

LAB-4

1. Do a transaction using UDP. Verify what all information are present in the header.

UDP header contains 4 fields:

- 1.Source Port
- 2.Destination Port
- 3.Length
- 4.Checksum

No.	Time	Source	Destination	Protocol	Length	Info
252	8.775239	192.168.0.9	106.51.115.154	DNS	76	Standard query 0xc9d A ogs.google.co.in
253	8.779570	106.51.115.154	192.168.0.9	DNS	123	Standard query response 0xc9d A ogs.google.co.in CNAME www3.l.google.com A 142.250.76.78
318	9.346479	192.168.0.9	106.51.115.154	DNS	87	Standard query 0xb682 A googleads.g.doubleclick.net
319	9.356973	106.51.115.154	192.168.0.9	DNS	128	Standard query response 0xb682 A googleads.g.doubleclick.net CNAME pagead46.l.doubleclick.net A 142.250.67.66
360	9.799736	192.168.0.9	106.51.115.154	DNS	75	Standard query 0xb09d A play.google.com
363	9.811539	106.51.115.154	192.168.0.9	DNS	91	Standard query response 0xb09d A play.google.com A 172.217.163.174
881	21.932822	192.168.0.9	106.51.115.154	DNS	75	Standard query 0xa271 A www.youtube.com
882	21.942825	106.51.115.154	192.168.0.9	DNS	365	Standard query response 0xa271 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.163.206 A 172.217.166.110 A 172.217.1.1
891	22.043345	192.168.0.9	106.51.115.154	DNS	75	Standard query 0x07d0 A www.youtube.com
892	22.051112	106.51.115.154	192.168.0.9	DNS	365	Standard query response 0x07d0 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.163.206 A 172.217.166.110 A 172.217.1.1
1077	25.360293	192.168.0.9	106.51.115.154	DNS	80	Standard query 0x31fd A fonts.googleapis.com
1079	25.367470	106.51.115.154	192.168.0.9	DNS	96	Standard query response 0x31fd A fonts.googleapis.com A 216.58.200.138
1141	27.977876	192.168.0.9	106.51.115.154	DNS	85	Standard query 0x9eea A lh4.googleusercontent.com
1143	27.986616	106.51.115.154	192.168.0.9	DNS	130	Standard query response 0x9eea A lh4.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 142.250.67.33
1408	28.663804	192.168.0.9	106.51.115.154	DNS	82	Standard query 0xc9f7 A static.doubleclick.net
1409	28.670454	106.51.115.154	192.168.0.9	DNS	147	Standard query response 0xc9f7 A static.doubleclick.net CNAME static-doubleclick-net.l.google.com A 142.250.67.70
1496	29.630148	192.168.0.9	106.51.115.154	DNS	79	Standard query 0xa508 A clients1.google.com
1497	29.639072	106.51.115.154	192.168.0.9	DNS	119	Standard query response 0xa508 A clients1.google.com CNAME clients.l.google.com A 172.217.163.110

> Frame 881: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{309848B1-796F-4478-94CE-2AE7C9DA600A}, id 0
> Ethernet II, Src: IntelCor_8a:c8:39 (5c:87:9c:8a:c8:39), Dst: D-LinkIn_a7:c6:ab (f4:8c:eb:a7:c6:ab)
> Internet Protocol Version 4, Src: 192.168.0.9, Dst: 106.51.115.154
v User Datagram Protocol, Src Port: 60588, Dst Port: 53
Source Port: 60588
Destination Port: 53
Length: 41
Checksum: 0x9eb9 [unverified]
[Checksum Status: Unverified]
[Stream index: 21]
> [Timestamps]
> Domain Name System (query)

