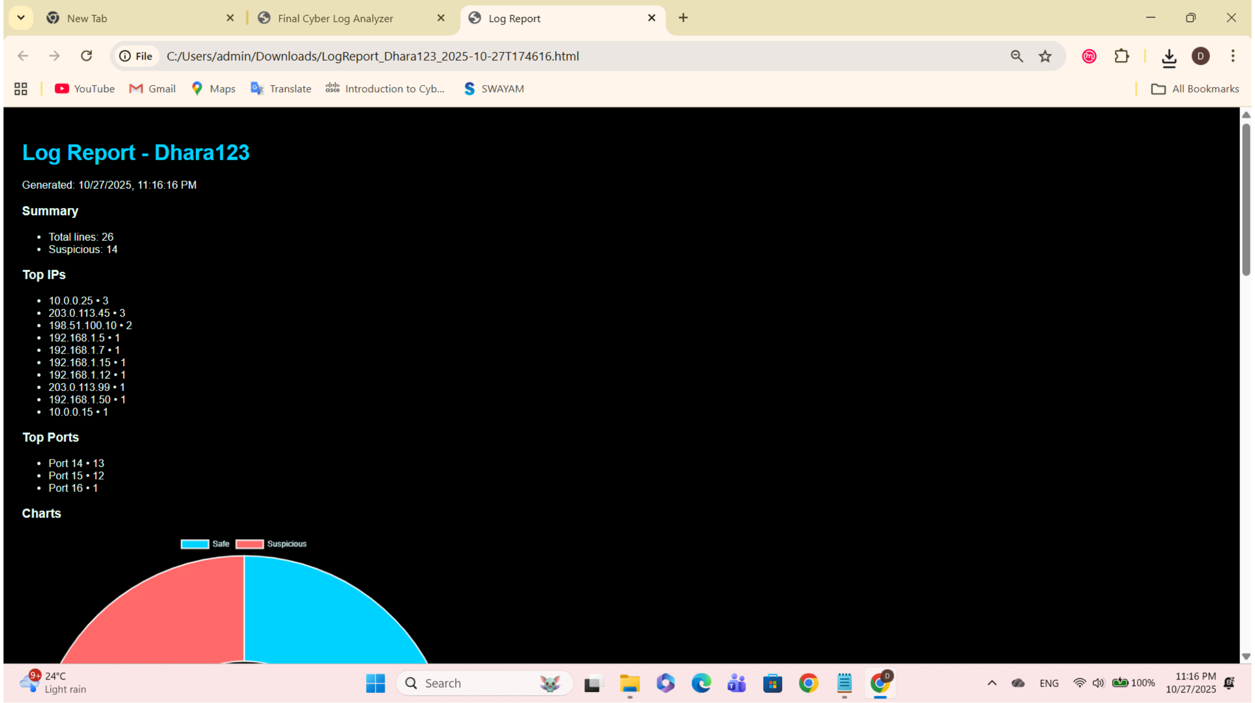
1. INTRODUCTION



Log Report - Dhara123

Generated: 10/27/2025, 11:16:16 PM

Summary

- Total lines: 26
- Suspicious: 14

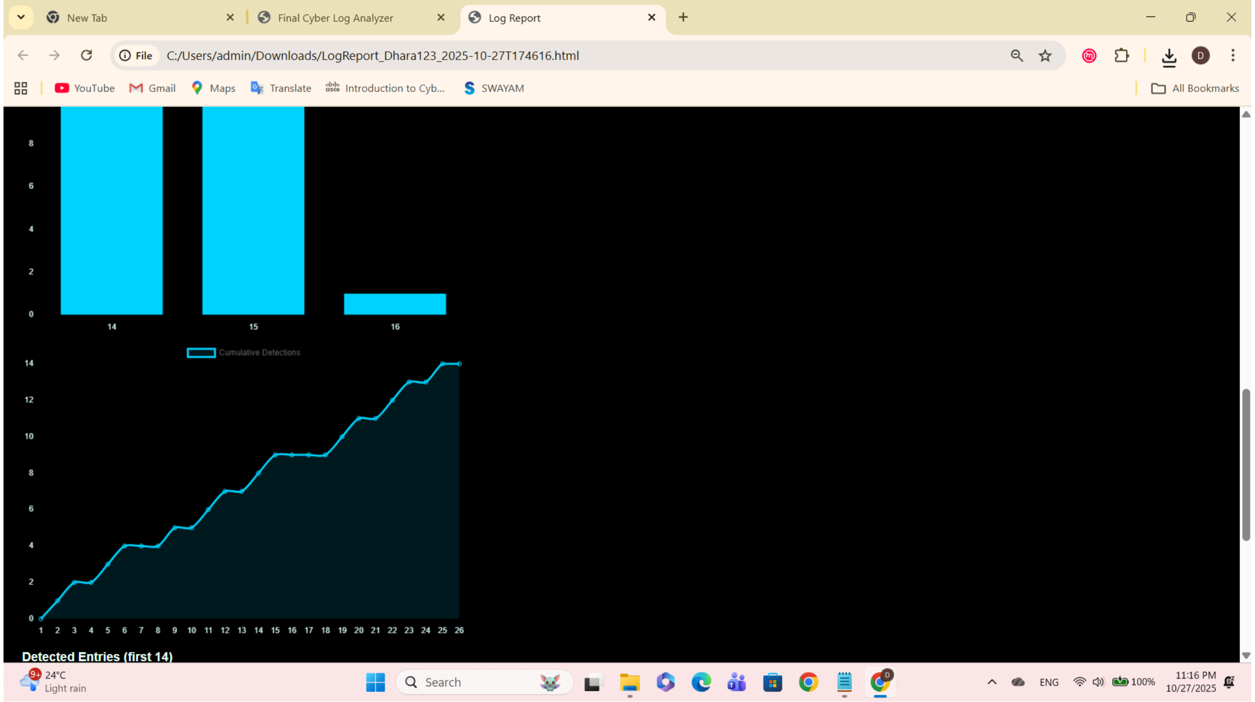
Top IPs

- 10.0.0.25 • 3
- 203.0.113.45 • 3
- 198.51.100.10 • 2
- 192.168.1.5 • 1
- 192.168.1.7 • 1
- 192.168.1.15 • 1
- 192.168.1.12 • 1
- 203.0.113.99 • 1
- 192.168.1.50 • 1
- 10.0.0.15 • 1

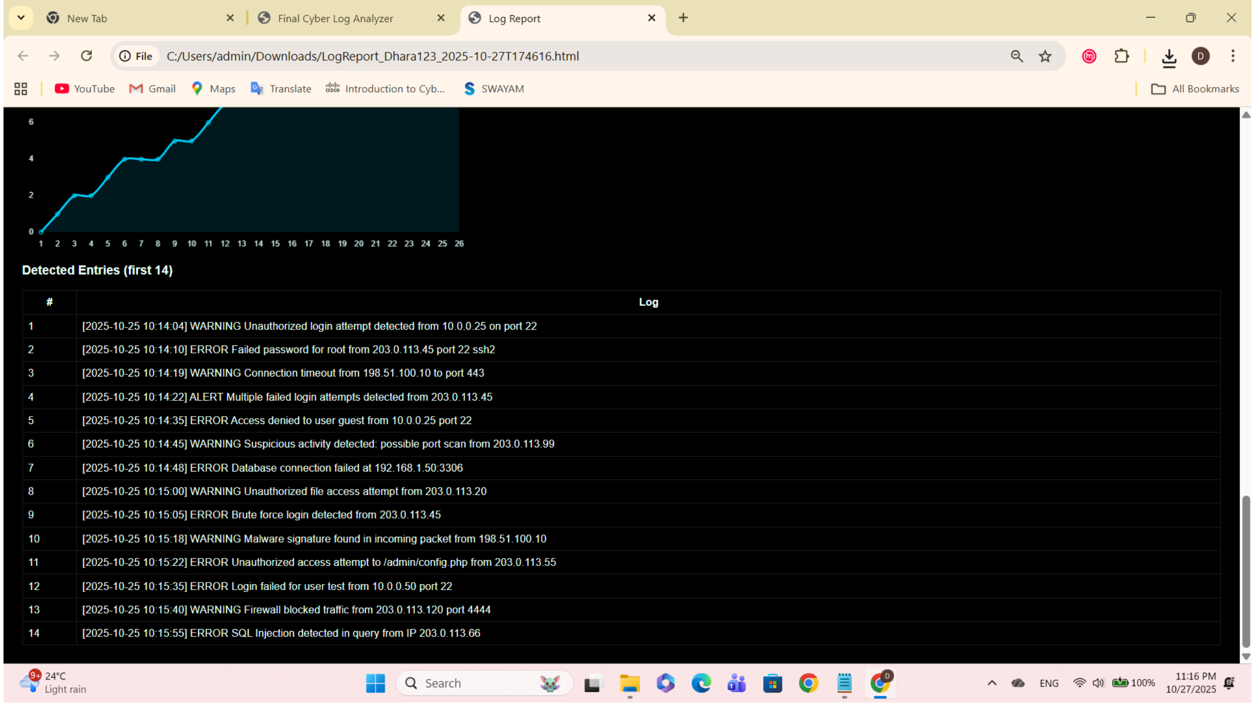
Top Ports

- Port 14 • 13
- Port 15 • 12
- Port 16 • 1

Charts



Detected Entries (first 14)



Detected Entries (first 14)

#	Log
1	[2025-10-25 10:14:04] WARNING Unauthorized login attempt detected from 10.0.0.25 on port 22
2	[2025-10-25 10:14:10] ERROR Failed password for root from 203.0.113.45 port 22 ssh2
3	[2025-10-25 10:14:19] WARNING Connection timeout from 198.51.100.10 to port 443
4	[2025-10-25 10:14:22] ALERT Multiple failed login attempts detected from 203.0.113.45
5	[2025-10-25 10:14:35] ERROR Access denied to user guest from 10.0.0.25 port 22
6	[2025-10-25 10:14:45] WARNING Suspicious activity detected: possible port scan from 203.0.113.99
7	[2025-10-25 10:14:48] ERROR Database connection failed at 192.168.1.50:3306
8	[2025-10-25 10:15:00] WARNING Unauthorized file access attempt from 203.0.113.20
9	[2025-10-25 10:15:05] ERROR Brute force login detected from 203.0.113.45
10	[2025-10-25 10:15:18] WARNING Malware signature found in incoming packet from 198.51.100.10
11	[2025-10-25 10:15:22] ERROR Unauthorized access attempt to /admin/config.php from 203.0.113.55
12	[2025-10-25 10:15:35] ERROR Login failed for user test from 10.0.0.50 port 22
13	[2025-10-25 10:15:40] WARNING Firewall blocked traffic from 203.0.113.120 port 4444
14	[2025-10-25 10:15:55] ERROR SQL Injection detected in query from IP 203.0.113.66

1.1 Project Summary

The Cyber Log Analyzer is a web-based security tool developed to detect and analyze suspicious activities from system or network log files. It automatically scans the uploaded log data, identifies anomalies or potential threats such as failed login attempts, unauthorized access, and error messages, and then visualizes the results using charts and summary reports. This tool helps cybersecurity students and professionals to monitor and enhance system security effectively.

