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.