

PP Final COMPLETE

by Ethan Hopkins

Submission date: 20-Oct-2024 10:15PM (UTC+0100)

Submission ID: 240722832

File name: 40786_Ethan_Hopkins_PP_Final_COMPLETE_586419_874491284.docx (57.71K)

Word count: 1734

Character count: 9279

Mobile Device Forensics

Research Proposal

Ethan Hopkins

Nitheesh

1500 words

Contents

1. Introduction 3

2. Background to the Proposed Research..... 3

3. Research Problem statement 4

4. Research Aim & Objectives 4

5. Methodology..... 5

6. Project Plan 6

7. References 8

1. Introduction

The use of mobile phones has grown exponentially in just the last 2 decades, with now over 80% of the population of US owning a smart phone [1] and is becoming more and more intertwined with our daily lives. Due to the usability and security that mobile phones offer, they are commonly used by criminals which makes mobile phones crucial for investigations as they almost always contain evidence of their users' crimes [2], whether that be for planning drug deals, planning attacks or scamming people online.

In this project I want to explore how effective Cellebrites tool kit is when carving data from mobile devices and see how its recovery techniques stack up against more modern phones and their advanced security measures.

I have chosen this project idea as I have always had an interest in working in the forensics side of cybersecurity, I enjoy problem solving and believe that I have the skill set required to do this effectively. I have also always had an interest for working in the police force, who also use Cellebrite as their primary tool for mobile phone forensics. I believe that this project will be the first stepping stone for me to build a foundational skill set for working with Cellebrite to help me stick out from the crowd when applying to work for the police.

2. Background to the Proposed Research

Mobile forensics can be viewed as the science of retrieving evidence in many formats from mobile phones in a forensically legal way. This evidence can be used in courts of law as evidence against those who may have committed crimes just like any other forensic data could [3]. The process for basic forensics goes as follows. Cellebrite is a cell phone hacking company that offer software and other services, according to Cellebrite, they provide a comprehensive digital intelligence platform that can be used for the whole end-to-end process of investigation, such as the collection process, analysis of the files and systems and management of said files, including management of other digital sources such as computers and data stored on the cloud. [4]

Step one would be collection, where the data is initially collected from any relevant source whether it seems related to the case or not. Step two would be the examination phase. Where data is flagged as suspicious and examined closer using a combination of manual and automated processes. Some data that may be of particular interest is extracted, all whilst preserving the integrity of the data. Step three would be analysis. Where all the flagged data from the examination is analysed using methods and techniques that prove to be well documented are used to derive information that may answer the questions that may be important to the case. Step four, reporting. Here the data is showcased, and the findings are all put together including a description of what tools and procedures have been used, chains of custody, additional sources etc [5].

There are many ways a mobile phone could contain evidence for a case. One example would be the SIM card. This is a very useful part of the data collection process due to a password not being required to access the data on board, and that it contains a lot of vital information such as SMS logs, incoming and outgoing call logs and often a lot of personal data. [6] another example would be internet history, as the internet is usually the first place people go when looking for information, especially if that information is about something malicious. [7] however this can be more difficult to access as you are required to get through some security features such as passwords to unlock the phone, and possibly account access to search engines.

Many papers about the comparison of different forensic tools are outdated, using older phones with that are owned by very few people, [8] I want to fill this gap by researching on a more modern phone, a phone that many people still own, or one that is popular with those who involve themselves in crime as these are the phones that you are most likely to come across for investigations.

3. Research Problem statement

What are the differences in accuracy and effectiveness of Cellebrite tools when compared to other mobile forensic tools, such as the wide range of open-source forensic tools that are readily available. My project will aim to address the differences for how each tool deals with the different aspects of mobile forensics such as data carving, handling deleted data and dealing with fragmented data.

4. Research Aim & Objectives

Aim 1

To evaluate how effective Cellebrite is at dealing with mobile data recovery when compared to open-source forensic tools.

