Digital Forensics Essentials

Provider: EC-Council (Coursera / EdX)
Completion Date: May 14, 2025

Overview
This course covered advanced digital forensics and malware investigation across Windows, Linux, and Mac systems, emphasizing practical tools and techniques for analyzing memory, disks, malware, emails, and network traffic. Labs focused on recovering deleted or hidden data, examining system and network activity, and investigating web and dark web activity.

Key Topics

- Memory forensics using Volatility and Bulk Extractor
- Disk image and SSD analysis, anti-forensics mitigation
- Malware static and dynamic analysis (Emotet, Office documents)
- Tor Browser and dark web artifact examination
- Email crime analysis (spoofing, phishing)
- Network forensics with Wireshark and Splunk Enterprise
- Web application attack investigation (XSS, SQLi)

Practical Applications

- Created Linux kernel profiles for Volatility to examine RAM dumps
- Recovered deleted files from forensic images
- Performed malware behavior analysis in lab environments
- Extracted Tor Browser artifacts from memory
- Conducted network and web server log investigations
- Produced structured forensic documentation

Reflection
These labs enhanced my skills in investigating system compromises, identifying malicious activity, and documenting findings across multiple platforms, preparing me for real-world forensic and cybersecurity challenges.