



The Canadian OSINT Centre

Level Two - OSINT Investigator

Course One: Attribution & Identity Tracing

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.

1

Uncover hidden identities by tracing digital artifacts across the entire internet landscape.

2

Decode hidden metadata and map connections with powerful visual link analysis.

3

Preserve evidence with integrity and apply court-ready OSINT standards.

14

Topics

Comprehensive curriculum

7

Hours

Course duration

\$500

Cost

plus applicable taxes



[Click here](#) to register for Level Two - OSINT Investigator - Course One or enrol in all 3 Investigator courses and receive a 10% discount (excludes \$75 exam fee).

*A \$75 examination fee applies at the conclusion of **all 3 Investigator courses** to receive certification.

1

Introduction to Attribution Principles

Master the legal and ethical boundaries that define responsible attribution — and learn how investigators connect digital activity to real-world identities.

2

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.

3

Data Breach Tools

Harness specialized data breach tools to uncover exposed credentials, link accounts, and turn leaked data into actionable investigative intelligence.

4

Username Search Techniques

Investigate usernames across social platforms, forums, breach databases, and meta-search aggregators to expose the full digital footprint.

5

OSINT in Action

Connect the dots — use partial identifiers to trace origins, uncover hidden links, and cross-reference findings with powerful OSINT tools.

6

Account Attribution Framework

Build airtight hypotheses by analyzing language patterns, timezones, behaviour, image reuse, metadata, and registration clues.

7

Identity Linkage via Data Analytics

Surface powerful user correlations by exploiting hidden data points that others overlook.

8

Visual Link Analysis Tools

Harness visual link analysis to map complex relationships, spot hidden patterns, and turn overwhelming data into clear investigative intelligence.

9

Image and Avatar Tracing

Perform reverse image lookups using powerful tools to locate reused photos, stock images, or EXIF data linked to unidentified personas.

10

Exploring Metadata in Public Files

Dig beneath the surface of PDFs, Word docs, and images — using tools like ExifTool and FOCA to extract hidden clues that reveal authorship, location, and more.

11

Investigating Email Headers

Analyze email headers to identify originating IPs, mail routes, sending infrastructure, and metadata that attribute messages to their true source.

12

Account Creation Clues & Behavioural Fingerprinting

Cross-reference user bios, writing style, platform behaviour, and activity timing to build a reliable behavioural fingerprint.

13

Fake Persona Red Flags & Sockpuppet Attribution

Learn to identify the telltale signs of fake personas and attribute sockpuppet accounts using structural, behavioural, and linguistic analysis.

14

Legal Considerations & Evidential Reporting

Apply rigorous evidence capture, documentation standards, and chain of custody protocols to produce attribution findings that hold up in legal proceedings.



The Canadian OSINT Centre

Level Two - Investigator

Course Two: Social Media & Emerging Platforms

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

Designed for all OSINT practitioners (intermediate)



Go beyond mainstream platforms to investigate fringe networks where critical intelligence often hides.



Deploy specialized tools to analyze privacy exposures and track digital behaviour across platforms.



Leverage multilingual search capabilities & metadata analysis to extract intelligence that crosses language & border barriers.

14

Topics

Comprehensive curriculum

8

Hours

Total course duration

\$500

Cost

Plus applicable taxes



Sign up now for Level Two - OSINT Investigator - Course Two or enrol in all 3 Investigator courses to receive a 10% discount (excludes \$75 exam fee).

