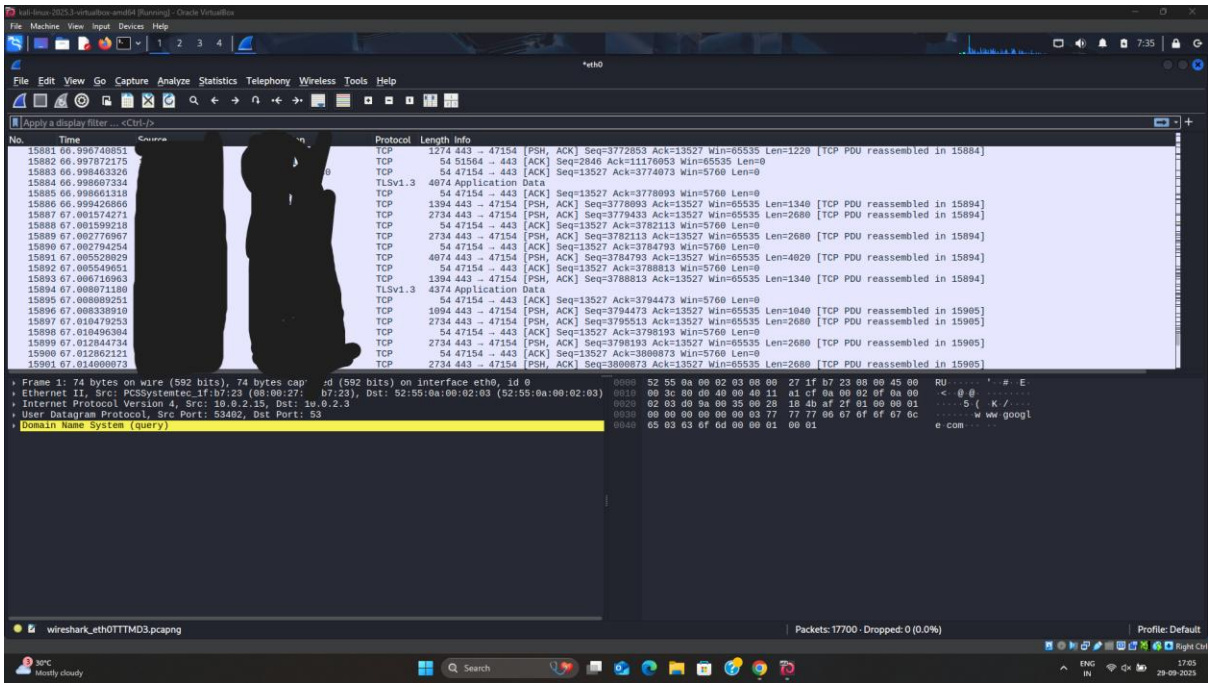
❖ **Hint:- 1 install Wireshark.**

❖ **Hint:- 2 capture packets.**

- **First open Wireshark.**
- **Click on start button.**
- **Browse the website.**

