द्वारा फैक्स/ई–मेल

पुलिस प्रशिक्षण निदेशालय, उत्तर प्रदेश

पुलिस मुख्यालय(सिग्नेचर बिल्डिगं), प्रथम/द्वितीय तल, (टावर–1), शहीद पथ, गोमतीनगर विस्तार, लखनऊ 226002

पत्र संख्या प्रनि–प–30(4) 2026/2383 दिनांक अगस्त 11 ,2026

सेवा में,

1. पुलिस महानिदेशक
   सीबीसीआईडी/अभिसूचना/ फायर सर्विस, अभियोजन /भर्ती एवं प्रोन्नति बोर्ड/विशेष अनुसंधान दल / मानवाधिकार आयोग/पीएसी/ रेलवे/ ईओडब्लू/सतर्कता अधिष्ठान/रूल्स एण्ड मैनुअल/यूपी 112/साइबर क्राइम उ0प्र0 ।
2. अपर पुलिस महानिदेशक,
   अभिसूचना/अपराध/महिला एवं बाल सुरक्षा /सुरक्षा/यातायात एवं सडक सुरक्षा/एसटीएफ /तकनीकी सेवायें/लाजिस्टिक्स /एटीएस/यूपी एसएसएफ/विशेष जॉच लखनऊ।
3. अपर पुलिस महानिदेशक, समस्त जोन, उ0प्र0।
4. संस्था प्रमुख, समस्त पुलिस प्रशिक्षण संस्थान उ0प्र0 ।
5. पुलिस आयुक्त, लखनऊ / गौतमबुद्धनगर/वाराणसी /कानपुर /गाजियाबाद/आगरा/प्रयागराज।
6. पुलिस महानिरीक्षक, ए0एन0टी0एफ0/ए0सी0ओ0 लखनऊ ।
7. अपर पुलिस अधीक्षक, सोशल मीडिया, मुख्यालय पुलिस महानिदेशक, उ0प्र0 लखनऊ ।

महोदय,

कृपया Campus Director LNJN NICFS,NFSU,Delhi Campus के पत्र संख्याः19/10/2026-NICFS (NFSU_DC)p दिनांक 20.07.2026, पत्र संख्याः19/11/2026-NICFS(NFSU_DC) दिनांक 20.07.2026 एवं पत्र संख्याः19/08/2026-NICFS(NFSU_DC) (छायाप्रति संलग्न) का अवलोकन करने का कष्ट करें, जिसके द्वारा NFSU,Delhi Campus में निम्नलिखित तिथियों में आयोजित होने वाले विभिन्न कोर्स हेतु पत्र में अंकित लेवल (उपनिरीक्षक से अपर पुलिस अधीक्षक) के अनुसार उपयुक्त अधिकारियों के नामांकन उपलब्ध कराये जाने अपेक्षा की गई हैं ।

1- 05 Days "Special Course on Digital Forensics & Cyber Security" (Level 06-08)हेतुः–

क0सं0	कोर्स का नाम	बैच नं	कोर्स की अवधि	पदस्तर/लेवल	आयोन स्थल
1	**"Digital Forensics & Cyber Security "**	1st	05-10-2026 to 09-10-2026	उपनिरीक्षक से निरीक्षक **(Level 06- 8).**	LNJN NICFS, NFSU,Delhi Campus
		2nd	16-11-2026 to 20-11-2026		
		3rd	28-12-2026 to 01-01-2027		
		4th	01-02-2027 to 05-02-2027		
		5th	01-03-2027 to 05-03-2027		
		6th	28-03-2027 to 02-04-2027		

2- 05 Days "Special Course on Cyber Security and Cyber Crime" (Level 09-11) हेतुः–

क0सं0	कोर्स का नाम	बैच नं	कोर्स की अवधि	पदस्तर/लेवल	आयोन स्थल
2	**"Cyber Security and Cyber Crime"**	1st	12-10-2026 to 16-10-2026	पुलिस उपाधीक्षक से अपर पुलिस अधीक्षक **(Level 09-11).**	LNJN NICFS, NFSU,Delhi Campus
		2nd	30-11-2026 to 04-12-2026		
		3rd	04-01-2027 to 08-01-2027		
		4th	15-02-2027 to 19-02-2027		
		5th	26-04-2027 to 30-04-2027		

3- **03 Days "Special Course on Crypto Currency Investigations" (Level 06-08)**

क्र0सं0	कोर्स का नाम	बैच नं	कोर्स की अवधि	पदस्तर / लेवल	आयोन स्थल
3	**"Special Course on Crypto Currency Investigations"**	1st	09-09-2026 to 10-09-2026	उपनिरीक्षक से निरीक्षक **(Level 06- 8).**	LNJN NICFS, NFSU,Delhi Campus
		2nd	21-10-2026 to 23-10-2026		
		3rd	25-11-2026 to 27-11-2027		
		4th	27-01-2027 to 29-01-2027		
		5th	24-03-2027 to 26-03-2027		
		6th	19-04-2027 to 21-04-2027		

निदेशानुसार अनुरोध है कि उपरोक्त कोर्स में प्रतिभाग किये जाने हेतु प्रत्येक जोन / कमिश्नरेट / इकाई / प्रशिक्षण संस्थानों से प्रत्येक कोर्स मे अंकित अंकित लेवल के अनुसार उपनिरीक्षक से अपर पुलिस अधीक्षक स्तर के नामांकन निर्धारित प्रारूप में यथाशीघ्र इस निदेशालय को उपलब्ध कराने का कष्ट करें।

संलग्न–यथोपरि।

प्रारूप

क्र0सं0	कोर्स का नाम	कोर्स की अवधि	नाम एवं पदनाम	नियुक्त स्थान / दिनांक	मोबाईल नं0	ई–मेल आईडी	प्रभारी अधिकारी का सीयूजी नं0 /ईमेल आईडी	विगत 06 माह मे किये गये कोर्स का विवरण

