THM_Wireshark 101 [Task 10 DNS]

The most important lesson I learned from the room is that if DNS is a TPC packet, one must be concerned.

dns+icmp.pcapng 8 kB

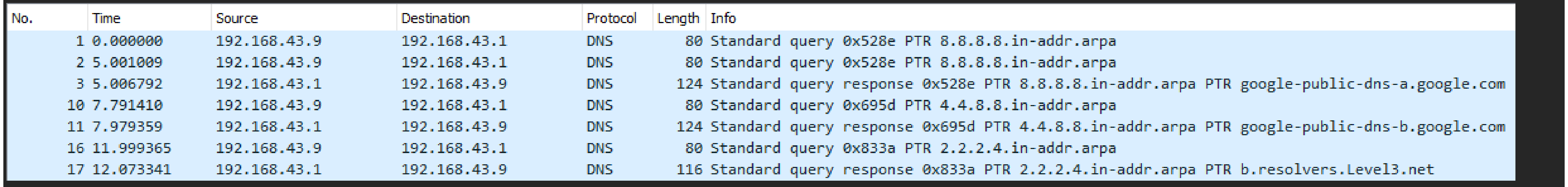
DNS or Domain Name Service protocol is used to resolves names with IP addresses. Just like the other protocols, you should be familiar with DNS; however, if you're not you can refresh with the IETF DNS Documentation.

There are a couple of things outlined below that you should keep in the back of your mind when analyzing DNS packets.

- Query-Response
- DNS-Servers Only
- UDP

If anyone of these is out of place then the packets should be looked at further and should be considered suspicious.

Below we can see a packet capture with multiple DNS queries and responses.



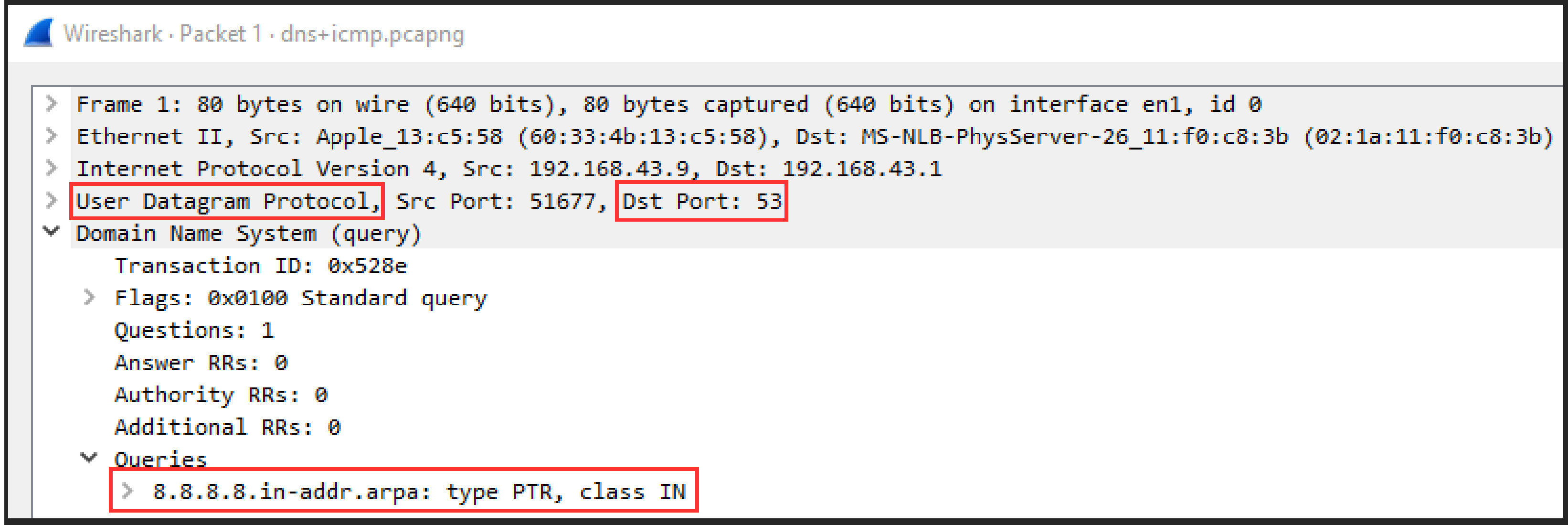
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x528e PTR 8.8.8.8.in-addr.arpa
2	5.001009	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x528e PTR 8.8.8.8.in-addr.arpa
3	5.006792	192.168.43.1	192.168.43.9	DNS	124	Standard query response 0x528e PTR 8.8.8.8.in-addr.arpa PTR google-public-dns-a.google.com
10	7.791410	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x695d PTR 4.4.8.8.in-addr.arpa
11	7.979359	192.168.43.1	192.168.43.9	DNS	124	Standard query response 0x695d PTR 4.4.8.8.in-addr.arpa PTR google-public-dns-b.google.com
16	11.999365	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x833a PTR 2.2.2.4.in-addr.arpa
17	12.073341	192.168.43.1	192.168.43.9	DNS	116	Standard query response 0x833a PTR 2.2.2.4.in-addr.arpa PTR b.resolvers.Level3.net

