COMPUTER NETWORKS

SAKSHAM KUMAR

COMPUTER SCIENCE AND ENGINEERING
ID - 2022UCP1700
SECTION- A4

ASSIGNMENT – 9

Task 1: Installing Wireshark

• Download Wireshark from the provided link.

• Follow the installation instructions for your operating system.

• Ensure Wireshark is installed correctly by launching the application.

I downloaded Wireshark from the provided link and successfully installed it.

Task 2: Capturing Network Traffic

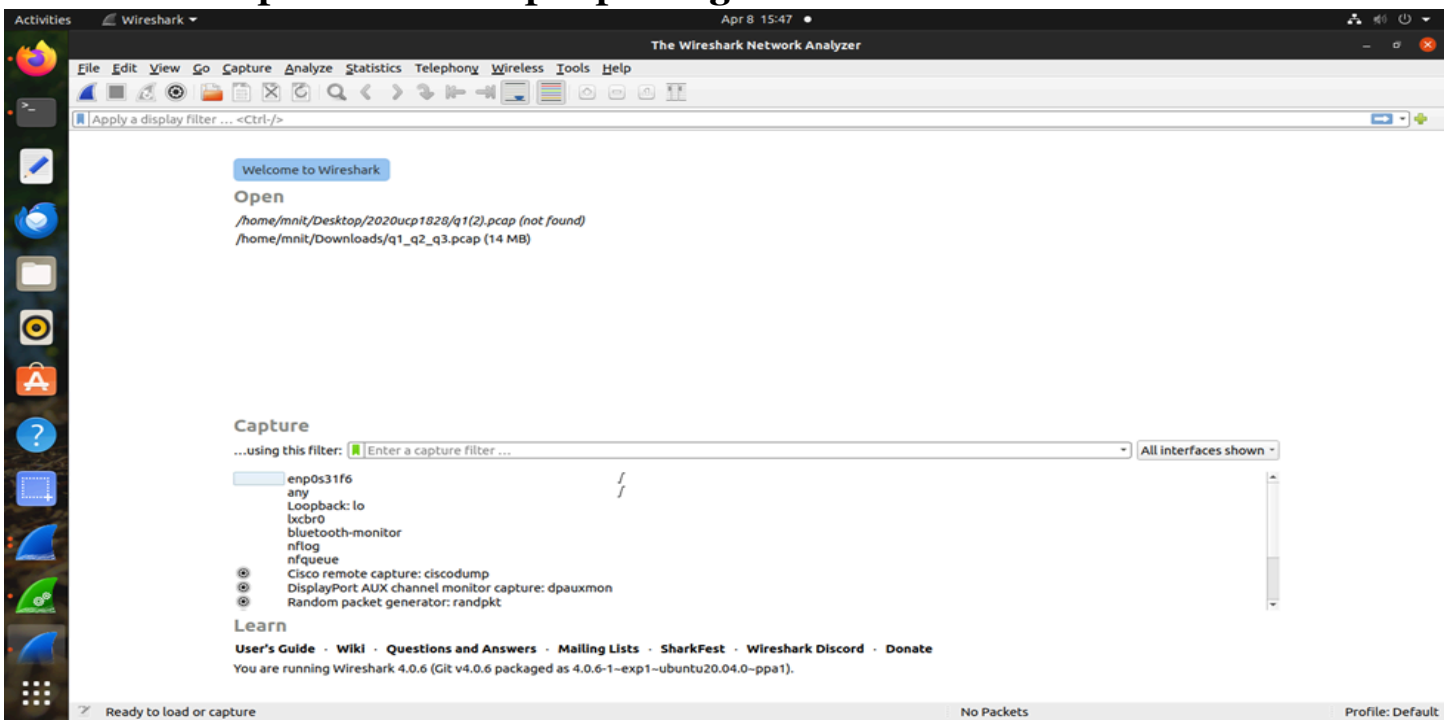
• Launch Wireshark.

