VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

**School of Information Technology & Engineering**

WINTER 2022 - 23

**Programme : B.Tech** **Due Date : 29-01-2022**
**Course Title : Information Security Management** **Course Code : CSE3502**

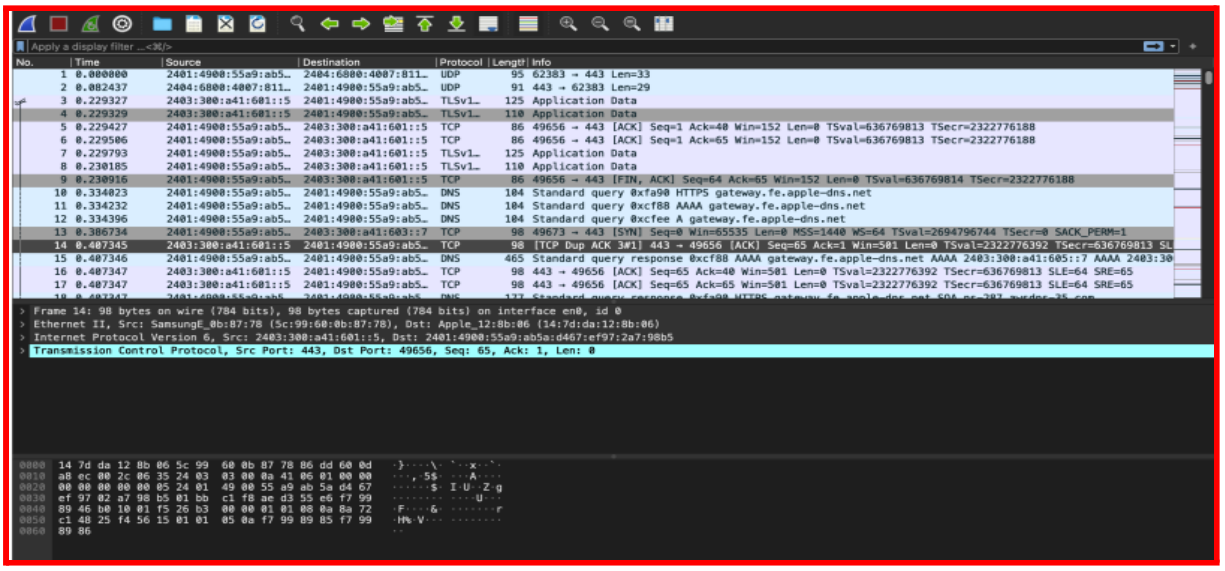
**Name: SHUBHAM AGARWAL**
**RegNo: 19BIT0010**

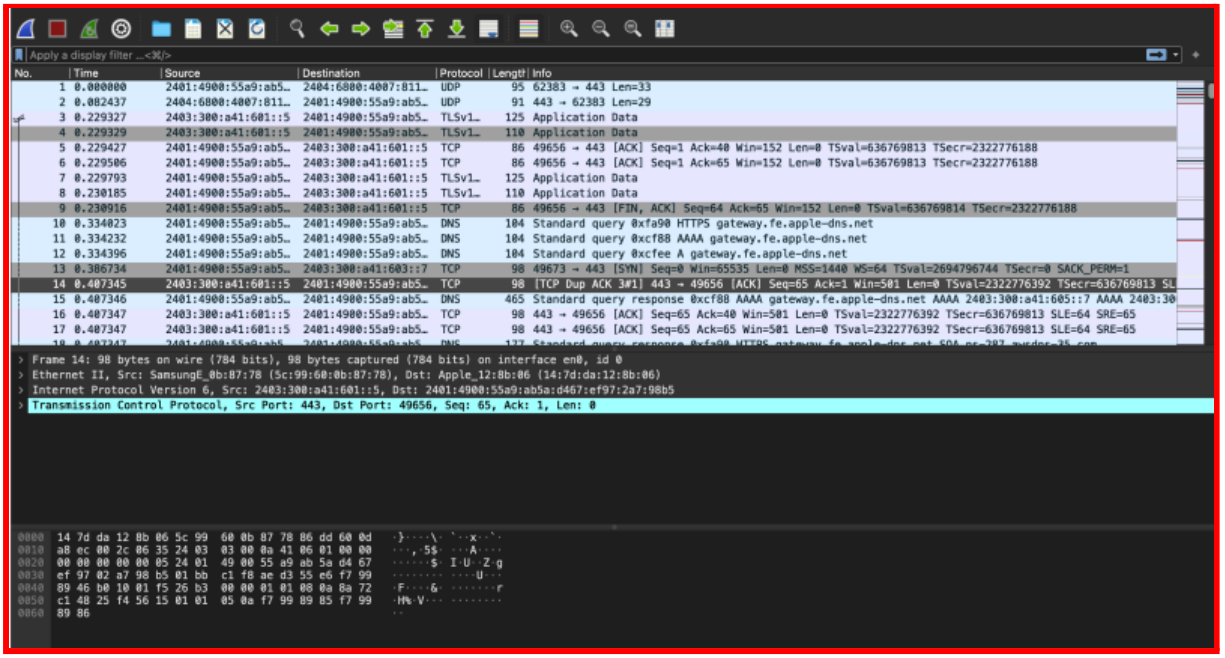
# Q) Demonstrate penetration testing using Wireshark.

