National College of Ireland

LedgerLock

Forensic Evidence Verification Framework Application

MSc Research Project (Thesis)
Cybersecurity

Sajid Hussain Jatoi
Student ID: X23265736

School of Computing
National College of Ireland

Supervisor: **Ross Spelman**

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name**:** SAJID HUSSAIN JATOI

Student ID: X23265736

Programme: MSc Cybersecurity (**MSCCYBE_JANO24_O)** **Year:** 2025
Module: Research Project (Thesis)

Supervisor: ROSS SPELMAN

Submission Due Date**:** 11 DECEMBER 2025

Project Title: LedgerLock – Forensic Evidence Verification Framework Application

Word Count**:** **5618** Page Count**: 17**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Sajid Hussain Jatoi
Date: 11 December 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

LedgerLock – Forensic Evidence Verification Framework Application

Sajid Hussain Jatoi
X23265736

Abstract

Digital forensics increasingly demands tools that are transparent and ensure digital records integrity, acceptable and legally defensible. Traditional tools provide important capabilities but lack comprehensive audit-trail and support for repeatability that create challenges and evidence can be tampered with. Existing solutions heavily rely on the analyst expertise, scripts executions, expensive license cost, and pre-requisite dependencies for the execution. This research introducing LedgerLock portable GUI application based on distributed ledger technology (blockchain), that unites cryptographic hash verification with blockchain anchoring supporting online and offline functionality to make it on-field usable. This application was designed to address the gap between current forensic practices to empower analysts with user friendly application with graphical user interface and comprehensive audit trail operating in both online and offline environments.

LedgerLock application offers anchoring and verification of digital footprints, allowing analysts to validate evidence through multiple cryptographic hash algorithms, such as MD5, SHA-256 and Keccak-256, widely used and accepted in forensic world. While anchoring records stores cryptographic hashes on the blockchain, providing full audit trail along with URL to access and verify on Etherscan platform.

LedgerLock demonstrates performance, portability, accuracy, and usability while following NIST, forensic standards and ISO regulations. Blockchain integration made this application legally defensible by strengthening transparency, audit-trail, and advanced forensic practices.

Keywords: Blockchain, Digital Evidence, Forensic Framework, Cryptographic-hash, Network Connectivity, anchor, verification, Integrity, audit-trail, authenticity

Abbreviations:

ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
BEMS	Blockchain Based Evidence Management System
MD5	Message Digest Algorithm 5
IEC	International Electrotechnical Commission
DSR	Design Science Research
GUI	Graphical User Interface

1. Introduction

1.1 Background and Context

Digital evidence has become critical part of the compliance audits, corporate organizational inquiries, judicial proceedings, and modern forensic investigations. Digital record to be trusted, it should remain unchanged, tampered free from the time it was collected until presented. Due to rise in cyber-incidents, courts and forensic investigations expect reliable methods, comprehensive and validated audit trails that prove that digital footprints have not been tampered with.

The common way to prove the integrity of digital records is through cryptographic hash, commonly used MD5, SHA-256 and Keccak-256 etc. These computed cryptographic hashes confirm whether this digital evidence has been altered during the time it was collected and at time of presentation. However, it does not provide the full audit trail that when that code was produced, who performed it, timestamp etc. or any permanent log that can be relied on and review later. This means that hashes can provide authenticity, however it cannot provide a full audit trail, as that relies on the tools, software solutions, methods, and mechanisms that were followed during that period that can be fragmented and fragile.

These limitations are critical from forensic investigation and court perspective, as these not only required digital footprints are intact, but also transparent audit trail that provides verification process.

1.2 Problem Statement

Current forensic solutions and verification mechanisms face three challenges:

1. **Evidence Authenticity Assurance**: Investigators must prove that digital records have not been altered and tampered with.
2. **Audit Trail Transparency:** Tools utilized and reports must be legally defensible as per NIST (2022), ISO standards, and courtroom proceedings etc.
3. **Limitations:** Existing solutions either do not provide full audit trail or require network connectivity to cloud/Blockchain, that restrict on field use of the applications.

The above highlighted challenges and limitations are the critical gaps in current forensic practices, and a digital forensic evidence verification solution with full and comprehensive audit trail support is required to bridge this gap and empower analyst to use it without any restrictions and challenges.

1.3 Gap Analysis

Several recent reszearch has shown that distributed ledger technology can provide full traceability and authenticity in digital footprints by anchoring digital records using blockchain (Olukoya, 2021; Kim, Ihm & Son, 2021; Sowmya et al., 2025). However, despite potential of this technology, significant gaps are still in current practices such as:

- **Audit trail gap:** cryptographic computed hashes confirm the authenticity but does not provide the data and traceability when this verification or process occurred (NIST, 2022), which addresses challenges and difficulties that can lead to disputes for compliance and courts.
- **Lack of integration:** current tools verify digital records but lack integration into the cloud and blockchain technologies as a single solution and analysts are required to switch between different systems that lead to fragmentation, human error and increase complexity (Atlam et al., 2024).
- **Usability gap:** most of the current solutions rely on command line tools, scripts and executions that require technical configurations, programming languages and dependencies that are difficult and complex sometimes for non-practitioners to achieve consistency (Jerald, 2023).

