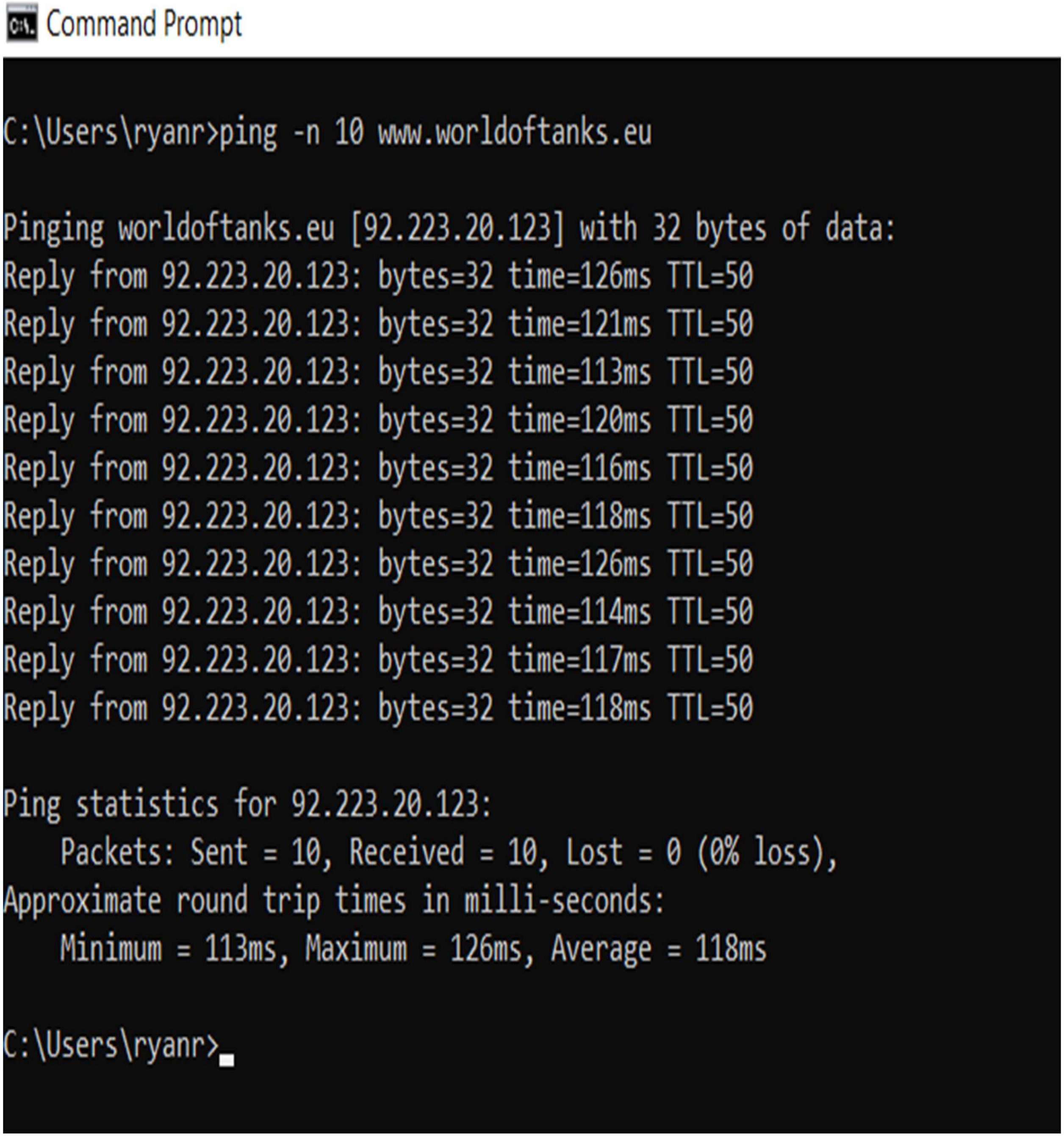
COMP-3670 Lab 4 - Wireshark Lab: ICMP v7.0 Questions 1-4

Ryan Raffoul

104834358

See the screenshots below for the command line when running ping and the Wireshark trace for this command.

