Forensic Investigator Advanced

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: Parts 1 through 8 of Forensics Investigator.

Runtime: 03:07:06

Course description: The third installment of the Forensic investigator series

Course outline:

Cloud Review
- Introduction
- Cloud Review
- Cloud Review (Cont.)
- IaaS
- PaaS
- SaaS
- Deployment Models
- Cloud Forensics
- Summary

Cloud Threats
- Introduction
- Cloud Computing Threats
- Insecure Interfaces and APIs
- Malicious Insiders
- Policy and Procedure Differences
- Isolation Failure
- Cloud Provider Acquisition
- Subpoena and E-Discovery
- VM-Level Attacks
- Summary

Challenges
- Introduction
- Challenges to Cloud Forensics
- Challenges to Cloud Forensics (Cont.)
- More Challenges to Cloud Forensics
- Summary

Dropbox Example
- Introduction
- Dropbox Forensic Example
- Dropbox
- Dropbox Version History and Events
- Dropbox Settings
- Dropbox and Forensic Tools
- Summary

Web Application Review
- Introduction
- Web Application Review
- Web Application Layers
- Summary

Web Threats
- Introduction
- Web Application Threats
- Types of Threats
- More Types of Threats
- Summary

Investigation Steps
- Introduction
- Investigative Steps to Follow
- Beginning Investigation Steps
- More Investigation Steps
- Further Investigation Steps
- Final Investigation Steps
- Summary

Windows Investigation
- Introduction
- Windows-Based Investigation
- Logs
- Command Line Tools
- Command Line Tools to Run (Cont.)
- More Command Line Tools
- Summary

Linux Investigation
- Introduction
- Linux-Based Investigation
- Apache Logs
- Error and Access Logs
- Common Log Format
- Summary

Mobile Overview
- Introduction
- Mobile Forensics Overview
- Mobile Forensics Overview (Cont.)
- Mobile Hardware and Software
- What Investigators Should Know
- Mobile Computing Architectural Layers
- Summary

Getting Started
- Introduction
- Getting Started
- Authorization and Policies
- Where to Find Data
- Where to Find Data (Cont.)
- Introduction to the Process
- The Process
- Summary

Mobile Tools
- Introduction
- What Can We Use
- Mobile Forensic Tools
- FTK Imager
- ViaExtract and iExplorer
- MOBILedit
- Other SIM Acquisition Tools
- Logical Acquisition Tools
- Physical Acquisition Tools
- File Carvers
- Try Before You Buy
- Demo: MOBILedit Forensic Express
- Demo: Creating a Report
- Demo: Report
- Summary

Reports
- Introduction
- What Is a Forensic Report
- Reporting
- Reporting Continued
- Report Sections: Title Page and Table of Contents
- Report Sections: Summary and Objectives
- Report Sections: Evidence Analyzed and Steps Taken
- Report Sections: Relevant Findings and Timeline
- Report Sections: Conclusion, Signature, Exhibits
- Types of Reports
- Summary

Recommendations
- Introduction
- The Report
- Report Recommendations
- Report Recommendations (Cont.)
- More Report Recommendations
- Summary

Report Examples
- Introduction
- Report Examples
- Using Templates
- Demo: Report Background
- Demo: Report Types
- Demo: HTML Report
- Summary