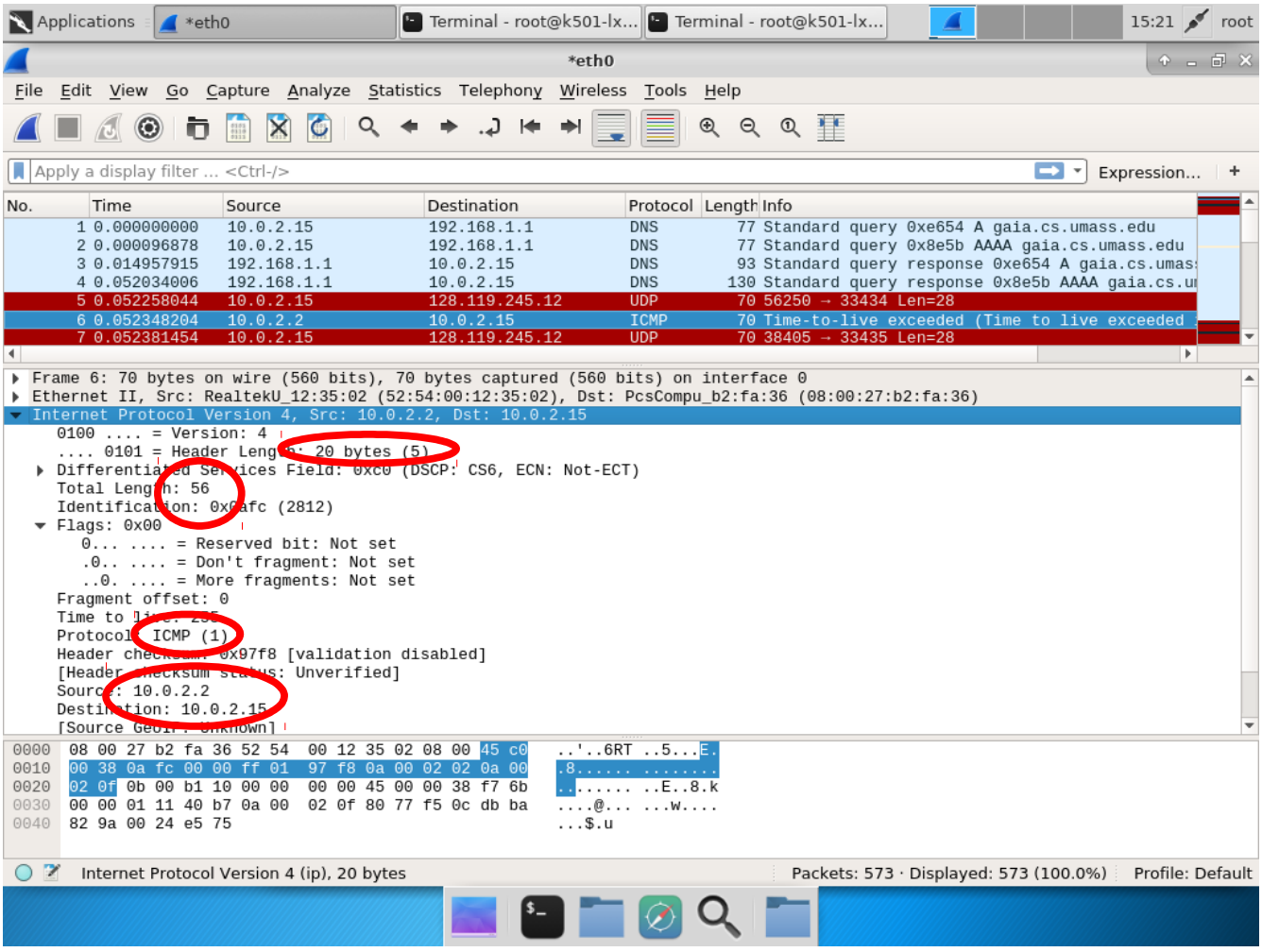
Luke Malloy

Wireshark Lab: IP

Questions:

