VPN SPYGLASS

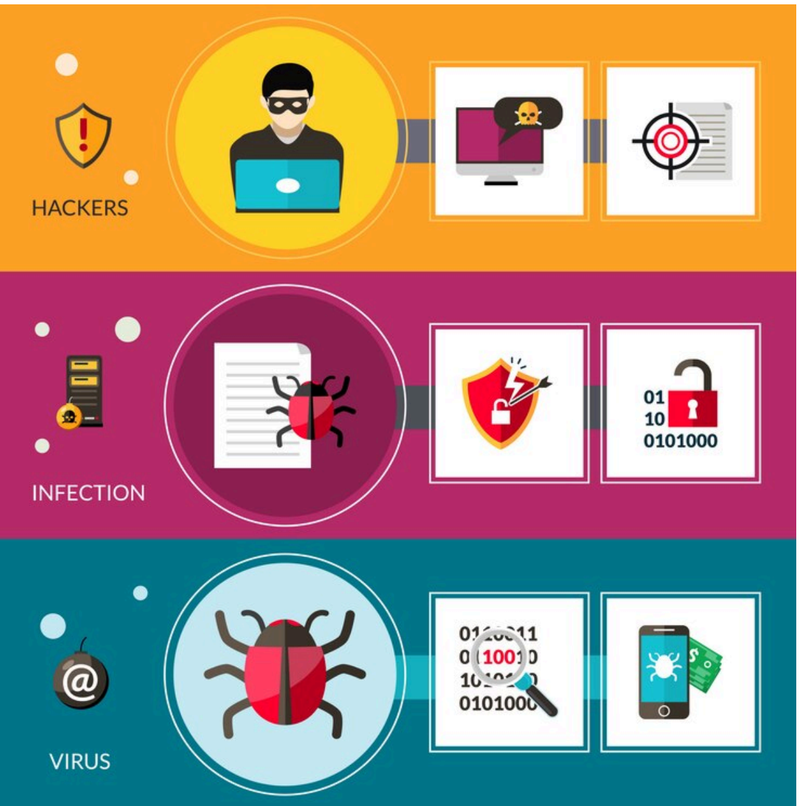
VPN TRAFFIC ANALYZER

Advisor Dr. Mehdi Hussain

Co - Advisor Dr. Arsalan Ahmed

2024

Table of Contents



Abstract

The usage of VPNs is expanding as people become more concerned about their online privacy and security, as well as the desire to go around **geo-restrictions and access region-specific material.**
The **Websites** and communication that are **blocked** by an **organization** or **state** can be accessed by use of a VPN. Thus, posing a data and security risk in an organization or state.

The purpose is to enable **network administrators** to **identify unauthorized VPN connections, categorize VPN traffic,** and **reduce security risks** by leveraging modern technology and deep packet inspection algorithms.

Introduction

Why is Encrypted Network Traffic Analysis important in Network Security?

1. Data Protection
2. Preventing Cyber Attack
3. Network Integrity
4. Enhanced Security Posture
5. Data Leak Prevention
6. Understand Encrypted Data

What will this research provide?

1. IP addresses, ports, packet lengths, and packet patterns to identify the VPN
2. The knowledge gathered from this study aided in the building of a Network Traffic Analysis and blocking tool for VPNs.
3. Wireshark and other cutting-edge tools will be used to monitor encrypted data via trace file analysis for network traffic monitoring.

Problems

PROBLEMS

The proliferation of VPNs poses a challenge to network admin, as these tools can bypass security measures and access restricted content pose security risks, violate agreements, and slow network performance. Moreover, **Existing methods** often struggle to identify VPN traffic due to **tunneling** and **masking techniques** employed by VPN services.

VPN SPYGLASS

Objectives

OBJECTIVES 01

Investigate the deep packet inspection (DPI) method for analyzing encrypted traffic.

OBJECTIVES 02

Design a real-time VPN traffic detection mechanism to enable user to respond to security threat

OBJECTIVES 03

Develop a VPN analyzer application with the goal of efficiently monitoring and managing VPN usage.

