SMFC-SalvationDATA Mobile Forensics Investigator Certification Training Course

Course Description

You will gain an advanced appreciation for the types of evidential data and actionable intelligence that can be recovered from a mobile device. You will understand how the data is recovered and when & where to find evidentiary data.

This course aims to teach any forensic investigators and will ensure you have gained the best knowledge with the ability to perform forensic investigation on mobile devices to investigate and solve problems.

By the end of this course, you will be able to use alternative methods to extract mobile device data and understand how and where data is stored on mobile devices.

Duration: 2 days
Location: China

What's Included

- **A Training license for SPF**
- **Mobile devices to practice on**
- **The learning environment consists of lectures, real world examples, and hands-on exercises.**
- **A comfortable training Room**

Course requirements

1. **Basic computer skills**
2. **A laptop capable of running our software**

Learning Objectives

- To learn how to use alternative methods to extract mobile device data
- To know how and where data is stored on mobile devices
- To learn how to get that data recovered
- How to make quicker, faster, more efficient decisions with the aid of visualizing mobile forensic data
- Improve your skills to meet the requirements of a mobile forensic examiner

Logical Extraction

1. Course Introduction
2. Intro to SIM Cards & Mobile Devices
3. SIM cloning & Non-smart phone extraction
4. Common Challenges with Mobile Devices

5. Android and IOS Basics
6. Windows Phone Basics
7. Triage Setup
8. Filters, Quick Views, & Tagging in Spotlight
9. Memory Cards& Memory Chip Knowledge
10. Logical File System Extractions
11. Data Hashing
12. GPS Location Data
13. Basic App Analysis
14. Page Headers, Freeblocks & Freelists
15. SQLite Data Types
16. Building & Modifying SQLite Databases
17. How to Exporting and Importing Backups

Hands-on section

1. Removing Passwords on Android Devices.
2. Backup extraction
3. ADB directives use
4. Rooting Androids
5. iPhone trust file password bypass
6. APP chats database records view
7. Restoring Original Device Firmware
8. Custom Recovery Images
9. Reporting.
10. Work with real cases (Provided by us)

Physical Extraction

1. Identify mobile device hardware
2. Learn how devices communicate
3. Understand where mobile device information can be stored
4. Forensic analysis of SIM cards

5. Data encoding on smartphones
6. Identification of SQLite database structures
7. How to recovering deleted information in SQLite databases
8. MTK, Qualcomm 9008 Imaging
9. Android forensics common challenges
10. Cracking locked and encrypted Android devices
11. Interpreting file systems on Android devices

Hands-on section

1. Understand how data is stored within SQLite databases
2. Understand what happens when data is deleted from an SQLite database
3. File Systems mounted on an Android device
4. Wireless networks to which an Android device connects
5. Partitioning schemas used by Android devices
6. How to find iOS backup files
7. Handling Encrypted iOS Backup and Extractions
8. Processing an iOS Backup
9. SMS messages analysis
10. Safely remove eMMC and proprietary flash memory chips from printed circuit boards
11. Successfully clean and “re-ball” flash memory chips in preparation for data recovery
12. Work with real cases. (Provided by us)

Advanced Acquisition

1. XACT Re-familiarization
2. Hex Refresh
3. Older Advanced Data Extraction Methods
4. Introduction to JTAG
5. Introduction to Necessary for JTAG Extractions
6. Determining if JTAG is an available option
7. JTAG Finder / Process / Probing –TAP Identification
8. Health and Safety
9. Intro to eMMC
10. Learn about eMMC/eMCP and UFS memory types
11. Chip-off Introduction
12. Discuss advantages and disadvantages of chip-off.
13. Summarize critical need-to-know elements of chip-off
14. Data interpretation
15. Partitions and File Systems
16. Encryption Schemes
17. Decrypting Android Storage

Hands-on section

1. Chip-off Practical I – Thumb Drives
2. Chip-off Practical 2 – Androids
3. Demonstrate Android device operating system version identification.
4. Explore software installation procedures needed to complete the chip-off course and lab usage
5. To practice on different types of mobile device memory
6. To know when to use the milling subtraction chip-off process
7. Compare and contrast the benefits and risks of milling chip-off procedures
8. Describe the equipment and setup required to safely conduct milling
9. Demonstrate the steps required to successfully complete the milling process on a chip
10. Work with real cases. (Provided by us)
11. Written and Practical examination

What you will get

This is a valuable Mobile forensics certification that certifies participants who have gained the knowledge and practical skills required to handle any cases need to investigate mobile devices.

By the end of this course you will be able to use alternative methods to extract mobile device data and understand how and where data is stored on mobile devices and how to get that data recovered. You will be also familiar with find the wealth of hidden information in smartphone apps and their databases and best ability to work with chip-off and JATG process.

A certificate(SMFC) will be granted to the trainee after the trainee passed the training examination.

Customization

In order to meet different customer needs and help learners best achieve their learning goals, we provide opportunities for our clients to customize the course attributes, including time, place, close-door requirements, etc.