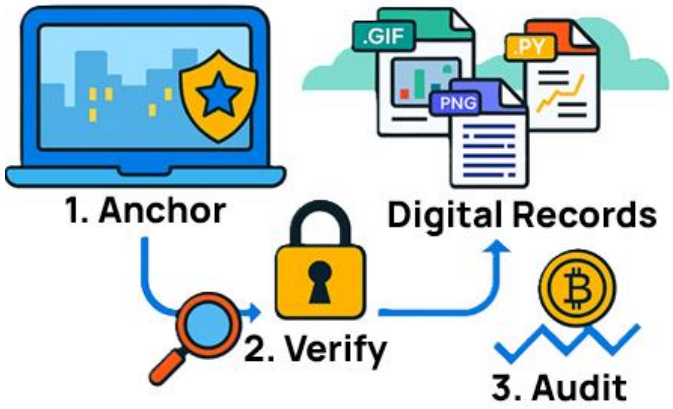
1.4 Research Questions

1. **How can immutable ledger technology be used in forensic digital footprint verification workflows to ensure integrity of digital records and chain of custody?**
2. **Limitations and challenges currently in forensic verification workflows, practices and how can these gaps be bridged?**
3. **What role can Offline / differed synchronization play in secure and intermittent network areas?**

1.5 Research Aim and Objectives

The aim of this research is to design, develop and implement a portable solution based on the forensic framework that addresses limitations and challenges of the current tools by combining blockchain anchoring of the digital footprints and cryptographic hash verifications supporting online and offline functionality. Proposed framework intended to offer analyst centric transparent, repeatable, and comprehensive audit trail with legally defensible workflows using distributed ledger technology for digital records management, that can be confirmed and verified over the internet. To achieve this, following goals are defined:

- **Develop Analyst friendly portable application,** allows researchers to anchor and verify digital records in a batch or single file, reduce the technical dependencies of any pre-requisite lab setup, installations and easy to use. So, this can be used in any environment.
- **Integrate Distributed Ledger Technology (Blockchain)**, to strengthen the chain of custody by creating tamper proof, timestamped records for full traceability and comprehensive audit trail.
- **Offline Functionality:** Application can anchor digital footprints offline, and export later can be imported to the blockchain with all the details upon connecting to the network using exported file.
- **Evidence verification** allows analysts to verify the digital records authenticity by verifying against the expected cryptographic hash and digital record.
- **Support multiple hash algorithms,** to ensure robust verification and support diverse forensic requirements.



[Figure 1] Application Main Design functionalities.

1.6 Contribution

This thesis makes a significant contribution to digital forensic practice by developing a portable solution that directly addresses the limitations and challenges highlighted in the current forensic evidence verification tools. This application records meta-data of digital footprints such as timestamp, hash, block number, transaction identification, gas used etc. ensuring the results are tampered proof and time stamped. Evidence verification functionality also provides the detailed report of the digital records and expected hashes produced during the time of collection against current records and expected hash either matches or not matches.

It clearly strengthens digital records traceability and authenticity by using distributed ledger technology integration with offline workflow, which moves beyond the theoretical discussions into a practical solution. It advances both academic research as well as forensic practices.

2. Literature Review

2.1 Cryptographic Algorithms in Digital Forensics

Hash algorithms are widely used in forensic practice to trust digital records. Commonly used algorithms include MD5, Keccack-256 and SHA-256. These algorithms generate unique and fixed value length hash codes for digital records and if any single letter or number changes within documents, these can generate a different hash. Due to this capability, it makes cryptographic algorithms dependable for integrity checks (Salih & Ibrahim, 2023).

Recent research has shown that perceptual and fuzzy hashing is used in multimedia evidence to detect similarities between images, videos, audios etc., where exact similar matches are not possible (McKeown & Buchanan, 2023). However, these functions can only prove the integrity of the digital records but do not provide the audit trail and it highlights a critical challenge.

2.2 Blockchain in Digital Forensics

Recent research has shown that Blockchain is a solid solution to strengthen the traceability and integrity of the digital records by anchoring hashes and storing immutable ledger. It provides comprehensive audit trail that is tampered proof and time stamped (Atlam et al., 2024). Distributed ledger technology can also support chain of custody, reducing risk of evidence forging and manipulation (Johri.s, 2024).

Systems built on Hyperledger Fabric, Ethereum, cloud and distributed platforms do provide tamper resistance audit trails and transparency, however most implementations do not support offline functionality and require continuous network connection. This limits tools usability on field investigations and restricted areas such as laboratories and crime scenes etc.

2.3 Audit Trail Standards in Digital Forensics

Digital evidence traceability is important for ensuring integrity so these can be trusted in any investigation and forensic practices. Transparent audit trails provide full chronological details and action taken on digital footprints such as verification, transfer, and analysis done on these records. As per NIST (2022) guidelines, audit trails should be tampered with proof, transparent and repeatable. Audit trails are needed in several investigation types, such as:

- **Internal Investigations:** in corporate environments, audit-trails play a key role in employees' misconduct, dismissals, data breaches, or policy violations. Research highlights that organizations often rely heavily on the manual logs, which are prone to human error and undermine credibility of the facts and findings (NIST,2022).
- **Compliance and Regulatory Audits**: In few sectors, such as healthcare, hospitality and finance, internal inquiries and investigations are also required to meet regulatory requirements and compliance with international standards such as HIPPA, GDPR etc. (Goldstraw-White, 2022).
- **Court Proceedings**: In Judiciary, digital evidence tracking logs are essential for admissibility of evidence. Judges need proof that evidence has not been tampered, mishandled and requires detailed comprehensive logs from collection to presentation so these can be trusted and accepted. The UK Forensic Research Regulator (Wortley, N. 2023) mandates that evidence must be defensible with proper tracking logs. Without this evidence, it may be excluded or challenged for further investigation and inquiries.
- **Research and Academic Contexts**: In academic contexts and research environments, tracking logs are equally important where reproducibility and transparency of digital footprint is essential. (Sitma,2024) addresses that most of the forensic tools lack automated change logs, which make replication difficult and reduce the level of trust in published studies. (McKeown and Buchanan) further point out that without proper validations and verifiable records, comparative studies of cryptographic hashing techniques risk inconsistency and cannot benchmarked reliably. "Audit trails therefore support not only integrity but also the credibility of academic contributions."

