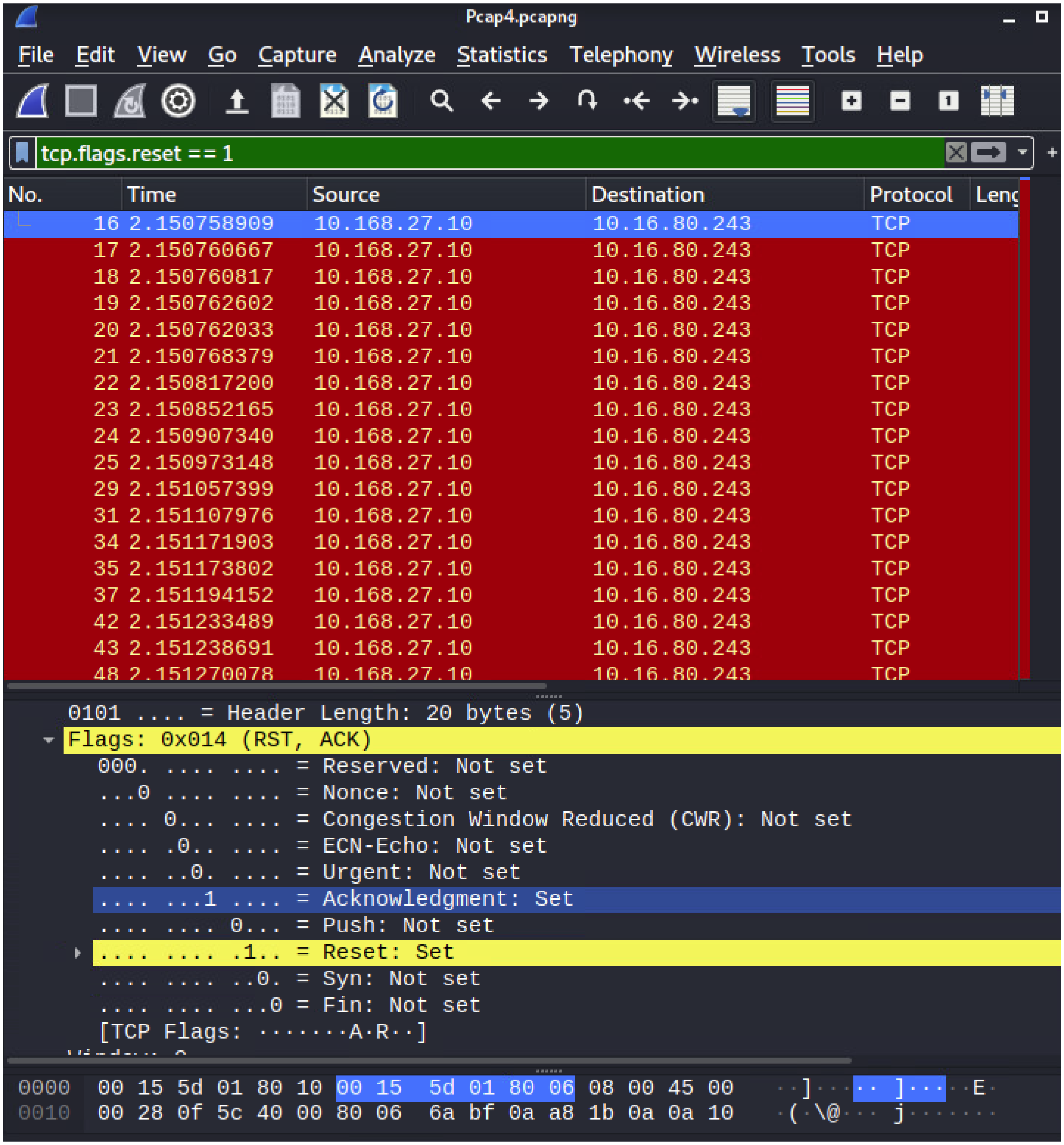
Wireshark Lab Session Picture

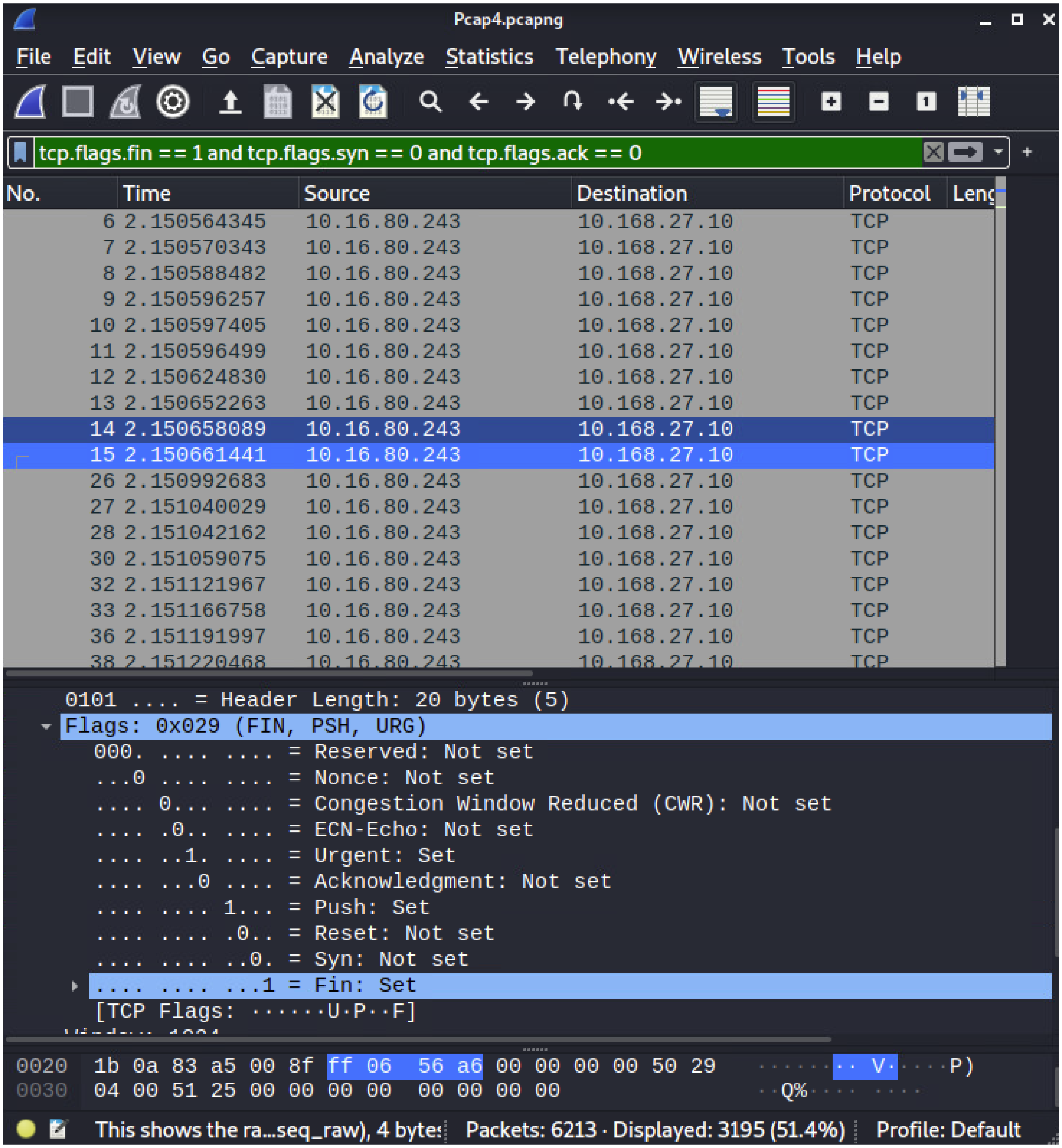

Pcap4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags.reset == 1
```

```
No.  Time         Source         Destination    Protocol  Leng
  16 2.150758909  10.168.27.10   10.16.80.243   TCP
  17 2.150760667  10.168.27.10   10.16.80.243   TCP
  18 2.150760817  10.168.27.10   10.16.80.243   TCP
  19 2.150762602  10.168.27.10   10.16.80.243   TCP
  20 2.150762033  10.168.27.10   10.16.80.243   TCP
  21 2.150768379  10.168.27.10   10.16.80.243   TCP
  22 2.150817200  10.168.27.10   10.16.80.243   TCP
  23 2.150852165  10.168.27.10   10.16.80.243   TCP
  24 2.150907340  10.168.27.10   10.16.80.243   TCP
  25 2.150973148  10.168.27.10   10.16.80.243   TCP
  29 2.151057399  10.168.27.10   10.16.80.243   TCP
  31 2.151107976  10.168.27.10   10.16.80.243   TCP
  34 2.151171903  10.168.27.10   10.16.80.243   TCP
  35 2.151173802  10.168.27.10   10.16.80.243   TCP
  37 2.151194152  10.168.27.10   10.16.80.243   TCP
  42 2.151233489  10.168.27.10   10.16.80.243   TCP
  43 2.151238691  10.168.27.10   10.16.80.243   TCP
  48 2.151270078  10.168.27.10   10.16.80.243   TCP
```

```
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x014 (RST, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .1.. = Reset: Set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A·R··]
```

```
0000  00 15 5d 01 80 10 00 15  5d 01 80 06 08 00 45 00   ··]·····]·····E·
0010  00 28 0f 5c 40 00 80 06  6a bf 0a a8 1b 0a 0a 10   ·(·\@···j·······
```


Pcap4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

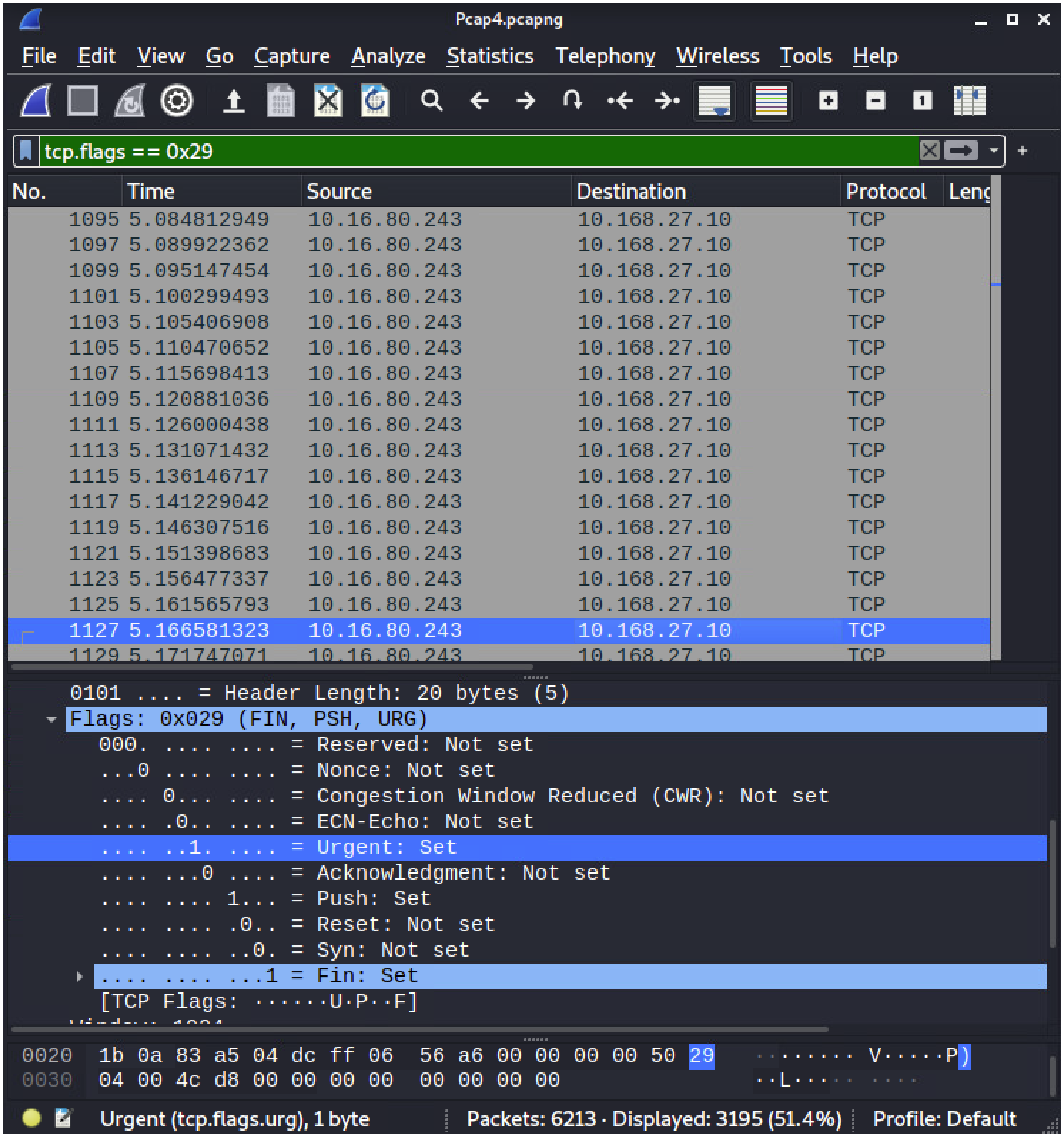
```
tcp.flags.fin == 1 and tcp.flags.syn == 0 and tcp.flags.ack == 0
```

```
No.   Time          Source          Destination     Protocol  Leng
    6 2.150564345   10.16.80.243    10.168.27.10    TCP
    7 2.150570343   10.16.80.243    10.168.27.10    TCP
    8 2.150588482   10.16.80.243    10.168.27.10    TCP
    9 2.150596257   10.16.80.243    10.168.27.10    TCP
   10 2.150597405   10.16.80.243    10.168.27.10    TCP
   11 2.150596499   10.16.80.243    10.168.27.10    TCP
   12 2.150624830   10.16.80.243    10.168.27.10    TCP
   13 2.150652263   10.16.80.243    10.168.27.10    TCP
   14 2.150658089   10.16.80.243    10.168.27.10    TCP
   15 2.150661441   10.16.80.243    10.168.27.10    TCP
   26 2.150992683   10.16.80.243    10.168.27.10    TCP
   27 2.151040029   10.16.80.243    10.168.27.10    TCP
   28 2.151042162   10.16.80.243    10.168.27.10    TCP
   30 2.151059075   10.16.80.243    10.168.27.10    TCP
   32 2.151121967   10.16.80.243    10.168.27.10    TCP
   33 2.151166758   10.16.80.243    10.168.27.10    TCP
   36 2.151191997   10.16.80.243    10.168.27.10    TCP
   38 2.151220468   10.16.80.243    10.168.27.10    TCP
```

```
  0101 .... = Header Length: 20 bytes (5)
▾ Flags: 0x029 (FIN, PSH, URG)
     000. .... .... = Reserved: Not set
     ...0 .... .... = Nonce: Not set
     .... 0... .... = Congestion Window Reduced (CWR): Not set
     .... .0.. .... = ECN-Echo: Not set
     .... ..1. .... = Urgent: Set
     .... ...0 .... = Acknowledgment: Not set
     .... .... 1... = Push: Set
     .... .... .0.. = Reset: Not set
     .... .... ..0. = Syn: Not set
   ▸ .... .... ...1 = Fin: Set
     [TCP Flags: ······U·P··F]
```