The purpose of this project is to design and implement a tool that:

- Analyzes log files to identify suspicious events.
- Provides a visual representation of the detected threats.
- Generates an easy-to-understand HTML report for users.
- Assists cybersecurity learners in understanding log-based intrusion detection.

1.3 Scope

The scope of this project includes:

- Uploading system or server log files.
- Automatic detection of anomalies and suspicious keywords.
- Interactive dashboard displaying safe vs suspicious logs.
- Report generation for analysis and documentation.
- Usable for educational and basic cybersecurity training purposes.

The tool focuses on log analysis and visualization, not real-time intrusion prevention or packet-level analysis.

1.4 Technical and Literature Review

Log analysis and intrusion detection are crucial in cybersecurity. Existing tools such as Splunk, Graylog, and ELK Stack (Elasticsearch, Logstash, Kibana) are powerful but complex to deploy for beginners.
This project aims to create a **lightweight, educational version** that demonstrates core detection principles using:

- **Frontend:** HTML, CSS, JavaScript

- **Backend (optional):** Python for preprocessing
- **Visualization:** Chart.js
- **Output:** HTML-based report generation

The concept is derived from the principles of **Network Intrusion Detection Systems (NIDS)** like Snort but adapted for static log file analysis in a simpler interface.

2. SYSTEM REQUIREMENT STUDY

2.1 User Characteristics

- **Primary Users:** Cybersecurity students, ethical hackers, and analysts.
- **Knowledge Level:** Basic understanding of log files and security terms.
- **Usage Pattern:** Upload log files → Run scan → View results and report.
- **Goal:** To analyze log data and learn how intrusion detection works.

2.2 Software Requirements

2.2.1 Software Requirements

- **Operating System:** Windows / Linux (Kali recommended for cybersecurity)
- **Programming Language:** HTML, CSS, JavaScript, Python
- **Libraries/Frameworks:** Chart.js, Plotly (optional)
- **Text Editor/IDE:** VS Code / Sublime Text
- **Browser:** Google Chrome, Mozilla Firefox
- **Additional Tools:** Tkinter (for Python UI, optional), Pandas (if data analysis used)

3. SYSTEM ANALYSIS

3.1 Study of Current System

Currently, log analysis in cybersecurity labs requires complex tools like SIEM or manual inspection, which are not suitable for beginners. Such tools are heavy, require high configuration, and are difficult to set up in a learning environment.

3.2 Problems in Existing Systems

- Complexity in installation and configuration.
- Overwhelming data representation without simplified visualization.
- No quick or lightweight option for students.
- Lack of HTML-based easy reporting in real time.

3.3 Requirement of New System

The new system — Cyber Log Analyzer — overcomes the above issues by:

- Providing a simple, browser-based interface.
- Automatically highlighting suspicious log entries.
- Generating clear visual charts.
- Allowing instant HTML report download for documentation.

3.4 Functional Requirements

- **User Registration & Login:** Secure access for different users.
- **Log Upload:** Accept and scan .txt or .log files.

- **Analyzer Engine:** Detect suspicious patterns using keywords.
- **Dashboard:** Show graphical analysis (safe vs suspicious logs).
- **Report Generation:** Export HTML report summarizing results.

3.5 Non-Functional Requirements

- **Performance:** Analyze medium-sized logs efficiently.
- **Usability:** Easy to use for beginners.
- **Portability:** Works on any modern browser.
- **Security:** Only local log data used (no cloud dependency).
- **Maintainability:** Simple structure for future updates.

3.6 Feasibility Study

Aspect	Description
Technical Feasibility	Developed using widely available web technologies; no expensive hardware required.
Operational Feasibility	The tool is user-friendly, needs minimal training, and runs on a local system.
Economic Feasibility	Free and open-source technologies are used, ensuring zero cost development.
Time Feasibility	The system can be implemented within a short duration for educational projects.

