SMART INDIA HACKATHON 2024

SMART INDIA HACKATHON 2024

Problem Statement ID – SIH1744

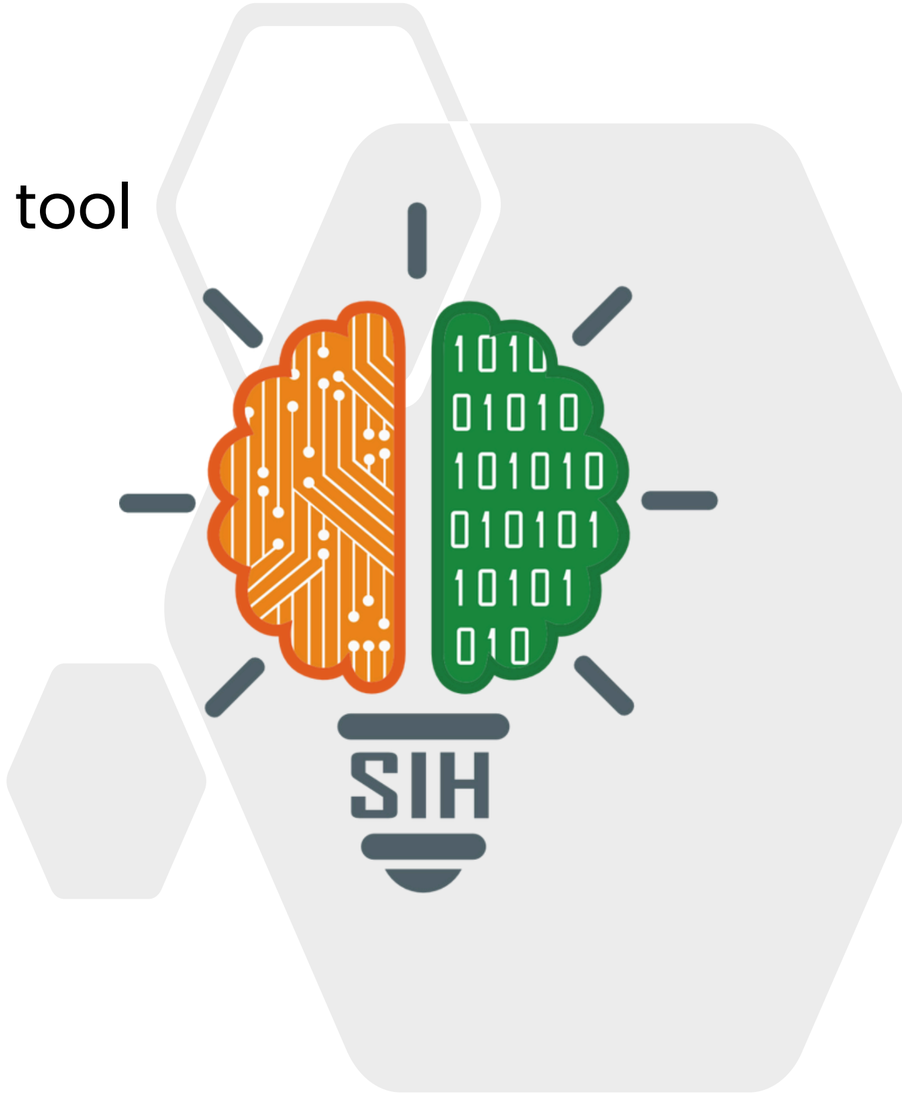
Problem Statement Title - Creating a cyber triage tool to streamline digital forensic investigation

