A PROJECT REPORT ON

"OBSIDIAN CIRCUIT"

Submitted for the fulfillment of the award of the degree

BACHELOR OF TECHNOLOGY
(Computer Science & Engineering)
BY

Roque Leon Martins	MITU22BTCS0664
Kathan Somani	MITU22BTCS0379
Soham Jagtap	MITU22BTCS0842
Aryan Dsouza	MITU22BTCS0160

Under the guidance of

Prof. Dr. Prashant Dhotre

Department of Computer Science and Engineering

MIT School of Computing

MIT Art, Design and Technology University, Pune

MAEER's Rajbaug Campus, Loni-Kalbhor, Pune 412201

November, 2024

MIT-ADT
UNIVERSITY
PUNE, INDIA.
(Established by Govt. of Maharashtra by MIT ADT University Act No. XXXIX of 2015)
A leap towards World Class Education

MIT SCHOOL OF COMPUTING

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

MAEER’s Rajbaug Campus, Loni-Kalbhor, Pune - 412201

CERTIFICATE

This is to certify that the project report entitled

“OBSIDIAN CIRCUIT”

Submitted by

Roque Leon Martins	MITU22BTCS0664
Kathan Somani	MITU22BTCS0379
Soham Jagtap	MITU22BTCS0842
Aryan Dsouza	MITU22BTCS0160

is a bonafide work carried out by students under the supervision of Prof. Dr. Prashant Dhotre and it is submitted towards the fulfillment of the requirement of MIT-ADT University, Pune for the award of the degree of Bachelor of Technology (Computer Science & Engineering)

(Prof. Dr. Prashant Dhotre)
Guide

Prof. Dr. Prashant Dhotre	Prof. Dr. Rajneeshkaur Sachdeo	Prof Dr. Vipul Dalal
Head of Department	Dean	Director

Seal/Stamp of the College
Place : Pune Date: 22nd November 2024

DECLARATION

We, the team members

Name	Enrollment No
Roque Leon Martins	MITU22BTCS0664
Kathan Somani	MITU22BTCS0379
Soham Jagtap	MITU22BTCS0842
Aryan Dsouza	MITU22BTCS0160

Hereby declare that the project work incorporated in the present project entitled "Obsidian Circuit " is original work. This work (in part or in full) has not been submitted to any University for the award or a Degree or a Diploma. We have properly acknowledged the material collected from secondary sources wherever required. We solely own the responsibility for the originality of the entire content.

Date:

Roque Leon Martins

Kathan Somani

Soham Jagtap

Aryan Dsouza
Name & Signature of the Team Members

Prof. Dr. Prashant Dhotre

Name & Signature of the Guide

Seal/Stamp of the College
Place : Pune Date: 22nd November 2024

MIT-ADT
UNIVERSITY
PUNE, INDIA
A leap towards World Class Education

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

MIT SCHOOL OF ENGINEERING,

RAJBAUG, LONI KALBHOR,

PUNE – 412201

EXAMINER’S APPROVAL CERTIFICATE

The project report entitled **“OBSIDIAN CIRCUIT”** submitted by **ROQUE LEON MARTINS (MITU22BTCS0664), KATHAN SOMANI (MITU22BTCS0379), SOHAM JAGTAP (MITU22BTCS0842) AND ARYAN DSOUZA (MITU22BTCS0160)** in partial fulfillment for the award of the degree of **“Bachelor of Technology (Computer Science & Engineering) ”** during the academic year 2019-20, of **MIT-ADT University, MIT School of Engineering, Pune,** is hereby approved.

Examiners:

1.

2.

ACKNOWLEDGEMENT

I express my profound thanks to my Guide **Prof. Dr. Prashant Dhotre,** for her expert guidance, encouragement, and inspiration during this project work.

I would like to thank **Prof. Suruchi Deshmukh**, Project Coordinator, Department of Computer Science & Engineering for extending all support during the execution of the project work.

I sincerely thank **Prof. Dr. Ganesh Pathak**, Head, Department of Computer Science & Engineering, MIT School of Engineering, MIT-ADT University, Pune, for providing the necessary facilities to complete the project.

I am grateful to **Prof. Dr. Rajneeshkaur Sachdeo**, Dean, MIT School of Engineering, MIT-ADT University, Pune, for providing the facilities to carry out my project work.

I also thank all the faculty members in the Department for their support and advice.

Roque Martins MITU22BTCS0664

Kathan Somani MITU22BTCS0379

Soham Jagtap MITU22BTCS0842

Aryan Dsouza MITU22BTCS0160

Abstract

The rapid growth of cyber threats has made digital forensics and incident response (DFIR) a critical area for ensuring cybersecurity. Traditional forensic tools face challenges such as tampering risks, inefficient analysis processes, and lack of automation, which hinder timely and accurate investigations. This project presents a comprehensive DFIR tool leveraging modern technologies like blockchain, IPFS, AI/ML, and full-stack web development to streamline forensic workflows and enhance evidence security.

The tool enables investigators to securely upload and analyze evidence, including disk images, network traffic, and system logs. Features such as metadata extraction, network anomaly detection, and log analysis are powered by AI/ML algorithms to provide automated insights and detect Indicators of Compromise (IOCs). Evidence is stored on IPFS for decentralized, tamper-proof storage, while blockchain ensures traceability through immutable audit logs. Real-time integration with external threat intelligence platforms like VirusTotal further enhances threat detection capabilities.

The tool also generates detailed, compliance-ready reports, making it an invaluable resource for forensic investigators, enterprise security teams, and law enforcement. By combining automation, security, and scalability, this project addresses critical gaps in existing forensic tools and sets a foundation for future advancements in the field.

CONTENTS

CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION:-

Within the context of cybersecurity, digital forensics encompasses a variety of techniques aimed at helping investigators look into incidents that include digital evidence. However, with more sophisticated challenges posed by cyber threats and an increase in digital data, traditional forensic aids face problems such as risks of tampering, poor management of data, and complicated processes. Such problems usually result in enhanced time consumption and less effectiveness of the evidence presented.

This project introduces a Digital Forensics and Incident Response (DFIR) tool designed to overcome these challenges. The technology adopts a blockchain system to store digital evidence to avoid loss or damage and maintain a distributed data structure. It has an easy-to-use interface designed using React, which allows analysis of system logs, network captures, and disk images, among other types of data.

The DFIR tool, by introducing automation in some, processes such as collection of evidence and analysis of its metadata, benefits investigations at the cost of human effort. The breadth and depth of its reporting power provide the ability to prepare full reports for the investigators that meet compliance conditions. This innovative solution aspires to improve the efficacy, precision, and safety of digital forensics processes as per the increasing needs of today’s cyber world.

1.2 EXISTING WORK:-

Sr.No	Title	Description	Limitations
1	Autopsy Digital Forensic Platform	Open-source forensic tool for analyzing file systems, timelines, and retrieving deleted data	Limited advanced features compared to commercial tools; no decentralized or blockchain storage support.
2	EnCase Forensic Toolkit	A comprehensive tool for collecting, analyzing, and reporting digital evidence from various sources like computers, servers, and mobile devices.	Expensive and resource-intensive, with a steep learning curve for new users.

1.3 MOTIVATION:-

In today's rapidly evolving digital landscape, the complexity and frequency of cyber threats have increased dramatically. Cyberattacks are no longer limited to large organizations; they now target individuals, small businesses, and governments alike. This escalation has created an urgent need for more efficient, secure, and automated tools to respond to these sophisticated threats.

1. **Sophistication of Cyber Threats**:
   Traditional tools struggle to detect and mitigate modern, evolving cyber threats that are becoming more sophisticated and harder to trace. Investigators need new methods to stay ahead of attackers.
2. **Limitations of Traditional Forensic Tools**:
   Conventional forensic tools are often slow, prone to human error, and lack automation. Investigators must manually process vast amounts of data, which delays threat detection and increases the chances of missing critical evidence.
3. **Need for Speed and Automation**:
   As cyberattacks occur in real-time, investigators must respond quickly. The delay in identifying and mitigating threats can result in significant damage, making speed and automation crucial to successful incident response.
4. **Ensuring Evidence Integrity**:
   Digital evidence must be secure and tamper-proof, especially in legal contexts. Traditional evidence storage solutions are vulnerable to manipulation. Blockchain integration ensures that all digital evidence remains immutable and traceable.
5. **Empowering Investigators with Advanced Tools**:
   Automation and advanced analytics enable investigators to focus on high-level decision-making. By providing tools for automated threat detection and comprehensive reporting, Obsidian Circuit empowers users to act quickly and efficiently.

In conclusion, the development of **Obsidian Circuit** is motivated by the growing need for a tool that enhances digital forensic investigations. It addresses critical challenges such as slow response times, human errors, and the integrity of evidence, offering a secure, efficient, and automated solution for modern cybersecurity threats. By automating key processes and ensuring the integrity of digital evidence, it enables faster and more reliable responses to incidents, ultimately making the digital world safer for everyone.

1.4 OBJECTIVE:-

Enhance Cyber Incident Response:

Provide an efficient platform for security professionals to detect, analyze, and respond to cyber incidents in real-time, reducing investigation time and improving response rates.

Ensure Integrity of Digital Evidence:

Use Blockchain and decentralized storage (IPFS) to secure digital evidence, ensuring its immutability and traceability for legal and forensic purposes.