2.4 Usability of Forensic Tools

In forensic research and investigations many tools rely on command line scripts, programming languages that require more dependencies as pre-requisite, which can be difficult for non-technical users and require expertise. Studies addresses that there is lack of GUI based system and tools that analyst prefer to use for clear and consistent workflows along with reporting and error handling features (Stima, 2024).
Recent reviews address that some tools do offer advanced features, accessibility but ease of use and analyst-centric systems are still limited, with lack of advanced technology, such as distributed ledger technology (DISC InfoSec, 2023). This usability gap reduces consistency, adoption and increases the risk of mistakes as it requires ability to use and manage evidence.

2.5 Comparison of Current Technologies in Evidence Verification Framework

Comparison of the current forensic tools that use different infrastructures and technologies for digital records anchoring, support blockchain and cloud.

Tool	Algorithm support	Blockchain Anchoring	Report Export	Offline Support	Deferred synchronization	Portability
Forensic TransMonitor	SHA-256, MD5	Ethereum-based	Yes	No	No	Cloud Based Only
Chain of Custody Blockchain Systems	Keccak-256	Yes	No	No	No	Internet / Network Dependent
Decentralized Evidence Management System (BEMS)	Standard Algorithms	Yes	Yes	No	No	Enterprise bound
Robust Evidence Management Framework	Standard Algorithms	Yes	Limited Formats	No	No	Web-based

[Table 2.1] Current Forensic framework digital records verification tools

- **Forensic TransMonitor** supports multi-algorithms and blockchain technology, however it is internet bound and uses cloud infrastructure.
- **Chain of Custody Blockchain Systems** restricted to Keccak-256 cryptographic algorithm and lack comprehensive audit trail reports to exports. Like other tools, this is also network dependent to function.
- **Decentralized Evidence Management Systems (BEMS)** does support multiple forensic standard algorithms, but it is limited to enterprise use only and does not support portable functionality and require consistent network connection.
- **Robust Evidence Management Framework** integrates distributed ledger technology and supports multiple hash algorithms, but it cannot be used in secure environments or on-field deployment as it requires continuous network connectivity to function, and it is web-based only.

Tools discussed in the literature do support immutable ledger, audit trail and cloud infrastructure but limited and missing out the offline functionality, detailed tracking of digital footprints and portability. This highlights significant limitations in the current forensic practicing tools and needs a solution that can bridge this gap.

2.6 Comparison of Widely Used Forensic Tools

Below are some of the widely used tools currently for forensic verification evidence to compare strengths, and lacking capabilities, limitations etc.

Tool	Strengths	Lacking Capabilities
Autopsy	Free to use, easier for disk analysis and extensible	Limited Audit trail and does not support blockchain technology
EnCase	Comprehensive acquisitions, widely accepted in forensic research and court-accepted	No blockchain verification, expensive and closed source
FTK	Strong Reporting and commonly used for disk imaging and chain of custody	Limited integration with blockchain
X-Ways	Efficient, easier to use and lightweight	Do not support immutable ledger
Magnet AXIOM	Cloud Focus and Mobile	Metadata is not supported and immutable, anchoring is limited
Cellebrite UFED	Widely used in Mobile extraction	Proprietary and no integration to cloud or blockchain
Chainalysis Reactor	Blockchain analytics and used for crypto	It is not designed to support forensic evidence verification
BlockSci	Blockchain analysis used commonly in academics	Designed to use in secure labs and not user-friendly
VeraCrypt	Integrity protection and encryption	Do not support anchoring records, and no audit trails
OpenTimestamps	Proof of existence used via Bitcoin	Lack forensic extraction, narrow scope

Table 2.2: Current Tools comparison, commonly used in Forensic evidence verification.

Above comparison of the current tools that are used widely in current forensic digital records anchoring and verification, either lacking the comprehensive audit trail, immutable ledger integration, not analyst friendly to use, proprietary and lacking capabilities that can be legally defensible. These challenges clearly highlight and demand a solution that unifies the cryptographic hashes, immutable ledger technology integration, offline resilience, exportable and verifiable comprehensive audit trail and portable solutions that can be used regardless of the environment.

The LedgerLock application is positioned to bridge this critical gap with best methodological and technical practices to deliver the solution that is easy to use, analyst centric, portable, and accepted academically and in legal context.

2.7 Research Gap

This literature review clearly addresses limitations and challenges of the existing forensic evidence verification framework tools and reveals, current solutions do not support deferred synchronization, portability, and offline functionality. Investigators and analysts working in offline environment cannot use these tools and generate defensible reports and must switch between different multiple tools to work.
LedgerLock GUI portable application bridge this gap by combining multiple cryptographic hash algorithms, anchoring digital records on immutable ledger to provide audit trails with offline resilience.

3 Methodology

This chapter highlights the design and methodology adopted for this research and evaluation of the proposed forensic framework.

3.1 Research Approach

This research adopts design science methodology, which focuses on the development and evaluation of the artifact that solves the identified problems (Hevner et al., 2004). In our case artifact is a GUI-based framework application, an analyst-centric portable solution that integrates anchoring evidence, storing the full audit trail on distributed ledger system, and verifying the digital footprints against expected and generated cryptographic hash. Design science methodology is more suitable because it emphasizes relevance of problem and ensuring that proposed solution addresses real-world forensic gaps.

