MIT School of Engineering
Department of Computer Science and Engineering

Project Synopsis

Group ID: TYCSF201
Project Title: Obsidian Circuit
Group Members:

Enrollment Number	Roll No.	Name of student	Email Id	Contact Number
MITU22BTCS0160	**2223638**	**Aryan Dsouza**	aryandsz14@gmail.com	9011010654
MITU22BTCS0379	**2223645**	**Kathan Somani**	kathansomani9875@gmail.com	9574943784
MITU22BTCS0664	**2223546**	**Roque Leon Martins**	roqueleonmartins@gmail.com	9284816402
MITU22BTCS0842	**2223607**	**Soham Jagtap**	soham1802d@gmail.com	7202062490

Problem Statement: In the digital era, where cyber threats are increasingly sophisticated, investigators face challenges in managing and responding to incidents effectively. Traditional tools often struggle with ensuring the integrity and traceability of digital evidence, making investigations time-consuming and prone to errors. Additionally, the lack of real-time enrichment for Indicators of Compromise (IOCs) hinders effective threat detection, while generating detailed, auditable reports that meet legal and organizational standards remains cumbersome. *Obsidian Circuit* addresses these issues by providing a secure, user-friendly platform that automates evidence analysis, ensures tamper-proof storage using blockchain, and delivers actionable insights, enabling investigators to focus on swift and accurate decision-making while upholding the highest standards of accountability.

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.

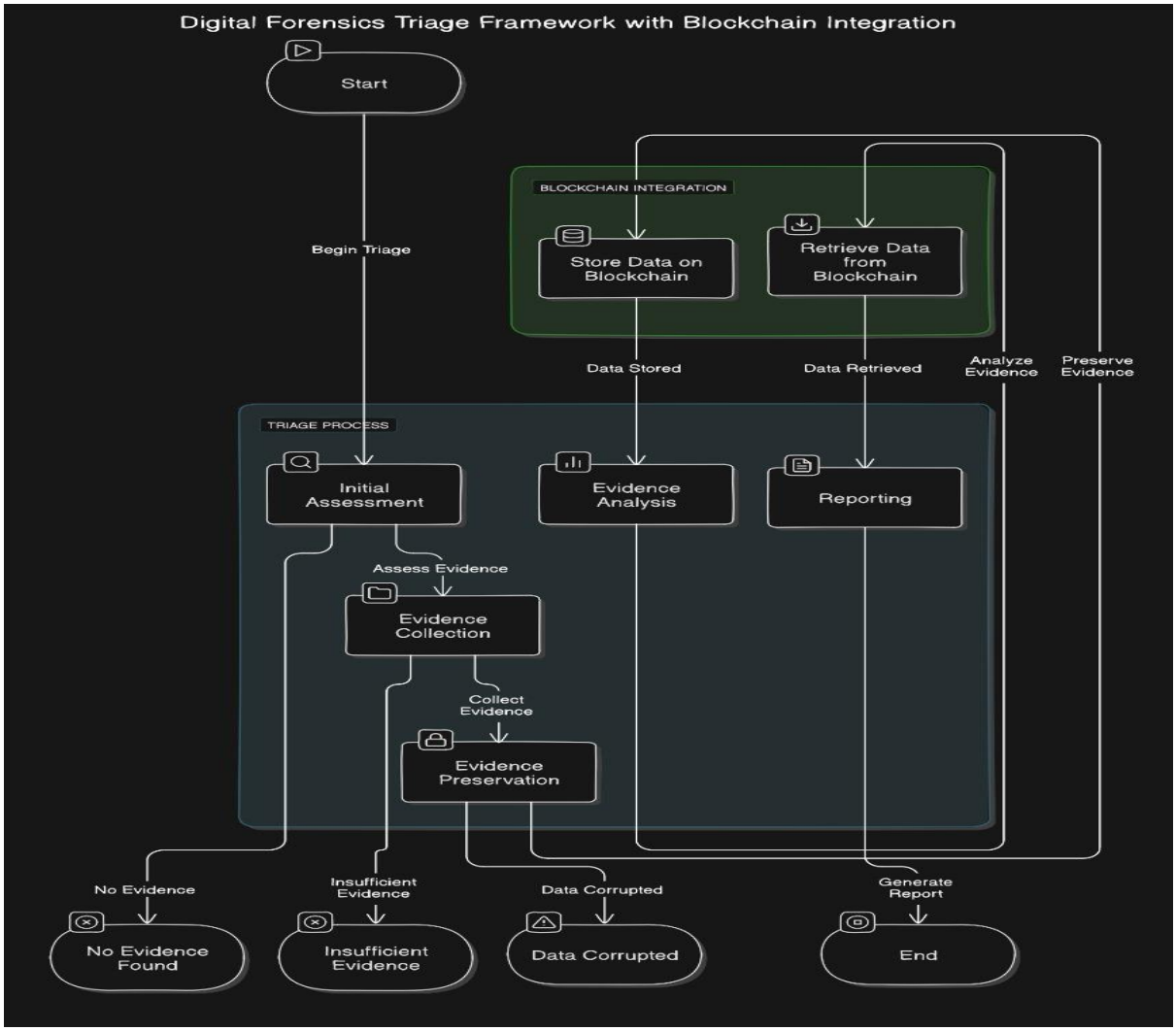
Literature Survey:

