University of Bahrain

College of Information Technology

Department of Network Engineering

ITNE 350

Network Management and Administration

Project

Submitted to: Dr. Alaudeen Yousif Alomari

Done by:

Hesham Ahmed Ghulam - 202003472

Yousif Ahmed Jassim - 202010375

Submitted on: May 27, 2024

Contents

Introduction of Management Tools

Wireshark

Wireshark is like a super detective for computer networks. It helps people see and understand what's happening in a network by showing all the data that's moving around. It's useful for fixing problems with networks, figuring out how different parts of a network talk to each other, and finding any sneaky security problems. Wireshark breaks down all the information into tiny pieces so people can look at each one closely and find any weird stuff going on. It's a must-have tool for keeping networks running smoothly and securely.

PRTG

Paessler PRTG is a comprehensive network monitoring and management solution. It provides a centralized dashboard to monitor the health, performance, and availability of your network devices, servers, and applications. PRTG offers a user-friendly web-based interface and supports a wide range of pre-configured sensors to quickly set up monitoring for various network components.

Installation & Configuration

Wireshark

To download Wireshark:

Navigate to http://www.wireshark.org.

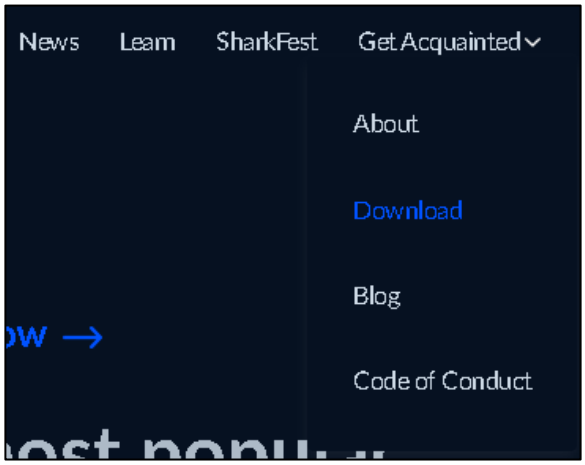


Figure 1: Select Download Wireshark.

Figure 2: Select the Wireshark Windows Installer matching your system type, either 32-bit or 64-bit.

To install Wireshark, follow the following steps:

Figure 3: Click next to proceed.

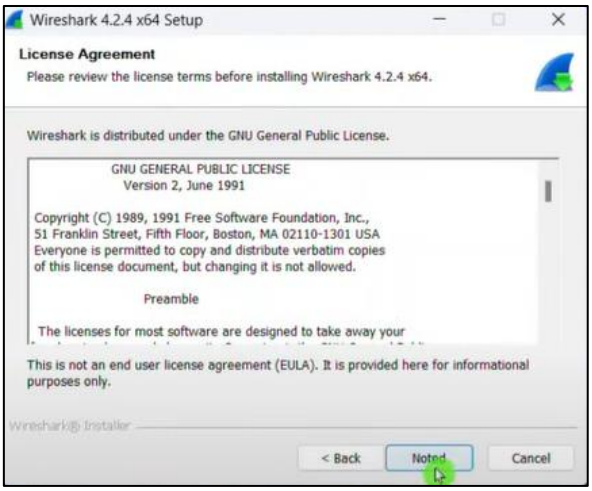


Figure 4: Here you can review Wireshark license term then click next.

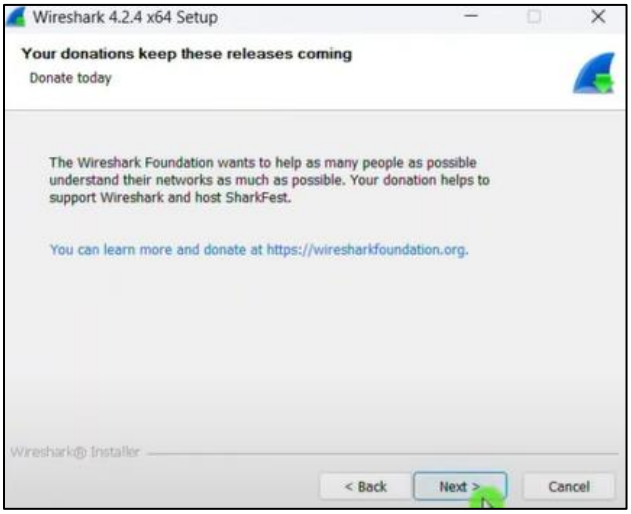


Figure 6: Click next.

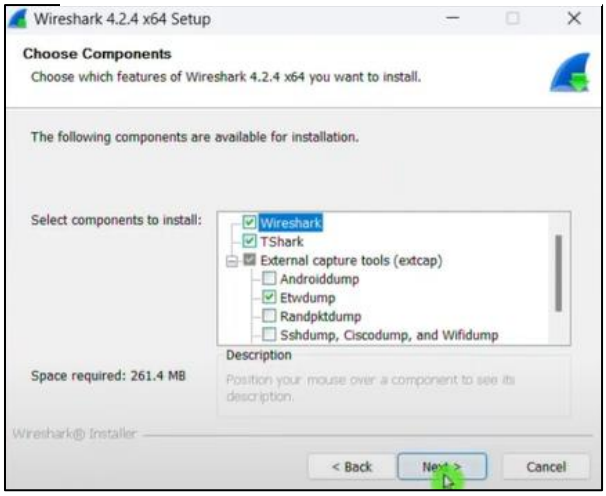


Figure 5: You can choose component as you want then to click next. Also, you can see the required space.

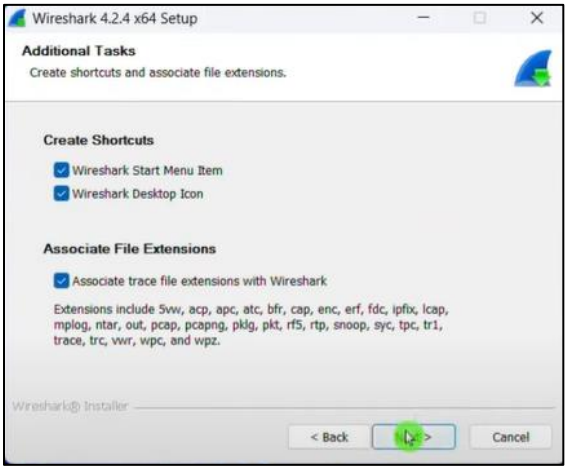


Figure 8: Select all boxes and click next.

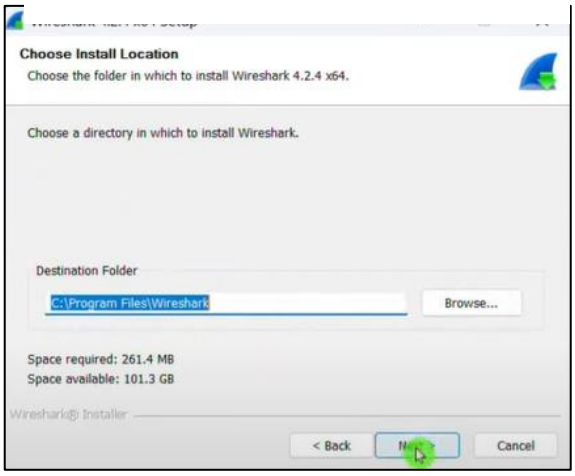


Figure 7: Click next.

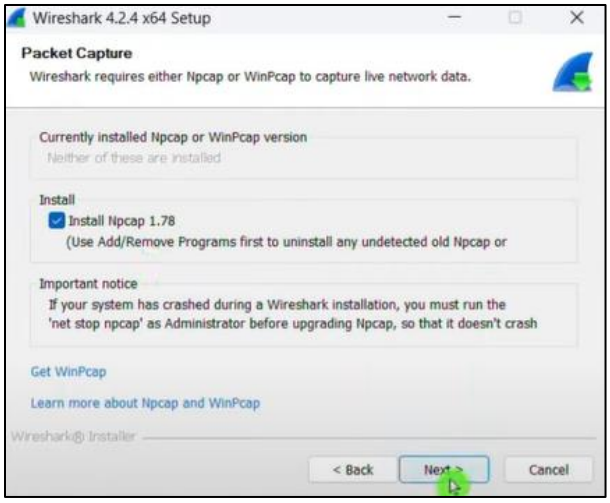


Figure 10:: Npcap automatically selected, then next

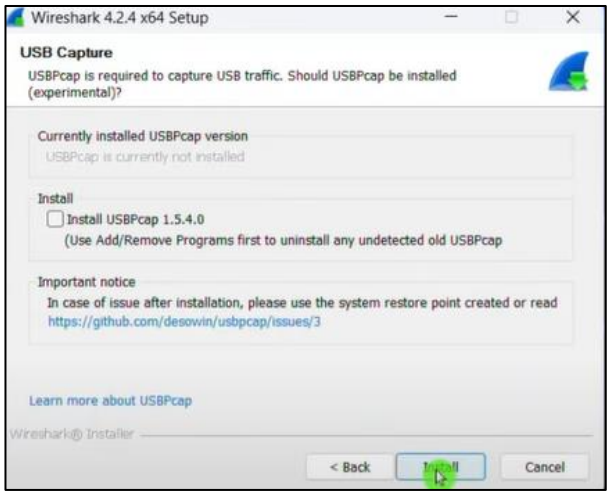


Figure 9: Click next.