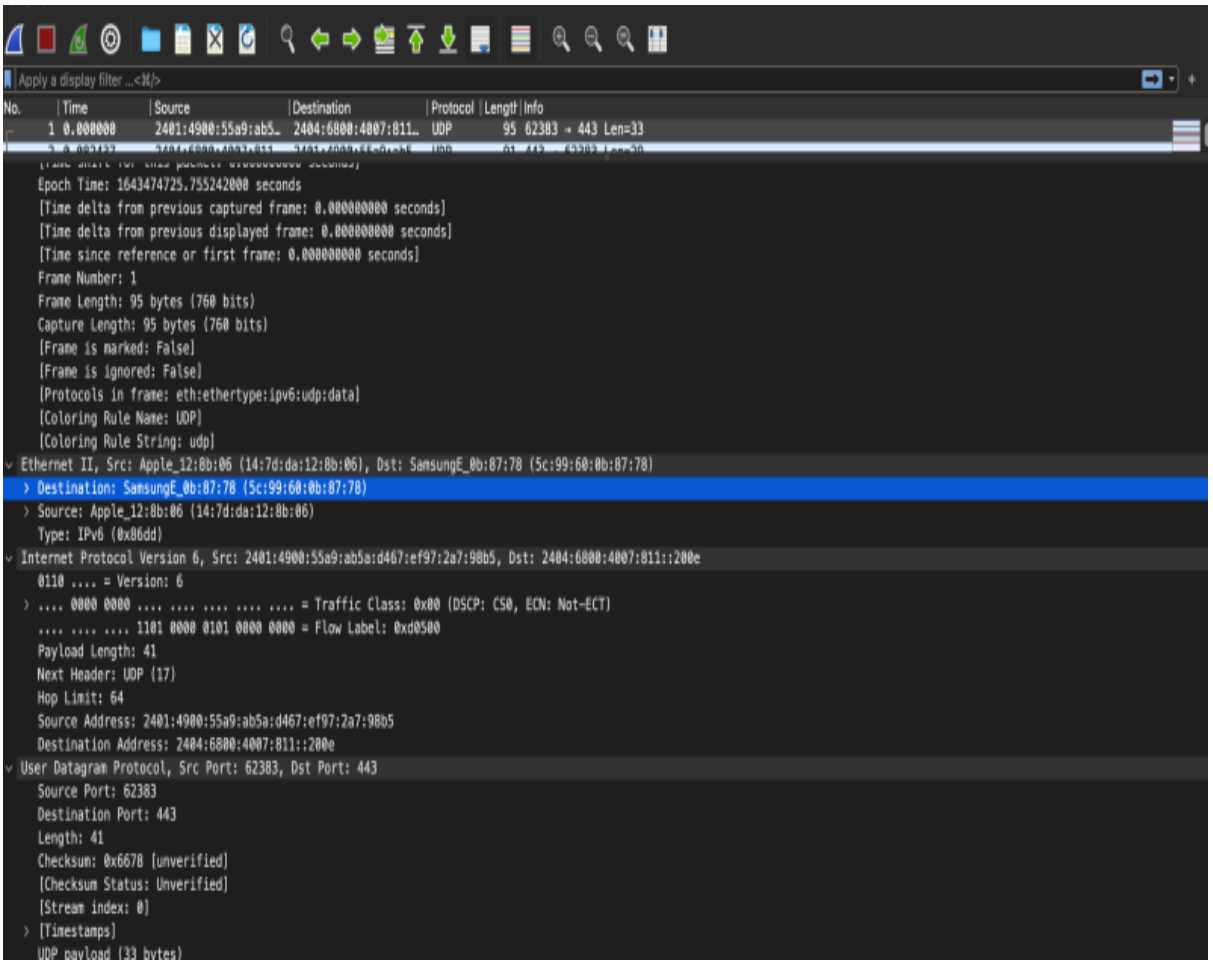
**ANS:**
**PROCEDURE:**

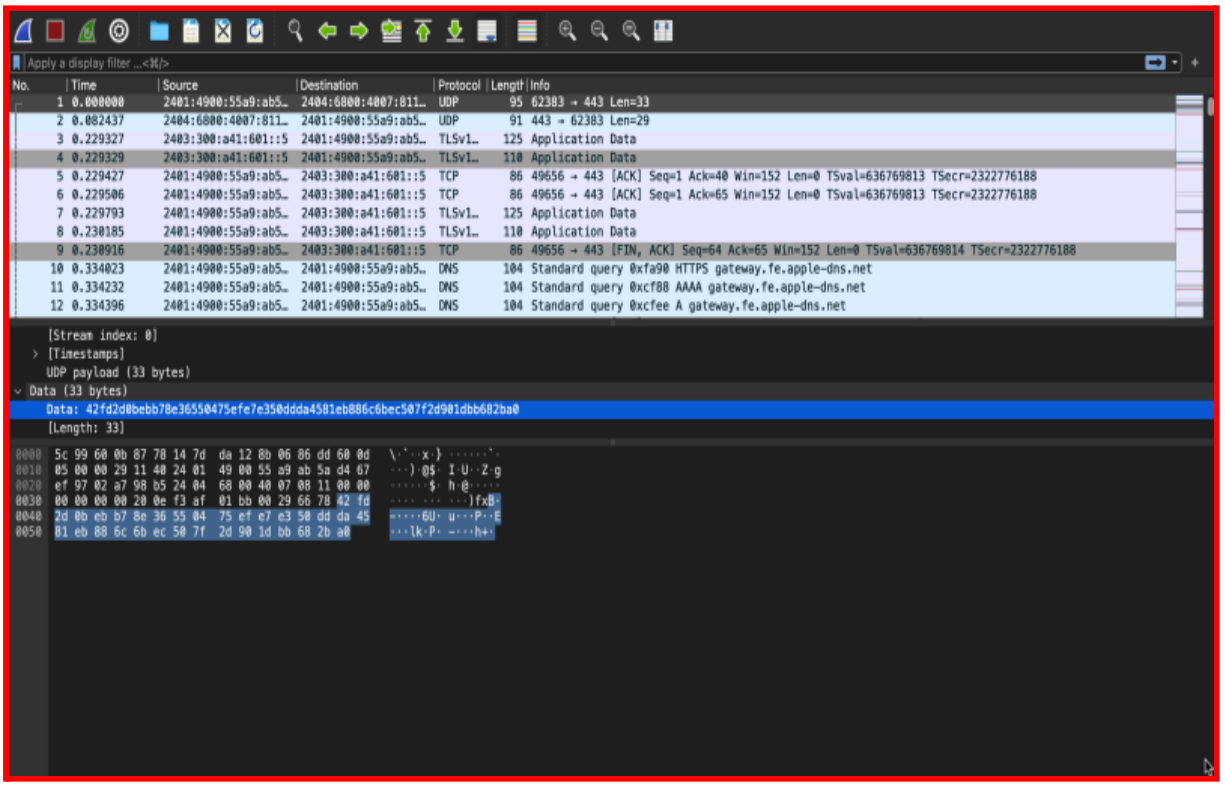
- Launch the Wireshark network analyzer.
- Then, in order to analyse the packet transfer in the network, select the wifi interface.
- The first panel shows all of the packets that are being transferred.
- Once a packet has been selected, the second panel displays information about that packet, including the source and destination IP addresses, packet length, protocol, and source and destination ports. It also contains the data in hexdecimal form that the packet carries.
- The third panel includes the encrypted data, which is displayed in hexadecimal format.
- The I/0 graph in the statistics panel can be used to further analyse network traffic, as it displays packet rate and tcp faults.

