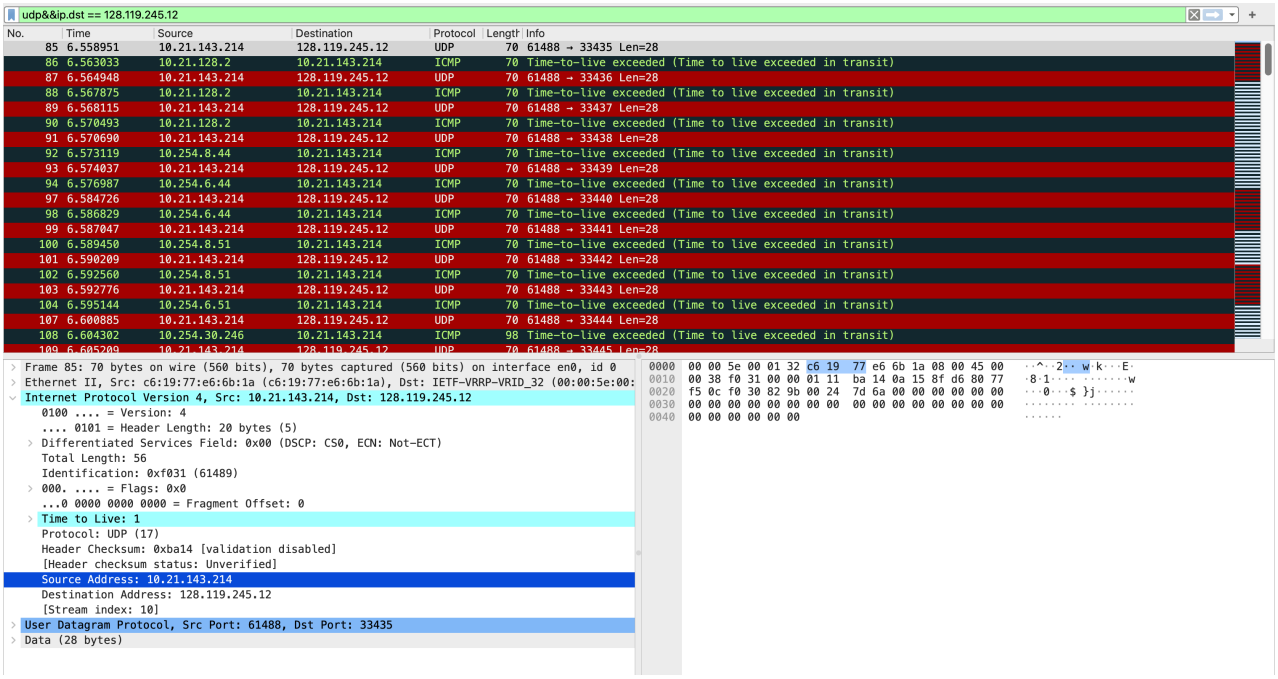
Lab4 - IP

Jiaxi Zhang

April 13, 2025

1 A look at the captured trace



```
No.     Time           Source                Destination           Protocol Length Info
     85 6.558951       10.21.143.214         128.119.245.12        UDP      70     61488 → 33435
Len=28
Frame 85: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0
Ethernet II, Src: c6:19:77:e6:6b:1a (c6:19:77:e6:6b:1a), Dst: IETF-VRRP-VRID_32 (00:00:5e:
00:01:32)
Internet Protocol Version 4, Src: 10.21.143.214, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xf031 (61489)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0xba14 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.21.143.214
    Destination Address: 128.119.245.12
    [Stream index: 10]
User Datagram Protocol, Src Port: 61488, Dst Port: 33435
Data (28 bytes)
0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0010  00 00 00 00 00 00 00 00 00 00 00 00               ............
```

The following questions are answered based on the above two figures.

1.1 Question 1

My IP address is 10.21.143.214

1.2 Question 2

The upper protocol is UDP, the protocol number is 17.

