Task 3 – Network Packet Sniffing and Analysis

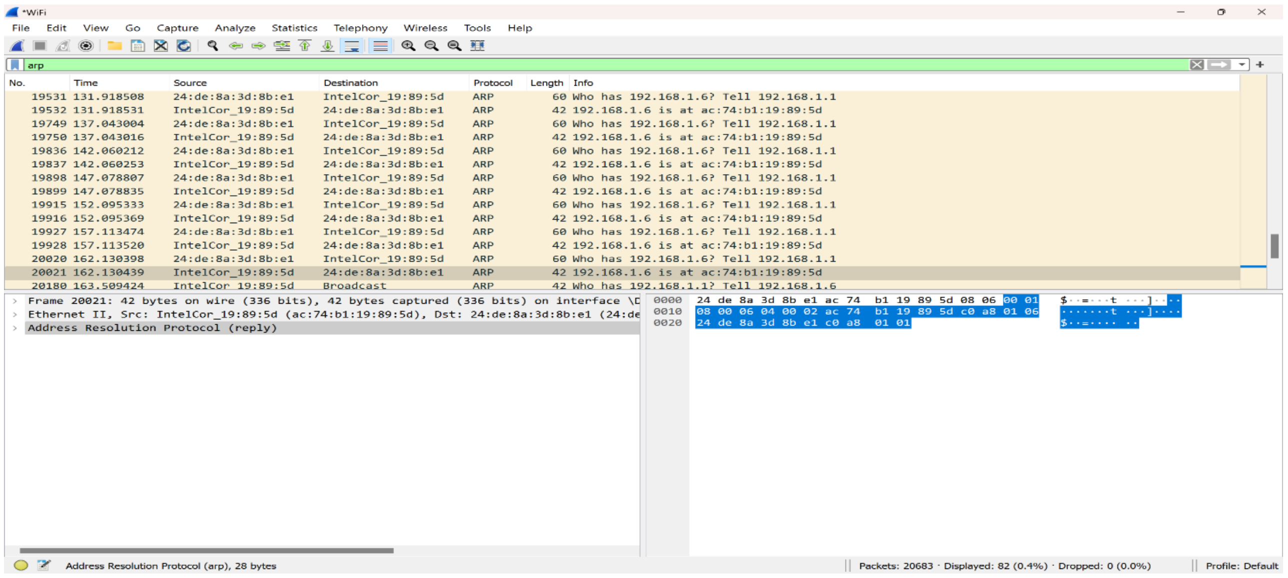
Objective:
Capture and analyze network traffic to demonstrate broadcast and unicast behavior, HTTP/HTTPS communication, and associated network-level security risks.

Tools & Setup:

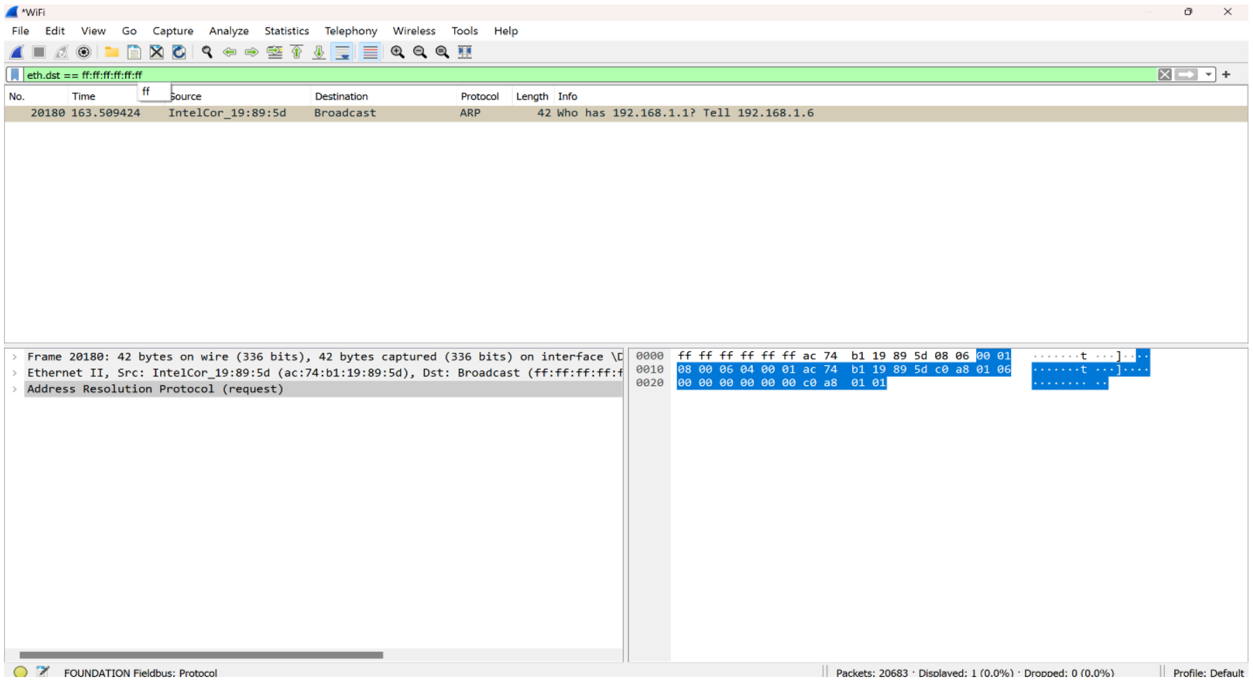
- Wireshark (Windows)
- Interface: Active Ethernet/Wi-Fi interface
- Filters Applied:
    - arp → ARP broadcast requests
    - eth.dst == ff:ff:ff:ff:ff:ff → broadcast packets
    - !eth.dst == ff:ff:ff:ff:ff:ff → unicast packets
    - http.request → HTTP traffic
    - tls / tcp.port == 443 → HTTPS traffic
- Environment: Lab machine, connected to local network; VPN disabled to observe unencrypted traffic.