❖ **Hint :- 3 .Browse a website or ping a server to generate traffic.**

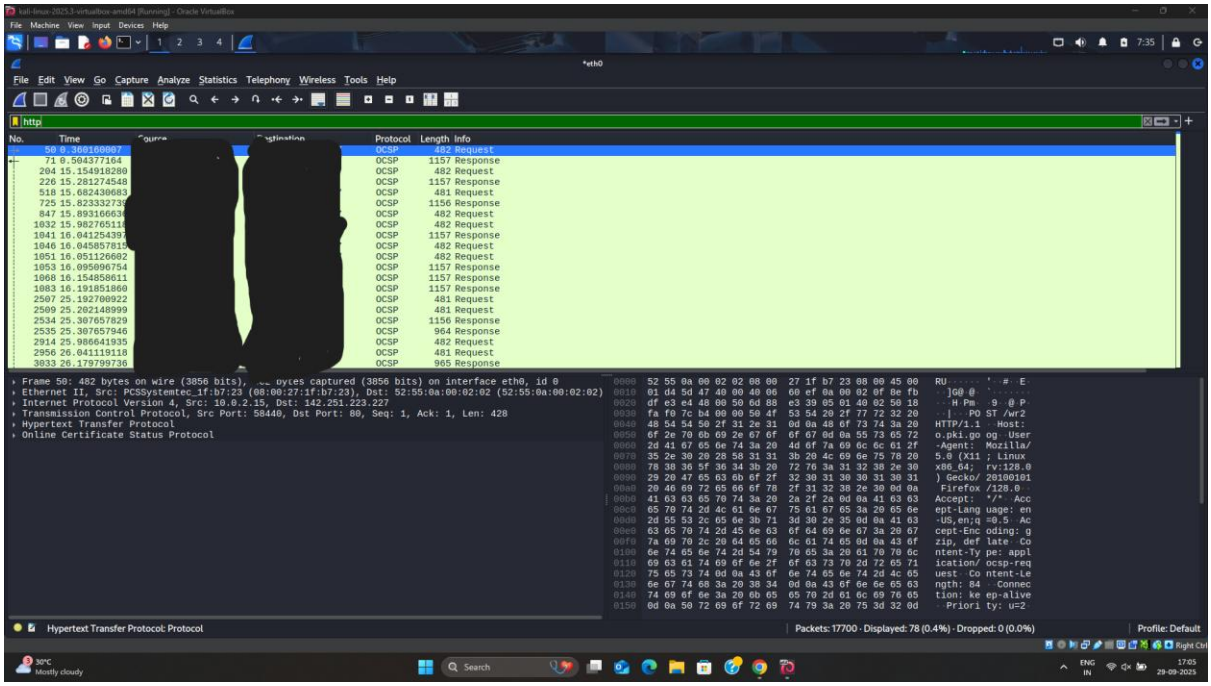


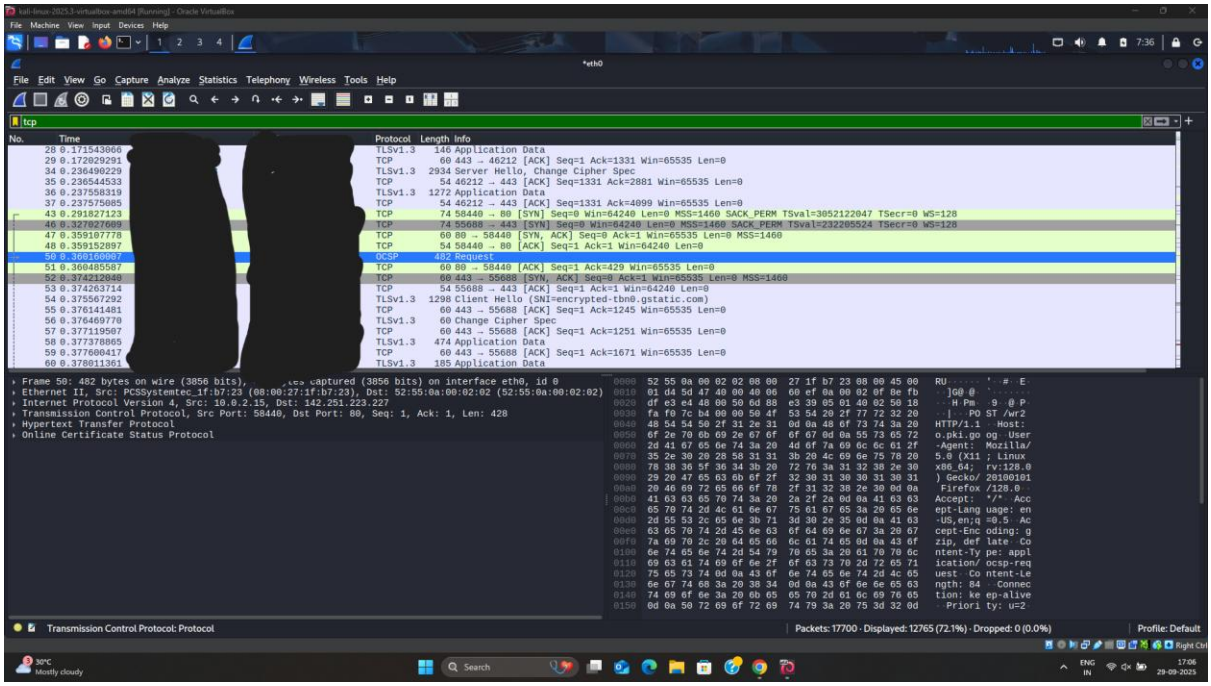
❖ **Hint:- 4 Stop capture after a minute.**

