Intern name – AMIT MAURYA

Task 5 : Capture and Analyze Network Traffic Using Wireshark

Objective

Capture live network packets using Wireshark and identify basic protocols and traffic types.

Steps Performed

• Installed Wireshark: Downloaded and installed the latest version of Wireshark from the official website.

• Started Packet Capture: Selected the active network interface and began capturing live network traffic.

• Generated Network Traffic: Opened a web browser, visited several websites, and used the ping command to generate ICMP traffic.

• Stopped Capture: Stopped the capture after approximately one minute.

• Filtered Captured Packets: Applied display filters: http, dns, tcp in the filter bar.

• Identified Different Protocols: Observed DNS, HTTP, TCP, and ICMP protocols in the capture.

• Saved Packet Capture: Exported the captured packets as a .pcap file.

Summary of Findings

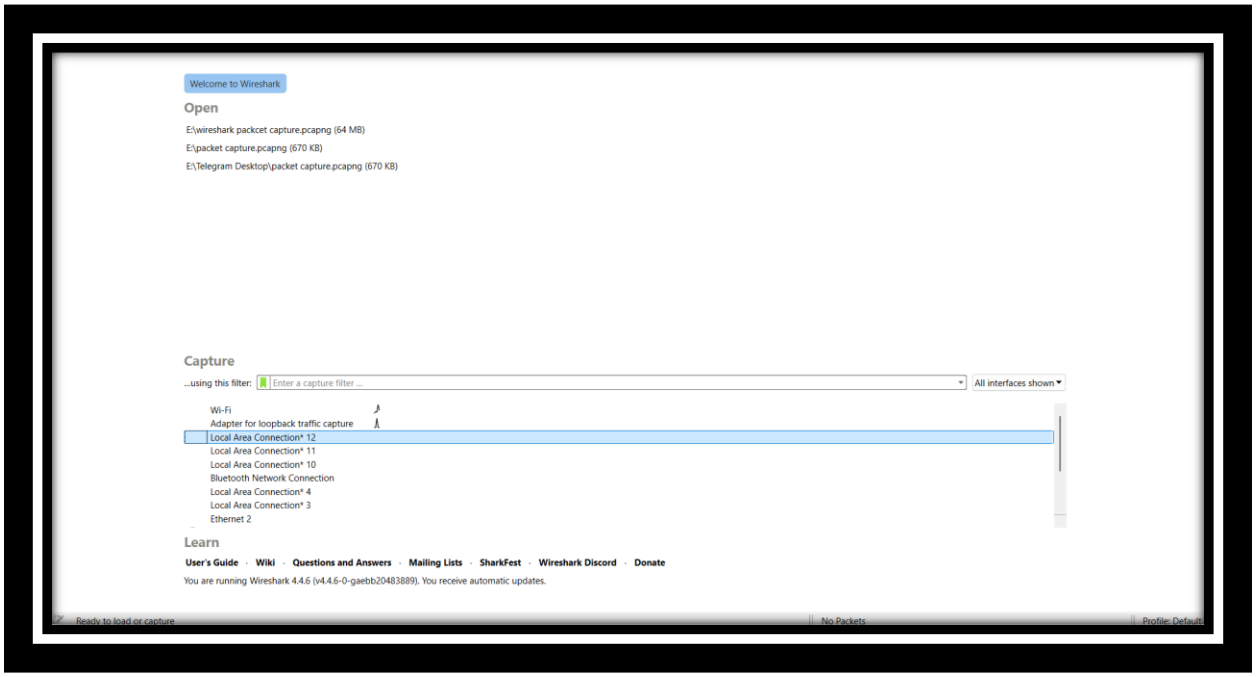
The following protocols were identified in the captured traffic:

Protocol	Purpose	Details Observed
DNS	**Resolves domain names to IP addresses**	**Multiple DNS query and response packets.**
HTTP	**Communication between web client and server**	**HTTP GET and response packets observed.**
TCP	**Establishes reliable communication**	**TCP handshake (SYN, SYN-ACK, ACK) and data transfer packets observed.**
ICMP	**Used for network**	**Echo request and**

