Wireshark Lab 1: IP

Group Details: Shayshu $\mathrm{NR}-1005035196,$ Johnathan Yan - 1004745476

Mark:

	Question	Answer
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?	My Ip address is 10.0.0.230
Annotated Screensho t (if needed)	<pre>V Internet Protocol Version 4, Src: 10.0.0.230, Dst: 104.244.42.193 0100 = Version: 4 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 56 Identification: 0xc5fb (50683) Flags: 0x00 Fragment Offset: 0 Time to Live: 255 Protocol: ICMP (1) Header Checksum: 0x0000 [validation disabled] [Header checksum status: Unverified] Source Address: 10.0.0.230 Destination Address: 104.244.42.193</pre>	
2	Within the IP packet header, what is the value in the upper layer protocol field?	The protocol is ICMP
Annotated Screensho t (if needed)	How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined	The IP header has 20 bytes, and the total message has 56 bytes of data. So, the payload is only 36 bytes.
Annotated	the number of payload bytes. Data (56 by	
Screensho t (if needed)	Tro bytes for header	

4	Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.	No because the more fragments flag is not set and the fragment offset is 0.	
Annotated	∨ Flags: 0x00		
Screensho	O = Reserved bit: Not set		
t (if	0 = Don't fragment: Not set		
needed)	0 = More fragments:	Not set	
	Fragment Offset: 0		
	Time to Live: 255		
5	Which fields in the IP datagram always	The time to live field, the header	
	change from one datagram to the next	checksum, and the identification	
	within this series of ICMP messages sent	fields will always change	
	by your computer?		
Annotated Screensho	Identification	Time to Live Header Checksum	
t (if	0x0000 (0),0x32e5 (13029)	/ 247,1 0xe906,0xf601	
needed)	0x32e6 (13030)	9 0x2516	
	0x32e7 (13031)	10 0x2415	
	0x0000 (0),0x32e6 (13030)	246,1 0x217f,0xf600	
	0x32e8 (13032)	11 0x2314	
	0x0000 (0),0x32e7 (13031)	244,1 0x220c,0xf5ff	
	0x32e9 (13033)	12 0x2213	
	0x32ea (13034)	13 0x2112	
	0x4b6b (19307),0x32e9 (13033)	243,1 0x38e7,0xf5fd	
	0x0952 (2386)	242 0x25a9	
	0x32eb (13035)	1 0x2d11	
	0x9db8 (40376),0x32eb (13035)	255,1 0x6c64,0xf5fb	
	0x32ec (13036)	2 0x2c10	
	0x0000 (0),0x32ec (13036)	254,1 0xe143,0xf5fa	
	0x32ed (13037)	3 0x2b0f	
	0x0000 (0),0x32ed (13037) 0x32ee (13038)	253,1 0x2471,0xf5f9 4 0x2a0e	
		252,1 0xe3d1,0xf5f8	
	0x0000 (0),0x32ee (13038) 0x32ef (13039)	5 0x290d	
	0x0000 (0),0x32ef (13039)	248,1 0xc508,0xf5f7	
6	Which fields stay constant? Which of the	The version, source address,	
O	fields must stay constant? Which fields	destination address, header length,	
	must change? Why?	the differentiated services field, and	
		the protocol type all stay constant.	
		The above also must stay constant.	
		The checksum, identification, and time to live must change.	
Annotated		time to five must change.	
Screensho			
	I		

