# ELEVATE LABS INTERNSHIP

## Day-5

Name : Mohamed Riyas

Role: Cyber Security Analyst

Task: 05

Title: Capture and Analyze Network Traffic Using Wireshark

Date: 30-06-2025

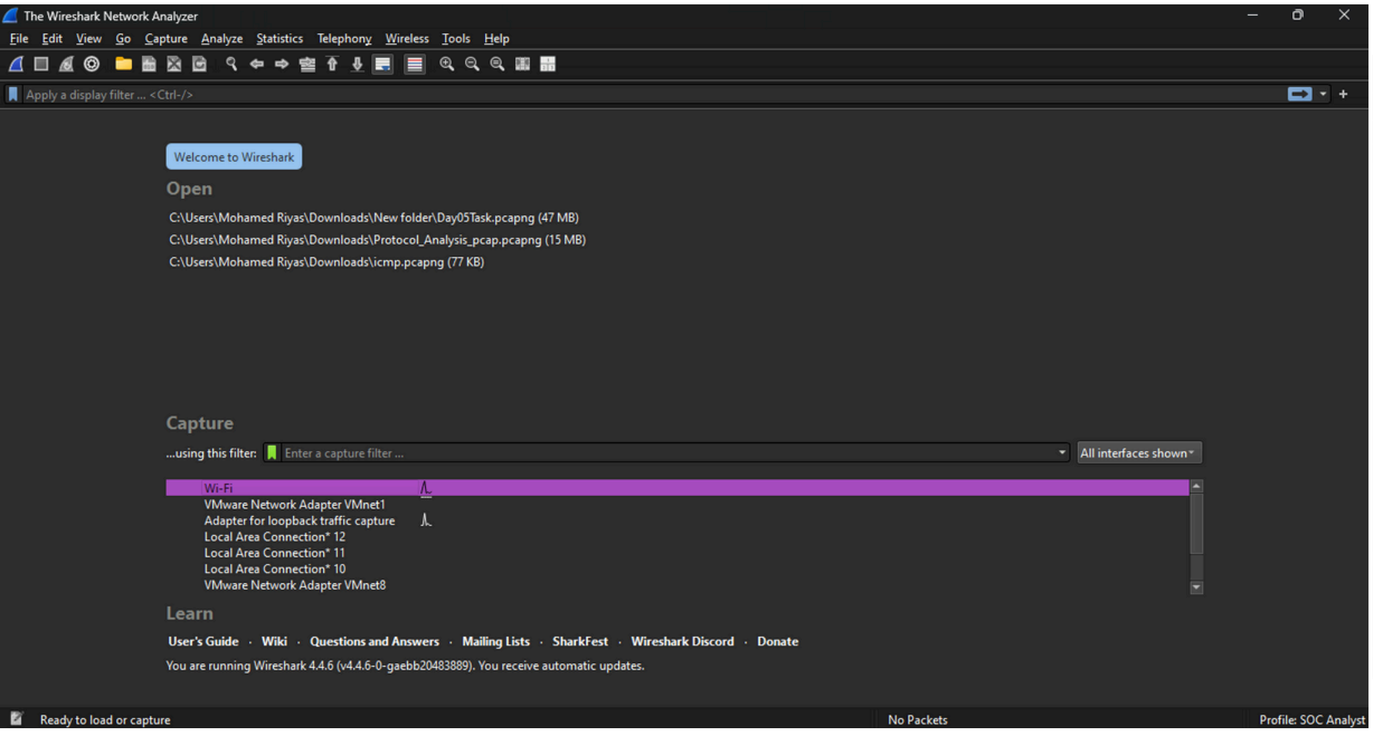
**Objective: Capture live network packets and identify basic protocols and traffic types.**

