WSA4

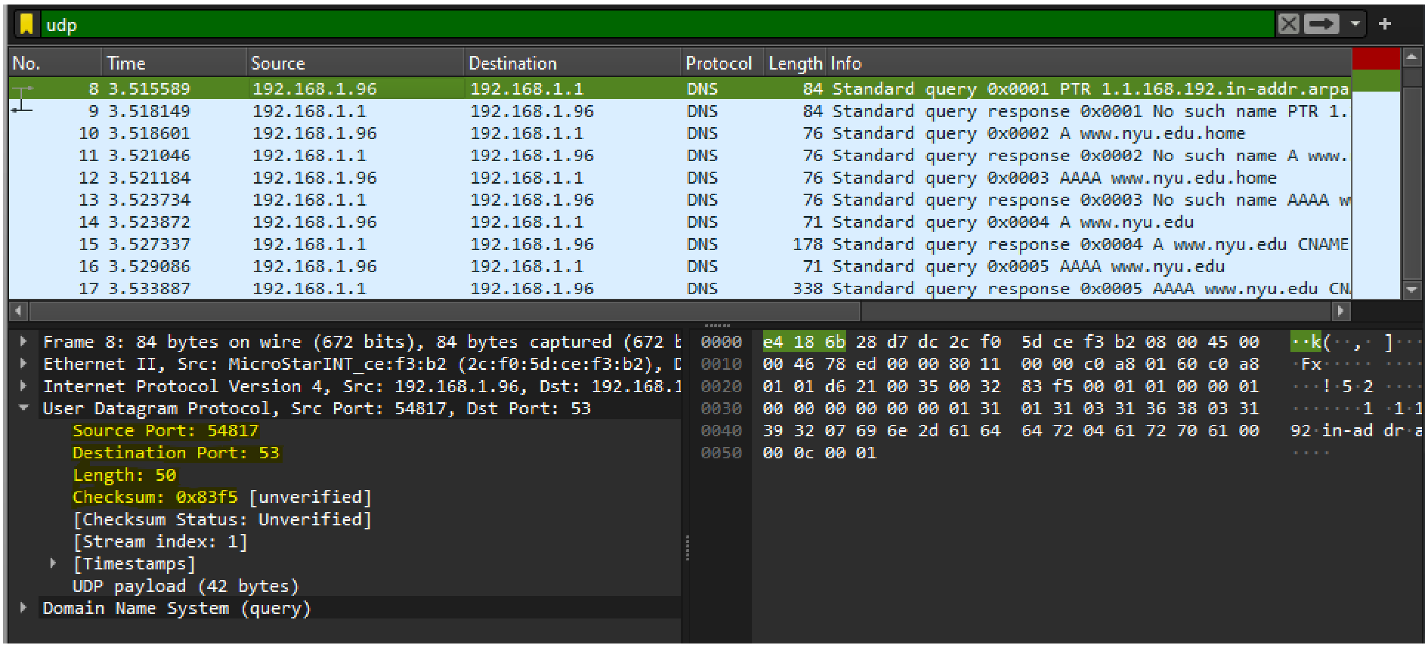
2448025

1.1. Packet Number : 8