PoC Procedure & Observations:

1. **Broadcast Traffic – ARP Request**
    - **Action:** Triggered ARP broadcast packets by running the arp command in Windows while capturing in Wireshark.
    - **Captured Packet:**
      Frame 20180: 42 bytes
      Src MAC/IP: ac:74:b1:XX:XX:XX / 192.168.1.6
      Dst MAC/IP: FF:FF:FF:FF:FF:FF / 192.168.1.255
      Protocol: ARP Request
    - **Analysis:**
        - Broadcast packet sent to all devices on LAN.
        - Demonstrates network discovery at Layer 2.
        - VAPT Relevance: Potential for reconnaissance and ARP spoofing attacks.


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
arp

No.   Time       Source             Destination        Protocol Length Info
19531 131.918508 24:de:8a:3d:8b:e1  IntelCor_19:89:5d  ARP      60 Who has 192.168.1.6? Tell 192.168.1.1
19532 131.918531 IntelCor_19:89:5d  24:de:8a:3d:8b:e1  ARP      42 192.168.1.6 is at ac:74:b1:19:89:5d
19749 137.043004 24:de:8a:3d:8b:e1  IntelCor_19:89:5d  ARP      60 Who has 192.168.1.6? Tell 192.168.1.1
19750 137.043016 IntelCor_19:89:5d  24:de:8a:3d:8b:e1  ARP      42 192.168.1.6 is at ac:74:b1:19:89:5d
19836 142.060212 24:de:8a:3d:8b:e1  IntelCor_19:89:5d  ARP      60 Who has 192.168.1.6? Tell 192.168.1.1
19837 142.060253 IntelCor_19:89:5d  24:de:8a:3d:8b:e1  ARP      42 192.168.1.6 is at ac:74:b1:19:89:5d
19898 147.078807 24:de:8a:3d:8b:e1  IntelCor_19:89:5d  ARP      60 Who has 192.168.1.6? Tell 192.168.1.1
19899 147.078835 IntelCor_19:89:5d  24:de:8a:3d:8b:e1  ARP      42 192.168.1.6 is at ac:74:b1:19:89:5d
19915 152.095333 24:de:8a:3d:8b:e1  IntelCor_19:89:5d  ARP      60 Who has 192.168.1.6? Tell 192.168.1.1
19916 152.095369 IntelCor_19:89:5d  24:de:8a:3d:8b:e1  ARP      42 192.168.1.6 is at ac:74:b1:19:89:5d
19927 157.113474 24:de:8a:3d:8b:e1  IntelCor_19:89:5d  ARP      60 Who has 192.168.1.6? Tell 192.168.1.1
19928 157.113520 IntelCor_19:89:5d  24:de:8a:3d:8b:e1  ARP      42 192.168.1.6 is at ac:74:b1:19:89:5d
20020 162.130398 24:de:8a:3d:8b:e1  IntelCor_19:89:5d  ARP      60 Who has 192.168.1.6? Tell 192.168.1.1
20021 162.130439 IntelCor_19:89:5d  24:de:8a:3d:8b:e1  ARP      42 192.168.1.6 is at ac:74:b1:19:89:5d
20180 163.509424 IntelCor_19:89:5d  Broadcast          ARP      42 Who has 192.168.1.1? Tell 192.168.1.6

> Frame 20021: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \D
> Ethernet II, Src: IntelCor_19:89:5d (ac:74:b1:19:89:5d), Dst: 24:de:8a:3d:8b:e1 (24:de
> Address Resolution Protocol (reply)

0000  24 de 8a 3d 8b e1 ac 74  b1 19 89 5d 08 06 00 01   $··=···t ···]····
0010  08 00 06 04 00 02 ac 74  b1 19 89 5d c0 a8 01 06   ·······t ···]····
0020  24 de 8a 3d 8b e1 c0 a8  01 01                     $··=···· ··