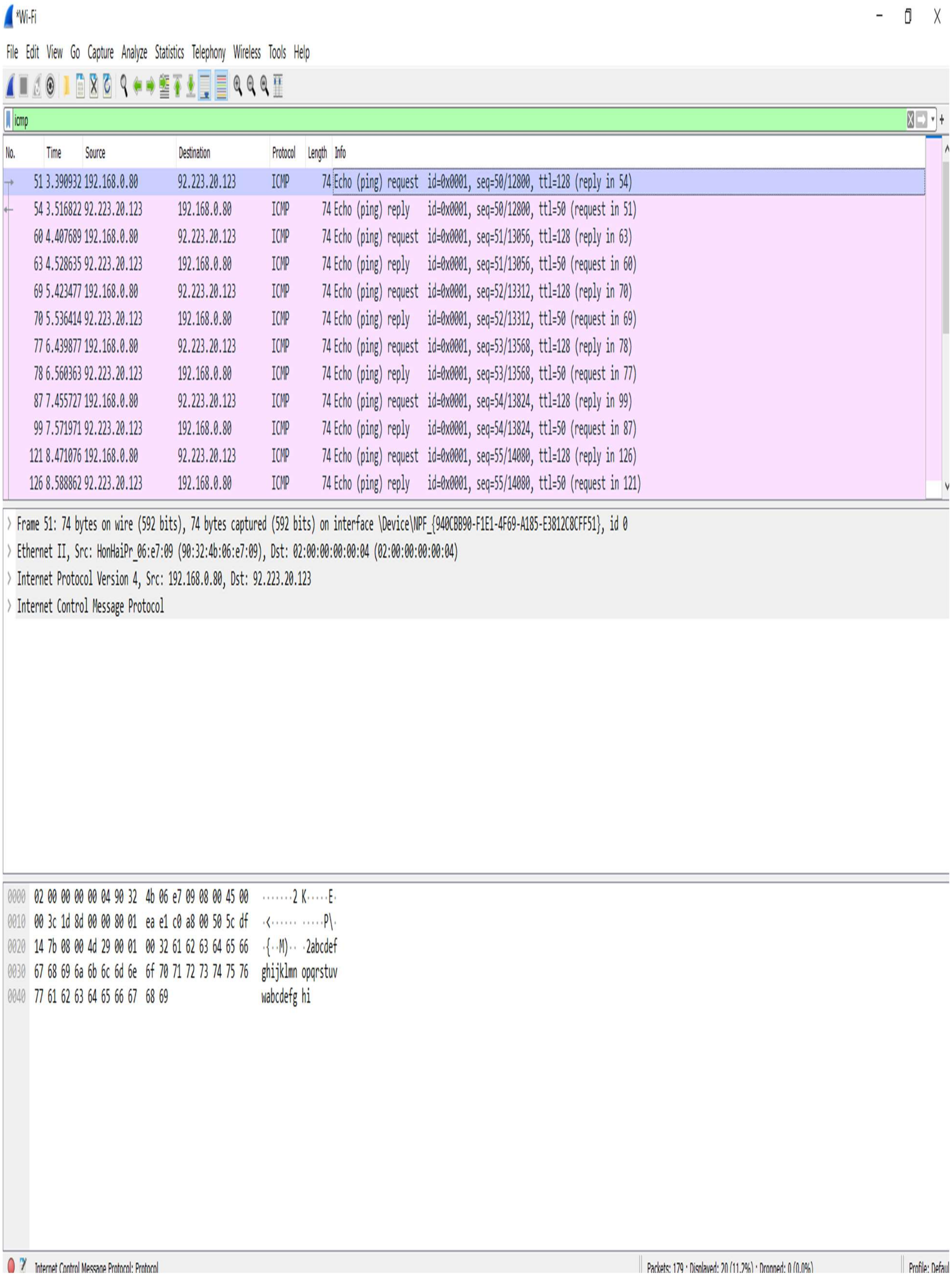


```
C:\Users\ryanr>ping -n 10 www.worldoftanks.eu

Pinging worldoftanks.eu [92.223.20.123] with 32 bytes of data:
Reply from 92.223.20.123: bytes=32 time=126ms TTL=50
Reply from 92.223.20.123: bytes=32 time=121ms TTL=50
Reply from 92.223.20.123: bytes=32 time=113ms TTL=50
Reply from 92.223.20.123: bytes=32 time=120ms TTL=50
Reply from 92.223.20.123: bytes=32 time=116ms TTL=50
Reply from 92.223.20.123: bytes=32 time=118ms TTL=50
Reply from 92.223.20.123: bytes=32 time=126ms TTL=50
Reply from 92.223.20.123: bytes=32 time=114ms TTL=50
Reply from 92.223.20.123: bytes=32 time=117ms TTL=50
Reply from 92.223.20.123: bytes=32 time=118ms TTL=50

Ping statistics for 92.223.20.123:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 113ms, Maximum = 126ms, Average = 118ms

C:\Users\ryanr>
```



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
51	3.390932	192.168.0.80	92.223.20.123	ICMP	74	Echo (ping) request id=0x0001, seq=50/12800, ttl=128 (reply in 54)
54	3.516822	92.223.20.123	192.168.0.80	ICMP	74	Echo (ping) reply id=0x0001, seq=50/12800, ttl=50 (request in 51)
60	4.407689	192.168.0.80	92.223.20.123	ICMP	74	Echo (ping) request id=0x0001, seq=51/13056, ttl=128 (reply in 63)
63	4.528635	92.223.20.123	192.168.0.80	ICMP	74	Echo (ping) reply id=0x0001, seq=51/13056, ttl=50 (request in 60)
69	5.423477	192.168.0.80	92.223.20.123	ICMP	74	Echo (ping) request id=0x0001, seq=52/13312, ttl=128 (reply in 70)