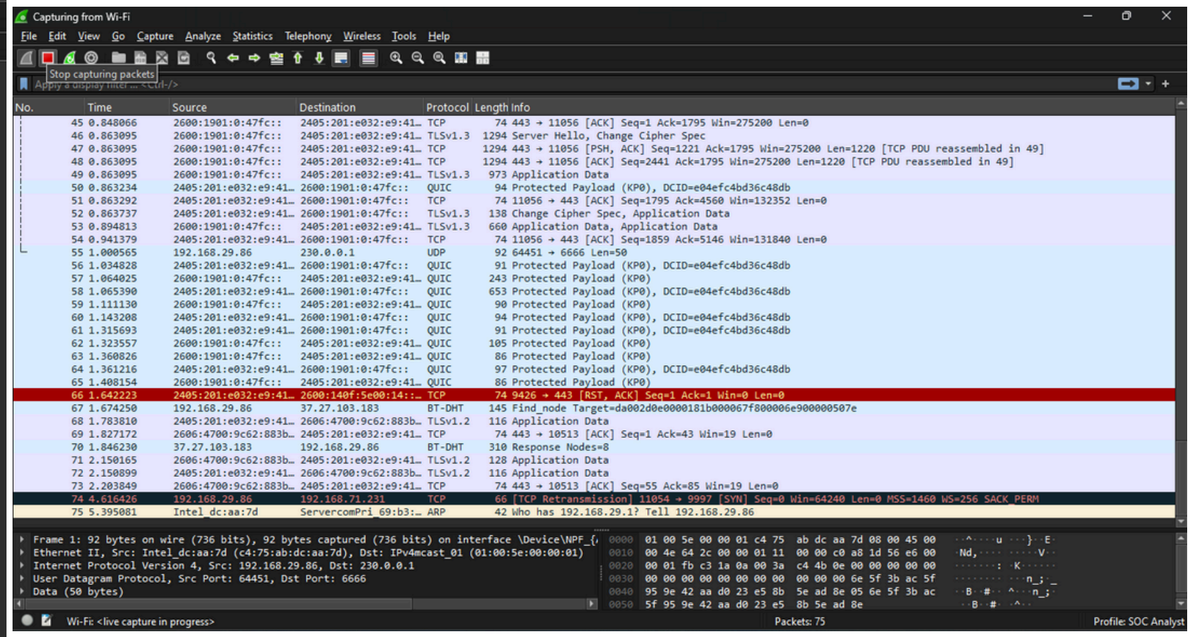
**Tools: Wireshark (free).**

**Deliverables: A packet capture (.pcap) file and a short report of protocols identified.**

## Step by step procedure to complete the task

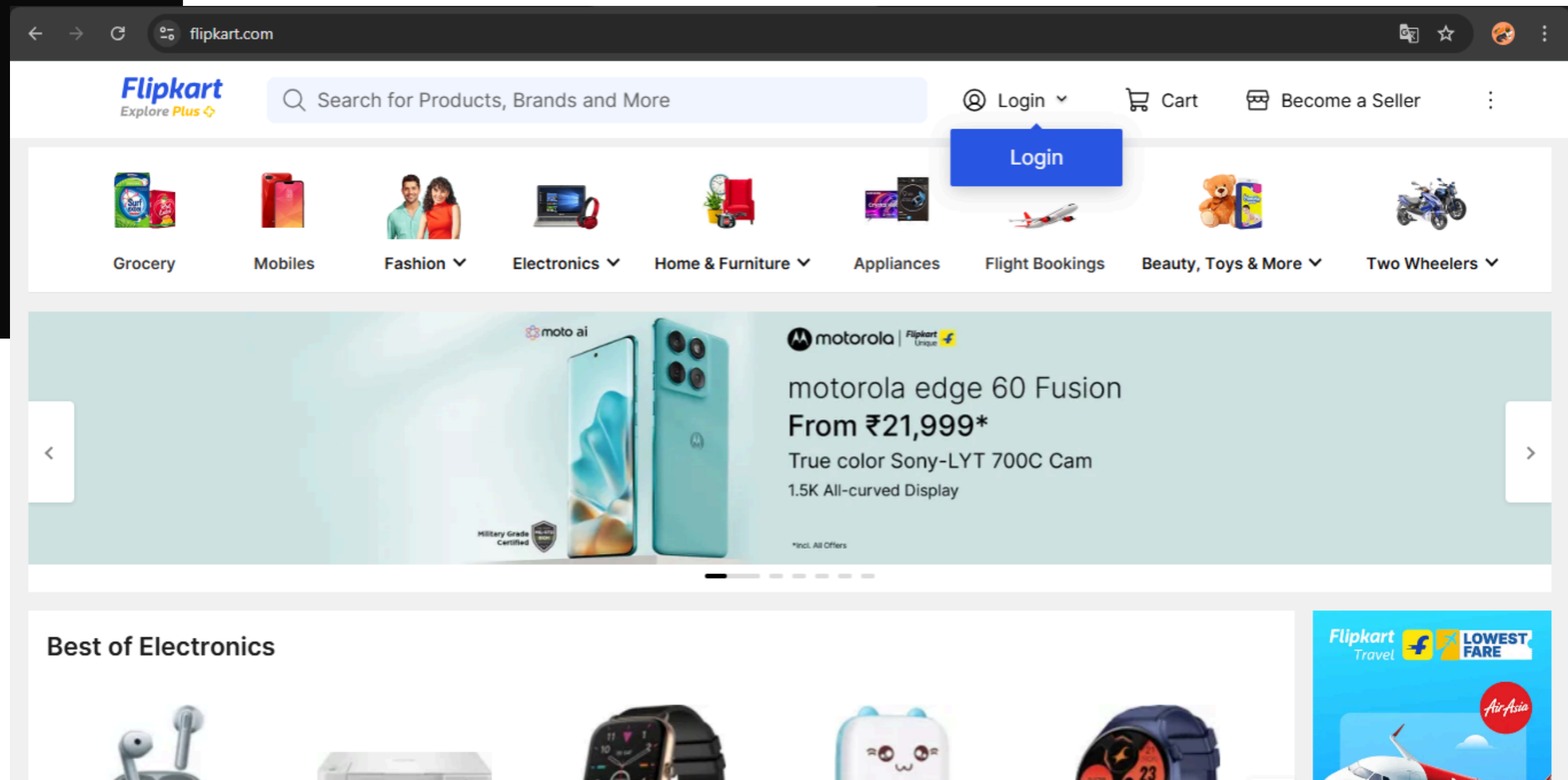
**Step-1 :** Install Wireshark and Start capturing on your active network interface.



