Digital Forensic Investigation Professional (DFIP)

Program Coverage

Part I - Introduction to Digital Forensics

1.1 Traditional & Non-traditional Forensics
1.2 Virtualization
1.3 History of Forensics
1.4 Legal Considerations
1.5 Computer Forensics

Part II - Computer Network Forensics

2.1 Network forensics
2.2 Database forensics
2.3 Network Infrastructure
2.4 Data link layer
2.5 Network Layer

- 2.5.1 IP Addressing
- 2.5.2 Examples of IP address calculation
- 2.5.3 Examples of Classes of IP Addresses
- 2.5.4 Subnet Mask - The Network address identifier
- 2.5.5 Private IP addresses
- 2.5.6 Time to live (TTL)

2.6 Routing

- 2.6.1 Static Routing
- 2.6.2 Dynamic Routing

2.7 Introduction to Subnetting

- 2.7.1 Subnetting Basics
- 2.7.2 Classless Inter-Domain Routing (CIDR)

2.8 Transport layer

- 2.8.1 Connection oriented protocol

2.9 Switching

- 2.9.1 Layer 2 Switching Methods
- 2.9.2 Store-and-Forward Switching
- 2.9.3 Cut-Through Switching
- 2.9.4 Carrier Sense Multiple Access / Collision Detection (CSMA/CD)

2.10 Layer 3 Switching

- 2.10.1 Spanning Tree protocol (STP)
- 2.10.2 Vlan Trunking Protocol (VTP)
- 2.10.3 VTP Modes of operation

Part III - Hand Held Devices Forensic

3.1 Mobile Device Forensics
3.2 Mobile operating Systems
3.3 Hand Held / Mobile Devices
3.4 Data Acquisition on Mobile devices
3.5 Evidence preservation for handheld devices

Part IV - File Structure on storage media

4.1 What is file system?

- 4.1.1 Windows file systems
- 4.1.2 FAT32

4.2 NTFS File System

- 4.2.1 Clusters and Sectors on an NTFS Volume
- 4.2.2 Sequence of Clusters on an NTFS Volume
- 4.2.3 Limitations of Cluster Sizes on an NTFS Volume
- 4.2.4 Increasing security
- 4.2.5 Supporting large volumes
- 4.2.6 Limited space on a volume

4.3 Resilient File System (ReFS)
4.4 Slack space
4.5 Mac OS file systems
4.6 Linux file systems

Part V - Protocol Filtering & Analysis

5.1 Protocol Analysis & Filters

- 5.1.1 Capture Filters
- 5.1.2 Display Filters
- 5.1.3 Filtering Parameters

5.2 Promiscuous Mode Capture
5.3 Protocol Analysis
5.4 Sequence and Acknowledgment Numbers
5.5 TCP flags
5.6 Port numbers
5.7 Dissectors
5.8 Importing files from other capture programs
5.9 Interpreting the captured data
5.10 Display time formats
5.11 Follow TCP streaming
5.12 Packet Colorization

Part VI - Data Carving

6.1 Header / Footer Carving
6.2 File Structure based Carving
6.3 Block Based Carving
6.4 Fragment Recovery Carving
6.5 Volatile Data carving
6.6 The limitations of data carving
6.7 Extracting the data from the media
6.8 Extracting hidden / deleted data
6.9 Digital Image Processing
6.10 Steganography
6.11 Hiding files

- 6.11.1 Hide Files using the Steganography Technique
- 6.11.2 The Secure Hiding of Files and Folders

Part VII - Crypto systems

7.1 What is Cryptography

- 7.1.1 Symmetric and Asymmetric crypto systems

7.2 Symmetric Cryptography

- 7.2.1 Strengths
- 7.2.2 Weaknesses

7.3 Asymmetric Cryptography

7.4 Types of Encryption

- 7.4.1 Symmetric methods
- 7.4.2 Asymmetric methods

7.5 Hashing
7.6 Brute force attack
7.7 Features of Secured Communication

Part VIII - Hacking, Attacks and Vulnerabilities

8.1 Type of computer crimes

- 8.1.1 Hacking
- 8.1.2 Phishing
- 8.1.3 Computer Viruses
- 8.1.4 Identity Theft
- 8.1.5 Digital Theft

8.2 ARP Poisoning

- 8.2.1 ARP Spoofing Attack
- 8.2.2 ARP Poisoning Attack

Part IX - Evidence Collection, Preservation, Analysis & Reporting

9.1 Guidelines for processing the evidence
9.2 Phases of Forensic Process
9.3 Identifying Sources of Data for Suspect Evidence

- 9.3.1 Admissibility
- 9.3.2 Authenticity
- 9.3.3 Incident Types

9.4 Planning Acquisition

- 9.4.1 Preparations for acquiring data
- 9.4.2 Safety of the Investigator

9.5 Evidence Collection

- 9.5.1 Evidence Preservation
- 9.5.2 Evidence Analysis
- 9.5.3 Bit Stream Image of the evidence
- 9.5.4 Evidence Handling

9.6 Reporting

- 9.6.1 Features of a good Report
- 9.6.2 Structure of A Digital Forensic Report

Part X - Forensic Analysis Tools

10.1 Forensic Tool Kit (FTK)
10.2 Encase
10.3 CAINE
10.4 Sans Investigative Forensics Toolkit - SIFT
10.5 Registry Recon
10.6 Facebook Forensic Toolkit
10.7 Forensic Explorer
10.8 COFEE
10.9 The Sleuth Kit
10.10 Open Computer Forensic Architecture
10.11 X-Ways Forensics

Part XI - The forensic process

11.1 Steps in the Forensic Examination Process
11.2 Chain of Custody
11.3 Forensic personnel
11.4 Cost
11.5 Response time
11.6 Data Sensitivity
11.7 Policies
11.8 Covering the trace
11.9 Social Media Forensic
11.10 Evidence from Destroyed Skype Logs
11.11 Issues in computer forensics
11.12 Technical issues - Encrypted Encoded Data
11.13 Legal issues
11.14 Administrative issues

Appendix

I Request For Comments (RFC)
II SIM Card Architecture
III Limitations in Mobile Device Forensics
IV Data Destruction Industry Standards
V Subnetting Class A, B and C networks
VI Challenges in present day Digital Forensics