Advanced Topics in Computer Digital Forensics

The H-11 Advanced Topics in Computer Digital Forensics is a certified 5-day course where students learn how to best manage evidence that includes MS-Windows, Linux, and Apple operating systems. Students will learn where to search a computer for needed and essential artifacts from both applications and the operation system. This includes evidence from Internet and Cloud interactions and connections.

This advanced course will include looking at data from several perspectives and tools. It includes an in-depth look at File and Operating Systems, Metadata and Application Artifacts, and Cloud Data. Students will learn what, where, when, how, and why of these technologies.

The following topics will be covered during this 5-day training course:

Computer Forensics Overview
Best Practices in Computer Forensics
Operating Systems
- MS-Windows
- Linux
- Apple
- Android

File Systems
- FAT, FAT32, and ExFat
- NTFS (different versions)
- HFS
- Ext2/Ext3/Ext4
- HPFS
- Universal Data Format (UDF)
- CDFS
- Other

Components of NTFS
- Versions of NTFS
- Master File Table (MFT)
- NTFS metafiles or system files
- Resident vs. non-resident attributes
- Alternate Data and other Stream files

User Accounts and Passwords
MS-Windows Registry
- SAM
- SYSTEM
- SECURITY
- SOFTWARE
- NTUSER.DAT (another file)

Other Registry components
Link Files
Jump Files
Shell Bag Files
Transaction Artifacts
Journal and Index Artifacts
Date and Time Artifacts
Event Log Files
Sign-in Options
User Assist Data
Prefetch and Startup Functions
Synched Data
Recycle Bin
File Deletion and Recovery
Folder Virtualization
Volume Shadow Files
Sparse Files
Windows Cortana
Defeating Encryption – BitLocker
Browsers Chrome, Edge, IE, Firefox, etc.
Browser Artifacts
Browser Vulnerabilities
Connecting files and people and places
Network and Wi-Fi connections
Internet of Things Artifacts
Timeline Analysis
Hands-on Labs
Written Exams
Final Hands-on Test
Final Written Examination