

Task 5: Capture and Analyze Network Traffic Using Wireshark

Objective

Capture live network packets on the host system, identify at least 3 basic protocols and traffic types, and summarize findings with supporting packet screenshots.

Tools Used

- **Wireshark** (free, open-source network protocol analyzer) on Kali Linux.

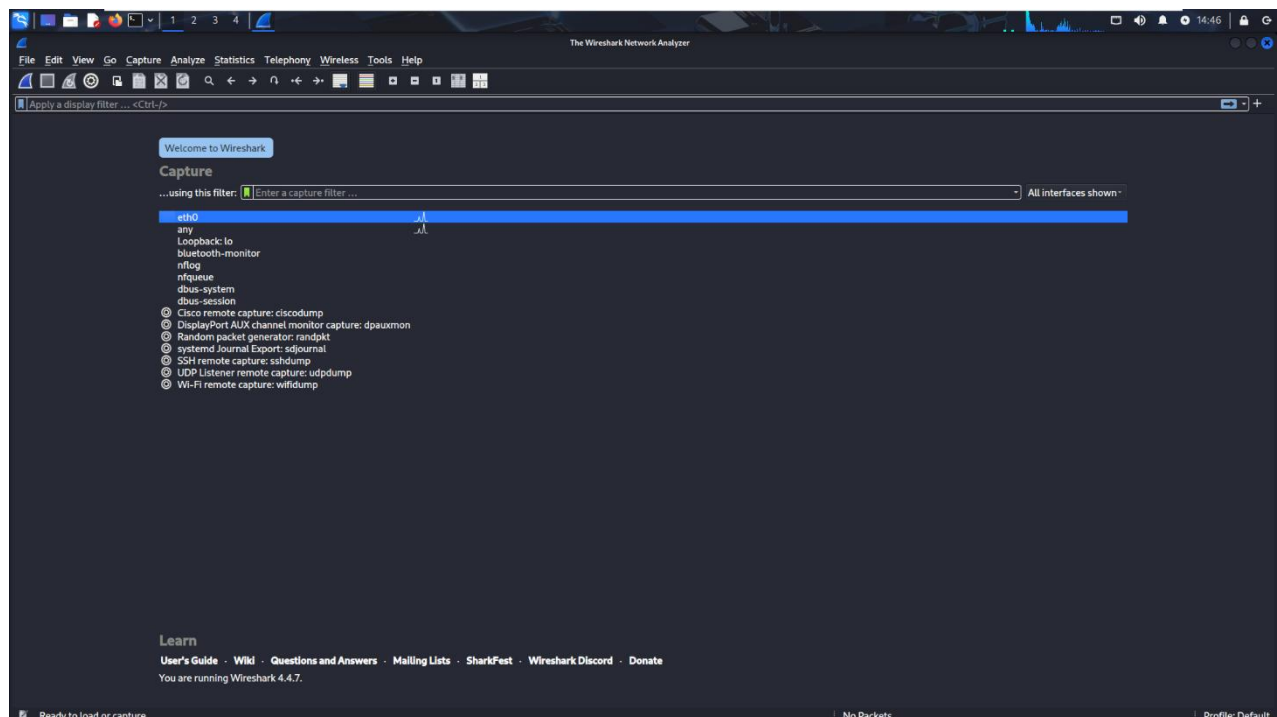
Steps Perform

1. Installing and Launching Wireshark

Wireshark was launched in the Kali Linux VMware environment. The active Ethernet interface (eth0) was selected for capturing.

2. Starting the Packet Capture

The capture commenced on the selected interface, eth0. During capturing, various online activities were performed (web browsing, DNS resolutions, etc.) to generate traffic.



3. Filtering Captured Packets by Protocol

To analyze results, Wireshark display filters (http, tcp, dns) were applied and packets were scrutinized for details and headers.

The image shows the Wireshark network traffic capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main display area is divided into three panes: the top pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info; the middle pane shows the details of the selected packet (Frame 1); and the bottom pane shows the raw packet data in hexadecimal and ASCII.