4. LIMITATIONS AND FUTURE ENHANCEMENT

4.1 Limitations

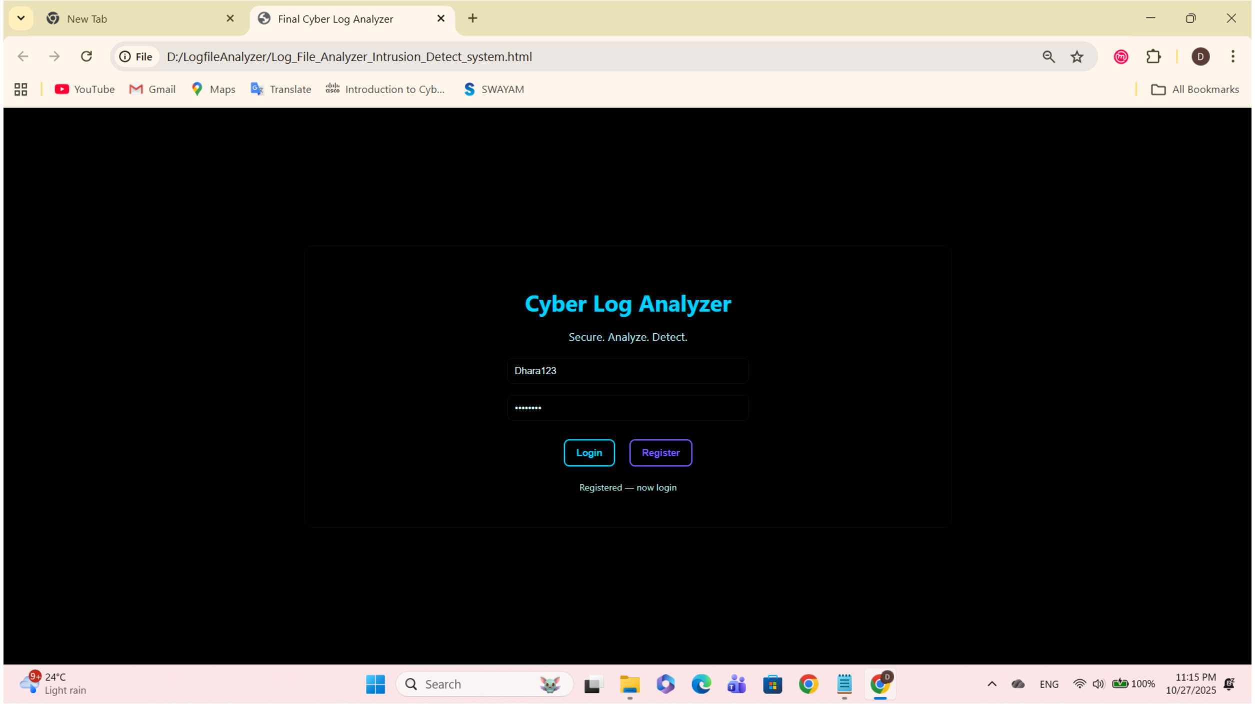
- Works only on static log files, not live monitoring.
- Limited to keyword-based detection (no AI/ML intelligence yet).
- Browser memory may limit very large log file uploads.

4.2 Future Enhancement

- Integration with real-time monitoring APIs.
- AI-based anomaly detection using machine learning models.
- Integration with SIEM platforms (like Splunk or ELK).
- Enhanced reporting (PDF/Excel export).
- Multi-user dashboard with cloud storage.

Login Page

Description: The user enters login credentials to access the Cyber Log Analyzer.
Ensures that only authorized users can access the system and perform analysis.



Cyber Log Analyzer

Secure. Analyze. Detect.

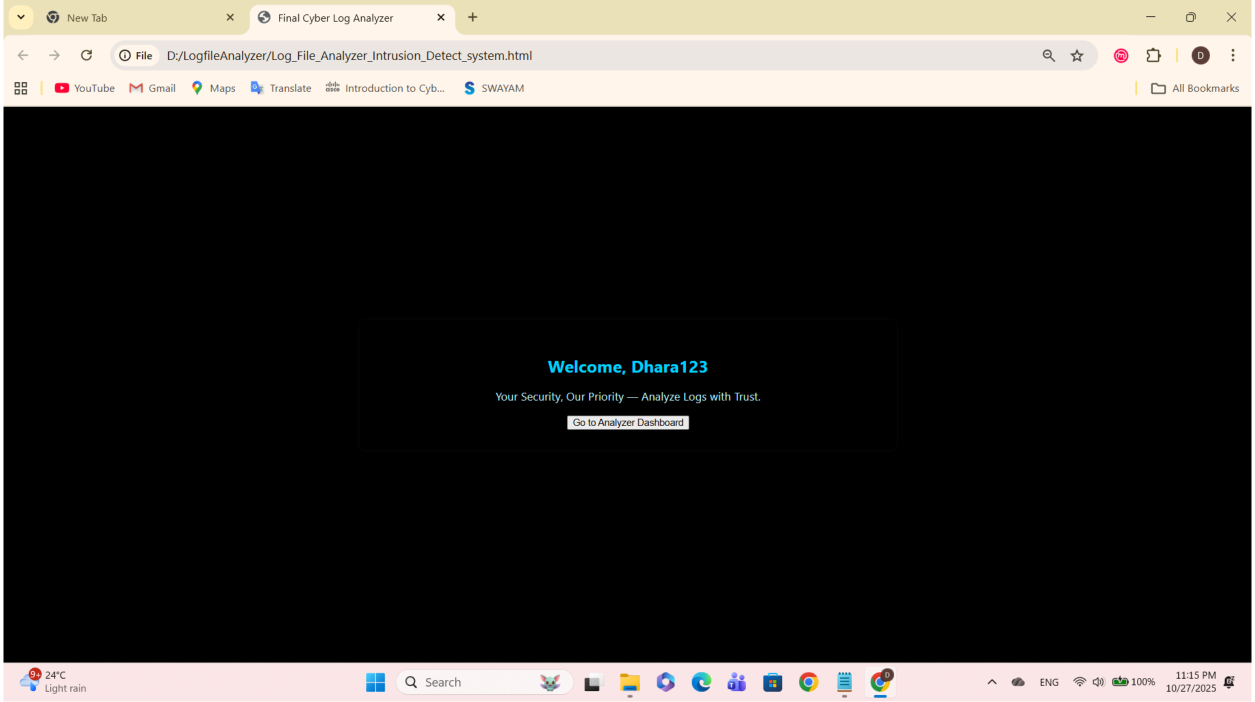
Dhara123

••••••••

Registered — now login

Welcome Page / Home Screen

Description: After login, the welcome screen is displayed with navigation options.
Helps users understand the next step — uploading log files or viewing the analyzer dashboard.



