



Lab 3

1. Select the first ICMP Echo Request 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?

Answer

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694 Destination port: 33435
2	0.00134100	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
3	0.00182800	192.168.1.8	192.168.1.1	DNS	67	Standard query 0xf944 A mac-air
4	0.00266500	192.168.1.1	192.168.1.8	DNS	83	Standard query response 0xf944 A 192.168.1.8
5	0.00299100	192.168.1.8	192.168.1.1	DNS	84	Standard query 0x7984 PTR 1.1.168.192.in-addr.arpa
6	0.00383300	192.168.1.1	192.168.1.8	DNS	104	Standard query response 0x7984 PTR DD-WRT
7	0.00406900	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694 Destination port: 33436
8	0.00468700	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
9	0.00478900	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694 Destination port: 33437
10	0.00537500	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)

<ul style="list-style-type: none"> ▣ Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0 ▣ Ethernet II, Src: Apple_1f:d4:56 (b8:e8:56:1f:d4:56), Dst: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9) ▣ Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 128.119.245.12 (128.119.245.12) <ul style="list-style-type: none"> Version: 4 Header length: 20 bytes ▣ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) Total Length: 56 Identification: 0xae97 (44695) ▣ Flags: 0x00 <ul style="list-style-type: none"> 0... = Reserved bit: Not set .0.. = Don't fragment: Not set ..0. = More fragments: Not set Fragment offset: 0 ▣ Time to live: 1 Protocol: UDP (17) ▣ Header checksum: 0xd3e9 [correct] Source: 192.168.1.8 (192.168.1.8) Destination: 128.119.245.12 (128.119.245.12) <ul style="list-style-type: none"> [Source GeoIP: Unknown] [Destination GeoIP: Unknown] ▣ User Datagram Protocol, Src Port: 44694 (44694), Dst Port: 33435 (33435)

Figure 1

According to the figure 1, the IP address of my computer is 192.168.1.8.

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

Answer

According to the figure 1, within the IP packet header, the value in the upper layer protocol field 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.

Answer

According to the figure 1, the header length is 20 bytes and the total length is 56 bytes. Therefore, the payload of the IP datagram should be 36 bytes (56 bytes – 20 bytes).

Home Page: <http://uniteng.com>

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

Answer

According to the figure 1, under flags section, the more fragments bit = 0, so the data is not fragmented.

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

Answer

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694 Destination port: 33435
2	0.00134100	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
3	0.00182800	192.168.1.8	192.168.1.1	DNS	67	Standard query 0xf944 A mac-air
4	0.00266500	192.168.1.1	192.168.1.8	DNS	83	Standard query response 0xf944 A 192.168.1.8
5	0.00299100	192.168.1.8	192.168.1.1	DNS	84	Standard query 0x7984 PTR 1.1.168.192.in-addr.arpa
6	0.00383300	192.168.1.1	192.168.1.8	DNS	104	Standard query response 0x7984 PTR DD-WRT
7	0.00406900	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694 Destination port: 33436
8	0.00468700	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
9	0.00478900	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694 Destination port: 33437
10	0.00537500	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)

```

[+] Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
[+] Ethernet II, Src: Apple_I_f:d4:56 (b8:e8:56:1f:d4:56), Dst: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
[+] Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 128.119.245.12 (128.119.245.12)
  Version: 4
  Header length: 20 bytes
  [x] Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 56
  Identification: 0xae97 (44695)
  [x] Flags: 0x00
    0... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..0... .... = More fragments: Not set
  Fragment offset: 0
  [x] Time to live: 1
  Protocol: UDP (17)
  [x] Header checksum: 0xd3e9 [correct]
  Source: 192.168.1.8 (192.168.1.8)
  Destination: 128.119.245.12 (128.119.245.12)
  [Source GeolP: Unknown]
  [Destination GeolP: Unknown]
[+] User Datagram Protocol, Src Port: 44694 (44694), Dst Port: 33435 (33435)

```

Home Page: <http://uniteng.com>

No.	Time	Source	Destination	Protocol	Length	Info
3	0.00182800	192.168.1.8	192.168.1.1	DNS	67	Standard query 0xf944 A mac-air
4	0.00266500	192.168.1.1	192.168.1.8	DNS	83	Standard query response 0xf944 A 192.168.1.8
5	0.00299100	192.168.1.8	192.168.1.1	DNS	84	Standard query 0x7984 PTR 1.1.168.192.in-addr.arpa
6	0.00383300	192.168.1.1	192.168.1.8	DNS	104	Standard query response 0x7984 PTR DD-WRT
7	0.00406900	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694 Destination port: 33436
8	0.00468700	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
9	0.00478900	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694 Destination port: 33437
10	0.00537500	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
11	0.00548500	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694 Destination port: 33438
12	0.01457000	10.35.48.1	192.168.1.8	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

```

Frame 11: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
Ethernet II, Src: Apple_1f:d4:56 (b8:e8:56:1f:d4:56), Dst: Tp-Linkt_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 128.119.245.12 (128.119.245.12)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 56
  Identification: 0xae9a (44698)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 2
  Protocol: UDP (17)
  Header checksum: 0xd2e6 [correct]
  Source: 192.168.1.8 (192.168.1.8)
  Destination: 128.119.245.12 (128.119.245.12)
  [Source GeoIP: unknown]
  [Destination GeoIP: unknown]
User Datagram Protocol, Src Port: 44694 (44694), Dst Port: 33438 (33438)

