



The Canadian OSINT Centre

Open-Source Intelligence Self-Directed Certification Program

A comprehensive OSINT certification program with multiple tracks and specialized courses.

Table of Contents

Table of Contents	2
Course Catalogue	3
Certification Overview	4
Level 1: OSINT Analyst Certification	5
Level 2: OSINT Investigator Certification	5
Level 3: OSINT Specialist Certification	6
Level 4: OSINT Expert Certification	6
Course 1 - OSINT Foundations, Tools, Tactics & Ethics	7
Course 1: Analyst Topics	8
Course 2: Introduction to Intelligence Analysis	10
Course 2: Analyst Topics	11
Course 3: Social Media & Digital Platform Investigations	13
Course 3: Analyst Topics	14
Course 4: Attribution & Identity Tracing	16
Course 4: Investigator Topics	17
Course 5: Intermediate Social Media & Emerging Platforms	19
Course 5: Investigator Topics	20
Course 6: Geolocation & Spatiotemporal Investigations	22
Course 6: Investigator Topics	23
Course 7: Advanced Intelligence Analysis & Behavioral Profiling	24
Course 7: Specialist Topics	25
Course 8: Covert Investigations & Sock Puppetry	27
Course 8: Specialist Topics	28
Course 9: Dark Web Investigations & De-anonymization	29
Course 9: Specialist Topics	30
Course 10: Advanced Technical OSINT	31
Course 10: Expert Topics	32
Course Sign-Up Information	34

Course Catalogue

Course	Course Title	Level	Duration	Certification Track
1	OSINT Foundations – Tools, Tactics & Ethics	Basic	10 hours	OSINT Analyst
2	Introduction to Intelligence Analysis	Basic	10 hours	OSINT Analyst
3	Social media & Digital Platform Investigations	Basic	10 hours	OSINT Analyst
4	Attribution & Identity Tracing	Intermediate	9 hours	OSINT Investigator
5	Intermediate social media & Emerging Platforms	Intermediate	9 hours	OSINT Investigator
6	Geolocation & Spatiotemporal Investigations	Intermediate	9 hours	OSINT Investigator
7	Advanced Intelligence Analysis & Behavioral Profiling	Advanced	8 hours	OSINT Specialist
8	Covert Investigations & Sock Puppetry	Advanced	8 hours	OSINT Specialist
9	Dark Web Investigations & De-anonymization	Advanced	6 hours	OSINT Specialist
10	Advanced Technical OSINT	Advanced	10 hours	OSINT Expert

