Basic Details of the Team and Problem Statement

PSID	**KVH0017**
Problem Statement Title	**Hardware forensic suite**
Team Name	**Heckerpeeps**
Team Leader Name	**Ausaf Ahmad**
Institute Code (AISHE)	
Institute Name	**Jamia Millia Islamia**

Problem Statement

The goal is to create a Hardware Forensic Suite that can analyze disk, memory, and network traffic on Windows, Linux, and Mac systems. It should have both on-premises and cloud deployment options.

Problem Statement Idea & Approach

The **Hardware Forensic Suite** consists of **three utilities/microservices - Disk, Memory, and Network** - and can also communicate with a Cloud Server for additional networking capabilities.
The app has been divided into two parts, **CLI and GUI respectively** for more capabilities for both **On-Prem and Cloud.**

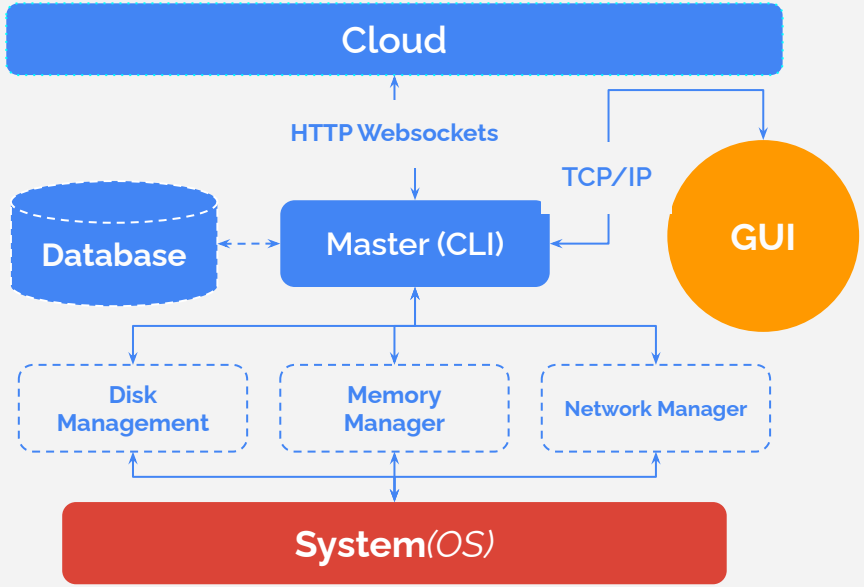
The **solution of each utility** has been explained **below** :

Disk Management

- **Metadata Analysis & GPS Localization**: Metadata embedded within the file can be analysed for forensic analysis along with GPS Location tracking.
- **File Hashing and Keyword search :** Techniques such as **Natural Language Processing(NLP)** are used to *stem & tokenize* file content for Quick Keyword Search Algorithms before Disk Forensics.
- **Signature Detection** : Signatures of the Disk files will be maintained depending on the file activity and severity in the context of **LOW-MEDIUM & HIGH** which will allow the user to analyse patterns and lookup **deleted, hidden and encrypted** data files.

Memory/Cache Management

- **Memory Acquisition** to collect volatile data dump.
- **Analysing process DLLs**, handles and dumps to detect potential malwares, identify rogue processes and to check for signs of a rootkit or evidence of code injection.
- **Examining network traffic logs** and other data to identify any suspicious network activity, such as connections to malicious IP addresses or unusual traffic patterns.
- **Retrieving SSL keys and certificates** to investigate potential security breaches and to perform security assessments.



Network Management

- **Packet capturing** using open source tools and saving packets (pcap files) for future analysis and logging.
- **Flagging logs** with suspicious hosts/keywords.
- **Bandwidth utilization** analysis to identify usage patterns.
- **Network topology** and **ISP** info logging to provide location-based information.
- **Real-time malware and anomaly detection** in network traffic using machine learning techniques like Decision Trees and SVMs.

Problem Statement Idea & Approach

Cloud Network

Cloud Communication and forensic is another crucial element of the application. The app will allow us to:

- ➔ Remotely analyze and perform **forensic investigations** when target device(s) is/are not feasible or practical.
- ➔ **Alert & User Notifications for Malicious** behaviors to help prevent data breaches and minimize cyber-attacks.
- ➔ Utilizes **HTTP, TCP/IP protocols** for communication between the **cloud and microservices**.
- ➔ **Amazon S3 and Storage Bucket**, which can be useful for securely storing and retrieving large backups. However, an additional database would be used for storing immediate data.

Use Cases

- ➔ **Intellectual Property (IP) Theft Investigation:** Dump Files & analysis for file changes can be used for File History, and recovering hidden/encrypted files in the target machine.
- ➔ **Malware Analysis:** Realtime Network Analysis & AI-based Malware Detection can help reducing data-breaches and cyber-security attacks in a machine.

Business Model

- ➔ **B2B** → Suite that provides customized realtime forensic and analysis for Office Laptops and Servers to prevent Data Breach & Cyber-Attacks.
- ➔ **Cloud-Based Subscription Service** providing the consumer a cloud admin UI for Server Management.

Libraries / Dependencies

- ➔ API's such as **PowerForensics** can be used for File Forensics.
- ➔ **Volatility CLI** for Analysis of Dump & DLLs.
- ➔ **TShark CLI** for Packet Logging.
- ➔ Libraries such a **Sci-Kit Learn & NLTK/Spacy** for Machine Learning.

Technology Stack

- Node.js , Electron
- Tensorflow/Pytorch
- Go
- gRPC
- WebSockets
- AWS
- Database (SQL based)

Team Member Details

Sr. No.	Name of Team Member	Branch *(Btech/Mtech/PhD etc):*	Stream *(ECE, CSE etc)*	Year	Position in team *(Team Leader, Front end Developer, Back end Developer, Full Stack, Database management etc.)*
1	Ausaf Ahmad	Btech	CSE	2024	Team Leader,Full Stack
2	Mohammad Sarfraz Alam	Btech	ECE	2024	AI/ML, Full Stack
3	Husain Shahid Rao	Btech	CSE	2024	AI/ML, Full Stack
4	Shairin Meraj	Btech	CSE	2024	Front End Developer
5	Sparsh Mahajan	Btech	CSE	2024	Backend Developer
6	Huzaif Malik	Btech	ECE	2025	Full Stack Developer

Team Mentor/s Details

Sr. No.	Name of Mentor	Category (Academic/Industry):	Expertise (AI/ML/Blockchain etc):	Domain Experience (in Years)
1	Ahmad Hassan Ansari	Industry	Software Development	2+
2				