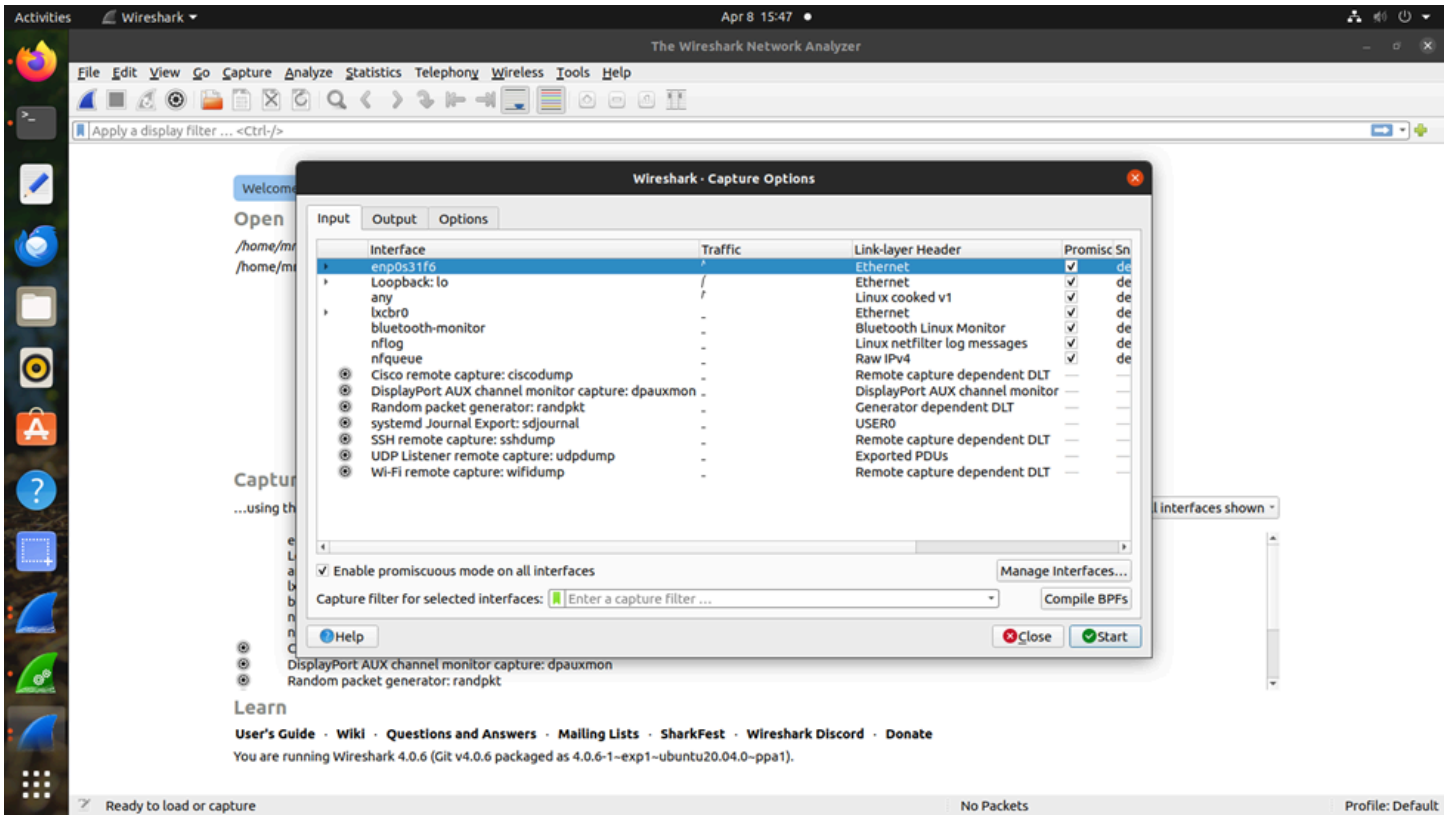
• Select the network interface through which you want to capture traffic (e.g., Wi-Fi, Ethernet).

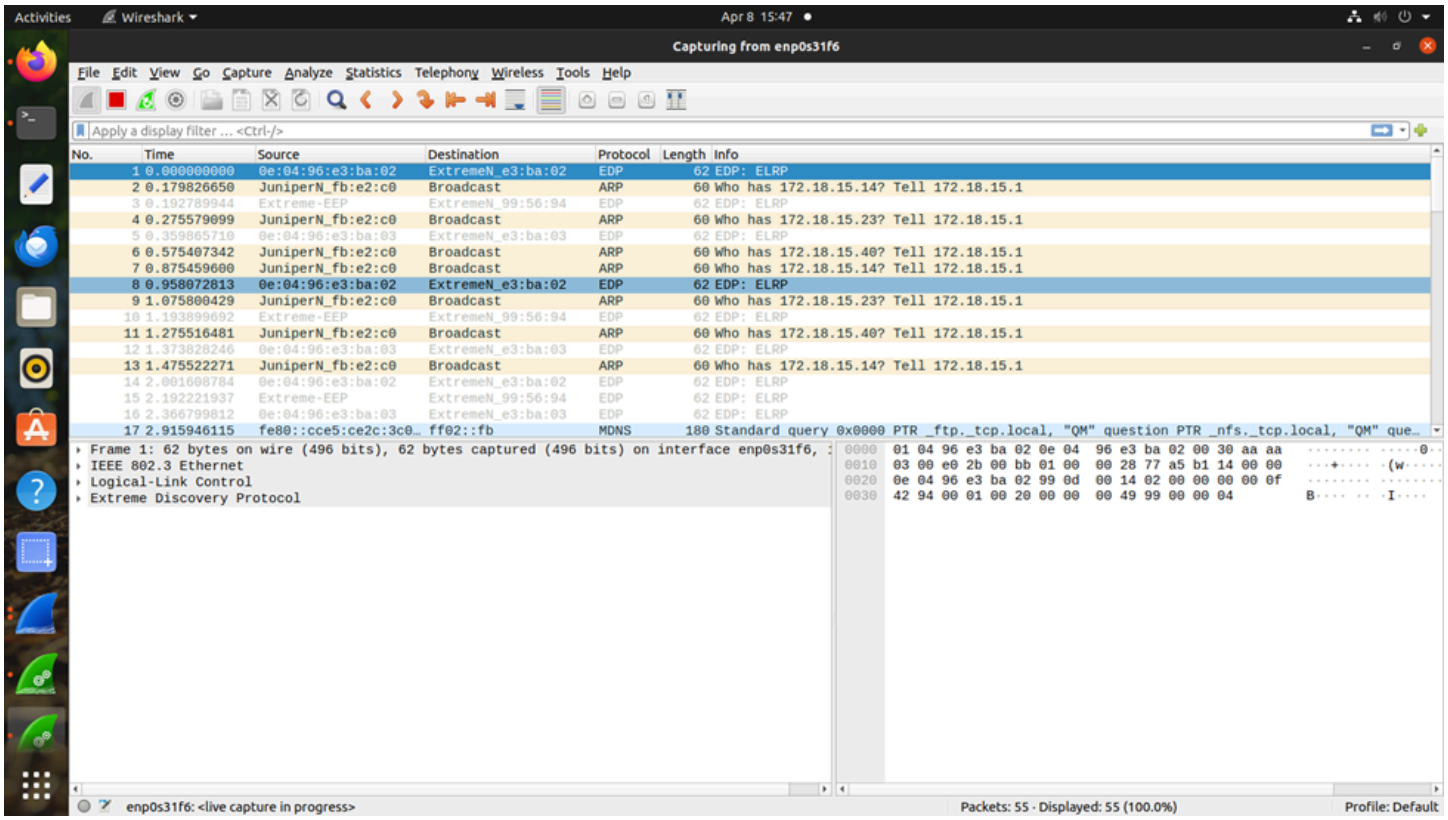
• Click on the green 'Start' button to begin capturing traffic.