70	5.536414	92.223.20.123	192.168.0.80	ICMP	74	Echo (ping) reply id=0x0001, seq=52/13312, ttl=50 (request in 69)
77	6.439877	192.168.0.80	92.223.20.123	ICMP	74	Echo (ping) request id=0x0001, seq=53/13568, ttl=128 (reply in 78)
78	6.560363	92.223.20.123	192.168.0.80	ICMP	74	Echo (ping) reply id=0x0001, seq=53/13568, ttl=50 (request in 77)
87	7.455727	192.168.0.80	92.223.20.123	ICMP	74	Echo (ping) request id=0x0001, seq=54/13824, ttl=128 (reply in 99)
99	7.571971	92.223.20.123	192.168.0.80	ICMP	74	Echo (ping) reply id=0x0001, seq=54/13824, ttl=50 (request in 87)
121	8.471076	192.168.0.80	92.223.20.123	ICMP	74	Echo (ping) request id=0x0001, seq=55/14080, ttl=128 (reply in 126)
126	8.588862	92.223.20.123	192.168.0.80	ICMP	74	Echo (ping) reply id=0x0001, seq=55/14080, ttl=50 (request in 121)

```
> Frame 51: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{940CBB90-F1E1-4F69-A185-E3812C8CFF51}, id 0
> Ethernet II, Src: HonHaiPr_06:e7:09 (90:32:4b:06:e7:09), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
> Internet Protocol Version 4, Src: 192.168.0.80, Dst: 92.223.20.123
> Internet Control Message Protocol
```

```
0000  02 00 00 00 00 04 90 32  4b 06 e7 09 08 00 45 00   ·······2 K·····E·
0010  00 3c 1d 8d 00 00 80 01  ea e1 c0 a8 00 50 5c df   ·<······ ·····P\·
0020  14 7b 08 00 4d 29 00 01  00 32 61 62 63 64 65 66   ·{··M)·· ·2abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

