Module Objective:
Learn ethical, legal OSINT investigation workflows: email and mobile profiling, advanced search operators, image/video verification, correlation, attribution confidence, and court-ready reporting.

Curriculum

SEGMENT 4:1 Introduction to OSINT & Investigative Mindset

What is OSINT?

Definition and scope of Open-Source Intelligence

Difference between:

- OSINT vs Surveillance
- OSINT vs Hacking

Legal and ethical boundaries (critical for law enforcement & professionals)

OSINT Intelligence Cycle

- Requirement definition
- Collection
- Validation
- Correlation
- Reporting

Key Principle:

- If it's not reproducible and legal, it's not OSINT.

SEGMENT 4.2 Email ID–Based OSINT

What an Email ID Can Reveal

- Username patterns
- Linked platforms & services
- Breach exposure
- Social media presence
- Cloud services & forums
- Professional profiles

Investigative Use-Cases

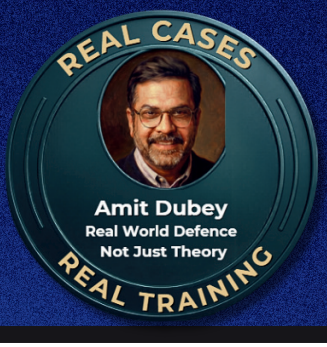
- Phishing source identification
- Fraudster profiling
- Insider threat analysis
- Impersonation cases

Practical Techniques

- Username enumeration logic
- Password reuse risk analysis
- Identifying burner vs primary email IDs

Legal Emphasis

- No credential testing
- No unauthorized access
- Passive intelligence only



SEGMENT 4.3 Mobile Number–Based OSINT

Intelligence from a Mobile Number

- Country & telecom circle
- Messaging app linkage
- Business listings
- Social media associations
- Fraud database presence

Practical Use-Cases

- Scam & extortion investigations
- Fake profiles & impersonation
- Threat actor attribution
- Victim–suspect linkage

Common Pitfalls

- Number recycling by telecom operators
- False attribution due to shared devices
- Over-reliance on a single source

4.4 Google Dorking for Investigators

What is Google Dorking?

Using advanced search operators to uncover:

- Exposed data
- Publicly indexed sensitive information
- Misconfigured systems
- Leaked documents

Core Google Operators

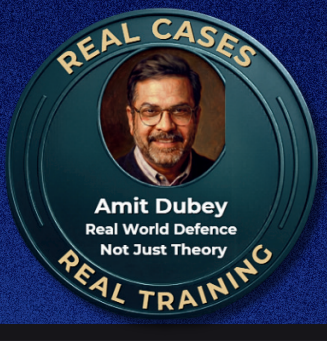
- site:
- filetype:
- intitle:
- inurl:
- cache:
- "" (exact match)
- -(exclude)

Investigative Applications

- Identifying leaked PDFs, Excel files
- Exposed credentials & configs
- Organization reconnaissance
- Tracking misinformation origins

Ethical Rule

- Discover ≠ Exploit
- Discovery must never turn into intrusion.



4.5 Image OSINT (Visual Intelligence)

What images can reveal:

- Geo clues
- Time/environment cues
- Reuse/manipulation
- Identity/affiliation indicators
- Metadata when available

Methods:

- Reverse image checking
- Metadata review (when available)
- Landmark/terrain analysis
- Shadow/weather estimation
- Signboard/language cues

Important Note:

- Most platforms strip metadata—rely on visual intelligence and corroboration, not EXIF alone.

4.6 Video OSINT (Advanced & High-Impact)

Why Video OSINT is Critical

Videos are primary tools of:

- Propaganda
- Disinformation
- Psychological operations

Video OSINT Techniques

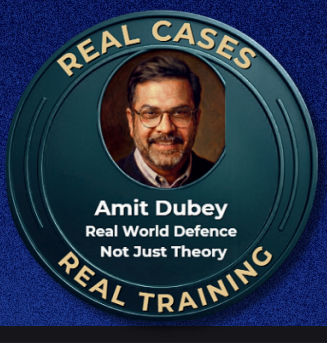
- Frame-by-frame analysis
- Audio accent & background noise
- Landmark & movement tracing
- Upload timeline reconstruction
- Identifying reused or edited clips

Investigative Scenarios

- Fake viral videos
- Deepfake suspicion
- Edited clips used for defamation
- Incident reconstruction

Key Skill

- Separating what is shown from what is claimed



4.7 Correlation & Attribution in OSINT

Correlation Methods

- Email ↔ Username ↔ Image ↔ Mobile
- Timeline matching
- Behavioral consistency analysis
- Platform cross-validation

Attribution Confidence Levels

- Low (single source)
- Medium (multi-source)
- High (multi-source + timeline match)

Golden Rule

- OSINT suggests — it does not accuse

4.8 OSINT Reporting & Court Readiness

How to Document OSINT Findings

- Screenshots with timestamps
- URLs & access dates
- Tool-independent explanations
- Clear assumptions & limitations

Report Structure

- Objective
- Sources used
- Findings
- Correlation logic
- Confidence assessment
- Limitations

Legal Reality

- Courts accept methodology clarity, not tool names

4.9 Practical Lab / Capstone Exercise

Scenario-Based Exercise

- Participants are given:
- One email ID
- One mobile number
- One image
- One short video clip

Tasks

- Build subject profile
- Identify inconsistencies
- Detect misinformation elements
- Prepare OSINT intelligence report