Objectives

- 1.1: Determine the percentage of examined cases in which Cellebrite was more successful than the selected open-source tools in the data recovery from mobile devices of deleted data.
- 1.2: Compares the effectiveness of two tools when recovering fragmented files on iOS
- 1.3: Determine which of the tools can restore encrypted data more efficiently. Comparing time taken, and how much data was decrypted.

Aim 2

To evaluate the strength, weakness, opportunities, and threats of Cellebrite and compare them to the open-source tool(s).

Objectives

- 2.1: to compare the advanced features and the functionalities of both Cellebrite, along with open-source tools, and uncover both their advantages and disadvantages.
- 2.2: examine whether the data collected kept its integrity and determine if the collected data could be used in legally critical contexts
- 2.3: Identify where one tool may significantly outperform the other and determine what factors may be causing these differences.

Aim 3

Propose possible improvements in mobile forensics tools and identify recommendations for the best practises.

Objectives

3.1: Suggest improvements of data recovery methods in open-source forensic tools based on the discovered gaps.

3.2: create a table showing each tool and their strengths and weaknesses, to help in picking the appropriate tools based on the needs of the investigation

3.3: Develop a list of guidelines on how to effectively use Cellebrite and the combination of open-source tools to improve overall results.

5. Methodology

This project will use a comparative experimental research design to test the accuracy and effectiveness of Cellebrite when compared to other open-source forensic tools. The research will include using controlled experiments conducted by myself, using a mobile phone loaded with deleted files, encrypted files and fragmented data. Both Cellebrite and an open-source tool will be used in every scenario when analysing and extracting data. The results will be measured based on metrics such as success rates, time efficiency and data integrity, ensuring that the comparisons are systematic and provide quantitative data to support findings.

Quantitative data will be used in this experiment as success rate, time taken to extract, and accuracy of the data recovered will be recorded in each experiment, including the percentage of data recovered, how accurate the reconstructed files are, and the time taken for each tool to complete the whole process of recovering files. the experiments will be conducted using synthetic data in order to prevent ethical issues arising and to stay compliant with data protection laws and regulations. Using this controlled test data also allows me to keep my tests consistent, making the results more comparable and more accurate. Qualitative data will also be used, as this experiment will be measuring user experience, ease of use or any other major differences in how the tools may "handle", as these are all aspects that needs to be considered when deciding on the superior tool.

6. Project Plan

November 2024

1st-10th – Finalize my research objectives, the scope of the project and methodology

11th-15th – Gather the tools that are required for all my experiments, such as Cellebrite, autopsy, SIFT etc. And obtain my synthetic data and create my testing environment.

16th-30th – Detailed literature review on mobile forensics, the tools, recovery methods and other studies about comparing forensic tools.

16th-30th – I also want to familiarize myself with the Cellebrite + Open-source toolkits through practice runs

December 2024

1st-7th – Design the experiments to simulate the different data recovery scenarios such as deleted, fragmented and encrypted data

8th-31st – proceed with initial experiments using the Cellebrite toolkit and open-source tools

January 2025

1-15 – Analyse my quantitative data

16-31 – make any adjustments to the experiments based on my previous results as needed for my comparison

February 2025

1-14 – carry out a comparative analysis of how Cellebrite performed against the open source tool kits, to show each tools strengths, weaknesses and performance gaps

15-28 – Create a draft for the recommendations for each toolkit and where they should be used to be most effective

March 2025

1-21 – research write up, introduction, methodology, analysis and results

22-31 – Refine my report based on feedback

Milestone – Draft report is ready for final revisions

April 2025

1-15 – Final editing and adjustments to be made based on feedback

16-30 – Final presentation and submit the completed report

Milestone – Report is finished and submitted, with much time still available in case of delays throughout any part of the report

