NALSAR
University of Law, Hyderabad
(Accredited with 'A++' grade by NAAC)

nalsar pro
e-nexus for Law
Directorate of Distance Education

THREE DAY ONLINE COURSE ON CYBER CRIMES INVESTIGATION AND DIGITAL FORENSICS USING OSINT TOOLS AND TECHNIQUES

About the Course

The amount of data being pushed to the Internet each minute is staggering. There are millions of hours of videos, billions of images, and zitabits of text that cannot be indexed by a mere search engine algorithm. The indexing of the data is distributed complexly across the Web technologies - on Surface web, Deep web and Dark web of the internet. Understanding, capturing and investigating these kinds of data sources needs special skills in cybernetics; this is what this certification does. This course enables the Law students and Legal professionals to undertand the art of Cyber Crime Investigation in conjunction of application of Cyber Laws in the domain of Digital Forensics.

The course starts with the process of collecting and analysing data from the confesticated Digital evidence and then quickly moves into investigating techniques to gain access to un-indexed data. It explains and practically demonstrates a broad array of Open-Source Intelligence (OSINT) tools, such as setting up an OSINT analysis platform, accessing data from surface web and deep web and exploring the world of dark web using encrypted web browsers on the internet.

This certification, being a foundational course in open-source intelligence (OSINT) tools and techniques, teaches participants how to find, collect, and analyse data from the Internet. Far from being a beginner class, this course teaches participants the OSINT framework to be successful in finding and using online information, reinforced with over 30 hands-on bootcamp exercises.

Course Objectives

- Usage of Social Media Intelligence paradigms on social media handles like Facebook. twitter, Instagram, LinkedIn etc for Cyber Crimes investigation
- Review, monitor and evaluate search engine information from Google, Bing, Yahoo, and others from dark web for Cyber Crimes investigation
- Monitoring information on Websites, Directories, search engines, meta search engines as well as review user activity on digital platforms for gathering information of the entities involved in the crime scenes.
- Access old cached data from internet by means of Website analysis and data collection
- Identify fake profiles, sock puppets, and fake emails, as well as mail addresses from social networks, or Google results.

- Search for photographs and videos on common social photo sharing sites such as Flickr, Google Photos, etc. , by image analysis tools
- Use Google Maps and other open satellite imagery sources to retrieve images of users' geographic location and establish connection between the suspects involved in a cyber-crime as per their Digital Foot prints for Cyber Crimes Investigation

Course Outcome

- Provide a comprehensive overview on the main work processes and general techniques that are necessary for the accomplishment of intelligence gathering on Cyber Crime scenarios from social media platforms and handles and using OSINT;
- Create an identified/anonymous presence to be used to conduct online investigative research and data collection;
- Identify risks to users from OSINT data collection and explain countermeasures to be utilised in providing anonymity for users
- Enhance and customize the art of using OSINT techniques suitable for the collection of information for intelligence and counter intelligence purpose ;
- Strengthen the investigative methods, analysis, and distribution of information for the purpose of tackling all forms of crimes in clear web, social media, and dark web.

Schedule and Details of the Sessions (Tentatively from December 12 – 14, 2025)

Day –1 Cyber Laws and Open Source Intelligence Basics:

- Introduction to Cyber Laws and Cyber Crimes (hacking, Cyber Terrorism , Pornography , ISP Liability and Case studies)
- Electronic evidence and it admissibility in the court of Law (Section 65B Indian Evidence Act)
- Basics to Internet Governance in reference to web Technologies –Web3.0
- Introduction to Digital Forensics and Cyber Crime Scene Management
- Cyber Crime Investigation law and procedure
- What is intelligence and OSINT
- Exploring various technical aspects of various social media frameworks and their architectures.
- Robin Sage – A powerful Social Engineering experiment
- Information is Everywhere
- Lab 1:
  - Understanding Practice Hands on Usage of Autopsy | An Open-Source Digital Forensics Tool
  - Using OSINT to trace, track and identify a fake/ puppet profile on social media platforms and using various OSINT tools for intelligence gathering purposes.
  - Explore and report concurrent timelines, motivated posting activates for similar type of profiles and connect their histograms and audit trails to any malicious or mollified agenda against governance

Day–2: Tools and engines for use in your OSINT searches:

- Introduction to Social media intelligence (SOCMINT)
- Looking at websites for SOCMINT analysis and reporting
- Understanding Web Search engines and indexing patterns.
- Disposable Search Engines and impact its impact on Social Media Analytics.

