FULL CURRICULUM

TCOA Complete Syllabus

Techonquer Certified OSINT Analyst: 14 modules covering search intelligence, identity tracing, geospatial analysis, human intelligence, darknet investigation, Python automation and career pathways.

14	2	TCOA
Modules	Months Duration	Certification

Module 1

Google Dorking Mastery & Multi-Engine OSINT Recon

From basic operators to advanced cross-engine intelligence gathering

Google Dorking Fundamentals

- Introduction to search operators and dork syntax, beginner to advanced level
- Core operators with real examples: site:, inurl:, intitle:, intext:, filetype:, ext:, cache:, related:, info:, link:
- Building and testing your first dork queries hands-on

Advanced Dork Combinations

- Advanced operator techniques: AROUND(), before:, after:, numrange for precision date and range filtering
- Powerful dork combinations for email harvesting, username hunting, and document leaks (PDF/DOCX/XLSX)
- Dork chains for phone number exposure, vehicle-related leaks, and darknet/onion mentions

Multi-Engine & Specialized Search

- Multi-engine coverage: Bing, DuckDuckGo, Yahoo, Yandex, Baidu, Startpage, Qwant, Mojeek
- Specialized OSINT engines: Shodan, Censys, ZoomEye, FOFA, Intelligence X, Leak-Lookup, Criminal IP

- Specialized OSINT engines: Shodan, Censys, ZoomEye, FOCA, Intelligence X, Leak-Lookup, Criminal IP
- Advanced cross-engine techniques: search engine swapping, cross-engine dorking, image reverse search
- Academic & archive search: Google Scholar, Wayback Machine, Archive.is, Archive.org

Module 2

Number Intelligence: Phone OSINT

Trace any phone number to a full identity profile

Number to Identity

- Number to name: open-source lookups, telecom databases, reverse phone directories
- Number to email: correlating phone numbers to registered email addresses across platforms
- Number to photo: locating profile images linked to phone numbers via social accounts
- Number to social media: mapping numbers to Facebook, WhatsApp, Telegram, Instagram, Twitter
- International phone OSINT: country code intelligence, carrier lookup outside India

Advanced Number Techniques

- Number to banking details: UPI ID correlation, payment app linkages (Paytm, PhonePe), financial exposure patterns
- SS7 protocol exploit awareness and mobile number porting traces
- SIM swap indicators and VoIP number intelligence

☆ **Live Case Study:** Jaish-E-Mohammed terrorist intelligence, how phone OSINT was used in real counter-terrorism investigations

Module 3

Email Intelligence

Deep-dive into email forensics and breach correlation

Email Validation & Breach Correlation

- Email validation and domain analysis: MX record lookup, domain age analysis
- SPF/DMARC/DKIM record investigation
- Gmail enumeration: alias detection, recovery hint leaks, linked Google service exposure
- Breach correlation using HaveIBeenPwned, DeHashed, and WeLeakInfo for compromised credentials

Email Forensics

- Linked account discovery: tracing email addresses to GitHub repositories, Pastebin dumps, dark web forums
- Disposable email detection: identifying throwaway services used to hide identity
- Ethical SMTP probing to verify if an email address is active
- Email header forensics: originating IP, mail server hops, timezone hints, client software

☆ **Live Case Study:** Spear-phishing attribution, tracing a real phishing campaign back to its operator using email intelligence

Module 4

Username Intelligence

Track individuals across the entire internet via their handles

Cross-Platform Username Search

- Unified username search: automated discovery across 500+ platforms simultaneously
- Profile correlation: connecting profiles via shared images, bios, posting patterns, writing style

Advanced Recovery Techniques

- Avatar reverse search across TinEye, Yandex Images, Google Images
- Handle variations and mutations to discover hidden accounts
- Username squatting detection: identifying fake or impersonation accounts
- Deleted account recovery using Wayback Machine snapshots and archive tools

☆ **Live Case Study:** Tracking darknet vendors via reused handles, how a single username exposed a marketplace operator's real identity

Module 5

Vehicle Intelligence

License plates, VINs, and vehicle trail reconstruction

License Plate & VIN Intelligence

- License plate lookup using open-source regional databases and government portals
- VIN decoding: manufacturer data, model year, production plant, factory specifications
- Ownership history: previous owners, transfer records, jurisdiction changes
- Insurance claims and publicly available accident reports

Vehicle Trail Reconstruction

- ANPR camera awareness: understanding Automatic Number Plate Recognition infrastructure
- Exploiting leaked toll records and e-challan systems to reconstruct vehicle movement
- Stolen vehicle tracking: cross-referencing databases with sighting reports
- Cross-border VIN cloning detection for vehicle fraud and smuggling

☆ **Live Case Study:** Smuggling and terror logistics vehicle trails, mapping cross-border smuggling routes using vehicle OSINT

Liking the syllabus so far?

Seats are limited, secure your spot in the next batch.

