HACETTEPE UNIVERSITY

COMPUTER ENGINEERING DEPARTMENT

BBM 453 LAB EXPERIMENT 5 (IP)

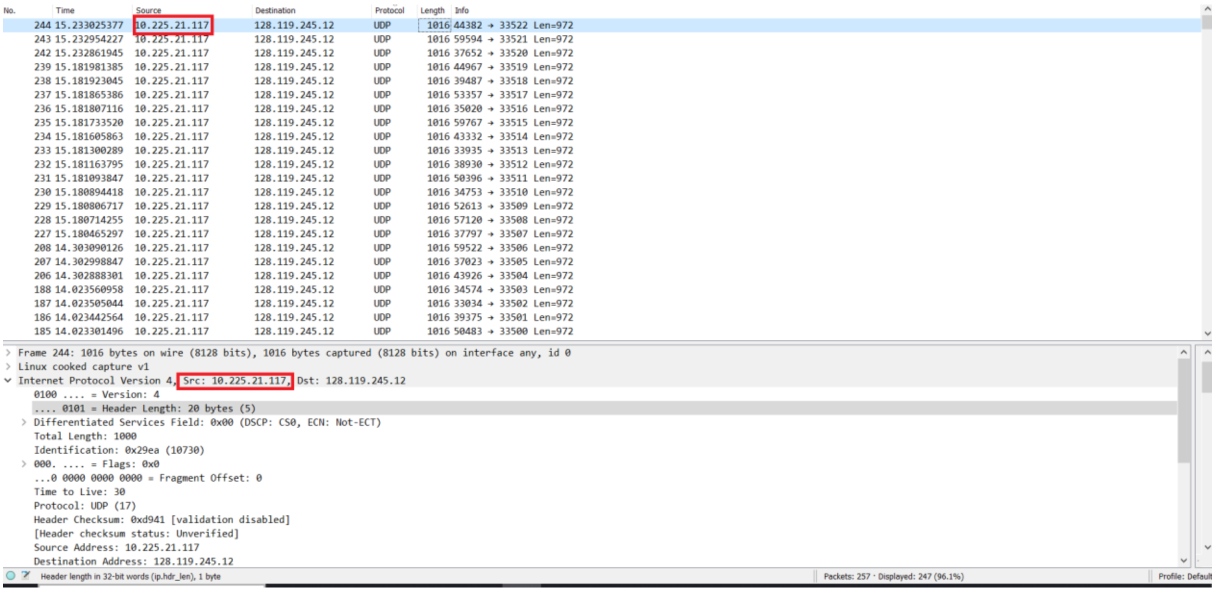
Group No: 41

Yiğit Emir İşıkçı: 2200356028

Ahmet Eren Akbaş: 21945757

1) A look at the capture trace

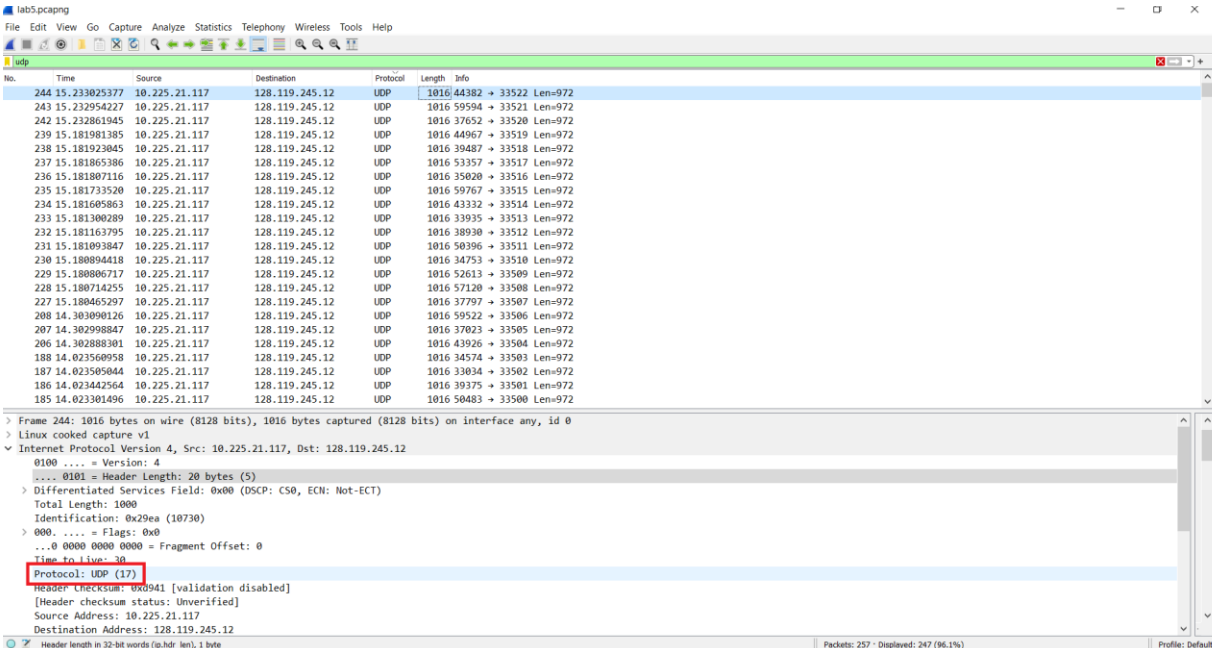
1-) Select the first UDP segment message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?



```
No.  Time          Source          Destination      Protocol  Length  Info
 244 15.233025377  10.225.21.117   128.119.245.12   UDP       1016 44382 → 33522 Len=972
 243 15.232954227  10.225.21.117   128.119.245.12   UDP       1016 59594 → 33521 Len=972
 242 15.232861945  10.225.21.117   128.119.245.12   UDP       1016 37652 → 33520 Len=972
 239 15.181981385  10.225.21.117   128.119.245.12   UDP       1016 44967 → 33519 Len=972
 238 15.181923045  10.225.21.117   128.119.245.12   UDP       1016 39487 → 33518 Len=972
 237 15.181865386  10.225.21.117   128.119.245.12   UDP       1016 53357 → 33517 Len=972
 236 15.181807116  10.225.21.117   128.119.245.12   UDP       1016 35020 → 33516 Len=972
 235 15.181733520  10.225.21.117   128.119.245.12   UDP       1016 59767 → 33515 Len=972
 234 15.181605863  10.225.21.117   128.119.245.12   UDP       1016 43332 → 33514 Len=972
 233 15.181300289  10.225.21.117   128.119.245.12   UDP       1016 33935 → 33513 Len=972
 232 15.181163795  10.225.21.117   128.119.245.12   UDP       1016 38930 → 33512 Len=972
 231 15.181093847  10.225.21.117   128.119.245.12   UDP       1016 50396 → 33511 Len=972
 230 15.180894418  10.225.21.117   128.119.245.12   UDP       1016 34753 → 33510 Len=972
 229 15.180806717  10.225.21.117   128.119.245.12   UDP       1016 52613 → 33509 Len=972
 228 15.180714255  10.225.21.117   128.119.245.12   UDP       1016 57120 → 33508 Len=972
 227 15.180465297  10.225.21.117   128.119.245.12   UDP       1016 37797 → 33507 Len=972
 208 14.303090126  10.225.21.117   128.119.245.12   UDP       1016 59522 → 33506 Len=972
 207 14.302998847  10.225.21.117   128.119.245.12   UDP       1016 37023 → 33505 Len=972
 206 14.302888301  10.225.21.117   128.119.245.12   UDP       1016 43926 → 33504 Len=972
 188 14.023560958  10.225.21.117   128.119.245.12   UDP       1016 34574 → 33503 Len=972
 187 14.023505044  10.225.21.117   128.119.245.12   UDP       1016 33034 → 33502 Len=972
 186 14.023442564  10.225.21.117   128.119.245.12   UDP       1016 39375 → 33501 Len=972
 185 14.023301496  10.225.21.117   128.119.245.12   UDP       1016 50483 → 33500 Len=972

> Frame 244: 1016 bytes on wire (8128 bits), 1016 bytes captured (8128 bits) on interface any, id 0
> Linux cooked capture v1
v Internet Protocol Version 4, Src: 10.225.21.117, 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: 1000
    Identification: 0x29ea (10730)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 30
    Protocol: UDP (17)
    Header Checksum: 0xd941 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.225.21.117
    Destination Address: 128.119.245.12

Header length in 32-bit words (ip.hdr_len), 1 byte     Packets: 257 · Displayed: 247 (96.1%)     Profile: Default
```

