NETWORK TRAFFIC ANALYSIS USING

WIRE SHARK AND ZEEK BY: MEHAK BERA

Institution : ABES ENGINEERING

College

course: BTECH

branch: computer science (ds)

DATE: 1 AUGUST 2025

GUIDED BY: NIKHIL PANDEY

ABSTRACT

In this we need to understand data travels across a network is essential for security, performance monitoring, and troubleshooting. Beginners often struggle with complex tools or lack real-time visibility into network activities. This project aims to provide a simple yet powerful solution to analyse, monitor and interpret network trafficusing two industry-standard tools: **Wireshark** and **Zeek .**

**TECHNOLOGY USED**

* This project uses **Wireshark** for detailed packet-level inspection and **Zeek** for real-time network traffic monitoring and behaviour-based analysis.

KEY RESULTS

* Identified the most active devices and services on the network.

Detected unusual traffic patterns (e.g., port scans, failed connections).

Compared normal vs suspicious behaviour using Zeek logs.

*TABLE OF CONTENT*

Introduction

Methodology

Result

Results and Discussion

Conclusions

Recommendations

References

**What is my project about?**

This project is about **analysing network traffic** to understand how data travels between devices over the internet or a local network. Every time we visit a website, send a message, or stream a video, packets of data are sent and received. This project helps us look at those packets, understand what protocols are used (like HTTP or DNS), which devices are talking, and whether there’s anything unusual or suspicious happening in the network.

**Why did I choose this project? Why is it important? What are the problem it going to solve?**

I chose this project because I wanted to explore **how the internet works behind the scenes** and how network activity can be monitored and secured. In many cases, people are unaware of the data being exchanged in the background or how vulnerabilities in a network can be exploited by attackers.

This project is important because it:

* Helps detect unusual behaviour or security threats (like unauthorized access or port scans),
* Identifies which devices or applications are using the most bandwidth,
* Improves understanding of basic networking and cybersecurity.

The problem this project addresses is the **lack of visibility and awareness** in network behaviour. Most users don’t know what’s going on in their own network, which can lead to security risks, slow performance, or mismanagement. My project offers a beginner-friendly solution to monitor, analyse, and interpret this traffic.

**How will I solve it or my problem solving approach?**

To solve this problem, I captured real network traffic using monitoring tools, then analysed the data to:

* Identify IP addresses communicating on the network,
* Understand which protocols are being used most frequently (e.g., HTTP, DNS, TCP),
* Detect any suspicious or repetitive patterns that might indicate a potential threat,
* Present the results using summaries and simple visual graphs for better understanding.

I also reviewed traffic logs to look at how devices interact and whether there were any warning signs like repeated failed connections or unknown protocol usage.

**What tools or methods did I use?**

For this project, I used the following tools and techniques:

* **Wireshark** – a widely-used network protocol analyser that helps inspect live traffic .
* **Zeek (formerly Bro)** – a powerful network analysis framework that creates detailed logs of traffic behaviour.

Background study

This project is based on two powerful and widely used tools in the field of network monitoring and cybersecurity: **Wireshark** and **Zeek**. Both tools are used in real-world companies and by cybersecurity professionals to watch over networks, detect threats, and fix problems.

**Wireshark**

Wireshark is a free tool that lets you see what’s happening on your network in real time. It shows you all the little packets of data that your device sends and receives. During my project, I used Wireshark to:

* **Capture live traffic** when I browsed websites or opened apps.
* **See which IP addresses** were talking to each other.
* **Check what protocols** were being used (like HTTP, DNS, etc.).

Wireshark helped me actually **see the internet in action**. It was like opening a window into the hidden world of my computer’s communication.

**Zeek**

Zeek is another tool, but it works differently. Instead of showing you each packet like Wireshark, Zeek watches the network and creates **log files** that tell you what happened. I used Zeek to:

* Generate logs of **who connected to what** and when.
* Understand **which websites were accessed** and how often.
* Spot any **suspicious behaviour**, like repeated connection attempt.

It was like having a smart assistant that writes a summary of everything going on in the background. Zeek made it easier to understand **patterns and behaviours** in the traffic.

**Why I Used These Tools**

I chose Wireshark and Zeek because:

* They are **easy to install and use** even for beginners,
* They are used in real companies and by cybersecurity experts,
* They helped me **learn by doing**.

There are also beginner friendly and does not require much coding skills.

**Approach**

The goal of my project was to understand what kind of traffic is flowing through a network, which devices are communicating, and whether any unusual or suspicious activity is happening. To do this, I needed tools that could **capture network traffic** and help me **analyse it in a simple way**.