## Output

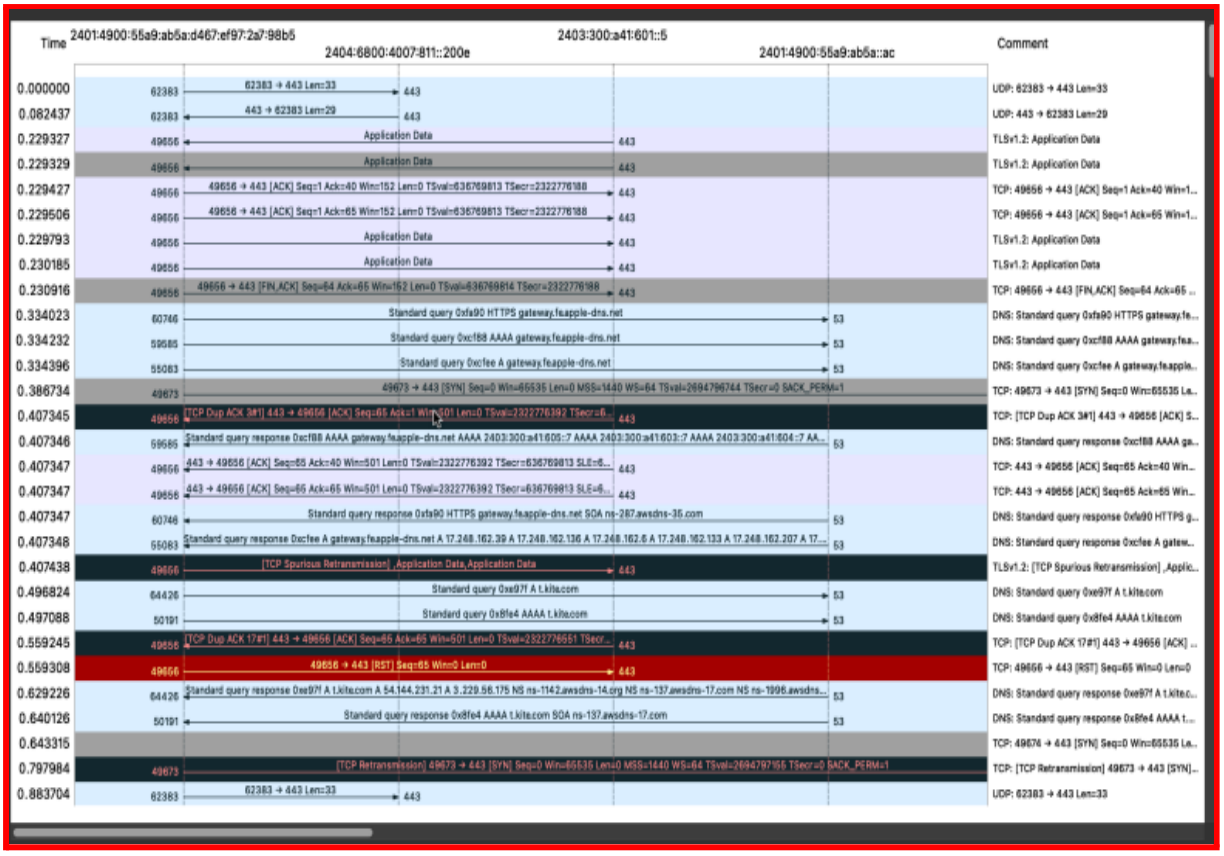

Apply a display filter ...<⌘/>
No. Time Source Destination Protocol Length Info
1 0.000000 2401:4900:55a9:ab5… 2404:6800:4007:811… UDP 95 62383 → 443 Len=33
2 0.082437 2404:6800:4007:811… 2401:4900:55a9:ab5… UDP 91 443 → 62383 Len=29
3 0.229327 2403:300:a41:601::5 2401:4900:55a9:ab5… TLSv1… 125 Application Data
4 0.229329 2403:300:a41:601::5 2401:4900:55a9:ab5… TLSv1… 110 Application Data
5 0.229427 2401:4900:55a9:ab5… 2403:300:a41:601::5 TCP 86 49656 → 443 [ACK] Seq=1 Ack=40 Win=152 Len=0 TSval=636769813 TSecr=2322776188
6 0.229506 2401:4900:55a9:ab5… 2403:300:a41:601::5 TCP 86 49656 → 443 [ACK] Seq=1 Ack=65 Win=152 Len=0 TSval=636769813 TSecr=2322776188
7 0.229793 2401:4900:55a9:ab5… 2403:300:a41:601::5 TLSv1… 125 Application Data
8 0.230185 2401:4900:55a9:ab5… 2403:300:a41:601::5 TLSv1… 110 Application Data
9 0.230916 2401:4900:55a9:ab5… 2403:300:a41:601::5 TCP 86 49656 → 443 [FIN, ACK] Seq=64 Ack=65 Win=152 Len=0 TSval=636769814 TSecr=2322776188
10 0.334023 2401:4900:55a9:ab5… 2401:4900:55a9:ab5… DNS 104 Standard query 0xfa90 HTTPS gateway.fe.apple-dns.net
11 0.334232 2401:4900:55a9:ab5… 2401:4900:55a9:ab5… DNS 104 Standard query 0xcf88 AAAA gateway.fe.apple-dns.net
12 0.334396 2401:4900:55a9:ab5… 2401:4900:55a9:ab5… DNS 104 Standard query 0xcfee A gateway.fe.apple-dns.net
