WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber Tool for Digital Forensic Investigation

Pratiksha Bombale[1], Shravani Adhav[2], Preeti Bhoge[3], Anuja. D. Mate[4]

[1] Department of Computer Technology Sou. Venutai Chavan Polytechnic, Pune Email: pratikshabombale2005@gmail.com
[2] Department of Computer Technology Sou. Venutai Chavan Polytechnic, Pune Email: shravaniadhav2@gmail.com
[3] Department of Computer Technology Sou. Venutai Chavan Polytechnic, Pune Email: preetibhoge212@gmail.com
[4] Lecturer Department of Computer Technology Sou. Venutai Chavan Polytechnic, Pune Email: anujamate12@gmail.com

ABSTRACT :

The present project is dedicated to the creation of a Cyber security tool for digital Forensic Investigation using modern web technologies. The challenge lies in creating a comprehensive tool that efficiently gathers, analyzes, and preserves digital evidence from multiple sources while ensuring the integrity of the data for legal proceedings. To address this issue, this project is dedicated to developing a cybersecurity tool tailored for digital forensic investigations using modern web technologies. The tool will integrate several key features, including web browser security, file detection, and network log analysis. The web browser security feature will allow investigators to examine browsing history, cookies, cached files, and downloads, helping identify malicious activities or suspect online behavior. The email security module will focus on analyzing email headers, attachments, and metadata to detect phishing, malware, or unauthorized access. Network log monitoring will enable the tool to detect unauthorized connections and other anomalies that may signal a security breach. In conclusion, this cyber forensic tool will provide investigators with a powerful platform to detect, trace, and analyze cyber threats across various domains. By integrating features that cover browser security, email analysis, and network log monitoring, the tool will enhance the accuracy and efficiency of digital forensic investigations while ensuring that all evidence is preserved for legal use.

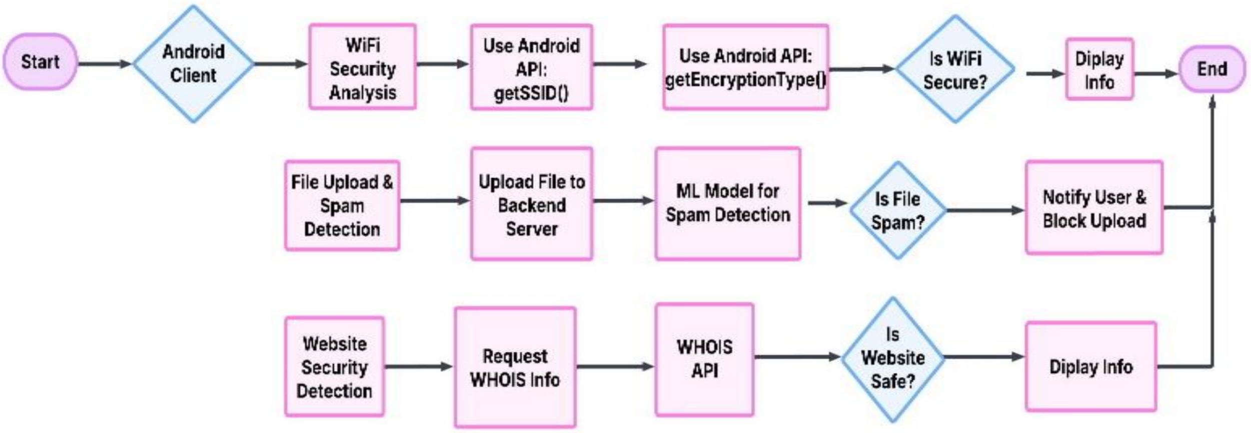
Keywords: Cybersecurity, Digital Forensics, Cyber Threats, Browser Security, File Detection, Network Log Analysis, Email Security, Digital Evidence, Threat Analysis.