I decided to use **Wireshark** for capturing and viewing packets in real-time, and **Zeek** to generate readable log files from the same traffic. My approach was to:

1. Monitor real-time network activity,
2. Capture data and save it for analysis,
3. Use tools to explore that data and look for patterns or red flags,

**My Plan**

Before I started the project, I knew I wanted to understand **how internet traffic works** and **what kind of data flows through a network**. But I didn’t want to just read about it—I wanted to **actually see it for myself**.

So, I made a simple plan:

1. **Learn the Basics**  
   First, I read about how computer networks work—things like IP addresses, protocols, and what packets are. I also watched videos and tutorials to learn how tools like **Wireshark** and **Zeek** are used.
2. **Choose the Right Tools**  
   I chose **Wireshark** because it can capture and show real-time traffic. It’s beginner-friendly and used by many people in the field.  
   I also picked **Zeek**, because it gives detailed logs and helps find strange or suspicious activity.
3. **Capture Real Traffic**  
   I planned to open Wireshark, use some apps (like opening websites or streaming), and let it record the traffic.
4. **Analyse and Understand**  
   After capturing the traffic, I would look at it in Wireshark to see:
   * Which devices talked to each other,
   * What kind of data was sent (e.g., HTTP, DNS),
   * And if anything looked strange.

Tools used

**Wireshark**

* Wireshark is a free and open-source tool used to **capture live network traffic**.
* It shows **every packet** of data being sent or received on the network.
* I used Wireshark to:
  + Start a live capture on my Wi-Fi,
  + Save the traffic
  + Use filters to look at certain if traffic like http, dns, or tcp,
  + Understand how devices were communicating and what protocols they used.

It gave me a **very detailed, real-time view** of everything happening on the network.

**2. Zeek**

* Zeek is also a network monitoring tool, but instead of showing each packet, it **creates summary logs** of network activity.
* It watches how devices behave and helps **detect any unusual or suspicious behaviour**.
* I used Zeek to:
  + Analyse by Wireshark,
  + Generate logs like conn.log (for connections), http.log (for web activity), and notice.log (for alerts),
  + Understand the overall behaviour of the network.

Steps

**Step 1: Installed Tools**

* I downloaded and installed **Wireshark** on my computer.
* I also installed **Zeek** using online tutorials.
* I made sure both tools were working and ready to analyse network traffic.

**Step 2: Captured Live Network Traffic**

* I opened **Wireshark** and selected my active network (Wi-Fi).
* I started a live capture while doing regular activities like browsing websites, watching videos, and sending messages.
* This helped generate real traffic that I could study.

**Step 3: Analysed Traffic in Wireshark**

* I opened Wireshark.
* I used **filters** to view specific types of traffic, like only http or dns.
* I noted:
  + Which **IP addresses** were communicating,
  + What **protocols** were most active,
  + How much data was transferred.

**What My Results Showed**

After using Wireshark and Zeek, I realized that **a lot is happening in the background** every time we use the internet. Even when I just opened a few websites or used some apps, my laptop was sending and receiving a lot of data.

Some key things I saw:

* Most of the traffic was using **HTTP, DNS, and TCP** – which are normal and used all the time.
* My computer was talking to **many different servers**, even some I didn’t click on directly. Some of them were for ads, updates, or background apps.

Using Zeek, I saw **all the logs of connections** my system made. This helped me understand which websites were accessed, and how often.

Even though I didn’t find **and understand** anything “bad” like a virus or hacker, I still saw how easy it is to **watch network behaviour** using the right tools.

**Things I Noticed**

* My device made **DNS requests** before loading any website — that means it first checks where to go.
* Some websites connected to **many different servers**, not just one.
* Some of the traffic was **encrypted (HTTPS)**, so I couldn’t see the exact content, but I could still see where it was going.