13 0.386734 2401:4900:55a9:ab5… 2403:300:a41:603::7 TCP 98 49673 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=2694796744 TSecr=0 SACK_PERM=1
14 0.407345 2403:300:a41:601::5 2401:4900:55a9:ab5… TCP 98 [TCP Dup ACK 3#1] 443 → 49656 [ACK] Seq=65 Ack=1 Win=501 Len=0 TSval=2322776392 TSecr=636769813 SL
15 0.407346 2401:4900:55a9:ab5… 2401:4900:55a9:ab5… DNS 465 Standard query response 0xcf88 AAAA gateway.fe.apple-dns.net AAAA 2403:300:a41:605::7 AAAA 2403:30
16 0.407347 2403:300:a41:601::5 2401:4900:55a9:ab5… TCP 98 443 → 49656 [ACK] Seq=65 Ack=40 Win=501 Len=0 TSval=2322776392 TSecr=636769813 SLE=64 SRE=65
17 0.407347 2403:300:a41:601::5 2401:4900:55a9:ab5… TCP 98 443 → 49656 [ACK] Seq=65 Ack=65 Win=501 Len=0 TSval=2322776392 TSecr=636769813 SLE=64 SRE=65
Frame 14: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
Ethernet II, Src: SamsungE_0b:87:78 (5c:99:60:0b:87:78), Dst: Apple_12:8b:06 (14:7d:da:12:8b:06)
Internet Protocol Version 6, Src: 2403:300:a41:601::5, Dst: 2401:4900:55a9:ab5a:d467:ef97:2a7:98b5
Transmission Control Protocol, Src Port: 443, Dst Port: 49656, Seq: 65, Ack: 1, Len: 0
0000 14 7d da 12 8b 06 5c 99 60 0b 87 78 86 dd 60 0d
0010 a8 ec 00 2c 06 35 24 03 03 00 0a 41 06 01 00 00
0020 00 00 00 00 00 05 24 01 49 00 55 a9 ab 5a d4 67
0030 ef 97 02 a7 98 b5 01 bb c1 f8 ae d3 55 e6 f7 99
0040 89 46 b0 10 01 f5 26 b3 00 00 01 01 08 0a 8a 72
0050 c1 48 25 f4 56 15 01 01 05 0a f7 99 89 85 f7 99
0060 89 86