DEEP PACKET INSPECTION

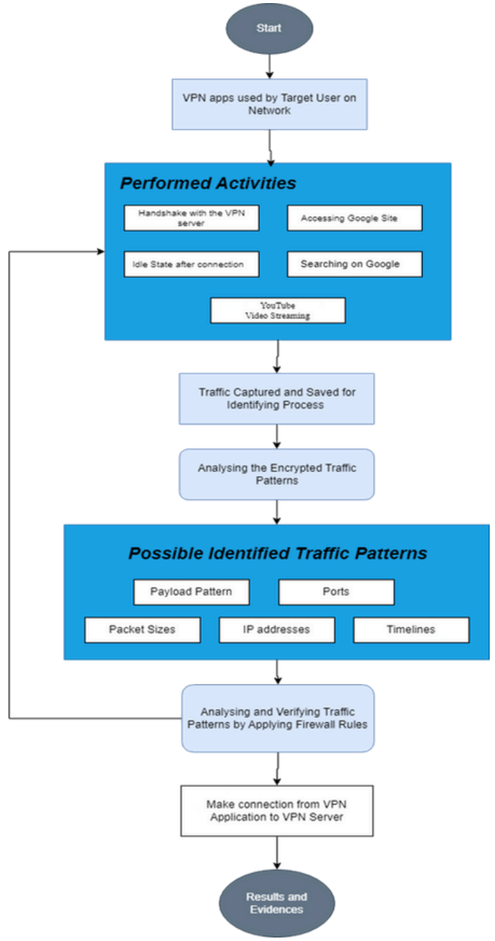
Deep packet inspection (DPI), enables us to thoroughly scrutinize data packets as they travel over the network. Unlike older approaches that just scan packet headers, DPI investigates packet contents in-depth and gives a full insight into network traffic patterns. DPI is an essential component of our design, allowing us to recognize and categorize packets based on critical information such as IP addresses, protocols, and port numbers.

RESEARCH METHOGOLOGY

Our methodology is built upon the foundational research outlined in *" **Afzal, A.; Hussain, M.; Encrypted Network Traffic Analysis of Secure Instant Messaging Application: A Case Study of Signal Messenger App.**"*

CATEGORIZATION ALGORITHM

Our algorithms classify VPN traffic based on features including VPN protocols, IP addresses, port numbers, payloads, and traffic behavior by utilizing DPI techniques by generating rules based on these characteristics.



