Cyber Forensics
19.-23. November, 2018
Helsinki

COURSE OVERVIEW

One of the most common skills needed and tasks conducted in a cyber security program is digital forensics and incident response. In order to properly collect and analyze digital data in support of IT investigations requires equal parts of technical mastery, investigation prowess, legal understanding, and business understanding. This requires deep knowledge of operating systems and file systems, attacker methodologies and threat landscape, location and meaning of forensic artifacts, and legal implications of conducting various types of investigations.

This course will introduce students to the tools, techniques, and procedures employed by digital investigations teams found at various sizes and types of organizations in order to be able to properly assess the effectiveness of these teams and how they fit into the larger picture of the IT security program. This is course is extracted from a course that prepares students for the CCFP, CCE, and CHFI certifications.

ABOUT THE INSTRUCTOR

Mr. Taylor is a technical and managerial professional with over 20 years of experience in Computer Security, with 17 of those years being focused on Digital Forensics and Incident Response, who has served both commercial and U.S. Federal Government clients. Mr. Taylor is a subject matter expert on digital forensics, having supported computer, network, and mobile device forensics cases in both civil and criminal environments. Mr. Taylor is a subject matter expert on breach response, having supported and helped build multiple Security Operations Centers (SOC) and Cyber Incident Response Teams (CIRT) as both an internal employee and as an external consultant. Mr. Taylor is a sought after speaker, who has presented at numerous conferences, to include DEFCON, HTCIA, TechnoForensics, TechnoSecurity, CEIC, and many others. Mr. Taylor has taught numerous classes related to network security, computer forensics, and intrusion methodology, to include Ultimate Hacking, Ultimate Hacking Expert, Forensics and Incident Response Education (FIRE) for FoundStone (McAfee's IR professional services division); EnCase Computer Forensics I & II, EnCase Enterprise Investigations, and others for Guidance Software; and CISSP and Certified Computer Examiner (CCE) boot camps for Intense School. Mr. Taylor was a co-author of ISC2's Certified Computer Forensics Practitioner (CCFP) Official Study Guide.

Why Attend this course

Students will learn basics of various digital forensics tools, techniques, and procedures. Students will learn the skills necessary to properly collect digital evidence, how to properly handle that evidence, what artefacts to look for in that evidence, and to properly report the findings. Specific attention will be placed on various industry best practices and when different practices should and should not be applied in order to prepare students to understand and audit the effectiveness of forensics teams.

COURSE AGENDA – 5 days (40 CPEs)

1. Introduction and Background

- What is forensics?
- Why do we need/use forensics?
- When should we not use forensics?
- Senior management/Board involvement
  - How forensics fits into business plan and corporate policies
  - How forensics affects a client’s risk posture
  - Policies and Procedures
  - Periodic review of program and personnel
- Organizational Team Structure
  - Investigative team’s core members
  - C-Level staff involvement
  - ISO (Information Security Organization/Officer)
  - Public Relation involvement
  - Network and desktop administrators
  - Managed Security Service Providers
  - What to look for when selecting tools and services from vendors

2. Legal and Ethical Principles

- Justification for investigation
- Authority to investigate
- Nature of Evidence
- Rules of Procedure
  - Privacy concerns
  - Dealing with suspects (internal vs. external)
  - When to and not to share of information with outside groups
- Role of Expert Witness
- Codes of Ethics

3. Investigations

- Investigative Process
- Evidence Management
  - Securing the scene
  - Proper collection
  - Handling procedures
  - Chain of custody
  - Controlling access to evidence
- Criminal Investigations
  - Working with Asst. US Attorney, Justice, FBI, USSS, etc.
- Civil Investigations
  - closed-bank, class-action, etc.
  - Intellectual Property
- Administrative Investigations
- Response to Security Incidents
- e-Discovery

4. Forensic Science

- Fundamental Principles
• Inman-Rudin Paradigm
a. Identification
b. Classification
c. Association
d. Reconstruction
- Case Planning
- Forensic Methods
• Identification of Digital Evidence
• Collection and Preservation of Digital Evidence
• Examination and Analysis of Digital Evidence
• Reporting and Presentation of Digital Evidence
- QA, Control, Management

5. Digital Forensics

- Media and File System Forensics
• Single-drive analysis
• Multi-drive analysis
• Live analysis
• Deleted file recovery
• Stochastic forensics
• Steganography
• Volatility of data
- Operating Systems Forensics
• Analysis of the operational patch management program
• Examination of operational configuration management practices
• Operational vs published policy compliance practices
• Logs
• Autorun Services
• Whitelisting and Blacklisting
- Network Forensics
• Analysis of network logs and compliance to institution policy
• SEIM and Centralized logging
• Central Time Stamping
• Internet keyword searches
- Mobile Devices
• iOS
• Android
• Windows Mobile
• Other
- Multimedia and Content
• Audio Forensics
• Video Forensics
• Digital Image Forensics
- Virtual System Forensics
• Physical vs. virtual?
- Forensic Techniques and Tools
• Investigative Tools

  - Analysis Tools
  - Case Management Tools
  - Note taking (electronic and paper)
  - Expendable Items (drives, flash media, labels, etc)
  - Go Bag
- Anti-Forensic Technology and Tools

6. Application Forensics

- Software Forensics
  - Code review
- Web, Email, and Messaging
  - Email client data
  - Email server data
  - Webmail
  - Cloud email providers
  - Chat clients
  - Social media
- Database Forensics
  - Data contents
  - Log analysis
- Malware Forensics
  - Behavioral analysis
  - Static analysis
  - Sandboxes

7. Hybrid and Emerging Technologies

- Cloud Forensics
- BYOD
- Social Networks
- Big Data Paradigm
- Control Systems
- Critical Infrastructure
- Virtual/Augmented Reality