Project Wireshark

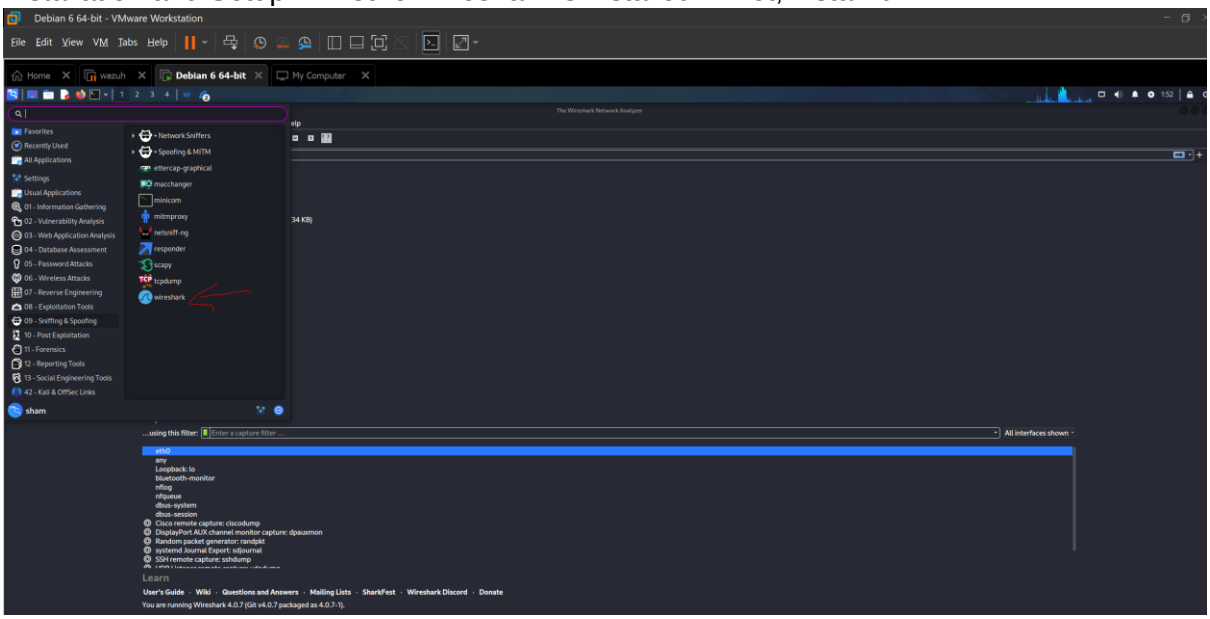
Objective:

To apply the knowledge acquired from the demo on Wireshark and execute a hands-on packet analysis.

Required Tools:

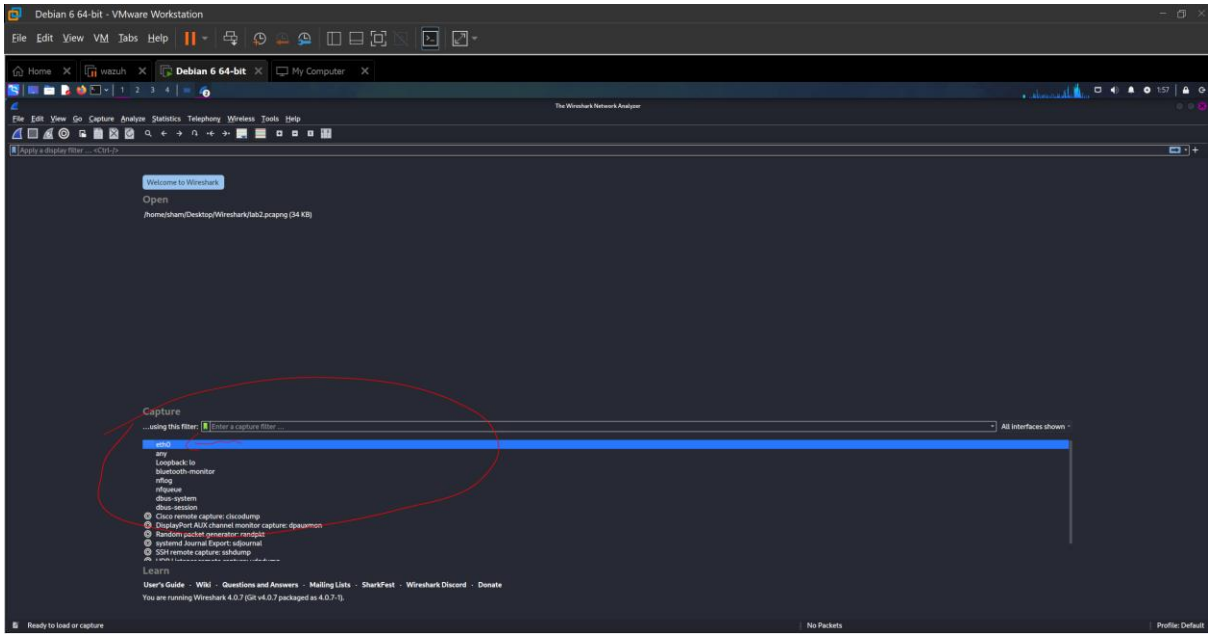
- Kali Linux
- Wireshark
- Network connection (Ethernet/Wi-Fi)