Methodology

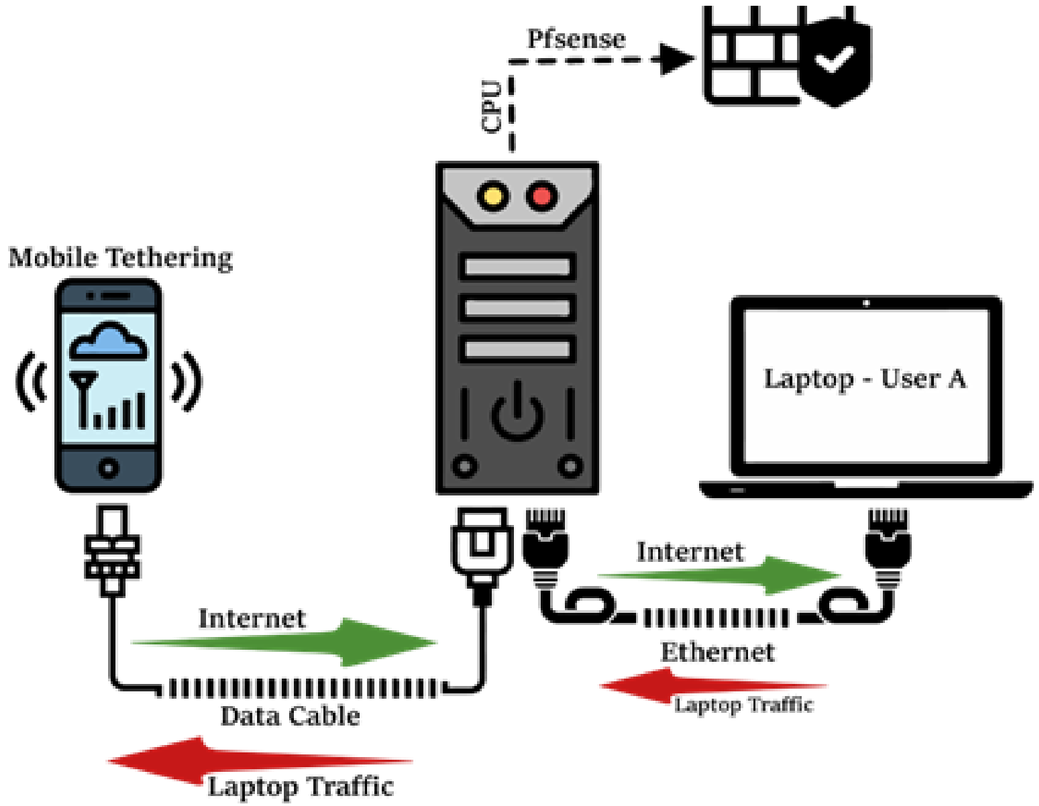
vpnspyglass.vercel.app

WEB DASHBOARD

ur Web dashboard has a clean and simple layout based on ReactJS and Vite, allowing for seamless display of real-time network traffic metrics. The dashboard has detailed graphs that display how much VPN is utilised

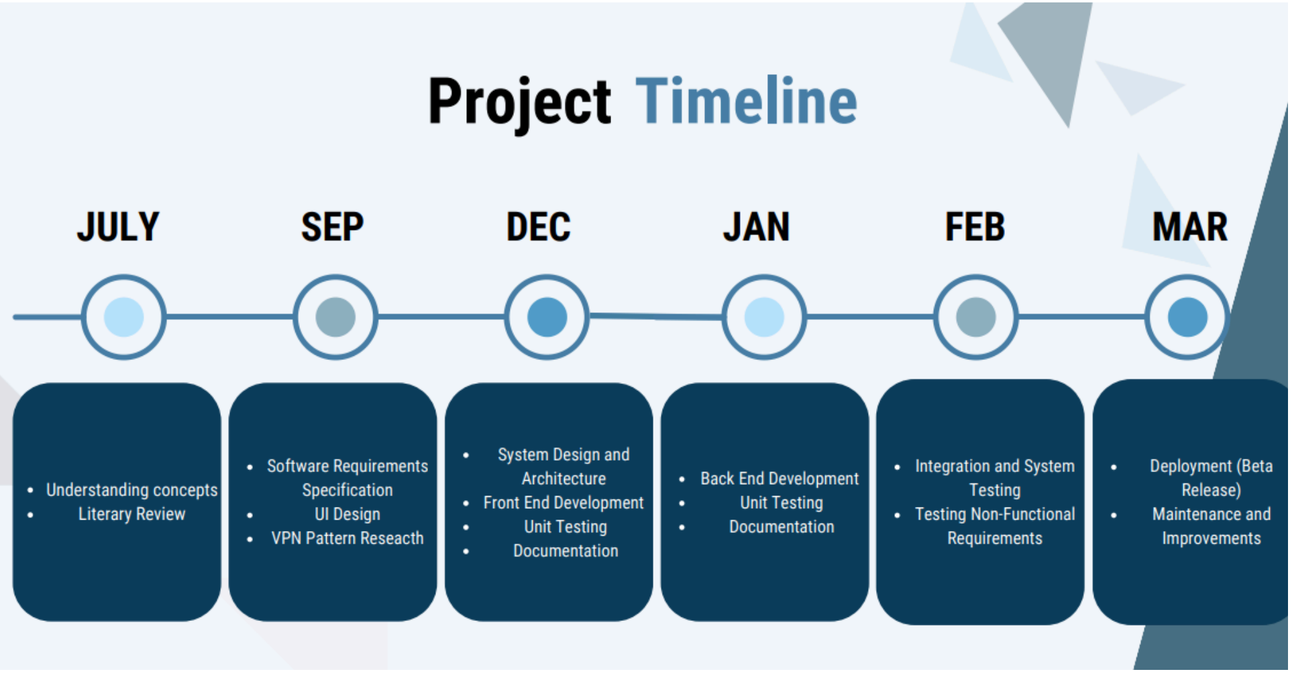
FIREWALL BLOCKING

By using the PfSense Firewall, we can block the VPN by using its IP, Port, and Packet Length which we have identified.



