Experiment-7

AIM: To capture network traffic on your machine and analyze packets to understand how data travels over a network.

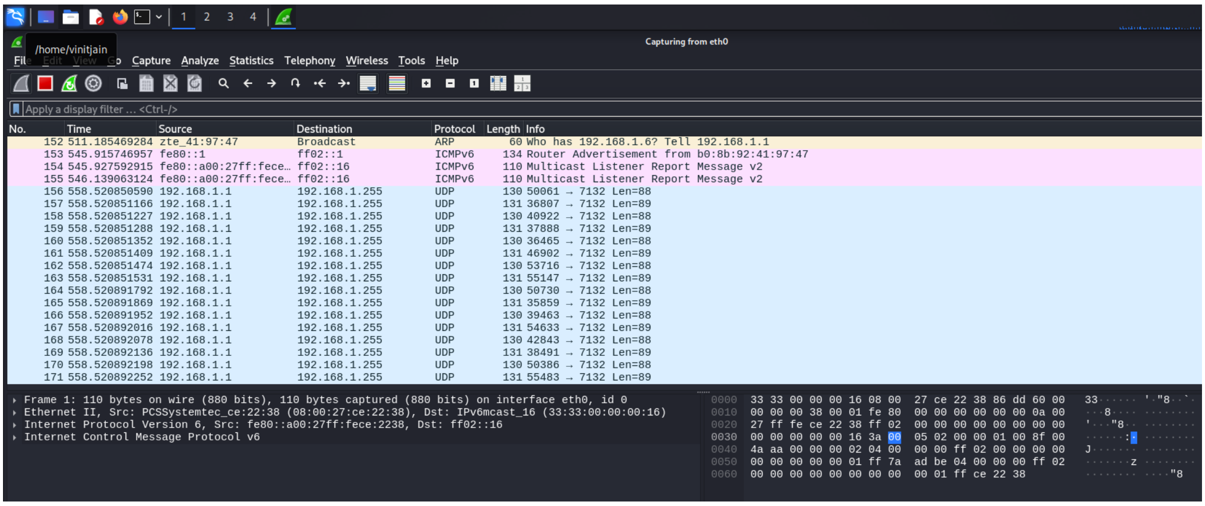
Objective: Capture and inspect network packets to understand the protocols in use and identify potential issues in the traffic.

Theory: Wireshark captures packets transmitted over a network and allows you to inspect them. It provides detailed information about each packet, including source and destination addresses, protocol types, and data payloads. Understanding this data is essential for network troubleshooting, security analysis, and protocol development.

Used **Commands** in Wireshark:

1. Start Capture:

- Go to Capture > Start or use the shortcut Ctrl + E to begin capturing packets.



