

CN LAB (ICMP):

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.

No.	Time	Source	Destination	Protocol	Length	Info
1631	17.352425	8.8.8.8	192.168.30.251	DNS	121	Standard query response 0x5fd6 AAAA www.nitgoa.ac.in SOA nitgoa.ac.in
1632	17.353022	8.8.8.8	192.168.30.251	DNS	92	Standard query response 0x0fcd A www.nitgoa.ac.in A 14.139.114.14
1633	17.378075	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 1634)
1634	17.471942	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=114 (request in 1633)
1635	18.386133	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 1636)
1636	18.507097	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=114 (request in 1635)
1637	19.392062	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 1638)
1638	19.492202	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=114 (request in 1637)
1639	20.399210	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 1640)
1640	20.493673	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=114 (request in 1639)
1641	20.914717	0a:d4:7d:58:7f:11	MonHaIPr_c6:45:21	ARP	42	Who has 192.168.30.251? Tell 192.168.30.94
1642	20.914757	MonHaIPr_c6:45:21	0a:d4:7d:58:7f:11	ARP	42	192.168.30.251 is at f8:2f:a8:c6:45:21
1643	20.996423	2404:6800:4009:813::	2404:6800:4009:813::	UDP	95	55818 → 443 Len=33
1644	21.118540	2404:6800:4009:813::	2409:4042:21f:27e5::	UDP	91	443 → 55818 Len=29
1645	24.874813	2404:6800:4009:813::	2409:4042:21f:27e5::	UDP	893	443 → 55818 Len=831

Internet Protocol Version 4, Src: 192.168.30.251, Dst: 14.139.114.14

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0x3df0 (15856)

> Flags: 0x00

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: ICMP (1)

Header Checksum: 0x9c94 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.30.251

Destination Address: 14.139.114.14

> Internet Control Message Protocol

0000 0a d4 7d 58 7f 11 f8 2f a8 c6 45 21 08 00 45 00 ...}X.../...E!...E-
0010 00 3c 3d f0 00 00 00 01 9c 94 c0 a8 1e fb 0e 8b ...<=.....

My IP address is 192.168.30.251

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

No.	Time	Source	Destination	Protocol	Length	Info
1633	17.378075	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 1634)
1634	17.471942	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=114 (request in 1633)
1635	18.386133	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 1636)
1636	18.507097	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=114 (request in 1635)
1637	19.392062	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 1638)
1638	19.492202	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=114 (request in 1637)
1639	20.399210	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 1640)
1640	20.493673	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=114 (request in 1639)

Internet Protocol Version 4, Src: 192.168.30.251, Dst: 14.139.114.14

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0x3df0 (15856)

> Flags: 0x00

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: ICMP (1)

Header Checksum: 0x9c94 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.30.251

Destination Address: 14.139.114.14

> Internet Control Message Protocol

0000 0a d4 7d 58 7f 11 f8 2f a8 c6 45 21 08 00 45 00 ...}X.../...E!...E-
0010 00 3c 3d f0 00 00 00 01 9c 94 c0 a8 1e fb 0e 8b ...<=.....

0100 is the value in the upper layer protocol field.

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.

20 bytes are in the IP header.

Payload = total length - IP header length

payload = 60-20=40

No.	Time	Source	Destination	Protocol	Length	Info
1633	17.378075	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 1634)
1634	17.471942	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=114 (request in 1633)
1635	18.306133	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 1636)
1636	18.507097	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=114 (request in 1635)
1637	19.392062	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 1638)
1638	19.492202	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=114 (request in 1637)
1639	20.399210	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 1640)
1640	20.493673	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=114 (request in 1639)

Ethernet II, Src: HonHaiPr_c6:45:21 (f8:2f:a8:c6:45:21), Dst: 0a:d4:7d:58:7f:11 (0a:d4:7d:58:7f:11)	
Internet Protocol Version 4, Src: 192.168.30.251, Dst: 14.139.114.14	
0100 = Version: 4	
... 0101 = Header Length: 20 bytes (5)	
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	
Total Length: 60	
Identification: 0x3df0 (15856)	
Flags: 0x00	
...0 0000 0000 0000 = Fragment Offset: 0	
Time to Live: 128	
Protocol: ICMP (1)	
Header Checksum: 0x9c94 [validation disabled]	
[Header checksum status: Unverified]	
Source Address: 192.168.30.251	
Destination Address: 14.139.114.14	
Internet Control Message Protocol	
0010 00 3d f0 00 00 00 01 9c 94 c0 a8 1e fb 0e 8b	

