CENG 435 - Data Communications and Networking 2023-1
Wireshark Assignment 4

Anıl Eren Göçer
e2448397@ceng.metu.edu.tr

November 29, 2023

1.a)

udp

No.	Time	Source	Destination	Protocol	Length	Info
28	2.115091	172.20.10.2	172.20.10.1	DNS	84	Standard query 0x0001 PTR 1.10.20.172.in-addr.arpa
29	2.168683	172.20.10.1	172.20.10.2	DNS	138	Standard query response 0x0001 No such name PTR 1.10.20.172.in-addr.arpa SOA 20.172.IN-ADDR.ARPA
30	2.170690	172.20.10.2	172.20.10.1	DNS	77	Standard query 0x0002 A stackoverflow.com
31	2.176088	172.20.10.1	172.20.10.2	DNS	109	Standard query response 0x0002 A stackoverflow.com A 172.64.155.249 A 104.18.32.7
32	2.179688	172.20.10.2	172.20.10.1	DNS	77	Standard query 0x0003 AAAA stackoverflow.com
33	2.230585	172.20.10.1	172.20.10.2	DNS	138	Standard query response 0x0003 AAAA stackoverflow.com SOA damian.ns.cloudflare.com
34	2.418985	172.20.10.1	224.0.0.251	MDNS	130	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question OPT
35	2.419582	fe80::f3:9fff:fe38:…	ff02::fb	MDNS	150	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question OPT
36	4.391948	fe80::bbdd:b7fb:403…	ff02::1:2	DHCPv6	157	Solicit XID: 0xd1f425 CID: 0001000128acf4eab025aa2ea5bc
37	4.562014	172.20.10.1	172.20.10.2	DNS	77	Standard query response 0xc20d Server failure HTTPS stackoverflow.com
38	4.566846	172.20.10.1	172.20.10.2	DNS	79	Standard query response 0x4144 Server failure HTTPS ajax.googleapis.com
39	4.566846	172.20.10.1	172.20.10.2	DNS	89	Standard query response 0x3835 Server failure HTTPS clientservices.googleapis.com
40	4.649454	172.20.10.1	172.20.10.2	DNS	75	Standard query response 0x1ba1 Server failure HTTPS cdn.sstatic.net
41	5.173903	172.20.10.1	172.20.10.2	DNS	76	Standard query response 0x9a16 Server failure HTTPS www.gravatar.com
42	5.173903	172.20.10.1	172.20.10.2	DNS	85	Standard query response 0x8cfe Server failure HTTPS lh3.googleusercontent.com
43	5.173903	172.20.10.1	172.20.10.2	DNS	77	Standard query response 0x8bb4 Server failure HTTPS i.stack.imgur.com
44	5.173903	172.20.10.1	172.20.10.2	DNS	85	Standard query response 0xcd56 Server failure HTTPS lh6.googleusercontent.com
45	5.190911	172.20.10.1	172.20.10.2	DNS	85	Standard query response 0x87d7 Server failure HTTPS lh4.googleusercontent.com
46	5.192072	172.20.10.1	172.20.10.2	DNS	85	Standard query response 0x70d7 Server failure HTTPS lh5.googleusercontent.com
47	5.193069	172.20.10.1	172.20.10.2	DNS	78	Standard query response 0xf94a Server failure HTTPS graph.facebook.com
48	5.626428	172.20.10.1	172.20.10.2	DNS	77	Standard query response 0x5226 Server failure HTTPS i.stack.imgur.com
49	5.628111	172.20.10.1	172.20.10.2	DNS	77	Standard query response 0xd8f6 Server failure HTTPS i.stack.imgur.com

