

Day 6 of Learning Cyber Security

Platform: Kali Linux

Name: Ayesha Nadeem

Topic: Wireshark

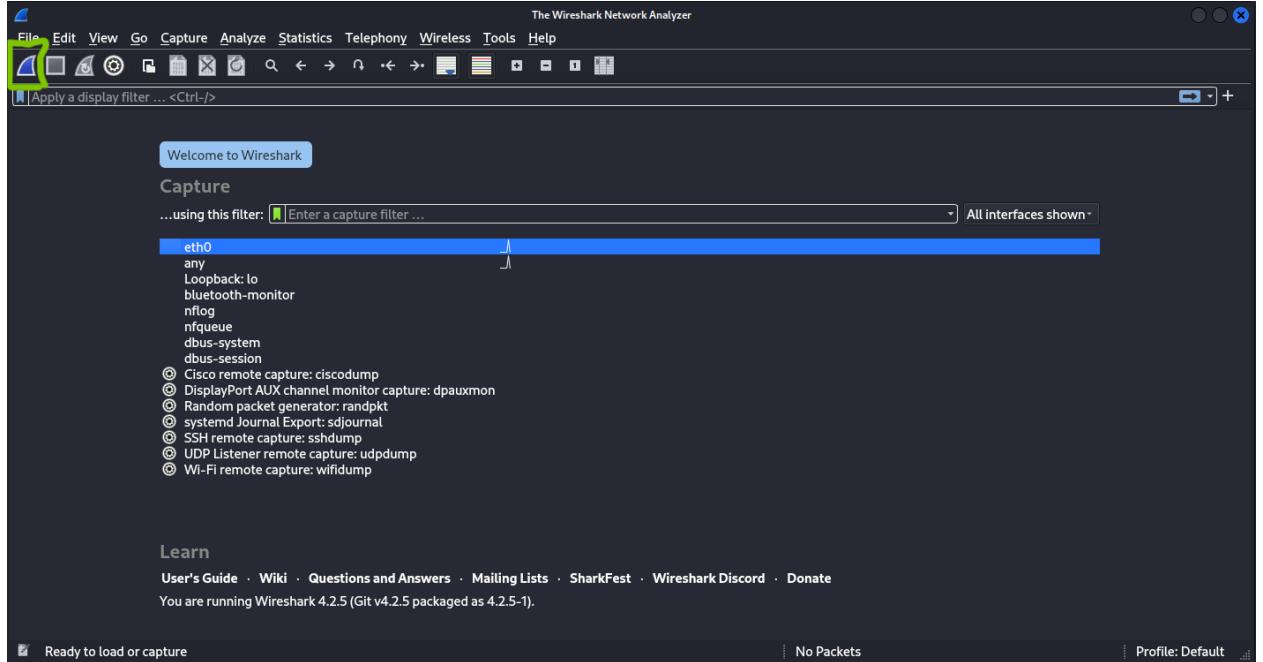


Contact Me: ayeshanm8@gmail.com

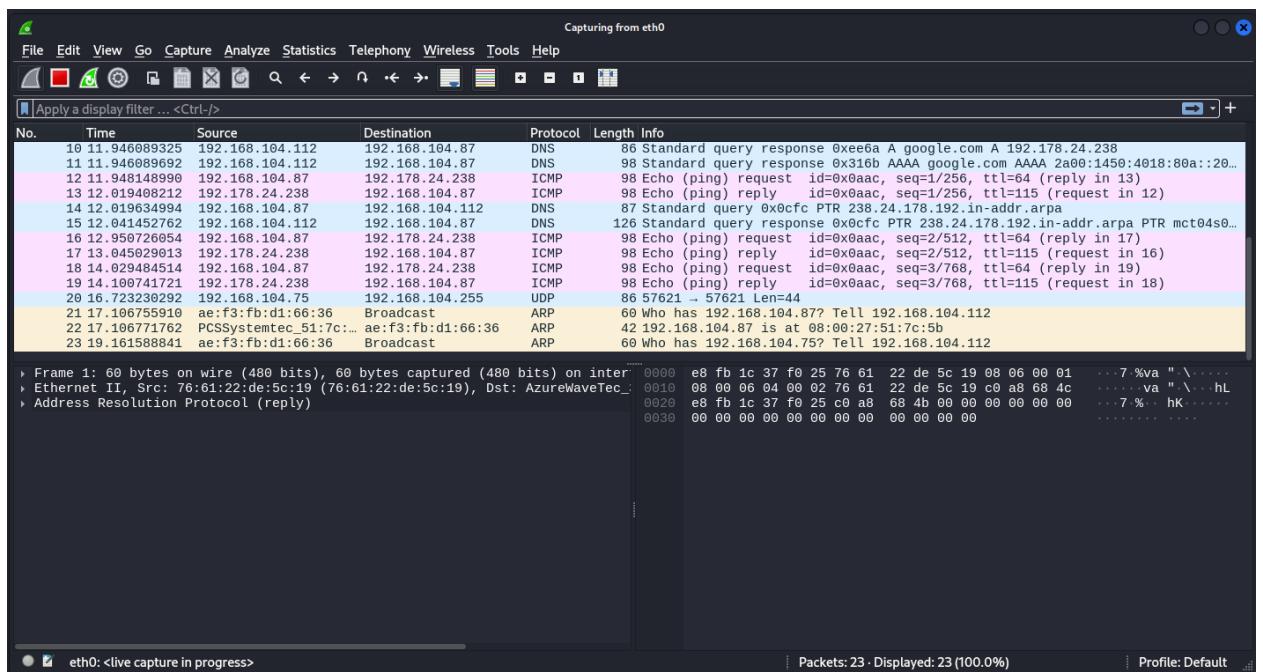
Date: 6th July, 2025

Wireshark: The Packet sniffer

1. Open Wireshark and Hit eth0

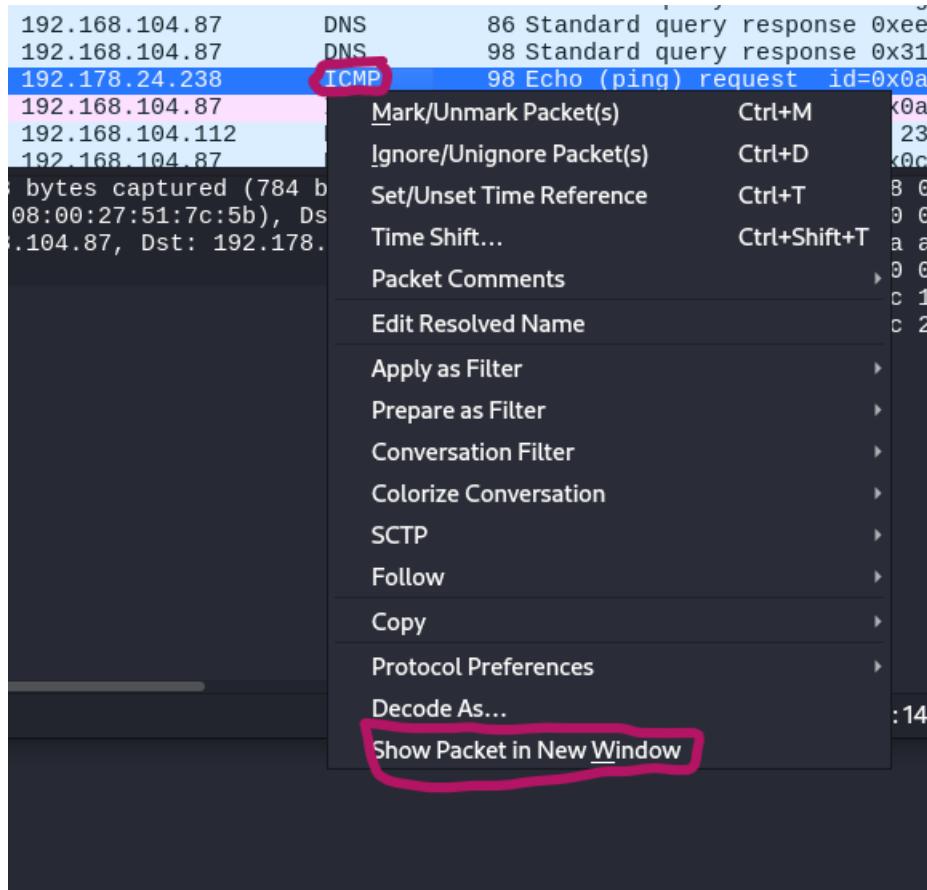


2. Packet Sniffed from eth0 network

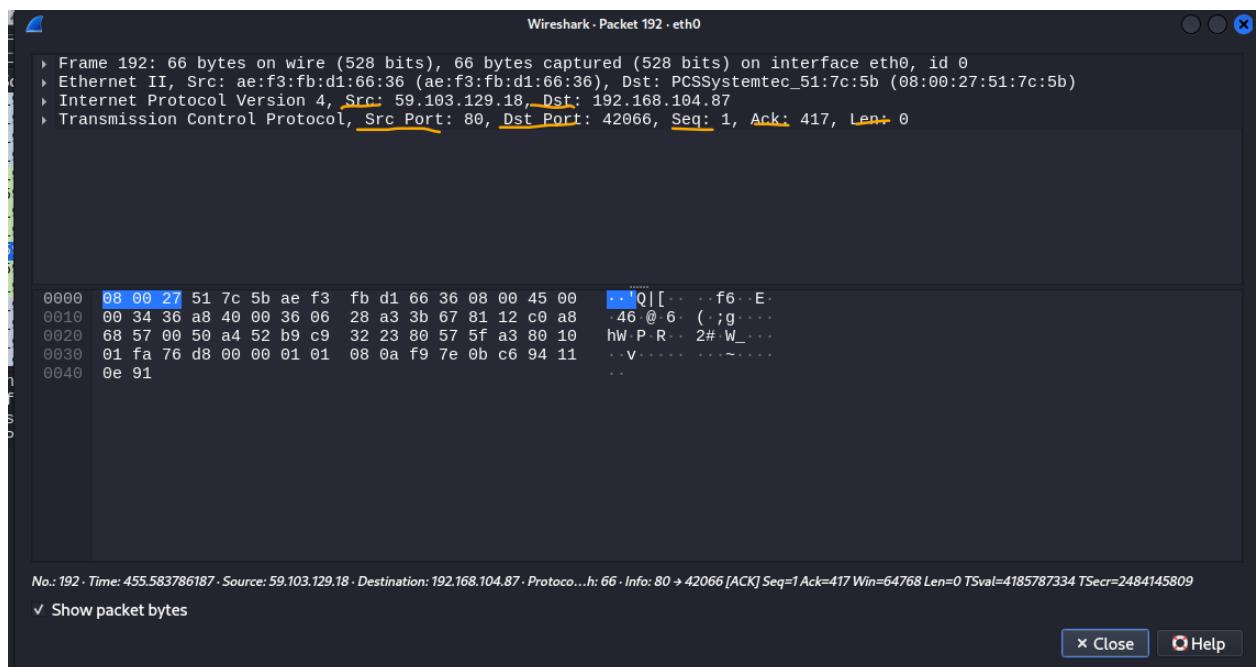


3. Inspect Packet Steps:

→ Right click on any packet and select “Show packet in new Windows”



TCP Packet Details:



UDP Packet Details:

Wireshark - Packet 4 · eth0

```

Frame 4: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface eth0, id 0
Ethernet II, Src: 76:61:22:de:5c:19 (76:61:22:de:5c:19), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.104.76, Dst: 192.168.104.255
User Datagram Protocol, Src Port: 57621, Dst Port: 57621
Data (40 bytes)

0000 ff ff ff ff ff ff 76 61 22 de 5c 19 08 00 45 00 .....va "\...E...
0010 00 44 04 19 40 00 40 11 e3 f3 c0 a8 68 4c c0 a8 .D @ @ ...hL...
0020 68 ff e1 15 e1 15 00 30 e2 e3 53 70 6f 74 55 64 h.....0 .SpotUd
0030 70 30 61 78 27 9e 82 00 c6 33 00 01 00 00 5d 7e p0ax!...3...]~TM..lk...z.$
0040 54 4d 86 ea 6c 6b ee b4 ef e2 af 60 2d 7a ce 24 .c
0050 7f 63

No.: 4 · Time: 0.354443736 · Source: 192.168.104.76 · Destination: 192.168.104.255 · Protocol: UDP · Length: 82 · Info: 57621 → 57621 Len=40
>Show packet bytes

```

x Close Help

ICMP Packet Details:

Wireshark - Packet 16 · eth0

```

Frame 16: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_51:7c:5b (08:00:27:51:7c:5b), Dst: ae:f3:fb:d1:66:36 (ae:f3:fb:d1:66:36)
Internet Protocol Version 4, Src: 192.168.104.87, Dst: 192.178.24.238
Internet Control Message Protocol

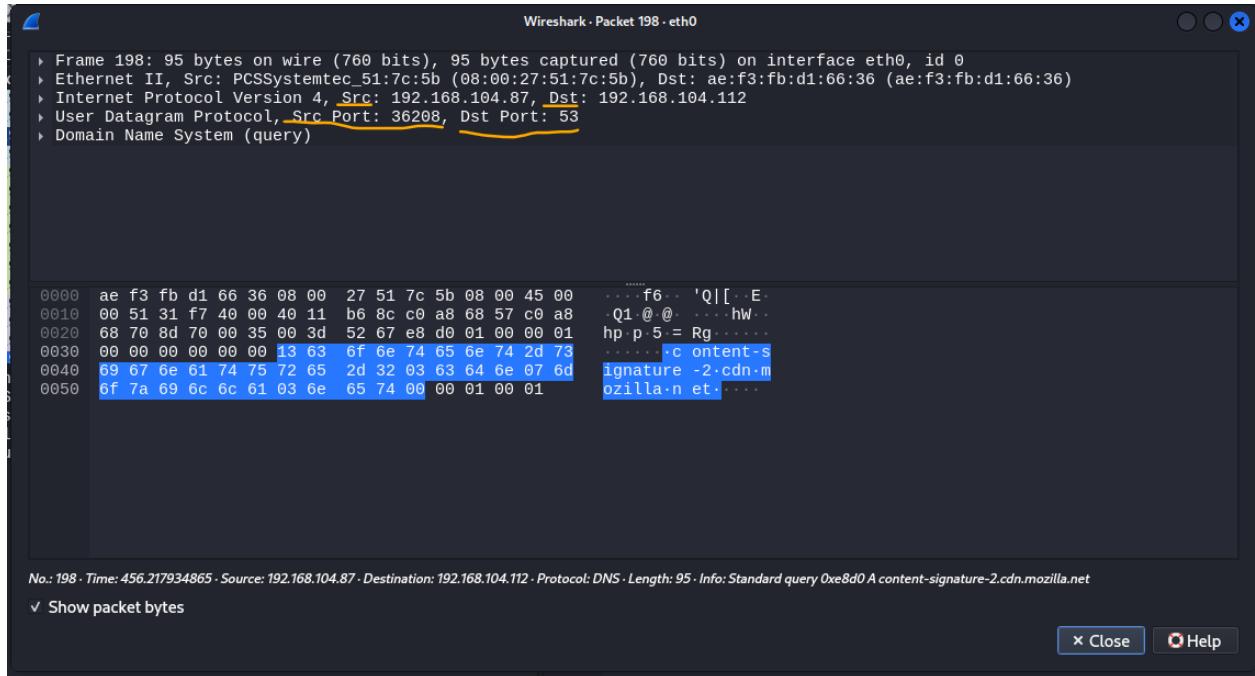
0000 ae f3 fb d1 66 36 08 00 27 51 7c 5b 08 00 45 00 .....f6 ..'Q|[..E...
0010 00 54 f2 5f 40 00 40 01 45 a9 c0 a8 68 57 c0 b2 .T _@ @ E ..hW...
0020 18 ee 08 00 ac f5 0a ac 00 02 ea 69 34 68 00 00 .i4h...
0030 00 00 61 b7 01 00 00 00 00 00 10 11 12 13 14 15 ..a.....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ....."!#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*, - ./012345
0060 36 37 67

No.: 16 · Time: 12.950726054 · Source: 192.168.104.87 · Destination: 192.178.24.238 · Protocol: ICMP · Length: 98 · Info: Echo (ping) request id=0x0aac, seq=2/512, ttl=64 (reply in 17)
>Show packet bytes

```

x Close Help

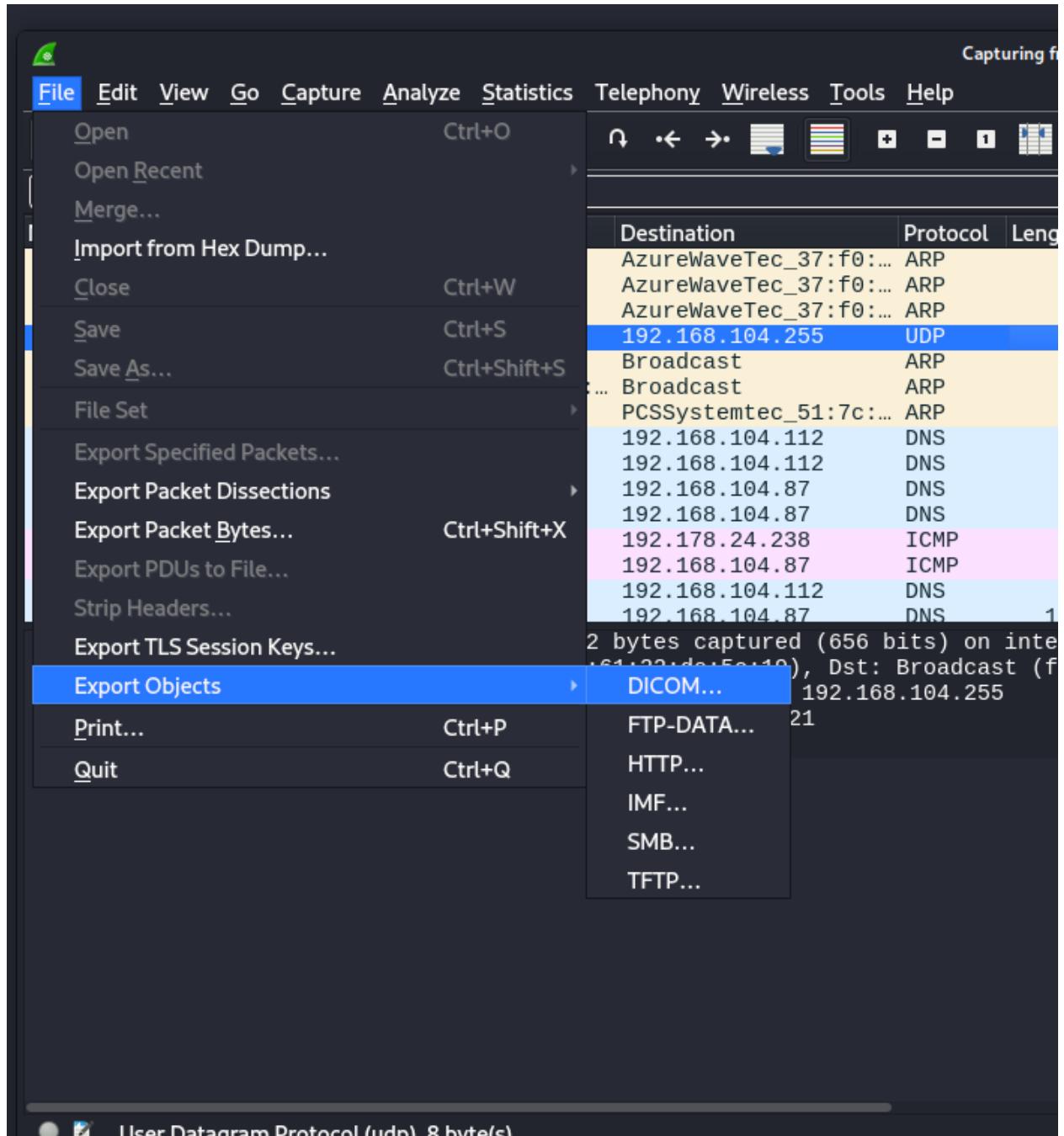
DNS Packets Details:

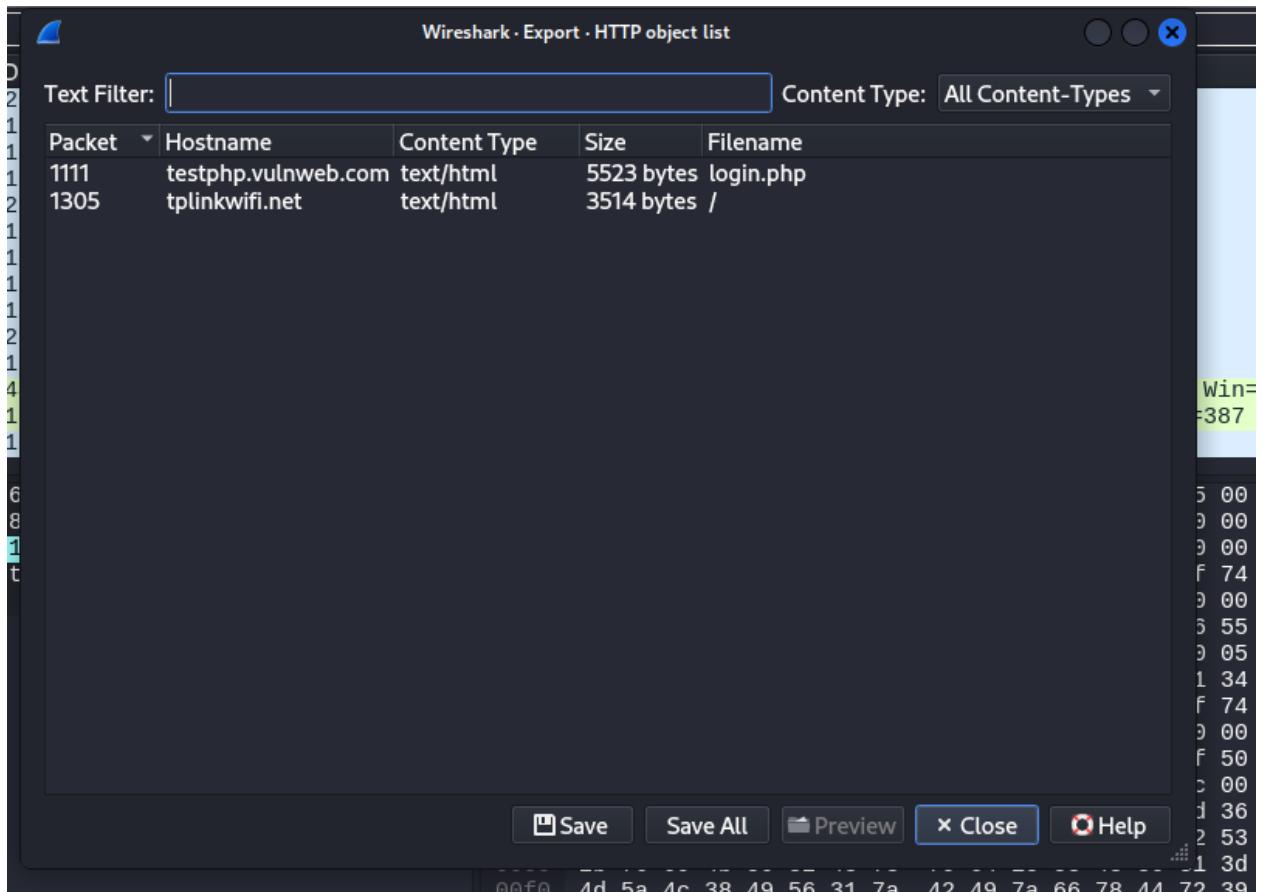


Similarly we can inspect any packet to get their IP's, port in which they communicates, sequence and acknowledgment numbers