Certification Overview



Certifications

Certified OSINT Analyst

Certified OSINT Investigations

Certified OSINT Specialist

Certified OSINT Expert



Overall Timeframe

Approximately 90 hours



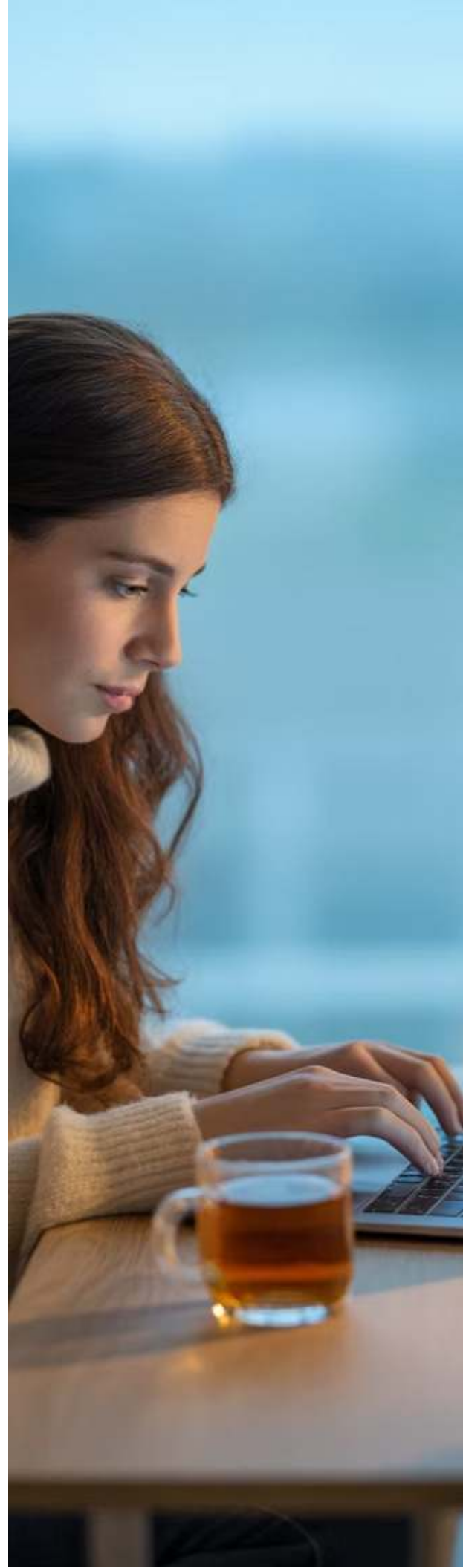
Audience

OSINT professionals in law enforcement, government, or corporate investigations



Total Certification Price

\$5000 CAD + exam fees (includes 10% discount for advanced program sign-up)



Level 1: OSINT Analyst Certification



OSINT Foundations – Tools, Tactics & Ethics

\$500



Introduction to Intelligence Analysis

\$500



Social media & Digital Platform Investigations

\$500

Timeframe

30 hours

Audience

Entry-level professionals in
law enforcement,
government, or corporate
investigations

Certification Price

\$1500 CAD + \$75 exam fee

Level 2: OSINT Investigator Certification



Attribution & Identity Tracing

\$500



Intermediate social media & Emerging Platforms

\$500



Geolocation & Spatiotemporal Investigations

\$500

Timeframe

~30 hours

Audience

Intermediate investigators,
security professionals,
private sector intelligence
teams

Certification Price

\$1400 CAD + \$75 exam fee

Level 3: OSINT Specialist Certification



**Covert Investigations
& Sock Puppetry**

\$500



**Dark Web
Investigations & De-
anonymization**

\$500



**Advanced Intelligence
Analysis & Behavioral
Profiling**

\$500

Timeframe

~30 hours

Audience

Cybercrime analysts, senior
intelligence officers, federal
and defense professionals

Certification Price

\$1500 CAD + \$75 exam fee

Level 4: OSINT Expert Certification



Advanced Technical OSINT

\$500

Timeframe

15 hours

Audience

Cybercrime analysts, senior
intelligence officers, federal
and defense professionals

Certification Price

\$500 CAD + \$50 exam fee



Course 1 – OSINT Analyst Level

OSINT Foundations: Tools, Tactics & Ethics

Description

Get started with the essentials. This course lays the groundwork for any OSINT investigation, introducing foundational tools, ethical considerations, and proven workflows. Whether you're new to the field or brushing up on the basics, it's your launchpad into the intelligence world.

Audience

All practitioners (beginner to intermediate)

Key Objectives

Understand OSINT fundamentals, ethical boundaries, and legal limitations

Learn basic search tools, operators, and documentation methods

Gain familiarity with planning and collection workflows

Basic

Level

10

Hours

15

Modules

Course 1: **Analyst** - Topics 1 - 8

Introduction to OSINT

Understand the role of OSINT in investigations and intelligence gathering.

OSINT Planning & Preparation

This session introduces a structured blueprint for launching professional-grade online investigations.

The Canadian Privacy Act

Explore key privacy laws, compliance guidelines, and investigative boundaries.

Basic Search Techniques

Master advanced operators and search tactics for efficient queries.

Google Advanced Functionality

A deep dive into Google's lesser-known search tools for predictive analysis, communications and search automation

Google Alternatives and Meta Search Tools

Explore powerful Google alternatives and meta search tools to expand your OSINT capabilities beyond conventional search engines.

OSINT Ethics

Discuss data protection, responsible collection, and ethical sourcing.

Overview of Online Environments

A strategic overview of online environments, from surface web to the lesser-known deep and dark web.

Course 1: **Analyst - Topics 11 - 15**

Browsers, Extensions, Add-Ons and Apps

Choosing the right web browser can make or break the privacy and success of an OSINT investigation. This session provides a detailed walkthrough of five major browsers—Firefox, Chrome, Edge, Safari, and Brave—comparing them through the lens of security, privacy, and functionality.

Reverse Image Search

Discover how to trace the origin and reuse of digital images.

Websites, Domain Structure & WHOIS Exploration (part 1)

The fundamental building blocks of the internet—domain names, DNS, IP addresses, and WHOIS data.