• Perform various activities such as visiting websites, sending/receiving emails, or using applications that require network connectivity.

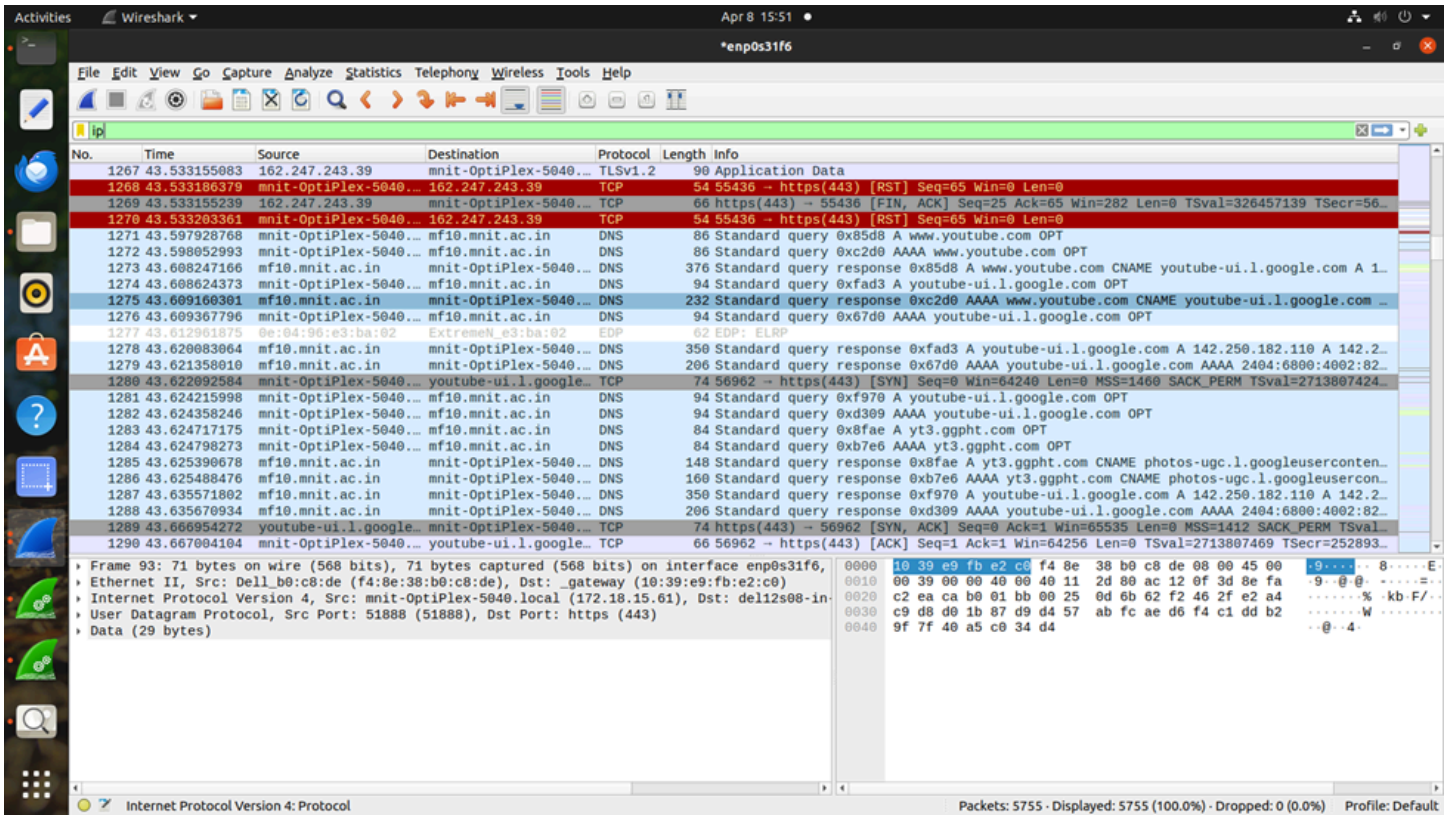
• After capturing traffic for a sufficient amount of time (at least 1 minute), click on the red 'Stop' button to stop capturing.





