MODULE 3:
CYBER CRIME INVESTIGATION & ADVANCED CYBER AWARENESS

"Think Like an Investigator, Not a Victim"

Amit Dubey
Real World Defence
Not Just Theory

Module Objective:
To help participants connect digital dots, verify identities, trace sources, and understand how attackers hide—and how investigators expose them.

Curriculum

SEGMENT 3.1 LINK ANALYSIS (Connecting the Invisible Dots)

What Is Link Analysis?

A method used by law enforcement and intelligence agencies to:

- Connect people Link devices
- Trace phone numbers Track
- email identities Associate
- online accounts Analyse
- financial transactions
-

Live Demonstration (Conceptual Mapping):

- One phone number → multiple WhatsApp accounts
- One email → social media profiles → payment applications
- Sm all, seemingl y harmless data points → combined to reveal a complete identity

Key Learning:

- Criminals don't make one mistake.
- They make many small ones that eventually connect.

SEGMENT 3.2. GRABIFY.LINK – UNDERSTANDING IP & LINK TRAPS (Awareness Only)

What It Teaches

How shortened links can reveal:

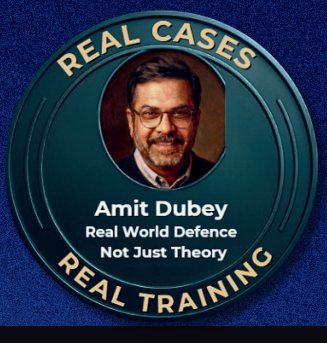
- IP address
- Device type
- Browser
- Approximate location

Ethical Awareness Only – Not for misuse

- Live Demo
- Click tracking explained
- How attackers use curiosity as bait

Defense Rule

- Never click unknown links
- Preview URLs before opening



SEGMENT 3.3. EMAIL HEADER ANALYSIS (Who Really Sent the Mail?)

What Headers Reveal

- True sending IP
- Mail server path
- Spoofed sender detection
- Country of origin

Hands-On Exercise

- Analyze a phishing email header
- Identify mismatch between:
- "From" name
- Actual sending server

Key Ins ights

- "Emails lie in the body,
- but tell the truth in headers."

SEGMENT 3.4. DEEPFAKE DETECTION (EYES,EARS& LOGIC)

What Participants Learn

- Facial artifacts
- Lip-sync mismatch
- Eye blinking anomalies
- Audio tone flatness
- Contextual logic failures

Practical Test

- Real vs deepfake comparison
- Spotting manipulation in 30 seconds

Golden Rule

- Urgency + authority + secrecy = verify twice

SEGMENT 3.5. AUTHENTICITY CHECK: MATRIMONIAL & DATING PROFILES

Platforms frequently misused:

- Jeevansathi
- Shaadi.com
- Tinder

Red Flags Covered

- Too-perfect profiles
- Overseas professions with poor verifiability
- Emotional escalation + money requests
- Reluctance for live video verification

Verification Checklist

- Reverse image search
- Social media cross-check
- Video call + real-time prompts

SEGMENT 3.6. SANCHAARSAATHI.GOV.IN – IDENTITY & SIM SAFETY

What This Portal Enables

- Check SIMs issued on your ID
- Block unauthorized connections
- Report stolen/lost phones

Live Walkthrough

- How to identify ghost SIMs
- Why SIM misuse enables banking fraud

Critical Learning

- "Most cyber frauds start with SIM compromise."

SEGMENT 3.7. RAT – REMOTE ACCESS TROJAN (How Complete Control Is Gained)

What Is a RAT? Malware that gives attackers:

- Screen view
- File access
- Mic & camera access
- Keyboard logging

Common Entry Points

- Fake APKs
  Cracked apps
- Screen-sharing tools misused

Demonstration

- Symptoms of RAT infection
- How attackers silently operate

Protection Strategy

- Install apps only from official stores
- Review permissions regularly
- Never install apps on request of callers