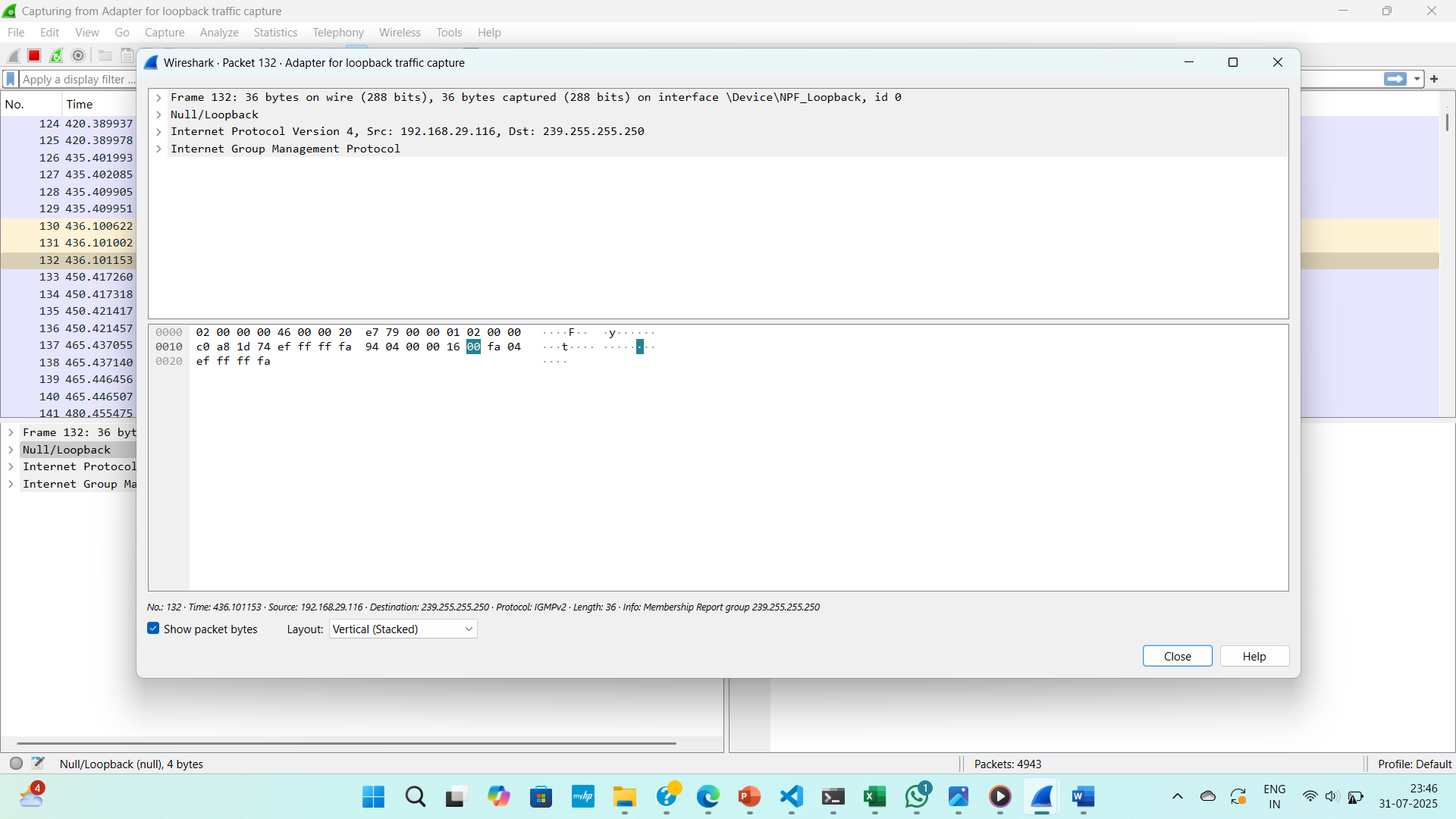
It made me think how **every click on the internet creates a chain of actions** in the background

