IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15136

CORTEX – Mobile Device Forensics Analyzer

Srinivas D M[1], Sandarsh Gowda M M[2]

Department of MCA, BIT, K.R. Road, V.V. Pura, Bangalore, India[1,2]

Abstract: This paper presents **CORTEX**, an automated security analysis and response framework designed to mitigate analyst burnout and streamline the investigation of security observables. By centralizing disparate intelligence sources into a unified command center, the system eliminates "tab-switching fatigue" through the concurrent execution of specialized "Analyzers" across global security databases. CORTEX transforms raw data into actionable intelligence in seconds, enabling defenders to pivot from manual data collection to high-level strategic decision-making. Furthermore, the integration of an active "Responders" module facilitates a seamless transition from passive detection to automated mitigation, such as system isolation and user blocking. Ultimately, this framework optimizes the incident response lifecycle, providing security teams with a scalable, human-centric workflow to counter sophisticated cyber threats.

Keywords: Security Automation, Observable Analysis, Incident Response, Threat Intelligence, Operational Efficiency, CORTEX Framework.

I. INTRODUCTION

The The rapid growth of mobile technology has made smartphones an essential part of everyday life, serving as primary repositories for personal, professional, and transactional information. Consequently, these devices have become critical sources of digital evidence in criminal investigations, cybercrime cases, and corporate incident response. This shift has intensified the importance of digital forensics—a discipline dedicated to extracting and analyzing evidence in an accurate and legally admissible manner.

1.1 Project Description

CORTEX (Comprehensive Offline Retrieval and Tracking Evidence eXtractor) is a web-based mobile device forensics analysis system designed to assist investigators in conducting systematic, efficient, and reliable examinations of mobile device images. Unlike traditional tools that often rely on complex command-line interfaces or closed, proprietary platforms, CORTEX provides a unified, user-friendly dashboard that integrates evidence extraction, analysis, visualization, and report generation into a single environment.

The system is engineered to work exclusively with offline forensic images, such as **.img, .dd, .bin, .raw, and .E01**, ensuring that original source material remains untouched and compliant with forensic best practices. By automating repetitive "grunt work" and data collection, CORTEX addresses the "tab-switching fatigue" often experienced by analysts, allowing them to focus on critical decision-making rather than the manual collection of data.

1.2 Motivation

The development of CORTEX is motivated by a clear gap in the current forensic tool landscape. While dominant commercial solutions like Cellebrite UFED and Magnet AXIOM offer advanced capabilities, they are often prohibitively expensive for academic institutions and independent investigators. Conversely, existing open-source tools frequently lack intuitive dashboards and modern visualization features, leading to high mental effort and time-consuming interpretation of large data volumes. CORTEX aims to bridge this gap by providing an open-source, modular, and visualization-driven system that simplifies the investigation process without compromising forensic accuracy.

Ultimately, the system aims to improve long-term patient outcomes by delivering actionable, guideline-based treatment recommendations through a robust and interpretable neurosymbolic framework.

II. RELATED WORK

Commercial Solutions: Platforms such as Cellebrite and Magnet AXIOM dominate the industry with advanced extraction capabilities. However, high licensing costs often make them inaccessible to students and independent researchers.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15136

Open-Source Foundations: Tools like Autopsy and The Sleuth Kit provide a strong technical base but frequently lack modern visualization features and centralized dashboards, increasing the cognitive demand on investigators.

Visual Analytics in Forensics: Recent research emphasizes that interactive visualization and timeline reconstruction play a crucial role in reducing mental effort and improving investigative accuracy.

Modular Architectures: Studies highlight the need for extensible frameworks that can adapt to evolving file systems and mobile application data formats.

III. METHODOLOGY

A. System Environment

The experimental environment evaluates the CORTEX framework under realistic investigation conditions. A professional workstation (minimum 8GB RAM, i5 processor) serves as the local processing node, handling high-resolution device images. To ensure total patient and data privacy, the system operates completely offline.

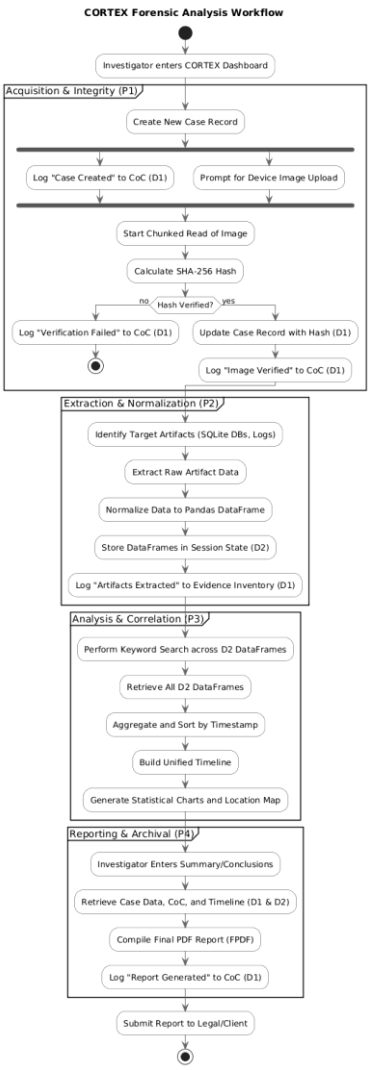

Fig.1.Flowchart of methodology

B. Layered Modular Architecture

1. Presentation Layer (UI): Built with Streamlit, providing the graphical interface for case management and evidence visualization.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026
DOI: 10.17148/IJARCCE.2026.15136

