# Wireshark Lab 4 – IP Xiaoying Li

NOTE: I used the downloaded trace to answer all the questions.

#### 1. What is the IP address of your computer?

IP address of the computer: 192.168.1.102

```
| No. | Tine | Source | Destination | Protocol | Length Info | 10.0000000 | CnetTech_73:8d:ce | Broadcast | ARP | 60 Who has 192.168.1.117? Tell 192.168.1.104 |
| 24.866867 | 192.168.1.100 | 192.168.1.1 | SSDP | 174 M-SEARCH * HITP/1.1 |
| 34.868147 | 192.168.1.100 | 192.168.1.1 | SSDP | 175 M-SEARCH * HITP/1.1 |
| 45.363536 | 192.168.1.100 | 192.168.1.1 | SSDP | 175 M-SEARCH * HITP/1.1 |
| 55.364799 | 192.168.1.100 | 192.168.1.1 | SSDP | 175 M-SEARCH * HITP/1.1 |
| 65.864428 | 192.168.1.100 | 192.168.1.1 | SSDP | 174 M-SEARCH * HITP/1.1 |
| 75.865461 | 192.168.1.100 | 192.168.1.1 | SSDP | 175 M-SEARCH * HITP/1.1 |
| 86.163045 | 192.168.1.102 | 128.59.23.100 | ICMP | 98 Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response foundl)
| > Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
| > Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys6_da:af:73 (00:06:25:da:af:73)
| > Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100 | Step | St
```

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

Value in the upper layer protocol field: ICMP (1)

```
Protocol Length Info
          1 0.000000
                                CnetTech_73:8d:ce
                                                                                                             60 Who has 192.168.1.117? Tell 192.168.1.104
                               CnetTech_73:8d
192.168.1.100
192.168.1.100
192.168.1.100
192.168.1.100
          2 4.866867
3 4.868147
                                                               192.168.1.1
192.168.1.1
                                                                                                            174 M-SEARCH * HTTP/1.
175 M-SEARCH * HTTP/1.
                                                               192.168.1.1
192.168.1.1
192.168.1.1
                                                                                                            174 M-SEARCH * HTTP/1.
175 M-SEARCH * HTTP/1.
174 M-SEARCH * HTTP/1.
                                                                                             SSDP
          5 5.364799
6 5.864428
         8 6.163045 192.168.1.102 128.59.23.100
                                                                                                         98 Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
   Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
  Ethernet II, Src: Actionte 8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG da:af:73 (00:06:25:da:af:73)
## Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100

1000 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
      Identification: 0x32d0 (13008)
   > Flags: 0x00
Fragment Offset: 0
     Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x2d2c [validation disabled]
[Header checksum status: Unverified]
      Source Address: 192.168.1.102
Destination Address: 128.59.23.100
> Internet Control Message Protoco
```

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.

```
IP header length = 20 bytes
```

IP datagram total length = 84 bytes

Payload of the IP datagram length

- = IP datagram total length IP header length
- = 84 bytes 20 bytes
- = 64 bytes

```
Destination
                                                                                                              Protocol Length Info
                                      CnetTech_73:8d:ce Broadcast
                                      192.168.1.100
192.168.1.100
192.168.1.100
                                                                          192.168.1.1
192.168.1.1
192.168.1.1
            2 4.866867
3 4.868147
                                                                                                                               174 M-SEARCH * HTTP/1.1
175 M-SEARCH * HTTP/1.1
174 M-SEARCH * HTTP/1.1
175 M-SEARCH * HTTP/1.1
175 M-SEARCH * HTTP/1.1
                                     192.168.1.100
192.168.1.100
192.168.1.100
            5 5.364799
6 5.864428
                                                                          192.168.1.1
192.168.1.1
                                                                                                            ICMP 98 Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
         8 6.163045 192.168.1.102
                                                                       128.59.23.100
   Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Themset II, Src: Actionte_8a:70ial (00:20:08:8a:70:1a), Ost: LinksysG_da:af:73 (00:06:25:da:af:73)

> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
      0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
Identification: 0x32d0 (13008)
Flags: 0x00
Fragment Offset: 0
Time to Live: 1
Protocol: ICMP (1)
      Protocol: ICMP (1)
Header checksum: 0x2dzc [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
> Internet Control Message Proto
```