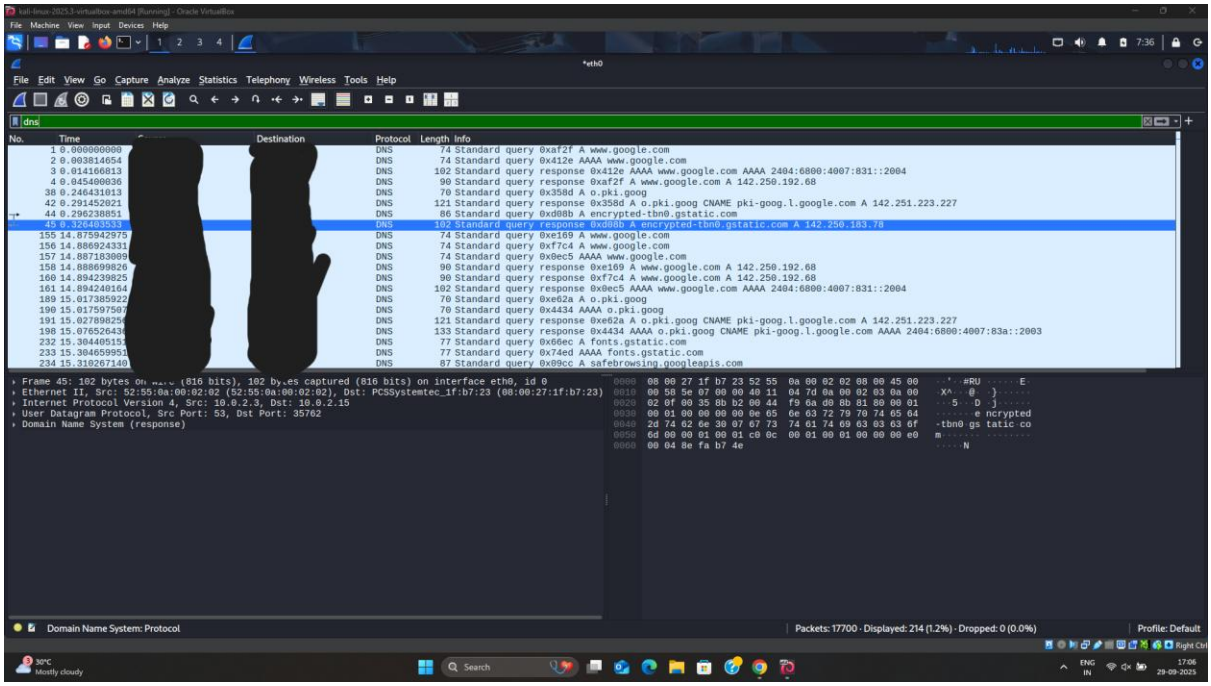
❖ **Hint:- 5 Filter captured packets by protocol (e.g., HTTP, DNS, TCP).**