- FOCA, Cree.py & Maltego
- Lab 2: Building your own Google Custom Search Engine for the purpose of SOCMINT analysis and reporting.

Day –3: Technical Scenarios and Use Cases:

- Counter Intelligence and Defenses
- Fake BBC news site and spreading misinformation
- Attacking the Stock Market
- General Petraeus and Clinton
- Volkswagen emissions scandal
- Mossack Fonseca (Mossfon)
- Intelligence Gathering Recipe
- Lab 3: Gathering intelligence on an organization in comprehensive manner.

Eligibility

Candidates who are pursuing graduation or had graduated are eligible to register.

Admission Procedure

- Submission of Online Application Form along with the required documents and the fee
- Direct admission subject to fulfilling the eligibility criteria

Course Fee:

Rs. 10,000/-

How to Apply

All the candidates should apply online through the website www.nalsarpro.org
Link to Apply : https://apply.nalsar.ac.in/application-form-for-short-term-courses
Last Date to Apply : December 10, 2025.

Conduct of the Course

Live sessions will be conducted online by the academicians, professionals and industry experts during weekend. Soft copy of the reference materials will be provided to the candidates.

If the enrollments are more than 100, then the University may conduct the classes in different batches on different dates.

Mode of Assessment

Online Examination will be conducted only once at the end of the course. The assessment may include MCQ, short answer questions, case study, problem based questions etc.

Award of Certificate (only soft copy through email):

- Course Completion Certificate: Candidates securing 50% or more in the Assessment Test will be awarded the ‘Course Completion Certificate’
- Certificate of Participation: All other enrolled candidates will be awarded ‘Certificate of Participation’

Please note that certificates will be issued in soft copy format only and will be sent via email. Printed (hard) copies will not be provided.

Course Coordinator & the Instructors

Prof. K. V. K. Santhy, Professor of Law & Director, Centre for Cyber Laws and Forensic Sciences, NALSAR University of Law
Course Coordinator

Prof. K. V. K. Santhy has over 24 years of teaching experience in Criminal Law and completed her Doctoral research on “Penal Reforms in India” from Osmania University. She currently serves as the Proctor of NALSAR University of Law, overseeing campus discipline and student affairs.

Prof. Santhy has led and contributed to several prestigious research projects, including the Study of the Indian Penal Code from a Gender Perspective (NCW), Law on Grievance Redressal in Public Offices in A.P. (Centre for Good Governance), and the Draft Amendment to the Transplantation of Human Organs Act, 1994 (National Deceased Donor Transplantation Network). She also coordinated major studies for the Bureau of Police Research and Development (BPR&D) and the UGC on sentencing perspectives and defective investigations.

She has been associated with the Global Internet Governance and Advocacy (GIGA) initiative of the Ministry of Electronics and Information Technology and has conducted international workshops with the ICRC on International Humanitarian and Criminal Law. As part of her post-doctoral research at the Max Planck Institute for International Criminal Law, Germany, she worked on “Punishment and Sentencing” and submitted a report on “Counterfeit Drugs in India.”

An accomplished author, Prof. Santhy has published books and articles on sentencing, police torture, fair trial standards, and human rights law. She is a sought-after speaker, having delivered lectures at leading institutions including NISA, CFSL, National Police Academy, NADT, and Women and Child Welfare Departments on topics such as criminal justice, cyber laws, and sentencing reforms.

Mr. Sai Manohar Aramane, IPS
Additional Director General of Police (Intelligence), Madhya Pradesh

Mr. Sai Manohar Aramane is a 1995–batch officer of the Indian Police Service (Madhya Pradesh Cadre). Over his distinguished career spanning nearly three decades, he has served in key positions in state and central agencies, including a significant tenure with the Central Bureau of Investigation (CBI). During his deputation to the CBI, he handled several high-profile investigations related to economic offences, bank frauds, and extradition cases.