Address Resolution Protocol (arp), 28 bytes    Packets: 20683 · Displayed: 82 (0.4%) · Dropped: 0 (0.0%)    Profile: Default
```

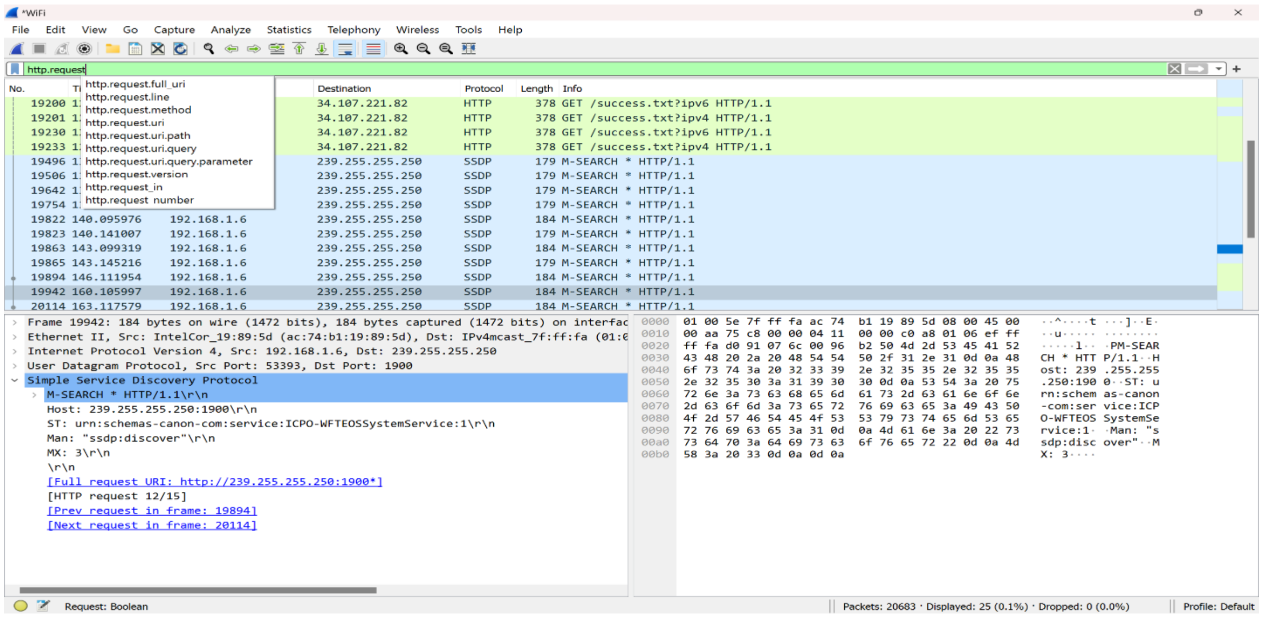

*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ff

```
eth.dst == ff:ff:ff:ff:ff:ff

No.   Time       Source             Destination  Protocol Length Info
20180 163.509424 IntelCor_19:89:5d  Broadcast    ARP      42 Who has 192.168.1.1? Tell 192.168.1.6

> Frame 20180: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \D
> Ethernet II, Src: IntelCor_19:89:5d (ac:74:b1:19:89:5d), Dst: Broadcast (ff:ff:ff:ff:f
> Address Resolution Protocol (request)

0000  ff ff ff ff ff ff ac 74  b1 19 89 5d 08 06 00 01   ·······t ···]····
0010  08 00 06 04 00 01 ac 74  b1 19 89 5d c0 a8 01 06   ·······t ···]····
0020  00 00 00 00 00 00 c0 a8  01 01                     ········ ··