1.) 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.

2.) 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.

3.) 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.

Proposed System (Block Diagram):



Conclusion:

The proposed Digital Forensics and Incident Response (DFIR) tool addresses key challenges in forensic investigations, such as evidence integrity, data overload, and slow analysis. By leveraging blockchain for secure storage, IPFS for decentralized management, and AI/ML for automated threat detection, the tool enhances both the speed and accuracy of investigations. Integration with external threat intelligence platforms like VirusTotal strengthens its ability to identify cyber threats in real-time. This solution streamlines evidence handling, ensures compliance, and provides a scalable foundation for future advancements in digital forensics.

Annexure: A

1.) **Publication Title: "A Filtering Model for Evidence Gathering in an SDN-Oriented Digital Forensic and Incident Response Context"**

- **Authors: Jiménez, M. B., Fernández, D., Rivadeneira, J. E., & Flores-Moyano, R.**
- **Publication Year: 2024**
- **Source: IEEE Access**
- **Pages: 75792-75808**
- **DOI: 10.1109/ACCESS.2024.3405588**

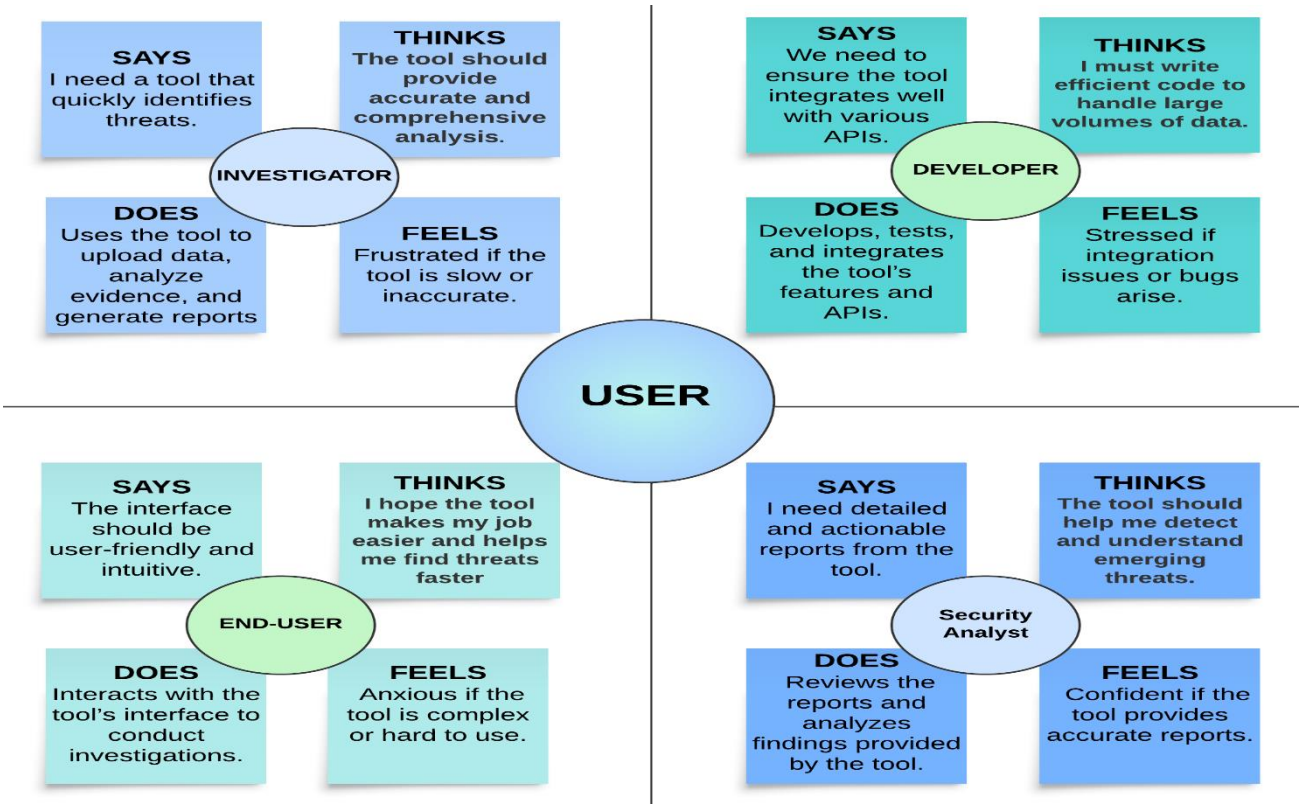
2.) **Publication Title: "An Assessment of Capabilities Required for Effective Cybersecurity Incident Management - A Systematic Literature Review"**