3.2 Alternative Methodologies

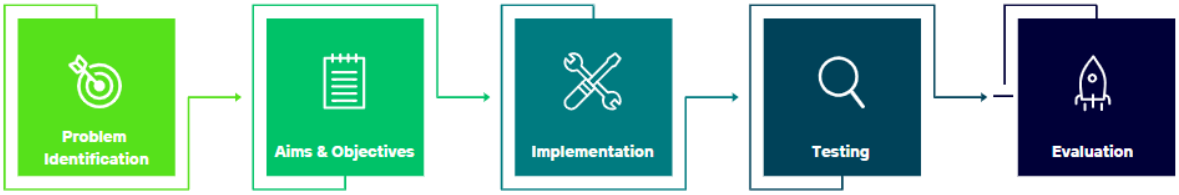
This project adopts a rigorous approach, supporting both creation and validation of the application development to ensure it is academically relevant and supporting the forensic framework, where application can be portable, used without elevated permissions, installations on client or systems. To support this, several methodological paradigms considered during the development and application planning phase.

- **Case Study Approach:** it is useful and related to aims and objectives of this thesis but limited to producing generalize tool rather than focusing on context specific and building new artifacts.
- **Experimental Research:** This research methodology focuses on the hypothesis testing through controlled trials and implementations, which is suitable for the forensic investigation techniques but lacks guidance and flexibility for the development of any novel tool creation and interface (Miles, K.L et el, 2020).
- **Agile Software Development:** This methodology is extremely popular and used for prototyping and software development in refining and tool testing. This supports modular features, delivery, and user cantered design, which encourage application testing, peer review, flexibility of the tool design and adaptability. (Staron, M. 2025).
- **Design Science Research (DSR):** This methodology is used developing innovative applications and for solving real-world problems to contribute academic knowledge (Gharaibeh, et el. 2024).

Exploring the limitations and alternative methodologies, this research adopts a Design Science Research (DSR) methodology, which is tailored and widely recognized in computer science for creating innovative artifacts that provide solutions for real-world problems. DSR methodology emphasizes rigorous evolution and construction of functional tools, resilience, utility, relevance, and contribution to knowledge as well (Hamid & Rahman, 2024).

3.3 Research Design Cycle

This methodology follows the design science research cycles defined as:



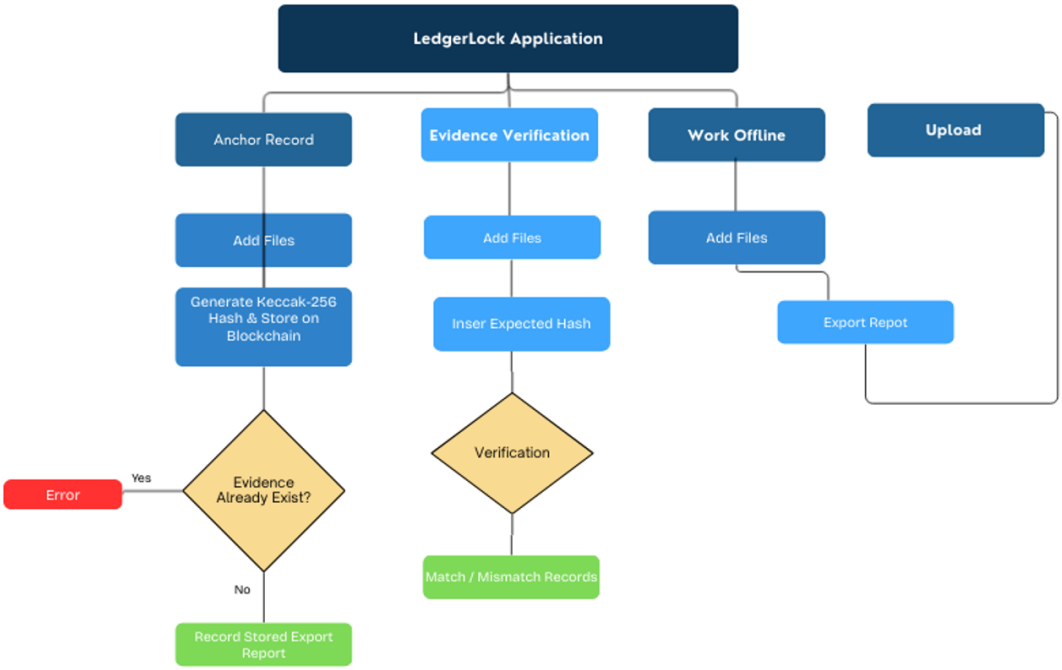
1. **Problem Identification:** Clear gap identified in digital footprints audit trail generation, usability, risk, and lack of integration.
2. **Aims & Objectives:** Develop a portable solution that provides comprehensive audit trail during anchoring digital evidence and support multi-algorithm verification system reduces time and effort of analysts to switch between multiple tools. Allow deferred synchronization to update the records later with file export functionality when network connection is available as per environment.

3. **Implementation:** implement a system using programming language that supports portability and easier integration with distributed ledger system.
4. **Testing & Demonstration:** Conduct rigorous testing with forensic datasets by verifying and anchoring with sample digital records and storing the hashes on the Sepolia Testnet network using smart contract and integration.
5. **Results and Evaluation:** Asses the results, accuracy, performance, and defensibility through rigorous testing in multiple different environments.