Theme - Blockchain & Cybersecurity

PS Category- Software

Team ID- 289

Team Name(Registered on Portal) - Arize



Arize

ZYPHERVERSE

SMART INDIA HACKATHON 2024

SOLUTION

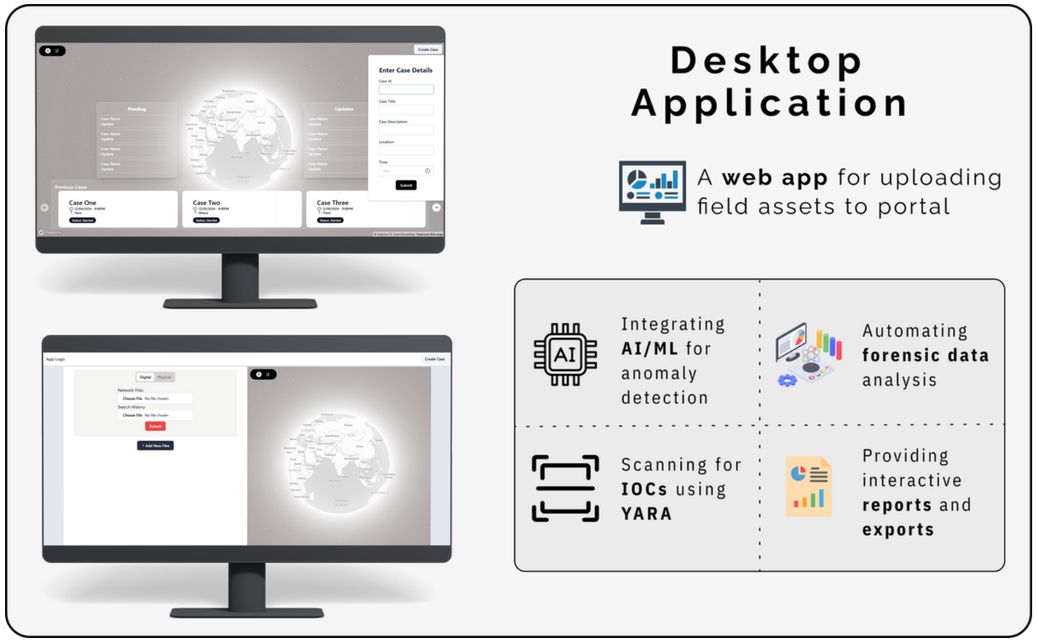
A digital forensics tool automating data collection, analysis, and reporting for faster, more efficient investigations.

- YARA scans data for indicators of **compromise**, **matching files** and **logs** to rules to detect suspicious files and IOCs.
- Automated data collection uses **Clonezilla**, **OSFMount**, **Autopsy**, **Bulk Extractor**, and **pytsk3** for efficient image extraction.
- **Log2Timeline** generates timelines, **Wireshark** and **NetworkMiner** analyze traffic, and pandas manipulates data.
- AI/ML algorithms like **Isolation Forest** and **Autoencoders** enhance anomaly detection.
- Advanced **analytics techniques** identify patterns in data to improve **threat detection** and **response times**.
- Integrating **deep learning models** enables more accurate identification of anomalies in **complex datasets**.

We enhance investigations with a comprehensive digital forensics toolkit, utilizing automated data collection, advanced analysis, and AI/ML algorithms for efficient anomaly detection.

PROTOTYPE

We support **10+ languages** with an easy **UI/UX**, hassle free logging of tasks using **smart voice controls**



Our innovative web app automates **digital forensics**, enhancing **investigation accuracy**, and **interactive reporting**

Cyber Triage is **50% completed**; testing and validation are ongoing.

WHY WE STAND OUT ?

AI-Enhanced Anomaly Detection
Our solution leverages AI/ML to enhance the accuracy of threat identification.

Customizable YARA Rules Integration
Users can easily define YARA rules for advanced, tailored threat detection.

Cross-Platform Solution with Docker Integration
Our Product ensure consistent performance and accessibility across different environments.

Interactive Timeline Visualization
Detailed event timelines improve clarity and investigation flow

TECHNICAL APPROACH

Arize

SMART INDIA HACKATHON 2024

FTKImager
For Speedy Data Disk Imaging

The Digital Forensic Evidences are collected effectively and processed by lending to the **powerful backend**

Digital & Physical Assets


Cyber attack happened at some place


Retrieving evidences from affected device


Scanning of network files


Searching for intruder's Location

Intrusion Pin-Point
Point out suspect IP and routing through different routers in map

Fast and Effortless Data Collection

3D World Interface
Interactive 3d World based Mapping for intutiveness

Authetication
Realtime Database
File Storage

Reverse Proxy for enhanced security

Reverse Proxy
Load balancer
NGINX

Services running virtually on Container

Storage Container

Backend

Client Request to container

Client

ex
Webserver

Frontend

Reverse Proxy
NGINX
Load balancer

Tensorflow Model run locally as cluster

Flask
Tensorflow

ARCHITECTURE

CYBER FORENSICS

Web App

React.js
Shadcn UI
Javascript
Redux
Radix UI
Socket.io

Uploading Field Assets to Portal
Searching for Uploading data gathered in secure way

AI Processing data
Analysing gathered data and representing it interactively with help of AI

Generating Report
Generating Report for field use and sharing with peer

Security
Zero Trust | SSL | 2FA/MFA | TLS/OAuth 2.0 | JWT | HSTS

The Web App runs on a local server instance with a secured gateway involving **Zero Trust Ideology**

Arize

FEASIBLITY AND VIABILITY

SMART INDIA HACKATHON 2024

FEASIBLITY

Technical Feasibility

AI/ML algorithms like **Isolation Forest and Autoencoders** achieve over **90% accuracy** in anomaly detection, enhancing the tool's reliability in identifying threats.