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

The more fragments bit = 0, so the data is not fragmented

No.	Time	Source	Destination	Protocol	Length	Info
1633	17.378075	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 1634)
1634	17.471942	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=114 (request in 1633)
1635	18.386133	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 1636)
1636	18.587097	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=114 (request in 1635)
1637	19.392062	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 1638)
1638	19.492202	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=114 (request in 1637)
1639	20.399210	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 1640)
1640	20.493673	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=114 (request in 1639)


```

> Ethernet II, Src: HonHaiPr_c6:45:21 (f8:2f:a8:c6:45:21), Dst: 0a:d4:7d:58:7f:11 (0a:d4:7d:58:7f:11)
> Internet Protocol Version 4, Src: 192.168.30.251, Dst: 14.139.114.14
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x3df0 (15856)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x9c94 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.30.251
    Destination Address: 14.139.114.14
> Internet Control Message Protocol
0010  00 3c 3d f0 00 00 00 01 9c 94 c0 a8 1e fb 0e 8b  <=...
0020  72 0e 08 00 4d 56 00 01 00 05 61 62 63 64 65 66  r...V...abcdef
  
```

Fragment offset (13 bits) (p.frag_offset), 2 bytes Packets: 1640 · Displayed: 8 (0.5%) · Dropped: 0 (0.0%) Profile: Default

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?

Identification and Header checksum always change.

No.	Time	Source	Destination	Protocol	Length	Info
1633	17.378075	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 1634)
1634	17.471942	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=114 (request in 1633)
1635	18.386133	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 1636)
1636	18.587097	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=114 (request in 1635)
1637	19.392062	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 1638)
1638	19.492202	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=114 (request in 1637)
1639	20.399210	192.168.30.251	14.139.114.14	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 1640)
1640	20.493673	14.139.114.14	192.168.30.251	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=114 (request in 1639)


```

> Frame 1633: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{5E726856-29FC-4192-828F-F9A836E4C1B9}, id 0
> Ethernet II, Src: HonHaiPr_c6:45:21 (f8:2f:a8:c6:45:21), Dst: 0a:d4:7d:58:7f:11 (0a:d4:7d:58:7f:11)
> Internet Protocol Version 4, Src: 192.168.30.251, Dst: 14.139.114.14
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x3df0 (15856)
  > Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragments: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x9c94 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.30.251
    Destination Address: 14.139.114.14
> Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
0000  0a d4 7d 58 7f 11 f8 2f a8 c6 45 21 08 00 45 00  ..X.../..E!...E
0010  00 3c 3d f0 00 00 00 01 9c 94 c0 a8 1e fb 0e 8b  <=...
0020  72 0e 08 00 4d 56 00 01 00 05 61 62 63 64 65 66  r...V...abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
  
```

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

Fields that stay constant across the IP datagrams :

IPv4
Header length
Source IP
Destination IP
Upper layer protocol (since these are ICMP packets)

fields must stay constant

Version
Header length
Source IP
Destination IP
Upper layer protocol

Fields must change

Header check sum
Identification bit
Time to live

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

The pattern is that the IP header Identification fields increment with each ICMP Echo (ping) request.

In my situation 0x3df0(15856)

“ “ 1
“ “ 2
“ “ 3

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

Identification field 0x3df0(15856)
TTL field 128

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?

The identification field changes for all the ICMP TTL-exceeded replies because the identification field is a unique value. When 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 remains unchanged because the TTL for the first hop router is always the same.