Figure 1: Packet number of the first UDP segment

1.b)

udp

No.	Time	Source	Destination	Protocol	Length	Info
28	2.115091	172.20.10.2	172.20.10.1	DNS	84	Standard query 0x0001 PTR 1.10.20.172.in-addr.arpa
29	2.168683	172.20.10.1	172.20.10.2	DNS	138	Standard query response 0x0001 No such name PTR 1.10.20.172.in-addr.arpa SOA 20.172.IN-ADDR.ARPA
30	2.170690	172.20.10.2	172.20.10.1	DNS	77	Standard query 0x0002 A stackoverflow.com
31	2.176088	172.20.10.1	172.20.10.2	DNS	109	Standard query response 0x0002 A stackoverflow.com A 172.64.155.249 A 104.18.32.7
32	2.179688	172.20.10.2	172.20.10.1	DNS	77	Standard query 0x0003 AAAA stackoverflow.com
33	2.230585	172.20.10.1	172.20.10.2	DNS	138	Standard query response 0x0003 AAAA stackoverflow.com SOA damian.ns.cloudflare.com
34	2.418985	172.20.10.1	224.0.0.251	MDNS	130	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question OPT
35	2.419582	fe80::f3:9fff:fe38:…	ff02::fb	MDNS	150	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question OPT
36	4.391948	fe80::bbdd:b7fb:403…	ff02::1:2	DHCPv6	157	Solicit XID: 0xd1f425 CID: 0001000128acf4eab025aa2ea5bc
37	4.562014	172.20.10.1	172.20.10.2	DNS	77	Standard query response 0xc20d Server failure HTTPS stackoverflow.com
38	4.566846	172.20.10.1	172.20.10.2	DNS	79	Standard query response 0x4144 Server failure HTTPS ajax.googleapis.com
39	4.566846	172.20.10.1	172.20.10.2	DNS	89	Standard query response 0x3835 Server failure HTTPS clientservices.googleapis.com
40	4.649454	172.20.10.1	172.20.10.2	DNS	75	Standard query response 0x1ba1 Server failure HTTPS cdn.sstatic.net
41	5.173903	172.20.10.1	172.20.10.2	DNS	76	Standard query response 0x9a16 Server failure HTTPS www.gravatar.com
42	5.173903	172.20.10.1	172.20.10.2	DNS	85	Standard query response 0x8cfe Server failure HTTPS lh3.googleusercontent.com
43	5.173903	172.20.10.1	172.20.10.2	DNS	77	Standard query response 0x8bb4 Server failure HTTPS i.stack.imgur.com
44	5.173903	172.20.10.1	172.20.10.2	DNS	85	Standard query response 0xcd56 Server failure HTTPS lh6.googleusercontent.com
45	5.190911	172.20.10.1	172.20.10.2	DNS	85	Standard query response 0x87d7 Server failure HTTPS lh4.googleusercontent.com
46	5.192072	172.20.10.1	172.20.10.2	DNS	85	Standard query response 0x70d7 Server failure HTTPS lh5.googleusercontent.com
47	5.193069	172.20.10.1	172.20.10.2	DNS	78	Standard query response 0xf94a Server failure HTTPS graph.facebook.com
48	5.626428	172.20.10.1	172.20.10.2	DNS	77	Standard query response 0x5226 Server failure HTTPS i.stack.imgur.com
49	5.628111	172.20.10.1	172.20.10.2	DNS	77	Standard query response 0xd8f6 Server failure HTTPS i.stack.imgur.com

Figure 2: Type of application-layer payload or protocol message

Wireshark · Packet 28 · wsa4.pcap

```
> Frame 28: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 172.20.10.1
> User Datagram Protocol, Src Port: 59774, Dst Port: 53
> Domain Name System (query)
```

Figure 3: Type of application-layer payload or protocol message

1.c) (together with 1.d)

1.d)