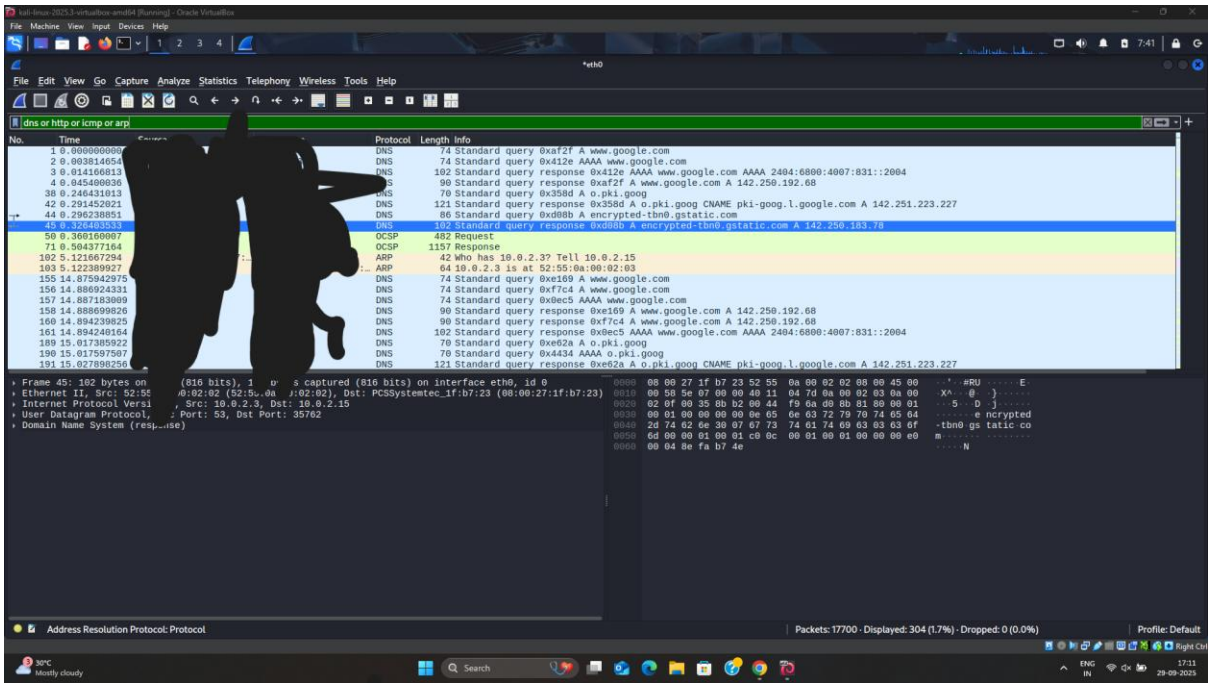
❖ **Hint:- 6 Identify at least 3 different protocols in the capture (e.g., HTTP, DNS, TCP).**

- **Packet filter. You can filter packet.in apply filter option below the start option you can see in screen shot.**


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
50 0.360160067 OCSP 482 Request
71 0.504377164 OCSP 1157 Response
204 15.154918280 OCSP 482 Request
226 15.281274548 OCSP 1157 Response
518 15.682430683 OCSP 481 Request
725 15.823332736 OCSP 1156 Response
847 15.893166636 OCSP 482 Request
1032 15.982765110 OCSP 482 Request
1041 16.041254397 OCSP 1157 Response
1046 16.045857814 OCSP 482 Request
1051 16.051126602 OCSP 482 Request
1053 16.095096754 OCSP 1157 Response
1068 16.154858611 OCSP 1157 Response
1083 16.191851860 OCSP 1157 Response
2507 25.192700922 OCSP 481 Request
2509 25.202148999 OCSP 481 Request
2534 25.307657829 OCSP 1156 Response
2535 25.307657946 OCSP 964 Response
2914 25.986641935 OCSP 482 Request
2956 26.041119118 OCSP 481 Request
3033 26.179799736 OCSP 965 Response
Frame 50: 482 bytes on wire (3856 bits), bytes captured (3856 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.251.223.227
Transmission Control Protocol, Src Port: 58440, Dst Port: 80, Seq: 1, Ack: 1, Len: 428
Hypertext Transfer Protocol
Online Certificate Status Protocol
Hypertext Transfer Protocol: Protocol
Packets: 17700 · Displayed: 78 (0.4%) · Dropped: 0 (0.0%)
Profile: Default