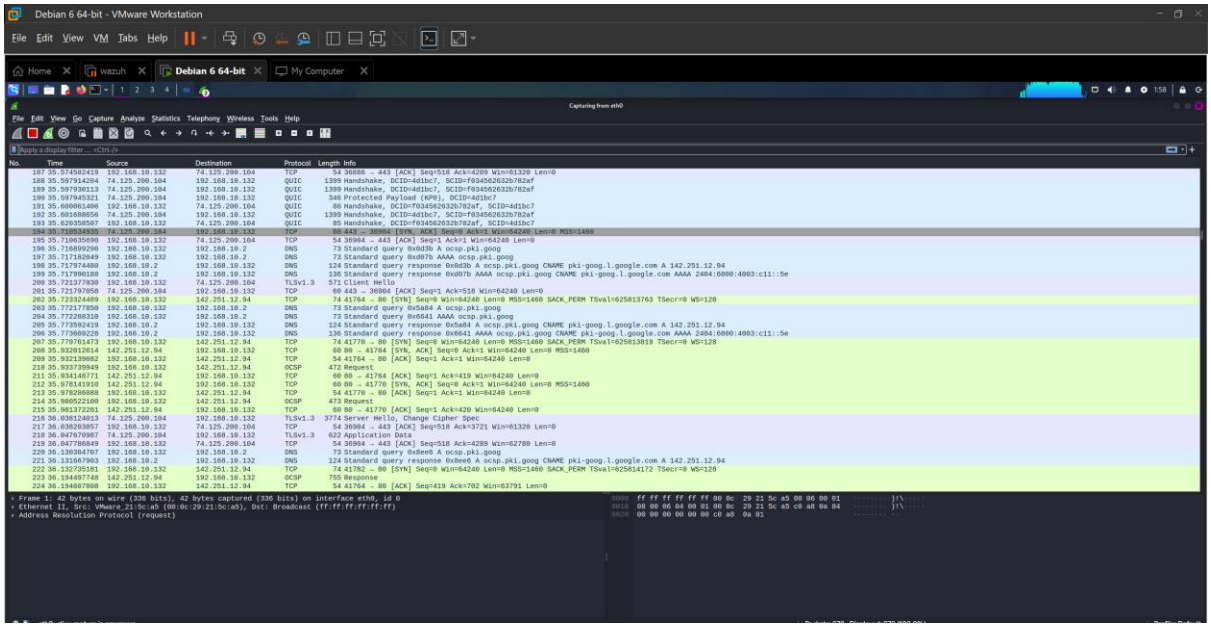
1. Installation and Setup • Ensure Wireshark is installed. If not, install it.



2. Capture Initial Traffic

- Initiate packet capture on your chosen interface (either eth0 or wlan0).
- Capture traffic for approximately 5 minutes. Make note of the total number of packets captured.

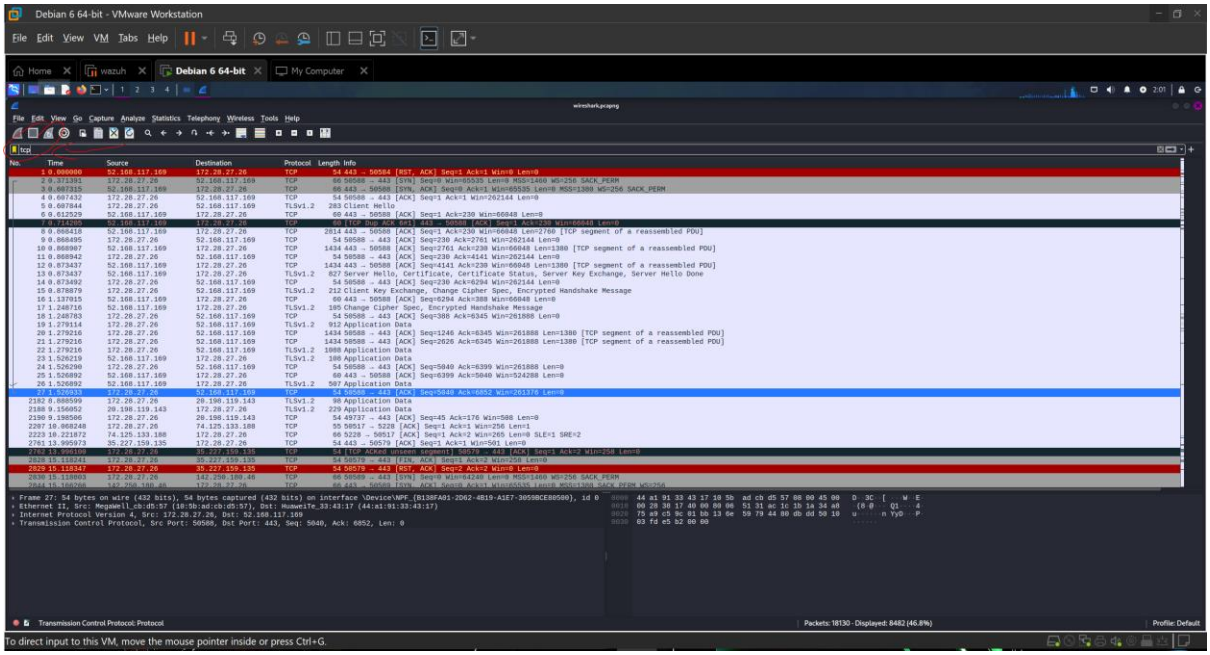




3. Filtering Techniques

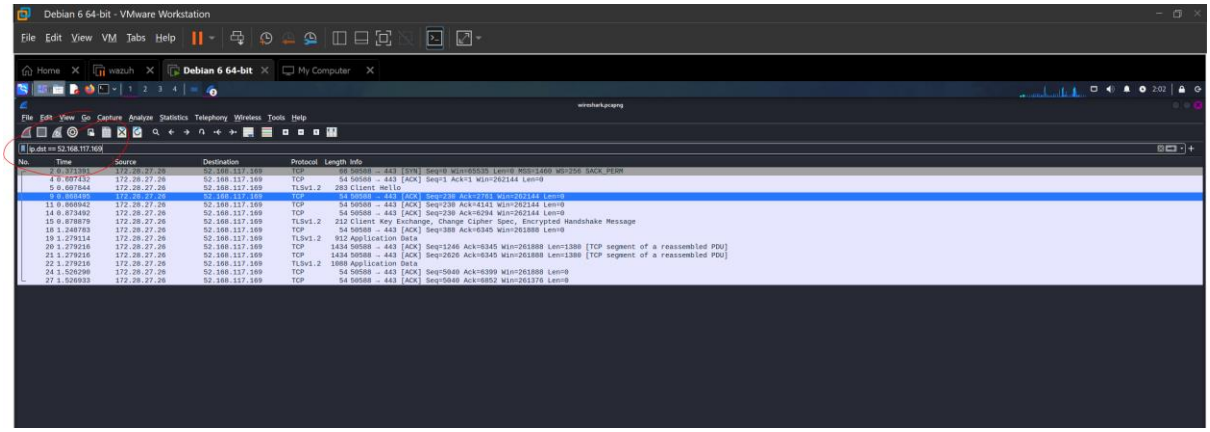
- **TCP Filter:** Display only TCP packets. How many acknowledgment packets did you observe?
- **Destination IP Filter:** Choose any destination IP from the initial capture and filter by it. Record your observations.
- **Protocol and Port Filter:** Filter packets using the UDP protocol and port 53 (DNS). What insights can you gather about DNS queries?