1.3 Question 3

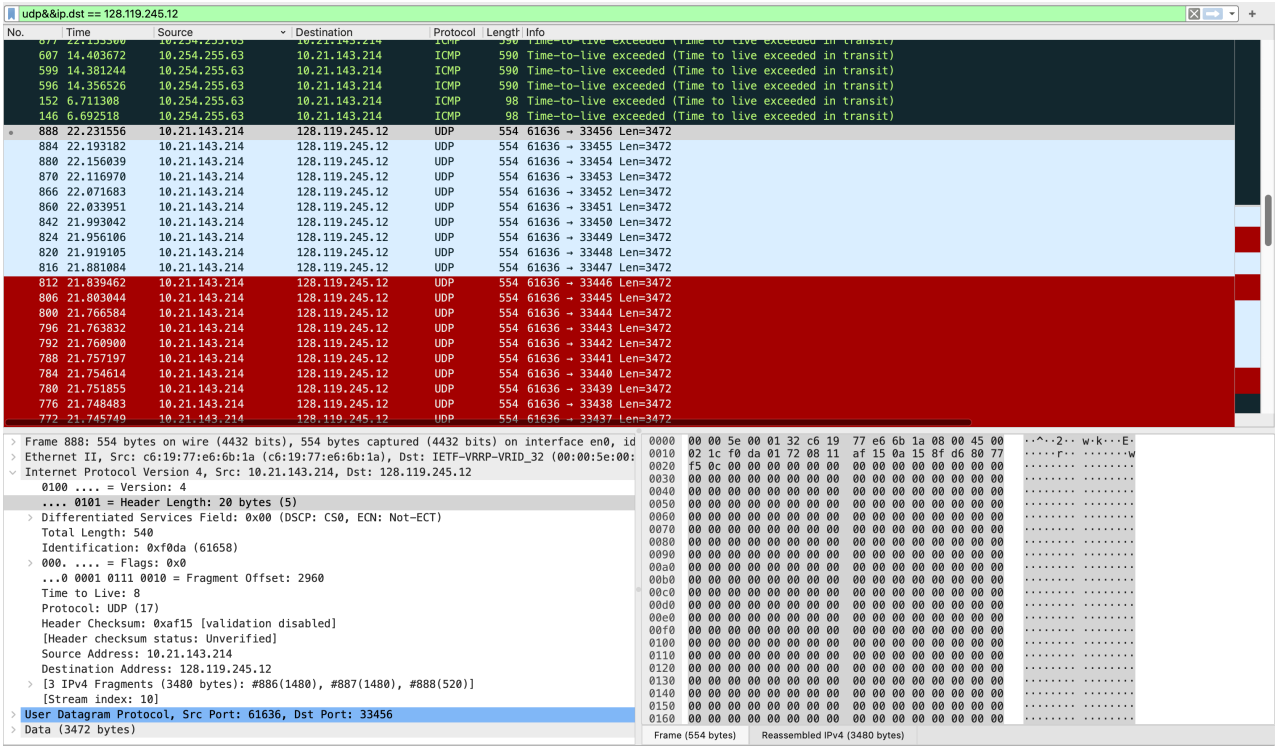
IP header length is 20 bytes, the total length is 56 bytes. Thus, the payload length is 56 - 20 = 36 bytes.

1.4 Question 4

This IP datagram is not fragmented. It can be seen from the screenshot that Fragment Offset is 0, and "Flags: 0x0" indicates that the datagram is not fragmented.

2 Sorted by source port

This is a screenshot after sorting by source port (with the arrow pointing down). It seems that since the arrow is pointing down, the time is in descending order.



2.1 Question 5

The always changing fields in the IP datagram are:

- Identification: Different datagrams have different identification numbers.
- Header Checksum: It is changed as Identification changes.

2.2 Question 6

The constant fields in the IP datagram are:

- Version: IPv4.
- Header Length: 20 bytes.
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

- Source Address and Destination Address.
- Protocol: UDP.