1.INTRODUCTION :

Cyber tools for digital forensic investigation have developed in response to the growing complexity of cybercrime, starting with the rise of computers in the 1970s and 1980s. Initially, crimes like financial fraud and hacking were difficult to investigate due to the lack of standardized methods or tools to retrieve and analyze digital data[2]. As the internet expanded in the 1990s, the need for specialized tools became urgent, leading to the creation of early forensic software like EnCase and Forensic Toolkit (FTK). These tools enabled investigators to recover deleted files, examine file systems, and present digital evidence in court. The 2000s saw the increasing importance of mobile devices, cloud computing, and encrypted data in investigations. This prompted the development of more advanced cyber forensic tools capable of extracting data from a wider range of sources, including smartphones, social media platforms, and cloud storage. Alongside technological advances, the legal framework for handling and presenting digital evidence became more structured, ensuring that evidence could meet judicial standards. Today, with the integration of AI, machine learning[3], and big data analytics, cyber forensic tools are more powerful and efficient. They can handle new challenges such as Internet of Things (IoT) forensics and blockchain investigations[6], making them crucial in combating modern cybercrime.

2.SYSTEM ARCHITECTURE :

Fig 1.1


Start
Android Client
WiFi Security Analysis
Use Android API: getSSID()
Use Android API: getEncryptionType()
Is WiFi Secure?
Diplay Info
End
File Upload & Spam Detection
Upload File to Backend Server
ML Model for Spam Detection
Is File Spam?
Notify User & Block Upload
Website Security Detection
Request WHOIS Info
WHOIS API
Is Website Safe?
Diplay Info

The fig 1.1 is a flowchart representing a cybersecurity process related to an Android client[6]. It outlines multiple security checks, including:

1. **WiFi Security Analysis:**
- The Android client uses APIs (getSSID() and getEncryptionType()) to analyze the WiFi security.
- If the WiFi is secure, information is displayed; otherwise, the process ends.

2. **File Upload & Spam Detection:**
- Files are uploaded to a backend server.
- A machine learning model checks for spam.
- If the file is spam, the user is notified, and the upload is blocked.

3. **Website Security Detection:**
- Whose information is requested via an API.
- The website's safety is evaluated.
- Information about website security is displayed.

The fig 1.1 is a flowchart visually represents a structured cybersecurity approach for handling WiFi security, file uploads, and website safety within an Android application.

3.PROPOSED METHODOLOGY :

1. Gathering and Ingestion of Data[2]:

- Describe the sources of the data: Determine the precise categories of information that will be gathered, such as network logs and email message browser history

2. Data ingestion:

- Establish a pipeline for data ingestion: Establish a system for gathering and storing data from sources.
- Data normalization: By converting data into a standard format, you may guarantee data compatibility and consistency.

3. Engineering features:

Extrapolate pertinent features: Determine important characteristics from the gathered data that can be analyzed, like:

- Sender, recipient, subject, body, attachments, external links, images, and web content are all examples of email metadata.

from current data to boost analysis skills, such as:

- Time-based features (time of day, day
- Behavioral characteristics (user interactions, click patterns)
- Features dependent on domains (URL structure, TLD, WHOIS data)

4.Preprocessing Data:

- Deal with missing values: Use methods like imputation or deletion to deal with missing data
- Deal with outliers: Find and deal with outliers that could distort the findings of an analysis.
- Normalize data: To enhance model performance, scale numerical features to a shared range.

Development of Machine Learning Models:

- Choose suitable algorithms: Select machine learning algorithms that are appropriate for the given tasks, like: Category (e.g., Random Forest, SVM, Gradient Boosting)
- Software Development Agile is the model utilized.
- Anomaly detection (e.g., One-Class SVM, Isolation Forest)
- Clustering, such as hierarchical clustering and K-means
- Develop and assess models: Use labeled or unlabeled data to train models, then use the right metrics to assess how well they perform.
- Iterative model refinement: Make constant improvements to models in response to user feedback and performance indicators.

4.IMPLEMENTATION :

4.1Technology Frontend:

Android Mobile Application (Java): Java for Android was used in the development of this application to enable file uploading, spam detection, and user interaction.
Backend: FastAPI (Python) is a high-performance, lightweight API framework that manages file uploads and spam identification.
PyMuPDF & NLTK: For processing natural language data and extracting text from PDFs.
Scikit-learn & Joblib: For machine learning models used in spam detection.
Pandas: For managing and modifying data.
Additional Libraries & Technologies[7]:
The Android SDK[5] is used to create and execute Android applications.