2. Determine the length (in bytes) of each of UDP header fields (use the packet content field)

UDP header size is 8 bytes. Each header field is 2 bytes long

363	9.811539	106.51.115.154	192.168.0.9	DNS	91	Standard query response 0xb09d A play.google.com A 172.217.163.174
881	21.932822	192.168.0.9	106.51.115.154	DNS	75	Standard query 0xa271 A www.youtube.com
882	21.942825	106.51.115.154	192.168.0.9	DNS	365	Standard query response 0xa271 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.163.206 A 172.217.166.110 A 172.217.1.1
891	22.043345	192.168.0.9	106.51.115.154	DNS	75	Standard query 0x07d0 A www.youtube.com
892	22.051112	106.51.115.154	192.168.0.9	DNS	365	Standard query response 0x07d0 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.163.206 A 172.217.166.110 A 172.217.1.1
1077	25.360293	192.168.0.9	106.51.115.154	DNS	80	Standard query 0x31fd A fonts.googleapis.com
1079	25.367470	106.51.115.154	192.168.0.9	DNS	96	Standard query response 0x31fd A fonts.googleapis.com A 216.58.200.138
1141	27.977876	192.168.0.9	106.51.115.154	DNS	85	Standard query 0x9eea A lh4.googleusercontent.com
1143	27.986616	106.51.115.154	192.168.0.9	DNS	130	Standard query response 0x9eea A lh4.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 142.250.67.33
1408	28.663804	192.168.0.9	106.51.115.154	DNS	82	Standard query 0xc9f7 A static.doubleclick.net
1409	28.670454	106.51.115.154	192.168.0.9	DNS	147	Standard query response 0xc9f7 A static.doubleclick.net CNAME static-doubleclick-net.l.google.com A 142.250.67.70
1496	29.630148	192.168.0.9	106.51.115.154	DNS	79	Standard query 0xa508 A clients1.google.com
1497	29.639072	106.51.115.154	192.168.0.9	DNS	119	Standard query response 0xa508 A clients1.google.com CNAME clients.l.google.com A 172.217.163.110

> Frame 881: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{309848B1-796F-4478-94CE-2AE7C9DA600A}, id 0
> Ethernet II, Src: IntelCor_8a:c8:39 (5c:87:9c:8a:c8:39), Dst: D-LinkIn_a7:c6:ab (f4:8c:eb:a7:c6:ab)
> Internet Protocol Version 4, Src: 192.168.0.9, Dst: 106.51.115.154
v User Datagram Protocol, Src Port: 60588, Dst Port: 53
Source Port: 60588
Destination Port: 53
Length: 41
Checksum: 0x9eb9 [unverified]
[Checksum Status: Unverified]
[Stream index: 21]
> [Timestamps]
> Domain Name System (query)

0000	f4 8c eb a7 c6 ab 5c 87	9c 8a c8 39 08 00 45 00\.....9..E:
0010	00 3d 49 8a c8 00 00 11	00 00 c0 a8 00 09 6a 33	-----j3
0020	73 9c	8c ac 00 35 00 20 9e 06	12 71 01 00 00 01 s...45...Q...
0030	00 00 00 00 00 00 05 77	07 77 07 79 6f 75 74 75	-----w ww-youtu
0040	62 65 03 63 6f 6d 00 00	01 00 01	be com

3. What is the protocol number for UDP? (You will get this from the IP protocol field)

The protocol number for UDP is 17

360 9.799736	192.168.0.9	106.51.115.154	DNS	75 Standard query 0xb09d A play.google.com
363 9.811539	106.51.115.154	192.168.0.9	DNS	91 Standard query response 0xb09d A play.google.com A 172.217.163.174
881 21.932822	192.168.0.9	106.51.115.154	DNS	75 Standard query 0xa271 A www.youtube.com
882 21.942825	106.51.115.154	192.168.0.9	DNS	365 Standard query response 0xa271 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.163.206 A 172.217.166.110 A 172.217.163.206 A 172.217.166.110
891 22.043345	192.168.0.9	106.51.115.154	DNS	75 Standard query 0x07d0 A www.youtube.com
892 22.051112	106.51.115.154	192.168.0.9	DNS	365 Standard query response 0x07d0 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.163.206 A 172.217.166.110 A 172.217.163.206 A 172.217.166.110
1077 25.360293	192.168.0.9	106.51.115.154	DNS	80 Standard query 0x31fd A fonts.googleapis.com
1079 25.367470	106.51.115.154	192.168.0.9	DNS	96 Standard query response 0x31fd A fonts.googleapis.com A 216.58.200.138
1141 27.977876	192.168.0.9	106.51.115.154	DNS	85 Standard query 0x9eea A lh4.googleusercontent.com
1143 27.986616	106.51.115.154	192.168.0.9	DNS	130 Standard query response 0x9eea A lh4.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 142.250.67.33
1408 28.663804	192.168.0.9	106.51.115.154	DNS	82 Standard query 0xc9f7 A static.doubleclick.net
1409 28.670454	106.51.115.154	192.168.0.9	DNS	147 Standard query response 0xc9f7 A static.doubleclick.net CNAME static-doubleclick-net.l.google.com A 142.250.67.70
1496 29.630148	192.168.0.9	106.51.115.154	DNS	79 Standard query 0xa508 A clients1.google.com
1497 29.639072	106.51.115.154	192.168.0.9	DNS	119 Standard query response 0xa508 A clients1.google.com CNAME clients.l.google.com A 172.217.163.110

