020) (45+5= 50 hours of Teaching & Assessment)
- **Mode**: Online
- **Medium:** English
- **Commencement**: From 27th June, 2025
- **Registration Deadline:** On 15th June, 2025

FEE STRUCTURE AND ELIGIBILITY

- **Program Fee**: ₹ 12,000/-
- Fee Non- Refundable
- For bulk participation and fees related query please contact at our e-mail id : **trainings@upsifs.ac.in**

- **Mode of Payment**: UPI, NEFT, Online Banking

- **Basic Eligibility for the program**: This certificate program is open to lawyers, students, cyber security enthusiasts, and professionals from law, IT, forensic science, and allied fields. Designed for all skill levels, it covers both basic concepts and advanced applications in law and digital forensics. There is no binding of education qualification, but candidates must have workable domain knowledge .

PROGRAM OBJECTIVES

- Understand the Adversary's Mindset: Examine the offensive tactics, motivations, and anti-forensic techniques employed by cyber attackers. Learn to think like an adversary in order to anticipate, identify, and thwart potential cyber intrusions.
- Master Advanced Digital Forensics: Develop the ability to detect, analyze, and recover digital evidence—even when deliberately concealed by attackers—using state-of-the-art forensic tools and methodologies, while ensuring evidence integrity and proper chain-of-custody.
- Integrate Cyber Law with Forensic Investigation: Analyze key legislation, case law, and regulatory frameworks that govern digital evidence and cybercrime. Learn how to effectively transform technical forensic findings into legally robust cases.
- Enhance Investigative & Legal Countermeasures: Equip yourself with practical skills to conduct comprehensive digital investigations. Bridge the gap between technical evidence and courtroom presentation, ensuring that every digital trace can be leveraged to prosecute cybercriminals.

LEARNING OUTCOMES

- Understand and apply cyber laws to real-world scenarios.
- Analyze cybercrimes from legal and forensic perspectives.
- Utilize basic cyber forensic tools and methods for investigation.
- Evaluate the challenges and emerging trends in cyber law and forensics.

TEACHING PEDAGOGY

- **Lectures**: Core legal principles and forensic methodologies.
- **Case Studies**: Legal analysis of the leading judgments of the Hon'ble Supreme Court and High Courts.
- **Tutorials**: Group discussions, problem-solving, and debates.
- **Practical Sessions**: Hands-on training in cyber forensic tools.

ASSESSMENT METHODS

- MCQ based test after every module

CURRICULUM OUTLINE

MODULE 1

Week 1: Foundations of Cyber Intrusions, Forensics, and Law

- **Introduction to the attacker's mindset and the Cyber Kill Chain**
- **Fundamentals of digital forensics (evidence collection, preservation)**
- **Overview of international & national cyber laws (unauthorized access, privacy)**
- **Hands-on: Simulated breach scenario analysis and real-world case study**

Week 2: Reconnaissance and Open-Source Intelligence (OSINT)

- **Techniques for passive/active reconnaissance (search engines, social media, network scans)**
- **OSINT methodologies for footprinting and attribution**
- **Legal boundaries in information gathering (privacy, CFAA considerations)**
- **Exercise: OSINT treasure hunt with documentation of potential vulnerabilities.**

MODULE 2

Week 3: Social Engineering and Phishing Attacks

- **Tactics of social engineering (phishing, spear-phishing, baiting, deepfakes)**
- **Forensic approaches for analyzing phishing attempts and digital traces**
- **Legal implications: Fraud, unauthorized access, and identity theft statutes**
- **Activity: Phishing simulation and analysis with case study review**

Week 4: Exploitation Techniques and Gaining Access

- **Common exploitation methods (vulnerability exploitation, SQL injection, zero-day attacks)**
- **Forensic detection: Analyzing logs, payloads, and incident reporting**
- **Legal context and liability issues surrounding unauthorized entry**
- **Lab: Vulnerability exploitation exercise and discussion of a high-profile breach**