Answer: We used kali linux from a virtualbox to capture packets. Our IP Address is: 10.225.21.117

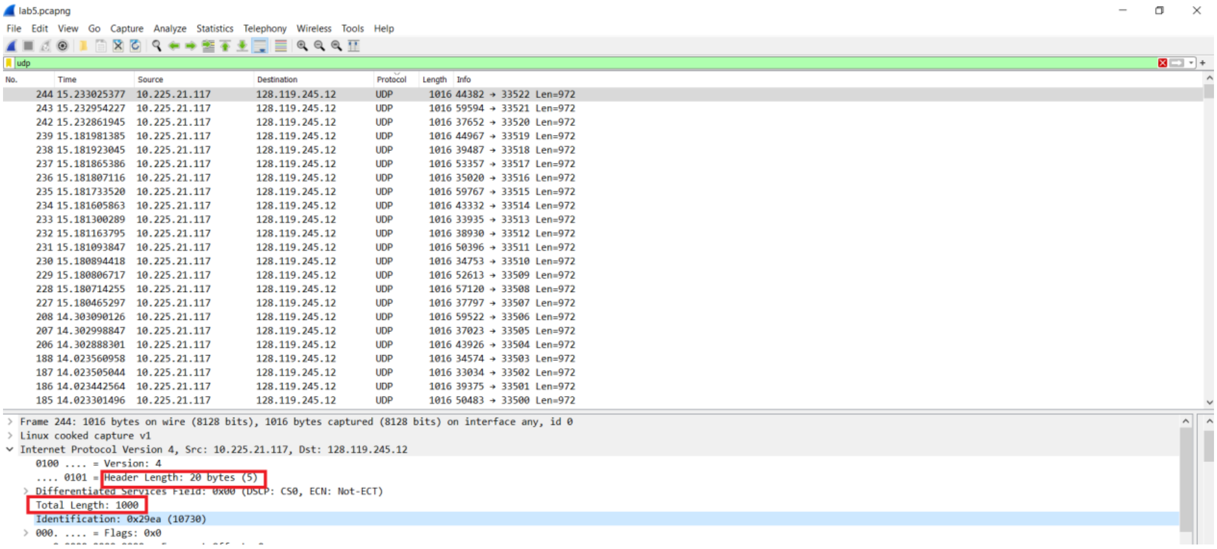
2-) Within the IP packet header, what is the value in the upper layer protocol field?



```
udp

No.  Time          Source          Destination      Protocol  Length  Info
 244 15.233025377  10.225.21.117   128.119.245.12   UDP       1016 44382 → 33522 Len=972
 243 15.232954227  10.225.21.117   128.119.245.12   UDP       1016 59594 → 33521 Len=972
 242 15.232861945  10.225.21.117   128.119.245.12   UDP       1016 37652 → 33520 Len=972
 239 15.181981385  10.225.21.117   128.119.245.12   UDP       1016 44967 → 33519 Len=972
 238 15.181923045  10.225.21.117   128.119.245.12   UDP       1016 39487 → 33518 Len=972
 237 15.181865386  10.225.21.117   128.119.245.12   UDP       1016 53357 → 33517 Len=972
 236 15.181807116  10.225.21.117   128.119.245.12   UDP       1016 35020 → 33516 Len=972
 235 15.181733520  10.225.21.117   128.119.245.12   UDP       1016 59767 → 33515 Len=972
 234 15.181605863  10.225.21.117   128.119.245.12   UDP       1016 43332 → 33514 Len=972
 233 15.181300289  10.225.21.117   128.119.245.12   UDP       1016 33935 → 33513 Len=972
 232 15.181163795  10.225.21.117   128.119.245.12   UDP       1016 38930 → 33512 Len=972
 231 15.181093847  10.225.21.117   128.119.245.12   UDP       1016 50396 → 33511 Len=972
 230 15.180894418  10.225.21.117   128.119.245.12   UDP       1016 34753 → 33510 Len=972
 229 15.180806717  10.225.21.117   128.119.245.12   UDP       1016 52613 → 33509 Len=972
 228 15.180714255  10.225.21.117   128.119.245.12   UDP       1016 57120 → 33508 Len=972
 227 15.180465297  10.225.21.117   128.119.245.12   UDP       1016 37797 → 33507 Len=972
 208 14.303090126  10.225.21.117   128.119.245.12   UDP       1016 59522 → 33506 Len=972
 207 14.302998847  10.225.21.117   128.119.245.12   UDP       1016 37023 → 33505 Len=972
 206 14.302888301  10.225.21.117   128.119.245.12   UDP       1016 43926 → 33504 Len=972
 188 14.023560958  10.225.21.117   128.119.245.12   UDP       1016 34574 → 33503 Len=972
 187 14.023505044  10.225.21.117   128.119.245.12   UDP       1016 33034 → 33502 Len=972
 186 14.023442564  10.225.21.117   128.119.245.12   UDP       1016 39375 → 33501 Len=972
 185 14.023301496  10.225.21.117   128.119.245.12   UDP       1016 50483 → 33500 Len=972

> Frame 244: 1016 bytes on wire (8128 bits), 1016 bytes captured (8128 bits) on interface any, id 0
> Linux cooked capture v1
v Internet Protocol Version 4, Src: 10.225.21.117, 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: 1000
    Identification: 0x29ea (10730)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 30
    Protocol: UDP (17)
    Header Checksum: 0xd941 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.225.21.117
    Destination Address: 128.119.245.12

Header length in 32-bit words (ip.hdr_len), 1 byte     Packets: 257 · Displayed: 247 (96.1%)     Profile: Default
```

Answer: Since we use a linux system, we got UDP packets instead of ICMP echo packets. Protocol field’s value is UDP (17).