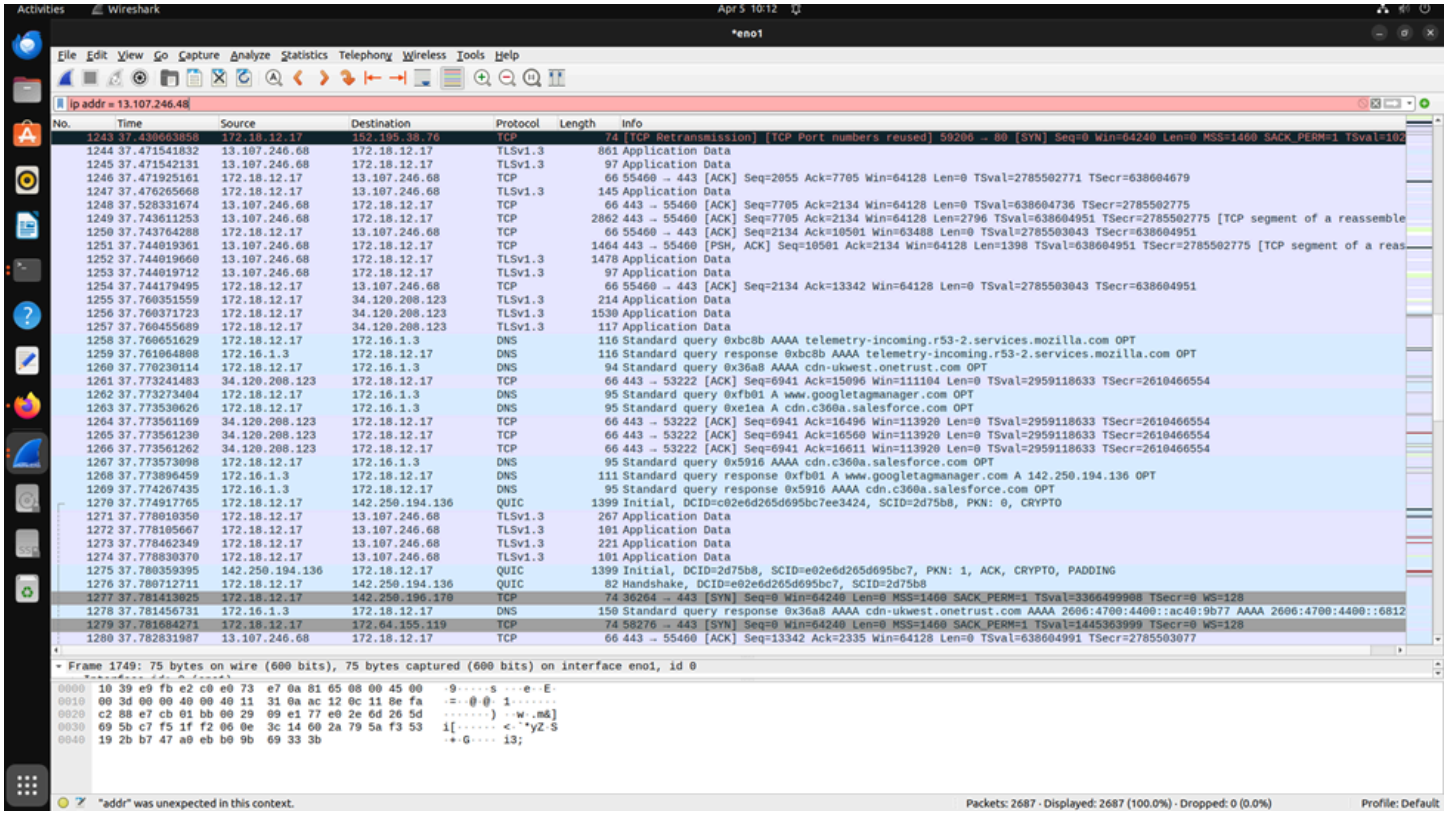


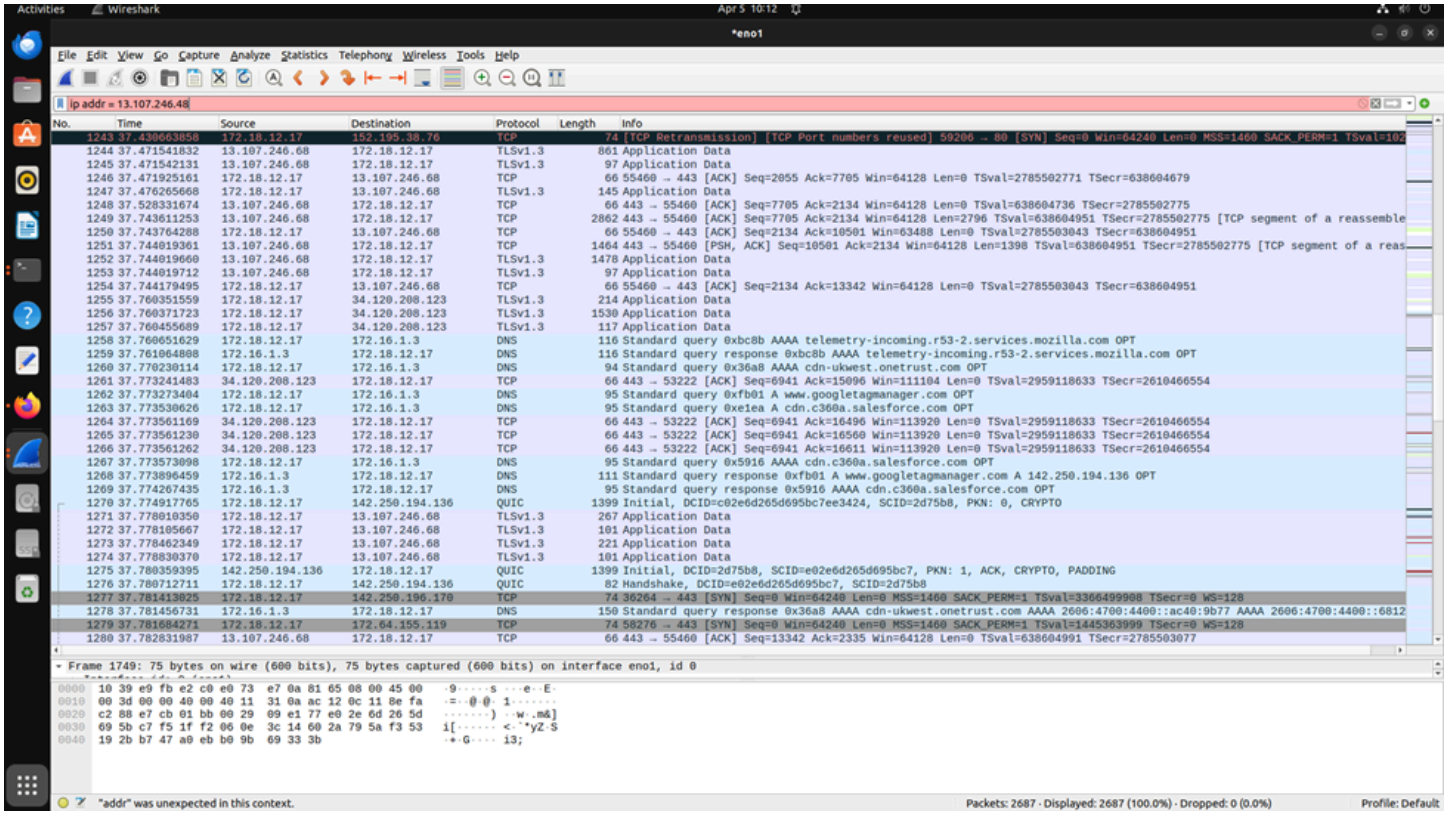
Then i visit youtube , and capture traffic for approx 1 minute