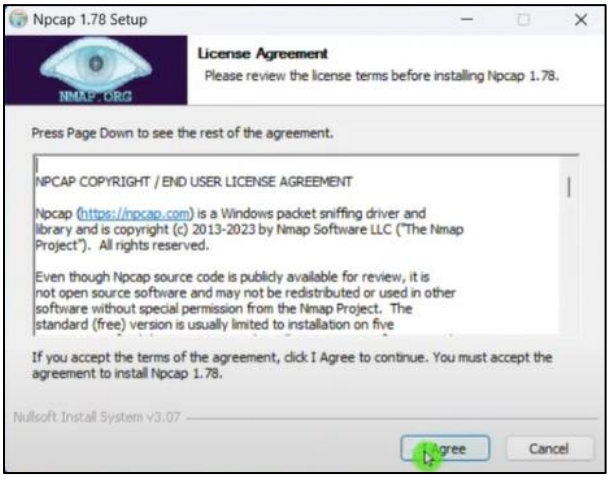


Figure 11: Accept the terms and click agree.

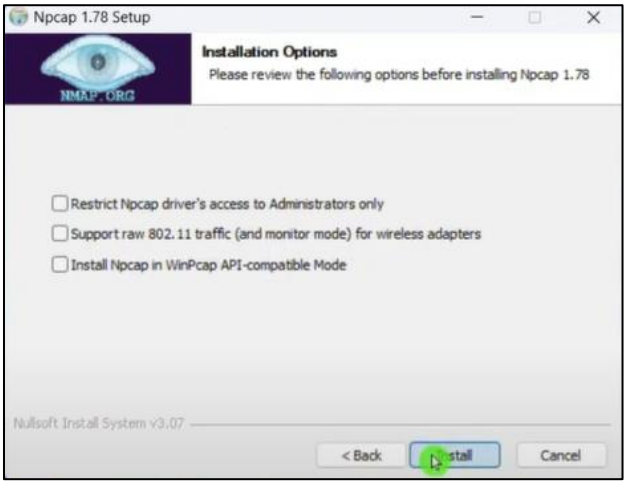


Figure 12: Click next.

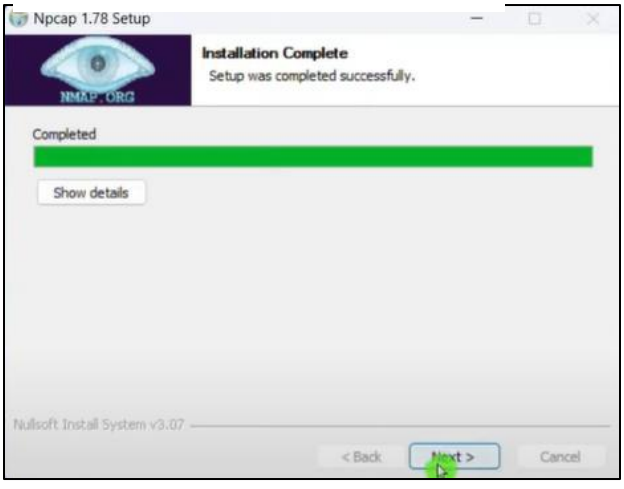


Figure 14: After installation complete, click next.

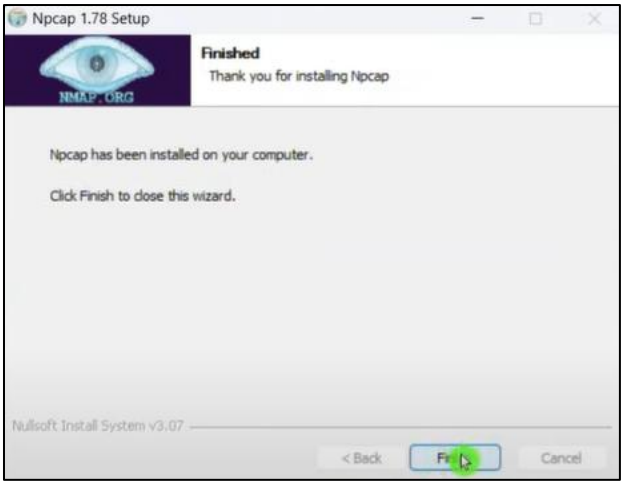


Figure 13: Now click finish.