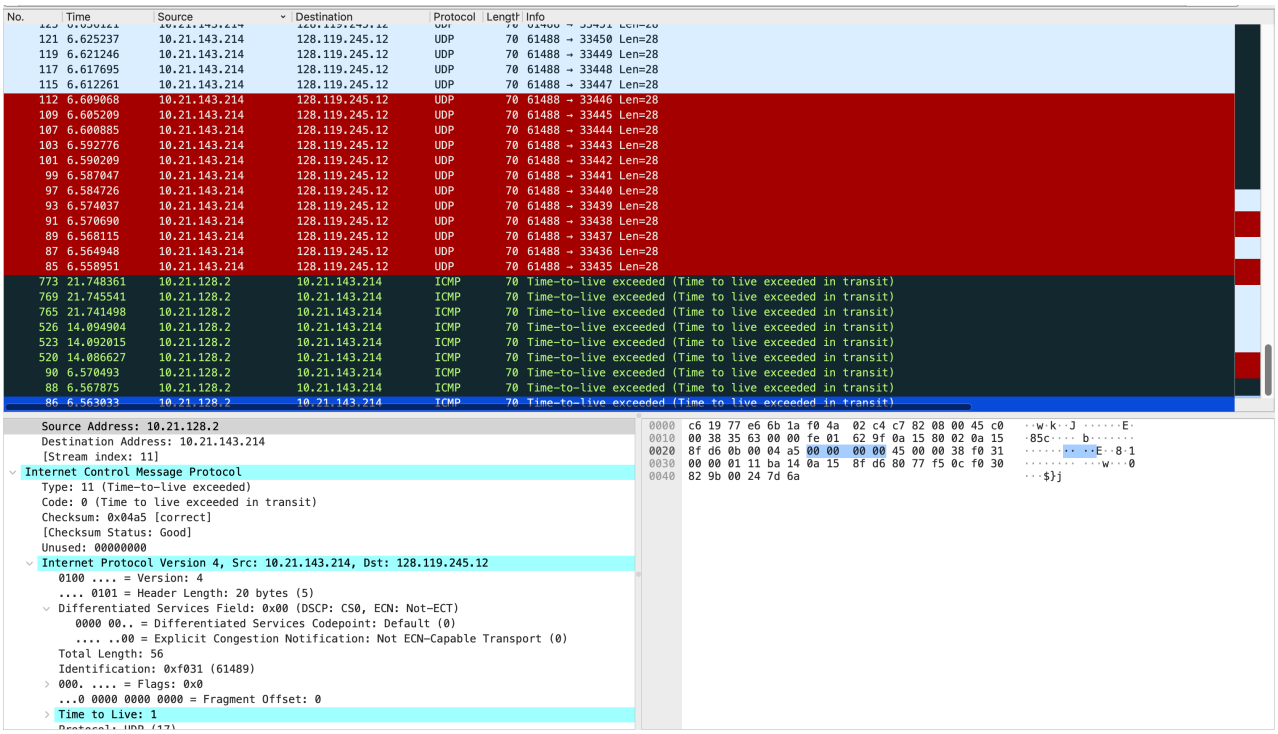
Identification and Checksum must be changing becuase each datagram is different and has the unique identification number, and the checksum is calculated based on the datagram with a changing identification number. Actually, TTL is also changing for each traceout, but it is not included in the list because it is not always changing (maybe 2 or 3 datagrams have the same TTL). It might be caused by multiple datagrams packet capturing at the same time.

The Source and Destination Address must be constant, because I have made the filter with the fixed destination address while sorting with a fixed source address. The protocol is also constant, because it is always UDP on MacOS. I suppose in the same traceout the version, total length, and fragment offset are also constant (the total length has changed but it is always 540, 520, or 56 bytes, and I have made 3 traceouts at all).

2.3 Question 7

The Identification is always changing. Actually, the identification number is decreased by 1 for each datagram. I think it is because now the time is in descending order, so actually when the datagram is captured in normal order (real-time), the identification number is increased by 1 for each datagram.