3.4 Application Design and Workflow

The proposed framework application designed as a portable solution GUI based forensic tool, integrates and store hashes on distributed ledger technology.
The design emphasizes:

- **User Friendly design:** Single portable application to support multiple features such as anchoring records, evidence verification and offline workflow.
- **Blockchain Integration:** Anchor digital records using the application to generate cryptographic hash, validate if hash recorded on the blockchain and stored on the blockchain for complete audit trail along with transaction id, block, gas used, meta-data etc.
- **Verification of Digital records:** Allow multiple cryptographic algorithms approach for diverse forensic standards to use, such as SHA-256, Keccak-256 and MD5 etc.
- **Audit Trail Generation:** Export reports in csv and pdf once either single or batch of multiple files anchored or verified to provide the full information including transaction block, timestamp, sender, recipient and block number, hash etc.
- **Offline and Differed Synchronization feature:** Built offline functionality to compute cryptographic hashes and generate audit logs that can be exported and stored on the blockchain once network is restored.



[Figure 3.1] Proposed Application LedgerLock – Main Workflow diagram

3.5 Application Architecture

Proposed application follows structured design to support both features anchoring and verification digital footprints ensuring modular design scalability and ease of use.

- **Presentation Layer:** Tkinter GUI for ease of use and interaction
- **Application Layer:** Python Programming Language libraries and modules to compute cryptographic hashes, threading and follow structed error handling and exception practices.
- **Distributed Ledger Technology:** Python Web3.py module for integration, Sepolia testnet network to deploy and use smart contract.
- **Data Layer:** comprehensive audit trail to export reports in .pdf/ .csv formats.

3.6 Evaluation Strategy

Evaluation will be focused on the technical accuracy, usability and defensibility of the application based on the verification of digital footprints obtaining the correct cryptographic hashes producing through application and validating to confirm if the evidence matches or mismatches. Retrieving data from the blockchain platform to confirm that digital record was anchored by whoever, when with full audit trail. Defensibility of the application will validate by generating reports as per NIST (2022), ISO/IEC 27037, and UK Forensic Science Regulator (Wortley, N. (2023) standards.

4. Implementation

This chapter explains technical details and implementation of the proposed application in this research project. The LedgerLock application is designed and developed to address highlighted challenges and support both verification and anchoring of digital records focusing legal defensibility through comprehensive audit trail, usability, and portability.

[Figure 4.1]: Application Main Dashboard

4.1 Application Architecture

The LedgerLock application implemented using Python 3.11 Programming language, because of its extensive library support, compatibilities across multiple operating systems and active community support. This system integrates:

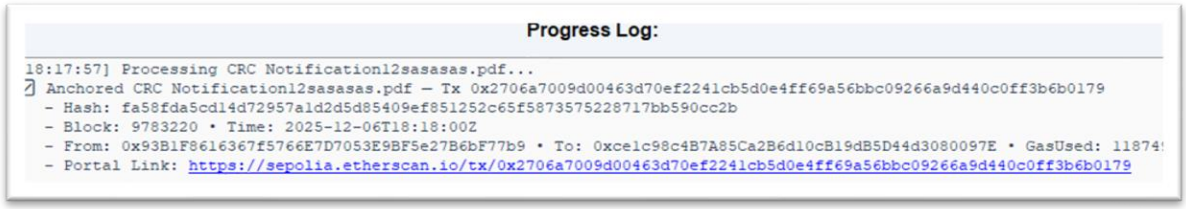
- **Cryptographic Hash Modules:** Compute Keccak-256, MD5 and SHA-256 Hash codes to validate integrity of the documents. Pysha3 python module is used to oversee Keccak-256 hash.
- **Portability and GUI:** Tkniter implemented for responsive dashboard, supports easy navigation, single and batch workflows.

```
try:
    w3 = Web3(Web3.HTTPProvider(INFURA_URL))
    account = w3.eth.account.from_key(PRIVATE_KEY)
    contract = w3.eth.contract(address=CONTRACT_ADDRESS, abi=ABI)
except Exception as e:
    messagebox.showerror("Blockchain Error", f"Web3 initialization failed: {e}")
    w3, account, contract = None, None, None
```

[Figure4.2] Use of web3.py file and smart contract deployed details, wallet-address etc.

4.2 Blockchain Integration

LedgerLock integration into immutable ledger technology is the core component along with offline functionality, which connects to the Sepolia network via Infura using python library Web3.py. This is used to store hashes and metadata of the digital footprints. To integrate this, custom solidity smart contract was deployed using Remix Ethereum IDE. On successful transaction anchoring digital records, system retrieves the transaction hash, timestamp details, metadata such as block number, gas used that provide a link to the blockchain portal to display the full audit trail, information of sender and receiver too.



[Figure 4.3]: Showing a sample record anchored and process logs.

This validation ensures that forensic evidence is dependently verifiable via public ledger blockchain and records are immutable.

4.3 Offline Workflow

The application support differed synchronization functionality to operate offline, allowing researchers to add records and compute hashes. Once all digital records are hashed, it allows the report with full meta-data that can be uploaded once connection is available to the network and provides full audit trail and details, storing hashes of the digital evidence on immutable ledger.

4.4 Audit Trail Generation

One of the main objectives of this research is to provide a forensic framework that produces defensible audit trail after each evidence anchored. To ensure system complies with standards, application generates this information by providing transaction code that used to store meta data and hash the record on the blockchain. It also provides a clickable URL link, where analysts can verify all details along with options to export either csv or pdf reports to save all the information. This is completely aligned with the requirements outlines by the UK Forensic Science Regulator (Wortley, N. 2023), that mandate the digital records handling should be logged, documented and in reproduceable manner.

4.5 Application Code and Error Handling

The system implemented with comprehensive error handling, exceptions, and rigorous checks to support real-time and on field forensic use. If files or evidence are already anchored, system will produce an error to show that this record already existed to prevent duplication. Unsupported files, connections failures also overseen gracefully with retry and analyst feedback logic to ensure system remains stable and dependable considering aspects.