3-) How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

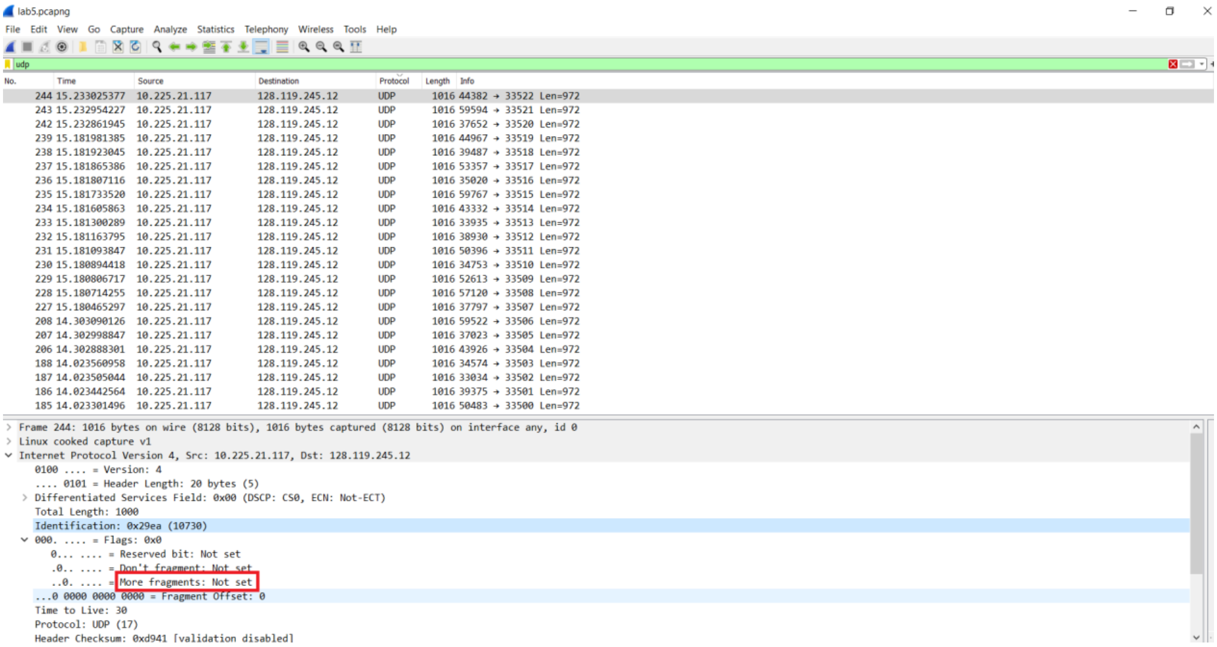

lab5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

```
No.   Time         Source         Destination     Protocol Length Info
  244 15.233025377 10.225.21.117  128.119.245.12  UDP      1016 44382 → 33522 Len=972
  243 15.232954227 10.225.21.117  128.119.245.12  UDP      1016 59594 → 33521 Len=972
  242 15.232861945 10.225.21.117  128.119.245.12  UDP      1016 37652 → 33520 Len=972
  239 15.181981385 10.225.21.117  128.119.245.12  UDP      1016 44967 → 33519 Len=972
  238 15.181923045 10.225.21.117  128.119.245.12  UDP      1016 39487 → 33518 Len=972
  237 15.181865386 10.225.21.117  128.119.245.12  UDP      1016 53357 → 33517 Len=972
  236 15.181807116 10.225.21.117  128.119.245.12  UDP      1016 35020 → 33516 Len=972
  235 15.181733520 10.225.21.117  128.119.245.12  UDP      1016 59767 → 33515 Len=972
  234 15.181605863 10.225.21.117  128.119.245.12  UDP      1016 43332 → 33514 Len=972
  233 15.181300289 10.225.21.117  128.119.245.12  UDP      1016 33935 → 33513 Len=972
  232 15.181163795 10.225.21.117  128.119.245.12  UDP      1016 38930 → 33512 Len=972
  231 15.181093847 10.225.21.117  128.119.245.12  UDP      1016 50396 → 33511 Len=972
  230 15.180894418 10.225.21.117  128.119.245.12  UDP      1016 34753 → 33510 Len=972
  229 15.180806717 10.225.21.117  128.119.245.12  UDP      1016 52613 → 33509 Len=972
  228 15.180714255 10.225.21.117  128.119.245.12  UDP      1016 57120 → 33508 Len=972
  227 15.180465297 10.225.21.117  128.119.245.12  UDP      1016 37797 → 33507 Len=972
  208 14.303090126 10.225.21.117  128.119.245.12  UDP      1016 59522 → 33506 Len=972
  207 14.302998847 10.225.21.117  128.119.245.12  UDP      1016 37023 → 33505 Len=972
  206 14.302888301 10.225.21.117  128.119.245.12  UDP      1016 43926 → 33504 Len=972
  188 14.023560958 10.225.21.117  128.119.245.12  UDP      1016 34574 → 33503 Len=972
  187 14.023505044 10.225.21.117  128.119.245.12  UDP      1016 33034 → 33502 Len=972
  186 14.023442564 10.225.21.117  128.119.245.12  UDP      1016 39375 → 33501 Len=972
  185 14.023301496 10.225.21.117  128.119.245.12  UDP      1016 50483 → 33500 Len=972
```

```
> Frame 244: 1016 bytes on wire (8128 bits), 1016 bytes captured (8128 bits) on interface any, id 0
> Linux cooked capture v1
v Internet Protocol Version 4, Src: 10.225.21.117, 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: 1000
    Identification: 0x29ea (10730)
  > 000. .... = Flags: 0x0
```

Answer: Header length is 20 bytes. Total length is 1000 bytes. To calculate the payload size we need to subtract header length from total length. 1000-20=980 bytes. Hence the payload size is 980 bytes.

4-) Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.