Operational Feasibility

Automated data collection and analysis reduce **manual efforts by 60%**, allowing investigators to efficiently manage cases, workflows, and focus on other critical tasks.

Economic Feasibility

Initial investment is offset by **long-term cost savings** through reduced accidents and increased productivity. ROI expected within **2-3 years.**

Regulatory Feasibility

The tool ensures compliance with **GDPR, HIPAA, and NIST standards**, offering robust data protection, secure evidence handling, and comprehensive audits.

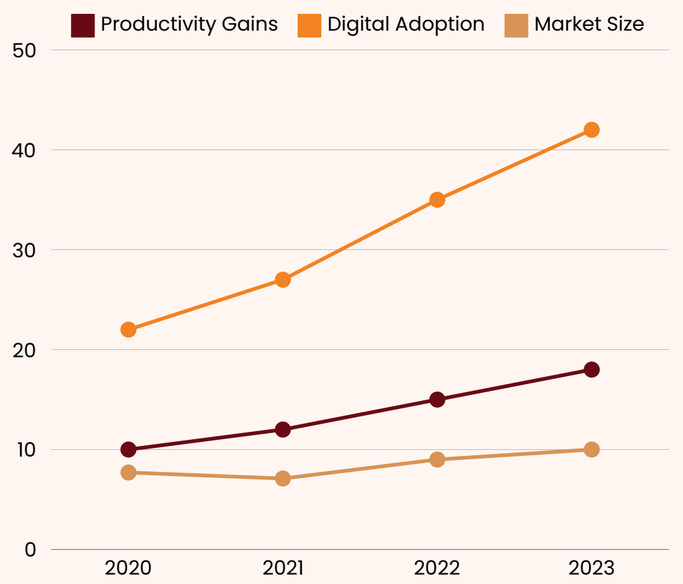
VIABILITY

Market Viability

Our AI-driven forensic tool addresses a growing demand for efficient digital investigations, projecting a **10% annual market growth by 2028**, attracting both private firms and government agencies.

Sustainable Viability

By automating labor-intensive tasks, our solution reduces **resource consumption and operational costs**, supporting sustainable practices and aligning with industry **ESG goals** for responsible and ethical digital forensics.



MARKET OPPURTUNITY

The digital forensics market is projected to see a 65% increase in demand for AI-driven solutions by 2030, driven by rising cyber threats and regulatory compliance needs.

Arize

IMPACTS AND BENEFITS

SMART INDIA HACKATHON 2024

IMPACTS

Accelerated Investigations

Our tool automates data analysis, significantly reducing investigation time, allowing faster resolution of cases.

Enhanced Accuracy

AI-driven analysis minimizes human error, improving the accuracy of identifying critical digital evidence.

Improved Efficiency

Streamlined workflows and automated reporting save valuable time, enabling investigators to handle more cases.

Strengthened Compliance

Automated audit trails ensure that all investigations adhere to legal and regulatory standards, reducing compliance risks.

BENEFITS

Reduced Investigation Costs

Automation and efficiency improvements lower operational expenses, leading to significant cost savings over time.

Industry Leadership

Advanced AI and forensic tools position your solution as a leader in digital forensics and incident response.

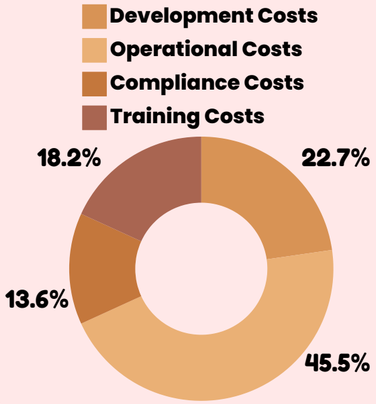
Sustainable Operations

Efficient data processing and resource management minimize waste, aligning with sustainable business practices.

Scalable Solution

The adaptable platform easily integrates with various forensic tools, supporting growth without compromising performance.

COST STRUCTURE



Development Costs

Building the app and web platform with AI integration and ERP linkage. **Estimated Cost: ₹15-25k.**

Investment in essential servers and cloud services.

Estimated Cost: ₹20-30k

Operational Costs

Regular Software Updates and System enhancements.

Estimated Cost: ₹10-15k

Investment in essential servers and cloud services.

Estimated Cost: ₹50k-1 lakh

Training & Implementation Costs

Training sessions for effective system use.

Estimated Cost: ₹20-30k

Integrating the system with existing operations.

Estimated Cost: ₹10-30k

Compliance & Security Costs

Implementing essential security protocols.

Estimated Cost: ₹10-15k

Regular audits to ensure compliance with safety standards.

Estimated Cost: ₹15-20k