4.6 Deployment

This framework was designed and implemented to support portability, and entire application packaged into a single executable file using PyInstaller. It allows researchers to use this application without installation and any additional dependencies or external libraries. It only requires an internet connection to anchor all the evidence on the immutable ledger to store hashes and produce the comprehensive audit trail. In offline workflow, it can provide the full data file that can be used and uploaded once network is available.

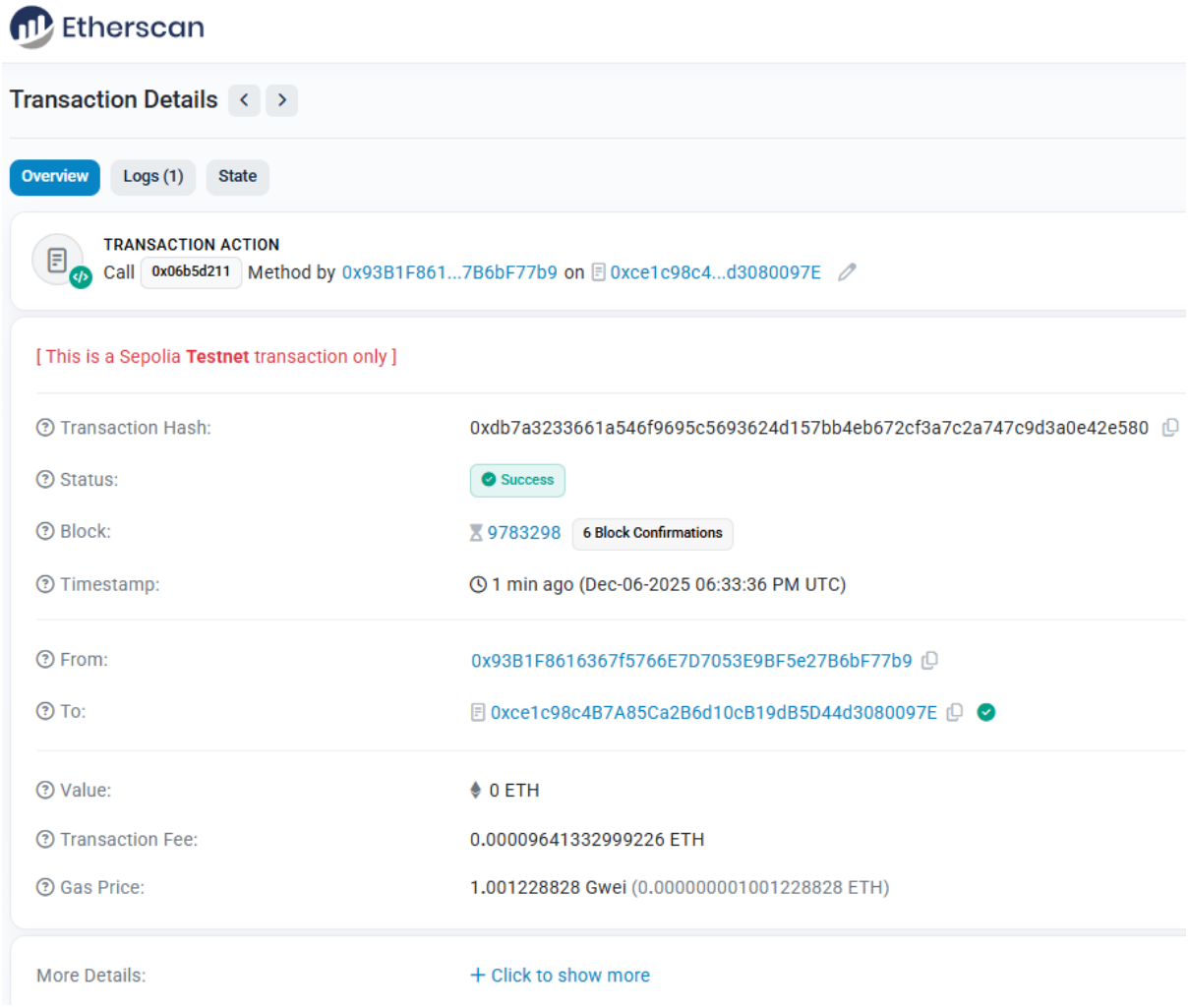
This design and deployment shows, LedgerLock application supports both workflows online and offline comprehensively.

5. Evaluation

This chapter evaluates proposed LedgerLock application based on three dimensions; Technical accuracy, legal defensibility, and usability to ensure application meets the objectives and forensic standards.

5.1 Technical Accuracy

Technical accuracy of the application (LedgerLock) validated in both functionalities Verification of the digital record against expected hash and anchoring. Verification accuracy was evaluated through computing cryptographic hashes for the dataset digital footprints. Each record processed and verified against SHA-256, Keccak-256 and MD5 hash codes. Output was verified against expected hash and current hash of the record to show it match or mismatch. However, anchoring was verified through transactions submitted on the Seplia testnet network and cross-checking details with Etherscan.



[Fig 5.1] Anchored digital records data tested and checked on Sepolia testnet Etherscan platform.

5.2 Application Usability

LedgerLock application usability was evaluated through both functionalities by performing multiple anchoring and verifying digital footprints against the traditional command-line interfaces. However, this application does not require any pre-requisites and does not depend on any other dependencies however other command line tools require special libraries and expertise to perform similar tasks. The Graphical User Interface was found interactive and easy to navigate with clear workflows. This application can perform and provide full comprehensive audit trail, which does not require users to move between different multiple applications and reduce minimal human intervention that make this application more user-friendly and allow export reports in both csv and pdf formats with full meta-data.