TCP Filter:



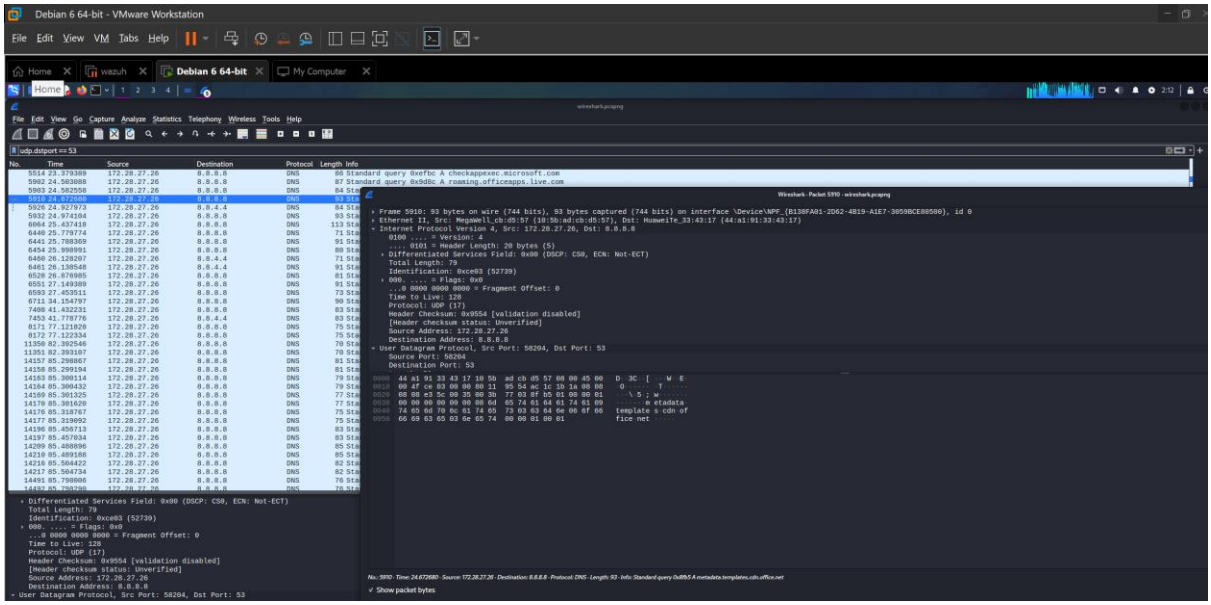
Destination IP Filter:

Ip.dst==52.168.177.169



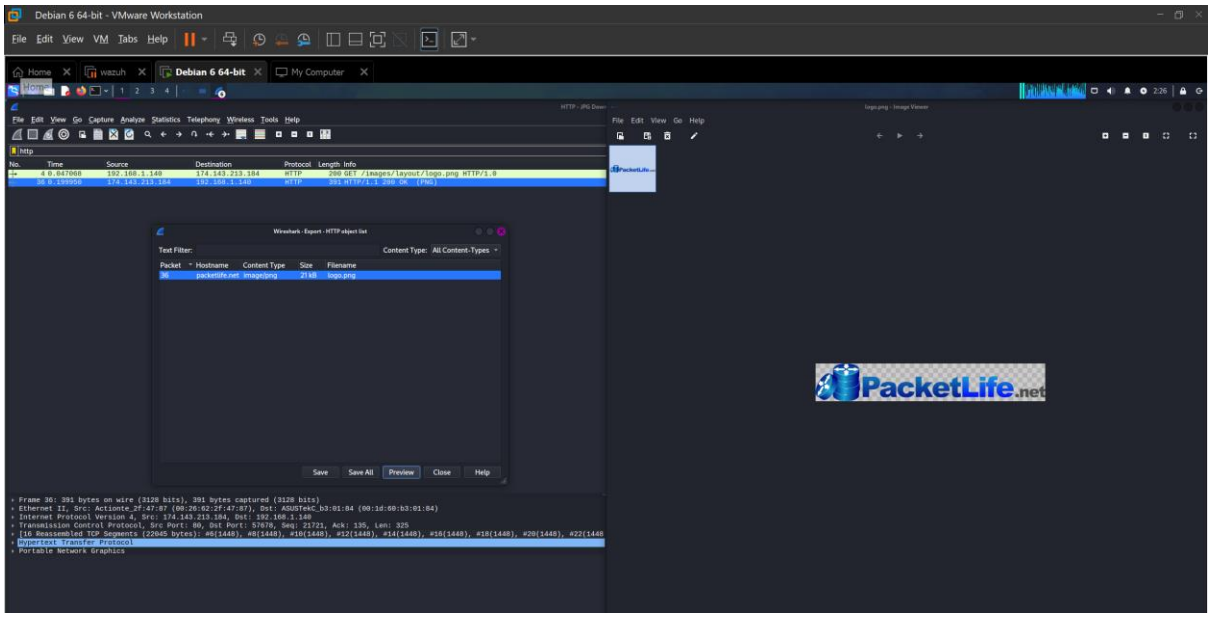
- **Protocol and Port Filter:** Filter packets using the UDP protocol and port 53 (DNS). What insights can you gather about DNS queries?

