

ASSIGNMENT 2 EECS 3214 – Winter 2021

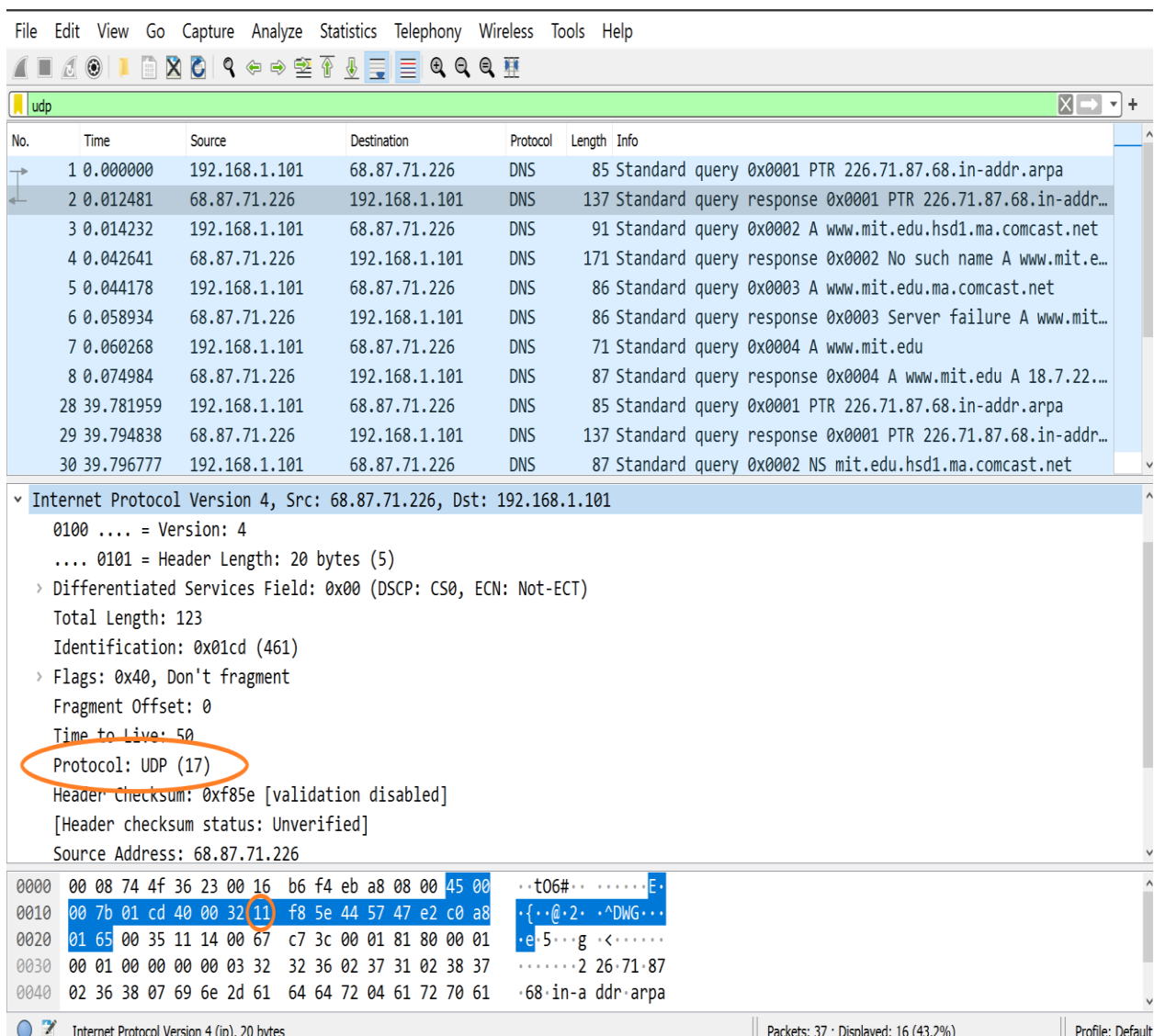
Name – Prit Amin

Student ID – 216831232

1) IP number for UDP

Decimal = 17

Hexadecimal = 000x11



Wireshark packet capture showing a DNS query and response. The packet list shows a query from 192.168.1.101 to 68.87.71.226. The packet details show the UDP header with the protocol set to 17 (UDP). The packet bytes show the UDP header with the destination port 11 (00000011 in hex).