1.2. The type of application-layer payload or protocol message : DNS.

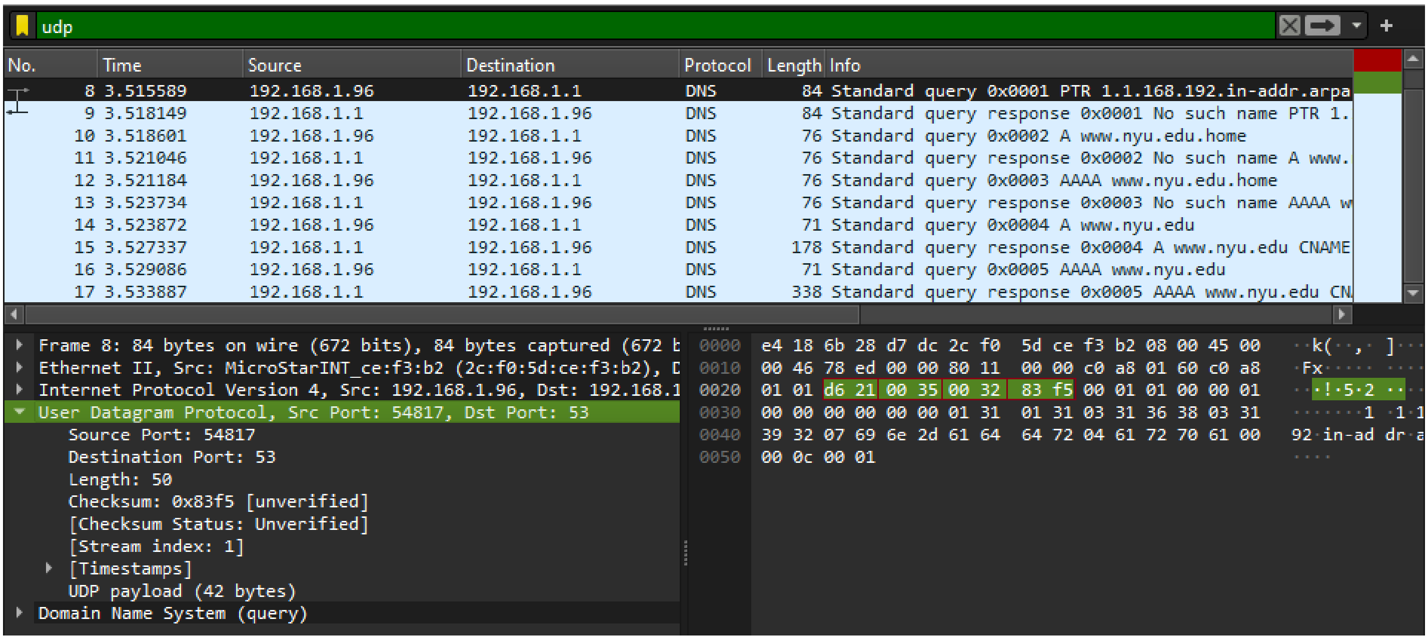
1.3. The header contains only 4 fields.

1.4. Source Port, Destination Port, Length, Checksum.



```
udp

No.   Time       Source         Destination    Protocol Length Info
    8 3.515589   192.168.1.96   192.168.1.1    DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
    9 3.518149   192.168.1.1    192.168.1.96   DNS        84 Standard query response 0x0001 No such name PTR 1.
   10 3.518601   192.168.1.96   192.168.1.1    DNS        76 Standard query 0x0002 A www.nyu.edu.home
   11 3.521046   192.168.1.1    192.168.1.96   DNS        76 Standard query response 0x0002 No such name A www.
   12 3.521184   192.168.1.96   192.168.1.1    DNS        76 Standard query 0x0003 AAAA www.nyu.edu.home
   13 3.523734   192.168.1.1    192.168.1.96   DNS        76 Standard query response 0x0003 No such name AAAA w
   14 3.523872   192.168.1.96   192.168.1.1    DNS        71 Standard query 0x0004 A www.nyu.edu
   15 3.527337   192.168.1.1    192.168.1.96   DNS       178 Standard query response 0x0004 A www.nyu.edu CNAME
   16 3.529086   192.168.1.96   192.168.1.1    DNS        71 Standard query 0x0005 AAAA www.nyu.edu
   17 3.533887   192.168.1.1    192.168.1.96   DNS       338 Standard query response 0x0005 AAAA www.nyu.edu CN

Frame 8: 84 bytes on wire (672 bits), 84 bytes captured (672 b