FOUNDATION Fieldbus: Protocol    Packets: 20683 · Displayed: 1 (0.0%) · Dropped: 0 (0.0%)    Profile: Default
```

2. **Unicast Traffic – HTTP Request**

   - **Captured Packet:**
     Frame 19193: 361 bytes
     Src MAC/IP: ac:74:b1:XX:XX:XX / 192.168.1.6
     Dst MAC/IP: 24:de:8a:3d:8b:e1 / 34.107.221.82
     Protocol: TCP / HTTP GET /canonical.html

- **Analysis:**
    - Sent to a specific server (unicast).
    - HTTP headers and URL are unencrypted.
    - VAPT Relevance: Demonstrates data exposure risks on unencrypted channels.



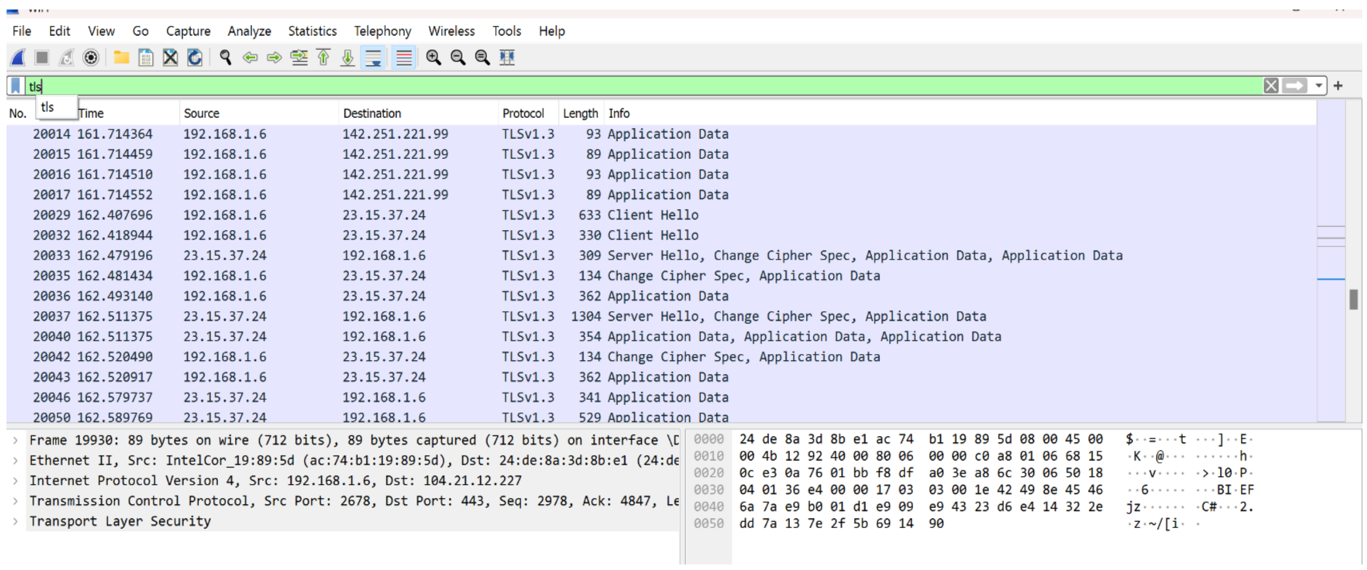
```
No.   Ti                     Destination       Protocol  Length Info
19200 1                      34.107.221.82     HTTP      378 GET /success.txt?ipv6 HTTP/1.1
19201 1                      34.107.221.82     HTTP      378 GET /success.txt?ipv4 HTTP/1.1
19230 1                      34.107.221.82     HTTP      378 GET /success.txt?ipv6 HTTP/1.1
19233 1                      34.107.221.82     HTTP      378 GET /success.txt?ipv4 HTTP/1.1
19496 1                      239.255.255.250   SSDP      179 M-SEARCH * HTTP/1.1
19506 1                      239.255.255.250   SSDP      179 M-SEARCH * HTTP/1.1
19642 1                      239.255.255.250   SSDP      179 M-SEARCH * HTTP/1.1
19754 1                      239.255.255.250   SSDP      179 M-SEARCH * HTTP/1.1
19822 140.095976 192.168.1.6 239.255.255.250   SSDP      184 M-SEARCH * HTTP/1.1
19823 140.141007 192.168.1.6 239.255.255.250   SSDP      179 M-SEARCH * HTTP/1.1
19863 143.099319 192.168.1.6 239.255.255.250   SSDP      184 M-SEARCH * HTTP/1.1
19865 143.145216 192.168.1.6 239.255.255.250   SSDP      179 M-SEARCH * HTTP/1.1
19894 146.111954 192.168.1.6 239.255.255.250   SSDP      184 M-SEARCH * HTTP/1.1
19942 160.105997 192.168.1.6 239.255.255.250   SSDP      184 M-SEARCH * HTTP/1.1
20114 163.117579 192.168.1.6 239.255.255.250   SSDP      184 M-SEARCH * HTTP/1.1
```

```
> Frame 19942: 184 bytes on wire (1472 bits), 184 bytes captured (1472 bits) on interfac
> Ethernet II, Src: IntelCor_19:89:5d (ac:74:b1:19:89:5d), Dst: IPv4mcast_7f:ff:fa (01:0
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 53393, Dst Port: 1900
v Simple Service Discovery Protocol
  > M-SEARCH * HTTP/1.1\r\n
    Host: 239.255.255.250:1900\r\n
    ST: urn:schemas-canon-com:service:ICPO-WFTEOSSystemService:1\r\n
    Man: "ssdp:discover"\r\n
    MX: 3\r\n
    \r\n
    [Full request URI: http://239.255.255.250:1900*]
    [HTTP request 12/15]
    [Prev request in frame: 19894]
    [Next request in frame: 20114]
```

