Exercise 3.1

1) Transport layer protocol used in dns query is UDP.

2) Destination MAC address for ARP request/response is 00:00:00:00:00:00.

3) ICMP header type for Echo request: 8.

ICMP header type for Echo reply: 0.

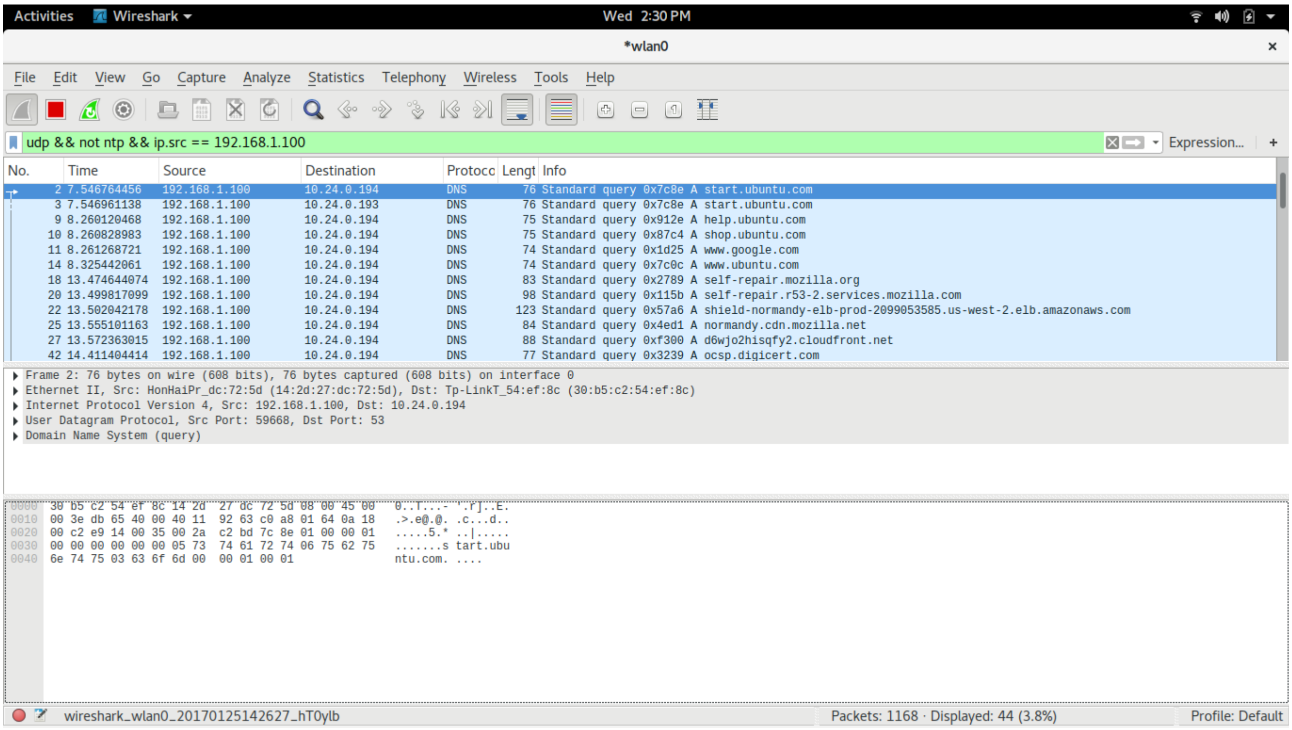
Size of the data field is 48 bytes.

Data found in one of the packet is 7f860600000000001011121314151617181 91a1b1c1d1e1f…

4) User-agent filed in http get request: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:50.0) Gecko/20100101 Firefox/50.0

5) Following are the filters used.

a) udp && not ntp && ip.src == 192.168.1.100



```
udp && not ntp && ip.src == 192.168.1.100
```