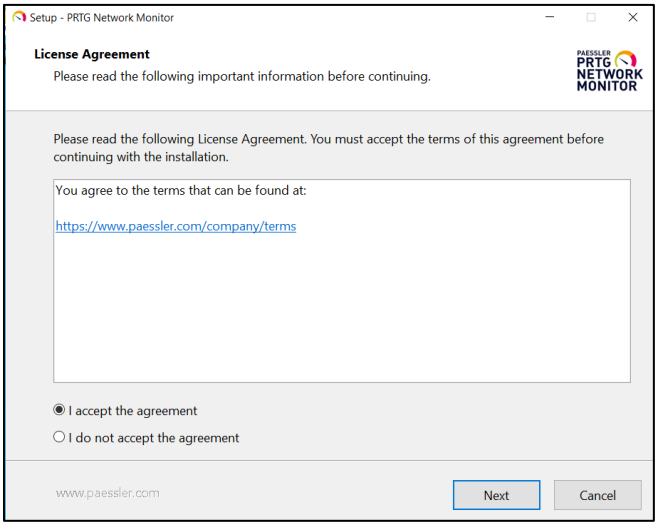


Figure 15

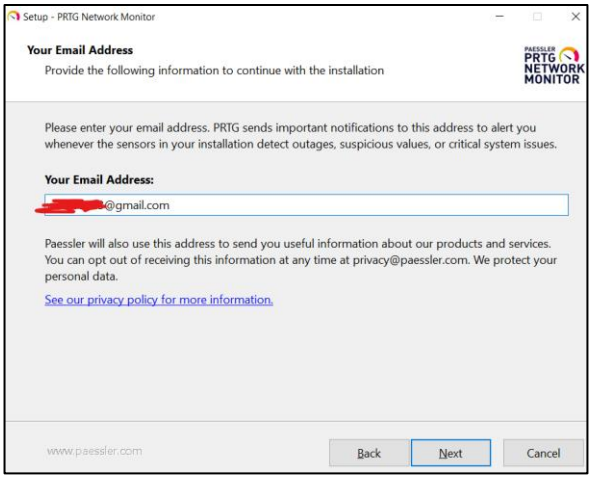


Figure 16

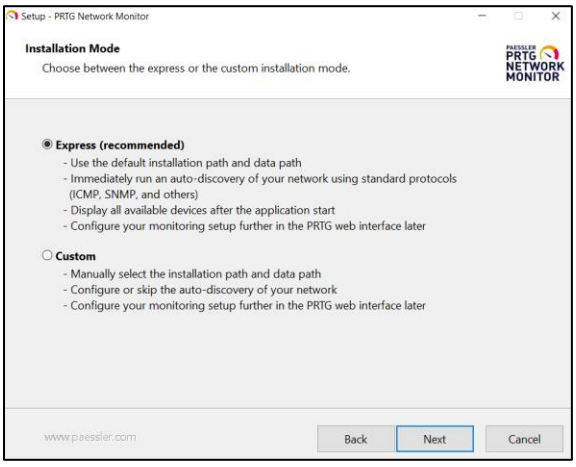


Figure 17

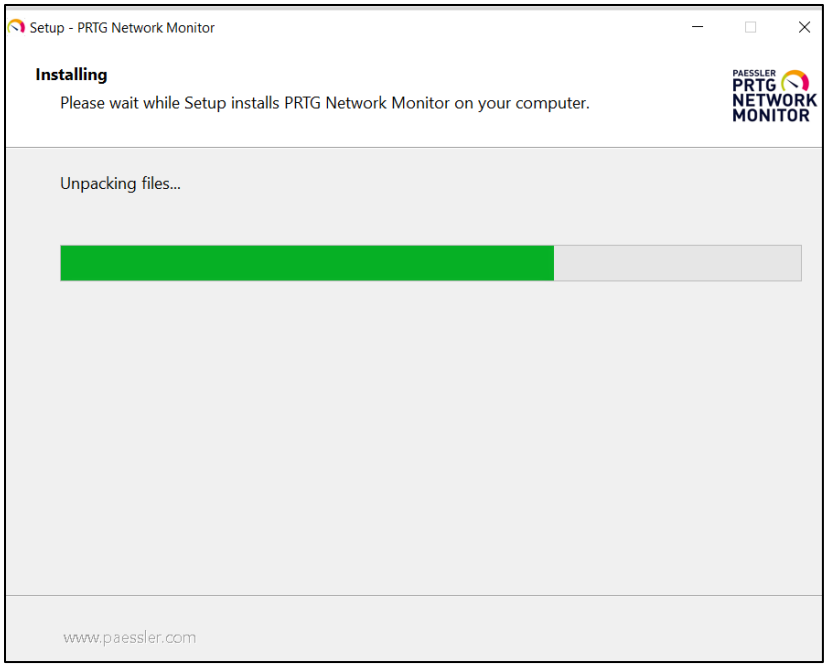


Figure 18

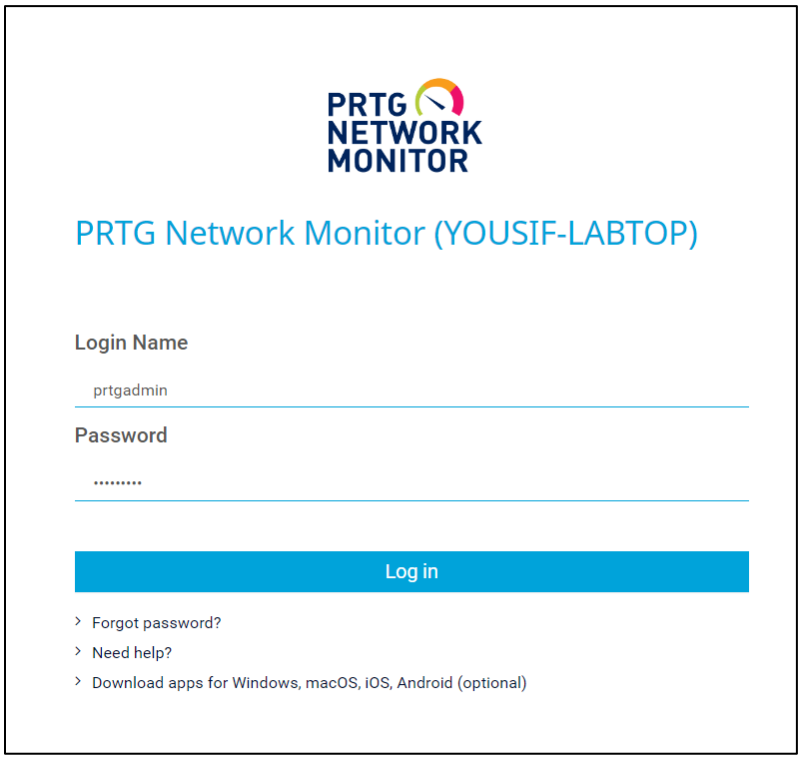


Figure 19

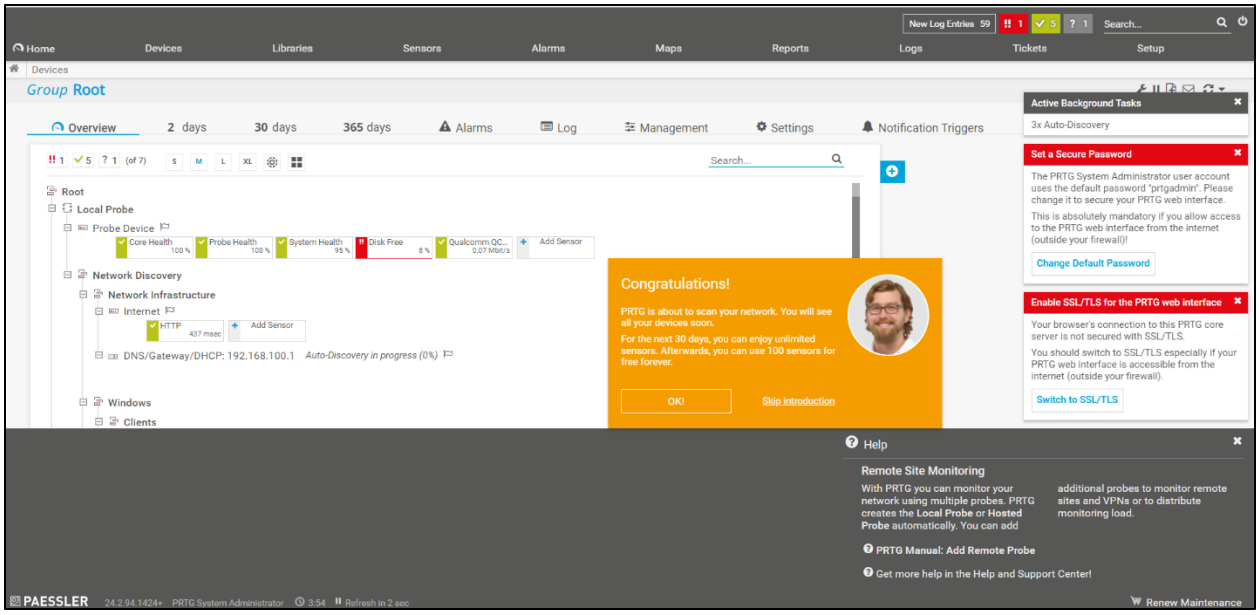


Figure 20

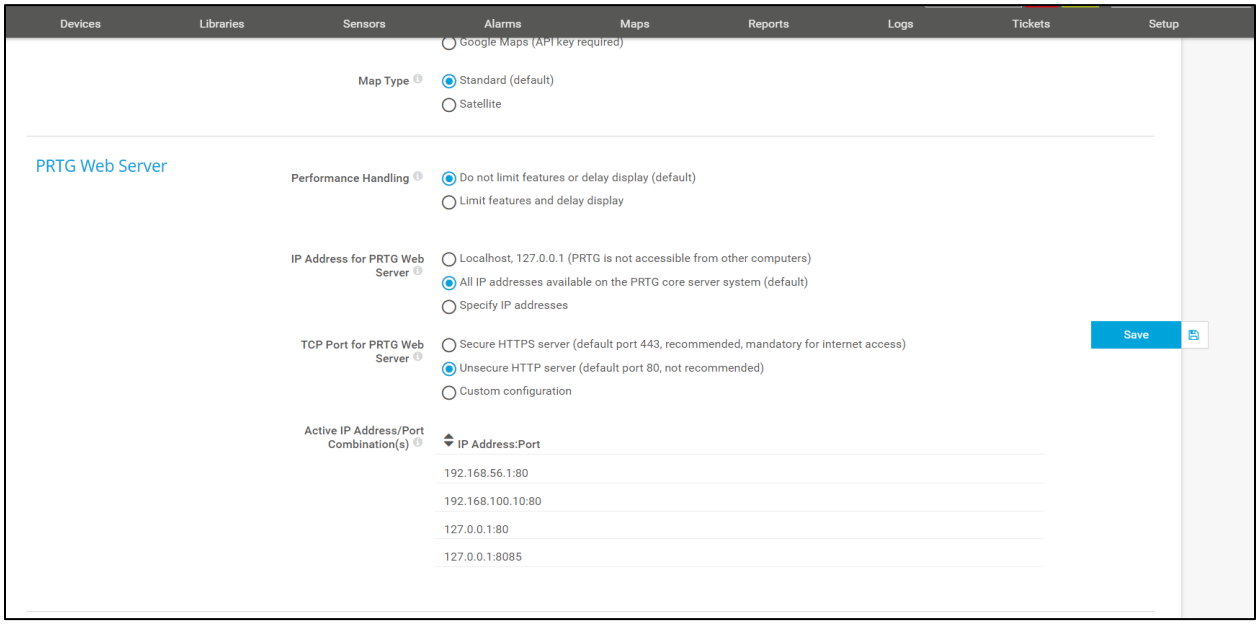


Figure 21

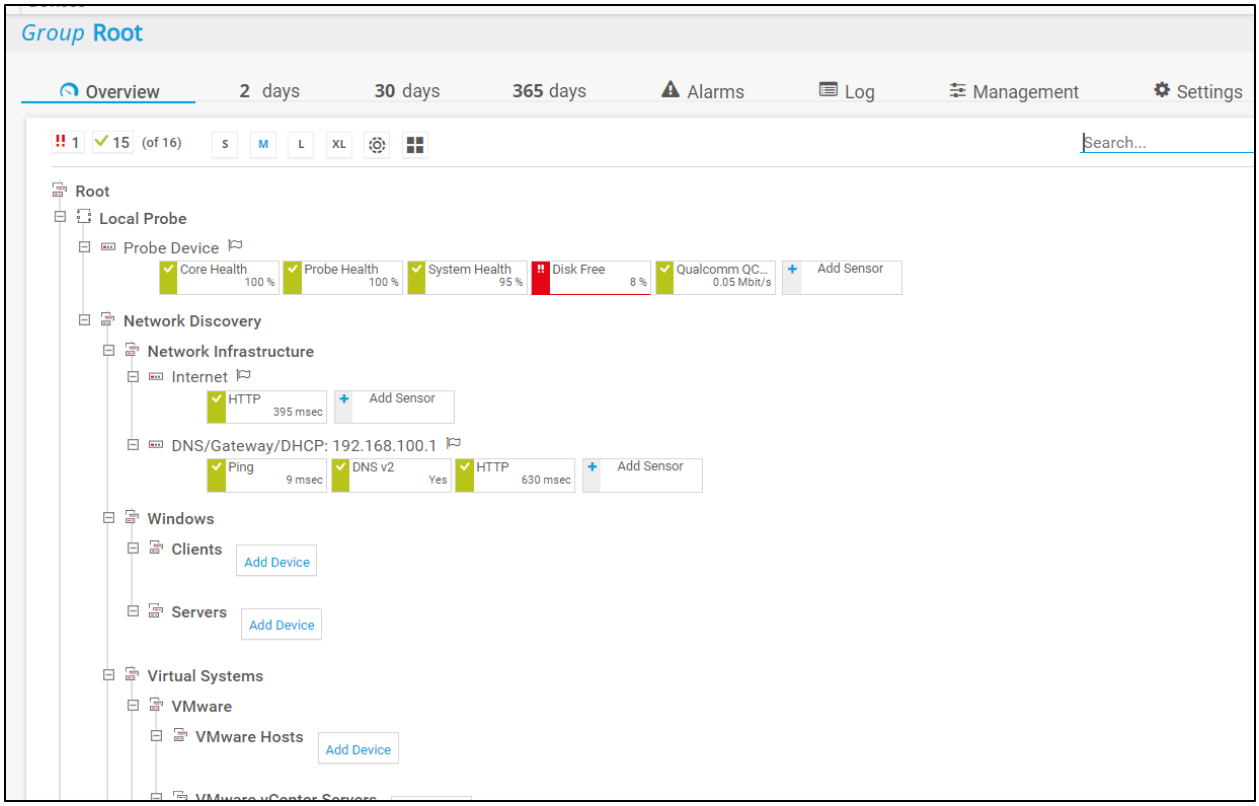

Group Root
Overview
2 days
30 days
365 days
Alarms
Log
Management
Settings
1
15 (of 16)
S
M
L
XL
Search...
Root
Local Probe
Probe Device
Core Health 100 %
Probe Health 100 %
System Health 95 %
Disk Free 8 %
Qualcomm QC... 0.05 Mbit/s
Add Sensor
Network Discovery
Network Infrastructure
Internet
HTTP 395 msec
Add Sensor
DNS/Gateway/DHCP: 192.168.100.1
Ping 9 msec
DNS v2 Yes
HTTP 630 msec
Add Sensor
Windows
Clients
Add Device
Servers
Add Device
Virtual Systems
VMware
VMware Hosts
Add Device

Figure 22

Functionalities of Management Tools

Wireshark

Wireshark is good at watching and studying the data that flows through a network. It does a lot of helpful things:

Packet Capturing: It can grab all the data passing through a network in real-time, whether it's from a computer's Ethernet, Wi-Fi, or Bluetooth connection. You can watch the data as it's happening or look at data that was saved earlier.

Protocol Analysis: Wireshark knows how to understand lots of different types of data, like when computers talk to each other using TCP, UDP, or other protocols. It can break down the data into smaller pieces, show you all the details, and tell you what each piece means.