Automate Threat Detection:

Automatically identify Indicators of Compromise (IOCs) through advanced detection algorithms and integration with external threat intelligence APIs, enhancing the speed and accuracy of threat identification.

Provide Comprehensive Forensic Analysis:

Enable investigators to perform detailed file metadata analysis, network traffic analysis, and log analysis to uncover critical evidence and identify security incidents more effectively.

Generate Legally-Compliant Reports:

Automatically generate detailed, actionable, and legally-compliant reports that meet forensic and organizational standards, simplifying documentation and presentation of findings.

Increase Efficiency through AI-Powered Insights:

Utilize machine learning algorithms to analyze vast amounts of forensic data, highlighting potential threats and anomalies faster than traditional methods.

Facilitate Real-Time Evidence Collection:

Allow seamless uploading and secure collection of forensic artifacts (e.g., logs, disk images, .pcap files) for immediate analysis and evidence preservation.

Provide Traceability and Auditability:

Maintain detailed logs of evidence access and modifications using blockchain technology to ensure full traceability and accountability throughout the investigation.

Improve Threat Intelligence Enrichment:

Enhance incident detection by integrating threat intelligence sources like VirusTotal, AbuseIPDB, and OTX for real-time enrichment of IOCs.

Ensure Scalable, Secure Storage:

Leverage decentralized storage (IPFS) to provide scalable and secure evidence storage that is resistant to tampering and data loss.

Support Cross-Team Collaboration:

Enable collaboration between investigators, legal teams, and cybersecurity professionals through shared access to evidence and reports in a secure environment.

Reduce Human Error:

Minimize manual tasks and human error in the investigative process by automating data analysis and report generation, ensuring more accurate results.

1.5 SCOPE:-

Evidence Collection and Handling:

Support for multiple evidence types, including disk images (.img, .dd), network capture files (.pcap), and system/application logs (.txt, .log, .json).

Secure evidence upload and collection processes to ensure data integrity from the start.

Blockchain-Based Evidence Storage:

Implementation of a decentralized and tamper-proof storage system using blockchain technology to log evidence interactions and ensure data integrity.

Evidence will be stored on IPFS for decentralized, immutable, and secure storage.

Metadata Extraction and Analysis:

Extraction and analysis of metadata from collected evidence to track changes, file permissions, and ownership, helping investigators identify unauthorized alterations.

Manual Evidence Analysis (Without AI/ML):

The initial version focuses on manual processes for analyzing evidence without integrating AI/ML algorithms for anomaly detection.

Provides essential forensic analysis tools, such as timeline analysis and keyword searching, to identify suspicious activity.

Network Traffic Analysis:

Analysis of network capture files (.pcap) to detect anomalies such as unauthorized data transfers or abnormal communication patterns.

Includes integration with external threat intelligence sources for enhancing detection.

Report Generation:

Automatic generation of detailed forensic reports that include metadata, network analysis findings, log analysis, and blockchain evidence logs.

Reports will be exportable in PDF format, ensuring compliance with legal and regulatory requirements.

User Interface (UI):

A simple, intuitive user interface built with React to ensure ease of use for investigators with minimal technical expertise.

The interface will allow for evidence upload, analysis review, and report generation with minimal training.

Security and Compliance:

The tool will be designed with high-security standards, ensuring that evidence cannot be tampered with and that it adheres to forensic standards for admissibility in legal proceedings.

1.6 SUMMARY:-

Obsidian Circuit is a cutting-edge Digital Forensics and Incident Response (DFIR) tool designed to meet the growing demands of cybersecurity professionals in the face of increasingly sophisticated cyber threats. It integrates state-of-the-art technologies such as Blockchain, decentralized storage (IPFS), AI-powered insights, and real-time threat intelligence enrichment to deliver a holistic and secure platform for forensic investigations. This tool provides a seamless, automated approach to the entire incident response lifecycle, from evidence collection to detailed reporting, allowing investigators to act quickly and effectively in identifying and mitigating threats.

A key strength of **Obsidian Circuit** lies in its ability to ensure the integrity and traceability of digital evidence. Through the use of Blockchain and IPFS, the tool provides an immutable and tamper-proof record of all forensic evidence, preserving its authenticity throughout the investigation. This is crucial for legal proceedings, as investigators can be confident that the evidence collected and analyzed has not been altered in any way.

The tool's automated threat detection features empower investigators by quickly identifying Indicators of Compromise (IOCs) such as malicious IP addresses, file hashes, and URLs. These IOCs are cross-referenced with external threat intelligence databases like VirusTotal, AbuseIPDB, and OTX to provide real-time enrichment and context, ensuring that investigators have access to the most up-to-date and relevant information. This significantly enhances the accuracy and efficiency of the investigation, enabling quicker detection of potential threats.

In addition to threat detection, **Obsidian Circuit** offers a comprehensive suite of forensic analysis tools, including file metadata analysis, network traffic analysis, and log analysis. These features allow forensic experts to analyze critical data, such as file creation and modification times, network traffic patterns, and system log events, to identify malicious activity and track the progression of cyber incidents. The tool's ability to process large volumes of data with minimal human intervention not only speeds up the analysis process but also reduces the risk of human error, ensuring more accurate and reliable results.

Obsidian Circuit also simplifies the reporting process by automatically generating detailed, legally-compliant reports. These reports provide a comprehensive overview of the investigation, including findings from file metadata analysis, network traffic, log events, and threat intelligence sources, and are formatted in a way that is ready for presentation to legal or organizational stakeholders. This feature significantly reduces the time and effort required to document and present forensic findings, ensuring that investigators can focus on the more critical aspects of the investigation.

The platform is designed for real-time evidence collection, with a user-friendly interface that allows investigators to upload files such as disk images, network capture files (.pcap), and system logs. This evidence is securely stored on the IPFS, ensuring that it is both decentralized and protected from tampering. Additionally, **Obsidian Circuit** allows for cross-team collaboration, enabling forensic experts, cybersecurity professionals, and legal teams to work together in a secure, integrated environment. This collaborative feature ensures that the investigative process is transparent, organized, and efficient.

By leveraging AI-powered insights, **Obsidian Circuit** can analyze vast amounts of forensic data to detect anomalies, patterns, and threats that may not be immediately visible through traditional manual analysis. This allows investigators to prioritize their efforts on the most critical findings, reducing the time required for human analysis and improving overall efficiency.

In summary, **Obsidian Circuit** provides a robust, scalable, and secure solution for modern forensic investigations. Its seamless integration of Blockchain for evidence integrity, decentralized storage for security, automated threat detection for efficiency, and AI-driven insights for deeper analysis offers a powerful toolset for cybersecurity professionals. With features designed to simplify evidence collection, streamline analysis, and automate reporting, **Obsidian Circuit** enables faster, more accurate incident response, helping organizations mitigate risks and respond to cyber threats with greater confidence and precision.

CHAPTER 2
CONCEPTS AND METHODS

2.1 BASIC DEFINITIONS:-

Digital Forensics:

The process of collecting, preserving, analyzing, and presenting digital evidence to support legal or organizational investigations related to cyber incidents, fraud, or other illegal activities.

Incident Response:

The approach and procedures followed to handle and mitigate the effects of a cybersecurity incident, such as a breach, attack, or data theft, and to prevent further damage or data loss.

Indicators of Compromise (IOCs):

Evidence or signs that indicate that a system, network, or device has been compromised, such as unusual IP addresses, file hashes, URLs, or patterns of network traffic.

File Metadata Analysis:

The process of examining the metadata (data about data) of files to gain insights into file activities, such as creation dates, modification history, ownership, and permissions, which can help detect unauthorized changes or tampering.

Network Traffic Analysis:

The process of monitoring and analyzing network traffic, such as data packets and communications, to detect suspicious patterns or activities, including unauthorized access, data exfiltration, or Denial of Service (DoS) attacks.

Log Analysis:

The examination of system or application logs to identify events or actions that may indicate malicious activities or breaches, such as failed login attempts, unauthorized access, or abnormal system behavior.

Blockchain:

A distributed, decentralized ledger technology that records transactions or data in a secure, tamper-resistant, and transparent manner. In digital forensics, blockchain is used to log actions taken on evidence to ensure its integrity.

InterPlanetary File System (IPFS):
A decentralized file storage system that ensures files are stored securely and are tamper-resistant, allowing for decentralized data storage and retrieval across a distributed network of nodes.

VirusTotal API:
A service that allows users to check files, URLs, or IP addresses against a large database of known threats to identify malicious content. The API integrates threat intelligence from multiple sources to provide detailed analysis of potential threats.

AI-Powered Insights:
The use of Artificial Intelligence (AI) and Machine Learning (ML) algorithms to automatically detect anomalies, unusual patterns, and potential threats in data, network traffic, or user behavior, helping investigators prioritize and respond to incidents more efficiently.

Threat Intelligence:
Information about existing or potential cyber threats, including details about known malicious actors, IP addresses, files, URLs, and tactics used in attacks. This intelligence helps security teams detect and respond to cyber threats quickly.

Comprehensive Reporting:
The process of automatically generating detailed reports that summarize findings from forensic analysis, including metadata, network traffic, and threat intelligence. These reports are typically used for legal documentation, compliance, and further investigation.

Evidence Integrity:
The assurance that digital evidence has not been tampered with or altered since it was collected, ensuring its authenticity and admissibility in legal or organizational proceedings.

