

Task - 5

Network Traffic Analysis Report – Wireshark

Title: Capture and Analysis of Network Traffic using Wireshark

Date: 11/08/2025

Name: Abinash I

Tool Used: Wireshark v4.x

System Used: Linux

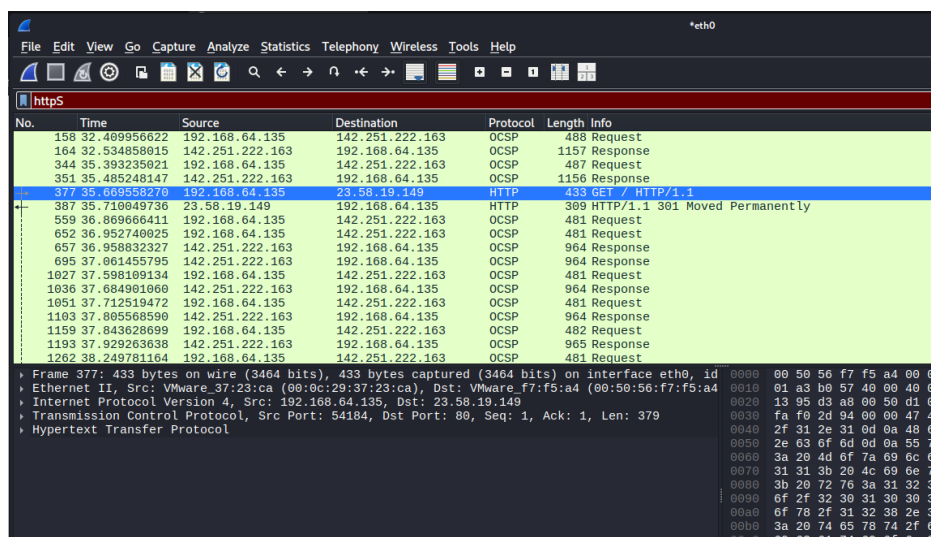
Objective

To capture live network traffic and identify common internet protocols such as HTTP, DNS, and TCP using Wireshark.

Procedure

1. Installed **Wireshark** and selected the active network interface (Wi-Fi).
2. Started a live packet capture for about 1 minute.
3. Generated traffic by:
 - o Visiting a website in a browser.
 - o Performing a ping command to an external server.
4. Applied protocol filters in Wireshark:
 - o http → to view HTTP requests and responses.
 - o dns → to see DNS queries and responses.
 - o tcp → to observe TCP handshake and communication.
5. Took screenshots for each filtered protocol.
6. Saved the packet capture as **network_capture.pcap**.

HTTP filtered packets



No.	Time	Source	Destination	Protocol	Length	Info
159	32.469956622	192.168.64.135	142.251.222.163	OCSP	488	Request
164	32.534858015	142.251.222.163	192.168.64.135	OCSP	1157	Response
344	35.393235021	192.168.64.135	142.251.222.163	OCSP	487	Request
351	35.485248147	142.251.222.163	192.168.64.135	OCSP	1156	Response
377	35.669558270	192.168.64.135	23.58.19.149	HTTP	433	GET / HTTP/1.1
387	35.710049736	23.58.19.149	192.168.64.135	HTTP	309	HTTP/1.1 301 Moved Permanently
559	36.869666411	192.168.64.135	142.251.222.163	OCSP	481	Request
652	36.952740825	192.168.64.135	142.251.222.163	OCSP	481	Request
657	36.958832327	142.251.222.163	192.168.64.135	OCSP	964	Response
695	37.061455795	142.251.222.163	192.168.64.135	OCSP	964	Response
1027	37.598109134	192.168.64.135	142.251.222.163	OCSP	481	Request
1036	37.684901060	142.251.222.163	192.168.64.135	OCSP	964	Response
1051	37.712519472	192.168.64.135	142.251.222.163	OCSP	481	Request
1103	37.805568590	142.251.222.163	192.168.64.135	OCSP	964	Response
1159	37.843620699	192.168.64.135	142.251.222.163	OCSP	482	Request
1193	37.929263638	142.251.222.163	192.168.64.135	OCSP	965	Response
1262	38.249781164	192.168.64.135	142.251.222.163	OCSP	481	Request

Frame 377: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface eth0, id 0000 00 50 56 f7 f5 a4 00 00 01 a3 b0 57 40 00 40 00 13 95 d3 a8 00 50 d1 00 fa f0 2d 94 00 00 47 40 2f 31 2e 31 0d 0a 48 60 2e 63 6f 6d 0d 0a 55 70 3a 20 4d 6f 7a 69 6c 60 31 31 3b 20 4c 69 6e 70 3b 20 72 76 3a 31 32 30 6f 2f 32 30 31 30 30 30 6f 78 2f 31 32 38 2e 30 3a 20 74 65 78 74 2f 60 69 63 61 74 69 6f 60 20