1
2
3
4
/home/vinitjain
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time           Source                    Destination     Protocol Length Info
 152 511.185469284 zte_41:97:47              Broadcast       ARP       60 Who has 192.168.1.6? Tell 192.168.1.1
 153 545.915746957 fe80::1                   ff02::1         ICMPv6   134 Router Advertisement from b0:8b:92:41:97:47
 154 545.927592915 fe80::a00:27ff:fece…      ff02::16        ICMPv6   110 Multicast Listener Report Message v2
 155 546.139063124 fe80::a00:27ff:fece…      ff02::16        ICMPv6   110 Multicast Listener Report Message v2
 156 558.520850590 192.168.1.1               192.168.1.255   UDP      130 50061 → 7132 Len=88
 157 558.520851166 192.168.1.1               192.168.1.255   UDP      131 36807 → 7132 Len=89
 158 558.520851227 192.168.1.1               192.168.1.255   UDP      130 40922 → 7132 Len=88
 159 558.520851288 192.168.1.1               192.168.1.255   UDP      131 37888 → 7132 Len=89
 160 558.520851352 192.168.1.1               192.168.1.255   UDP      130 36465 → 7132 Len=88
 161 558.520851409 192.168.1.1               192.168.1.255   UDP      131 46902 → 7132 Len=89
 162 558.520851474 192.168.1.1               192.168.1.255   UDP      130 53716 → 7132 Len=88
 163 558.520851531 192.168.1.1               192.168.1.255   UDP      131 55147 → 7132 Len=89
 164 558.520891792 192.168.1.1               192.168.1.255   UDP      130 50730 → 7132 Len=88
 165 558.520891869 192.168.1.1               192.168.1.255   UDP      131 35859 → 7132 Len=89
 166 558.520891952 192.168.1.1               192.168.1.255   UDP      130 39463 → 7132 Len=88
 167 558.520892016 192.168.1.1               192.168.1.255   UDP      131 54633 → 7132 Len=89
 168 558.520892078 192.168.1.1               192.168.1.255   UDP      130 42843 → 7132 Len=88
 169 558.520892136 192.168.1.1               192.168.1.255   UDP      131 38491 → 7132 Len=89
 170 558.520892198 192.168.1.1               192.168.1.255   UDP      130 50386 → 7132 Len=88
 171 558.520892252 192.168.1.1               192.168.1.255   UDP      131 55483 → 7132 Len=89
```

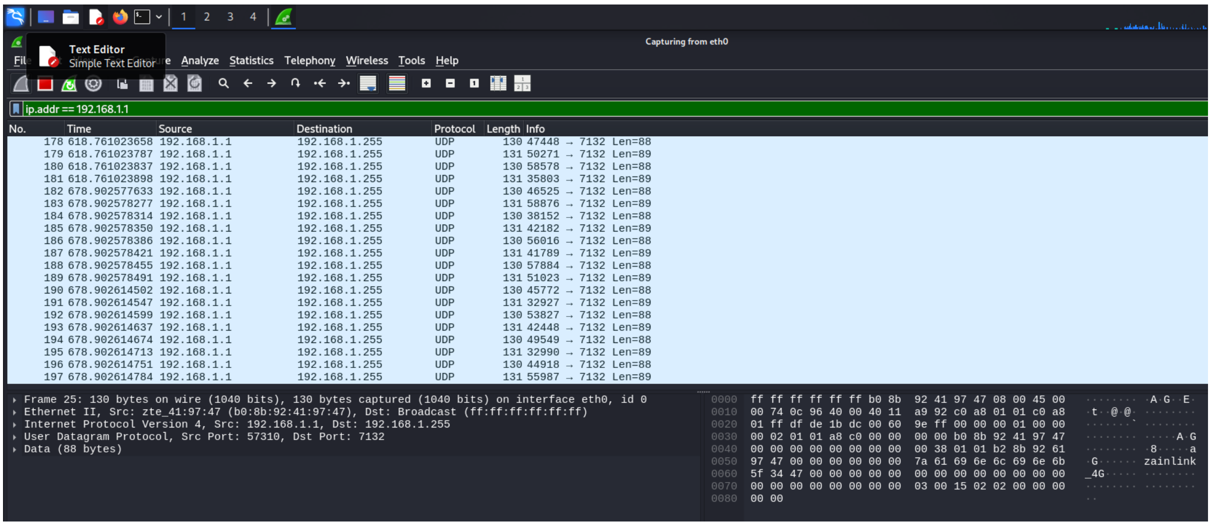
```
▸ Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface eth0, id 0
▸ Ethernet II, Src: PCSSystemtec_ce:22:38 (08:00:27:ce:22:38), Dst: IPv6mcast_16 (33:33:00:00:00:16)
▸ Internet Protocol Version 6, Src: fe80::a00:27ff:fece:2238, Dst: ff02::16
▸ Internet Control Message Protocol v6
```

