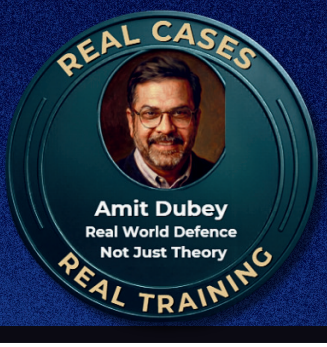


Module Objective: This module trains a complete investigative workflow:

Router/Firewall Logs → Suspicious Patterns → PCAP Validation → Correlation → Attribu tion → Defensible R eporting

Curriculum

SEGMENT 2.1. SOP to Check if a Mobile Phone is Hacked

Topics Covered:

- Common hacking methods (Spyware, RATs, Phishing, SIM Swap)
- Behavioral indicators of a hacked phone
- Network & data usage anomalies
- App permission abuse
- Background process monitoring
- Battery & performance red flags

SOP Checklist:

- Check unknown apps
- Review app permissions
- Monitor data usage
- Scan with trusted security tools
- Che ck system lo gs
- Verify Google/Apple account security
- Network traffic analysis
- Backup & reset decision matrix

Practical Demo:

- Live phone inspection walkthrough

SEGMENT 2.2. Android Phone Security & Forensic Check

Topics:

- Android OS security architecture
- Google Play Protect & system integrity
- Detecting malicious APKs
- Root detection
- USB debugging risks
- Developer mode misuse
- Safe configuration checklist

Hands-on:

- App permission audit
- Malware det ection demo

SEGMENT 2.3. Phone Security & Forensic Check

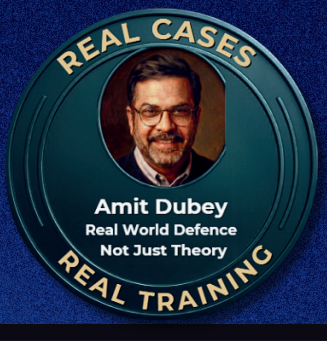
Topics:

- iOS security model
- Jailbreak detection
- iCloud account compromise
- Profile & MDM abuse
- Pegasus-like spyware awareness
- Secure iPhone settings SOP

Hands-on:

- Privacy & security audit walkthrough
- iCloud protection checklist

MODULE 2:
MOBILE & DIGITAL DEVICE SECURITY – Detection, Protection & Recovery



SEGMENT 2.4. Securing CCTV Systems

Topics:

- How CCTV systems get hacked
- Default password risks
- Port forwarding dangers
- Cloud CCTV vulnerabilities
- Insider threats

Security SOP:

- Password policy
- Firmware updates
- Network isolation
- Logging & monitoring
- Access control
- Legal compliance

Case Studies:

- Real CCTV hacking incidents

SEGMENT 2.5. Authentication & Security Enhancement

Topics:

- Password best practices
- Multi-Factor Authentication (MFA)
- Biometric risks & myths
- OTP hijacking
- Session hijacking
- Zero-trust concept

Practical:

- Building a strong authentication model
- Password manager usage demo

SEGMENT 2.6. Securing Routers / Wi-Fi Networks

Topics:

- Router hacking methods
- Evil Twin attacks
- DNS hijacking
- Firmware vulnerabilities
- IoT risks

SOP Checklist:

- Change default credentials
- WPA3 configuration
- Disable WPS
- Firmware update
- Guest network setup
- MAC filtering & logging

SEGMENT 2.7. Deleted Data Recovery

Topics:

- How deletion works in mobiles
- Logical vs Physical deletion
- Cloud backup recovery
- Forensic recovery limitations
- Legal & ethical aspects

Demonstration:

- Recovery from Android
- iPhone backup recovery
- SD card recovery