Filtering and Search: It helps you sort through all the data quickly by letting you search for specific things, like a particular IP address or type of data. This way, you can focus on what's important and skip the rest.

Packet Decoding: Wireshark can translate technical data into words that humans can understand, so you can see what's being sent and received.

Statistics and Graphing: It can also give you stats and graphs to show you patterns in the data, like which protocols are being used the most or how big the data packets are. This helps you get a better idea of what's normal and what might be a problem.

PRTG

- Automatically discovers devices and services on your network.
- Monitors network performance, bandwidth usage, server health, and more
- Provides pre-configured sensors for common network components.
- Offers customizable dashboards and reports.
- Sends alerts and notifications for detected issues.

Network Monitoring for One Day.

Wireshark

Here in this figure, we can choose the interface that we want to monitor and capture its ongoing and outgoing packets.

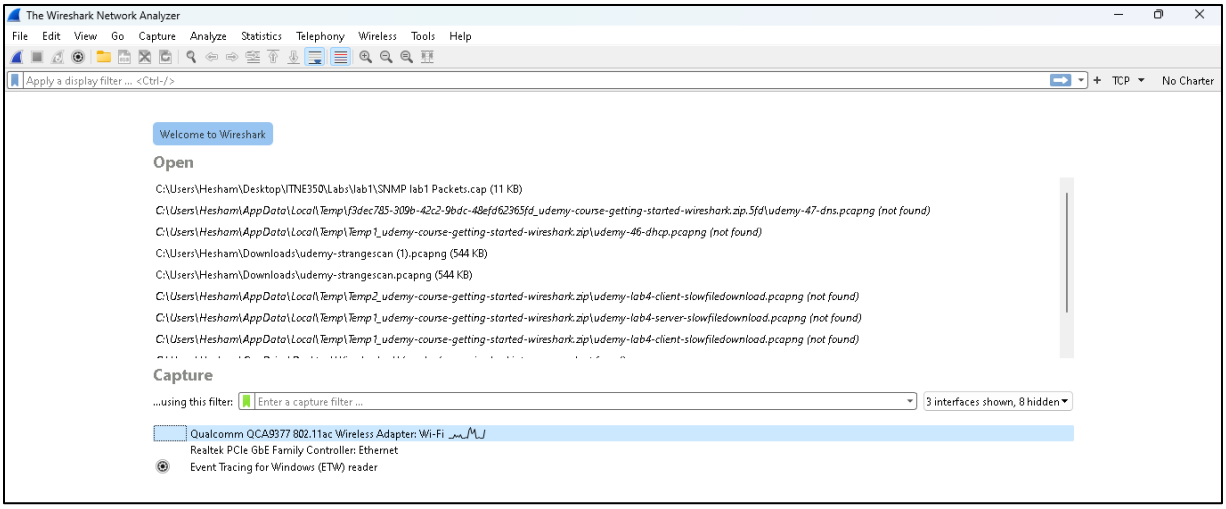


Figure 23: First page when we start the Wireshark.

Below are some captures packets of my home network. And you can the total number of packets captured (662654).

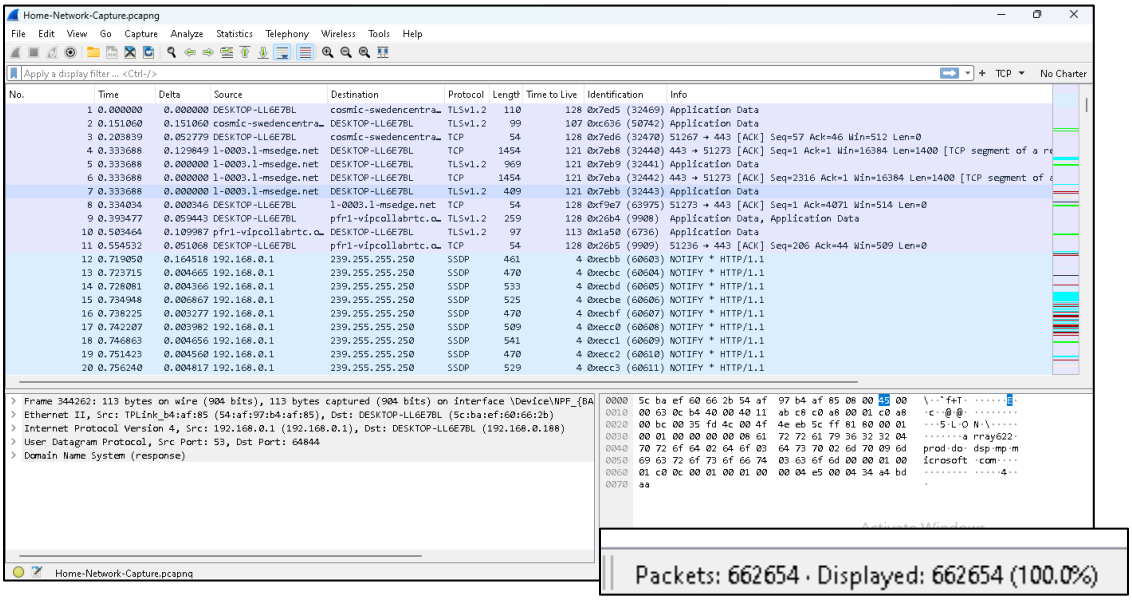


Figure 24

Wireshark has several ways to measure your bandwidth, and one of the easiest is the I/O Graph. This tool lets you plot your data in different ways.

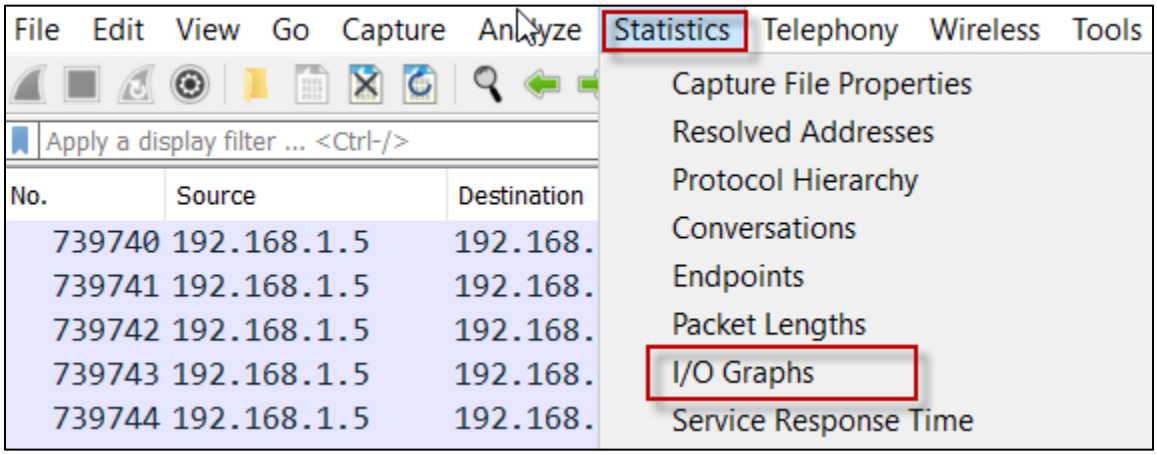


Figure 25: Go to statistic, then I/O Graph.

