

# WIRESHARK

Name: C.Chenna Mounika

Reg No: 192011054

## 1. TCP

The screenshot shows a Wireshark capture of a NetBIOS Name Service packet. The packet list shows five ARP requests from HewlettP\_92:95:30 to a broadcast destination. The selected packet (No. 8930) is a NetBIOS Name Service packet over TCP. The packet details pane shows the following structure:

- Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF\_{5DFD1EE8-0788-4C51-ABD1-E8B941C02E8E}.
- Ethernet II, Src: IntelCor\_29:20:dc (00:1b:77:29:20:dc), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 169.254.229.194, Dst: 169.254.255.255
- User Datagram Protocol, Src Port: 137, Dst Port: 137
- NetBIOS Name Service

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 ff ff ff ff ff 00 1b 77 29 20 dc 08 00 45 00 ..... w) ...E.
0010 00 4e 5f 9e 00 00 80 11 a1 41 a9 fe e5 c2 a9 fe .N.....A.....
0020 ff ff 00 89 00 89 00 3a 6c 60 cb c6 01 10 00 01 .....: 1`.....
0030 00 00 00 00 00 00 20 45 4e 44 43 44 46 43 4f 45 ..... E NDCFCOE
0040 45 45 46 45 42 45 4d 46 41 45 42 46 45 46 46 43 EEFE BEMF AEBFEFFC
0050 4f 46 43 46 46 41 41 00 00 20 00 01 OFCFFAA . . .
```

## 2. IP

The screenshot shows a Wireshark capture of an IP packet. The packet list shows five packets: a DNS query, a TCP ACK, and three more TCP ACKs. The selected packet (No. 1662) is a TCP ACK packet. The packet details pane shows the following structure:

- Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{5DFD1EE8-0788-4C51-ABD1-E8B941C02E8E}.
- Ethernet II, Src: 2a:59:b8:88:38:94 (2a:59:b8:88:38:94), Dst: IntelCor\_b6:77:f4 (80:38:fb:b6:77:f4)
- Internet Protocol Version 4, Src: 13.107.42.12, Dst: 192.168.6.212
- Transmission Control Protocol, Src Port: 443, Dst Port: 56197, Seq: 1, Ack: 1, Len: 0

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 80 38 fb b6 77 f4 2a 59 b8 88 38 94 08 00 45 00 .8..w.*Y..8...E.
0010 00 28 2c d1 40 00 73 06 dc 0b 0d 6b 2a 0c c0 a8 .(.@.s...k*...
0020 06 d4 01 bb db 85 41 bc e6 e1 63 51 56 08 50 10 .....A...cQV.P.
0030 40 03 b1 a5 00 00 @.....
```

## 3. ICMP

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	icmp	Source	Destination	Protocol	Length	Info
1	icmpv6	192.168.6.212	8.241.137.254	TCP	54	56236 → 80 [ACK] Seq=1 Ack=127401 Win=71 Len=0
1216	4.453611	8.241.137.254	192.168.6.212	TCP	1354	80 → 56236 [ACK] Seq=127401 Ack=1 Win=11 Len=1300
1217	4.496179	2401:4900:234c:b190...	2001:1900:2381:d08:...	TCP	86	56234 → 80 [ACK] Seq=1 Ack=548601 Win=568 Len=0 SLE=5
1218	4.496241	192.168.6.212	8.241.137.254	TCP	54	56236 → 80 [ACK] Seq=1 Ack=128701 Win=71 Len=0
1219	4.760653	8.241.137.254	192.168.6.212	TCP	1354	80 → 56236 [ACK] Seq=128701 Ack=1 Win=11 Len=1300

> Frame 1: 1354 bytes on wire (10832 bits), 1354 bytes captured (10832 bits) on interface \Device\NPF\_{5DFD1EE8-0788-4C51-ABD1-E8B94...}