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

This IP datagram has not been fragmented. Because the "More fragment" flag is "Not set".

```
Protocol Length Info
ARP 60 Who has 192.168.1.117? Tell 192.168.1.104
                                Source
CnetTech_73:8d:ce
                                                                                                               174 M-SEARCH * HTTP/1.1
175 M-SEARCH * HTTP/1.1
174 M-SEARCH * HTTP/1.1
175 M-SEARCH * HTTP/1.1
174 M-SEARCH * HTTP/1.1
175 M-SEARCH * HTTP/1.1
         2 4.866867
3 4.868147
4 5.363536
                                192.168.1.100
192.168.1.100
192.168.1.100
192.168.1.100
                                                                192.168.1.1
192.168.1.1
192.168.1.1
         5 5.364799
                                                                192.168.1.1
                                192.168.1.100
192.168.1.100
         6 5 . 864428
     8 6.163045 192.168.1.102 128.59.23.100
                                                                                                            98 Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
                                                                                             ICMP
 Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
 Ethernet II, Snc: Actionte 8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Snc: 192.168.1.102, Dst: 128.59.23.100
  0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 84
     Identification: 0x32d0 (13008)
 Flags: 0x00

0... = Reserved bit: Not set
 .0.... = Don't fragment: Not set
.0.... = More fragments: Not set
Fragment Offset: 0
> Time to Live: 1
     Protocol: ICMP (1)
     | Header Checksum: 0x2d2c [validation disabled]
| Header checksum status: Unverified]
| Source Address: 192.168.1.102
     Destination Address: 128.59.23.100
Internet Control Message Pr
```

# 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, Time to Live, and Header Checksum in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by the computer.

No.	Tine	Source	Destination	Protocol	Length Info							
	8 6.163045	192,168,1,102	128.59.23.100	ICMP	-	(ning)	request	id=0x0300	seq=20483/848,	ttl=1 (no	resnonse	foundl
	9 6.176826	10.216.228.1	192.168.1.102	ICMP					live exceeded i			
	10 6,188629	192,168,1,102	128,59,23,100	ICMP					seq=20739/849			found
	11 6.202957	24.218.0.153	192.168.1.102	ICMP					live exceeded i			
	12 6.208597	192.168.1.102	128.59.23.100	ICMP	98 Echo	(ping)	request	id=0x0300,	seq=20995/850,	ttl=3 (no	response	found
	13 6.234505	24.128.190.197	192.168.1.102	ICMP	70 Time-	to-liv	e exceede	ed (Time to	live exceeded i	n transit	)	
	14 6.238695	192.168.1.102	128.59.23.100	ICMP	98 Echo	(ping)	request	id=0x0300,	seq=21251/851,	ttl=4 (no	response	found
	15 6.257672	24.128.0.101	192.168.1.102	ICMP	70 Time-	to-liv	e exceede	ed (Time to	live exceeded i	n transit	)	
> Fra	me 8: 98 bytes	on wire (784 bits).	98 bytes captured (78	4 bits)								
> Eth	ernet II, Src:	Actionte 8a:70:1a (6	0:20:e0:8a:70:1a), Ds	t: LinksysG	da:af:73 (6	0:06:2	5:da:af:	73)				
∨ Int	ernet Protocol	Version 4, Src: 192.	168.1.102, Dst: 128.5	9.23.100	_ `			Ĺ				
	0100 = Ver	sion: 4										
0101 = Header Length: 20 bytes (5)												
>	Differentiated:	Services Field: 0x00	(DSCP: CS0, ECN: Not-	ECT)								
	Total Length: 8	4										
	Identification:	0x32d0 (13008)										
~	Flags: 0x00											
	0 = F	Reserved bit: Not set										
	.0 = 0	Oon't fragment: Not s	et									
	0 = N	Nore fragments: Not s	et									
	Fragment Offset	: 0										
>	Time to Live: 1											
	Protocol: ICMP	(1)										
	Header Checksum	: 0x2d2c [validation	disabled]									
	[Header checksu	m status: Unverified	]									
	Source Address:	192.168.1.102										
	Destination Add	ress: 128.59.23.100										
> Int	ernet Control M	Message Protocol										