Decentralized Storage:
The practice of storing data in a distributed manner across multiple locations, instead of a centralized server, to reduce the risk of tampering, data loss, or unauthorized access.

CHAPTER 3

LITERATURE SURVEY

Sr. no	Literature Title	Author	Findings
1.	A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response	D. Dunsin, M. Ghanem, K. Ouazzane, and V. Vassilev	● Explores the potential of AI/ML in automating anomaly detection and identifying IOCs. ● Addresses challenges like data quality and model accuracy for practical implementation.
2.	An Assessment of Capabilities Required for Effective Cybersecurity Incident Management - A Systematic Literature Review	O. I. Falowo, K. Koshoedo, and M. Ozer	● Identifies essential capabilities for effective incident management, including detection and recovery. ● Highlights the need for better integration of threat intelligence and automation in incident response.
3.	A Filtering Model for Evidence Gathering in an SDN-Oriented Digital Forensic and Incident Response Context	M. B. Jiménez, D. Fernández, J. E. Rivadeneira, and R. Flores-Moyano	● Introduces a filtering model to enhance evidence collection in SDN environments. ● Focuses on improving data relevance and ensuring integrity during forensic investigations.

CHAPTER 4

PROPOSED SYSTEM

4.1 SYSTEM ARCHITECTURE:-

Frontend Layer:

- **Technologies Used:** React.js, HTML, CSS.
- **Function:** This layer serves as the user interface where forensic investigators upload, view, and interact with the evidence. It allows users to easily view the results of the analysis, metadata, logs, and other related details.
- **Components:** Upload functionality, dashboard for viewing evidence, analysis results, and reports.

Backend Layer:

- **Technologies Used:** Node.js, Express.js.
- **Function:** Handles the server logic, processing evidence uploads, making API calls, and managing communication between the frontend and backend. It’s responsible for performing automated analysis (detecting IOCs) and interacting with the blockchain for evidence storage.
- **Components:** API server for handling user requests, file processing logic, IOC scanning, and data validation.

Automated Analysis Layer:

- **Technologies Used:** Backend server, Analysis libraries.
- **Function:** This layer scans uploaded data for Indicators of Compromise (IOCs) and suspicious patterns in logs or network traffic files (.pcap, disk images, etc.).
- **Components:** IOC pattern matching, malware detection logic, anomaly detection scripts.

Threat Intelligence Layer:

- **Technologies Used:** VirusTotal API.
- **Function:** Enriches evidence with additional context by checking for known threats using external sources like VirusTotal. It validates whether any of the indicators are linked to known malicious activities.
- **Components:** VirusTotal API integration for real-time IOC enrichment, threat detection, and validation.

Secure Evidence Storage Layer:

- **Technologies Used:** IPFS (InterPlanetary File System), Blockchain (Ethereum, Solidity).
- **Function:** This layer securely stores the evidence on the decentralized IPFS system, ensuring immutability and traceability. Additionally, all actions related to evidence, such as uploads and analysis, are recorded on the blockchain to maintain a tamper-proof record.
- **Components:** Evidence storage on IPFS, blockchain for logging actions, decentralized storage.

Database Layer:

- **Technologies Used:** MongoDB.
- **Function:** Stores the metadata of evidence, analysis results, logs, and any other relevant forensic data required for reporting and querying.
- **Components:** MongoDB stores logs, analysis findings, metadata, and IOC information, enabling fast querying and reporting.

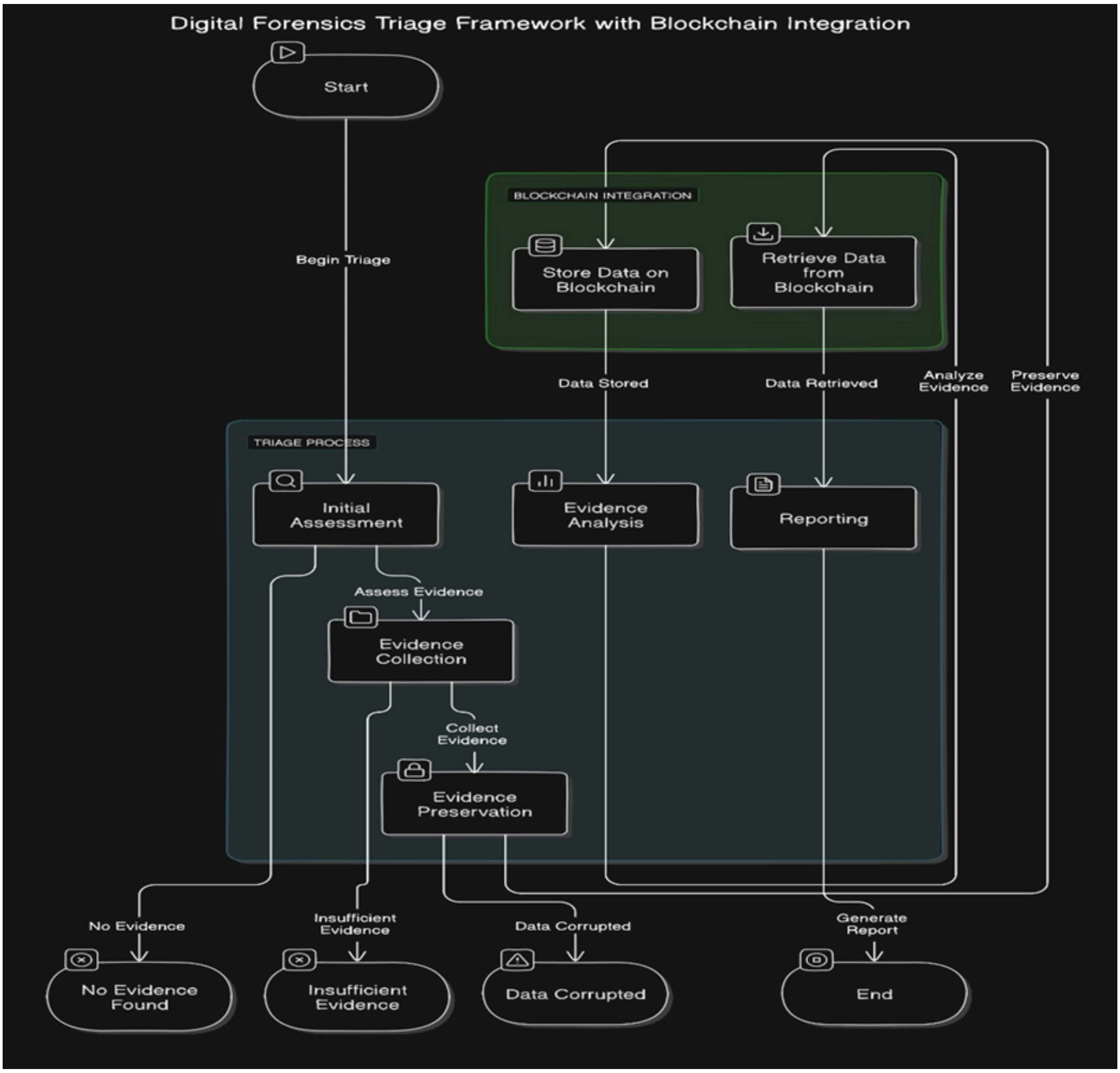
Reporting Layer:

- **Technologies Used:** Backend logic, PDF generation libraries.
- **Function:** Generates and exports comprehensive PDF reports with all findings, including evidence metadata, logs, IOCs, and analysis results. This report can be used for legal

purposes or as a detailed investigation summary.