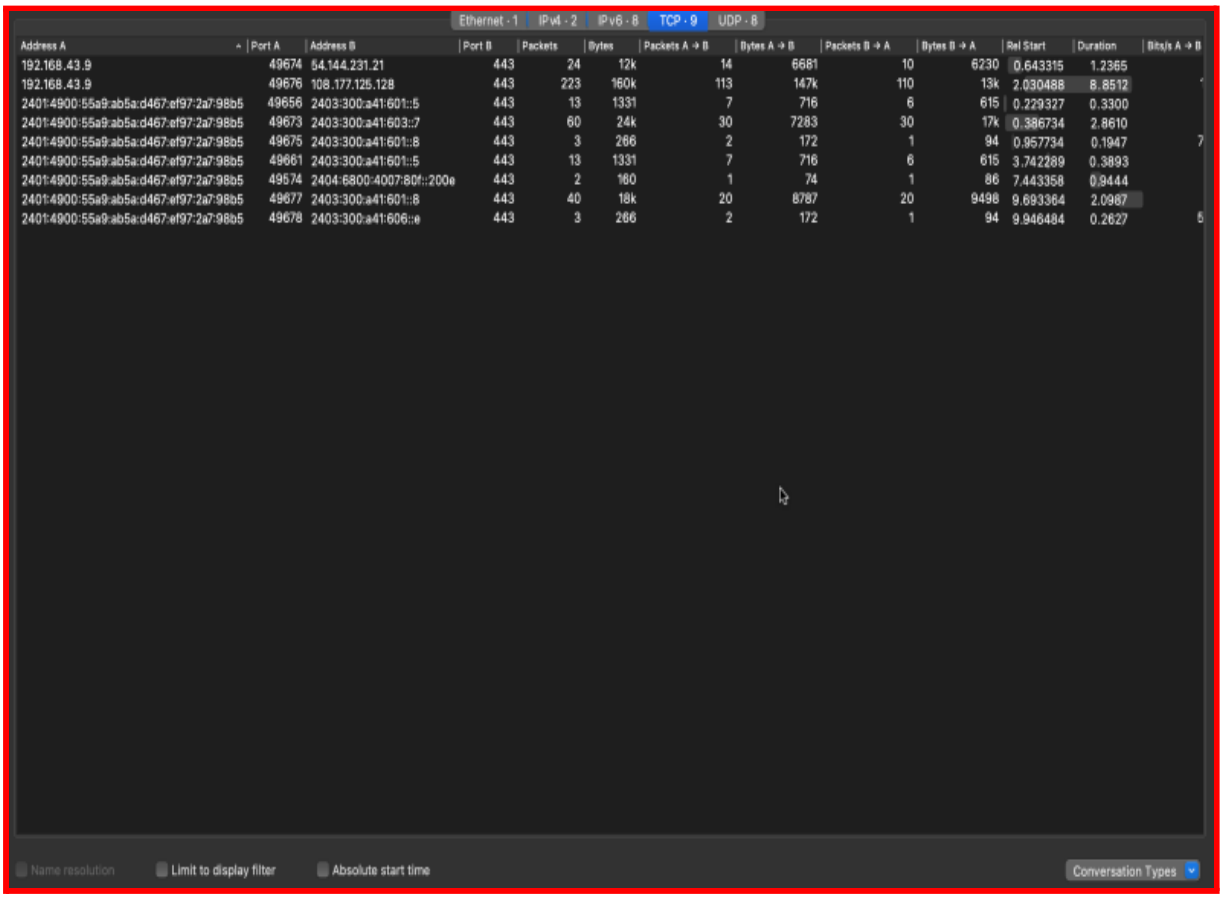

Apply a display filter ...<⌘/>
No. Time Source Destination Protocol Length Info
1 0.000000 2401:4900:55a9:ab5… 2404:6800:4007:811… UDP 95 62383 → 443 Len=33
2 0.082437 2404:6800:4007:811… 2401:4900:55a9:ab5… UDP 91 443 → 62383 Len=29
3 0.229327 2403:300:a41:601::5 2401:4900:55a9:ab5… TLSv1… 125 Application Data
4 0.229329 2403:300:a41:601::5 2401:4900:55a9:ab5… TLSv1… 110 Application Data
5 0.229427 2401:4900:55a9:ab5… 2403:300:a41:601::5 TCP 86 49656 → 443 [ACK] Seq=1 Ack=40 Win=152 Len=0 TSval=636769813 TSecr=2322776188
6 0.229506 2401:4900:55a9:ab5… 2403:300:a41:601::5 TCP 86 49656 → 443 [ACK] Seq=1 Ack=65 Win=152 Len=0 TSval=636769813 TSecr=2322776188
7 0.229793 2401:4900:55a9:ab5… 2403:300:a41:601::5 TLSv1… 125 Application Data
8 0.230185 2401:4900:55a9:ab5… 2403:300:a41:601::5 TLSv1… 110 Application Data
9 0.230916 2401:4900:55a9:ab5… 2403:300:a41:601::5 TCP 86 49656 → 443 [FIN, ACK] Seq=64 Ack=65 Win=152 Len=0 TSval=636769814 TSecr=2322776188
10 0.334023 2401:4900:55a9:ab5… 2401:4900:55a9:ab5… DNS 104 Standard query 0xfa90 HTTPS gateway.fe.apple-dns.net
11 0.334232 2401:4900:55a9:ab5… 2401:4900:55a9:ab5… DNS 104 Standard query 0xcf88 AAAA gateway.fe.apple-dns.net
12 0.334396 2401:4900:55a9:ab5… 2401:4900:55a9:ab5… DNS 104 Standard query 0xcfee A gateway.fe.apple-dns.net
13 0.386734 2401:4900:55a9:ab5… 2403:300:a41:603::7 TCP 98 49673 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=2694796744 TSecr=0 SACK_PERM=1
14 0.407345 2403:300:a41:601::5 2401:4900:55a9:ab5… TCP 98 [TCP Dup ACK 3#1] 443 → 49656 [ACK] Seq=65 Ack=1 Win=501 Len=0 TSval=2322776392 TSecr=636769813 SL
15 0.407346 2401:4900:55a9:ab5… 2401:4900:55a9:ab5… DNS 465 Standard query response 0xcf88 AAAA gateway.fe.apple-dns.net AAAA 2403:300:a41:605::7 AAAA 2403:30
16 0.407347 2403:300:a41:601::5 2401:4900:55a9:ab5… TCP 98 443 → 49656 [ACK] Seq=65 Ack=40 Win=501 Len=0 TSval=2322776392 TSecr=636769813 SLE=64 SRE=65
