Summary

Your task in Assignment 1 (Mobile Forensics) is to analyze data on a mobile device (Samsung Galaxy S6). Again, you will conduct the assignment in teams of two.

This assignment has two steps:

1. *18.2. - 25.2.* You are given a Samsung Galaxy S6 with a valid SIM card. Use the device "as normal", but make sure you do not leave any of your personal data on it (i.e. create new accounts if you want to, do not enter your own passwords). You can use mobile data, but please note the device DOES NOT have a data flatrate, so limit the amount of mobile data you use. In addition, you will receive a task to carry out with the phone. Please complete that until **February 25** and bring the device to the lecture on that day (February 25).
2. *25.2. - 9.3.* We'll then swap phones between groups. You will then analyze the mobile phone used by another group.

Do's while using the phone

- Try to generate interesting data: connect to open hotspots, use Google Maps, browse the web, take pictures, ...
- You can login into services and apps, but then please create temporary accounts for that purpose.
- I will distribute a list with phone numbers - send texts (not too many) between groups
- Make sure to limit the amount of mobile data you use (use Wifi for larger downloads)
- Handle the device with care

Dont's while using the phone

- Do not use the phone for any illegal purposes or outside the scope of this assignment. You will be responsible for all your actions.
- Do not use excessive mobile data volume, calls, texts
- Do not root the device or change firmware
- Do not set a passcode or enable encryption
- Do not activate a Samsung account, if you do factory-resetting later becomes very hard for me
- Do not lose or damage the device
- Do not use your own, personal accounts with the device. If you want to login into apps or services, create temporary accounts for that purpose.

Your goal

This part starts when we have swapped phones - please do NOT do anything described here before

You are in the role of a forensic analyst tasked with inspecting the device. The devices have a TWRP recovery image installed that can be booted by turning the device off and then pressing and holding:

Home, Power, Volume Up

at the same time. The device will then boot into TWRP. Then, you can:

- Mount the device as mass storage
- Use an adb shell
- Create a backup

As a minimum, complete the following tasks by proper forensic examination:

1. Retrieve and document all pictures that were taken, along with their timestamp and geolocation.
2. Retrieve and document all Wifi networks that the device connected to or logged.
3. Retrieve and document the location history from the Maps application.
4. Retrieve and document all contacts in the address book.
5. Retrieve and document the call log and all sent text messages.
6. Did the user install any apps or was logged into any major service?
7. Is there any additional information of forensic value (optional).

Based on this, reconstruct and briefly describe the actions taken by the user of the phone. As usual, follow proper forensic practice, i.e. ensure that the evidence copied from the device is sound and that no data was changed during the investigation. Also, if your conclusion are speculative, then make that very clear.

Tools

Feel free to use any tools you like. You may also use tools that have not been shown in the lectures before. You may also implement tools by yourself should you not find suitable tools for the task.