(देव रंजन वर्मा)
पुलिस उपमहानिरीक्षक, प्रशिक्षण
उ0प्र0 लखनऊ।
11.9.26

प्रतिलिपिः– पुलिस महानिरीक्षक / पुलिस महानिदेशक के जीएसओ, मुख्यालय पुलिस महानिदेशक, उ0प्र0 लखनऊ को सादर सूचनार्थ ।

Cc "Dr. Minakshi Sinha"<minakshi.sinha_dc@nfsu.ac.in>

Dear Sir/Madam,

The National Forensic Sciences University, Delhi Campus (LNJN NICFS, NFSU - Delhi Campus), under the scheme of Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs is organizing the following courses for Law Enforcement Agencies:

- **05 Days Special Course on Digital Forensics & Cyber Security (Level 06-08).**
- **05 Days Special Course on Cyber Security and Cyber Crime (Level 06-08).**
- **03 Days Special Course on Crypto Currency Investigations (Level 06-08).**

The courses will be conducted in Offline/Physical Mode at NFSU Delhi Campus. The nominations may kindly be sent as per the information contained in the nomination letter at the earliest possible.

The calling of nominations letter is attached herewith for your reference.

विस महानिदेशक प्रशिक्षण
उ०प्र० लखनऊ।

साभार | **Best Regards,**

राजन कुमार | Rajan Kumar
प्रभारी प्रशिक्षण **| In-charge Training**
राष्ट्रीय न्यायालयिक विज्ञान विश्वविद्यालय, दिल्ली परिसर**| National Forensic Sciences University, Delhi Campus**
(भारत सरकार द्वारा घोषित राष्ट्रीय महत्व का संस्थान) गृह मंत्रालय, भारत सरकार
(An Institution of National Importance) Ministry of Home Affairs, Govt. of India
Contact No.: +91-9812411994

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

National Forensic Sciences University
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)

3 Attachment(s)

I4C MHA- Spl Course on Digit... 2.9 MB

I4C MHA- Spl Course on Crypt... 2.5 MB

I4C MHA - Cyber Security Cyb...

Calling of Nominations -Special Courses on Digital Forensics, Cyber Security & Crypto Currency Investigations

DG Training < dgtraining@ c.in >

Training Delhi Campus < training_dc@nfsu.ac.in >

Wed, 22 Jul 2026 4:16:04 PM +0530

To "dgtraining"<dgtraining@nic.in>,"dgtraining"<dgtraining@up.nic.in>,"dgp" <dgp@appolice.gov.in>,"igptrainingap" <igptrainingap@gmail.com>,"appoliceacademy2023" <appoliceacademy2023@gmail.com>,"ig-trg"<ig-trg@jhpolice.gov.in>,"DGP Maharashtra"<dgpms.mumbai@mahapolice.gov.in>,"adg.trg.office" <adg.trg.office@mahapolice.gov.in>,"A. A. Patvardhan" <trg.directorate@mahapolice.gov.in>,"ig.training" <ig.training@mahapolice.gov.in>,"Assam DGP" <dgp@assampolice.gov.in>,"digp-adm"<digp-adm@assampolice.gov.in>,"aigp-trg"<aigp-trg@assampolice.gov.in>,"dgp"<dgp@tripurapolice.nic.in>,"digp-hqtpa" <digp-hqtpa@tripura.gov.in>,"cp"<cp@kolkatapolice.gov.in>,"jtcp-training"<jtcp-training@kolkatapolice.gov.in>,"police"<police@ksp.gov.in>,"dgptraining" <dgptraining@ksp.gov.in>,"igptrg"<igptrg@ksp.gov.in>,"dgp-chattisgarh"<dgp-chattisgarh@yahoo.co.in>,"adgptrg18" <adgptrg18@gmail.com>,"aigtrainingphq007" <aigtrainingphq007@gmail.com>,"hpa.director" <hpa.director@hry.nic.in>,"trgpolice"<trgpolice@hry.nic.in>,"igp-apt-hp"<igp-apt-hp@nic.in>,"adgptrg.pol"<adgptrg.pol@kerala.gov.in>,"Shailesh Singh" <adg_trg@mppolice.gov.in>,"Arunachal Pradesh Police" <arpolice@rediffmail.com>,"principal-pts"<principal-pts@goapolice.gov.in>,"compr-trg"<compr-trg@gujarat.gov.in>,"Clay Khongsai" <ckhongsaiips@gmail.com>,"trgphq"<trgphq@gmail.com>,"igptrg-meg"<igptrg-meg@gov.in>,"trg.mlp-meg"<trg.mlp-meg@gov.in>,"DIG Training" <digtraining.mizoram@gmail.com>,"dir.bpspa" <dir.bpspa@nic.in>,"crl.ppa.phlr.police" <crl.ppa.phlr.police@punjab.gov.in>,"adgptrgraj" <adgptrgraj@gmail.com>,"aphq.skmpol"<aphq.skmpol@nic.in>,"adgptraining" <adgptraining@sikkimpolice.nic.in>,"dysppts.and"<dysppts.and@nic.in>,"dgp-police-ua"<dgp-police-ua@nic.in>,"police.chd" <police.chd@nic.in>,"hareshwar.swami"<hareshwar.swami@gov.in>,"splcp-trg-dl"<splcp-trg-dl@nic.in>,"sppts.pon"<sppts.pon@nic.in>,"ccr.pon" <ccr.pon@nic.in>,"gso1trgdgar"<gso1trgdgar@gmail.com>,"trgdte" <trgdte@bsf.nic.in>,"DIG(Trg), CBI Academy"<digtrg@cbi.gov.in>,"IG TRG" <igtrg@cisf.gov.in>,"adgtrg"<adgtrg@crpf.gov.in>,"rkverma" <rkverma@dcpw.gov.in>,"IG(Trg) Dte.Gen. ITBP"<igtrgdte@itbp.gov.in>,"NCRB" <ncrbtrg@gmail.com>,"director"<director@ncrb.gov.in>,"dig trgopsndrf" <dig.trgops.ndrf@gov.in>,"dir academy-ndrf"<dir.academy-ndrf@gov.in>,"nepa-meg"<nepa-meg@nic.in>,"digtrg"<digtrg@nsg.gov.in>,"ig.trgssb" <ig.trgssb@ssb.gov.in>,"Rajesh Kumar"<trgspm.35@gov.in>,"training.nia" <training.nia@gov.in>,"dgp"<dgp@jhpolice.gov.in>,"dgpjharkhand" <dgpjharkhand@gmail.com>,"IG Training" <igtraining.bih@gmail.com>,"naptrainingcentre@gmail.com" <naptrainingcentre@gmail.com>,"adgp.trg.police" <adgp.trg.police@punjab.gov.in>,"Training Branch, West Bengal Police Directorate"<trgbranchwbp@gmail.com>,"Training Section TS" <igptraining2017@gmail.com>