Instantly looking at the packets we can see what they are querying, this can be useful when you have many packets and need to identify suspicious or unusual traffic quickly.

DNS Traffic Overview

DNS Query:

Looking at the below query we really have two bits of information that we can use to analyze the packet. The first bit of information we can look at is where the query is originating from, in this case, it is UDP53 which means that this packet passes that check, **if it was TCP 53 then it should be considered suspicious traffic and needs to analyzed further.** We can also look at what it is querying as well, this can be useful with other information to build a story of what happened.



Wireshark · Packet 1 · dns+icmp.pcapng

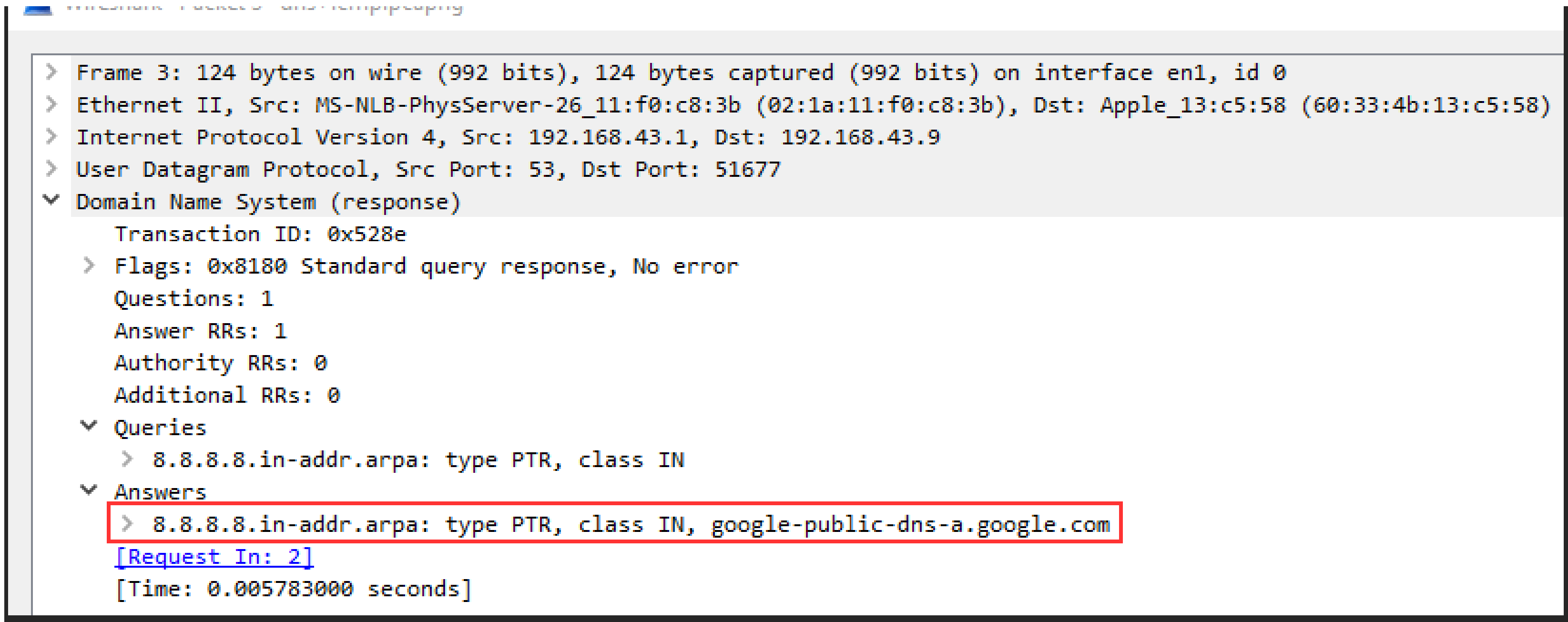
```
> Frame 1: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface en1, id 0
> Ethernet II, Src: Apple_13:c5:58 (60:33:4b:13:c5:58), Dst: MS-NLB-PhysServer-26_11:f0:c8:3b (02:1a:11:f0:c8:3b)
> Internet Protocol Version 4, Src: 192.168.43.9, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 51677, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x528e
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > 8.8.8.8.in-addr.arpa: type PTR, class IN
```

When analyzing DNS packets you really need to understand your environment and whether or not the traffic would be considered normal within your environment.