  UDP (udp.dstport == 53)



4. Data Insights

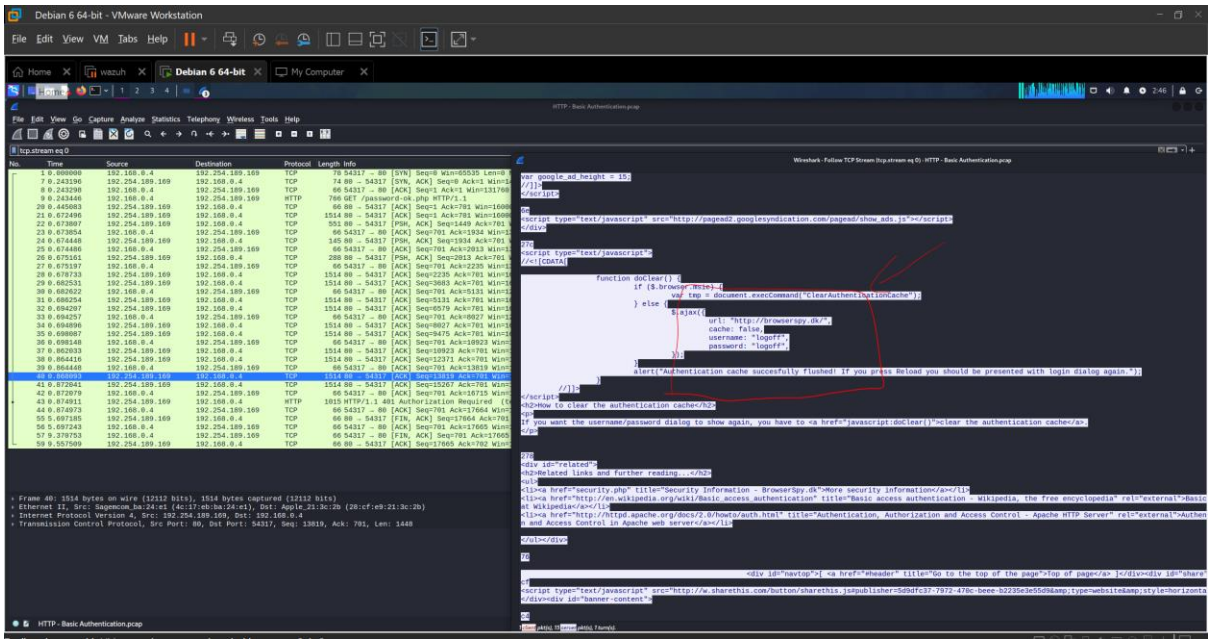
- HTTP Content Extraction: From the HTTP traffic, identify an image transfer, extract, and save the image. Attach the image in your report.



The data image.png

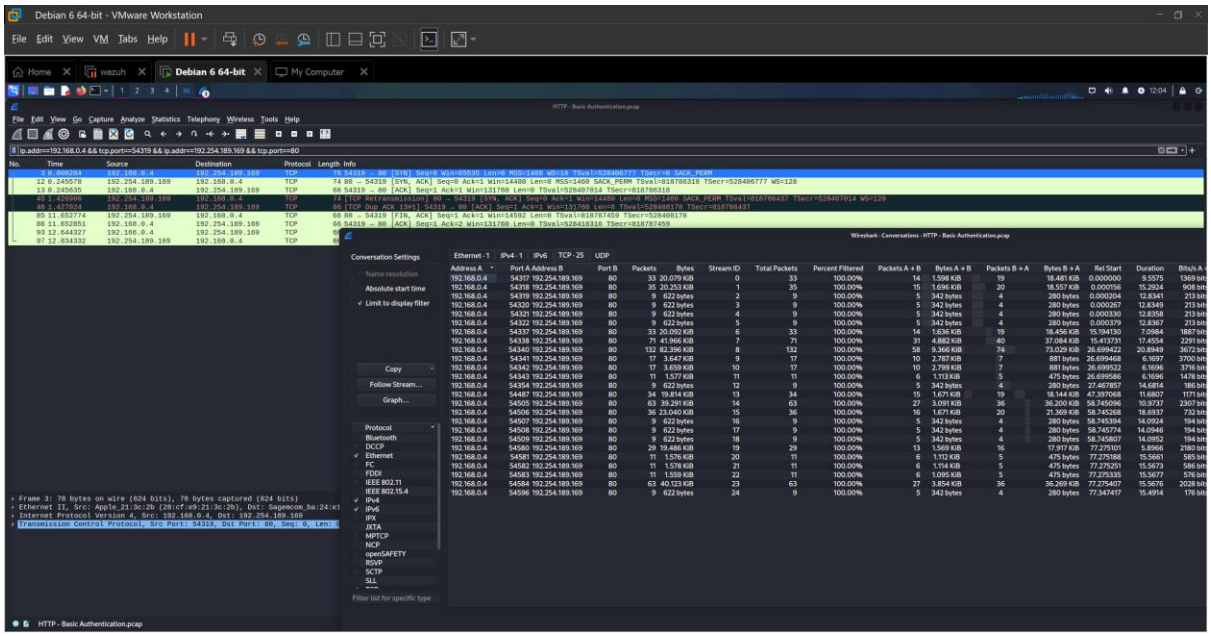
PacketLife.net

- Capture POST Data: Identify a POST request to any website. Document the content of the POST data (ensure no sensitive data is included).



- Firewall Analysis: If you find any denied or blocked traffic, hypothesize potential firewall rules that might be causing it.