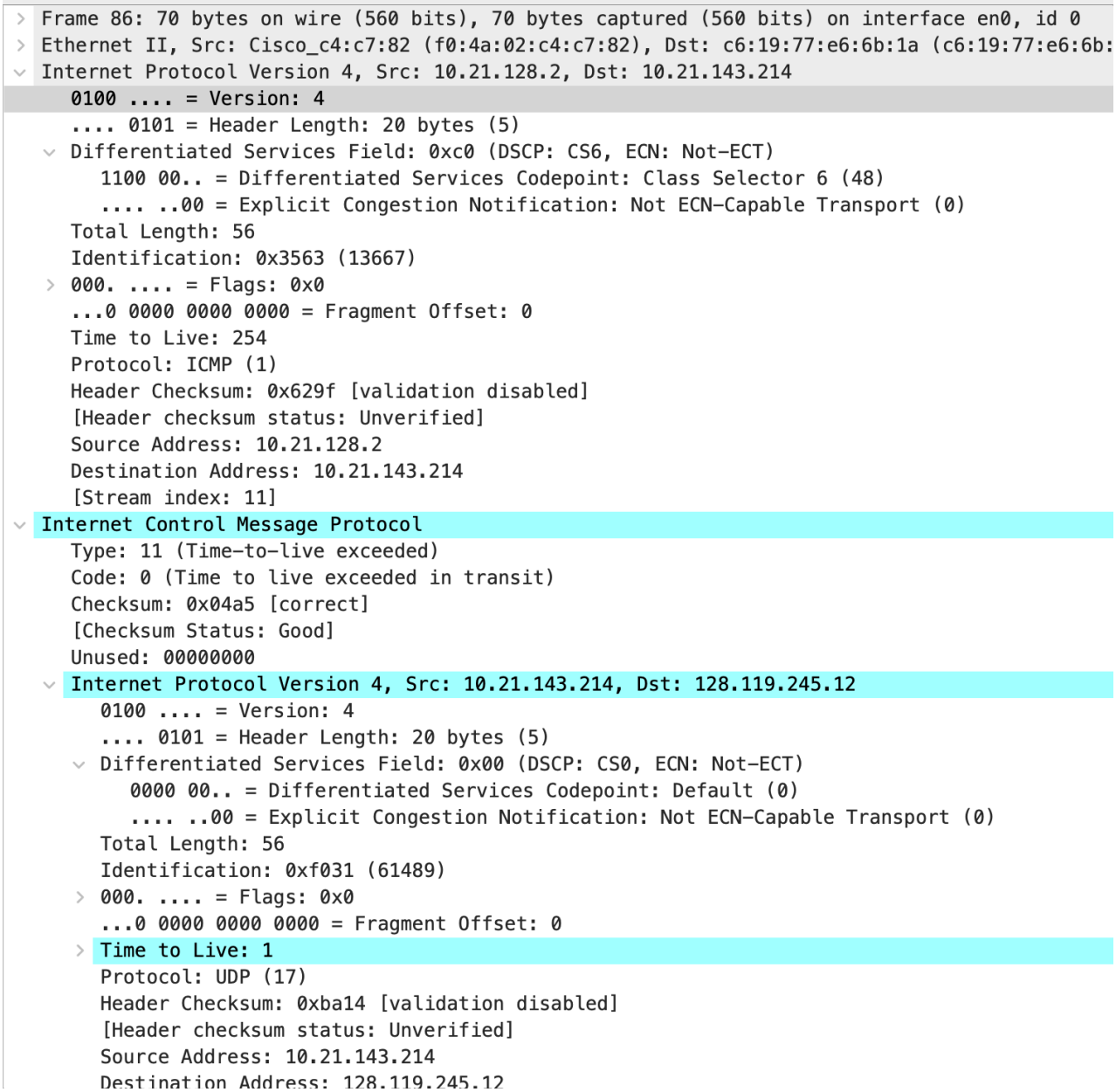
3 ICMP TTLexceeded replies



The packet 773 - 86 shown in the figure above is the ICMP TTLexceeded reply by the first hop router.

3.1 Question 8-9

More detailed information can be found in the attached file 8-9.pdf.



In the IP protocol, the TTL field is always 254 which remains unchanged. (But in the ICMP protocol, the TTL field is always 1.) The Identification field for frame 86 (screenshot above) is 0x3563 (13667). This field is always changing.

4 Fragmentation

```
No.     Time           Source                Destination           Protocol Length Info
    518 14.082217      10.21.143.214         128.119.245.12        IPv4     1514   Fragmented IP
protocol (proto=UDP 17, off=0, ID=f06d) [Reassembled in #519]
Frame 518: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id
0
Ethernet II, Src: c6:19:77:e6:6b:1a (c6:19:77:e6:6b:1a), Dst: IETF-VRRP-VRID_32 (00:00:5e:
00:01:32)
Internet Protocol Version 4, Src: 10.21.143.214, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0xf06d (61549)
    001. .... = Flags: 0x1, More fragments
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x9434 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.21.143.214
    Destination Address: 128.119.245.12
    [Reassembled IPv4 in frame: 519]
    [Stream index: 10]
Data (1480 bytes)
0000  f0 6c 82 9b 07 bc 6d fe 00 00 00 00 00 00 00 00   .l....m.........
0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

```
Ethernet II, Src: c6:19:77:e6:6b:1a (c6:19:77:e6:6b:1a), Dst: IETF-VRRP-VRID_32 (00:00:5e:
00:01:32)
Internet Protocol Version 4, Src: 10.21.143.214, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 520
    Identification: 0xf06d (61549)
    000. .... = Flags: 0x0
    ...0 0000 1011 1001 = Fragment Offset: 1480
    Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0xb74f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.21.143.214
    Destination Address: 128.119.245.12
    [2 IPv4 Fragments (1980 bytes): #518(1480), #519(500)]
    [Stream index: 10]
User Datagram Protocol, Src Port: 61548, Dst Port: 33435
Data (1972 bytes)
0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

The two figures above show the ICMP Echo Request message sent with a packet size of 2000 bytes. The first figure shows the first fragment, and the second figure shows the second fragment.