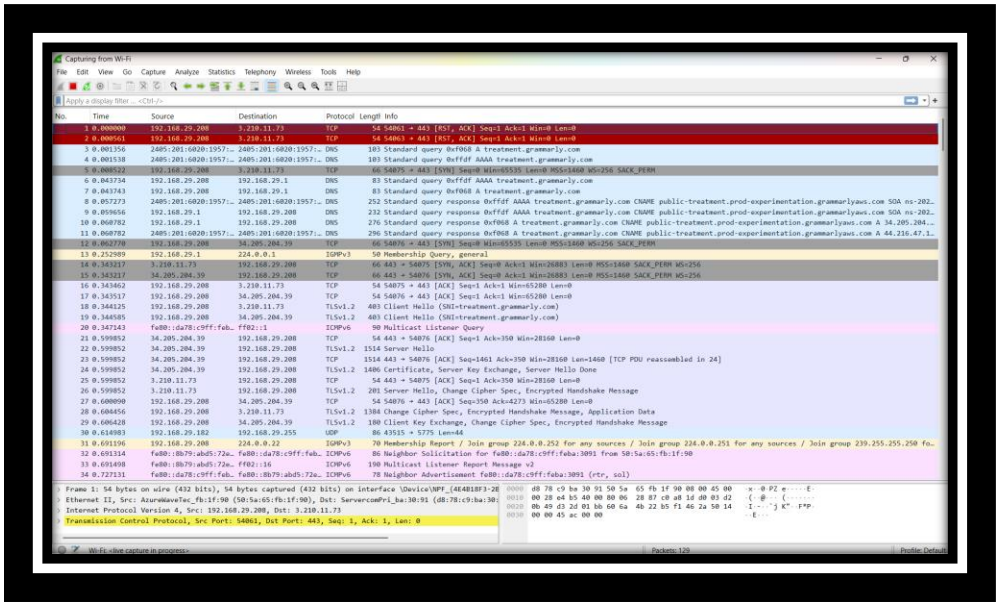
	diagnostics	reply (ping) packets observed.