٥.	Tine	Source	Destination	Protocol	Length Info							
	8 6.163045	192.168.1.102	128.59.23.100	ICMP	98 Echo	(ping)	request	id=0x0300,	seq=20483/848,	ttl=1	(no resp	onse found
	9 6.176826	10.216.228.1	192.168.1.102	ICMP	70 Time-	to-liv	e exceede	d (Time to	live exceeded i	n trans	sit)	
	10 6.188629	192.168.1.102	128.59.23.100	ICMP	98 Echo	(ping)	request	id=0x0300,	seq=20739/849,	ttl=2	(no resp	onse found
	11 6.202957	24.218.0.153	192.168.1.102	ICMP	70 Time-	to-liv	e exceede	d (Time to	live exceeded i	n trans	sit)	
	12 6.208597	192.168.1.102	128.59.23.100	ICMP					seq=20995/850,			onse found
	13 6.234505	24.128.190.197	192.168.1.102	ICMP					live exceeded i			
	14 6.238695	192.168.1.102	128.59.23.100	ICMP					seq=21251/851,			onse found
	15 6.257672	24.128.0.101	192.168.1.102	ICMP	70 Time-	to-liv	e exceede	d (Time to	live exceeded i	n trans	it)	
Fr	ame 10: 98 bytes	on wire (784 bits),	98 bytes captured (7	84 bits)								
Et	hernet II, Src:	Actionte 8a:70:1a (0	0:20:e0:8a:70:1a), Ds	t: LinksysG	da:af:73 (6	0:06:2	5:da:af:	73)				
In	ternet Protocol	Version 4, Src: 192.	168.1.102, Dst: 128.5	9.23.100								
0100 = Version: 4												
0101 = Header Length: 20 bytes (5)												
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)												
	Total Length: 8	4										
	Identification:	0x32d1 (13009)										
~	Flags: 0x00											
	0 = F	Reserved bit: Not set										
		Oon't fragment: Not s										
		More fragments: Not s	et									
	Fragment Offset											
>	Time to Live: 2											
	Protocol: ICMP	(1)										
		: 0x2c2b [validation										
	[Header checksu	m status: Unverified										
	Source Address:											
	Destination Add	ress: 128.59.23.100										
In	ternet Control M	Message Protocol										

No.	Tine	Source	Destination	Protocol	Length Info							
	8 6.163045	192,168,1,102	128,59,23,100	ICMP		(ping)	request	id=0x0300.	seq=20483/848	ttl=1 (	no response	found!)
	9 6.176826	10.216.228.1	192.168.1.102	ICMP	70 Time-	to-liv	e exceede	d (Time to	live exceeded	in transi	t)	,
	10 6.188629	192.168.1.102	128.59.23.100	ICMP	98 Echo	(ping)	request	id=0x0300,	seq=20739/849	ttl=2 (	no response	found!)
	11 6.202957	24.218.0.153	192.168.1.102	ICMP	70 Time-	to-liv	e exceede	d (Time to	live exceeded	in transi	.t)	,
	12 6.208597	192.168.1.102	128.59.23.100	ICMP	98 Echo	(ping)	request	id=0x0300,	seq=20995/850	ttl=3 (	no response	found!)
	13 6.234505	24.128.190.197	192.168.1.102	ICMP	70 Time	to-liv	e exceede	d (Time to	live exceeded	in transi	t)	
	14 6.238695	192.168.1.102	128.59.23.100	ICMP	98 Echo	(ping)	request	id=0x0300,	seq=21251/851	ttl=4 (	no response	found!)
	15 6.257672	24.128.0.101	192.168.1.102	ICMP	70 Time	to-liv	e exceede	d (Time to	live exceeded	in transi	.t)	
> F	rame 12: 98 bytes	on wire (784 bits)	, 98 bytes captured (7	34 bits)								
			00:20:e0:8a:70:1a), Ds		da:af:73 (	00:06:2	5:da:af:	73)				
v I	nternet Protocol	Version 4, Src: 192	.168.1.102, Dst: 128.59	.23.100								
"	0100 = Version: 4											
	0101 = Head	der Length: 20 bytes	5 (5)									
>	Differentiated 5	Services Field: 0x00	(DSCP: CS0, ECN: Not-	ECT)								
	Total Length: 84	4										
	Identification:	0x32d2 (13010)										
~	Flags: 0x00											
	0 = R	eserved bit: Not se	t									
	.0 = D	on't fragment: Not	set									
	0 = M	Nore fragments: Not	set									
	Fragment Offset	: 0										
>	Time to Live: 3											
	Protocol: ICMP	(1)										
	Header Checksum: 0x2b2a [validation disabled]											
	[Header checksum status: Unverified]											
	Source Address: 192.168.1.102											
_	Destination Address: 128.59.23.100											
> I	> Internet Control Message Protocol											

