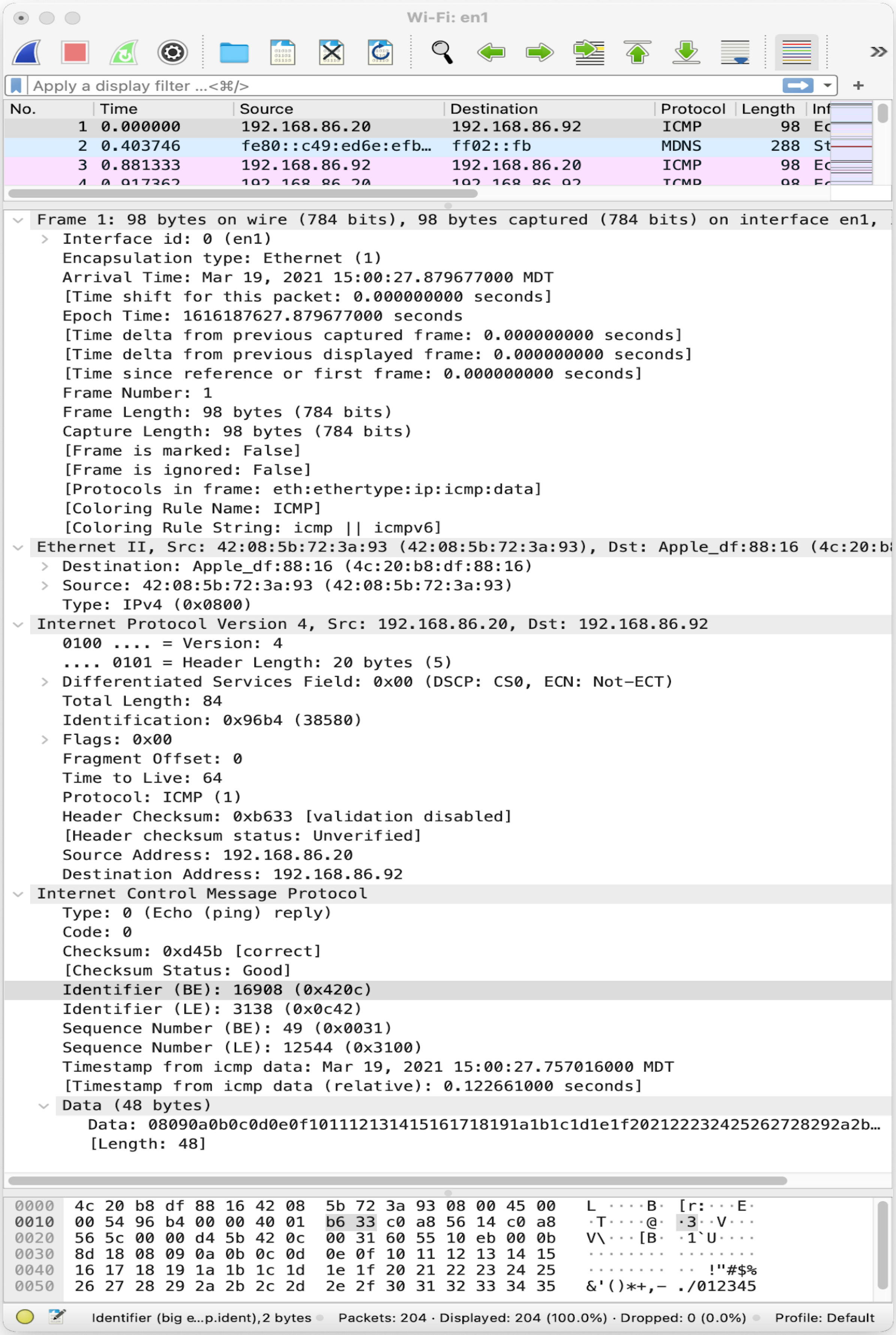
Ali Serdar Aydogdu
CS 2600 - X01
Lab 3
3/19/2021

Lab Exercise 3: Wireshark Installation and Introduction

1. The frame length of an ICMP Echo Request is 98 bytes.
2. The Ethernet MAC addresses of the source and destination:
   Destination: 4c:20:b8:df:88:16
   Source: 42:08:5b:72:3a:93
3. My computer is a 2020 M1 Mac mini. The source does not have a manufacturer name. I also checked the IEEE database and it is also not there yet.
   Source: 42:08:5b:72:3a:93 (42:08:5b:72:3a:93)
4. Type: IPv4 (0x0800)
5. 0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
6. The IP addresses of the source and destination:
   Source Address: 192.168.86.20
   Destination Address: 192.168.86.92
7. The ICMP Tyoe numbers for request and reply:
   Type: 8 (Echo (ping) request)
   Type: 0 (Echo (ping) reply)
8. See page 2 for the screenshot



```
No.   Time       Source                   Destination      Protocol  Length  Inf
    1 0.000000   192.168.86.20            192.168.86.92    ICMP          98  Ec
    2 0.403746   fe80::c49:ed6e:efb…      ff02::fb         MDNS         288  St
    3 0.881333   192.168.86.92            192.168.86.20    ICMP          98  Ec
    4 0.917362   192.168.86.20            192.168.86.92    ICMP          98  Ec
```

```
∨ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en1,
  > Interface id: 0 (en1)
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 19, 2021 15:00:27.879677000 MDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1616187627.879677000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 98 bytes (784 bits)
    Capture Length: 98 bytes (784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
∨ Ethernet II, Src: 42:08:5b:72:3a:93 (42:08:5b:72:3a:93), Dst: Apple_df:88:16 (4c:20:b
  > Destination: Apple_df:88:16 (4c:20:b8:df:88:16)
  > Source: 42:08:5b:72:3a:93 (42:08:5b:72:3a:93)
    Type: IPv4 (0x0800)
∨ Internet Protocol Version 4, Src: 192.168.86.20, Dst: 192.168.86.92
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x96b4 (38580)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xb633 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.20
    Destination Address: 192.168.86.92
∨ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xd45b [correct]
    [Checksum Status: Good]
    Identifier (BE): 16908 (0x420c)
    Identifier (LE): 3138 (0x0c42)
    Sequence Number (BE): 49 (0x0031)
    Sequence Number (LE): 12544 (0x3100)
    Timestamp from icmp data: Mar 19, 2021 15:00:27.757016000 MDT
    [Timestamp from icmp data (relative): 0.122661000 seconds]
  ∨ Data (48 bytes)
      Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b…
      [Length: 48]
```

```
0000  4c 20 b8 df 88 16 42 08  5b 72 3a 93 08 00 45 00   L ····B· [r:···E·
0010  00 54 96 b4 00 00 40 01  b6 33 c0 a8 56 14 c0 a8   ·T····@· ·3··V···
0020  56 5c 00 00 d4 5b 42 0c  00 31 60 55 10 eb 00 0b   V\···[B· ·1`U····
0030  8d 18 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
```

Identifier (big e...p.ident),2 bytes · Packets: 204 · Displayed: 204 (100.0%) · Dropped: 0 (0.0%) · Profile: Default