```

According to above two screenshots, identification, Time to live and Header checksum always change.

6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Answer

The fields that stay constant are:

Version (since we are using IPv4), header length (since these are UDP packets), source IP (since all packets are sent from my computer), destination IP (since we are sending to the same host), Differentiated Services (since all packets are UDP), Upper Layer Protocol (since these are UDP packets)

The fields that must stay constant are:

Version (since we are using IPv4), header length (since these are UDP packets), source IP (since all packets are sent from my computer), destination IP (since we are sending to the same host), Differentiated Services (since all packets are UDP), Upper Layer Protocol (since these are UDP packets)

The fields that must change are:

Identification (IP packets have different ids), Time to live (traceroute increments each packet), Header checksum (since header changes)

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

Answer

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694 Destination port: 33435
2	0.00134100	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
3	0.00182800	192.168.1.8	192.168.1.1	DNS	67	Standard query 0xf944 A mac-air
4	0.00266500	192.168.1.1	192.168.1.8	DNS	83	Standard query response 0xf944 A 192.168.1.8
5	0.00299100	192.168.1.8	192.168.1.1	DNS	84	Standard query 0x7984 PTR 1.1.168.192.in-addr.arpa
6	0.00383300	192.168.1.1	192.168.1.8	DNS	104	Standard query response 0x7984 PTR DD-WRT
7	0.00406900	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694 Destination port: 33436
8	0.00468700	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
9	0.00478900	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694 Destination port: 33437
10	0.00537500	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)

Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
 Ethernet II, Src: Apple1f:d4:56 (b8:e8:56:1f:d4:56), Dst: Tp-LinkTf8:6d:f9 (a0:f3:c1:f8:6d:f9)
 Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 128.119.245.12 (128.119.245.12)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
 Total Length: 56
 Identification: 0xae97 (44695)

The first request, values in the identification: 44695

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694 Destination port: 33435
2	0.00134100	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
3	0.00182800	192.168.1.8	192.168.1.1	DNS	67	Standard query 0xf944 A mac-air
4	0.00266500	192.168.1.1	192.168.1.8	DNS	83	Standard query response 0xf944 A 192.168.1.8
5	0.00299100	192.168.1.8	192.168.1.1	DNS	84	Standard query 0x7984 PTR 1.1.168.192.in-addr.arpa
6	0.00383300	192.168.1.1	192.168.1.8	DNS	104	Standard query response 0x7984 PTR DD-WRT
7	0.00406900	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694 Destination port: 33436
8	0.00468700	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
9	0.00478900	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694 Destination port: 33437
10	0.00537500	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)

Frame 7: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
 Ethernet II, Src: Apple1f:d4:56 (b8:e8:56:1f:d4:56), Dst: Tp-LinkTf8:6d:f9 (a0:f3:c1:f8:6d:f9)
 Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 128.119.245.12 (128.119.245.12)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
 Total Length: 56
 Identification: 0xae98 (44696)

The second request, values in the identification: 44696

According to above two screenshots, the pattern is the IP header Identification field increment with each UDP request.

8. What is the value in the Identification field and the TTL field?

Answer

Home Page: <http://uniteng.com>

1	0.00000000	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694	Destination port: 33435
2	0.00134100	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)	
3	0.00182800	192.168.1.8	192.168.1.1	DNS	67	Standard query 0xf944 A mac-air	
4	0.00266500	192.168.1.1	192.168.1.8	DNS	83	Standard query response 0xf944 A 192.168.1.8	
5	0.00299100	192.168.1.8	192.168.1.1	DNS	84	Standard query 0x7984 PTR 1.1.168.192.in-addr.arpa	
6	0.00383300	192.168.1.1	192.168.1.8	DNS	104	Standard query response 0x7984 PTR DD-WRT	
7	0.00406900	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694	Destination port: 33436
8	0.00468700	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)	
9	0.00478900	192.168.1.8	128.119.245.12	UDP	70	Source port: 44694	Destination port: 33437
10	0.00537500	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)	

Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
 Ethernet II, Src: Tp-Link_Tf8:6d:f9 (a0:f3:c1:f8:6d:f9), Dst: Apple_1f:d4:56 (b8:e8:56:1f:d4:56)
 Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.8 (192.168.1.8)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0xc0 (DSCP 0x30: Class selector 6; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
 Total Length: 84
 Identification: 0xdef5 (57077)
 Flags: 0x00
 0... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
 Fragment offset: 0
 Time to live: 64
 Protocol: ICMP (1)

According to above screenshot, Identification: 57077, TTL: 64

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 values of identification field changes for all the ICMP TTL-exceeded replies since the identification field is a unique value. If two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram.