Methodology

vpnspyglass.vercel.app



Implementation

PHASE 01

Detection of VPN traffic using Deep Packet Inspection based on their IP, Port Number, and Packet Length.

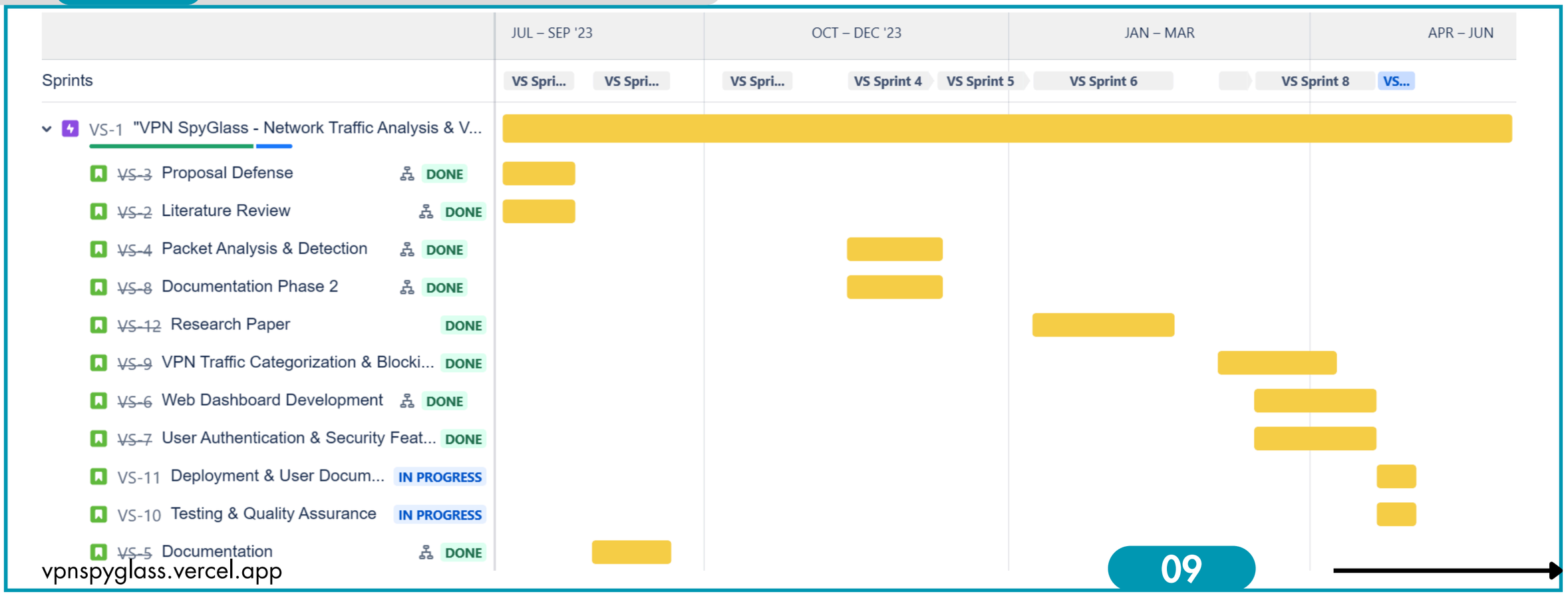
PHASE 02

Development of Web Page. Setting up of implementation environment.