```
0000  33 33 00 00 00 16 08 00  27 ce 22 38 86 dd 60 00   33······ '·"8··`·
0010  00 00 00 38 00 01 fe 80  00 00 00 00 00 00 0a 00   ···8···· ········
0020  27 ff fe ce 22 38 ff 02  00 00 00 00 00 00 00 00   '···"8·· ········
0030  00 00 00 00 00 16 3a 00  05 02 00 00 01 00 8f 00   ······:· ········
0040  4a aa 00 00 00 02 04 00  00 00 ff 02 00 00 00 00   J······· ········
0050  00 00 00 00 00 01 ff 7a  ad be 04 00 00 00 ff 02   ·······z ········
0060  00 00 00 00 00 00 00 00  00 01 ff ce 22 38         ········ ····"8
```

2. Display Filters (to filter the traffic):

- Use display filters to narrow down the captured traffic based on criteria such as IP address, protocol, or port number.

- Example: ip.addr == 192.168.1.1 (Filters packets to or from a specific IP address).



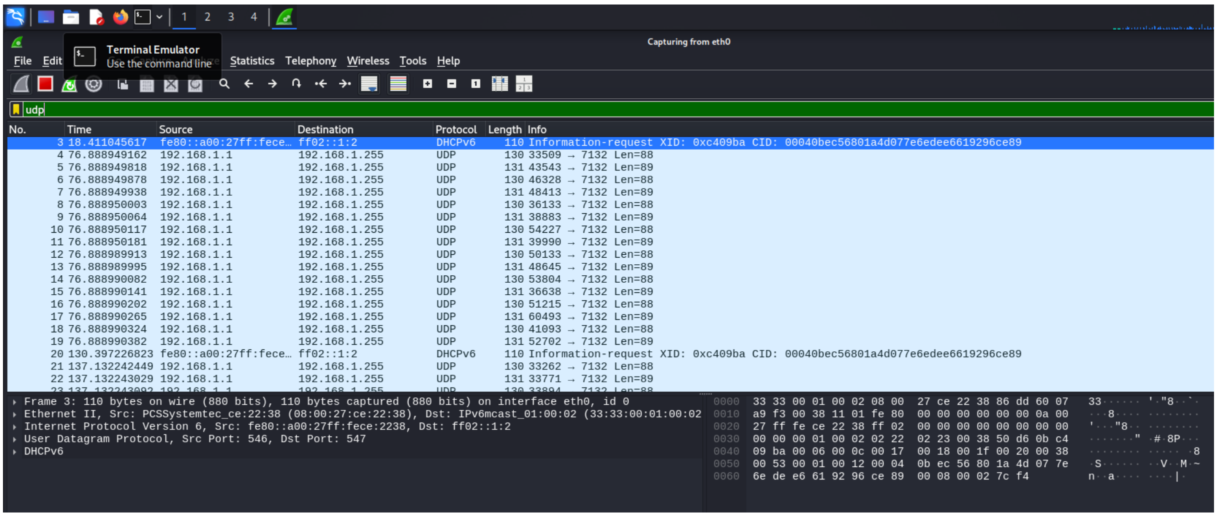
```
ip.addr == 192.168.1.1
```