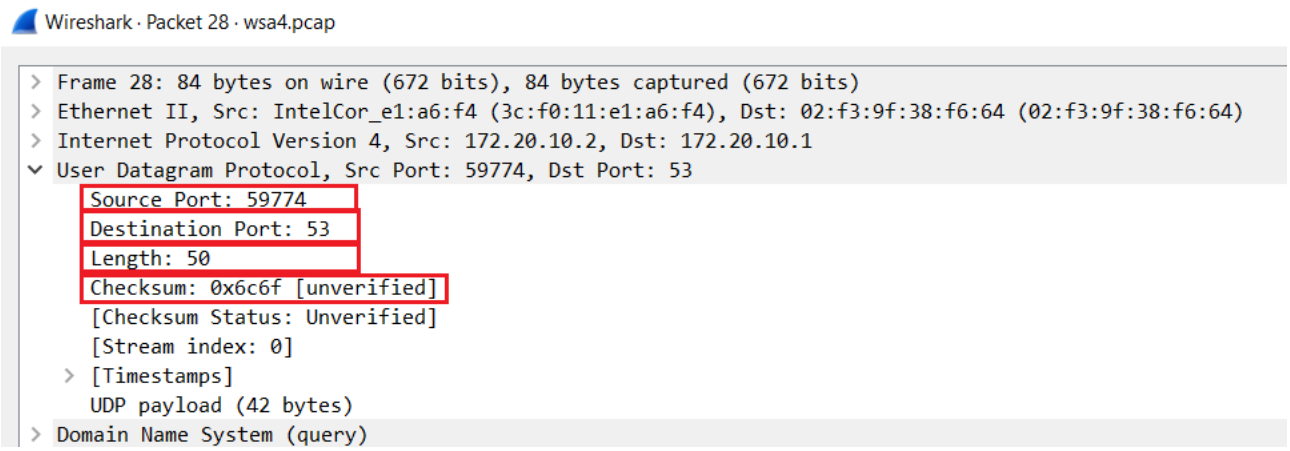


Figure 4: UDP Header

2)