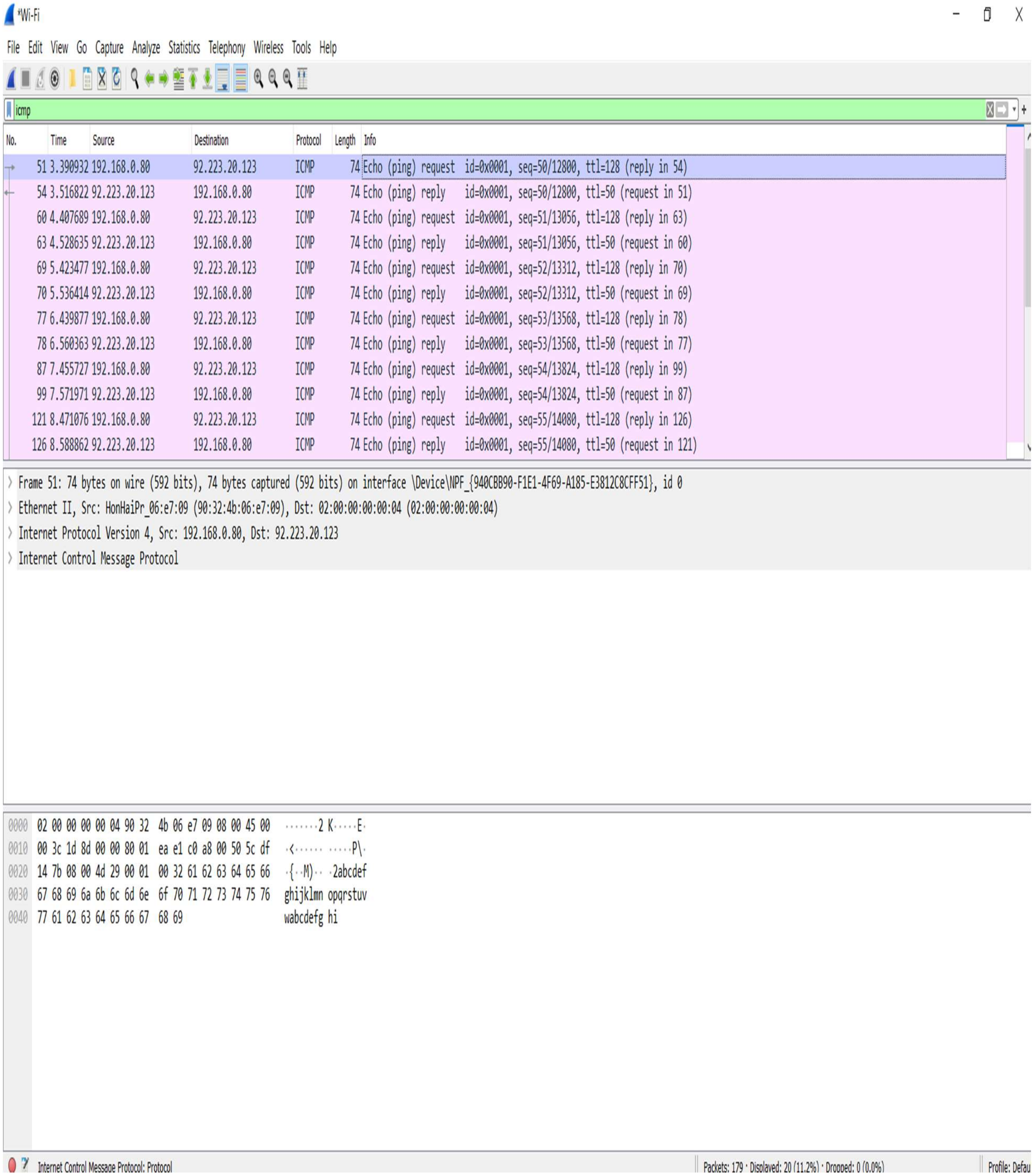
Internet Control Message Protocol: Protocol

Packets: 179 · Displayed: 20 (11.2%) · Dropped: 0 (0.0%)

Profile: Defaul

1. The IP Address of my host is 192.168.0.80.

The IP Address of the destination host is 92.223.20.123.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

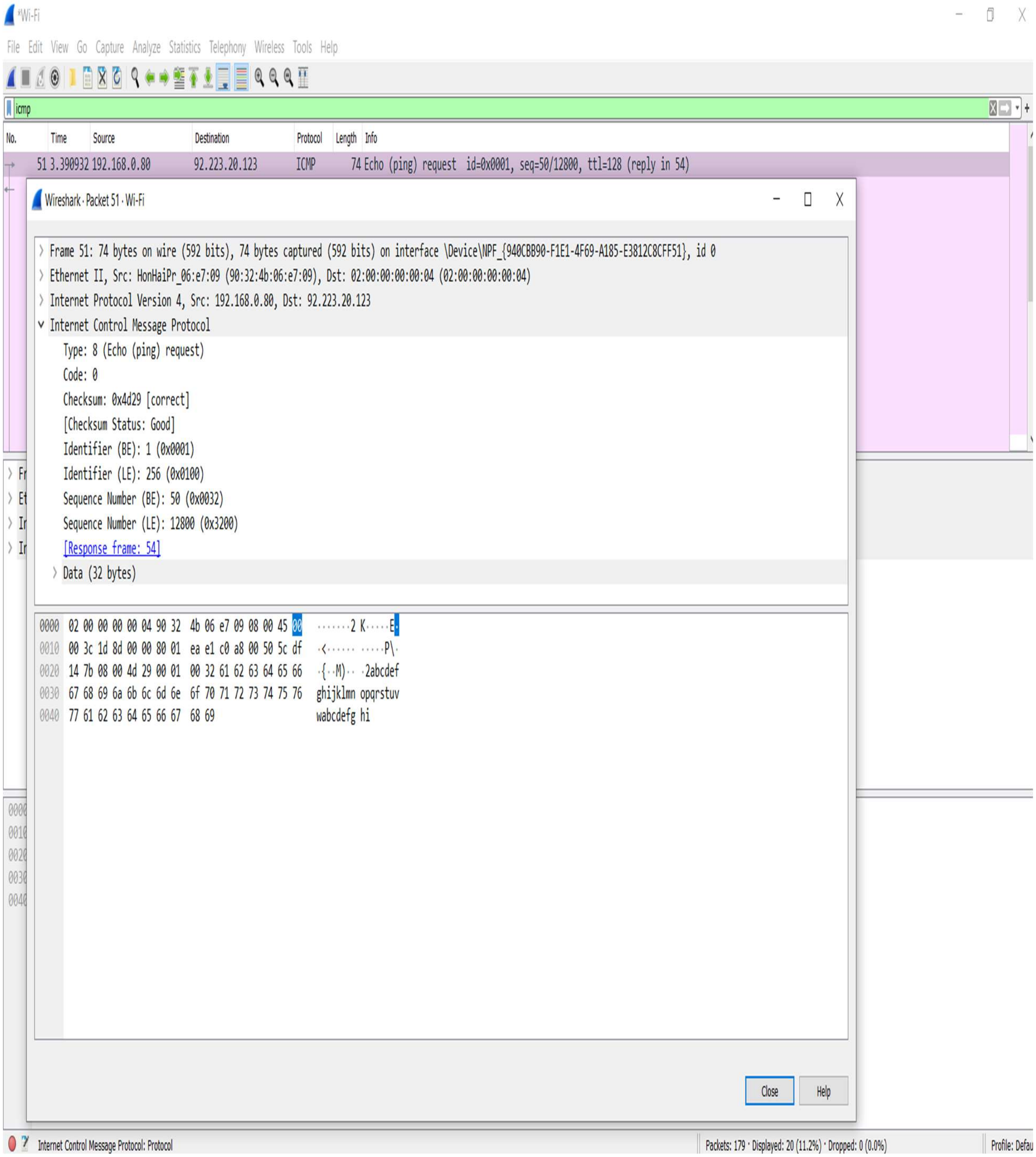
No.	Time	Source	Destination	Protocol	Length	Info
51	3.390932	192.168.0.80	92.223.20.123	ICMP	74	Echo (ping) request id=0x0001, seq=50/12800, ttl=128 (reply in 54)
54	3.516822	92.223.20.123	192.168.0.80	ICMP	74	Echo (ping) reply id=0x0001, seq=50/12800, ttl=50 (request in 51)
60	4.407689	192.168.0.80	92.223.20.123	ICMP	74	Echo (ping) request id=0x0001, seq=51/13056, ttl=128 (reply in 63)
63	4.528635	92.223.20.123	192.168.0.80	ICMP	74	Echo (ping) reply id=0x0001, seq=51/13056, ttl=50 (request in 60)
69	5.423477	192.168.0.80	92.223.20.123	ICMP	74	Echo (ping) request id=0x0001, seq=52/13312, ttl=128 (reply in 70)
70	5.536414	92.223.20.123	192.168.0.80	ICMP	74	Echo (ping) reply id=0x0001, seq=52/13312, ttl=50 (request in 69)
77	6.439877	192.168.0.80	92.223.20.123	ICMP	74	Echo (ping) request id=0x0001, seq=53/13568, ttl=128 (reply in 78)
78	6.560363	92.223.20.123	192.168.0.80	ICMP	74	Echo (ping) reply id=0x0001, seq=53/13568, ttl=50 (request in 77)
87	7.455727	192.168.0.80	92.223.20.123	ICMP	74	Echo (ping) request id=0x0001, seq=54/13824, ttl=128 (reply in 99)
