Forensic investigator, Part 09 of 10: Cloud and Web 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: This is part 9 of the series.

Runtime: 01:42:22

Course description: The Cloud is everywhere and along with it comes unique challenges for an investigator such as Infrastructure as a service, jurisdictional issues, data locations and web applications. Who owns the data? is it in the same country? how do you find it? This course will guide you through some of these challenges, threats and pitfalls of investigating in the cloud.

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