Ethernet II, Src: MicroStarINT_ce:f3:b2 (2c:f0:5d:ce:f3:b2), D
Internet Protocol Version 4, Src: 192.168.1.96, Dst: 192.168.1
User Datagram Protocol, Src Port: 54817, Dst Port: 53
    Source Port: 54817
    Destination Port: 53
    Length: 50
    Checksum: 0x83f5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  [Timestamps]
    UDP payload (42 bytes)
Domain Name System (query)

0000  e4 18 6b 28 d7 dc 2c f0  5d ce f3 b2 08 00 45 00   ··k(··,· ]·····E·
0010  00 46 78 ed 00 00 80 11  00 00 c0 a8 01 60 c0 a8   ·Fx····· ·····`··
0020  01 01 d6 21 00 35 00 32  83 f5 00 01 01 00 00 01   ···!·5·2 ········
0030  00 00 00 00 00 00 01 31  01 31 03 31 36 38 03 31   ·······1 ·1·168·1
0040  39 32 07 69 6e 2d 61 64  64 72 04 61 72 70 61 00   92·in-ad dr·arpa·
0050  00 0c 00 01                                        ····
```

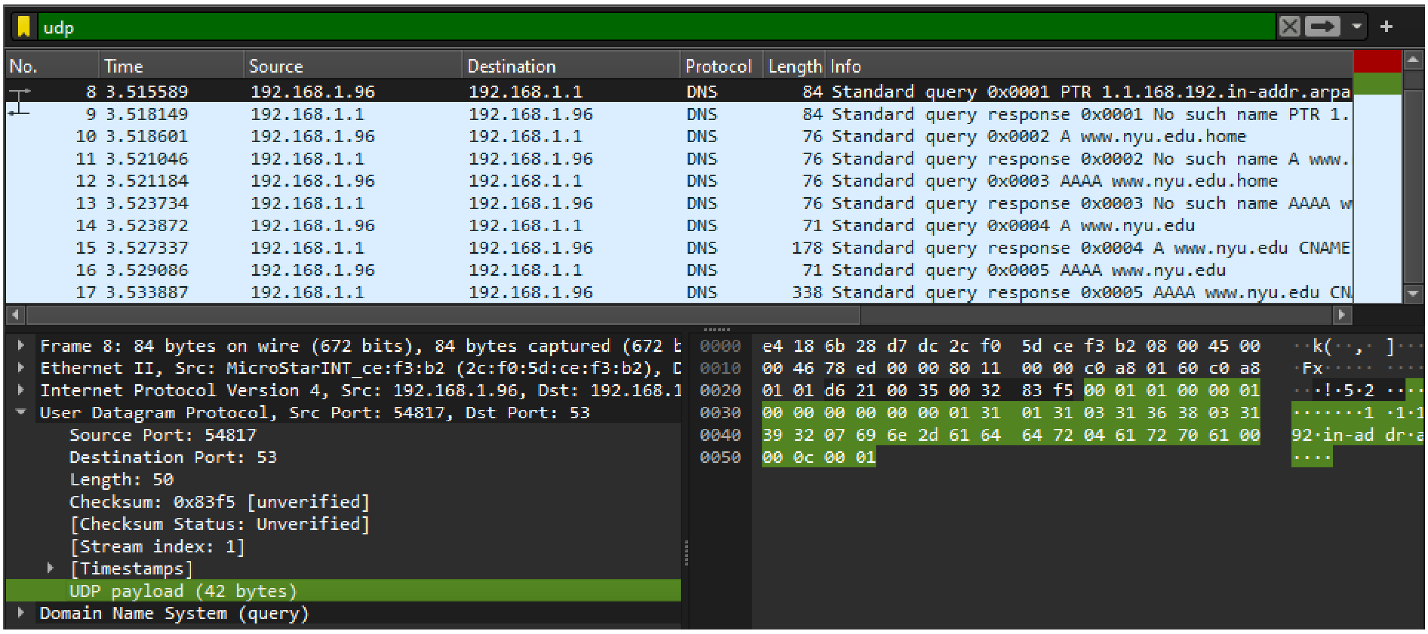
2. Each of header fields is 2 bytes. Total UDP header is 8 bytes long.



```
udp

No.   Time       Source         Destination    Protocol Length Info
    8 3.515589   192.168.1.96   192.168.1.1    DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
    9 3.518149   192.168.1.1    192.168.1.96   DNS        84 Standard query response 0x0001 No such name PTR 1.
   10 3.518601   192.168.1.96   192.168.1.1    DNS        76 Standard query 0x0002 A www.nyu.edu.home
   11 3.521046   192.168.1.1    192.168.1.96   DNS        76 Standard query response 0x0002 No such name A www.