Screenshot captured during packet capture and analysis

- **SELECTING INTERFACE OR MODE FOR CAPTURING PACKETS**

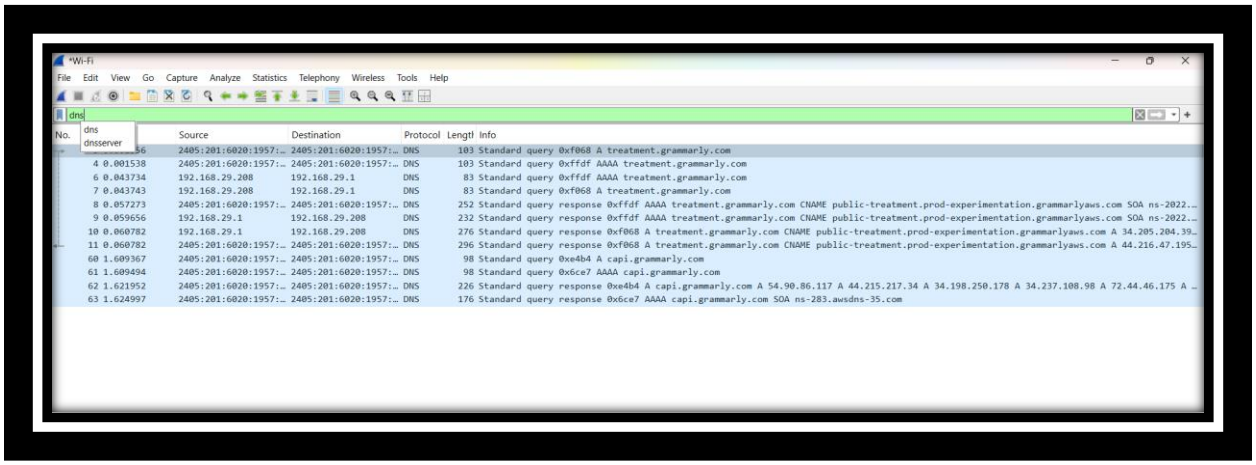


- **Packet capture starts**

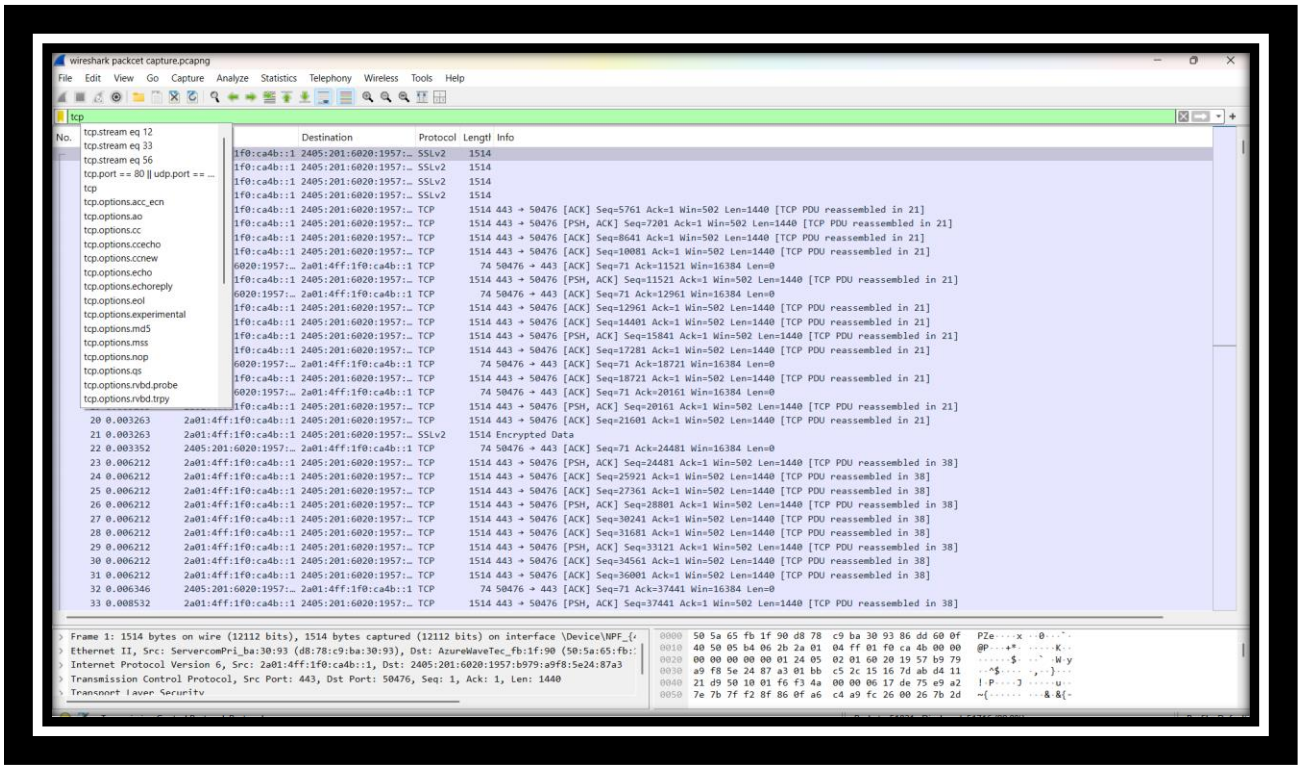


APPLYING FILTERS

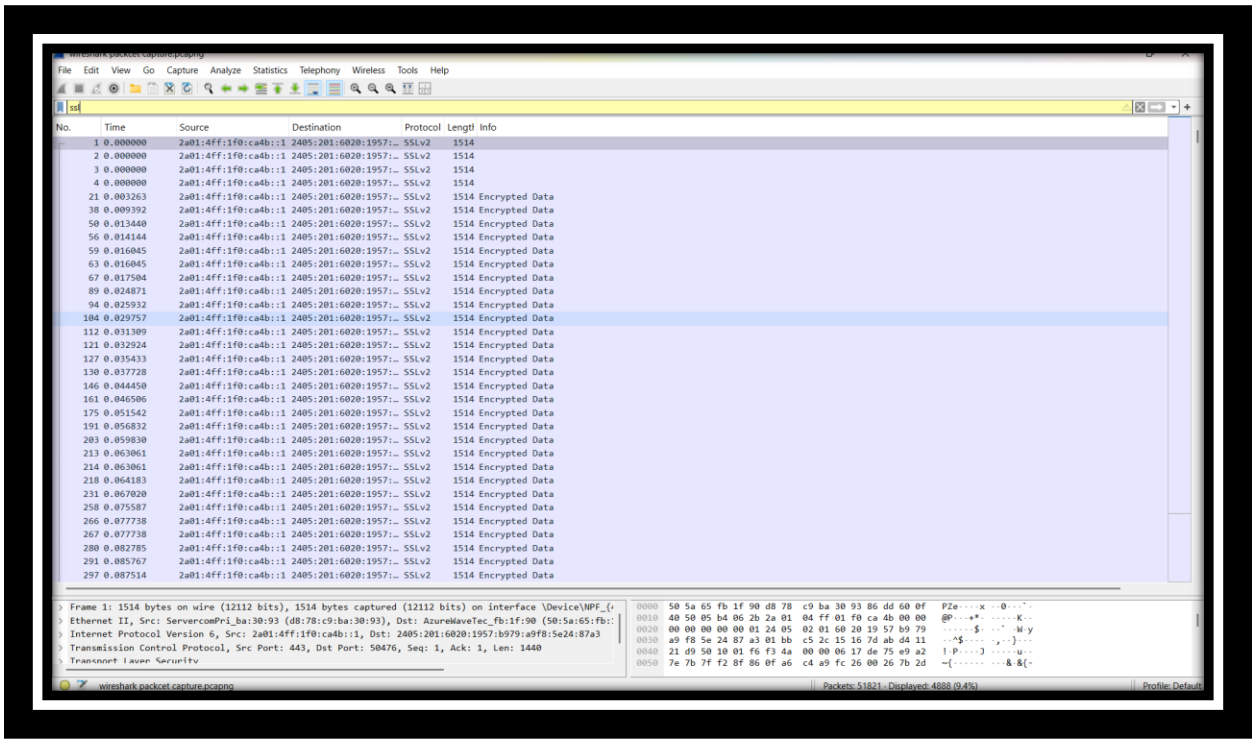
- **DNS**



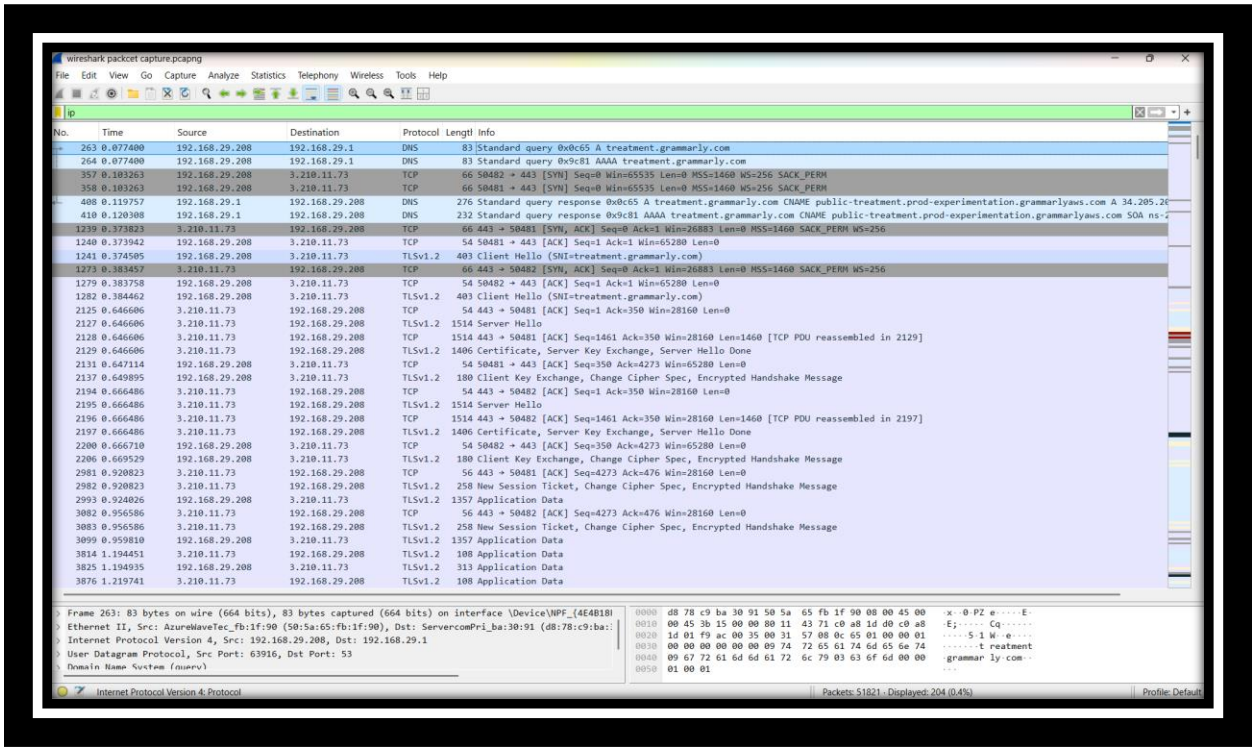
TCP



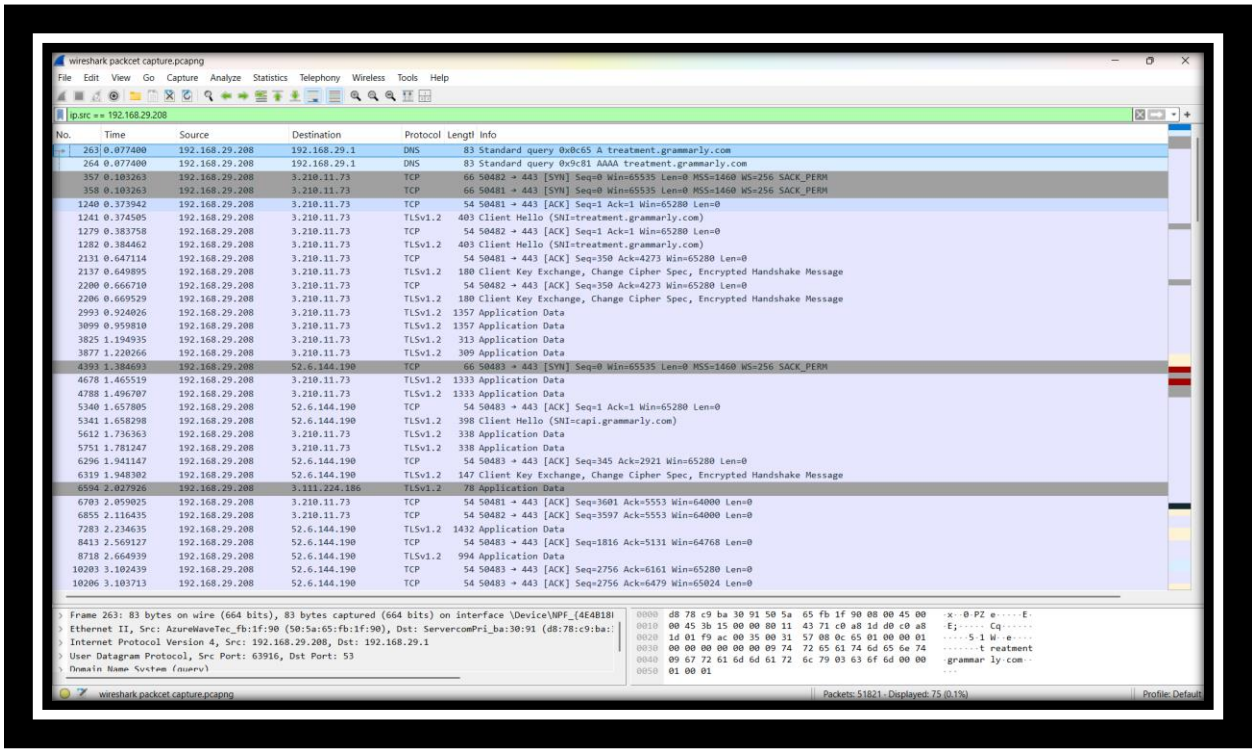
SSL


wireshark packcet capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
No. Time Source Destination Protocol Lengtl Info
1 0.000000 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514
2 0.000000 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514
3 0.000000 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514
4 0.000000 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514
21 0.003263 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
