Excercise 5 Rendell Cale, February 24, 2018

1

The echo request was sent from src 192.168.1.102 to dst 128.59.23.100, so the clients IP address was 192.168.1.102.

```
▶ Frame 10: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▶ Ethernet II, Src: PremaxPe_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:
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d1 (13009)
   ▶ Flags: 0x00
    Fragment offset: 0
  ▶ Time to live: 2
    Protocol: ICMP (1)
    Header checksum: 0x2c2b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Cource Coott: Unknown]
0000 00 06 25 da af 73 00 20
                                e0 8a 70 1a 08 00 45
                                                           ..%..s. ..p...
0010
      17 64 08 00 f6 ca 03 00
0020
                                51 03 37 32 20 aa aa aa
                                                            d..... Q.72 ...
      aa aa aa aa aa aa
                                aa aa aa aa aa aa aa
                                                           . . . . . . . . . . . . . . . . .
      aa aa aa aa aa aa aa
                                aa aa aa aa aa aa aa
      aa aa aa aa aa aa
                                aa aa aa aa aa aa
                                                           . . . . . . . . . . . . . . . . . . .

○ Internet Protocol Version 4 (ip). 20 bytes
```

$\mathbf{2}$

Clicking on the the message and pressing the Internet Protocol Version 4 tab highlights the header bytes. Counting them up show that the IPv4 header has $\underline{20}$ bytes, which corresponds well with what we would expect. This is also illustrated by the screenshot above.

3

The IP datagram has a payload of size 64 bytes which is the ICMP.

```
Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf6ca [correct]
    [Checksum Status: Good]
    Identifier (BE): 768 (0x0300)
    Identifier (LE): 3 (0x0003)
    Sequence number (BE): 20739 (0x5103)
    Sequence number (LE): 849 (0x0351)
  ▶ [No response seen]
  ▶ Data (56 bytes)
      00 54 32 d1 00 00 02 01
                                2c 2b c0 a8 01 66 80 3b
0020
      17 64 08 00 f6 ca 03
                                                            .d
0040
0050
                                aa aa aa aa aa aa aa
       aa aa aa aa aa aa aa
0060
O Month Internet Control Message Protocol (icmp), 64 bytes
```

4

The IP header has none of the flags set and a fragmentation offset equal to zero. Thus the packet was <u>not fragmenteed</u>. This makes sense since the payload is quite small, and it is using ethernet.

5

In the IP header we see that the fields "Identification", "Time to live", and of course "Header checksum" always change. In the ICMP part we see that the two sequence numbers (BE and LE) change, and also the chacksum.

6

In the header, the most interesting contant fields are source, destination, but note also that the vesion field, header length, differentiated services field, flags, and protocol fields are also constant. The total length and fragment offset does change but infrequently.

In the ICMP, the type is consistently 8 (Echo (ping) request) and code is 0. The identifiers also never change for both BE and LE.

7

The value in the identification field is ??

8

TTL value is 255.