- **Authors: Falowo, O. I., Koshoedo, K., & Ozer, M.**
- **Publication Year: 2023**
- **Source: 2023 International Conference on Data Security and Privacy Protection (DSPP)**
- **Pages: 1-11**
- **DOI: 10.1109/DSPP58763.2023.10404318**

3.) **Publication Title: "A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response"**

- **Authors: Dunsin, D., Ghanem, M., Ouazzane, K., & Vassilev, V.**
- **Publication Year: 2024**
- **Source: Forensic Science International: Digital Investigation**
- **Pages: 2666-2817**
- **DOI: 10.1016/j.fsidi.2023.301675**

Annexure: B- Empathy Chart



Annexure: C – Project tracker sheet

Project Development and Completion Tracker

Porject ID: Obsidian Circuit

Project Start Date: 07-08-2024 **Project End Date:21-11-2024**

Project Description: Obsidian Circuit is a cutting-edge cyber triage and incident response tool that combines real-time analysis of files, networks, and logs with AI/ML-driven incident prioritization and decentralized blockchain for secure data storage, providing a comprehensive solution for digital forensic investigations.

	Name of Team member	Task
Project Obsidian Circuit Team Members	Aryan Dsouza	**Documentation**
	Kathan Somani	**Ideation & Frontend**
	Roque Martins	**Blockchain Integration & Backend**
	Soham Jagtap	**Frontend & Backend Integration**

Task1:	Data Collection & Analysis: Implement mechanisms to collect and analyze file, network, and log data for indicators of compromise (IOCs).
Task2:	AI/ML Integration: Integrate artificial intelligence and machine learning algorithms to prioritize incidents and suggest responses.
Task3:	Blockchain Integration: Incorporate decentralized blockchain for secure, high-speed data storage with encryption and backup features.
Task4:	User Interface & Alerts: Develop an intuitive dashboard for users to view and manage investigations, including real-time notifications for critical incidents.

Task Name	Sub Tasks	Task Status	Assigned To	Assigned Date	Deadline	Start Date	Completion Date	Completion Status
Data Collection ,Analysis, Documentation	Gather and analyze files for threat detection and classification.	Complete	Aryan , Soham, Kathan	2024-08-07	2024-08-15	2024-08-07	2024-08-15	100%
AI/ML Integration	Research AI/ML models for detecting and classifying cyber threats.	Partially Complete	Roque ,Aryan	2024-08-15	2024-08-30	2024-08-15	2024-08-30	60% Partial
Feasibility & Viability	Feasibility & Cost Cutting	Complete	Kathan , Aryan	2024-08-20	2024-08-25	2024-08-20	2024-08-25	100%
Blockchain Integration & Backend	Backend Designing		Soham ,Kathan	2024-08-30	2024-09-20	2024-08-30	2024-09-20	100%
	Blockchain Working & Backend	Complete	Roque, Soham	2024-09-20	2024-10-10	2024-09-20	2024-10-10	100%
Frontend & Prototyping	Website Design	Complete	All Team Members (Lead -Ro	2024-10-10	2024-10-30	2024-10-10	2024-10-30	100%
	Designing Prototype	Complete	All Team Members	2024-10-30	2024-11-20	2024-10-30	2024-11-20	100%