38 0.009392 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
50 0.013440 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
56 0.014144 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
59 0.016045 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
63 0.016045 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
67 0.017504 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
89 0.024871 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
94 0.025932 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
104 0.029757 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
112 0.031309 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
121 0.032924 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
127 0.035433 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
130 0.037728 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
146 0.044450 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
161 0.046506 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
175 0.051542 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
191 0.056832 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
203 0.059830 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
213 0.063061 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
214 0.063061 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
218 0.064183 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
231 0.067020 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
258 0.075587 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
266 0.077738 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
267 0.077738 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
280 0.082785 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
291 0.085767 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
297 0.087514 2a01:4ff:1f0:ca4b::1 2405:201:6020:1957:… SSLv2 1514 Encrypted Data
Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{
Ethernet II, Src: ServercomPri_ba:30:93 (d8:78:c9:ba:30:93), Dst: AzureWaveTec_fb:1f:90 (50:5a:65:fb:
Internet Protocol Version 6, Src: 2a01:4ff:1f0:ca4b::1, Dst: 2405:201:6020:1957:b979:a9f8:5e24:87a3
Transmission Control Protocol, Src Port: 443, Dst Port: 50476, Seq: 1, Ack: 1, Len: 1440
Transport Layer Security
0000 50 5a 65 fb 1f 90 d8 78 c9 ba 30 93 86 dd 60 0f
0010 40 50 05 b4 06 2b 2a 01 04 ff 01 f0 ca 4b 00 00
0020 00 00 00 00 00 01 24 05 02 01 60 20 19 57 b9 79
0030 a9 f8 5e 24 87 a3 01 bb c5 2c 15 16 7d ab d4 11
0040 21 d9 50 10 01 f6 f3 4a 00 00 06 17 de 75 e9 a2
0050 7e 7b 7f f2 8f 86 0f a6 c4 a9 fc 26 00 26 7b 2d
wireshark packcet capture.pcapng
Packets: 51821 · Displayed: 4888 (9.4%)
Profile: Default