Course Topics:

- 1 Lesser-Known Social Platforms**
Map the digital terrain of fringe networks and emerging platforms where hard-to-reach communities operate beyond mainstream visibility.
- 2 Investigating Online Shopping Channels**
Track fraudulent sellers, expose scam operations, and uncover deceptive activity hiding in plain sight across online marketplaces.
- 3 Investigating Weibo and WeChat**
Explore how to use Chinese-based social media platforms to collect, search and preserve information, how to analyze sentiment trends and attribute identity.
- 4 Investigating Telegram**
Infiltrate Telegram's ecosystem by tracing usernames, monitoring groups, identifying bots, and extracting intelligence from media-rich public channels.
- 5 Investigating Discord**
Investigate Discord servers to monitor conversations, map community networks, and extract shared content for actionable intelligence.
- 6 Long-Form User Generated Content**
Explore how to identify, analyze, and extract intelligence from blogs, forums, and other long-form user-generated content.
- 7 Investigating Online News Sources**
Cut through media noise by filtering news coverage, detecting bias, and tracking how narratives develop and shift across sources.
- 8 Encoded Language: Emojis in OSINT**
Decode the hidden language of emojis used in coded communications and learn how to incorporate them into targeted OSINT search strategies.
- 9 Linguistics and Terminology Basics**
Master the evolving language of online communities — from slang and acronyms to localized terminology — to better interpret and contextualize digital intelligence.
- 10 Foreign Language Search**
Break language barriers by applying translation tools and native-language search techniques to conduct effective OSINT investigations across international targets.
- 11 Exploring Metadata in Social Content**
Analyze hidden data in media files to uncover user details and timelines.
- 12 Preserving Multimedia Files**
Systematically capture, preserve, and archive video, audio, and image content in formats that meet evidentiary standards for investigative and legal use.
- 13 AI Considerations in OSINT**
Artificial intelligence is transforming open-source investigations. You'll learn how AI tools enhance OSINT processes, from data collection to analysis, while also examining their legal, ethical, and operational risks.
- 14 Query String Modification**
Manipulate URL structures and query strings to surface hidden files, indexed content, and web parameters that standard searches miss.



The Canadian OSINT Centre

Level Two - Investigator

Course Three: Geolocation & Spatio-temporal Investigations

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.



Pin down exact locations using photos, video frames, metadata analysis, and triangulation techniques to place subjects in the physical world.

10

Modules

Comprehensive curriculum



Harness satellite imagery and advanced mapping platforms to verify locations, track movements, and build geospatial intelligence from open sources.

8

Hours

Total course duration



Apply predictive and spatiotemporal analysis to anticipate movements, reconstruct timelines, and support strategic investigative decisions.

\$500

Cost

Plus applicable taxes



[Click here](#) to register for Level Two - OSINT Investigator - Course One or enrol in all 3 Investigator courses and receive a 10% discount (excludes \$75 exam fee).

Course Topics:

1

Introduction to Geolocation

Build a solid foundation in geographic targeting — learning how to read location clues, interpret geo-coordinated systems, and apply them to real investigative scenarios.

2

Geofencing Concepts

Define precise digital boundaries and monitor user activity within geo-fenced zones to build location-based intelligence and track movement patterns.

3

Mapping Tools & Satellite Imagery

Tap into tools like Google Earth, Sentinel Hub, and live satellite feeds to visually track real-world locations, monitor changes over time, and corroborate ground-level intelligence.

4

Examining Images for Geolocation Cues

Scrutinize photos for landmark recognition, shadow direction, vegetation, signage, and environmental details that reveal exactly where and when an image was taken.

5

Triangulating Locations Using Visual Analysis

Combine object orientation, light direction, and skyline geometry to triangulate precise positions from visual evidence alone.

6

Pinpointing Using Technical Data

Pull geotags, timestamps, and EXIF fields from images and videos to establish precise location and time data that anchors your investigation.

7

Searching Video Platforms with Location Context

Leverage platform filters, hashtags, and geotags to surface region-specific video content on YouTube, TikTok, and beyond — turning public posts into precise location intelligence.

8

Spatiotemporal Patterns in Reporting

Fuse location and time data to identify operational patterns, detect behavioural anomalies, and build a chronological picture of events as they unfolded.

9

Advanced Geolocation Techniques

Integrate images, timestamps, terrain data, and contextual intelligence to achieve high-precision geolocation results that go beyond what any single source can provide.

10

Creating Interactive Maps for Investigations

Build dynamic, interactive maps that transform raw location data into compelling visual narratives — easy to explore, share with stakeholders, and update as investigations evolve.