7. References

- [1] K. Patrick, W. G. Griswold, F. Raab, and S. S. Intille, 'Health and the Mobile Phone', Aug. 2008. doi: 10.1016/j.amepre.2008.05.001.
- [2] J. E. R. McMillan, W. B. Glisson, and M. Bromby, 'Investigating the increase in mobile phone evidence in criminal activities', in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2013, pp. 4900–4909. doi: 10.1109/HICSS.2013.366.
- [3] D. Sandhya, S. Daware, and V. M. Thakare, 'Recent Trends in Computing', IJCA, 2012. [Online]. Available: <https://www.researchgate.net/publication/267986937>
- [4] Cellebrite, 'Cellebrite Provides Facts About its Business and Solutions'.
- [5] D. Sandhya, S. Daware, and V. M. Thakare, 'Recent Trends in Computing', IJCA, 2012. [Online]. Available: <https://www.researchgate.net/publication/267986937>
- [6] A. Pal, M. Maheswari, K. B. Jena, and G. K. Singh, 'SIM Card Data Extraction in Digital Investigations: A UFED Cellebrite Approach', *International Journal of Medical Toxicology and Legal Medicine*, vol. 27, no. 1, pp. 27–37, 2024, doi: 10.52710/ijmtlm.5.
- [7] A. A. Alyas and V. Kumar, 'Lawfully Data Collection Techniques in Mobile Forensic & Analysis Using Cellebrite Physical Analyzer'. [Online]. Available: <https://ssrn.com/abstract=4483864>
- [8] *2016 Ninth International Conference on Contemporary Computing (IC3)*. Institute of Electrical and Electronics Engineers, 2016.

FINAL GRADE

GENERAL COMMENTS

63/100

PROJECT PROPOSAL – ACCA6020 INDEPENDENT PROJECT

Student Ethan Hopkins Mark 63

Intro / A&O (400 words)		
Project title; Identification of a specific problem to be investigated; Well-defined aims and SMART objectives; Explaining why this project is worth doing; Discussion of what the project needs to do in order to be a success; Description any deliverables that will be produced at the end of the project	20	12
Your project proposal is very interesting. I appreciate your efforts in selecting a project work within your interest. It need to be tailored to be an Major Project. With considerable adjustments to your aim		

and objectives, this proposal could be a very good project work. Comparison of 2 tools? What do you want to achieve in comparing the tools? To Do: + Your Aim should be a broad statement on what you want to achieve. Adding multiple aims to 1 project is not a great way to move forward. + The aim must tell the reader what the end result is likely to be. It doesn't need to specify how, but it need to clarify the work on focus. + Break down your aim into Specific, Measurable, Achievable, Relevant, and Time-bound tasks.		
Background to the Project / Literature Review (400 words)		
Description of how the work to be done by in the project relates to the work identified in the literature review; Discussion of any ethical issues raised by the project Identifying what has already been done within the field; Topic familiarity; Brief literature review using appropriate sources – 6-8 journal papers and book chapters rather than just websites;	20	10

Selection of relevant models & concepts

Literature

review done. However, more adequate literatures, critical appraisals could have added value to the work. Literatures on Open Source Mobile Forensics Tools could have given insights.

To Do:

+

Define Keywords and Search for Literatures ScienceDirect, ACM, and IEEE (Accessible via UWTSD Library)

+

Review literatures that focus on Mobile Forensics, Challenges, Tools.

+

What is the problem these literatures are addressing?

+

Explain the problem in existing technologies or approaches.

+

Identify the Gap.

+

Cite evidence from recent research to show the impact of this gap.

+

Clearly state how your project will address this gap.

Project Design (500 words)		
Clear statement of which development methods are to be used and why they are appropriate; Clear statement of which tools are to be used and why they are appropriate; Clear description of how data collected will be analysed More work on the design required. Which Open Source tool are you proposing to compare with Cellebrite? Why comparing Cellebrite – Is it to find any open source tool that could be equally efficient as Cellebrite? How about the data to be used? To Do: + Adapt to the existing Digital Forensics Framework + Complete the Literature Review and identify the gap to finalise the Design + Tools, Data and the progression can be worked based on the identified Gap.	30	20
Resources / Planning (200 words)		

List of any deliverables; Clear diagram showing both timing and resource use; Completed ethics form; Limited and relevant appendices		
More adequate details required.	15	8
Document Presentation		
Correct spelling, grammar and punctuation; Flow of narrative/fluency; Coherence; Word processed ; Correct use of referencing with bibliography; Strict word limit		
Presented well	15	13
TOTAL	100	63

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8