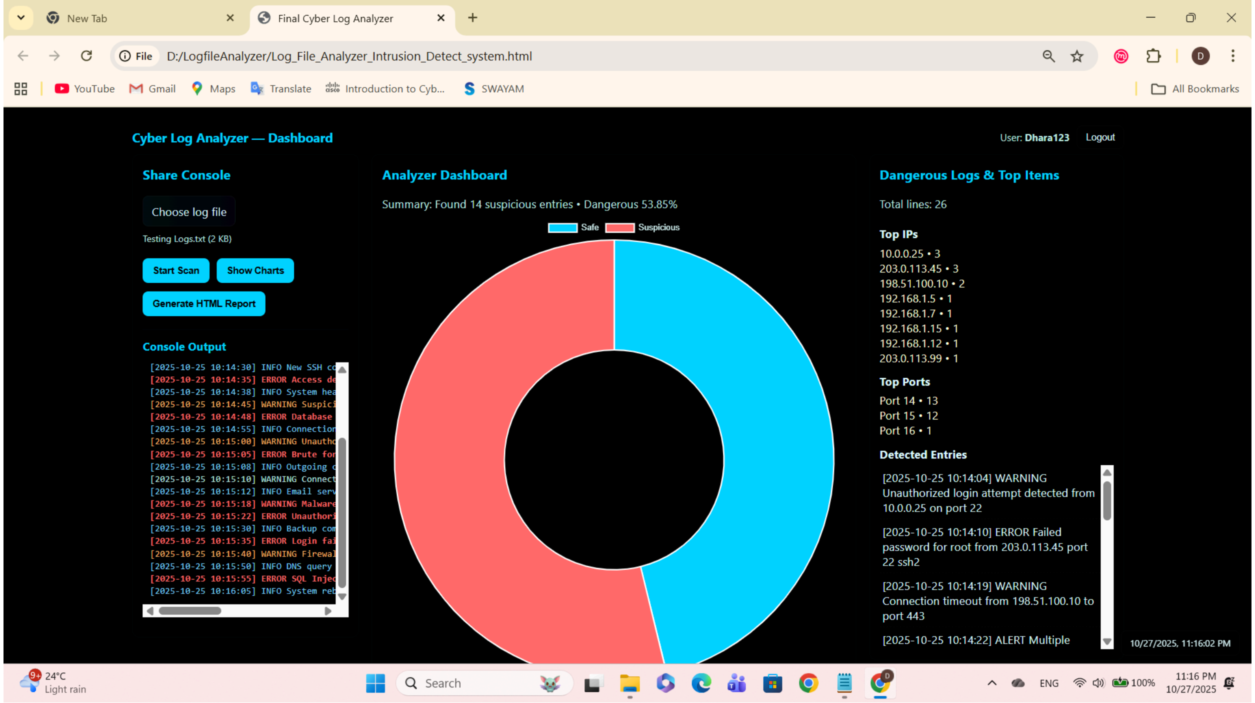
Welcome, Dhara123

Your Security, Our Priority — Analyze Logs with Trust.

Go to Analyzer Dashboard

Chart Visualization

Description: Displays the total number of safe and suspicious entries using a pie chart. Helps users quickly understand the proportion of threats visually.



Cyber Log Analyzer — Dashboard

User: **Dhara123**

Share Console

Testing Logs.txt (2 KB)

Console Output

```
[2025-10-25 10:14:30] INFO New SSH co
[2025-10-25 10:14:35] ERROR Access de
[2025-10-25 10:14:38] INFO System hea
[2025-10-25 10:14:45] WARNING Suspici
[2025-10-25 10:14:48] ERROR Database
[2025-10-25 10:14:55] INFO Connection
[2025-10-25 10:15:00] WARNING Unautho
[2025-10-25 10:15:05] ERROR Brute for
[2025-10-25 10:15:08] INFO Outgoing c
[2025-10-25 10:15:10] WARNING Connect
[2025-10-25 10:15:12] INFO Email serv
[2025-10-25 10:15:18] WARNING Malware
[2025-10-25 10:15:22] ERROR Unauthori
[2025-10-25 10:15:30] INFO Backup com
[2025-10-25 10:15:35] ERROR Login fai
[2025-10-25 10:15:40] WARNING Firewal
[2025-10-25 10:15:50] INFO DNS query
[2025-10-25 10:15:55] ERROR SQL Injec
[2025-10-25 10:16:05] INFO System reb
```

Analyzer Dashboard

Summary: Found 14 suspicious entries • Dangerous 53.85%

Dangerous Logs & Top Items

Total lines: 26

Top IPs

10.0.0.25 • 3
203.0.113.45 • 3
198.51.100.10 • 2
192.168.1.5 • 1
192.168.1.7 • 1
192.168.1.15 • 1
192.168.1.12 • 1
203.0.113.99 • 1