After opening the I/O Graph, you'll see your bandwidth usage displayed as the number of "packets." To view it in bits per second, change the Y Axis value to "Bits" and keep the "interval" set to 1 second.

The I/O Graph window lets you customize the plots. If you want to compare traffic from two different Ips or two different protocols, you can add multiple rows and create display filters to show only the traffic you care about. In the example below, I set up two display filters to show two different graphs in the same window. This helps us compare the traffic and get a better understanding.

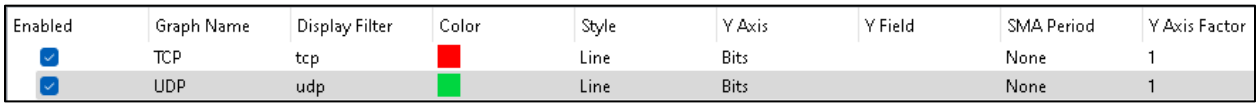


Figure 26: Here we are preparing two plots for two protocols (TCP & UDP)

The red plot represents TCP, and the green plot represents UDP. In the figure below, you can clearly see how much bandwidth was used during that time. Since the plot is based on actual data (packets), it is the most accurate way to measure bandwidth.

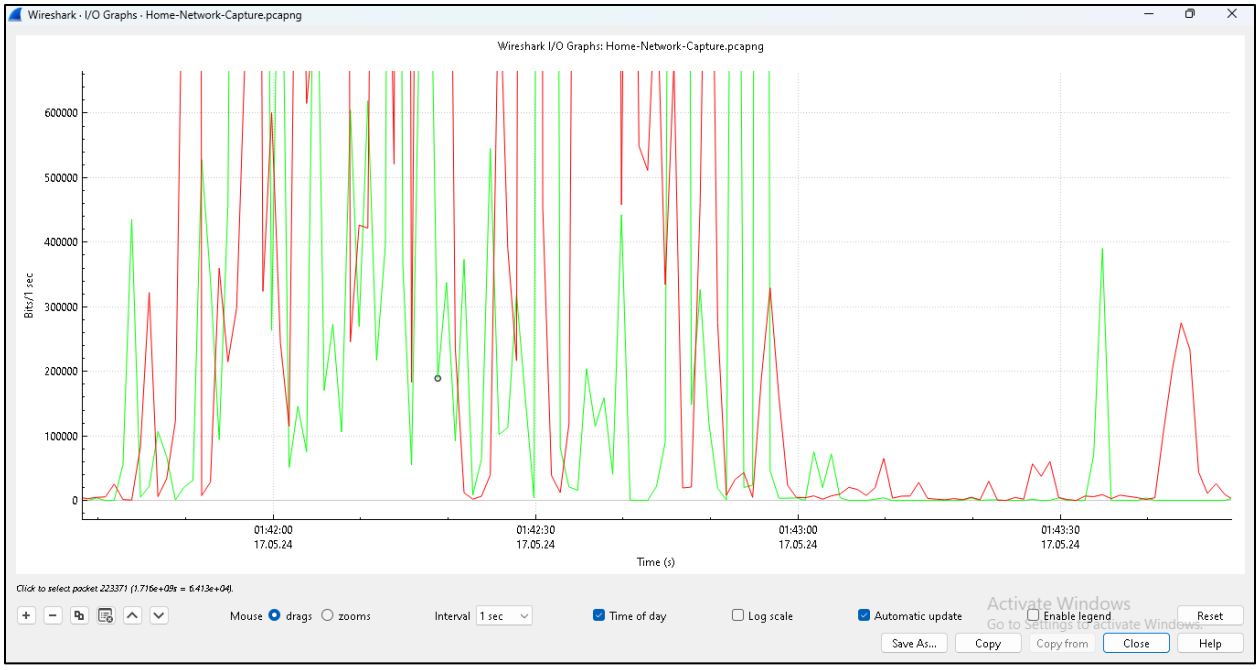


Figure 27: Here we want to compare which protocol consuming bandwidth more.

Bandwidth overuse can slow down your network performance. It can be hard to figure out which application or client is using the most bandwidth. One way to find out is by collecting flows (like NetFlow or SFlow) but setting this up is complicated and expensive. Another option is to use Wireshark to identify top bandwidth users. Wireshark has many useful tools, some of which are explained below.

In this window, we will be able to see layer 2, 3 and 4 endpoints, which are Ethernet, IP, and TCP or UDP. Let's sniff our interface and discover who is consuming most of our bandwidth. The steps are below.

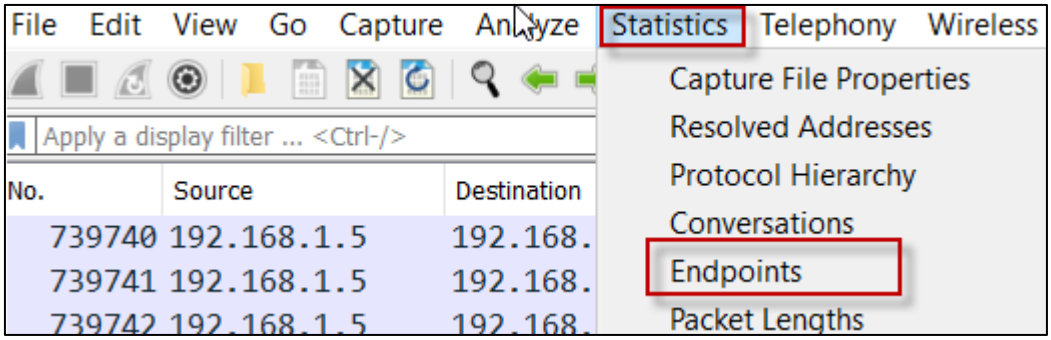


Figure 28: From statistic menu, Click Endpoints.

Now, I select the IPv4 tab and sort the IP addresses (Endpoints) by Tx Bytes (transmitted bytes). You can sort by various criteria like Packets, Bytes, Tx Packets, Tx Bytes, Rx Packets, Rx Bytes, and more. After sorting by transmitted bytes, the top row shows the endpoint that used the most bandwidth. See my output below.

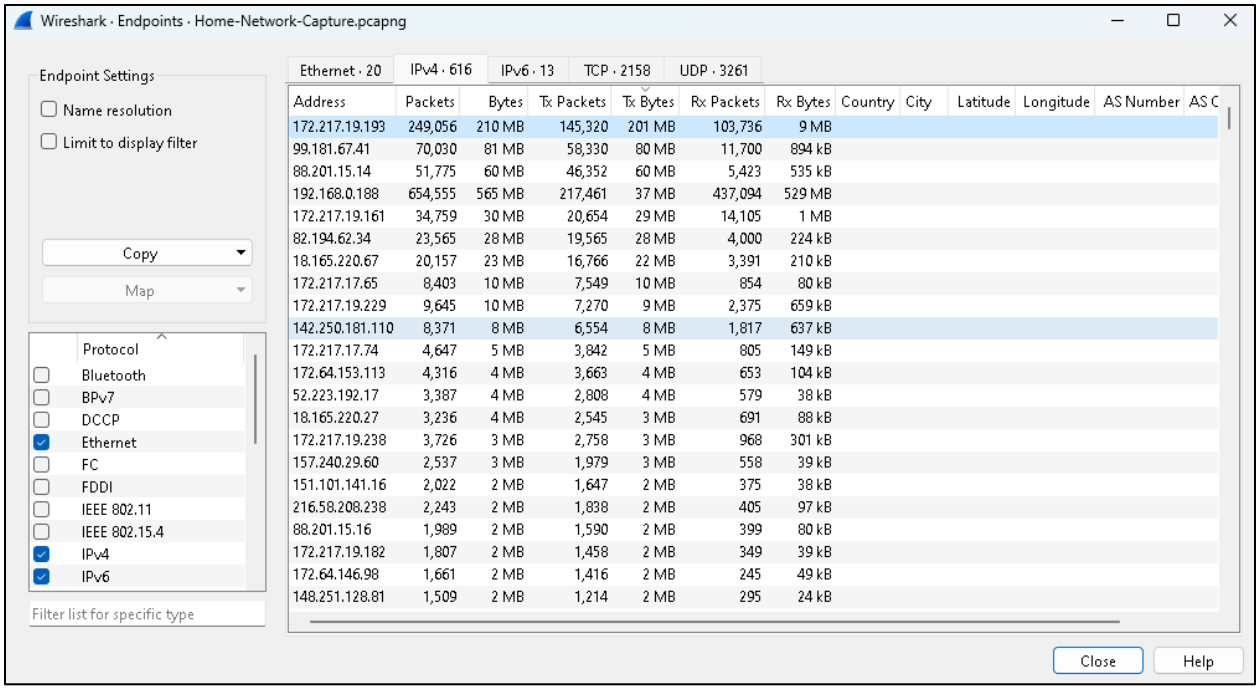


Figure 29: The first row is using most bandwidth.