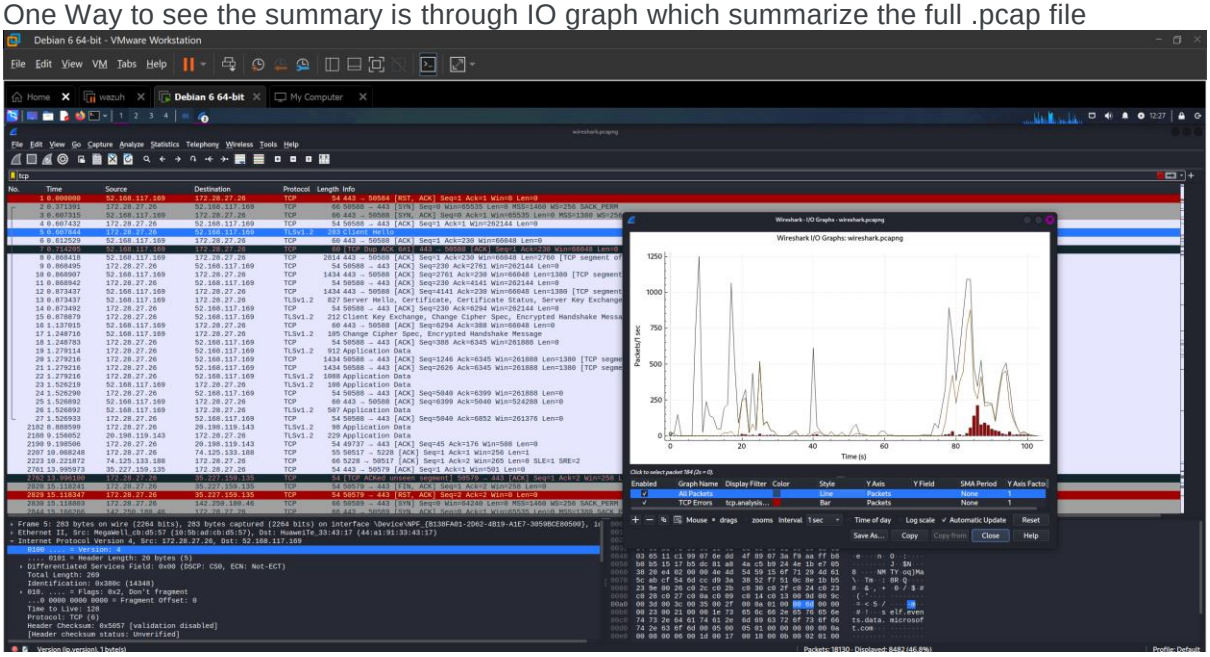
  We can view firewall access or denied traffic by checking TCP SYN-ACK from statistics->Conversional -> TCP and we can see Firewall Access or blocked rules.



5. Advanced Analysis

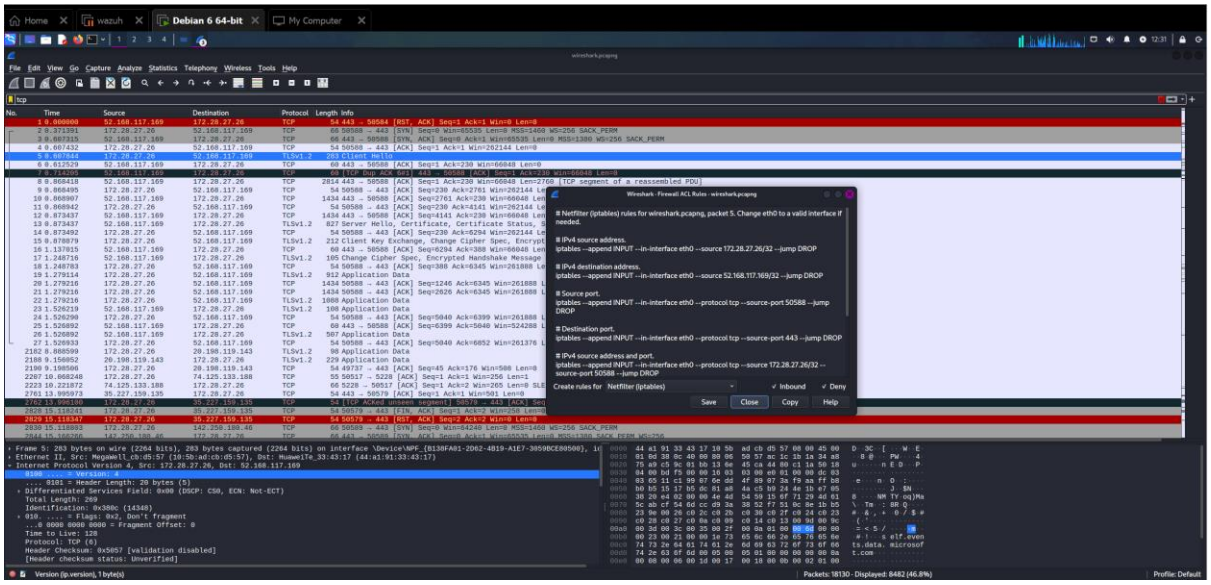
- Traffic Summary: Generate a summary report of your entire capture session. Highlight any anomalies or unexpected findings.
- Top 3 Endpoints: List the top 3 endpoints based on the number of packets. Provide their MAC, IP addresses, and associated protocols.
- Bandwidth Consumption: Using the statistics feature, identify the top 3 IP addresses consuming the most bandwidth. Provide a brief analysis of your findings.

