Course Introduction

Smartphone technologies are constantly changing, and most forensic professionals are unfamiliar with the data formats for each technology. Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, and more. Understanding how to leverage the data from the device in a correct manner can solve the forensic case. Smartphone forensics is infancy. Examining and interpreting the data from a various platforms play a crucial role. This course will provide examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. To enhance the capability to find and extract the correct evidence from smartphones with confidence, the learners will gain hands-on experience with the different data formats on multiple platforms and learn how the data is stored and encoded on each type of mobile device.

Course Objectives

- To do forensic analysis on smartphone data by using appropriate forensic tools
- To understand how smartphone file systems store data, how they differ, and how the evidence will be stored on each device
- To interpret file systems on smartphones and locate information that is not generally accessible to users
- To associate a user to a smartphone at a specific date/time and at various locations
- To decrypt or decode application data that are not parsed by forensic tools
- To understand how data is stored on smartphone components (SD cards) and how encrypted data can be examined by leveraging the smartphone
- To analyze SQLite databases and raw data dumps from smartphones to recover deleted information

Learning Level

- Intermediate

Course Duration

- 5 Days

For More Information & Registration, Please Contact Training Division
Tel:(66) 2253-4736, Fax:(66) 2253-4737, Hotline:(66) 86-325-7129, E-mail: registration@acisonline.net

Target Group

- Information Security Officer
- Network administrator
- System administrator
- Law enforcement

Course Outline

Day 1

- Malware and Spyware Forensics
- Introduction to Smartphones
- Smartphone Handling
- Forensic Acquisition
- Smartphone Forensic Tools
- JTAG Forensics
- Smartphone Components

Day 2

- Android Forensics Overview
- Handling Locked Android Devices
- Android File System Structures
- Android Evidentiary Locations
- Traces of User Activity on Android Devices
- Salvaging Deleted SQLite Records

Day 3

- iOS Forensic Overview and Acquisition
- iOS File System Structures
- iOS Evidentiary Locations
- Handling Locked iOS Devices
- Traces of User Activity on iOS Devices

For More Information & Registration, Please Contact Training Division
Tel:(66) 2253-4736, Fax:(66) 2253-4737, Hotline:(66) 86-325-7129, E-mail: registration@acisonline.net

– Salvaging Deleted SQLite Records

Day 4

– Backup File Forensics Overview
– Common File Formats For Smartphone Backups
– Creating and Parsing Backup Files
– Evidentiary Locations on Backup Files
– Locked Backup Files
– Windows Forensic Overview
– Windows File System, Evidentiary Locations and Forensic Analysis

Day 5

– Third-Party Applications on Smartphones Overview
– Third-Party Application Locations on Smartphones
– Decoding Third-Party Application Data on Smartphones
– Knock-off Phone Forensics

Official Training Partner

For More Information & Registration, Please Contact Training Division
Tel:(66) 2253-4736, Fax:(66) 2253-4737, Hotline:(66) 86-325-7129, E-mail: registration@acisonline.net