

Research Report and Digital Forensics Progress Report

Mobile Device Forensic Investigation Using FTK Imager and Cellebrite Physical Analyzer

2505249 – Sanjay kumar Unkili

UNIVERSITY OF WALES TRINITY SAINT DAVID – Wales Institute of Science and Arts –
School of Applied Computing

Table of Contents

1. Abstract
2. Introduction
3. Objectives
4. Devices Under Examination
5. Chain of Custody
6. Tools Used
7. Methodology
8. Current Progress
9. Conclusion
10. References

Abstract

This report presents the current progress of a digital forensic investigation involving four mobile devices: Huawei, Nokia, Samsung, and Ule. The primary objective of the investigation is to identify, acquire, and analyze digital evidence using industry-standard forensic tools while maintaining the integrity of the evidence. The examination is currently ongoing; therefore, this report documents and the work completed to date rather than providing final conclusions. All activities performed during the investigation was follow accepted digital forensic procedures to ensure the reliability of digital evidence.

Introduction

Digital forensics is a specialized branch of forensic science that focuses on the identification, preservation, acquisition, examination, analysis, and reporting of digital evidence obtained from electronic devices. Mobile devices are frequently contain valuable information such as call records, messages, contacts, multimedia files, application data, internet history, and location information, which may assist an investigation.

In this assignment, four mobile devices (Huawei, Nokia, Samsung, and Ule) were submitted for forensic examination. The investigation is being conducted using FTK Imager and Cellebrite Physical Analyser, following standard forensic procedures to ensure that the original evidence remains unaltered. Since the forensic analysis has not yet been completed, this document serves is in progress report.

Objectives

The objectives of this digital forensic investigation are:

- To preserve the integrity of all digital evidence.
- To acquire forensic data from the submitted mobile devices.
- To analyze extracted data using professional forensic software.
- To document all forensic examination procedures.
- To progress reports to the supervisor authority until the investigation is completed.

Devices Under Examination

The following mobile devices are currently being examined:

Device	Current Status
Huawei	Data extraction completed; analysis in progress
Nokia	Data extraction completed; analysis in progress
Samsung	Data extraction completed; analysis in progress
Ule	No significant user data identified so far; examination is continuing

Chain of Custody

Maintaining the chain of custody is an essential part of every digital forensic investigation. Each mobile device was received from the investigating authority, documented, assigned a unique evidence identifier, and securely stored before any forensic examination was performed. Only authorized personnel have access to the evidence throughout the investigation. Every activity performed on each device is recorded to maintain secure and ensure the integrity of the evidence.

Chain of Custody Record

Device	Received By	Examiner	Date	Process
Huawei	Nitheesh Kaliyamurthy	Sanjay kumar	30/06/2026	ongoing
Nokia	Nitheesh Kaliyamurthy	Sanjay kumar	30/06/2026	ongoing
Samsung	Nitheesh Kaliyamurthy	Sanjay kumar	30/06/2026	ongoing
Ule	Nitheesh Kaliyamurthy	Sanjay kumar	30/06/2026	ongoing

Tools Used

The examination is being conducted by using **FTK Imager** and **Cellebrite Physical Analyzer**, which are widely recognized tools in the field of digital forensics.

FTK Imager is used to acquire and verify forensic images while ensuring that the original evidence remains unchanged. The software supports forensic acquisition and integrity verification through cryptographic hash values, allowing investigators to confirm that no modifications have occurred during the process.

Cellebrite Physical Analyzer is used to process and analyze extracted mobile device data. The software will enables to investigators to examine contacts, call logs, SMS

messages, multimedia files, application data, browser history, location information, and other digital artifacts. It also assists in organizing and interpreting extracted information in a forensically manner.

Methodology

The forensic investigation follows the standard digital forensic process to ensure that every examination is conducted according to accepted forensic principles.

Initially, all submitted devices are identified, documented, labeled, and securely stored. Before any examination begins, the condition of each device is recorded. Where possible, forensic acquisition is performed while preserving the integrity of the original evidence. FTK Imager is used to acquire forensic images and verify their integrity by using cryptographic hash values.

Following acquisition, Cellebrite Physical Analyzer is used to examine the extracted data. The analysis includes reviewing communication records, contacts, multimedia files, application artifacts, internet activity, and other available digital evidence. Throughout the investigation, detailed documentation is maintained to ensure that every step of the forensic process can be reproduced and verified.

Current Progress

The digital forensic investigation is currently ongoing and has not yet been completed. Data extraction has been successfully performed on the available mobile devices, and they are investigators are currently conducting a detailed examination of the recovered digital artifacts.

Based on the analysis completed so far, the **Nokia** device appears to belong to **Norman**. The **Huawei** device appears to belong to **Emma**; however, the available evidence suggests that the user may have been identifying himself as **Peter**. The **Samsung** device appears to belong to **Joe**. The **Ule** device has not produced any significant user data during the current stage of the examination.

These observations are preliminary and are based only on the evidence analyzed to date. Since the forensic investigation is still in progress, additional analysis may identify further information. Therefore, no final conclusions have been reached, and all observations remain subject to verification until the examination.

Conclusion

This report represents the current progress of the digital forensic investigation and summarizes the work completed during the present stage of the examination. The investigation of the Huawei, Nokia, Samsung, and Ule mobile devices is continuing in accordance with accepted digital forensic procedures. Evidence integrity has been maintained throughout the investigation, and all examination activities have been documented. A comprehensive final report containing verified findings, supporting evidence, and final conclusions will be prepared once the forensic analysis has been completed.

References (IEEE Style)

- [1] National Institute of Standards and Technology (NIST), *Guidelines on Mobile Device Forensics*, NIST Special Publication 800-101 Rev. 1, Gaithersburg, MD, USA, 2014.
- [2] Cellebrite, *Cellebrite Physical Analyzer User Guide*, Cellebrite, Petah Tikva, Israel.
- [3] Exterro, *FTK Imager User Guide*, Exterro Inc., Portland, OR, USA.
- [4] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed. Burlington, MA, USA: Academic Press, 2011.