Task 3: Analysing Captured Traffic

- **Explore the captured packets in Wireshark.**
- **Identify different protocols used in the captured traffic (e.g., HTTP, TCP, UDP).**
- **Filter the captured packets based on specific protocols or criteria (e.g., HTTP traffic only, packets from a specific IP address).**
- **Analyse the contents of selected packets to understand the communication between devices.**
- **Take note of any suspicious or interesting findings during the analysis.**


Activities
Wireshark
Apr 5 10:12
*eno1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip addr = 13.107.246.48
No. Time Source Destination Protocol Length Info
1243 37.430663858 172.18.12.17 152.195.38.76 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 59206 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=102
1244 37.471541832 13.107.246.68 172.18.12.17 TLSv1.3 861 Application Data
1245 37.471542131 13.107.246.68 172.18.12.17 TLSv1.3 97 Application Data
1246 37.471925161 172.18.12.17 13.107.246.68 TCP 66 55460 → 443 [ACK] Seq=2055 Ack=7705 Win=64128 Len=0 TSval=2785502771 TSecr=638604679
1247 37.476265668 172.18.12.17 13.107.246.68 TLSv1.3 145 Application Data
1248 37.528331674 13.107.246.68 172.18.12.17 TCP 66 443 → 55460 [ACK] Seq=7705 Ack=2134 Win=64128 Len=0 TSval=638604736 TSecr=2785502775
1249 37.743611253 13.107.246.68 172.18.12.17 TCP 2862 443 → 55460 [ACK] Seq=7705 Ack=2134 Win=64128 Len=2796 TSval=638604951 TSecr=2785502775 [TCP segment of a reassemble
1250 37.743764288 172.18.12.17 13.107.246.68 TCP 66 55460 → 443 [ACK] Seq=2134 Ack=10501 Win=63488 Len=0 TSval=2785503043 TSecr=638604951
1251 37.744019361 13.107.246.68 172.18.12.17 TCP 1464 443 → 55460 [PSH, ACK] Seq=10501 Ack=2134 Win=64128 Len=1398 TSval=638604951 TSecr=2785502775 [TCP segment of a reas
1252 37.744019660 13.107.246.68 172.18.12.17 TLSv1.3 1478 Application Data
1253 37.744019712 13.107.246.68 172.18.12.17 TLSv1.3 97 Application Data
1254 37.744179495 172.18.12.17 13.107.246.68 TCP 66 55460 → 443 [ACK] Seq=2134 Ack=13342 Win=64128 Len=0 TSval=2785503043 TSecr=638604951
1255 37.760351559 172.18.12.17 34.120.208.123 TLSv1.3 214 Application Data
1256 37.760371723 172.18.12.17 34.120.208.123 TLSv1.3 1530 Application Data
1257 37.760455689 172.18.12.17 34.120.208.123 TLSv1.3 117 Application Data
1258 37.760651629 172.18.12.17 172.16.1.3 DNS 116 Standard query 0xbc8b AAAA telemetry-incoming.r53-2.services.mozilla.com OPT
1259 37.761064808 172.16.1.3 172.18.12.17 DNS 116 Standard query response 0xbc8b AAAA telemetry-incoming.r53-2.services.mozilla.com OPT
1260 37.770230114 172.18.12.17 172.16.1.3 DNS 94 Standard query 0x36a8 AAAA cdn-ukwest.onetrust.com OPT
1261 37.773241483 34.120.208.123 172.18.12.17 TCP 66 443 → 53222 [ACK] Seq=6941 Ack=15096 Win=111104 Len=0 TSval=2959118633 TSecr=2610466554
1262 37.773273404 172.18.12.17 172.16.1.3 DNS 95 Standard query 0xfb01 A www.googletagmanager.com OPT
1263 37.773530626 172.18.12.17 172.16.1.3 DNS 95 Standard query 0xe1ea A cdn.c360a.salesforce.com OPT
1264 37.773561169 34.120.208.123 172.18.12.17 TCP 66 443 → 53222 [ACK] Seq=6941 Ack=16496 Win=113920 Len=0 TSval=2959118633 TSecr=2610466554
1265 37.773561230 34.120.208.123 172.18.12.17 TCP 66 443 → 53222 [ACK] Seq=6941 Ack=16560 Win=113920 Len=0 TSval=2959118633 TSecr=2610466554
1266 37.773561262 34.120.208.123 172.18.12.17 TCP 66 443 → 53222 [ACK] Seq=6941 Ack=16611 Win=113920 Len=0 TSval=2959118633 TSecr=2610466554
1267 37.773573098 172.18.12.17 172.16.1.3 DNS 95 Standard query 0x5916 AAAA cdn.c360a.salesforce.com OPT
1268 37.773896459 172.16.1.3 172.18.12.17 DNS 111 Standard query response 0xfb01 A www.googletagmanager.com A 142.250.194.136 OPT
1269 37.774267435 172.16.1.3 172.18.12.17 DNS 95 Standard query response 0x5916 AAAA cdn.c360a.salesforce.com OPT
1270 37.774917765 172.18.12.17 142.250.194.136 QUIC 1399 Initial, DCID=c02e6d265d695bc7ee3424, SCID=2d75b8, PKN: 0, CRYPTO
1271 37.778010350 172.18.12.17 13.107.246.68 TLSv1.3 267 Application Data
1272 37.778105667 172.18.12.17 13.107.246.68 TLSv1.3 101 Application Data
1273 37.778462349 172.18.12.17 13.107.246.68 TLSv1.3 221 Application Data
1274 37.778830370 172.18.12.17 13.107.246.68 TLSv1.3 101 Application Data
1275 37.780359395 142.250.194.136 172.18.12.17 QUIC 1399 Initial, DCID=2d75b8, SCID=e02e6d265d695bc7, PKN: 1, ACK, CRYPTO, PADDING
1276 37.780712711 172.18.12.17 142.250.194.136 QUIC 82 Handshake, DCID=e02e6d265d695bc7, SCID=2d75b8
1277 37.781413025 172.18.12.17 142.250.196.170 TCP 74 36264 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3366499908 TSecr=0 WS=128
1278 37.781456731 172.16.1.3 172.18.12.17 DNS 150 Standard query response 0x36a8 AAAA cdn-ukwest.onetrust.com AAAA 2606:4700:4400::ac40:9b77 AAAA 2606:4700:4400::6812
1279 37.781684271 172.18.12.17 172.64.155.119 TCP 74 58276 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1445363999 TSecr=0 WS=128
1280 37.782831987 13.107.246.68 172.18.12.17 TCP 66 443 → 55460 [ACK] Seq=13342 Ack=2335 Win=64128 Len=0 TSval=638604991 TSecr=2785503077
Frame 1749: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface eno1, id 0
0000 10 39 e9 fb e2 c0 e0 73 e7 0a 81 65 08 00 45 00
0010 00 3d 00 00 40 00 40 11 31 0a ac 12 0c 11 8e fa
0020 c2 88 e7 cb 01 bb 00 29 09 e1 77 e0 2e 6d 26 5d
0030 69 5b c7 f5 1f f2 06 0e 3c 14 60 2a 79 5a f3 53
0040 19 2b b7 47 a0 eb b0 9b 69 33 3b
"addr" was unexpected in this context.
Packets: 2687 · Displayed: 2687 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