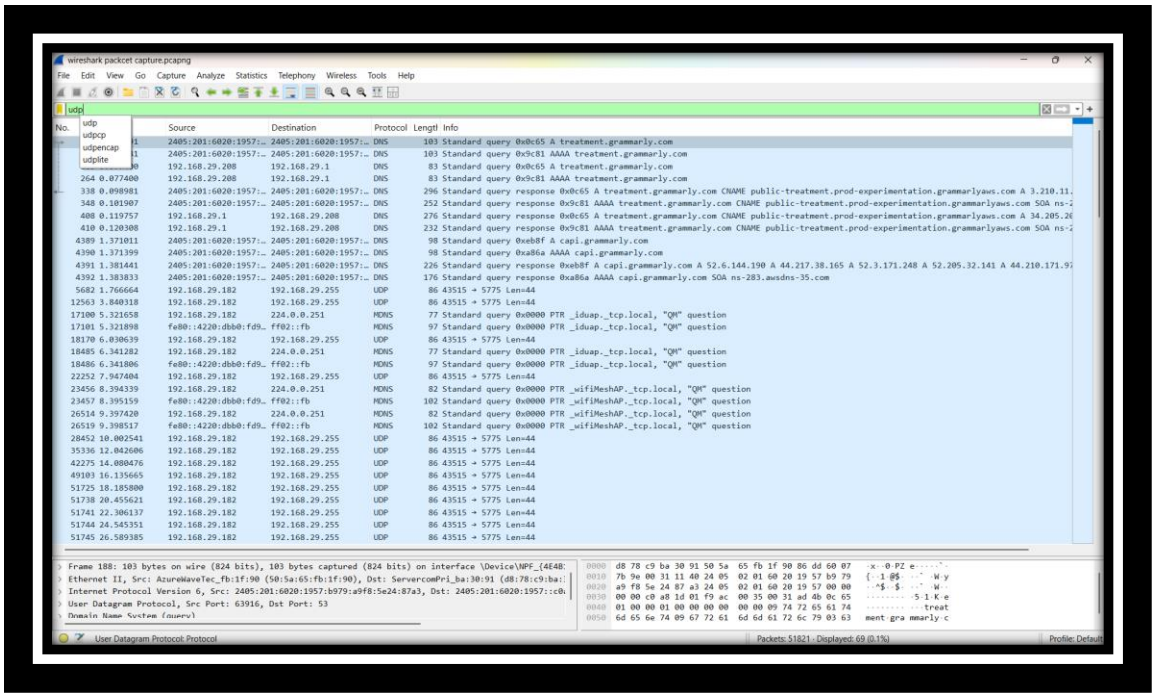
IP


wireshark packcet capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip
No. Time Source Destination Protocol Lengtl Info
263 0.077400 192.168.29.208 192.168.29.1 DNS 83 Standard query 0x0c65 A treatment.grammarly.com
264 0.077400 192.168.29.208 192.168.29.1 DNS 83 Standard query 0x9c81 AAAA treatment.grammarly.com
357 0.103263 192.168.29.208 3.210.11.73 TCP 66 50482 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
358 0.103263 192.168.29.208 3.210.11.73 TCP 66 50481 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
408 0.119757 192.168.29.1 192.168.29.208 DNS 276 Standard query response 0x0c65 A treatment.grammarly.com CNAME public-treatment.prod-experimentation.grammarlyaws.com A 34.205.26
410 0.120308 192.168.29.1 192.168.29.208 DNS 232 Standard query response 0x9c81 AAAA treatment.grammarly.com CNAME public-treatment.prod-experimentation.grammarlyaws.com SOA ns-
1239 0.373823 3.210.11.73 192.168.29.208 TCP 66 443 → 50481 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM WS=256
1240 0.373942 192.168.29.208 3.210.11.73 TCP 54 50481 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1241 0.374505 192.168.29.208 3.210.11.73 TLSv1.2 403 Client Hello (SNI=treatment.grammarly.com)
1273 0.383457 3.210.11.73 192.168.29.208 TCP 66 443 → 50482 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM WS=256
1279 0.383758 192.168.29.208 3.210.11.73 TCP 54 50482 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1282 0.384462 192.168.29.208 3.210.11.73 TLSv1.2 403 Client Hello (SNI=treatment.grammarly.com)
2125 0.646606 3.210.11.73 192.168.29.208 TCP 54 443 → 50481 [ACK] Seq=1 Ack=350 Win=28160 Len=0
2127 0.646606 3.210.11.73 192.168.29.208 TLSv1.2 1514 Server Hello
2128 0.646606 3.210.11.73 192.168.29.208 TCP 1514 443 → 50481 [ACK] Seq=1461 Ack=350 Win=28160 Len=1460 [TCP PDU reassembled in 2129]
2129 0.646606 3.210.11.73 192.168.29.208 TLSv1.2 1406 Certificate, Server Key Exchange, Server Hello Done
2131 0.647114 192.168.29.208 3.210.11.73 TCP 54 50481 → 443 [ACK] Seq=350 Ack=4273 Win=65280 Len=0
2137 0.649895 192.168.29.208 3.210.11.73 TLSv1.2 180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2194 0.666486 3.210.11.73 192.168.29.208 TCP 54 443 → 50482 [ACK] Seq=1 Ack=350 Win=28160 Len=0
2195 0.666486 3.210.11.73 192.168.29.208 TLSv1.2 1514 Server Hello
2196 0.666486 3.210.11.73 192.168.29.208 TCP 1514 443 → 50482 [ACK] Seq=1461 Ack=350 Win=28160 Len=1460 [TCP PDU reassembled in 2197]
2197 0.666486 3.210.11.73 192.168.29.208 TLSv1.2 1406 Certificate, Server Key Exchange, Server Hello Done
2200 0.666710 192.168.29.208 3.210.11.73 TCP 54 50482 → 443 [ACK] Seq=350 Ack=4273 Win=65280 Len=0
2206 0.669529 192.168.29.208 3.210.11.73 TLSv1.2 180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2981 0.920823 3.210.11.73 192.168.29.208 TCP 56 443 → 50481 [ACK] Seq=4273 Ack=476 Win=28160 Len=0
2982 0.920823 3.210.11.73 192.168.29.208 TLSv1.2 258 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2993 0.924026 192.168.29.208 3.210.11.73 TLSv1.2 1357 Application Data
3082 0.956586 3.210.11.73 192.168.29.208 TCP 56 443 → 50482 [ACK] Seq=4273 Ack=476 Win=28160 Len=0
3083 0.956586 3.210.11.73 192.168.29.208 TLSv1.2 258 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
3099 0.959810 192.168.29.208 3.210.11.73 TLSv1.2 1357 Application Data
3814 1.194451 3.210.11.73 192.168.29.208 TLSv1.2 108 Application Data
3825 1.194935 192.168.29.208 3.210.11.73 TLSv1.2 313 Application Data
3876 1.219741 3.210.11.73 192.168.29.208 TLSv1.2 108 Application Data
Frame 263: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{4E4B18
Ethernet II, Src: AzureWaveTec_fb:1f:90 (50:5a:65:fb:1f:90), Dst: ServercomPri_ba:30:91 (d8:78:c9:ba:
Internet Protocol Version 4, Src: 192.168.29.208, Dst: 192.168.29.1
User Datagram Protocol, Src Port: 63916, Dst Port: 53
Domain Name System (query)
0000 d8 78 c9 ba 30 91 50 5a 65 fb 1f 90 08 00 45 00
0010 00 45 3b 15 00 00 80 11 43 71 c0 a8 1d d0 c0 a8
0020 1d 01 f9 ac 00 35 00 31 57 08 0c 65 01 00 00 01
0030 00 00 00 00 00 00 09 74 72 65 61 74 6d 65 6e 74
0040 09 67 72 61 6d 6d 61 72 6c 79 03 63 6f 6d 00 00
0050 01 00 01
Internet Protocol Version 4: Protocol
Packets: 51821 · Displayed: 204 (0.4%)
Profile: Default