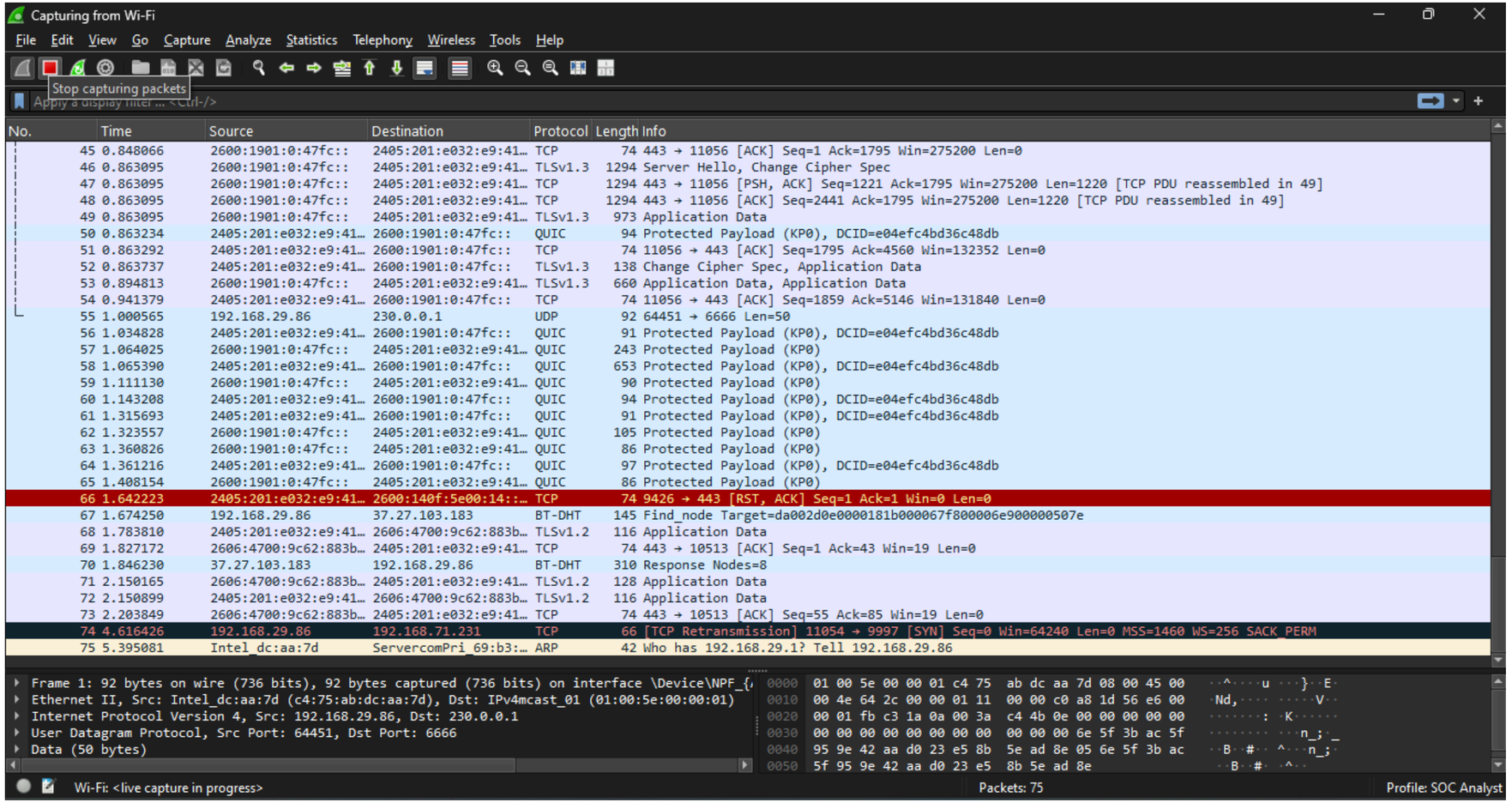



# **Step2 :** .Browse a website or ping a server to generate traffic

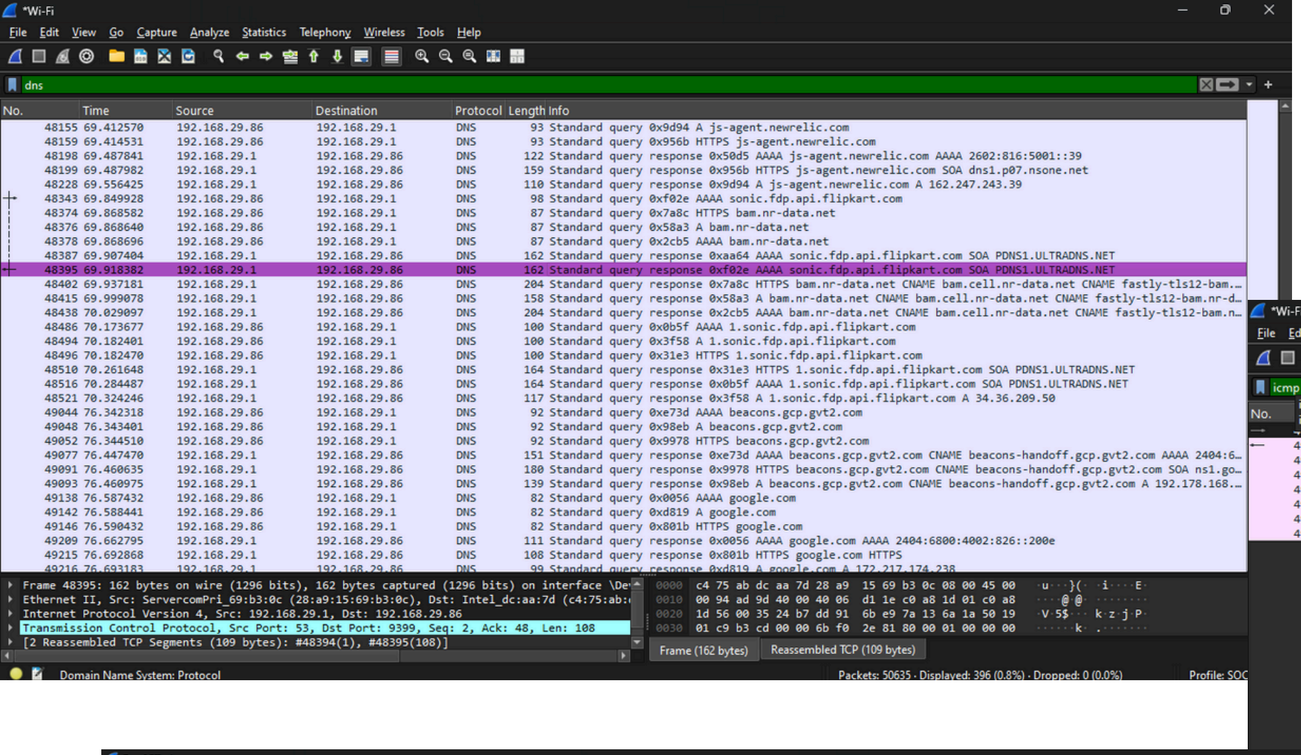
```
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Mohamed Riyas> ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=25ms TTL=112
Reply from 8.8.8.8: bytes=32 time=20ms TTL=112
Reply from 8.8.8.8: bytes=32 time=20ms TTL=112
Reply from 8.8.8.8: bytes=32 time=24ms TTL=112

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 25ms, Average = 22ms
PS C:\Users\Mohamed Riyas> nslookup youtube
Server:  reliance.reliance
Address:  2405:201:e032:e9::c0a8:1d01

Name:    youtube.

PS C:\Users\Mohamed Riyas> nslookup google
Server:  reliance.reliance
Address:  2405:201:e032:e9::c0a8:1d01

Name:    google.

PS C:\Users\Mohamed Riyas>
```