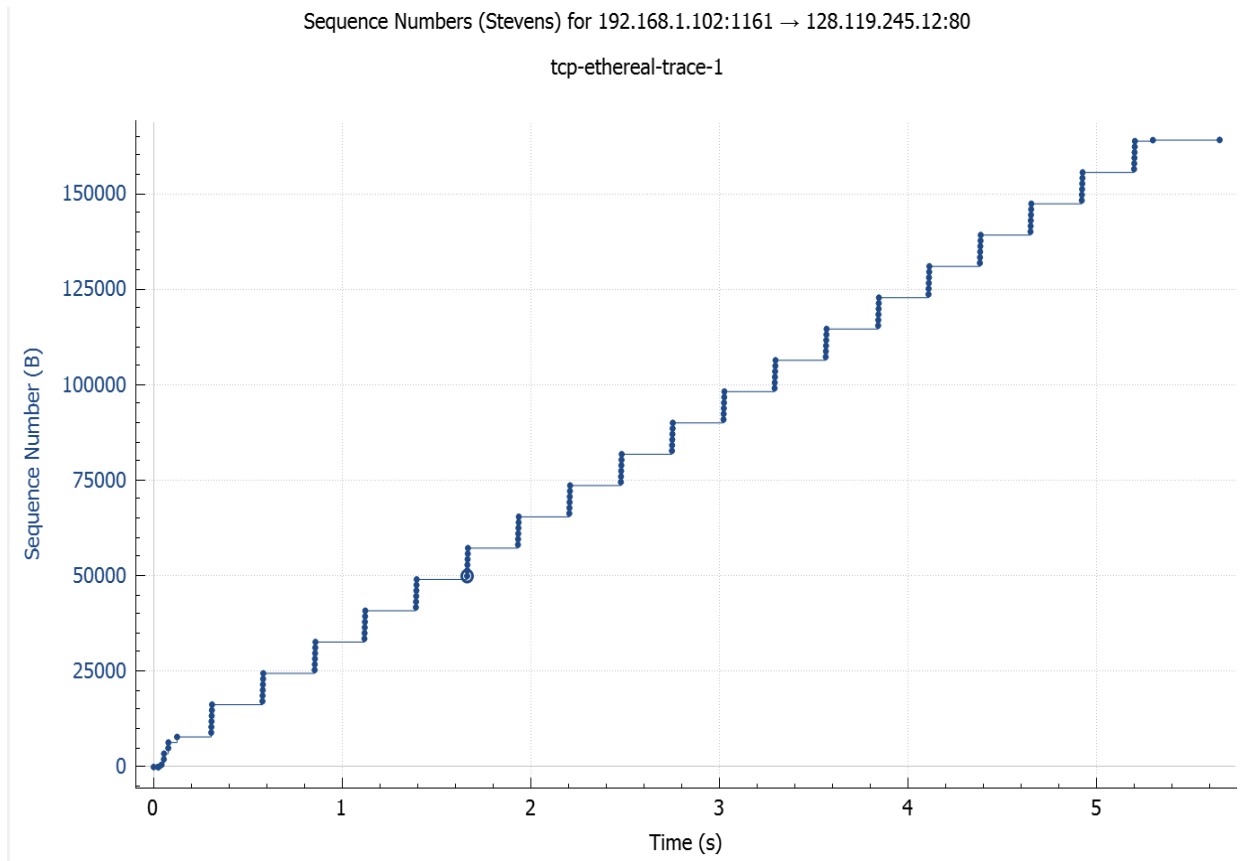
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
2	0.012481	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0x0001 PTR 226.71.87.68.in-addr...
3	0.014232	192.168.1.101	68.87.71.226	DNS	91	Standard query 0x0002 A www.mit.edu.hsd1.ma.comcast.net
4	0.042641	68.87.71.226	192.168.1.101	DNS	171	Standard query response 0x0002 No such name A www.mit.e...
5	0.044178	192.168.1.101	68.87.71.226	DNS	86	Standard query 0x0003 A www.mit.edu.ma.comcast.net
6	0.058934	68.87.71.226	192.168.1.101	DNS	86	Standard query response 0x0003 Server failure A www.mit...
7	0.060268	192.168.1.101	68.87.71.226	DNS	71	Standard query 0x0004 A www.mit.edu
8	0.074984	68.87.71.226	192.168.1.101	DNS	87	Standard query response 0x0004 A www.mit.edu A 18.7.22...
28	39.781959	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
29	39.794838	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0x0001 PTR 226.71.87.68.in-addr...
30	39.796777	192.168.1.101	68.87.71.226	DNS	87	Standard query 0x0002 NS mit.edu.hsd1.ma.comcast.net

Internet Protocol Version 4, Src: 68.87.71.226, Dst: 192.168.1.101

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 123
- Identification: 0x01cd (461)
- > Flags: 0x40, Don't fragment
- Fragment Offset: 0
- Time to Live: 50
- Protocol: UDP (17)
- Header Checksum: 0xf85e [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 68.87.71.226

0000 00 08 74 4f 36 23 00 16 b6 f4 eb a8 08 00 45 00 ..tO6#.. ..E.
0010 00 7b 01 cd 40 00 32 11 f8 5e 44 57 47 e2 c0 a8 .{..@.2. ^DWG..
0020 01 65 00 35 11 14 00 67 c7 3c 00 01 81 80 00 01 .e.5...g .<.....
0030 00 01 00 00 00 00 03 32 32 36 02 37 31 02 38 372 26.71.87
0040 02 36 38 07 69 6e 2d 61 64 64 72 04 61 72 70 61 .68.in-a ddr.arpa

2A) As we can see there is no linear growth in the graph. First, there is slow start for about 1.5 seconds and then slope increases gradually. These shows packets are transmitted in some amount.