lab5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

```
No.   Time         Source         Destination     Protocol Length Info
  244 15.233025377 10.225.21.117  128.119.245.12  UDP      1016 44382 → 33522 Len=972
  243 15.232954227 10.225.21.117  128.119.245.12  UDP      1016 59594 → 33521 Len=972
  242 15.232861945 10.225.21.117  128.119.245.12  UDP      1016 37652 → 33520 Len=972
  239 15.181981385 10.225.21.117  128.119.245.12  UDP      1016 44967 → 33519 Len=972
  238 15.181923045 10.225.21.117  128.119.245.12  UDP      1016 39487 → 33518 Len=972
  237 15.181865386 10.225.21.117  128.119.245.12  UDP      1016 53357 → 33517 Len=972
  236 15.181807116 10.225.21.117  128.119.245.12  UDP      1016 35020 → 33516 Len=972
  235 15.181733520 10.225.21.117  128.119.245.12  UDP      1016 59767 → 33515 Len=972
  234 15.181605863 10.225.21.117  128.119.245.12  UDP      1016 43332 → 33514 Len=972
  233 15.181300289 10.225.21.117  128.119.245.12  UDP      1016 33935 → 33513 Len=972
  232 15.181163795 10.225.21.117  128.119.245.12  UDP      1016 38930 → 33512 Len=972
  231 15.181093847 10.225.21.117  128.119.245.12  UDP      1016 50396 → 33511 Len=972
  230 15.180894418 10.225.21.117  128.119.245.12  UDP      1016 34753 → 33510 Len=972
  229 15.180806717 10.225.21.117  128.119.245.12  UDP      1016 52613 → 33509 Len=972
  228 15.180714255 10.225.21.117  128.119.245.12  UDP      1016 57120 → 33508 Len=972
  227 15.180465297 10.225.21.117  128.119.245.12  UDP      1016 37797 → 33507 Len=972
  208 14.303090126 10.225.21.117  128.119.245.12  UDP      1016 59522 → 33506 Len=972
  207 14.302998847 10.225.21.117  128.119.245.12  UDP      1016 37023 → 33505 Len=972
  206 14.302888301 10.225.21.117  128.119.245.12  UDP      1016 43926 → 33504 Len=972
  188 14.023560958 10.225.21.117  128.119.245.12  UDP      1016 34574 → 33503 Len=972
  187 14.023505044 10.225.21.117  128.119.245.12  UDP      1016 33034 → 33502 Len=972
  186 14.023442564 10.225.21.117  128.119.245.12  UDP      1016 39375 → 33501 Len=972
  185 14.023301496 10.225.21.117  128.119.245.12  UDP      1016 50483 → 33500 Len=972
```

```
> Frame 244: 1016 bytes on wire (8128 bits), 1016 bytes captured (8128 bits) on interface any, id 0
> Linux cooked capture v1
v Internet Protocol Version 4, Src: 10.225.21.117, 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: 1000
    Identification: 0x29ea (10730)
  v 000. .... = Flags: 0x0
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 30
    Protocol: UDP (17)
    Header Checksum: 0xd941 [validation disabled]
```

Answer: It is not fragmented because “More fragments” flag is not set (it’s bit is 0).

5-) Which fields in the IP datagram always change from one datagram to the next within this series of UDP messages sent by your computer?

Answer: Time to live, identification and header checksum fields change on each UDP messages sent by our computer.

6-) Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Answer: The fields stay constant:

- Version: since we use IPv4 for all packets
- Header Length: since all the packets are ICMP packets
- Source IP: since we sent requests from same system (PC)
- Destination IP: since we sent requests to same destination
- Differentiated Services Field: since all the packets are ICMP, they use same Type of Service class
- Upper Layer Protocol: since all of them are ICMP packets

The fields must stay constant:

- Same as the above. They must stay constant.

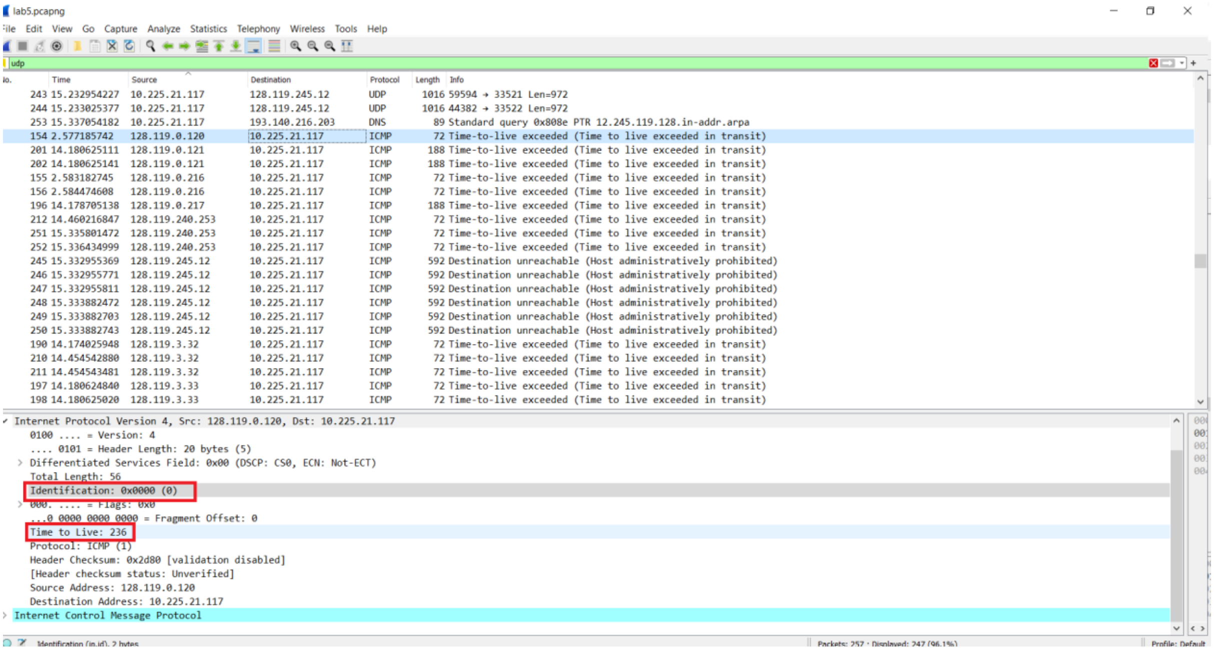
The fields must change:

- Identification: each of the packets must have unique own ID
- Time to Live: traceroute increments each subsequent packet.
- Header Checksum: header changes so checksum must change.

7-) Describe the pattern you see in the values in the Identification field of the IP datagram.

Answer: There isn't any pattern in our packets Identification field, we couldn't observe it. Maybe it is because we examine UDP packets.

8-) What is the value in the Identification field and the TTL field?


lab5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

No.	Time	Source	Destination	Protocol	Length	Info
243	15.232954227	10.225.21.117	128.119.245.12	UDP	1016	59594 → 33521 Len=972
244	15.233025377	10.225.21.117	128.119.245.12	UDP	1016	44382 → 33522 Len=972
253	15.337054182	10.225.21.117	193.140.216.203	DNS	89	Standard query 0x808e PTR 12.245.119.128.in-addr.arpa
154	2.577185742	128.119.0.120	10.225.21.117	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
201	14.180625111	128.119.0.121	10.225.21.117	ICMP	188	Time-to-live exceeded (Time to live exceeded in transit)
202	14.180625141	128.119.0.121	10.225.21.117	ICMP	188	Time-to-live exceeded (Time to live exceeded in transit)
155	2.583182745	128.119.0.216	10.225.21.117	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
156	2.584474608	128.119.0.216	10.225.21.117	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
196	14.178705138	128.119.0.217	10.225.21.117	ICMP	188	Time-to-live exceeded (Time to live exceeded in transit)
212	14.460216847	128.119.240.253	10.225.21.117	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
251	15.335801472	128.119.240.253	10.225.21.117	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
252	15.336434999	128.119.240.253	10.225.21.117	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
245	15.332955369	128.119.245.12	10.225.21.117	ICMP	592	Destination unreachable (Host administratively prohibited)
246	15.332955771	128.119.245.12	10.225.21.117	ICMP	592	Destination unreachable (Host administratively prohibited)
247	15.332955811	128.119.245.12	10.225.21.117	ICMP	592	Destination unreachable (Host administratively prohibited)
248	15.333882472	128.119.245.12	10.225.21.117	ICMP	592	Destination unreachable (Host administratively prohibited)
249	15.333882703	128.119.245.12	10.225.21.117	ICMP	592	Destination unreachable (Host administratively prohibited)
250	15.333882743	128.119.245.12	10.225.21.117	ICMP	592	Destination unreachable (Host administratively prohibited)
190	14.174025948	128.119.3.32	10.225.21.117	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
210	14.454542880	128.119.3.32	10.225.21.117	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
211	14.454543481	128.119.3.32	10.225.21.117	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
197	14.180624840	128.119.3.33	10.225.21.117	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
198	14.180625020	128.119.3.33	10.225.21.117	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)

```
✓ Internet Protocol Version 4, Src: 128.119.0.120, Dst: 10.225.21.117
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x0000 (0)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 236
    Protocol: ICMP (1)
    Header Checksum: 0x2d80 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.0.120
    Destination Address: 10.225.21.117
> Internet Control Message Protocol
```