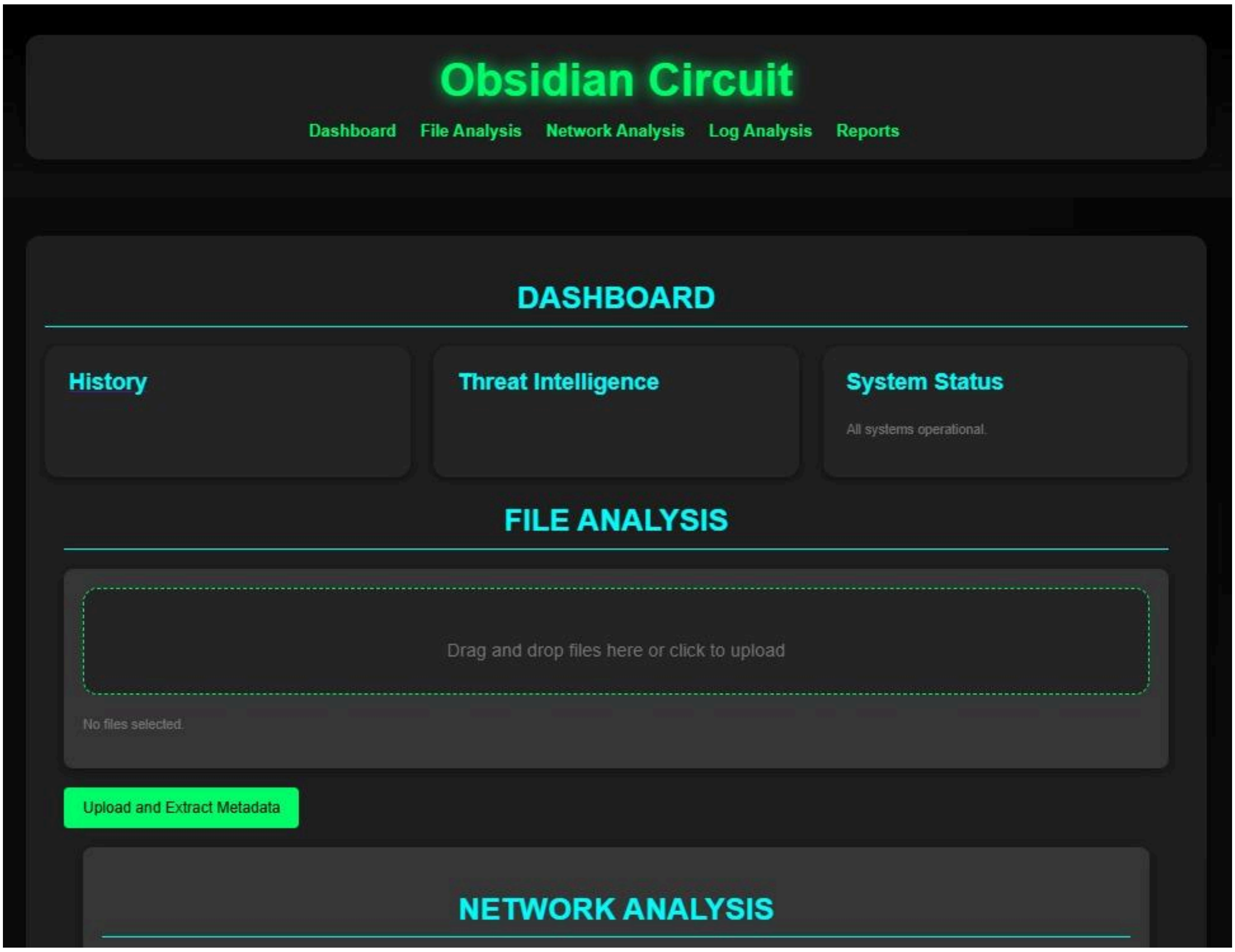
- **Components:** PDF report generation, detailed findings including IOCs, timestamps, file system metadata, and analysis results.

4.2 BLOCK DIAGRAM:-



4.3 RESULT:-

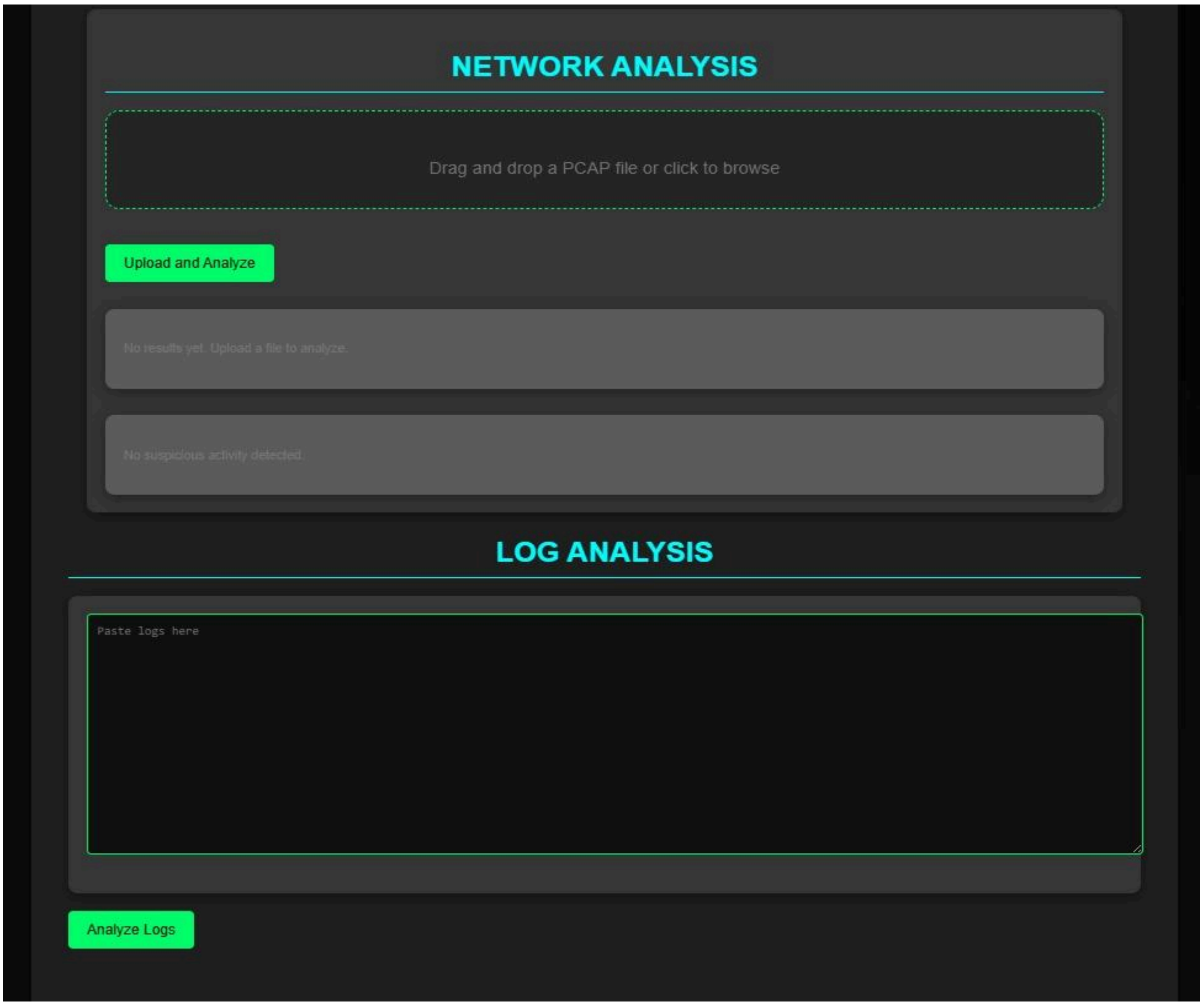
1) HOMEPAGE INTERFACE



All systems operational.

Drag and drop files here or click to upload

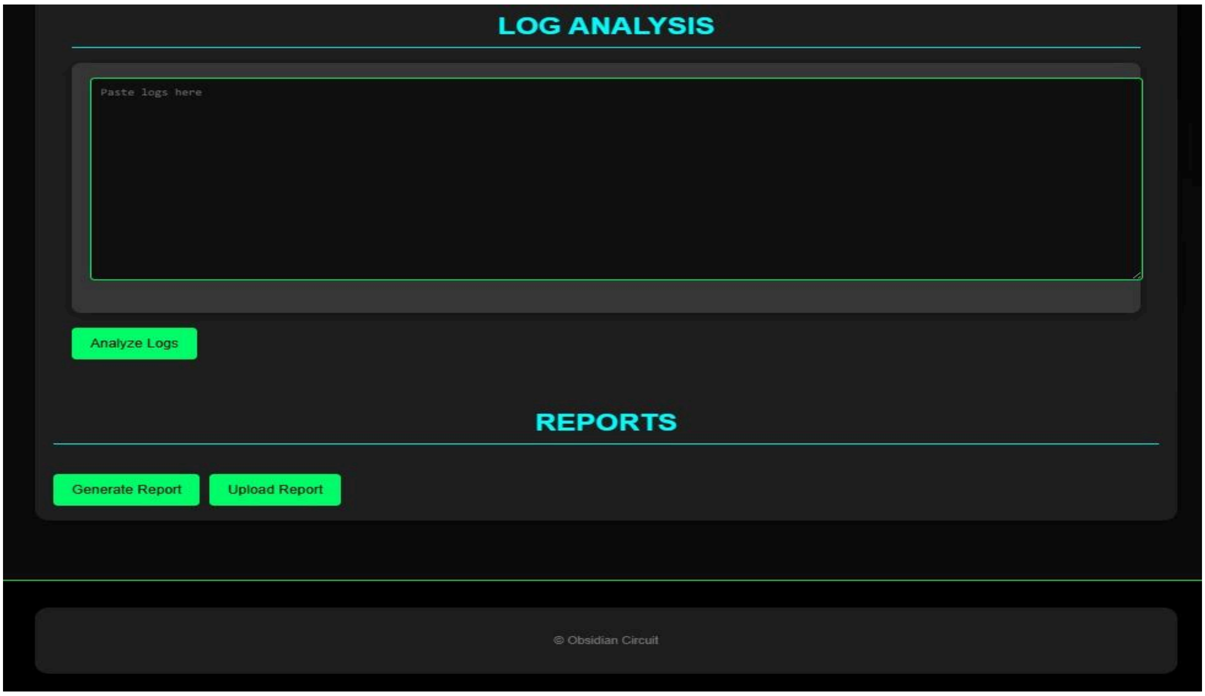
No files selected.