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

Yes, this packet has been fragmented across more than one IP datagram

The image shows a Wireshark packet capture of an ICMP Echo request and its fragments. The packet list shows a sequence of ICMP Echo requests from 192.168.30.251 to 200.200.4.5. The 343rd packet is a 'Time-to-live exceeded' message. The 352nd packet is a 'Destination unreachable' message. The 362nd packet is an ICMP Echo request with a length of 1500 bytes. The packet details pane shows the IP header with the 'More Fragments' flag set and a fragment offset of 0. The packet bytes pane shows the raw data of the IP datagram, which is fragmented into two parts: a first fragment of 1480 bytes and a second fragment of 20 bytes.

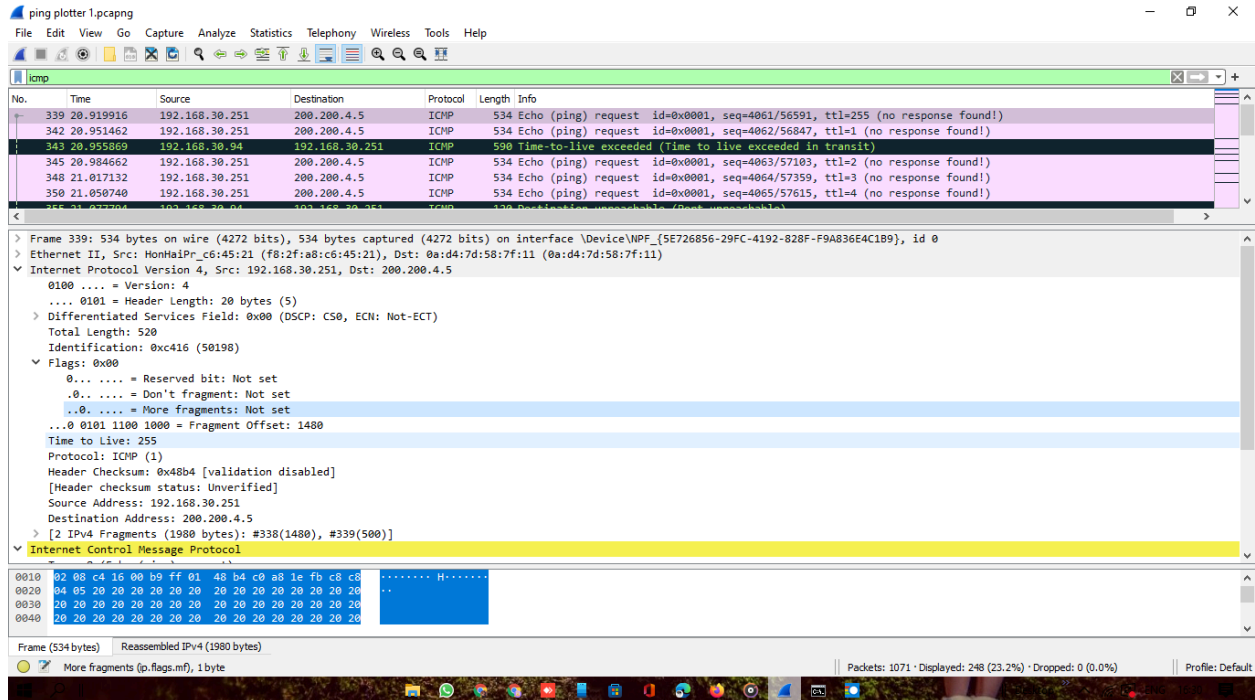
No.	Time	Source	Destination	Protocol	Length	Info
339	20.919916	192.168.30.251	200.200.4.5	ICMP	534	Echo (ping) request id=0x0001, seq=4061/56591, ttl=255 (no response found!)
342	20.951462	192.168.30.251	200.200.4.5	ICMP	534	Echo (ping) request id=0x0001, seq=4062/56847, ttl=1 (no response found!)
343	20.955869	192.168.30.94	192.168.30.251	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
345	20.984662	192.168.30.251	200.200.4.5	ICMP	534	Echo (ping) request id=0x0001, seq=4063/57103, ttl=2 (no response found!)
348	21.017132	192.168.30.251	200.200.4.5	ICMP	534	Echo (ping) request id=0x0001, seq=4064/57359, ttl=3 (no response found!)
350	21.050740	192.168.30.251	200.200.4.5	ICMP	534	Echo (ping) request id=0x0001, seq=4065/57615, ttl=4 (no response found!)
352	21.077794	192.168.30.94	192.168.30.251	ICMP	120	Destination unreachable (Port unreachable)
357	21.083708	192.168.30.251	200.200.4.5	ICMP	534	Echo (ping) request id=0x0001, seq=4066/57871, ttl=5 (no response found!)
360	21.116368	192.168.30.251	200.200.4.5	ICMP	534	Echo (ping) request id=0x0001, seq=4067/58127, ttl=6 (no response found!)
362	21.148609	192.168.30.251	200.200.4.5	ICMP	534	Echo (ping) request id=0x0001, seq=4068/58383, ttl=7 (no response found!)
362	21.157245	192.168.30.251	192.168.30.251	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 520
Identification: 0xc416 (50198)
▼ Flags: 0x00
0... .. = Reserved bit: Not set
..0... .. = Don't fragment: Not set
...0... .. = More fragments: Not set
...0 0101 1100 1000 = Fragment Offset: 1480
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0x48b4 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.30.251
Destination Address: 200.200.4.5
> [2 IPv4 Fragments (1980 bytes): #338(1480), #339(500)]
Internet Control Message Protocol

