**A SYNOPSIS OF PROJECT ON**

**HackShield**

(KCA 451)

Session 2024-25

Submitted In Partial

Fulfillment of The Requirements for the Award of the Degree of

Master of Computer Applications

By

Himanshu Khatri

(2301920140068)

Under the Supervision of

(Mr. Akhilesh Nagar)



Department of Master of Computer Applications G.L. Bajaj Institute of Technology &Management Greater Noida

**PROJECT TITLE: HACKSHIELD**

For cybersecurity, the demand has increased for effective and powerful digital forensic tools. Digital Forensics Toolkit came to fill the gap with an array of solutions to digital evidence analysis and security incident response.

**Features:**

* **File Metadata Analysis**: Identifies key information such as file type, size, and MD5 hash to facilitate authentication of file integrity and authenticity.
* **Malware Detection with YARA:** YARA analyzes identified malware signatures through file scans by using rules which detect hazardous content immediately.
* **Deleted File Recovery:** The system employs deleted file recovery tools to maintain crucial evidence in current forensic investigations.
* **Network Packet Analysis:** Enables teams to sniff network traffic while inspecting traffic patterns for identifying potential threats alongside suspected breaches and unauthorized data transfers.
* **Ease to Use Interface:** Users can avoid complicated command-line interfaces by accessing the easy-to-use Tkinter graphical user interface that enables them to complete their forensic operations.

**OBJECTIVE OF THE PROJECT**

The main purpose of HackShield is to construct an Artificial Intelligence-based Digital Forensics Toolkit to assist cybersecurity experts alongside forensic investigators and IT security operators in their cyber-attack identification and analytical and defensive efforts. The proposed end-to-end forensic investigation framework will provide cyber protection through its components including malware discovery and file inspection together with file recovery as well as network traffic analysis and encryption examination services.

**Principal Objectives:**

* **File Integrity & Metadata:** The system will perform File Integrity & Metadata Analysis by generating hash values and discovering file anomalies in addition to extensive file metadata.
* **AI and YARA:** The implementation of AI and YARA rules allows the system to detect previously identified malware and previously unknown malicious programs in files.
* **File Recovery:** The tool recovers hidden or erased files through the deleted file recovery functionality.
* **Packet Monitoring:** Real-time network packet monitoring using Trap tools and analysis methods serves to detect security threats through network behavior detection.
* **Encryption & Password Security**: Test password strength, analyze encryption techniques, and attempt decryption of weakly secured files.
* **Generation of Forensic Report**: Store and generate forensic logs securely to assist audit and legal investigations.
* **GUI and Web Dashboard**: Provide an easy GUI and web-based dashboard for easy forensic investigation.

With the integration of machine learning, cryptography, and network security principles, HackShield will be a powerful forensic tool to successfully counter cyber-attacks.

**PROBLEM STATEMENT**

### As the new digital age unfolded, cyber-attacks including malware infection, data compromise, and unauthorized access became more high-tech and consequential attacks on people, organizations, and law enforcement agencies. Classical forensic tools are costly, less efficient, or are manual and it is not easy for cyber security professionals to simply scan files, identify malicious behavior, undelete data, and monitor network traffic.

### Apart from this, encryption and password protection are absolutely important in cyber forensics, but none of the current solutions have an in-built function for quantification of encryption strength and recovery of deleted or encrypted information. Failure to provide a cost-effective, AI-based, and user-friendly forensic tool makes investigation in cyberspace cumbersome and time-consuming.

### **HackShield aims to solve these challenges by:**

* **Providing a Digital Forensics Toolkit that is AI-powered and can scan files, perform malware scans, recover deleted data, and examine network traffic.**
* **Enhancing cybersecurity investigations with automated threat detection, encryption analysis, and forensic report generation.**
* **Offering an easy-to-use and accessible solution to IT security teams, forensic investigators, and cybersecurity experts.**

**HackShield** will serve as a **comprehensive and intelligent forensic toolkit**, helping users detect cyber threats, recover digital evidence, and enhance security investigations efficiently.

**BACKGROUND**

In the era of information, data breach, cyber espionage, and malware attack have grown manifold, impacting individuals, organizations, and government ministries across the globe. As hackers improve hacking techniques, more advanced, automated, and AI-based forensic investigation tools are needed more than ever.