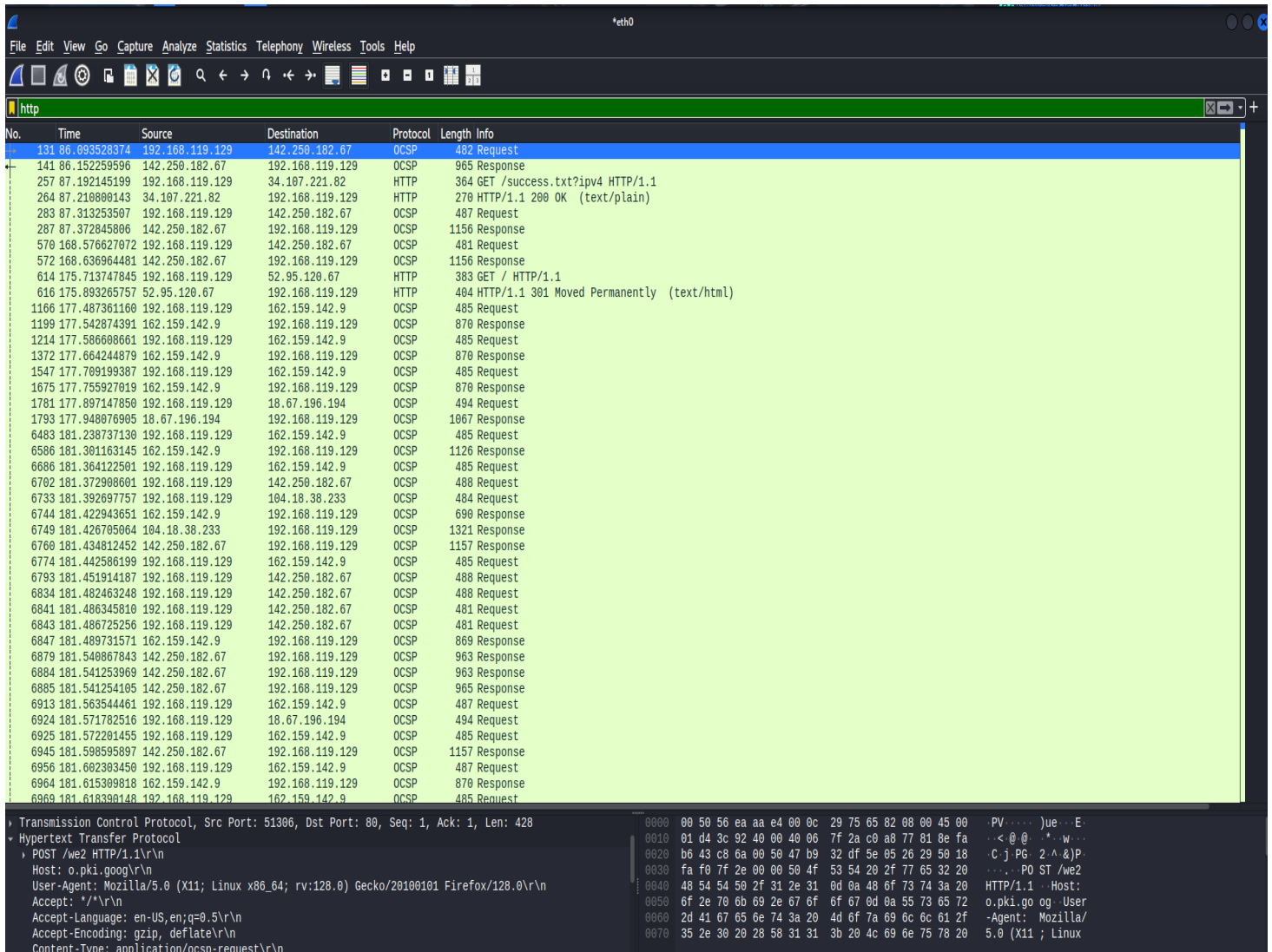
No.	Time	Source	Destination	Protocol	Length	Info
9228	254.429064350	192.168.119.129	162.159.142.9	TCP	54	[TCP Keep-Alive] 36178 → 80 [ACK] Seq=866 Ack=1633 Win=62608 Len=0
9229	254.429088418	192.168.119.129	18.67.196.194	TCP	54	[TCP Keep-Alive] 36884 → 80 [ACK] Seq=1320 Ack=3018 Win=61223 Len=0
9230	254.429150442	18.239.153.81	192.168.119.129	TCP	60	[TCP Keep-Alive ACK] 443 → 32876 [ACK] Seq=6852 Ack=1864 Win=64240 Len=0
9231	254.429151096	18.239.150.190	192.168.119.129	TCP	60	[TCP Keep-Alive ACK] 80 → 51234 [ACK] Seq=924 Ack=441 Win=64240 Len=0
9232	254.429151128	18.239.150.190	192.168.119.129	TCP	60	[TCP Keep-Alive ACK] 80 → 51246 [ACK] Seq=924 Ack=441 Win=64240 Len=0
9233	254.429301499	18.67.196.194	192.168.119.129	TCP	60	[TCP Keep-Alive ACK] 80 → 36902 [ACK] Seq=820 Ack=441 Win=64240 Len=0
9234	254.429301600	162.159.142.9	192.168.119.129	TCP	60	[TCP Keep-Alive ACK] 80 → 36170 [ACK] Seq=3108 Ack=1725 Win=64240 Len=0
9235	254.429301656	162.159.142.9	192.168.119.129	TCP	60	[TCP Keep-Alive ACK] 80 → 36200 [ACK] Seq=1611 Ack=863 Win=64240 Len=0
9236	254.429301712	162.159.142.9	192.168.119.129	TCP	60	[TCP Keep-Alive ACK] 80 → 36178 [ACK] Seq=1633 Ack=867 Win=64240 Len=0
9237	254.429301754	18.67.196.194	192.168.119.129	TCP	60	[TCP Keep-Alive ACK] 80 → 36884 [ACK] Seq=3018 Ack=1321 Win=64240 Len=0
9238	254.684909615	192.168.119.129	162.159.142.9	TCP	54	[TCP Keep-Alive] 36168 → 80 [ACK] Seq=4310 Ack=8492 Win=62832 Len=0
9239	254.685188754	192.168.119.129	67.220.228.203	TCP	54	[TCP Keep-Alive] 32842 → 443 [ACK] Seq=8965 Ack=23995 Win=65535 Len=0
9240	254.685194346	192.168.119.129	104.18.20.226	TCP	54	[TCP Keep-Alive] 35154 → 80 [ACK] Seq=892 Ack=3797 Win=60444 Len=0
9241	254.685376300	162.159.142.9	192.168.119.129	TCP	60	[TCP Keep-Alive ACK] 80 → 36168 [ACK] Seq=8492 Ack=4311 Win=64240 Len=0
9242	254.685376709	67.220.228.203	192.168.119.129	TCP	60	[TCP Keep-Alive ACK] 443 → 32842 [ACK] Seq=23995 Ack=8966 Win=64240 Len=0
9243	254.685376759	104.18.20.226	192.168.119.129	TCP	60	[TCP Keep-Alive ACK] 80 → 35154 [ACK] Seq=3797 Ack=893 Win=64240 Len=0
9244	254.940933142	192.168.119.129	67.220.228.203	TCP	54	[TCP Keep-Alive] 32856 → 443 [ACK] Seq=1959 Ack=1322 Win=63996 Len=0
9245	254.941239872	67.220.228.203	192.168.119.129	TCP	60	[TCP Keep-Alive ACK] 443 → 32856 [ACK] Seq=1322 Ack=1960 Win=64240 Len=0