4. Export Object:

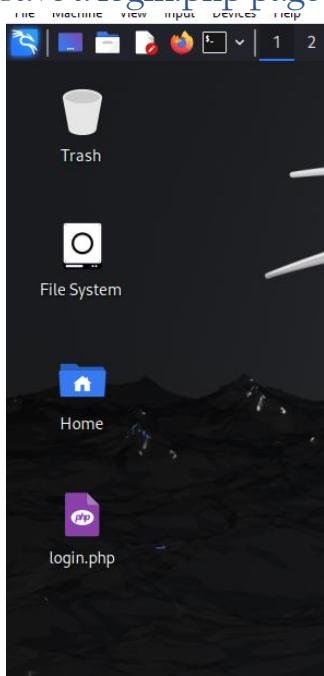
- Go to File
- Select Export Object
- Click on HTTP

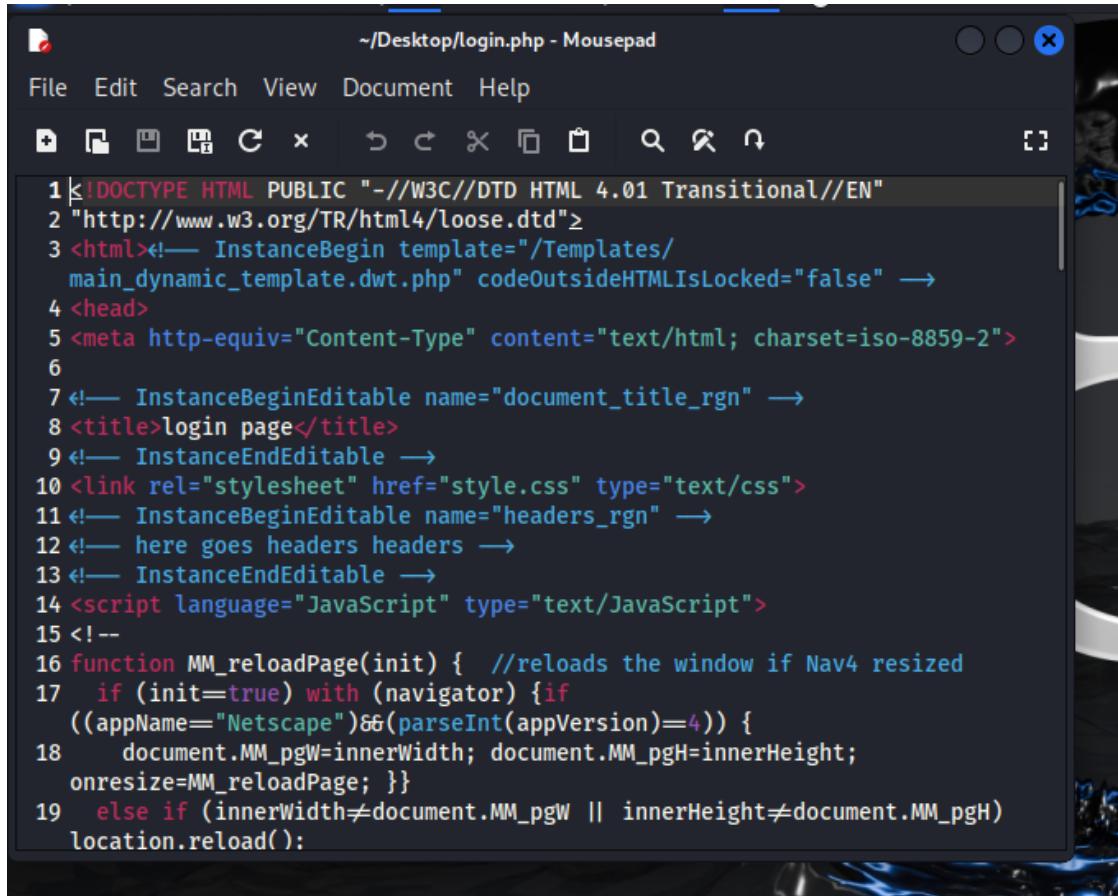




So it capture the site you opened in your firefox/chrome.

[Save a login.php page to get its code:](#)

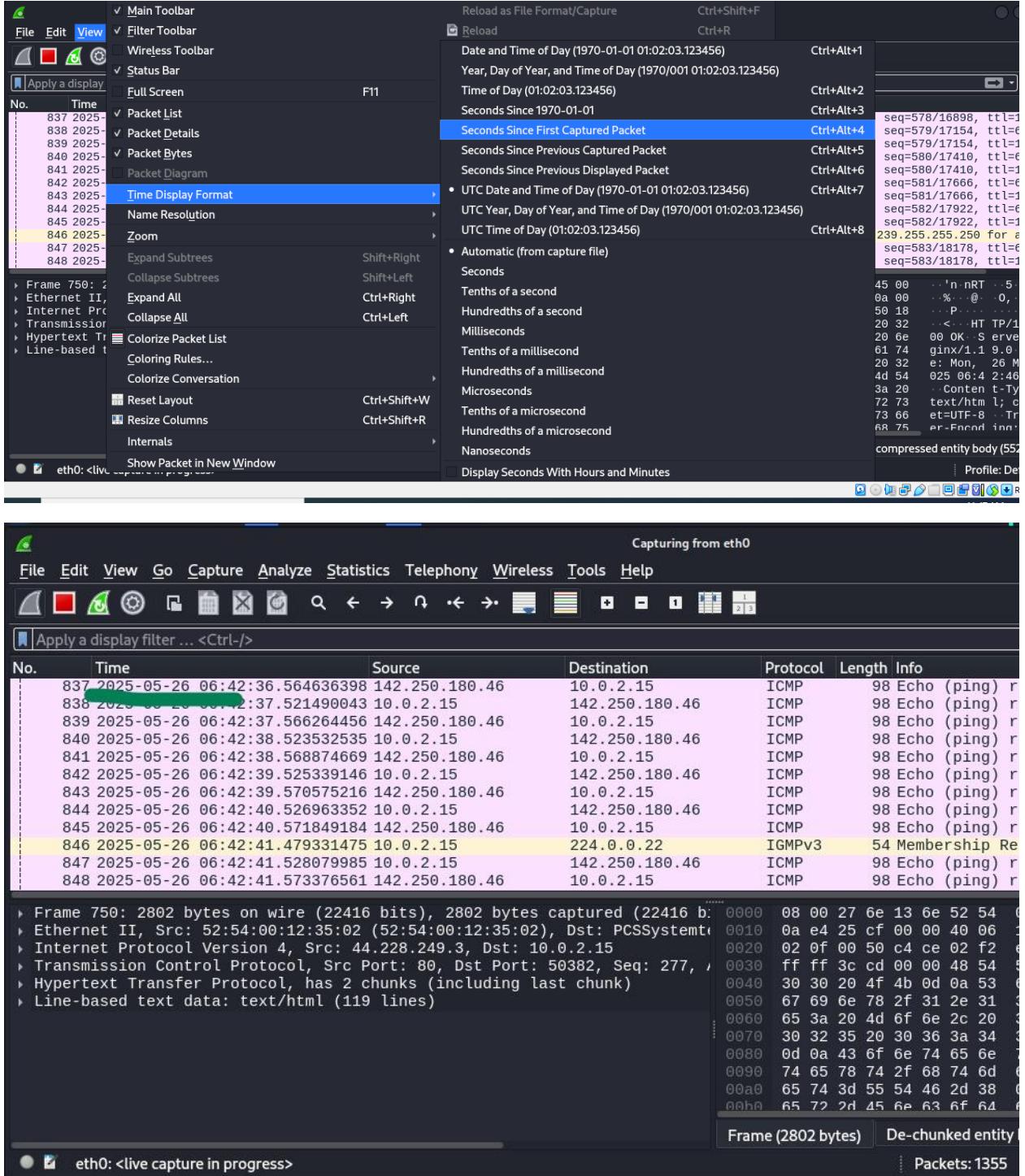




```
1 !DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
2 "http://www.w3.org/TR/html4/loose.dtd">
3 <html><!-- InstanceBegin template="/Templates/
  main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->
4 <head>
5 <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
6
7 <!-- InstanceBeginEditable name="document_title_rgn" -->
8 <title>login page</title>
9 <!-- InstanceEndEditable -->
10 <link rel="stylesheet" href="style.css" type="text/css">
11 <!-- InstanceBeginEditable name="headers_rgn" -->
12 <!-- here goes headers headers -->
13 <!-- InstanceEndEditable -->
14 <script language="JavaScript" type="text/JavaScript">
15 <!--
16 function MM_reloadPage(init) { // reloads the window if Nav4 resized
17   if (init==true) with (navigator) {if
    ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
18     document.MM_pgW=innerWidth; document.MM_pgH=innerHeight;
      onresize=MM_reloadPage; }}
19   else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH)
      location.reload(); }
```

