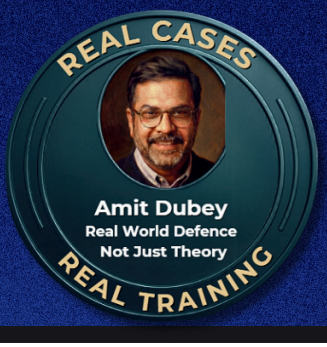
MODULE 6:
DIGITAL FORENSICS & AI THREAT INVESTIGATION



Module Objective:
Extract real digital evidence from browsers, emails, chats and audio. Detect deepfakes, assess AI-driven cyber risks, and identify hidden data (steganography) using an evidence-first, court-aware workflow.

Curriculum

SEGMENT 6.1 Web Browser Forensics

Topics Covered

- Browser artifact locations
- History analysis
- Cookie interpretation
- Download logs
- Cache inspection
- Private browsing myths
- Timeline reconstruction

Practical

- Chrome, Firefox, Edge evidence extraction
- Case simulation

SEGMENT 6.2 Email Investigation

Topics

- Email architecture
- Header structure
- IP tracing
- SPF, DKIM, DMARC analysis
- Spoofing detection
- Phishing identification
- Attachment forensics

Practical

- Live header decoding
- Phishing email case study

MODULE 6:
DIGITAL FORENSICS & AI THREAT INVESTIGATION

SEGMENT 6.3 Chat & App Forensics

Platforms

- WhatsApp
- Telegram
- Signal overview
- Instagram, Facebook Messenger

Topics

- Message artifacts
- Deleted message recovery concept
- Media metadata
- Contact extraction
- Call logs
- Location history
- Cloud backups

Practical

- App database analysis demo

SEGMENT 6.4 Audio Forensics

Topics

- Audio formats
- Noise analysis
- Voice comparison basics
- Spectrogram reading
- Audio enhancement
- Tampering detection
- Authentication of recordings

Practical

- Spectrogram analysis demo

SEGMENT 6.5 Deepfake Detection

Topics

- How deepfakes are created
- Facial artifacts
- Eye movement anomalies
- Lip sync mismatch
- Audio deepfake clues
- AI watermarking
- Legal implications

Practical

- Deepfake vs real comparison

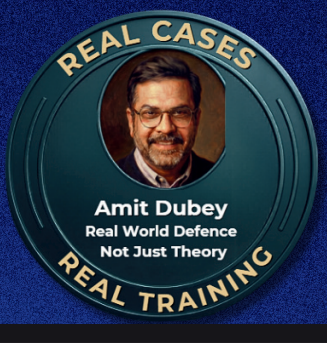
SEGMENT 6.6 AI Risk & Forensics

Topics

- AI-generated crime evidence
- Prompt abuse
- Synthetic identity fraud
- AI voice cloning
- AI phishing
- Forensic challenges
- Legal admissibility

Case Studies

- Real-world AI misuse incidents



SEGMENT 6.7 Steganography & Hidden Data Detection

Topics

- Image steganography
- Audio steganography
- File signature analysis
- Metadata mismatch
- Pixel anomaly detection
- Tool-based detection
- Limitations

Practical

- Hidden data extraction demo