You can enable name resolution, if the IP addresses in the figure above are not familiar to you. From the Edit menu, click on the Preferences then Name Resolution:

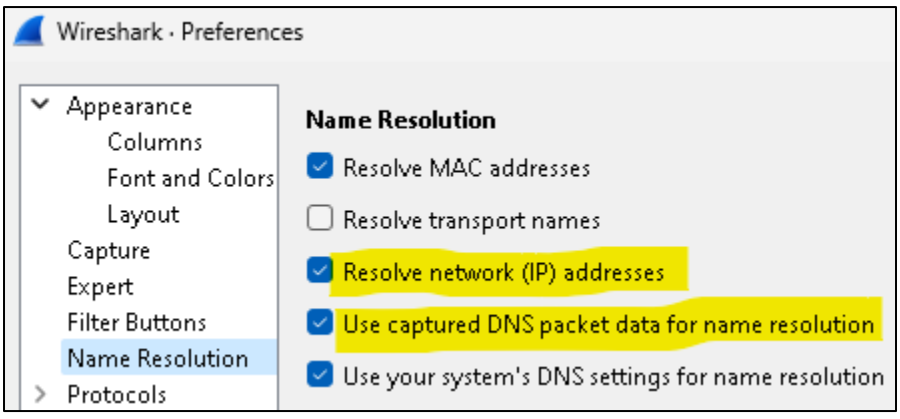
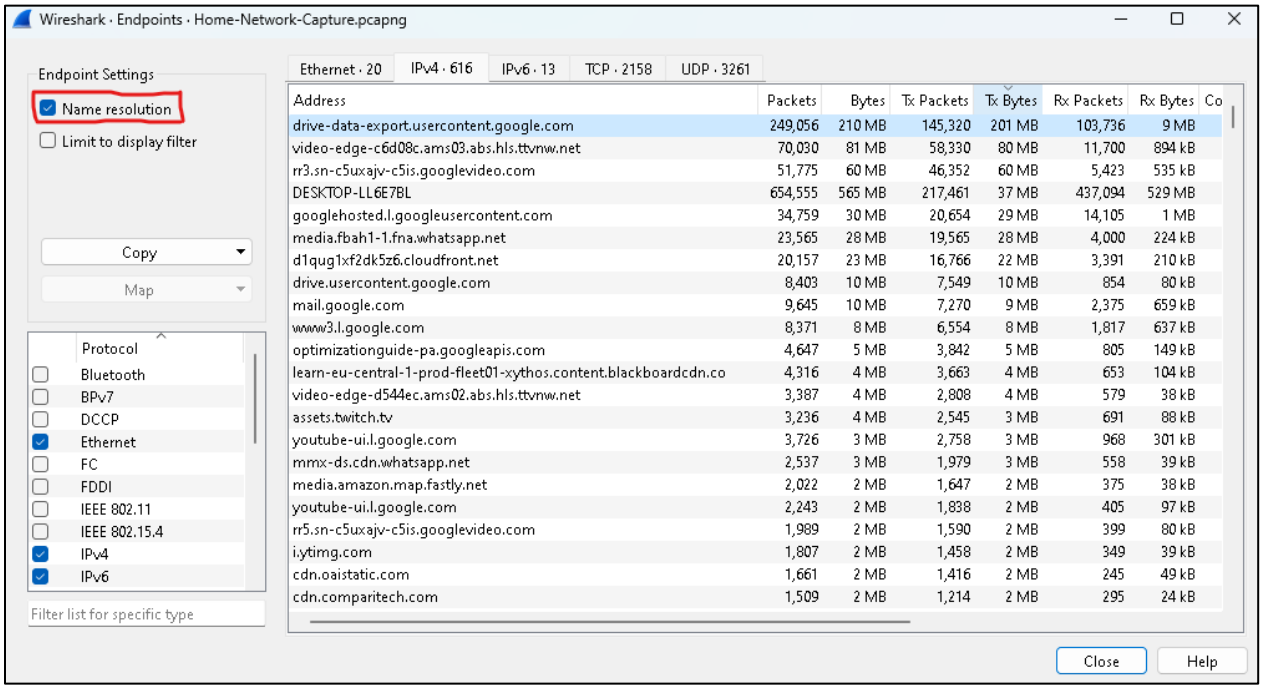


Figure 30

As you can see below now you are able to see which endpoint is consuming more bandwidth with its domain name.