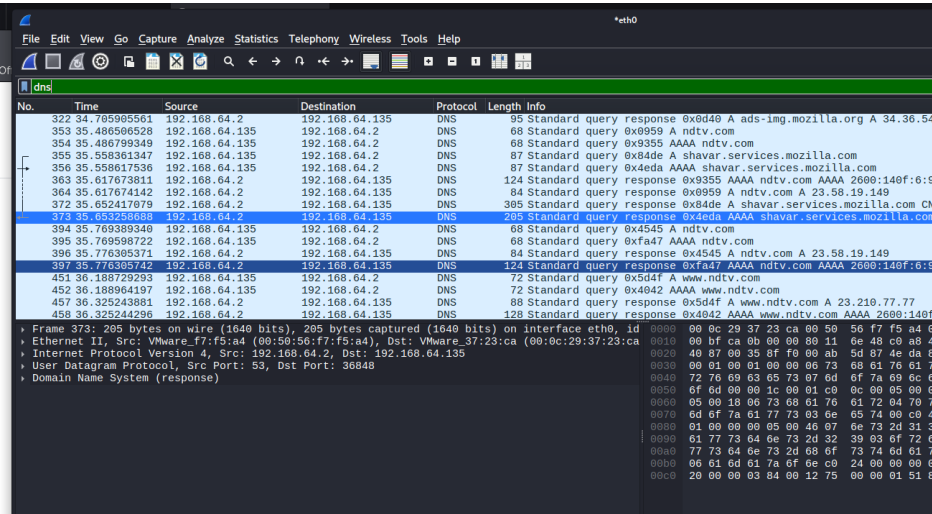
Ethernet II, Src: VMware_37:23:ca (00:0c:29:37:23:ca), Dst: VMware_f7:f5:a4 (00:50:56:f7:f5:a4)

Internet Protocol Version 4, Src: 192.168.64.135, Dst: 23.58.19.149

Transmission Control Protocol, Src Port: 54184, Dst Port: 80, Seq: 1, Ack: 1, Len: 379