   12 3.521184   192.168.1.96   192.168.1.1    DNS        76 Standard query 0x0003 AAAA www.nyu.edu.home
   13 3.523734   192.168.1.1    192.168.1.96   DNS        76 Standard query response 0x0003 No such name AAAA w
   14 3.523872   192.168.1.96   192.168.1.1    DNS        71 Standard query 0x0004 A www.nyu.edu
   15 3.527337   192.168.1.1    192.168.1.96   DNS       178 Standard query response 0x0004 A www.nyu.edu CNAME
   16 3.529086   192.168.1.96   192.168.1.1    DNS        71 Standard query 0x0005 AAAA www.nyu.edu
   17 3.533887   192.168.1.1    192.168.1.96   DNS       338 Standard query response 0x0005 AAAA www.nyu.edu CN

Frame 8: 84 bytes on wire (672 bits), 84 bytes captured (672 b
Ethernet II, Src: MicroStarINT_ce:f3:b2 (2c:f0:5d:ce:f3:b2), D
Internet Protocol Version 4, Src: 192.168.1.96, Dst: 192.168.1
User Datagram Protocol, Src Port: 54817, Dst Port: 53
    Source Port: 54817
    Destination Port: 53
    Length: 50
    Checksum: 0x83f5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  [Timestamps]
    UDP payload (42 bytes)
Domain Name System (query)

0000  e4 18 6b 28 d7 dc 2c f0  5d ce f3 b2 08 00 45 00   ··k(··,· ]·····E·
0010  00 46 78 ed 00 00 80 11  00 00 c0 a8 01 60 c0 a8   ·Fx····· ·····`··
0020  01 01 d6 21 00 35 00 32  83 f5 00 01 01 00 00 01   ···!·5·2 ········
0030  00 00 00 00 00 00 01 31  01 31 03 31 36 38 03 31   ·······1 ·1·168·1
0040  39 32 07 69 6e 2d 61 64  64 72 04 61 72 70 61 00   92·in-ad dr·arpa·
0050  00 0c 00 01                                        ····
```

3. (2^{16} – 1) – Header Length = Max Payload Size

   65535 - 8 = 65527 bytes.

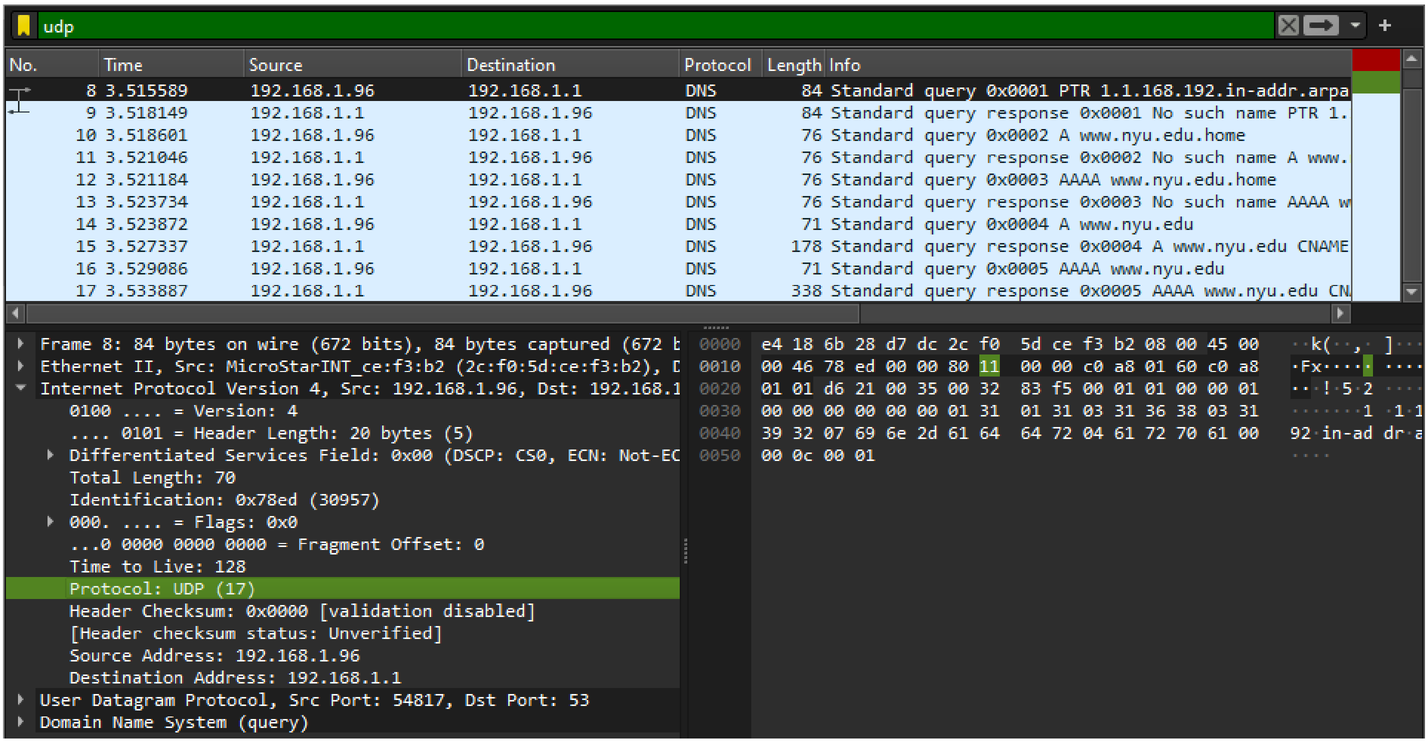


```
No.   Time       Source          Destination     Protocol Length Info
    8 3.515589   192.168.1.96    192.168.1.1     DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
    9 3.518149   192.168.1.1     192.168.1.96    DNS        84 Standard query response 0x0001 No such name PTR 1.