1. One Way to see the summary is through IO graph which summarize the full .pcap file



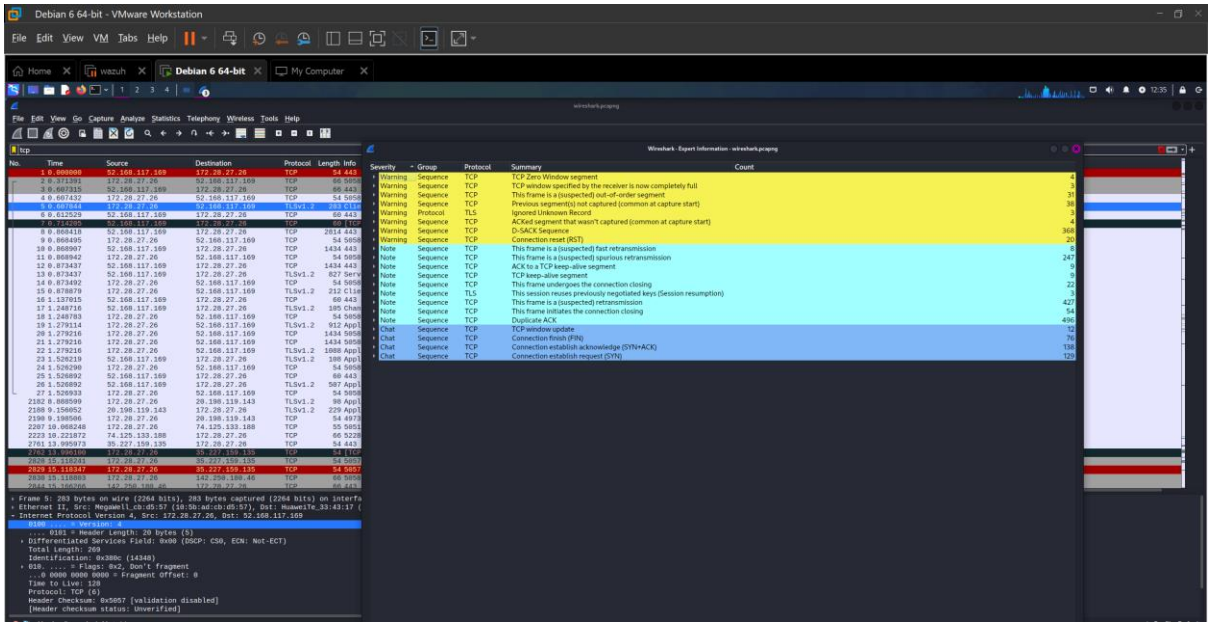
2.Firewall Rule Analysis: Examine any denied traffic to infer potential firewall rules.

We can go to Tools and check the Firewall ACL

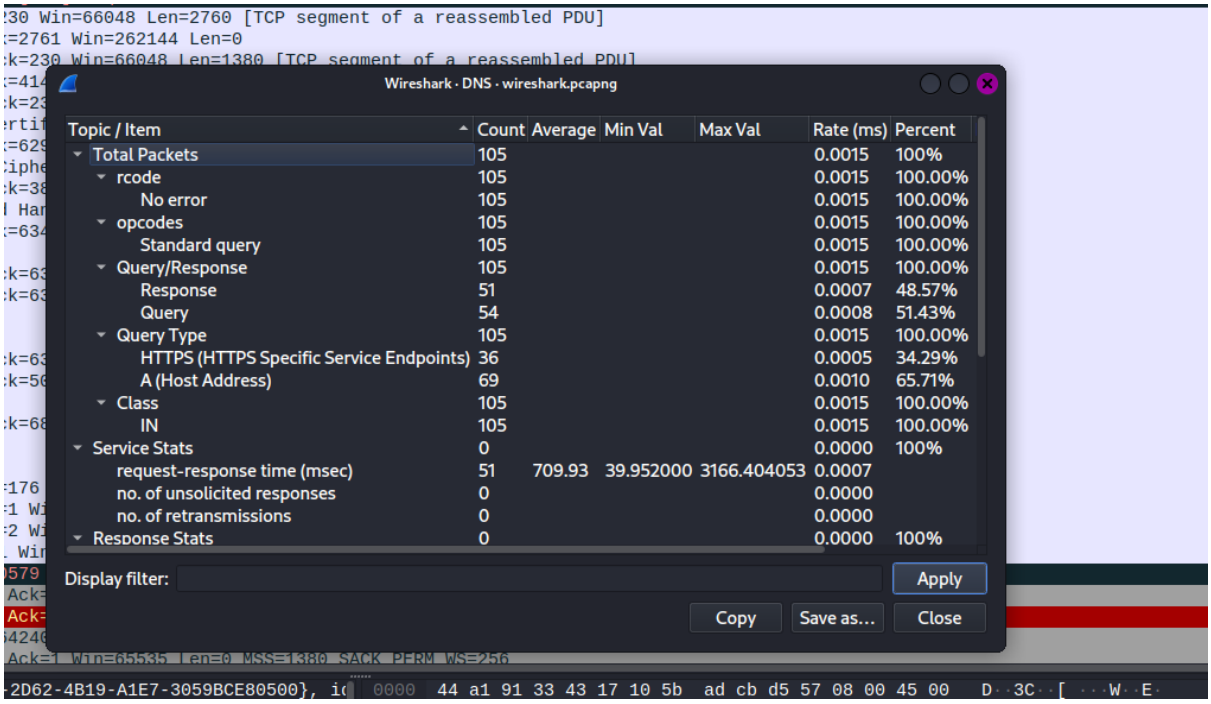


7. Analysis Tools Export Summary: Extract a summary of network traffic, noting any errors or warnings

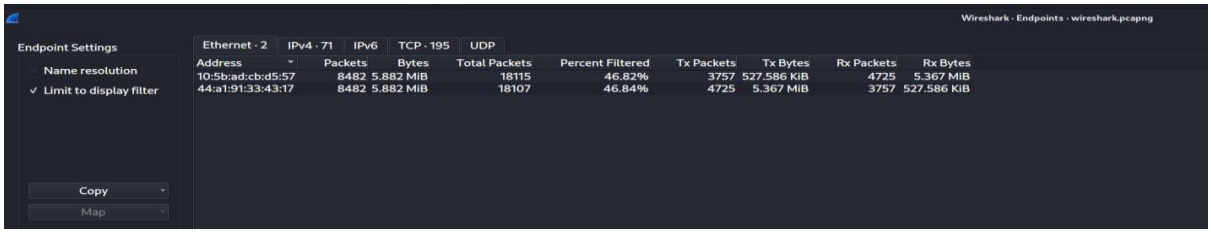
Go to Analyze -> Expert Information and you will see.