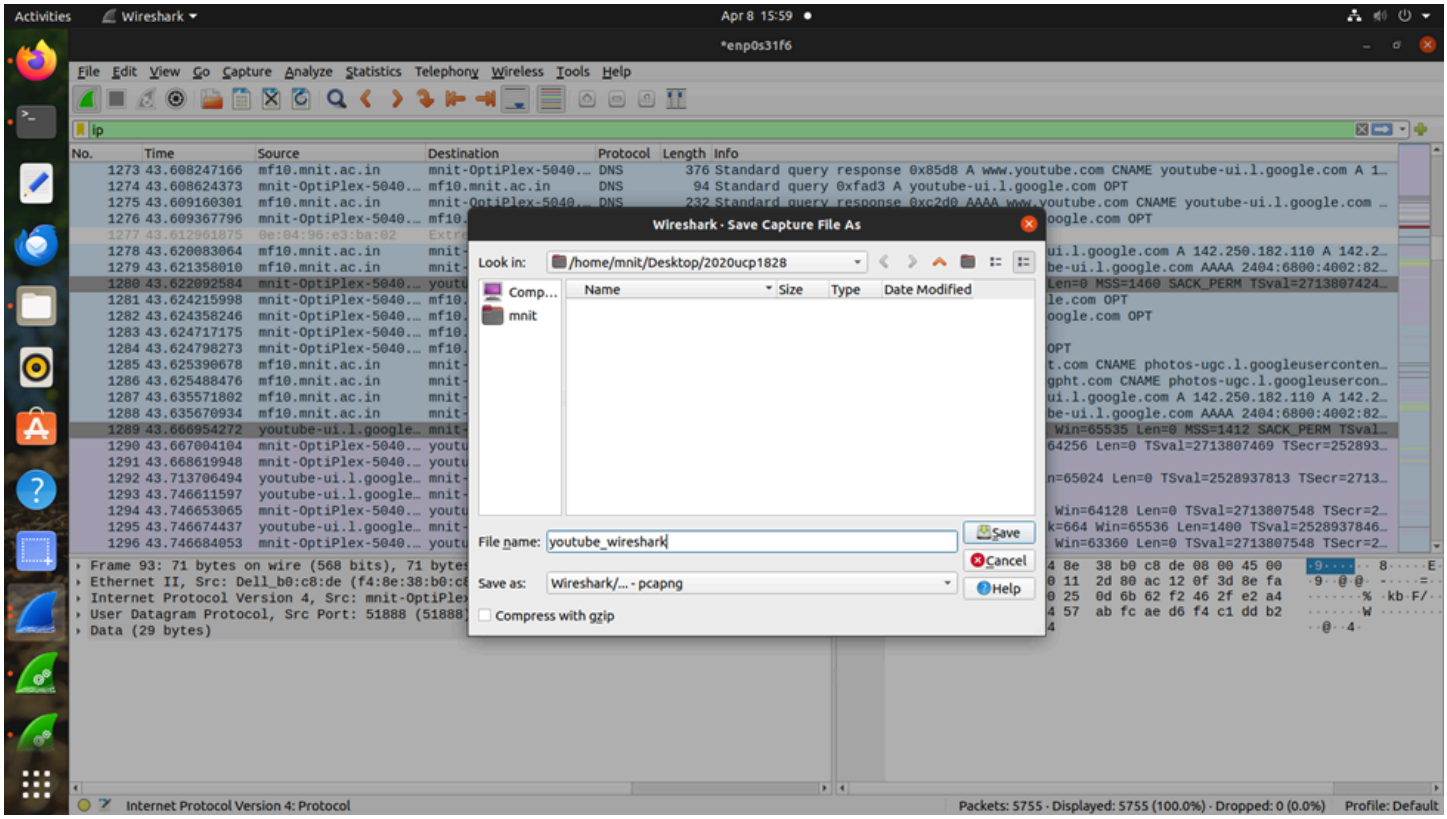

Activities
Wireshark
Apr 5 10:12
*eno1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip addr = 13.107.246.48
No. Time Source Destination Protocol Length Info
1243 37.430663858 172.18.12.17 152.195.38.76 TCP 74 [TCP Retransmission] [TCP Port numbers reused] 59206 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=102
1244 37.471541832 13.107.246.68 172.18.12.17 TLSv1.3 861 Application Data
1245 37.471542131 13.107.246.68 172.18.12.17 TLSv1.3 97 Application Data
1246 37.471925161 172.18.12.17 13.107.246.68 TCP 66 55460 → 443 [ACK] Seq=2055 Ack=7705 Win=64128 Len=0 TSval=2785502771 TSecr=638604679
1247 37.476265668 172.18.12.17 13.107.246.68 TLSv1.3 145 Application Data
1248 37.528331674 13.107.246.68 172.18.12.17 TCP 66 443 → 55460 [ACK] Seq=7705 Ack=2134 Win=64128 Len=0 TSval=638604736 TSecr=2785502775
1249 37.743611253 13.107.246.68 172.18.12.17 TCP 2862 443 → 55460 [ACK] Seq=7705 Ack=2134 Win=64128 Len=2796 TSval=638604951 TSecr=2785502775 [TCP segment of a reassemble
1250 37.743764288 172.18.12.17 13.107.246.68 TCP 66 55460 → 443 [ACK] Seq=2134 Ack=10501 Win=63488 Len=0 TSval=2785503043 TSecr=638604951
1251 37.744019361 13.107.246.68 172.18.12.17 TCP 1464 443 → 55460 [PSH, ACK] Seq=10501 Ack=2134 Win=64128 Len=1398 TSval=638604951 TSecr=2785502775 [TCP segment of a reas
1252 37.744019660 13.107.246.68 172.18.12.17 TLSv1.3 1478 Application Data
1253 37.744019712 13.107.246.68 172.18.12.17 TLSv1.3 97 Application Data
1254 37.744179495 172.18.12.17 13.107.246.68 TCP 66 55460 → 443 [ACK] Seq=2134 Ack=13342 Win=64128 Len=0 TSval=2785503043 TSecr=638604951
1255 37.760351559 172.18.12.17 34.120.208.123 TLSv1.3 214 Application Data
1256 37.760371723 172.18.12.17 34.120.208.123 TLSv1.3 1530 Application Data
1257 37.760455689 172.18.12.17 34.120.208.123 TLSv1.3 117 Application Data
1258 37.760651629 172.18.12.17 172.16.1.3 DNS 116 Standard query 0xbc8b AAAA telemetry-incoming.r53-2.services.mozilla.com OPT
1259 37.761064808 172.16.1.3 172.18.12.17 DNS 116 Standard query response 0xbc8b AAAA telemetry-incoming.r53-2.services.mozilla.com OPT
1260 37.770230114 172.18.12.17 172.16.1.3 DNS 94 Standard query 0x36a8 AAAA cdn-ukwest.onetrust.com OPT
1261 37.773241483 34.120.208.123 172.18.12.17 TCP 66 443 → 53222 [ACK] Seq=6941 Ack=15096 Win=111104 Len=0 TSval=2959118633 TSecr=2610466554
1262 37.773273404 172.18.12.17 172.16.1.3 DNS 95 Standard query 0xfb01 A www.googletagmanager.com OPT
1263 37.773530626 172.18.12.17 172.16.1.3 DNS 95 Standard query 0xe1ea A cdn.c360a.salesforce.com OPT