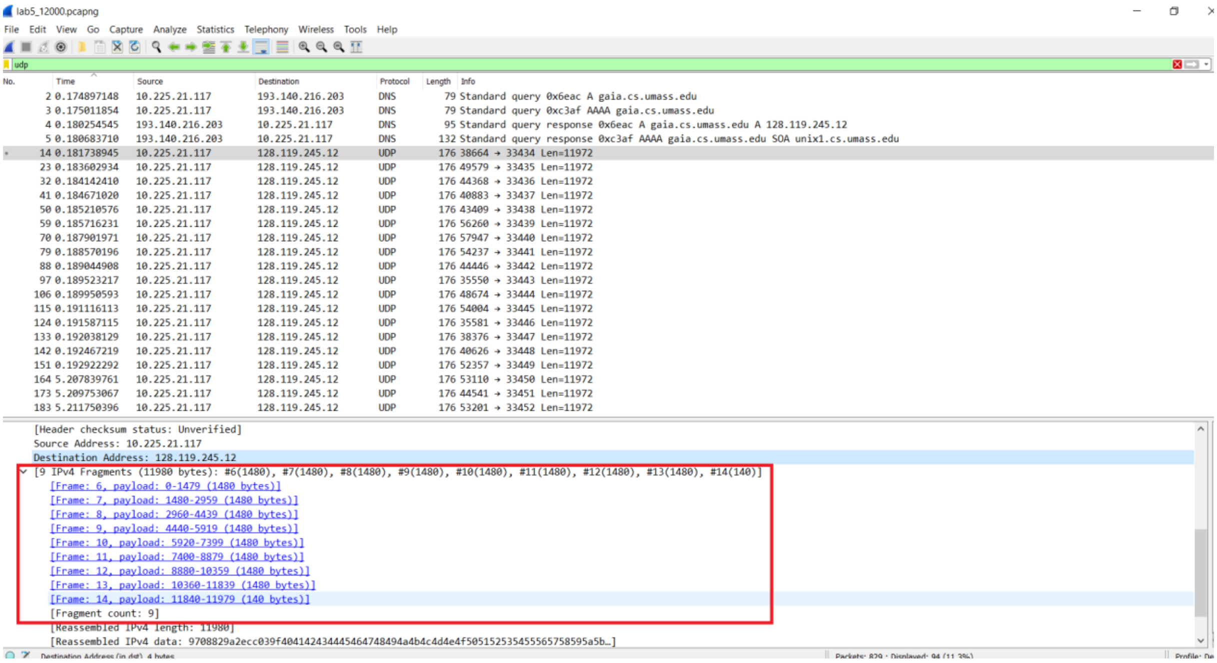
Identification (ip.id), 2 bytes
Packets: 257 · Displayed: 247 (96.1%)
Profile: Default

Answer: Identification field: 0, Time to Live: 236

9-) Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

Answer: The Identification Field varies for each ICMP TTL-exceeded reply as it is unique for every request-reply pair. In the case of fragments of a single large IP datagram, they share the same identification value. The TTL (Time to Live) field remains constant for all replies because the TTL for the first hop router always has the same value.

10-) Find the first UDP segment message that was sent by your computer after you changed the Packet to be 12000. Has that message been fragmented across more than one IP datagram?



lab5_12000.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

```
No.     Time           Source           Destination      Protocol  Length  Info
      2 0.174897148    10.225.21.117    193.140.216.203  DNS           79 Standard query 0x6eac A gaia.cs.umass.edu
      3 0.175011854    10.225.21.117    193.140.216.203  DNS           79 Standard query 0xc3af AAAA gaia.cs.umass.edu
      4 0.180254545    193.140.216.203  10.225.21.117    DNS           95 Standard query response 0x6eac A gaia.cs.umass.edu A 128.119.245.12
      5 0.180683710    193.140.216.203  10.225.21.117    DNS          132 Standard query response 0xc3af AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
     14 0.181738945    10.225.21.117    128.119.245.12   UDP          176 38664 → 33434 Len=11972
     23 0.183602934    10.225.21.117    128.119.245.12   UDP          176 49579 → 33435 Len=11972
     32 0.184142410    10.225.21.117    128.119.245.12   UDP          176 44368 → 33436 Len=11972
     41 0.184671020    10.225.21.117    128.119.245.12   UDP          176 40883 → 33437 Len=11972
     50 0.185210576    10.225.21.117    128.119.245.12   UDP          176 43409 → 33438 Len=11972
     59 0.185716231    10.225.21.117    128.119.245.12   UDP          176 56260 → 33439 Len=11972
     70 0.187901971    10.225.21.117    128.119.245.12   UDP          176 57947 → 33440 Len=11972
     79 0.188570196    10.225.21.117    128.119.245.12   UDP          176 54237 → 33441 Len=11972
     88 0.189044908    10.225.21.117    128.119.245.12   UDP          176 44446 → 33442 Len=11972
     97 0.189523217    10.225.21.117    128.119.245.12   UDP          176 35550 → 33443 Len=11972
    106 0.189950593    10.225.21.117    128.119.245.12   UDP          176 48674 → 33444 Len=11972
    115 0.191116113    10.225.21.117    128.119.245.12   UDP          176 54004 → 33445 Len=11972
    124 0.191587115    10.225.21.117    128.119.245.12   UDP          176 35581 → 33446 Len=11972
    133 0.192038129    10.225.21.117    128.119.245.12   UDP          176 38376 → 33447 Len=11972
    142 0.192467219    10.225.21.117    128.119.245.12   UDP          176 40626 → 33448 Len=11972
    151 0.192922292    10.225.21.117    128.119.245.12   UDP          176 52357 → 33449 Len=11972
    164 5.207839761    10.225.21.117    128.119.245.12   UDP          176 53110 → 33450 Len=11972
    173 5.209753067    10.225.21.117    128.119.245.12   UDP          176 44541 → 33451 Len=11972
    183 5.211750396    10.225.21.117    128.119.245.12   UDP          176 53201 → 33452 Len=11972
```