Fragment offset: 0
Time to live: 128
Protocol: UDP (17)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.0.9
Destination: 106.51.115.154

✓ User Datagram Protocol, Src Port: 60588, Dst Port: 53
Source Port: 60588
Destination Port: 53
Length: 41
Checksum: 0x9eb9 [unverified]
[Checksum Status: Unverified]

0000 f4 8c eb a7 c6 ab 5c 87 9c 8a c8 39 08 00 45 00 \. . . . 9 . . E .
0010 00 3d 89 b8 00 00 80 11 00 00 c0 a8 00 09 6a 33 . = j 3
0020 73 9a ec ac 00 35 00 29 9e b9 a2 71 01 00 00 01 s 5 .) . . . q . . .
0030 00 00 00 00 00 00 03 77 77 77 07 79 6f 75 74 75 w w w . y o u t u
0040 62 65 03 63 6f 6d 00 00 01 00 01 b e . c o m

4. Select a request/response pair for a UDP transaction. How can you see that they are related? Mark your observations and explain

From the leftmost column, we can see the mark of the request/response pair for a UDP transaction

318 9.346479	192.168.0.9	106.51.115.154	DNS	87 Standard query 0xb682 A googleads.g.doubleclick.net
319 9.356973	106.51.115.154	192.168.0.9	DNS	128 Standard query response 0xb682 A googleads.g.doubleclick.net CNAME pagead46.l.doubleclick.net A 142.250.67.66
360 9.799736	192.168.0.9	106.51.115.154	DNS	75 Standard query 0xb09d A play.google.com
363 9.811539	106.51.115.154	192.168.0.9	DNS	91 Standard query response 0xb09d A play.google.com A 172.217.163.174
881 21.932822	192.168.0.9	106.51.115.154	DNS	75 Standard query 0xa271 A www.youtube.com
882 21.942825	106.51.115.154	192.168.0.9	DNS	365 Standard query response 0xa271 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.163.206 A 172.217.166.110 A 172.217.163.206 A 172.217.166.110
891 22.043345	192.168.0.9	106.51.115.154	DNS	75 Standard query 0x07d0 A www.youtube.com
892 22.051112	106.51.115.154	192.168.0.9	DNS	365 Standard query response 0x07d0 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.163.206 A 172.217.166.110 A 172.217.163.206 A 172.217.166.110
1077 25.360293	192.168.0.9	106.51.115.154	DNS	80 Standard query 0x31fd A fonts.googleapis.com
1079 25.367470	106.51.115.154	192.168.0.9	DNS	96 Standard query response 0x31fd A fonts.googleapis.com A 216.58.200.138
1141 27.977876	192.168.0.9	106.51.115.154	DNS	85 Standard query 0x9eea A lh4.googleusercontent.com
1143 27.986616	106.51.115.154	192.168.0.9	DNS	130 Standard query response 0x9eea A lh4.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 142.250.67.33
1408 28.663804	192.168.0.9	106.51.115.154	DNS	82 Standard query 0xc9f7 A static.doubleclick.net
1409 28.670454	106.51.115.154	192.168.0.9	DNS	147 Standard query response 0xc9f7 A static.doubleclick.net CNAME static-doubleclick-net.l.google.com A 142.250.67.70
1496 29.630148	192.168.0.9	106.51.115.154	DNS	79 Standard query 0xa508 A clients1.google.com
1497 29.639072	106.51.115.154	192.168.0.9	DNS	119 Standard query response 0xa508 A clients1.google.com CNAME clients.l.google.com A 172.217.163.110