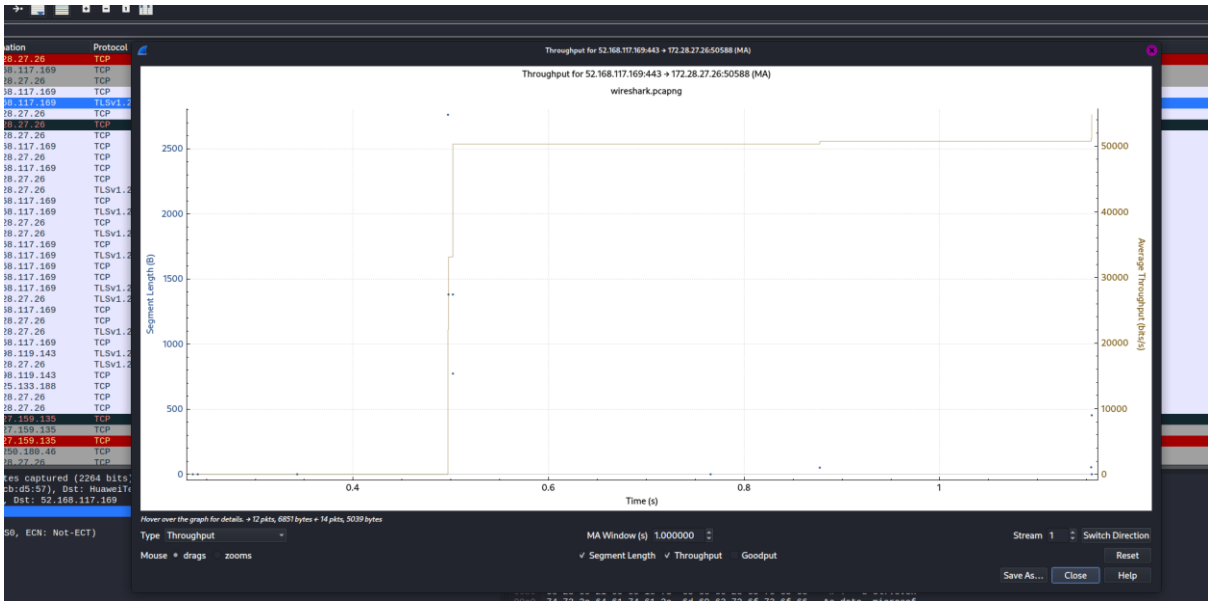
We can also see the statistics of DNS



Endpoints: Analyze endpoint data, noting MAC and IP addresses and the associated protocol.

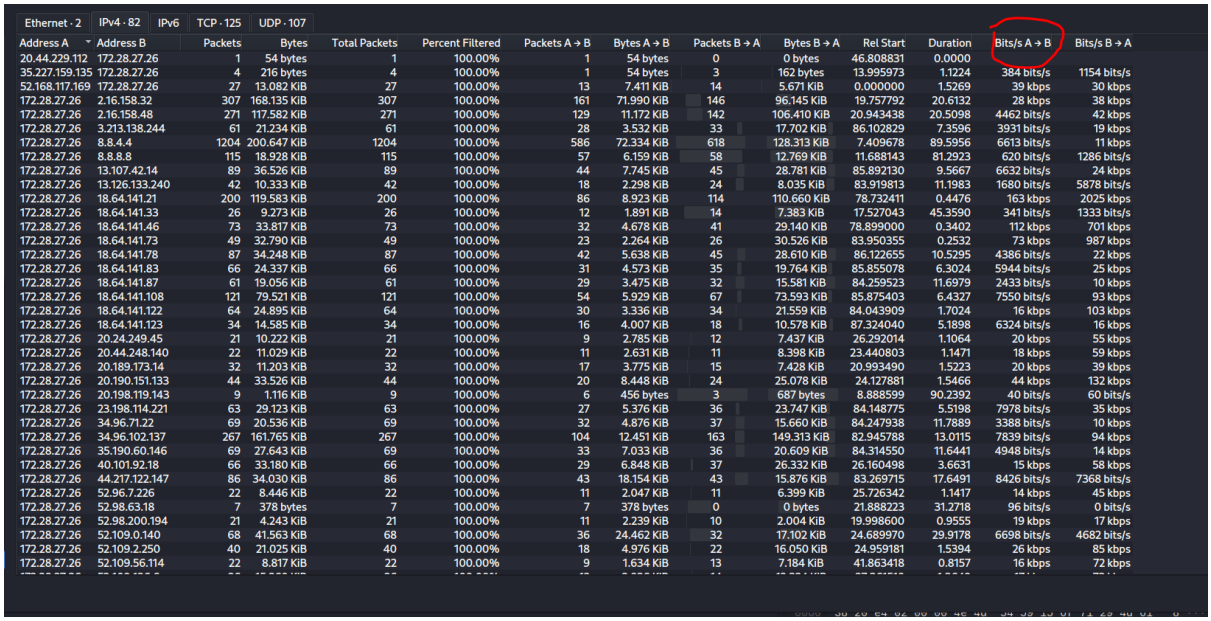


TCP Throughput: Observe the throughput graph for TCP packets.



Bandwidth Consumption: Using the statistics feature, identify the top 3 IP addresses consuming the most bandwidth.

In the "Conversations" window, make sure the "IPv4"



