

**COMPUTER NETWORKING**  
**WIRESHARK LAB: IP**  
**BY:**  
**MONIL SHAH**  
**mds747**

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?

Ans) 192.168.1.1

No.	Time	Source	Destination	Protocol	Length	Info
1	12:17:53.287459	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
2	12:17:56.768970	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
3	12:17:57.793774	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
4	12:17:58.817049	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
5	12:17:59.312401	192.168.1.161	192.168.1.1	DNS	77	Standard query 0x179c A gaia.cs.umass.edu
6	12:17:59.328510	192.168.1.1	192.168.1.161	DNS	93	Standard query response 0x179c A gaia.cs.umass.edu A 128.119.245.12
7	12:17:59.329464	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
8	12:17:59.333180	192.168.1.1	192.168.1.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
9	12:17:59.333900	192.168.1.161	192.168.1.1	DNS	84	Standard query 0xdad9 PTR 1.1.168.192.in-addr.arpa
10	12:17:59.335497	192.168.1.1	192.168.1.161	DNS	165	Standard query response 0xdad9 PTR 1.1.168.192.in-addr.arpa PTR FIOS_Quantum
11	12:17:59.335825	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
12	12:17:59.336847	192.168.1.1	192.168.1.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
13	12:17:59.336970	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
14	12:17:59.337904	192.168.1.1	192.168.1.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
15	12:17:59.338057	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
16	12:17:59.340279	98.109.25.1	192.168.1.161	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
Ethernet II, Src: Verizon\_f1:47:66 (48:5d:36:f1:47:66), Dst: Apple\_9c:a6:65 (4c:32:75:9c:a6:65)  
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.161  
 0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)  
Total Length: 84  
Identification: 0x449c (17564)  
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)  
Header checksum: 0xb15a [validation disabled]

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

Ans.) ICMP (1)

No.	Time	Source	Destination	Protocol	Length	Info
1	12:17:53.287459	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
2	12:17:56.768970	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
3	12:17:57.793774	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
4	12:17:58.817049	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
5	12:17:59.312401	192.168.1.161	192.168.1.1	DNS	77	Standard query 0x179c A gaia.cs.umass.edu
6	12:17:59.328510	192.168.1.1	192.168.1.161	DNS	93	Standard query response 0x179c A gaia.cs.umass.edu A 128.119.245.12
7	12:17:59.329464	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
8	12:17:59.333189	192.168.1.1	192.168.1.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
9	12:17:59.333908	192.168.1.161	192.168.1.1	DNS	84	Standard query 0xdad9 PTR 1.1.168.192.in-addr.arpa
10	12:17:59.335497	192.168.1.1	192.168.1.161	DNS	165	Standard query response 0xdad9 PTR 1.1.168.192.in-addr.arpa PTR FIOS_Quantum
11	12:17:59.335825	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
12	12:17:59.336847	192.168.1.1	192.168.1.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
13	12:17:59.336970	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
14	12:17:59.337904	192.168.1.1	192.168.1.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
15	12:17:59.338057	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
16	12:17:59.340279	98.109.25.1	192.168.1.161	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

► Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
 ► Ethernet II, Src: Verizon\_f1:47:66 (48:5d:36:f1:47:66), Dst: Apple\_9c:a6:65 (4c:32:75:9c:a6:65)  
 ▼ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.161  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)  
 Total Length: 84  
 Identification: 0x449c (17564)  
 ▼ Flags: 0x00  
 ... .... = 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) (1)  
 Header checksum: 0xb15a [validation disabled]

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.

Ans.) IP Header Length = 20 bytes

Payload bytes in IP datagram = 64 bytes

Payload bytes in IP datagram = Total length - Header length

No.	Time	Source	Destination	Protocol	Length	Info
1	12:17:53.287459	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
2	12:17:56.768970	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
3	12:17:57.793774	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
4	12:17:58.817049	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
5	12:17:59.312401	192.168.1.161	192.168.1.1	DNS	77	Standard query 0x179c A gaia.cs.umass.edu
6	12:17:59.328510	192.168.1.1	192.168.1.161	DNS	93	Standard query response 0x179c A gaia.cs.umass.edu A 128.119.245.12
7	12:17:59.329464	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
8	12:17:59.333189	192.168.1.1	192.168.1.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
9	12:17:59.333908	192.168.1.161	192.168.1.1	DNS	84	Standard query 0xdad9 PTR 1.1.168.192.in-addr.arpa
10	12:17:59.335497	192.168.1.1	192.168.1.161	DNS	165	Standard query response 0xdad9 PTR 1.1.168.192.in-addr.arpa PTR FIOS_Quantum
11	12:17:59.335825	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
12	12:17:59.336847	192.168.1.1	192.168.1.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
13	12:17:59.336970	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
14	12:17:59.337904	192.168.1.1	192.168.1.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
15	12:17:59.338057	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
16	12:17:59.340279	98.109.25.1	192.168.1.161	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

► Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
 ► Ethernet II, Src: Verizon\_f1:47:66 (48:5d:36:f1:47:66), Dst: Apple\_9c:a6:65 (4c:32:75:9c:a6:65)  
 ▼ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.161  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)  
 Total Length: 84  
 Identification: 0x449c (17564)  
 ▼ Flags: 0x00  
 ... .... = 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) (1)  
 Header checksum: 0xb15a [validation disabled]

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

Ans.) IP datagram is not fragmented. The datagram is not fragment as in the Flags : 0x00 -> More Fragments : Not Set.

Refer Fig. below

No.	Time	Source	Destination	Protocol	Length	Info
1	12:17:53.287459	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
2	12:17:56.768970	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
3	12:17:57.793774	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
4	12:17:58.817049	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
5	12:17:59.312401	192.168.1.161	192.168.1.1	DNS	77	Standard query 0x179c A gaia.cs.umass.edu
6	12:17:59.328510	192.168.1.1	192.168.1.161	DNS	93	Standard query response 0x179c A gaia.cs.umass.edu A 128.119.245.12
7	12:17:59.329464	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
8	12:17:59.333189	192.168.1.1	192.168.1.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
9	12:17:59.333908	192.168.1.161	192.168.1.1	DNS	84	Standard query 0xdad9 PTR 1.1.168.192.in-addr.arpa
10	12:17:59.335497	192.168.1.1	192.168.1.161	DNS	165	Standard query response 0xdad9 PTR 1.1.168.192.in-addr.arpa PTR FIOS_Quantum
11	12:17:59.335825	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
12	12:17:59.336847	192.168.1.1	192.168.1.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
13	12:17:59.336970	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
14	12:17:59.337904	192.168.1.1	192.168.1.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
15	12:17:59.338057	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
16	12:17:59.340279	98.109.25.1	192.168.1.161	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
 ▶ Ethernet II, Src: Verizon\_f1:47:66 (48:5d:36:f1:47:66), Dst: Apple\_9c:a6:65 (4c:32:75:9c:a6:65)  
 ▶ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.161

```

  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  Total Length: 84
  Identification: 0x449c (17564)
  ▶ 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)
  Header checksum: 0xb15a [validation disabled]
  
```

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?

Ans.) Identification , Time-to-live and Header checksum change.

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

Ans.) The fields that stay constant across the IP datagrams are:

- Version
- header length
- source IP
- destination IP
- Differentiated Services
- Upper Layer Protocol

The fields that must stay constant are:

- Version
- header length
- destination IP (since we are sending to the same dest)
- Differentiated Services (since all packets are ICMP they use the same Type of Service class)

- Upper Layer Protocol (since these are ICMP packets)

The fields that must change are:

- Identification
- Time to live
- Header checksum

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

Ans.) Decrement by 1 every time.

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

Ans.) Identification field : 17564

TTL field : 64

No.	Time	Source	Destination	Protocol	Length	Info
1	12:17:53.287459	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
2	12:17:56.768970	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
3	12:17:57.793774	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
4	12:17:58.817049	Verizon_f1:47:66	Broadcast	ARP	42	Who has 192.168.1.155? Tell 192.168.1.1
5	12:17:59.312401	192.168.1.161	192.168.1.1	DNS	77	Standard query 0x179c A gaia.cs.umass.edu
6	12:17:59.328519	192.168.1.1	192.168.1.161	DNS	93	Standard query response 0x179c A gaia.cs.umass.edu A 128.119.245.12
7	12:17:59.329464	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
8	12:17:59.333180	192.168.1.1	192.168.1.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
9	12:17:59.333900	192.168.1.161	192.168.1.1	DNS	84	Standard query 0xdad9 PTR 1.1.168.192.in-addr.arpa
10	12:17:59.335497	192.168.1.1	192.168.1.161	DNS	165	Standard query response 0xdad9 PTR 1.1.168.192.in-addr.arpa PTR FIOS_Quantum
11	12:17:59.335825	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
12	12:17:59.336847	192.168.1.1	192.168.1.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
13	12:17:59.336970	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
14	12:17:59.337904	192.168.1.1	192.168.1.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
15	12:17:59.338057	192.168.1.161	128.119.245.12	SKYPE	70	Unknown_0
16	12:17:59.340279	98.109.25.1	192.168.1.161	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

► Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
 ► Ethernet II, Src: Verizon\_f1:47:66 (48:5d:36:f1:47:66), Dst: Apple\_9c:a6:65 (4c:32:75:9c:a6:65)  
 ▾ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.161  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 ▾ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)  
 Total Length: 84  
 Identification: 0x449c (17564)  
 ▾ 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)  
 Header checksum: 0xb15a [validation disabled]

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?

