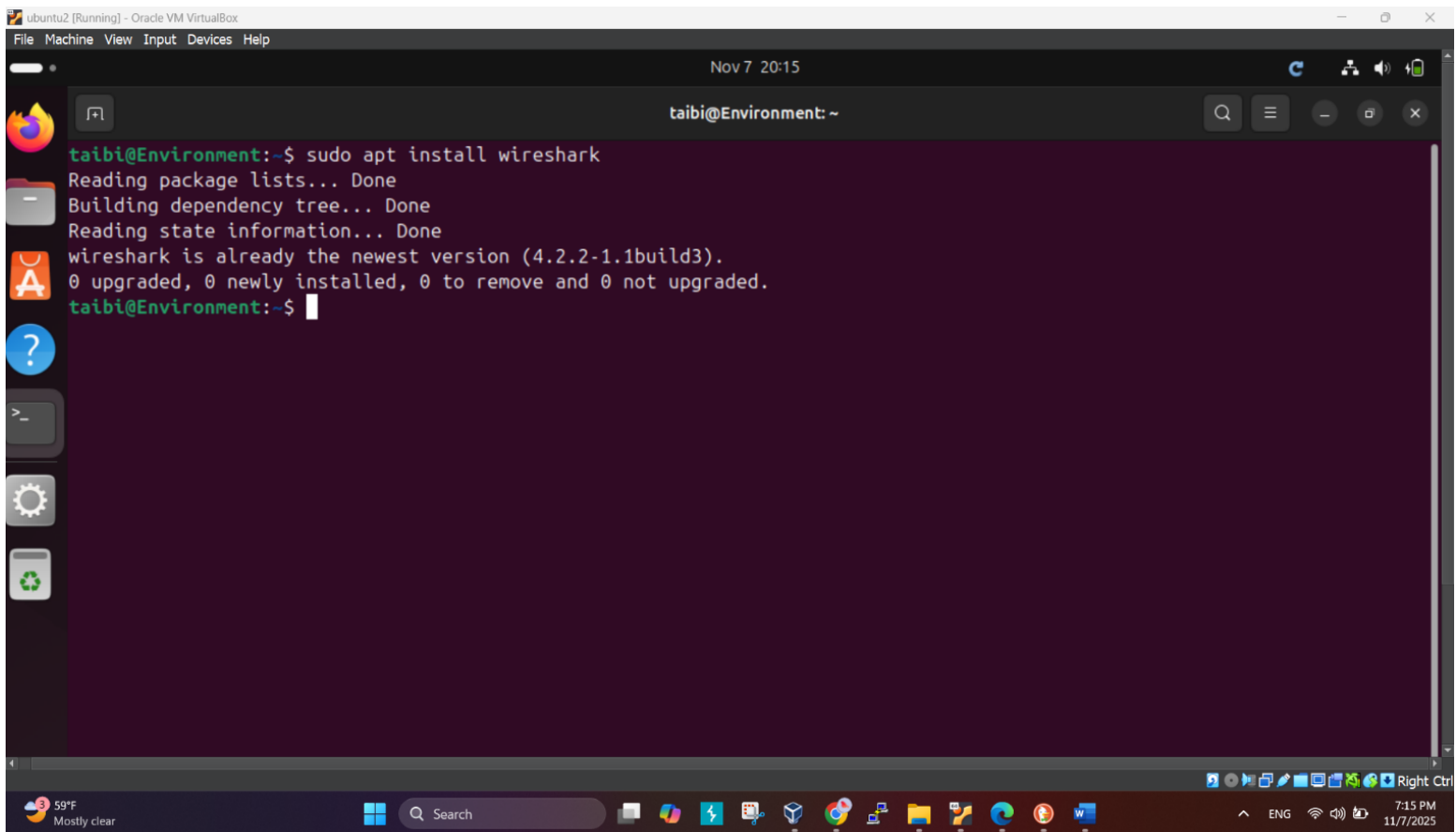