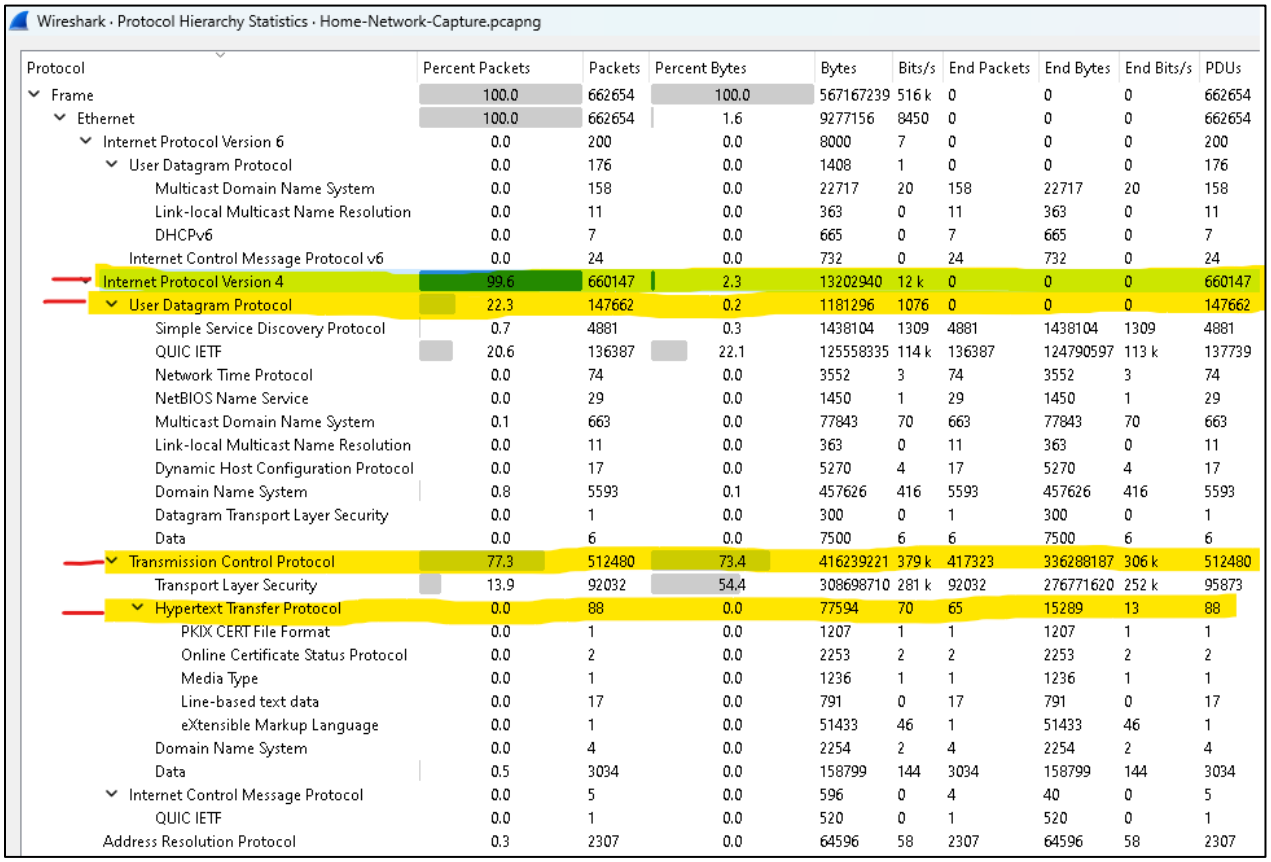


Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Co
drive-data-export.usercontent.google.com	249,056	210 MB	145,320	201 MB	103,736	9 MB	
video-edge-c6d08c.ams03.abs.hls.ttvnw.net	70,030	81 MB	58,330	80 MB	11,700	894 kB	
rr3.sn-c5uxajv-c5is.googlevideo.com	51,775	60 MB	46,352	60 MB	5,423	535 kB	
DESKTOP-LL6E7BL	654,555	565 MB	217,461	37 MB	437,094	529 MB	
googlehosted.l.googleusercontent.com	34,759	30 MB	20,654	29 MB	14,105	1 MB	
media.fbah1-1.fna.whatsapp.net	23,565	28 MB	19,565	28 MB	4,000	224 kB	
d1qug1xf2dk5z6.cloudfront.net	20,157	23 MB	16,766	22 MB	3,391	210 kB	
drive.usercontent.google.com	8,403	10 MB	7,549	10 MB	854	80 kB	
mail.google.com	9,645	10 MB	7,270	9 MB	2,375	659 kB	
www3.l.google.com	8,371	8 MB	6,554	8 MB	1,817	637 kB	
optimizationguide-pa.googleapis.com	4,647	5 MB	3,842	5 MB	805	149 kB	
learn-eu-central-1-prod-fleet01-xythos.content.blackboardcdn.co	4,316	4 MB	3,663	4 MB	653	104 kB	
video-edge-d544ec.ams02.abs.hls.ttvnw.net	3,387	4 MB	2,808	4 MB	579	38 kB	
assets.twitch.tv	3,236	4 MB	2,545	3 MB	691	88 kB	
youtube-ui.l.google.com	3,726	3 MB	2,758	3 MB	968	301 kB	
mmx-ds.cdn.whatsapp.net	2,537	3 MB	1,979	3 MB	558	39 kB	
media.amazon.map.fastly.net	2,022	2 MB	1,647	2 MB	375	38 kB	
youtube-ui.l.google.com	2,243	2 MB	1,838	2 MB	405	97 kB	
rr5.sn-c5uxajv-c5is.googlevideo.com	1,989	2 MB	1,590	2 MB	399	80 kB	
i.ytimg.com	1,807	2 MB	1,458	2 MB	349	39 kB	
cdn.oaistatic.com	1,661	2 MB	1,416	2 MB	245	49 kB	
cdn.comparitech.com	1,509	2 MB	1,214	2 MB	295	24 kB	

Figure 31: The first row is using most bandwidth.

Sometimes we need to know how much bandwidth each protocol is using. The "Protocol Hierarchy" window is useful for this. It shows the protocol distribution in the captured file. To analyze packets by protocol, go to the Statistics menu and click on Protocol Hierarchy.

In the figure below, we see that all packets use IPv4. At the transport layer, TCP (Transmission Control Protocol) takes the largest share with 77.3 percent. UDP (User Datagram Protocol) accounts for only 22.3 percent, and HTTP is just 0.0 percent:



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	662654	100.0	567167239	516 k	0	0	0	662654
Ethernet	100.0	662654	1.6	9277156	8450	0	0	0	662654
Internet Protocol Version 6	0.0	200	0.0	8000	7	0	0	0	200
User Datagram Protocol	0.0	176	0.0	1408	1	0	0	0	176
Multicast Domain Name System	0.0	158	0.0	22717	20	158	22717	20	158
Link-local Multicast Name Resolution	0.0	11	0.0	363	0	11	363	0	11
DHCPv6	0.0	7	0.0	665	0	7	665	0	7
Internet Control Message Protocol v6	0.0	24	0.0	732	0	24	732	0	24
Internet Protocol Version 4	99.6	660147	2.3	13202940	12 k	0	0	0	660147
User Datagram Protocol	22.3	147662	0.2	1181296	1076	0	0	0	147662
Simple Service Discovery Protocol	0.7	4881	0.3	1438104	1309	4881	1438104	1309	4881
QUIC IETF	20.6	136387	22.1	125558335	114 k	136387	124790597	113 k	137739
Network Time Protocol	0.0	74	0.0	3552	3	74	3552	3	74
NetBIOS Name Service	0.0	29	0.0	1450	1	29	1450	1	29
Multicast Domain Name System	0.1	663	0.0	77843	70	663	77843	70	663
Link-local Multicast Name Resolution	0.0	11	0.0	363	0	11	363	0	11
Dynamic Host Configuration Protocol	0.0	17	0.0	5270	4	17	5270	4	17
Domain Name System	0.8	5593	0.1	457626	416	5593	457626	416	5593
Datagram Transport Layer Security	0.0	1	0.0	300	0	1	300	0	1
Data	0.0	6	0.0	7500	6	6	7500	6	6
Transmission Control Protocol	77.3	512480	73.4	416239221	379 k	417323	336288187	306 k	512480
Transport Layer Security	13.9	92032	54.4	308698710	281 k	92032	276771620	252 k	95873
Hypertext Transfer Protocol	0.0	88	0.0	77594	70	65	15289	13	88
PKIX CERT File Format	0.0	1	0.0	1207	1	1	1207	1	1
Online Certificate Status Protocol	0.0	2	0.0	2253	2	2	2253	2	2
Media Type	0.0	1	0.0	1236	1	1	1236	1	1
Line-based text data	0.0	17	0.0	791	0	17	791	0	17
eXtensible Markup Language	0.0	1	0.0	51433	46	1	51433	46	1
Domain Name System	0.0	4	0.0	2254	2	4	2254	2	4
Data	0.5	3034	0.0	158799	144	3034	158799	144	3034
Internet Control Message Protocol	0.0	5	0.0	596	0	4	40	0	5
QUIC IETF	0.0	1	0.0	520	0	1	520	0	1
Address Resolution Protocol	0.3	2307	0.0	64596	58	2307	64596	58	2307

Figure 32: Bandwidth used by each protocol in Protocol Hierarchy tab.

