

Using Python and SQLite to Further Your Mobile Device Forensic Investigations

They say there is no one tool that can do everything during a forensic examination. The solution - *Create Your Own Tools!*

Learn to create your own Mobile Device Forensic tools with Python and SQLite!

Despite the best efforts of existing mobile forensics solutions, they're unable to support every mobile device (thousands) and every app (over a million). Eventually (if it hasn't happened already), the data critical to your examination will be passed over by your existing tools. Don't let it happen! If you're lucky, you've found the data...but now what? Manually parsing out hundreds or thousands of SMS can be a very time consuming challenge.

This course is broken into three major parts:

Analysis of Data Structures

After a brief recap of numbering systems (binary, decimal, and hexadecimal), data types/sizes, and endian, we cover numbers, strings, fixed and variable length records, common file storage formats, and manual analysis of data. A handful of analysis tools (all included with tuition) are covered to demonstrate how they can help in your analysis of data structures.

Introduction to Programming with Python

This part of the course covers the basics of setting up and programming with Python version 3. The focus of this part is to familiarize you with the core features of Python 3.

Python Programming for Mobile Forensics

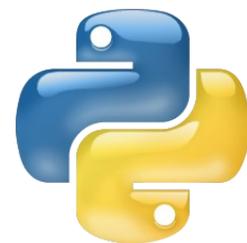
After learning the basics of Python 3, we will use what was learned during Analysis of Data Structures to create a Python script that will analyze your data and create custom output or a report detailing this information. Additionally, while not a core part of this course, sample Cellebrite Python scripts will be briefly covered for students wanting to use Cellebrite's existing reporting features.

This course is very "hands on" and includes numerous practical exercises. While this course will focus on data obtained from mobile devices, the skills learned will be very similar for working with any type of data (e.g., computer instant messenger logs, etc.).

Course Requirements

Students will need to bring a computer capable of running Windows XP or higher. This course will require a significant amount of typing, and students should be comfortable typing at an average speed. While no programming experience is required, this is an intermediate to advanced course. If you have any questions, please contact Teel Technologies.

```
sevenDecode.py
1 def sevenDecode(encodedbytes):
2     """
3     Convert bytes from a 7-bit string to a standard string.
4     """
5
6     offset = 0
7     length = len(encodedbytes)
8     mask = 0
9     decoded = bytearray()
```



Learn how programming for Forensics Can Help Recover Data From Today's Popular Apps...



Coming to...



PINELLAS COUNTY SHERIFF'S OFFICE

July 13th to 17th, 2015



Location:
Pinellas County
Sherriff's Office
10750 Ulmerton Rd.
Largo, Florida 33778

Local Contact:
Korey Diener
kdiener@pcsonet.com

Sign-up Today at:
www.teeltechtraining.com