PHASE 03

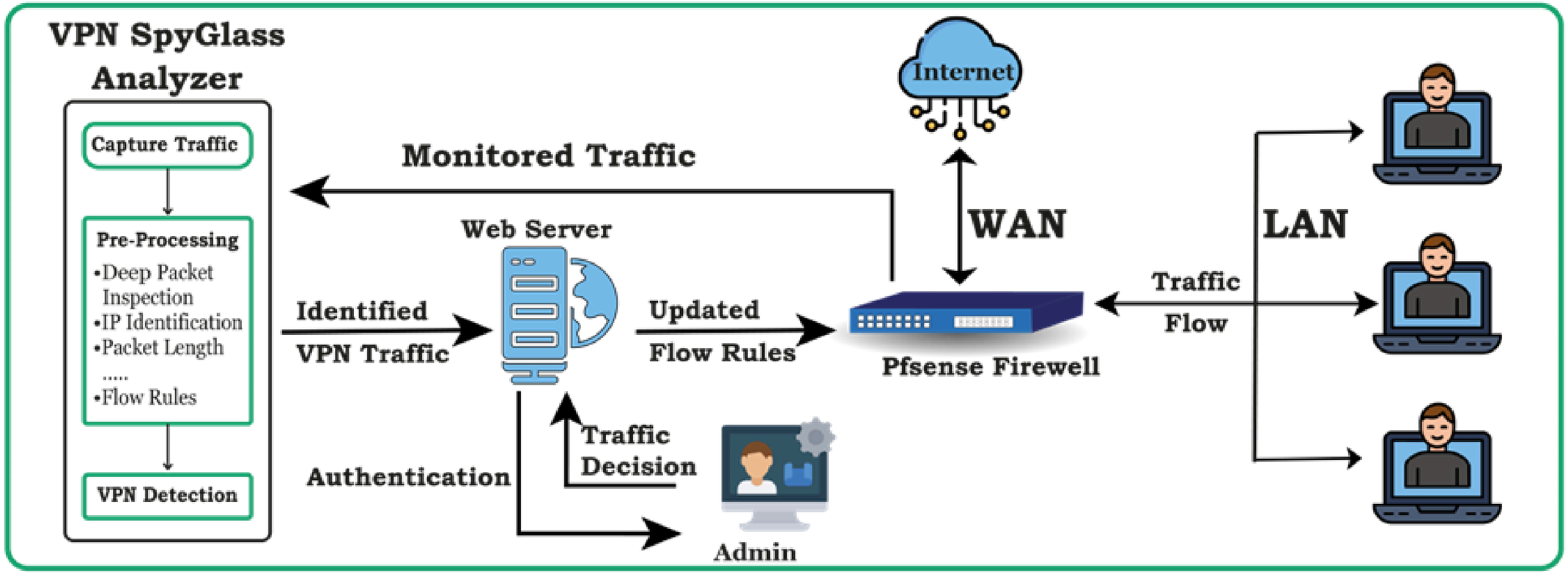
Implementation of code, integrate Firewall, and integrate with the webpage.

JIRA



vpnspyglass.vercel.app

Architecture



Testing

UNIT TESTING

```
PROBLEMS    OUTPUT    DEBUG CONSOLE    TERMINAL    PORTS

PS C:\Users\hassa\Desktop\FYP\Code> pytest
============================= test session starts ==============================
platform win32 -- Python 3.10.7, pytest-8.1.1, pluggy-1.4.0
rootdir: C:\Users\hassa\Desktop\FYP\Code
plugins: anyio-3.7.1
collected 5 items

test_identify_vpn.py .....

============================== 5 passed in 17.87s ==============================
PS C:\Users\hassa\Desktop\FYP\Code>
```