```
No.  Time           Source        Destination     Protocol Length Info
 178 618.761023658 192.168.1.1   192.168.1.255   UDP      130 47448 → 7132 Len=88
 179 618.761023787 192.168.1.1   192.168.1.255   UDP      131 50271 → 7132 Len=89
 180 618.761023837 192.168.1.1   192.168.1.255   UDP      130 58578 → 7132 Len=88
 181 618.761023898 192.168.1.1   192.168.1.255   UDP      131 35803 → 7132 Len=89
 182 678.902577633 192.168.1.1   192.168.1.255   UDP      130 46525 → 7132 Len=88
 183 678.902578277 192.168.1.1   192.168.1.255   UDP      131 58876 → 7132 Len=89
 184 678.902578314 192.168.1.1   192.168.1.255   UDP      130 38152 → 7132 Len=88
 185 678.902578350 192.168.1.1   192.168.1.255   UDP      131 42182 → 7132 Len=89
 186 678.902578386 192.168.1.1   192.168.1.255   UDP      130 56016 → 7132 Len=88
 187 678.902578421 192.168.1.1   192.168.1.255   UDP      131 41789 → 7132 Len=89
 188 678.902578455 192.168.1.1   192.168.1.255   UDP      130 57884 → 7132 Len=88
 189 678.902578491 192.168.1.1   192.168.1.255   UDP      131 51023 → 7132 Len=89
 190 678.902614502 192.168.1.1   192.168.1.255   UDP      130 45772 → 7132 Len=88
 191 678.902614547 192.168.1.1   192.168.1.255   UDP      131 32927 → 7132 Len=89
 192 678.902614599 192.168.1.1   192.168.1.255   UDP      130 53827 → 7132 Len=88
 193 678.902614637 192.168.1.1   192.168.1.255   UDP      131 42448 → 7132 Len=89
 194 678.902614674 192.168.1.1   192.168.1.255   UDP      130 49549 → 7132 Len=88
 195 678.902614713 192.168.1.1   192.168.1.255   UDP      131 32990 → 7132 Len=89
 196 678.902614751 192.168.1.1   192.168.1.255   UDP      130 44918 → 7132 Len=88
 197 678.902614784 192.168.1.1   192.168.1.255   UDP      131 55987 → 7132 Len=89
```

```
› Frame 25: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface eth0, id 0
› Ethernet II, Src: zte_41:97:47 (b0:8b:92:41:97:47), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.255
› User Datagram Protocol, Src Port: 57310, Dst Port: 7132
› Data (88 bytes)
```

```
0000  ff ff ff ff ff ff b0 8b  92 41 97 47 08 00 45 00   ········ ·A·G··E·
0010  00 74 0c 96 40 00 40 11  a9 92 c0 a8 01 01 c0 a8   ·t··@·@· ········
0020  01 ff df de 1b dc 00 60  9e ff 00 00 00 01 00 00   ·······` ········
0030  00 02 01 01 a8 c0 00 00  00 00 b0 8b 92 41 97 47   ········ ·····A·G
0040  00 00 00 00 00 00 00 00  00 38 01 01 b2 8b 92 61   ········ ·8·····a
0050  97 47 00 00 00 00 00 00  7a 61 69 6e 6c 69 6e 6b   ·G······ zainlink
0060  5f 34 47 00 00 00 00 00  00 00 00 00 00 00 00 00   _4G····· ········
0070  00 00 00 00 00 00 00 00  03 00 15 02 02 00 00 00   ········ ········
0080  00 00                                              ··
```

- Example: udp (Filters UDP packets).