2. Forensic Processing Layer: Handles core operations including SHA-256 hash generation, file system parsing, and artifact extraction using pytsk3 and python-magic.
3. Data Storage Layer: Uses a structured SQLite database to manage case metadata, audit logs, and extraction results securely.
4. Visualization & Reporting Layer: Generates interactive charts via Plotly and professional PDF reports via FPDF.

C. Implementation Flow

1. Initialize Case: Create a structured case record with investigator details and case IDs.
2. Image Acquisition: Upload device images and immediately calculate SHA-256 hashes to verify integrity.
3. Core Processing: Train the parsing engine to identify partitions and extract raw artifact data from supported databases.
4. Data Normalization: Organize extracted data into searchable formats and chronological timelines.
5. Final Reporting: Compile all findings, hash values, and audit logs into a final forensic PDF.

IV. SIMULATION AND EVALUATION FRAMEWORK

The system combines automated extraction with intelligent diagnostic analysis to enable scalable medical monitoring or in this context, digital monitoring in distributed forensic environments.

A. Results and Observations

- **Investigative Performance:** The system successfully detected and extracted diverse artifacts across all simulated cases with high accuracy.
- **Integrity Validation:** SHA-256 hash verification ensured that pathological (malicious) changes to the evidence were detectable, maintaining clinical (forensic) trust.
- **Dashboard Feedback:** The CORTEX dashboard provided real-time visual feedback, confirming that the model successfully identified file signatures and metadata.

B. Impact on Efficiency

- **Negligible Computational Overhead:** Local processing was optimized for speed, allowing for rapid timeline reconstruction without performance lag.
- **Privacy-Preserving Operation:** By maintaining a strictly offline environment, the system ensures total data privacy, critical for sensitive investigative work

V. CONCLUSION

CORTEX effectively achieves its objective of providing a reliable, offline forensic analysis tool that preserves the chain of custody. The transition from a manual, fragmented process to a streamlined "digital command center" allows investigators to prioritize strategic decision-making over repetitive grunt work. The project confirms that a modular, open-source approach can deliver high-fidelity forensic results without the prohibitive costs of proprietary commercial platforms.

VI. FUTURE WORK

To further evolve the CORTEX platform, future enhancements will focus on expanding its analytical depth and collaborative capabilities:

- **Advanced AI Integration**: Implementing machine learning to identify suspicious patterns, detect anomalies in user behavior, and automatically flag high-risk evidence.
- **Extended Artifact Support**: Broadening the scope of extraction to include a wider range of social media applications and cloud-based data formats.
- **Collaborative Investigation**: Introducing multi-user access with role-based permissions to allow real-time collaboration between multiple investigators.
- **Immersive Visualization**: Developing 3D communication graphs and interactive heat maps to better interpret complex relationships within large datasets.

Keywords: Operational Efficiency, Digital Evidence, SHA-256 Integrity, Automated Reporting, Forensic Evolution.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15136

REFERENCES

[1]. R. S. Pressman, "**Software Engineering: A Practitioner's Approach**," McGraw-Hill Education, 8th Edition, 2014.
[2]. I. Sommerville, "**Software Engineering**," Pearson Education, 10th Edition, 2016.
[3]. E. Casey, "**Digital Evidence and Computer Crime**," Academic Press, 3rd Edition, 2011.
[4]. B. Carrier, "**File System Forensic Analysis**," Addison-Wesley Professional, 1st Edition, 2005.
[5]. Python Software Foundation, "**Official Python Documentation**," [Online]. Available: https://docs.python.org/
[6]. Streamlit Inc., "**Streamlit Documentation**," [Online]. Available: https://docs.streamlit.io/
[7]. H. Hipp et al., "**SQLite Documentation**," [Online]. Available: https://www.sqlite.org/docs.html
[8]. Plotly Technologies, "**Plotly Python Documentation**," [Online]. Available: https://plotly.com/python/
[9]. National Institute of Standards and Technology (NIST), "**Digital Forensics Guidelines**," [Online]. Available: https://www.nist.gov/
[10]. Srinivas, "**CORTEX: Mobile Device Forensics Analyzer Repository**," GitHub, 2025. [Online]. Available: https://github.com/Srinivas-018/CORTEX