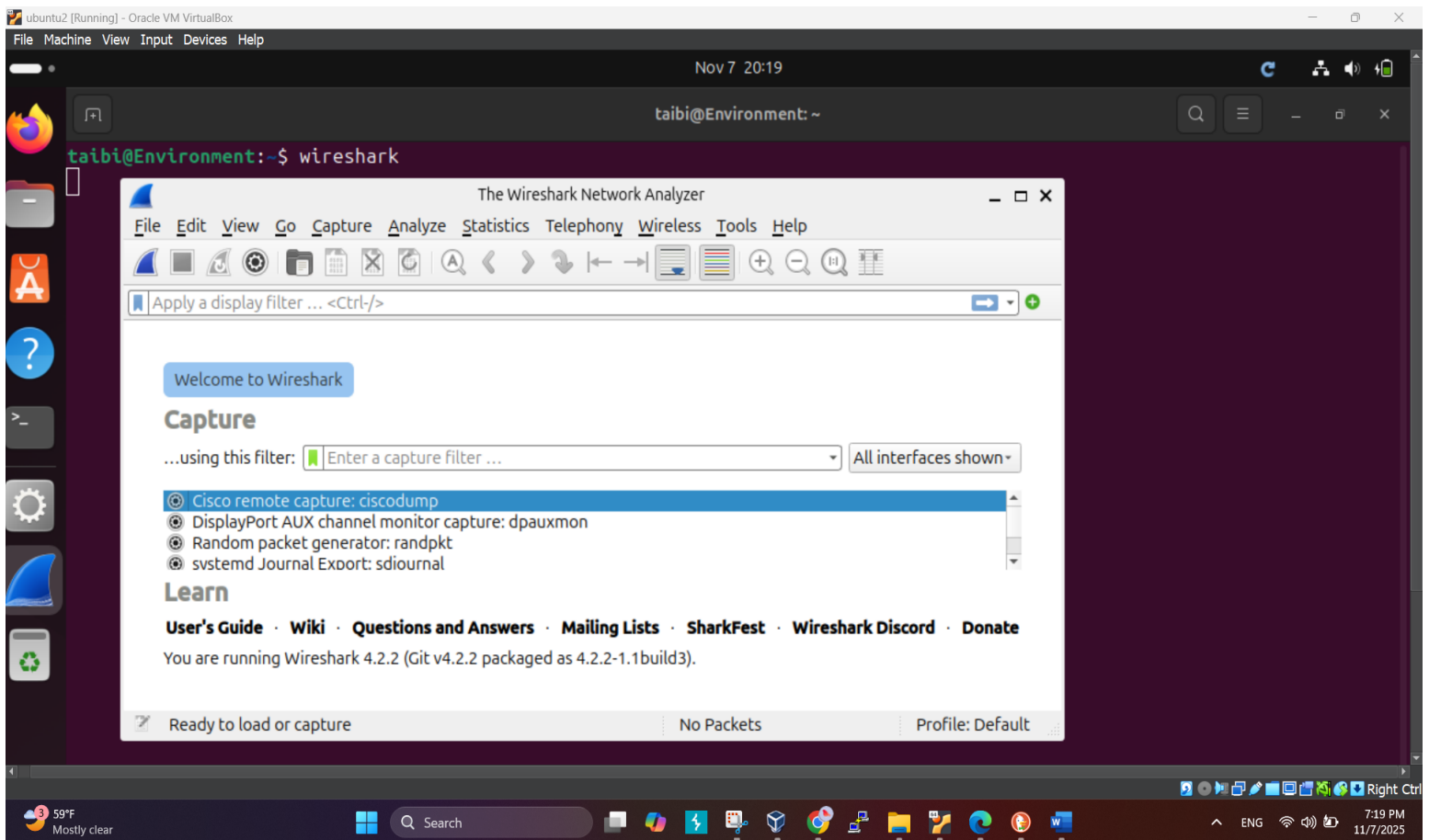