17 0.407347 2403:300:a41:601::5 2401:4900:55a9:ab5… TCP 98 443 → 49656 [ACK] Seq=65 Ack=65 Win=501 Len=0 TSval=2322776392 TSecr=636769813 SLE=64 SRE=65
Frame 14: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
Ethernet II, Src: SamsungE_0b:87:78 (5c:99:60:0b:87:78), Dst: Apple_12:8b:06 (14:7d:da:12:8b:06)
Internet Protocol Version 6, Src: 2403:300:a41:601::5, Dst: 2401:4900:55a9:ab5a:d467:ef97:2a7:98b5
Transmission Control Protocol, Src Port: 443, Dst Port: 49656, Seq: 65, Ack: 1, Len: 0
0000 14 7d da 12 8b 06 5c 99 60 0b 87 78 86 dd 60 0d
0010 a8 ec 00 2c 06 35 24 03 03 00 0a 41 06 01 00 00
0020 00 00 00 00 00 05 24 01 49 00 55 a9 ab 5a d4 67
0030 ef 97 02 a7 98 b5 01 bb c1 f8 ae d3 55 e6 f7 99
0040 89 46 b0 10 01 f5 26 b3 00 00 01 01 08 0a 8a 72
0050 c1 48 25 f4 56 15 01 01 05 0a f7 99 89 85 f7 99
0060 89 86


Apply a display filter ...<⌘/>
No. Time Source Destination Protocol Length Info
1 0.000000 2401:4900:55a9:ab5… 2404:6800:4007:811… UDP 95 62383 → 443 Len=33
Epoch Time: 1643474725.755242000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 95 bytes (760 bits)
Capture Length: 95 bytes (760 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ipv6:udp:data]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Apple_12:8b:06 (14:7d:da:12:8b:06), Dst: SamsungE_0b:87:78 (5c:99:60:0b:87:78)
Destination: SamsungE_0b:87:78 (5c:99:60:0b:87:78)
Source: Apple_12:8b:06 (14:7d:da:12:8b:06)
Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: 2401:4900:55a9:ab5a:d467:ef97:2a7:98b5, Dst: 2404:6800:4007:811::200e
0110 .... = Version: 6
.... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
.... .... .... 1101 0000 0101 0000 0000 = Flow Label: 0xd0500
Payload Length: 41
Next Header: UDP (17)
Hop Limit: 64
Source Address: 2401:4900:55a9:ab5a:d467:ef97:2a7:98b5
Destination Address: 2404:6800:4007:811::200e
User Datagram Protocol, Src Port: 62383, Dst Port: 443
Source Port: 62383
Destination Port: 443
Length: 41
Checksum: 0x6678 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
UDP payload (33 bytes)