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

#### Fields stay constant:

Version, Header length, Differentiated Services Field, Upper Layer Protocol, Source Address, Destination Address

#### Fields must stay constant and why:

Version – because we are using IPv4 for all IP datagram packets
Header Length – because these IP datagrams are all ICMP packets
Differentiated Services Field – because these IP datagrams are all ICMP packets
Upper Layer Protocol – because these IP datagrams are all ICMP packets
Source Address – because these IP datagrams are all sent by the same computer
Destination Address – because these IP datagrams are all sent to the same destination

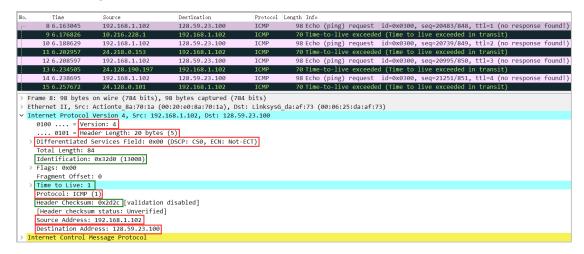
#### Fields must change and why:

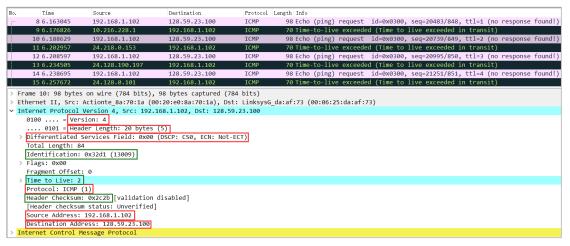
Identification – because every Ip datagram packet must have different ids

Time to Live – because traceroute increments every time an IP datagram is sent

Header Checksum – because IP datagram's header changes, so header checksum

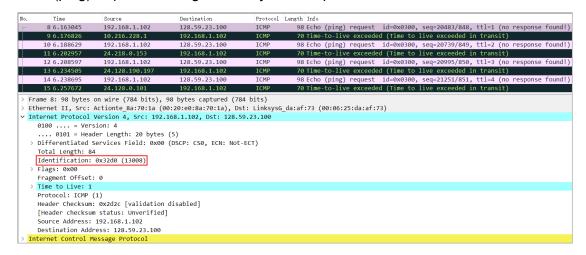
must change





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

The values in the Identification field of the IP datagram increment by 1 with every ICMP Echo (ping) request messages sent by the computer.



No.	Tine	Source	Destination	Protocol	Length Info							
Г	8 6.163045	192.168.1.102	128.59.23.100	ICMP					seq=20483/848,			found!)
	9 6.176826	10.216.228.1	192.168.1.102	ICMP	70 Time	-to-liv	e exceede	d (Time to	live exceeded i	n trans	it)	
	10 6.188629	192.168.1.102	128.59.23.100	ICMP	98 Echo	(ping)	request	id=0x0300,	seq=20739/849,	ttl=2	(no response	found!)
	11 6.202957	24.218.0.153	192.168.1.102	ICMP	70 Time	-to-liv	e exceede	d (Time to	live exceeded i	n trans	it)	
	12 6.208597	192.168.1.102	128.59.23.100	ICMP					seq=20995/850,			found!)
	13 6.234505	24.128.190.197	192.168.1.102	ICMP	70 Time		e exceede	d (Time to	live exceeded i	n trans	it)	
П	14 6.238695	192.168.1.102	128.59.23.100	ICMP	98 Echo	(ping)	request	id=0x0300,	seq=21251/851,	ttl=4	(no response	found!)
	15 6.257672	24.128.0.101	192.168.1.102	ICMP	70 Time	-to-liv	e exceede	d (Time to	live exceeded i	n trans	it)	
> Fra	ame 10: 98 bytes	on wire (784 bits),	98 bytes captured (78	34 bits)								
			0:20:e0:8a:70:1a), Dst		da:af:73 (	00:06:2	5:da:af:7	73)				
v Int	ternet Protocol	Version 4, Src: 192.	168.1.102, Dst: 128.59	.23.100	- '			·				
	0100 = Ver	sion: 4	•									
	0101 = Hea	der Length: 20 bytes	(5)									
>	Differentiated:	Services Field: 0x00	(DSCP: CS0, ECN: Not-	ECT)								
	Total Length: 8	4										
	Identification:	0x32d1 (13009)										
>	Flags: 0x00											
	Fragment Offset	: 0										
>	Time to Live: 2											
1 '	Protocol: ICMP	(1)										
	Header Checksum	: 0x2c2b [validation	disabled]									
	[Header checksum status: Unverified]											
	Source Address: 192.168.1.102											
	Destination Address: 128.59.23.100											
> Int	ternet Control M	Message Protocol										
_												