99	7.571971	92.223.20.123	192.168.0.80	ICMP	74	Echo (ping) reply id=0x0001, seq=54/13824, ttl=50 (request in 87)
121	8.471076	192.168.0.80	92.223.20.123	ICMP	74	Echo (ping) request id=0x0001, seq=55/14080, ttl=128 (reply in 126)
126	8.588862	92.223.20.123	192.168.0.80	ICMP	74	Echo (ping) reply id=0x0001, seq=55/14080, ttl=50 (request in 121)

```
> Frame 51: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{940CBB90-F1E1-4F69-A185-E3812C8CFF51}, id 0
> Ethernet II, Src: HonHaiPr_06:e7:09 (90:32:4b:06:e7:09), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
> Internet Protocol Version 4, Src: 192.168.0.80, Dst: 92.223.20.123
> Internet Control Message Protocol
```

```
0000  02 00 00 00 00 04 90 32  4b 06 e7 09 08 00 45 00   ·······2 K·····E·
0010  00 3c 1d 8d 00 00 80 01  ea e1 c0 a8 00 50 5c df   ·<······ ·····P\·
0020  14 7b 08 00 4d 29 00 01  00 32 61 62 63 64 65 66   ·{··M)·· ·2abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Internet Control Message Protocol: Protocol | Packets: 179 · Displayed: 20 (11.2%) · Dropped: 0 (0.0%) | Profile: Defau

2. The ICMP packet does not have source and destination port numbers because it communicates network-layer information between hosts and routers, not between the application layer processes. Each ICMP packet has a “Type” and “Code”. This combo identifies the specific message being received. Since the network software itself interprets all ICMP messages, no port numbers are needed to direct the ICMP message to an application layer process.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 51 · Wi-Fi