installing wireshark tool



Opening the wireshark



Capturing the traffic:

Captured Dns Traffic analyze To observe the resolution of Domain name to it's IP address.

The screenshot shows a Wireshark capture of network traffic on the interface *enp0s3. The filter bar is set to 'dns'. The packet list shows several DNS queries and responses. The selected packet is a DNS query (Standard query) from 10.241.30.246 to 10.241.30.208, asking for the IP address of mozilla.cloudflare-dns.com. The packet details pane shows the Ethernet II header, Internet Protocol Version 4 header, and the Domain Name System (query) section. The packet bytes pane shows the raw data of the DNS query.

No.	Time	Source	Destination	Protocol	Length	Info
06493538	10.241.30.246	10.241.30.208	DNS	86	Standard query 0x66c3 A mozilla.cloudflare-dns.com	
07399571	10.241.30.246	10.241.30.208	DNS	86	Standard query 0x6599 AAAA mozilla.cloudflare-dns.com	
09307470	10.241.30.208	10.241.30.246	DNS	118	Standard query response 0x66c3 A mozilla.cloudflare-dns.com A...	
071277450	10.241.30.208	10.241.30.246	DNS	142	Standard query response 0x6599 AAAA mozilla.cloudflare-dns.co...	
09437290	10.241.30.246	10.241.30.208	DNS	89	Standard query 0x449f AAAA connectivity-check.ubuntu.com	
09497716	10.241.30.208	10.241.30.246	DNS	425	Standard query response 0x449f AAAA connectivity-check.ubuntu...	
0720549	10.241.30.246	10.241.30.208	DNS	89	Standard query 0x1adf A connectivity-check.ubuntu.com	
071000998	10.241.30.208	10.241.30.246	DNS	281	Standard query response 0x1adf A connectivity-check.ubuntu.co...	
068677871	10.241.30.246	10.241.30.208	DNS	76	Standard query 0xa4df A api.snapcraft.io	
069299899	10.241.30.246	10.241.30.208	DNS	76	Standard query 0xb932 AAAA api.snapcraft.io	
023623179	10.241.30.208	10.241.30.246	DNS	188	Standard query response 0xb932 AAAA api.snapcraft.io AAAA 262...	
023623491	10.241.30.208	10.241.30.246	DNS	140	Standard query response 0xa4df A api.snapcraft.io A 185.125.1...	
015082027	10.241.30.246	10.241.30.208	DNS	86	Standard query 0x8b45 A mozilla.cloudflare-dns.com	
015628215	10.241.30.246	10.241.30.208	DNS	86	Standard query 0x63c0 AAAA mozilla.cloudflare-dns.com	
0179917611	10.241.30.208	10.241.30.246	DNS	118	Standard query response 0x8b45 A mozilla.cloudflare-dns.com A...	
01195538	10.241.30.208	10.241.30.246	DNS	142	Standard query response 0x63c0 AAAA mozilla.cloudflare-dns.co...	

Analyzing General traffic using wireshark

The screenshot shows a Wireshark capture of network traffic on the interface *enp0s3. The filter bar is set to 'Apply a display filter ... <Ctrl-/>'. The packet list shows various traffic types including ARP, SNMP, MDNS, and TLSv1.2. The selected packet is an ARP request (Standard query) from 10.241.30.246 to 10.241.30.208, asking for the IP address of mozilla.cloudflare-dns.com. The packet details pane shows the Ethernet II header, Internet Protocol Version 4 header, and the Address Resolution Protocol (request) section. The packet bytes pane shows the raw data of the ARP request.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	f2:65:a1:aa:5f:35	Broadcast	ARP	60	Who has 10.241.30.117? Tell 10.241.30.208
2	0.480492243	10.241.30.117	255.255.255.255	SNMP	166	get-request 1.3.6.1.4.1.1602.1.3.1.13.0 1.3
3	0.480492620	10.241.30.117	255.255.255.255	SNMP	166	get-request 1.3.6.1.4.1.1602.1.3.1.13.0 1.3
4	1.325169703	10.241.30.246	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ipps._tcp.local,
5	3.239290307	2600:1015:b151:2c8d:a00:27...	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local,
6	19.152857927	10.241.30.246	172.64.41.4	TLSv1.2	105	Application Data
7	19.202472549	f2:65:a1:aa:5f:35	Broadcast	ARP	60	Who has 10.241.30.246? Tell 10.241.30.208
8	19.202490802	PCSSystemtec_d9:1e:d0	f2:65:a1:aa:5f:35	ARP	42	10.241.30.246 is at 08:00:27:d9:1e:d0
9	19.208039271	172.64.41.4	10.241.30.246	TLSv1.2	105	Application Data
10	19.208064081	10.241.30.246	172.64.41.4	TCP	66	54598 -> 443 [ACK] Seq=40 Ack=40 Win=460 Len=
11	24.273160923	PCSSystemtec_d9:1e:d0	f2:65:a1:aa:5f:35	ARP	42	Who has 10.241.30.208? Tell 10.241.30.246
12	24.283178976	f2:65:a1:aa:5f:35	PCSSystemtec_d9:1e:...	ARP	60	10.241.30.208 is at f2:65:a1:aa:5f:35
13	27.893965325	f2:65:a1:aa:5f:35	Broadcast	ARP	60	Who has 10.241.30.117? Tell 10.241.30.208
14	35.600734943	10.241.30.117	255.255.255.255	SNMP	166	get-request 1.3.6.1.4.1.1602.1.3.1.13.0 1.3
15	35.600735229	10.241.30.117	255.255.255.255	SNMP	166	get-request 1.3.6.1.4.1.1602.1.3.1.13.0 1.3
16	54.158808514	10.241.30.246	10.241.30.208	DNS	89	Standard query 0x99dc A connectivity-check...