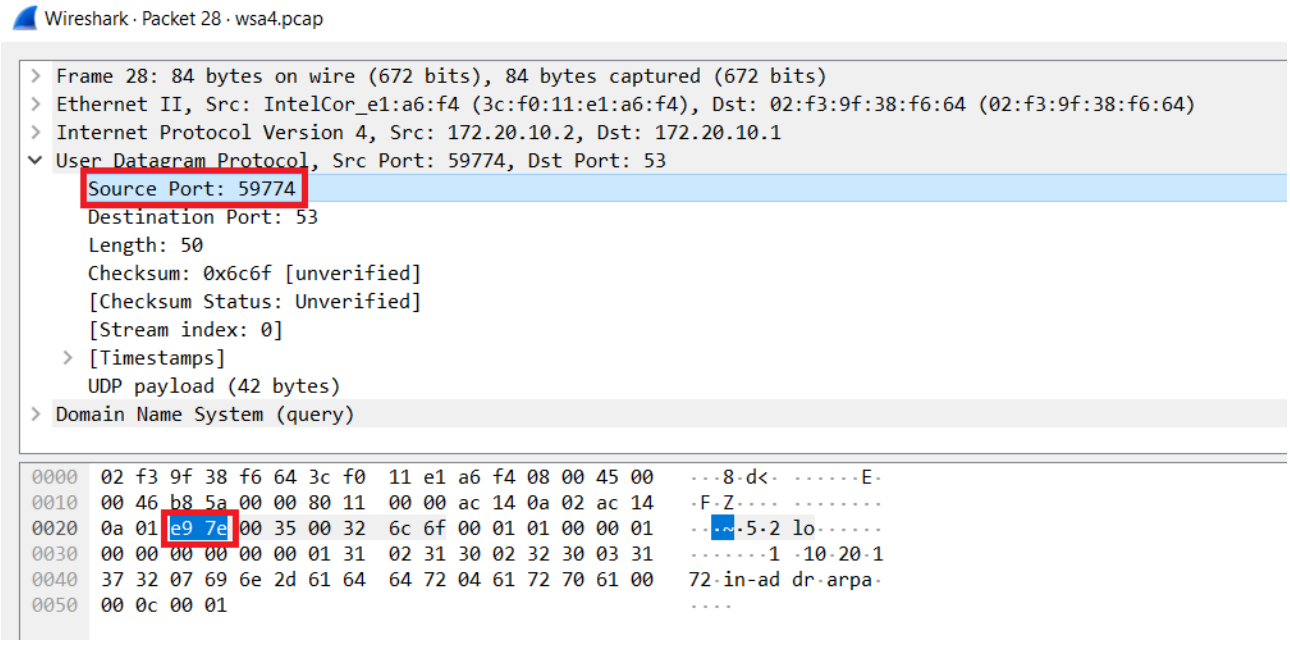


Figure 5: Number of bytes of Source Port field

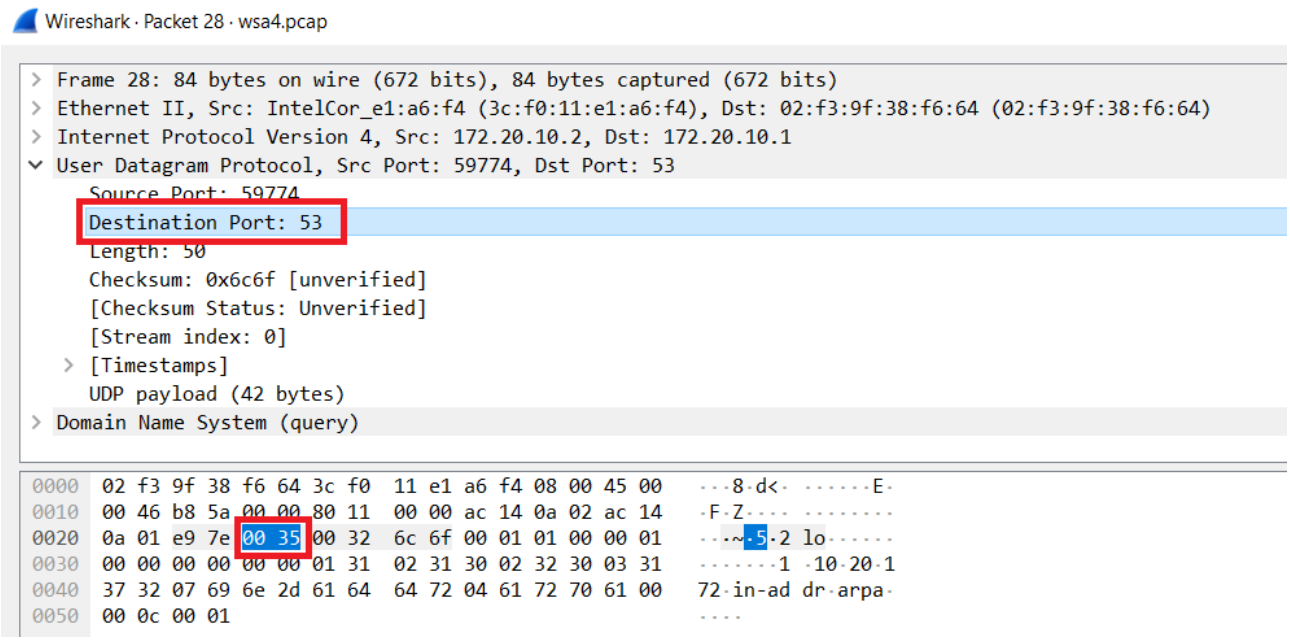


Figure 6: Number of bytes of Destination Port field

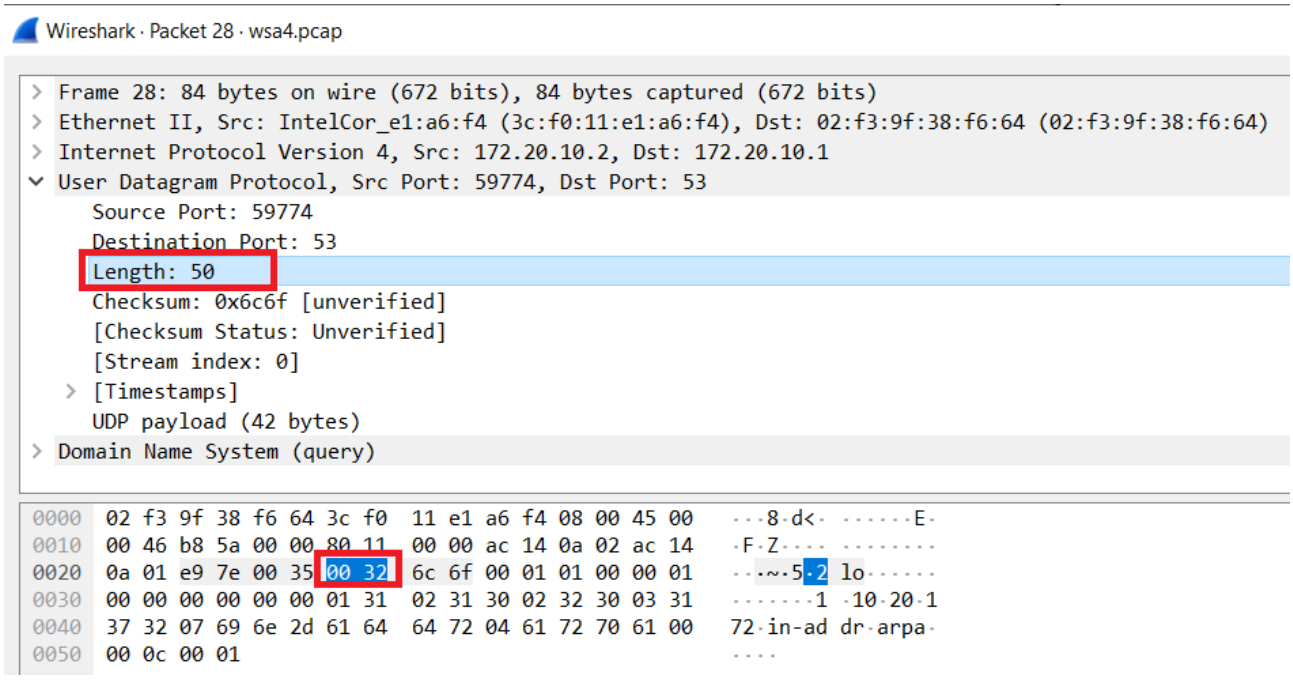