t (if needed)		
7	Describe the pattern you see in the values in the Identification field of the IP datagram.	The identification field increases by one for every ping request sent out
Annotated Screensho t (if needed)		
8	What is the value in the Identification field and the TTL field?	Identification 0x9d7c, time to live 255.
Annotated Screensho t (if needed)	<pre>Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.102 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT) Total Length: 56 Identification: 0x9d7c (40316) > Flags: 0x00 Fragment Offset: 0 Time to Live: 255 Protocol: ICMP (1) Header Checksum: 0x6ca0 [validation disabled] [Header checksum status: Unverified] Source Address: 10.216.228.1 Destination Address: 192.168.1.102</pre>	
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 time to live values stay consistent but the identification values change.
Annotated Screensho t (if needed)	Identification 0x9d7c (40316),0x32d0 (30x9d98 (40344),0x32de (30x9d98 (40376),0x32eb (30x9e06 (40454),0x32f9 (30x9e2c (40492),0x3307 (30x9e5a (40572),0x3330 (30x9e95 (40597),0x3330 (30x9e95 (40635),0x333e (30x9ebb (40635),0x33ae (40x9ebb (40635),0x33ae (40x9ebb (40635),0x3ae (40x9ebb (40635),0x3ae (40x9ebb (40635),0x3ae (40x9ebb (40635),0x3ae (40x9ebb (40635),0xae (40x9ebb (40635),0xae (40x9ebb (40635),0xae (40x9ebb (40635),0xae (40x9ebb (40x	13022) 255,1 13035) 255,1 13049) 255,1 13063) 255,1 13077) 255,1 13091) 255,1 13104) 255,1
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 it was fragmented

Annotated	1500 Fragmented IP protocol (proto=ICMP 1	, off=0, ID=32f9) [Reassembled in #93]		
Screensho	548 Echo (ping) request id=0x0300, seq=			
t (if	56,1500 Time-to-live exceeded (Time to live exceeded in transit)			
,	1500 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]			
548 Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response				
	1500 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled			
	548 Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found!)			
1500 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled				
	548 Echo (ping) request id=0x0300, seq=			
11	Print out the first fragment of the	The More fragments flag is set.		
	fragmented IP datagram. What	The fragment offset is set to zero.		
	information in the IP header indicates that	The first one is 1500 bytes, this size		
	the datagram been fragmented? What	includes the size of the header.		
	information in the IP header indicates			
	whether this is the first fragment versus a			
	latter fragment?			
	How long is this IP datagram?			
Annotated	Internet Protocol Version 4, Src: 192.168	.1.102, Dst: 128.59.23.100		
Screensho	0100 = Version: 4			
t (if	0101 = Header Length: 20 bytes (5)			
needed)	> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)			
necaca)	Total Length: 1500	- 5.70 of Johnson		
	Identification: 0x32f9 (13049)	rife of Warn Jeans		
	Total Length: 1500 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: 0x077h [validation disabled]			
	<pre>0 = Reserved bit: Not set</pre>	- us as buch		
	.0 = Don't fragment: Not set	Tell'S 123 1200		
	1 = More fragments: Set	more		
	Fragment Offset: 0	are the		
	> Time to Live: 1	Coancots		
	Protocol: ICMP (1)	ten 2.		
	Header Checksum: 0x077b [validation dis	sabled]		
	[Header checksum status: Unverified]			
	Source Address: 192.168.1.102			
	Destination Address: 128.59.23.100			
12	[Reassembled IPv4 in frame: 93]	The Comment offers		
12	Print out the second fragment of the	The fragment offset is non-zero.		
	fragmented IP datagram. What	There are no more fragments		
	information in the IP header indicates that	because the More fragments flag is		
	this is not the first datagram fragment? Are	not set.		
	the more			
	fragments? How can you tell?			
L				