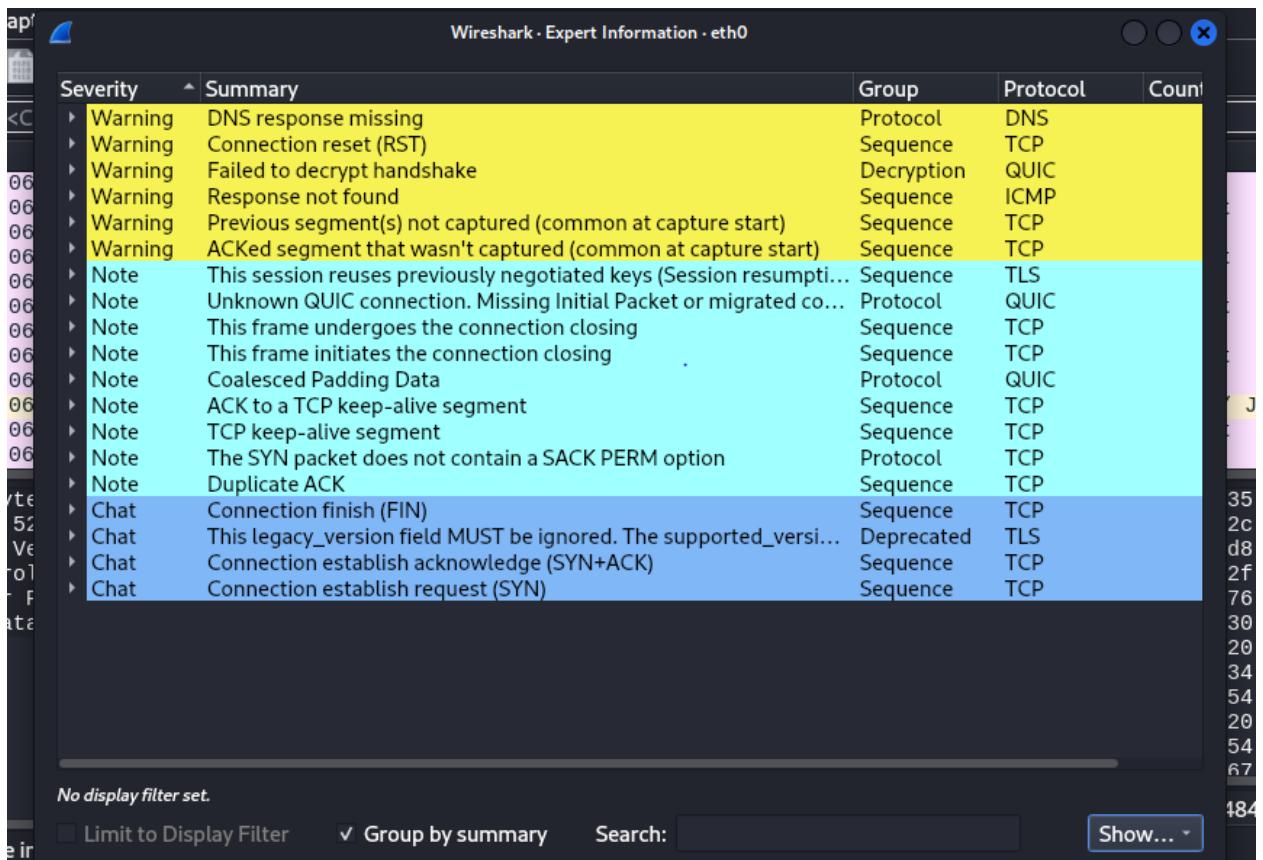
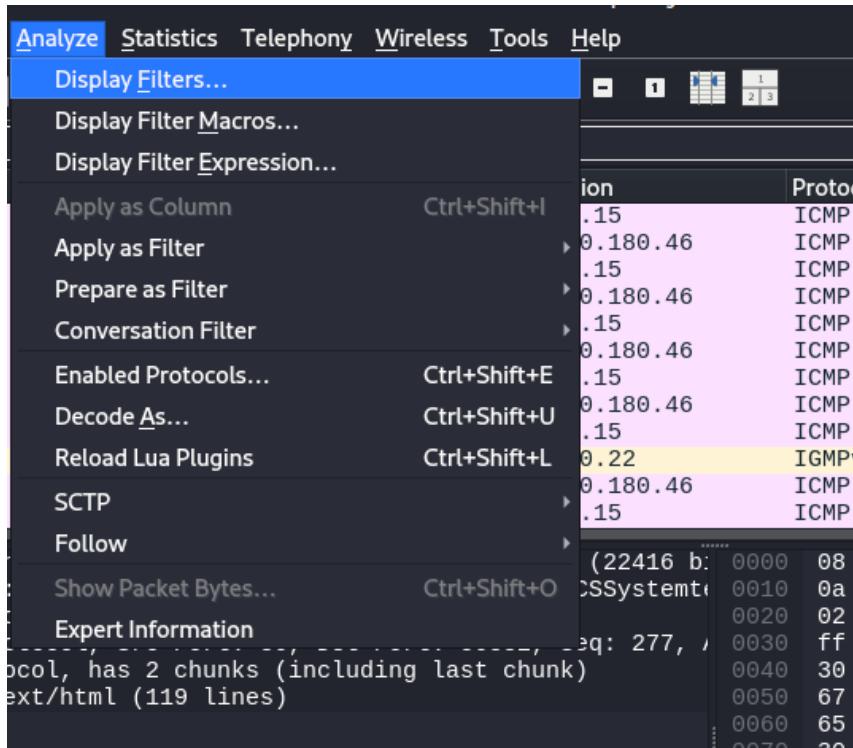
5. Setting data Format:

Go to view, select “Time Display Format” and click on any format you want.



6. Analyzing packet with color strategy:

Go to analyze then go to Expert Information



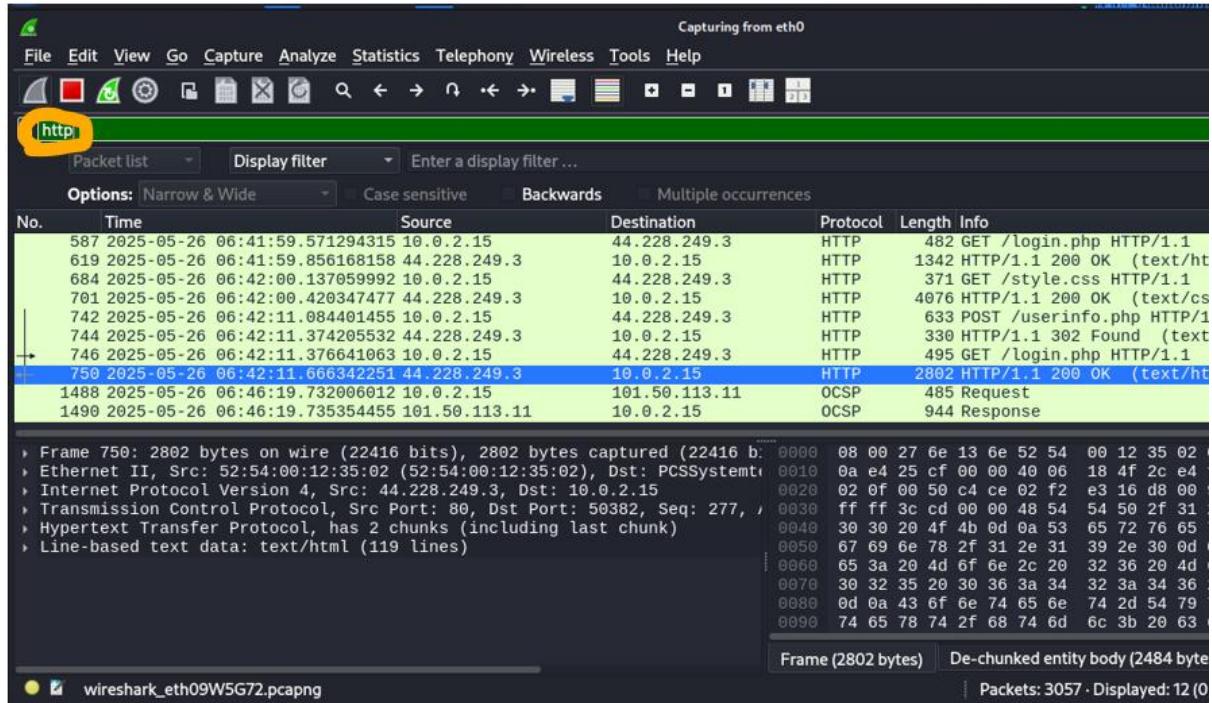
This shows the network event happened with severity levels like:

- **Notes:** Informational messages, like TCP keep-alives.
- **Warnings:** Potential issues like missing responses.
- **Errors or Chats:** More serious anomalies, e.g. resets or failed handshakes

It helps in quick triage of issues without deep packet digging.

7. Filtering in Wireshark:

Applied filter of HTTP to just show http packets



8. Extracting credentials using Wireshark packet filtering:

First go to <http://testphp.vulnweb.com/login.php> and enter fake credentials.

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

If you are already registered please enter your login information below:

Username : ayeshanadeem

Password : *****

login

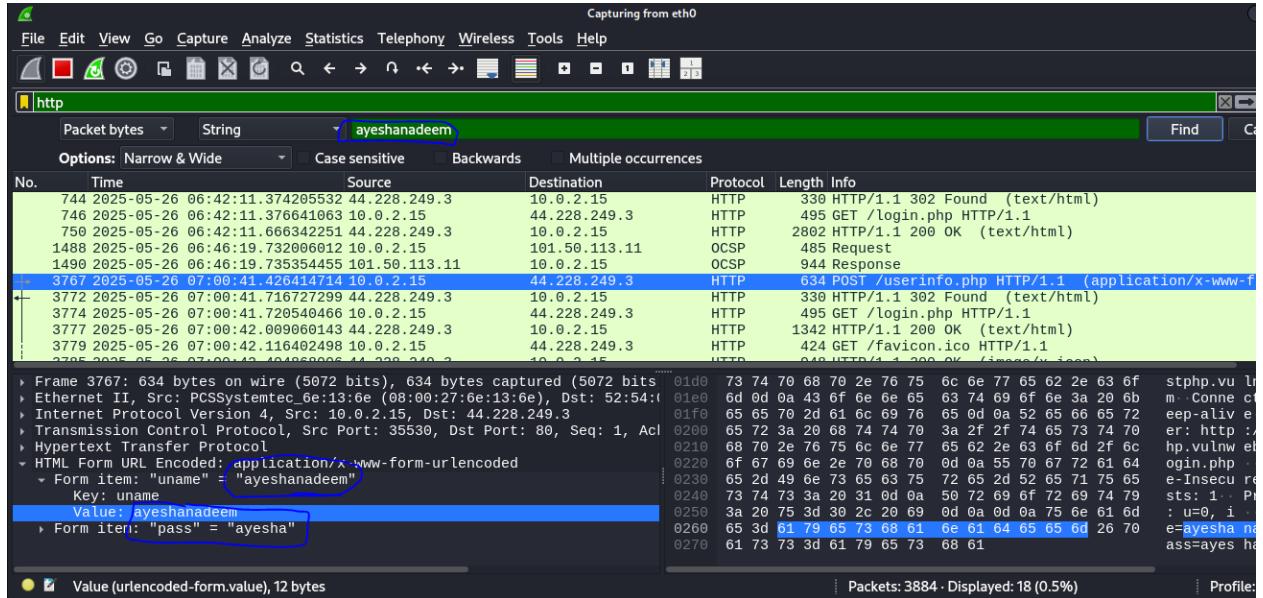
You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

Links

- Security art
- PHP scanner
- PHP vuln help
- Fractal Explorer

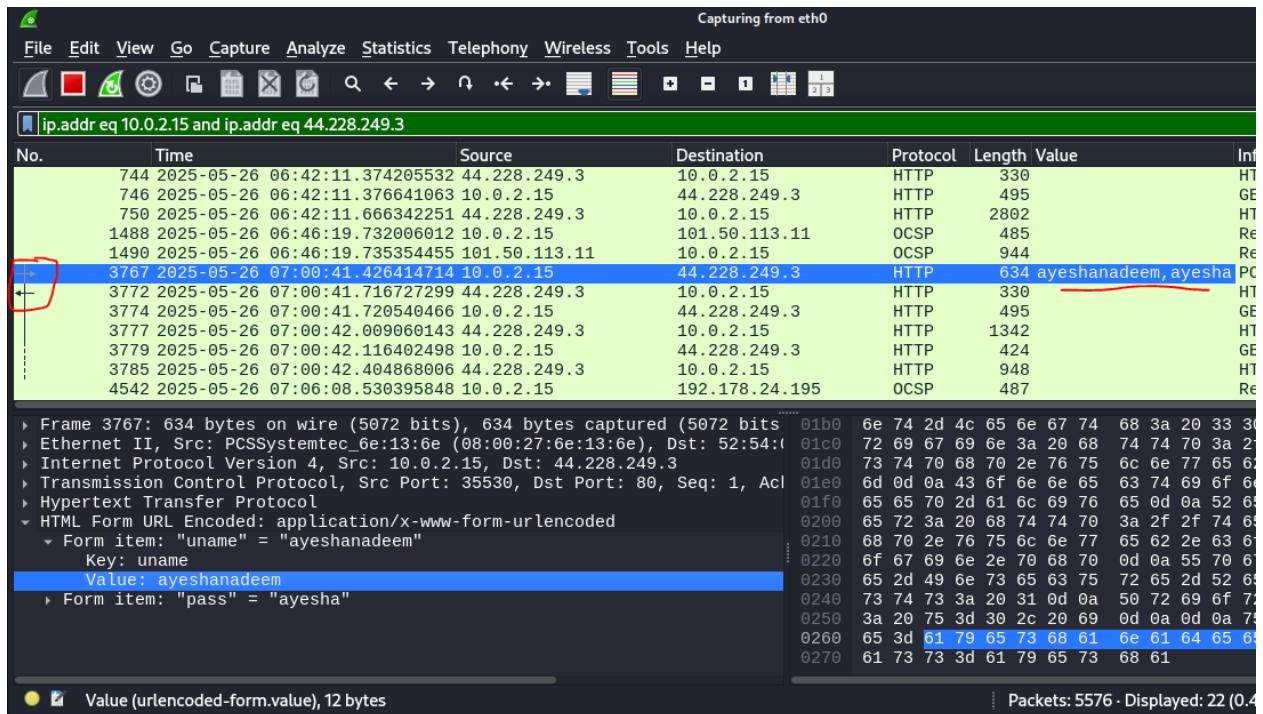
Come back to wireshark. Click on Edit on toolbar and select “Find Packet”

First set parameter like “stirng”, “packetbytes” and then type in search bar username.

