Advanced Smartphone and IoT Device Forensics

The H-11 Advanced Smartphone and IoT Device Forensics is a certified 5-day course where students learn how to access, find, and then recover evidence found on smartphone, smart devices, and Internet of Things (IoT) devices. Students will learn ways of extracting data from a variety of smartphone devices.

Students will learn advanced methods of defeating data protection schemes, including data from embedded systems that are locked, damaged or unsupported. This recovery method works on newer devices that store data on eMMC or eMCP flash memory chips and recovered through the device's test points.

Students will also learn how to use EDL to bypass device locks and encryption and identify JTAG connections, read data from "live" Internet of Things (IoT) devices and more. These techniques and methods are used in order to bypass security and perform full memory acquisitions for complete analysis of evidence. This course will use, and cover smart device tools included in the ***H-11 ISP-IoT-EDL-JTAG Forensics Lab Kit***.

The following topics will be covered during this 5-day training course:

Mobile and Smartphone Forensics Overview
Smartphone Applications and Artifacts
- Network connections and artifacts
- IP, Server, and Gateway addresses,
- Wi-Fi Networks
- Cell towers and provider networks
- Bluetooth connections and issues
- Other "trace" evidence left by connections

Coding of data
- Hexadecimal
- Binary vs. Base64
- ASCII vs. Unicode
- UTF-8 and other code pages
- Big Indian vs. Little Indian
- Encoding metadata
- Date/Time Formats
- Date/Time Stamps

Types of Extractions
- File System
- Logical
- Physical
- Backup
- Cloud
- Screen Capture

Procedures for Smartphone Extractions
Understanding the Apple iOS
Understanding Apple iTunes
Understanding the Android OS
Smartphone Extraction Lab
Smart Device Extraction Lab
Smartphone Triage Tools
Using OCR in smartphone tools
Using Facial Recognition in smartphone tools
Cloud Data Introduction
Other methods to extracting smartphone data
Understanding NAND, NOR, and Flash Memory
Purpose of Online Research
Websites for ISP, IoT, EDL, and JTAG
Ways to obtain internal images of a device
Open-source tools
HEX Editors
7Zip and Other Tools
JTAG Origin and Purpose
JTAG Demonstration
In-System Programming (ISP) Overview
Devices to use and perform ISP examinations
Tools used for direct eMMC and eMCP reading
ISP Demonstration
Hands-on Labs
Written Exams
Final Hands-on Test
Final Written Examination

Join our Mobile Forensic User Group: https://groups.google.com/forum/#!forum/mobile-device-forensics-and-analysis