   10 3.518601   192.168.1.96    192.168.1.1     DNS        76 Standard query 0x0002 A www.nyu.edu.home
   11 3.521046   192.168.1.1     192.168.1.96    DNS        76 Standard query response 0x0002 No such name A www.
   12 3.521184   192.168.1.96    192.168.1.1     DNS        76 Standard query 0x0003 AAAA www.nyu.edu.home
   13 3.523734   192.168.1.1     192.168.1.96    DNS        76 Standard query response 0x0003 No such name AAAA w
   14 3.523872   192.168.1.96    192.168.1.1     DNS        71 Standard query 0x0004 A www.nyu.edu
   15 3.527337   192.168.1.1     192.168.1.96    DNS       178 Standard query response 0x0004 A www.nyu.edu CNAME
   16 3.529086   192.168.1.96    192.168.1.1     DNS        71 Standard query 0x0005 AAAA www.nyu.edu
   17 3.533887   192.168.1.1     192.168.1.96    DNS       338 Standard query response 0x0005 AAAA www.nyu.edu CN
```

```
> Frame 8: 84 bytes on wire (672 bits), 84 bytes captured (672 b
> Ethernet II, Src: MicroStarINT_ce:f3:b2 (2c:f0:5d:ce:f3:b2), D
> Internet Protocol Version 4, Src: 192.168.1.96, Dst: 192.168.1
v User Datagram Protocol, Src Port: 54817, Dst Port: 53
    Source Port: 54817
    Destination Port: 53
    Length: 50
    Checksum: 0x83f5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (42 bytes)
> Domain Name System (query)
```

```
0000  e4 18 6b 28 d7 dc 2c f0  5d ce f3 b2 08 00 45 00   ··k(··,· ]·····
0010  00 46 78 ed 00 00 80 11  00 00 c0 a8 01 60 c0 a8   ·Fx····· ····
0020  01 01 d6 21 00 35 00 32  83 f5 00 01 01 00 00 01   ···!·5·2 ····
0030  00 00 00 00 00 00 01 31  01 31 03 31 36 38 03 31   ·······1 ·1·1
0040  39 32 07 69 6e 2d 61 64  64 72 04 61 72 70 61 00   92·in-ad dr·a
0050  00 0c 00 01                                        ····
```

4. Protocol Number : 17



```
No.   Time       Source          Destination     Protocol Length Info
    8 3.515589   192.168.1.96    192.168.1.1     DNS        84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
    9 3.518149   192.168.1.1     192.168.1.96    DNS        84 Standard query response 0x0001 No such name PTR 1.
   10 3.518601   192.168.1.96    192.168.1.1     DNS        76 Standard query 0x0002 A www.nyu.edu.home
   11 3.521046   192.168.1.1     192.168.1.96    DNS        76 Standard query response 0x0002 No such name A www.