Enroll Now

Module 6 New

Website & Domain Intelligence

Investigating websites, domains, and hosting infrastructure

Domain & Ownership Intelligence

- WHOIS intelligence: registrant details, historical WHOIS records, privacy-protected domains
- DNS intelligence: A, MX, TXT, NS records, reverse DNS lookups
- SSL certificate transparency logs: uncovering subdomains and infrastructure via certificate history
- Hosting history: tracing IP changes, hosting providers, CDN detection

Infrastructure Mapping

- Tech stack fingerprinting: identifying CMS, frameworks, analytics IDs, ad network IDs
- Subdomain enumeration using passive and active techniques
- Wayback Machine analysis: reconstructing a site's history and detecting content changes
- Linking websites to owners via shared analytics IDs, tech fingerprints, and hosting patterns

Module 7 New

GEOINT: Geospatial Intelligence

Pinpointing locations from images and video using open-source clues

Image Geolocation Fundamentals

- Image geolocation methodology: reading signage, architecture, vegetation, and terrain clues
- Using Google Earth and Google Maps for satellite comparison and verification
- Street View analysis: matching ground-level imagery to a photo's vantage point

Advanced Geospatial Analysis

- Shadow and sun position analysis to estimate time, date, and geographic latitude
- Terrain analysis: elevation, coastlines, and landform matching for narrowing search areas
- Video geolocation: frame-by-frame analysis, audio cues, and reflections

> ☆ **Live Case Study:** Geolocating a hostage video to a specific district using shadow angle and terrain matching

Module 8

Social Media Intelligence (SOCMINT)

Platform-specific deep OSINT across every major social network

Twitter/X & Instagram OSINT

- Advanced search operators and historical tweet extraction with Twint forks
- Follower/following graph analysis
- Profile scraping with Instaloader, story archive extraction, tagged photo correlation

Facebook, LinkedIn, TikTok & Telegram OSINT

- Privacy setting bypass techniques and employer history extraction
- Social graph mapping across Facebook and LinkedIn intelligence gathering
- Channel subscriber profiling and forwarded message tracing on Telegram
- Telegram group member extraction and TikTok profiling

Graph & Geo Intelligence

- Graph analysis and friend-of-friend mapping using Maltego transforms
- Sentiment and influence scoring through post analysis
- Geotag intelligence and location extraction from embedded GPS metadata
- Private account pivots via followers, mentions, and tagged posts

Module 9 New

HUMINT: Human Intelligence

Where technical OSINT ends and human-source tradecraft begins

HUMINT Fundamentals

- HUMINT fundamentals: how human intelligence complements technical OSINT
- Social engineering awareness: recognizing and understanding manipulation tactics
- Elicitation techniques: extracting information through natural conversation

Source Validation & Ethics

- Human source validation: cross-checking credibility and reliability of information
- Ethical boundaries: legal limits, consent, and responsible investigation conduct
- HUMINT case study: a real investigation where human sources confirmed technical findings

Module 10

Darknet Intelligence

Safe navigation, monitoring, and attribution on the dark web

Safe Darknet Navigation

- Configuring Tor Browser for anonymous investigation and understanding traffic correlation risks
- I2P and Freenet: alternative anonymity networks used by threat actors, structure, access, and monitoring

Market & Forum Monitoring

- Darknet market monitoring: drug markets, weapons listings, credential shops, data leak marketplaces
- Forum scraping: extracting intelligence from Dread and hidden service boards using custom Tor crawlers
- Search tools in practice: Ahmia, DarkSearch, Torch

Vendor Attribution

- Vendor profiling using PGP keys, writing style (stylometry), pricing patterns, reused usernames
- PGP key correlation: identifying individuals through reused public keys and key server records
- Ethical cryptocurrency tracing: blockchain analysis, tracing Bitcoin/Monero transactions, clustering wallets

Module 11 New

Python for OSINT

Automate every technique from earlier modules using Python

Python OSINT Fundamentals

- Python setup for OSINT: requests, BeautifulSoup, and working with public APIs
- Writing a script to automate Google dorking and search result collection
- Web scraping fundamentals: parsing HTML, handling pagination, and rate limiting responsibly
- Working with JSON responses from breach-check, username-check, and geolocation APIs

Building Your Own OSINT Tool

- Combining multiple modules into one script: username check, email breach check, and social lookup
- Automating username availability checks across 500+ platforms with Python
- Packaging your script as a command-line OSINT tool
- Exporting investigation results into structured reports (CSV, JSON)

☆ **Hands-On Build:** Every student leaves this module with a working self-built Python OSINT tool

Module 12

Breach Correlation & Tool Mastery

Consolidating breach intelligence and hands-on tool workshops

Breach Correlation Deep-Dive

- Advanced use of HaveIBeenPwned, DeHashed, and WeLeakInfo for cross-platform breach correlation
- Linking breached data to real identities and building composite profiles

Tool Mastery Workshop

- Hands-on lab with Maltego for link analysis and entity mapping
- SpiderFoot, theHarvester, and Recon-ng for automated reconnaissance workflows
- Building a repeatable OSINT investigation pipeline using multiple tools together

Module 13 New

Career Opportunities in OSINT

Where an OSINT skill set can take you professionally

Career Pathways & Roles

- Understanding where OSINT skills fit across cybersecurity, law enforcement, journalism, and corporate risk
- Building a portfolio and resume that highlights OSINT investigation skills
- How the TCOA certification is positioned for freelance and full-time roles

Roles this course prepares you for:

- OSINT Investigator
- Cyber Crime Investigator
- Threat Intelligence Analyst
- Fraud & Risk Analyst
- Due Diligence Analyst
- Investigative Journalist Support
- Freelance OSINT Consultant
- Government & Defence Intelligence Roles

Module 14

Capstone & Certification

Bringing every discipline together in a final live investigation

Real-World Case Study Capstone

- Combining Google Dorking, number, email, username, website, GEOINT, social media, HUMINT and darknet intelligence on a single live investigation
- Using your self-built Python tool as part of the capstone investigation
- Guided capstone walkthrough with mentor feedback
- Certification assessment and award of the Techonquer Certified OSINT Analyst (TCOA) certificate

That's the full 14-module curriculum.

Ready to become a Techonquer Certified OSINT Analyst?

Enroll Now