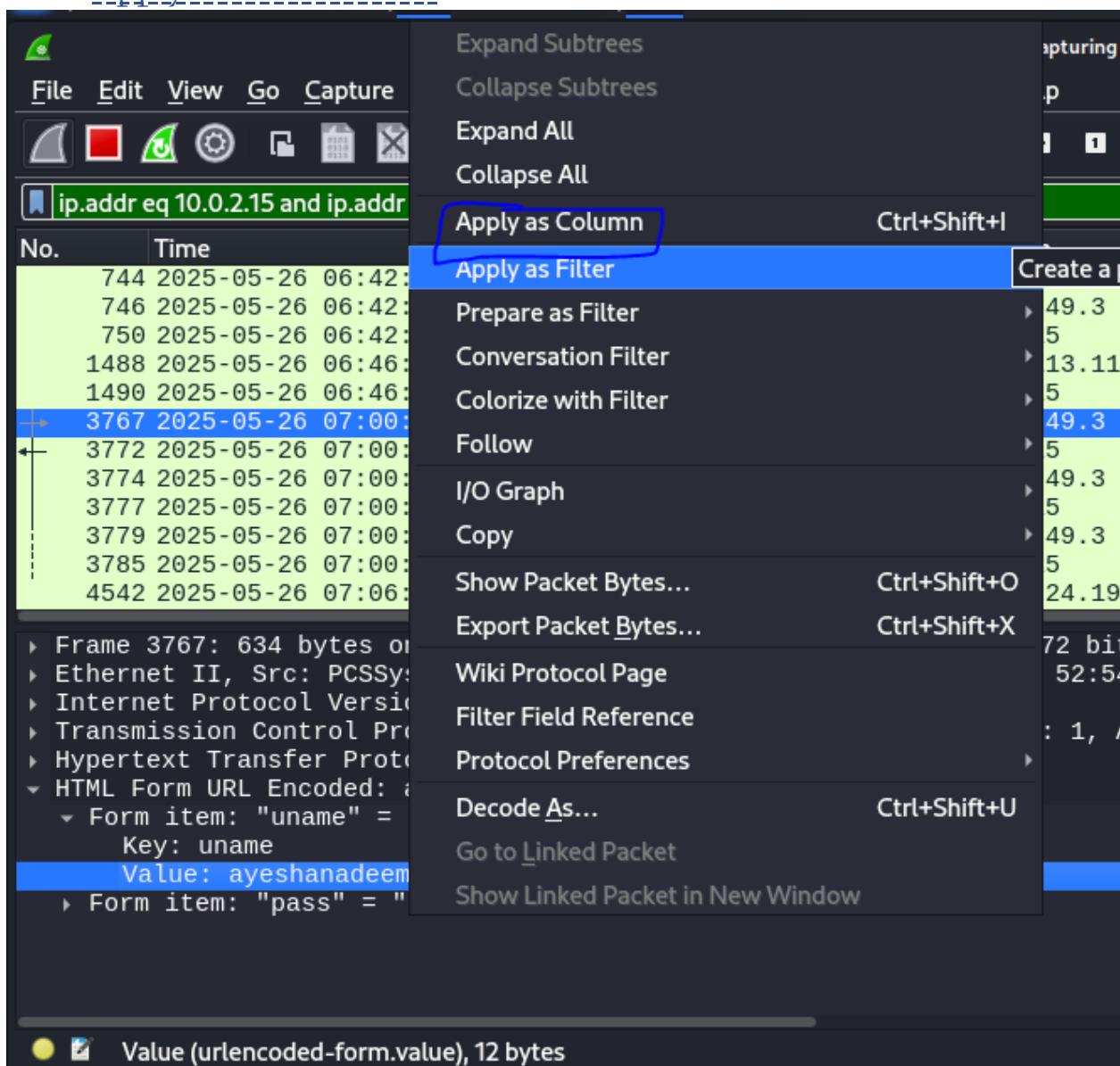


Forward arrow shows request packet

Backward arrow shows response packet



9. Apply filter as column:



Before

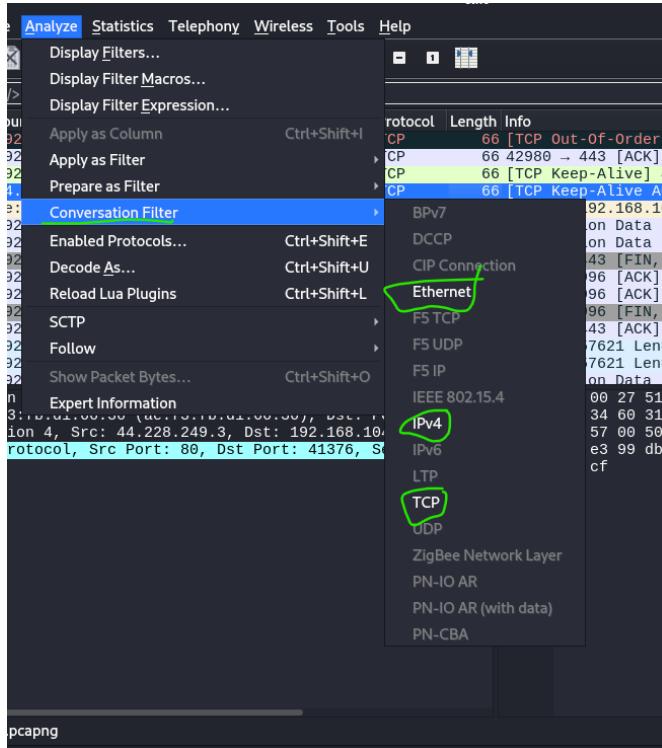
Capturing from eth0							
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help		http					
Packet bytes String ayeshanadeem							
Options: Narrow & Wide	Case sensitive	Backwards	Multiple occurrences				
No.	Time	Source	Destination	Protocol	Length	Info	
744	2025-05-26 06:42:11.374205532	44.228.249.3	10.0.2.15	HTTP	336	HTTP/1.1 302 Found (text/html)	
746	2025-05-26 06:42:11.376641063	10.0.2.15	44.228.249.3	HTTP	495	GET /login.php HTTP/1.1	
750	2025-05-26 06:42:11.666342251	44.228.249.3	10.0.2.15	HTTP	2802	HTTP/1.1 200 OK (text/html)	
1488	2025-05-26 06:46:19.732006012	10.0.2.15	101.50.113.11	OCSP	485	Request	
1490	2025-05-26 06:46:19.735354455	101.50.113.11	10.0.2.15	OCSP	944	Response	
3767	2025-05-26 07:00:41.426414714	10.0.2.15	44.228.249.3	HTTP	634	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)	
3772	2025-05-26 07:00:41.716727299	44.228.249.3	10.0.2.15	HTTP	336	HTTP/1.1 302 Found (text/html)	
3774	2025-05-26 07:00:41.720540466	10.0.2.15	44.228.249.3	HTTP	495	GET /login.php HTTP/1.1	
3777	2025-05-26 07:00:42.009060143	44.228.249.3	10.0.2.15	HTTP	1342	HTTP/1.1 200 OK (text/html)	
3779	2025-05-26 07:00:42.116402498	10.0.2.15	44.228.249.3	HTTP	424	GET /favicon.ico HTTP/1.1	
3785	2025-05-26 07:00:42.404868006	44.228.249.3	10.0.2.15	HTTP	948	HTTP/1.1 200 OK (text/html)	
4542	2025-05-26 07:06:08.530395848	10.0.2.15	192.178.24.195	OCSP	487	Request	
Frame 3767: 634 bytes on wire (5072 bits), 634 bytes captured (5072 bits) on interface stphpu1l Ethernet II, Src: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e), Dst: 52:54:00:1f:00:00 (eth0) Internet Protocol Version 4, Src: 10.0.2.15, Dst: 44.228.249.3 Transmission Control Protocol, Src Port: 35530, Dst Port: 80, Seq: 1, Ack: 1, Len: 634 Hypertext Transfer Protocol HTML Form URL Encoded: application/x-www-form-urlencoded Form item: "uname" = "ayeshanadeem" Key: uname Value: ayeshanadeem Form item: "pass" = "ayesha"							
01e0 73 74 70 68 70 2e 76 75 6c 6e 77 65 62 2e 63 6f stphpu1l 01e0 6d 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b m...Conne 01f0 65 65 70 2d 61 6c 69 76 65 0d 0a 52 65 66 65 72 eep-aliv 0200 65 72 3a 20 68 74 74 70 3a 2f 74 65 73 74 70 er: http : 0210 68 70 2e 76 75 6c 66 77 65 62 2e 63 6f 0d 2f 6c hp.vulnwe 0220 6f 67 69 6e 2e 70 68 70 0d 0a 55 78 67 72 61 64 ogin.php 0230 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 e-Insecu 0240 73 74 73 3a 20 31 0d 0a 50 72 69 6f 72 69 74 79 sts: 1... P 0250 3a 20 75 3d 30 2c 20 69 0d 0a 0d 0a 75 6e 61 6d : u=0, i=0 0260 65 3d 61 79 65 73 68 61 6e 61 64 65 65 6d 26 70 e=ayeshan 0270 61 73 73 3d 61 79 65 73 68 61 ass=ayeshanadeem Value (urlencoded-form.value), 12 bytes							
Packets: 3884 · Displayed: 18 (0.5%)							
Profile							

After:

Capturing from eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help		http				
ip.addr eq 10.0.2.15 and ip.addr eq 44.228.249.3						
No.	Time	Source	Destination	Protocol	Length	Value
744	2025-05-26 06:42:11.374205532	44.228.249.3	10.0.2.15	HTTP	330	
746	2025-05-26 06:42:11.376641063	10.0.2.15	44.228.249.3	HTTP	495	
750	2025-05-26 06:42:11.666342251	44.228.249.3	10.0.2.15	HTTP	2802	
1488	2025-05-26 06:46:19.732006012	10.0.2.15	101.50.113.11	OCSP	485	
1490	2025-05-26 06:46:19.735354455	101.50.113.11	10.0.2.15	OCSP	944	
3767	2025-05-26 07:00:41.426414714	10.0.2.15	44.228.249.3	HTTP	634	ayeshanadeem, ayesha
3772	2025-05-26 07:00:41.716727299	44.228.249.3	10.0.2.15	HTTP	330	
3774	2025-05-26 07:00:41.720540466	10.0.2.15	44.228.249.3	HTTP	495	
3777	2025-05-26 07:00:42.009060143	44.228.249.3	10.0.2.15	HTTP	1342	
3779	2025-05-26 07:00:42.116402498	10.0.2.15	44.228.249.3	HTTP	424	
3785	2025-05-26 07:00:42.404868006	44.228.249.3	10.0.2.15	HTTP	948	
4542	2025-05-26 07:06:08.530395848	10.0.2.15	192.178.24.195	OCSP	487	
Frame 3767: 634 bytes on wire (5072 bits), 634 bytes captured (5072 bits) on interface stphpu1l Ethernet II, Src: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e), Dst: 52:54:00:1f:00:00 (eth0) Internet Protocol Version 4, Src: 10.0.2.15, Dst: 44.228.249.3 Transmission Control Protocol, Src Port: 35530, Dst Port: 80, Seq: 1, Ack: 1, Len: 634 Hypertext Transfer Protocol HTML Form URL Encoded: application/x-www-form-urlencoded Form item: "uname" = "ayeshanadeem" Key: uname Value: ayeshanadeem Form item: "pass" = "ayesha"						
01b0 6e 74 2d 4c 65 6e 67 74 68 3a 20 33 30 01c0 72 69 67 69 6e 3a 20 68 74 74 70 70 3a 21 01d0 73 74 70 68 70 2e 76 75 6c 6e 77 65 62 01e0 6d 0d 0a 43 6f 6e 66 65 63 74 69 6f 66 65 01f0 65 65 70 2d 61 6c 69 76 65 0d 0a 52 65 66 0200 65 72 3a 20 68 74 74 70 3a 2f 74 65 66 65 0210 68 70 2e 76 75 6c 6e 77 65 62 2e 63 61 66 0220 6f 67 69 6e 2e 70 68 70 0d 0a 55 70 67 61 0230 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 0240 73 74 73 3a 20 31 0d 0a 50 72 69 6f 72 69 0250 3a 20 75 3d 30 2c 20 69 0d 0a 0d 0a 75 6e 0260 65 3d 61 79 65 73 68 61 6e 61 64 65 65 6d 0270 61 73 73 3d 61 79 65 73 68 61 Value (urlencoded-form.value), 12 bytes						
Packets: 5576 · Displayed: 22 (0.4%)						
Profile						

