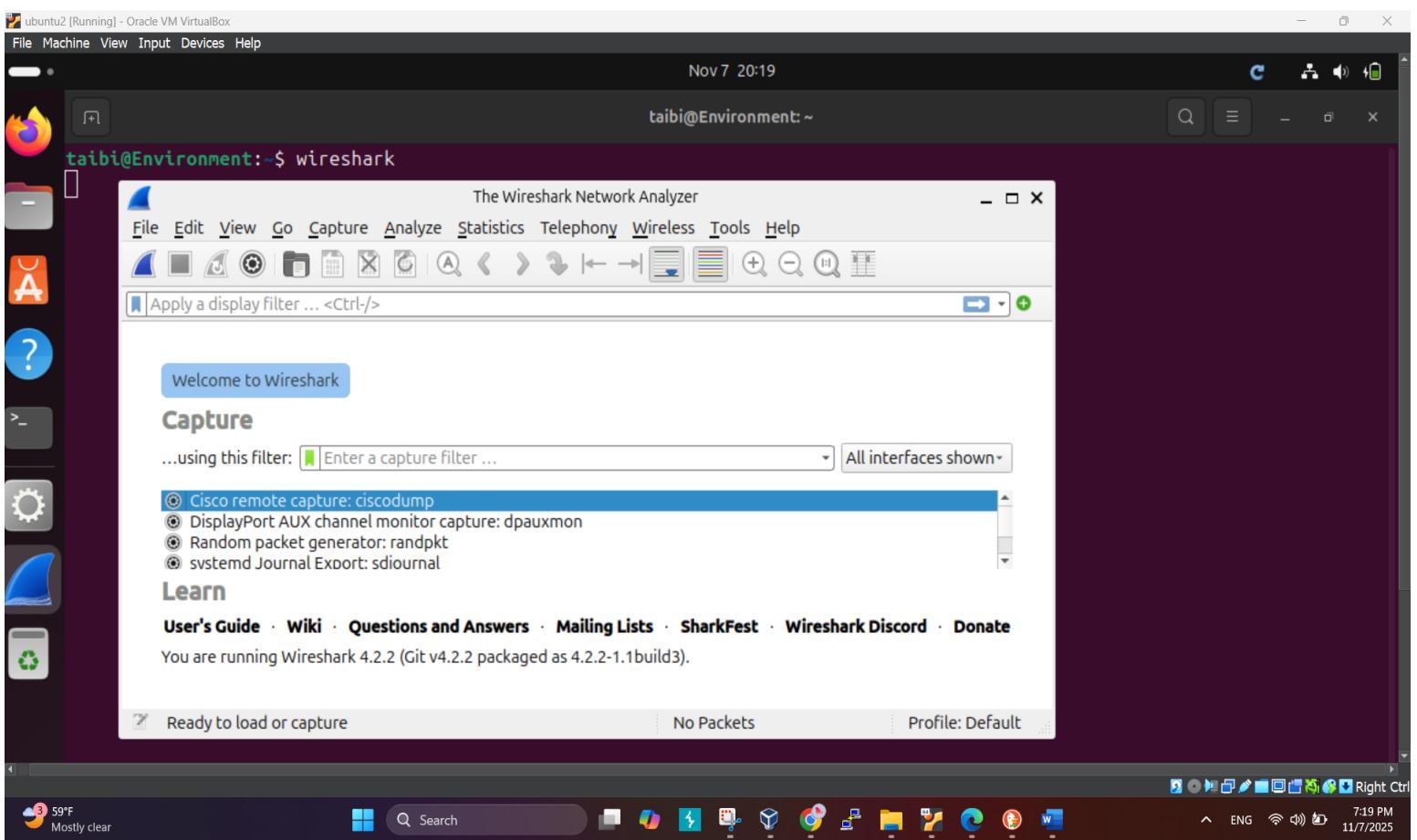


# installing wireshark tool

A screenshot of a Ubuntu desktop environment. A terminal window titled 'ubuntu2 [Running] - Oracle VM VirtualBox' is open, showing the command 'sudo apt install wireshark' being run. The output indicates that Wireshark is already the newest version (4.2.2-1.1build3). The desktop interface includes a dock with various icons like Dash, Home, and Settings, and a system tray at the bottom.