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

राष्ट्रीय न्यायालयिक विज्ञान विश्वविद्यालय
(राष्ट्रीय महत्त्व का संस्थान, गृह मंत्रालय, भारत सरकार)
National Forensic Sciences University
(An Institution of National Importance, Ministry of Home Affairs, Government of India)

NFSU
विद्यया अमृतं अश्नुते

Most Immediate

No. 19/10/2026-NICFS(NFSU_DC)p

Dated 20 July, 2026

01 Director, All CPOs
02 DGP/IGP, All States/UTs
03 Commissioner of Police, Delhi/Kolkata/Mumbai/Chennai

Sub: Nominations for 05 Days "Special Course on **Digital Forensics & Cyber Security"** for LEAs Officers (Level 06 to 08) **- reg.**

Sir/Madam,

The National Forensic Sciences University, Delhi Campus (LNJN National Institute of Criminology & Forensic Science) is conducting the above mentioned Course for LEAs Officers (Level 06 to 08) under the scheme of Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs (MHA), New Delhi.

2. NFSU Delhi Campus will be organizing these courses in **Offline/Physical Mode** at its NFSU Delhi Campus. NFSU Delhi Campus invites nominations of minimum **four (04)** Officers. The NFSU Delhi Campus proposes to organize **06** such batches as per the following schedule:

S. No.	Batch No.	Duration (05 Days)
1	1st	05-09 October, 2026
2	2nd	16-20 November, 2026
3	3rd	28 December-01 January, 2027
4	4th	01-05 February, 2027
5	5th	01-05 March, 2027
6	6th	29 March-02 April, 2027

The Nominations may be sent together for **all the above batches or batch wise** prior to 02 weeks before the commencement of the batches. Nominated officers can be replaced by another in the same category by the department.

Contd/-...

एनएफएसयू मुख्यालय / NFSU Headquarter
सेक्टर-09, गांधीनगर, गुजरात–382007/ Sector-09 Gandhinagar,
फोन / Ph.: 079-23977102/103
फैक्स / Fax : 079-23247465
ईमेल / Email : exe_registrar@nfsu.ac.in
वेबसाइट / Website : https://www.nfsu.ac.in

दिल्ली परिसर / Delhi Campus
एलएनजेएन एनआईसीएफएस, एनएफएसयू / LNJN NICFS NFSU
सेक्टर-03, आउटर रिंग रोड, राहिणी, दिल्ली-110085 /
Sector-03, Outer Ring Road, Rohini, Delhi-110085
फोन / Ph.: 011-27521433, 27514161, 27525084
फैक्स / Fax : 011-27510586 | ईमेल / Email : admin_dc@nfsu.ac.in
वेबसाइट / Website : https://www.nfsu.ac.in

03 The details of the nominated officer may please be intimated as per the following Proforma:

Batch No. & Duration	Name and Designation	Mobile No	Email-id

04 Officers will be accommodated in NICFS NFSU, Delhi Campus. The 06 days accommodation for officers coming from outside Delhi will be arranged by NFSU Delhi. **No Course Fee will be charged for these Courses (including boarding/lodging)**.

05 The University welcomes the reply by E-mail ID: **training_dc@nfsu.ac.in** in its endeavor to be an eco-friendly organization.

Prof. (Dr) Purvi Pokhariyal
Campus Director
LNJN NICFS, NFSU, Delhi Campus

Copy to: Col. Tarun Uppal, Director (14C), Indian Cyber Crime Coordination Centre, CIS Division, 5th floor, NDCC-II, Jai Singh Road, New Delhi(though mail)

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

NFSU

Special Course on Digital Forensic and Cyber Security for Law Enforcement Agencies

(Level 06-08)

NFSU

National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Special Course on Digital Forensic and Cyber Security for Law Enforcement Agencies (Level 06-08)

ABOUT THE COURSE

The rapid growth of digital technology has significantly transformed the nature of crime and criminal investigation. Computers, mobile phones, internet-based platforms, digital payment systems, cloud services, CCTV systems, IoT devices, drones, cryptocurrency platforms, and AI-enabled tools are now increasingly being used either as instruments of crime or as sources of crucial evidence. As a result, digital evidence has become an important component in the investigation of cybercrime as well as technology-assisted conventional crimes.

Law Enforcement Officers, particularly Investigating Officers, are often the first responders in cases involving digital evidence. Their actions at the initial stage of investigation play a vital role in ensuring that electronic evidence is properly identified, collected, preserved, documented, and forwarded for forensic examination. Any improper handling, alteration, delay, or lack of documentation may affect the integrity, authenticity, and admissibility of digital evidence during investigation and trial.