1. 10.0.2.15
2. The value is ICMP 0x01 or (1)
3. There are 20 bytes in the IP header, 36 bytes in the payload datagram for a total of 56 bytes.
4. The More Fragments flag is not set, therefore, the data is not fragmented
5. Frame, Identification Time to Live, and Header checksum always change

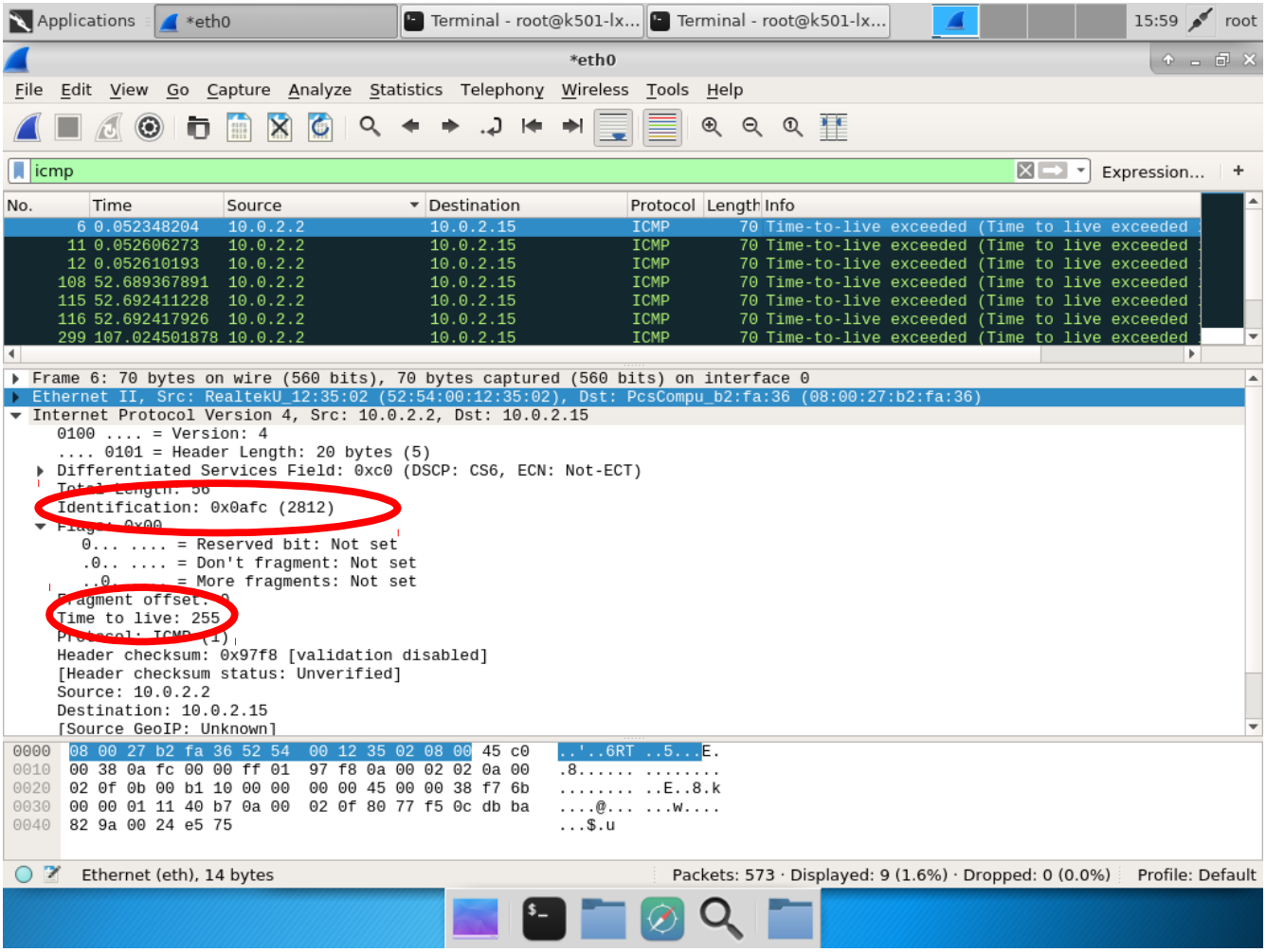


6. The fields that are constant and must stay constant are the Version due to IPv4 use for all packets, Header length due to ICMP packet type, source and destination IP addresses because they are being sent and received by the same machines, Upper Layer Protocol due to ICMP packet type, and Differentiated Services because ICMP packets use the same Type of Service.

