

AN EVALUATION AND COMPARATIVE ANALYSIS OF A WIDE RANGE OF EVIDENCE USING A COMMERCIAL MOBILE FORENSIC TOOL (CELLBRITE)

Ethan Hopkins | Email: 2201011@student.uwtsd.ac.uk

School of Applied Computing | BSc Computing (Computer Networks and Cybersecurity)

Introduction

Mobile phones play a crucial role in modern investigations due to their widespread use and the volume of personal data they hold. As criminals increasingly rely on mobile devices, mobile forensics has become a vital field for extracting legally admissible digital evidence [1]. This project evaluates the effectiveness of Cellebrite, a widely used commercial mobile forensic tool, in recovering data such as deleted files, encrypted content, and app data across different mobile platforms.

Aim

To evaluate the effectiveness of a commercial mobile phone forensic tool comparing a wide range of evidence, benchmarking its performance in recovering digital evidence, including deleted, fragmented and encrypted data.

Objectives

- **Conduct a systematic literature review** by identifying and categorising peer-reviewed research on commercial and open-source mobile forensic tools.
- **Develop and document a clear research methodology** using the research onion framework, including systematic literature review and experimental design, completed by the milestone date.
- **Formulate clear evaluation criteria and experiment design** using synthetic mobile datasets (calls, messages, location data), with detailed documentation completed by the project midpoint.
- **Conduct comparative analysis experiments** with selected toolkits, measure against defined criteria, analyse outcomes, and complete final reporting by the project deadline.

Methodology

A **mixed-method approach** was adopted, combining a literature review with experimental testing. The forensic tool **Cellebrite** was evaluated by performing data extractions on three different mobile devices using both physical and logical methods.

Devices tested:

- **iPhone 11 (iOS)** – Physical extraction
- **Pixel 7a (Android)** – Physical extraction
- **Samsung A13 (Android)** – Logical extraction

Data categories examined included: **images, call logs, messages, app data, deleted files, and encrypted content.**

All data was **synthetic or educational**, ensuring ethical and GDPR-compliant procedures.

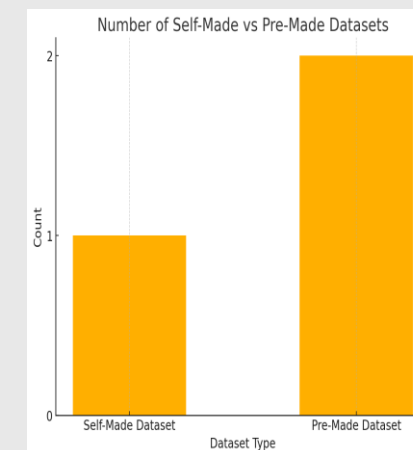
Design and Implementation

The experiment was designed to test Cellebrite's effectiveness in real-world scenarios using both **pre-made forensic images** and a **custom dataset**.

- **Pre-made images** (Pixel 7a & iPhone 11) were sourced online and included known deleted and encrypted data.
- A **self-made dataset** was created on the Samsung A13, with self-planted encrypted and deleted files.

Cellebrite's **UFED and Physical Analyzer** were used to perform extractions and generate reports.

Effectiveness was measured by comparing recovered artifacts to known dataset contents and assessing **data recovery rates by category.**



Findings

Cellebrite's effectiveness varied significantly based on **extraction method** and **device compatibility**:

•iPhone 11 (Physical Extraction):

Cellebrite performed exceptionally well, extracting **392,909 artifacts**, including **deleted and encrypted data**, demonstrating its strength with iOS devices.

•Pixel 7a (Physical Extraction):

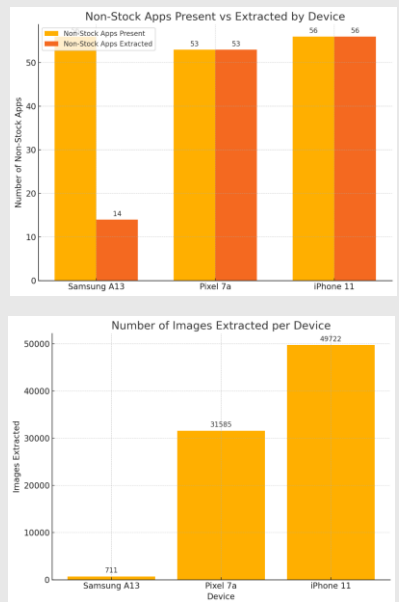
Despite using a physical method, Cellebrite failed to recover **messages and call logs**, suggesting limitations with newer **Android OS versions**.

•Samsung A13 (Logical Extraction):

Cellebrite extracted only **6,709 artifacts** and missed **deleted and encrypted data**, reflecting the reduced capability of **logical extractions**.

Key Insight:

Cellebrite is highly effective when physical access is possible, especially with iOS, but its performance is **inconsistent across Android devices** and **limited by extraction method**.



Conclusion

Cellebrite is a powerful mobile forensic tool, but its effectiveness is **highly dependent on device compatibility** and the **type of extraction method used**.

• **Physical extractions**, particularly on iOS devices like the iPhone 11, yielded the most comprehensive results.

• **Logical extractions** and certain Android models showed **significant limitations**, especially in recovering encrypted or deleted data.

Key takeaway:

No single tool provides complete coverage — a **hybrid forensic approach** using both commercial and open-source tools is recommended for thorough investigations.

References

[1] E-SPIN, "Importance of Mobile Device Forensics," E-SPIN Group, Apr. 13, 2018. <https://www.e-spincorp.com/importance-of-mobile-device-forensics/>