```
0000  01 00 5e 7f ff fa ac 74  b1 19 89 5d 08 00 45 00   ··^····t ···]··E·
0010  00 aa 75 c8 00 00 04 11  00 00 c0 a8 01 06 ef ff   ··u····· ········
0020  ff fa d0 91 07 6c 00 96  b2 50 4d 2d 53 45 41 52   ·····l·· ·PM-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  6f 73 74 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   ost: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 53 54 3a 20 75   .250:190 0··ST: u
0060  72 6e 3a 73 63 68 65 6d  61 73 2d 63 61 6e 6f 6e   rn:schem as-canon
0070  2d 63 6f 6d 3a 73 65 72  76 69 63 65 3a 49 43 50   -com:ser vice:ICP
0080  4f 2d 57 46 54 45 4f 53  53 79 73 74 65 6d 53 65   O-WFTEOS SystemSe
0090  72 76 69 63 65 3a 31 0d  0a 4d 61 6e 3a 20 22 73   rvice:1· ·Man: "s
00a0  73 64 70 3a 64 69 73 63  6f 76 65 72 22 0d 0a 4d   sdp:disc over"··M
00b0  58 3a 20 33 0d 0a 0d 0a                            X: 3····
```

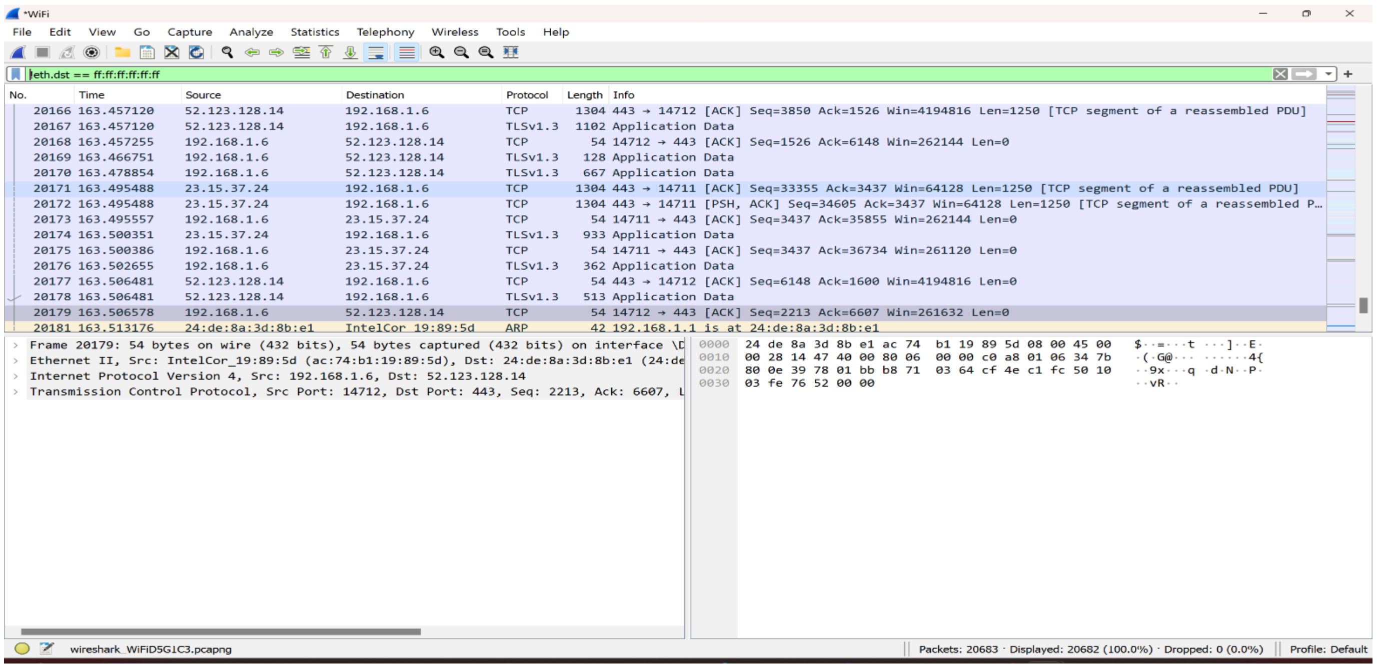
Request: Boolean | Packets: 20683 · Displayed: 25 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

3. **Encrypted Traffic – HTTPS / TLS**
    - **Captured Packet:**
      Protocol: TLS 1.3 handshake
      Src/Dst IPs visible; payload encrypted
    - **Analysis:**
    - Content is encrypted; only metadata visible.
    - VAPT Relevance: Shows protection against eavesdropping and MITM attacks.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls

```
No.   Time        Source        Destination     Protocol Length Info
20014 161.714364  192.168.1.6   142.251.221.99  TLSv1.3    93 Application Data
20015 161.714459  192.168.1.6   142.251.221.99  TLSv1.3    89 Application Data
20016 161.714510  192.168.1.6   142.251.221.99  TLSv1.3    93 Application Data
20017 161.714552  192.168.1.6   142.251.221.99  TLSv1.3    89 Application Data
20029 162.407696  192.168.1.6   23.15.37.24     TLSv1.3   633 Client Hello
20032 162.418944  192.168.1.6   23.15.37.24     TLSv1.3   330 Client Hello
20033 162.479196  23.15.37.24   192.168.1.6     TLSv1.3   309 Server Hello, Change Cipher Spec, Application Data, Application Data
20035 162.481434  192.168.1.6   23.15.37.24     TLSv1.3   134 Change Cipher Spec, Application Data
20036 162.493140  192.168.1.6   23.15.37.24     TLSv1.3   362 Application Data
20037 162.511375  23.15.37.24   192.168.1.6     TLSv1.3  1304 Server Hello, Change Cipher Spec, Application Data
20040 162.511375  23.15.37.24   192.168.1.6     TLSv1.3   354 Application Data, Application Data, Application Data
20042 162.520490  192.168.1.6   23.15.37.24     TLSv1.3   134 Change Cipher Spec, Application Data
20043 162.520917  192.168.1.6   23.15.37.24     TLSv1.3   362 Application Data
20046 162.579737  23.15.37.24   192.168.1.6     TLSv1.3   341 Application Data
20050 162.589769  23.15.37.24   192.168.1.6     TLSv1.3   529 Application Data

