Forensic Investigator, Part 05 of 10: Operating System Forensics

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: 01:16:59

Course description: Which operating system are you best with? Do you prefer Linux over Windows, Windows over a Mac or a combination of the three? We are going to take a look at Operating System forensics so you can see in inner workings so we can find potential evidence. We will look at volatile and non-volatile data, how deal with both and techniques we can use to collect it to start off with. Once we understand data, then the operating systems will be picked apart so we, as investigators, know where to look for information. Afterwards, maybe you will change your mind from your favorite to different operating systems. This course is part of a series covering the EC-Council Computer Hacking Forensic Investigator (CHFI).

Course outline:

Windows Volatile Data
- Introduction
- Operating System Forensics
- Windows Volatile Data
- Windows Volatile Data Examples
- System Time and Open Files
- Shares and Command History
- Clipboard Contents and Logged On Users
- Mapped Drives and Process Information
- Network Information
- Demo for Network Information
- Demo: Network Information, Ipconfig
- Demo: Network Information, Netstat
- Summary

Windows Non-Volatile Data
- Introduction
- Windows Non-Volatile Data
- Event Logs
- Registry Settings
- Registry Information Available
- Registry and the USB
- Browser Information
- Chrome Browser Information
- Edge Browser Information
- Firefox Browser Information
- Thumbcaches
- Slack Space
- Hidden Partitions
- The Page File
- Summary

Linux Forensics
- Introduction
- Linux Forensics
- Linux Log Files
- Other Linux Files
- Linux Shell Commands
- Collecting Linux Network Information
- Summary

Mac Forensics
- Introduction
- Mac Forensics
- Mac Log Files
- Evidence on a Mac
- Safari
- Viewing Evidence on a Mac
- Summary