9246	256.398883428	192.168.119.129	34.107.243.93	TLSv1.3	93	Application Data
9247	256.400239339	34.107.243.93	192.168.119.129	TCP	60	443 → 44500 [ACK] Seq=3808 Ack=978 Win=64240 Len=0
9248	256.400416577	192.168.119.129	34.107.243.93	TLSv1.3	78	Application Data
9249	256.400545728	192.168.119.129	34.107.243.93	TCP	54	44500 → 443 [FIN, ACK] Seq=1002 Ack=3808 Win=65535 Len=0
9250	256.400805920	34.107.243.93	192.168.119.129	TCP	60	443 → 44500 [ACK] Seq=3808 Ack=1002 Win=64240 Len=0
9251	256.401159841	34.107.243.93	192.168.119.129	TCP	60	443 → 44500 [ACK] Seq=3808 Ack=1003 Win=64239 Len=0
9252	256.421337264	34.107.243.93	192.168.119.129	TCP	60	443 → 44500 [FIN, PSH, ACK] Seq=3808 Ack=1003 Win=64239 Len=0
9253	256.421416904	192.168.119.129	34.107.243.93	TCP	54	44500 → 443 [ACK] Seq=1003 Ack=3809 Win=7464 Len=0
9254	256.477112279	192.168.119.129	3.254.239.146	TCP	54	[TCP Keep-Alive] 40454 → 443 [ACK] Seq=80389 Ack=8427 Win=65535 Len=0
9255	256.477900270	3.254.239.146	192.168.119.129	TCP	60	[TCP Keep-Alive ACK] 443 → 40454 [ACK] Seq=8427 Ack=80390 Win=64240 Len=0
9256	256.610713242	3.254.239.146	192.168.119.129	TLSv1.3	78	Application Data
9257	256.611307196	192.168.119.129	3.254.239.146	TLSv1.3	78	Application Data
9258	256.611448323	192.168.119.129	3.254.239.146	TCP	54	40460 → 443 [FIN, ACK] Seq=6069 Ack=7837 Win=65535 Len=0
9259	256.611678304	3.254.239.146	192.168.119.129	TCP	60	443 → 40460 [ACK] Seq=7837 Ack=6069 Win=64240 Len=0
9260	256.611678573	3.254.239.146	192.168.119.129	TCP	60	443 → 40460 [ACK] Seq=7837 Ack=6070 Win=64239 Len=0
9261	257.076383065	18.183.0.120	192.168.119.129	TLSv1.3	117	Application Data, Application Data
9262	257.076793581	192.168.119.129	18.183.0.120	TLSv1.3	93	Application Data
9263	257.077063606	18.183.0.120	192.168.119.129	TCP	60	443 → 58740 [ACK] Seq=3046 Ack=1351 Win=64240 Len=0
9264	257.077071422	192.168.119.129	18.183.0.120	TLSv1.3	78	Application Data
9265	257.077147440	192.168.119.129	18.183.0.120	TCP	54	58740 → 443 [FIN, ACK] Seq=1375 Ack=3046 Win=65535 Len=0
9266	257.077520653	18.183.0.120	192.168.119.129	TCP	60	443 → 58740 [ACK] Seq=3046 Ack=1375 Win=64240 Len=0
9267	257.077520807	18.183.0.120	192.168.119.129	TCP	60	443 → 58740 [ACK] Seq=3046 Ack=1376 Win=64239 Len=0
9268	257.757023185	192.168.119.129	142.250.182.67	TCP	54	[TCP Keep-Alive] 51320 → 80 [ACK] Seq=3023 Ack=7526 Win=64240 Len=0