1264 37.773561169 34.120.208.123 172.18.12.17 TCP 66 443 → 53222 [ACK] Seq=6941 Ack=16496 Win=113920 Len=0 TSval=2959118633 TSecr=2610466554
1265 37.773561230 34.120.208.123 172.18.12.17 TCP 66 443 → 53222 [ACK] Seq=6941 Ack=16560 Win=113920 Len=0 TSval=2959118633 TSecr=2610466554
1266 37.773561262 34.120.208.123 172.18.12.17 TCP 66 443 → 53222 [ACK] Seq=6941 Ack=16611 Win=113920 Len=0 TSval=2959118633 TSecr=2610466554
1267 37.773573098 172.18.12.17 172.16.1.3 DNS 95 Standard query 0x5916 AAAA cdn.c360a.salesforce.com OPT
1268 37.773896459 172.16.1.3 172.18.12.17 DNS 111 Standard query response 0xfb01 A www.googletagmanager.com A 142.250.194.136 OPT
1269 37.774267435 172.16.1.3 172.18.12.17 DNS 95 Standard query response 0x5916 AAAA cdn.c360a.salesforce.com OPT
1270 37.774917765 172.18.12.17 142.250.194.136 QUIC 1399 Initial, DCID=c02e6d265d695bc7ee3424, SCID=2d75b8, PKN: 0, CRYPTO
1271 37.778010350 172.18.12.17 13.107.246.68 TLSv1.3 267 Application Data
1272 37.778105667 172.18.12.17 13.107.246.68 TLSv1.3 101 Application Data
1273 37.778462349 172.18.12.17 13.107.246.68 TLSv1.3 221 Application Data
1274 37.778830370 172.18.12.17 13.107.246.68 TLSv1.3 101 Application Data
1275 37.780359395 142.250.194.136 172.18.12.17 QUIC 1399 Initial, DCID=2d75b8, SCID=e02e6d265d695bc7, PKN: 1, ACK, CRYPTO, PADDING
1276 37.780712711 172.18.12.17 142.250.194.136 QUIC 82 Handshake, DCID=e02e6d265d695bc7, SCID=2d75b8
1277 37.781413025 172.18.12.17 142.250.196.170 TCP 74 36264 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3366499908 TSecr=0 WS=128
1278 37.781456731 172.16.1.3 172.18.12.17 DNS 150 Standard query response 0x36a8 AAAA cdn-ukwest.onetrust.com AAAA 2606:4700:4400::ac40:9b77 AAAA 2606:4700:4400::6812
1279 37.781684271 172.18.12.17 172.64.155.119 TCP 74 58276 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1445363999 TSecr=0 WS=128
1280 37.782831987 13.107.246.68 172.18.12.17 TCP 66 443 → 55460 [ACK] Seq=13342 Ack=2335 Win=64128 Len=0 TSval=638604991 TSecr=2785503077
Frame 1749: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface eno1, id 0
0000 10 39 e9 fb e2 c0 e0 73 e7 0a 81 65 08 00 45 00
0010 00 3d 00 00 40 00 40 11 31 0a ac 12 0c 11 8e fa
0020 c2 88 e7 cb 01 bb 00 29 09 e1 77 e0 2e 6d 26 5d
0030 69 5b c7 f5 1f f2 06 0e 3c 14 60 2a 79 5a f3 53
0040 19 2b b7 47 a0 eb b0 9b 69 33 3b
"addr" was unexpected in this context.
Packets: 2687 · Displayed: 2687 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Task 4: Exporting Captured Data