   12 3.521184   192.168.1.96    192.168.1.1     DNS        76 Standard query 0x0003 AAAA www.nyu.edu.home
   13 3.523734   192.168.1.1     192.168.1.96    DNS        76 Standard query response 0x0003 No such name AAAA w
   14 3.523872   192.168.1.96    192.168.1.1     DNS        71 Standard query 0x0004 A www.nyu.edu
   15 3.527337   192.168.1.1     192.168.1.96    DNS       178 Standard query response 0x0004 A www.nyu.edu CNAME
   16 3.529086   192.168.1.96    192.168.1.1     DNS        71 Standard query 0x0005 AAAA www.nyu.edu
   17 3.533887   192.168.1.1     192.168.1.96    DNS       338 Standard query response 0x0005 AAAA www.nyu.edu CN
```

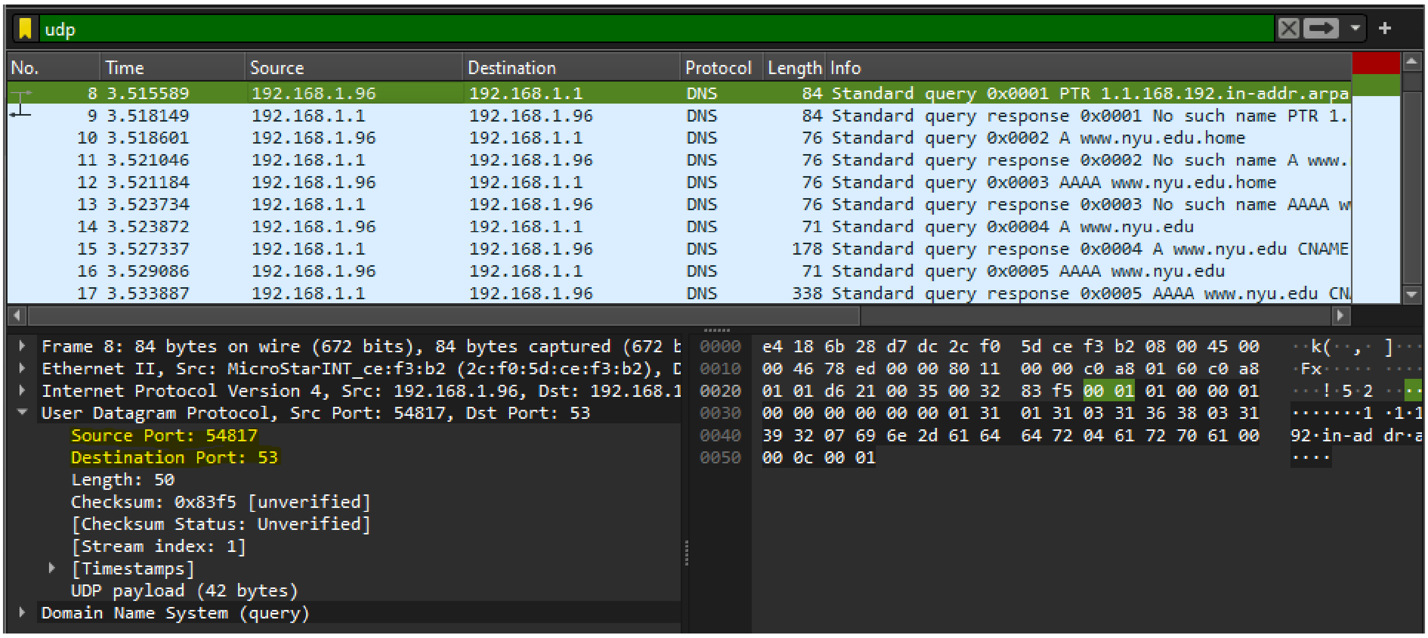
```
> Frame 8: 84 bytes on wire (672 bits), 84 bytes captured (672 b
> Ethernet II, Src: MicroStarINT_ce:f3:b2 (2c:f0:5d:ce:f3:b2), D
v Internet Protocol Version 4, Src: 192.168.1.96, Dst: 192.168.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-EC
    Total Length: 70
    Identification: 0x78ed (30957)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.96
    Destination Address: 192.168.1.1
> User Datagram Protocol, Src Port: 54817, Dst Port: 53
> Domain Name System (query)