```
0020  1b 0a 83 a5 00 8f ff 06  56 a6 00 00 00 00 50 29   ········ ·V····P)
0030  04 00 51 25 00 00 00 00  00 00 00 00               ··Q%···· ····
```

This shows the ra...seq_raw), 4 byte:
Packets: 6213 · Displayed: 3195 (51.4%)
Profile: Default


Pcap4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

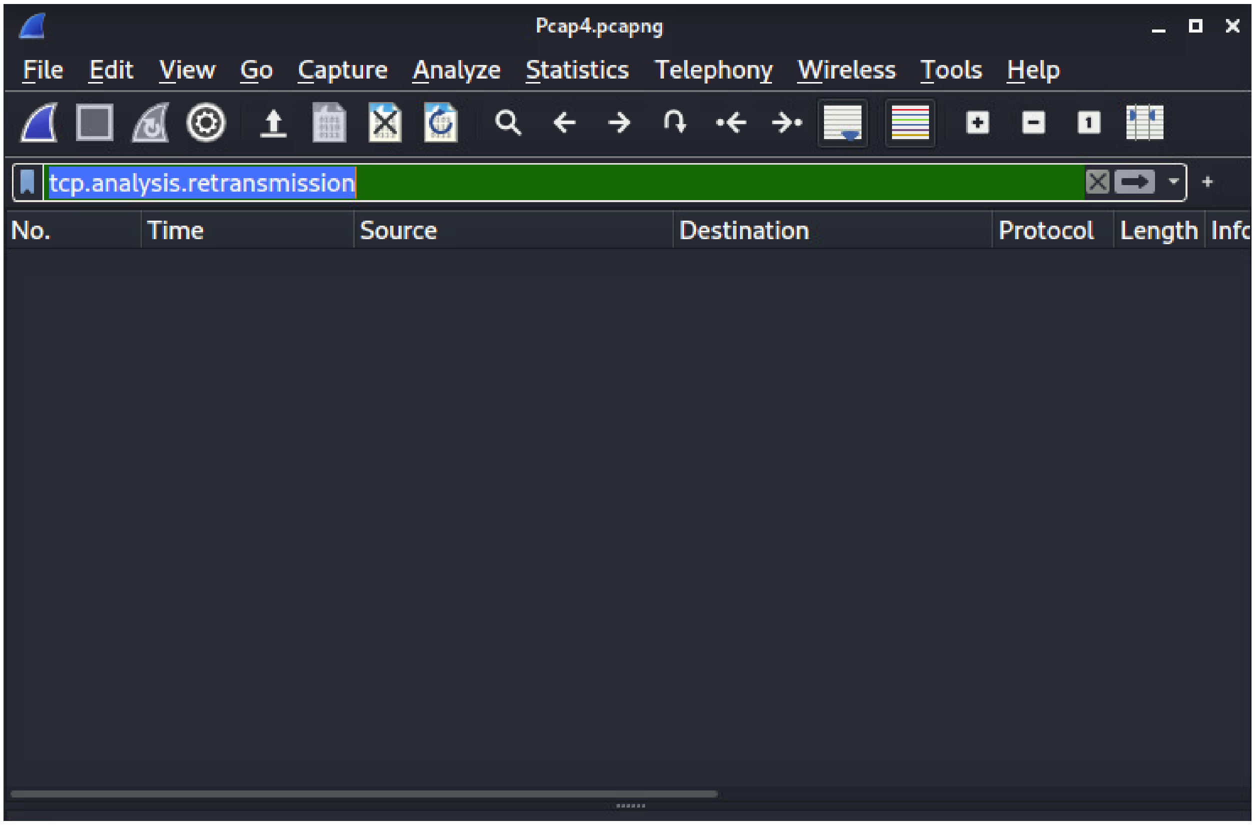
tcp.flags == 0x29

```
No.   Time         Source          Destination     Protocol  Leng
 1095 5.084812949  10.16.80.243    10.168.27.10    TCP
 1097 5.089922362  10.16.80.243    10.168.27.10    TCP
 1099 5.095147454  10.16.80.243    10.168.27.10    TCP
 1101 5.100299493  10.16.80.243    10.168.27.10    TCP
 1103 5.105406908  10.16.80.243    10.168.27.10    TCP
 1105 5.110470652  10.16.80.243    10.168.27.10    TCP
 1107 5.115698413  10.16.80.243    10.168.27.10    TCP
 1109 5.120881036  10.16.80.243    10.168.27.10    TCP
 1111 5.126000438  10.16.80.243    10.168.27.10    TCP
 1113 5.131071432  10.16.80.243    10.168.27.10    TCP
 1115 5.136146717  10.16.80.243    10.168.27.10    TCP
 1117 5.141229042  10.16.80.243    10.168.27.10    TCP
 1119 5.146307516  10.16.80.243    10.168.27.10    TCP
 1121 5.151398683  10.16.80.243    10.168.27.10    TCP
 1123 5.156477337  10.16.80.243    10.168.27.10    TCP
 1125 5.161565793  10.16.80.243    10.168.27.10    TCP
 1127 5.166581323  10.16.80.243    10.168.27.10    TCP
 1129 5.171747071  10.16.80.243    10.168.27.10    TCP
```

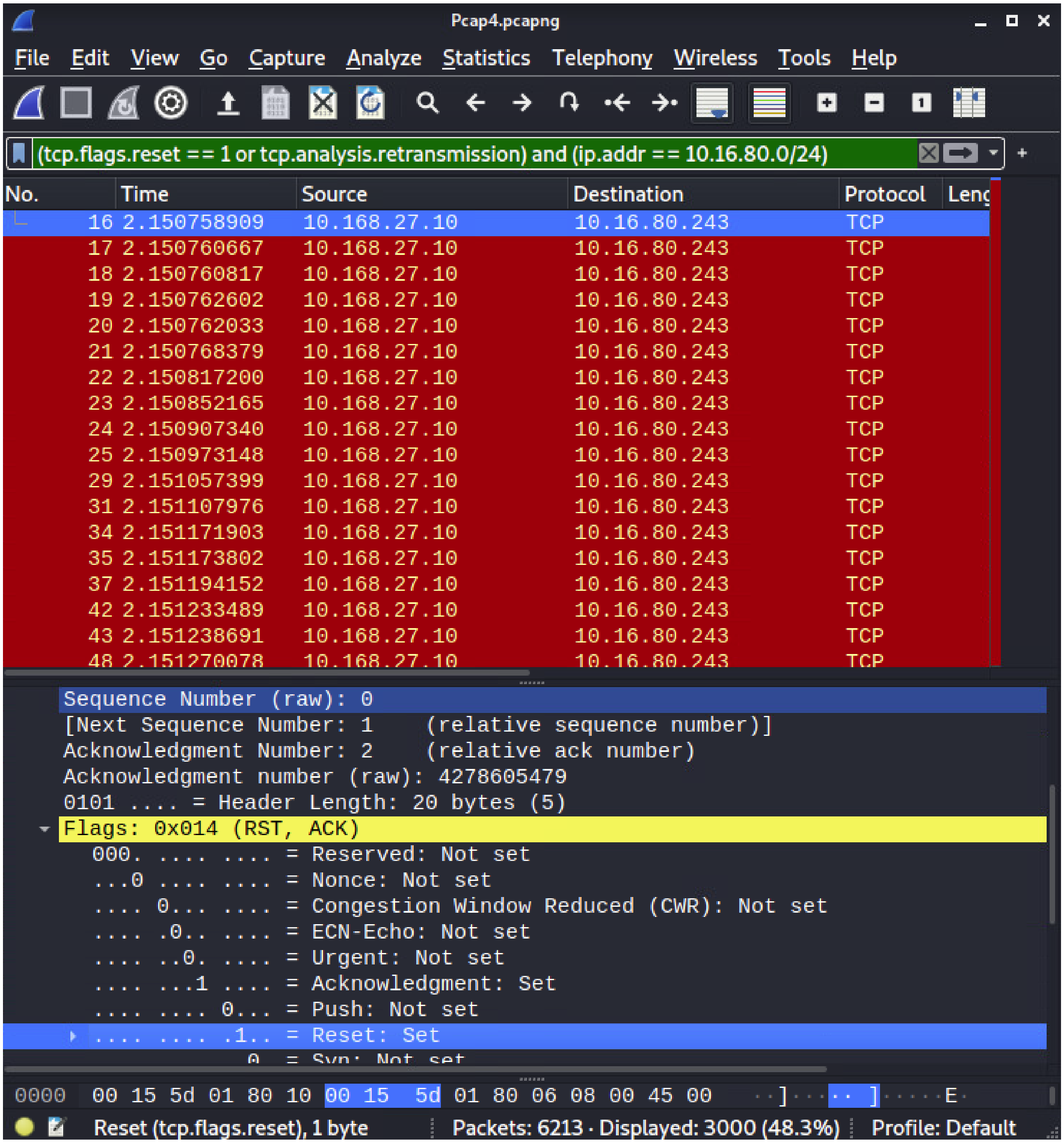
```
  0101 .... = Header Length: 20 bytes (5)
▾ Flags: 0x029 (FIN, PSH, URG)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..1. .... = Urgent: Set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
  ▸ .... .... ...1 = Fin: Set
    [TCP Flags: ······U·P··F]
```

```
0020  1b 0a 83 a5 04 dc ff 06  56 a6 00 00 00 00 50 29   ········ V·····P)
0030  04 00 4c d8 00 00 00 00  00 00 00 00               ··L····· ····
```

Urgent (tcp.flags.urg), 1 byte | Packets: 6213 · Displayed: 3195 (51.4%) | Profile: Default



tcp.analysis.retransmission



Pcap4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

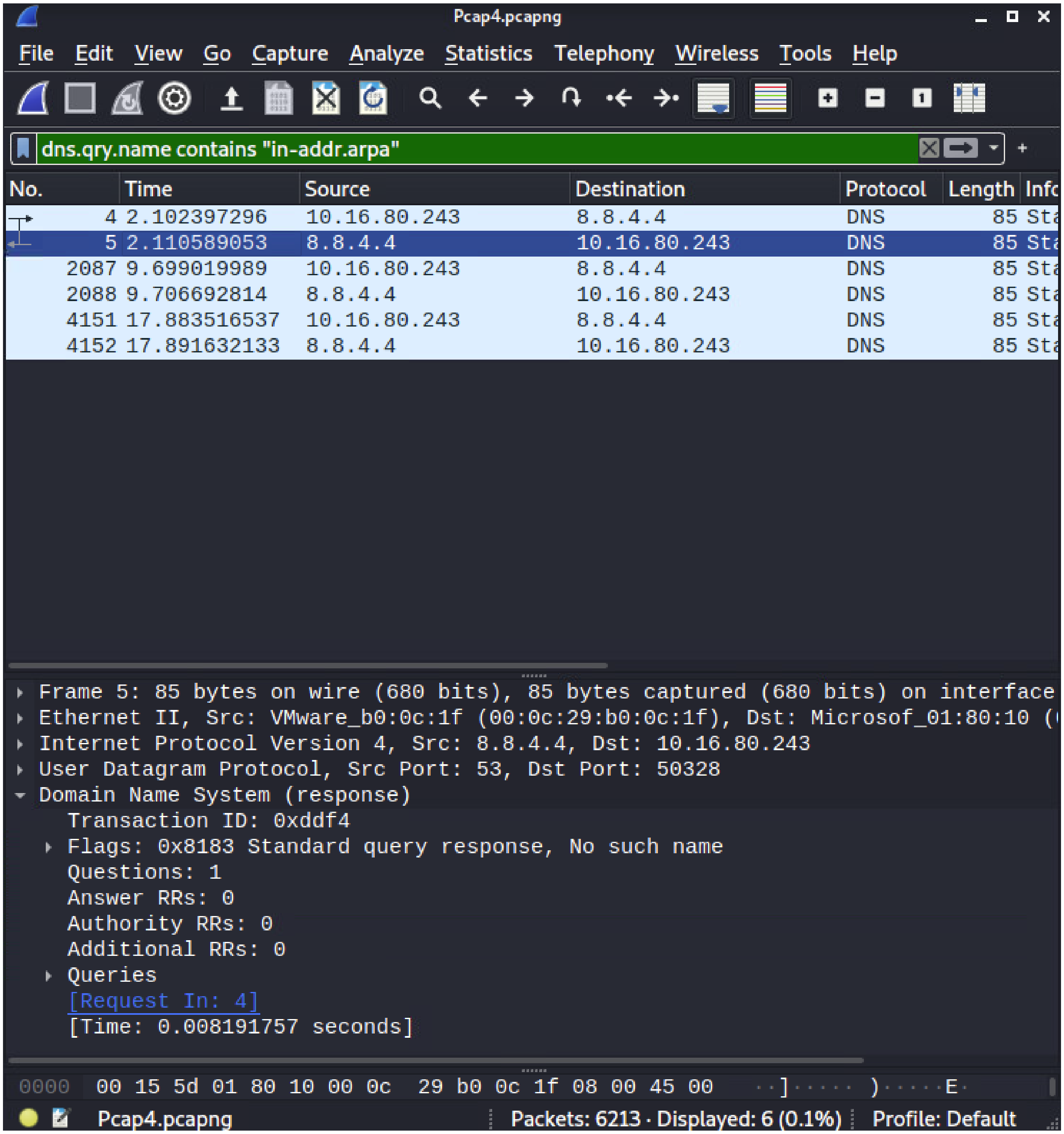
```
(tcp.flags.reset == 1 or tcp.analysis.retransmission) and (ip.addr == 10.16.80.0/24)
```

```
No.      Time          Source         Destination    Protocol  Leng
     16 2.150758909   10.168.27.10   10.16.80.243   TCP
     17 2.150760667   10.168.27.10   10.16.80.243   TCP
     18 2.150760817   10.168.27.10   10.16.80.243   TCP
     19 2.150762602   10.168.27.10   10.16.80.243   TCP
     20 2.150762033   10.168.27.10   10.16.80.243   TCP
     21 2.150768379   10.168.27.10   10.16.80.243   TCP
     22 2.150817200   10.168.27.10   10.16.80.243   TCP
     23 2.150852165   10.168.27.10   10.16.80.243   TCP
     24 2.150907340   10.168.27.10   10.16.80.243   TCP
     25 2.150973148   10.168.27.10   10.16.80.243   TCP
     29 2.151057399   10.168.27.10   10.16.80.243   TCP
     31 2.151107976   10.168.27.10   10.16.80.243   TCP
     34 2.151171903   10.168.27.10   10.16.80.243   TCP
     35 2.151173802   10.168.27.10   10.16.80.243   TCP
     37 2.151194152   10.168.27.10   10.16.80.243   TCP
     42 2.151233489   10.168.27.10   10.16.80.243   TCP
     43 2.151238691   10.168.27.10   10.16.80.243   TCP
     48 2.151270078   10.168.27.10   10.16.80.243   TCP
```

```
    Sequence Number (raw): 0
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 2    (relative ack number)
    Acknowledgment number (raw): 4278605479
    0101 .... = Header Length: 20 bytes (5)
  ▾ Flags: 0x014 (RST, ACK)
       000. .... .... = Reserved: Not set
       ...0 .... .... = Nonce: Not set
       .... 0... .... = Congestion Window Reduced (CWR): Not set
       .... .0.. .... = ECN-Echo: Not set
       .... ..0. .... = Urgent: Not set
       .... ...1 .... = Acknowledgment: Set
       .... .... 0... = Push: Not set
     ▸ .... .... .1.. = Reset: Set
                    0 = Syn: Not set
```

```
0000  00 15 5d 01 80 10 00 15  5d 01 80 06 08 00 45 00   ··]·····]·····E·
```