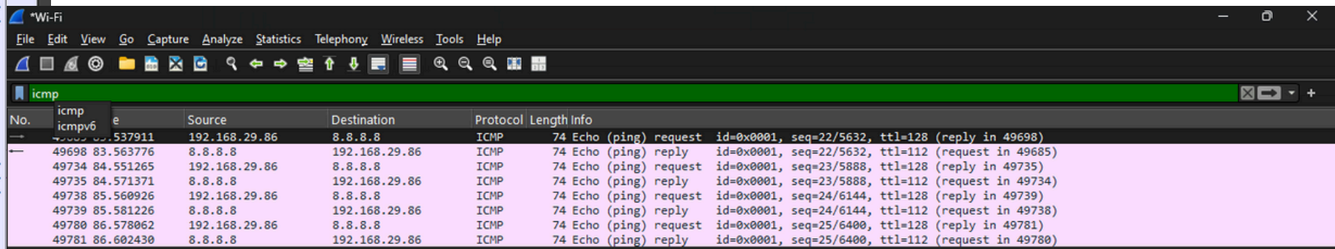


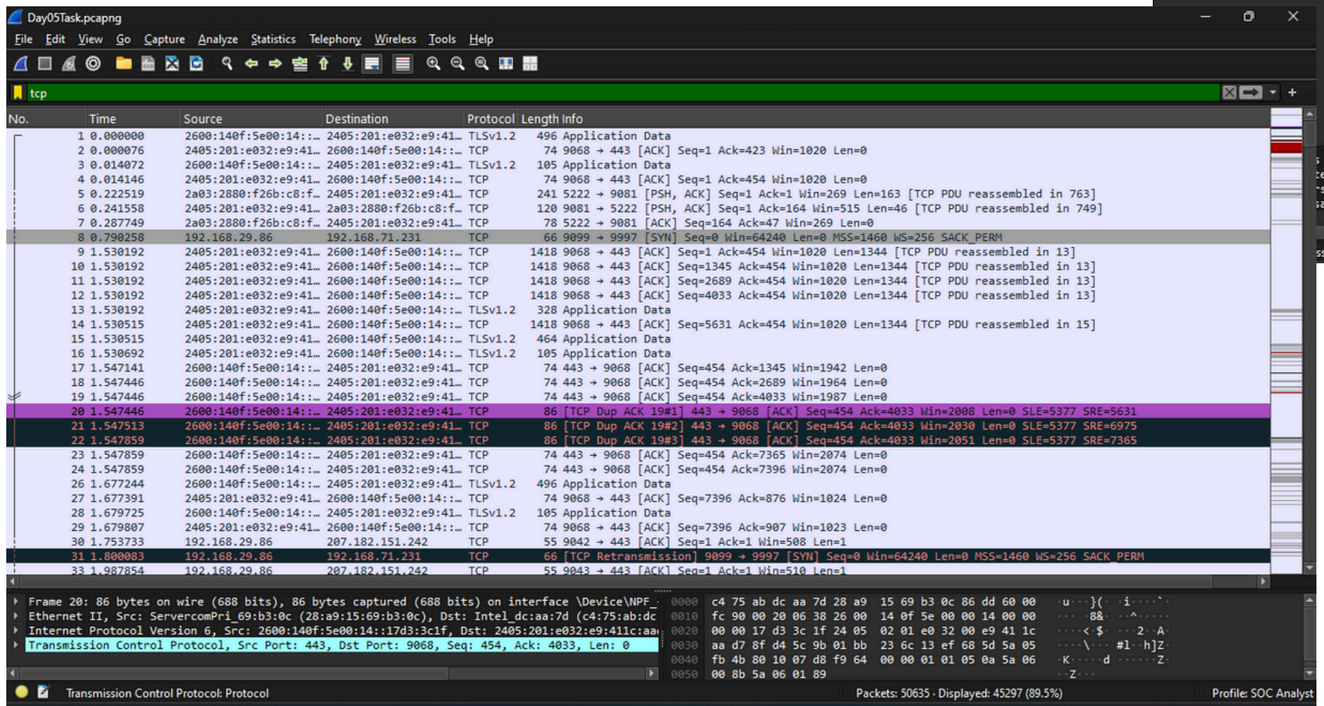
**Step3 :** .Stop capture after a minute.