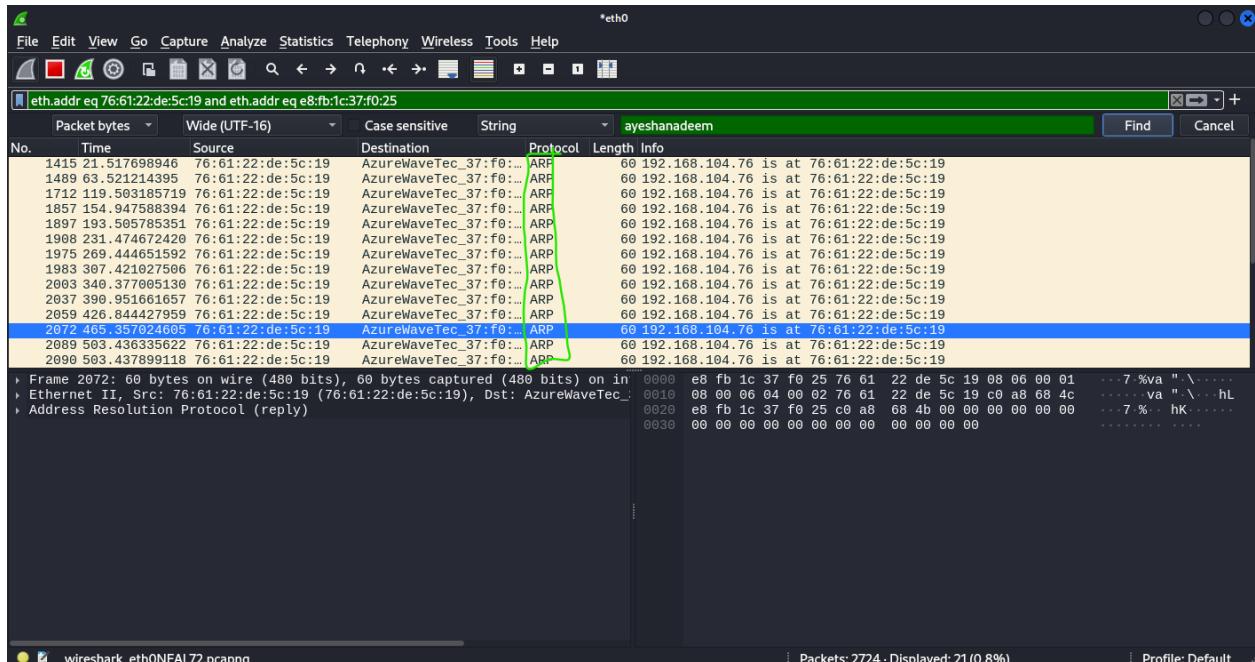
10. Conversational Filtering:

Go to analyze, select conversation filter.



From here select any conversational filter for showing off specific traffic.

Ethernet filter



The conversation of ethernet follows ARP communication protocols.

IPv4 filter

The conversation of IPv4 follows TCP, & HTTP communication protocols.

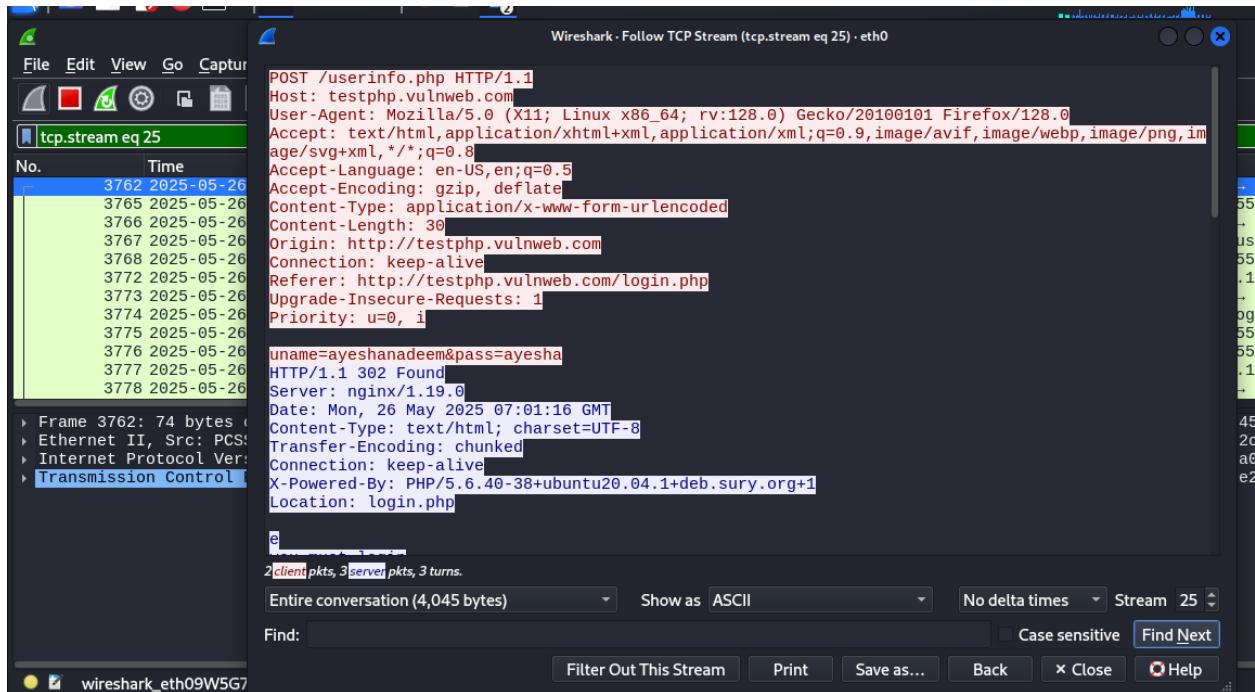
11. TCP Stream:

Right click on any **TCP** packet. Select **follow** and click on **TCP stream**

The screenshot shows the Wireshark interface with a context menu open over a selected packet (packet 3762). The menu items are:

- Mark/Unmark Selected
- Ignore/Unignore Selected
- Set/Unset Time Reference
- Time Shift...
- Packet Comments
- Edit Resolved Name
- Apply as Filter
- Prepare as Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow** (highlighted with a red box)
- Copy
- Protocol Preferences
- Decode As...
- Show Packet in New Window

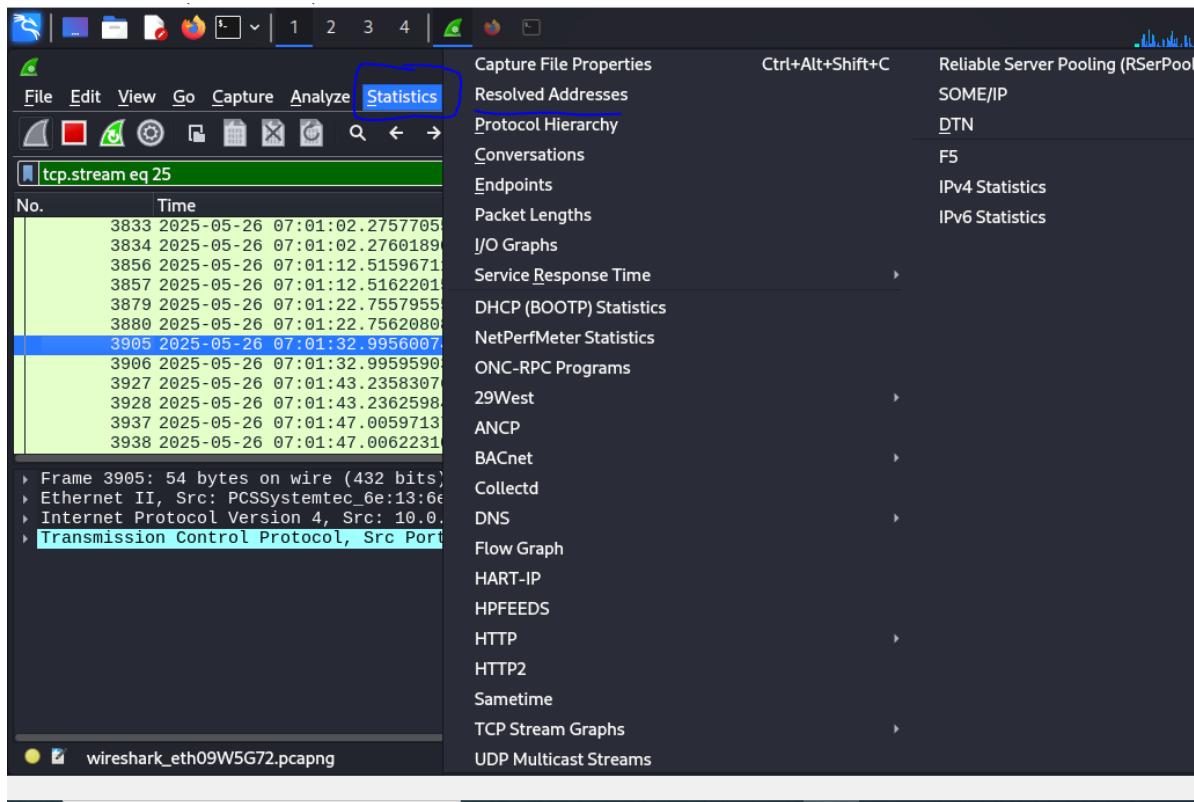
Below the menu, the TCP Stream for this connection is displayed, also highlighted with a red box.