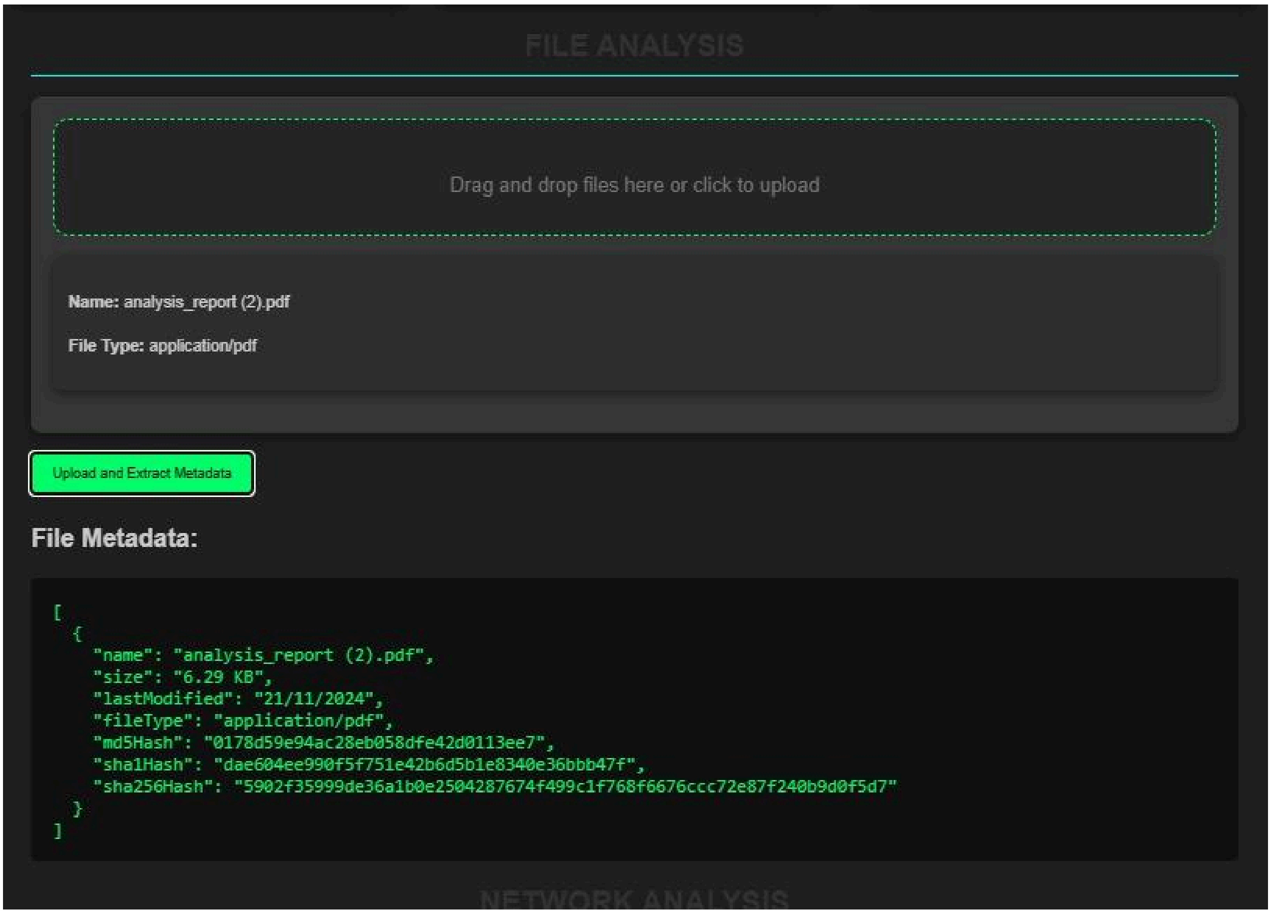
Drag and drop a PCAP file or click to browse

No results yet. Upload a file to analyze.

No suspicious activity detected.



2) FILE METADATA ANALYSIS REFERENCE


FILE ANALYSIS
Drag and drop files here or click to upload

Name: analysis_report (2).pdf

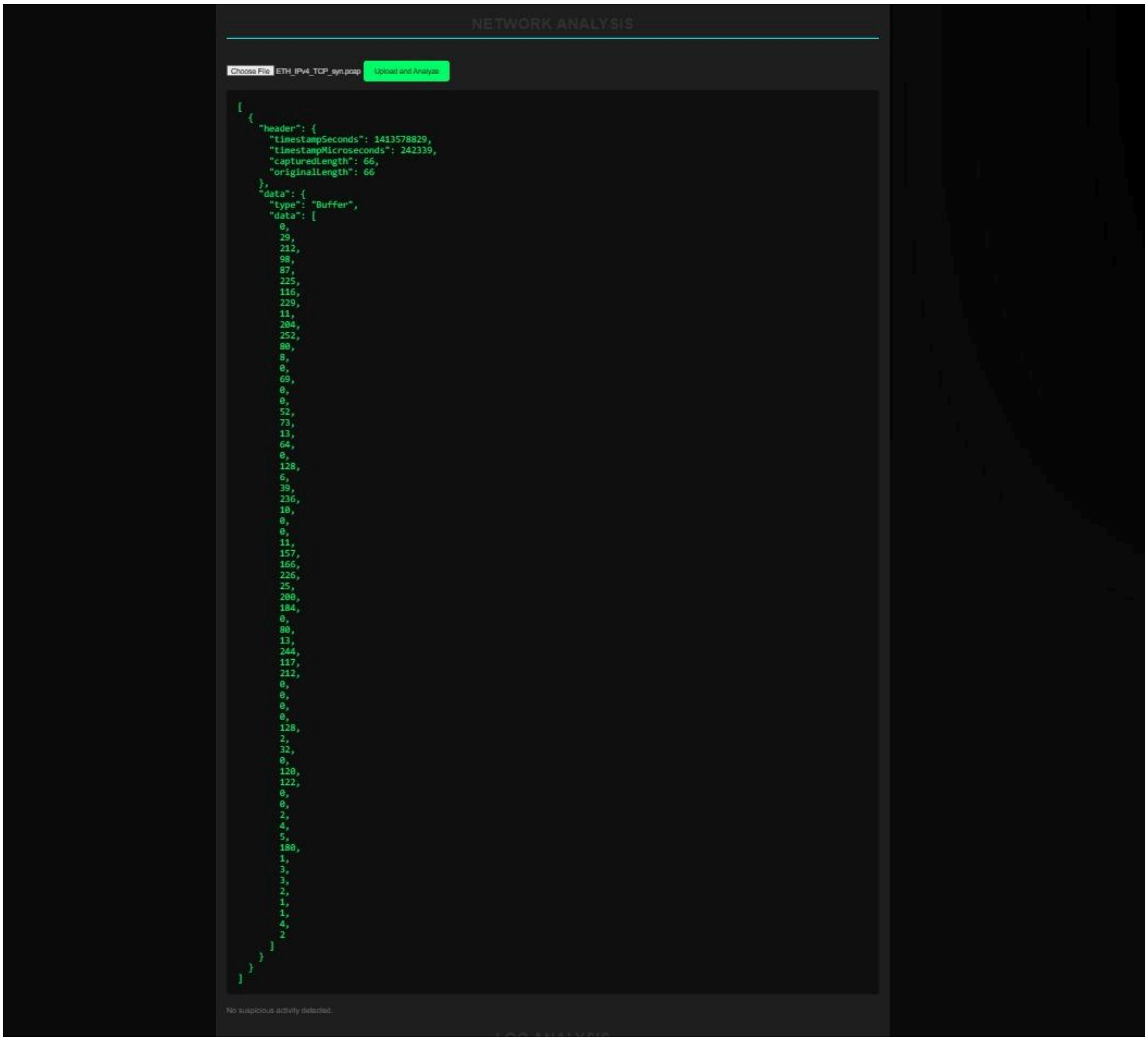
File Type: application/pdf

Upload and Extract Metadata

File Metadata:

```
[
  {
    "name": "analysis_report (2).pdf",
    "size": "6.29 KB",
    "lastModified": "21/11/2024",
    "fileType": "application/pdf",
    "md5Hash": "0178d59e94ac28eb058dfe42d0113ee7",
    "sha1Hash": "dae604ee990f5f751e42b6d5b1e8340e36bbb47f",
    "sha256Hash": "5902f35999de36a1b0e2504287674f499c1f768f6676ccc72e87f240b9d0f5d7"
  }
]
```

