JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Internet Intelligence Investigation Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Advanced Internet Intelligence Investigation Training Course

Internet Intelligence Investigation is a 2-week advanced training course for financial crime investigators, fraud and anti-money laundering analysts and bank compliance and security staff, who build an online investigation case file during the course. Fraudsters, money mules and sanctioned parties leave traces across websites, social platforms, company registries and blockchains, so banks that read those traces quickly stop losses earlier. Jupiter Prime Training designed this course around that open-source evidence.

Why Internet Intelligence Investigation Matters Now

Three forces shape online investigation in banks today. Fraud and laundering schemes now start and spread through social media, messaging apps and marketplaces before any transaction alert fires. Supervisors and courts expect suspicious activity reports and enhanced due diligence files to rest on documented, repeatable research rather than screenshots without provenance. Crypto-assets and shell companies let criminals move value across borders in minutes. A bank whose investigators collect open-source evidence lawfully and record it well can freeze funds and exit risky clients; one that searches casually risks tipping off suspects or producing evidence that will not stand. The course rests on the open-source intelligence cycle and digital evidence handling principles.

Who Gains Most from Internet Intelligence Investigation

- Financial crime investigators who build cases on fraud, bribery and laundering networks
- Anti-money laundering analysts who research customers, beneficial owners and counterparties during alerts
- Fraud prevention analysts who trace scam websites, mule accounts and impersonation campaigns
- Sanctions and enhanced due diligence staff who verify identities, ownership and adverse media
- Bank security and cyber staff who investigate account takeover and insider threats

Banks gain most when an AML analyst, a fraud investigator and a security specialist attend together, because online evidence often links a cyber incident, a mule network and a laundering pattern that each team sees only in part.

Internet Intelligence Investigation Capabilities

Participants leave able to plan, run and record an online inquiry from first lead to evidential report, without exposing themselves or the bank.

- Design search strategies with advanced operators and pivoting techniques — case leads for investigators
- Apply corporate registry and beneficial ownership research to shell structures — enhanced due diligence decisions
- Assess social media profiles, images and metadata for identity links — fraud network mapping
- Calculate cryptocurrency flows using blockchain explorers and clustering clues — asset tracing and freezing requests
- Specify evidence capture, hashing and logging procedures — admissibility and audit trails
- Build an online investigation case file with findings and confidence levels — suspicious activity reporting

Key Internet Intelligence Investigation Terms

- Open-source intelligence — information collected from publicly available sources and analysed to answer a specific investigative question.
- Pivoting — moving from one identifier, such as an email or phone number, to discover linked accounts, sites and people.
- Beneficial owner — the natural person who ultimately owns or controls a company or account, often hidden behind nominees.
- Digital footprint — the trail of accounts, posts, registrations and metadata a person or company leaves online.
- Blockchain explorer — a public tool that shows transactions, addresses and balances recorded on a cryptocurrency ledger.
- Operational security — measures that stop an investigator's research from revealing identity, intent or employer to the subject.

Internet Intelligence Investigation Day by Day

Day 1: Online Financial Crime and the Intelligence Cycle

- Fraud, Mule and Laundering Typologies Online — Where Digital Traces Appear
- Open-Source Intelligence Cycle — Requirements, Collection, Analysis and Reporting
- Legal and Ethical Boundaries of Online Research — Lawful Collection Limits
- Tipping-Off Risk and Case Confidentiality — Protecting Ongoing Investigations
- Intelligence Requirements From Alerts — Framing Investigative Questions

Day 2: Operational Security for Investigators

- Research Environments and Virtual Machines — Isolating Investigation Activity
- Sock Puppet Accounts and Attribution Risk — Safe Persona Management
- Browser Hardening and Network Masking — Hiding Investigator Footprints
- Account and Device Hygiene Policies — Bank Security Alignment
- Investigation Logs and Activity Records — Defensible Research Trails

Day 3: Advanced Search and Pivoting Techniques

- Search Engine Operators and Query Design — Precise Result Sets
- Cached, Archived and Deleted Content Retrieval — Recovering Removed Evidence
- Email, Phone and Username Pivoting — Linking Identities Across Platforms
- Domain Registration and Hosting Records — Mapping Scam Infrastructure
- Leaked Data and Breach Sources Handling — Ethical Use Decisions