Apply a display filter ...<⌘/>
No. Time Source Destination Protocol Length Info
1 0.000000 2401:4900:55a9:ab5… 2404:6800:4007:811… UDP 95 62383 → 443 Len=33
2 0.082437 2404:6800:4007:811… 2401:4900:55a9:ab5… UDP 91 443 → 62383 Len=29
3 0.229327 2403:300:a41:601::5 2401:4900:55a9:ab5… TLSv1… 125 Application Data
4 0.229329 2403:300:a41:601::5 2401:4900:55a9:ab5… TLSv1… 110 Application Data
5 0.229427 2401:4900:55a9:ab5… 2403:300:a41:601::5 TCP 86 49656 → 443 [ACK] Seq=1 Ack=40 Win=152 Len=0 TSval=636769813 TSecr=2322776188
6 0.229506 2401:4900:55a9:ab5… 2403:300:a41:601::5 TCP 86 49656 → 443 [ACK] Seq=1 Ack=65 Win=152 Len=0 TSval=636769813 TSecr=2322776188
7 0.229793 2401:4900:55a9:ab5… 2403:300:a41:601::5 TLSv1… 125 Application Data
8 0.230185 2401:4900:55a9:ab5… 2403:300:a41:601::5 TLSv1… 110 Application Data
9 0.230916 2401:4900:55a9:ab5… 2403:300:a41:601::5 TCP 86 49656 → 443 [FIN, ACK] Seq=64 Ack=65 Win=152 Len=0 TSval=636769814 TSecr=2322776188
10 0.334023 2401:4900:55a9:ab5… 2401:4900:55a9:ab5… DNS 104 Standard query 0xfa90 HTTPS gateway.fe.apple-dns.net
11 0.334232 2401:4900:55a9:ab5… 2401:4900:55a9:ab5… DNS 104 Standard query 0xcf88 AAAA gateway.fe.apple-dns.net
12 0.334396 2401:4900:55a9:ab5… 2401:4900:55a9:ab5… DNS 104 Standard query 0xcfee A gateway.fe.apple-dns.net
[Stream index: 0]
[Timestamps]
UDP payload (33 bytes)
Data (33 bytes)
Data: 42fd2d0bebb78e36550475efe7e350ddda4581eb886c6bec507f2d901dbb682ba0
[Length: 33]
0000 5c 99 60 0b 87 78 14 7d da 12 8b 06 86 dd 60 0d
0010 05 00 00 29 11 40 24 01 49 00 55 a9 ab 5a d4 67
0020 ef 97 02 a7 98 b5 24 04 68 00 40 07 08 11 00 00
0030 00 00 00 00 20 0e f3 af 01 bb 00 29 66 78 42 fd
0040 2d 0b eb b7 8e 36 55 04 75 ef e7 e3 50 dd da 45
0050 81 eb 88 6c 6b ec 50 7f 2d 90 1d bb 68 2b a0


Wireshark I/O Graphs: Wi-Fi: en0
100
75
50
25
0
Packets/1 sec
0
2.5
5
7.5
10
Time (s)
Click to select packet 323 (0s = 0).
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
All Packets
Line
Packets
None
TCP Errors
tcp.analysis....
Bar
Packets
None
Filtered pack...
Line
Packets
None


