

Xueyang (Sean) Wang
XW1154
02/24/2017
CS4793
Homework 03

*For this homework, I used the .zip file (http-ethereal-trace-5) downloaded from the website

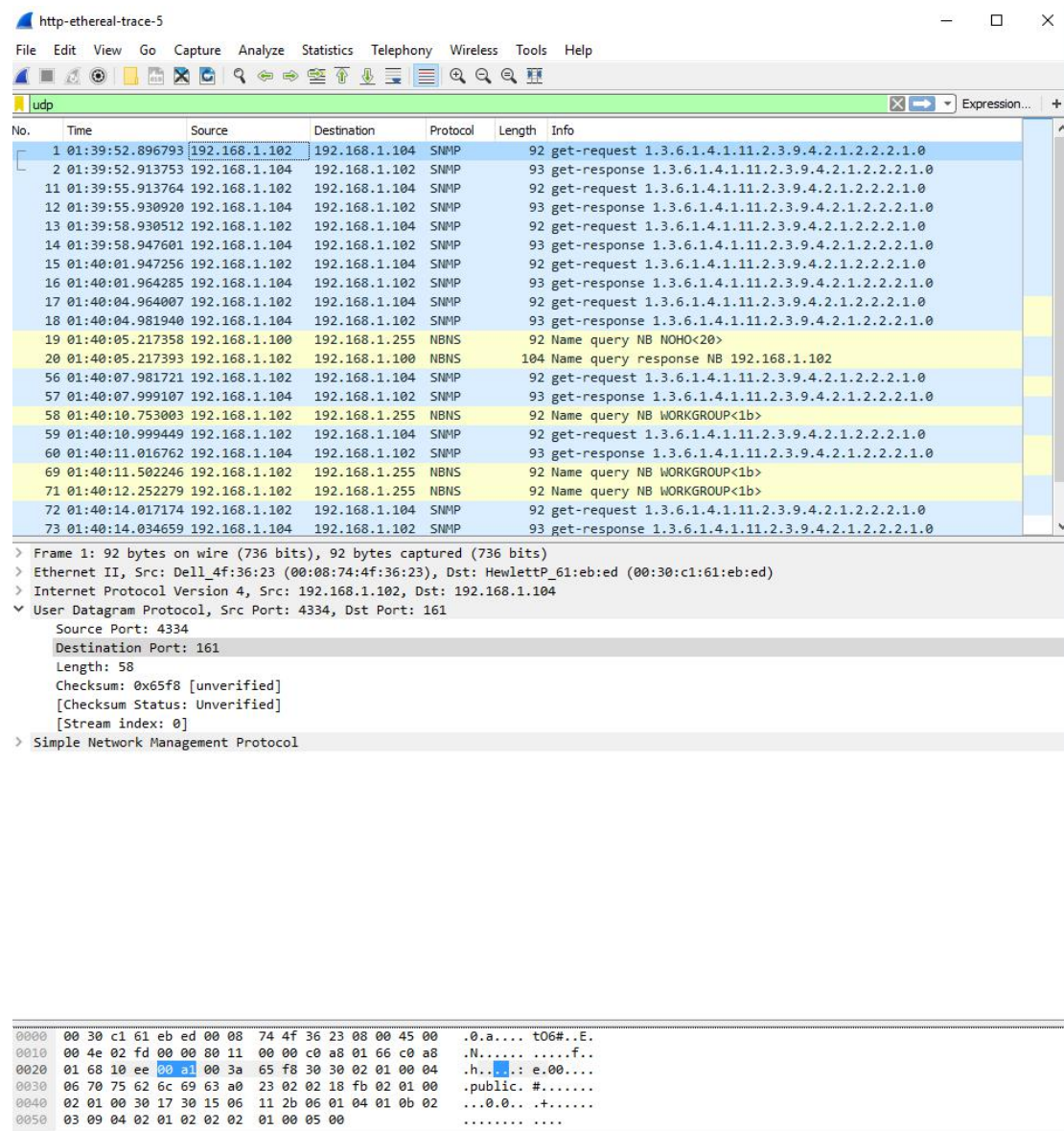


Figure 1. Wireshark UDP file

1. The UDP header contains 4 fields: source port, destination port, length, and checksum.
2. Each of the UDP header fields is 2 bytes long.
3. The value in the length field is the sum of the 8 header bytes. In the example, the length is 58.
4. The maximum number of bytes in a UDP payload is $2^{16} - 1$ less the header bytes, which equals to $65535 - 8 = 65527$ bytes.
5. The largest possible port number is $2^{16} - 1 = 65535$.

```

✓ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 78
    Identification: 0x02fd (765)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 128
  Protocol: UDP (17)
  Header checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.1.102
  Destination: 192.168.1.104

```

Figure 2. UDP protocol

6. The UDP protocol is 0x11(hex), which is 17 in decimal value.

```

> Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: HewlettP_61:eb:ed (00:30:c1:61:eb:ed)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
✓ User Datagram Protocol, Src Port: 4334, Dst Port: 161
  Source Port: 4334
  Destination Port: 161
  Length: 58
  Checksum: 0x65f8 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
> Simple Network Management Protocol

```

```

0000 00 30 c1 61 eb ed 00 08 74 4f 36 23 08 00 45 00 .0.a....t06#...E.
0010 00 4e 02 fd 00 00 00 11 00 00 c0 a8 01 66 c0 a8 .N.....f..
0020 01 68 10 ea 00 a1 00 3a 65 f8 30 30 02 01 00 04 .h....e.00...
0030 06 70 75 62 6c 69 63 a0 23 02 02 18 fb 02 01 00 .public.#.....
0040 02 01 00 30 17 30 15 06 11 2b 06 01 04 01 0b 02 ...0.0..+.....
0050 03 09 04 02 01 02 02 02 01 00 05 00 .....

```

Figure 3. Sending

```

> Frame 2: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
> Ethernet II, Src: HewlettP_61:eb:ed (00:30:c1:61:eb:ed), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.102
✓ User Datagram Protocol, Src Port: 161, Dst Port: 4334
  Source Port: 161
  Destination Port: 4334
  Length: 59
  Checksum: 0x53f2 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
> Simple Network Management Protocol

```

```

0000 00 08 74 4f 36 23 00 30 c1 61 eb ed 08 00 45 00 ..t06#.0.a....E.
0010 00 4f ed a2 00 00 3c 11 0c dd c0 a8 01 68 c0 a8 .O....<.....h..
0020 01 66 00 a1 10 ea 00 3b 53 f2 30 31 02 01 00 04 .f.;S.01....
0030 06 70 75 62 6c 69 63 a2 24 02 02 18 fb 02 01 00 .public.$.....
0040 02 01 00 30 18 30 16 06 11 2b 06 01 04 01 0b 02 ...0.0..+.....
0050 03 09 04 02 01 02 02 02 01 00 04 01 10 .....

```

Figure 4. Receiving

7. The source port of the UDP packet sent is the same as the destination port of the reply packet, and the destination port of the UDP packet sent is the same as the source port of the reply packet.