Analyzing the ip address in the filter bar:

I captured a network traffic to analyze communication between my machine IP address 10.241.30.246 and Dns Server IP address 34.107.243.93 confirming a secured connection established via TlsV1.3, this involved observing TCP 3 ways handshake and initial cipher negotiation.

FileMachineViewInputDevicesHelp

Nov 7 21:42

*any

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

ip.addr == 34.107.243.93

No.	Time	Source	Destination	Protocol	Length	Info
2...	245.514254274	34.107.243.93	10.241.30.246	TLSv1.3	107	Application Data
2...	245.514292089	10.241.30.246	34.107.243.93	TCP	68	60248 → 443 [ACK] Seq=2791 Ack=940 Win=63616
3...	299.676065928	10.241.30.246	34.107.243.93	TLSv1.3	107	Application Data
3...	299.678195225	10.241.30.246	34.107.243.93	TLSv1.3	92	Application Data
3...	299.678383551	10.241.30.246	34.107.243.93	TCP	68	60248 → 443 [FIN, ACK] Seq=2854 Ack=940 Win=
3...	299.761921754	10.241.30.246	34.107.243.93	TCP	68	[TCP Retransmission] 60248 → 443 [FIN, ACK]
3...	300.009690567	10.241.30.246	34.107.243.93	TCP	131	[TCP Retransmission] 60248 → 443 [FIN, PSH,
3...	300.497860926	10.241.30.246	34.107.243.93	TCP	131	[TCP Retransmission] 60248 → 443 [FIN, PSH,
3...	301.521970886	10.241.30.246	34.107.243.93	TCP	131	[TCP Retransmission] 60248 → 443 [FIN, PSH,
3...	303.508171295	10.241.30.246	34.107.243.93	TCP	131	[TCP Retransmission] 60248 → 443 [FIN, PSH,
3...	303.705219520	34.107.243.93	10.241.30.246	TCP	68	443 → 60248 [FIN, ACK] Seq=940 Ack=2855 Win=
3...	303.705255851	10.241.30.246	34.107.243.93	TCP	68	60248 → 443 [ACK] Seq=2855 Ack=941 Win=63616
4...	428.388759980	34.107.243.93	10.241.30.246	TLSv1.3	92	Application Data
4...	428.388820887	10.241.30.246	34.107.243.93	TCP	68	60256 → 443 [ACK] Seq=2084 Ack=1267 Win=6323
4...	428.389087382	10.241.30.246	34.107.243.93	TLSv1.3	96	Application Data
4...	428.423889201	10.241.30.246	10.241.30.246	TCP	68	443 → 60256 [ACK] Seq=1267 Ack=2112 Win=2672

Frame 339: 68 bytes on wire (544 bits), 68 bytes captured (544 b)

Section number: 1

Interface id: 0 (any)

Interface name: any

Encapsulation type: Linux cooked-mode capture v1 (25)