In view of these challenges, this **Special Course on Digital Forensic and Cyber Security for Law Enforcement Agencies** has been designed to provide practical and investigation-oriented training to officers dealing with cybercrime and digital evidence. The course focuses on field-level procedures such as digital evidence identification, first response, seizure, preservation, hashing, chain of custody, documentation, forensic examination, and admissibility of electronic evidence.

The programme also provides exposure to important areas such as computer frauds, banking and digital payment frauds, CDR/IPDR and subscriber information, mobile device evidence, CCTV and digital image authentication, IoT forensics, cloud and email evidence, cryptocurrency fraud investigation, drone forensics, deepfake and AI-enabled cybercrime, and the legal framework relating to digital evidence under the new criminal laws. These topics are aligned with the revised course schedule prepared for Law Enforcement Agencies.

The course aims to strengthen the practical capacity of Investigating Officers to handle digital evidence in a forensically sound and legally acceptable manner. It will also help participants coordinate effectively with forensic laboratories, banks, service providers, cyber cells, and specialised agencies during the investigation of cybercrime and technology-assisted offences.

COURSE OBJECTIVES

The course objective to equip Law Enforcement Officerswith specialized knowledge and skills relevant to the intersection of criminal justice and digital forensics. Participants will:

- Understand the role of Investigating Officers in cybercrime and digital forensic investigation.
- Learn the principles of digital evidence identification, collection, preservation, seizure, hashing, documentation, and chain of custody.
- Gain practical exposure to mobile forensics, CCTV and image forensics, IoT forensics, cloud and email forensics, drone forensics, and cryptocurrency-related evidence.
- Understand the investigation approach for banking frauds, digital payment frauds, computer frauds, AI-enabled cybercrime, deepfakes, and online financial crimes.
- Develop familiarity with CDR, IPDR, subscriber information, service provider coordination, and digital evidence requisition procedures.
- Learn the legal requirements for admissibility of digital evidence, SOP compliance, and presentation of forensic findings during investigation and trial.

TRAINING CURRICULUM

The **Special Course on Digital Forensic and Cyber Security for Law Enforcement Agencies** is designed to equip Law Enforcement Officers, particularly Investigating Officers, with practical knowledge and skills required for handling cybercrime cases and digital evidence in a forensically sound manner.

The programme focuses on the complete digital evidence lifecycle, including identification, collection, preservation, seizure, hashing, documentation, chain of custody, forensic examination, and admissibility of digital evidence during investigation and trial. The course also provides exposure to important areas such as computer frauds, digital payment frauds, mobile forensics, CCTV and image evidence, IoT devices, cloud and email evidence, cryptocurrency fraud, drone forensics, deepfake investigation, and the legal framework under new criminal laws.

The following critical topics will be covered during the programme:

1. Digital Evidence Identification, Collection and Preservation:

- Understand the nature and importance of digital evidence in cybercrime and technology-assisted criminal cases.
- Learn how to identify, collect, preserve, and document electronic devices and digital evidence at the initial stage of investigation.
- Understand the role of the first responder in preventing alteration, deletion, or contamination of digital evidence.

2. First Response and Documentation of Digital Evidence:

- Learn the correct procedure for seizure, packing, sealing, labelling, and forwarding of digital evidence.
- Understand the importance of seizure memo, hash value, chain of custody, forwarding letter, and other documentation.
- Appreciate how proper documentation strengthens the admissibility and reliability of digital evidence.

3. Computer Frauds: Issues and Challenges:

- Understand common types of computer-related frauds and their modus operandi.
- Learn how digital footprints are generated through computers, networks, applications, and online platforms.
- Discuss practical challenges faced during investigation of computer fraud cases.

4. Banking and Digital Payment Frauds:

- Understand common online financial frauds such as UPI fraud, wallet fraud, banking fraud, phishing, fake customer care fraud, and QR code fraud.
- Learn how to trace transaction details, beneficiary accounts, wallet details, IP logs, mobile numbers, and device information.
- Understand the importance of timely action for freezing transactions and preserving financial evidence.

5. CDR, IPDR and Subscriber Information:

- Develop basic understanding of CDR, IPDR, subscriber details, CAF, tower location, and internet usage records.
- Learn how telecom records assist in establishing communication links, location patterns, internet activity, and suspect association.
- Understand the precautions and limitations while interpreting telecom-related data.

6. Mobile Device Evidence and Forensic Analysis:

- Understand the importance of mobile phones as a major source of digital evidence.
- Identify evidence such as call logs, chats, images, videos, documents, application data, location data, and cloud-linked information.
- Learn precautions during seizure and witness demonstration of mobile device acquisition and basic analysis

7. CCTV Footage Examination and Digital Image Authentication:

- Understand the forensic value of CCTV footage, DVR/NVR systems, IP cameras, and digital images.
- Learn correct procedures for collection, export, preservation, and documentation of CCTV footage.
- Understand basic concepts of image authentication, metadata examination, and tampering indicators.

8. IoT Forensics and Smart Device Evidence

- Understand the relevance of IoT and smart devices in modern investigations.
- Identify evidence from routers, IP cameras, smart watches, GPS devices, vehicle trackers, smart TVs, and home automation devices.
- Learn precautions for preserving IoT devices, logs, network details, and cloud-linked information.

9. Cloud Evidence and Email Forensics:

- Understand the role of cloud services, email accounts, online storage, and platform-based evidence in investigation.
- Learn the relevance of login history, IP logs, user activity, metadata, email headers, attachments, and phishing indicators.
- Understand preservation requests, legal requisitions, and coordination with service providers.

10. Cryptocurrency Fraud Investigation:

- Understand basic concepts of cryptocurrency, wallets, exchanges, blockchain transactions, and digital assets.
- Learn how wallet addresses, transaction trails, exchange records, KYC details, IP logs, and bank account links assist investigation.
- Understand the importance of timely preservation requests to cryptocurrency exchanges and related platforms.