Dynamic fields include the Identification header because the ids are unique, the Time to live as this value is incremented with every packet as well as the checksum because of the header change.

7. The identification header is incremented by one with each request.

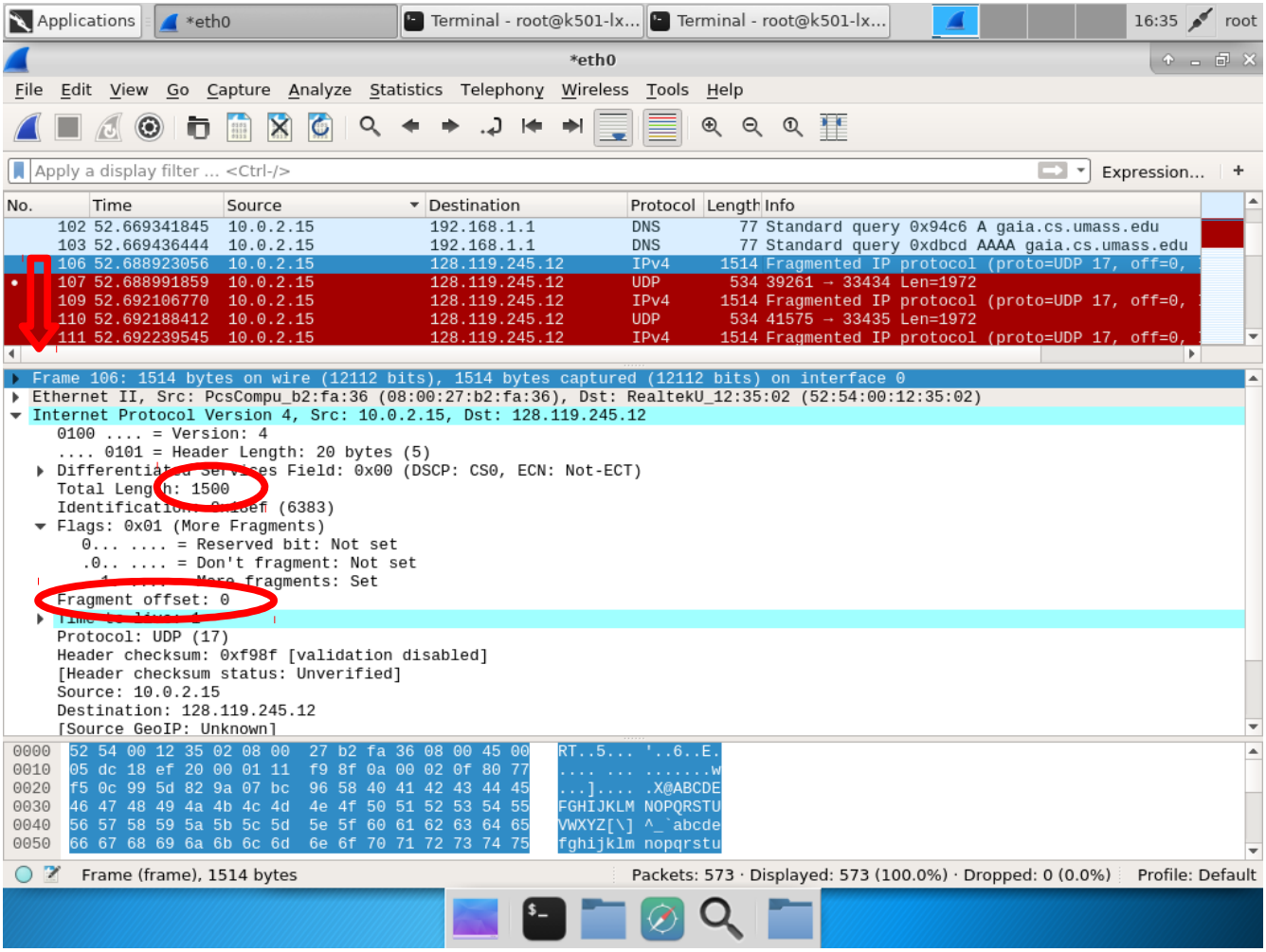
8. 2812 is in the identification field, 255 is the total time to live value



