Introduction to OSINT and Forensics Analysis fundamentals

Duration: 5 days (40 hours)

Day 1: Introduction to OSINT (Open Source Intelligence)

1. **Understanding OSINT**
    - Definition of OSINT and its Role in Cybersecurity
    - History and Evolution of OSINT
    - OSINT vs. SIGINT, HUMINT, and TECHINT
2. **Legal and Ethical Aspects of OSINT**
    - Privacy Laws, Data Protection, and Regulatory Compliance (GDPR, etc.)
    - Ethical Boundaries in OSINT Collection
    - Impact of Unethical Practices in OSINT
3. **Sources of OSINT**
    - Overview of Publicly Available Information (PAI)
    - Search Engines, Websites, and Public Databases
    - Social Media and Online Communities
    - Government Websites, WHOIS, DNS, and IP Addresses
4. **OSINT Tools Overview**
    - Introduction to OSINT Tools (e.g., Maltego, Shodan, TheHarvester, etc.)
    - Search Engine Dorking and Metadata Extraction
    - Tools for Collecting Data from Social Media and Websites

---

Day 2: Advanced OSINT Collection Techniques

1. **Advanced Search Techniques**
    - Using Boolean Operators for Precise Search Results
    - Google Dorking for Information Gathering
    - Web Scraping and Automated Data Collection
2. **Social Media Intelligence (SOCMINT)**
    - Analyzing Social Media Platforms (Twitter, Facebook, LinkedIn, Instagram)
    - Identifying Digital Footprints: Usernames, IPs, and Activity Patterns
    - Extracting Intelligence from Social Media Profiles and Posts

3. **Deep and Dark Web OSINT**
    - Understanding the Deep Web and Dark Web
    - Techniques for Extracting OSINT from Dark Web Sources
    - Legal Considerations and Ethical Implications
4. **Data Validation and Evaluation**
    - Verifying the Credibility and Authenticity of OSINT
    - Cross-Referencing Data from Multiple Sources
    - Spotting Fake Information and Misinformation

Day 3: Introduction to Digital Forensics

1. **Introduction to Digital Forensics**
    - What is Digital Forensics and its Role in Cyber Investigations
    - Key Stages of Digital Forensics: Identification, Preservation, Analysis, and Reporting
    - Chain of Custody and Ensuring Data Integrity
2. **Types of Digital Evidence**
    - Categories of Digital Evidence: Files, Devices, Communications, and Networks
    - Best Practices for Preserving Digital Evidence
    - Importance of Legal Standards in Forensic Analysis
3. **Digital Forensics Process**
    - Collection of Digital Evidence: Imaging, Seizing Devices, and Preserving Integrity
    - Analysis Techniques for Digital Forensics: File Carving, Timeline Creation, Metadata Analysis
    - Reporting Forensic Findings: Documentation and Chain of Custody Maintenance

---

Day 4: Forensic Data Collection and Analysis

1. **File System Forensics**
    - Understanding File Systems (NTFS, FAT, EXT, APFS) and Their Forensic Relevance
    - Analyzing File Metadata: Timestamps, Ownership, and Modifications
    - Recovering Deleted Files and Investigating Fragmented Data
2. **Network Forensics**

- Fundamentals of Network Forensics and Packet Analysis
- Analyzing Network Logs for Malicious Activity
- Investigating Network Intrusions and Compromise

3. **Communication Forensics**
   - Analyzing Emails: Header Analysis and Tracing Communication
   - Forensics of Instant Messaging and Social Media Communication
   - Investigating VoIP and Video Communications

Day 5: Integrating OSINT with Digital Forensics in Investigations

1. **Combining OSINT with Digital Forensics**
   - Using OSINT to Support Forensic Investigations
   - Leveraging OSINT for Real-Time Threat Intelligence
   - Tracking Threat Actors through OSINT and Forensics
2. **Incident Response and OSINT**
   - Role of OSINT in Incident Response and Cyber Investigations
   - Integrating OSINT into the Cyber Incident Lifecycle
   - Mitigating Cyber Threats Using OSINT and Forensics Together
3. **Forensic Reporting and Legal Aspects**
   - Writing Forensic Reports for Legal and Compliance Requirements
   - Communicating Findings to Stakeholders: What to Include and Exclude
   - Ensuring Admissibility of Digital Evidence in Court
4. **Emerging Trends in OSINT and Digital Forensics**
   - Future of OSINT: AI, Automation, and Advanced Data Analytics
   - New Challenges in Digital Forensics: Cloud Forensics, Mobile Devices, and Blockchain
   - Addressing Privacy and Encryption Challenges in OSINT and Forensics