Ans.) The identification value changes but the TTL values remain the same because all values are received from same router.

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? [Note: if you find your packet has

not been fragmented, you should download the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> and extract the ipethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.<sup>3</sup> ]

Ans.) The message is fragmented in two packets that are of length 1500 and 520.

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?

Ans.) Flags 0x01:

More Fragments: Set, indicates datagram has been fragmented.

Fragment Offset = 0 indicates this is first fragment.

IP datagram Length = 1500 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
665	12:19:08.711127	192.168.1.161	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
667	12:19:09.711426	192.168.1.161	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
669	12:19:09.713489	192.168.1.161	172.217.9.234	TCP	66	[TCP Previous segment not captured] 50697 → 443 [ACK] Seq=2 Ack=64 Win=4094
672	12:19:09.713769	192.168.1.161	172.217.9.234	TCP	66	50697 → 443 [FIN, ACK] Seq=2 Ack=64 Win=4096 Len=0 TStamp=336497091 TSect=11
673	12:19:09.713799	192.168.1.161	172.217.9.234	TCP	66	[TCP Out-Of-Order] 50697 → 443 [FIN, ACK] Seq=2 Ack=65 Win=4096 Len=0 TStamp=336497091 TSect=11
674	12:19:09.713971	192.168.1.161	172.217.9.234	TCP	66	[TCP Out-Of-Order] 50697 → 443 [FIN, ACK] Seq=2 Ack=65 Win=4096 Len=0 TStamp=336497091 TSect=11
679	12:19:10.711480	192.168.1.161	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
680	12:19:11.799558	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8332) [Reassembled in #681]
681	12:19:11.799559	192.168.1.161	128.119.245.12	SKYPE	534	Unknown_0
683	12:19:11.803213	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8333) [Reassembled in #684]
684	12:19:11.803214	192.168.1.161	128.119.245.12	SKYPE	534	Unknown_0
686	12:19:11.805275	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8334) [Reassembled in #687]
687	12:19:11.805275	192.168.1.161	128.119.245.12	SKYPE	534	Unknown_0
689	12:19:11.807774	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8335) [Reassembled in #690]
690	12:19:11.807775	192.168.1.161	128.119.245.12	SKYPE	534	Unknown_0
692	12:19:11.813783	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8336) [Reassembled in #693]
▶ Frame 680: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0						
▶ Ethernet II, Src: Apple_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon_f1:47:66 (48:5d:36:f1:47:66)						
▼ Internet Protocol Version 4, Src: 192.168.1.161, Dst: 128.119.245.12						
0100 .... = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
► Differentiated Services Field: 0x00 (DSSCP: CS0, ECN: Not-ECT)						
Total Length: 1500						
Identification: 0x8332 (33586)						
▼ Flags: 0x01 (More Fragments)						
0... .... = Reserved bit: Not set						
..0.. .... = Don't fragment: Not set						
..1.... = More fragments: <u>Set</u>						
Fragment offset: 0						
► Time to live: 1						
Protocol: UDP (17)						
Header checksum: 0xd911 [validation disabled]						
0010	05 dc 83 32 20 00 b1 11 d9 11 c0 a8 01 a1 80 77	.....2	....	.....	.....	.....
0020	f5 0c 83 31 82 9b 07 bc b2 db 00 00 00 00 00 00	.....1.	.....	.....	.....	.....
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	.....	.....	.....	.....	.....

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?

Ans.) Fragment Offset: 1480 bytes , hence not first datagram fragment.

Flags:

More Fragments: Not Set., indicates there are no more fragments.

