Advanced Wireless Analysis for Mobile Devices

The purpose of this course is to give forensic analysts in-depth knowledge and techniques on how smart devices connect and communicate on wireless networks and help them use that information to further their investigations. Students will learn skills to identify: geolocating and mapping historical device locations, enumerating the ways in which the device communicates on the networks, find additional devices and networks that the device has communicated with, enrich the phone's data with open-source intelligence (OSINT), use advanced Python scripts to export evidence data, and create meaningful reports to convey information to investigators.

Course Outline:

Day 1

- Welcome and Introductions
- Context and Background of the course (introduction to the purpose behind the course, i.e., tracking, DFIR, pentesting, site security)
- Discuss tools and computer setup for examination
    - BlackLight, Oxygen Forensics, AXIOM, Physical Analyzer, and Python
    - Date/time setup
    - Case Data
    - Evidence
    - Investigations Folders
- Review of the forensic tools, how to export data, how to report information, how to analyze
- First look at smart phone and computer databases
    - Performing sqlite queries to pull the information
    - Exporting the data to a usable format
    - Create Report

Day 2

- Review of previous day and written quiz.
- Review of smart phone app types, what type of data they have and how can it be useful, with specific focus on what apps hold what information, such as timelines, searches, geolocation data, etc.
- Practical exercise in reporting timeline and geo data to a useful format, Instructor Led.
- Background of wireless in general and Cell/GSM/CDMA/LTE/WiFi/Bluetooth in particular.
- Peculiarities of wireless signals, transmission power, antenna types, range, etc.
- MAC Addressing, vendors, trends, random MACs, BSSIDs, patterns of MAC addresses in WiFi and Bluetooth

Day 3

- Review of previous day and written quiz.
- Connection behaviors – scanning, probe requests, handshaking, disconnection, broadcast vs. non-broadcasting, etc. (basically, things to look for and what they mean) Correlation of wireless items with real-world things, small intro to online searching.
- Types of WiFi devices and their implications and behaviors (APs, clients, game systems, smart watches, laptops, phones, tablets, iOT devices, etc.) How do they act, where will you see them and what it all means. How our suspect's device may interact with those devices and what types of traces this leaves.
- How we can use those devices to geolocate other devices, build a profile of our suspect, and use that information to further an investigation.
- Practical exercise in building a comprehensive timeline in Google Earth of device activity, locations, etc., around the time of the commission of a crime.
- WiFi and BT collection/scanning tools and what they are good for: Kismet, Wigle, Acrylic, Cain, blue_hydra, RamBLE

Advanced Wireless Analysis for Mobile Devices

Day 4

- Review of previous day and written quiz
- Geolocation and geocoding basics.
- Geolocation from digital forensic tools, such as Cellebrite, Axiom, and Oxygen. Limitations and strengths. How to augment the information they already have with more data and analysis. (Some prepared Python scripts will be used here to find evidence)
- Web sites that can be used, tools for plotting and tracking
    - OpenCellid.org
    - Wigle.net
    - Mozilla MLS
    - Other sites to find historical locations of devices
- Open-Source Intel (OSINT) Augmentation of forensic data
    - Theory of enriching forensic data with openly-available information on the net
    - Demonstration
- Practical exercise in finding, correlating, plotting, and reporting on different types of data using web and other open-source tools
- Building a profile of a suspect based on the data found on the device and augmentation with OSINT techniques

Day 5

- Review of previous four days and written quiz.
- Reporting: Pulling it all together, review of integrating device activity, wireless activity, positional data, OSINT sources, and all other previously-shown technique to produce a coherent report
- (FINAL TEST AND PRACTICAL SHOULD TAKE 3+ HOURS)
    - Final Written Test: combination knowledge-based and Internet-search based practical test
    - Final Practical: given a phone dump and a defined objective, time of crime, etc., and produce:
    - Comprehensive profile of the suspect, personal info, where they live, etc.
    - Analysis of background patterns and behaviors, such as locations and activities (historical)
    - Complete yet concise timeline of relevant suspect activities around the time of the crime
    - Maps and details of WHERE, WHAT, and WHEN the suspect did things
    - Readable report
- Setting up their own accounts
- Hands-on Case Final Exam

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