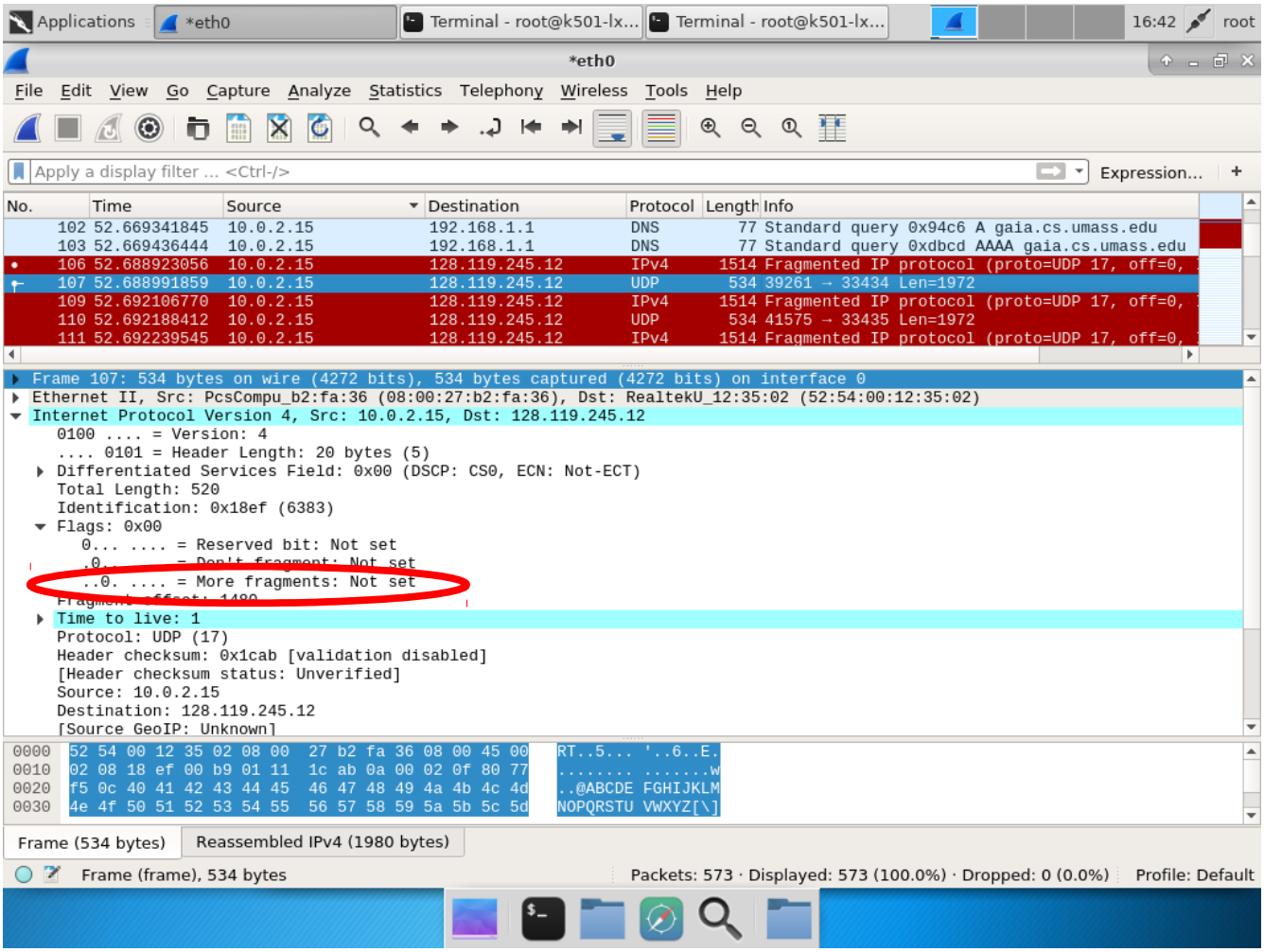
9. The identification field contains a unique value, therefore it must change for all exceeded replies. The same identification number would indicate a fragmented IP datagram. The total time to live does not change because it remains constant for the first hop router.