Annotated	✓ Internet Protocol Version 4, Src: 19	92.168.1.102. Dst: 128.59.23.100		
Screensho	0100 = Version: 4	,		
t (if	0101 = Header Length: 20 byt	es (5)		
`	> Differentiated Services Field: 0x	And the following the control of the		
needed)	Total Length: 548			
	Identification: 0x32f9 (13049)			
	✓ Flags: 0x00	ala man		
	0 = Reserved bit: Not set			
	.0 = Don't fragment: Not set frag 15			
	= More fragments: Not set			
	Fragment Offset: 1480			
	> Time to Live: 1			
	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: ICMP (1) Not the 1st fragment			
	Header Checksum: 0x2a7a [validati	on 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)]		
13	What fields change in the IP header	The more fragments flag, the		
	between the first and second fragment?	checksum, the fragment offset field,		
	out the me and second nagment.	and the total length.		
		and the total length.		
Annotated		rnet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100		
Screensho	0101 = Header Length: 20 bytes (5)	100 = Version: 4 0101 = Header Length: 20 bytes (5)		
t (if	Total Length: 1500 Z	ifferentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) otal Length: 548		
`	→ Flags: 0x20, More fragments	dentification: 0x32f9 (13049) lags: 0x00		
needed)	0 = Reserved bit: Not set .0 = Don't fragment: Not set	<pre>0 = Reserved bit: Not set .0 = Don't fragment: Not set</pre>		
		.0 = More fragments: Not set ragment Offset: 1480		
	Protocol: ICMP (1)	ime to Live: 1 Potocol: ICMP (1)		
	[Header checksum status: Unverified]	<mark>eader Checksum: 0x2a7a</mark> [validation disabled] Header checksum status: Unverified]		
	Destination Address: 128.59.23.100	ource Address: 192.168.1.102 estination Address: 128.59.23.100		
1.4		2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]		
14	How many fragments were created from	3 fragments were created		
	the original datagram?			
	1 1500 Fragmented ID protectal (prote-TCMD 1 of	f_0 ID_2222\ [Paggambled in #210]		
Annotaated	1500 Fragmented IP protocol (proto=ICMP 1, of 1500 Fragmented IP protocol (proto=ICMP 1, of			
Screensho	3 568 Echo (ping) request id=0x0300, seq=4045			
t (if				
needed)	3 fragments created t	,		
15	What fields change in the IP header among	The total length, the more fragments		
	the fragments?	flag, the fragment offset, and the		
		checksum change. Note that the		
		total length only differs between the		
		3 rd fragment. And the more		
		fragments flag is only set to 0 in the		
		3 rd fragment.		
		J magment.		

```
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
                                                                                                                                  Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
Annotated
                                0100 ... - Version: 4
... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
                                                                                                                                     0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Screensho
t (if
                                   Identification: 0x3323 (13091)
                                                                                                                                      Identification: 0x3323 (13091)
                                Flags: 0x20, More fragments
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
                                                                                                                                  Identification: 0x3323 (13091)

*Flags: 0x20, More fragments

0..... = Reserved bit: Not set

.0..... = Don't fragment: Not, set

.1... = More fragments: Set

Fragment Offset: 1480
needed)
                                  .1. ... = More fragments: Set
Fragment Offset: 0
Time to Live: 1
Protocol: ICMP (1)
                                                                                                                                   Fragment Offset: 1480

> Time to Live: 1

Protocol: ICMP (1)

Header Checksum: 0x6698 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.162

Destination Address: 128.59.23.100

[Bracerabled Tibut in Fragment 202]
                                   Protocol: ICMP (1)
Header Checksum: 0x0751 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
                                   Destination Address: 128.59.23.100 [Reassembled IPv4 in frame: 218]
                                                                                                                                      [Reassembled IPv4 in frame: 218]
                                Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
                                    0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
                                                                                                                                                                     All different

1st and 2nd some

2nd different
                                 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
                                    Identification: 0x3323 (13091)
                                ∨ Flags: 0x01
                                         0... = Reserved bit: Not set
                                          .0.. .... = Don't fragment: Not set
                                  Fragment Offset: 2960
                                 > Time to Live: 1
                                    Protocol: ICMP (1)
                                    Header Checksum: 0x2983 [validation disabled]
                                    [Header checksum status: Unverified]
                                    Source Address: 192.168.1.102
                                    Destination Address: 128.59.23.100
                                    [3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]
```