30-Day Computer Forensic Investigator Syllabus

Week 1: Introduction and Investigation Process

- **Module 1**: Computer Forensics in Today's World (Day 1-2)
  - Overview of computer forensics, types of cybercrimes, and investigation procedures.
  - Importance of regulations and standards in computer forensics.
- **Module 2**: Computer Forensics Investigation Process (Day 3-4)
  - Phases of the computer forensics investigation process.
  - The role of a forensic investigator in cybersecurity cases.

Week 2: Understanding Disk Drives and Data Acquisition

- **Module 3**: Understanding Hard Disks and File Systems (Day 5-6)
  - Types of disk drives, booting process, and file systems in Windows, Linux, and Mac.
  - Tools for file system examination.
- **Module 4**: Data Acquisition and Duplication (Day 7-8)
  - Data acquisition fundamentals, eDiscovery, creating forensic images.
  - Preparing image files for forensics examination.

Week 3: Forensics Tools and Anti-Forensics Techniques

- **Module 5**: Defeating Anti-Forensics Techniques (Day 9-10)
  - Anti-forensics techniques and tools used by attackers.
  - Detecting and counteracting anti-forensics efforts.
- **Module 6**: Windows Forensics (Day 11-12)
  - Volatile and non-volatile data acquisition in Windows-based operating systems.
  - Memory and registry analysis, web browser forensics.

Week 4: Advanced Forensics Concepts

- **Module 7**: Malware Forensics (Day 13-14)
  - Static and dynamic malware analysis.
  - Techniques for analyzing ransomware and network behavior analysis.
- **Module 8**: Investigating Web Attacks (Day 15)
  - Web application threats and attacks.
  - Logs analysis (IIS logs, Apache web server logs), investigating web application attacks.

45-Day Computer Forensic Investigator Syllabus

Week 1-2: Foundations and Data Acquisition

- **Modules 1-4** (Covered in 30-day syllabus).

Week 3: Forensics Techniques and Anti-Forensics

- **Module 5**: Defeating Anti-Forensics Techniques (Day 9-10)
  - Same as 30-day syllabus.
- **Module 6**: Windows Forensics (Day 11-12)
  - Detailed examination of Windows-based volatile and non-volatile data, including advanced file system artifacts.

Week 4: Linux, Mac, and Network Forensics

- **Module 7**: Linux and Mac Forensics (Day 13-14)
  - Memory forensics and data acquisition in Linux and Mac operating systems.
- **Module 8**: Network Forensics (Day 15-16)
  - Introduction to network forensics, IOCs, network traffic investigation, and incident detection.

Week 5: Malware and Web Forensics

- **Module 9**: Malware Forensics (Day 17-18)
  - Malware analysis, static vs dynamic analysis, and ransomware behavior.
- **Module 10**: Investigating Web Attacks (Day 19-20)
  - Advanced web application forensics, examining logs, and detecting web vulnerabilities.

Week 6: Advanced Topics

- **Module 11**: Dark Web Forensics (Day 21)
  - Forensic techniques for Tor browser analysis, accessing and investigating dark web activities.
- **Module 12**: Cloud Forensics (Day 22-23)
  - Investigating cloud platforms (AWS, Azure, Google Cloud) and associated challenges.

Week 7-8: Mobile, IoT Forensics, and Final Project

- **Module 13**: Mobile Forensics (Day 24-25)
  - Mobile device architecture, Android & iOS forensics, SIM file system acquisition.

- **Module 14**: IoT Forensics (Day 26-27)
    - IoT vulnerabilities, security risks, and IoT forensic processes.
- **Module 15**: Final Project (Day 28-30)
    - Practical lab and final review of key topics through a simulated forensics case.

60-Day Computer Forensic Investigator Syllabus

Week 1-4: Foundations and Data Acquisition

- **Modules 1-6** (Covered in 45-day syllabus).