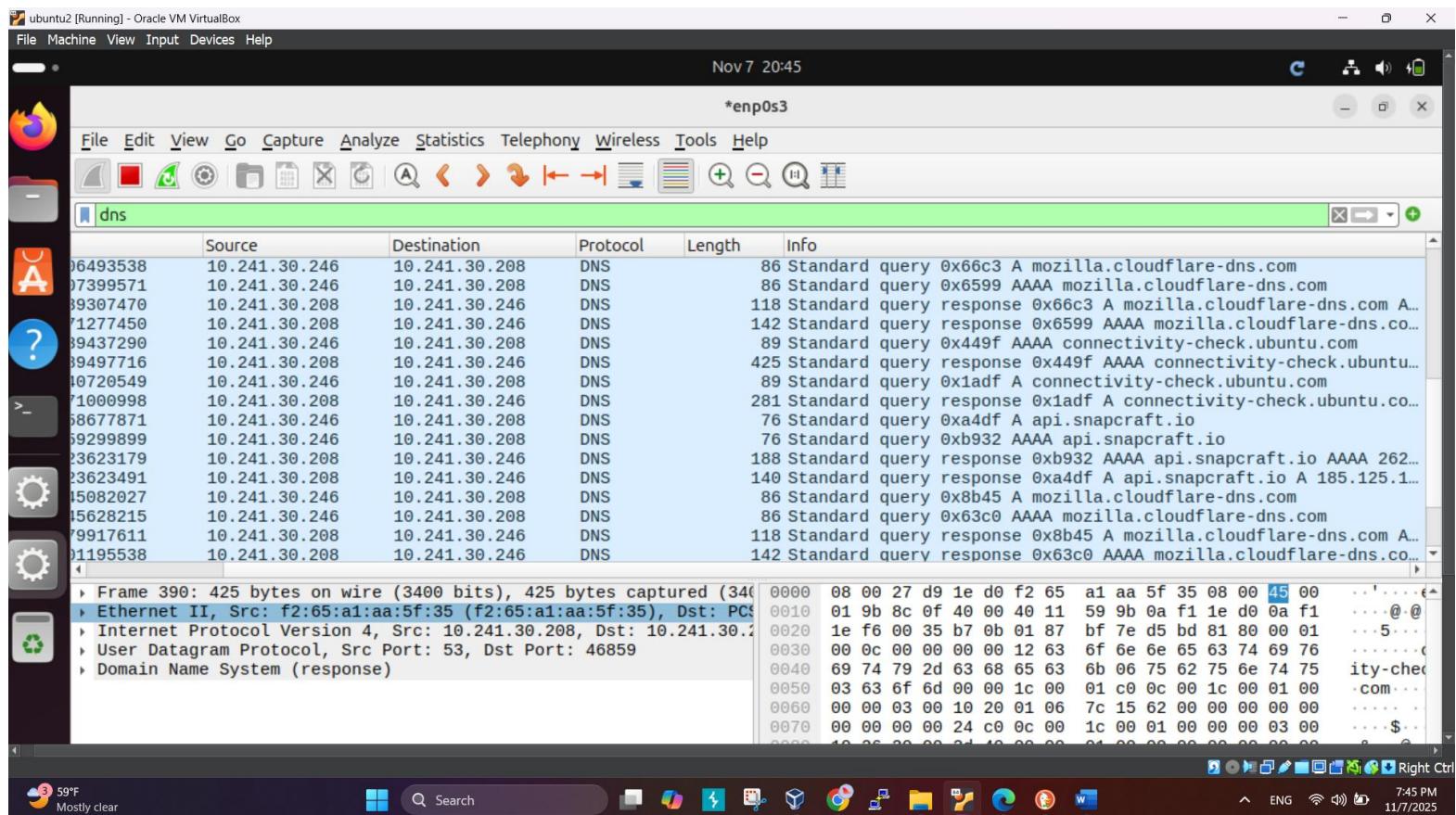
```
taibi@Environment:~$ sudo apt install wireshark
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wireshark is already the newest version (4.2.2-1.1build3).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
taibi@Environment:~$
```