Top Ports

Port 14 • 13
Port 15 • 12
Port 16 • 1

Detected Entries

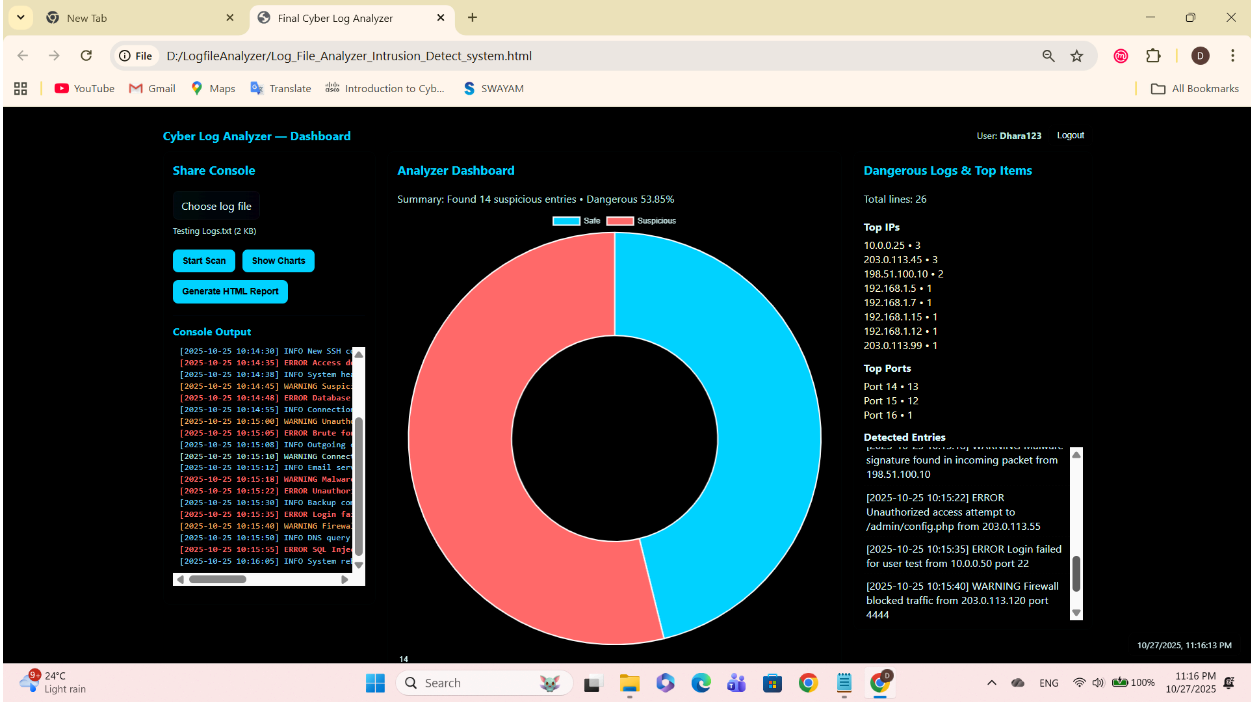
[2025-10-25 10:14:04] WARNING Unauthorized login attempt detected from 10.0.0.25 on port 22

[2025-10-25 10:14:10] ERROR Failed password for root from 203.0.113.45 port 22 ssh2

[2025-10-25 10:14:19] WARNING Connection timeout from 198.51.100.10 to port 443

[2025-10-25 10:14:22] ALERT Multiple

10/27/2025, 11:16:02 PM



D:/LogfileAnalyzer/Log_File_Analyzer_Intrusion_Detect_system.html

Cyber Log Analyzer — Dashboard

User: Dhara123 Logout

Share Console

Choose log file

Testing Logs.txt (2 KB)

Start Scan | Show Charts | Generate HTML Report

Console Output

```
[2025-10-25 10:14:30] INFO New SSH co
[2025-10-25 10:14:35] ERROR Access de
[2025-10-25 10:14:38] INFO System hea
[2025-10-25 10:14:45] WARNING Suspici
[2025-10-25 10:14:48] ERROR Database
[2025-10-25 10:14:55] INFO Connection
[2025-10-25 10:15:00] WARNING Unautho
[2025-10-25 10:15:05] ERROR Brute for
[2025-10-25 10:15:08] INFO Outgoing c
[2025-10-25 10:15:10] WARNING Connect
[2025-10-25 10:15:12] INFO Email serv
[2025-10-25 10:15:18] WARNING Malware
[2025-10-25 10:15:22] ERROR Unauthori
[2025-10-25 10:15:30] INFO Backup com
[2025-10-25 10:15:35] ERROR Login fai
[2025-10-25 10:15:40] WARNING Firewal
[2025-10-25 10:15:50] INFO DNS query
[2025-10-25 10:15:55] ERROR SQL Injec
[2025-10-25 10:16:05] INFO System reb
```

Analyzer Dashboard

Summary: Found 14 suspicious entries • Dangerous 53.85%

Dangerous Logs & Top Items

Total lines: 26

Top IPs

10.0.0.25 • 3
203.0.113.45 • 3
198.51.100.10 • 2
192.168.1.5 • 1
192.168.1.7 • 1
192.168.1.15 • 1
192.168.1.12 • 1
203.0.113.99 • 1

Top Ports

Port 14 • 13
Port 15 • 12
Port 16 • 1

Detected Entries

signature found in incoming packet from 198.51.100.10

[2025-10-25 10:15:22] ERROR Unauthorized access attempt to /admin/config.php from 203.0.113.55

