H-11 DIGITAL FORENSICS

Advanced Mobile Forensic Analysis with Python

The H-11 Python for Advanced Mobile-Forensics Analysis Course will take a mobile-forensics practitioner beyond simply pointing and clicking. This course will provide students the ability to search out and decode data that hasn't been found, was missed, and not analyzed by automated mobile-forensic tools. Students will use Python both in and outside the mobile-forensic tool to quickly take raw data and make it presentable and reportable.

Students will use a variety of proprietary and open-source tools, including database-analysis tools, raw-data conversion utilities, Python libraries and other tools to learn skills and techniques for finding low-level evidence data found on smart phones/devices.

Course Outline:

Day 1

Module 1: Intro and Review

- Introduction – Welcome Overview
- The Forensic Process
- Review of Mobile-Device Forensics

Module 2: Low-Level Data Recovery and Decoding

- Raw Storage Formats Used in Mobile Phones
  - Binary
  - Hexadecimal
  - Little vs. Big-Endian
  - Reverse Nibble
  - 7-bit
  - Base64
  - Hashing
  - Timestamp Formats
- Manual Decoding of Raw Phone Data
- Recovery of Phone Data with 3rd Party Tools
- Identify and Recovery of Unsupported App Data
- Decoding Raw Storage Formats using Python
- Creating a function library for decoding

Day 2

Module 3: Intro to Python and Working with Data

- Python Background and Environment Setup
- The Python Shell
- References and Basic Commands
- Getting Python to do what you want it to
- Modifying existing code
- Finding Python short-cuts and technique tricks
- Automating Repetitive Tasks
- Practical Exercises

Day 3

Module 4: Python inside the Mobile-Forensic Tool

- Why do we need it? And what can it do for us?
- Specific Application-Programming Interfaces (APIs)
- Recovering Non-Decoded Application Information
- Practical Exercises

Day 4

Module 5: Adding Device Information

- Searching for and recovering Mobile-Phone Identifying Information
- IMSI – IMEI – ICCID Phone Numbers
- Unique Device IDs and Android IDs Advertising Identifiers
- Practical Exercises

Module 6: Phonebook, Call Lists, and SMS Messages

- Recovering Simple Information from Basic Phones
- API lookups for Wi-Fi and cellular location data
- Practical Exercises

Day 5

Module 7: SQLite and other Databases

- Manual Analysis
- Microsoft Excel / Spreadsheet use to analyze
- 3rd Party Tools
- Command-Line Analysis
- Custom-Built Tools
- Automated Analysis within a Mobile-Forensics Tool
- Decoding unsupported applications
- Exporting data from Mobile-Forensic Tool Using CSV, TSV, and other formats

Module 8: Final Practical and Group Collaboration

- Group Exercise to create a complex program for decoding and recovering data
- Apply PyQT to build custom tool for use in forensic cases finding/carving evidence
- Creating and Maintaining a Script Database
- Create a Custom Graphical Tool for Decoding Data from Forensics Images

Final Hands-On and Written Exams

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