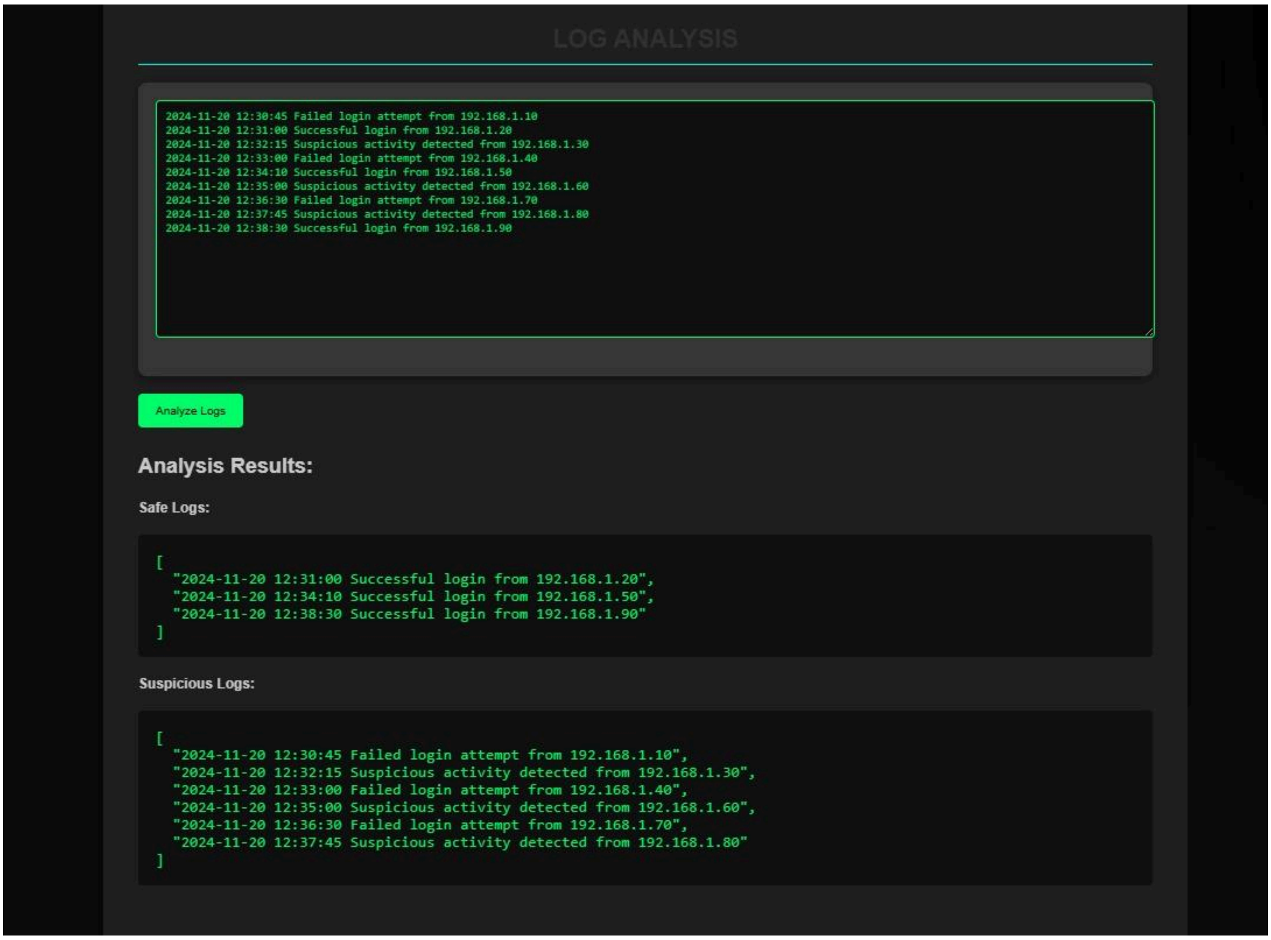
3) NETWORK ANALYSIS REFERENCE



```
[
  {
    "header": {
      "timestampSeconds": 1413578829,
      "timestampMicroseconds": 242339,
      "capturedLength": 66,
      "originalLength": 66
    },
    "data": {
      "type": "Buffer",
      "data": [
        0,
        29,
        212,
        98,
        87,
        225,
        116,
        229,
        11,
        204,
        252,
        80,
        8,
        0,
        69,
        0,
        0,
        52,
        73,
        13,
        64,
        0,
        128,
        6,
        39,
        236,
        10,
        0,
        0,
        11,
        157,
        166,
        226,
        25,
        200,
        184,
        0,
        80,
        13,
        244,
        117,
        212,
        0,
        0,
        0,
        0,
        128,
        2,
        32,
        0,
        120,
        122,
        0,
        0,
        2,
        4,
        5,
        180,
        1,
        3,
        3,
        2,
        1,
        1,
        4,
        2
      ]
    }
  }
]
```

No suspicious activity detected.

4) LOG ANALYSIS REFERENCE



```
2024-11-20 12:30:45 Failed login attempt from 192.168.1.10
2024-11-20 12:31:00 Successful login from 192.168.1.20
2024-11-20 12:32:15 Suspicious activity detected from 192.168.1.30
2024-11-20 12:33:00 Failed login attempt from 192.168.1.40
2024-11-20 12:34:10 Successful login from 192.168.1.50
2024-11-20 12:35:00 Suspicious activity detected from 192.168.1.60
2024-11-20 12:36:30 Failed login attempt from 192.168.1.70
2024-11-20 12:37:45 Suspicious activity detected from 192.168.1.80
2024-11-20 12:38:30 Successful login from 192.168.1.90
```

Analysis Results:

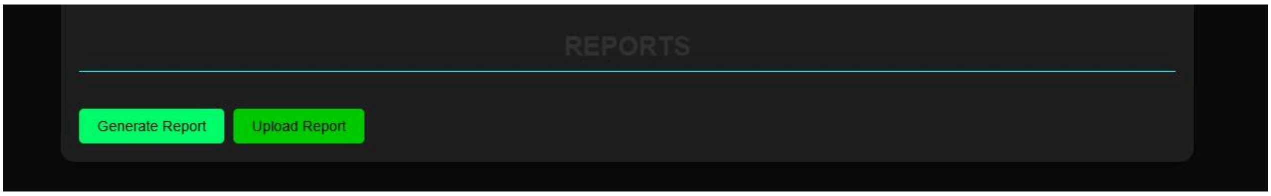
Safe Logs:

```
[
  "2024-11-20 12:31:00 Successful login from 192.168.1.20",
  "2024-11-20 12:34:10 Successful login from 192.168.1.50",
  "2024-11-20 12:38:30 Successful login from 192.168.1.90"
]
```

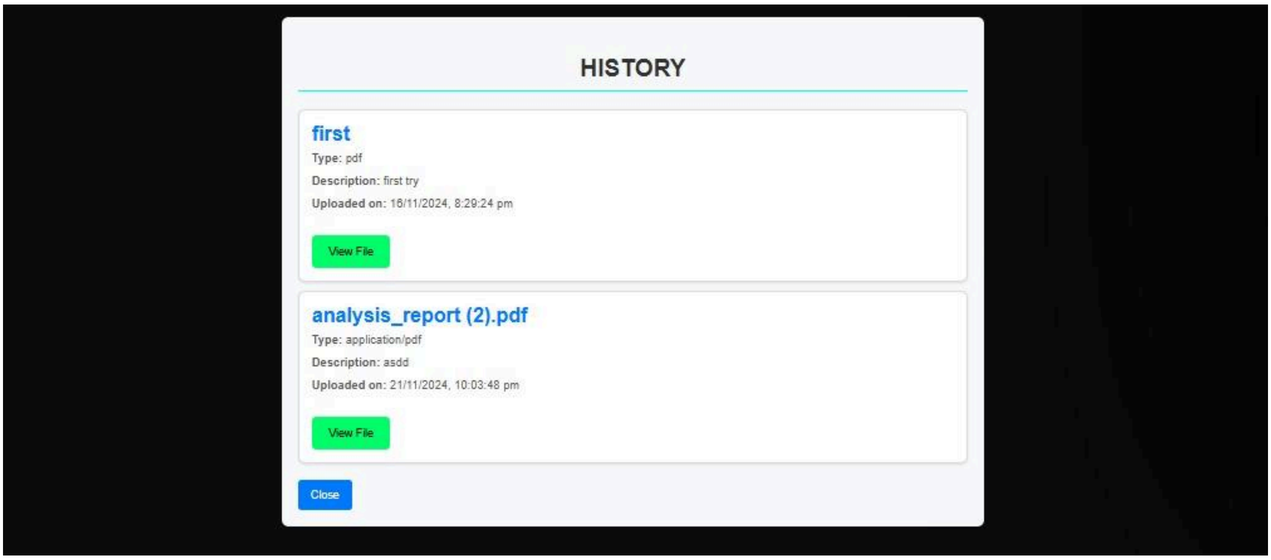
Suspicious Logs:

```
[
  "2024-11-20 12:30:45 Failed login attempt from 192.168.1.10",
  "2024-11-20 12:32:15 Suspicious activity detected from 192.168.1.30",
  "2024-11-20 12:33:00 Failed login attempt from 192.168.1.40",
  "2024-11-20 12:35:00 Suspicious activity detected from 192.168.1.60",
  "2024-11-20 12:36:30 Failed login attempt from 192.168.1.70",
  "2024-11-20 12:37:45 Suspicious activity detected from 192.168.1.80"
]
```