Day 4: Corporate Registries and Beneficial Ownership

- International Company Registry Searches — Directors, Filings and Addresses
- Beneficial Ownership Chains and Nominee Indicators — Control Identification
- Shell and Front Company Red Flags — Trade-Based Laundering Clues
- Court Records, Insolvency Notices and Litigation Searches — Reputation Risk
- Adverse Media Screening Methods — Enhanced Due Diligence Evidence

Day 5: Social Media and People Investigation

- Social Platform Profiling and Network Mapping — Associate Identification
- Image Reverse Search and Geolocation — Verifying Claimed Locations
- Metadata Extraction From Photos and Documents — Hidden Attribution Clues
- Messaging Apps and Closed Group Monitoring Limits — Lawful Access Choices
- Online Marketplaces and Classified Listings — Mule Recruitment Detection

Day 6: Digital Footprint and Fraud Infrastructure

- Phishing and Impersonation Site Analysis — Takedown and Customer Warnings
- Fake Investment and Romance Scam Tracing — Victim Fund Recovery Leads
- Mule Account Network Analysis — Linking Online and Transaction Data
- Device, IP and Session Indicators — Account Takeover Investigations
- Payment Processor and Merchant Research — Card Fraud Patterns

Day 7: Cryptocurrency Tracing

- Wallet, Address and Transaction Basics — Reading Public Ledgers
- Blockchain Explorer Use and Address Clustering — Following Value Flows
- Mixers, Privacy Coins and Chain Hopping — Obfuscation Recognition
- Virtual Asset Service Provider Identification — Information Request Targets
- Crypto Cash-Out Points and Fiat Ramps — Bank Exposure Detection

Day 8: Analysis, Link Charts and Confidence

- Link Analysis and Network Charts — Visualising Relationships
- Timeline Construction From Online Events — Sequence of Conduct
- Source Reliability and Information Grading — Confidence Statements
- Hypothesis Testing and Bias Checks — Sound Investigative Conclusions
- Combining Open Sources With Internal Bank Data — Case Corroboration

Day 9: Evidence Capture and Reporting

- Web Page Capture, Hashing and Timestamps — Evidential Integrity
- Chain of Custody for Digital Material — Admissibility Requirements
- Investigation Report Structure and Findings — Decision-Ready Writing
- Suspicious Activity Report Narratives From Online Findings — Regulatory Quality
- Sharing Intelligence With Law Enforcement — Requests and Disclosures

Day 10: Practising the Online Investigation Case File

- Case Planning and Operational Security Set-Up — Applying Days 1 and 2
- Identity, Ownership and Social Research — Applying Days 3 to 5
- Fraud Infrastructure and Crypto Tracing — Applying Days 6 and 7
- Link Charts and Evidence Capture — Applying Days 8 and 9
- Online Investigation Case File — Presentation to a Financial Crime Committee

Applying Internet Intelligence Investigation After the Course

- Write an operational security standard for your team covering research devices, personas, logging and evidence capture, and agree it with information security.
- Re-open one closed alert and apply the pivoting and ownership methods to test whether online evidence would have changed the outcome.

Internet Intelligence Investigation Questions FAQ

What is Internet Intelligence Investigation and why does it matter now?

Internet intelligence investigation is the lawful collection and analysis of online public information to build financial crime cases. It matters now because fraud, mule recruitment and laundering increasingly run through social media, shell companies and crypto-assets before transaction monitoring sees them.

Which roles gain most from Internet Intelligence Investigation training?

Financial crime investigators, AML and fraud analysts, sanctions and due diligence staff and bank security teams gain most. Examples come from both retail scam cases and corporate trade-based laundering, so participants apply the methods across customer types.

How does Internet Intelligence Investigation training differ from a transaction monitoring course?

It differs by looking outside the bank's own data. A transaction monitoring course tunes alerts and scenarios, while this one researches websites, registries, social platforms and blockchains to explain who is behind an alert and how they connect.

What will you bring back from Internet Intelligence Investigation training?

You bring back an online investigation case file built on a realistic scenario. It contains search logs, ownership charts, crypto traces, captured evidence and a report your financial crime committee can act on.

Internet Intelligence Investigation: The Way Forward

The online investigation case file first informs whether a bank files a suspicious activity report, exits a relationship or requests a freeze. Investigators, compliance officers and financial crime committees use it to agree action on documented evidence. After its first use, the operational security settings and source list deserve a fresh look, since platforms and criminal methods change quickly.