Testing

USER TESTING

Test Case ID	Description	Test Steps	Expected Result	Status
UAT_AUTH_001	Verify user access by logging in with valid credentials	Login with valid username and password	Successful login redirects to the dashboard	**Passed**
UAT_DATA_001	Ensure accurate data retrieval and display on the dashboard.	View displayed data on the dashboard	Real-time data accurately presented.	**Passed**
UAT_VISUAL_001	Confirm proper data analysis and visualization.	Review graphical representations on dashboard	Clear and accurate visualization of traffic patterns.	**Passed**
UAT_VPN_001	Validate correct categorization of VPN traffic.	Analyze categorized VPN traffic	Accurate VPN traffic labeling.	**Passed**
UAT_RULES_001	Verify the functionality of rules for categorizing VPN traffic.	Send packets representing different VPN protocols, port numbers, and IP addresses. Analyze the categorized traffic based on predefined rules.	Each packet is accurately categorized according to the defined rules, with proper identification of VPN usage.	**Passed**
UAT_BLOCKING_001	Ensure seamless transition from VPN traffic blocking to normal flow.	Apply and remove VPN traffic block	Smooth transition to normal traffic upon block removal	**Passed**

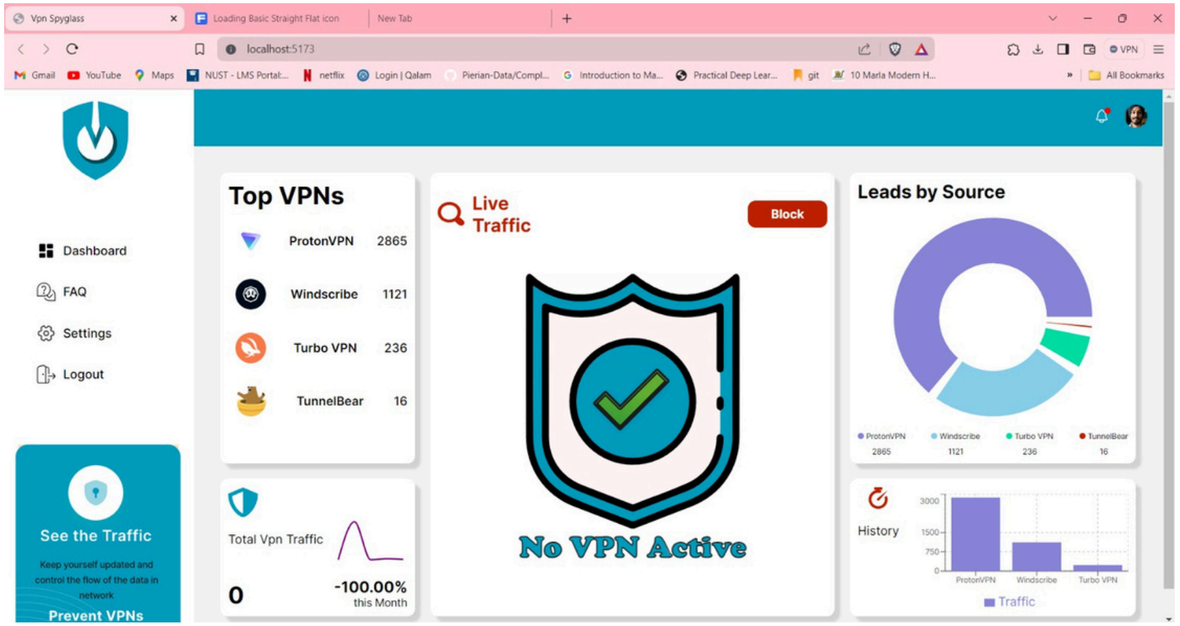
Result

VPN SpyGlass is an **open-source tool** that employs **deep packet inspection** to detect and categorize VPN traffic within a network. By **classifying VPNs based on protocol, ports and IPs,** it enables network administrators to efficiently **monitor and control VPN usage**, identify unauthorized connections, and uncover potential security risk.

What it offers:

- **Real-Time** VPN Detection
- **Detect VPN Application**
- VPN **Ports** and **IP Addresses**
- **Realtime** VPN Traffic **Blocking**

** Research Paper Under Review
vpnspyglass.vercel.app



Visit: *vpnspyglass.vercel.app*

DEMO

Thank You So Much!

Presentation by :

HASSAN ABDULLAH
SAMEEN MUBASHAR