5) GENERATE REPORT & UPLOAD REPORT BUTTON INTERFACE



6) HISTORY PAGE REFERENCE



HISTORY

first

Type: pdf

Description: first try

Uploaded on: 16/11/2024, 8:29:24 pm

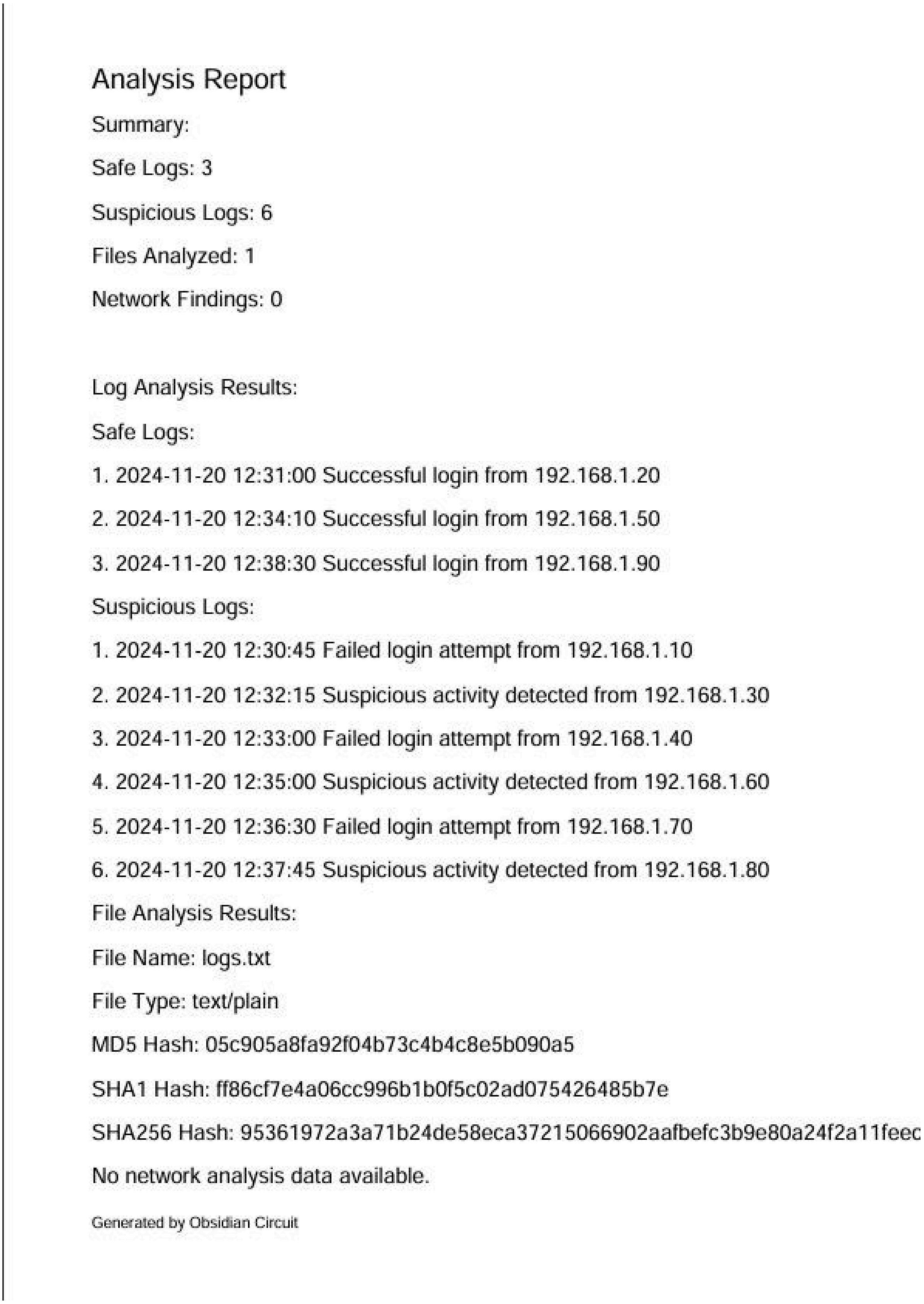
analysis_report (2).pdf

Type: application/pdf

Description: asdd

Uploaded on: 21/11/2024, 10:03:48 pm

7) REPORT PDF REFERENCE



Analysis Report

Summary:

Safe Logs: 3

Suspicious Logs: 6

Files Analyzed: 1

Network Findings: 0

Log Analysis Results:

Safe Logs:

1. 2024-11-20 12:31:00 Successful login from 192.168.1.20
2. 2024-11-20 12:34:10 Successful login from 192.168.1.50
3. 2024-11-20 12:38:30 Successful login from 192.168.1.90

Suspicious Logs:

1. 2024-11-20 12:30:45 Failed login attempt from 192.168.1.10
2. 2024-11-20 12:32:15 Suspicious activity detected from 192.168.1.30
3. 2024-11-20 12:33:00 Failed login attempt from 192.168.1.40
4. 2024-11-20 12:35:00 Suspicious activity detected from 192.168.1.60
5. 2024-11-20 12:36:30 Failed login attempt from 192.168.1.70
6. 2024-11-20 12:37:45 Suspicious activity detected from 192.168.1.80

File Analysis Results:

File Name: logs.txt

File Type: text/plain

MD5 Hash: 05c905a8fa92f04b73c4b4c8e5b090a5

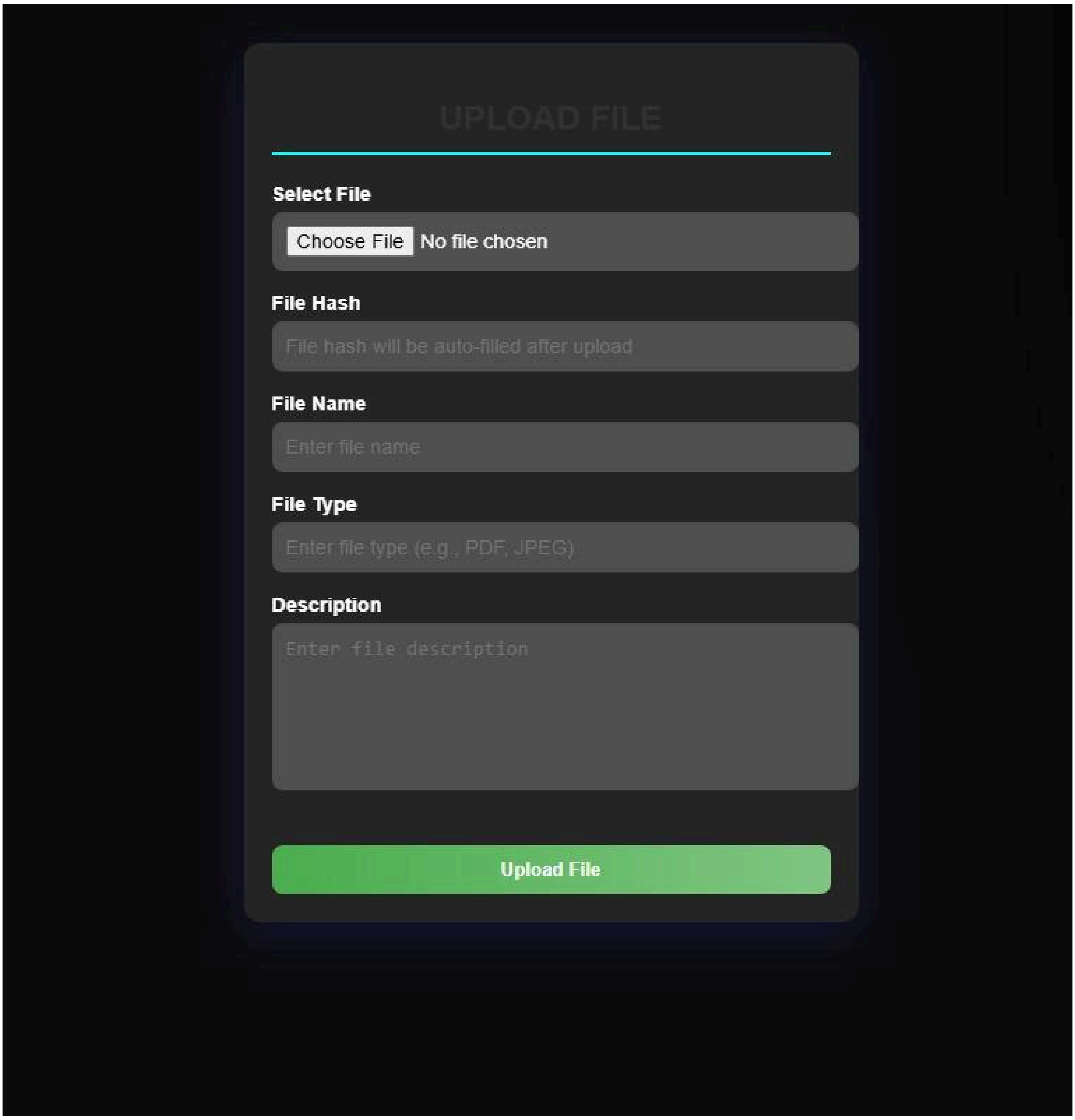
SHA1 Hash: ff86cf7e4a06cc996b1b0f5c02ad075426485b7e

SHA256 Hash: 95361972a3a71b24de58eca37215066902aafbefc3b9e80a24f2a11feec

No network analysis data available.

Generated by Obsidian Circuit

8) UPLOAD REPORT REFERENCE



CHAPTER 5
TOOLS AND LANGUAGES

Frontend Development

The frontend of **Obsidian Circuit** is designed to be intuitive and user-friendly. It is built using **React.js**, a powerful JavaScript library for creating dynamic user interfaces. This allows for seamless interaction between the user and the tool. **HTML** and **CSS** are used for the structure and styling of the web pages, ensuring a responsive design that adapts to various screen sizes and provides a smooth user experience.

Backend Development

The backend of **Obsidian Circuit** is powered by **Node.js**, a runtime environment that allows for server-side JavaScript execution. It is supported by **Express.js**, a lightweight framework that simplifies routing and API development. Together, they enable the tool to handle multiple requests efficiently, interact with databases, and communicate with external APIs, such as VirusTotal and other threat intelligence sources.

Database & Storage

For secure, decentralized storage of forensic evidence, **Obsidian Circuit** uses **IPFS** (InterPlanetary File System). IPFS ensures that evidence is stored in a distributed network, preventing tampering and guaranteeing availability even if some nodes go offline. Additionally, **Ethereum Blockchain** is used to create immutable records of evidence access and modification, enhancing the tool's auditability and ensuring that any interaction with the stored data is transparently logged and resistant to unauthorized changes.