**Why Digital Forensics Matters?**

Digital forensics is the process of examining digital evidence to identify cyber threats, establish cybercrimes, and provide data security. Conventional forensic tools are in short supply, including:

* **High Costs**: Forensic tools are costly and cannot be managed by small organizations.
* **Limited Capabilities**: Certain tools specialize in a specific area such as malware detection or file recovery, without interdisciplinary focus.
* **Manual Investigations**: Manual investigation is included in all forensic processes, which makes them time consuming and prone to errors.

**How HackShield Fills This Gap?**

HackShield is an intelligent digital forensics solution that includes:

* **File Analysis**: Generation of hash values and recovery of metadata to ascertain file integrity.
* **Malware Detection**: Malware and unknown malware detection by YARA rule and machine learning.
* **Recovery of Deleted Files**: Efficient recovery of deleted and hidden files.
* **Network Traffic Analysis**: Detection of security events through real-time network traffic inspection and analysis.
* **Encryption & Password Security**: Checks for the strength of encryption and decryption attempt.

As ransomware, cyberattacks, and data breaches become more frequent, HackShield will become a complete, affordable, and AI-based forensic tool that will assist security professionals in identifying cyber threats, retrieving stolen data, and safeguarding digital assets.

**TOOLS AND PLATFORM**

### **Tools, Platforms, and System Requirements – HackShield**

HackShield is designed to operate efficiently across multiple platforms with well-defined hardware and software requirements. The project uses modern **cybersecurity, forensics, and AI technologies** to ensure a best experience for forensic investigators and security professionals.

### **1. Development Tools and Platforms**

#### ****Programming and Frameworks****

* **Backend:** Django (for managing user authentication, database, and report generation)
* **API Services:** Flask (for handling file and network analysis requests)
* **Frontend:** HTML5, CSS3, JavaScript (Bootstrap for styling)
* **Cybersecurity & Forensics Libraries:**

1. PyShark (Network Packet Analysis)
2. Malware Detection (YARA)
3. python-magic (File Metadata Analysis)
4. hashlib (File Hashing)
5. Cryptodome (File Encryption & Decryption)

* **Machine Learning Tools:** TensorFlow, Scikit-learn (for AI-powered malware detection)

#### ****Database & Storage****

* **Database:** SQLite, MySQL
* **Storage:** Local File System, Cloud Storage (AWS S3, Google Drive API – optional)

#### ****Hosting & Deployment Platforms****

* **Operating Systems:** Windows, Linux, macOS (Cross-platform compatibility)
* **Hosting:** AWS, Heroku, DigitalOcean (for cloud deployment)
* **Containerization (Optional):** Docker for scalable deployment

### **2. Hardware Requirements**

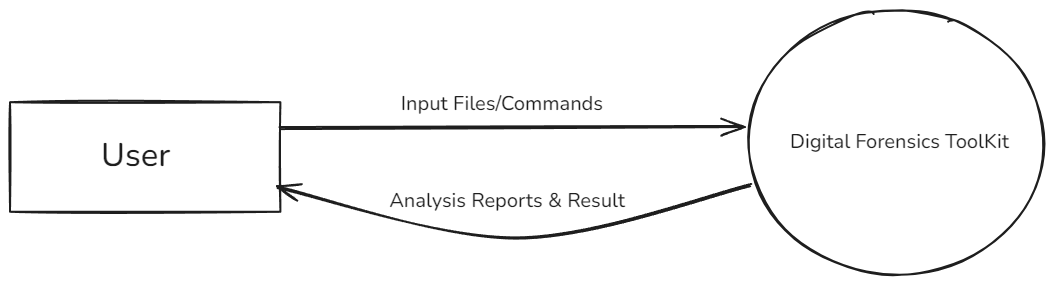
|  |  |  |
| --- | --- | --- |
| Component | Minimum Requirements | Recommended Requirements |
| Processor | Intel Core i5 (or AMD equivalent) | Intel Core i7/i9 |
| Ram | 8 GB | 16 GB or higher |
| Storage | 100 GB HDD | 256 GB SDD or higher |
| GPU | Integrated Graphics | NVIDIDIA RTX 2060 |
| Network | Stable internet connection | High-Speed network |