```
Reset (tcp.flags.reset), 1 byte    Packets: 6213 · Displayed: 3000 (48.3%)    Profile: Default
```



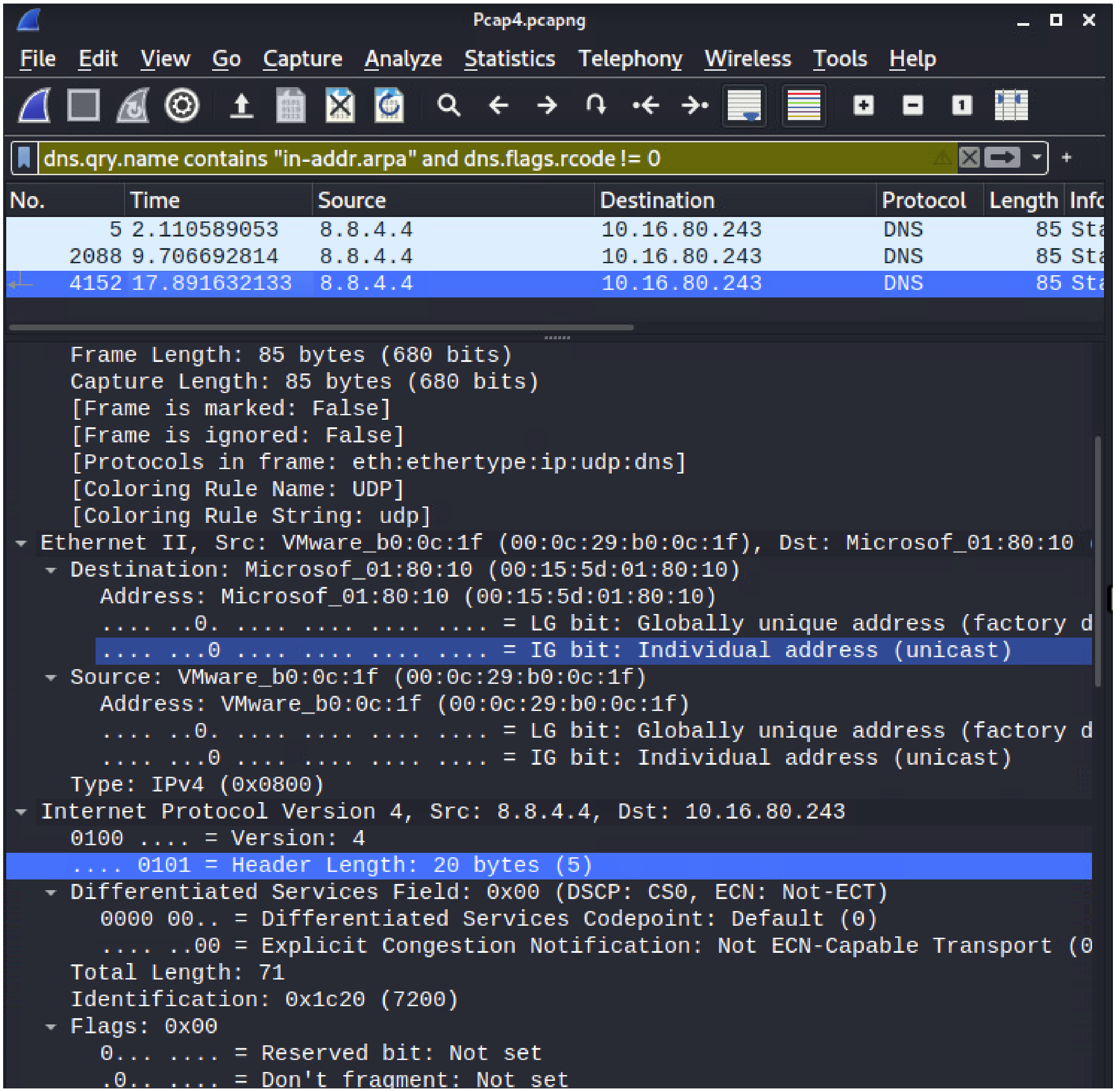
```
dns.qry.name contains "in-addr.arpa"
```

```
No.    Time         Source        Destination   Protocol Length Info
     4 2.102397296  10.16.80.243  8.8.4.4       DNS          85 Sta
     5 2.110589053  8.8.4.4       10.16.80.243  DNS          85 Sta
  2087 9.699019989  10.16.80.243  8.8.4.4       DNS          85 Sta
  2088 9.706692814  8.8.4.4       10.16.80.243  DNS          85 Sta
  4151 17.883516537 10.16.80.243  8.8.4.4       DNS          85 Sta
  4152 17.891632133 8.8.4.4       10.16.80.243  DNS          85 Sta
```

```
› Frame 5: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface
› Ethernet II, Src: VMware_b0:0c:1f (00:0c:29:b0:0c:1f), Dst: Microsof_01:80:10 (
› Internet Protocol Version 4, Src: 8.8.4.4, Dst: 10.16.80.243
› User Datagram Protocol, Src Port: 53, Dst Port: 50328
⌄ Domain Name System (response)
    Transaction ID: 0xddf4
  › Flags: 0x8183 Standard query response, No such name
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  › Queries
    [Request In: 4]
    [Time: 0.008191757 seconds]
```

```
0000  00 15 5d 01 80 10 00 0c  29 b0 0c 1f 08 00 45 00   ··]·····)·····E·
```

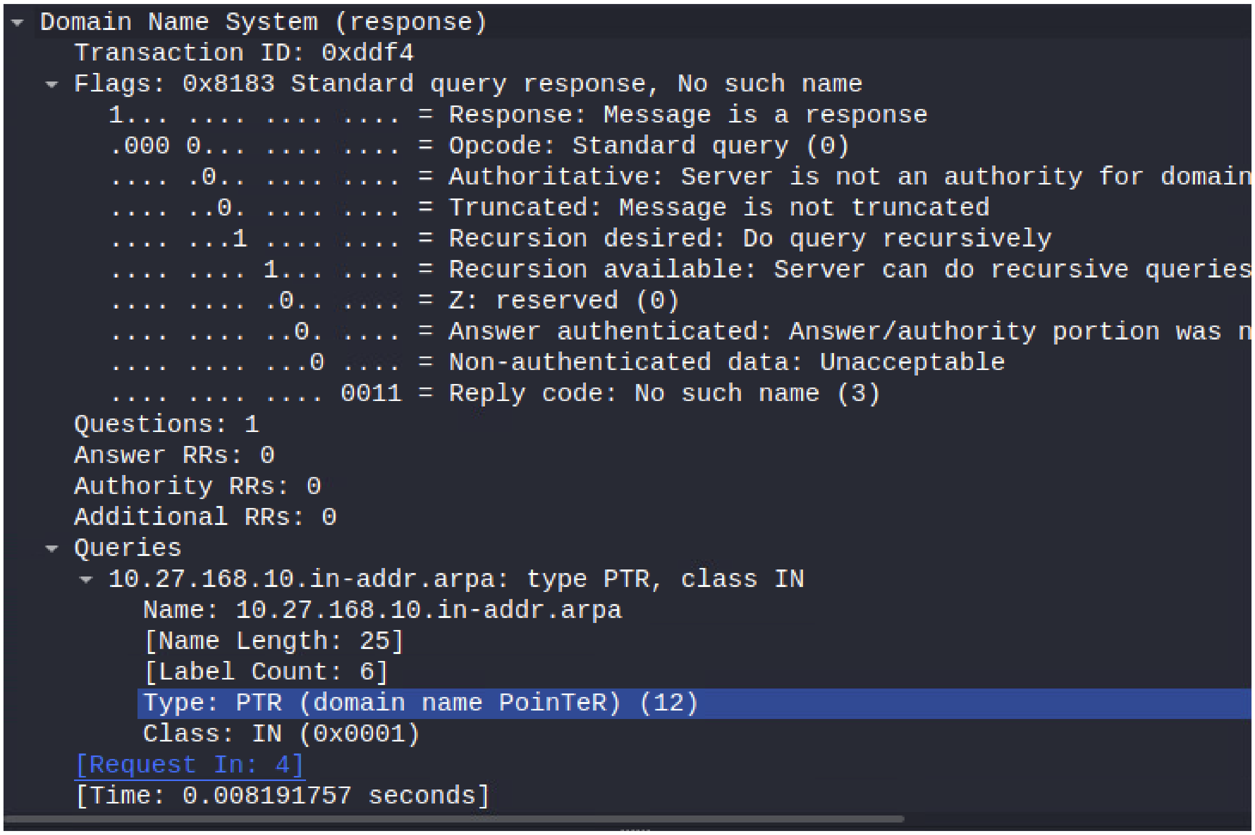
Pcap4.pcapng | Packets: 6213 · Displayed: 6 (0.1%) | Profile: Default


Pcap4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

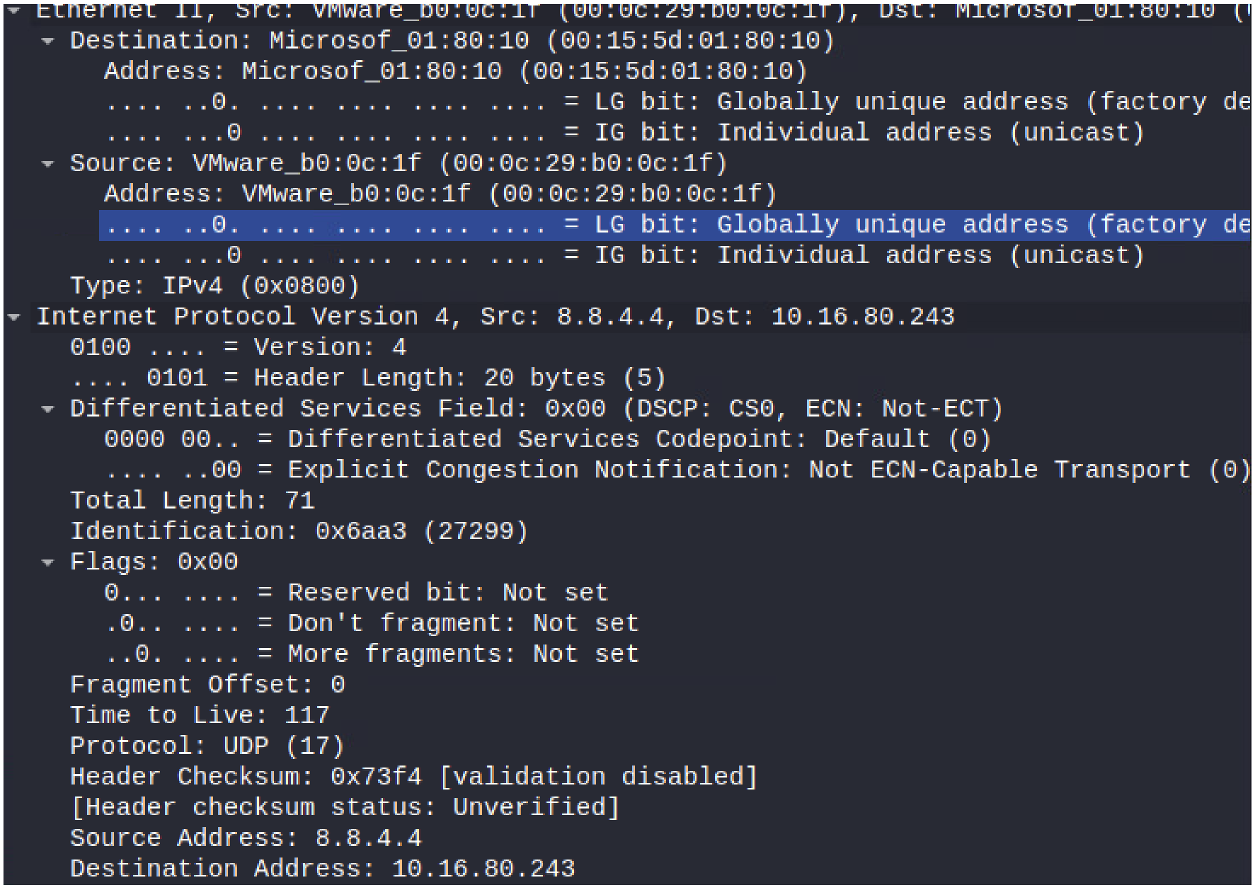
```
dns.qry.name contains "in-addr.arpa" and dns.flags.rcode != 0
```