10. Yes, the packet is fragmented across multiple datagrams.

11. The more fragments bit is set, indicating fragmentation and the fragment offset is 0, indicating the first fragment of the set. This IP datagram has a length of 1500.



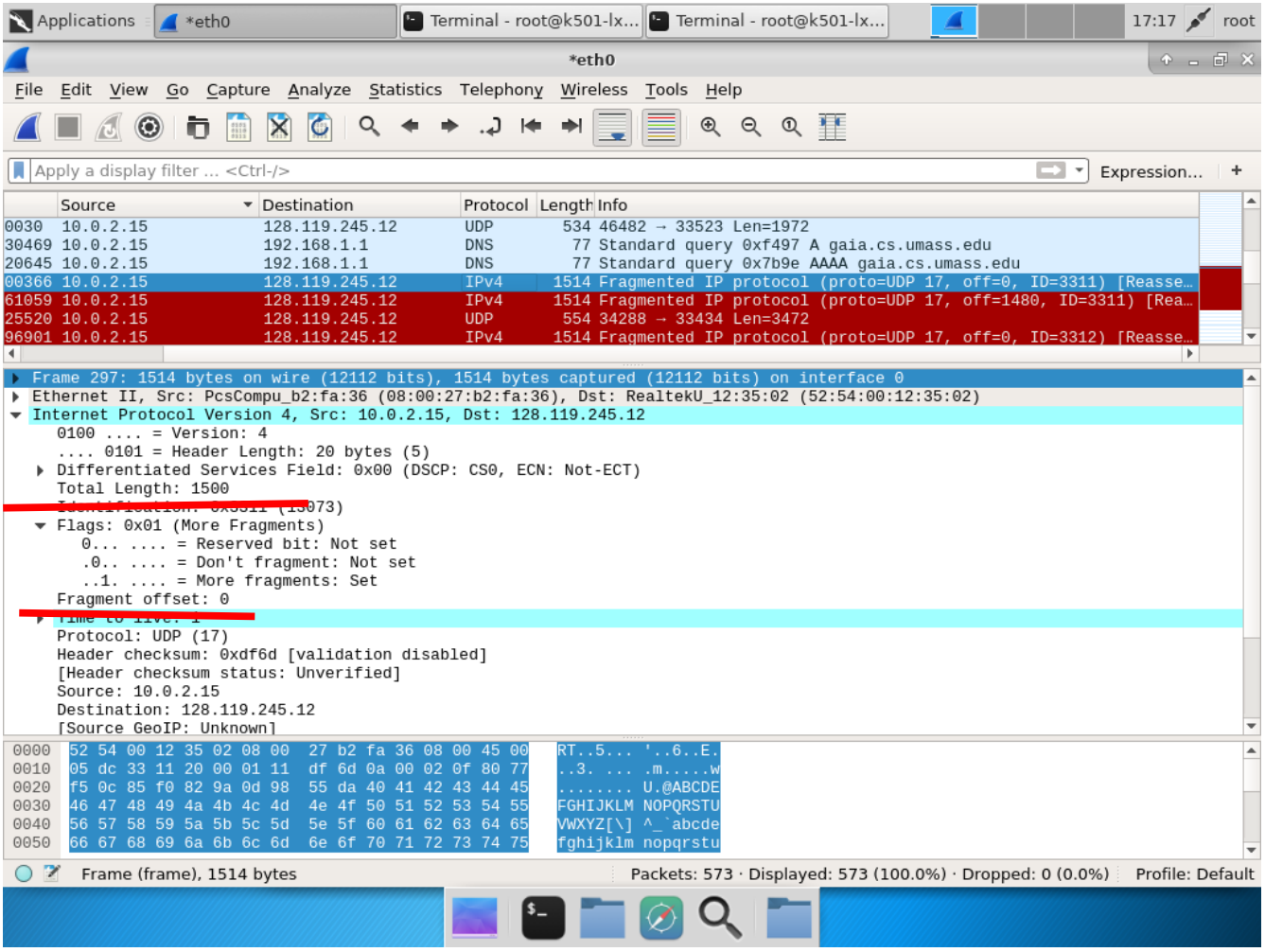
12. The more fragments flag is not set, therefore we know this is the last in the set. This is also not the first fragment in the set, the total length is 1480 for the segment in question.