4.1 Question 10-13

Yes, the ICMP Echo Request message sent with a packet size of 2000 bytes has been fragmented into multiple IP datagrams.

It can be seen that the "Flags: 0x1" in the first fragment, and fragment offset is 0 which indicates that this is the first fragment (instead of a latter fragment). This datagram length is 1500 bytes with the header length of 20 bytes and the payload length of 1480 bytes.

For the second fragment, fragment offset is 1480 which indicates that this is the second fragment (instead of a first fragment). There are no more fragments after this datagram, so the "Flags: 0x0" indicates that this is

the last fragment.

The changed fields are:

- Identification: Different identification numbers for different fragments.
- Fragment Offset: 0 for the first fragment, 1480 for the second fragment.
- Flags: 0x1 for the first fragment, 0x0 for the second fragment.
- Total (and payload) Length: First fragment: 1500 bytes, second fragment: 520 bytes.
- Header Checksum: Changed as Identification changes.

4.2 Question 14-15

```
No.     Time           Source                Destination           Protocol Length Info
    762 21.735798      10.21.143.214         128.119.245.12        IPv4     1514   Fragmented IP
protocol (proto=UDP 17, off=0, ID=f0c5) [Reassembled in #764]
Frame 762: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id
0
Ethernet II, Src: c6:19:77:e6:6b:1a (c6:19:77:e6:6b:1a), Dst: IETF-VRRP-VRID_32 (00:00:5e:
00:01:32)
Internet Protocol Version 4, Src: 10.21.143.214, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0xf0c5 (61637)
    001. .... = Flags: 0x1, More fragments
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x93dc [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.21.143.214
    Destination Address: 128.119.245.12
    [Reassembled IPv4 in frame: 764]
    [Stream index: 10]
Data (1480 bytes)
0000  f0 c4 82 9b 0d 98 61 ee 00 00 00 00 00 00 00 00   ......a.........
0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ----------------
```

```
05b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
05c0  00 00 00 00 00 00 00 00                           ........
No.     Time           Source                Destination           Protocol Length Info
    763 21.735814      10.21.143.214         128.119.245.12        IPv4     1514   Fragmented IP
protocol (proto=UDP 17, off=1480, ID=f0c5) [Reassembled in #764]
Frame 763: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id
0
```

```
Ethernet II, Src: c6:19:77:e6:6b:1a (c6:19:77:e6:6b:1a), Dst: IETF-VRRP-VRID_32 (00:00:5e:
00:01:32)
Internet Protocol Version 4, Src: 10.21.143.214, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0xf0c5 (61637)
    001. .... = Flags: 0x1, More fragments
    ...0 0000 1011 1001 = Fragment Offset: 1480
    Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x9323 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.21.143.214
    Destination Address: 128.119.245.12
    [Reassembled IPv4 in frame: 764]
    [Stream index: 10]
Data (1480 bytes)
0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

```
05c0  00 00 00 00 00 00 00 00                           ........
No.     Time           Source                Destination           Protocol Length Info
    764 21.735817      10.21.143.214         128.119.245.12        UDP      554    61636 → 33435
Len=3472
Frame 764: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface en0, id 0
Ethernet II, Src: c6:19:77:e6:6b:1a (c6:19:77:e6:6b:1a), Dst: IETF-VRRP-VRID_32 (00:00:5e:
00:01:32)
Internet Protocol Version 4, Src: 10.21.143.214, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
```

```
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 540
    Identification: 0xf0c5 (61637)
    000. .... = Flags: 0x0
    ...0 0001 0111 0010 = Fragment Offset: 2960
    Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0xb62a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.21.143.214
    Destination Address: 128.119.245.12
    [3 IPv4 Fragments (3480 bytes): #762(1480), #763(1480), #764(520)]
    [Stream index: 10]
User Datagram Protocol, Src Port: 61636, Dst Port: 33435
Data (3472 bytes)
0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

The three figures above show the ICMP Echo Request message sent with a packet size of 3500 bytes. So the total amount of fragments is 3: The first fragment and the second fragment have "Flags: 0x1" and the third

fragment has "Flags: 0x0". Fields that are changed:

- Identification: Different identification numbers for different fragments.
- Fragment Offset: 0 for the first fragment, 1480 for the second fragment, and 2960 for the third fragment.
- Flags: 0x1 for the first and second fragments, 0x0 for the third fragment.
- Total (and payload) Length: First fragment: 1500 bytes, second fragment: 1500 bytes, third fragment: 540 bytes.
- Header Checksum: Changed as Identification changes.