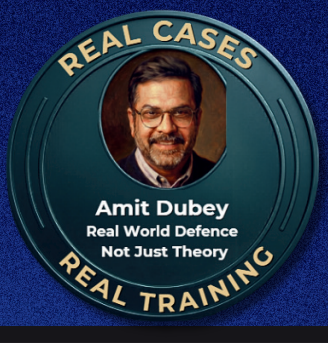


Curriculum

SEGMENT 7.1 Networking & Traffic Flow Refresher (Foundation)

(Short but essential)

How data actually flows through:

- Routers
- Switches
- Firewalls
- TCP/IP vs UDP behavior in attacks
- NAT, PAT, and Port Forwarding (critical for attribution)
- Internal vs External IP interpretation

Why this matters:

- Most investigators misinterpret logs because of NAT & shared IPs.

SEGMENT 7.2 Router Logs – Types & Significance

Types of Router Logs

System Logs

- Boot, reboot, firmware updates

Authentication Logs

- Login attempts (success/failure)

Traffic Logs

- Source IP, Destination IP, Ports, Protocols

Security Logs

- Firewall blocks
- IDS/IPS alerts

Configuration Change Logs

- Admin access, rule modification

Common Log Fields Explained

- Timestamp (UTC vs local – legal importance)
- Source / Destination IP
- Source / Destination Port
- Protocol
- Action (ALLOW / DROP / REJECT)
- Interface (WAN/LAN)

MODULE 7:
ROUTER LOG ANALYSIS & WIRESHARK

(Designed for cyber forensics, SOC, law enforcement, network security & incident response audiences)

SEGMENT 7.3 Interpreting Router Logs for Cybercrime Detection

Attack Indicators in Logs

- Port scanning patterns
- Repeated failed login attempts
- Sudden outbound traffic spikes
- Repeated connections to unknown foreign IPs
- DNS queries to suspicious domains

Case Scenarios

- Malware-infected device inside LAN
- IoT botnet traffic
- Insider misuse
- Data exfiltration indicators

Hands-on Exercise

- Given router logs → identify:
- Compromised device
- Time window of attack
- Possible attack type

SEGMENT 7.4 Log Correlation & Timeline Reconstruction

Aligning logs with:

- System logs
- Application logs
- ISP logs
- Creating an attack timeline
- Importance of time synchronization (NTP)

Common Mistakes

- Confusing scan traffic with attack traffic
- Misattributing NAT traffic to wrong device

SEGMENT 7.5 Introduction to Packet Capture (PCAP)

What is a packet capture?

Difference between:

- Logs vs Packets
- Metadata vs Content
- Legal considerations in packet capture
- Where PCAP fits in investigations

SEGMENT 7.6: Mobile Hardening Framework (MobiArmour Approach)

A practical mobile security framework (not “one app that solves it all”).

Protection layers

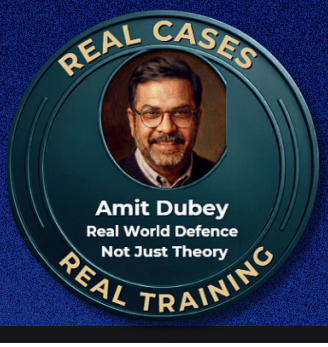
- App permission hygiene
- Rogue / over-permissioned app detection
- Device lock + backup discipline
- Public Wi-Fi safety

Live demo

- Identify risky permissions and remove spyware-like apps

MODULE 7:
ROUTER LOG ANALYSIS & WIRESHARK

(Designed for cyber forensics, SOC, law enforcement, network security & incident response audiences)



SEGMENT 7.7 Wireshark – Interface & Core Concepts

Wireshark Interface Overview

- Packet list pane
- Packet details pane
- Packet bytes pane

Capture vs Display Filters

- Why most analysts get this wrong
- Real-world examples

SEGMENT 7.8 Wireshark Filters for Investigators Essential Display Filters

- ip.addr ==
- tcp.port ==
- udp.port ==
- http, https, dns
- tcp.flags.syn == 1
- frame contains

Attack-Focused Filters

- Brute force detection
- Suspicious DNS queries
- Beaconing behavior
- Command & Control traffic

Lab Exercise

- Identify:
- Malicious IP
- Exfiltration attempt
- Malware beacon pattern

7.9 Analyzing Attacks Using Wireshark

Practical Analysis

- TCP stream reconstruction
- Suspicious HTTP headers
- DNS tunneling indicators
- Encrypted traffic metadata analysis

Common Threat Scenarios

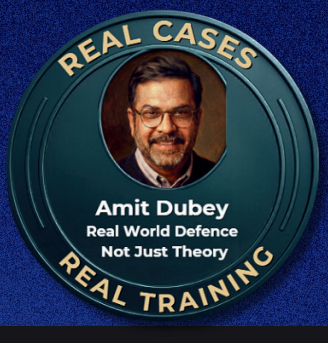
- Phishing payload download
- RAT communication
- Data leakage via DNS / HTTP

SEGMENT 7.10 Correlating Router Logs with Wireshark Evidence

Step-by-Step Correlation

- Identify suspicious IP from router logs
- Filter same IP in PCAP
- Validate traffic type
- Confirm attack intent
- Attribute internal device

This is the MOST important investigative skill in this module



SEGMENT 7.11 Reporting & Legal Readiness

- How to present findings clearly
- Screenshots vs exports (what courts accept)
- Preserving chain of custody
- Writing a technical but court-friendly report
- Sample Report Sections
- Summary of incident
- Timeline
- Evidence (logs + PCAP)
- Observations
- Expert opinion

7.12 Capstone Exercise (Realistic Simulation)

Scenario

- Organization reports suspicious data leak

Given:

- Router logs
- PCAP file

Task:

- Identify compromised system
- Determine attack vector
- Extract indicators of compromise (IOCs)
- Prepare final investigation report