The TTL field was unchanged since the TTL for the nearest router is always the same (Linux, TTL 64).

10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

Answer

101	5.32732600	192.168.1.8	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae98) [R]	
102	5.32732700	192.168.1.8	128.119.245.12	UDP	534	Source port: 44695	Destination port: 33435
103	5.32907900	192.168.1.1	192.168.1.8	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)	
104	5.32965400	192.168.1.8	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae99) [R]	
105	5.32965600	192.168.1.8	128.119.245.12	UDP	534	Source port: 44695	Destination port: 33436
106	5.33044100	192.168.1.1	192.168.1.8	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)	
107	5.33054400	192.168.1.8	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae9a) [R]	
108	5.33054500	192.168.1.8	128.119.245.12	UDP	534	Source port: 44695	Destination port: 33437
109	5.33132200	192.168.1.1	192.168.1.8	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)	
110	5.33142200	192.168.1.8	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae9b) [R]	

Frame 101: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
 Ethernet II, Src: Apple_1f:d4:56 (b8:e8:56:1f:d4:56), Dst: Tp-Link_Tf8:6d:f9 (a0:f3:c1:f8:6d:f9)
 Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 128.119.245.12 (128.119.245.12)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
 Total Length: 1500
 Identification: 0xae98 (44696)

No. 101 has identification: 44696

No.	Time	Source	Destination	Protocol	Length	Info
100	2.78212400	128.119.245.12	192.168.1.8	ICMP	98	Destination unreachable (Port unreachable)
101	5.32732600	192.168.1.8	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae98) [R]
102	5.32732700	192.168.1.8	128.119.245.12	UDP	534	Source port: 44695 Destination port: 33435
103	5.32907900	192.168.1.1	192.168.1.8	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
104	5.32965400	192.168.1.8	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae99) [R]
105	5.32965600	192.168.1.8	128.119.245.12	UDP	534	Source port: 44695 Destination port: 33436
106	5.33044100	192.168.1.1	192.168.1.8	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
107	5.33054400	192.168.1.8	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae9a) [R]
108	5.33054500	192.168.1.8	128.119.245.12	UDP	534	Source port: 44695 Destination port: 33437
109	5.33132200	192.168.1.1	192.168.1.8	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
110	5.33132300	192.168.1.8	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae9b) [R]

```

Frame 102: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0
Ethernet II, Src: Apple_1f:d4:56 (b8:e8:56:1f:d4:56), Dst: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 128.119.245.12 (128.119.245.12)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 520
  Identification: 0xae98 (44696)

```

No. 102 has identification: 44696

According to above to screenshots, above 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?

Answer

No.	Time	Source	Destination	Protocol	Length	Info
100	2.78212400	128.119.245.12	192.168.1.8	ICMP	98	Destination unreachable (Port unreachable)
101	5.32732600	192.168.1.8	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae98) [R]
102	5.32732700	192.168.1.8	128.119.245.12	UDP	534	Source port: 44695 Destination port: 33435
103	5.32907900	192.168.1.1	192.168.1.8	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
104	5.32965400	192.168.1.8	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae99) [R]
105	5.32965600	192.168.1.8	128.119.245.12	UDP	534	Source port: 44695 Destination port: 33436
106	5.33044100	192.168.1.1	192.168.1.8	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
107	5.33054400	192.168.1.8	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae9a) [R]
108	5.33054500	192.168.1.8	128.119.245.12	UDP	534	Source port: 44695 Destination port: 33437
109	5.33132200	192.168.1.1	192.168.1.8	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
110	5.33132300	192.168.1.8	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae9b) [R]

```

Frame 101: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Ethernet II, Src: Apple_1f:d4:56 (b8:e8:56:1f:d4:56), Dst: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 128.119.245.12 (128.119.245.12)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 1500
  Identification: 0xae98 (44696)
  Flags: 0x01 (More Fragments)
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
  Fragment offset: 0
  Time to live: 1
  Protocol: UDP (17)
  Header checksum: 0xae44 [correct]
  Source: 192.168.1.8 (192.168.1.8)
  Destination: 128.119.245.12 (128.119.245.12)
  [Source GeoIP: unknown]
  [Destination GeoIP: unknown]
  Reassembled IPv4 in frame: 102

```

According to above screenshot, The Flags bit for more fragments is set which means the datagram has been fragmented. The fragment offset is 0, we know this is the first fragment. The length of this first datagram is 1500 including the header.