DNS Response:

Below we see a response packet, it is similar to the query packet, but it includes an answer as well which can be used to verify the query.

Wireshark · Packet 3 · dns+icmp.pcapng



```
> Frame 3: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface en1, id 0
> Ethernet II, Src: MS-NLB-PhysServer-26_11:f0:c8:3b (02:1a:11:f0:c8:3b), Dst: Apple_13:c5:58 (60:33:4b:13:c5:58)
> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.9
> User Datagram Protocol, Src Port: 53, Dst Port: 51677
v Domain Name System (response)
    Transaction ID: 0x528e
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > 8.8.8.8.in-addr.arpa: type PTR, class IN
  v Answers
    > 8.8.8.8.in-addr.arpa: type PTR, class IN, google-public-dns-a.google.com
    [Request In: 2]
    [Time: 0.005783000 seconds]
```

Practical DNS Packet Analysis

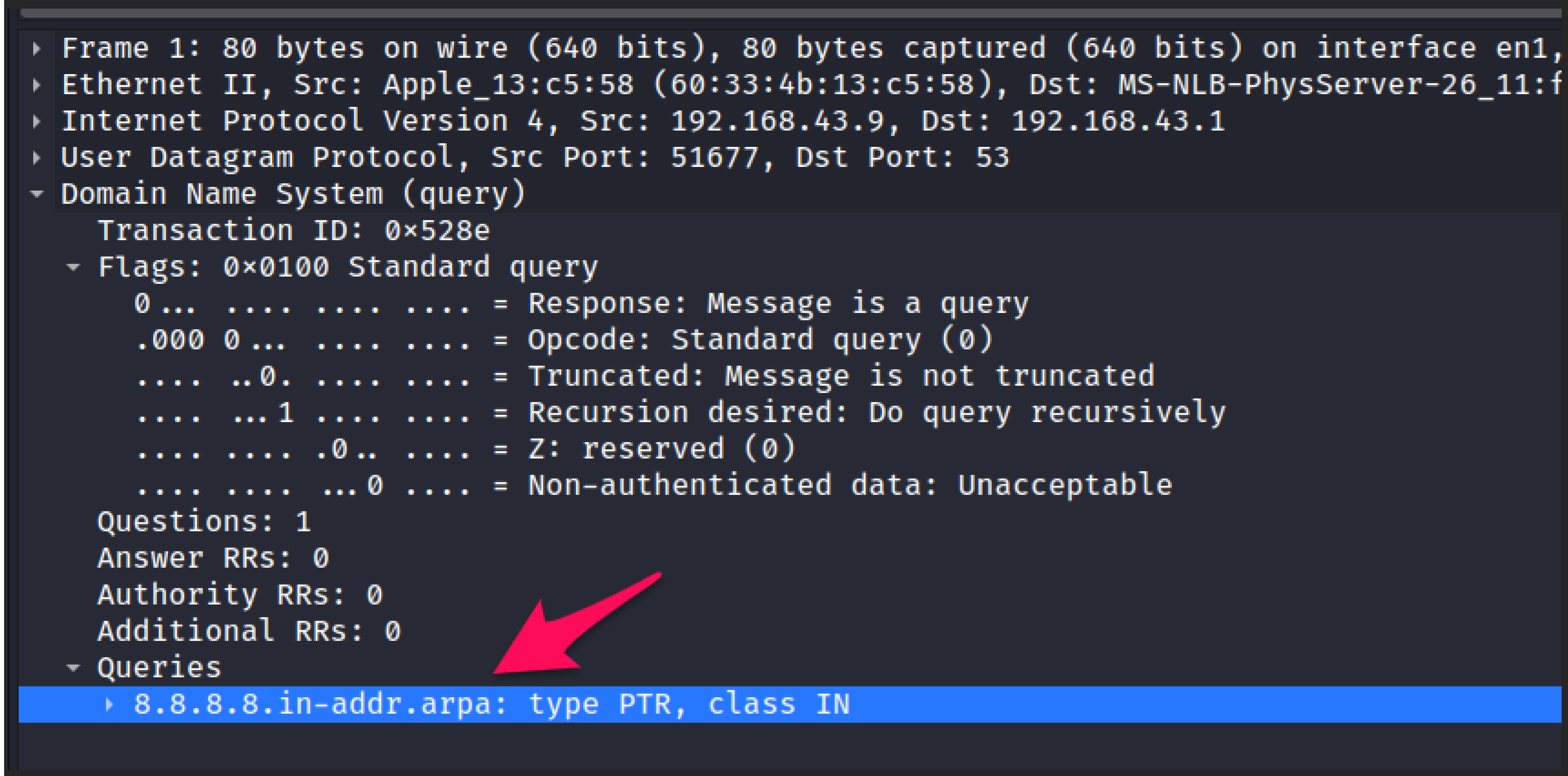
Now that we understand the basics of how DNS traffic looks and interacts. Go to the folder /root/Rooms/Wireshark101 on the AttackBox and double click the task10.pcap file to open it in Wireshark; you can also download the pcap on this task.