Investigating Domains, Companies and Current and Historical WHOIS Lookup Tools (part 2)

Walk through a real-world OSINT workflow—starting from a public-facing website and expanding outward to uncover infrastructure, ownership, and digital linkages.

Basic OSINT Tools Overview

Preview essential OSINT platforms and tools used for digital investigations.

Search Automation

Learn how to streamline your investigations using automated search tools that enhance efficiency and uncover hidden insights.

The Wayback Machine

Uncover archived web content and trace digital footprints using the Wayback Machine and Internet Archive tools.



Course 2 - OSINT Analyst Level

Introduction to Intelligence Analysis

Description

Start thinking like an analyst. This foundational course introduces core intelligence principles, structured thinking models, and reporting logic. Ideal for students, new investigators, and anyone transitioning into intelligence roles.

Key Objectives

01

Understand the Intelligence
Cycle and analytic
frameworks

02

Recognize bias, logic errors,
and data source integrity

03

Build structured BLUF-style
reports

04

Learn to distinguish
between raw data and
actionable intelligence

Basic

Level

10

Hours

15

Modules

Course 2: Analyst – Topics 1 – 8

Introduction to Intelligence Analysis

Learn the steps of the intelligence process, from direction to dissemination.

The Investigative Mindset

Learn to think like an investigator by mastering the critical, analytical, and ethical mindset essential for effective OSINT investigations.

Logic Fallacies, Biases, Discernment and Critical Thinking

Identify logical fallacies and learn to question assumptions. Identify and avoid common analytical errors and cognitive traps.

Source and Data Evaluation and Verification

Evaluate the trustworthiness of a source and the reliability of its information and confirm the accuracy and legitimacy of data.

Bookmarking & OSINT Organization Tools

Use digital tools to track, organize, and revisit investigation sources.

Creating Timelines

explores how chronological sequencing of events helps uncover hidden patterns, track the evolution of incidents, and improve analytical clarity

Mind Mapping

How to use mind maps to track evolving investigations, organize large volumes of information, and uncover relationships between people, organizations, assets, & locations.

Using Forensic OSINT to Gather and Preserve OSINT Evidence

Document and preserve digital evidence in a court-admissible format.

Course 2: **Analyst** – Topics 9 – 15

Using Hunchly to Gather & Preserve OSINT Evidence

Discover how to capture, organize, and preserve online investigative evidence using Hunchly browser add-on

Note Taking

Structure field notes and organize observations for clarity and efficiency.

Basic Report Writing

Draft reports that are concise, clear, and driven by intelligence priorities.

Canadian Case Law

Examine precedent-setting court decisions that define what's admissible, what crosses legal lines, and how OSINT can support legal outcomes when properly collected.

Privacy Impact and Sensitivity Assessment

Privacy Impact Assessments ensure OSINT investigations are not just effective, but legally & ethically sound.

Deep Web Tools

Utilize specialized search engines, indexing tools, and analysis platforms

Internet Archives

Explore historical imagery, cached sites, and archived elements to verify changes over time.



Course 3 - OSINT Analyst Level

Social Media & Digital Platform Investigations

Unlock the secrets behind the screens. This course explores mainstream social media platforms through an investigative lens, teaching you how to gather intel, attribute activity, and uncover key details across the most-used platforms in the world.

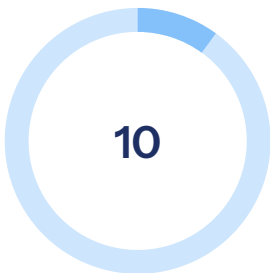
Audience

LE units, investigators, journalists, analysts

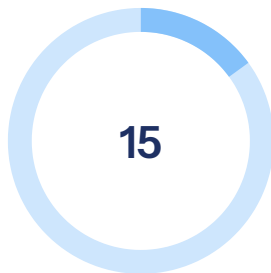
Course Details Overview



Level



Hours



Modules

Key Objectives



Identify
Platforms

Analyze User
Patterns

Understand
Attribution

Infer
Identities

Apply
Workflows

Course 3: Analyst Topics 1 – 8

Introduction to Social Media Platforms

Understand how each platform operates and what data is publicly accessible.

Investigating Facebook

Learn to trace posts, friends, photos, and activity timelines.

Investigating Facebook Marketplace

Identify seller identities and track item postings through investigative clues.