```
No.      Time           Source        Destination      Protocol   Length  Info
      5  2.110589053    8.8.4.4       10.16.80.243     DNS            85  Sta
   2088  9.706692814    8.8.4.4       10.16.80.243     DNS            85  Sta
   4152  17.891632133   8.8.4.4       10.16.80.243     DNS            85  Sta
```

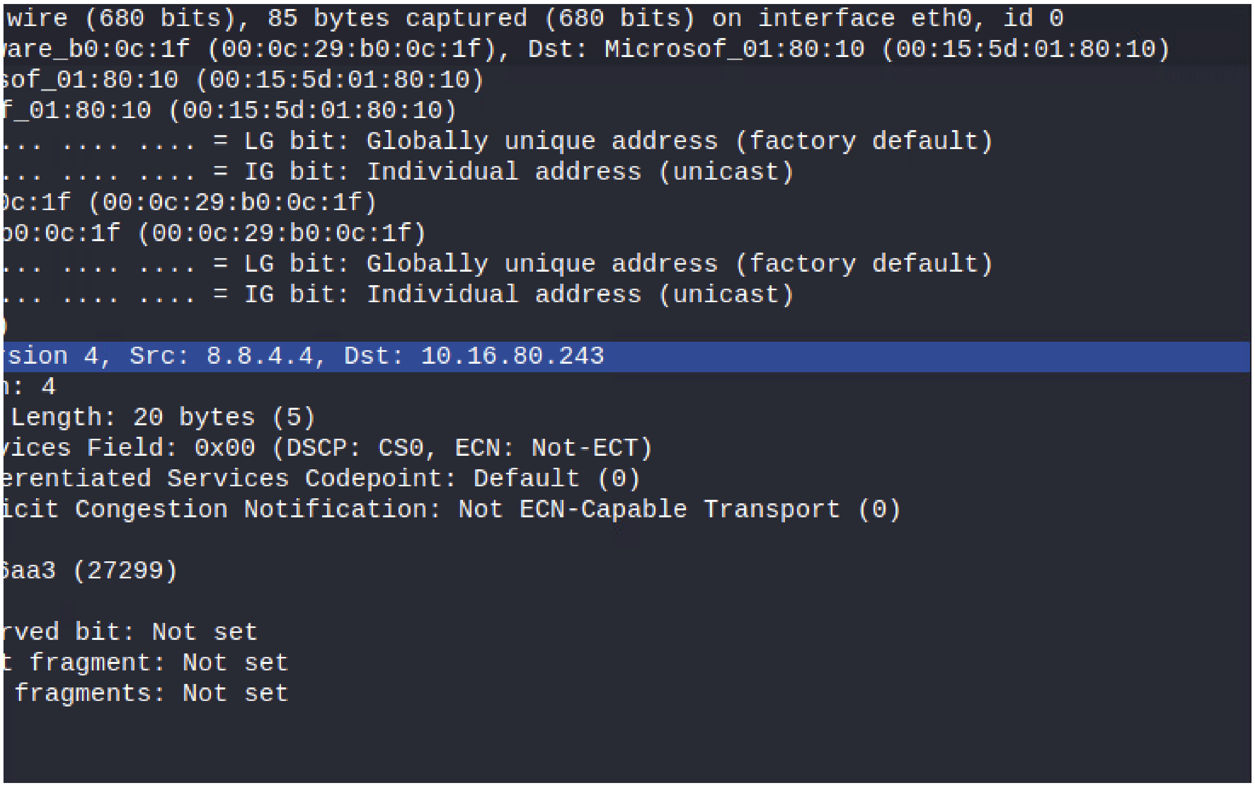
```
    Frame Length: 85 bytes (680 bits)
    Capture Length: 85 bytes (680 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
  Ethernet II, Src: VMware_b0:0c:1f (00:0c:29:b0:0c:1f), Dst: Microsof_01:80:10 (
    Destination: Microsof_01:80:10 (00:15:5d:01:80:10)
      Address: Microsof_01:80:10 (00:15:5d:01:80:10)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory d
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
      Address: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory d
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 8.8.4.4, Dst: 10.16.80.243
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0
    Total Length: 71
    Identification: 0x1c20 (7200)
    Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
```



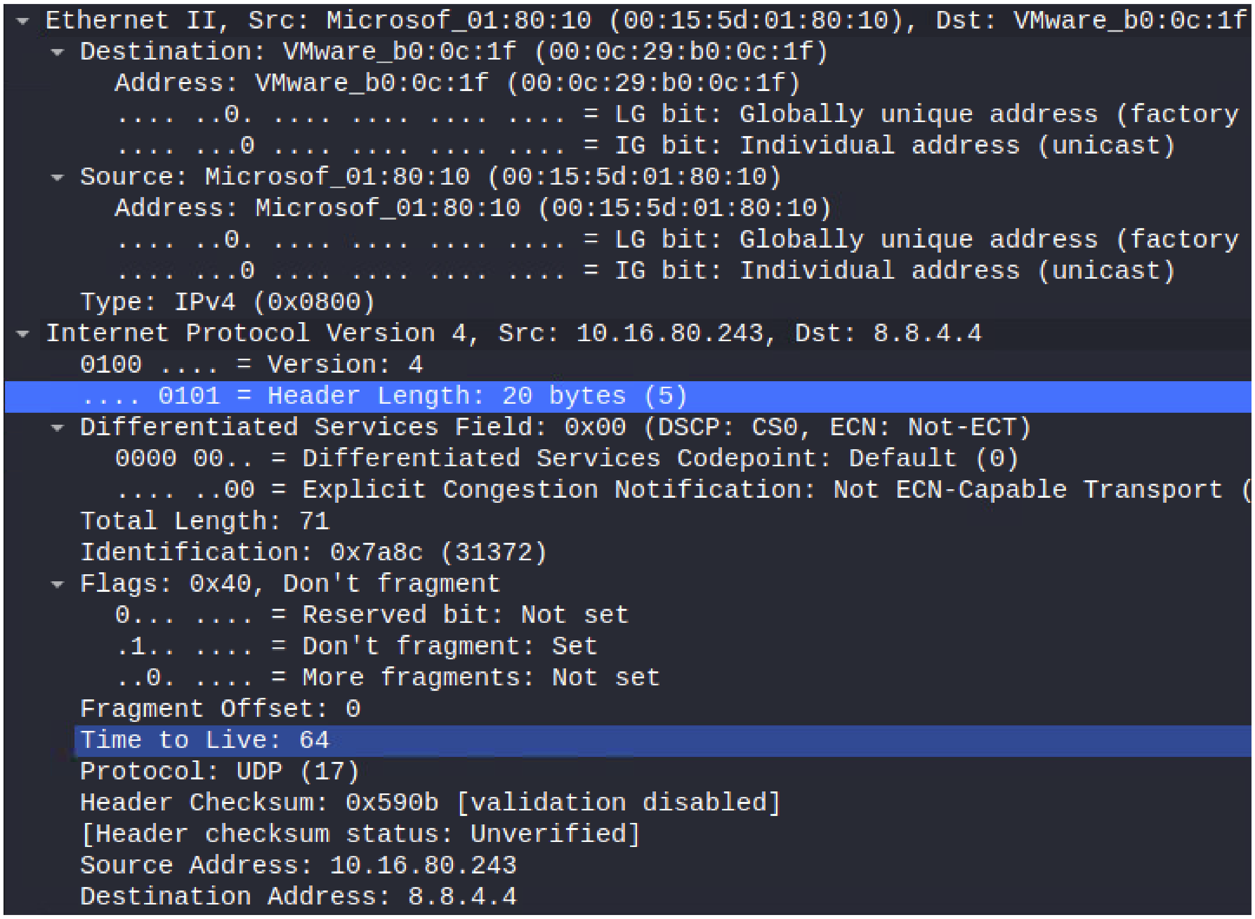
```
▾ Domain Name System (response)
    Transaction ID: 0xddf4
  ▾ Flags: 0x8183 Standard query response, No such name
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was n
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0011 = Reply code: No such name (3)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ 10.27.168.10.in-addr.arpa: type PTR, class IN
        Name: 10.27.168.10.in-addr.arpa
        [Name Length: 25]
        [Label Count: 6]
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
    [Request In: 4]
    [Time: 0.008191757 seconds]
```



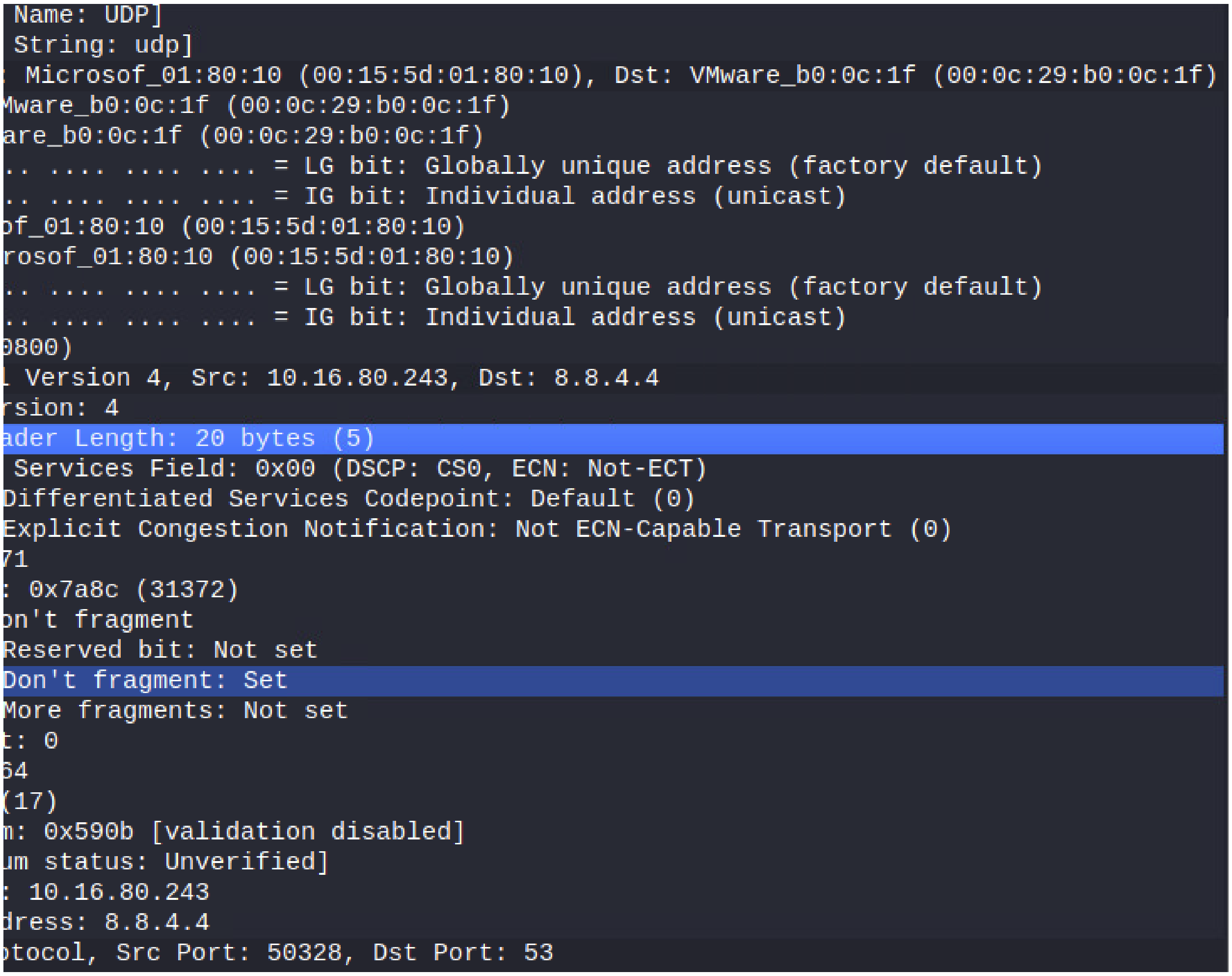
```
▾ Ethernet II, Src: VMware_b0:0c:1f (00:0c:29:b0:0c:1f), Dst: Microsof_01:80:10 (
  ▾ Destination: Microsof_01:80:10 (00:15:5d:01:80:10)
      Address: Microsof_01:80:10 (00:15:5d:01:80:10)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory de
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
      Address: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory de
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 8.8.4.4, Dst: 10.16.80.243
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 71
    Identification: 0x6aa3 (27299)
  ▾ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 117
    Protocol: UDP (17)
    Header Checksum: 0x73f4 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 8.8.4.4
    Destination Address: 10.16.80.243
```



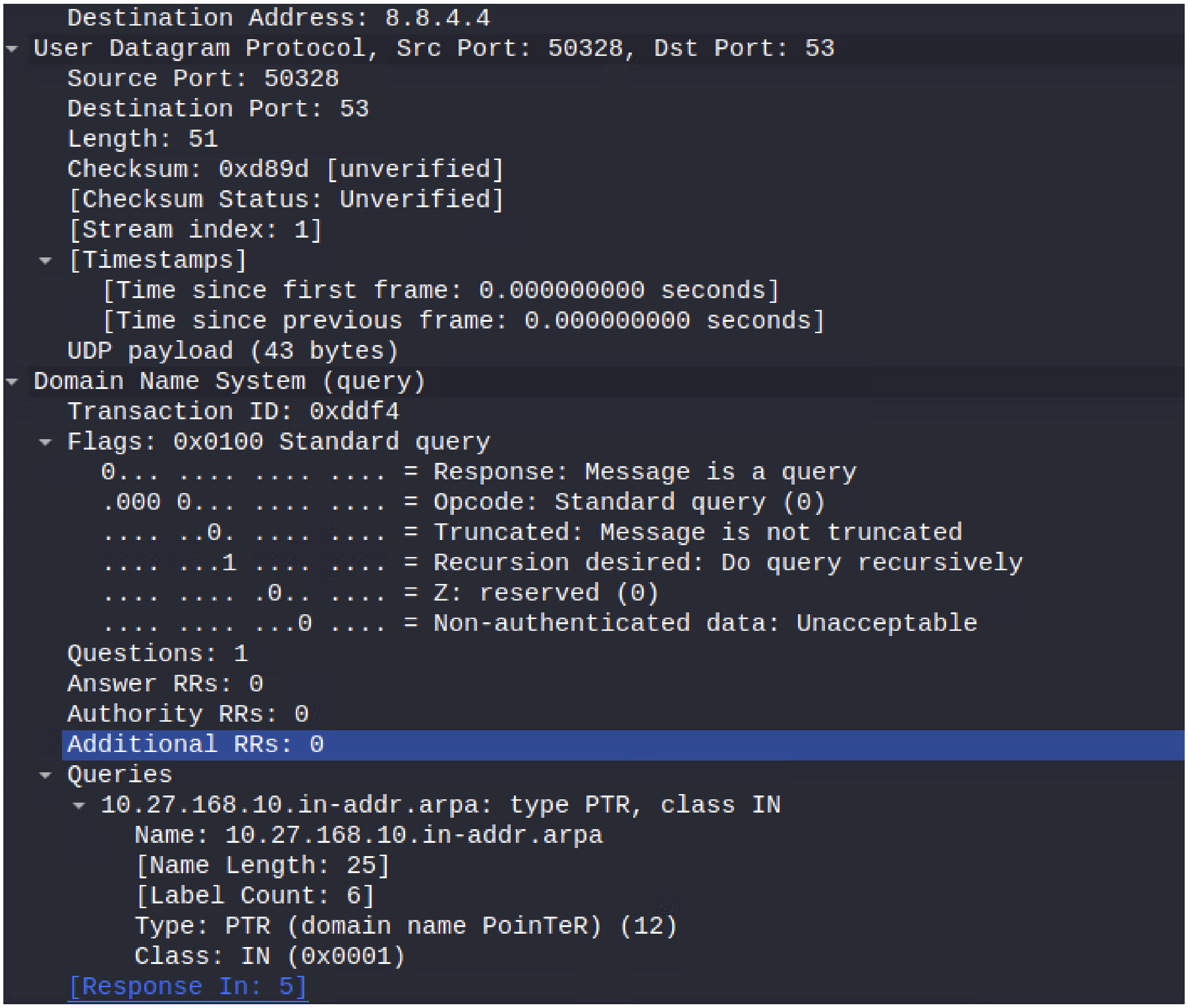
```
wire (680 bits), 85 bytes captured (680 bits) on interface eth0, id 0
are_b0:0c:1f (00:0c:29:b0:0c:1f), Dst: Microsof_01:80:10 (00:15:5d:01:80:10)
sof_01:80:10 (00:15:5d:01:80:10)
f_01:80:10 (00:15:5d:01:80:10)
... .... .... = LG bit: Globally unique address (factory default)
... .... .... = IG bit: Individual address (unicast)
0c:1f (00:0c:29:b0:0c:1f)
b0:0c:1f (00:0c:29:b0:0c:1f)
... .... .... = LG bit: Globally unique address (factory default)
... .... .... = IG bit: Individual address (unicast)
)
sion 4, Src: 8.8.4.4, Dst: 10.16.80.243
: 4
 Length: 20 bytes (5)
vices Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
erentiated Services Codepoint: Default (0)
icit Congestion Notification: Not ECN-Capable Transport (0)

aa3 (27299)