Time
2401:4900:55a9:ab5a:d467:ef97:2a7:98b5
2404:6800:4007:811::200e
2403:300:a41:601::5
2401:4900:55a9:ab5a::ac
Comment
0.000000 62383 62383 → 443 Len=33 443 UDP: 62383 → 443 Len=33
0.082437 62383 443 → 62383 Len=29 443 UDP: 443 → 62383 Len=29
0.229327 49656 Application Data 443 TLSv1.2: Application Data
0.229329 49656 Application Data 443 TLSv1.2: Application Data
0.229427 49656 49656 → 443 [ACK] Seq=1 Ack=40 Win=152 Len=0 TSval=636769813 TSecr=2322776188 443 TCP: 49656 → 443 [ACK] Seq=1 Ack=40 Win=1...
0.229506 49656 49656 → 443 [ACK] Seq=1 Ack=65 Win=152 Len=0 TSval=636769813 TSecr=2322776188 443 TCP: 49656 → 443 [ACK] Seq=1 Ack=65 Win=1...
0.229793 49656 Application Data 443 TLSv1.2: Application Data
0.230185 49656 Application Data 443 TLSv1.2: Application Data
0.230916 49656 49656 → 443 [FIN,ACK] Seq=64 Ack=65 Win=152 Len=0 TSval=636769814 TSecr=2322776188 443 TCP: 49656 → 443 [FIN,ACK] Seq=64 Ack=65 ...
0.334023 60746 Standard query 0xfa90 HTTPS gateway.fe.apple-dns.net 53 DNS: Standard query 0xfa90 HTTPS gateway.fe...
0.334232 59585 Standard query 0xcf88 AAAA gateway.fe.apple-dns.net 53 DNS: Standard query 0xcf88 AAAA gateway.fea...
0.334396 55083 Standard query 0xcfee A gateway.fe.apple-dns.net 53 DNS: Standard query 0xcfee A gateway.fe.apple...
0.386734 49673 49673 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=2694796744 TSecr=0 SACK_PERM=1 TCP: 49673 → 443 [SYN] Seq=0 Win=65535 Le...
0.407345 49656 [TCP Dup ACK 3#1] 443 → 49656 [ACK] Seq=65 Ack=1 Win=501 Len=0 TSval=2322776392 TSecr=6... 443 TCP: [TCP Dup ACK 3#1] 443 → 49656 [ACK] S...
0.407346 59585 Standard query response 0xcf88 AAAA gateway.fe.apple-dns.net AAAA 2403:300:a41:605::7 AAAA 2403:300:a41:603::7 AAAA 2403:300:a41:604::7 AA... 53 DNS: Standard query response 0xcf88 AAAA ga...
0.407347 49656 443 → 49656 [ACK] Seq=65 Ack=40 Win=501 Len=0 TSval=2322776392 TSecr=636769813 SLE=6... 443 TCP: 443 → 49656 [ACK] Seq=65 Ack=40 Win...
0.407347 49656 443 → 49656 [ACK] Seq=65 Ack=65 Win=501 Len=0 TSval=2322776392 TSecr=636769813 SLE=6... 443 TCP: 443 → 49656 [ACK] Seq=65 Ack=65 Win...
0.407347 60746 Standard query response 0xfa90 HTTPS gateway.fe.apple-dns.net SOA ns-287.awsdns-35.com 53 DNS: Standard query response 0xfa90 HTTPS g...
0.407348 55083 Standard query response 0xcfee A gateway.fe.apple-dns.net A 17.248.162.39 A 17.248.162.136 A 17.248.162.6 A 17.248.162.133 A 17.248.162.207 A 17... 53 DNS: Standard query response 0xcfee A gatew...
0.407438 49656 [TCP Spurious Retransmission] , Application Data, Application Data 443 TLSv1.2: [TCP Spurious Retransmission] , Applic...
0.496824 64426 Standard query 0xe97f A t.kite.com 53 DNS: Standard query 0xe97f A t.kite.com
0.497088 50191 Standard query 0x8fe4 AAAA t.kite.com 53 DNS: Standard query 0x8fe4 AAAA t.kite.com
0.559245 49656 [TCP Dup ACK 17#1] 443 → 49656 [ACK] Seq=65 Ack=65 Win=501 Len=0 TSval=2322776551 TSecr... 443 TCP: [TCP Dup ACK 17#1] 443 → 49656 [ACK] ...
0.559308 49656 49656 → 443 [RST] Seq=65 Win=0 Len=0 443 TCP: 49656 → 443 [RST] Seq=65 Win=0 Len=0
0.629226 64426 Standard query response 0xe97f A t.kite.com A 54.144.231.21 A 3.229.56.175 NS ns-1142.awsdns-14.org NS ns-137.awsdns-17.com NS ns-1996.awsdns... 53 DNS: Standard query response 0xe97f A t.kite.c...
0.640126 50191 Standard query response 0x8fe4 AAAA t.kite.com SOA ns-137.awsdns-17.com 53 DNS: Standard query response 0x8fe4 AAAA t....
0.643315 TCP: 49674 → 443 [SYN] Seq=0 Win=65535 Le...
0.797984 49673 [TCP Retransmission] 49673 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=2694797155 TSecr=0 SACK_PERM=1 TCP: [TCP Retransmission] 49673 → 443 [SYN]...
0.883704 62383 62383 → 443 Len=33 443 UDP: 62383 → 443 Len=33


Ethernet · 1
IPv4 · 2
IPv6 · 8
TCP · 9
UDP · 8
Address A | Port A | Address B | Port B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration | Bits/s A → B
192.168.43.9 49674 54.144.231.21 443 24 12k 14 6681 10 6230 0.643315 1.2365
192.168.43.9 49676 108.177.125.128 443 223 160k 113 147k 110 13k 2.030488 8.8512
2401:4900:55a9:ab5a:d467:ef97:2a7:98b5 49656 2403:300:a41:601::5 443 13 1331 7 716 6 615 0.229327 0.3300
2401:4900:55a9:ab5a:d467:ef97:2a7:98b5 49673 2403:300:a41:603::7 443 60 24k 30 7283 30 17k 0.386734 2.8610
2401:4900:55a9:ab5a:d467:ef97:2a7:98b5 49675 2403:300:a41:601::8 443 3 266 2 172 1 94 0.957734 0.1947
2401:4900:55a9:ab5a:d467:ef97:2a7:98b5 49661 2403:300:a41:601::5 443 13 1331 7 716 6 615 3.742289 0.3893
2401:4900:55a9:ab5a:d467:ef97:2a7:98b5 49674 2404:6800:4007:80f::200e 443 2 160 1 74 1 86 7.443358 0.9444
2401:4900:55a9:ab5a:d467:ef97:2a7:98b5 49677 2403:300:a41:601::8 443 40 18k 20 8787 20 9498 9.693364 2.0987
2401:4900:55a9:ab5a:d467:ef97:2a7:98b5 49678 2403:300:a41:606::e 443 3 266 2 172 1 94 9.946484 0.2627
Name resolution
Limit to display filter
Absolute start time
Conversation Types