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
28 0.171543066 TLSv1.3 146 Application Data
29 0.172029291 TCP 60 443 → 46212 [ACK] Seq=1 Ack=1331 Win=65535 Len=0
34 0.236490229 TLSv1.3 2934 Server Hello, Change Cipher Spec
35 0.236544533 TCP 54 46212 → 443 [ACK] Seq=1331 Ack=2881 Win=65535 Len=0
36 0.237558319 TLSv1.3 1272 Application Data
37 0.237575085 TCP 54 46212 → 443 [ACK] Seq=1331 Ack=4099 Win=65535 Len=0
43 0.291827123 TCP 74 58440 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3052122047 TSecr=0 WS=128
46 0.327027699 TCP 74 55688 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=232265524 TSecr=0 WS=128
47 0.359107778 TCP 60 80 → 58440 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
48 0.359152897 TCP 54 58440 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
50 0.360160067 OCSP 482 Request
51 0.360485587 TCP 60 80 → 58440 [ACK] Seq=1 Ack=429 Win=65535 Len=0
52 0.374212840 TCP 60 443 → 55688 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
53 0.374263714 TCP 54 55688 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
54 0.375567292 TLSv1.3 1298 Client Hello (SNI=encrypted-tbn0.gstatic.com)
55 0.376141481 TCP 60 443 → 55688 [ACK] Seq=1 Ack=1245 Win=65535 Len=0
56 0.376469770 TLSv1.3 60 Change Cipher Spec
57 0.377119507 TCP 60 443 → 55688 [ACK] Seq=1 Ack=1251 Win=65535 Len=0
58 0.377378865 TLSv1.3 474 Application Data
59 0.377600417 TCP 60 443 → 55688 [ACK] Seq=1 Ack=1671 Win=65535 Len=0
60 0.378011361 TLSv1.3 185 Application Data
Frame 50: 482 bytes on wire (3856 bits), bytes captured (3856 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.251.223.227
Transmission Control Protocol, Src Port: 58440, Dst Port: 80, Seq: 1, Ack: 1, Len: 428
Hypertext Transfer Protocol
Online Certificate Status Protocol
Transmission Control Protocol: Protocol
Packets: 17700 · Displayed: 12765 (72.1%) · Dropped: 0 (0.0%)
Profile: Default


File Machine View Input Devices Help
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Destination Protocol Length Info
1 0.000000000 DNS 74 Standard query 0xaf2f A www.google.com
2 0.003814654 DNS 74 Standard query 0x412e AAAA www.google.com
3 0.014166813 DNS 102 Standard query response 0x412e AAAA www.google.com AAAA 2404:6800:4007:831::2004
4 0.045400036 DNS 90 Standard query response 0xaf2f A www.google.com A 142.250.192.68
38 0.246431013 DNS 70 Standard query 0x358d A o.pki.goog
42 0.291452021 DNS 121 Standard query response 0x358d A o.pki.goog CNAME pki-goog.l.google.com A 142.251.223.227
44 0.296238851 DNS 86 Standard query 0xd08b A encrypted-tbn0.gstatic.com
45 0.326403533 DNS 102 Standard query response 0xd08b A encrypted-tbn0.gstatic.com A 142.250.183.78
155 14.875942975 DNS 74 Standard query 0xe169 A www.google.com
156 14.886924331 DNS 74 Standard query 0xf7c4 A www.google.com
157 14.887183009 DNS 74 Standard query 0x0ec5 AAAA www.google.com
158 14.888699826 DNS 90 Standard query response 0xe169 A www.google.com A 142.250.192.68
160 14.894239825 DNS 90 Standard query response 0xf7c4 A www.google.com A 142.250.192.68
161 14.894240164 DNS 102 Standard query response 0x0ec5 AAAA www.google.com AAAA 2404:6800:4007:831::2004
189 15.017385922 DNS 70 Standard query 0xe62a A o.pki.goog
190 15.017597507 DNS 70 Standard query 0x4434 AAAA o.pki.goog
191 15.027898256 DNS 121 Standard query response 0xe62a A o.pki.goog CNAME pki-goog.l.google.com A 142.251.223.227
198 15.076526430 DNS 133 Standard query response 0x4434 AAAA o.pki.goog CNAME pki-goog.l.google.com AAAA 2404:6800:4007:83a::2003
232 15.304405153 DNS 77 Standard query 0x66ec A fonts.gstatic.com
233 15.304659951 DNS 77 Standard query 0x74ed AAAA fonts.gstatic.com
234 15.310267140 DNS 87 Standard query 0x09cc A safebrowsing.googleapis.com
Frame 45: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface eth0, id 0
Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23)
Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53, Dst Port: 35762
Domain Name System (response)
0000 08 00 27 1f b7 23 52 55 0a 00 02 02 08 00 45 00
0010 00 58 5e 07 00 00 40 11 04 7d 0a 00 02 03 0a 00
0020 02 0f 00 35 8b b2 00 44 f9 6a d0 8b 81 80 00 01
0030 00 01 00 00 00 00 0e 65 6e 63 72 79 70 74 65 64
0040 2d 74 62 6e 30 07 67 73 74 61 74 69 63 03 63 6f
0050 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00 e0
0060 00 04 8e fa b7 4e
Domain Name System: Protocol
Packets: 17700 · Displayed: 214 (1.2%) · Dropped: 0 (0.0%)
Profile: Default
30°C Mostly cloudy
Search
ENG IN
17:06 29-09-2025