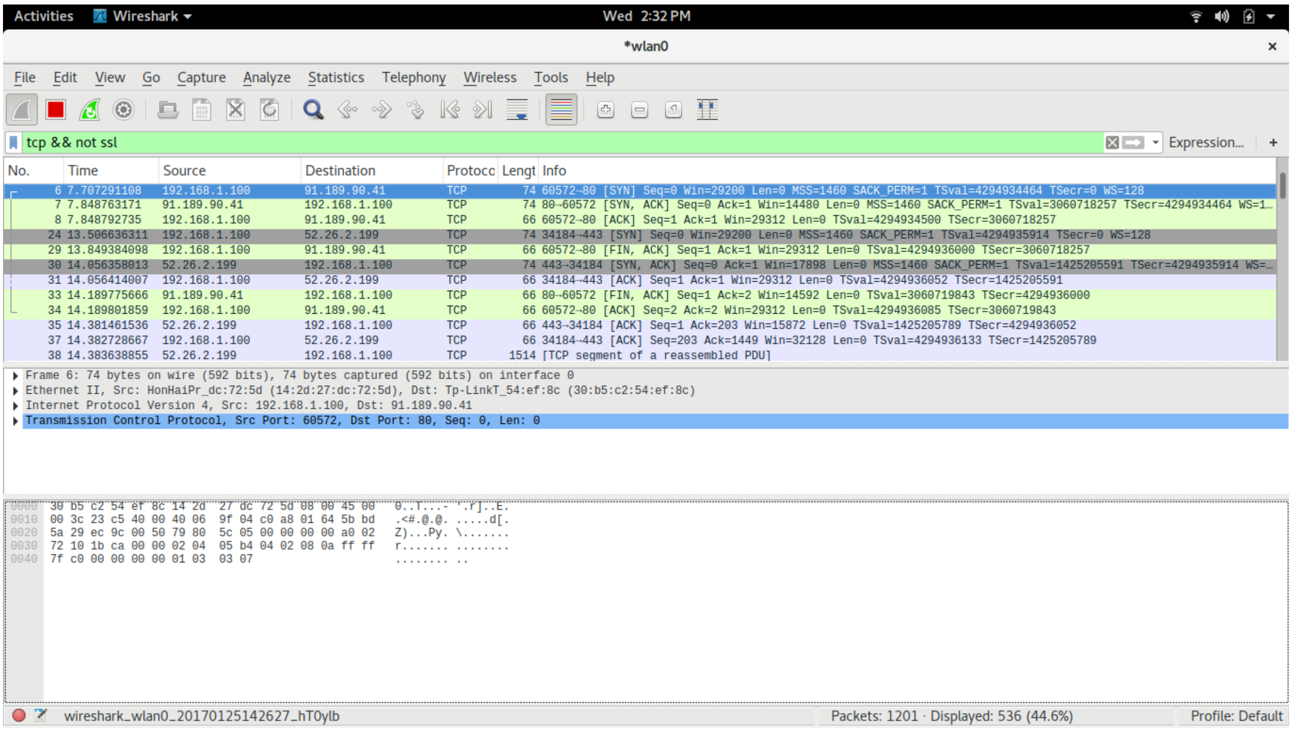
```
No.  Time          Source         Destination   Protoco Lengt Info
   2 7.546764456   192.168.1.100  10.24.0.194   DNS       76 Standard query 0x7c8e A start.ubuntu.com
   3 7.546961138   192.168.1.100  10.24.0.193   DNS       76 Standard query 0x7c8e A start.ubuntu.com
   9 8.260120468   192.168.1.100  10.24.0.194   DNS       75 Standard query 0x912e A help.ubuntu.com
  10 8.260828983   192.168.1.100  10.24.0.194   DNS       75 Standard query 0x87c4 A shop.ubuntu.com
  11 8.261268721   192.168.1.100  10.24.0.194   DNS       74 Standard query 0x1d25 A www.google.com
  14 8.325442061   192.168.1.100  10.24.0.194   DNS       74 Standard query 0x7c0c A www.ubuntu.com
  18 13.474644074  192.168.1.100  10.24.0.194   DNS       83 Standard query 0x2789 A self-repair.mozilla.org
  20 13.499817099  192.168.1.100  10.24.0.194   DNS       98 Standard query 0x115b A self-repair.r53-2.services.mozilla.com
  22 13.502042178  192.168.1.100  10.24.0.194   DNS      123 Standard query 0x57a6 A shield-normandy-elb-prod-2099053585.us-west-2.elb.amazonaws.com
  25 13.555101163  192.168.1.100  10.24.0.194   DNS       84 Standard query 0x4ed1 A normandy.cdn.mozilla.net
  27 13.572363015  192.168.1.100  10.24.0.194   DNS       88 Standard query 0xf300 A d6wjo2hisqfy2.cloudfront.net
  42 14.411404414  192.168.1.100  10.24.0.194   DNS       77 Standard query 0x3239 A ocsp.digicert.com
```

```
▸ Frame 2: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
▸ Ethernet II, Src: HonHaiPr_dc:72:5d (14:2d:27:dc:72:5d), Dst: Tp-LinkT_54:ef:8c (30:b5:c2:54:ef:8c)
▸ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 10.24.0.194
▸ User Datagram Protocol, Src Port: 59668, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  30 b5 c2 54 ef 8c 14 2d  27 dc 72 5d 08 00 45 00   0..T...- '.r]..E.
0010  00 3e db 65 40 00 40 11  92 63 c0 a8 01 64 0a 18   .>.e@.@. .c...d..
0020  00 c2 e9 14 00 35 00 2a  c2 bd 7c 8e 01 00 00 01   .....5.* ..|.....
0030  00 00 00 00 00 00 05 73  74 61 72 74 06 75 62 75   .......s tart.ubu
0040  6e 74 75 03 63 6f 6d 00  00 01 00 01              ntu.com. ....
```