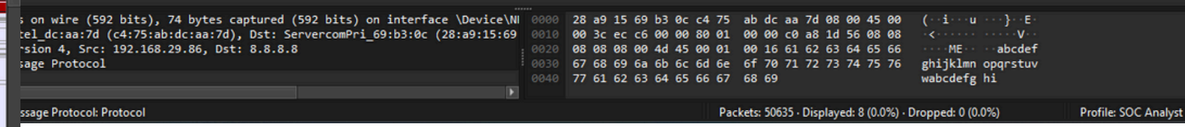



**Step4 :** .Filter captured packets by protocol (e.g., HTTP, DNS, TCP).


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
48155 69.412570 192.168.29.86 192.168.29.1 DNS 93 Standard query 0x9d94 A js-agent.newrelic.com
48159 69.414531 192.168.29.86 192.168.29.1 DNS 93 Standard query 0x956b HTTPS js-agent.newrelic.com
48198 69.487841 192.168.29.1 192.168.29.86 DNS 122 Standard query response 0x50d5 AAAA js-agent.newrelic.com AAAA 2602:816:5001::39
48199 69.487982 192.168.29.1 192.168.29.86 DNS 159 Standard query response 0x956b HTTPS js-agent.newrelic.com SOA dns1.p07.nsone.net
48228 69.556425 192.168.29.1 192.168.29.86 DNS 110 Standard query response 0x9d94 A js-agent.newrelic.com A 162.247.243.39
48343 69.849928 192.168.29.86 192.168.29.1 DNS 98 Standard query 0xf02e AAAA sonic.fdp.api.flipkart.com
48374 69.868582 192.168.29.86 192.168.29.1 DNS 87 Standard query 0x7a8c HTTPS bam.nr-data.net
48376 69.868640 192.168.29.86 192.168.29.1 DNS 87 Standard query 0x58a3 A bam.nr-data.net
48378 69.868696 192.168.29.86 192.168.29.1 DNS 87 Standard query 0x2cb5 AAAA bam.nr-data.net
48387 69.907404 192.168.29.1 192.168.29.86 DNS 162 Standard query response 0xaa64 AAAA sonic.fdp.api.flipkart.com SOA PDNS1.ULTRADNS.NET
48395 69.918382 192.168.29.1 192.168.29.86 DNS 162 Standard query response 0xf02e AAAA sonic.fdp.api.flipkart.com SOA PDNS1.ULTRADNS.NET
48402 69.937181 192.168.29.1 192.168.29.86 DNS 204 Standard query response 0x7a8c HTTPS bam.nr-data.net CNAME bam.cell.nr-data.net CNAME fastly-tls12-bam...
48415 69.999078 192.168.29.1 192.168.29.86 DNS 158 Standard query response 0x58a3 A bam.nr-data.net CNAME bam.cell.nr-data.net CNAME fastly-tls12-bam.nr-d...
48438 70.029097 192.168.29.1 192.168.29.86 DNS 204 Standard query response 0x2cb5 AAAA bam.nr-data.net CNAME bam.cell.nr-data.net CNAME fastly-tls12-bam.n...
48486 70.173677 192.168.29.86 192.168.29.1 DNS 100 Standard query 0x0b5f AAAA 1.sonic.fdp.api.flipkart.com
48494 70.182401 192.168.29.86 192.168.29.1 DNS 100 Standard query 0x3f58 A 1.sonic.fdp.api.flipkart.com
48496 70.182470 192.168.29.86 192.168.29.1 DNS 100 Standard query 0x31e3 HTTPS 1.sonic.fdp.api.flipkart.com
48510 70.261648 192.168.29.1 192.168.29.86 DNS 164 Standard query response 0x31e3 HTTPS 1.sonic.fdp.api.flipkart.com SOA PDNS1.ULTRADNS.NET
48516 70.284487 192.168.29.1 192.168.29.86 DNS 164 Standard query response 0x0b5f AAAA 1.sonic.fdp.api.flipkart.com SOA PDNS1.ULTRADNS.NET
48521 70.324246 192.168.29.1 192.168.29.86 DNS 117 Standard query response 0x3f58 A 1.sonic.fdp.api.flipkart.com A 34.36.209.50
49044 76.342318 192.168.29.86 192.168.29.1 DNS 92 Standard query 0xe73d AAAA beacons.gcp.gvt2.com
49048 76.343401 192.168.29.86 192.168.29.1 DNS 92 Standard query 0x98eb A beacons.gcp.gvt2.com
49052 76.344510 192.168.29.86 192.168.29.1 DNS 92 Standard query 0x9978 HTTPS beacons.gcp.gvt2.com
49077 76.447470 192.168.29.1 192.168.29.86 DNS 151 Standard query response 0xe73d AAAA beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com AAAA 2404:6...
49091 76.460635 192.168.29.1 192.168.29.86 DNS 180 Standard query response 0x9978 HTTPS beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com SOA ns1.go...
49093 76.460975 192.168.29.1 192.168.29.86 DNS 139 Standard query response 0x98eb A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 192.178.168...
49138 76.587432 192.168.29.86 192.168.29.1 DNS 82 Standard query 0x0056 AAAA google.com
49142 76.588441 192.168.29.86 192.168.29.1 DNS 82 Standard query 0xd819 A google.com
49146 76.590432 192.168.29.86 192.168.29.1 DNS 82 Standard query 0x801b HTTPS google.com
49209 76.662795 192.168.29.1 192.168.29.86 DNS 111 Standard query response 0x0056 AAAA google.com AAAA 2404:6800:4002:826::200e
49215 76.692868 192.168.29.1 192.168.29.86 DNS 108 Standard query response 0x801b HTTPS google.com HTTPS
49216 76.693183 192.168.29.1 192.168.29.86 DNS 99 Standard query response 0xd819 A google.com A 172.217.174.238
Frame 48395: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface \De
Ethernet II, Src: ServercomPri_69:b3:0c (28:a9:15:69:b3:0c), Dst: Intel_dc:aa:7d (c4:75:ab:
Internet Protocol Version 4, Src: 192.168.29.1, Dst: 192.168.29.86
Transmission Control Protocol, Src Port: 53, Dst Port: 9399, Seq: 2, Ack: 48, Len: 108
[2 Reassembled TCP Segments (109 bytes): #48394(1), #48395(108)]
0000 c4 75 ab dc aa 7d 28 a9 15 69 b3 0c 08 00 45 00 ·u···}( ··i····E·
0010 00 94 ad 9d 40 00 40 06 d1 1e c0 a8 1d 01 c0 a8 ····@·@· ········
0020 1d 56 00 35 24 b7 dd 91 6b e9 7a 13 6a 1a 50 19 ·V·5$··· k·z·j·P·
0030 01 c9 b3 cd 00 00 6b f0 2e 81 80 00 01 00 00 00 ·····k· ········
Frame (162 bytes)
Reassembled TCP (109 bytes)
Domain Name System: Protocol
Packets: 50635 · Displayed: 396 (0.8%) · Dropped: 0 (0.0%)
Profile: SOC


