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.