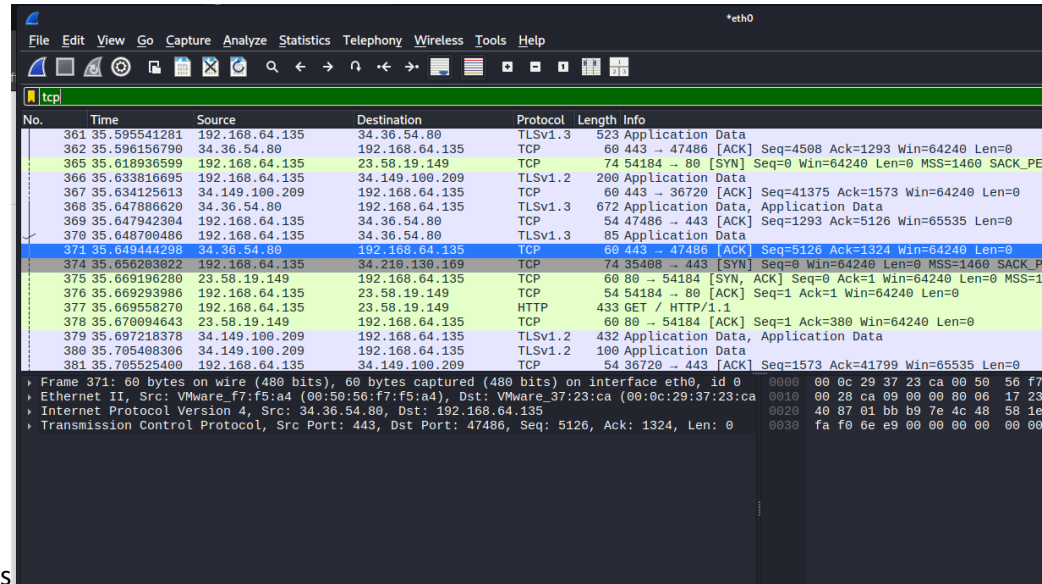
Hypertext Transfer Protocol

DNS filtered packets



No.	Time	Source	Destination	Protocol	Length	Info
322	34.765995591	192.168.64.2	192.168.64.135	DNS	95	Standard query response 0x8d40 A ads-img.mozilla.org A 34.36.54.80
353	35.486560528	192.168.64.135	192.168.64.2	DNS	68	Standard query 0x9959 A ndtv.com
354	35.486799349	192.168.64.135	192.168.64.2	DNS	68	Standard query 0x9355 AAAA ndtv.com
355	35.558361347	192.168.64.135	192.168.64.2	DNS	87	Standard query 0x84de A shavar.services.mozilla.com
356	35.558617536	192.168.64.135	192.168.64.2	DNS	87	Standard query 0x4eda AAAA shavar.services.mozilla.com
363	35.617673811	192.168.64.2	192.168.64.135	DNS	124	Standard query response 0x9355 AAAA ndtv.com AAAA 2680:140f:6:9:3::
364	35.617674142	192.168.64.2	192.168.64.135	DNS	84	Standard query response 0x9959 A ndtv.com A 23.58.19.149
372	35.652417079	192.168.64.2	192.168.64.135	DNS	305	Standard query response 0x84de A shavar.services.mozilla.com CNAME 2680:140f:6:9:3::
373	35.652420503	192.168.64.2	192.168.64.135	DNS	258	Standard query response 0x4eda AAAA shavar.services.mozilla.com
394	35.769389340	192.168.64.135	192.168.64.2	DNS	68	Standard query 0x4545 A ndtv.com
395	35.769598722	192.168.64.135	192.168.64.2	DNS	68	Standard query 0xfa47 AAAA ndtv.com
396	35.776385371	192.168.64.2	192.168.64.135	DNS	84	Standard query response 0x4545 A ndtv.com A 23.58.19.149
397	35.776385742	192.168.64.2	192.168.64.135	DNS	124	Standard query response 0x4eda AAAA ndtv.com AAAA 2680:140f:6:9:3::
451	36.188729293	192.168.64.135	192.168.64.2	DNS	72	Standard query 0x5d4f A www.ndtv.com
452	36.188964197	192.168.64.135	192.168.64.2	DNS	72	Standard query 0x4042 AAAA www.ndtv.com
452	36.325243881	192.168.64.2	192.168.64.135	DNS	88	Standard query response 0x5d4f A www.ndtv.com A 23.210.77.77
459	36.325244296	192.168.64.2	192.168.64.135	DNS	128	Standard query response 0x4042 AAAA www.ndtv.com AAAA 2680:140f:6:9:3::

TCP filtered packets



No.	Time	Source	Destination	Protocol	Length	Info
361	35.595541281	192.168.64.135	34.36.54.80	TLSv1.3	523	Application Data
362	35.596156790	34.36.54.80	192.168.64.135	TCP	60	443 → 47486 [ACK] Seq=4508 Ack=1293 Win=64240 Len=0
365	35.618936599	192.168.64.135	23.58.19.149	TCP	74	54184 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
366	35.633816695	192.168.64.135	34.149.100.209	TLSv1.2	200	Application Data
367	35.634125613	34.149.100.209	192.168.64.135	TCP	60	443 → 36720 [ACK] Seq=41375 Ack=1573 Win=64240 Len=0
368	35.647886620	34.36.54.80	192.168.64.135	TLSv1.3	672	Application Data, Application Data
369	35.647942384	192.168.64.135	34.36.54.80	TCP	54	47486 → 443 [ACK] Seq=1293 Ack=5126 Win=65535 Len=0
370	35.648700486	192.168.64.135	34.36.54.80	TLSv1.3	85	Application Data
371	35.649444298	34.36.54.80	192.168.64.135	TCP	60	443 → 47486 [ACK] Seq=5126 Ack=1324 Win=64240 Len=0
374	35.659009022	192.168.64.135	34.210.130.109	TCP	74	35408 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
375	35.669196280	23.58.19.149	192.168.64.135	TCP	60	80 → 54184 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
376	35.669293986	192.168.64.135	23.58.19.149	TCP	54	54184 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
377	35.669558270	192.168.64.135	23.58.19.149	HTTP	433	GET / HTTP/1.1
378	35.670946443	23.58.19.149	192.168.64.135	TCP	60	80 → 54184 [ACK] Seq=1 Ack=380 Win=64240 Len=0
379	35.697218378	34.149.100.209	192.168.64.135	TLSv1.2	432	Application Data, Application Data
380	35.705408306	34.149.100.209	192.168.64.135	TLSv1.2	100	Application Data
381	35.705525400	192.168.64.135	34.149.100.209	TCP	54	36720 → 443 [ACK] Seq=1573 Ack=41799 Win=65535 Len=0

Conclusion

The network capture confirmed the presence of HTTP, DNS, and TCP traffic. Each protocol serves a distinct role in enabling web browsing:

- **DNS** translates domain names into IP addresses.
- **TCP** ensures reliable data delivery.
- **HTTP** enables content retrieval from web servers.