Forensic Investigator, Part 03 of 10: Hard Disks and File Systems

Meet the expert: David Bigger is the lead trainer at Bigger IT Solutions. He has been information technology for a little over 20 years and has been training all over the US. He has worked with companies like US Military, Lockheed Martin, General Dynamics, Dominos Pizza, University of Utah and Expedia

Prerequisites: Recommended:
Understanding of networking; How data flows from source and destination
Computer security basics such as passwords, encryption and physical security
Basic understanding of computing and computer systems
Experience with various operating systems

Runtime: 01:00:22

Course description: When conducting a forensic investigation, you will be looking for potential evidence that can be used in the court of law to support charges against a criminal. This evidence will be located somewhere on a device, likely on a hard disk or in the files systems. Discover the physical make-up of hard disk drives and solid state drives, and explore the logical file system where the data is actually located on the drive. Additionally, examine partitions and the booting processes for the three major operating systems: Windows, Linux, and Mac OS X. This course is part of a series covering the EC-Council Computer Hacking Forensic Investigator (CHFI).

Course outline:

Hard Disks
• Introduction
• Hard Disks and File Systems
• Hard Drive or Disk
• Hard Drive Structure
• HDD - Hard Drvie Disk
• SSD - Solid State Drive
• Physical Structure
• Clusters
• Slack Space
• Some Hard Disk Terms
• Interfaces and Connections
• RAID
• Summary

File Systems
• Introduction
• File Systems
• Partitions
• MBR vs. GPT
• File Systems
• Windows File Systems
• FAT or FAT16
• FAT32
• NTFS
• NTFS Cluster Size
• NTFS Master File Table
• Linux File Systems
• Linux File System - Ext
• Linux File System - Ext2
• Linux File System - Ext3
• Linux File System - Ext4
• Apple File Systems
• HFS
• HFS+
• Summary

Booting
• Introduction
• The Boot Process
• Windows Boot Process
• Windows Boot Process - BIOS
• Windows Boot Process - MBR
• Windows Boot Process - UEFI
• Linux Boot Process
• Mac Boot Process
• Summary