
# CERTIFIED OSINT INVESTIGATOR

# Module 1: Introduction

- Introduction to Open Source Intelligence (OSINT).
- Basic Terminologies in OSINT
- The OSINT Rule
- OSINT Life-Cycle
- Real World Use Cases
- Legal and Ethical Considerations of OSINT

# Module 2: Operation Security

- Introduction to Operation Security (OPSEC)
- Importance of OPSEC in OSINT
- Real-world examples of OPSEC failures
- Anonymity v/s Pseudonymity
- Introduction to VPNs and Proxies
- Dangers of Free VPNs

# Module 3: Building Virtual Lab

- Introduction to Virtual Machines
- Setting Up OSINT Lab
- Setting Up Browsers
- Anti-fingerprinting Settings in Browser
- Introduction to I2P Network and Setting Up I2P in a Browser
- Proxychains Basics

# Module 4: Web Osint

- Introduction to Web OSINT
- Search Engines: Google, Bing, DuckDuckGo
- Introduction to Google Dorks
- Collecting Website Information using Google Dorks.
- Website Info Gathering (Whois, ICANN, WhoisXML API, etc.)
- DNS Records (A, AAAA, CNAME, and others)
- Subdomain Enumeration
- IP and Hosting Analysis
- Web Archives and Snapshots
- CMS and Technology Fingerprinting

- URL Analysis and Redirect Tracking
- Website Monitoring

# Module 5: Username OSINT

- Introduction To Username Investigation
- Why Username Matters in Investigation
- Username Investigation Using Search Engines (Google, Bing, DuckDuckGo, Yandex)
- Using Google Dorks for Investigation
- Cross-Platform Username Search
- Identifying linked Accounts
- Tracking User Activity
- Setting Up Username Monitoring

# Module 6: Email Osint

- Introduction To Email Investigation
- Understanding Email Formats
- Email Investigation Using Google Dorks
- Email Verification and Validity Check
- Email Metadata Analysis
- Finding Connected Social Media Accounts
- Breach and Leak Detection

# Module 7: Phone Number Osint

- Introduction to Phone Number Investigation
- Identifying Telecom Provider and Region
- Reverse Search
- Social Media Footprints
- Finding Linked Emails/Social Media Accounts
- Data breach and leak Lookup

# Module 8: Image & Geolocation Osint

- Introduction to Image & Geo Location Investigation
- Image Investigation using Reverse Image Search
- Metadata Extraction and Analysis
- Facial Recognition and Analysis

# Module 9: SOCMINT

- Understanding Social Media Intelligence (SOCMINT)
- Difference b/w Socimint and Osint
- SOCMINT Investigation On Facebook
- SOCMINT Investigation On Instagram
- SOCMINT Investigation On X (Twitter)
- SOCMINT Investigation On LinkedIn
- Locating GeoTagged Posts

# Module 10: Telegram Osint

- Introduction to Telegram Investigation
- Telegram Account Footprinting
- Groups and Channel Discovery
- Comments Investigation
- Set up Telegram Monitoring On Channels/Groups
- Set Up Monitoring on Telegram User

# Module 11: Darkweb Osint

- Introduction to Surface Web, Deep web, and Dark web
- Common Myths and Facts about the Dark Web
- How the TOR Network Works
- Installing and Configuring TOR
- Access Onion Websites
- Safe Practices while using TOR
- Overview of Marketplaces
- Search Engines for Onion
- Dark Web OSINT Tools
- Darkweb Monitoring Techniques

# Module 12: Maltego

- Introduction to Maltego Community Edition (CE)
- Setting Up Maltego For Investigation
- Conducting A Socmint Investigation

# Bonus

- Making a Report for the findings.
- Creating your own SOCMINT search engine.
- Additional Resources for further studies about OSINT.

# CTF-BASED EXAM

At the end of this course, you'll take on a real-world investigative challenge through a Capture The Flag (CTF) exam. This hands-on assessment tests your OSINT skills—from digital footprinting and social media profiling to deep web research and data correlation. Solve realistic scenarios using open-source intelligence techniques and earn your certification by proving your investigative expertise.

# CONNECT WITH US