12. Statistic in Wireshark:

To see the list of IP's and DNS resolved:

→ Go to statistic, select resolved addresses



Wireshark - Resolved Addresses - /tmp/wireshark_eth0Nfal72.pcapng

Hosts Ports Capture File Comments

Search for entry (min 3 characters) All entries

Address	Name
2a00:1450:4018:80a::200a	ogads-pa.clients6.google.com
2a00:1450:4018:802::200a	ogads-pa.clients6.google.com
192.178.24.142	play.google.com
192.178.24.174	play.google.com
142.250.201.142	play.google.com
2a00:1450:4018:803::200e	play.google.com
192.178.24.170	safebrowsing.googleapis.com
142.250.201.138	safebrowsing.googleapis.com
44.228.249.3	testphp.vulnweb.com

Close

Statistic of http:

Capture File Properties Ctrl+Alt+Shift+C Reliable Server Pooling (RSerPool)

Resolved Addresses SOME/IP DTN

Protocol Hierarchy F5

Conversations IPv4 Statistics

Endpoints IPv6 Statistics

Packet Lengths

I/O Graphs

Service Response Time

DHCP (BOOTP) Statistics

NetPerfMeter Statistics

ONC-RPC Programs

29West

ANCP

BACnet

Collectd

DNS

Flow Graph

HART-IP

HPFEEDS

HTTP

HTTP2

Sametime

TCP Stream Graphs

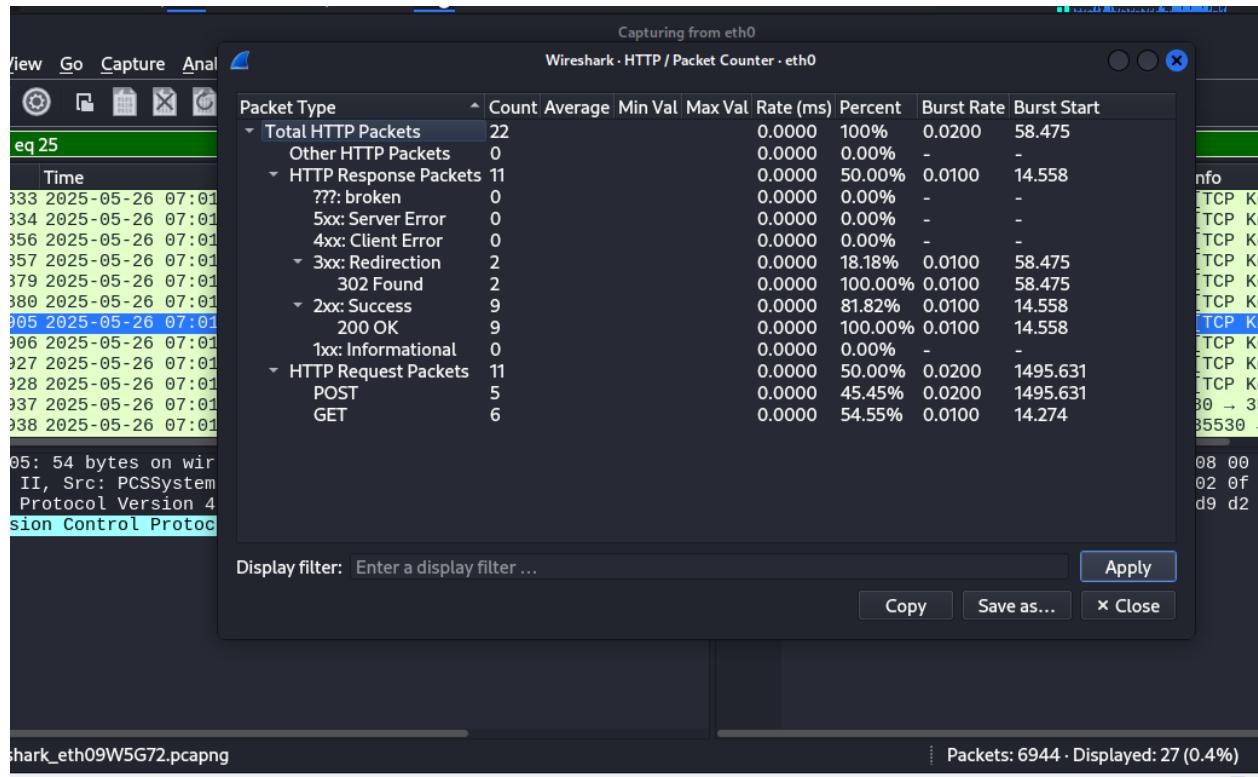
UDP Multicast Streams

Frame 3905: 54 bytes on wire (432 bits)
Ethernet II, Src: PCSSystemtec_6e:13:6e
Internet Protocol Version 4, Src: 10.0.0.11
Transmission Control Protocol, Src Port: 50000 (TCP), Dst Port: 80 (HTTP)

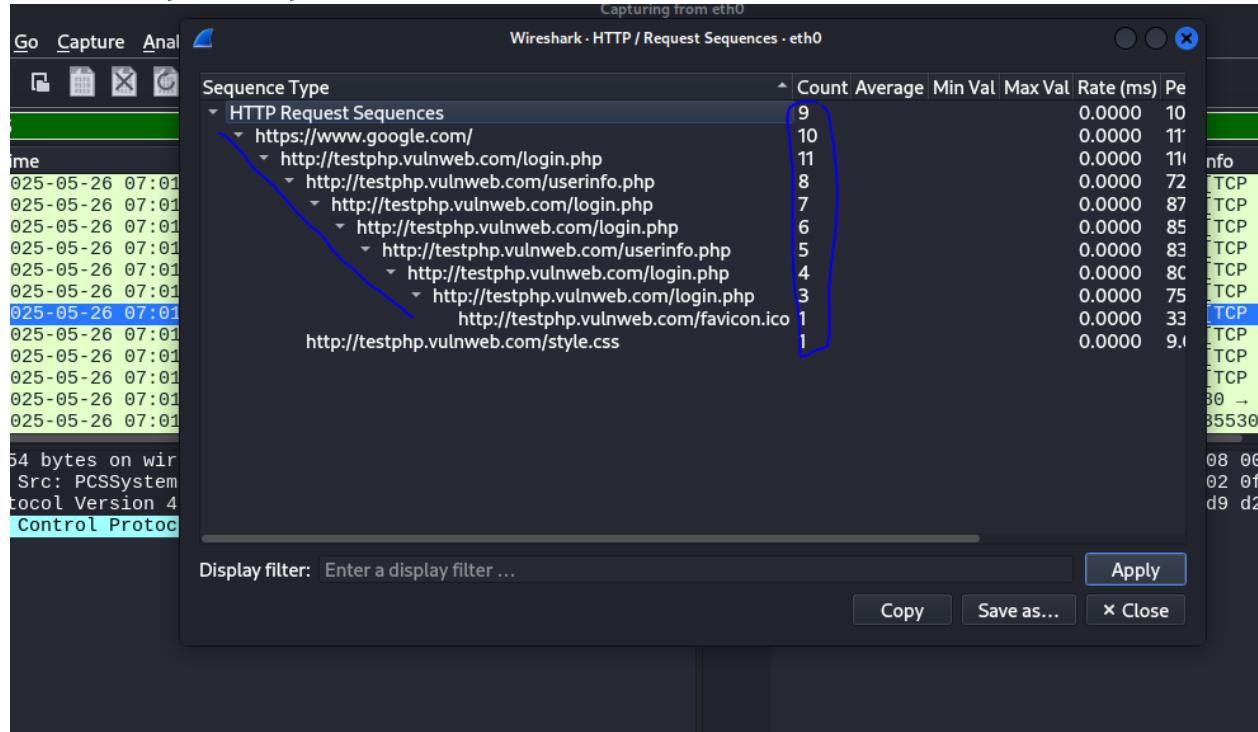
Packet Counter Requests Load Distribution Request Sequences

wireshark_eth0W5G72.pcapng

Packet counter:



HTTP Request sequences:



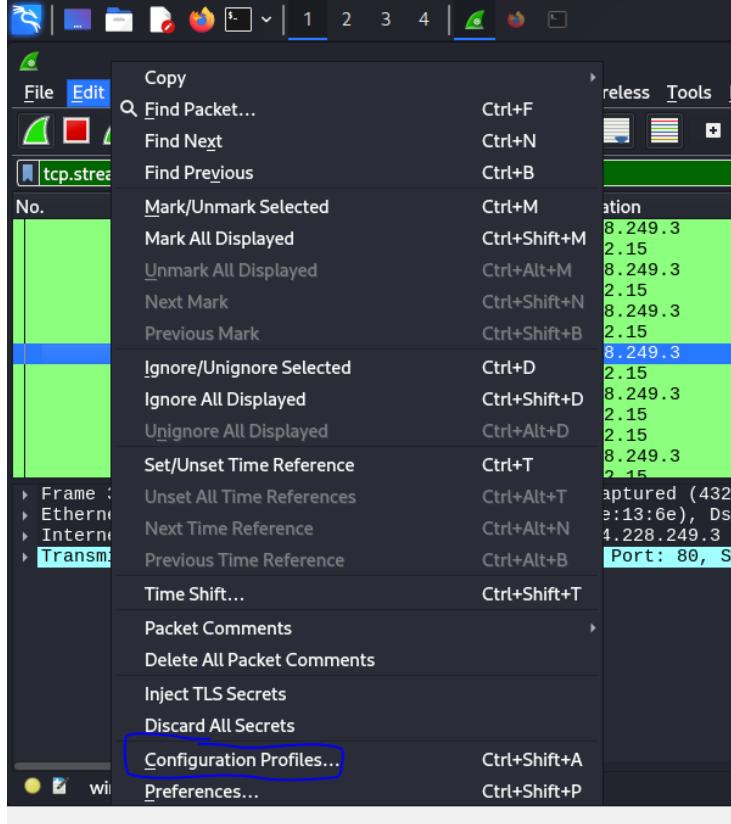
DNS Statistics:

The screenshot shows two instances of Wireshark running side-by-side. The top window displays the 'Statistics' menu, which is open to the 'DNS' section. The 'DNS' section contains various statistics such as 'Total Packets' (75), 'rcode' (75), 'opcodes' (75), 'Service Stats' (0), 'Response Stats' (0), 'Response' (75), and 'Query Type' (75). The bottom window shows the main Wireshark interface with the title 'Wireshark - DNS - eth0'. It displays a list of DNS packets with columns for 'Count', 'Average', 'Min Val', 'Max Val', 'Rate (ms)', 'Percent', 'Burst Rate', and 'Burst'. The first few rows show 'Total Packets' (75), 'rcode' (75), 'opcodes' (75), 'Service Stats' (0), 'Response Stats' (0), 'Response' (75), and 'Query Type' (75). The packet list shows several DNS queries and responses, with some entries highlighted in blue.