Investigating Instagram

Extract insights from bios, hashtags, image content, and tagged locations.

Investigating X (formerly Twitter)

Track account creation, user behavior, follower networks, and timelines.

Investigating TikTok

Understand short-form content tracking and audio-based trend tracing.

Investigating Reddit

Map activity across subreddits, user histories, and conversation threads.

Investigating Reddit Part 2

Put theory into practice using real-world Reddit scenarios – safely, ethically, and effectively.

Course 3: Analyst Topics 9 – 15

Investigating LinkedIn

Profile professional identities, work history, and company connections.

Investigating Snapchat

Learn what's recoverable through usernames, Snap Maps, and linked content.

Investigating Multimedia

Analyze shared videos, images, and sound for embedded metadata and origins.

Searching Video Platforms

Learn to find user-generated content and filter by date, type, and region.

Investigating Message Groups & Forums

Locate, access, and investigate private or fringe communities and discussion boards.

Social Media Analysis & Attribution Basics

Correlate behavior patterns and content clues to identify real-world actors.

Analysis & Attribution Demo

Observe the principles of account attribution, data correlation and triangulation in action across multiple platforms.

Course 4 – OSINT Investigator Level

Attribution & Identity Tracing

Description

Learn the structured process of identifying, validating, and attributing digital identities across platforms. This course equips learners with investigative techniques to track usernames, link digital trails, and confirm account ownership—all while maintaining legal and ethical standards.

Key Objectives

Perform deep-dive identity tracing via usernames, emails, photos

Use meta-search and visual link analysis

Understand preservation and evidential OSINT practices



Level

Intermediate



Modules

13



Hours

15



Course 4: Investigator Topics 1 - 9

Introduction to Attribution Principles

Understand the legal, ethical, and investigative foundations of linking digital activity to real-world identities.

Ethical and Legal Considerations of Using Breach Data

Discover the fundamentals of breach data—what it is, where it comes from, and the ethical considerations of its use in OSINT investigations.

Username Search Techniques

Investigate usernames across social platforms, forums, breach databases, and meta-search aggregators.

Origin Tracing – Name, Username, Email, Phone, IP, Image

Using partial identifiers to trace origin data and cross-reference with OSINT tools.

Account Attribution Framework

Build hypotheses based on language, timezones, behavior, image reuse, metadata, and registration patterns.

Identity Linkage via Data Analytics

Uncover user correlation using hidden data points

Visual Link Analysis Tools

the power of visual link analysis—a core technique in OSINT for mapping relationships, identifying patterns, and making sense of large-scale data.

Image and Avatar Tracing

Perform reverse image lookups to find reused photos, stock images, or photo EXIF data linked to personas.

Exploring Metadata in Public Files

Extract clues from PDFs, Word Docs, and images using tools like ExifTool and FOCA.

Course 4: Investigator Topics 10 – 13



Investigating Email Headers

Learn to dissect header strings to extract IPs, mail routes, originating systems, and metadata trails.

Account Creation Clues & Behavioral Fingerprinting

Identify consistencies in user bios, spelling, platform behavior, and time patterns.

Fake Persona Red Flags & Sockpuppet Attribution

Spot inconsistencies and trace back poorly built covert or fraudulent accounts.

Legal Considerations & Evidential Reporting

Ensure proper evidence capture, documentation, and chain of custody for attribution in court-ready formats.



Course 5 – OSINT Investigator Level

Intermediate Social Media & Emerging Platforms

Description

Stay ahead of the curve. Investigate lesser-known platforms, analyze online behavior, and leverage advanced tools for multilingual, metadata-rich intelligence gathering. Tailored for those seeking a deeper reach in the digital space.

Key Objectives

- 1

Investigate lesser-known and fringe platforms
- 2

Utilize tools for privacy analysis and digital behavior tracking
- 3

Employ multilingual and metadata tools

Intermediate

Level

14

Modules

9

Hours

Audience

OSINT investigators, law enforcement, brand protection, PIs, Reputation Management, HR

Course 5: Investigator Topics 1 – 9



Lesser Known Social Platforms Overview

Explore emerging platforms used by fringe groups and hard-to-reach communities.

Investigating Online Shopping Channels

Identify sellers, scams, and fraudulent activities in online marketplaces.

Investigating Telegram

Search for usernames, groups, bots, and media-rich public channels.

