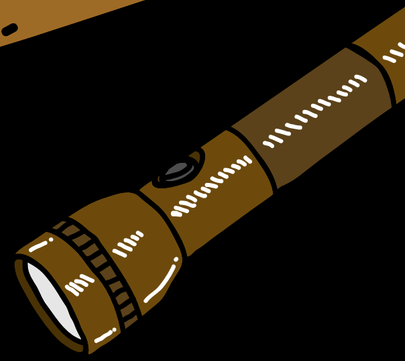
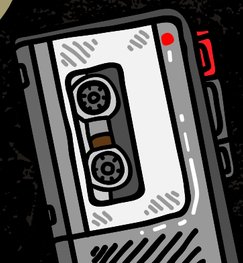
INTRO TO

CYBER CRIME INVESTIGATION (TCCI) TRAINING





LEARNING GOALS

Frequency: 3 classes per week

Total Duration: 12 weeks (Approx. 35 Sessions)

Goal: To empower learners with real-world OSINT & digital forensics investigation skills using legal and ethical methods.

PHASE 1: OSINT INVESTIGATION MASTERY

1. Introduction to Cyber Laws & OSINT
   - What is OSINT? Types & Importance
   - IPC & IT Act Sections relevant to OSINT (Sec 66, 67, 43, 72 etc.)
   - Ethics & Legal Boundaries of Investigation
   - Use cases: Law Enforcement, Pentesting, Journalism

2. OSINT Frameworks & Tools Overview
   - OSINTFramework.com, IntelTechniques overview
   - Installation and intro to tools: Recon-ng, SpiderFoot
   - Passive vs Active Information Gathering Demo

PHASE 1: OSINT INVESTIGATION MASTERY

3. Search Engine Mastery (Google Dorking)

- Google Dorking: intitle, filetype, inurl, site
- Creating Custom Search Engines (CSE)
- Hands-on Dorking Lab Practice

4. People Search (Name, Email, Phone)

- Lookup tools and many other private tools
- Email tracing
- Mobile number investigation & linking handles

PHASE 1: OSINT INVESTIGATION MASTERY

5. Username & Handle Tracing

- Tools: Sherlock, Maigret, WhatsMyName and many other private too
- Cross-platform identity mapping
- GitHub, Telegram, Reddit, Twitter profiling

6. Social Media OSINT – Facebook Focus

- UID extraction, mutual friend enumeration
- Image & profile scraping
- Legacy Graph search & manual techniques

PHASE 1: OSINT INVESTIGATION MASTERY

7. Social Media OSINT – Instagram & LinkedIn
   - Insta analysis: tags, followers, locations
   - LinkedIn scraping: mapping employees, connections

8. Image & Video OSINT
   - Reverse Image Search
   - EXIF Data extraction
   - Deepfake spotting & frame analysis

PHASE 1: OSINT INVESTIGATION MASTERY

9. Breach Data & Credential Exposure
   - Tools: HaveIBeenPwned, Dehashed, Snusbase and other private tools and databases
   - Hash types, password reuse patterns
   - Building a digital footprint from leaks
10. Domain & Website Footprinting
   - WHOIS, DNSdumpster, crt.sh
   - Subdomain discovery: Amass, Sublist3r
   - Website metadata, favicon hash, tech stack analysis
11. Dark Web & Pastebin OSINT
   - Basics of TOR, Ghostbin, Pastebin
   - Finding leaks on dark forums
   - Dark web search engines

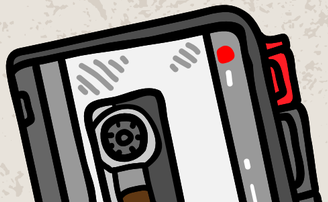
PHASE 1: OSINT INVESTIGATION MASTERY

12. Geolocation OSINT
- Image/video-based location tracking
- Tools: GeoCreepy, EXIF GPS, Google Earth
- Travel & transport tracking (flight & marine)

13. Real-Time OSINT Monitoring
- Google Alerts, GitHub Dorks
- Twitter monitoring
- Shodan alerts, RSS feeds for tracking changes

14. Building a Case File – OSINT Reporting
- Documenting findings with Maltego/Obsidian
- Visual link analysis
- Data preservation and chain of custody

PHASE 2: DIGITAL FORENSICS SPECIALIZATION



16. Introduction to Digital Forensics

- Digital Forensics Process: Identify, Preserve, Analyze, Report
- Chain of custody, evidence handling
- Tools setup: Autopsy, FTK Imager, Volatility

17. Windows Forensics – Basics

- NTFS File System, Registry Basics
- Event Logs (Security, Application, System)
- User Data: AppData, Prefetch, Recycle Bin

18. Windows Artefact Analysis

- Registry: USB history, MRU, Run keys
- Prefetch, Jump Lists, LNK, ShimCache, AmCache

19. Windows Log Analysis

- Logon/logoff events (Event IDs)
- Tools: Log Parser Studio, Event Log Explorer
- Timeline creation

20. Linux Forensics – Basics

- EXT4 File System, Directory Structure
- Important paths: /etc, /var/log, /tmp
- Bash History, Sudo logs, Cron jobs

21. Linux Forensics – Deep Analysis

- Syslog, Auth.log, Wtmp/Btmp/Utmp
- Auditd Parsing
- Deleted file recovery in Linux

22. Disk Imaging & Mounting

- MBR, GPT, Partitions
- Imaging: dd, FTK Imager, Guymager
- Hashing & mounting for analysis

23. File System Analysis

- File carving (Foremost, Scalpel)
- NTFS & EXT4 parsing
- MAC Times, metadata examination

24. Deleted & Hidden Data Recovery

- Unallocated & slack space analysis
- Identifying hidden partitions
- Tools for data recovery

25. RAM Forensics – Introduction

- Memory capture tools: DumpIt, Belkasoft, LiME
- Volatility usage
- Memory structures and formats

26. RAM Analysis Techniques

- Process Injection, DLLs, Hidden processes
- Extracting passwords and credentials
- Network artifacts in memory

27. Android Forensics – Basics

- File systems: YAFFS, EXT
- Data paths: /data/data, /sdcard
- Extraction: ADB, physical, logical

28. Android App Data Analysis

- Analyzing WhatsApp, Telegram, SMS
- SQLite DBs, browser artifacts
- Tools: Cellebrite Reader, Andriller, MobSF

29. Forensic Report Writing

- Structuring reports
- Including hash values, screenshots, notes
- Documenting timeline & findings

30. Final Forensics CTF Challenge

- Disk + RAM + Android + Windows evidence combo
- Students solve live case
- Debriefing & feedback session

🎁 Bonus Resources

- OSINT Toolkits & GitHub Repos
- PDF Handbooks & Cheat Sheets
- Practice Platforms: Trace Labs, OSINT Dojo, CTFs