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
icmp
icmpv6
No. Source Destination Protocol Length Info
49698 83.563776 8.8.8.8 192.168.29.86 ICMP 74 Echo (ping) reply id=0x0001, seq=22/5632, ttl=112 (request in 49685)
49734 84.551265 192.168.29.86 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 49735)
49735 84.571371 8.8.8.8 192.168.29.86 ICMP 74 Echo (ping) reply id=0x0001, seq=23/5888, ttl=112 (request in 49734)
49738 85.560926 192.168.29.86 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 49739)
49739 85.581226 8.8.8.8 192.168.29.86 ICMP 74 Echo (ping) reply id=0x0001, seq=24/6144, ttl=112 (request in 49738)
49780 86.578062 192.168.29.86 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 49781)
49781 86.602430 8.8.8.8 192.168.29.86 ICMP 74 Echo (ping) reply id=0x0001, seq=25/6400, ttl=112 (request in 49780)


Day05Task.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
1 0.000000 2600:140f:5e00:14::... 2405:201:e032:e9:41... TLSv1.2 496 Application Data
2 0.000076 2405:201:e032:e9:41... 2600:140f:5e00:14::... TCP 74 9068 → 443 [ACK] Seq=1 Ack=423 Win=1020 Len=0
3 0.014072 2600:140f:5e00:14::... 2405:201:e032:e9:41... TLSv1.2 105 Application Data
4 0.014146 2405:201:e032:e9:41... 2600:140f:5e00:14::... TCP 74 9068 → 443 [ACK] Seq=1 Ack=454 Win=1020 Len=0
5 0.222519 2a03:2880:f26b:c8:f... 2405:201:e032:e9:41... TCP 241 5222 → 9081 [PSH, ACK] Seq=1 Ack=1 Win=269 Len=163 [TCP PDU reassembled in 763]
6 0.241558 2405:201:e032:e9:41... 2a03:2880:f26b:c8:f... TCP 120 9081 → 5222 [PSH, ACK] Seq=1 Ack=164 Win=515 Len=46 [TCP PDU reassembled in 749]
7 0.287749 2a03:2880:f26b:c8:f... 2405:201:e032:e9:41... TCP 78 5222 → 9081 [ACK] Seq=164 Ack=47 Win=269 Len=0
8 0.790258 192.168.29.86 192.168.71.231 TCP 66 9099 → 9997 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9 1.530192 2405:201:e032:e9:41... 2600:140f:5e00:14::... TCP 1418 9068 → 443 [ACK] Seq=1 Ack=454 Win=1020 Len=1344 [TCP PDU reassembled in 13]
10 1.530192 2405:201:e032:e9:41... 2600:140f:5e00:14::... TCP 1418 9068 → 443 [ACK] Seq=1345 Ack=454 Win=1020 Len=1344 [TCP PDU reassembled in 13]
11 1.530192 2405:201:e032:e9:41... 2600:140f:5e00:14::... TCP 1418 9068 → 443 [ACK] Seq=2689 Ack=454 Win=1020 Len=1344 [TCP PDU reassembled in 13]
12 1.530192 2405:201:e032:e9:41... 2600:140f:5e00:14::... TCP 1418 9068 → 443 [ACK] Seq=4033 Ack=454 Win=1020 Len=1344 [TCP PDU reassembled in 13]
13 1.530192 2405:201:e032:e9:41... 2600:140f:5e00:14::... TLSv1.2 328 Application Data
14 1.530515 2405:201:e032:e9:41... 2600:140f:5e00:14::... TCP 1418 9068 → 443 [ACK] Seq=5631 Ack=454 Win=1020 Len=1344 [TCP PDU reassembled in 15]
15 1.530515 2405:201:e032:e9:41... 2600:140f:5e00:14::... TLSv1.2 464 Application Data
16 1.530692 2405:201:e032:e9:41... 2600:140f:5e00:14::... TLSv1.2 105 Application Data
17 1.547141 2600:140f:5e00:14::... 2405:201:e032:e9:41... TCP 74 443 → 9068 [ACK] Seq=454 Ack=1345 Win=1942 Len=0
18 1.547446 2600:140f:5e00:14::... 2405:201:e032:e9:41... TCP 74 443 → 9068 [ACK] Seq=454 Ack=2689 Win=1964 Len=0
19 1.547446 2600:140f:5e00:14::... 2405:201:e032:e9:41... TCP 74 443 → 9068 [ACK] Seq=454 Ack=4033 Win=1987 Len=0