11. Drone Forensics:

- Understand the relevance of drones in investigation, surveillance, unauthorised photography, smuggling, and security-related incidents.
- Identify evidence from drones, controllers, memory cards, mobile applications, flight logs, GPS records, images, and videos.
- Witness demonstration of drone forensic examination and evidence handling.

12. Deepfake and AI-Enabled Cybercrime Forensics:

- Understand emerging threats such as deepfakes, synthetic media, voice cloning, AI-generated content, and digital impersonation.
- Learn how such content may be used in fraud, blackmail, misinformation, impersonation, and social engineering.
- Understand the importance of preserving original files, metadata, platform links, source URLs, and associated devices.

13. Admissibility of digital evidence and Legal challenges in cybercrime investigation:

- Gain practical guidance on how to prepare digital evidence for legal presentation, ensuring it meets the standards required for admissibility in court.
- Learn the essential steps to verify the authenticity and integrity of digital evidence, from its collection to its presentation in legal proceedings, ensuring it is accepted by judges and juries.
- Learn the Standard Operating Procedures (SOPs) for handling, processing, and presenting digital evidence to boost the credibility and success of digital crime prosecutions.
- Legal challenges like jurisdiction issues and admissibility of digital evidence in cybercrime investigation.

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

24 JUL 2026 R. No. 6238
Date: 24/07/26

राष्ट्रीय न्यायालयिक विज्ञान विश्वविद्यालय
(राष्ट्रीय महत्त्व का संस्थान, गृह मंत्रालय, भारत सरकार)
National Forensic Sciences University
(An Institution of National Importance, Ministry of Home Affairs, Government of India)

NFSU
विद्यया अमृतं अश्नुते

Most Immediate

No. 19/11/2026-NICFS(NFSU_DC)

Dated 20 July, 2026

01 Registrar General, All High Courts
02 Director, All CPOs
03 DGP/IGP, All States/UTs
04 Commissioner of Police, Delhi/Kolkata/Mumbai/Chennai
05 Director General/Director of Public Prosecutions, All States/UTs
06 Director, CFSLs/FSLs, All States/UTs

Sub: Nominations for 05 Days "Special Course on **Cyber Security & Cyber Crime**" for Judicial Officers, Prosecution Officials, Dy. SP/ACP/AC and above & Forensics Scientists/SSO from CFSLs/FSLs (Level 09 to 11) **- reg.**

Sir/Madam,

पुलिस महानिदेशक प्रशिक्षण
उ०प्र० लखनऊ।
24/07/26

The National Forensic Sciences University, Delhi Campus (LNJN National Institute of Criminology & Forensic Science) is conducting the above mentioned Course for Judicial Officers, Prosecution Officials, Dy. SP/ACP/AC and above & Forensics Scientists/SSO from CFSLs/FSLs (Level 09 to 11) under the scheme of Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs (MHA), New Delhi.

2. NFSU Delhi Campus will be organizing these courses in **Offline/Physical Mode** at its NFSU Delhi Campus. NFSU Delhi Campus invites nominations of minimum **four (04)** Officers. The NFSU Delhi Campus proposes to organize **05** such batches as per the following schedule:

S. No.	Batch No.	Duration (05 Days)
1	1st	12-16 October, 2026
2	2nd	30 November-04 December, 2026
3	3rd	04-08 January, 2027
4	4th	15-19 February, 2027
5	5th	26-30 April, 2027

Contd/-...

एनएफएसयू मुख्यालय / NFSU Headquarter
सेक्टर-09, गांधीनगर, गुजरात–382007/ Sector-09 Gandhinagar,
फोन / Ph.: 079-23977102/103
फैक्स / Fax : 079-23247465
ईमेल / Email : exe_registrar@nfsu.ac.in
वेबसाइट / Website : https://www.nfsu.ac.in

दिल्ली परिसर / Delhi Campus
एलएनजेएन एनआईसीएफएस, एनएफएसयू / LNJN NICFS NFSU
सेक्टर-03, आउटर रिंग रोड, राहिणी, दिल्ली-110085 /
Sector-03, Outer Ring Road, Rohini, Delhi-110085
फोन / Ph.: 011-27521433, 27514161, 27525084
फैक्स / Fax : 011-27510586 | ईमेल / Email : admin_dc@nfsu.ac.ir
वेबसाइट / Website : https://www.nfsu.ac.in

The Nominations may be sent together for **all the above batches or batch wise** prior to 02 weeks before the commencement of the batches. Nominated officers can be replaced by another in the same category by the department.

03 The details of the nominated officer may please be intimated as per the following Proforma:

Batch No. & Duration	Name and Designation	Mobile No	Email-id

04 Officers will be accommodated in NICFS NFSU, Delhi Campus. The 06 days accommodation for officers coming from outside Delhi will be arranged by NFSU Delhi. **No Course Fee will be charged for these Courses (including boarding/lodging)**.

05 The University welcomes the reply by E-mail ID: **training_dc@nfsu.ac.in** in its endeavor to be an eco-friendly organization.

Prof. (Dr) Purvi Pokhariyal
Campus Director
LNJN NICFS, NFSU, Delhi Campus

Copy to: Col. Tarun Uppal, Director (14C), Indian Cyber Crime Coordination Centre, CIS Division, 5th floor, NDCC-II, Jai Singh Road, New Delhi(though mail)

ABOUT THE COURSE

In today's increasingly digital world, the rise of cybercrimes and the growing reliance on technology have made cybersecurity a critical concern for law enforcement agencies, the judiciary, and national security. Cybercrimes, ranging from data breaches and financial fraud to more serious offenses such as cyber terrorism and hacking, pose significant challenges to legal systems and law enforcement agencies. In this context, it is essential for senior officials in the police, judiciary, defence, and forensic sectors to be equipped with the knowledge, skills, and tools to address these emerging threats effectively.