rved bit: Not set
t fragment: Not set
 fragments: Not set
```



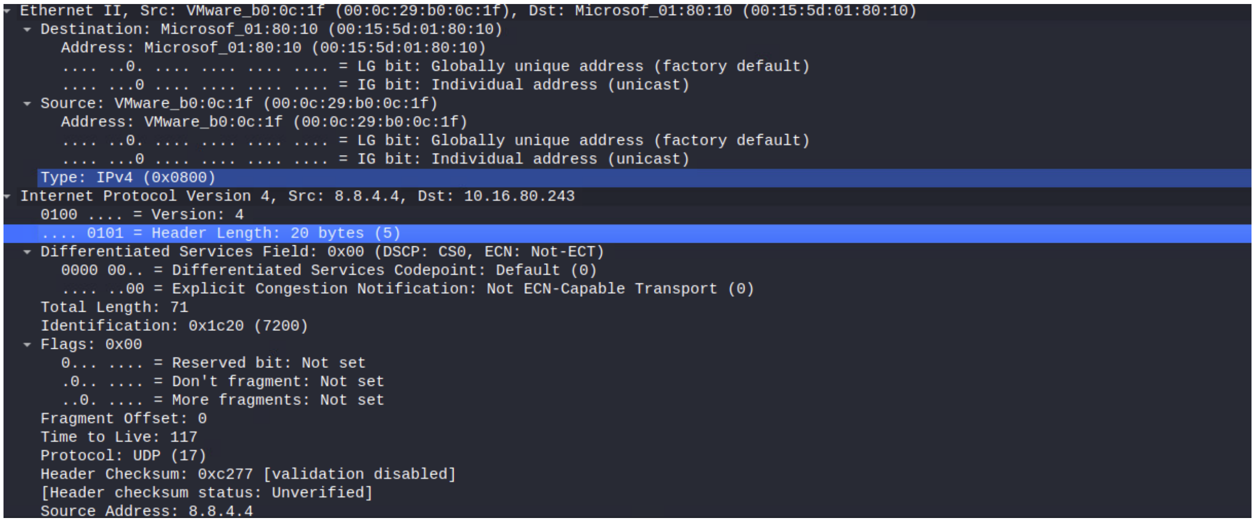
```
Ethernet II, Src: Microsof_01:80:10 (00:15:5d:01:80:10), Dst: VMware_b0:0c:1f
  Destination: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
    Address: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: Microsof_01:80:10 (00:15:5d:01:80:10)
    Address: Microsof_01:80:10 (00:15:5d:01:80:10)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.16.80.243, Dst: 8.8.4.4
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (
  Total Length: 71
  Identification: 0x7a8c (31372)
  Flags: 0x40, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0x590b [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.16.80.243
  Destination Address: 8.8.4.4
```



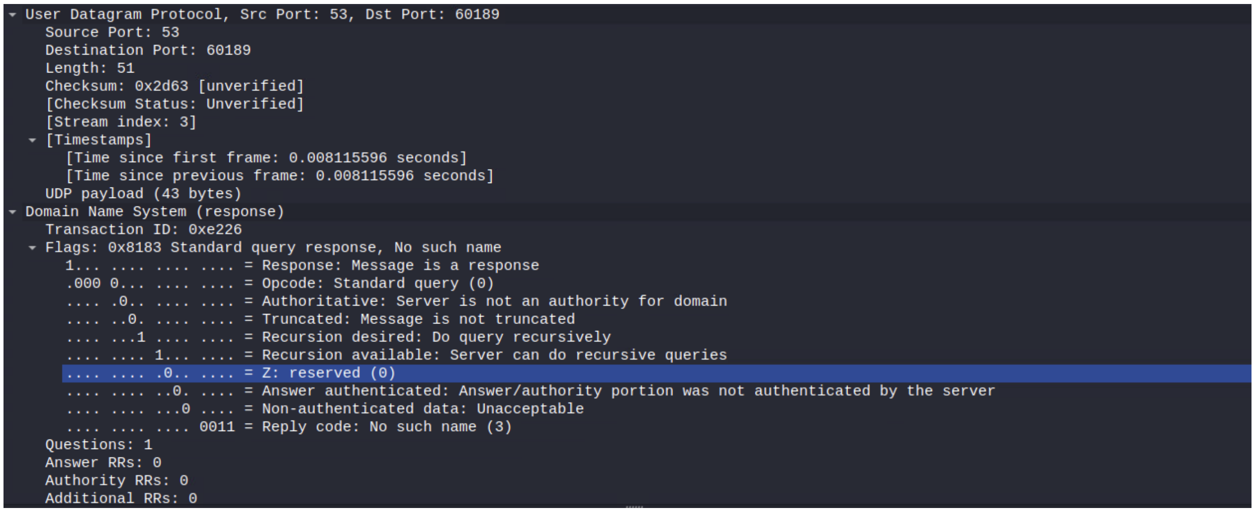
```
 Name: UDP]
 String: udp]
: Microsof_01:80:10 (00:15:5d:01:80:10), Dst: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
Mware_b0:0c:1f (00:0c:29:b0:0c:1f)
are_b0:0c:1f (00:0c:29:b0:0c:1f)
.. .... .... .... = LG bit: Globally unique address (factory default)
.. .... .... .... = IG bit: Individual address (unicast)
of_01:80:10 (00:15:5d:01:80:10)
rosof_01:80:10 (00:15:5d:01:80:10)
.. .... .... .... = LG bit: Globally unique address (factory default)
.. .... .... .... = IG bit: Individual address (unicast)
0800)
l Version 4, Src: 10.16.80.243, Dst: 8.8.4.4
rsion: 4
ader Length: 20 bytes (5)
 Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Differentiated Services Codepoint: Default (0)
Explicit Congestion Notification: Not ECN-Capable Transport (0)
71
: 0x7a8c (31372)
on't fragment
Reserved bit: Not set
Don't fragment: Set
More fragments: Not set
t: 0
64
(17)
m: 0x590b [validation disabled]
um status: Unverified]
: 10.16.80.243
dress: 8.8.4.4
otocol, Src Port: 50328, Dst Port: 53
```



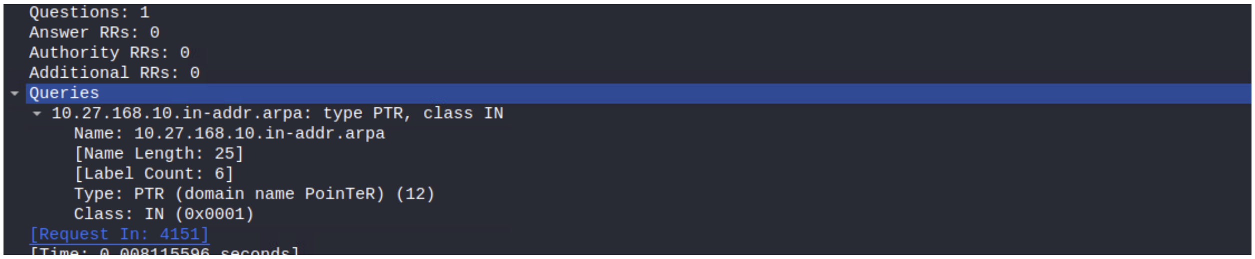
```
    Destination Address: 8.8.4.4
User Datagram Protocol, Src Port: 50328, Dst Port: 53
    Source Port: 50328
    Destination Port: 53
    Length: 51
    Checksum: 0xd89d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
    [Timestamps]
        [Time since first frame: 0.000000000 seconds]
        [Time since previous frame: 0.000000000 seconds]
    UDP payload (43 bytes)
Domain Name System (query)
    Transaction ID: 0xddf4
    Flags: 0x0100 Standard query
        0... .... .... .... = Response: Message is a query
        .000 0... .... .... = Opcode: Standard query (0)
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        10.27.168.10.in-addr.arpa: type PTR, class IN
            Name: 10.27.168.10.in-addr.arpa
            [Name Length: 25]
            [Label Count: 6]
            Type: PTR (domain name PoinTeR) (12)
            Class: IN (0x0001)
    [Response In: 5]
```



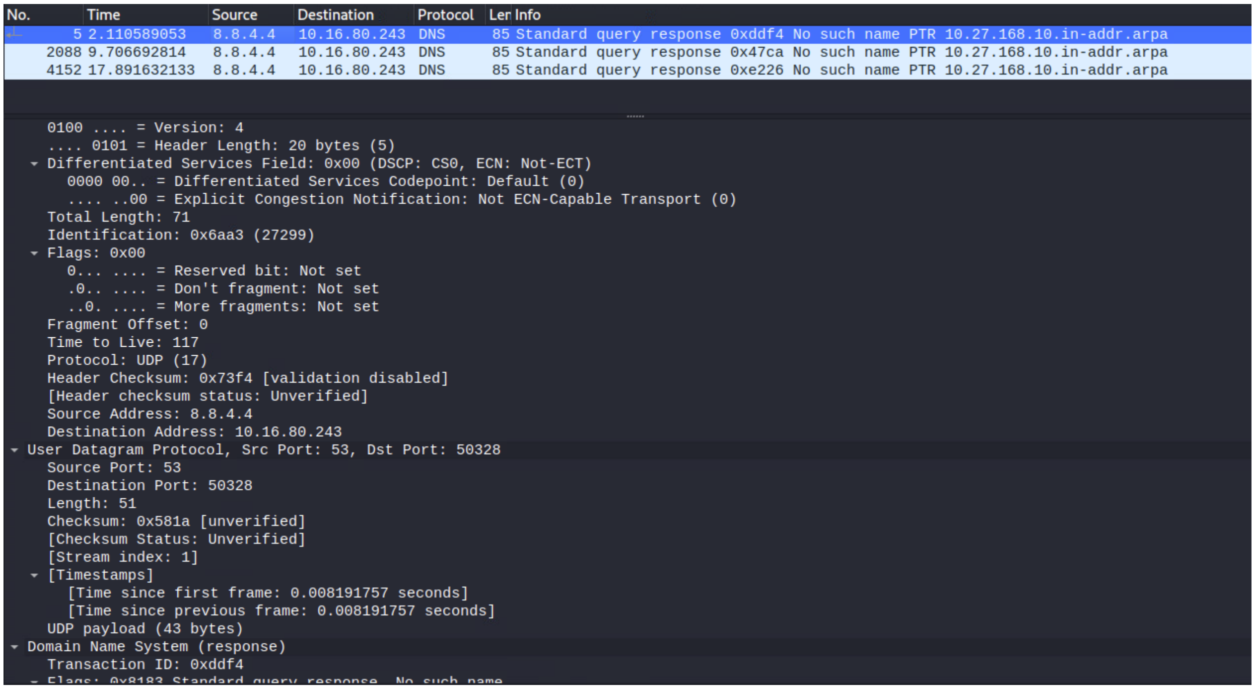
```
Ethernet II, Src: VMware_b0:0c:1f (00:0c:29:b0:0c:1f), Dst: Microsof_01:80:10 (00:15:5d:01:80:10)
  Destination: Microsof_01:80:10 (00:15:5d:01:80:10)
    Address: Microsof_01:80:10 (00:15:5d:01:80:10)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
    Address: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 8.8.4.4, Dst: 10.16.80.243
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 71
  Identification: 0x1c20 (7200)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment Offset: 0
  Time to Live: 117
  Protocol: UDP (17)
  Header Checksum: 0xc277 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 8.8.4.4
```



```
▾ User Datagram Protocol, Src Port: 53, Dst Port: 60189
    Source Port: 53
    Destination Port: 60189
    Length: 51
    Checksum: 0x2d63 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  ▾ [Timestamps]
      [Time since first frame: 0.008115596 seconds]
      [Time since previous frame: 0.008115596 seconds]
    UDP payload (43 bytes)
▾ Domain Name System (response)
    Transaction ID: 0xe226
  ▾ Flags: 0x8183 Standard query response, No such name
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0011 = Reply code: No such name (3)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
```

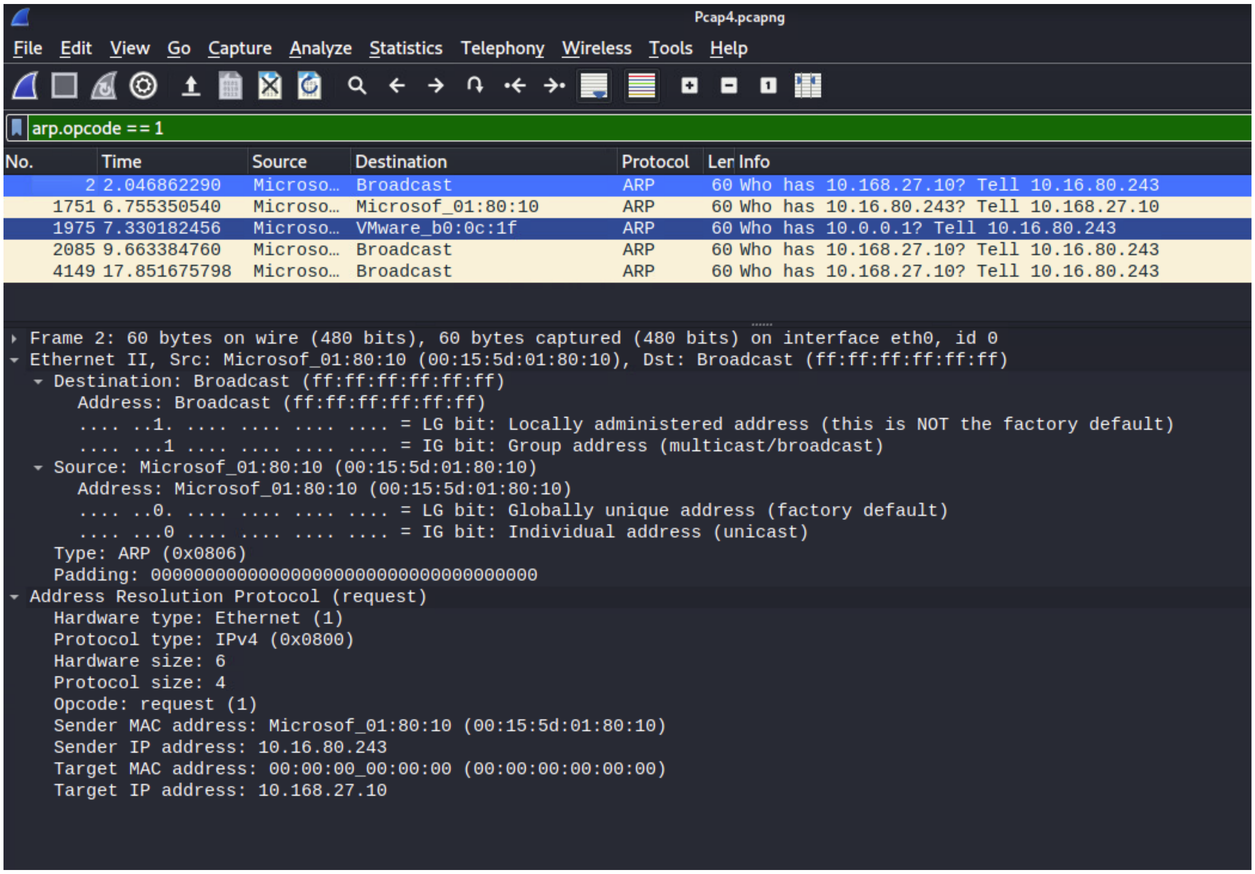


```
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
▾ Queries
  ▾ 10.27.168.10.in-addr.arpa: type PTR, class IN
      Name: 10.27.168.10.in-addr.arpa
      [Name Length: 25]
      [Label Count: 6]
      Type: PTR (domain name PoinTeR) (12)
      Class: IN (0x0001)
  [Request In: 4151]
  [Time: 0.008115596 seconds]
```



```
No.    Time         Source   Destination   Protocol Len Info
     5 2.110589053  8.8.4.4  10.16.80.243  DNS       85 Standard query response 0xddf4 No such name PTR 10.27.168.10.in-addr.arpa
  2088 9.706692814  8.8.4.4  10.16.80.243  DNS       85 Standard query response 0x47ca No such name PTR 10.27.168.10.in-addr.arpa
  4152 17.891632133 8.8.4.4  10.16.80.243  DNS       85 Standard query response 0xe226 No such name PTR 10.27.168.10.in-addr.arpa
```

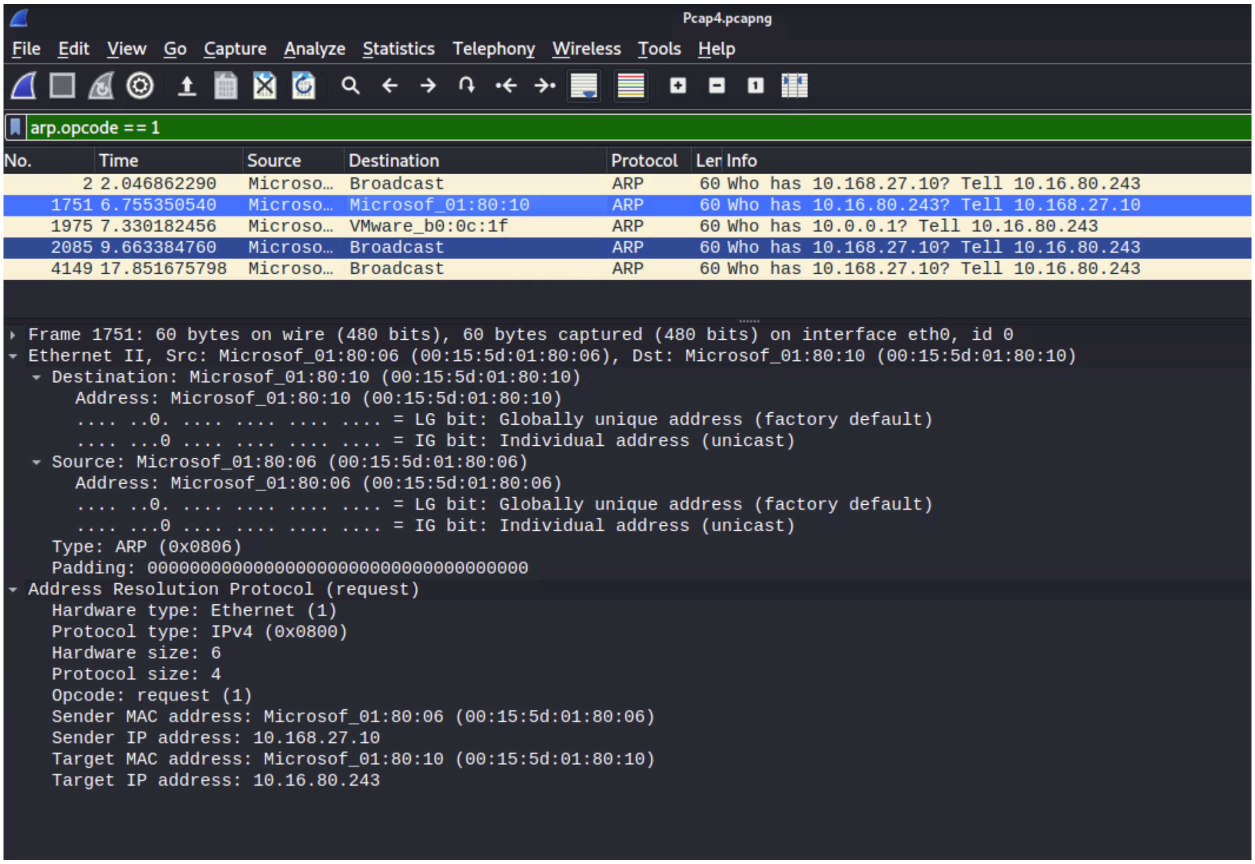
```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 71
    Identification: 0x6aa3 (27299)
  ▾ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 117
    Protocol: UDP (17)
    Header Checksum: 0x73f4 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 8.8.4.4
    Destination Address: 10.16.80.243
▾ User Datagram Protocol, Src Port: 53, Dst Port: 50328
    Source Port: 53
    Destination Port: 50328
    Length: 51
    Checksum: 0x581a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  ▾ [Timestamps]
      [Time since first frame: 0.008191757 seconds]
      [Time since previous frame: 0.008191757 seconds]
    UDP payload (43 bytes)
▾ Domain Name System (response)
    Transaction ID: 0xddf4
  ▾ Flags: 0x8183 Standard query response, No such name
```


Pcap4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
arp.opcode == 1
```

```
No.   Time          Source     Destination       Protocol  Len Info
    2 2.046862290   Microso…   Broadcast         ARP       60 Who has 10.168.27.10? Tell 10.16.80.243
 1751 6.755350540   Microso…   Microsof_01:80:10 ARP       60 Who has 10.16.80.243? Tell 10.168.27.10
 1975 7.330182456   Microso…   VMware_b0:0c:1f   ARP       60 Who has 10.0.0.1? Tell 10.16.80.243
 2085 9.663384760   Microso…   Broadcast         ARP       60 Who has 10.168.27.10? Tell 10.16.80.243
 4149 17.851675798  Microso…   Broadcast         ARP       60 Who has 10.168.27.10? Tell 10.16.80.243
```

