Forensic Investigator, Part 02 of 10: The Investigation Process

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: 01:09:11

Course description: Becoming a computer forensic investigator requires not only time and effort, but also learning the necessary steps to follow in order to ensure a sound investigation. Take a closer look at the investigation process including what should be done before the investigation, during the investigation, and after the investigation to guarantee that your investigation is thorough, isn't breaking any laws, and can be upheld should it be brought to court. This course is part of a series covering the EC-Council Computer Hacking Forensic Investigator (CHFI).

Course outline:

Before the Investigation
- Introduction
- Before the Investigation
- The Investigation Team
- The Lab Area
- Our Forensic Workstation
- Investigation Toolkit
- Summary

During the Investigation
- Introduction
- During the Investigation
- Seizing and Searching
- Collecting Evidence
- Collecting Electronic Evidence
- Collecting Physical Evidence
- Securing the Evidence
- Chain of Custody
- Evidence Bags
- The Logbook
- Storing and Transporting
- Acquiring the Data
- Bit-for-Bit Copies
- Verification of the Copy
- Analyzing the Data
- First Responders
- Summary

After the Investigation
- Introduction
- After the Investigation
- Reporting
- Being an Expert Witness
- Summary