```

```
0000  e4 18 6b 28 d7 dc 2c f0  5d ce f3 b2 08 00 45 00   ··k(··,· ]·····
0010  00 46 78 ed 00 00 80 11  00 00 c0 a8 01 60 c0 a8   ·Fx····· ····
0020  01 01 d6 21 00 35 00 32  83 f5 00 01 01 00 00 01   ···!·5·2 ····
0030  00 00 00 00 00 00 01 31  01 31 03 31 36 38 03 31   ·······1 ·1·1
0040  39 32 07 69 6e 2d 61 64  64 72 04 61 72 70 61 00   92·in-ad dr·a
0050  00 0c 00 01                                        ····
```

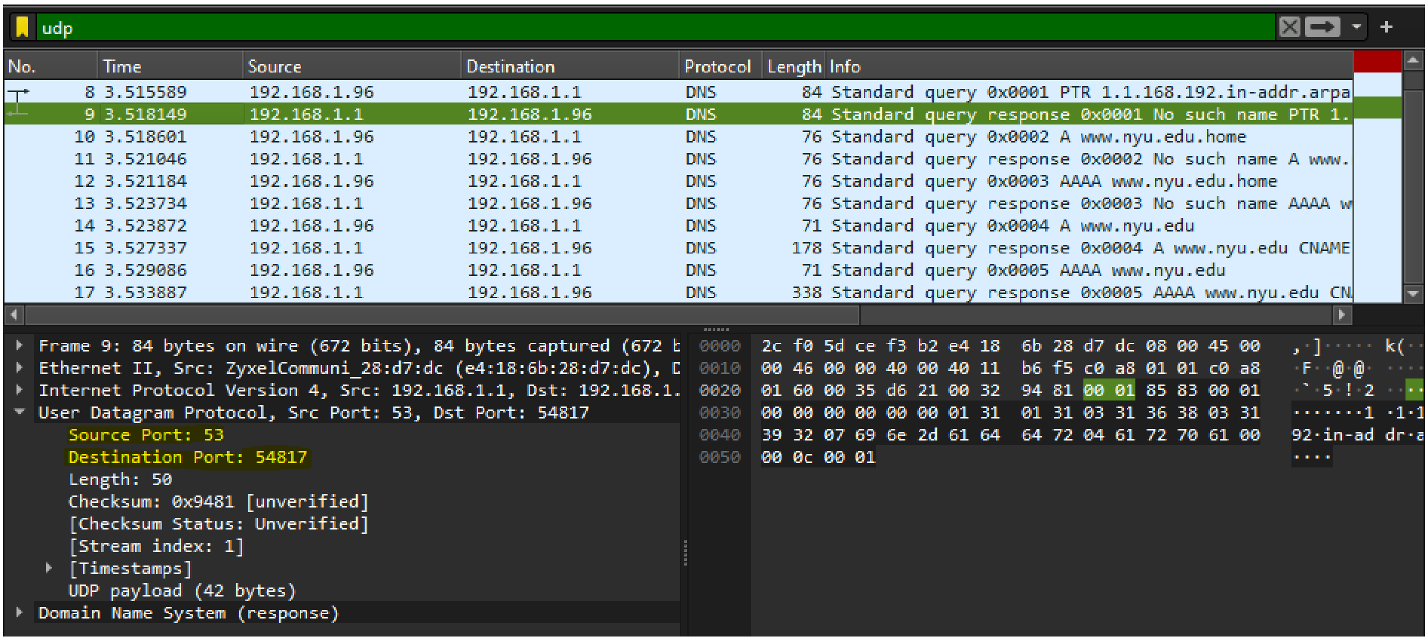
5.1. First UDP Segment Packet Number : 8

5.2. Second UDP Segment Packet Number : 9

The source port of a UDP packet sent by the host corresponds to the destination port of a reply packet, and vice versa.



```
udp
No.  Time        Source        Destination   Protocol Length Info
  8 3.515589    192.168.1.96  192.168.1.1   DNS       84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
  9 3.518149    192.168.1.1   192.168.1.96  DNS       84 Standard query response 0x0001 No such name PTR 1.
 10 3.518601    192.168.1.96  192.168.1.1   DNS       76 Standard query 0x0002 A www.nyu.edu.home
 11 3.521046    192.168.1.1   192.168.1.96  DNS       76 Standard query response 0x0002 No such name A www.
