

Digital Forensic Analysis Platform Practical Report

1. Introduction to the Digital Forensic Analysis Platform

This project focuses on developing a **Digital Forensic Analysis Platform** designed to support cybersecurity professionals, forensic investigators, and researchers in analyzing digital evidence efficiently and securely. The platform is equipped to handle network traffic data (e.g., PCAP files) and perform malware analysis, providing users with detailed forensic reports.

Key features include:

- **User-friendly interface** for seamless navigation
 - **Secure upload and storage** of forensic evidence
 - **Real-time analysis** and report generation for forensic investigations
-

2. Project Goals and Technical Objectives

The primary objectives of this project were:

1. **To create a secure platform** for uploading and analyzing network packets and malware files.
 2. **To perform in-depth packet analysis** using tools like PyShark and Wireshark, extracting information like IP addresses, protocols, and timestamps.
 3. **To provide malware analysis capabilities**, identifying any potential threats in user-uploaded files.
 4. **To generate comprehensive forensic reports** that summarize findings for further analysis or legal purposes.
-

3. Technical Tools and Frameworks Used

This section covers the main technologies integrated into the platform:

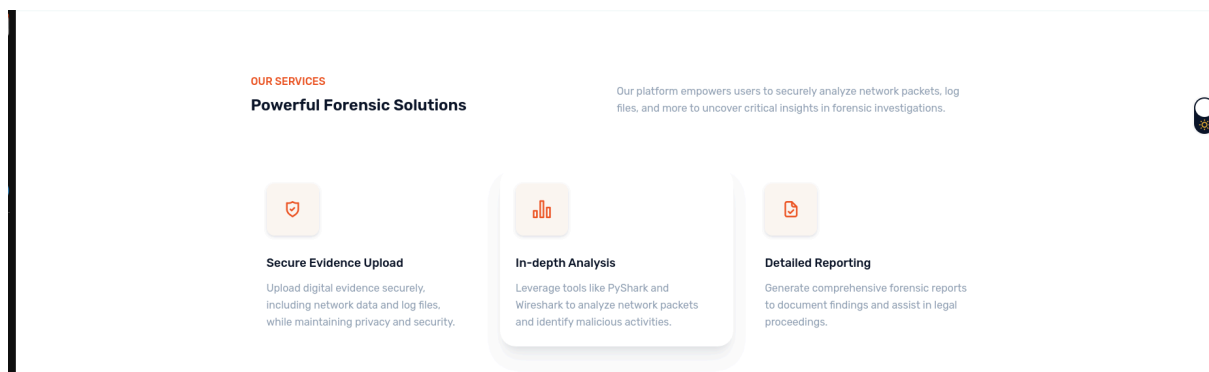
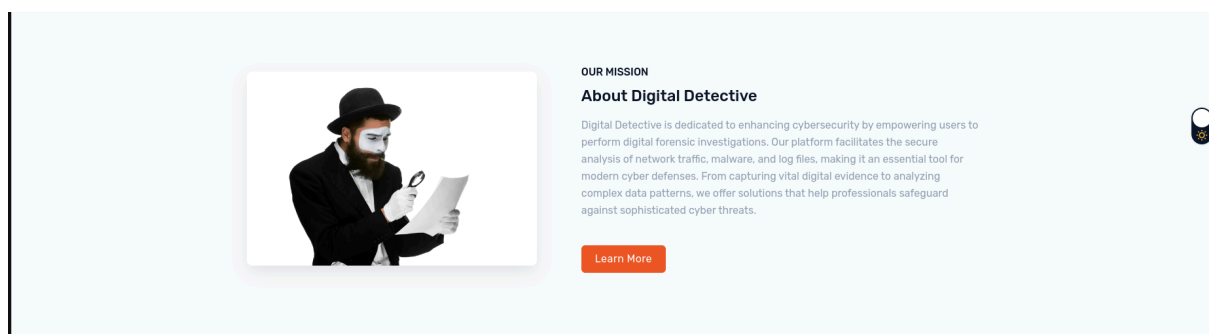
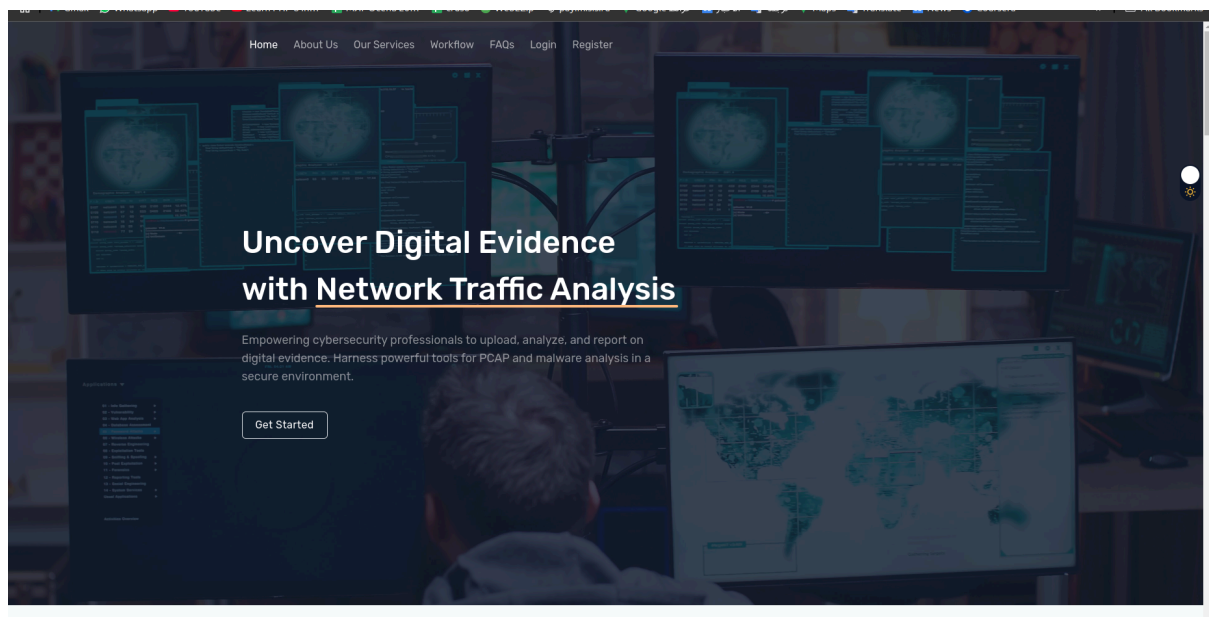
- **Django**: Used as the web framework for handling the platform's backend. Django manages user authentication, file handling, and secure data storage.
- **PyShark**: A Python wrapper for Wireshark, PyShark is utilized for capturing and analyzing network packet data from PCAP files.
- **Wireshark/TShark**: Wireshark is used for manual packet analysis, while TShark (the command-line version) provides automated packet processing and analysis in the backend.
- **Bootstrap and Tailwind CSS**: These frameworks ensure the frontend is responsive and accessible across devices.