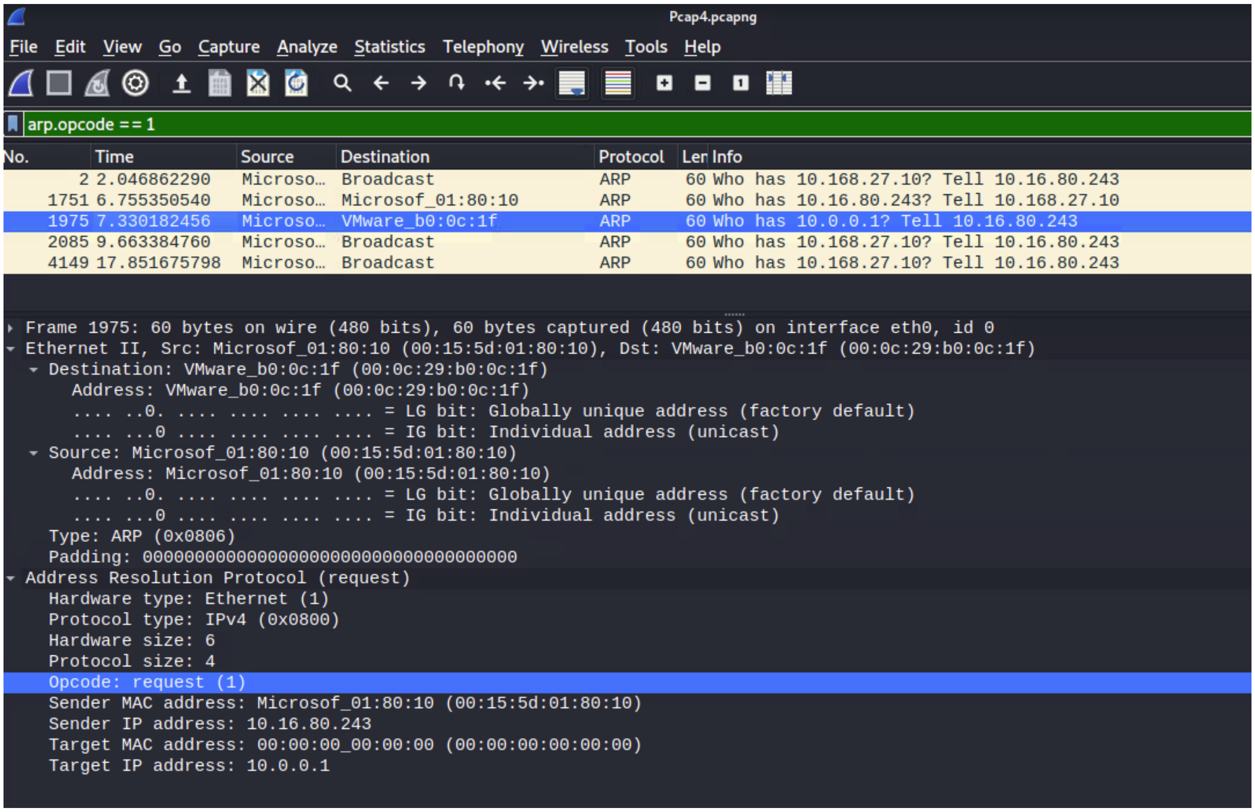
```
▸ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▾ Ethernet II, Src: Microsof_01:80:10 (00:15:5d:01:80:10), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▾ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ▾ Source: Microsof_01:80:10 (00:15:5d:01:80:10)
      Address: Microsof_01:80:10 (00:15:5d:01:80:10)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Microsof_01:80:10 (00:15:5d:01:80:10)
    Sender IP address: 10.16.80.243
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.168.27.10
```



```
arp.opcode == 1
```

```
No.   Time          Source     Destination        Protocol  Ler Info
    2 2.046862290   Microso…   Broadcast          ARP       60 Who has 10.168.27.10? Tell 10.16.80.243
 1751 6.755350540   Microso…   Microsof_01:80:10  ARP       60 Who has 10.16.80.243? Tell 10.168.27.10
 1975 7.330182456   Microso…   VMware_b0:0c:1f    ARP       60 Who has 10.0.0.1? Tell 10.16.80.243
 2085 9.663384760   Microso…   Broadcast          ARP       60 Who has 10.168.27.10? Tell 10.16.80.243
 4149 17.851675798  Microso…   Broadcast          ARP       60 Who has 10.168.27.10? Tell 10.16.80.243
```

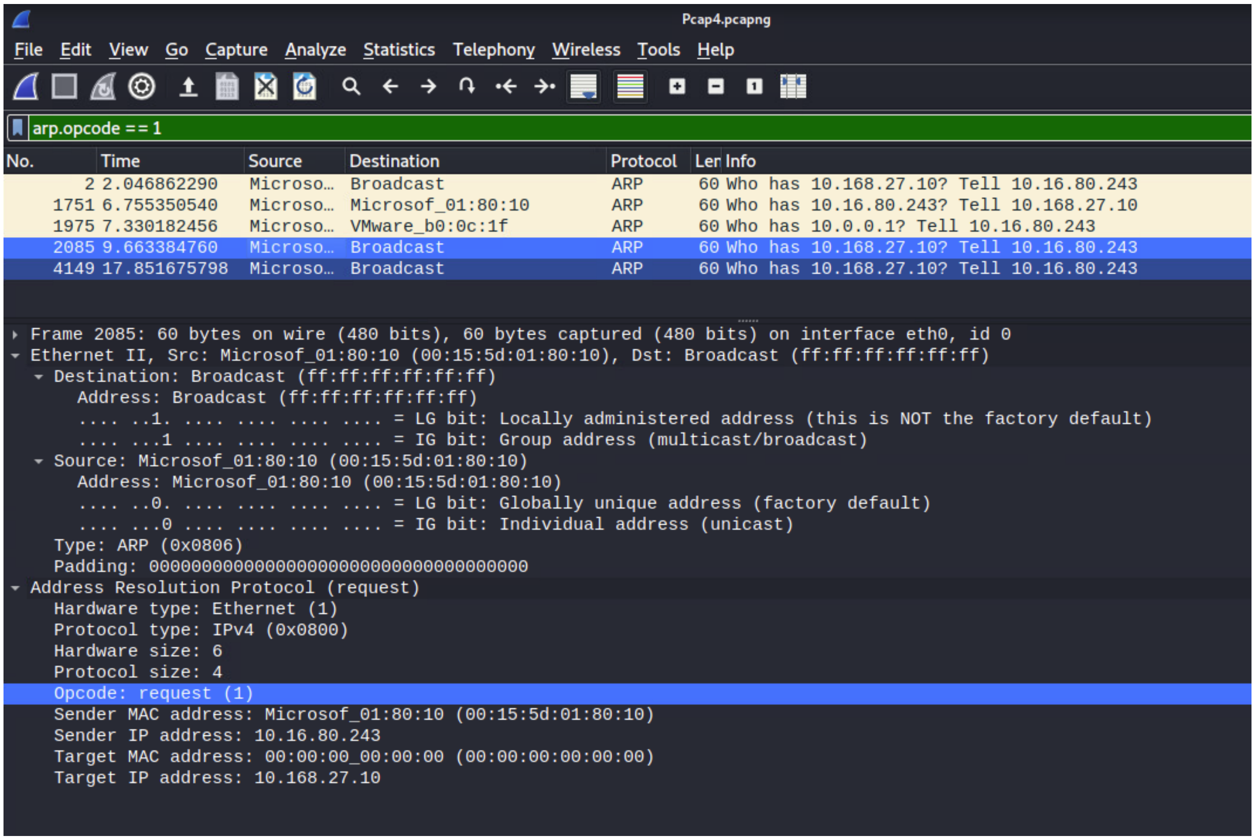
```
Frame 1751: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_01:80:06 (00:15:5d:01:80:06), Dst: Microsof_01:80:10 (00:15:5d:01:80:10)
  Destination: Microsof_01:80:10 (00:15:5d:01:80:10)
    Address: Microsof_01:80:10 (00:15:5d:01:80:10)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: Microsof_01:80:06 (00:15:5d:01:80:06)
    Address: Microsof_01:80:06 (00:15:5d:01:80:06)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  Padding: 000000000000000000000000000000000000
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Microsof_01:80:06 (00:15:5d:01:80:06)
  Sender IP address: 10.168.27.10
  Target MAC address: Microsof_01:80:10 (00:15:5d:01:80:10)
  Target IP address: 10.16.80.243
```



```
arp.opcode == 1
```

```
No.   Time          Source     Destination        Protocol  Ler Info
    2 2.046862290   Microso…   Broadcast          ARP       60 Who has 10.168.27.10? Tell 10.16.80.243
 1751 6.755350540   Microso…   Microsof_01:80:10  ARP       60 Who has 10.16.80.243? Tell 10.168.27.10
 1975 7.330182456   Microso…   VMware_b0:0c:1f    ARP       60 Who has 10.0.0.1? Tell 10.16.80.243
 2085 9.663384760   Microso…   Broadcast          ARP       60 Who has 10.168.27.10? Tell 10.16.80.243
 4149 17.851675798  Microso…   Broadcast          ARP       60 Who has 10.168.27.10? Tell 10.16.80.243
```

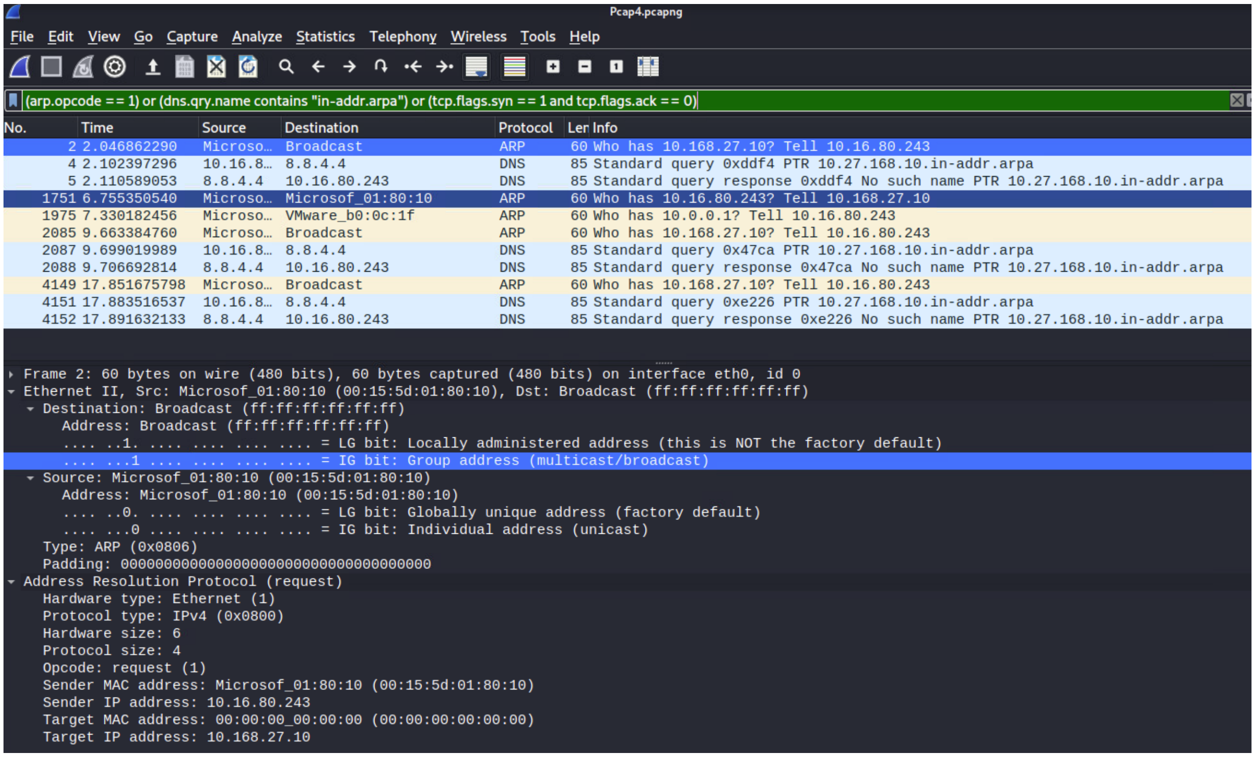
```
Frame 1975: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_01:80:10 (00:15:5d:01:80:10), Dst: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
  Destination: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
    Address: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: Microsof_01:80:10 (00:15:5d:01:80:10)
    Address: Microsof_01:80:10 (00:15:5d:01:80:10)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  Padding: 000000000000000000000000000000000000
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Microsof_01:80:10 (00:15:5d:01:80:10)
  Sender IP address: 10.16.80.243
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 10.0.0.1
```


Pcap4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp.opcode == 1

```
No.   Time          Source     Destination        Protocol Ler Info
    2 2.046862290   Microso…  Broadcast          ARP       60 Who has 10.168.27.10? Tell 10.16.80.243
 1751 6.755350540   Microso…  Microsof_01:80:10  ARP       60 Who has 10.16.80.243? Tell 10.168.27.10
 1975 7.330182456   Microso…  VMware_b0:0c:1f    ARP       60 Who has 10.0.0.1? Tell 10.16.80.243
 2085 9.663384760   Microso…  Broadcast          ARP       60 Who has 10.168.27.10? Tell 10.16.80.243
 4149 17.851675798  Microso…  Broadcast          ARP       60 Who has 10.168.27.10? Tell 10.16.80.243
```