Investigating Discord

Monitor servers, analyze conversations, and investigate shared content.

Searching Online News Sources

Filter news coverage, identify bias, and track evolving narratives.

Searching Using Emojis

Understand emoji use in coded communications and search strategies.

Linguistics and Terminology Basics

Decode slang, acronyms, and localized language in digital communities.

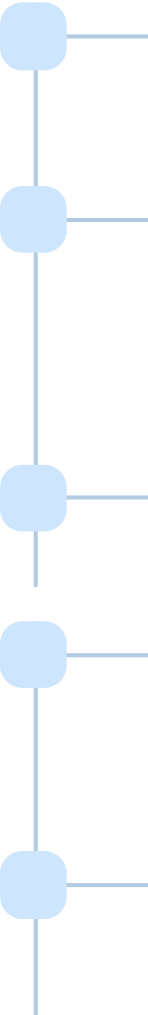
Foreign Language Search

Apply translation and native-language tools for international OSINT work.

Exploring Metadata in Social Content

Analyze hidden data in media files to uncover user details and timelines.

Course 5: Investigator Topics 10 – 14



Preserving Multimedia Files

Capture and archive video, audio, and image content for evidence use.

AI Considerations In OSINT

artificial intelligence is transforming open-source investigations across Canada. You'll learn how AI tools enhance OSINT processes—from data collection to analysis—while also examining their legal, ethical, and operational risks.

Query String Modification

Use URL structures to access hidden files, indexed content, and web parameters.

Long-Form User Generated Content

Explore how to identify, analyze, and extract intelligence from blogs, forums, and other long-form user-generated content

Investigating Weibo and WeChat

Learn how to investigate digital footprints, user behavior, and shared content on Chinese platforms like Weibo and WeChat.



Course 6 – OSINT Investigator Level

Geolocation & Spatiotemporal Investigations

Description

Map the unseen. Harness the power of geospatial intelligence to locate images, verify locations, and reconstruct timelines. From triangulation to satellite tools, this course equips professionals with advanced field techniques.

Key Objectives

 Perform precise geolocation using photos, video, metadata	 Employ triangulation and spatiotemporal logic
 Use satellite imagery and mapping platforms	 Leverage predictive and spatiotemporal techniques for strategic assessment

Audience

Major crimes teams, investigators, intelligence personnel



Level

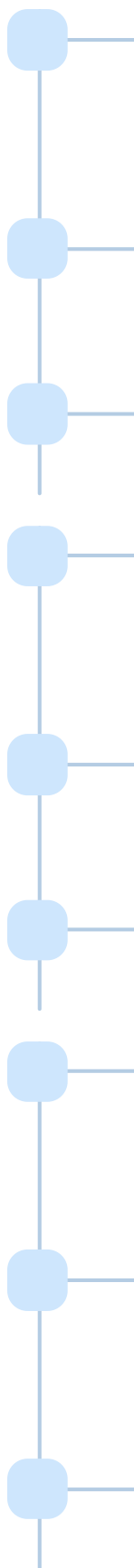


Modules



Hours

Course 6: Investigator Topics 1 – 9



Introduction to Geolocation

Understand the basics of geographic targeting, location clues, and geo-coordinate systems.

Mapping Tools & Satellite Imagery

Use tools like Google Earth, Sentinel Hub, and satellite feeds for real-world visual tracking.

Geofencing Concepts

Learn how to define digital boundaries and track user activity within geo-fenced regions.

Advanced Geolocation Techniques

Combine images, timestamps, terrain, and contextual data for high-precision location analysis.

Examining Images for Geolocation Cues

Analyze photo content for landmark recognition, shadow analysis, and environment clues.

Triangulating Locations via Visuals

Use object orientation, light direction, and skyline geometry to estimate position.

Pinpointing via Metadata

Extract and interpret geotags, timestamps, and EXIF fields embedded in images and videos.

Searching Video Platforms with Location Context

Use filters and hashtags to locate region-specific content on platforms like YouTube and TikTok.

Spatio-temporal Patterns in Reporting

Combine location and time data to reveal operational trends and anomalies

Course 7 - OSINT Specialist Level

Advanced Intelligence Analysis & Behavioral Profiling

Description:

Go beyond structured reporting with an intensive focus on behavior-driven insights. This course dives into online behavioral profiling, linguistic analysis, misinformation patterns, and advanced analytical methods. Built for professionals seeking to turn complex data into human intelligence.