MODULE 3

Week 5: Malware, Trojans, and Persistence Mechanisms

- **Deployment of malware for persistence (RATs, ransomware, rootkits)**
- **Malware analysis: Static/dynamic techniques and identifying indicators of compromise**
- **Legal considerations for malware creation and deployment**
- **Lab: Malware forensic exercise and case study on WannaCry or Stuxnet**

Week 6: Post-Exploitation, Lateral Movement & Anti-Forensics

- **Techniques for lateral movement, privilege escalation, and anti-forensics**
- **Forensic countermeasures: Timeline analysis, log recovery, and evidence triage**
- **Legal issues: Obstruction of justice, tampering, and chain-of-custody challenges**
- **Exercise: Intrusion trace hunting and review of real case studies (e.g., Sony Pictures hack)**

MODULE 4

Week 7: Incident Response and Digital Forensic Methodology

- Overview of Incident Response phases (Preparation, Detection, Containment, Eradication, Recovery, Post-Incident)
- Formal digital forensic processes: Evidence identification, collection, and reporting
- Emphasis on maintaining evidence integrity (chain-of-custody, admissibility)
- Simulation: Tabletop exercise culminating in an incident report

Week 8: Network Security Monitoring and Cloud Intrusions

- Network forensics: Packet analysis, IDS/IPS, and SIEM systems for threat hunting
- Cloud attacks: Analyzing misconfigured storage, API exploits, and provider logs
- Jurisdictional challenges and legal issues in cross-border data investigations
- Lab: Cloud breach investigation exercise with a case study review (e.g., Capital One hack)

MODULE 5

Week 9: Mobile Device and IoT Forensics and Security

- Attacks targeting mobile devices and IoT endpoints (malicious apps, SIM swapping, default credentials)
- Forensic methods for extracting and analyzing data from mobile/IoT devices
- Legal considerations: Privacy expectations, search warrants, and cross-jurisdiction data rights
- Activity: Mobile forensics demo and case study analysis (e.g., smart speaker evidence)

Week 10: Legal Frameworks, Cybercrime Laws, and Ethics

- Key cybercrime laws & regulations (IT Act, IT Rules, Digital Personal Data Protection Act, CFAA, EU directives, Budapest Convention, GDPR)
- Cyber Crime: Classification of cybercrimes, Conventional vs. Contemporary,
- International jurisdiction and cooperation in digital evidence gathering
- Admissibility of digital evidence and expert testimony preparation
- Interactive Session: Guest lecture/Q&A and landmark cybercrime legal case review

MODULE 5

- **Blocking of unauthorised and unlawful websites in India – Blocking Rules, 2009, and nodal agencies empowered to issue blocking**
- **Cybercrime Offences – Nature and Penalties under the Indian laws (Cognizable, non-cognizable, bailable, non-bailable and prescribed punishments)**
- **Compliance requirements: Internet Intermediaries and Legal Aspects (IT Rules, 201 and due diligence requirements on the part of Intermediaries)**
- **Ethical and Professional Responsibilities**
- **Case Study: Landmark Indian Cybercrime Cases (e.g., Cosmos Bank Heist, Aadhaar Data Leaks)**
- **Interactive Session: Guest lecture/Q&A and landmark cybercrime legal case review**
- **RBI, Cyber Security Framework is a comprehensive and mandatory requirement, will be helpful.**
- **Section 2 to 13 of IT Act 2000 will be useful.**
- **Singapore, Protection from Online Falsehoods and Manipulation Act (POFMA) is a good reference legislation on the topic. Otherwise in India we have Social Media Ethics Rules under IT Act, 2000. (These are limited and sketchy)**
- **For the understanding of digital evidence law, chandrabhan Sudam Sanap vs State of Maharashtra can be used for teaching.**

