Python for Advanced Mobile-Forensics Analysis

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 and other smart devices.

Course Topics and Learning Points:

- Raw Storage Formats used in Mobile Phones
- Decoding of Raw Phone Data
- Intro to Python
    - The Python Shell
    - Basic Commands
    - Modifying Existing Code
- Python inside the Mobile-Forensics Tool
    - Application-Programming Interfaces (APIs)
- SQLite Databases
    - Manual Analysis
        - Command-Line Analysis
    - Automated Analysis
        - Within a Mobile-Forensics Tool
- Plugins and Chains in Mobile-Forensics Tools

Cost:

H-11 Python for Advanced Mobile-Forensics Analysis $3,795

* Call and ask about available scholarships, early registration discounts and custom equipment packages

Required Equipment:

Laptop – Windows 7 or Windows 10

Contact H-11 Digital Forensics today

Phone: +1.801.596.2727 Email: training@h11dfs.com Web: www.h11dfs.com

H-11 DIGITAL FORENSICS

Python for Advanced Mobile-Forensics Analysis

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 and other smart 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 Using Excel and Other 3rd Party Tools

Day 2

Module 3: Intro to Python

- Background
- Environment Setup
- The Python Shell
- References
- Basic Commands
- Getting Python to do what you want it to
- Modifying Existing Code
- Finding Techniques to do what you want with Python
- Practical Exercises

Day 3

Module 4: Python inside the Mobile-Forensic Tool

- Why do we need it?
- What can it do for us?
- Specific Application-Programming Interfaces (APIs) we can use
- First Program that Recovers Previously-Uudecoded Information
- Practical Exercises

Day 4

Module 5: Adding Device Information

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

Module 6: Phonebook, Call Lists, and BREW Phones

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

Day 5

Databases and Final Practicals

Module 7: SQLite Databases

- Manual Analysis
  - 3rd Party Tools
  - Command-Line Analysis
- Automated Analysis
  - Within a Mobile=Forensics Tool

Module 8: Plugins and Chains in Mobile Forensics

Module 9: PDU-Formatted SMS in GSM Phones

Module 10: Final Practical and Group Collaboration

Group Exercise to create a complex program for decoding data