```
udp
```

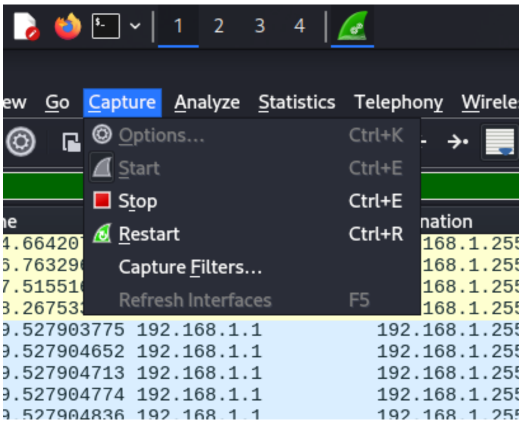
```
No.  Time           Source                Destination     Protocol Length Info
   3 18.411045617  fe80::a00:27ff:fece…  ff02::1:2       DHCPv6   110 Information-request XID: 0xc409ba CID: 00040bec56801a4d077e6edee6619296ce89
   4 76.888949162  192.168.1.1           192.168.1.255   UDP      130 33509 → 7132 Len=88
   5 76.888949818  192.168.1.1           192.168.1.255   UDP      131 43543 → 7132 Len=89
   6 76.888949878  192.168.1.1           192.168.1.255   UDP      130 46328 → 7132 Len=88
   7 76.888949938  192.168.1.1           192.168.1.255   UDP      131 48413 → 7132 Len=89
   8 76.888950003  192.168.1.1           192.168.1.255   UDP      130 36133 → 7132 Len=88
   9 76.888950064  192.168.1.1           192.168.1.255   UDP      131 38883 → 7132 Len=89
  10 76.888950117  192.168.1.1           192.168.1.255   UDP      130 54227 → 7132 Len=88
  11 76.888950181  192.168.1.1           192.168.1.255   UDP      131 39990 → 7132 Len=89
  12 76.888989913  192.168.1.1           192.168.1.255   UDP      130 50133 → 7132 Len=88
  13 76.888989995  192.168.1.1           192.168.1.255   UDP      131 48645 → 7132 Len=89
  14 76.888990082  192.168.1.1           192.168.1.255   UDP      130 53804 → 7132 Len=88
  15 76.888990141  192.168.1.1           192.168.1.255   UDP      131 36638 → 7132 Len=89
  16 76.888990202  192.168.1.1           192.168.1.255   UDP      130 51215 → 7132 Len=88
  17 76.888990265  192.168.1.1           192.168.1.255   UDP      131 60493 → 7132 Len=89
  18 76.888990324  192.168.1.1           192.168.1.255   UDP      130 41093 → 7132 Len=88
  19 76.888990382  192.168.1.1           192.168.1.255   UDP      131 52702 → 7132 Len=89
  20 130.397226823 fe80::a00:27ff:fece…  ff02::1:2       DHCPv6   110 Information-request XID: 0xc409ba CID: 00040bec56801a4d077e6edee6619296ce89
  21 137.132242449 192.168.1.1           192.168.1.255   UDP      130 33262 → 7132 Len=88
  22 137.132243029 192.168.1.1           192.168.1.255   UDP      131 33771 → 7132 Len=89
  23 137.132243092 192.168.1.1           192.168.1.255   UDP      130 33894 → 7132 Len=88
```

```
› Frame 3: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_ce:22:38 (08:00:27:ce:22:38), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02
› Internet Protocol Version 6, Src: fe80::a00:27ff:fece:2238, Dst: ff02::1:2
› User Datagram Protocol, Src Port: 546, Dst Port: 547
› DHCPv6
```

