



NALSAR
UNIVERSITY OF LAW
HYDERABAD



**Center for Cyber Laws
and Forensic Sciences**

**THREE DAY ONLINE
CERTIFICATE COURSE
ON**

**CYBER-CRIMES INVESTIGATION USING
OPEN SOURCE INTELLIGENCE (OSINT)
TOOLS & TECHNIQUES**



NALSAR
UNIVERSITY OF LAW
HYDERABAD



**Center for Cyber Laws
and Forensic Sciences**

CYBER-CRIMES INVESTIGATION USING OPEN SOURCE INTELLIGENCE (OSINT) TOOLS & TECHNIQUES

Course Fee: **Rs. 4,000/- (INR)**

Eligibility: **Any graduate / Any student pursuing graduation can apply**

Date of the programme: **9 to 11 December 2022 (3 Days)**

Last date to apply: **7 December 2022**

[**Click Here to Apply**](#)

LEARNING OUTCOMES

The learning strategy is focused to enhance the capacity of participants to integrate OSINT tools into cyber investigations. Upon completion of the course, the participants are expected to be able to

- 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 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

LEARNING MODULES: DAY WISE

Day -1 OSINT Basics:

What is intelligence and OSINT, Grey Areas and Ethics, Robin Sage – A powerful Social Engineering experiment, Exploring the concept of "Information is Everywhere".

Lab 1: Using OSINT to build a fake/ puppet profile for intelligence gathering purpose.

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

Thinking and Analysis, Looking at websites, Google Custom Searches, Disposable Search Engines, Exploring FOCA, Creepy & Maltego tools etc.

Lab 2: Building your own Google Custom Search Engine

Day -3: Technical Scenarios and Case Studies:

1. Fake news websites and spreading misinformation.
2. Attacking the Stock Market portals.
3. General Petraeus and Clinton case.
4. Volkswagen emissions scandal
5. Mossack Fonseca (Mossfon).

Lab 3: Gathering intelligence of a proxy organization as a case study analysis and reporting.

Final Lab Assessment Test (FLAT)

SCAN TO APPLY

INTAKE : 70 PER BATCH