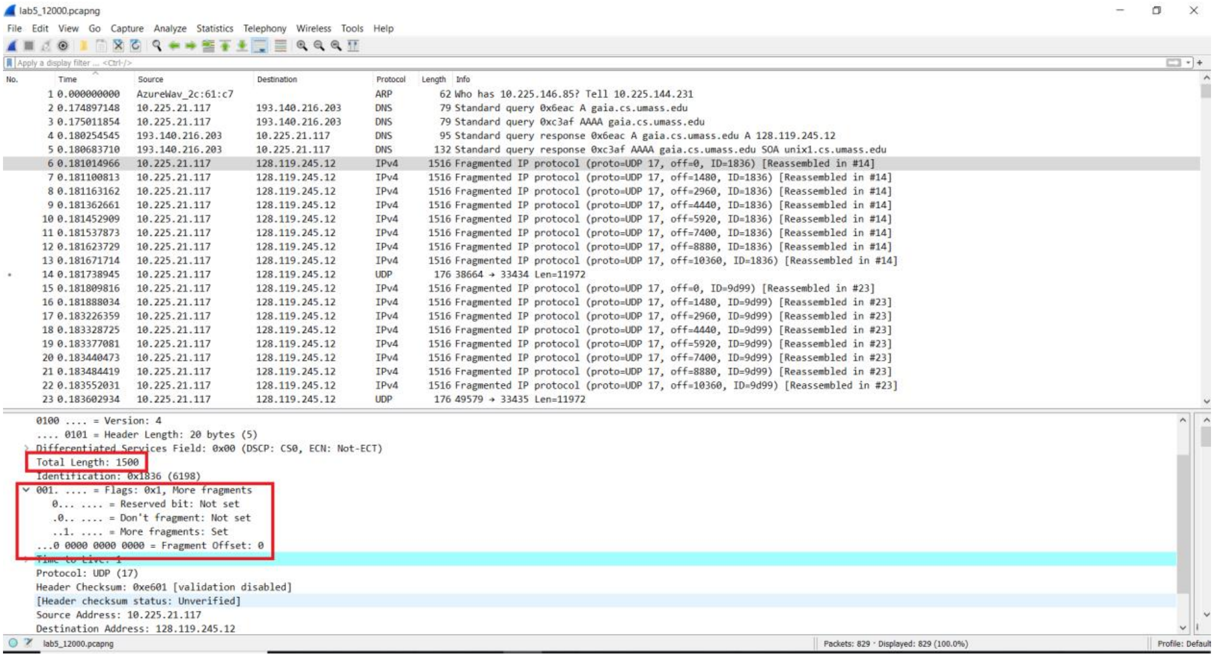
```
    [Header checksum status: Unverified]
    Source Address: 10.225.21.117
    Destination Address: 128.119.245.12
  [9 IPv4 Fragments (11980 bytes): #6(1480), #7(1480), #8(1480), #9(1480), #10(1480), #11(1480), #12(1480), #13(1480), #14(140)]
      [Frame: 6, payload: 0-1479 (1480 bytes)]
      [Frame: 7, payload: 1480-2959 (1480 bytes)]
      [Frame: 8, payload: 2960-4439 (1480 bytes)]
      [Frame: 9, payload: 4440-5919 (1480 bytes)]
      [Frame: 10, payload: 5920-7399 (1480 bytes)]
      [Frame: 11, payload: 7400-8879 (1480 bytes)]
      [Frame: 12, payload: 8880-10359 (1480 bytes)]
      [Frame: 13, payload: 10360-11839 (1480 bytes)]
      [Frame: 14, payload: 11840-11979 (140 bytes)]
      [Fragment count: 9]
      [Reassembled IPv4 length: 11980]
      [Reassembled IPv4 data: 9708829a2ecc039f4041424344454647484494a4b4c4d4e4f505152535455565758595a5b…]
```

Destination Address (ip.dst), 4 bytes
Packets: 829 · Displayed: 94 (11.3%)
Profile: De

Answer:

Yes, the message has been fragmented across more than one IP datagram.

11-) Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?



lab5_12000.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time          Source              Destination       Protocol  Length  Info
    1 0.000000000   AzureWav_2c:61:c7                     ARP         62 Who has 10.225.146.85? Tell 10.225.144.231
    2 0.174897148   10.225.21.117       193.140.216.203   DNS         79 Standard query 0x6eac A gaia.cs.umass.edu
    3 0.175011854   10.225.21.117       193.140.216.203   DNS         79 Standard query 0xc3af AAAA gaia.cs.umass.edu
    4 0.180254545   193.140.216.203     10.225.21.117     DNS         95 Standard query response 0x6eac A gaia.cs.umass.edu A 128.119.245.12
    5 0.180683710   193.140.216.203     10.225.21.117     DNS        132 Standard query response 0xc3af AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
    6 0.181014966   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=0, ID=1836) [Reassembled in #14]
    7 0.181100813   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=1480, ID=1836) [Reassembled in #14]
    8 0.181163162   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=2960, ID=1836) [Reassembled in #14]
    9 0.181362661   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=4440, ID=1836) [Reassembled in #14]
   10 0.181452909   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=5920, ID=1836) [Reassembled in #14]
   11 0.181537873   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=7400, ID=1836) [Reassembled in #14]
   12 0.181623729   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=8880, ID=1836) [Reassembled in #14]
   13 0.181671714   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=10360, ID=1836) [Reassembled in #14]
   14 0.181738945   10.225.21.117       128.119.245.12    UDP        176 38664 → 33434 Len=11972
   15 0.181809816   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=0, ID=9d99) [Reassembled in #23]
   16 0.181888034   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=1480, ID=9d99) [Reassembled in #23]
   17 0.183226359   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=2960, ID=9d99) [Reassembled in #23]
   18 0.183328725   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=4440, ID=9d99) [Reassembled in #23]
   19 0.183377081   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=5920, ID=9d99) [Reassembled in #23]
   20 0.183440473   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=7400, ID=9d99) [Reassembled in #23]
   21 0.183484419   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=8880, ID=9d99) [Reassembled in #23]
   22 0.183552031   10.225.21.117       128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=10360, ID=9d99) [Reassembled in #23]
   23 0.183602934   10.225.21.117       128.119.245.12    UDP        176 49579 → 33435 Len=11972
```

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x1836 (6198)
  v 001. .... = Flags: 0x1, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0xe601 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.225.21.117
    Destination Address: 128.119.245.12
```