Ethernet · 2 | IPv4 · 82 | IPv6 | TCP · 125 | UDP · 107

Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
20.44.229.112	172.28.27.26	1	54 bytes	1	100.00%	1	54 bytes	0	0 bytes	46.808831	0.0000		
35.227.159.135	172.28.27.26	4	216 bytes	4	100.00%	1	54 bytes	3	162 bytes	13.995973	1.1224	384 bits/s	1154 bits/s
52.168.117.169	172.28.27.26	27	13.082 KiB	27	100.00%	13	7.411 KiB	14	5.671 KiB	0.000000	1.5269	39 kbps	30 kbps
172.28.27.26	2.16.158.32	307	168.135 KiB	307	100.00%	161	71.990 KiB	146	96.145 KiB	19.757792	20.6132	28 kbps	38 kbps
172.28.27.26	2.16.158.48	271	117.582 KiB	271	100.00%	129	11.172 KiB	142	106.410 KiB	20.943438	20.5098	4462 bits/s	42 kbps
172.28.27.26	3.213.138.244	61	21.234 KiB	61	100.00%	28	3.532 KiB	33	17.702 KiB	86.102829	7.3596	3931 bits/s	19 kbps
172.28.27.26	8.8.4.4	1204	200.647 KiB	1204	100.00%	586	72.334 KiB	618	128.313 KiB	7.409678	89.5956	6613 bits/s	11 kbps
172.28.27.26	8.8.8.8	115	18.928 KiB	115	100.00%	57	6.159 KiB	58	12.769 KiB	11.688143	81.2923	620 bits/s	1286 bits/s
172.28.27.26	13.107.42.14	89	36.526 KiB	89	100.00%	44	7.745 KiB	45	28.781 KiB	85.892130	9.5667	6632 bits/s	24 kbps
172.28.27.26	13.126.133.240	42	10.333 KiB	42	100.00%	18	2.298 KiB	24	8.035 KiB	83.919813	11.1983	1680 bits/s	5878 bits/s
172.28.27.26	18.64.141.21	200	119.583 KiB	200	100.00%	86	8.923 KiB	114	110.660 KiB	78.732411	0.4476	163 kbps	2025 kbps
172.28.27.26	18.64.141.33	26	9.273 KiB	26	100.00%	12	1.891 KiB	14	7.383 KiB	17.527043	45.3590	341 bits/s	1333 bits/s
172.28.27.26	18.64.141.46	73	33.817 KiB	73	100.00%	32	4.678 KiB	41	29.140 KiB	78.899000	0.3402	112 kbps	701 kbps
172.28.27.26	18.64.141.73	49	32.790 KiB	49	100.00%	23	2.264 KiB	26	30.526 KiB	83.950355	0.2532	73 kbps	987 kbps
172.28.27.26	18.64.141.78	87	34.248 KiB	87	100.00%	42	5.638 KiB	45	28.610 KiB	86.122655	10.5295	4386 bits/s	22 kbps
172.28.27.26	18.64.141.83	66	24.337 KiB	66	100.00%	31	4.573 KiB	35	19.764 KiB	85.855078	6.3024	5944 bits/s	25 kbps
172.28.27.26	18.64.141.87	61	19.056 KiB	61	100.00%	29	3.475 KiB	32	15.581 KiB	84.259523	11.6979	2433 bits/s	10 kbps
172.28.27.26	18.64.141.108	121	79.521 KiB	121	100.00%	54	5.929 KiB	67	73.593 KiB	85.875403	6.4327	7550 bits/s	93 kbps
172.28.27.26	18.64.141.122	64	24.895 KiB	64	100.00%	30	3.336 KiB	34	21.559 KiB	84.043909	1.7024	16 kbps	103 kbps
172.28.27.26	18.64.141.123	34	14.585 KiB	34	100.00%	16	4.007 KiB	18	10.578 KiB	87.324040	5.1898	6324 bits/s	16 kbps
172.28.27.26	20.24.249.45	21	10.222 KiB	21	100.00%	9	2.785 KiB	12	7.437 KiB	26.292014	1.1064	20 kbps	55 kbps
172.28.27.26	20.44.248.140	22	11.029 KiB	22	100.00%	11	2.631 KiB	11	8.398 KiB	23.440803	1.1471	18 kbps	59 kbps
172.28.27.26	20.189.173.14	32	11.203 KiB	32	100.00%	17	3.775 KiB	15	7.428 KiB	20.993490	1.5223	20 kbps	39 kbps
172.28.27.26	20.190.151.133	44	33.526 KiB	44	100.00%	20	8.448 KiB	24	25.078 KiB	24.127881	1.5466	44 kbps	132 kbps
172.28.27.26	20.198.119.143	9	1.116 KiB	9	100.00%	6	456 bytes	3	687 bytes	8.888599	90.2392	40 bits/s	60 bits/s
172.28.27.26	23.198.114.221	63	29.123 KiB	63	100.00%	27	5.376 KiB	36	23.747 KiB	84.148775	5.5198	7978 bits/s	35 kbps
172.28.27.26	34.96.71.22	69	20.536 KiB	69	100.00%	32	4.876 KiB	37	15.660 KiB	84.247938	11.7889	3388 bits/s	10 kbps
172.28.27.26	34.96.102.137	267	161.765 KiB	267	100.00%	104	12.451 KiB	163	149.313 KiB	82.945788	13.0115	7839 bits/s	94 kbps
172.28.27.26	35.190.60.146	69	27.643 KiB	69	100.00%	33	7.033 KiB	36	20.609 KiB	84.314550	11.6441	4948 bits/s	14 kbps
172.28.27.26	40.101.92.18	66	33.180 KiB	66	100.00%	29	6.848 KiB	37	26.332 KiB	26.160498	3.6631	15 kbps	58 kbps
172.28.27.26	44.217.122.147	86	34.030 KiB	86	100.00%	43	18.154 KiB	43	15.876 KiB	83.269715	17.6491	8426 bits/s	7368 bits/s
172.28.27.26	52.96.7.226	22	8.446 KiB	22	100.00%	11	2.047 KiB	11	6.399 KiB	25.726342	1.1417	14 kbps	45 kbps
172.28.27.26	52.98.63.18	7	378 bytes	7	100.00%	7	378 bytes	0	0 bytes	21.888223	31.2718	96 bits/s	0 bits/s
172.28.27.26	52.98.200.194	21	4.243 KiB	21	100.00%	11	2.239 KiB	10	2.004 KiB	19.998600	0.9555	19 kbps	17 kbps
172.28.27.26	52.109.0.140	68	41.563 KiB	68	100.00%	36	24.462 KiB	32	17.102 KiB	24.689970	29.9178	6698 bits/s	4682 bits/s
172.28.27.26	52.109.2.250	40	21.025 KiB	40	100.00%	18	4.976 KiB	22	16.050 KiB	24.959181	1.5394	26 kbps	85 kbps
172.28.27.26	52.109.56.114	22	8.817 KiB	22	100.00%	9	1.634 KiB	13	7.184 KiB	41.863418	0.8157	16 kbps	72 kbps

Conclusion:

In conclusion, this lab allowed us to gain practical experience in network packet analysis using Wireshark. We successfully applied various filtering techniques, extracted data from HTTP traffic, and identified potential firewall rules. The advanced analysis provided valuable insights into network endpoints and bandwidth consumption. Overall, this exercise enhanced our understanding of network security and monitoring.