Week 5: Malware, Web, and Dark Web Forensics

- **Module 7**: Malware Forensics (Day 29-30)
    - Deep dive into malware analysis and network behavior.
- **Module 8**: Investigating Web Attacks (Day 31-33)
    - Advanced techniques for web attack analysis.
- **Module 9**: Dark Web Forensics (Day 34-35)
    - Investigation of dark web activities and Tor browser forensics.

Week 6: Cloud and Mobile Forensics

- **Module 10**: Cloud Forensics (Day 36-37)
    - Cloud forensics on platforms like AWS, Azure, and Google Cloud.
- **Module 11**: Mobile Forensics (Day 38-40)
    - Detailed mobile forensics, device acquisition, and data extraction methods.

Week 7: IoT Forensics and Network Investigation

- **Module 12**: IoT Forensics (Day 41-42)
    - Analyzing IoT devices, security issues, and attack surfaces.
- **Module 13**: Network Forensics (Day 43-44)
    - Advanced network forensic techniques for traffic investigation.

Week 8: Final Project and Review

- **Module 14**: Final Project (Day 45-48)
    - Complete case study covering all learned techniques.

90-Day Computer Forensic Investigator Syllabus

Week 1-5: Foundations and Advanced Acquisition

- **Modules 1-12** (Covered in 60-day syllabus).

Week 6: In-Depth Investigation Techniques

- **Module 13**: Advanced Malware Forensics (Day 49-51)
  - In-depth malware reverse engineering and static/dynamic analysis.
- **Module 14**: Investigating Web Attacks and Application Security (Day 52-53)
  - Analyzing complex web vulnerabilities.

Week 7: Dark Web and Cloud Forensics

- **Module 15**: Dark Web Forensics (Day 54-55)
  - Deep dive into dark web investigations and related challenges.
- **Module 16**: Cloud Forensics (Day 56-58)
  - Advanced cloud forensics on AWS, Google Cloud, and Azure.

Week 8-9: Mobile, IoT, and Social Media Forensics

- **Module 17**: Mobile Forensics (Day 59-61)
  - Physical and logical acquisition, iOS and Android forensics.
- **Module 18**: IoT and Social Media Forensics (Day 62-64)
  - IoT device analysis, social media investigation, and email forensics.

Week 10-12: Final Project and Review

- **Module 19**: Final Project (Day 65-75)
  - Forensic investigation of a real-life case, applying all learned tools and techniques.
- **Module 20**: Final Review and Exam (Day 76-90)
  - Review of key concepts and practical exam preparation.

180-Day Computer Forensic Investigator Syllabus

Weeks 1-12: Comprehensive Study and Data Acquisition

- **Modules 1-16** (Covered in 90-day syllabus).

Weeks 13-18: Advanced Forensics and Incident Response

- **Module 17**: Advanced Malware Forensics (Day 91-95)
  - In-depth analysis and advanced techniques for malware identification and analysis.
- **Module 18**: Investigating Web Attacks, Social Media Forensics (Day 96-100)

    - Thorough examination of web application vulnerabilities, social media account forensics.

Weeks 19-24: Advanced Forensics Practices

- **Module 19**: Dark Web Forensics and Incident Response (Day 101-110)
    - Practical application of dark web forensics and data extraction from Tor.
- **Module 20**: Cloud Forensics (Day 111-120)
    - Advanced techniques in cloud computing forensic investigations.

Weeks 25-30: Mobile and IoT Forensics

- **Module 21**: Mobile Device Forensics (Day 121-130)
    - Detailed analysis of mobile devices, recovery methods for data from Android and iOS devices.
- **Module 22**: IoT Forensics (Day 131-140)
    - Advanced IoT forensics, including data recovery and security vulnerabilities.

Weeks 31-36: Final Project and Certification Preparation

- **Module 23**: Final Project (Day 141-160)
    - A large-scale project that covers data acquisition, malware analysis, web attack investigation, and cloud forensics.
- **Module 24**: Certification Preparation and Review (Day 161-180)
    - Extensive revision, exam preparation, and mock forensic investigations.