5.3 Legal Defensibility

Audit trails generated by the LedgerLock application were as per the requirements outlined in UK Forensic Regulator (Wortley, N. 2023) and ISO/SEC 27037 and NIST (2022). That requires file name, verification result, computed hash and blockchain metadata along with link to verify the details on Etherscan, so record can be independently verified. This strengthens the defensibility of the forensic analysts and application to be used in the field following forensic standards and compliance mechanisms.

5.4 Offline workflow

Offline capabilities of the LedgerLock application evaluated during disconnecting network. Sample dataset of files anchored to compute different hashes and generate report in json/csv format to synchronize later while connecting back to the network. Deferred synchronization successfully updated using the exported file and retrieved the all metadata from the blockchain that provide the transparent and comprehensive audit trail.


{"evidence_id": "3b890fa1-a0c1-4cd4-8a6a-fe2723f8221d", "filename": "1.pdf", "filetype": ".pdf", "hash_algorithm": "MD5", "hash_value": "e542479ef295ea40e439621b0b25044e060ccfd95dc3f5db534d3cac9b92d37a", "collected_at": "2025-12-06T18:33:01.637069"}
{"evidence_id": "d7ee825c-4a8d-475c-ae7a-c0792d26626e", "filename": "CRC Notification12sasasas.pdf", "filetype": ".pdf", "hash_algorithm": "MD5", "hash_value": "e252b3e402d94442c6dc25dd66a1373ac4f9a598bdead8ff0a89f3648656e10a", "collected_at": "2025-12-06T18:33:01.637069"}
{"evidence_id": "957f48a6-d18f-421d-b44d-cfa9bf339d10", "filename": "r.pdf", "filetype": ".pdf", "hash_algorithm": "MD5", "hash_value": "b128020ff248c39a4f42d58ba555599d", "collected_at": "2025-12-06T18:33:01.637069"}

[Fig 5.2] multiple sample files hashed during offline workflow and exported data in JSON format.

5.5 Discussion

The development of LedgerLock application clearly demonstrates how distributed ledger technology can be used and implemented in digital forensic practices to ensure digital records integrity, reproducibility, and legal defensibility. Anchoring digital footprints, storing hashes on the Sepolia Testnet network, and providing verification blockchain and evidence-based hashes empower analysts with immutable and comprehensive audit trail.

The integration of differed synchronization highlights and addresses the system capabilities and adaptabilities to the real-world forensic problems and environments where connectivity can be a problem and intermittent. This feature ensures and proves that evidence can still be auditable, captured in real-time and later it can be anchored with all the meta-data that was created and exported during the evidence anchoring in offline mode.

Nevertheless, this discussion does acknowledge the challenges and limitations. The current implementations are restricted to testing blockchain networks, which does not fully replicate the scalability, usability and cost challenges during the deployment and usage of the application while anchoring the digital records. Hashing was also limited to SHA-256, Keccak-256 it can also be expanded too.

These challenges directly point out the work required on this to be conducted in future including multi-blockchain technology, legal evaluation, testing, scalability, performance, stress testing, and advanced hashing. Overall, LedgerLock application shows the immutable ledger technology anchored, and verification is both feasible and academically defensible. This research lays the groundwork for future researchers to expand into broader forensic, compliance and legal defensibility.

5.6 Evaluation Summary

Gaps identified and challenges highlighted in chapter two along with forensic verification comparison technologies (Table 2.1 and 2.2) lacking portability and offline functionality have been clearly addressed and bridged by LedgerLock application. It provides comprehensive audit trail while disconnected from the network and upon restoration that represents a significant advancement in forensic practice supporting portable functionality without any dependency. This empowers forensic researchers to maintain the integrity of digital footprints and defensibility even in secure and restricted environments.

This evaluation summarizes that LedgerLock application can be used and relied on to reduce the manual interventions with full comprehensive audit trail, audit trail with deferred synchronization functionality.

6 Conclusion and Future Work

6.1 Conclusion

This research addresses critical limitations and challenges in current forensic practices and bridges these gaps by developing a fully functional portable application along with implementations of offline functionalities and deferred synchronization into immutable ledger technology. It clearly shows that the records anchored are forensically auditable, traceable and application can be used in secure environments. This research has clearly filled this gap by providing complete solutions to empower research and analysts.

This application has been critically evaluated and shown to be technically aligned with forensic standards, user-friendly, analyst centric and accurate. LedgerLock application enhances reproducibility, legal defensibility and transparency with hashing verification and anchoring. It provides comprehensive reports as per forensic, legal standards and requirements.

The contribution of this research lies in GUI functionality with deferred synchronization, portability and integration of immutable ledger that bridges forensic requirements with technical innovation. It empowers analysts in law enforcement, research, and legal compliances by delivering comprehensive, defensible audit trail and independent verification mechanisms.

6.2 Limitations

LedgerLock application clearly demonstrates significant advancements in forensic anchoring digital footprints practices. However, there are several limitations that can be improved such as:

- Application currently relies on Sepolia testnet network, which is a test environment not production environment. This choice was made to reduce the transactions cost during the development and required for anchoring records on blockchain.
- System currently does not support multiple blockchain networks.
- System designed does not support case management and login features to use this application securely.
- Anchoring digital footprints only used with Keccak-256 cryptographic hash.

6.3 Future Work

This project addresses and invites researchers to explore further and improve this framework by extending and utilizing multiple blockchain networks. Furthermore, deployment of this application on-field and more usability may bring more challenges that are not captured in this evaluation and research but will help this to make it more advantageous tool for analysts. However, apart from these, there are many other areas that can be extended and improved further.

