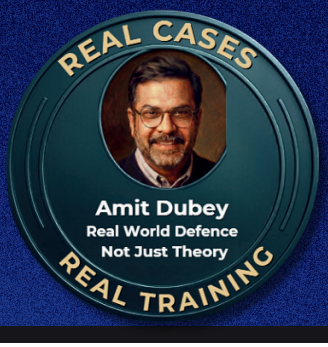


Module Objective:
Turn raw CDRs into evidence: interpret CDR fields accurately, clean datasets, map relationships, trace movement using cell tower data, correlate multiple numbers/devices, reconstruct timelines, and present findings in a court-ready format.

Curriculum

SEGMENT 11.1 IoT Forensics Fundamentals

Topics

- IoT ecosystem architecture
- Protocols: MQTT, CoAP, HTTP, BLE, Zigbee
- Cloud-IoT integration
- Evidence volatility in IoT
- Legal challenges

Evidence types

- Device logs, mobile app logs, cloud sync records, network traffic

11.2 Smart Device Log Analysis

Devices covered

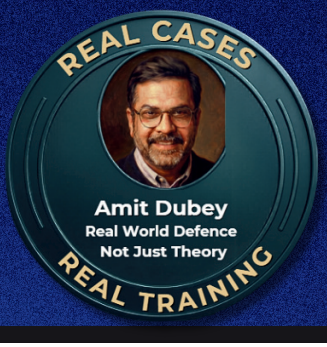
- Smart TV
- Alexa / Google Home
- Smart plugs, cameras
- Home automation hubs

Topics

- Local storage locations
- User activity logs
- Voice command history
- Device pairing records
- Network connection logs
- Firmware tampering indicators

Practical

- Smart TV log interpretation
- Alexa voice activity evidence



11.3 Wearable Forensics (Fitbit, Smartwatch)

Topics

- Step count logs
- Heart rate history
- Sleep records
- GPS workout routes
- App synchronization logs
- Timeline reconstruction

Use cases

- Presence at crime scene
- Activity verification
- Health timeline correlation

11.4 Drone Forensics Fundamentals

- Drone components
- Remote controller logs
- Mobile app data
- SD card artifacts
- Cloud flight backups

11.5 Drone Flight Log & GPS Analysis

Evidence extraction

- Flight time, altitude, speed
- Take-off / landing points
- GPS tracks, waypoints
- Battery data
- Camera trigger logs

Analysis

- Flight path reconstruction
- No-fly zone violations
- Pilot location estimation
- Mission profiling

Practical

- DJI / Autel log interpretation
- GPS track plotting

11.6 Drone Crime Use Cases

- **Smuggling**: Border flight paths
- **Surveillance**: Hovering logs
- **Terror**: Restricted zone access
- **Privacy breach**: Camera activation logs
- **Accident**: Impact location

MODULE 11:
ADVANCED IOT, DRONE, VEHICLE & CLOUD FORENSICS

Amit Dubey
Real World Defence
Not Just Theory

11.7 Vehicle Forensics- (EDR & Telematics)

Topics

- Event Data Recorder (EDR)
- Airbag module logs
- Speed history
- Brake application
- Steering angle
- Seatbelt status
- GPS route history
- Infotainment logs
- Evidence uses
- Accident reconstruction
- Driver behavior
- Timeline verification
- Hit & run analysis
- Practical
- Sample EDR data interpretation

11.8 Cloud Forensics

Platforms

- AWS, Google Cloud, Azure

Topics

- Cloud log types
- IAM activity logs
- Access timestamps
- IP address history
- Object access records
- VM logs
- Storage bucket access

Evidence acquisition

- Legal process
- Preservation request
- Data integrity
- Metadata validation

11.9 Cloud Crime Use Cases

- Data breach
- Insider threat
- Cloud ransomware
- Unauthorized access
- Evidence destruction attempt

11.10 Flipper Zero Based IoT Security Testing (Ethics-first)

- Topics (risk awareness + controlled demonstration)
- RFID cloning risks
- NFC replay attack risk awareness
- Sub-GHz signal capture risk awareness
- Garage/gate vulnerability risk awareness
- Bluetooth spoofing awareness
- IoT penetration testing ethics
- Forensic value
- Demonstrating security weaknesses
- Reproducing attack scenarios in controlled environments
- Court demonstration support

MODULE 11:
ADVANCED IOT, DRONE, VEHICLE & CLOUD FORENSICS

11.11 Evidence Correlation Framework

Examples of how evidence connects:

- Drone GPS ↔ CCTV
- Vehicle EDR ↔ Mobile CDR
- Fitbit GPS ↔ IPDR
- Alexa logs ↔ Mobile audio
- Cloud logs ↔ Laptop logs
- IoT network ↔ Router PCAP

11.12 Timeline Reconstruction

Topics:

- Multi-device timeline
- Cross-platform synchronization
- Incident window mapping
- Activity clustering

11.13 Evidence Identification

- IoT evidence types: Behavioral, location, interaction, control, communication
- Drone evidence: Flight intent, operator location, payload usage
- Vehicle evidence: Driver actions, accident dynamics
- Cloud evidence: Access intent, data manipulation

11.14 Timeline Reconstruction

- Chain of custody
- Section 65B
- Forensic report format
- Expert testimony preparation
- Visualization exhibits

11.15 Evidence Identification

Scenario:

- Drone surveillance crime
- Vehicle escape route
- Fitbit location proof
- Cloud file upload
- Alexa voice command
- Participants must
- Extract evidence
- Correlate logs
- Build timeline
- Prepare final forensic report