> Frame 19930: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \D
> Ethernet II, Src: IntelCor_19:89:5d (ac:74:b1:19:89:5d), Dst: 24:de:8a:3d:8b:e1 (24:de
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 104.21.12.227
> Transmission Control Protocol, Src Port: 2678, Dst Port: 443, Seq: 2978, Ack: 4847, Le
> Transport Layer Security

0000  24 de 8a 3d 8b e1 ac 74  b1 19 89 5d 08 00 45 00   $··=···t ···]··E·
0010  00 4b 12 92 40 00 80 06  00 00 c0 a8 01 06 68 15   ·K··@··· ······h·
0020  0c e3 0a 76 01 bb f8 df  a0 3e a8 6c 30 06 50 18   ···v···· ·>·l0·P·
0030  04 01 36 e4 00 00 17 03  03 00 1e 42 49 8e 45 46   ··6····· ···BI·EF
0040  6a 7a e9 b0 01 d1 e9 09  e9 43 23 d6 e4 14 32 2e   jz······ ·C#···2.
0050  dd 7a 13 7e 2f 5b 69 14  90                        ·z·~/[i· ·
```



*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
eth.dst == ff:ff:ff:ff:ff:ff

```
No.   Time        Source             Destination        Protocol Length Info
20166 163.457120  52.123.128.14      192.168.1.6        TCP      1304 443 → 14712 [ACK] Seq=3850 Ack=1526 Win=4194816 Len=1250 [TCP segment of a reassembled PDU]
20167 163.457120  52.123.128.14      192.168.1.6        TLSv1.3  1102 Application Data
20168 163.457255  192.168.1.6        52.123.128.14      TCP        54 14712 → 443 [ACK] Seq=1526 Ack=6148 Win=262144 Len=0
20169 163.466751  192.168.1.6        52.123.128.14      TLSv1.3   128 Application Data
20170 163.478854  192.168.1.6        52.123.128.14      TLSv1.3   667 Application Data
20171 163.495488  23.15.37.24        192.168.1.6        TCP      1304 443 → 14711 [ACK] Seq=33355 Ack=3437 Win=64128 Len=1250 [TCP segment of a reassembled PDU]
20172 163.495488  23.15.37.24        192.168.1.6        TCP      1304 443 → 14711 [PSH, ACK] Seq=34605 Ack=3437 Win=64128 Len=1250 [TCP segment of a reassembled P…
20173 163.495557  192.168.1.6        23.15.37.24        TCP        54 14711 → 443 [ACK] Seq=3437 Ack=35855 Win=262144 Len=0
20174 163.500351  23.15.37.24        192.168.1.6        TLSv1.3   933 Application Data
20175 163.500386  192.168.1.6        23.15.37.24        TCP        54 14711 → 443 [ACK] Seq=3437 Ack=36734 Win=261120 Len=0
20176 163.502655  192.168.1.6        23.15.37.24        TLSv1.3   362 Application Data
20177 163.506481  52.123.128.14      192.168.1.6        TCP        54 443 → 14712 [ACK] Seq=6148 Ack=1600 Win=4194816 Len=0
20178 163.506481  52.123.128.14      192.168.1.6        TLSv1.3   513 Application Data
20179 163.506578  192.168.1.6        52.123.128.14      TCP        54 14712 → 443 [ACK] Seq=2213 Ack=6607 Win=261632 Len=0
20181 163.513176  24:de:8a:3d:8b:e1  IntelCor_19:89:5d  ARP        42 192.168.1.1 is at 24:de:8a:3d:8b:e1

> Frame 20179: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \D
> Ethernet II, Src: IntelCor_19:89:5d (ac:74:b1:19:89:5d), Dst: 24:de:8a:3d:8b:e1 (24:de
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 52.123.128.14
> Transmission Control Protocol, Src Port: 14712, Dst Port: 443, Seq: 2213, Ack: 6607, L