18.6.163045	No.	. Time	Source	Destination	Protocol	Length Info							
10 6.188629 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (mo response f 11 6.202957 24.218.0.153 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit) 12 6.208597 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=20739/849, ttl=3 (mo response f 13 6.234505 24.128.190.197 192.168.1.102 ICMP 98 Echo (ping) request id=0x0300, seq=20739/849, ttl=3 (mo response f 13 6.234505 24.128.190.197 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit) 14 6.238695 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (mo response f 15 6.257672 24.128.0.101 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)   > Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)   > Ethernet II, Src: Actionte 8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)    Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100   0100 = Version: 4	Г	8 6.163045	192.168.1.102	128.59.23.100	ICMP								found!)
11 6.203957 24.218.0.153 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit) 12 6.208597 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response f 13 6.234505 24.128.190.197 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit) 14 6.238695 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response f 15 6.257672 24.128.0101 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)  Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)  Ethernet II, Src: Actionte_8a:70:1a (00:20:00:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)  Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100 0100 = Version: 4  olal = Header Length: 20 bytes (5)  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  Total Length: 84  Identification: 0x32d2 (13010)  Flags: 0x00  Fragment Offset: 0  Time to Live: 3  Protocol: ICMP (1)  Header checksum: 0x2b2a [validation disabled]  [Header checksum: 0x2b2a [validation disabled]  [Header checksum: status: Unverified]  Source Address: 192.168.1.102		9 6.176826	10.216.228.1	192.168.1.102	ICMP	70 Time	-to-liv	e exceede	d (Time to	live exceeded i	n trans	it)	
12 6.208597 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response f 13 6.234595 24.128.190.197 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)  14 6.238695 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response f 15 6.257672 24.128.0.101 192.168.1.102 ICMP 98 Echo (ping) request id=0x0300, seq=21951/851, ttl=4 (no response f 15 6.257672 24.128.0.101 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)  > Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)  > Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)  > Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100  0100 = Version: 4  0101 = Header Length: 20 bytes (5)  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  Total Length: 84  Identification: 0x32d2 (13010)  > Flags: 0x00  Fragment Offset: 0  > Time to Live: 3  Protocol: ICMP  10 Header Checksum: 0x2b2a [validation disabled]  [Header checksum status: Unverified]  Source Address: 192.168.1.102		10 6.188629	192.168.1.102	128.59.23.100	ICMP								found!)
13 6.234505		11 6.202957	24.218.0.153	192.168.1.102	ICMP								
14 6.238695 192.168.1.102 128.59.23.100 ICMP 98 Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response f 15 6.257672 24.128.6.101 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)  > Frame 12: 98 bytes on wine (784 bits), 98 bytes captured (784 bits)  > Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys6_da:af:73 (00:06:25:da:af:73)  > Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100  0100 = Version: 4  0101 = Header Length: 20 bytes (5)  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  Total Length: 84  Identification: 0x32d2 (13010)  > Flags: 0x00  Fragment Offset: 0  > Time to Live: 3  Protocol: ICMP (1)  Header Checksum: 0x2b2a [validation disabled]  [Header checksum status: Unverified]  Source Address: 192.168.1.102			192.168.1.102	128.59.23.100	ICMP								found!)
15 6.257672 24.128.0.101 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)  > Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)  > Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)  > Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100  0100 = Version: 4  0101 = Header Length: 20 bytes (5)  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  Total Length: 84  Identification: 0x32d2 (13010)  > Flags: 0x00  Fragment Offset: 0  > Time to Live: 3  Protocol: ICMP (1)  Header Checksum: 0x2b2a [validation disabled]  [Header checksum status: Unverified]  Source Address: 192.168.1.102		13 6.234505	24.128.190.197	192.168.1.102	ICMP								
> Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) > Ethernet II, Src: Actionte 8a:70:1a (00:20:00:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)  **Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100  0100 = Version: 4  0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  Total Length: 84  Identification: 0x32d2 (13010) > Flags: 0x00 Fragment Offset: 0  **Time to Live: 3 Protocol: ICNP (1) Header Checksum: 0x2b2a [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.102	Ш												found!)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)  **Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100 0100 = Version: 4 0101 = Header Length: 20 bytes (5)  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  **Total Length: 84    Identification: 0x32d2 (13010)  **Flags: 0x00  Fragment Offset: 0  **Time to Live: 3  **Protocol: ICMP (1)  **Header Checksum: 0x2ba [validation disabled]  [Header checksum status: Unverified]  Source Address: 192.168.1.102		15 6.257672	24.128.0.101	192.168.1.102	ICMP	70 Time	-to-liv	e exceede	d (Time to	live exceeded i	n trans	it)	
<pre> V Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100 0100 = Version: 4 0101 = Header Length: 20 bytes (5)  &gt; Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 84 Identification: 0x32d2 (13010)  &gt; Flags: 0x00 Fragment Offset: 0  &gt; Time to Live: 3 Protocol: ICMP (1) Header Checksum: 0x2b2a [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.102 </pre>	>	Frame 12: 98 bytes	on wire (784 bits)	), 98 bytes captured (784	bits)								
0100 = Version: 4 101 = Header Length: 20 bytes (5)  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 84  Identification: 0x32d2 (13010)  > Flags: 0x00  Fragment Offset: 0  Time to Live: 3  Protocol: ICMP (1)  Header Checksum: 0x2b2a [validation disabled]  [Header checksum status: Unverified]  Source Address: 192.168.1.102	>												
0101 = Header Length: 20 bytes (5)  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  Total Length: 84  Identification: 0x32d2 (13010)  Flags: 0x00  Fragment Offset: 0  Time to Live: 3  Protocol: ICMP (1)  Header checksum: 0x2b2a [validation disabled]  [Header checksum status: Unverified]  Source Address: 192.168.1.102	~	v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100											
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  Total Length: 84  Identification: 0x32d2 (13010)  > Flags: 0x00  Fragment Offset: 0  Time to Live: 3  Protocol: ICMP (1)  Header Checksum: 0x2b2a [validation disabled]  [Header checksum status: Unverified]  Source Address: 192.168.1.102		0100 = Version: 4											
Total Length: 84  Identification: 0x32d2 (13010)  > Flags: 0x00  Fragment Offset: 0  > Time to Live: 3  Protocol: ICMP (1)  Header Checksum: 0x2b2a [validation disabled]  [Header checksum status: Unverified]  Source Address: 192.168.1.102		0101 = Header Length: 20 bytes (5)											
Identification: 0x32d2 (13010)  > Flags: 0x00 Fragment Offset: 0  > Time to Live: 3 Protocol: ICMP (1) Header Checksum: 0x2b2a [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.102		> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)											
> Flags: 0x00 Fragment Offset: 0 > Time to Live: 3 Protocol: ICMP (1) Header Checksum: 0x2b2a [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.102													
Fragment Offset: 0 > Time to Live: 3 Protocol: ICMP (1) Header Checksum: 0x2b2a [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.102			0x32d2 (13010)										
> Time to Live: 3 Protocol: ICMP (1) Header Checksum: 0x2b2a [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.102		0											
Protocol: ICMP (1) Header Checksum: 0x2b2a [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.102			0										
Header Checksum: 0x2b2a [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.102													
[Header checksum status: Unverified] Source Address: 192.168.1.102			. ,										
Source Address: 192.168.1.102													
Destination Address: 128.59.23.100													
> Internet Control Message Protocol	>	Internet Control M	essage Protocol										