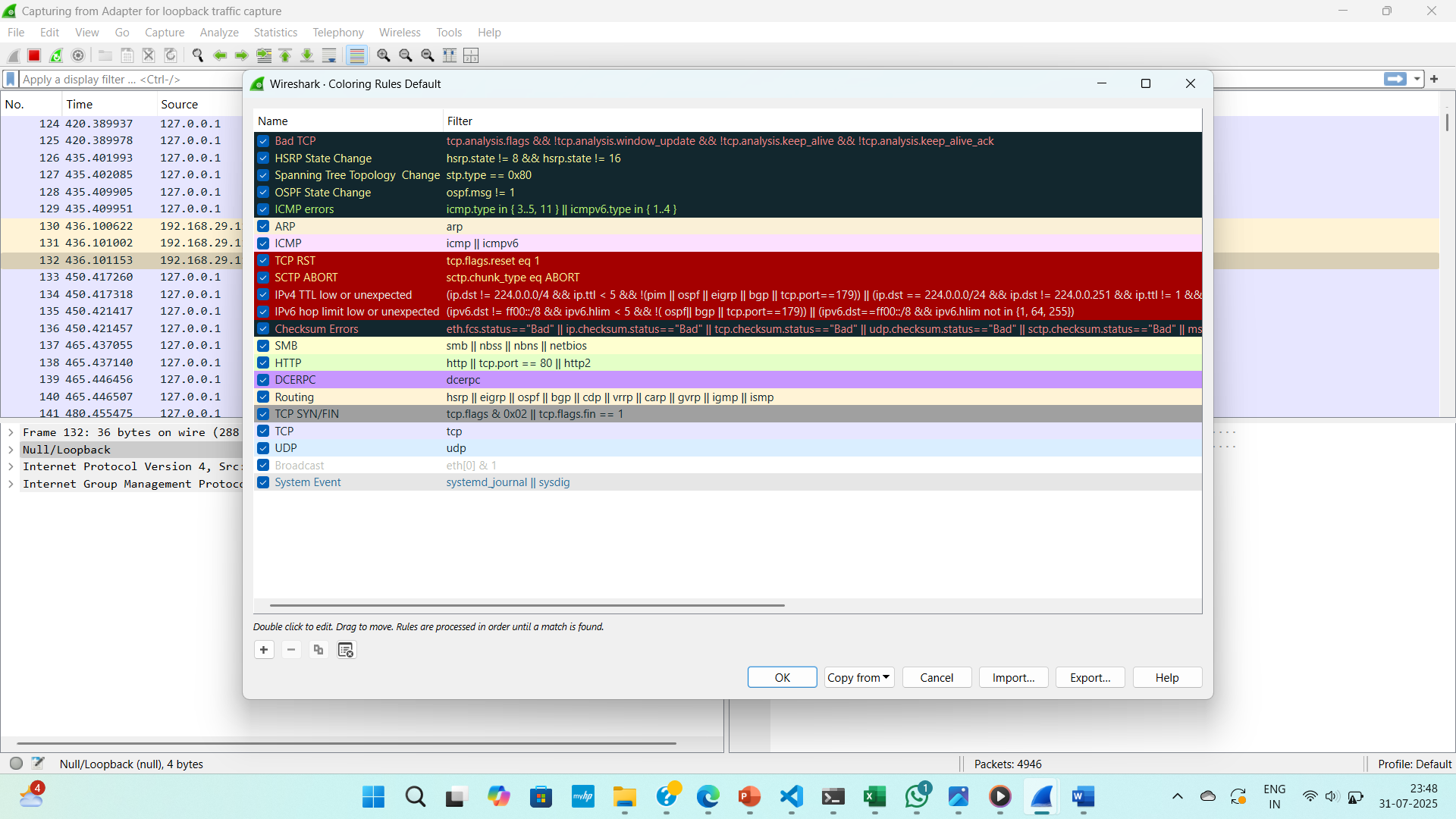


Packet capturing