- **SQLite:** Used as the database to store user information, uploaded files, and analysis results.

4. Project Structure and Functionality

4.1 Homepage

The homepage serves as the landing page, providing essential information for all users, particularly those not logged in. It includes an overview of the platform's features and benefits.



كل ما تحتاج معرفته

إجابات عن الأسئلة الشائعة لمساعدتك في استخدام منصتنا بسهولة.



+

١. ما هو البرنامج؟

+

٢. كيف يمكنني إنشاء حساب؟

+

٣. ما هي الملفات التي يمكنني رفعها؟

+

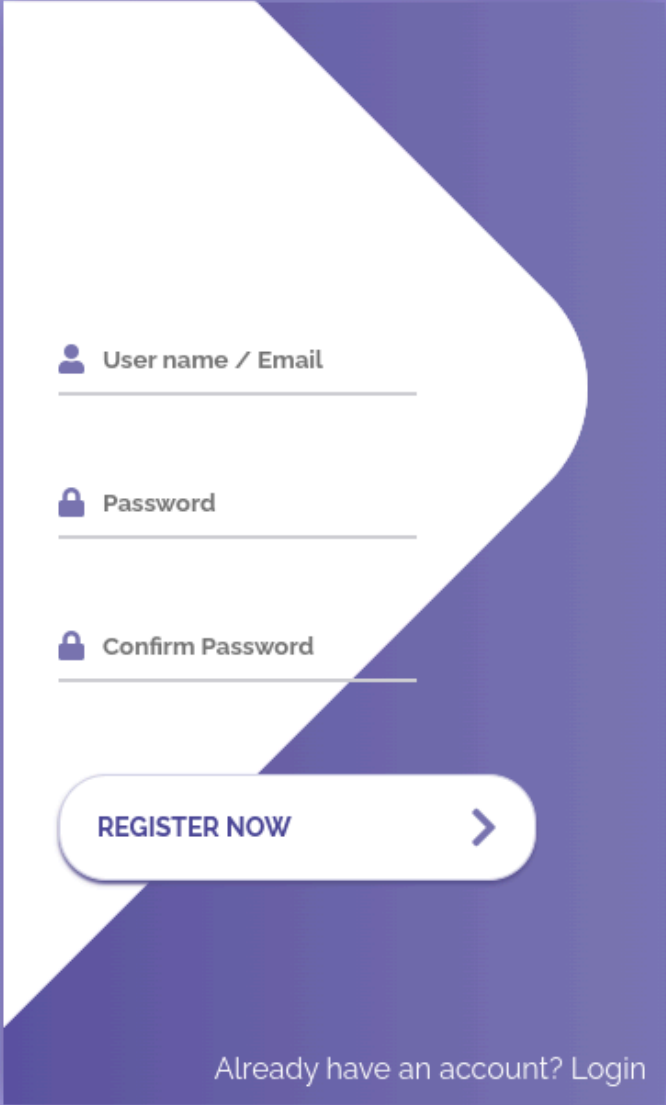
٤. كيف يتم تحليل الملفات؟

+

٥. هل الملفات التي أرفعها آمنة؟

4.2 Register and Login Pages

The Register page allows users to create accounts by entering a username, email, and password. The Login page enables existing users to access their dashboard securely.

The image shows a registration form on a purple gradient background. The form is a white card with a dark purple shadow. It features three input fields with user and lock icons, a 'REGISTER NOW' button with a right arrow, and a 'Login' link at the bottom.