Close
Help

Filter: icmp

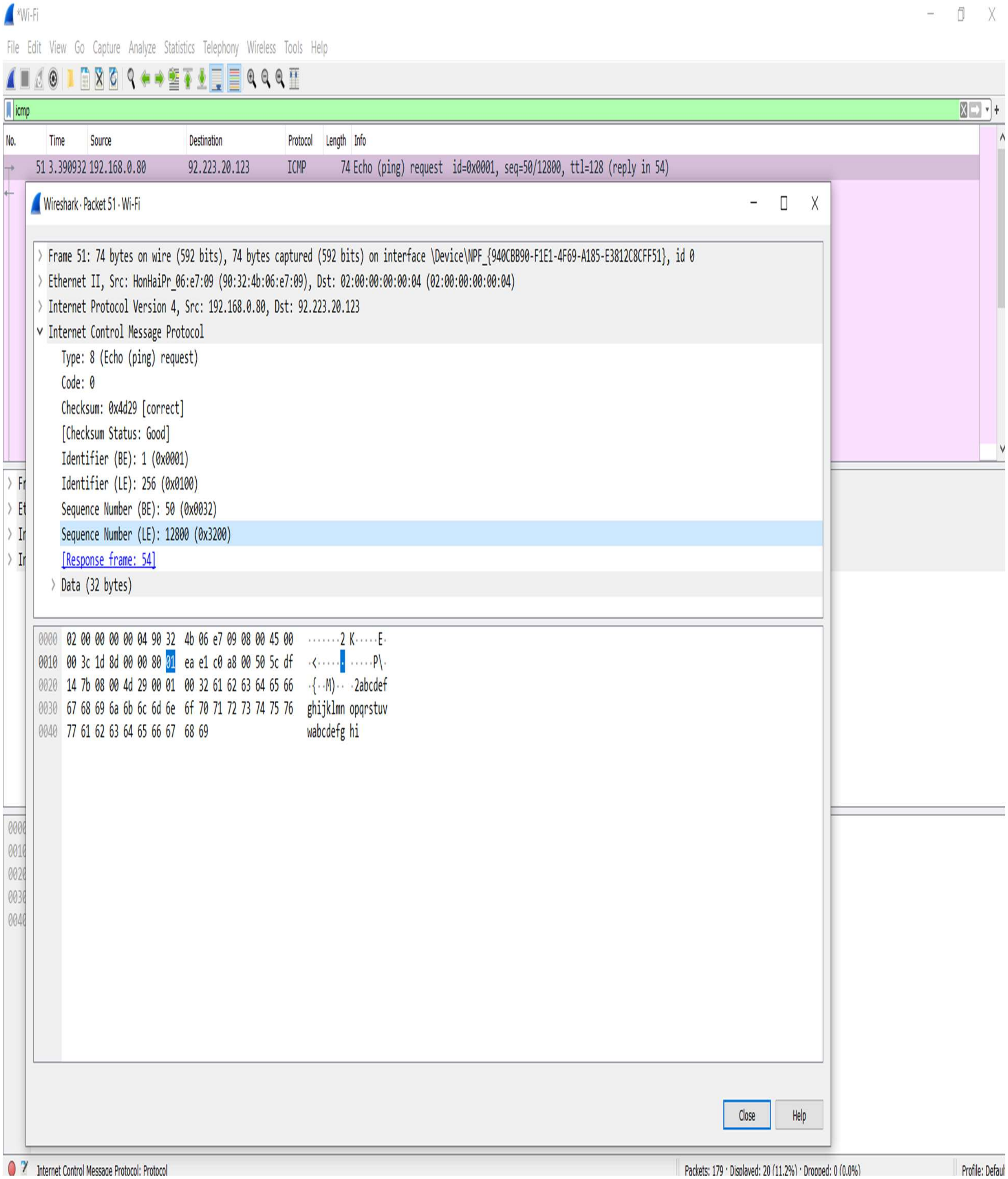
```
No.  Time     Source        Destination   Protocol Length Info
  51 3.390932 192.168.0.80  92.223.20.123 ICMP         74 Echo (ping) request  id=0x0001, seq=50/12800, ttl=128 (reply in 54)
```

```
> Frame 51: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{940CBB90-F1E1-4F69-A185-E3812C8CFF51}, id 0
> Ethernet II, Src: HonHaiPr_06:e7:09 (90:32:4b:06:e7:09), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
> Internet Protocol Version 4, Src: 192.168.0.80, Dst: 92.223.20.123
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d29 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 50 (0x0032)
    Sequence Number (LE): 12800 (0x3200)
    [Response frame: 54]
  > Data (32 bytes)
```

```
0000  02 00 00 00 00 04 90 32  4b 06 e7 09 08 00 45 00   ·······2 K·····E·
0010  00 3c 1d 8d 00 00 80 01  ea e1 c0 a8 00 50 5c df   ·<······ ·····P\·
0020  14 7b 08 00 4d 29 00 01  00 32 61 62 63 64 65 66   ·{··M)·· ·2abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Internet Control Message Protocol: Protocol | Packets: 179 · Displayed: 20 (11.2%) · Dropped: 0 (0.0%) | Profile: Defau