Packet Type	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst
Total Packets	75				0.0000	100%	0.1100	45.19%
rcode	75				0.0000	100%	0.0200	306.7
Server failure	2				0.0000	2.67%	0.1100	45.19%
No error	73				0.0000	97.33%	0.1100	45.19%
opcodes	75				0.0000	100%	0.1100	45.19%
Standard query	75				0.0000	100.00%	0.1100	45.19%
Service Stats	0				0.0000	100%	-	-
request-response time (msec)	37	187.50	1.079570	5837.075195	0.0000		0.0500	45.19%
no. of unsolicited responses	0				0.0000		-	-
no. of retransmissions	0				0.0000		-	-
Response Stats	0				0.0000	100%	-	-
no. of questions	74	1.00	1	1	0.0000		0.1000	45.19%
no. of authorities	74	0.11	0	1	0.0000		0.1000	45.19%
no. of answers	74	1.16	0	4	0.0000		0.1000	45.19%
no. of additionals	74	0.00	0	0	0.0000		0.1000	45.19%
Response	75				0.0000	100%	0.1100	45.19%
Response	37				0.0000	49.33%	0.0500	45.19%
Query	38				0.0000	50.67%	0.0600	45.19%
Query Type	75				0.0000	100%	0.1100	45.19%

13. Configuration Profile:

→ Go to Edit and Select Configuration file

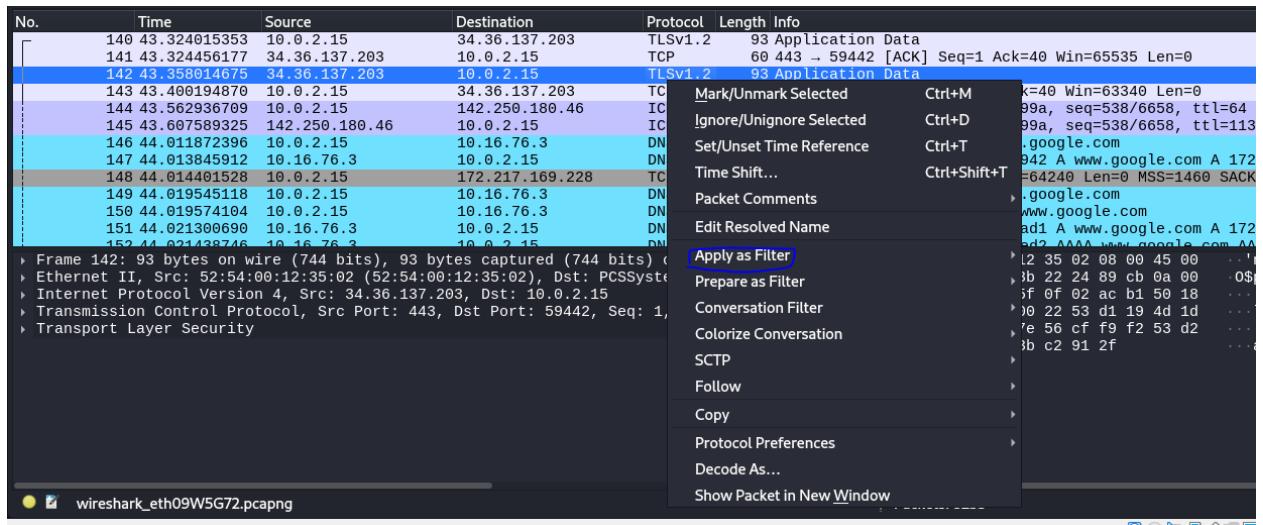


→ Variate packet into unique color to easy and quick analysis:

No.	Time	Source	Destination	Protocol	Length	Info
1378	91.136742256	142.250.180.46	10.0.2.15	ICMP	98	Echo (ping) reply id=0x099a, seq=4084/62479, ttl=113 (req)
1379	91.500690813	10.0.2.15	142.250.180.46	TCP	54	[TCP Keep-Alive] 60186 → 80 [ACK] Seq=376 Ack=966 Win=63275 L
1380	91.501255428	142.250.180.46	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 60186 [ACK] Seq=966 Ack=377 Win=655
1381	91.562035546	44.228.249.3	10.0.2.15	TCP	60	80 → 54646 [FIN, ACK] Seq=5773 Ack=1463 Win=65535 Len=0
1382	91.562221079	10.0.2.15	44.228.249.3	TCP	54	54646 → 80 [FIN, ACK] Seq=1463 Ack=5774 Win=65535 Len=0
1383	91.562523995	44.228.249.3	10.0.2.15	TCP	60	80 → 54646 [ACK] Seq=5774 Ack=1464 Win=65535 Len=0
1384	92.092166468	10.0.2.15	142.250.180.46	ICMP	98	Echo (ping) request id=0x099a, seq=4085/62735, ttl=64 (reply)
1385	92.137188926	142.250.180.46	10.0.2.15	ICMP	98	Echo (ping) reply id=0x099a, seq=4085/62735, ttl=113 (req)
1386	93.092529644	10.0.2.15	142.250.180.46	ICMP	98	Echo (ping) request id=0x099a, seq=4086/62991, ttl=64 (reply)
1387	93.137851786	142.250.180.46	10.0.2.15	ICMP	98	Echo (ping) reply id=0x099a, seq=4086/62991, ttl=113 (req)
1388	94.093172430	10.0.2.15	142.250.180.46	ICMP	98	Echo (ping) request id=0x099a, seq=4087/63247, ttl=64 (reply)
1389	94.138447484	142.250.180.46	10.0.2.15	ICMP	98	Echo (ping) reply id=0x099a, seq=4087/63247, ttl=113 (req)
1390	95.093414555	10.0.2.15	142.250.180.46	ICMP	98	Echo (ping) request id=0x099a, seq=4088/63250, ttl=64 (reply)
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0 at 00:00:27:0e:13:6e (PCSSystemtec_6e:13:6e) (Ethernet II, Src: PCSSystemtec_6e:13:6e (00:00:27:0e:13:6e), Dst: 52:54:00:1c:4e:40 (eth0)) at 00:00:27:0e:13:6e [ether]						
Ethernet II, Src: PCSSystemtec_6e:13:6e (00:00:27:0e:13:6e), Dst: 52:54:00:1c:4e:40 (eth0) [ether]						
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.180.46 [inet]						
Internet Control Message Protocol [icmp]						

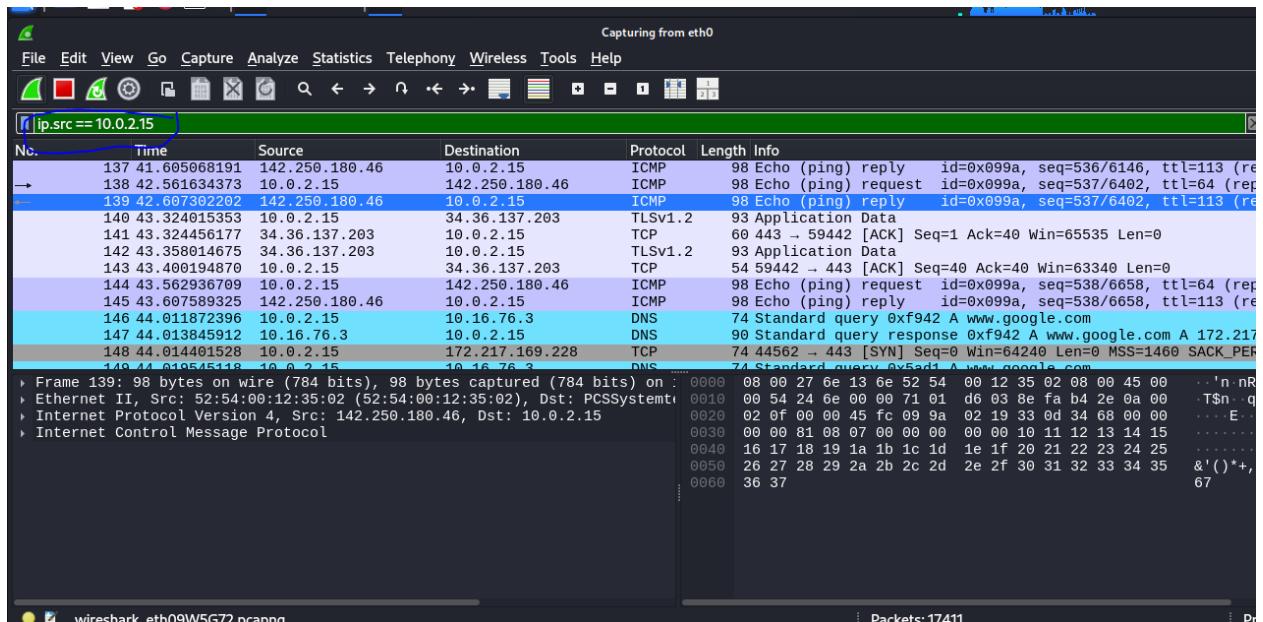
Target a specific IP:

→ Right click on any packet and select apply as filter



So this is showing you the packets of 10.0.2.15

- ICMP packet in purple color
- DNS packet in blue color
- TLS packet in light purple color



A blend of Nmap & Wireshark:

What ping command actually do?

```
└─(ayeshanadeem㉿ayeshanadeem)-[~]
$ ping cinesagerecommender.vercel.app
PING cinesagerecommender.vercel.app (216.198.79.1) 56(84) bytes of data.
64 bytes from 216.198.79.1: icmp_seq=7 ttl=245 time=93.7 ms
64 bytes from 216.198.79.1: icmp_seq=7 ttl=245 time=93.7 ms (DUP!)
64 bytes from 216.198.79.1: icmp_seq=7 ttl=245 time=119 ms (DUP!)
64 bytes from 216.198.79.1: icmp_seq=8 ttl=245 time=80.2 ms
64 bytes from 216.198.79.1: icmp_seq=9 ttl=245 time=71.8 ms
64 bytes from 216.198.79.1: icmp_seq=10 ttl=245 time=81.5 ms
64 bytes from 216.198.79.1: icmp_seq=11 ttl=245 time=122 ms
64 bytes from 216.198.79.1: icmp_seq=12 ttl=245 time=76.6 ms
```

The answer is, it only send an ICMP echo request just to check either host is up or down.

6224 2615.7609714...	192.168.104.87	216.198.79.1	ICMP	98 Echo (ping) request	id=0x87fa, seq=115/29440, ttl=64 (reply in 6225)
6225 2615.8309966...	216.198.79.1	192.168.104.87	ICMP	98 Echo (ping) reply	id=0x87fa, seq=115/29440, ttl=245 (request in 6224)
6226 2616.7622219...	192.168.104.87	216.198.79.1	ICMP	98 Echo (ping) request	id=0x87fa, seq=116/29696, ttl=64 (reply in 6227)
6227 2616.8301203...	216.198.79.1	192.168.104.87	ICMP	98 Echo (ping) reply	id=0x87fa, seq=116/29696, ttl=245 (request in 6226)
6228 2617.7638648...	192.168.104.87	216.198.79.1	ICMP	98 Echo (ping) request	id=0x87fa, seq=117/29952, ttl=64 (reply in 6229)
6229 2617.8401835...	216.198.79.1	192.168.104.87	ICMP	98 Echo (ping) reply	id=0x87fa, seq=117/29952, ttl=245 (request in 6228)
6230 2618.7654018...	192.168.104.87	216.198.79.1	ICMP	98 Echo (ping) request	id=0x87fa, seq=118/30208, ttl=64 (reply in 6231)
6231 2618.8430260...	216.198.79.1	192.168.104.87	ICMP	98 Echo (ping) reply	id=0x87fa, seq=118/30208, ttl=245 (request in 6230)
6232 2619.7676137...	192.168.104.87	216.198.79.1	ICMP	98 Echo (ping) request	id=0x87fa, seq=119/30464, ttl=64 (reply in 6233)
6233 2619.8475248...	216.198.79.1	192.168.104.87	ICMP	98 Echo (ping) reply	id=0x87fa, seq=119/30464, ttl=245 (request in 6232)

TCP three way handshake illustration using nmap command

```
└─(ayeshanadeem㉿ayeshanadeem)-[~]
$ nmap cinesagerecommender.vercel.app
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 10:34 EDT
Nmap scan report for cinesagerecommender.vercel.app (216.198.79.65)
Host is up (0.086s latency).

Other addresses for cinesagerecommender.vercel.app (not scanned): 64.29.17.65
Not shown: 998 filtered tcp ports (no-response) [progress]
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 8.44 seconds
```

Wireshark output:

28 3.146808270	192.168.104.87	216.198.79.193	ICMP	42 Echo (ping) request id=0xe2f0, seq=0/0, ttl=52 (no response found!)	
29 3.147175181	192.168.104.87	216.198.79.193	TCP	58 58063 - 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
30 3.147372151	192.168.104.87	216.198.79.193	TCP	54 58063 - 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0	
31 3.147546414	192.168.104.87	216.198.79.193	ICMP	54 Timestamp request id=0x49a0, seq=0/0, ttl=46	
32 3.229122753	216.198.79.193	192.168.104.87	TCP	60 443 - 58063 [TSYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1388	
33 3.229186875	192.168.104.87	216.198.79.193	TCP	54 58063 - 443 [RST] Seq=1 Win=0 Len=0	
34 3.267876193	192.168.104.87	192.168.104.112	DNS	87 Standard query 0xc002 PTR 193.79.198.216.in-addr.arpa	