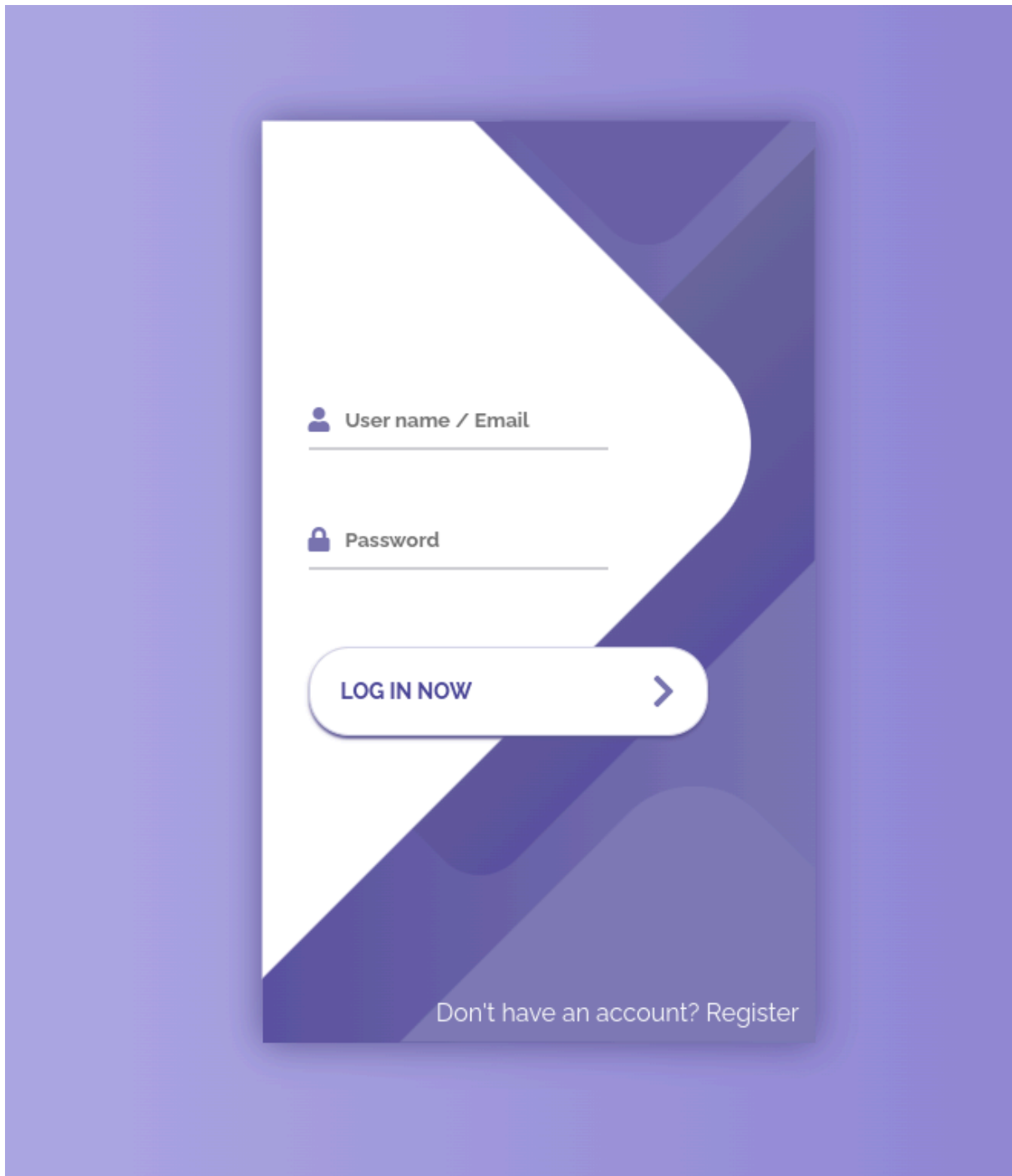
User name / Email

Password

Confirm Password

REGISTER NOW >

Already have an account? [Login](#)

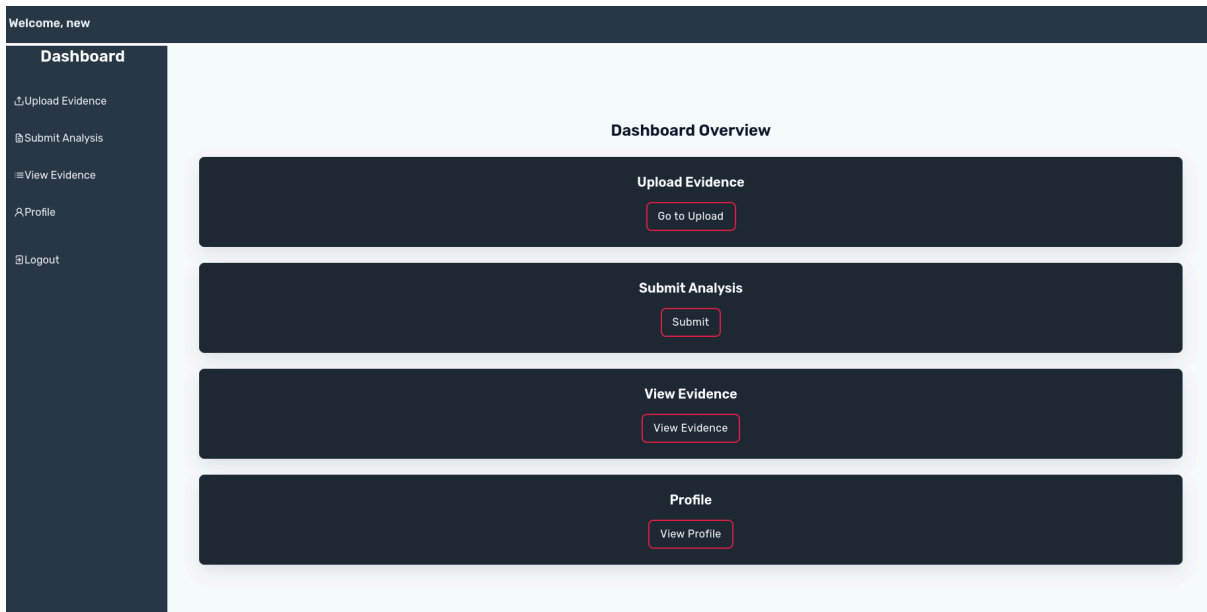


4.3 Dashboard

After logging in, users access the dashboard, where they see a sidebar with options to:

- Upload digital evidence
- Add analysis to the uploaded evidence
- View the list of uploaded evidence

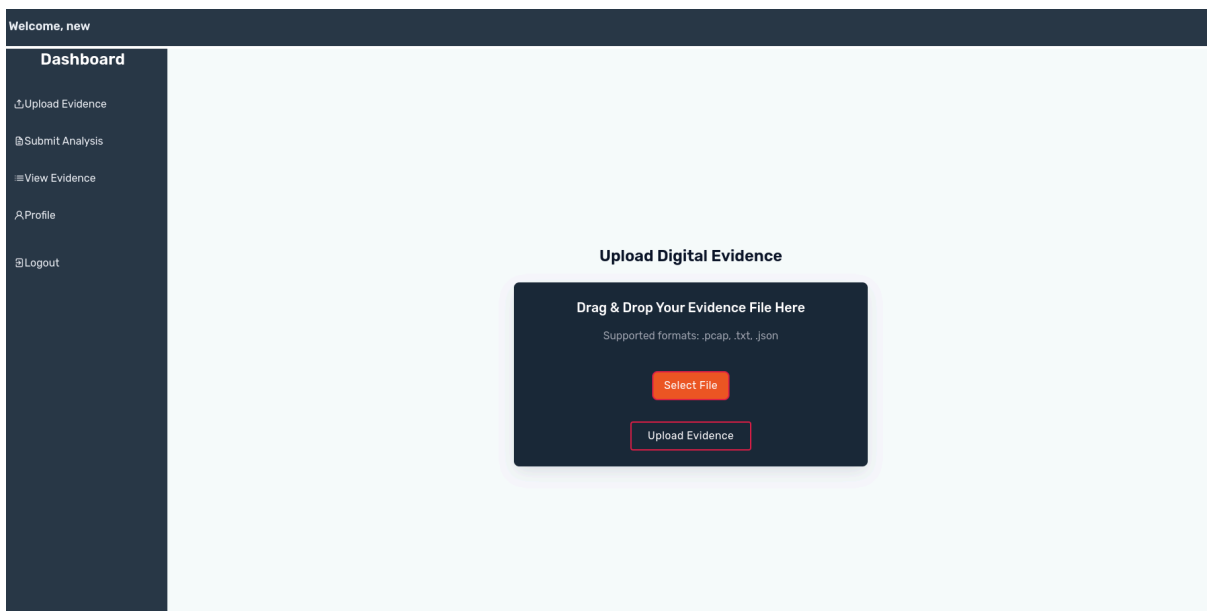
Users can also edit their profile and log out securely.



4.4 Evidence Upload and Management

Purpose: Allows users to securely upload PCAP files, log files, or malware samples.

File Storage and Security: Uploaded files are encrypted and stored in the platform's database, ensuring privacy. The platform supports common file formats for network analysis (e.g., .pcap, .json).



4.5 PCAP File Analysis Using PyShark

Purpose: Analyzes network packets in user-uploaded PCAP files to detect suspicious activities.

Workflow:

- 1. **Packet Capture:** PyShark captures network data and extracts important metadata.
- 2. **Analysis and Visualization:** The platform displays extracted IP addresses, protocols, and packet sizes in a user-friendly table and graph format.