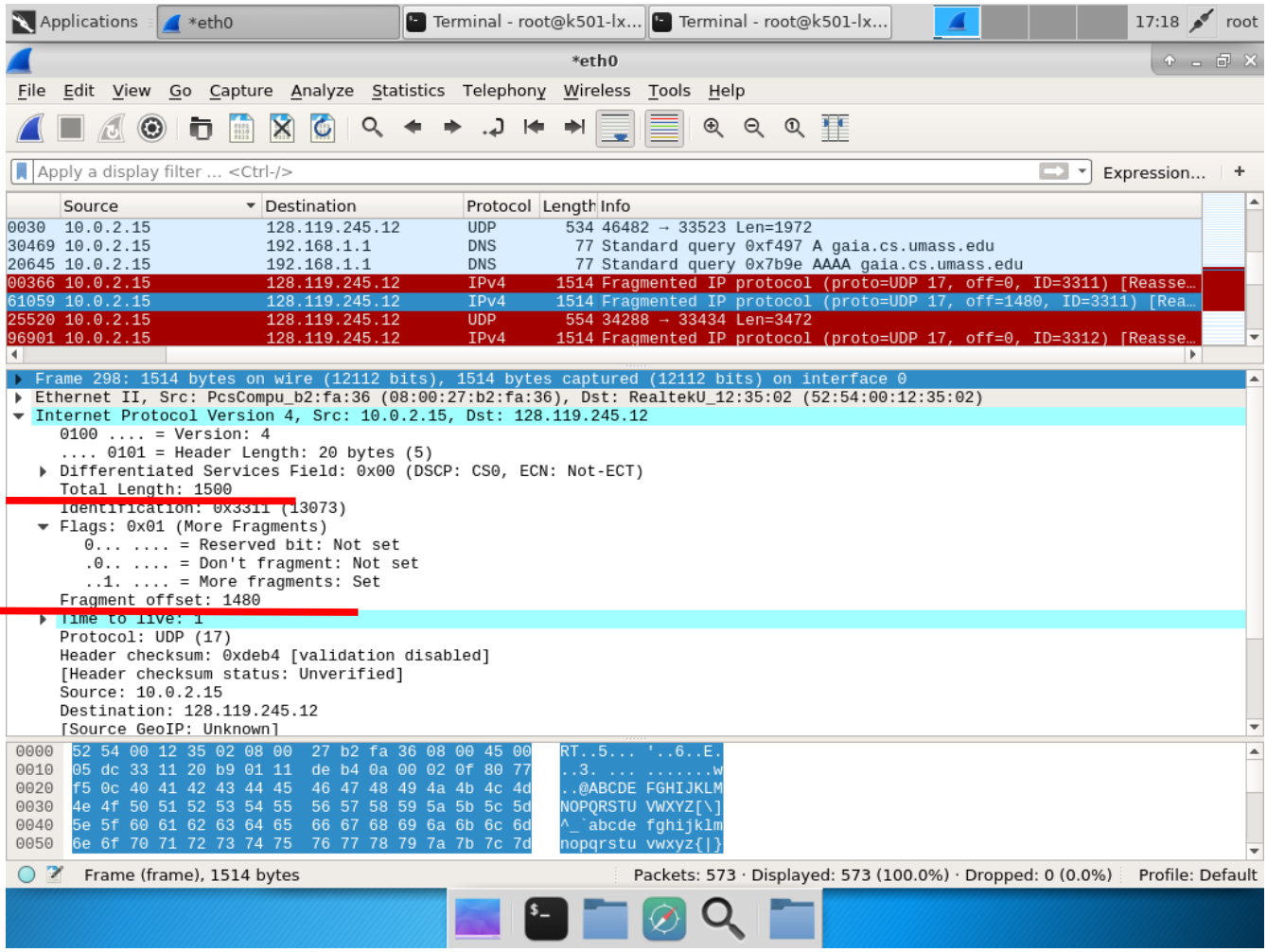


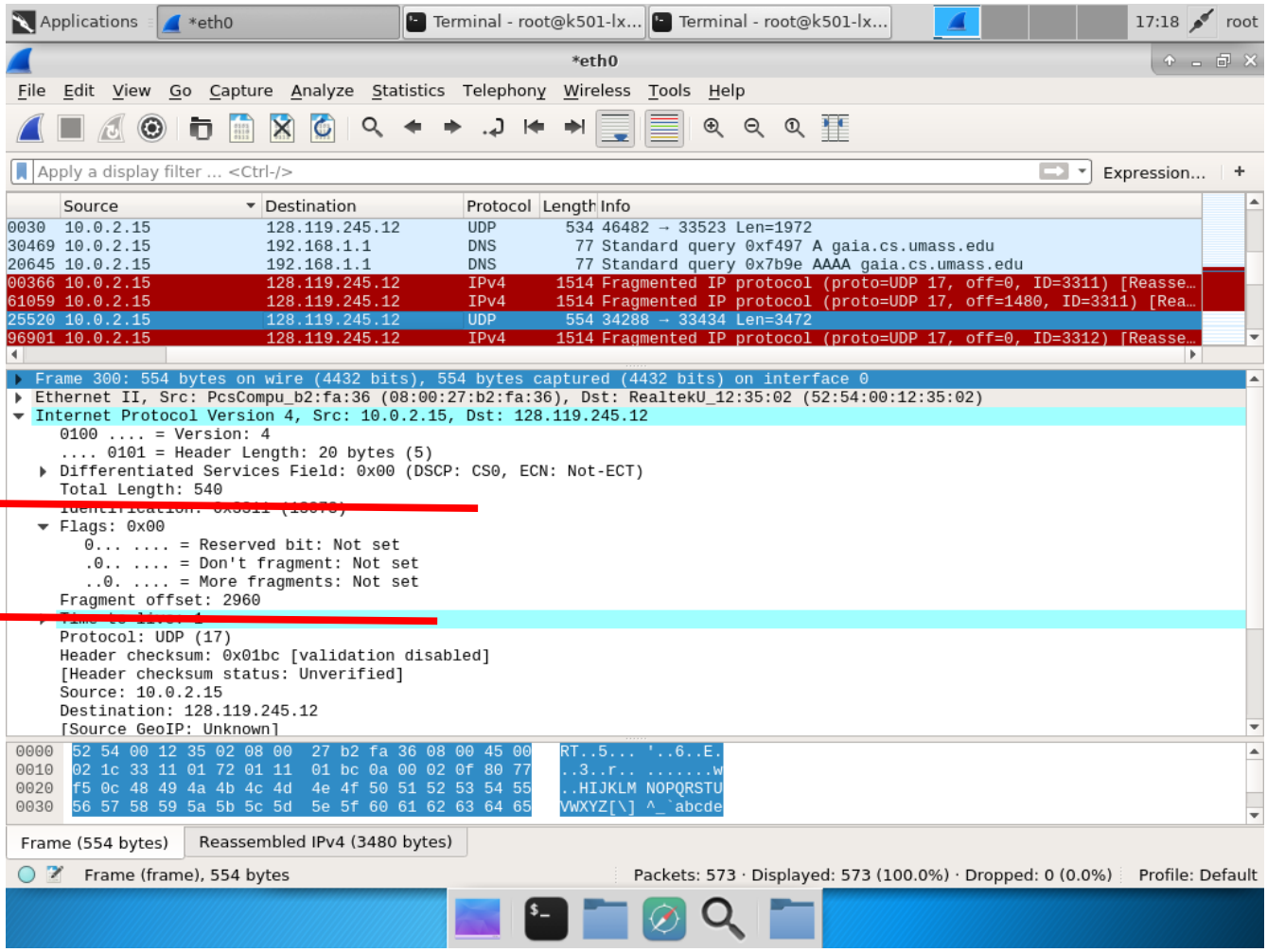
13. The IP header fields that change are total length, flags, checksum and fragment offsets.