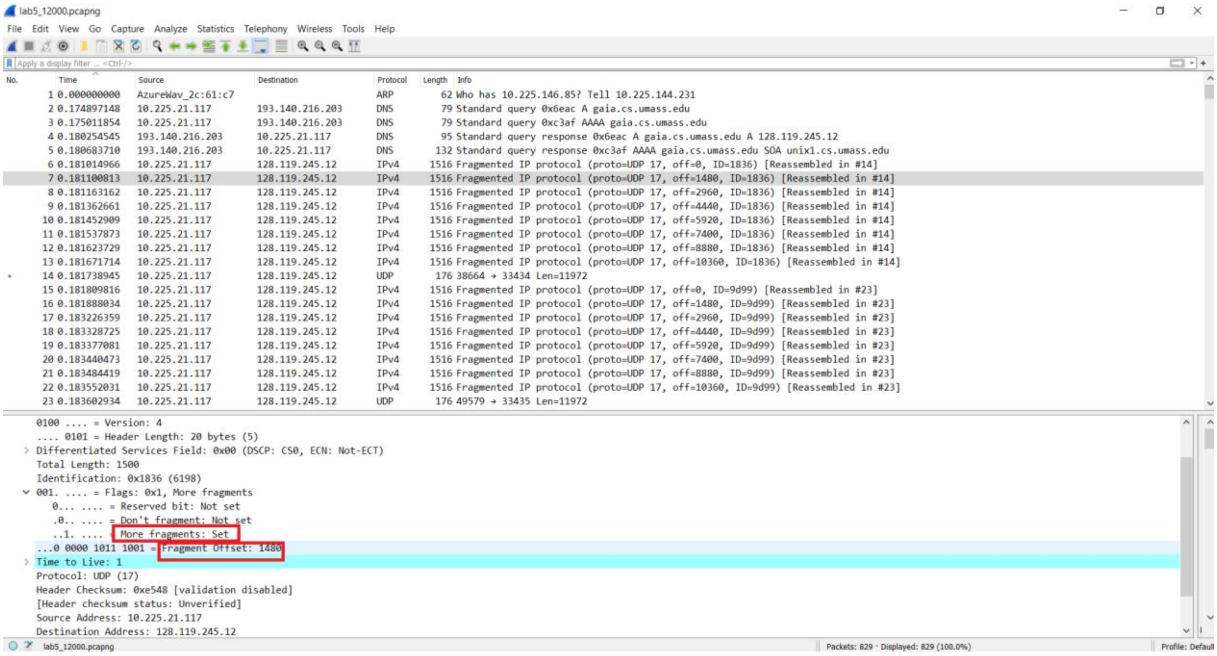
Answer:

The “More fragments” flag in “Flags Section” set to 1, this shows our datagram has been fragmented.

The Fragment Offset field shows this is the first fragment.

This first IP datagram is 1500 bytes.

12-) Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?



```
lab5_12000.pcapng
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
Apply a display filter ... <Ctrl-/>

No.   Time         Source            Destination       Protocol  Length  Info
    1 0.000000000  AzureWav_2c:61:c7                   ARP         62 Who has 10.225.146.85? Tell 10.225.144.231
    2 0.174897148  10.225.21.117     193.140.216.203   DNS         79 Standard query 0x6eac A gaia.cs.umass.edu
    3 0.175011854  10.225.21.117     193.140.216.203   DNS         79 Standard query 0xc3af AAAA gaia.cs.umass.edu
    4 0.180254545  193.140.216.203   10.225.21.117     DNS         95 Standard query response 0x6eac A gaia.cs.umass.edu A 128.119.245.12
    5 0.180683710  193.140.216.203   10.225.21.117     DNS        132 Standard query response 0xc3af AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
    6 0.181014966  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=0, ID=1836) [Reassembled in #14]
    7 0.181100813  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=1480, ID=1836) [Reassembled in #14]
    8 0.181163162  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=2960, ID=1836) [Reassembled in #14]
    9 0.181362661  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=4440, ID=1836) [Reassembled in #14]
   10 0.181452909  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=5920, ID=1836) [Reassembled in #14]
   11 0.181537873  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=7400, ID=1836) [Reassembled in #14]
   12 0.181623729  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=8880, ID=1836) [Reassembled in #14]
   13 0.181671714  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=10360, ID=1836) [Reassembled in #14]
   14 0.181738945  10.225.21.117     128.119.245.12    UDP        176 38664 → 33434 Len=11972
   15 0.181809816  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=0, ID=9d99) [Reassembled in #23]
   16 0.181888034  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=1480, ID=9d99) [Reassembled in #23]
   17 0.183226359  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=2960, ID=9d99) [Reassembled in #23]
   18 0.183328725  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=4440, ID=9d99) [Reassembled in #23]
   19 0.183377081  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=5920, ID=9d99) [Reassembled in #23]
   20 0.183440473  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=7400, ID=9d99) [Reassembled in #23]
   21 0.183484419  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=8880, ID=9d99) [Reassembled in #23]
   22 0.183552031  10.225.21.117     128.119.245.12    IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=10360, ID=9d99) [Reassembled in #23]
   23 0.183602934  10.225.21.117     128.119.245.12    UDP        176 49579 → 33435 Len=11972

    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x1836 (6198)
  v 001. .... = Flags: 0x1, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0000 1011 1001 = Fragment Offset: 1480
  > Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0xe548 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.225.21.117
    Destination Address: 128.119.245.12

lab5_12000.pcapng                    Packets: 829 · Displayed: 829 (100.0%)        Profile: Default
```

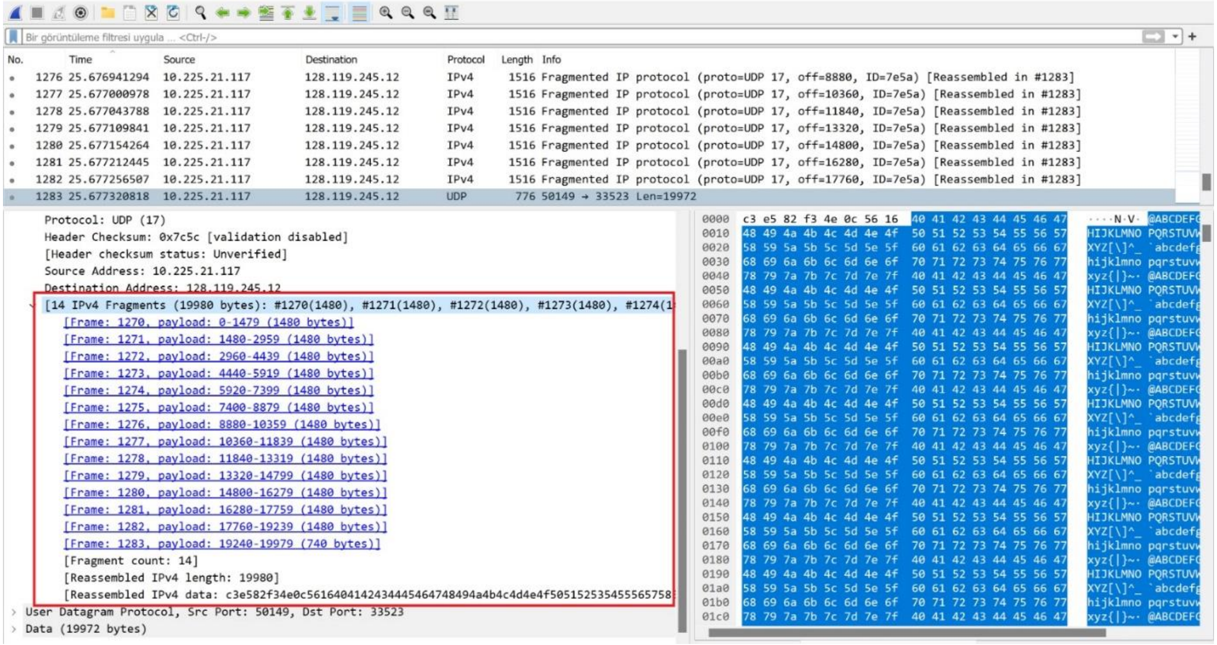
Answer: It is not the first fragmented IP datagram since the fragment offset is 1480.

There are more fragments because more fragments is set to 1.

13-) What fields change in the IP header between the first and second fragment?

Answer: total length, fragment offset and header checksum change. Flags are the same.