Key Objectives:

- Identify behavioral patterns and linguistic cues in digital content
- Conduct deep analysis on disinformation and online manipulation
- Apply investigative mindset principles to advanced data sets

Advanced Level

8 Hours

11 Modules



Course 7: Specialist Topics 1 – 8



Advanced Intelligence Analysis

Expand on the standard intelligence cycle by integrating complex workflows and multi-layered data for richer insights and more accurate assessments.



Minimizing Your Digital Footprint

Learn strategies to reduce identifying traces and exposure through meticulous browser hygiene and digital discipline, including understanding the impact of web server logs.



Online Behavioral Profiling

Identify distinct behavioral traits, recurring activity patterns, and comprehensive digital personas by analyzing online interactions and content consumption.



Online Pattern Analysis

Map recurring habits, digital routines, and usage timelines to reveal consistent patterns and predict future online behaviors.



Detecting Disinformation and Misinformation

Uncover deceptive narratives and recognize coordinated influence operations by analyzing content, source, and propagation methods.



Deep Fakes and Generative AI Analysis

Develop methods to detect synthetic media, identify fake personas, and expose content manipulation created using advanced AI techniques.



Advanced Report Writing

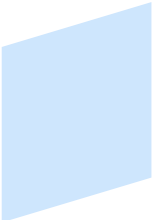
Master the art of structuring long-form intelligence products with exceptional analytical depth, strategic clarity, and actionable recommendations.



Predictive Analysis Basics

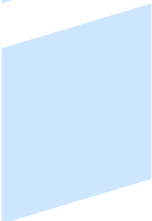
Learn to identify emerging threats and forecast potential behavior or trends by applying fundamental predictive analytical models to OSINT data.

Course 7: Specialist Topics 9 – 11



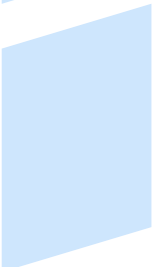
Linguistics and Social Engineering

Decode emotional language, recognize subtle linguistic cues, and identify manipulative phrasing to understand intent and influence in communications.



Visual Data Analysis

Utilize specialized tools to visually analyze complex data sets, create link graphs, and identify content clusters for a more intuitive understanding of relationships.



Analyzing Large Data Sets

Acquire skills to efficiently filter, sort, and visualize complex OSINT data, enabling you to spot critical patterns and extract actionable insights from high-volume information during investigations.



Course 8 – OSINT Specialist Level

Covert Investigations & Sock Puppetry

Description:

Operate under the radar. Learn how to build and manage covert online identities, safely access restricted communities, and protect your digital footprint. A must-have course for undercover professionals and cybercrime teams.

Audience: Undercover officers, digital detectives, researchers, journalists

Key Objectives:

Understand covert personas, OPSEC and VM environments

Develop, manage and safely use sock puppet accounts

Navigate private forums and secure browsing

Length
8 hours

Modules
10

Level
Intermediate

Course 8: Specialist Topics 1 - 10



Introduction to Covert Accounts

Learn the purpose, risks, and foundational strategies for using covert online identities.



Using Covert Accounts Safely

Maintain operational security (OPSEC) and reduce traceability while using false personas.



Creating Sock Puppet Accounts

Build credible, trace-resistant identities that align with real-world behaviors.



Developing Sock Puppet Personas

Flesh out backgrounds, language use, and digital trails to build trust with targets



Advanced Sock Puppet Tactics

Use cross-platform posting, media , and staged interaction to enhance believability.



Introduction to Covert Investigations

Understand what defines covert operations and their application in OSINT contexts.



Proxy Servers & VPNs's

Use digital cloaking tools to mask location and system information.



Introduction to Virtual Machines

Isolate investigations from your primary system and simulate multiple user environments.



Risk & Privacy Assessments

Evaluate your exposure and build mitigation strategies for investigators and organizations.



OSINT In Action

Use digital cloaking tools to mask location and system information.



Course 9 – OSINT Specialist Level

Dark Web Investigations & De-anonymization

Description:

Enter the shadows. This advanced course guides you through dark web navigation, actor profiling, de-anonymization techniques, and secure data collection. Built for cybercrime investigators and national security professionals.