Figure 7: Number of bytes of Length field

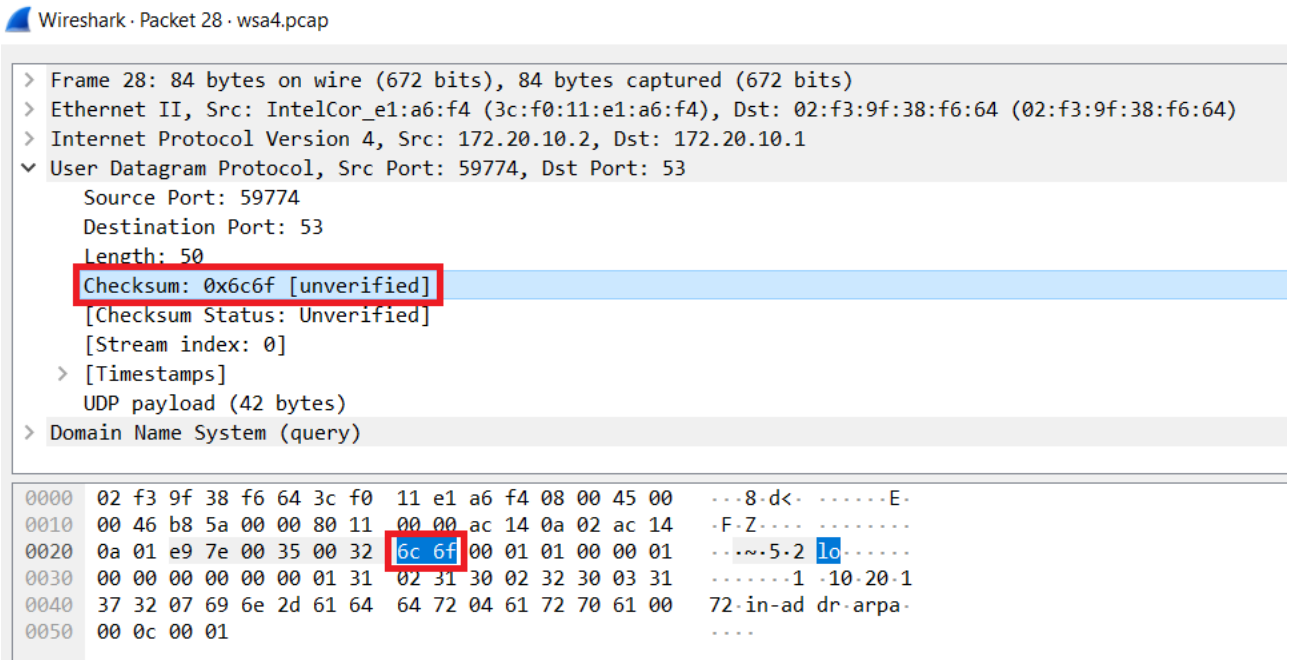


Figure 8: Number of bytes of Checksum field

3.) Length field is 2 bytes (16 bits). Therefore, maximum length is 2^{16} - 1 = 65535. And 655535 = payload + header. Since there are 4 header fiels of size of 2 bytes, header size is 8 bytes. As a result, maximum payload size is 65535 - 8 = 65527 bytes.

4.)

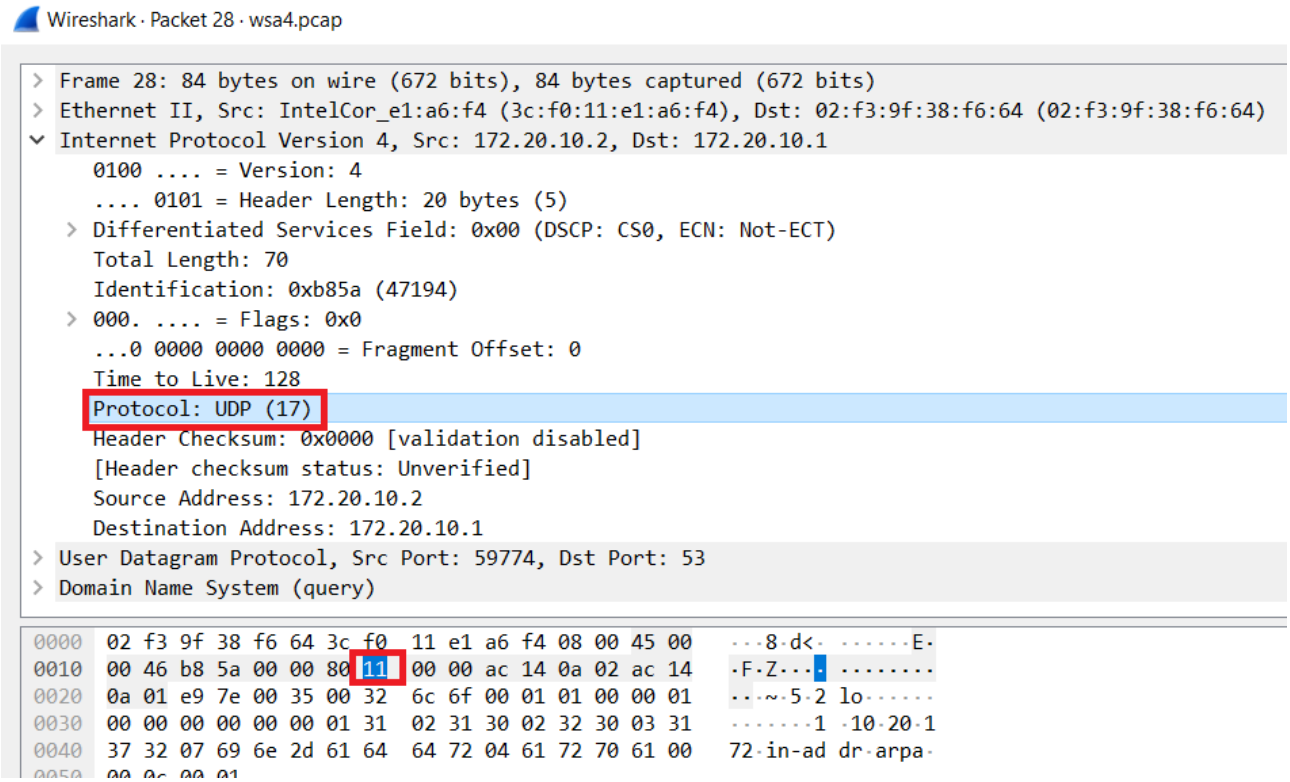
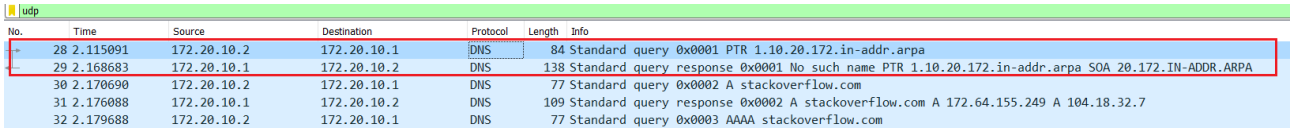