This capture only has two protocols so it is up to you whether or not you decide to filter the ICMP protocol or not.

Answer the questions below

What is being queried in packet 1?

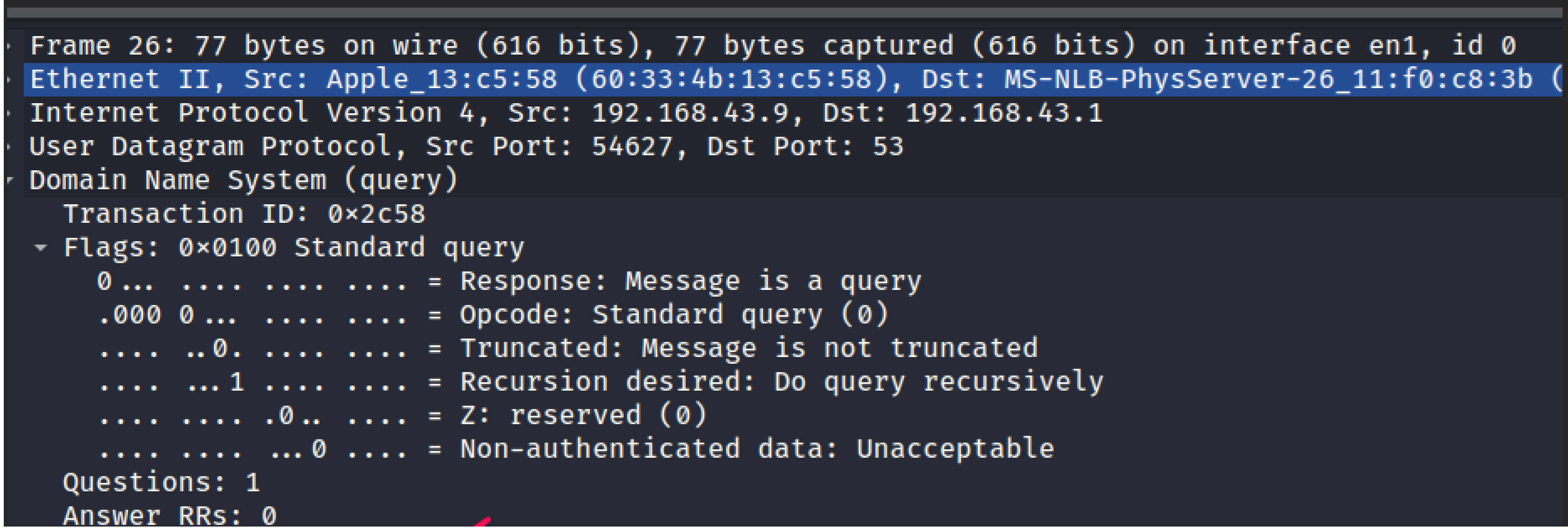
8.8.8.8.in-addr.arpa~~: type PTR, class IN~~



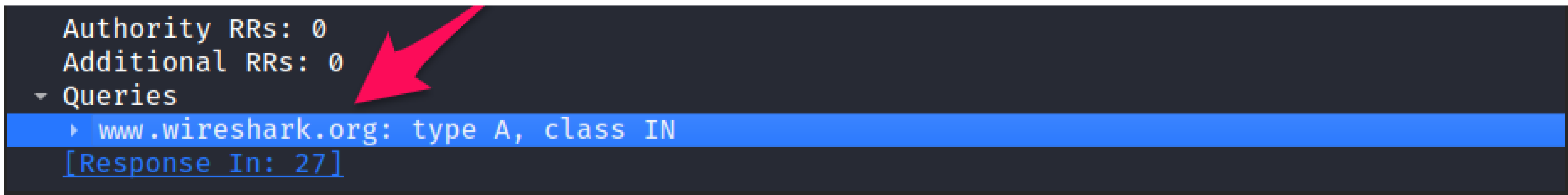
```
> Frame 1: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface en1,
> Ethernet II, Src: Apple_13:c5:58 (60:33:4b:13:c5:58), Dst: MS-NLB-PhysServer-26_11:f
> Internet Protocol Version 4, Src: 192.168.43.9, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 51677, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x528e
  v 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
  v Queries
    > 8.8.8.8.in-addr.arpa: type PTR, class IN
```