14-) How many fragments were created from the original datagram?



```
Bir görüntüleme filtresi uygula ... <Ctrl-/>

No.    Time          Source          Destination      Protocol  Length  Info
• 1276 25.676941294  10.225.21.117   128.119.245.12   IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=8880, ID=7e5a) [Reassembled in #1283]
• 1277 25.677000978  10.225.21.117   128.119.245.12   IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=10360, ID=7e5a) [Reassembled in #1283]
• 1278 25.677043788  10.225.21.117   128.119.245.12   IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=11840, ID=7e5a) [Reassembled in #1283]
• 1279 25.677109841  10.225.21.117   128.119.245.12   IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=13320, ID=7e5a) [Reassembled in #1283]
• 1280 25.677154264  10.225.21.117   128.119.245.12   IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=14800, ID=7e5a) [Reassembled in #1283]
• 1281 25.677212445  10.225.21.117   128.119.245.12   IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=16280, ID=7e5a) [Reassembled in #1283]
• 1282 25.677256507  10.225.21.117   128.119.245.12   IPv4      1516 Fragmented IP protocol (proto=UDP 17, off=17760, ID=7e5a) [Reassembled in #1283]
• 1283 25.677320818  10.225.21.117   128.119.245.12   UDP        776 50149 → 33523 Len=19972

    Protocol: UDP (17)
    Header Checksum: 0x7c5c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.225.21.117
    Destination Address: 128.119.245.12
  v [14 IPv4 Fragments (19980 bytes): #1270(1480), #1271(1480), #1272(1480), #1273(1480), #1274(1
      [Frame: 1270, payload: 0-1479 (1480 bytes)]
      [Frame: 1271, payload: 1480-2959 (1480 bytes)]
      [Frame: 1272, payload: 2960-4439 (1480 bytes)]
      [Frame: 1273, payload: 4440-5919 (1480 bytes)]
      [Frame: 1274, payload: 5920-7399 (1480 bytes)]
      [Frame: 1275, payload: 7400-8879 (1480 bytes)]
      [Frame: 1276, payload: 8880-10359 (1480 bytes)]
      [Frame: 1277, payload: 10360-11839 (1480 bytes)]
      [Frame: 1278, payload: 11840-13319 (1480 bytes)]
      [Frame: 1279, payload: 13320-14799 (1480 bytes)]
      [Frame: 1280, payload: 14800-16279 (1480 bytes)]
      [Frame: 1281, payload: 16280-17759 (1480 bytes)]
      [Frame: 1282, payload: 17760-19239 (1480 bytes)]
      [Frame: 1283, payload: 19240-19979 (740 bytes)]
      [Fragment count: 14]
      [Reassembled IPv4 length: 19980]
      [Reassembled IPv4 data: c3e582f34e0c5616404142434445464748494a4b4c4d4e4f505152535455565758
  > User Datagram Protocol, Src Port: 50149, Dst Port: 33523
  > Data (19972 bytes)

0000  c3 e5 82 f3 4e 0c 56 16  40 41 42 43 44 45 46 47   ····N·V· @ABCDEF
0010  48 49 4a 4b 4c 4d 4e 4f  50 51 52 53 54 55 56 57   HIJKLMNO PQRSTUV
0020  58 59 5a 5b 5c 5d 5e 5f  60 61 62 63 64 65 66 67   XYZ[\]^_ `abcdef
0030  68 69 6a 6b 6c 6d 6e 6f  70 71 72 73 74 75 76 77   hijklmno pqrstuv
0040  78 79 7a 7b 7c 7d 7e 7f  40 41 42 43 44 45 46 47   xyz{|}~· @ABCDEF
0050  48 49 4a 4b 4c 4d 4e 4f  50 51 52 53 54 55 56 57   HIJKLMNO PQRSTUV
0060  58 59 5a 5b 5c 5d 5e 5f  60 61 62 63 64 65 66 67   XYZ[\]^_ `abcdef
0070  68 69 6a 6b 6c 6d 6e 6f  70 71 72 73 74 75 76 77   hijklmno pqrstuv
0080  78 79 7a 7b 7c 7d 7e 7f  40 41 42 43 44 45 46 47   xyz{|}~· @ABCDEF
0090  48 49 4a 4b 4c 4d 4e 4f  50 51 52 53 54 55 56 57   HIJKLMNO PQRSTUV
00a0  58 59 5a 5b 5c 5d 5e 5f  60 61 62 63 64 65 66 67   XYZ[\]^_ `abcdef
00b0  68 69 6a 6b 6c 6d 6e 6f  70 71 72 73 74 75 76 77   hijklmno pqrstuv
00c0  78 79 7a 7b 7c 7d 7e 7f  40 41 42 43 44 45 46 47   xyz{|}~· @ABCDEF
00d0  48 49 4a 4b 4c 4d 4e 4f  50 51 52 53 54 55 56 57   HIJKLMNO PQRSTUV
00e0  58 59 5a 5b 5c 5d 5e 5f  60 61 62 63 64 65 66 67   XYZ[\]^_ `abcdef
00f0  68 69 6a 6b 6c 6d 6e 6f  70 71 72 73 74 75 76 77   hijklmno pqrstuv
0100  78 79 7a 7b 7c 7d 7e 7f  40 41 42 43 44 45 46 47   xyz{|}~· @ABCDEF
0110  48 49 4a 4b 4c 4d 4e 4f  50 51 52 53 54 55 56 57   HIJKLMNO PQRSTUV
0120  58 59 5a 5b 5c 5d 5e 5f  60 61 62 63 64 65 66 67   XYZ[\]^_ `abcdef
0130  68 69 6a 6b 6c 6d 6e 6f  70 71 72 73 74 75 76 77   hijklmno pqrstuv
0140  78 79 7a 7b 7c 7d 7e 7f  40 41 42 43 44 45 46 47   xyz{|}~· @ABCDEF
0150  48 49 4a 4b 4c 4d 4e 4f  50 51 52 53 54 55 56 57   HIJKLMNO PQRSTUV
0160  58 59 5a 5b 5c 5d 5e 5f  60 61 62 63 64 65 66 67   XYZ[\]^_ `abcdef
0170  68 69 6a 6b 6c 6d 6e 6f  70 71 72 73 74 75 76 77   hijklmno pqrstuv
0180  78 79 7a 7b 7c 7d 7e 7f  40 41 42 43 44 45 46 47   xyz{|}~· @ABCDEF
0190  48 49 4a 4b 4c 4d 4e 4f  50 51 52 53 54 55 56 57   HIJKLMNO PQRSTUV
01a0  58 59 5a 5b 5c 5d 5e 5f  60 61 62 63 64 65 66 67   XYZ[\]^_ `abcdef
01b0  68 69 6a 6b 6c 6d 6e 6f  70 71 72 73 74 75 76 77   hijklmno pqrstuv
01c0  78 79 7a 7b 7c 7d 7e 7f  40 41 42 43 44 45 46 47   xyz{|}~· @ABCDEF
```

Answer: The original datagram was fragmented into 14 IPv4 fragments.

15-) What fields change in the IP header among the fragments?

Answer:

Fragment Offset: This field changes among the fragments as it indicates the position

More Fragments (MF) flag: this flag is set to 1 except the last one.

Total Length: last packet is 740 bytes.

Header Checksum: packets header checksum changes on each fragment