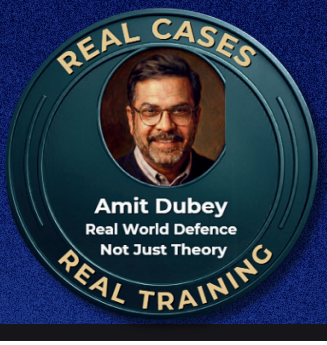
MODULE 10:
ADVANCED IPDR ANALYSIS & INTERNET TRAFFIC FORENSICS



Module Objective:
Turn raw CDRs into evidence: interpret CDR fields accurately, clean datasets, map relationships, trace movement using cell tower data, correlate multiple numbers/devices, reconstruct timelines, and present findings in a court-ready format.

Curriculum

Segment 10.1 Internet Architecture & IPDR Generation

Topics:

- ISP network architecture
- Broadband, Mobile data, FTTH, Hotspot IPDR
- NAT, CGNAT, Proxy impact
- Dynamic vs Static IP
- IPv4 vs IPv6
- How IPDR is generated by ISPs
- Legal obligations of ISPs

Segment 10.2 IPDR Record Structure

Fields Explained:

- User IP
- Public IP
- Port number
- Start & end time
- Session duration
- Upload / download bytes
- Protocol type
- Destination IP
- URL / Domain
- IMEI / IMSI / MAC
- APN / Device type

Segment 10.3 Data Cleaning & Normalization

Techniques:

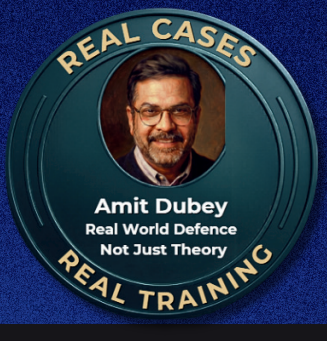
- Time normalization
- Duplicate removal
- Port separation
- Protocol filtering
- NAT port mapping
- Session merging

Segment 10.4 Core IPDR Analysis Techniques

Analysis Types:

- Time-based usage
- High data bursts
- Night-time activity
- Protocol misuse
- VPN usage indicators
- TOR traffic patterns
- Proxy detection

MODULE 10:
ADVANCED IPDR ANALYSIS & INTERNET TRAFFIC FORENSICS



Segment 10.5 Website & Application Identification

Topics:

- Domain resolution via IP
- CDN challenges
- App signature mapping
- Cloud service differentiation
- Social media traffic identificationFinal report preparation
- Encrypted traffic inference

Segment 10.6 VPN, TOR & Anonymization Detection

Indicators:

- Known VPN IP ranges
- Port anomalies
- Session patterns
- Repeated foreign IPs
- TOR exit node correlation
- DNS mismatches

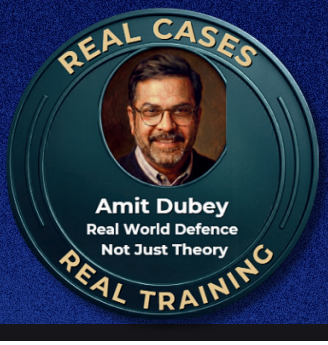
Segment 10.7 User Behavior Profiling

Patterns:

- Work vs personal usage
- Risk behavior indicators
- Obsession patterns
- Communication intensity
- Transaction behavior

Segment 10.8 Correlation with Other Evidence

- Evidence Type - Correlation Use
- CDR - Location & communication
- Mobile Forensics - App usage confirmation
- CCTV - Physical presence
- Bank Logs - Transaction timing
- Email - Account access
- Social Media - Content posting
- Cloud Logs- File access



Segment 10.9 Cyber Crime Use Cases

Use Case 1 – Online Fraud

- IPDR shows access to fake banking site
- VPN used during transaction
- Correlated with bank timestamp

Use Case 2 – Cyber Stalking

- Repeated late-night social media traffic
- Same IP access pattern

Use Case 3 – Data Leakage

- High upload volume to foreign IP
- Non-business hours

Use Case 4 – Terror / Extremism Content

- Visits to flagged domains
- Encrypted traffic spikes

Use Case 5 – Insider Threat

- Cloud upload sessions
- USB usage time correlation

Segment 10.10 Evidence Identification in IPDR

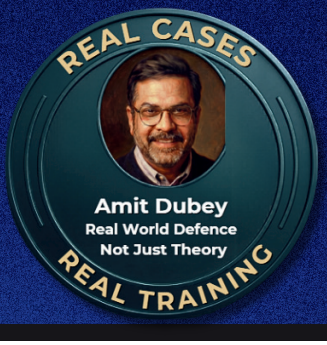
Key Evidence Indicators:

- Time of access
- Destination IP / Domain
- Port usage
- Protocol type
- Data volume
- Device identifier
- Repeated patterns

Evidence Types:

- Behavioral evidence
- Technical evidence
- Circumstantial evidence

MODULE 10:
ADVANCED IPDR ANALYSIS & INTERNET TRAFFIC FORENSICS



Segment 10.11 Timeline Reconstruction

Topics:

- Multi-day timeline
- Incident window
- Session clustering
- Cross-platform correlation

Segment 10.12 Legal Admissibility

Topics:

- Chain of custody
- IPDR authenticity verification
- Section 65B certification
- Expert report drafting
- Cross-examination preparedness

Segment 10.13 Advanced Practical Case Lab

Case Simulation:

- Fraud suspect IPDR
- VPN usage detection
- Location correlation
- Device identification