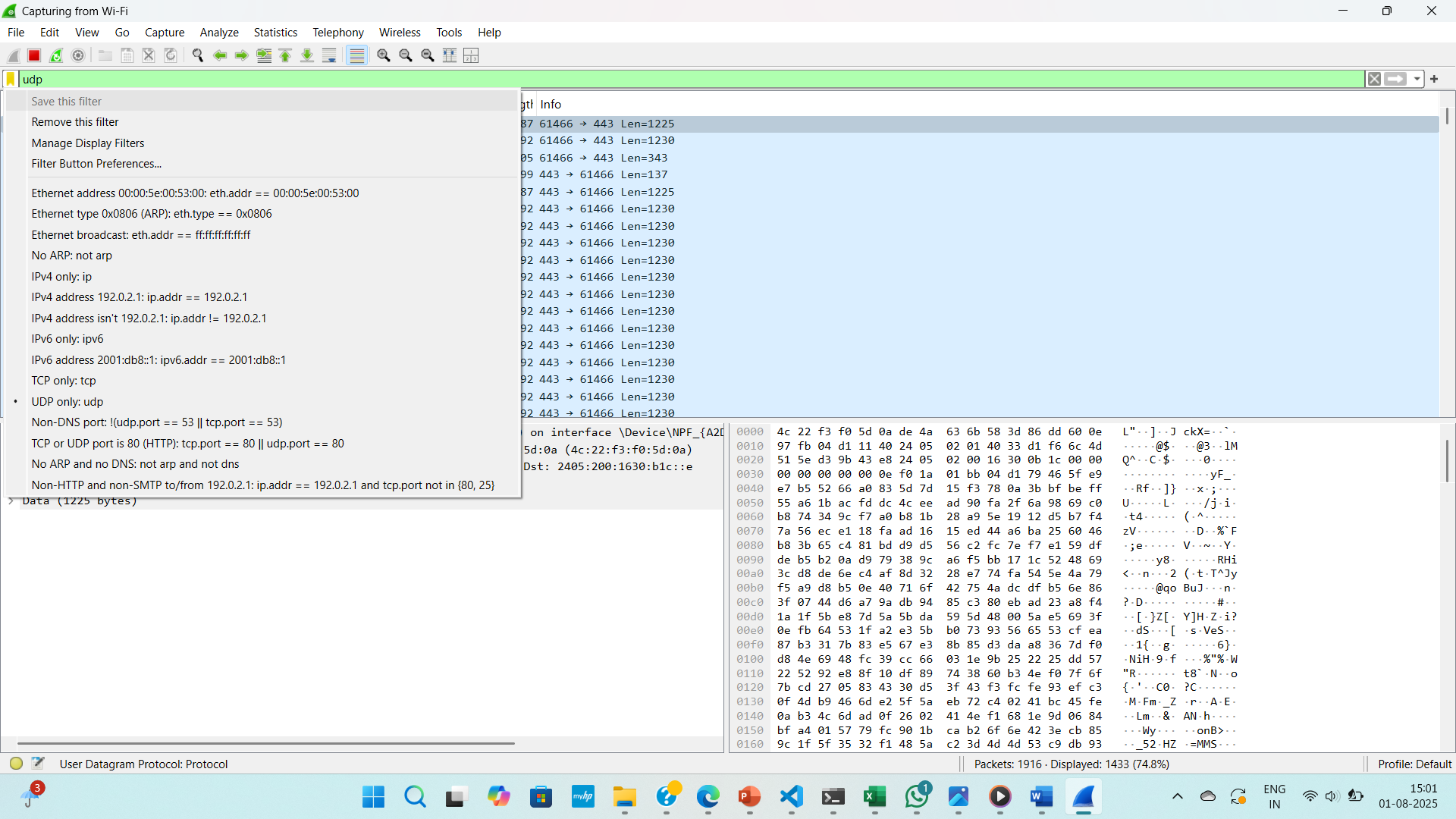
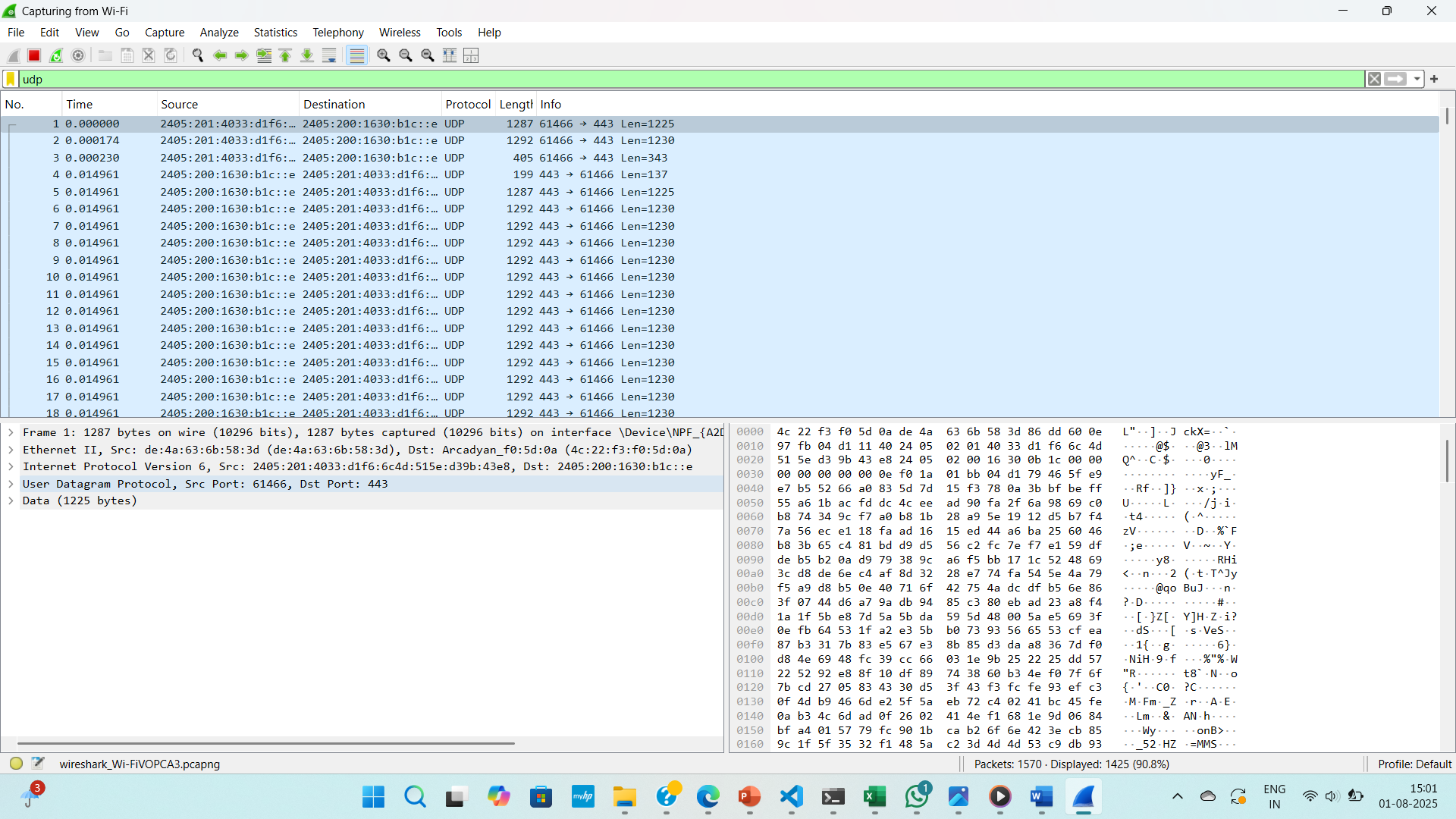
# 