The Special Course on Cybersecurity and Cyber Crime Investigation has been specifically designed for senior officials, including Additional Director Generals (ADG), Magistrates, Superintendents of Police (SP), Assistant Commissioners of Police (ACP), Defence Officers, and senior officials from Central Forensic Science Laboratories (CFSLs) and Forensic Science Laboratories (FSLs). The course aims to provide these senior officers with an advanced understanding of the evolving cyber threat landscape, cutting-edge investigative techniques, and the legal frameworks that govern cybersecurity and cybercrimes.

This intensive training program will help judicial officers and law enforcement personnel sharpen their expertise in cybercrime investigation, digital forensics, and cybersecurity, enabling them to lead investigations, manage high-stakes cybercrime cases, and formulate effective policies. With a focus on practical

applications, legal knowledge, and strategic leadership, this course empowers participants to tackle cybercrimes with confidence and proficiency, while ensuring justice and protecting critical infrastructure.

This course is a unique opportunity for senior officials to gain specialized knowledge and expertise in one of the most critical fields of modern law enforcement and judicial practice. It ensures that participants can lead cybercrime investigations, address challenges in handling digital evidence, and contribute effectively to the development of cybersecurity policies. As cybercrimes continue to evolve, the ability of these leaders to understand the technical, legal, and strategic aspects of cybersecurity and cybercrime investigation is paramount to safeguarding the public, national security, and critical infrastructure.

COURSE OBJECTIVES

The course objective to equip senior officers with specialized knowledge and skills relevant to the Cyber Security and Cyber Crime Investigation. Participants will:

- Enhance Knowledge of Cybersecurity Threats: Equip senior officers with a comprehensive understanding of emerging cyber threats, including ransomware, phishing, and cyber terrorism.
- Strengthen Cybercrime Investigation Skills: Provide practical training in digital forensics, including evidence collection, data recovery, and analysis to support cybercrime investigations.
- Improve Legal Understanding: Familiarize judicial officers and law enforcement leaders with cybercrime laws, data protection regulations, and the legal processes surrounding digital evidence in court.
- Develop Incident Management Expertise: Train participants to design and lead incident response strategies for addressing major cyberattacks and cybersecurity breaches.
- Facilitate Inter-agency Coordination: Promote effective collaboration between law enforcement, defense agencies, judicial bodies, and international organizations in the fight against cybercrime.
- Enhance Leadership in Cybercrime Cases: Equip senior officials with leadership skills to manage and oversee high-profile cybercrime investigations and cybersecurity initiatives at the regional and national levels.
- Build Capacity for Handling Cybercrime Trials: Enable judicial officers to effectively manage cybercrime trials,

ensuring the legal integrity of digital evidence and proper legal procedures.

TRAINING CURRICULUM

This specialized training program is designed to provide senior law enforcement, defense officers, forensic experts, and judicial officers with the knowledge and skills required to lead and oversee cybersecurity efforts, investigate cybercrimes, and manage digital evidence. The course will provide a balanced combination of technical expertise, legal knowledge, and strategic leadership in cybersecurity and cybercrime investigations.

1. OVERVIEW OF CYBERSECURITY
    - Importance of cybersecurity in the modern digital landscape.
    - Types of cyber threats: malware, ransomware, phishing, data breaches, etc.
    - Understanding the relationship between cybersecurity and cybercrime.
    - Cybercrime Types: Financial Cybercrimes, Crimes Against Individuals, Cyber Terrorism, Cyber Espionage, Hacking and Malware
    - Understanding the evolving landscape of cybercrime
    - Identifying challenges in digital forensic investigations of computer frauds

2. Digital Deception: Deepfake and Deep Web
    - Introduction of Deepfake technology
    - Social, political, legal, and psychological implications of Deepfake
    - Deepfake creation technology and Deepfake detection
    - Understanding of Dark web and Deep web
    - Dark web and Deep web investigation

3. Forensic Discovery of Digital Evidence
    - Techniques and methodologies for forensic discovery
    - Gathering and analyzing digital evidence for legal presentation

4. Mobile Phone Technology and Forensics
    - Understanding mobile phone technology and its relevance in digital forensics

- Data extraction from smartphones, tablets, and other mobile devices and their analysis.
- Hands-on exercises and case studies in mobile phone forensics
- Tools for mobile forensics: Cellebrite, XRY, etc.

5. Collection and Preservation of Volatile and Non-Volatile Data
   - Best practices for collecting and preserving digital evidence
   - Legal considerations in data preservation
   - Practical exercises in data collection and preservation techniques
   - Computer-based Evidence: Hard drives, laptops, desktops, and servers
   - Techniques for ensuring data integrity during evidence collection.
   - Understanding forensic imaging and using write blockers for evidence preservation
   - EnCase and FTK for disk imaging and evidence collection
   - Techniques for ensuring data integrity during evidence collection.
   - Understanding forensic imaging and using write blockers for evidence preservation

6. Cloud Forenscis: Collecting Evidence from cloud
   - Overview of Cloud Computing
   - Key Challenges in collecting evidence from cloud environments: Jurisdiction, data residency, and multi-tenancy
   - Data Collection Techniques in Cloud Environments
   - Cloud Forensics Process and Emerging Trends in Cloud Forensics
   - Investigating data stored in the cloud and navigating legal challenges.