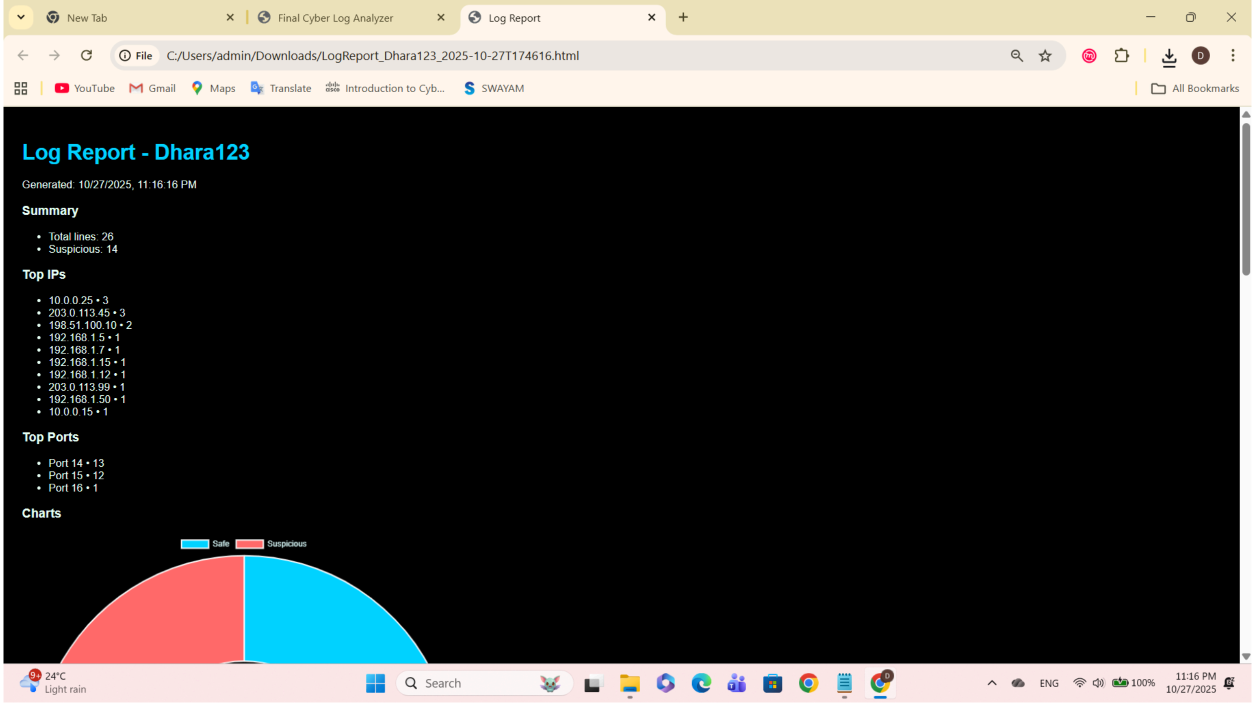
[2025-10-25 10:15:35] ERROR Login failed for user test from 10.0.0.50 port 22

[2025-10-25 10:15:40] WARNING Firewall blocked traffic from 203.0.113.120 port 4444

10/27/2025, 11:16:13 PM

Report Generation Interface

Description: Shows the option to generate a detailed HTML report from the analyzed data. Allows users to save and share results for further investigation.



C:/Users/admin/Downloads/LogReport_Dhara123_2025-10-27T174616.html

Log Report - Dhara123

Generated: 10/27/2025, 11:16:16 PM

Summary

- Total lines: 26
- Suspicious: 14

Top IPs

- 10.0.0.25 • 3
- 203.0.113.45 • 3
- 198.51.100.10 • 2
- 192.168.1.5 • 1
- 192.168.1.7 • 1
- 192.168.1.15 • 1
- 192.168.1.12 • 1
- 203.0.113.99 • 1
- 192.168.1.50 • 1
- 10.0.0.15 • 1