LedgerLock application scalability, running stress tests using thousands of files, testing with multiple batches of larger datasets will prove the accuracy, time duration, optimization and can explore further options that can be looked at. Usability of the application is also necessary, specifically used on-field and by law enforcement agencies including forensic researchers and their feedback.

7 References

1. NIST (2022), *Digital Investigation Techniques: A Scientific Foundation Review*. NIST IR 8354, Available at: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354.pdf, (accessed 17 July 2025).

2. Olukoya, O. (2021) Distilling Blockchain Requirements for Digital Investigation Platforms', *Journal of Information Security and Applications*, 62, 102969, available at: https://doi.org/10.1016/j.jisa.2021.102969, (accessed 20 July 2025).

3. Kim, D., and Son, Y. (2021) Two-Level Blockchain System for Digital Crime Evidence Management', Sensors, 21(9), p. 3051. doi: 10.3390/s21093051, (accessed 17 July 2025)

4. Sowmya, K.N., Singh, S., Chennamma, H.R., Kumari, S., and Shivani (2025) Securing Evidence in Digital Forensics Using Blockchain', in *Advances in Data Science and Artificial Intelligence*. Springer, pp. 395–408, Available at: https://doi.org/10.1007/978-981-96-4430-8_28, (accessed 17 July 2025).

5. Atlam, H.F., Ekuri, N., Azad, M.A. and Lallie, H.S. (2024) Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions', *Electronics*, 13(17), 3568, available at: https://doi.org/10.3390/electronics13173568, (accessed 25 July 2025)

6. Johri, S. (2024) 'Strengthening Digital Forensics with Blockchain Technology and Algorithms', World Journal of Advanced Research and Reviews, 24(2), pp. 459–467. doi: 10.30574/wjarr.2024.24.2.3317, accessed (25 July 2025)

7. Jerald, J. (2023) *File Integrity Verifier (FIV): A Lightweight Python-based Digital Forensic Tool*. GitHub Repository. Available at: https://github.com/jerald-6/File_Integrity_Verifier_FIV (accessed, 28 July 2025).

8. Salih, K.M.M. and Ibrahim, N.B. (2023) 'Digital Forensic Tools: A Literature Review', Journal of Education and Science, 32(1), pp. 109–124, available at: https://doi.org/10.33899/edusj.2023.137420.1304, (accessed 28 July 2025).
9. McKeown, S. and Buchanan, W.J. (2023) Hamming Distributions of Popular Perceptual Hashing Techniques', Forensic Science International: Digital Investigation, 44, 301509. Available at: https://doi.org/10.1016/j.fsidi.2023.301509, (accessed 01 August 2025)
10. Goldstraw-White, J. (2022) Legal and Policy Framework for Digital Forensics: A Resource for Practitioners. University College London. Available at: https://perpetuityresearch.com/wp-content/uploads/2022/09/Final-Legal-Procedural-and-Guidance.pdf, (Accessed 15 August 2025).
11. Wortley, N. (2023). Forensic Science Regulator: Code of Practice. Criminal Law Week, 2023(13), 8-10. Available at: https://www.gov.uk/government/publications/statutory-code-of-practice-for-forensic-science-activities/forensic-science-regulator-code-of-practice-accessible, (accessed 15 August 2025).
12. Sitima, J. (2024) Understanding Digital Forensic Tools: Their Features, Applicability and Key Shortcomings', International Journal of Forensic and Management Research, 6(30026). Available at: https://www.ijfmr.com/papers/2024/6/30026.pdf, (accessed 15 Sept 2025).
13. Hamid, M., and Rahman, A. (2024) Digital Forensics Meets Blockchain: Enhancing Evidence Authenticity and Traceability', IEEE Access. doi: 10.1109/ACCESS.2024.10532961, (accessed 28 Sept 2025)
14.
15. DISC InfoSec (2023) Most Important Computer Forensics Tools for 2023. Available at: https://blog.deurainfosec.com, (accessed: 28 Sept 2025).

16. Hevner, A.R., March, S.T., Park, J., and Ram, S. (2004) 'Design Science in Information Systems Research', *MIS Quarterly*, 28(1), pp. 75–105, (accessed 28 Sept 2025).

17. ISO (2012) *ISO/IEC 27037: Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. International Organization for Standardization, (accessed 28 sept 2025).

18. Miles, K.L., Stray, V., Hoda, R., Paasivaara, M. & Kruchten, P. (2020). Agile Processes in Software Engineering and Extreme Programming: Proceedings of the 21st International Conference on Agile Software Development (XP 2020), Copenhagen, (accessed 10 Oct 2025)
19. Staron, M. (2025). Agile in 2025: Embracing a Mindset Over a Method. LucidTrac Blog. Available at: https://lucidtrac.com/blog/read/Agile_in_2025_Embracing_a_Mindset_Over_a_Method, (accessed 18 Oct 2025).
20. Gharaibeh, L., Mandviwalla, M., Söllner, M. & Tuunanen, T. (2024). Design Science Research for a Resilient Future: Proceedings of the 19th International Conference on Design Science Research in Information Systems and Technology (DESRIST 2024) (accessed 01 November 2025)

AI Acknowledgement Supplement

[**Research Project**]

[Thesis]

Your Name/Student Number	Course	**Date**
Sajid Hussain Jatoi / X23265736	**MSCCYBE_JANO24_O**	11/12/2025

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool
N/A	N/A	N/A

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. One table should be used for each tool used.

[Insert Tool Name]	
[Insert Description of use]	
[Insert Sample prompt]	[Insert Sample response]

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Additional Evidence:

[Place evidence here]

Additional Evidence:

[Place evidence here]