wireshark_wlan0_20170125142627_hT0ylb   Packets: 1168 · Displayed: 44 (3.8%)   Profile: Default

b) tcp && not ssl



tcp && not ssl

```
No.   Time          Source          Destination     Protocc Lengt Info
    6 7.707291108   192.168.1.100   91.189.90.41    TCP       74 60572→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4294934464 TSecr=0 WS=128
    7 7.848763171   91.189.90.41    192.168.1.100   TCP       74 80→60572 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=3060718257 TSecr=4294934464 WS=1…
    8 7.848792735   192.168.1.100   91.189.90.41    TCP       66 60572→80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=4294934500 TSecr=3060718257
   24 13.506636311  192.168.1.100   52.26.2.199     TCP       74 34184→443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4294935914 TSecr=0 WS=128
   29 13.849384098  192.168.1.100   91.189.90.41    TCP       66 60572→80 [FIN, ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=4294936000 TSecr=3060718257
   30 14.056358013  52.26.2.199     192.168.1.100   TCP       74 443→34184 [SYN, ACK] Seq=0 Ack=1 Win=17898 Len=0 MSS=1460 SACK_PERM=1 TSval=1425205591 TSecr=4294935914 WS=…
   31 14.056414007  192.168.1.100   52.26.2.199     TCP       66 34184→443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=4294936052 TSecr=1425205591
   33 14.189775666  91.189.90.41    192.168.1.100   TCP       66 80→60572 [FIN, ACK] Seq=1 Ack=2 Win=14592 Len=0 TSval=3060719843 TSecr=4294936000
   34 14.189801859  192.168.1.100   91.189.90.41    TCP       66 60572→80 [ACK] Seq=2 Ack=2 Win=29312 Len=0 TSval=4294936085 TSecr=3060719843
   35 14.381461536  52.26.2.199     192.168.1.100   TCP       66 443→34184 [ACK] Seq=1 Ack=203 Win=15872 Len=0 TSval=1425205789 TSecr=4294936052
   37 14.382728667  192.168.1.100   52.26.2.199     TCP       66 34184→443 [ACK] Seq=203 Ack=1449 Win=32128 Len=0 TSval=4294936133 TSecr=1425205789
   38 14.383638855  52.26.2.199     192.168.1.100   TCP     1514 [TCP segment of a reassembled PDU]
```

```
▸ Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: HonHaiPr_dc:72:5d (14:2d:27:dc:72:5d), Dst: Tp-LinkT_54:ef:8c (30:b5:c2:54:ef:8c)
▸ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 91.189.90.41
▸ Transmission Control Protocol, Src Port: 60572, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  30 b5 c2 54 ef 8c 14 2d  27 dc 72 5d 08 00 45 00   0..T...- '.r]..E.
0010  00 3c 23 c5 40 00 40 06  9f 04 c0 a8 01 64 5b bd   .<#.@.@. .....d[.
0020  5a 29 ec 9c 00 50 79 80  5c 05 00 00 00 00 a0 02   Z)...Py. \.......
0030  72 10 1b ca 00 00 02 04  05 b4 04 02 08 0a ff ff   r....... ........
0040  7f c0 00 00 00 00 01 03  03 07                     ........ ..
```

wireshark_wlan0_20170125142627_hT0ylb | Packets: 1201 · Displayed: 536 (44.6%) | Profile: Default

Exercise 2.4

A's IP address is set to 192.168.123.1 and B's IP address is set to 192.168.123.2 through GUI. Netmask is set to 255.255.255.0, gateway in B is set to 192.168.123.1 and dns in B is set to 10.6.0.11.

Following are the commands used in A to allow packet forwarding:-

1. sudo echo 1 > /proc/sys/net/ipv4/ip_forward
   This command is used to enable IP forwarding.

2. sudo iptables -t nat -A POSTROUTING --out-interface wlan0 -j MASQUERADE
   This command is used to set the outgoing interface for ip forwarding. Here it is set to wlan0.

3. sudo iptables -A FORWARD --in-interface eth0 -j ACCEPT
   This command is used to set the incoming interface for ip forwarding. Here it is set to eth0.

Exercise 3.2

1. Abhik 10.6.15.92 and Bob 10.22.21.249. First message is "Hi Abhik!" and last message is ":)".

2. The file is splitted into 10 packets. The type of the file is jpeg.

3. Watch Dogs is the game, Bob was taking about.