20 1.547446 2600:140f:5e00:14::... 2405:201:e032:e9:41... TCP 86 [TCP Dup ACK 19#1] 443 → 9068 [ACK] Seq=454 Ack=4033 Win=2008 Len=0 SLE=5377 SRE=5631
21 1.547513 2600:140f:5e00:14::... 2405:201:e032:e9:41... TCP 86 [TCP Dup ACK 19#2] 443 → 9068 [ACK] Seq=454 Ack=4033 Win=2030 Len=0 SLE=5377 SRE=6975
22 1.547859 2600:140f:5e00:14::... 2405:201:e032:e9:41... TCP 86 [TCP Dup ACK 19#3] 443 → 9068 [ACK] Seq=454 Ack=4033 Win=2051 Len=0 SLE=5377 SRE=7365
23 1.547859 2600:140f:5e00:14::... 2405:201:e032:e9:41... TCP 74 443 → 9068 [ACK] Seq=454 Ack=7365 Win=2074 Len=0
24 1.547859 2600:140f:5e00:14::... 2405:201:e032:e9:41... TCP 74 443 → 9068 [ACK] Seq=454 Ack=7396 Win=2074 Len=0
26 1.677244 2600:140f:5e00:14::... 2405:201:e032:e9:41... TLSv1.2 496 Application Data
27 1.677391 2405:201:e032:e9:41... 2600:140f:5e00:14::... TCP 74 9068 → 443 [ACK] Seq=7396 Ack=876 Win=1024 Len=0
28 1.679725 2600:140f:5e00:14::... 2405:201:e032:e9:41... TLSv1.2 105 Application Data
29 1.679807 2405:201:e032:e9:41... 2600:140f:5e00:14::... TCP 74 9068 → 443 [ACK] Seq=7396 Ack=907 Win=1023 Len=0
30 1.753733 192.168.29.86 207.182.151.242 TCP 55 9042 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1
31 1.800083 192.168.29.86 192.168.71.231 TCP 66 [TCP Retransmission] 9099 → 9997 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
33 1.987854 192.168.29.86 207.182.151.242 TCP 55 9043 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1
Frame 20: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_
Ethernet II, Src: ServercomPri_69:b3:0c (28:a9:15:69:b3:0c), Dst: Intel_dc:aa:7d (c4:75:ab:dc
Internet Protocol Version 6, Src: 2600:140f:5e00:14::17d3:3c1f, Dst: 2405:201:e032:e9:411c:aa
Transmission Control Protocol, Src Port: 443, Dst Port: 9068, Seq: 454, Ack: 4033, Len: 0
0000 c4 75 ab dc aa 7d 28 a9 15 69 b3 0c 86 dd 60 00 ·u···}( ·i····`·
0010 fc 90 00 20 06 38 26 00 14 0f 5e 00 00 14 00 00 ··· ·8& ··^·····
0020 00 00 17 d3 3c 1f 24 05 02 01 e0 32 00 e9 41 1c ····<·$· ···2··A·
0030 aa d7 8f d4 5c 9b 01 bb 23 6c 13 ef 68 5d 5a 05 ····\··· #l··h]Z·
0040 fb 4b 80 10 07 d8 f9 64 00 00 01 01 05 0a 5a 06 ·K·····d ·····Z·
0050 00 8b 5a 06 01 89 ··Z···
Transmission Control Protocol: Protocol
Packets: 50635 · Displayed: 45297 (89.5%)
Profile: SOC Analyst


on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NI
tel_dc:aa:7d (c4:75:ab:dc:aa:7d), Dst: ServercomPri_69:b3:0c (28:a9:15:69
rsion 4, Src: 192.168.29.86, Dst: 8.8.8.8
sage Protocol
0000 28 a9 15 69 b3 0c c4 75 ab dc aa 7d 08 00 45 00 (··i···u ···}··E·
0010 00 3c ec c6 00 00 80 01 00 00 c0 a8 1d 56 08 08 ·<····· ·····V··
0020 08 08 08 00 4d 45 00 01 00 16 61 62 63 64 65 66 ····ME·· ··abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi
ssage Protocol: Protocol
Packets: 50635 · Displayed: 8 (0.0%) · Dropped: 0 (0.0%)
Profile: SOC Analyst

**Step 5 :** Summarize your findings and packet details.

Captured Protocols:

- DNS (Domain Name System)
- ICMP (Internet Control Message Protocol)
- TCP (Transmission Control Protocol)
- HTTP (HyperText Transfer Protocol)

==========

COMPLETED DAY 05 TASK