IP SRC ==192.168.29.208



UDP



Detailed Protocol-wise Analysis:

1. IP Source (ip.src)

From the Endpoints statistics:

- **The most active IP sources:**
    - **6c:e8:c6:c7:fe:d2 with 51,763 packets (SSDP related traffic).**
    - **d8:78:c9:ba:30:91 with 13,591 packets.**
    - **Other minor IP sources involved in smaller packet counts.**

Observation:
The majority of traffic is local broadcast/multicast related to SSDP and MDNS protocols.

2. DNS Traffic

From the Filtered Display and Packet List:

- **Total DNS packets: 8 packets**
- **Domains queried:**
    - **treatment.grammarly.com**
    - **capi.grammarly.com**
- **Both IPv6 and IPv4 DNS resolutions observed.**

Observation:
DNS queries are mainly directed toward Grammarly services, indicating web application communication.

3. HTTP Traffic

- **HTTP traffic not detected in the provided capture based on your filtered views and protocol hierarchy.**

Note:
If browsing occurred over HTTPS, it would not appear as HTTP but as encrypted TLS traffic.

4. ICMP Traffic

- **ICMP traffic not detected in this capture.**

Possible Reason:
No ping or traceroute operations were performed during the capture.

5. TCP Traffic

- **TCP traffic is negligible or not prominently visible in the provided screenshots.**
- **Likely traffic was predominantly UDP-based services.**

6. UDP Traffic

From the Protocol Hierarchy and Filters:

- **Total UDP packets: 41 packets**
- **UDP was used for:**
    - **Simple Service Discovery Protocol (SSDP): 22 packets**
    - **Multicast Domain Name System (MDNS): 4 packets**
    - **Domain Name System (DNS): 8 packets**
    - **Other local broadcast messages.**

Observation:
UDP traffic dominated this capture and was mainly involved in network service discovery and name resolution.

Key Observations:

- **The network traffic captured was mostly service discovery and DNS resolution related.**
- **Major IP traffic sources were local devices broadcasting service discovery packets.**
- **No HTTP (unencrypted web) or ICMP traffic was found.**
- **DNS queries indicate that some web-related services (like Grammarly) were accessed.**