Figure 9: Protocol number for UDP

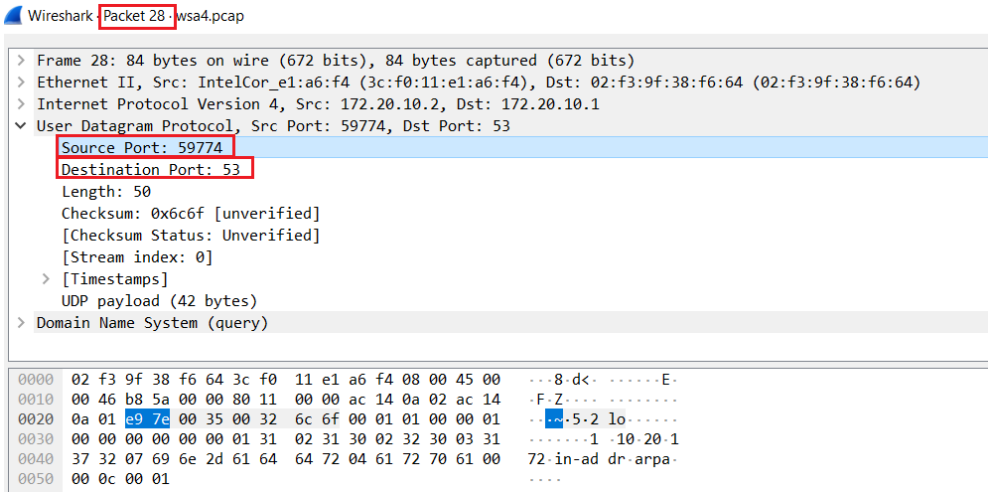
5.) **Relationship between the port numbers in the two packets**

The source port of the first packet is equal to destination port of the second packet. And the destination port of the first packet is equal to source port of the second packet.



No.	Time	Source	Destination	Protocol	Length	Info
28	2.115091	172.20.10.2	172.20.10.1	DNS	84	Standard query 0x0001 PTR 1.10.20.172.in-addr.arpa
29	2.168683	172.20.10.1	172.20.10.2	DNS	138	Standard query response 0x0001 No such name PTR 1.10.20.172.in-addr.arpa SOA 20.172.IN-ADDR.ARPA
30	2.170690	172.20.10.2	172.20.10.1	DNS	77	Standard query 0x0002 A stackoverflow.com
31	2.176088	172.20.10.1	172.20.10.2	DNS	109	Standard query response 0x0002 A stackoverflow.com A 172.64.155.249 A 104.18.32.7
32	2.179688	172.20.10.2	172.20.10.1	DNS	77	Standard query 0x0003 AAAA stackoverflow.com