## Opening the wireshark

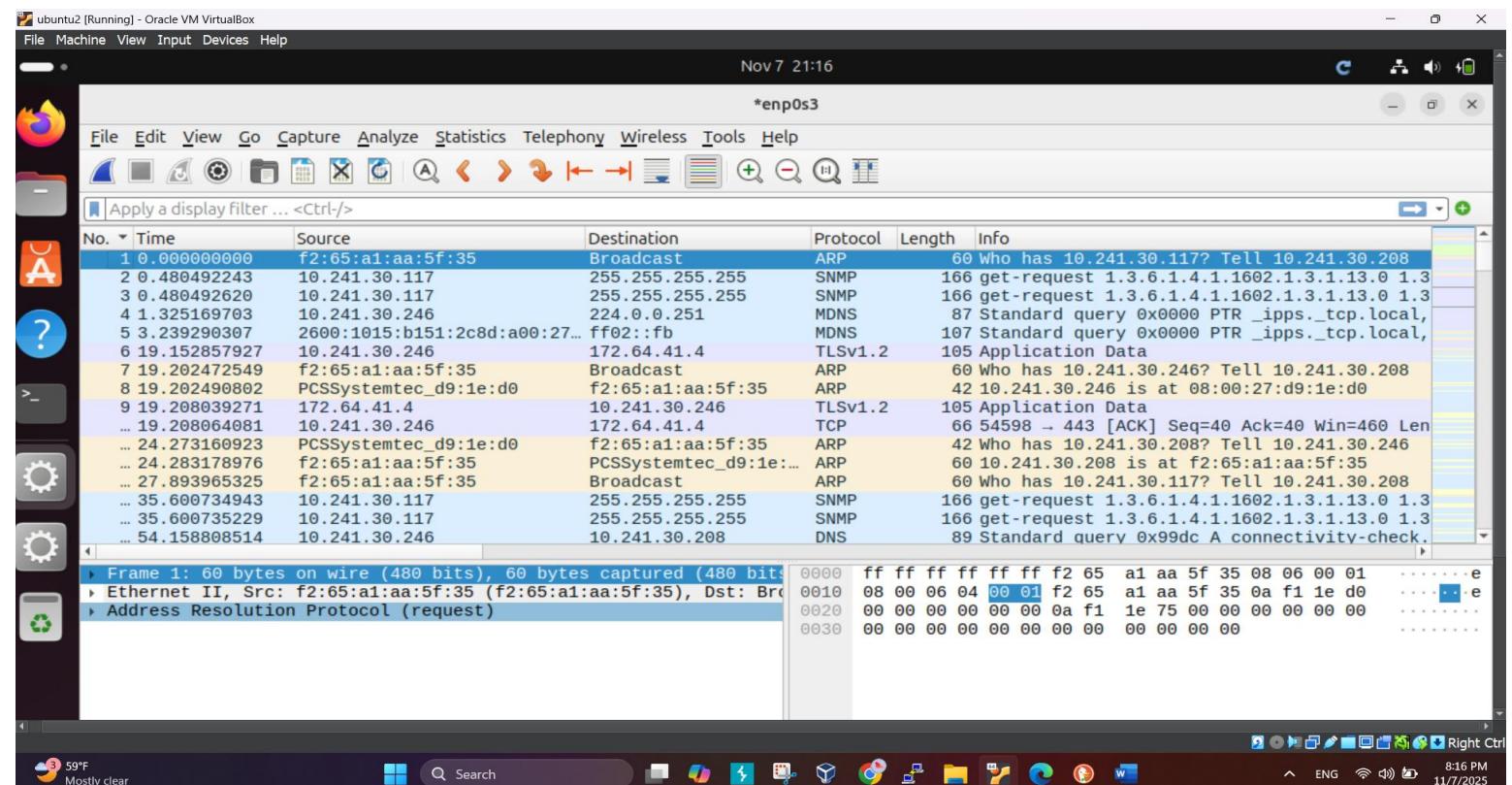


## Capturing the traffic:

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



## Analyzing General traffic using wireshark



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.

ubuntu2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Nov 7 21:42

\*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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	34.107.243.93	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 bits)

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	E..4..@..
0020	22 6b f3 5d eb 58 01 bb	c2 47 3f a7 8d f3 74 8c	"k.j.X..
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

8:42 PM 11/7/2025

ubuntu2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Nov 7 22:07

\*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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=1368
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=4080039
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=4080039
112	128.1789898424	34.107.243.93	10.241.30.246	TCP	68	443 → 60256 [ACK] Seq=1 Ack=1251 Win=267776 Len=0 TSval=34080039
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=4080039
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=34080039
118	128.283824083	34.107.243.93	10.241.30.246	TLSv1.3	900	Application Data, Application Data
119	128.291399698	10.241.30.246	34.107.243.93	TLSv1.3	207	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=34080039
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 bits)

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	E..4..@..
0020	22 6b f3 5d eb 58 01 bb	c2 47 34 81 8d f3 70 e0	"k.j.X..
0030	80 10 01 f1 3f d6 00 00	01 01 08 0a f3 30 73 e7	...?...
0040	27 16 d8 a8		....

59°F Mostly clear

9:07 PM 11/7/2025