File Machine View Input Devices Help
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns or http or icmp or arp
No. Time Protocol Length Info
1 0.000000000 DNS 74 Standard query 0xaf2f A www.google.com
2 0.003814654 DNS 74 Standard query 0x412e AAAA www.google.com
3 0.014166813 DNS 102 Standard query response 0x412e AAAA www.google.com AAAA 2404:6800:4007:831::2004
4 0.045400036 DNS 90 Standard query response 0xaf2f A www.google.com A 142.250.192.68
38 0.246431013 DNS 70 Standard query 0x358d A o.pki.goog
42 0.291452021 DNS 121 Standard query response 0x358d A o.pki.goog CNAME pki-goog.l.google.com A 142.251.223.227
44 0.296238851 DNS 86 Standard query 0xd08b A encrypted-tbn0.gstatic.com
45 0.326403533 DNS 102 Standard query response 0xd08b A encrypted-tbn0.gstatic.com A 142.250.183.78
50 0.360160007 OCSP 482 Request
71 0.504377164 OCSP 1157 Response
102 5.121667294 ARP 42 Who has 10.0.2.3? Tell 10.0.2.15
103 5.122389927 ARP 64 10.0.2.3 is at 52:55:0a:00:02:03
155 14.875942975 DNS 74 Standard query 0xe169 A www.google.com
156 14.886924331 DNS 74 Standard query 0xf7c4 A www.google.com
157 14.887183009 DNS 74 Standard query 0x0ec5 AAAA www.google.com
158 14.888699826 DNS 90 Standard query response 0xe169 A www.google.com A 142.250.192.68
160 14.894239825 DNS 90 Standard query response 0xf7c4 A www.google.com A 142.250.192.68
161 14.894240164 DNS 102 Standard query response 0x0ec5 AAAA www.google.com AAAA 2404:6800:4007:831::2004
189 15.017385922 DNS 70 Standard query 0xe62a A o.pki.goog
190 15.017597507 DNS 70 Standard query 0x4434 AAAA o.pki.goog
191 15.027898256 DNS 121 Standard query response 0xe62a A o.pki.goog CNAME pki-goog.l.google.com A 142.251.223.227
Frame 45: 102 bytes on (816 bits), 1 s captured (816 bits) on interface eth0, id 0
Ethernet II, Src: 52:55 :02:02 (52:55:0a :02:02), Dst: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23)
Internet Protocol Versi , Src: 10.0.2.3, Dst: 10.0.2.15
User Datagram Protocol, Port: 53, Dst Port: 35762
Domain Name System (resp se)
0000 08 00 27 1f b7 23 52 55 0a 00 02 02 08 00 45 00
0010 00 58 5e 07 00 00 40 11 04 7d 0a 00 02 03 0a 00
0020 02 0f 00 35 8b b2 00 44 f9 6a d0 8b 81 80 00 01
0030 00 01 00 00 00 00 0e 65 6e 63 72 79 70 74 65 64
0040 2d 74 62 6e 30 07 67 73 74 61 74 69 63 03 63 6f
0050 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00 e0
0060 00 04 8e fa b7 4e
Address Resolution Protocol: Protocol
Packets: 17700 · Displayed: 304 (1.7%) · Dropped: 0 (0.0%)
Profile: Default
30°C Mostly cloudy
Search
ENG IN
17:11 29-09-2025