No.	Time	Source	Destination	Protocol	Length	Info
665	12:19:08.711127	192.168.1.161	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
667	12:19:09.711426	192.168.1.161	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
669	12:19:09.713489	192.168.1.161	172.217.9.234	TCP	66	[TCP Previous segment not captured] 50697 → 443 [ACK] Seq=2 Ack=64 Win=4094
672	12:19:09.713769	192.168.1.161	172.217.9.234	TCP	66	50697 → 443 [FIN, ACK] Seq=2 Ack=64 Win=4094 Len=0 TSval=336497091 TSecr=11
673	12:19:09.713799	192.168.1.161	172.217.9.234	TCP	66	[TCP Out-Of-Order] 50697 → 443 [FIN, ACK] Seq=2 Ack=65 Win=4096 Len=0 TSval=336497091 TSecr=11
674	12:19:09.713971	192.168.1.161	172.217.9.234	TCP	66	[TCP Out-Of-Order] 50697 → 443 [FIN, ACK] Seq=2 Ack=65 Win=4096 Len=0 TSval=336497091 TSecr=11
679	12:19:10.711480	192.168.1.161	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
680	12:19:11.799558	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8332) [Reassembled in #681]
681	12:19:11.799559	192.168.1.161	128.119.245.12	SKYPE	534	Unknown_0
683	12:19:11.803213	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8333) [Reassembled in #684]
684	12:19:11.803214	192.168.1.161	128.119.245.12	SKYPE	534	Unknown_0
686	12:19:11.805275	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8334) [Reassembled in #687]
687	12:19:11.805275	192.168.1.161	128.119.245.12	SKYPE	534	Unknown_0
689	12:19:11.807774	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8335) [Reassembled in #690]
690	12:19:11.807775	192.168.1.161	128.119.245.12	SKYPE	534	Unknown_0
692	12:19:11.813783	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8336) [Reassembled in #693]

```

> Frame 681: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0
> Ethernet II, Src: Apple_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon_f1:47:66 (48:5d:36:f1:47:66)
> Internet Protocol Version 4, Src: 192.168.1.161, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSFP: CS0, ECN: Not-ECT)
    Total Length: 520
    Identification: 0x8332 (33586)
    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: 0xfc2c [validation disabled]
0010  02 08 83 32 00 b9 01 11 fc 2c c0 a8 01 a1 80 77  ...2.... ,.....W
0020  f5 0c 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  ..... .

```

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

Ans.) The fields like Total Length, flags and fragment Offset change between the first and second fragment.

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

Ans.) Three fragments were created from the original datagram.

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

Ans.) Fragment 1 -> Fragment2 : Fragment Offset (0 -> 1480)

Fragment 2 -> Fragment 3 : Total Length (1500-> 540) , Fragment Offset( 1490 -> 2960) , Flags(More Fragment: Set -> More Fragment : Not Set)

Apply a display filter ... <%>/

No.	Time	Source	Destination	Protocol	Length	Info
661	12:19:06.197457	192.168.1.234	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
85	12:18:27.286634	192.168.1.234	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
82	12:18:26.262049	192.168.1.234	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
81	12:18:25.238099	192.168.1.234	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
79	12:18:24.214021	192.168.1.234	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1147	12:21:47.276168	192.168.1.161	104.154.164.197	TCP	66	5079 -> 443 [ACK] Seq=1 Ack=409 Win=4094 Len=0 TSval=336654576 TSecr=236291
1140	12:21:42.256630	192.168.1.161	128.119.245.12	SKYPE	554	Unknown_0
1139	12:21:42.256629	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=8359) [Reassembled in #1140]
1138	12:21:42.256629	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8359) [Reassembled in #1140]
1136	12:21:42.240649	192.168.1.161	128.119.245.12	SKYPE	554	Unknown_0
1135	12:21:42.240648	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=8358) [Reassembled in #1136]
1134	12:21:42.240648	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8358) [Reassembled in #1136]
1132	12:21:42.212035	192.168.1.161	128.119.245.12	SKYPE	554	Unknown_0
1131	12:21:42.212034	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=8357) [Reassembled in #1132]
1130	12:21:42.212033	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8357) [Reassembled in #1132]
1128	12:21:40.419629	192.168.1.161	172.217.10.14	TCP	54	[TCP Keep-Alive] 50729 -> 443 [ACK] Seq=5871 Ack=43718 Win=131072 Len=0
> Frame 1138: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0						
> Ethernet II, Src: Apple_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon_f1:47:66 (48:5d:36:f1:47:66)						
> Internet Protocol Version 4, Src: 192.168.1.161, 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: 0x8359 (33625)						
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: 13						
Protocol: UDP (17)						
Header checksum: 0xccea [validation disabled]						
0010 05 dc 83 59 20 00 0d 11 cc ea c0 a8 01 a1 80 77 ...Y... ....w						
0020 f5 0c 83 32 82 c1 0d 98 a6 fc 00 00 00 00 00 00 ...2....						
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 .....						
Identification (ip.id), 2 bytes						
Packets: 1152 · Displayed: 1152 (100.0%)						
Profile: Default						
No.	Time	Source	Destination	Protocol	Length	Info
1114	12:21:37.915946	192.168.1.161	172.217.10.131	TCP	54	[TCP Keep-Alive] 50735 -> 443 [ACK] Seq=465 Ack=4611 Win=130656 Len=0
1113	12:21:37.208903	192.168.1.161	128.119.245.12	SKYPE	554	Unknown_0
1112	12:21:37.208902	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=8356) [Reassembled in #1113]
1111	12:21:37.208901	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8356) [Reassembled in #1113]
1110	12:21:32.206473	192.168.1.161	128.119.245.12	SKYPE	554	Unknown_0
1109	12:21:32.206472	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=8355) [Reassembled in #1110]
1108	12:21:32.206471	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8355) [Reassembled in #1110]
1107	12:21:27.204421	192.168.1.161	128.119.245.12	SKYPE	554	Unknown_0
1106	12:21:27.204420	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=8354) [Reassembled in #1107]
1105	12:21:27.204420	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8354) [Reassembled in #1107]
1103	12:21:27.193341	192.168.1.161	128.119.245.12	SKYPE	554	Unknown_0
1102	12:21:27.193341	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=8353) [Reassembled in #1103]
1101	12:21:27.193340	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8353) [Reassembled in #1103]
1099	12:21:27.182149	192.168.1.161	128.119.245.12	SKYPE	554	Unknown_0
1098	12:21:27.182149	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=8352) [Reassembled in #1097]
1097	12:21:27.182148	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=8352) [Reassembled in #1099]
> Frame 1113: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0						
> Ethernet II, Src: Apple_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon_f1:47:66 (48:5d:36:f1:47:66)						
> Internet Protocol Version 4, Src: 192.168.1.161, 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						
Identification: 0x8356 (33622)						
Flags: 0x00						
0... .... = Reserved bit: Not set						
.0. .... = Don't fragment: Not set						
..0. .... = More fragments: Not set						
Fragment offset: 2960						
Time to live: 12						
Protocol: UDP (17)						
Header checksum: 0xf03b [validation disabled]						
0010 02 1c 83 56 01 72 0c 11 f0 3b c0 a8 01 a1 80 77 ...V.r. .;....w						
0020 f5 0c 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 .....						