### **3. Software Requirements**

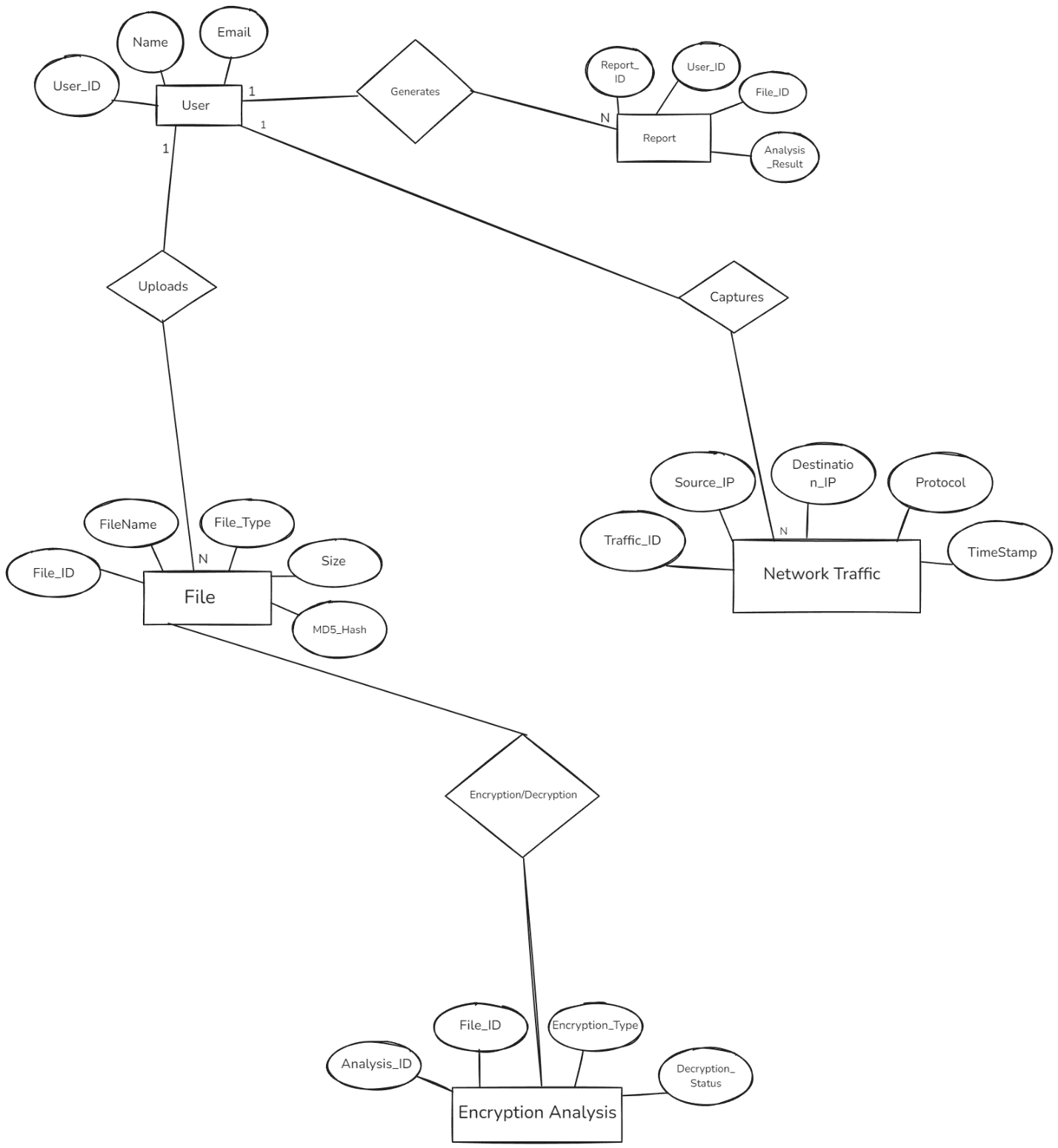
|  |  |
| --- | --- |
| **Software** | **Required Version** |
| Operating System | Windows 10/11, Linux, macOS |
| Python Version | Python 3.8 or higher |
| Database | SQLite 3/ MySQL 8 |
| Web Frameworks | Django 4, Flask 2 |
| Forensic Tools | Wireshark, TShark, YARA, PyShark |

**DFD & ER Diagram**

**Level-0 DFD:**

****

**ER Diagram:**

****

### CONCLUSION

### HackShield functions as an artificial intelligence-based powerful digital forensics tool for use in

### The tool assists investigators in solving contemporary computer-based challenges pertaining to digital forensics and cybersecurity.