> Frame 881: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{309848B1-796F-4478-94CE-2AE7C9DA600A}, id 0
> Ethernet II, Src: IntelCor_8a:c8:39 (5c:87:9c:8a:c8:39), Dst: D-LinkIn_a7:c6:ab (f4:8c:eba7:c6:ab)
> Internet Protocol Version 4, Src: 192.168.0.9, Dst: 106.51.115.154
✓ User Datagram Protocol, Src Port: 60588, Dst Port: 53
Source Port: 60588
Destination Port: 53
Length: 41
Checksum: 0x9eb9 [unverified]
[Checksum Status: Unverified]
[Stream index: 21]
> [Timestamps]

319 9.356973	106.51.115.154	192.168.0.9	DNS	128 Standard query response 0xb682 A googleads.g.doubleclick.net CNAME pagead46.l.doubleclick.net A 142.250.67.66
360 9.799736	192.168.0.9	106.51.115.154	DNS	75 Standard query 0xb09d A play.google.com
363 9.811539	106.51.115.154	192.168.0.9	DNS	91 Standard query response 0xb09d A play.google.com A 172.217.163.174
881 21.932822	192.168.0.9	106.51.115.154	DNS	75 Standard query 0xa271 A www.youtube.com
882 21.942825	106.51.115.154	192.168.0.9	DNS	365 Standard query response 0xa271 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.163.206 A 172.217.166.110 A 172.2
891 22.043345	192.168.0.9	106.51.115.154	DNS	75 Standard query 0x07d0 A www.youtube.com
892 22.051112	106.51.115.154	192.168.0.9	DNS	365 Standard query response 0x07d0 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.163.206 A 172.217.166.110 A 172.2
1077 25.360293	192.168.0.9	106.51.115.154	DNS	80 Standard query 0x31fd A fonts.googleapis.com
1079 25.367470	106.51.115.154	192.168.0.9	DNS	96 Standard query response 0x31fd A fonts.googleapis.com A 216.58.200.138
1141 27.977876	192.168.0.9	106.51.115.154	DNS	85 Standard query 0x9eea A lh4.googleusercontent.com
1143 27.986516	106.51.115.154	192.168.0.9	DNS	130 Standard query response 0x9eea A lh4.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 142.250.67.33
1408 28.663804	192.168.0.9	106.51.115.154	DNS	82 Standard query 0xc9f7 A static.doubleclick.net
1409 28.670454	106.51.115.154	192.168.0.9	DNS	147 Standard query response 0xc9f7 A static.doubleclick.net CNAME static-doubleclick-net.l.google.com A 142.250.67.70
1496 29.630148	192.168.0.9	106.51.115.154	DNS	79 Standard query 0xa508 A clients1.google.com
1497 29.639072	106.51.115.154	192.168.0.9	DNS	119 Standard query response 0xa508 A clients1.google.com CNAME clients1.google.com A 172.217.163.110

> Frame 882: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits) on interface \Device\NPF_{30984881-796F-4478-94CE-2AE7C9DA600A}, id 0				
> Ethernet II, Src: D-LinkIn_a7:c6:ab (f4:8c:eb:a7:c6:ab), Dst: IntelCor_8a:c8:39 (5c:87:9c:8a:c8:39)				
> Internet Protocol Version 4, Src: 106.51.115.154, Dst: 192.168.0.9				
▼ User Datagram Protocol, Src Port: 53, Dst Port: 60588				
Source Port: 53 Destination Port: 60588 Length: 331 Checksum: 0x940b [unverified] [Checksum Status: Unverified] [Stream index: 21]				
> [Timestamps]				
> Domain Name System (response)				

Moreover, the source port send by the client is same as the destination port of the server packet. Similarly, the destination port by the client is the same as the source port of the client packet