0000  24 de 8a 3d 8b e1 ac 74  b1 19 89 5d 08 00 45 00   $··=···t ···]··E·
0010  00 28 14 47 40 00 80 06  00 00 c0 a8 01 06 34 7b   ·(·G@··· ······4{
0020  80 0e 39 78 01 bb b8 71  03 64 cf 4e c1 fc 50 10   ··9x···q ·d·N··P·
0030  03 fe 76 52 00 00                                  ··vR··
```

wireshark_WiFiD5G1C3.pcapng
Packets: 20683 · Displayed: 20682 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Key VAPT Insights:

1. Broadcast packets reveal active hosts and MAC addresses (network mapping).
2. HTTP unicast packets show plaintext data exposure.
3. TLS/HTTPS protects sensitive information.
4. Hands-on exercise reinforces Layer 2/3 traffic, network discovery, and capture techniques.

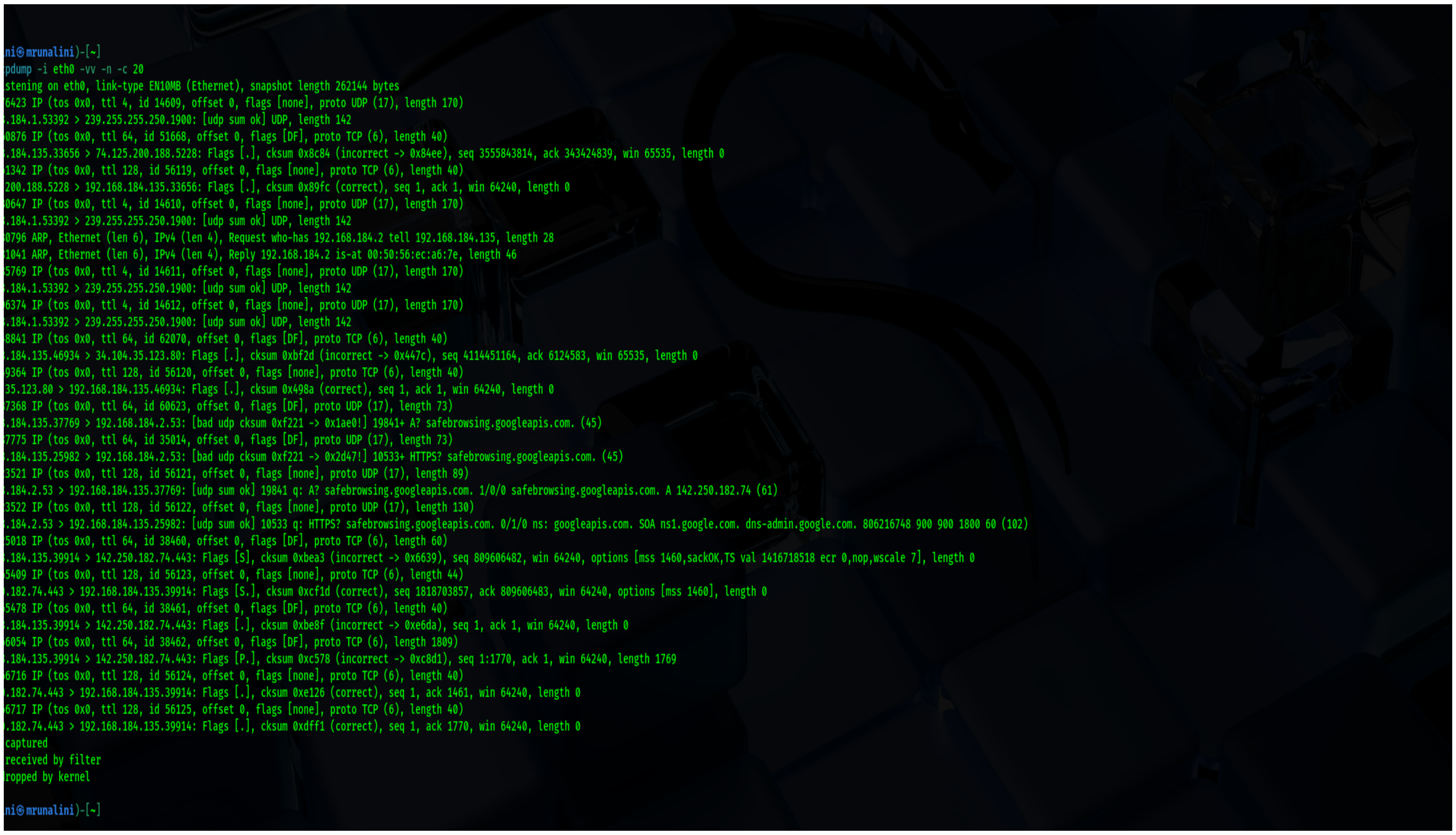
Conclusion:

This PoC demonstrates practical packet sniffing and analysis using Wireshark, highlighting broadcast vs unicast traffic, HTTP exposure, and TLS protection. Provides a clear understanding of network-level risks and the importance of securing communication channels for VAPT exercises.

tcpdump Observations (Linux, eth0)

Command Used:

sudo tcpdump -i eth0 -vv -n -c 20