Audience:

Cybercrime units, government analysts, national security

Key Objectives:

1. Navigate the dark web safely via TOR and TAILS environments
2. Perform de-anonymization using blockchain and OSINT
3. Profile actors and recover dark marketplace artifacts



6 hours

Length



9

Modules



Advanced

Level

Course 9: Specialist Topics 1 – 9



Introduction to the Dark Web

Define the dark web and understand how it's accessed and structured.



The TOR Browser

Learn how TOR works, including setup, navigation, and safe practices.



Dark Web Orientation & Navigation

Discover techniques for exploring hidden services and marketplaces



Dark Web Profile De-Anonymization

Identify actors by analyzing writing style, behavior, and reused metadata.



Basic Dark Web Investigations

Conduct safe entry-level investigations using secure platforms and tools.



Advanced Dark Web Investigations

Employ advanced tactics for tracking actors, wallets, and activity.



Introduction to Cryptocurrency

Follow crypto transactions and trace wallets using open-source tools.



Exploring Breach Data Tools

Leverage breach repositories to connect emails, IPs, and passwords.



Evidence Handling In Dark Web Operations

Leverage breach repositories to connect emails, IPs, and passwords.



Course 10 – OSINT Expert Level

Advanced Technical OSINT

Description:

Advanced Technical OSINT is where digital curiosity meets practical skill—designed for investigators who want to go beyond browser searches and into the guts of the internet. In this course, you'll get hands-on with web page elements, decode the basics of JavaScript and Python, navigate APIs, and harness the power of GitHub and Linux. From command line tactics to spyware detection, data scrapers to large datasets, this course empowers you with the tools to extract, process, and protect information like a true digital detective.

Audience:

Cybercrime investigators, threat analysts, and digital journalists, private investigators, corporate security teams

Key Objectives:

1. **Develop foundational technical skills** essential for OSINT investigations, including command-line navigation, scripting basics, and interacting with Linux-based tools.
2. **Utilize advanced online investigation techniques**, such as inspecting web elements, analyzing GitHub repositories, and leveraging APIs and data scrapers to extract and structure online intelligence.
3. **Enhance investigative accuracy and efficiency** by working with large datasets, identifying and mitigating spyware threats, and automating repetitive tasks using Python and other open-source utilities.



Level



Length



Modules

Course 10: Expert Topics 1 – 7

Github for OSINT

Discover how to identify, analyze, and leverage public repositories and developer activity on GitHub to support your investigations and uncover digital breadcrumbs.

Introduction to Javascript

Learn how JavaScript shapes the web and how understanding its structure can uncover hidden data, dynamic content, and investigative leads.

Effective Use of Web Page Inspector in OSINT

Master the browser's inspection tools to reveal hidden code, uncover embedded links, and access behind-the-scenes data on any website.

Understanding and Using API's

Understand how APIs work and learn to extract structured data directly from platforms to supercharge your OSINT investigations.

Connected Devices and Networks

Explore how devices communicate across networks, and learn to identify digital footprints, trace connections, and uncover hidden infrastructure in investigations.

Introduction to Command Line Interface (CLI)

Get comfortable navigating the command line as you learn the essential commands and workflows that form the backbone of technical OSINT work

Using Terminal for OSINT

Unlock the power of the command line to streamline tasks, run powerful tools, and dig deeper into digital investigations with speed and precision.

Course 10: Expert Topics 8 - 12

Introduction to Python for OSINT

Learn the basics of Python scripting to automate OSINT tasks, manipulate data, and build custom tools for more efficient investigations.

Introduction to Linux for OSINT

Dive into the Linux environment to harness its powerful tools, boost your digital privacy, and streamline investigative workflows in open-source intelligence.

Investigating SIM-Based Threat Vectors

Uncover how attackers exploit mobile networks through SIM swapping and cloning, and learn to recognize the signs and investigate these threats using OSINT techniques.

Data Scrapers and JSON

Learn how to use data scrapers to collect online information efficiently and make sense of JSON formats to extract actionable intelligence from structured data sources.

Analyzing Big Data

Learn to extract insights and identify patterns from large datasets using OSINT techniques tailored for real-world investigations.



How to Sign Up for Online Training



Step 1: Visit

[OSINT Courses | Expert-Led Open Source Intelligence Training in Canada](#)



Step 3: Select desired training program



Step 2: Create an account including a username and secure password



Step 4: Make payment



Step 5: Access course