```
0000  33 33 00 01 00 02 08 00  27 ce 22 38 86 dd 60 07   33······ '·"8··`·
0010  a9 f3 00 38 11 01 fe 80  00 00 00 00 00 00 0a 00   ···8···· ········
0020  27 ff fe ce 22 38 ff 02  00 00 00 00 00 00 00 00   '···"8·· ········
0030  00 00 00 01 00 02 02 22  02 23 00 38 50 d6 0b c4   ·······" ·#·8P···
0040  09 ba 00 06 00 0c 00 17  00 18 00 1f 00 20 00 38   ········ ·····  ·8
0050  00 53 00 01 00 12 00 04  0b ec 56 80 1a 4d 07 7e   ·S······ ··V··M·~
0060  6e de e6 61 92 96 ce 89  00 08 00 02 7c f4         n··a···· ····|·
```

3. Stop Capture:

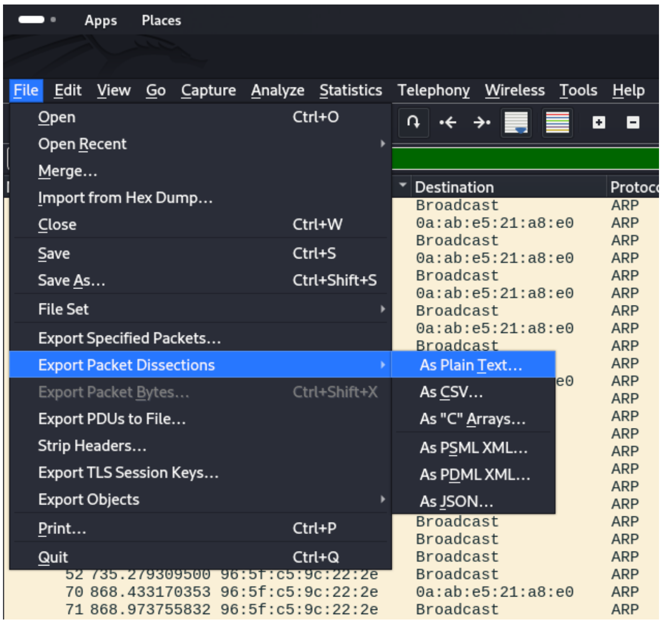
- Go to Capture > Stop or press Ctrl + E to stop the capture.



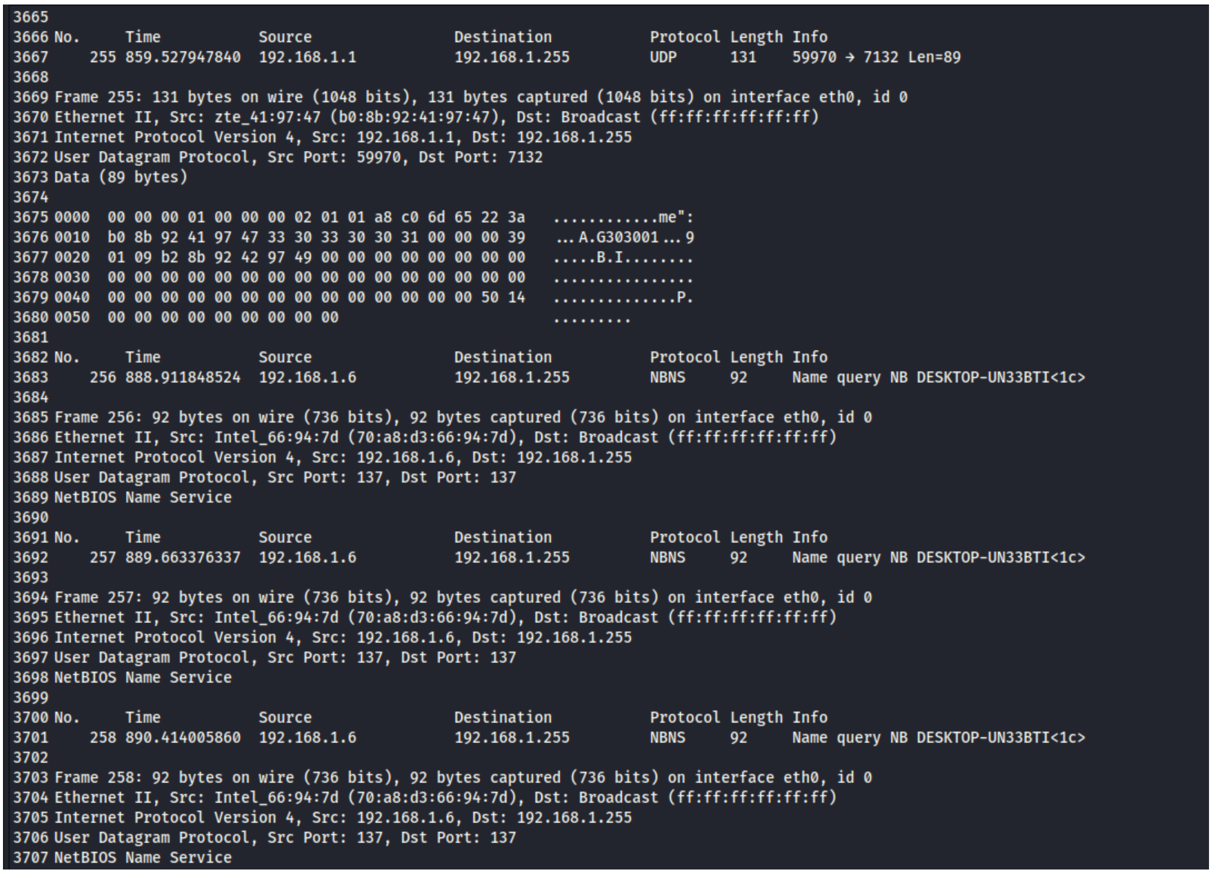
```
4.66420      168.1.255
5.76329      168.1.255
7.51551      168.1.255
3.26753      168.1.255
9.527903775 192.168.1.1    192.168.1.255
9.527904652 192.168.1.1    192.168.1.255
9.527904713 192.168.1.1    192.168.1.255
9.527904774 192.168.1.1    192.168.1.255
9.527904836 192.168.1.1    192.168.1.255
```

4. Export Packet Capture:

- Go to File > Export Packet Dissections > As Plain Text to save captured packets for later analysis.