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface eth0, id 0
Ethernet II, Src: VMware_75:65:82 (00:0c:29:75:65:82), Dst: IPv6mcast_02 (33:33:00:00:00:02)
Internet Protocol Version 6, Src: fe80::20c:29ff:fe75:6582, Dst: ff02::2
Internet Control Message Protocol v6

0000 33 33 00 00 00 02 00 0c 29 75 65 82 00 dd 60 0c 33)ue...
0010 4e 4b 00 00 3a ff fe 00 00 00 00 00 00 02 0c NK... ..
0020 29 ff fe 75 65 82 ff 02 00 00 00 00 00 00 00) ue...
0030 00 00 00 00 00 02 85 00 ed 33 00 00 00 00 3....

HTTP

- Multiple HTTP packets with request lines (GET, POST) and HTTP response codes.
- Headers such as Host, User-Agent, Content-Type visible in detail.



No.	Time	Source	Destination	Protocol	Length	Info
131	86.093528374	192.168.119.129	142.250.182.67	OCSP	482	Request
141	86.152259596	142.250.182.67	192.168.119.129	OCSP	965	Response
257	87.192145199	192.168.119.129	34.107.221.82	HTTP	364	GET /success.txt?ipv4 HTTP/1.1
264	87.210800143	34.107.221.82	192.168.119.129	HTTP	270	HTTP/1.1 200 OK (text/plain)
283	87.313253507	192.168.119.129	142.250.182.67	OCSP	487	Request
287	87.372845006	142.250.182.67	192.168.119.129	OCSP	1156	Response
570	168.576627072	192.168.119.129	142.250.182.67	OCSP	481	Request
572	168.636964481	142.250.182.67	192.168.119.129	OCSP	1156	Response
614	175.713747845	192.168.119.129	52.95.120.67	HTTP	383	GET / HTTP/1.1
616	175.893265757	52.95.120.67	192.168.119.129	HTTP	404	HTTP/1.1 301 Moved Permanently (text/html)
1166	177.487361100	192.168.119.129	162.159.142.9	OCSP	485	Request
1199	177.542874391	162.159.142.9	192.168.119.129	OCSP	870	Response
1214	177.586608661	192.168.119.129	162.159.142.9	OCSP	485	Request
1372	177.664244879	162.159.142.9	192.168.119.129	OCSP	870	Response
1547	177.709199387	192.168.119.129	162.159.142.9	OCSP	485	Request
1675	177.755927019	162.159.142.9	192.168.119.129	OCSP	870	Response
1781	177.897147850	192.168.119.129	18.67.196.194	OCSP	494	Request
1793	177.948076905	18.67.196.194	192.168.119.129	OCSP	1067	Response
6483	181.238737130	192.168.119.129	162.159.142.9	OCSP	485	Request
6586	181.301163145	162.159.142.9	192.168.119.129	OCSP	1126	Response
6686	181.364122501	192.168.119.129	162.159.142.9	OCSP	485	Request
6702	181.372908601	192.168.119.129	142.250.182.67	OCSP	488	Request
6733	181.392697757	192.168.119.129	104.18.38.233	OCSP	484	Request
6744	181.422943651	162.159.142.9	192.168.119.129	OCSP	690	Response
6749	181.426705064	104.18.38.233	192.168.119.129	OCSP	1321	Response
6760	181.434812452	142.250.182.67	192.168.119.129	OCSP	1157	Response
6774	181.442586199	192.168.119.129	162.159.142.9	OCSP	485	Request
6793	181.451914187	192.168.119.129	142.250.182.67	OCSP	488	Request
6834	181.482463248	192.168.119.129	142.250.182.67	OCSP	488	Request
6841	181.486345810	192.168.119.129	142.250.182.67	OCSP	481	Request
6843	181.486725256	192.168.119.129	142.250.182.67	OCSP	481	Request
6847	181.489731571	162.159.142.9	192.168.119.129	OCSP	869	Response
6879	181.540867843	142.250.182.67	192.168.119.129	OCSP	963	Response