7. Online Abuse on Children: Measures, Prevention, and Control
   - Definition and scope of online abuse: Cyberbullying, online grooming, sexting, exploitation, and trafficking
   - Understanding the digital landscape and how children are targeted online

- Statistics and trends: Global and regional prevalence of online child abuse
- Impact of online abuse on children: Psychological, emotional, and social consequences
- Common platforms and technologies where children are exposed to online abuse (social media, gaming, chat rooms, etc.)
- Legal Framework and Protection Mechanisms
- Implementing measures for prevention and control

8. CCTV Analysis and Digital Image Forensics
    - Overview of CCTV systems: Types of cameras (analog vs. digital, IP cameras, PTZ cameras)
    - Key components of a CCTV system: Cameras, recording devices, storage systems, monitors
    - Role of CCTV in law enforcement and criminal investigations
    - Introduction to digital image forensics: Definition and significance
    - Digital evidence: Types of digital images, video files, and metadata
    - Tools for video analysis like Amped FIVE
    - Techniques for video enhancement: Noise reduction, sharpness, color correction
    - Techniques for identifying faces, license plates, and other key objects in video

9. Investigating Financial Cybercrime
    - Definition of financial cybercrime: Overview of key types (fraud, money laundering, identity theft, cyber theft)
    - Impact of financial cybercrime on businesses, individuals, and economies
    - The evolution of financial cybercrime in the digital age
    - Understanding criminal motivations: Financial gain, espionage, extortion
    - Types of financial fraud: Securities fraud, insurance fraud, loan fraud, Ponzi schemes, insider trading
    - Common techniques used in financial fraud: Document falsification, fraudulent transactions, forgery, misrepresentation
    - Indicators and red flags of financial fraud

- Implementing fraud prevention systems and controls (e.g., two-factor authentication, encryption)
- Techniques for tracking digital money trails.
- Anti-money laundering (AML) measures in cybercrime investigations

10. Legal Framework for Cybercrime
    - Information Technology Act, 2000 (IT Act) and its amendments.
    - Indian Penal Code (IPC) provisions relevant to cybercrime.
    - Data Protection Laws and Privacy issues in digital spaces.
    - Introduction of new criminal laws in digital era

11. Preparation, Admissibility of Digital Evidence, and Standard Operating Procedures (SOPs)
    - Guidance on preparing digital evidence for legal presentation
    - Ensuring the admissibility of digital evidence in court proceedings
    - Developing SOPs for handling digital evidence effectively

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

राष्ट्रीय न्यायालयिक विज्ञान विश्वविद्यालय
(राष्ट्रीय महत्त्व का संस्थान, गृह मंत्रालय, भारत सरकार)
National Forensic Sciences University
(An Institution of National Importance, Ministry of Home Affairs, Government of India)

NFSU
विद्यया अमृतं अश्नुते

Most Immediate

No. 19/08/2026-NICFS(NFSU_DC)

Dated 20 July, 2026

01 Director, All CPOs
02 DGP/IGP, All States/UTs
03 Commissioner of Police, Delhi/Kolkata/Mumbai/Chennai

Sub: Nominations for 03 Days "Special Course on **Crypto Currency Investigation"** for LEAs Officers (Level 06 to 08) **- reg.**

Sir/Madam,

The National Forensic Sciences University, Delhi Campus (LNJN National Institute of Criminology & Forensic Science), is conducting the above mentioned Course for Law Enforcement Officers (Level 06 to 08) under the scheme of Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs (MHA), New Delhi.

2. NFSU Delhi Campus will be organizing these courses in **Offline/Physical Mode** at its NFSU Delhi Campus. NFSU Delhi Campus invites nominations of minimum **four (04)** Officers. The NFSU Delhi Campus proposes to organize **06** such batches as per the following schedule:

S. No.	Batch No.	Duration (03 Days)
1	1st	09-10 September, 2026
2	2nd	21-23 October, 2026
3	3rd	25-27 November, 2026
4	4th	27-29 January, 2027
5	5th	24-26 March, 2027
6	6th	19-21 April, 2027

The Nominations may be sent together for **all the above batches or batch wise** prior to 02 weeks before the commencement of the batches. Nominated officers can be replaced by another in the same category by the department.

Contd/-...

एनएफएसयू मुख्यालय / NFSU Headquarter
सेक्टर-09, गांधीनगर, गुजरात–382007/ Sector-09 Gandhinagar,
फोन / Ph.: 079-23977102/103
फैक्स / Fax : 079-23247465
ईमेल / Email : exe_registrar@nfsu.ac.in
वेबसाइट / Website : https://www.nfsu.ac.in

दिल्ली परिसर / Delhi Campus
एलएनजेएन एनआईसीएफएस, एनएफएसयू / LNJN NICFS NFSU
सेक्टर-03, आउटर रिंग रोड, राहिणी, दिल्ली-110085 /
Sector-03, Outer Ring Road, Rohini, Delhi-110085
फोन / Ph.: 011-27521433, 27514161, 27525084
फैक्स / Fax : 011-27510586 | ईमेल / Email : admin_dc@nfsu.ac.in
वेबसाइट / Website : https://www.nfsu.ac.in

03 The details of the nominated officer may please be intimated as per the following Proforma:

Batch No. & Duration	Name and Designation	Mobile No	Email-id

04 Officers will be accommodated in NICFS NFSU, Delhi Campus. The 04 days accommodation for officers coming from outside Delhi will be arranged by NFSU Delhi. **No Course Fee will be charged for these Courses (including boarding/lodging)**.

05 The University welcomes the reply by E-mail ID: **training_dc@nfsu.ac.in** in its endeavor to be an eco-friendly organization.

Prof. (Dr) Purvi Pokhariyal
Campus Director
LNJN NICFS, NFSU, Delhi Campus

Copy to: Col. Tarun Uppal, Director (14C), Indian Cyber Crime Coordination Centre (I4C), CIS Division, 5th floor, NDCC-II, Jai Singh Road, New Delhi(though mail)

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

NFSU

Special Course on Crypto Currency Investigations for Law Enforcement Agencies

(Level 06-03)