0000 08 00 2c 66 00 01 0f dd 20 20 20 20 20 20 20 20 ..,f....
0100 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0200 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0300 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram has 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?

The Flags bit for more fragments is set, indicating that the datagram has been fragmented. Since the fragment offset is 0, we know that this is the first fragment. This first datagram has a total length of 1500, including the header.



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?

We can tell that this is not the first fragment, since the fragment offset is 1480. It is the last fragment, since the more fragments flag is not set.

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

The IP header fields that changed between the fragments are: total length, flags, fragment offset, and checksum.

No.	Time	Source	Destination	Protocol	Length	Info
339	20.919916	192.168.30.251	200.200.4.5	ICMP	534	Echo (ping) request id=0x0001, seq=4061/56591, ttl=255 (no response found!)
342	20.951462	192.168.30.251	200.200.4.5	ICMP	534	Echo (ping) request id=0x0001, seq=4062/56847, ttl=1 (no response found!)
343	20.955869	192.168.30.94	192.168.30.251	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
345	20.984662	192.168.30.251	200.200.4.5	ICMP	534	Echo (ping) request id=0x0001, seq=4063/57103, ttl=2 (no response found!)
348	21.017132	192.168.30.251	200.200.4.5	ICMP	534	Echo (ping) request id=0x0001, seq=4064/57359, ttl=3 (no response found!)
350	21.050740	192.168.30.251	200.200.4.5	ICMP	534	Echo (ping) request id=0x0001, seq=4065/57615, ttl=4 (no response found!)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 520 Identification: 0xc416 (50198) > Flags: 0x00 0... .. = Reserved bit: Not set .0.. .. = Don't fragment: Not set ..0. .. = More fragments: Not set ...0 0101 1100 1000 = Fragment Offset: 1480 Time to Live: 255 Protocol: ICMP (1) Header Checksum: 0x48b4 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.30.251 Destination Address: 200.200.4.5 > [2 IPv4 Fragments (1980 bytes): #338(1480), #339(500)] > Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0 Checksum: 0x2c66 [correct] [Checksum Status: Good] Identifier (BE): 1 (0x0001)	
--	--

0010	02 08 c4 16 00 b5 ff 01 48 b4 c0 a0 1e fb c8 c8	H.....
0020	04 05 20 20 20 20 20 20 20 20 20 20 20 20 20	
0030	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0040	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	

14. How many fragments were created from the original datagram?
 After switching to 3500, there are 3 packets created from the original datagram.

15. What fields change in the IP header among the fragments?
 The IP header fields that changed between all of the packets are: fragment offset, and checksum. Between the first two packets and the last packet, we see a change in total length, and also in the flags. The first two packets have a total length of 1500, with the more fragments bit set to 1, and the last packet has a total length of 540, with the more fragments bit set to 0.