### Several sophisticated digital attacks occur daily which requires an immediate solution through easy-to-use automated smart tools. The tool serves forensic purposes by effectively examining digital evidence and security breaches while retrieving needed data.

### valuable data.

### This multi-tool system performs an extensive file examination function and malware scanning alongside data restoration abilities from deleted files and network traffic examination and encryption key analysis capabilities.

### HackShield uses machine learning with network forensics and cryptography techniques after its implementation.

### **Key Achievements**

### **Effective File Analysis**: Reads the metadata, computes hash values, and maintains file integrity.

### **Artificial Intelligence-Driven Malware Detection**: Finds known and unknown attacks with YARA rules and ML rules.

### **Returns File Recovery**: Reconstructs lost or concealed files from storage units.

### **Virtual Network Packet Examination**: Scans and detects network packets to attempt to find evil deeds.

### **Crypto and Password Protection**: Encrypt strength testing, finds vulnerabilities, and will attempt to decrypt if possible.

### **Secure Forensic Log Processing**: Processes forensic logs at scale, produces comprehensive reports, and ensures data integrity.

### **FUTURE SCOPE**

HackShield is end-to-end automated digital forensics and significantly increases the speed, accuracy, and efficiency of digital forensic analysis. Time-consuming, manual, and labor-intensive is the nature of conventional forensic analysis, but HackShield automated them and AI-based analysis.

The future can have the following inclusion with HackShield:

* **Real-Time Security Monitoring**: For real-time detection and prevention of cyber-attacks.
* **AI-Based Threat Prediction**: With deep learning-based prediction and combat of future security threats.
* **Cloud-Based Digital Forensics**: Forensic analysis and storage in the cloud.
* **Blockchain-Based Evidence Integrity**: Integrity of evidence with tamper-evident forensic report storage and digital evidence.
* **Integration with Law Enforcement Systems**: Assistance to police, military, and intelligence services in cybercrime investigations.

HackShield is a forthcoming next-gen initiative in digital forensic research and cybersecurity with an economical, scalable, and smart forensic suite. With threats over the internet persistently evolving, this initiative will be a tool for ever-improving cybersecurity, forensics driven by AI, and secure online investigation.

**REFERENCES**

[1] A. Casey, G. Stellatos, and J. Jansen, **"Network forensics analysis: Tools and techniques,"** IEEE Security & Privacy, vol. 13, no. 3, pp. 26-34, May-Jun. 2015. DOI: 10.1109/MSP.2015.45.

[2] A. S. M. Kayes, M. A. Islam, and P. Watters, **"A machine learning approach to detecting malware using network traffic analysis,"** IEEE Access, vol. 8, pp. 211040-211051, 2020. DOI: 10.1109/ACCESS.2020.3038253.

[3] E. Hjelmvik and W. John, **"Breaking and improving protocol obfuscation,"** Proc. IEEE Int. Workshop Traffic Monitoring Anal. (TMA), pp. 3-15, Apr. 2010. DOI: 10.1007/978-3-642-12365-8\_1.

[4] S. Garfinkel, **"Digital forensics research: The next 10 years,"** Digital Investigation, vol. 7, pp. S64-S73, Aug. 2010. DOI: 10.1016/j.diin.2010.05.009.

[5] F. Pagani, M. Caselli, and M. A. C. Fernandez, **"Cyber threat intelligence: Automatic IoC extraction and analysis,"** IEEE Trans. Dependable Secure Comput., vol. 19, no. 2, pp. 1200-1216, 2022. DOI: 10.1109/TDSC.2021.3072836.

[6] B. Carrier, **"File System Forensic Analysis,"** Addison-Wesley, 2005.

[7] H. Liu, **"Cybersecurity and Digital Forensics: Investigating Network Intrusions and Cybercrime,"** Springer, 2018.

[8] N. L. Petroni and W. A. Arbaugh, **"Memory analysis in digital forensics,"** CRC Press, 2019.

[9] National Institute of Standards and Technology (NIST), **"Guide to Integrating Forensic Techniques into Incident Response,"** Special Publication 800-86, 2006. [Online]. Available: <https://nvlpubs.nist.gov/>.

[10] MITRE ATT&CK Framework, **"Cyber Threat Intelligence for Network Security,"** [Online]. Available: https://attack.mitre.org/.