What site is being queried in packet 26?

www.wireshark.org



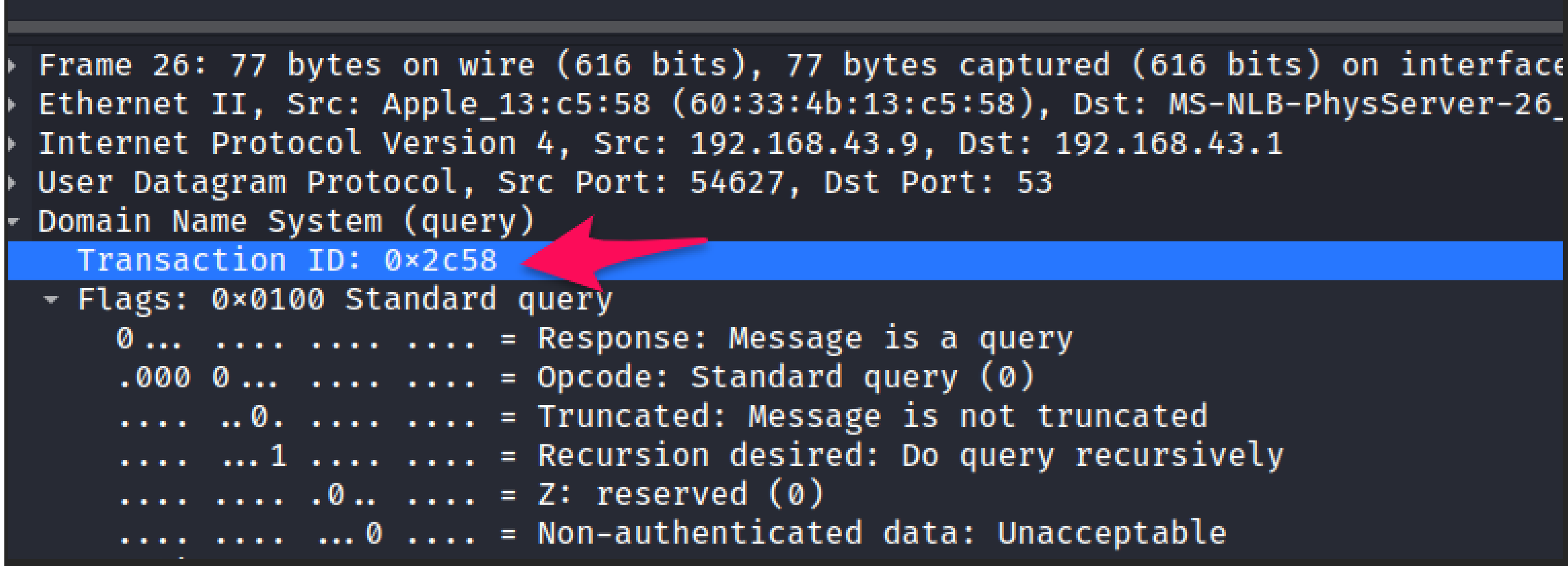
```
> Frame 26: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface en1, id 0
> Ethernet II, Src: Apple_13:c5:58 (60:33:4b:13:c5:58), Dst: MS-NLB-PhysServer-26_11:f0:c8:3b (
> Internet Protocol Version 4, Src: 192.168.43.9, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 54627, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x2c58
  v 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
    ▸ www.wireshark.org: type A, class IN
    [Response In: 27]
```

What is the Transaction ID for packet 26?

0x2c58



```
▸ Frame 26: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface
▸ Ethernet II, Src: Apple_13:c5:58 (60:33:4b:13:c5:58), Dst: MS-NLB-PhysServer-26_
▸ Internet Protocol Version 4, Src: 192.168.43.9, Dst: 192.168.43.1
▸ User Datagram Protocol, Src Port: 54627, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0×2c58
  ▾ Flags: 0×0100 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
```