```
ni㉿mrunalini)-[~]
pdump -i eth0 -vv -n -c 20
stening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
6423 IP (tos 0x0, ttl 4, id 14609, offset 0, flags [none], proto UDP (17), length 170)
.184.1.53392 > 239.255.255.250.1900: [udp sum ok] UDP, length 142
0876 IP (tos 0x0, ttl 64, id 51668, offset 0, flags [DF], proto TCP (6), length 40)
.184.135.33656 > 74.125.200.188.5228: Flags [.], cksum 0x8c84 (incorrect -> 0x84ee), seq 3555843814, ack 343424839, win 65535, length 0
1342 IP (tos 0x0, ttl 128, id 56119, offset 0, flags [none], proto TCP (6), length 40)
200.188.5228 > 192.168.184.135.33656: Flags [.], cksum 0x89fc (correct), seq 1, ack 1, win 64240, length 0
0647 IP (tos 0x0, ttl 4, id 14610, offset 0, flags [none], proto UDP (17), length 170)
.184.1.53392 > 239.255.255.250.1900: [udp sum ok] UDP, length 142
0796 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.184.2 tell 192.168.184.135, length 28
1041 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.184.2 is-at 00:50:56:ec:a6:7e, length 46
5769 IP (tos 0x0, ttl 4, id 14611, offset 0, flags [none], proto UDP (17), length 170)
.184.1.53392 > 239.255.255.250.1900: [udp sum ok] UDP, length 142
6374 IP (tos 0x0, ttl 4, id 14612, offset 0, flags [none], proto UDP (17), length 170)
.184.1.53392 > 239.255.255.250.1900: [udp sum ok] UDP, length 142
8841 IP (tos 0x0, ttl 64, id 62070, offset 0, flags [DF], proto TCP (6), length 40)
.184.135.46934 > 34.104.35.123.80: Flags [.], cksum 0xbf2d (incorrect -> 0x447c), seq 4114451164, ack 6124583, win 65535, length 0
9364 IP (tos 0x0, ttl 128, id 56120, offset 0, flags [none], proto TCP (6), length 40)
35.123.80 > 192.168.184.135.46934: Flags [.], cksum 0x498a (correct), seq 1, ack 1, win 64240, length 0
7368 IP (tos 0x0, ttl 64, id 60623, offset 0, flags [DF], proto UDP (17), length 73)
.184.135.37769 > 192.168.184.2.53: [bad udp cksum 0xf221 -> 0x1ae0!] 19841+ A? safebrowsing.googleapis.com. (45)
7775 IP (tos 0x0, ttl 64, id 35014, offset 0, flags [DF], proto UDP (17), length 73)
.184.135.25982 > 192.168.184.2.53: [bad udp cksum 0xf221 -> 0x2d47!] 10533+ HTTPS? safebrowsing.googleapis.com. (45)
3521 IP (tos 0x0, ttl 128, id 56121, offset 0, flags [none], proto UDP (17), length 89)
.184.2.53 > 192.168.184.135.37769: [udp sum ok] 19841 q: A? safebrowsing.googleapis.com. 1/0/0 safebrowsing.googleapis.com. A 142.250.182.74 (61)
3522 IP (tos 0x0, ttl 128, id 56122, offset 0, flags [none], proto UDP (17), length 130)
.184.2.53 > 192.168.184.135.25982: [udp sum ok] 10533 q: HTTPS? safebrowsing.googleapis.com. 0/1/0 ns: googleapis.com. SOA ns1.google.com. dns-admin.google.com. 806216748 900 900 1800 60 (102)
5018 IP (tos 0x0, ttl 64, id 38460, offset 0, flags [DF], proto TCP (6), length 60)
.184.135.39914 > 142.250.182.74.443: Flags [S], cksum 0xbea3 (incorrect -> 0x6639), seq 809606482, win 64240, options [mss 1460,sackOK,TS val 1416718518 ecr 0,nop,wscale 7], length 0
5409 IP (tos 0x0, ttl 128, id 56123, offset 0, flags [none], proto TCP (6), length 44)
.182.74.443 > 192.168.184.135.39914: Flags [S.], cksum 0xcf1d (correct), seq 1818703857, ack 809606483, win 64240, options [mss 1460], length 0
5478 IP (tos 0x0, ttl 64, id 38461, offset 0, flags [DF], proto TCP (6), length 40)
.184.135.39914 > 142.250.182.74.443: Flags [.], cksum 0xbe8f (incorrect -> 0xe6da), seq 1, ack 1, win 64240, length 0
6054 IP (tos 0x0, ttl 64, id 38462, offset 0, flags [DF], proto TCP (6), length 1809)
.184.135.39914 > 142.250.182.74.443: Flags [P.], cksum 0xc578 (incorrect -> 0xc8d1), seq 1:1770, ack 1, win 64240, length 1769
6716 IP (tos 0x0, ttl 128, id 56124, offset 0, flags [none], proto TCP (6), length 40)
.182.74.443 > 192.168.184.135.39914: Flags [.], cksum 0xe126 (correct), seq 1, ack 1461, win 64240, length 0
6717 IP (tos 0x0, ttl 128, id 56125, offset 0, flags [none], proto TCP (6), length 40)
.182.74.443 > 192.168.184.135.39914: Flags [.], cksum 0xdff1 (correct), seq 1, ack 1770, win 64240, length 0
captured
received by filter
ropped by kernel

ni㉿mrunalini)-[~]
```

Analysis:

- **UDP traffic:** Multicast traffic on the network.
- **TCP traffic:** Unicast communication with external servers.
- **ARP traffic:** Broadcast request and reply showing LAN discovery.

Practical Takeaways

1. **Wireshark** is excellent for **learning, visualizing, and documenting PoC** traffic.
2. **tcpdump** is excellent for **real-time CLI captures, automation, and remote network analysis**.
3. Both tools are complementary: you can **capture with tcpdump and analyze with Wireshark**, which is a common VAPT workflow.