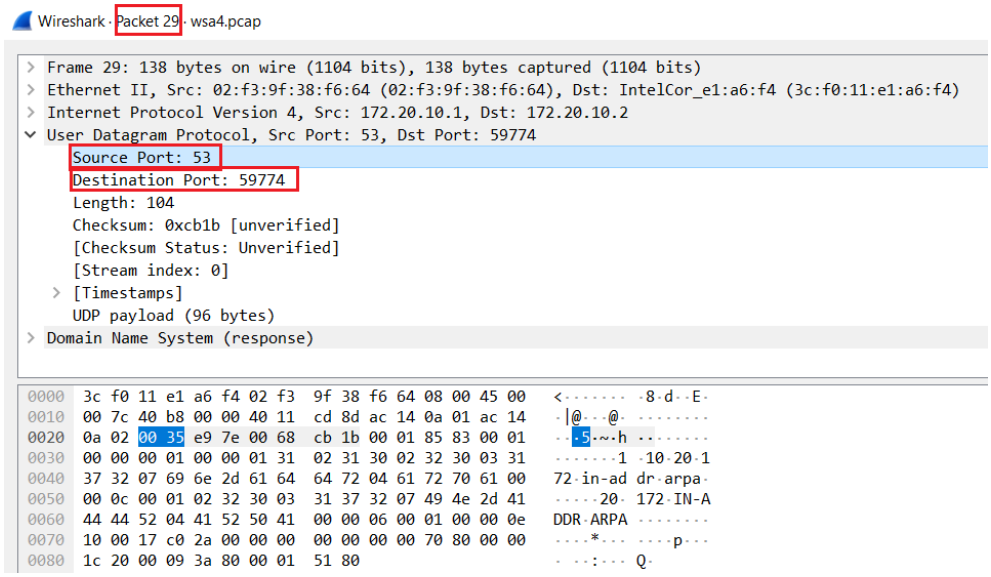
Figure 10: Packet numbers of these packets



```
Wireshark · Packet 28 · wsa4.pcap
> Frame 28: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 172.20.10.1
v User Datagram Protocol, Src Port: 59774, Dst Port: 53
    Source Port: 59774
    Destination Port: 53
    Length: 50
    Checksum: 0x6c6f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (42 bytes)
> Domain Name System (query)

0000  02 f3 9f 38 f6 64 3c f0  11 e1 a6 f4 08 00 45 00   ···8·d<· ------E·
0010  00 46 b8 5a 00 00 80 11  00 00 ac 14 0a 02 ac 14   ·F·Z···· ........
0020  0a 01 e9 7e 00 35 00 32  6c 6f 00 01 01 00 00 01   ···~·5·2 lo......
0030  00 00 00 00 00 00 01 31  02 31 30 02 32 30 03 31   -------1 ·10·20·1
0040  37 32 07 69 6e 2d 61 64  64 72 04 61 72 70 61 00   72·in-ad dr·arpa·
0050  00 0c 00 01                                         ····
```

Figure 11: Port numbers of the first packet



```
Wireshark · Packet 29 · wsa4.pcap
> Frame 29: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
> Ethernet II, Src: 02:f3:9f:38:f6:64 (02:f3:9f:38:f6:64), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
> Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.2
v User Datagram Protocol, Src Port: 53, Dst Port: 59774
    Source Port: 53
    Destination Port: 59774
    Length: 104
    Checksum: 0xcb1b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (96 bytes)
> Domain Name System (response)

0000  3c f0 11 e1 a6 f4 02 f3  9f 38 f6 64 08 00 45 00   <------- ·8·d··E·
0010  00 7c 40 b8 00 00 40 11  cd 8d ac 14 0a 01 ac 14   ·|@···@· --------
0020  0a 02 00 35 e9 7e 00 68  cb 1b 00 01 85 83 00 01   ···5·~·h --------
0030  00 00 00 01 00 00 01 31  02 31 30 02 32 30 03 31   -------1 ·10·20·1
0040  37 32 07 69 6e 2d 61 64  64 72 04 61 72 70 61 00   72·in-ad dr·arpa·
0050  00 0c 00 01 02 32 30 03  31 37 32 07 49 4e 2d 41   -----20· 172·IN-A
0060  44 44 52 04 41 52 50 41  00 00 06 00 01 00 00 0e   DDR·ARPA --------
0070  10 00 17 c0 2a 00 00 00  00 00 00 00 70 80 00 00   ····*··· ····p···
0080  1c 20 00 09 3a 80 00 01  51 80                     · ··:··· Q·
```

Figure 12: Port numbers of the second packet