14. Three fragments are created from the original datagram.

15. Fragment offset changes from 0 to 1480 to 2960. The checksums, total length varies between the first two fragments and the 3rd. The more fragments flag is 0 in the last segment.




Applications
*eth0
Terminal - root@k501-lx...
Terminal - root@k501-lx...
17:18
root
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Source Destination Protocol Length Info
0030 10.0.2.15 128.119.245.12 UDP 534 46482 → 33523 Len=1972
30469 10.0.2.15 192.168.1.1 DNS 77 Standard query 0xf497 A gaia.cs.umass.edu
20645 10.0.2.15 192.168.1.1 DNS 77 Standard query 0x7b9e AAAA gaia.cs.umass.edu
00366 10.0.2.15 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=3311) [Reasse…
61059 10.0.2.15 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=3311) [Rea…
25520 10.0.2.15 128.119.245.12 UDP 554 34288 → 33434 Len=3472
96901 10.0.2.15 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=3312) [Reasse…
Frame 298: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Ethernet II, Src: PcsCompu_b2:fa:36 (08:00:27:b2:fa:36), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, 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: 1500
Identification: 0x3311 (13073)
Flags: 0x01 (More Fragments)
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..1. .... = More fragments: Set
Fragment offset: 1480
Time to live: 1
Protocol: UDP (17)
Header checksum: 0xdeb4 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.15
Destination: 128.119.245.12
[Source GeoIP: Unknown]
0000 52 54 00 12 35 02 08 00 27 b2 fa 36 08 00 45 00 RT..5... '..6..E.
0010 05 dc 33 11 20 b9 01 11 de b4 0a 00 02 0f 80 77 ..3. ... .w
0020 f5 0c 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d ..@ABCDE FGHIJKLM
0030 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d NOPQRSTU VWXYZ[\]
0040 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d ^_`abcde fghijklm
0050 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d nopqrstu vwxyz{|}
Frame (frame), 1514 bytes
Packets: 573 · Displayed: 573 (100.0%) · Dropped: 0 (0.0%)
Profile: Default


Applications
*eth0
Terminal - root@k501-lx...
Terminal - root@k501-lx...
17:18
root
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Source Destination Protocol Length Info
0030 10.0.2.15 128.119.245.12 UDP 534 46482 → 33523 Len=1972
30469 10.0.2.15 192.168.1.1 DNS 77 Standard query 0xf497 A gaia.cs.umass.edu
20645 10.0.2.15 192.168.1.1 DNS 77 Standard query 0x7b9e AAAA gaia.cs.umass.edu
00366 10.0.2.15 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=3311) [Reasse…
61059 10.0.2.15 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=3311) [Rea…
25520 10.0.2.15 128.119.245.12 UDP 554 34288 → 33434 Len=3472
96901 10.0.2.15 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=3312) [Reasse…
Frame 300: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
Ethernet II, Src: PcsCompu_b2:fa:36 (08:00:27:b2:fa:36), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, 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: 540
Flags: 0x00
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
Fragment offset: 2960
Protocol: UDP (17)
Header checksum: 0x01bc [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.15
Destination: 128.119.245.12
[Source GeoIP: Unknown]
0000 52 54 00 12 35 02 08 00 27 b2 fa 36 08 00 45 00 RT..5... '..6..E.
0010 02 1c 33 11 01 72 01 11 01 bc 0a 00 02 0f 80 77 ..3..r.. ....w
0020 f5 0c 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 ..HIJKLM NOPQRSTU
0030 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 VWXYZ[\] ^_`abcde
Frame (554 bytes)
Reassembled IPv4 (3480 bytes)
Frame (frame), 554 bytes
Packets: 573 · Displayed: 573 (100.0%) · Dropped: 0 (0.0%)
Profile: Default