Forensic Investigator, Part 04 of 10: Data and Anti-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: 01:27:13

Course description: Dive into data acquisition to discover the differences between live and static acquisitions, as well as to learn about volatile data, or the data that should be acquired first once a system has been determined to be a crime scene. Additionally, explore the various tools and the necessary hardware and software required to carry out a successful investigation. Following an exploration of data acquisition, take a closer look at anti-forensics to understand the techniques criminals may use to make your acquisition more difficult including encryption and file deletion. Then, learn about the countermeasures that can be implemented to overcome acquisition obstacles including password crackers and undelete utilities. This course is part of a series covering the EC-Council Computer Hacking Forensic Investigator (CHFI).

Course outline:

Data Acquisition
- Introduction
- Data Acquisition
- Volatile Data
- Non-Volatile Data
- Do We Need Copies?
- Copies or Duplicates
- Chain of Custody
- Chain of Custody Form
- Forensic Tools
- Software Forensic Tools for Acquisition
- Hardware Forensic Tools for Acquisition
- Summary

Live Acquisition
- Introduction
- Live Acquisition
- Live Acquisition Common Items
- Which Volatile Data First
- Live Acquisition Steps
- Live Acquisiton Tools
- Live Acquisition Common Mistakes
- Locard's Exhchange Principle
- Summary

Static Acquisition
- Introduction
- Static Acquisition
- Write Blockers
- Destination Media
- Static Acquisition Tools
- Acquisition Methods
- Disk to Disk
- Disk to Image
- Static Acquisition Image Formats
- Format
- Sparse and Logical Acquisition
- Are the Copies Good?
- Summary

Anti-Forensics
- Introduction
- Anti-Forensics
- Why Do They Use Anti-Forensics?
- Techniques Used
- Case Study
- Tools and Techniques Used
- Summary

Techniques
- Introduction
- Techniques Used: An In-Depth Look
- Password Protection
- Password Cracking Techniques
- Deleting Files
- Encryption
- Rootkits
- Rootkit Types
- Summary

Countermeasures
- Introduction
- Countermeasures
- Challenges
- Challenges
- Summary