2B) 14th Bytes shows segment type in TCP header.

2C) SYN

Binary Data – 00000010

Hexadecimal – 000x02

```
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0
Source Port: 1161
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 232129012
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0111 .... = Header Length: 28 bytes (7)
Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Not set
.... .... 0... = Push: Not set
.... .... .0.. = Reset: Not set
> .... .... ..1. = Syn: Set
.... .... ...0 = Fin: Not set
[TCP Flags: .....S.]
Window: 16384
[Calculated window size: 16384]
Checksum: 0xf6e9 [unverified]
[Checksum Status: Unverified]

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00  .%.s. .p..E.
0010 00 30 1e 1d 40 00 80 06 a5 18 c0 a8 01 66 80 77  .0.@... ..f.w
0020 f5 0c 04 89 00 50 0d d6 01 f4 00 00 00 00 70 02  ....P. ....p.
0030 40 00 f6 e9 00 00 02 04 05 b4 01 01 04 02  @.....
```

ACK

Binary Data – 00010000

Hexadecimal – 000x10

```

> Frame 8: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 178.119.245.12
< Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 3486, Ack: 1, Len: 1460
  Source Port: 1161
  Destination Port: 80
  [Stream index: 0]
  [TCP Segment Len: 1460]
  Sequence Number: 3486 (relative sequence number)
  Sequence Number (raw): 232132498
  [Next Sequence Number: 4946 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 883061786
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x010 (ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    .... 0... = Congestion Window Reduced (CWR): Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  [TCP Flags: .....A....]
0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00  .%.s. .p...E.
0010 05 dc 1e 24 40 00 80 06 9f 65 c0 a8 01 66 80 77  ...$@... .e...f.w
0020 f5 0c 04 89 00 50 0d d6 0f 92 34 a2 74 1a 50 10  ....P...4.t.P.
0030 44 70 dd 01 00 00 20 73 6f 6d 65 20 65 69 67 58  Dp... s ome eigh
0040 74 20 74 65 78 74 0d 0a 66 69 6c 65 73 20 70 65  t text.. files pe
0050 72 20 6d 6f 6e 74 68 3a 20 20 74 68 75 73 20 75  r month: thus u

```

ACK-PSH

Binary Data – 00011000

Hexadecimal – 000x18

```

> Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
< Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 1, Ack: 1, Len: 565

```

```

Source Port: 1161
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 565]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 232129013
[Next Sequence Number: 566 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 883061786
0101 .... = Header Length: 20 bytes (5)

```

```

v Flags: 0x018 (PSH, ACK)
 000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 .... = Acknowledgment: Set
.... .... 1... = Push: Set
.... ..... 0... = Reset: Not set
.... ..... ..0. = Syn: Not set
.... ..... ...0 = Fin: Not set
[TCP Flags: .....AP...]

```

```

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00  ..%.S. .p..E.
0010 02 5d 1e 21 40 00 80 06 a2 e7 c0 a8 01 66 80 77  .]!@... ..f.w
0020 f5 0c 04 89 00 50 0d d6 01 f5 34 a2 74 1a 50 18  ....P... .4.t.P.
0030 44 70 1f bd 00 00 50 4f 53 54 20 2f 65 74 68 65  Dp...PO ST /ethe
0040 72 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 33 2d 31  real-lab s/lab3-1

```

SYN-ACK

Binary Data – 00010010

Hexadecimal – 000x12

```
> Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
v Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 1161
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence Number: 0 (relative sequence number)
    Sequence Number (raw): 883061785
    [Next Sequence Number: 1 (relative sequence number)]
    Acknowledgment Number: 1 (relative ack number)
    Acknowledgment number (raw): 232129013
    0111 .... = Header Length: 28 bytes (7)
v Flags: 0x012 (SYN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ....0... = Congestion Window Reduced (CWR): Not set
    ....0... = ECN-Echo: Not set
    ....0... = Urgent: Not set
    ....1... = Acknowledgment: Set
    ....0... = Push: Not set
    ....0... = Reset: Not set
    ....1... = Syn: Set
    ....0... = Fin: Not set
    [TCP Flags: .....A..S.]

0000 00 20 e0 8a 70 1a 00 06 25 da af 73 08 00 45 00  . . .p . . % . .s . .E .
0010 00 30 00 00 40 00 37 06 0c 36 80 77 f5 0c c0 a8  .0 . .@ .7 . .6 .w . . .
0020 01 66 00 50 04 89 34 a2 74 19 0d d6 01 f5 70 12  .f .P . .4 . t . . . . .p .
0030 16 d0 77 4d 00 00 02 04 05 b4 01 01 04 02  . .wM . . . . . . . . . .
```

FIN

Binary data – 00000001

Hexadecimal – 000x01