Home Page: <http://uniteng.com>

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 there more fragments? How can you tell?

Answer

No.	Time	Source	Destination	Protocol	Length	Info
100	2.78212400	128.119.245.12	192.168.1.8	ICMP	98	Destination unreachable (Port unreachable)
101	5.32732600	192.168.1.8	128.119.245.12	IPV4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae98) [F
102	5.32732700	192.168.1.8	128.119.245.12	UDP	534	Source port: 44695 Destination port: 33435
103	5.32907900	192.168.1.1	192.168.1.8	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
104	5.32965400	192.168.1.8	128.119.245.12	IPV4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae99) [F
105	5.32965600	192.168.1.8	128.119.245.12	UDP	534	Source port: 44695 Destination port: 33436
106	5.33044100	192.168.1.1	192.168.1.8	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
107	5.33054400	192.168.1.8	128.119.245.12	IPV4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae9a) [F
108	5.33054500	192.168.1.8	128.119.245.12	UDP	534	Source port: 44695 Destination port: 33437
109	5.33132200	192.168.1.1	192.168.1.8	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
110	5.33132300	192.168.1.8	128.119.245.12	IPV4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae9b) [F

Frame 102: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0
 Ethernet II, Src: Apple_1f:d4:56 (b8:e8:56:1f:d4:56), Dst: Tp-Link_t_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
 Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 128.119.245.12 (128.119.245.12)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
 Total Length: 520
 Identification: 0xae98 (44696)
 Flags: 0x00
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0... = More fragments: Not set
 Fragment offset: 1480
 Time to live: 1
 Protocol: UDP (17)
 Header checksum: 0xd15f [correct]
 Source: 192.168.1.8 (192.168.1.8)
 Destination: 128.119.245.12 (128.119.245.12)
 [Source GeoIP: unknown]
 [Destination GeoIP: unknown]
 [7] IPv4 Fragments (1980 bytes): #101(1480). #102(500)

According to above screenshot, this is not the first fragment since the fragment offset is 1480 and this should be the last fragment, since the status of more fragments flag is not set.

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

Answer

Total length, flags, fragment offset, and checksum.

14. How many fragments were created from the original datagram?

Answer

Home Page: <http://uniteng.com>

No.	Time	Source	Destination	Protocol	Length	Info
243	27.8273800	Apple_1f:d4:56	Tp-LinkT_f8:6d:f9	ARP	42	192.168.1.8 is at b8:e8:56:1f:d4:56
244	28.5736730	192.168.1.8	128.119.245.12	IPV4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae99) [R]
245	28.5736740	192.168.1.8	128.119.245.12	IPV4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=ae99) [R]
246	28.5736750	192.168.1.8	128.119.245.12	UDP	554	Source port: 44696 Destination port: 33435
247	28.5757440	192.168.1.1	192.168.1.8	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
248	28.5761460	192.168.1.8	192.168.1.1	DNS	67	Standard query 0x3dec A mac-air
249	28.5770350	192.168.1.1	192.168.1.8	DNS	83	Standard query response 0x3dec A 192.168.1.8
250	28.5773800	192.168.1.8	192.168.1.1	DNS	84	Standard query 0x916b PTR 1.1.168.192.in-addr.arpa
251	28.5782660	192.168.1.1	192.168.1.8	DNS	104	Standard query response 0x916b PTR DD-WRT
252	28.5784500	192.168.1.8	128.119.245.12	IPV4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=ae9a) [R]

Frame 244: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
 Ethernet II, Src: Apple_1f:d4:56 (b8:e8:56:1f:d4:56), Dst: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
 Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 128.119.245.12 (128.119.245.12)

```

Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 1500
Identification: 0xae99 (44697)
Flags: 0x01 (More Fragments)
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..1. .... = More fragments: Set
Fragment offset: 0
Time to live: 1
Protocol: UDP (17)
Header checksum: 0xae43 [correct]
Source: 192.168.1.8 (192.168.1.8)
Destination: 128.119.245.12 (128.119.245.12)
[Source GeolP: Unknown]
[Destination GeolP: Unknown]
reassembled toM in frame: 246
  
```

According to above screenshot, 3 packets created from the original datagram.

15. What fields change in the IP header among the fragments?

Answer

Fragment offset, checksum. Moreover, for the first two packets, the total length is 1500 with the more fragments flag set to 1, and the third packet's total length is 540 with the more fragments flag set to 0.