MODULE 6

Week 11: Emerging Technologies and Future Challenges

- **AI & machine learning applications in offensive and defensive cyber operations**
- **Laws and Institutions governing AI in India: Introduction to AI Advisory, 2022, Comparative analysis with EU AI Act, Institutions (Ministry of Electronics and Information Technology, Govt. of India, NITI Aayog, MIB, Ministry of Defence)**
- **Blockchain, cryptocurrency forensics, and smart contract vulnerabilities**
- **Future challenges: Cloud evolution, zero trust architectures, and quantum computing threats**
- **Exercise: Group work on futuristic threat scenarios and policy implications**

Week 12: Capstone Simulation and course Integration

- **Comprehensive simulation of a cyber attack from inception to legal resolution**
- **Role assignments for attackers (red teaming), responders, forensic investigators, and legal teams**
- **Collaborative creation of an investigation report, chain-of-custody documentation, and legal brief**
- **Wrap-up: Debrief, program review, and discussion of further resources/next steps**

ACADEMIC ADVISORS/EXPERTS

- Dr. G.K. Goswami (IPS), Founding Director, UPSIFS, Lucknow
- Sh. Ravi Sharma, Chairman, IIIT UNA, IIT Nagpur and TEMA, India
- Prof. G.S. Bajpai, Hon'ble Vice-chancellor, NLU, Delhi
- Dr. A P Singh, VC, RMLNLU, Lucknow
- Prof. Preeti Saxena, VC, HPNLU, Shimla
- Prof Arun Mohan Sherry, Director, IIIT, Lucknow
- Prof. VK Ahuja, Director, Indian Law Institute, New Delhi
- Sh. Pawan Sharma, Founder and CEO, Braviti Digital Inc, USA
- Sh. Upendra Giri, Founder, North India Chapter, PMI, USA.
- Dr. Ranjeet Singh, CEO, SIFS, India
- Prof. Arvind Kumar Tiwari, Dean, School of Law, Rights and Constitutional Governance, TISS, Mumbai
- Dr. Kishan S Kardam, Former Senior Joint Controller of Patents and Designs and Former Head, Patent Office, New Delhi
- Adv. Anuj Agrawal, Chairman, Centre for Research on Cyber Crime and Cyber Law, N. Delhi
- Prof. Arunabha Mukhopadhyay, Information Technology and Systems, IIM Lucknow
- Prof. Mohd A. Arafa, Professor, Cornell Law School, USA
- Dr. A. Nagarathna, NLSIU, Bangalore
- Sh. Triveni Singh, Retd IPS, Cyber Expert
- Sh. Atul Kumar, Director, DSCI, New Delhi
- Advocate Prashant Mali, Cyber Expert, Bombay High Court
- Dr. Rakshit Tandon, Cyber Security Expert, India
- Shri Rohit Negi, Senior Vice President, C3i Hub, IIT Kanpur
- Sh. Samir Kumar Datt, CEO, Foundation Futuristic Technologies Pvt. Ltd. New Delhi
- Sh. Arvind Tripathy, Blockchain Expert & General Secretary, Youth for Nation
- Dr. Anil Sain, LC-1, Delhi University, New Delhi
- Dr. Shekhar Shukla, Assistant Professor, IIM Indore
- Sh. Atul Yadav, Additional SP, Cyber Crime, UPSIFS, Lucknow
- Sh. Balaji Venkateshwar, Cyber Defense Researcher, New Delhi
- Sh. Milind Raj, Drone Man of India
- Sh. Harold D'Costa, President, Cyber Security Corporation, Pune
- Dr. Bhavna Sharma, Practicing Advocate, Highcourt of Delhi

Note: Renowned international cyber experts, central government security agency officials, and officers from UP ATS and STF will also deliver lectures as a part of the program.

PROGRAM ORGANIZATION

- **Program Coordinator:** Dr. Manish Kumar Rai
  Mobile No. 7003241229
- **Program Co-Coordinator:** Mr. Kartikeya Srivastava
  Mobile No. 8765558348
- **E-mail Id :** trainings@upsifs.ac.in

SCAN

TO REGISTER

For more details visit our website

www.upsifs.ac.in