4.2 Roles of users

1. To identify spam, the user (Android App User) uploads files (text, PDF).

gets information on whether or not the file is spam.
examines the criteria and justifications for classification.
2. The user uploads a file, which is received by the server (Backend-FastAPI).
Processes the file to extract text.
Uses machine learning to analyze and classify the file as spam or not.
Returns the results to the user, including reasons for spam detection.

5. SCOPE FOR FUTURE WORK :

Given the increasing complexity of cyberthreats, your cyber tool's potential for forensic digital investigation is enormous[3]. The use of AI and machine learning to automate investigative procedures, like anomaly identification and log analysis, is a crucial area of study that will improve the precision and speed of forensic operations. By using previous data to predict future threats, predictive analytics could also be used to improve proactive defence's[4]. Cloud forensics will become increasingly important as cloud computing grows. It will be crucial to extend the tool's capabilities to look into and examine data from cloud environments, such as logs and snapshots of virtual machines. Furthermore, adding capabilities for blockchain forensics, Internet of Things (IoT) investigations, and mobile device forensics can expand the tool's reach.Overall, these enhancements will provide deeper insights, faster response times, and better adaptability to the changing nature of cybercrime.

6.CONCLUSION :

To sum up, cyber technologies for digital forensic investigations[1] offer priceless benefits that improve the effectiveness, precision, and dependability of gathering and analyzing digital evidence. These solutions greatly speed up the investigation process while reducing errors by automating difficult processes, guaranteeing the integrity of the evidence, and facilitating multi-platform and extensive investigations[7]. They are crucial in locating important information, guaranteeing legal compliance, and assisting with incident response because of their proficiency in data recovery, pattern recognition, and metadata analysis

7.ACKNOWLEDGMENT

We appreciate Ms. A.D. Mate, our guide, for her invaluable advice and assistance with this endeavor. The availability of programs like Android Studio, Java, and Firebase, which simplified the application development process, is greatly appreciated. The project was a very unique experience, and we are grateful for the direction and innovative applications that made it possible.

8.REFERENCES :

[1] Vihara Fernando viharaf@gmail.com Department of Computer Systems Engineering, Faculty of Graduate Studies and Research, Sri Lanka Institute of Information Technology, New Kandy Road, Malabe. “Cyber Forensics Tools: A Review on Mechanism and Emerging Challenges”

[2] Mary Geddes De Montfort University Leicester, UK Dr Pooneh Bagheri Zadeh De Montfort University Leicester, UK “Forensic Analysis of Private Browsing”

[3] Ifeoma U. Ohaeri1 Computer Science Department North-West University Mafikeng North West Province, South Africa Bukohwo M. Esiefarienhe2 Computer Science Department North West University Mafikeng North-West Province, South Africa Digital “Forensic Process Model for Information System and Network Security Management”

[4] Arjun Anand V,Buvanasri A K,Meenakshi R,Karthika S, Ashok Kumar Mohan,2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP) Year: 2020 “PeopleXploit: A hybrid tool to collect public data ”Year: 2020

[5] S. Al Sharif1, M. Al Ali1, N. Al Reqabi1, F. Iqbal1, T. Baker2, A. Marrington1 1College of Technological Innovation, Zayed University, UAE 2Department of Computer Science, Liverpool John Moores University, UK “Magec: An Image Searching Tool for Detecting Forged Images in Forensic Investigation”

[6] Arpita Singh,Nilu Singh,Sanjay K. Singh,Sandeep k. Nayak “Cyber-Crime and Digital Forensics: Challenges Resolution IEEE Xplore”

[7] Mohammad Rasmi Al-Mousa,Qutaiba Al-Zaqebah,Ala'a Saeb Al-Sherideh,Mohammed Al Ghanim,Ghassan Samara,Sattam Al-Matarneh,Mahmoud Asassfeh 2022 International Arab Conference on Information Technology (ACIT) “Examining Digital Forensic Evidence for Android Applications IEEE Xplore” Year: 2022