No.	Time	Source	Destination	Protocol	Length	Info
1114	12:21:37.915946	192.168.1.161	172.217.10.131	TCP	54	[TCP Keep-Alive] 50735 → 443 [ACK] Seq=465 Ack=4611 Win=130656 Len=0
1113	12:21:37.208903	192.168.1.161	128.119.245.12	SKYPE	554	Unknown_0
1112	12:21:37.208902	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, offf=1480, ID=8356) [Reassembled in #1113]
1111	12:21:37.208901	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, offf=0, ID=8356) [Reassembled in #1113]
1110	12:21:32.206473	192.168.1.161	128.119.245.12	SKYPE	554	Unknown_0
1109	12:21:32.206472	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, offf=1480, ID=8355) [Reassembled in #1109]
1108	12:21:32.206471	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, offf=0, ID=8355) [Reassembled in #1108]
1107	12:21:27.204421	192.168.1.161	128.119.245.12	SKYPE	554	Unknown_0
1106	12:21:27.204420	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, offf=1480, ID=8354) [Reassembled in #1106]
1105	12:21:27.204420	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, offf=0, ID=8354) [Reassembled in #1107]
1103	12:21:27.193341	192.168.1.161	128.119.245.12	SKYPE	554	Unknown_0
1102	12:21:27.193341	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, offf=1480, ID=8353) [Reassembled in #1102]
1101	12:21:27.193340	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, offf=0, ID=8353) [Reassembled in #1103]
1099	12:21:27.182149	192.168.1.161	128.119.245.12	SKYPE	554	Unknown_0
1098	12:21:27.182149	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, offf=1480, ID=8352) [Reassembled in #1098]
1097	12:21:27.182148	192.168.1.161	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, offf=0, ID=8352) [Reassembled in #1099]
▶ Frame 1112: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0						
▶ Ethernet II, Src: Apple_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon_f1:47:66 (48:5d:36:f1:47:66)						
▼ Internet Protocol Version 4, Src: 192.168.1.161, Dst: 128.119.245.12						
0100 .... = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
▶ Differentiated Services Field: 0x00 (DSFP: CS0, ECN: Not-ECT)						
Total Length: 1500						
Identification: 0x8356 (3662)						
▶ 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: 12						
Protocol: UDP (17)						
Header checksum: 0xcd34 [validation disabled]						
0010	05 dc 83 56 20 b5 0c 11 cd 34 c8 a8 01 a1 80 77	..V	...	4.....w		
0020	f5 0c 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	.....	.....	.....		