```
Broadcast          ARP
0a:ab:e5:21:a8:e0  ARP
Broadcast          ARP
0a:ab:e5:21:a8:e0  ARP
Broadcast          ARP
0a:ab:e5:21:a8:e0  ARP
Broadcast          ARP
0a:ab:e5:21:a8:e0  ARP
Broadcast          ARP
52 735.279309500 96:5f:c5:9c:22:2e  Broadcast          ARP
70 868.433170353 96:5f:c5:9c:22:2e  0a:ab:e5:21:a8:e0  ARP
71 868.973755832 96:5f:c5:9c:22:2e  Broadcast          ARP
```



```
No.     Time           Source                Destination           Protocol Length Info
    255 859.527947840  192.168.1.1           192.168.1.255         UDP      131    59970 → 7132 Len=89

Frame 255: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits) on interface eth0, id 0
Ethernet II, Src: zte_41:97:47 (b0:8b:92:41:97:47), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.255
User Datagram Protocol, Src Port: 59970, Dst Port: 7132
Data (89 bytes)

0000  00 00 00 01 00 00 00 02 01 01 a8 c0 6d 65 22 3a   ...........me":
0010  b0 8b 92 41 97 47 33 30 33 30 30 31 00 00 00 39   ...A.G303001...9
0020  01 09 b2 8b 92 42 97 49 00 00 00 00 00 00 00 00   .....B.I........
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 14   ..............P.
0050  00 00 00 00 00 00 00 00 00                        .........

No.     Time           Source                Destination           Protocol Length Info
    256 888.911848524  192.168.1.6           192.168.1.255         NBNS     92     Name query NB DESKTOP-UN33BTI<1c>

Frame 256: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface eth0, id 0
Ethernet II, Src: Intel_66:94:7d (70:a8:d3:66:94:7d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service

No.     Time           Source                Destination           Protocol Length Info
    257 889.663376337  192.168.1.6           192.168.1.255         NBNS     92     Name query NB DESKTOP-UN33BTI<1c>

Frame 257: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface eth0, id 0
Ethernet II, Src: Intel_66:94:7d (70:a8:d3:66:94:7d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service

No.     Time           Source                Destination           Protocol Length Info
    258 890.414005860  192.168.1.6           192.168.1.255         NBNS     92     Name query NB DESKTOP-UN33BTI<1c>

Frame 258: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface eth0, id 0
Ethernet II, Src: Intel_66:94:7d (70:a8:d3:66:94:7d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
```

Conclusion: By capturing and analyzing network packets with Wireshark, we gain insights into data transmission, protocols, and potential network issues. Filtering traffic helps focus on specific IPs, protocols, or ports for detailed inspection. Understanding captured packets is crucial for troubleshooting, security monitoring, and protocol analysis. Wireshark serves as a powerful tool for network analysis and diagnostics.