Dashboard

Upload Evidence

Submit Analysis

View Evidence

Profile

Logout

PCAP Analysis for Evidence 60

Packet Capture Data

Packet Number	Protocol	Source IP	Destination IP	Length	Info
1	NBNS	192.168.1.2	192.168.1.255	92	N/A
2	NBNS	192.168.1.2	192.168.1.255	92	N/A
3	_WS.MALFORMED	217.168.1.2	192.168.1.255	92	N/A
4	ARP	N/A	N/A	42	N/A
5	ARP	N/A	N/A	60	N/A
6	_WS.MALFORMED	192.168.1.2	192.168.1.1	76	N/A
7	DNS	192.168.1.2	192.37.115.0	76	N/A
8	DNS	192.168.1.2	192.168.1.1	76	N/A
9	DNS	192.168.1.3	192.168.1.2	144	N/A
10	_WS.MALFORMED	192.168.1.2	192.168.1.1	86	N/A

4.6 Malware Analysis

Purpose: Enables basic malware detection on uploaded files, identifying potential threats.

Process: The platform scans for known malicious patterns within files, alerting users if suspicious indicators are detected.

Welcome, new

Dashboard

Upload Evidence

Submit Analysis

View Evidence

Profile

Logout

Submit Malware Analysis

Fill out the details below:

Evidence

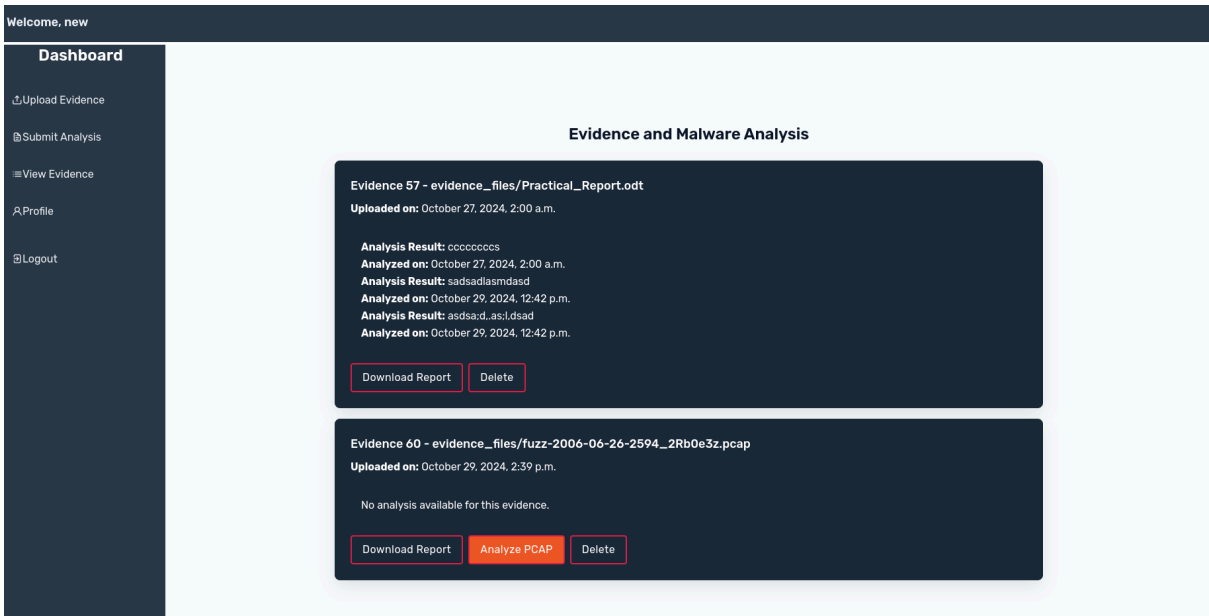
Analysis Result

Submit Analysis

4.7 Forensic Report Generation

Purpose: Provides users with downloadable reports of analysis results.

Report Contents: The forensic report includes key findings such as detected IP addresses, packet data, and timestamps, along with malware analysis results if applicable.



5. Technical Features and Data Security Measures

- **Data Encryption:** All files are encrypted before storage to ensure secure handling of sensitive forensic evidence.
- **Session Management:** User sessions are managed by Django to protect user data and restrict unauthorized access.
- **Role-Based Access Control:** Users have limited access based on their role (e.g., not logged in user vs. logged in user), ensuring that data privacy is maintained.

6. Conclusion

This Digital Forensic Analysis Platform successfully demonstrates how open-source tools can be harnessed to develop a secure and scalable solution for digital forensics. With its user-friendly interface and robust backend, the platform is designed to support users in conducting comprehensive forensic investigations while ensuring data privacy and security.