Arrival Time: Nov 7, 2025 21:39:42.072532114 EST

UTC Arrival Time: Nov 8, 2025 02:39:42.072532114 UTC

Epoch Arrival Time: 1762569582.072532114

[Time shift for this packet: 0.000000000 seconds]

0000

00 04 00 01 00 06 08 00 27 d9 1e d0 00 01 08 00

0010

45 00 00 34 84 1a 40 00 40 06 76 fa 0a f1 1e f6

0020

22 6b f3 5d eb 58 01 bb c2 47 3f a7 8d f3 74 8c

0030

80 10 01 f1 3f d6 00 00 01 01 08 0a f3 33 22 4b

0040

27 19 87 08

59°F

Mostly clear

Search

8:42 PM

11/7/2025

FileMachineViewInputDevicesHelp

Nov 7 22:07

*any

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

ip.addr == 34.107.243.93

No.	Time	Source	Destination	Protocol	Length	Info
106	128.096108758	34.107.243.93	10.241.30.246	TLSv1.3	99	Application Data
107	128.133623665	34.107.243.93	10.241.30.246	TCP	76	443 → 60256 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=136
108	128.133690532	10.241.30.246	34.107.243.93	TCP	68	60256 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4080039
109	128.134599865	10.241.30.246	34.107.243.93	TLSv1.3	1318	Client Hello (SNI=push.services.mozilla.com)
110	128.136655525	10.241.30.246	34.107.243.93	TCP	68	60248 → 443 [ACK] Seq=2713 Ack=862 Win=63616 Len=0 TSval=46
111	128.139311263	34.107.243.93	10.241.30.246	TCP	68	443 → 60248 [ACK] Seq=862 Ack=2713 Win=266496 Len=0 TSval=6
112	128.178989424	34.107.243.93	10.241.30.246	TCP	68	443 → 60256 [ACK] Seq=1 Ack=1251 Win=267776 Len=0 TSval=346
113	128.188322139	34.107.243.93	10.241.30.246	TLSv1.3	286	Server Hello, Change Cipher Spec, Application Data
114	128.188349757	10.241.30.246	34.107.243.93	TCP	68	60256 → 443 [ACK] Seq=1251 Ack=219 Win=64128 Len=0 TSval=46
115	128.189019710	10.241.30.246	34.107.243.93	TLSv1.3	132	Change Cipher Spec, Application Data
116	128.190959040	10.241.30.246	34.107.243.93	TLSv1.3	698	Application Data
117	128.241974485	34.107.243.93	10.241.30.246	TCP	68	443 → 60256 [ACK] Seq=219 Ack=1945 Win=267264 Len=0 TSval=5
118	128.283824083	34.107.243.93	10.241.30.246	TLSv1.3	900	Application Data
119	128.291399698	10.241.30.246	34.107.243.93	TLSv1.3	297	Application Data
120	128.340480421	34.107.243.93	10.241.30.246	TCP	68	443 → 60256 [ACK] Seq=1051 Ack=2084 Win=267264 Len=0 TSval=
121	128.379675740	34.107.243.93	10.241.30.246	TLSv1.3	260	Application Data

Frame 96: 68 bytes on wire (544 bits), 68 bytes captured (544 b)

Section number: 1

Interface id: 0 (any)

Interface name: any

Encapsulation type: Linux cooked-mode capture v1 (25)

Arrival Time: Nov 7, 2025 21:36:46.356700716 EST

UTC Arrival Time: Nov 8, 2025 02:36:46.356700716 UTC

Epoch Arrival Time: 1762569406.356700716

[Time shift for this packet: 0.000000000 seconds]

0000

00 04 00 01 00 06 08 00 27 d9 1e d0 00 00 08 00

0010

45 00 00 34 84 06 40 00 40 06 77 0e 0a f1 1e f6

0020

22 6b f3 5d eb 58 01 bb c2 47 34 81 8d f3 70 e0

0030

80 10 01 f6 3f d6 00 00 01 01 08 0a f3 30 73 e7

0040

27 16 d8 a8

59°F

Mostly clear

Search

9:07 PM

11/7/2025