GEORGE, Samuel  
SCHIQUETTI, Felipe A.

PROJECT PLAN - INTRODUCTION TO DIGITAL

FORENSICS

7 weeks to complete.

Task: 20 minutes presentation about the mobile forensics state of the art. Including  
but not limiting to tools to get important info from the phones, actual use of one (or  
more) of those softwares, diferences beetween SOs and how this interfere in the  
forensics activity, how secure a platform is and how much info we can get from the  
most important operacional systems from this platform.

Introduction:

Mobile device forensics is a sub-branch of digital forensics relating to recovery of  
digital evidence or data from a mobile device. It differs from Computer forensics in  
that a mobile device will have an inbuilt communication system (e.g. GSM) and,  
usually, proprietary storage mechanisms. Investigations usually focus on simple data  
such as call data and communications (SMS/Email) rather than in-depth recovery of  
deleted data. SMS data from a mobile device investigation helped to exonerate  
Patrick Lumumba in the murder of Meredith Kercher. [1]

This field is the answer to the demand of forensically sound examination procedures  
of gathering, retrieving, identifying, storing and documenting evidence of any digital  
device that has both internal memory and communication ability. [2]

This platform becomes more and more important in the world. And a consequence  
generated by this fact is the increase of crimes related with this kind of tool. So, as a  
new field, not much research was developed yet, and a lot of tools demands tests to  
comprove it's usability.

The mobile devices that this field try to cover is broad and for this work the focus will  
remain in the 2 biggest operational system available, iOS and Android.

FIRST WEEK - GIT preparation and Project Plan.

Status: Done.

SECOND WEEK - Reunion to stabilish the scope of the work and to research what kind of  
software leads the area. If possible, starts the tests.

**Scope to continue to focus on iOS and Android systems.**

**Tools Identified for use but no testing actually done.**

iOS: Tools that use iOS backups to get data (e.g.iPhone Analyzer, Paraben Device Seizure, Mobile sync Data, etc)

Android: Magnet Acquire; Android backup service

**Identifying what sort of complications we can run into.**

- Acquiring volatile data on mobile devices is tricky

* Keeping the phone on in an attempt to save volatile memory doesn't work because it's connected to the mobile network which will change volatile memory
* Attempting to turn off the mobile network in an attempt to save volatile memory will in-effect change volatile memory in the process

- Limited Resources may cause the OS to remove/close volatile systems in order to free space/resources resulting in lost information

- Mobile phones are very similar to computers but come with more variety but "8/10" is either iOS or Android. This is why we're focusing on these two

**General research done.**

Mobile phone communication information

Phone Identifiers (MEID/IMEI, MIN, SIC)

The iOS environment is increasingly difficult to obtain information, with recent updates the system is well protected. Therefore, to obtain the desired information i got a tool that extracts information through backups.

This tool is similar to many other branch, but has greater recognition and contains several online tutorials.

The tool worked properly for polls testing, but further search should be made.

A private network was created to try to get information through mobile connections. But I have not been able to obtain them.

Status: Done

THIRD WEEK - Start testing and studies of how these operational systems works internally  
and what is important to a forensic investigator searchs and why.

Update: Online brainstorm about how we would work and share some articles about it.

Status: In time.

FORTH WEEK - More complex testing and approfundation in what tools are available to this  
kind of platform.

Status: In time.

FIFTH WEEK - Start discussing the results and start the presentation plans.

Status: In time.

SIXTH WEEK - Finnish the presentation slides and discuss about how the presentation will be  
separated.

Status: In time.

SEVENTH WEEK - Finnish everything and preparing mentally to the presentation.

Status: In time.

Presentation: To be discussed.

Tools: To be decided.

Conclusions:

<empty>

References:

[1] <<https://en.wikipedia.org/wiki/Digital_forensics>> Acessed: 10/26/15.

[2] Wayne Jansen and RickAyers, "Guidelines on Cell Phone Forensics", NIST, May 2007.  
<empty>