 12 3.521184    192.168.1.96  192.168.1.1   DNS       76 Standard query 0x0003 AAAA www.nyu.edu.home
 13 3.523734    192.168.1.1   192.168.1.96  DNS       76 Standard query response 0x0003 No such name AAAA w
 14 3.523872    192.168.1.96  192.168.1.1   DNS       71 Standard query 0x0004 A www.nyu.edu
 15 3.527337    192.168.1.1   192.168.1.96  DNS      178 Standard query response 0x0004 A www.nyu.edu CNAME
 16 3.529086    192.168.1.96  192.168.1.1   DNS       71 Standard query 0x0005 AAAA www.nyu.edu
 17 3.533887    192.168.1.1   192.168.1.96  DNS      338 Standard query response 0x0005 AAAA www.nyu.edu CN

> Frame 8: 84 bytes on wire (672 bits), 84 bytes captured (672 b
> Ethernet II, Src: MicroStarINT_ce:f3:b2 (2c:f0:5d:ce:f3:b2), D
> Internet Protocol Version 4, Src: 192.168.1.96, Dst: 192.168.1
v User Datagram Protocol, Src Port: 54817, Dst Port: 53
    Source Port: 54817
    Destination Port: 53
    Length: 50
    Checksum: 0x83f5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (42 bytes)
> Domain Name System (query)

0000  e4 18 6b 28 d7 dc 2c f0  5d ce f3 b2 08 00 45 00   ··k(··,· ]·····E·
0010  00 46 78 ed 00 00 80 11  00 00 c0 a8 01 60 c0 a8   ·Fx····· ·····`··
0020  01 01 d6 21 00 35 00 32  83 f5 00 01 01 00 00 01   ···!·5·2 ········
0030  00 00 00 00 00 00 01 31  01 31 03 31 36 38 03 31   ·······1 ·1·168·1
0040  39 32 07 69 6e 2d 61 64  64 72 04 61 72 70 61 00   92·in-ad dr·arpa·
0050  00 0c 00 01                                        ····
```



```
udp
No.  Time        Source        Destination   Protocol Length Info
  8 3.515589    192.168.1.96  192.168.1.1   DNS       84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
  9 3.518149    192.168.1.1   192.168.1.96  DNS       84 Standard query response 0x0001 No such name PTR 1.
 10 3.518601    192.168.1.96  192.168.1.1   DNS       76 Standard query 0x0002 A www.nyu.edu.home
 11 3.521046    192.168.1.1   192.168.1.96  DNS       76 Standard query response 0x0002 No such name A www.
 12 3.521184    192.168.1.96  192.168.1.1   DNS       76 Standard query 0x0003 AAAA www.nyu.edu.home
 13 3.523734    192.168.1.1   192.168.1.96  DNS       76 Standard query response 0x0003 No such name AAAA w
 14 3.523872    192.168.1.96  192.168.1.1   DNS       71 Standard query 0x0004 A www.nyu.edu
 15 3.527337    192.168.1.1   192.168.1.96  DNS      178 Standard query response 0x0004 A www.nyu.edu CNAME
 16 3.529086    192.168.1.96  192.168.1.1   DNS       71 Standard query 0x0005 AAAA www.nyu.edu
 17 3.533887    192.168.1.1   192.168.1.96  DNS      338 Standard query response 0x0005 AAAA www.nyu.edu CN

> Frame 9: 84 bytes on wire (672 bits), 84 bytes captured (672 b
> Ethernet II, Src: ZyxelCommuni_28:d7:dc (e4:18:6b:28:d7:dc), D
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.
v User Datagram Protocol, Src Port: 53, Dst Port: 54817
    Source Port: 53
    Destination Port: 54817
    Length: 50
    Checksum: 0x9481 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (42 bytes)
> Domain Name System (response)

0000  2c f0 5d ce f3 b2 e4 18  6b 28 d7 dc 08 00 45 00   ,·]····· k(····E·
0010  00 46 00 00 40 00 40 11  b6 f5 c0 a8 01 01 c0 a8   ·F··@·@· ········
0020  01 60 00 35 d6 21 00 32  94 81 00 01 85 83 00 01   ·`·5·!·2 ········
0030  00 00 00 00 00 00 01 31  01 31 03 31 36 38 03 31   ·······1 ·1·168·1
0040  39 32 07 69 6e 2d 61 64  64 72 04 61 72 70 61 00   92·in-ad dr·arpa·
0050  00 0c 00 01                                        ····
```