PRTG

Figure 33

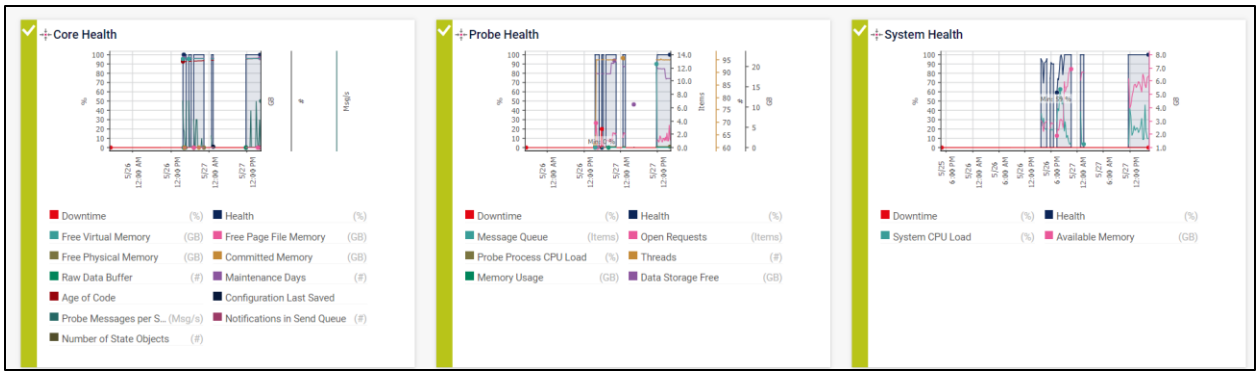


Figure 34

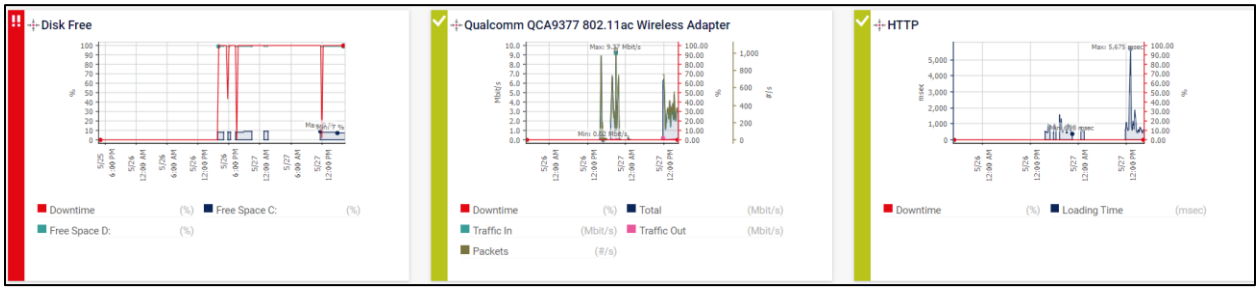


Figure 35

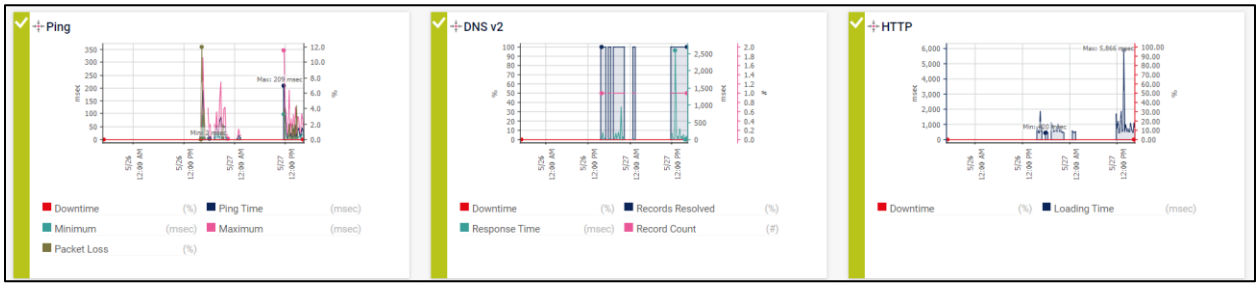


Figure 36

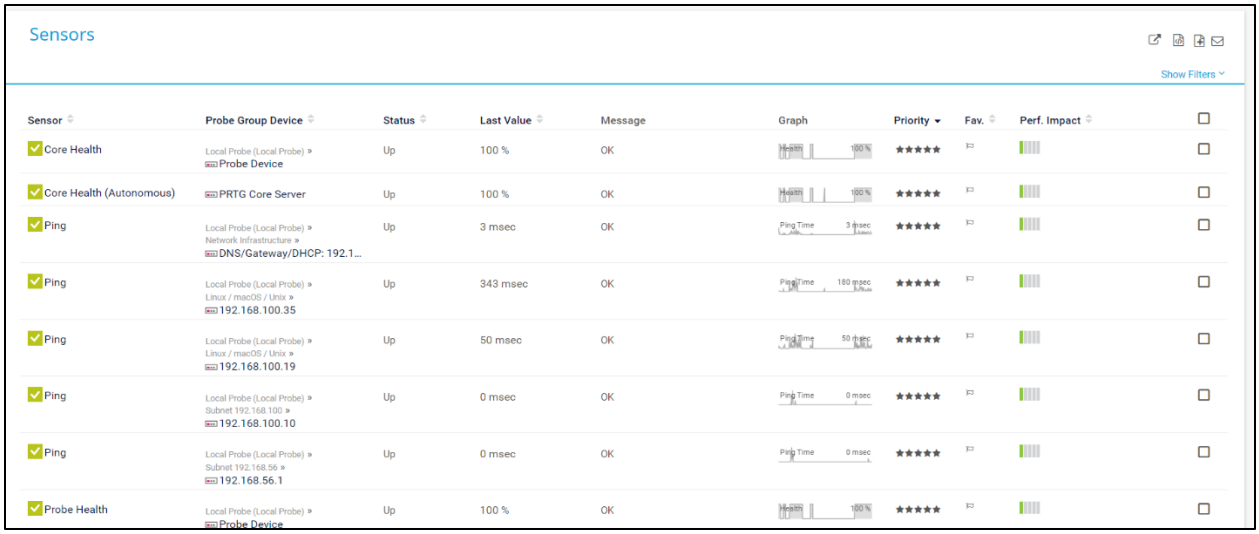


Figure 37

Figure 38

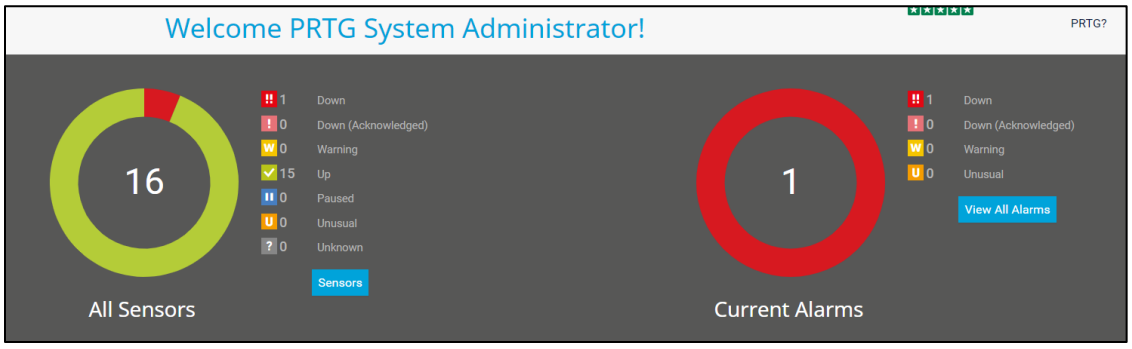


Figure 39

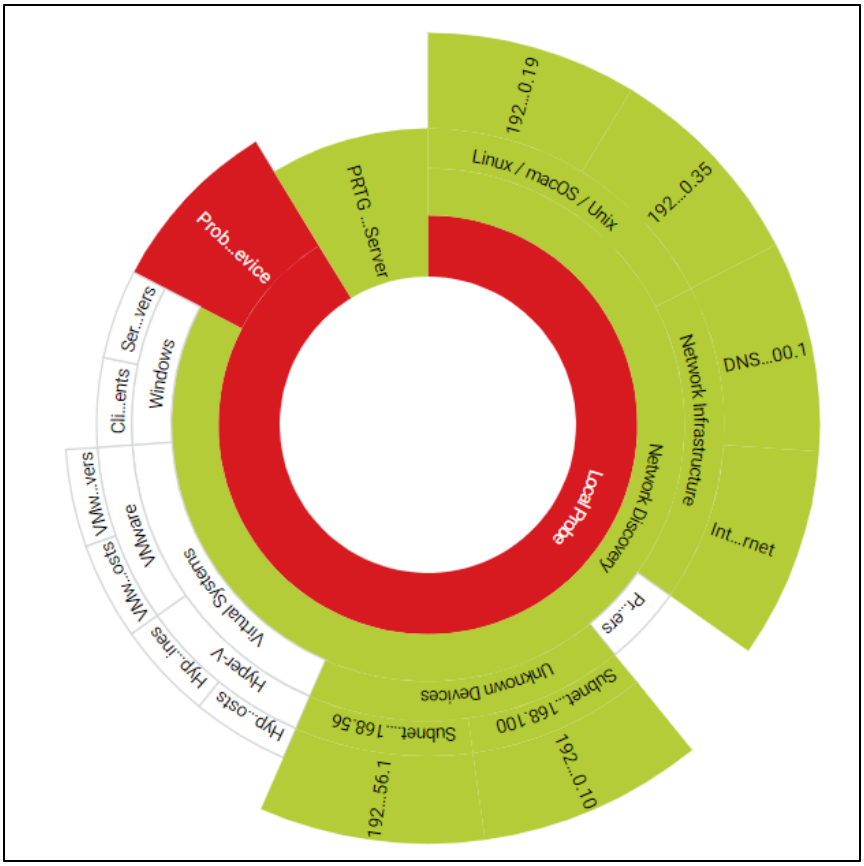


Figure 40

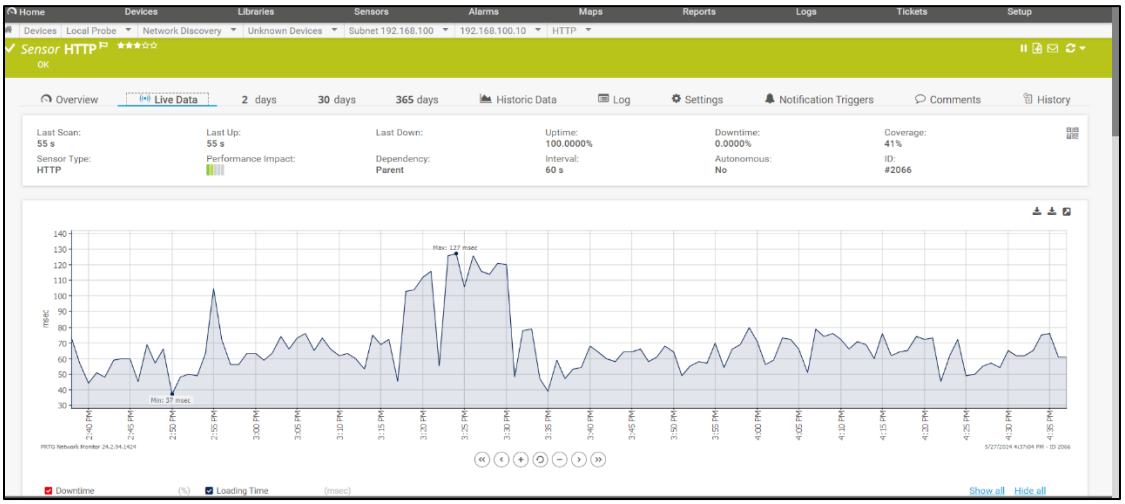


Figure 41

Comparison Between Management Tools.

Wireshark

Advantages

- **Powerful Packet Analysis Capabilities:** Wireshark is good at breaking down data to help users understand how networks work. It can find problems accurately and show exactly what's going on with the data.
- **Real-time Monitoring:** Wireshark can watch data flow as it happens, so users can catch and fix issues right away.
- **Shows Detailed Information:** It gives a lot of detailed info about each piece of data in the network, helping users spot any strange or problematic stuff easily.

Disadvantages

- Hard for Beginners
- Needs Lots of Computer Power

PRTG

Advantages

- Comprehensive network monitoring with pre-configured sensors.
- Intuitive web-based interface for easy setup and management.
- Automated device discovery and monitoring.
- Customizable dashboards and reporting.
- Alerting and notification capabilities.

Disadvantages

- Focused more on high-level network monitoring.
- May require additional configuration for advanced use cases.
- Paid software with a limited free version.