• Export captured packets to a file for further analysis or sharing.

• Choose an appropriate file format for export (e.g., .pcap, .csv).

• Save the exported file to a location of your choice.



Task 5: Documentation and Reflection

• Document your observations and findings during the packet capture and analysis process.

• Reflect on the importance of network protocol analysis and the potential real-world applications of Wireshark.

• Discuss any challenges encountered during the assignment and how you overcame them.

Documentation and Reflection:

During the packet capture and analysis process using Wireshark, several observations and findings were made:

Protocol Identification: Various protocols were identified in the captured traffic, including HTTP, TCP, UDP, DNS, and ARP. HTTP traffic was prominent due to web browsing activities.TCP and UDP were commonly used for data transmission between applications. DNS requests were frequent as devices resolved domain names to IP addresses for communication. ARP packets were observed for resolving MAC addresses within the local network.

Filtering: Filtering based on specific protocols or criteria was easily achieved using Wireshark's filtering capabilities. Filtering for HTTP traffic allowed for a focused analysis on web browsing activities. Filtering packets from a specific IP address helped isolate communication between specific devices.

Packet Analysis: The contents of selected packets were analyzed to understand the communication between devices. HTTP requests and responses provided insights into web page retrieval and data exchange. TCP conversations revealed the establishment and termination of connections between devices. DNS queries and responses showed the translation of domain names to IP addresses.

Suspicious Findings: Anomalies such as unexpected DNS queries or unusual patterns in TCP traffic could indicate potential security threats. Identifying abnormal traffic patterns could be crucial for detecting network intrusions or malicious activities.

Reflection on the Importance of Network Protocol Analysis and Wireshark:

Network protocol analysis plays a vital role in understanding and troubleshooting network communications. By utilizing tools like Wireshark, network administrators can:

Detect and diagnose network performance issues such as latency or packet loss.

Identify security threats such as malware infections, unauthorized access attempts, or data exfiltration.

Monitor network usage and bandwidth consumption to optimize resource allocation.

Ensure compliance with network policies and regulations by monitoring for unauthorized activities.

Investigate incidents or breaches by analyzing network traffic for evidence.

Wireshark, with its user-friendly interface and powerful features, empowers users to capture, analyze, and interpret network traffic effectively. Its real-time packet capture capabilities make it indispensable for both proactive network monitoring and reactive incident response.

Challenges Encountered and Overcoming Them:

One challenge encountered during the assignment was interpreting the contents of certain packets, especially when dealing with encrypted traffic. In such cases, it was challenging to extract meaningful information from encrypted payloads. However, by focusing on other aspects such as packet headers, source-destination addresses, and timing patterns, it was still possible to gain insights into the communication flow.

Another challenge was ensuring proper filtering to narrow down the scope of analysis without excluding relevant packets. Experimentation with different filter expressions and refining them based on observed traffic helped overcome this challenge.

Overall, the hands-on experience with Wireshark provided valuable insights into network protocol analysis and reinforced the importance of proactive monitoring and analysis for maintaining network security and performance.

THE END