NFSU

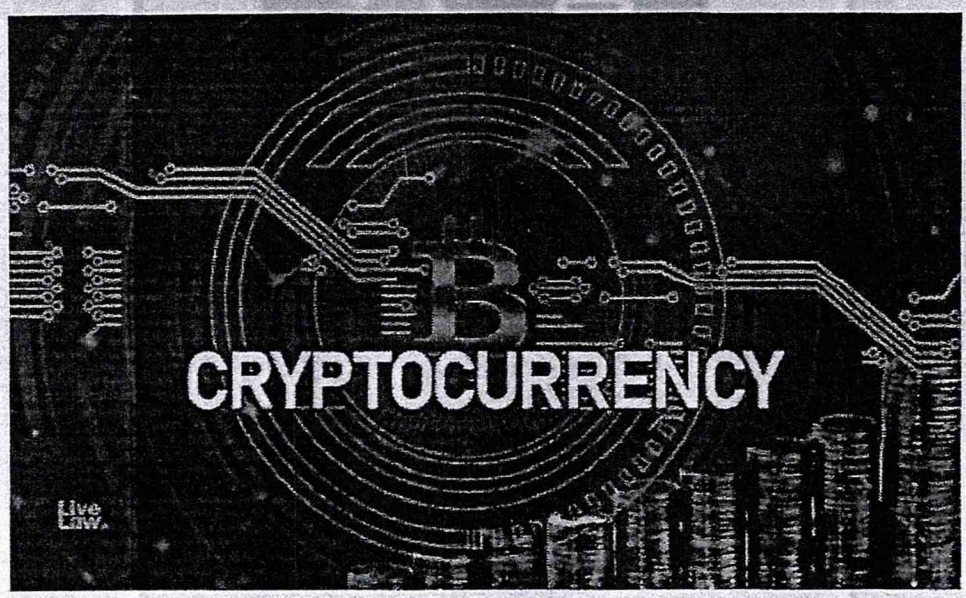
National Forensic Sciences University

Knowledge | Wisdom | Dedication

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Special Course on **Crypto Currency Investigations for Law Enforcement Agencies**

(Level 06-08)



ABOUT THE COURSE

This specialized course is designed to build the investigative and analytical capabilities of Law Enforcement and Judiciary officers in handling cryptocurrency-related crimes. It provides an in-depth understanding of blockchain fundamentals, crypto transactions, wallets, and exchanges, along with practical exposure to tracing illicit funds using blockchain explorers, forensic tools, and OSINT techniques. Participants will learn how to analyse transaction patterns, identify wallet owners, trace funds across multiple blockchains, and preserve digital evidence in compliance with legal standards under the IT Act, PMLA, UAPA, and FATF recommendations.

Through live demonstrations, case studies, and practical exercises, the course will familiarize participants with real-world crypto investigations involving ransomware, darknet markets, terror financing, and fraud schemes. It also addresses emerging threats such as DeFi-based laundering, NFT frauds, and metaverse crimes, highlighting the challenges of anonymity and decentralized systems. By the end of the program, participants will be equipped to investigate, interpret, and present blockchain evidence effectively, enhancing their capability to counter cryptocurrency-enabled crimes.

COURSE OBJECTIVES

The course objective is to equip Law Enforcement Officers, particularly Investigating Officers, with practical knowledge and skills required for handling cryptocurrency-related offences and blockchain-based digital evidence Participants will:

1. Understand the fundamentals of cryptocurrency, blockchain networks, wallets, exchanges, and crypto transactions.

2. Learn common types of cryptocurrency-enabled crimes such as investment fraud, ransomware, cyber extortion, darknet transactions, wallet fraud, and crypto-based laundering.

3. Develop practical understanding of wallet addresses, transaction IDs, blockchain explorers, transaction trails, and crypto evidence identification.

4. Gain exposure to OSINT techniques, blockchain analysis tools, and transaction tracking workflows used in cryptocurrency investigations.

5. Learn procedures for preservation, seizure, freezing, documentation, and forwarding of cryptocurrency-related digital evidence.

6. Understand the role of exchanges, banks, payment gateways, virtual digital asset service providers, and FIU-related mechanisms in crypto investigation.

7. Develop familiarity with legal and procedural aspects relating to search, seizure, freezing, KYC/AML compliance, admissibility of evidence, and preparation of investigation records.

8. Enhance investigation skills through case studies and demonstrations involving real-world cryptocurrency frauds and blockchain transaction analysis.

TRAINING CURRICULUM

1. Introduction to Cryptocurrency and Blockchain Technology

- Overview of decentralized and peer-to-peer finance
- Types of cryptocurrencies and their digital infrastructure
- Public, Private and Consortium Blockchains

2. Cryptocurrency-Enabled Crimes and Their Modus Operandi

- Fraud, darknet transactions, ransomware and cyber-extortion
- Use of privacy coins, mixers, tumblers and chain-hopping
- Role of decentralized exchanges (DEXs) in obfuscation

3. Wallet Tracing and Transaction Analysis

- Identification and classification of wallet addresses
- Transaction graph analysis and linking transaction flows
- Live demonstration using blockchain explorers and Case study-based wallet tracking exercises

4. Blockchain Forensics and Intelligence Platforms

- Open-source and professional blockchain forensics tools
- Entity clustering and wallet attribution techniques
- Demonstrations with real-world investigation workflows

5. Investigation of Darknet and Crypto market Activities

- Structure of Darknet markets and crypto-mediated commerce
- Cryptocurrency escrow and P2P trade practices
- OSINT & undercover access methods (awareness level)

6. Legal, Regulatory, and Procedural Aspects

- Indian legal framework: IT Act, PMLA, UAPA, BNS & related rules
- Exchange compliance, KYC/AML mandates & FATF travel rule
- Search, seizure, freezing, and documentation of digital evidence
- The existing legal position in India pertaining to crypto and the various aspects of development of Crypto law in India.

7. Evidence Collection, Preservation and Chain of Custody

- Forensically sound acquisition of blockchain-based evidence
- Preparation of investigation reports and forensic audit summaries
- Courtroom admissibility & testimony best practices

8. Future Challenges and Evolving Trends

- DeFi-based laundering pathways and smart contract crime
- NFT scams, rug-pulls, phishing pools and metaverse crime vectors and global developments