Forensic Investigator, Part 08 of 10: Network and Email 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: 01:39:00

Course description: When is the last time you sent an email? Have you used a network lately to surf the Internet or post to your Facebook? Networks and email are an integral part of today's enterprise infrastructures, not to mention everyday life at home. Knowing where to look for evidence on a network, if it's a firewall, IPS/IDS solution, or a router is essential for an investigator. Do we check the logs first or is there another place to look? What about emails? Do we know where to find evidence there? If you know where to look, what exactly will you be looking for? Coming up we will answer all these questions and more on your way to becoming a forensic investigator. This course is part of a series covering the EC-Council Computer Hacking Forensic Investigator (CHFI).

Course outline:

Network Review
- Introduction
- Quick Networking Review
- IP Addressing
- Networking Devices
- DNS
- DHCP
- Routers
- IDS/IPS
- Firewalls
- Routing
- Summary

Network Forensics
- Introduction
- What to Look for in Network Forensics
- Log Files
- Log Usage and Legalities
- Log Collection
- Event Correlation
- Centralized Logging
- Centralized Logging Advantages
- Summary

Firewall Analysis
- Introduction
- Firewall Analysis
- Checkpoint Firewall Forensics
- Cisco Firewalls
- Summary

IDS Analysis
- Introduction
- IDS Analysis
- Juniper IDS
- Juniper IDS Logs
- Checkpoint IDS
- Summary

Router Analysis
- Introduction
- Router Analysis
- Cisco Routers
- Juniper Routers
- Summary

Live Analysis
- Introduction
- Live Analysis
- Wireshark
- Live Analysis, Continued
- Summary

Email Review
- Introduction
- Email Review
- Email Review, Protocols
- Summary

Email Crimes
- Introduction
- What Can Happen
- What Can Happen, Identity Fraud
- What Can Happen, Cyber Stalking
- What Can Happen, Child Abuse
- What Can Happen, Human Trafficking
- Tools to Use
- Summary

Email Analysis
- Introduction
- Where to Find Email Evidence
- Email Header
- Where to Find Email Evidence, Client Information
- Email Headers, Information Focus
- Where to Find Email Evidence, Files
- Email Logs
- Summary