Full detail of selected packets

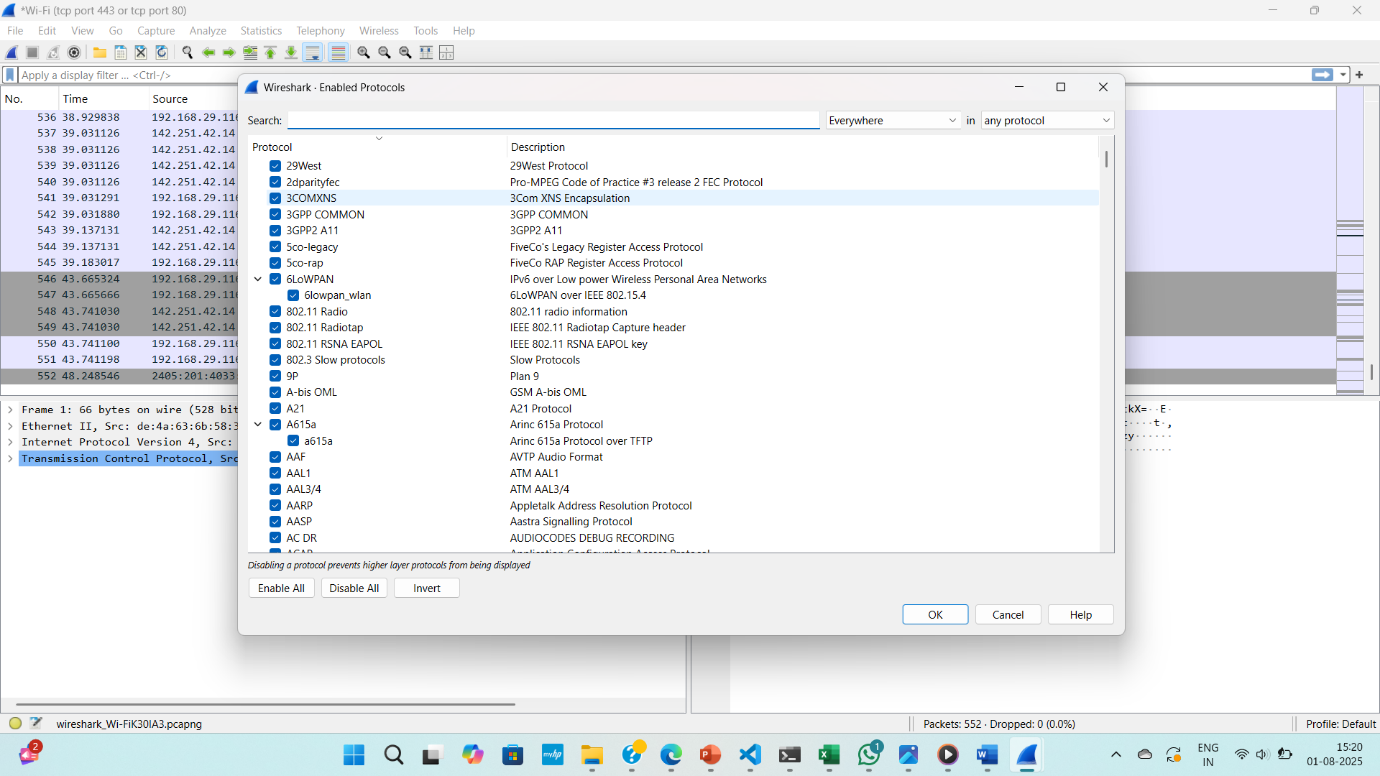


Colouring rule to analyse different traffic rules

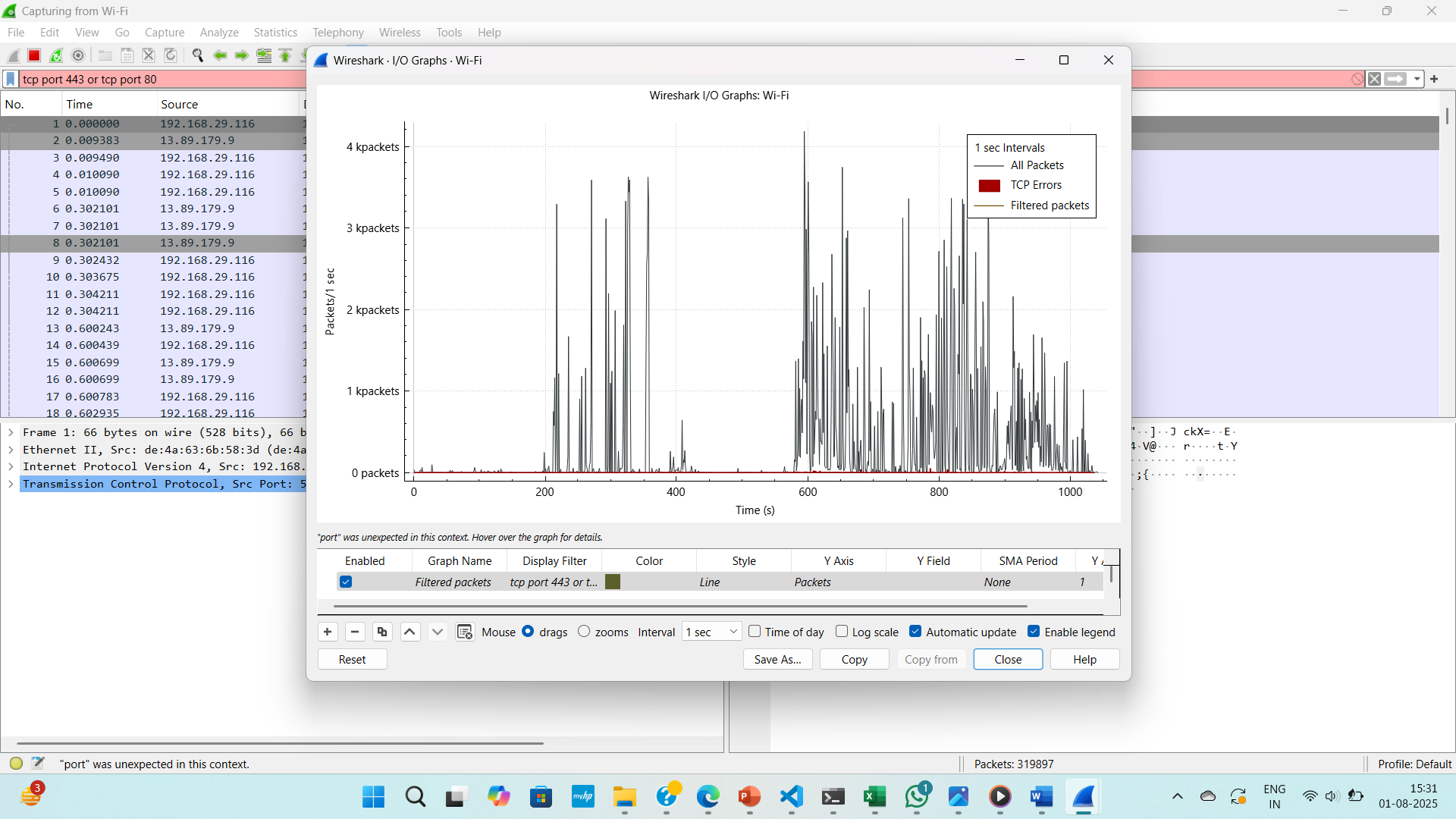
Filter and all filter options



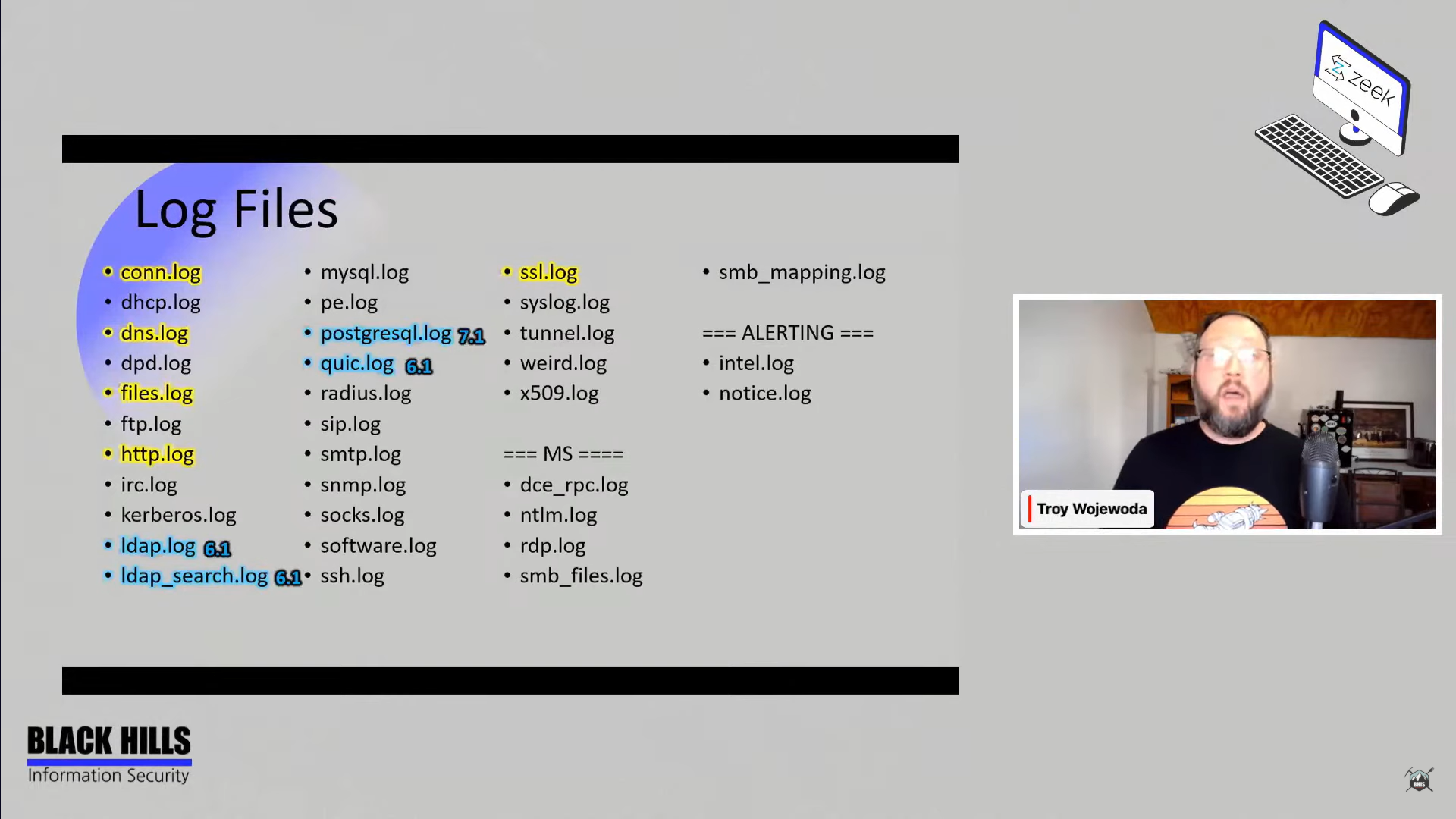
protocols



Graph between traffic volume overtime in wide shark



log files in zeek



Challenges I Faced

 **Wireshark showed too many packets**, and it got confusing. I had to learn how to use filters to make things clearer.

 **Some terms were new** to me (like SYN, ACK, flags, etc.), so I had to Google a lot to understand them.

 I wanted to find something suspicious, but since I was just capturing normal traffic, everything seemed okay. For deeper analysis, I’d need to simulate a hacking attempt or test an app

**Conclusion**

This project helped me **understand what actually happens on a computer network**. By using tools like **Wireshark** and **Zeek**, I was able to **capture, analyse, and understand** real internet traffic. I saw which protocols were used the most, which websites were accessed, and how devices communicate in the background.

Even though this was a beginner-level project, it gave me a solid foundation in:

* **Network traffic monitoring**,
* **Basic cybersecurity tools**, and
* **Interpreting real-world data**.

It also made me more aware of how important it is to keep an eye on network activity—especially in today’s world where data and privacy matter so much.

REFRENCES

 Wireshark Official Website – https://www.wireshark.org/

 Zeek Network Security Monitor – https://zeek.org/

 “Wireshark Tutorial for Beginners” – YouTube