Analysis & Detection

To detect threats and analyze forensic data, **Obsidian Circuit** integrates AI and machine learning (AI/ML) algorithms. These algorithms are used to identify patterns in logs, network traffic, and file metadata that could indicate malicious activity or compromised systems. Additionally, the tool integrates external threat intelligence APIs such as **VirusTotal** to cross-check files, IPs, and URLs against known malicious databases, enriching the analysis with real-time threat intelligence. These combined techniques help to automate the detection of Indicators of Compromise (IOCs) and expedite the analysis process.

Security

The security of **Obsidian Circuit** is one of its key features. The use of **Ethereum Blockchain** ensures the integrity and traceability of the evidence stored within the tool. By logging every access and modification event on the blockchain, the tool provides an immutable record that prevents tampering and assures investigators that the evidence remains unchanged throughout the investigation. This guarantees trustworthiness in the forensic process and the tool's outputs.

Report Generation

Obsidian Circuit provides the ability to generate detailed reports of the investigation findings. The reports include evidence analysis, threat detection results, and blockchain logs, which are crucial for auditing and documentation. **PDF generation** is used to export these reports, ensuring that they are easily shareable, printable, and compliant with legal and organizational standards. The ability to generate and export comprehensive, tamper-proof reports is essential for presenting the results of forensic investigations.

Development Tools

During development, tools like **Visual Studio Code** (VS Code) were used for coding, offering an efficient integrated development environment (IDE) for JavaScript and Node.js. **Git** is employed for version control, ensuring that code is well-managed, tracked, and collaborative development is streamlined. **Postman** is used for testing APIs, ensuring that all external integrations, such as with VirusTotal and the blockchain, work smoothly and securely.

CHAPTER 6
CONCLUSION AND FUTURE WORK

This project focuses on developing a Digital Forensics and Incident Response (DFIR) tool that enables forensic investigators to securely collect, analyze, and store digital evidence. By leveraging blockchain for secure evidence storage and decentralized management, the tool ensures tamper-proof data integrity, making it a valuable asset for forensic investigations. The tool simplifies the process of evidence analysis by automating the detection of Indicators of Compromise (IOCs) and enriching data with external threat intelligence sources like VirusTotal. Furthermore, it generates comprehensive reports that can be used for legal and investigative purposes, while maintaining a user-friendly interface built with React.js for ease of use. The blockchain-based architecture provides a high level of security, ensuring that evidence is traceable and immutable throughout the investigation lifecycle.

AI/ML Integration:

- Future versions of the tool will incorporate Artificial Intelligence (AI) and Machine Learning (ML) algorithms to automate the detection of anomalies and recognize patterns in the data. This will significantly reduce manual effort and improve the speed and accuracy of identifying threats and incidents.

Threat Intelligence Integration:

- The tool will be enhanced with integrations from external threat intelligence platforms like VirusTotal. This will provide real-time validation of Indicators of Compromise (IOCs) and enrich data with up-to-date threat intelligence to better identify malicious activity.

Enhanced Blockchain Storage:

- As the tool expands, the blockchain architecture will be optimized to handle larger volumes of forensic data efficiently. This will ensure secure, tamper-proof storage even for extensive datasets, improving scalability for large-scale investigations.

Broader Tool Compatibility:

- Future versions will focus on extending the compatibility of the tool with other widely-used forensic tools and frameworks. This will enable investigators to seamlessly incorporate data from various sources and provide a more comprehensive analysis.

Improved User Interface:

- The user interface will be refined to improve usability, making it more intuitive for forensic professionals. Additionally, there will be enhanced features for report customization, allowing users to generate reports tailored to specific investigation needs.

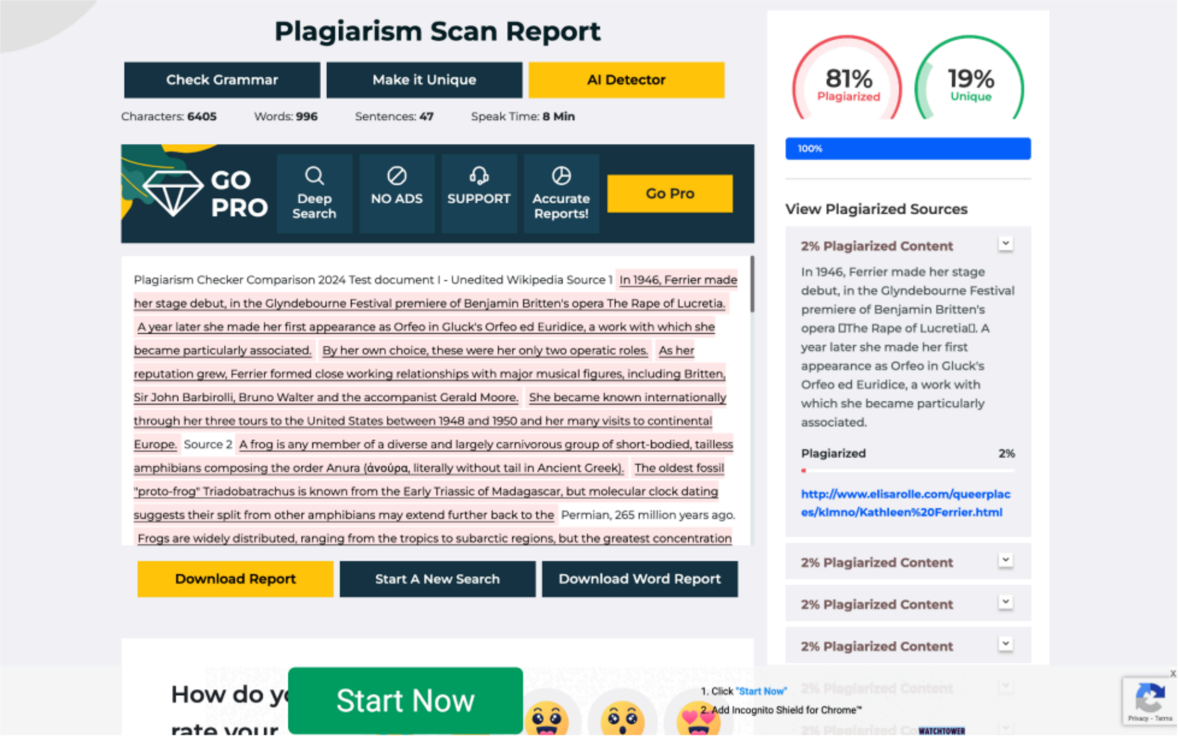
CHAPTER 7

BIBLIOGRAPHY

- M. B. Jiménez, D. Fernández, J. E. Rivadeneira, and R. Flores-Moyano, "A Filtering Model for Evidence Gathering in an SDN-Oriented Digital Forensic and Incident Response Context," *IEEE Access*, vol. 12, pp. 75792-75808, 2024. doi: 10.1109/ACCESS.2024.3405588.
- O. I. Falowo, K. Koshoedo, and M. Ozer, "An Assessment of Capabilities Required for Effective Cybersecurity Incident Management - A Systematic Literature Review," in *2023 International Conference on Data Security and Privacy Protection (DSPP)*, Xi'an, China, 2023, pp. 1-11. doi: 10.1109/DSPP58763.2023.10404318.
- D. Dunsin, M. Ghanem, K. Ouazzane, and V. Vassilev, "A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response," *Forensic Science International: Digital Investigation*, vol. 47, pp. 2666-2817, 2024. doi: 10.1016/j.fsidi.2023.301675.

CHAPTER 8

PLAGIARISM REPORT



Plagiarism Scan Report

Characters: **6405** Words: **996** Sentences: **47** Speak Time: **8 Min**

Plagiarism Checker Comparison 2024 Test document I - Unedited Wikipedia Source 1 In 1946, Ferrier made her stage debut, in the Glyndebourne Festival premiere of Benjamin Britten's opera The Rape of Lucretia. A year later she made her first appearance as Orfeo in Gluck's Orfeo ed Euridice, a work with which she became particularly associated. By her own choice, these were her only two operatic roles. As her reputation grew, Ferrier formed close working relationships with major musical figures, including Britten, Sir John Barbirolli, Bruno Walter and the accompanist Gerald Moore. She became known internationally through her three tours to the United States between 1948 and 1950 and her many visits to continental Europe. Source 2 A frog is any member of a diverse and largely carnivorous group of short-bodied, tailless amphibians composing the order Anura (ἀνούρα, literally without tail in Ancient Greek). The oldest fossil "proto-frog" Triadobatrachus is known from the Early Triassic of Madagascar, but molecular clock dating suggests their split from other amphibians may extend further back to the Permian, 265 million years ago. Frogs are widely distributed, ranging from the tropics to subarctic regions, but the greatest concentration

81% Plagiarized

19% Unique

100%

View Plagiarized Sources

2% Plagiarized Content

In 1946, Ferrier made her stage debut, in the Glyndebourne Festival premiere of Benjamin Britten's opera □The Rape of Lucretia□. A year later she made her first appearance as Orfeo in Gluck's Orfeo ed Euridice, a work with which she became particularly associated.

Plagiarized 2%

http://www.elisarolle.com/queerplaces/klmno/Kathleen%20Ferrier.html

2% Plagiarized Content

2% Plagiarized Content

2% Plagiarized Content