COMP6445 Digital Forensics

Week 9 Activity Instruction

Objective

The objective of this week's tutorial/lab is to:

- Familiarise students with the Cellebrite UFED tool commonly used by Police and Defence forces to perform mobile phone extractions and to analyse the results;
- Use other tools, more suited to civil matters, and compare the results.

Preparation

For this activity, student should self-organise into groups of 4-6. Each group should have one mobile phone used as the "evidence phone" and it should be:

- An Apple iPhone (4 up to X);
- A Samsung Galaxy (S4 up to S9).

The students offering the evidence phones should understand that:

1. The process will extract all data on the phone and potential recover data that has been previously deleted; and
2. There is a possibility that data may be deleted or damaged. The phone should be backed up prior to being offered for extraction.

Materials

Each group should have:

1. An evidence phone;
2. The passcode for the evidence phone (only one person needs this);
3. Standard data cable for the evidence phone;
4. Cellebrite UFED 4PC or UFED T2 tools;
5. For iPhones:
    a. iTunes;
    b. Reincubate iPhone Backup extractor (on the course Win10 VM);
6. For Samsung:
    a. Kingoroot (on the course Win10 VM);
    b. Andriller (on the course Win10 VM);
7. An Sqlite database browser (these are on both the course Win10 VM and Kali Linux)
8. Graphviz;
9. A USB key with storage at least 1½ x that of the evidence phone.

Activity Instruction

The activity is in three parts:

1. Using Cellebrite;
2. Using other tools;
3. Analysis of the artefacts obtained from Parts 1 & 2.

Part 1 – Cellebrite

1. Use Celebrite to perform a Logical extract of the evidence phone. Save the extraction onto a USB key. Use the standard data cable for your phone i.e. don't use the Cellebrite cable;
2. Use Cellebrite Logical Analyser to create a default report of the extraction. Groups using the T2 for extraction will need to swap to UFED 4PC. Save the report onto the USB key;
3. Review the report;
4. Complete the other part of the Activity before coming back and exploring other functions of Cellebrite e.g. Advanced or Physical extractions.

NOTE: a sample extraction has been provided in case you don't complete this part of the activity. It is ~600Mb zipped, so please ask your tutors if you need this.

Part 2 – iPhone Backup Extractor and Andriller

iPhone Backup Extractor

For those groups with iPhone:

1. Use iTunes to make a backup of the evidence phone, making sure not to password protect the backup. Take note of where the backup is being saved (it may be simpler to change the default location);
2. Use iPhone Backup Extrator to view the iPhone backup. You will need to add the backup location to get started;
3. Save artefacts for call history and SMS as CSV files;
4. Extract the call history and SMS databases:
   a. Use Expert Mode → Library → CallHistoryDB and extract Callhistory.storedata
   b. Use Expert Mode → Library → SMS and extract SMS.db
5. Explore other artefacts as time permits.

NOTE: iPhone Backup Extractor has a sample pre-loaded (i.e. John Appleseed). You may use this is needed.

Andriller

For those groups with Samsung:

1. Turn ON Developer Options on the Samsung phone (see https://www.samsung.com/uk/support/mobile-devices/how-do-i-turn-on-the-developer-options-menu-on-my-samsung-galaxy-device/);
2. Turn ON USB Debug mode;
3. Check if the device is rooted. There are several ways, one is to run a terminal, check if the login prompt has changed from "$" (not rooted) to "#" (rooted) and run SU;
4. If needed, use Kingoroot to root the device;
5. Use Andriller to perform the extraction using the Extraction (USB) tab and don't check Use AB method;
6. Save the default report that already includes call history and SMS.

7. Extract and save the call history and SMS databases;
8. Explore other artefacts as time permits.

NOTE: if you are unable to complete the activity based on Samsung, go to the iPhone activity and use the John Appleseed sample.

Part 3 – Analysis

1. Use an Sqlite database browser to explore the call history and SMS databases. Are you able to recover deleted snippets that were not already recovered by the tools? Whether or not you can will depend on the evidence phone.
2. Use Graphviz to construct appropriate visualisations of the call history and the SMS.

Assessment

All team members will receive the same mark (up to 2.5% of the overall course marks). As a group, show artefacts to your tutor and explain what you have done. Marking based on:

- Up to one mark for extracting the call history and SMS databases (evidenced by artefacts);
- Up to one mark for constructing the visualisations;
- Up to ½ mark for the verbal explanation given to tutor.