> Ethernet II, Src: 2a:59:b8:88:38:94 (2a:59:b8:88:38:94), Dst: IntelCor\_b6:77:f4 (80:38:fb:b6:77:f4)

> Internet Protocol Version 4, Src: 8.241.158.254, Dst: 192.168.6.212

> Transmission Control Protocol, Src Port: 80, Dst Port: 56235, Seq: 1, Ack: 1, Len: 1300

```

0000  80 38 fb b6 77 f4 2a 59 b8 88 38 94 08 00 45 00  :8..w.*Y..8...E.
0010  05 3c 99 2c 00 00 39 06 74 24 08 f1 9e fe c0 a8  :<.,..9..t$......
0020  06 d4 00 50 db ab ff 78 81 b1 be 84 09 fd 50 10  :..P...x.....P.
0030  00 0b d5 d4 00 00 62 7d b1 4c f3 3e 93 2b 74 74  :....b}.L.>..+tt
0040  18 b3 65 63 93 6d d5 83 8a 07 dc f1 0a 9e 58 f2  :..ec..m.....X.
0050  c2 b6 c9 af 67 8c 94 ee 7d b9 65 26 a7 6c ef 79  :...g...}..e&.l.y
0060  e3 1a 75 ae e9 7d b8 ac aa 75 13 c2 b7 7a f5 9f  :..u..}...u...z..
0070  e2 f7 24 73 31 6e ef dc a4 48 fe 4e 91 89 75 8b  :..$sln...H.N..u.
0080  1c c2 47 71 02 fe a6 15 e1 27 6e 00 d8 84 c0 4b  :..Gq....'n....K

```

Internet Control Message Protocol: Protocol

Packets: 1219 - Displayed: 1219 (100.0%)

Profile: Default

#### 4.UDP

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	udp	Source	Destination	Protocol	Length	Info
25	udpcp	2a:59:b8:88:38:94	IntelCor_b6:77:f4	ARP	42	Who has 192.168.6.212? Tell 192.168.6.152
30	udpcap	IntelCor_b6:77:f4	2a:59:b8:88:38:94	ARP	42	192.168.6.212 is at 80:38:fb:b6:77:f4
29	udplite	192.168.6.212	113.29.117.28	TLSv1.2	132	Application Data
30	5.767061	192.168.6.212	113.29.117.28	TLSv1.2	354	Application Data
31	5.926320	113.29.117.28	192.168.6.212	TCP	54	443 → 56146 [ACK] Seq=752 Ack=1189 Win=63700 Len=0

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{5DFD1EE8-0788-4C51-ABD1-E8B941C02E8E}.

> Ethernet II, Src: IntelCor\_b6:77:f4 (80:38:fb:b6:77:f4), Dst: 2a:59:b8:88:38:94 (2a:59:b8:88:38:94)

> Internet Protocol Version 4, Src: 192.168.6.212, Dst: 180.87.4.152

> Transmission Control Protocol, Src Port: 56134, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

```

0000  2a 59 b8 88 38 94 80 38 fb b6 77 f4 08 00 45 00  :*Y...8..8..w...E.
0010  00 28 91 23 40 00 80 06 00 00 c0 a8 06 d4 b4 57  :.(.#@... ..W
0020  04 98 db 46 01 bb cf c2 82 b9 cd 46 d5 c9 50 10  :...F....F..P.
0030  22 38 80 86 00 00  :8....