6884	181.541253969	142.250.182.67	192.168.119.129	OCSP	963	Response
6885	181.541254105	142.250.182.67	192.168.119.129	OCSP	965	Response
6913	181.563544461	192.168.119.129	162.159.142.9	OCSP	487	Request
6924	181.571782516	192.168.119.129	18.67.196.194	OCSP	494	Request
6925	181.572201455	192.168.119.129	162.159.142.9	OCSP	485	Request
6945	181.598595897	142.250.182.67	192.168.119.129	OCSP	1157	Response
6956	181.602303450	192.168.119.129	162.159.142.9	OCSP	487	Request
6964	181.615309818	162.159.142.9	192.168.119.129	OCSP	870	Response
6969	181.618390148	192.168.119.129	162.159.142.9	OCSP	485	Request

Transmission Control Protocol, Src Port: 51306, Dst Port: 80, Seq: 1, Ack: 1, Len: 428	
Hypertext Transfer Protocol	
POST /we2 HTTP/1.1\r\n	
Host: o.pki.goog\r\n	
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0\r\n	
Accept: */*\r\n	
Accept-Language: en-US,en;q=0.5\r\n	
Accept-Encoding: gzip, deflate\r\n	
Content-Type: application/ocsp-request\r\n	

0000	00 50 56 ea aa e4 00 0c 29 75 65 82 08 00 45 00	.PV....jue...E
0010	01 d4 3c 92 40 00 40 06 7f 2a c0 a8 77 81 8e fa	..<@. *.w...
0020	b6 43 c8 6a 00 50 47 b9 32 df 5e 05 26 29 50 18	.C j PG 2 ^ &) P
0030	fa f0 7f 2e 00 00 50 4f 53 54 20 2f 77 65 32 20PO ST /we2
0040	48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20	HTTP/1.1 .Host:
0050	6f 2e 70 6b 69 2e 67 6f 6f 67 8d 0a 55 73 65 72	o.pki.go og .User
0060	2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f	-Agent: Mozilla/
0070	35 2e 30 20 28 58 31 31 3b 20 4c 69 6e 75 78 20	5.0 (X11 ; Linux

TCP/TLS

- TCP handshake steps observed (SYN, SYN-ACK, ACK), followed by encrypted data (Application Data over TLSv1.3).
- Evident secure communications between local and remote hosts.^{[4][5]}

[illegible]

DNS

- Outgoing DNS queries and incoming responses were observed for multiple domain names.
- Evidence of A and CNAME record queries and responses.

[illegible]

Packet Details

- **HTTP:** The frame shows HTTP/1.1 headers, including a POST request to a web server and relevant HTTP headers.
- **TCP:** Shows sequence of TCP handshake with SYN, ACK flags, and subsequent application data over the session.
- **DNS:** DNS response includes mapping of domain names to IP addresses with relevant transaction IDs.

Conclusion:

Wireshark proved to be an essential tool for capturing and analyzing network traffic at a granular level, offering deep insights into network communications and protocols. By performing this task, hands-on skills were developed in using filters, interpreting protocol-specific packets (HTTP, TCP, and DNS), and identifying key elements within real-time traffic. The exercise built a strong foundation for protocol awareness and network troubleshooting, demonstrating how effective packet analysis can uncover the structure and status of network conversations. This foundational experience with Wireshark enhances both analytical and investigative abilities for any cybersecurity or network management role.