Currently serving as the Additional Director General of Police (Intelligence), Government of Madhya Pradesh, Mr. Aramane continues to play a pivotal role in strengthening intelligence operations and law enforcement coordination. His professional excellence has been recognized with the President’s Police Medal for Distinguished Service and the Police Medal for Meritorious Service.

A career officer with a deep commitment to integrity and national service, Mr. Aramane is widely regarded for his expertise in investigation, intelligence management, and leadership in policing.

Sri Vamshi Krishna
IPS, DIG, ED, Karnataka

Sri Vamshi Krishna is an Indian Police Service (IPS) officer in the Karnataka cadre. He has served as Joint Commissioner of Police (West Zone), Bengaluru City. He is described as a police officer and trainer with a strong background in cybercrime and information security.

Mr. U. Ramamohan
Director, Digital Forensics and Cyber Security, Truth Labs International

Mr. U. Ramamohan holds an M.Sc. in Statistics from S. V. University, Tirupati, and a Post Graduate Diploma in Computer Applications from the University of Hyderabad. A retired Superintendent of Police from Telangana and Andhra Pradesh States, he brings over 25 years of expertise in digital evidence handling and forensic analysis, having investigated more than 1000 cases as a Computer Forensic Expert with APFSL and CID.

With an additional 15 years of experience in field crime investigations, including cybercrimes, bomb, and explosive cases, Mr. Ramamohan now leads the Digital Forensics and Cyber Security division at Truth Labs International, providing expert guidance and technical insight in complex forensic investigations.

Dr. Shilohu Rao

Dr. Shilohu Rao is a Professor at the National Law University, Jodhpur, where he specializes in the intersection of law and technology. With extensive experience in legal education, research, and academic administration, he has contributed significantly to developing interdisciplinary perspectives on digital governance, cybersecurity, and emerging technologies. Dr. Rao has been closely associated with several national initiatives and academic collaborations that explore the evolving relationship between technology and legal frameworks, particularly in areas like data protection, cyber law, and digital forensics.

He has been invited as a speaker and resource person at various national conferences and workshops, including joint programmes organized by NLU Jodhpur and IIT Jodhpur on “Law and Technology.” Dr. Rao’s teaching and research integrate contemporary issues such as artificial intelligence, blockchain, and cybercrime regulation into the broader discourse of law and policy. His academic leadership and policy engagement make him a key voice in shaping legal education and research on technology law in India.

Mr. Ram Ganesh
Founder and CEO of CyberEye

Ram Ganesh is the Founder and CEO of CyberEye and a distinguished expert with over 13 years of experience in Cyber Intelligence, Investigations and Digital Forensics. A Chevening Cybersecurity Fellow from Cranfield University (UK Defence Academy), he has served with leading organisations including DRDO and TCS in Cyber Security R&D and Analysis.

An international speaker, Ram is part of and has presented his work on Cyber Intelligence, Forensics and Investigations at global platforms such as Defcon US, Underground Economy - Council of Europe HQ, UN conventions (UNTOC, UN-AHC), Bsides, GC3B Geneva, Interpol’s DFEG and Intersec Dubai. He has trained over 25,000 professionals across ISRO, DRDO, CBI, NIA, Armed Forces, and State Police, among others.

At NALSAR, Ram brings his extensive expertise in cyber security strategy, digital forensics, and cyber law enablement to strengthen interdisciplinary initiatives between law, technology, and national security.

Mr. Rajesh Gopal
Cyber Security Consultant – Lab Sessions

Rajesh Gopal is a seasoned cybersecurity and digital forensics leader with 18+ years of international experience in cyber defense, incident response, IoT/OT security, threat intelligence, and security governance for government, law enforcement, and Fortune 500–scale organizations. He currently serves as Director of IT – Cyber Security at Skillsoft Software India Pvt. Ltd., and has led high-impact security programs across critical sectors including BFSI, semiconductor, aerospace, telecom, and heavy industry. He has directed global incident response and complex cybercrime investigations, advised on national-level security transformation, built and matured Security Operations Centers, and driven compliance across frameworks such as SOX, PCI DSS, ISO 27001, FedRAMP, StateRAMP, and ISO 17025. A founder, consultant, and adjunct professor, he is also recognized for delivering 2000+ hours of expert training to enterprises, government, and law enforcement on advanced cyber operations, digital forensics, and financial fraud.