```

User Datagram Protocol: Protocol

Packets: 31 - Displayed: 31 (100.0%)

Profile: Default

#### 5.ARP

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Info
86	8.854881	192.168.6.212	180.87.4.152	TCP	54	56134 → 443 [ACK] Seq=353 Ack=491 Win=8270 Len=0
87	9.901949	2a:59:b8:88:38:94	IntelCor_b6:77:f4	ARP	42	Who has 192.168.6.212? Tell 192.168.6.152
88	9.901949	fe80::2859:b8ff:fe8...	2401:4900:234c:b190...	ICMPv6	86	Neighbor Solicitation for 2401:4900:234c:b190:b1cd:a920
89	9.901974	IntelCor_b6:77:f4	2a:59:b8:88:38:94	ARP	42	192.168.6.212 is at 80:38:fb:b6:77:f4
90	9.902177	2401:4900:234c:b190...	fe80::2859:b8ff:fe8...	ICMPv6	86	Neighbor Advertisement 2401:4900:234c:b190:b1cd:a920

> Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF\_{5DFD1EE8-0788-4C51-ABD1-E8B941C02E8E}

> Ethernet II, Src: IntelCor\_b6:77:f4 (80:38:fb:b6:77:f4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Internet Protocol Version 4, Src: 192.168.6.212, Dst: 192.168.6.255

> User Datagram Protocol, Src Port: 137, Dst Port: 137

> NetBIOS Name Service

```

0000  ff ff ff ff ff ff 80 38  fb b6 77 f4 08 00 45 00  .....8..W...E.
0010  00 4e f6 59 00 00 80 11  00 00 c0 a8 06 d4 c0 a8  -N.Y.....
0020  06 ff 00 89 00 89 00 3a  0a ad b8 11 01 10 00 01  .....
0030  00 00 00 00 00 00 20 45  4d 45 42 46 41 46 45 45  .....E MEBFAFEE
0040  50 46 41 43 4e 45 4b 45  50 45 48 45 47 46 47 45  PFACNEKE PEHEGFGE
0050  4b 44 43 46 47 42 4d 00  00 20 00 01                KDCFGBM...

```

Address Resolution Protocol: Protocol

Packets: 90 - Displayed: 90 (100.0%)

Profile: Default

## 6.HTTP

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
http2	16.262006	2a03:2880:f268:c1:f...	2401:4900:234c:b190...	TCP	74	443 → 56160 [ACK] Seq=97 Ack=75 Win=269 Len=0
http3	16.569638	2401:4900:234c:b190...	2a03:2880:f268:c1:f...	TLSv1.2	149	Application Data
24	17.723403	2a03:2880:f268:c1:f...	2401:4900:234c:b190...	TCP	74	443 → 56160 [ACK] Seq=97 Ack=150 Win=269 Len=0
25	17.946845	2a03:2880:f268:c1:f...	2401:4900:234c:b190...	TLSv1.2	146	Application Data
26	18.000554	2401:4900:234c:b190...	2a03:2880:f268:c1:f...	TCP	74	56160 → 443 [ACK] Seq=150 Ack=169 Win=28 Len=0

> Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF\_{5DFD1EE8-0788-4C51-ABD1-E8B941C02E8E}

> Ethernet II, Src: IntelCor\_b6:77:f4 (80:38:fb:b6:77:f4), Dst: 2a:59:b8:88:38:94 (2a:59:b8:88:38:94)

> Internet Protocol Version 6, Src: 2401:4900:234c:b190:b1cd:a920:e52d:c103, Dst: 2404:6800:4003:c00::bc

> Transmission Control Protocol, Src Port: 56229, Dst Port: 5228, Seq: 1, Ack: 1, Len: 1

> Data (1 byte)

```

0000  2a 59 b8 88 38 94 80 38  fb b6 77 f4 86 dd 60 05  *Y...8..8..W...`
0010  29 b6 00 15 06 3f 24 01  49 00 23 4c b1 90 b1 cd  )....?$. I.#L....
0020  a9 20 e5 2d c1 03 24 04  68 00 40 03 0c 00 00 00  -...$. h.@.....
0030  00 00 00 00 00 bc db a5  14 6c af 6b fa a9 bd 3f  .....l.k...?
0040  5e 8d 50 10 00 1f 1b dd  00 00 00                ^.P.....

```

Hypertext Transfer Protocol: Protocol

Packets: 26 - Displayed: 26 (100.0%)

Profile: Default