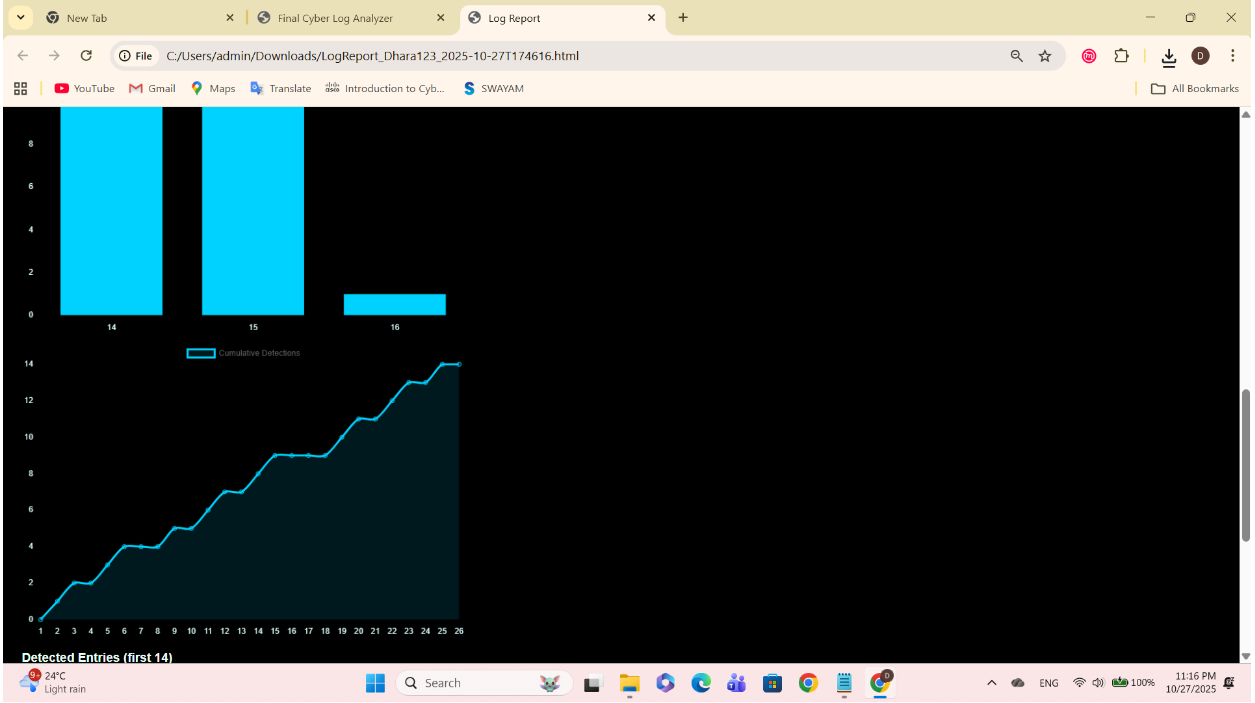
Top Ports

- Port 14 • 13
- Port 15 • 12
- Port 16 • 1

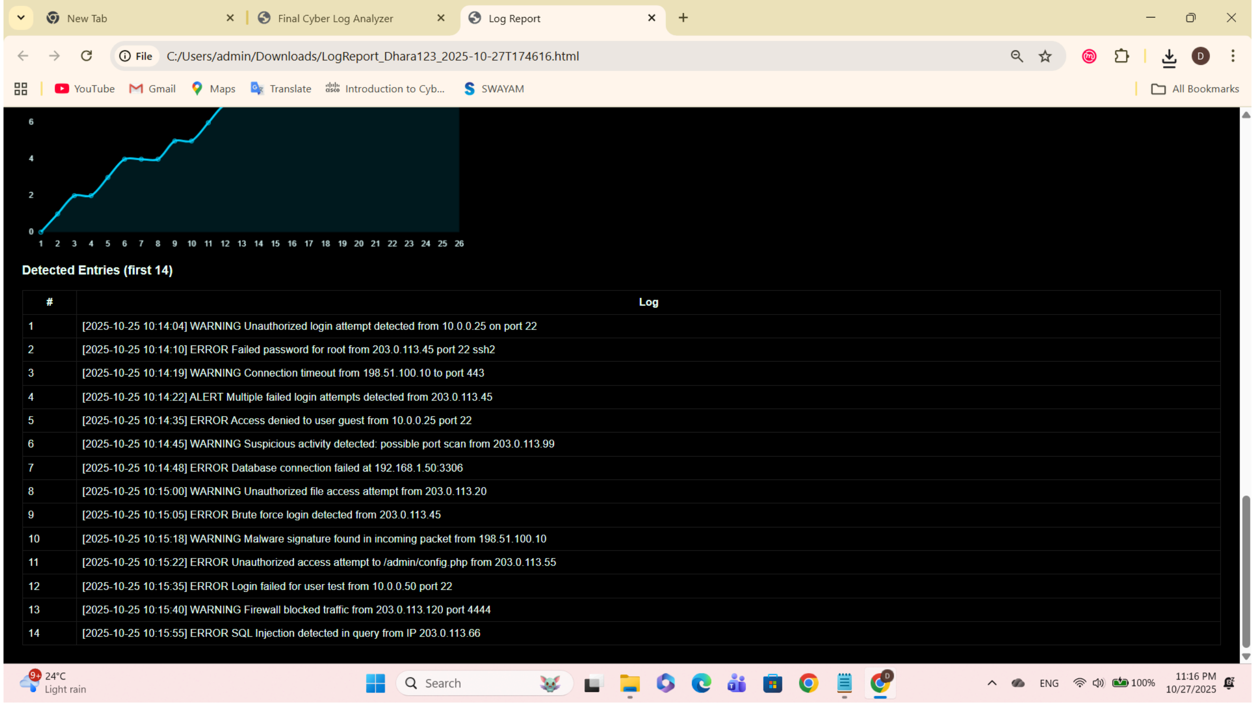
Charts

Generated HTML Report (LogReport_Dhara123.html)

Description: Displays the automatically created HTML report with detailed findings and summary. Provides a structured record of analysis that can be reviewed later.



Detected Entries (first 14)



Detected Entries (first 14)

#	Log
1	[2025-10-25 10:14:04] WARNING Unauthorized login attempt detected from 10.0.0.25 on port 22
2	[2025-10-25 10:14:10] ERROR Failed password for root from 203.0.113.45 port 22 ssh2
3	[2025-10-25 10:14:19] WARNING Connection timeout from 198.51.100.10 to port 443
4	[2025-10-25 10:14:22] ALERT Multiple failed login attempts detected from 203.0.113.45
5	[2025-10-25 10:14:35] ERROR Access denied to user guest from 10.0.0.25 port 22
6	[2025-10-25 10:14:45] WARNING Suspicious activity detected: possible port scan from 203.0.113.99
7	[2025-10-25 10:14:48] ERROR Database connection failed at 192.168.1.50:3306
8	[2025-10-25 10:15:00] WARNING Unauthorized file access attempt from 203.0.113.20
9	[2025-10-25 10:15:05] ERROR Brute force login detected from 203.0.113.45
10	[2025-10-25 10:15:18] WARNING Malware signature found in incoming packet from 198.51.100.10
11	[2025-10-25 10:15:22] ERROR Unauthorized access attempt to /admin/config.php from 203.0.113.55
12	[2025-10-25 10:15:35] ERROR Login failed for user test from 10.0.0.50 port 22
13	[2025-10-25 10:15:40] WARNING Firewall blocked traffic from 203.0.113.120 port 4444
14	[2025-10-25 10:15:55] ERROR SQL Injection detected in query from IP 203.0.113.66