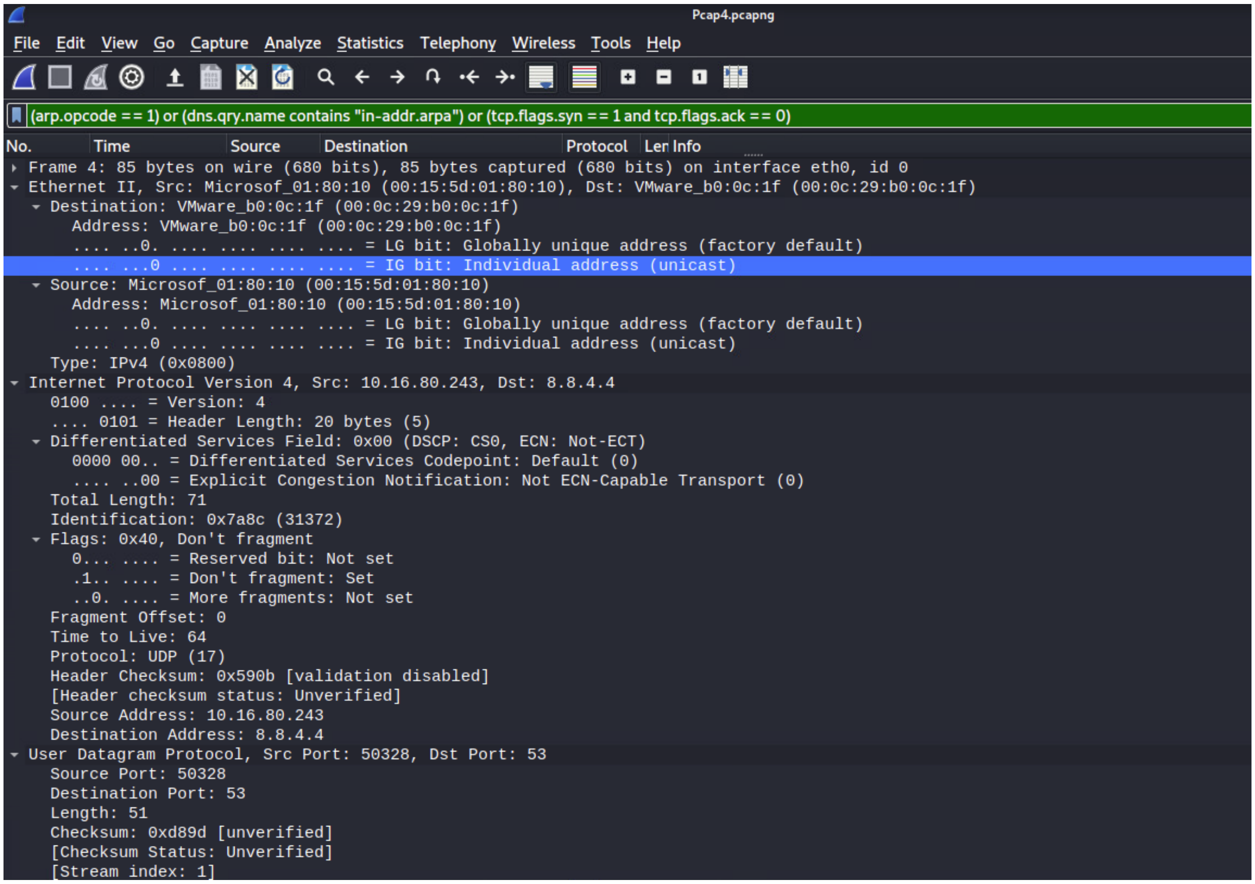
```
▸ Frame 2085: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▾ Ethernet II, Src: Microsof_01:80:10 (00:15:5d:01:80:10), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▾ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ▾ Source: Microsof_01:80:10 (00:15:5d:01:80:10)
      Address: Microsof_01:80:10 (00:15:5d:01:80:10)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Microsof_01:80:10 (00:15:5d:01:80:10)
    Sender IP address: 10.16.80.243
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.168.27.10
```


Pcap4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(arp.opcode == 1) or (dns.qry.name contains "in-addr.arpa") or (tcp.flags.syn == 1 and tcp.flags.ack == 0)

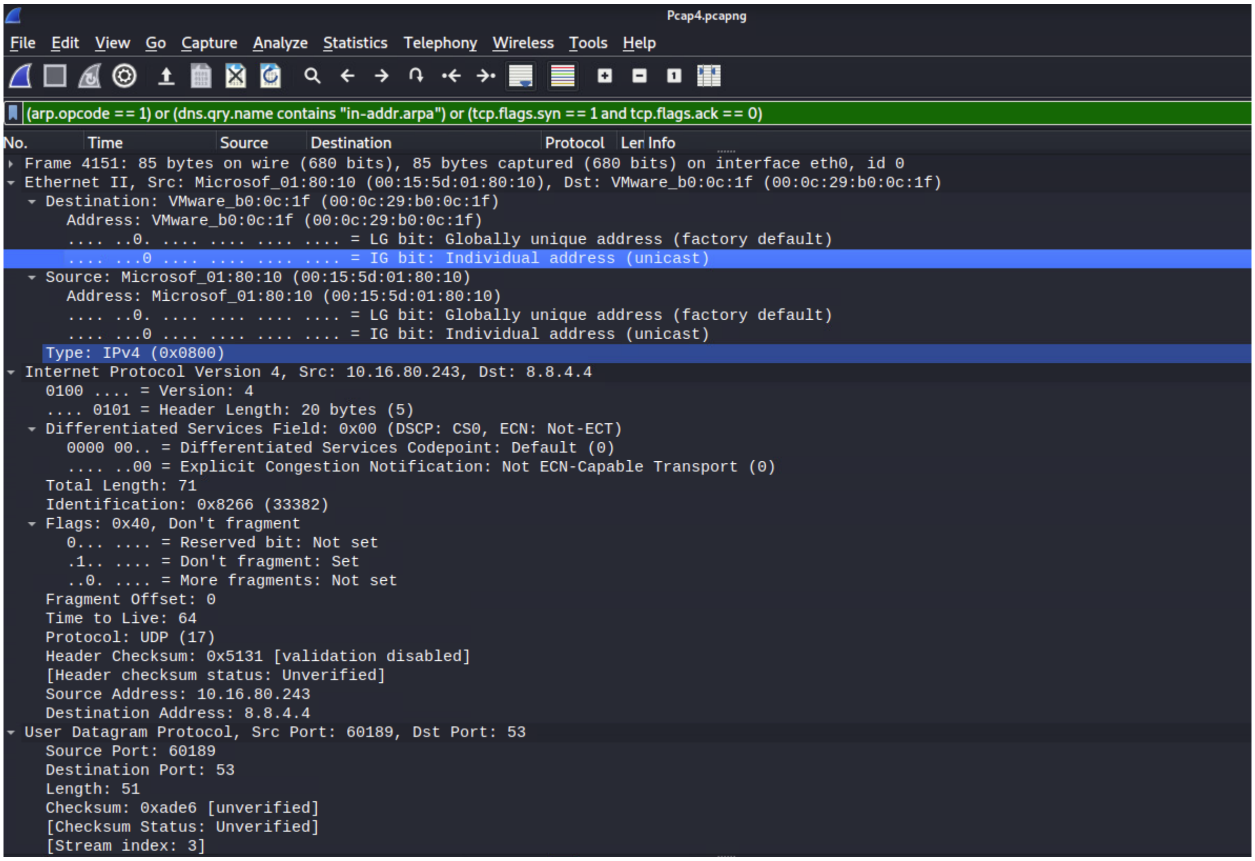
```
No.   Time          Source     Destination        Protocol Ler Info
    2 2.046862290   Microso…  Broadcast          ARP       60 Who has 10.168.27.10? Tell 10.16.80.243
    4 2.102397296   10.16.8…  8.8.4.4            DNS       85 Standard query 0xddf4 PTR 10.27.168.10.in-addr.arpa
    5 2.110589053   8.8.4.4   10.16.80.243       DNS       85 Standard query response 0xddf4 No such name PTR 10.27.168.10.in-addr.arpa
 1751 6.755350540   Microso…  Microsof_01:80:10  ARP       60 Who has 10.16.80.243? Tell 10.168.27.10
 1975 7.330182456   Microso…  VMware_b0:0c:1f    ARP       60 Who has 10.0.0.1? Tell 10.16.80.243
 2085 9.663384760   Microso…  Broadcast          ARP       60 Who has 10.168.27.10? Tell 10.16.80.243
 2087 9.699019989   10.16.8…  8.8.4.4            DNS       85 Standard query 0x47ca PTR 10.27.168.10.in-addr.arpa
 2088 9.706692814   8.8.4.4   10.16.80.243       DNS       85 Standard query response 0x47ca No such name PTR 10.27.168.10.in-addr.arpa
 4149 17.851675798  Microso…  Broadcast          ARP       60 Who has 10.168.27.10? Tell 10.16.80.243
 4151 17.883516537  10.16.8…  8.8.4.4            DNS       85 Standard query 0xe226 PTR 10.27.168.10.in-addr.arpa
 4152 17.891632133  8.8.4.4   10.16.80.243       DNS       85 Standard query response 0xe226 No such name PTR 10.27.168.10.in-addr.arpa
```

```
▸ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▾ Ethernet II, Src: Microsof_01:80:10 (00:15:5d:01:80:10), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▾ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ▾ Source: Microsof_01:80:10 (00:15:5d:01:80:10)
      Address: Microsof_01:80:10 (00:15:5d:01:80:10)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Microsof_01:80:10 (00:15:5d:01:80:10)
    Sender IP address: 10.16.80.243
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.168.27.10
```



(arp.opcode == 1) or (dns.qry.name contains "in-addr.arpa") or (tcp.flags.syn == 1 and tcp.flags.ack == 0)

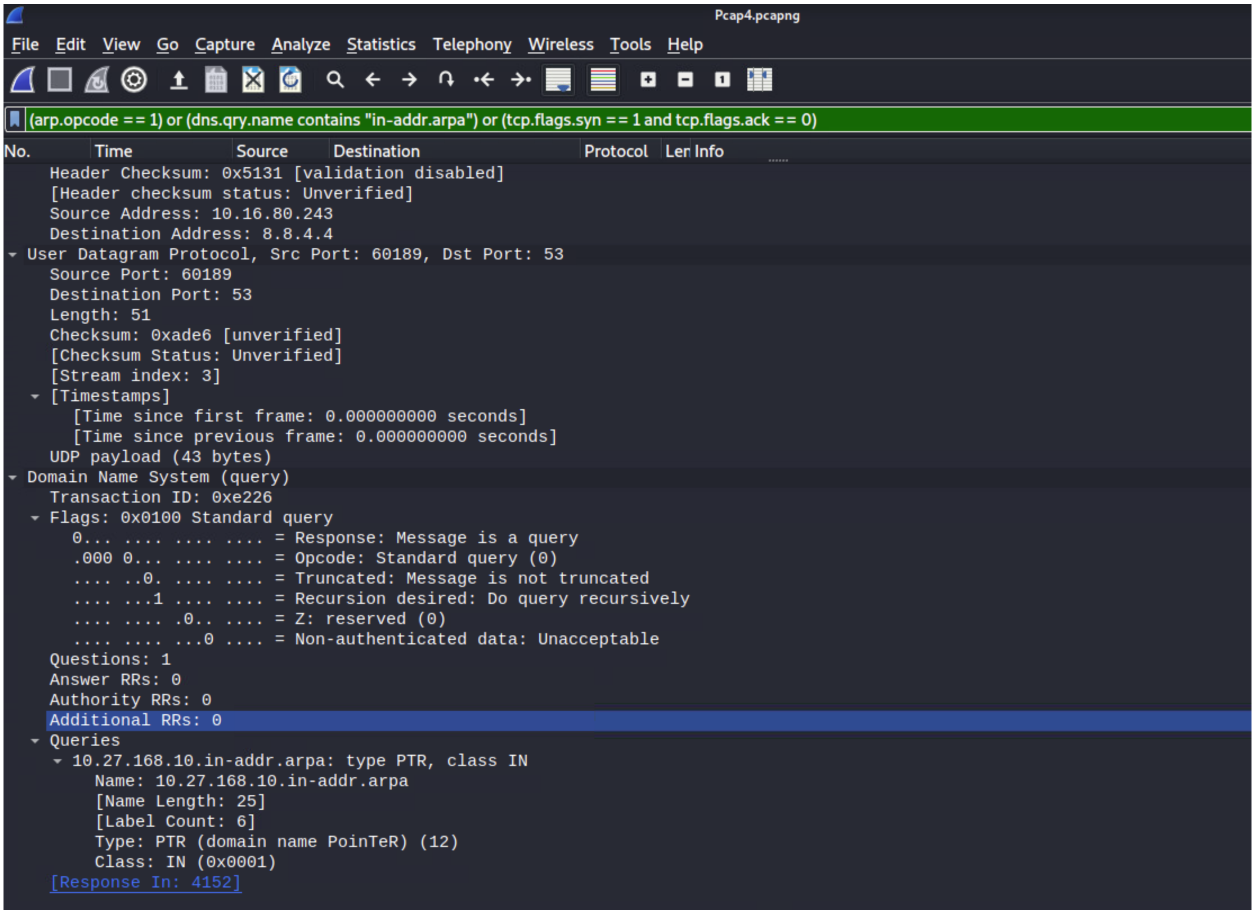
```
› Frame 4: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface eth0, id 0
▾ Ethernet II, Src: Microsof_01:80:10 (00:15:5d:01:80:10), Dst: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
  ▾ Destination: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
      Address: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: Microsof_01:80:10 (00:15:5d:01:80:10)
      Address: Microsof_01:80:10 (00:15:5d:01:80:10)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.16.80.243, Dst: 8.8.4.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 71
    Identification: 0x7a8c (31372)
  ▾ Flags: 0x40, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x590b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.16.80.243
    Destination Address: 8.8.4.4
▾ User Datagram Protocol, Src Port: 50328, Dst Port: 53
    Source Port: 50328
    Destination Port: 53
    Length: 51
    Checksum: 0xd89d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
```


Pcap4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
(arp.opcode == 1) or (dns.qry.name contains "in-addr.arpa") or (tcp.flags.syn == 1 and tcp.flags.ack == 0)
```

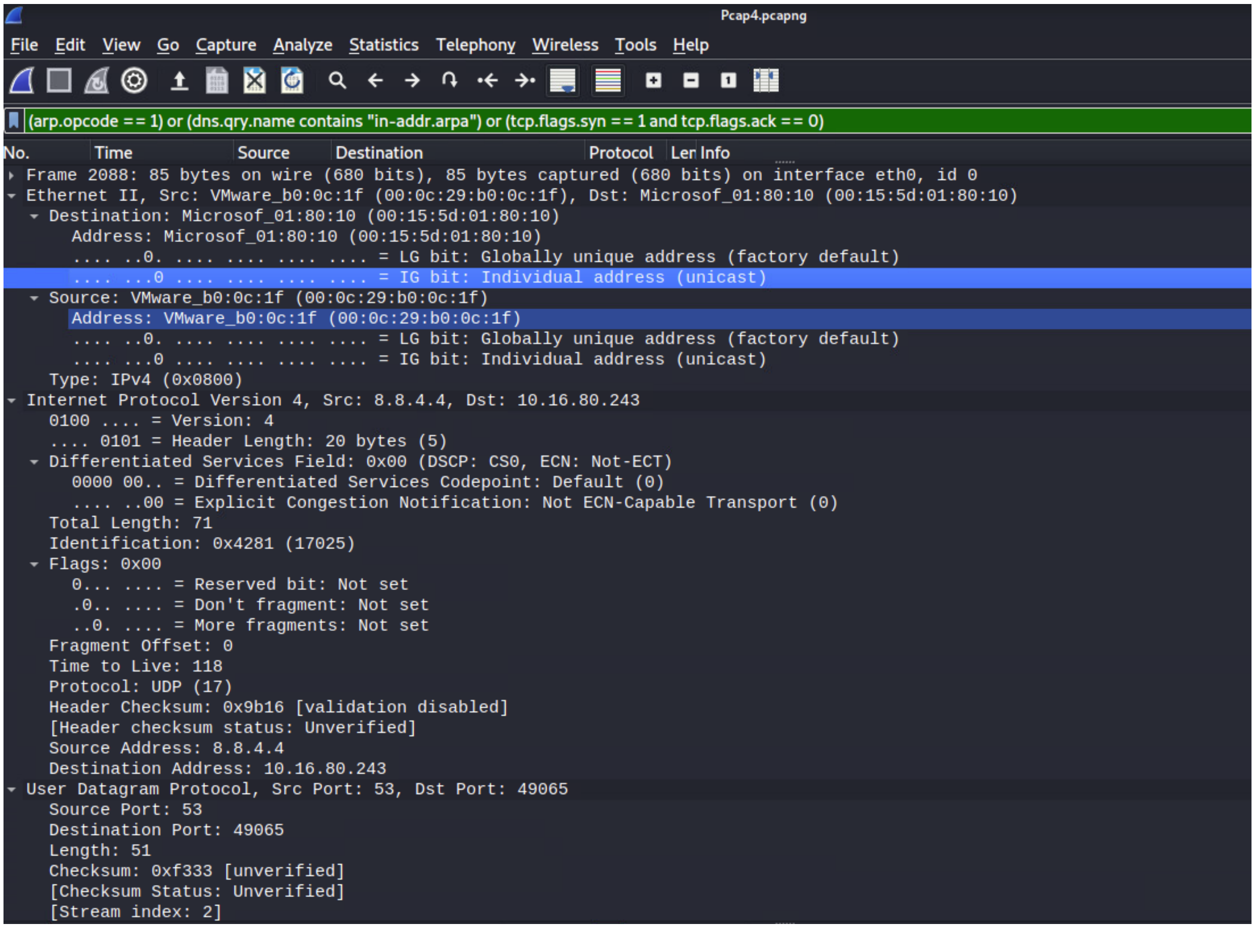
No. Time Source Destination Protocol Ler Info

