Initial plan: Forensic Analysis of Smart watches
Author: Patricia Booth
Supervisor: Helen Phillips
Moderator: Bailin Deng
Module Number : CM3203
Module Name : One Semester Individual Project
Module credits : 40

Project description
One of the main questions that this investigation attempts to answer is:
Is forensic analysis of smart watches worth further research and development for forensic analysts, if so what type of relevant and useful information can be retrieved?

As the technology of smart watches develop and more consumer growth continues, its value as digital evidence also increases. Understanding what type of data/information can be collected from smart watches can be beneficial from a forensic analyst point of view. More of these devices are being found in crime scenes but has yet to have the correct procedures in how to handle the device in terms of utilising all of what can be retrieved or filtering out which pieces of information are most relevant to retrieve in the first place. Thus, leading to more efficient evidence retrieval.

This recent technology has yet to be looked into with much detail; because of its freshness the research and development in terms of forensic analysis is only beginning to increase. Highlighting the type of sensitive user information that can be gathered on a smart watch alone will showcase its forensic value.

Forensic analysis will be performed on 2 Android smart watch(**Smartwatch1:**Sony Smartwatch3 SWR50/ **Smartwatch2:** TBD device) along with their synchronised phones. The watch will need to be previously synchronised to the phone but disconnected when forensically analysing to recreate the circumstance when the watch is found in a crime scene without its matching phone.

The data stored on the phone and the data stored on the phone differs comparing the phone and watch images will hopefully highlight which information is stored on the watch or is just copied onto the watch as it synchronised to the phone. This emphasises what data can be retrieved if the watch was found on its own.

In addition, examining two watches will allow the comparison of their results as the next part of the project is to provide a list/guide of material filtering the most relevant pieces of information that is ideal for a forensic analyst to investigate.

Project Aims and objectives

Access devices: Android Smart Watches

- Must root the device and provide its access to the computer to make it possible to practically get into the device . Both must be able to communicate, and access root folders must be owned.
    - Watch developer option: The watch has a Developer Option setting that needs to be enabled to allow root access

Computer environment set up:

- Set up perquisites - the Android Smart watch is setup to communicate with a computer via ADB which needs an installation of Android SDK

Establish connection between watch and computer via USB cable:

- Using command prompt use ADB which is what the watch is compatible with to communicate with the computer. Check if bootloader is unlocked (ensure it is unlocked)

Imaging devices:

- The smart watch and its synchronised phones must be imaged so that further forensic analysis can be performed without altering the original data also

Hashing images:

- Hashing the images will authenticate their validation which is ideal when doing forensic analysis on devices

User data forensic image examination:

- Record all findings
- Highlight and evaluate interesting finds
    - Types of information most interested in:
        - Location access
        - communication channels
        - Personal user information: calendar events
        - Voice recorder of watch
        - Activity monitor
- Compare results of the two watches: depending on findings highlight what the differences imply
- Compare Smartwatch1 image data with phone image data: demonstrates if data found on the watch alone can be exploited by an attacker thus giving it value to forensic analysts
- Compare Smartwatch2 image data with phone image data: demonstrates if data found on the watch alone can be exploited by an attacker thus giving it value to forensic analysts

Create a list/guide of the most relevant data that should be investigated by forensic analyst:

- List can be used by analyst as a guide to find the most useful information, can be used as a draft forensic methodology when dealing with smart watches on a crime scene

Work Plan

Week 1

- Research: Background research into forensic analysis of smart watches, articles and papers for further guidance.

Week 2

- MILESTONE: Initial plan submission
- Supervisor meeting(Every two weeks): Meeting about initial stages of the project checking if any areas are missed
- Research: Once meeting has occurred do further research putting into consideration what was discussed in the meeting

Week 3

- MILESTONE: Environment Setup: The computer used to establish a connection with the smart watches will need to have the correct software to communicate with the Watches e.g. one of the watches is setup to communicate with a computer via ADB which needs an installation of Android SDK
- Watch Setup: root access is needed to retrieve the information intended, the watch has a developer option that allows this.

Week 4

- Supervisor meeting(Every two weeks)
- Imaging Android Smartwatch1 and synchronised phone
- Hashing images: the images must be hashed to authenticate validation
- Begin Final report draft

Week 5

- Imaging Android Smartwatch2 and synchronised phone
- Hashing images: the images must be hashed to authenticate validation
- Continue Final report draft adding on findings of this week

Week 6 – 7

- Supervisor meeting(Every two weeks)
- MILESTONE: User data forensic image examination Smartwatch1 image and synchronised phone
    - Record all findings
    - Evaluate results
- Continue Final report draft adding on findings of these weeks

Week 8 – 9

- Supervisor meeting(Every two weeks)
- MILESTONE: User data forensic image examination on Smartwatch2 image and synchronised phone
    - Record all findings

    - Evaluate results
- Continue Final report draft adding on findings of these weeks

Week 10

- Supervisor meeting(Every two weeks)
- Compare Smartwatch1 image data with phone image data
- Compare Smartwatch2 image data with phone image data
- Continue Final report draft adding on findings of this week

Week 11

- MILESTONE: Compare results between the two watches
- Create list/guide of most relevant data a forensic analyst should investigate
- Continue Final report draft adding on findings of this week

Easter Break (3 weeks)

Week 12

- Supervisor meeting(Every two weeks)
- MILESTONE: Final Report Submission