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

Identification: 40316 TTL (Time to Live): 255

No.	Tine	Source	Destination	Protocol		
	8 6.163045	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (	
	9 6.176826	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transi	
	10 6.188629	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (	
	11 6.202957	24.218.0.153	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transi	
	12 6.208597	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (	
	13 6.234505	24.128.190.197	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transi	
	14 6.238695	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (	
	15 6.257672	24.128.0.101	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transi	t)
> Int	ernet Protocol 0100 = Vers 0101 = Head Differentiated S Total Length: 56 Identification: Flags: 0x00 Fragment Offset: Time to Live: 25 Protocol: ICMP ( Header Checksum: [Header checksum: Source Address:	Version 4, Src: 10.2 sion: 4 s	(16.228.1, Dst: 192.16 (5) (DSCP: CS6, ECN: Not	8.1.102	:70:1a (00:20:e0:8a:70:1a)	

# 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 value in the Identification field changes for all of the ICMP TTL-exceeded replies sent to the computer by the nearest (first hop) router. Because every IP datagram has a unique identification number, unless they are fragments of a large IP datagram.

The value of the TTL field remains unchanged for all of the ICMP TTL-exceeded replies sent to the computer by the nearest (first hop) router. Because the value of TTL only changes (minus one) when the IP datagram transfers through another 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?

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

11. Screenshot the first fragment of the fragmented IP datagram (with sufficient details to answer these questions). 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?

Information in the IP header indicates that the datagram been fragmented:

The flag bit for "More fragments" is set.

Information in the IP header indicates this is the first fragment:

The fragment offset is 0.

IP datagram length:

Total Length – 1500 bytes.

```
Source
128.119.245.12
                                                                                                   TCP
IPv4
                                                                                                               60 22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
        92 28.441511
                                  192.168.1.102
                                                                   128.59.23.100
                                  192,168,1,102
                                                                                                    TCMP
                                                                                                                     562 Echo (ping) request id=0x0300, seq=30467/887, tt]=1 (no response found!)
        96 28.471338 192.168.1.102
                                                                  128,59,23,100
                                                                                                    TCMP
                                                                                                                      562 Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response found!)
        97 28.490663 192.168.1.102
98 28.491323 192.168.1.102
                                                                                                                     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98
562 Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found!)
                                                                   128.59.23.100
    rame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
  Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys6_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
     0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 1500
Identification: 0x32f9 (13049)
  Identification: 0x32f9 (13049)

Flags: 0x20, 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: ICMP (1)
Header Checksum: 0x077b [validation disabled]
[Header checksum status: Unverified]
      Source Address: 192.168.1.102
      Destination Address: 128.59.23.100
[Reassembled IPv4 in frame: 93]
> Data (1480 bytes)
```

12. Screenshot the second fragment of the fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

The fragment offset is 1480 instead of 0, indicates that this is not the first datagram fragment. There are no more fragments, because flag bit for "More fragments" is not set.

```
Destination
192.168.1.102
                                                                                                                       Protocol Length Info

TCP 60 22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
        Time
91 22.952738
                                        Source
128.119.245.12
                                                                                                                                          1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93 562 Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)
          92 28,441511
                                                                                                                                         70 Time-to-live exceeded (Time to live exceeded in transit)
1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
552 Echo (ping) request id=0x0300, seq=30723888, ttl=2 (no response foundl)
1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
       94 28.462264
                                      10.216.228.1
                                                                               192.168.1.102
      96 28.471338 192.168.1.102
                                                                              128.59.23.100
        98 28.491323 192.168.1.102
                                                                               128.59.23.100
                                                                                                                       ICMP
                                                                                                                                            562 Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found!)
  Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
Ethernet II, Src: Actionte 8a:70:1a (00:20:e0:8a:70:1a), Dst: Links
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
  0100 ... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 548
Identification: 0x32f9 (13049)
 V Flags: 0x00

0... = Reserved bit: Not set
    0..... = Reserved bit: Not set
.0.... = Don't fragment: Not set
.0.... = More fragments: Not set
Fragment Offset: 1480
Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x2a7a [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[2 IPV4 Fragments (2008 bytes): #92(1480), #93
     [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
```

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

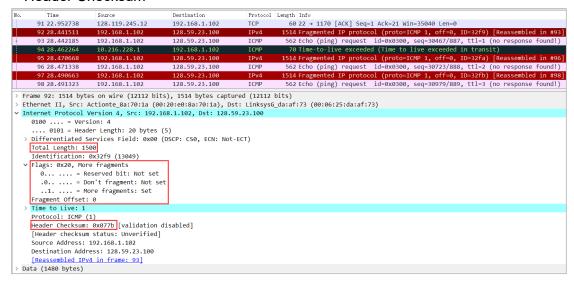
Fields change in the IP header between the first and second fragment:

**Total Length** 

Flags

Fragment Offset

Header Checksum



```
Destination
192.168.1.102
                                                                                                              Protocol Length Info

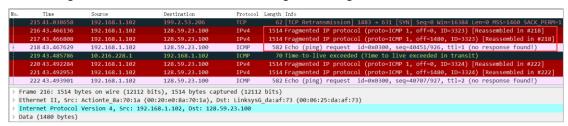
TCP 60 22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
       Time
91 22.952738
                                    Source
128.119.245.12
        92 28,441511
      94 28.462264
                                   10.216.228.1
                                                                        192.168.1.102
                                                                                                                                  70 Time-to-live exceeded (Time to live exceeded in transit) 514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Ref
                                                                                                                               1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96] 562 Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response found!) 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
      96 28.471338 192.168.1.102
      98 28.491323 192.168.1.102
                                                                         128.59.23.100
                                                                                                              ICMP
                                                                                                                                 562 Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found!)
     ame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Links
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
   0100 ... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 548

Identification: 0x32f9 (13049)

Flags: 0x00
       O... = Reserved bit: Not set
O... = Don't fragment: Not set
O... = More fragments: Not set
    Fragment Offset: 1480
Time to Live: 1
Protocol: ICMP (1)
   Protocol: ICMP (1)
Header Checksum: 0x2a7a [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
    [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
ternet Control Message Protocol
```

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

Three fragments were created from the original datagram.



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

Fields change in the IP header among the fragments:

Fragment Offset Header Checksum

No.	Time	Source	Destination		Length Info						
					62 [TCP Retransmission] 1483 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1						
	216 43.466136	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]						
	217 43.466808	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]						
+	218 43.467629	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)						
	219 43.485786	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)						
Ш	220 43.492284	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]						
	221 43.492953	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]						
	222 43.493901	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=40707/927, ttl=2 (no response found!)						
> F	rame 217: 1514 by	tes on wire (12112	bits), 1514 bytes capt	ured (1211	2 bits)						
> E	thernet II, Src: /	Actionte_8a:70:1a (	(00:20:e0:8a:70:1a), Ds	t: Linksys	G_da:af:73 (00:06:25:da:af:73)						
~ I	nternet Protocol \	Version 4, Src: 192	2.168.1.102, Dst: 128.5	9.23.100							
	0100 = Version: 4										
	0101 = Header Length: 20 bytes (5)										
	> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)										
	Total Length: 1500										
	Identification:										
'	Flags: 0x20, Mor										
		eserved bit: Not se									
	.0 = Do	on't fragment: Not	set								
		ore fragments: Set									
	Fragment Offset:	1480									
	Time to Live: 1										
	Protocol: ICMP (										
		0x0698 [validation									
	[Header checksum status: Unverified]										
	Source Address: 192.168.1.102										
		ess: 128.59.23.100									
Ι.	[Reassembled IPv4 in frame: 218]										
> 0	ata (1480 bytes)										

No.	Time	Source	Destination	Protocol	Length Info						
	215 41.038658	192.168.1.102	199.2.53.206	TCP	62 [TCP Retransmission] 1483 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK PERM=1						
1	216 43.466136	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]						
ш	217 43,466808	192,168,1,102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]						
	218 43,467629	192,168,1,102	128,59,23,100	ICMP	582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)						
	219 43.485786	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)						
	220 43.492284	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]						
Ш	221 43.492953	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]						
	222 43.493901	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=40707/927, ttl=2 (no response found!)						
> F	rame 218: 582 byt	es on wire (4656 bi	ts), 582 bytes capture	d (4656 bit	rs)						
> E	thernet II, Src:	Actionte_8a:70:1a (	00:20:e0:8a:70:1a), Ds	t: LinksysG	G_da:af:73 (00:06:25:da:af:73)						
V ]	V Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100										
-	0100 = Version: 4										
	0101 = Header Length: 20 bytes (5)										
	> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)										
	Total Length: 568										
	Identification:	0x3323 (13091)									
•	Flags: 0x01										
	0 = R	eserved bit: Not se	t								
	.0 = D	on't fragment: Not	set								
	0 = M	ore fragments: Not	set								
	Fragment Offset:	2960									
	Time to Live: 1										
	Protocol: ICMP (										
	Header Checksum:	0x2983 [validation	disabled]								
	[Header checksum status: Unverified]										
	Source Address:	192.168.1.102									
	Destination Addr	ess: 128.59.23.100									
	> [3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]										
> 1	internet Control M	essage Protocol									