3. The ICMP type is 8 (echo (ping) request) and the code number is 0. The ICMP packet also has a checksum, 2 identifiers (BE and LE), 2 sequence numbers, and Data fields. The checksum, sequence numbers, and identifiers are two bytes each.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 51 · Wi-Fi
Close
Help
Internet Control Message Protocol: Protocol
Packets: 179 · Displayed: 20 (11.2%) · Dropped: 0 (0.0%)
Profile: Defaul

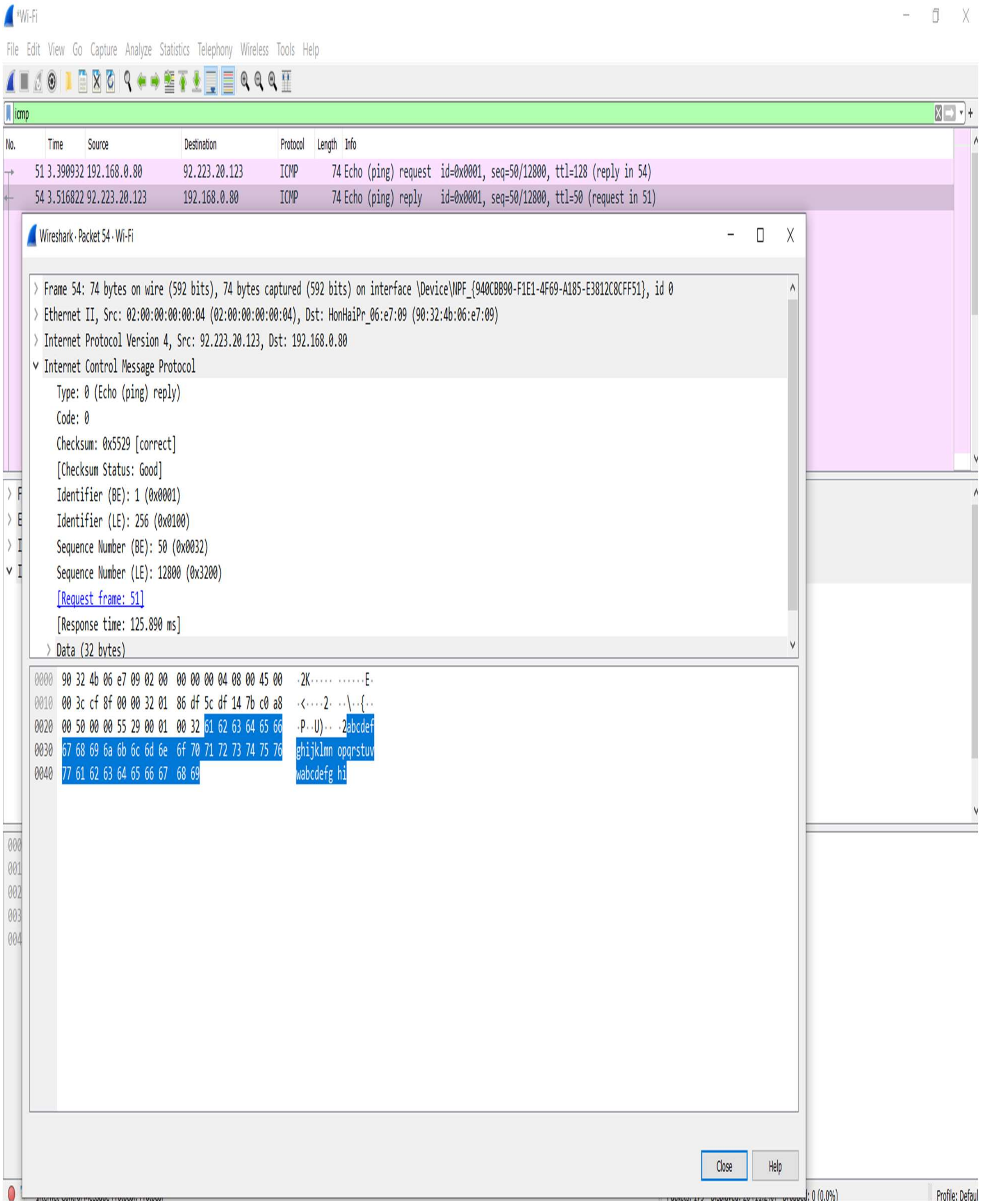
icmp

No.	Time	Source	Destination	Protocol	Length	Info
51	3.390932	192.168.0.80	92.223.20.123	ICMP	74	Echo (ping) request id=0x0001, seq=50/12800, ttl=128 (reply in 54)

```
> Frame 51: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{940CBB90-F1E1-4F69-A185-E3812C8CFF51}, id 0
> Ethernet II, Src: HonHaiPr_06:e7:09 (90:32:4b:06:e7:09), Dst: 02:00:00:00:00:04 (02:00:00:00:00:04)
> Internet Protocol Version 4, Src: 192.168.0.80, Dst: 92.223.20.123
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d29 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 50 (0x0032)
    Sequence Number (LE): 12800 (0x3200)
    [Response frame: 54]
  > Data (32 bytes)
```

```
0000  02 00 00 00 00 04 90 32  4b 06 e7 09 08 00 45 00   ·······2 K·····E·
0010  00 3c 1d 8d 00 00 80 01  ea e1 c0 a8 00 50 5c df   ·<······ ·····P\·
0020  14 7b 08 00 4d 29 00 01  00 32 61 62 63 64 65 66   ·{··M)·· ·2abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