```
▸ Frame 4151: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface eth0, id 0
▾ Ethernet II, Src: Microsof_01:80:10 (00:15:5d:01:80:10), Dst: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
  ▾ Destination: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
      Address: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: Microsof_01:80:10 (00:15:5d:01:80:10)
      Address: Microsof_01:80:10 (00:15:5d:01:80:10)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.16.80.243, Dst: 8.8.4.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 71
    Identification: 0x8266 (33382)
  ▾ Flags: 0x40, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x5131 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.16.80.243
    Destination Address: 8.8.4.4
▾ User Datagram Protocol, Src Port: 60189, Dst Port: 53
    Source Port: 60189
    Destination Port: 53
    Length: 51
    Checksum: 0xade6 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
```


Pcap4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Len Info

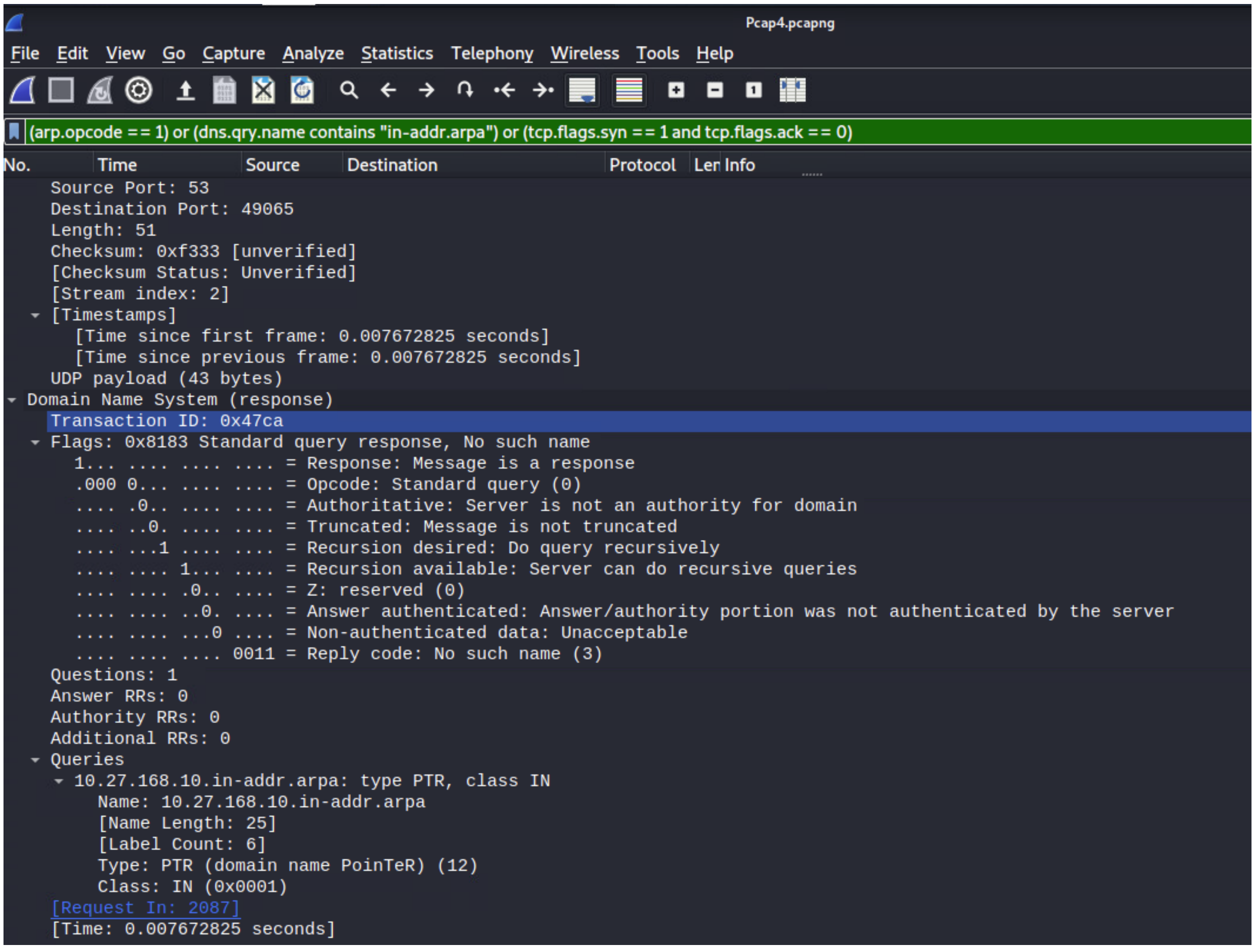
(arp.opcode == 1) or (dns.qry.name contains "in-addr.arpa") or (tcp.flags.syn == 1 and tcp.flags.ack == 0)

```
    Header Checksum: 0x5131 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.16.80.243
    Destination Address: 8.8.4.4
User Datagram Protocol, Src Port: 60189, Dst Port: 53
    Source Port: 60189
    Destination Port: 53
    Length: 51
    Checksum: 0xade6 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
    [Timestamps]
        [Time since first frame: 0.000000000 seconds]
        [Time since previous frame: 0.000000000 seconds]
    UDP payload (43 bytes)
Domain Name System (query)
    Transaction ID: 0xe226
    Flags: 0x0100 Standard query
        0... .... .... .... = Response: Message is a query
        .000 0... .... .... = Opcode: Standard query (0)
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        10.27.168.10.in-addr.arpa: type PTR, class IN
            Name: 10.27.168.10.in-addr.arpa
            [Name Length: 25]
            [Label Count: 6]
            Type: PTR (domain name PoinTeR) (12)
            Class: IN (0x0001)
    [Response In: 4152]
```


Pcap4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Ler Info

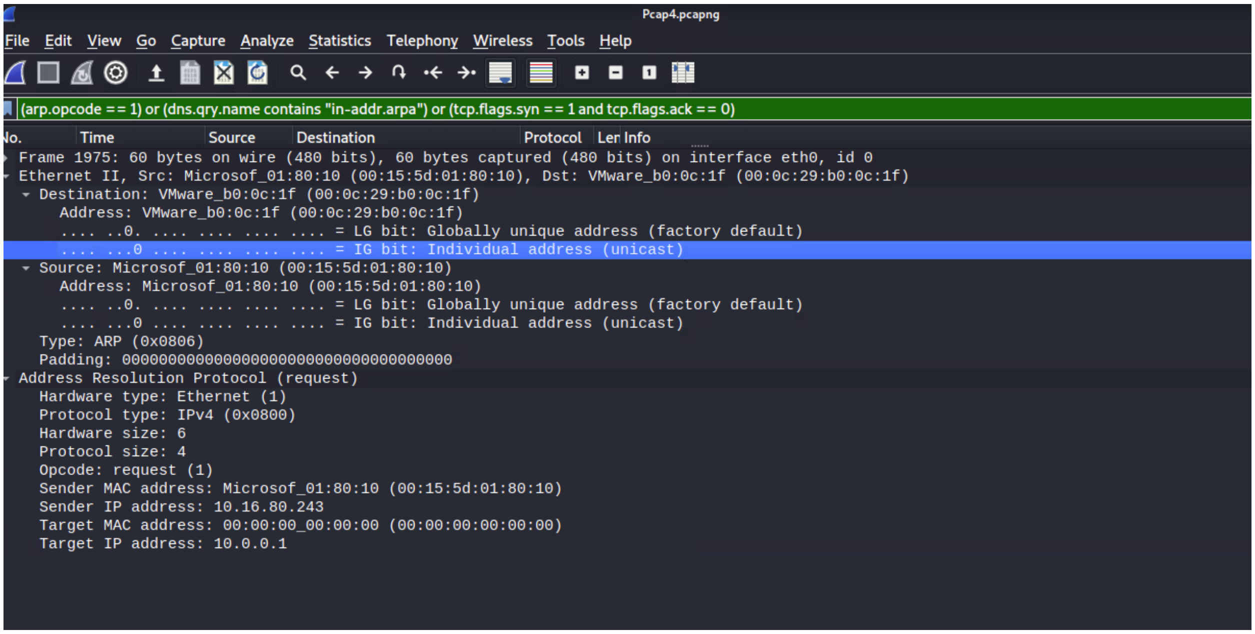
```
(arp.opcode == 1) or (dns.qry.name contains "in-addr.arpa") or (tcp.flags.syn == 1 and tcp.flags.ack == 0)
```

```
› Frame 2088: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface eth0, id 0
▾ Ethernet II, Src: VMware_b0:0c:1f (00:0c:29:b0:0c:1f), Dst: Microsof_01:80:10 (00:15:5d:01:80:10)
  ▾ Destination: Microsof_01:80:10 (00:15:5d:01:80:10)
      Address: Microsof_01:80:10 (00:15:5d:01:80:10)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
      Address: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 8.8.4.4, Dst: 10.16.80.243
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 71
    Identification: 0x4281 (17025)
  ▾ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 118
    Protocol: UDP (17)
    Header Checksum: 0x9b16 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 8.8.4.4
    Destination Address: 10.16.80.243
▾ User Datagram Protocol, Src Port: 53, Dst Port: 49065
    Source Port: 53
    Destination Port: 49065
    Length: 51
    Checksum: 0xf333 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
```


Pcap4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Len Info

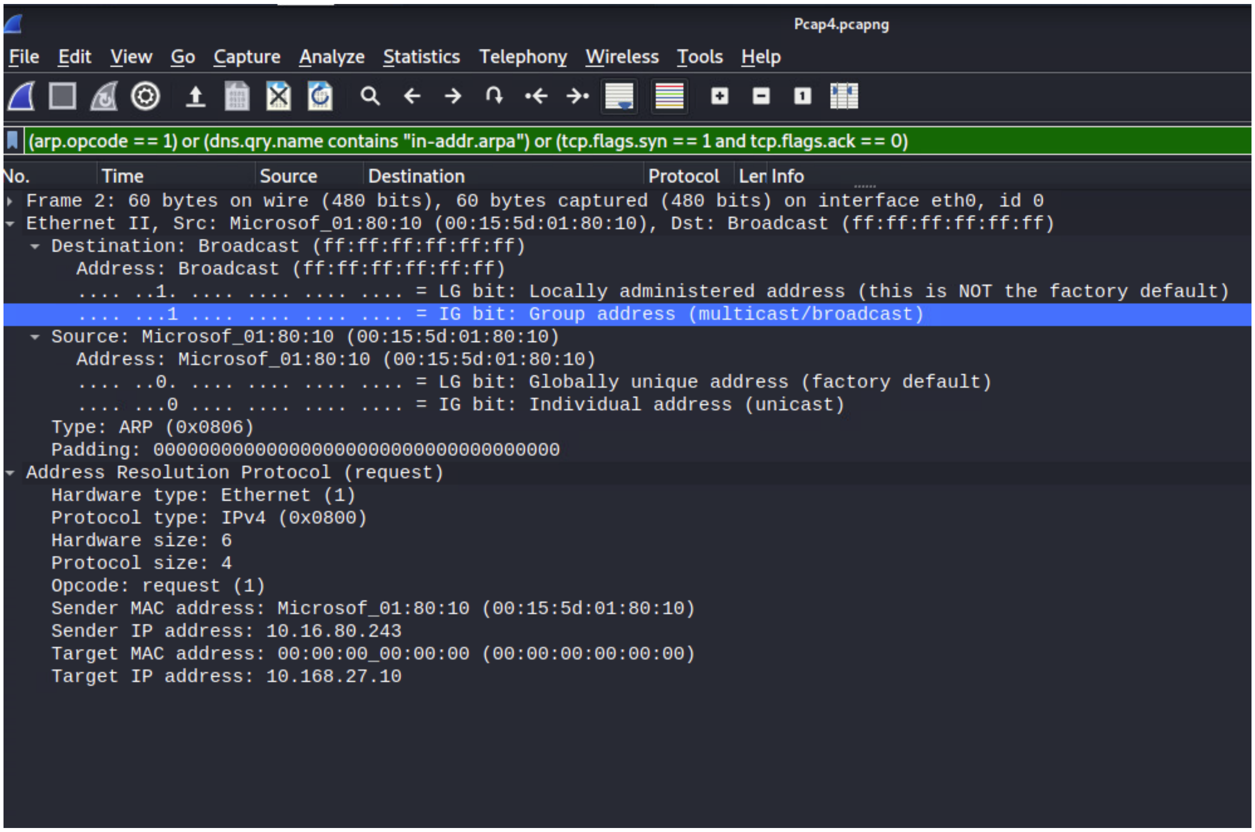
```
(arp.opcode == 1) or (dns.qry.name contains "in-addr.arpa") or (tcp.flags.syn == 1 and tcp.flags.ack == 0)
```

```
    Source Port: 53
    Destination Port: 49065
    Length: 51
    Checksum: 0xf333 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  ▾ [Timestamps]
      [Time since first frame: 0.007672825 seconds]
      [Time since previous frame: 0.007672825 seconds]
    UDP payload (43 bytes)
▾ Domain Name System (response)
    Transaction ID: 0x47ca
  ▾ Flags: 0x8183 Standard query response, No such name
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0011 = Reply code: No such name (3)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ 10.27.168.10.in-addr.arpa: type PTR, class IN
        Name: 10.27.168.10.in-addr.arpa
        [Name Length: 25]
        [Label Count: 6]
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
    [Request In: 2087]
    [Time: 0.007672825 seconds]
```


Pcap4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Len Info

```
(arp.opcode == 1) or (dns.qry.name contains "in-addr.arpa") or (tcp.flags.syn == 1 and tcp.flags.ack == 0)
```

```
▸ Frame 1975: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▾ Ethernet II, Src: Microsof_01:80:10 (00:15:5d:01:80:10), Dst: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
  ▾ Destination: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
      Address: VMware_b0:0c:1f (00:0c:29:b0:0c:1f)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: Microsof_01:80:10 (00:15:5d:01:80:10)
      Address: Microsof_01:80:10 (00:15:5d:01:80:10)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Microsof_01:80:10 (00:15:5d:01:80:10)
    Sender IP address: 10.16.80.243
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.0.0.1
```


Pcap4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Len Info

```
(arp.opcode == 1) or (dns.qry.name contains "in-addr.arpa") or (tcp.flags.syn == 1 and tcp.flags.ack == 0)
```

```
Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_01:80:10 (00:15:5d:01:80:10), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
    .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
    .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  Source: Microsof_01:80:10 (00:15:5d:01:80:10)
    Address: Microsof_01:80:10 (00:15:5d:01:80:10)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  Padding: 000000000000000000000000000000000000
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Microsof_01:80:10 (00:15:5d:01:80:10)
  Sender IP address: 10.16.80.243
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 10.168.27.10
```