4. The ICMP type is 0 (echo (ping) reply) and the code number is 0. The ICMP packet also has a checksum, 2 identifiers (BE and LE), 2 sequence numbers, and Data fields. The checksum, sequence number, and identifier fields are two bytes each.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Wireshark · Packet 54 · Wi-Fi
Close
Help
Dropped: 0 (0.0%)
Profile: Defaul

No.	Time	Source	Destination	Protocol	Length	Info
51	3.390932	192.168.0.80	92.223.20.123	ICMP	74	Echo (ping) request id=0x0001, seq=50/12800, ttl=128 (reply in 54)
54	3.516822	92.223.20.123	192.168.0.80	ICMP	74	Echo (ping) reply id=0x0001, seq=50/12800, ttl=50 (request in 51)

```
> Frame 54: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{940CBB90-F1E1-4F69-A185-E3812C8CFF51}, id 0
> Ethernet II, Src: 02:00:00:00:00:04 (02:00:00:00:00:04), Dst: HonHaiPr_06:e7:09 (90:32:4b:06:e7:09)
> Internet Protocol Version 4, Src: 92.223.20.123, Dst: 192.168.0.80
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5529 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 50 (0x0032)
    Sequence Number (LE): 12800 (0x3200)
    [Request frame: 51]
    [Response time: 125.890 ms]
  > Data (32 bytes)
```

```
0000  90 32 4b 06 e7 09 02 00  00 00 00 04 08 00 45 00   ·2K····· ······E·
0010  00 3c cf 8f 00 00 32 01  86 df 5c df 14 7b c0 a8   ·<····2· ··\··{··
0020  00 50 00 00 55 29 00 01  00 32 61 62 63 64 65 66   ·P··U)·· ·2abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```