Wireshark Lab 1: IP

Group Details:

Leting Ni 1006255446 Yuhe Chen 1005689480

Mark:

	Question	Answer	
1	Select the first ICMP Echo Request	192.168.1.102	
	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?		
Annotated	V Internet Ductocal Vancian 4 Cock	102 109 1 102 Det. 129 F0 22 100	
Screenshot	∨ Internet Protocol Version 4, Src:	192.168.1.102, DSC: 128.59.25.100	
(if needed)			
2	Within the IP packet header, what	ICMP (1)	
2	is the value in the upper layer	icivii (1)	
	protocol field?		
	protocor neid:		
Annotated	> Time to Live: 1		
Screenshot	Protocol: ICMP (1)		
(if needed)	Header Checksum: 0x2d2c [valid	dation disabled]	
	[Header checksum status: Unver	rified]	
3	How many bytes are in the IP	Header: 20 bytes	
	header? How many bytes are in the		
	payload of the IP datagram?	Total: 84 bytes	
	Explain how you determined the	Payload: $84 - 20 = 64$ bytes	
	number of payload bytes.		
Annotated	<pre> VInternet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100 0100 = Version: 4 </pre>		
Screenshot	0101 = Header Length: 20 b	vtes (5)	
(if needed)	> Differentiated Services Field:		
	Total Length: 84		
	Identification: 0x32d0 (13008)		
4	Has this IP datagram been	Fragment Offset is 0 and More	
	fragmented? Explain how you	fragments flag is not set, therefore	
	determined whether or not the	this IP datagram is not fragmented.	
	datagram has been fragmented.		

Annotated	∨ Flags: 0x00		
Screenshot	0 = Reserved bit: Not set		
(if needed)	.0 = Don't fragment: Not set		
(II liceaca)	0 = More	_	
	0 0000 0000 0000	_	
5			Identification, Time to Live, and
3	Which fields in the IP data always change from one d	_	Header Checksum.
	to the next	iatagrain	ricader Cheeksum.
	within this series of ICMP)	
	messages sent by your cor		
	messages sent by your cor	inputer:	
Annotated	368 53.778721 192.168.1.102 128.59.		368 53.778721 192.168.1.102 128.59.23.100 ICMP 365 53.758584 [192.168.1.102 128.59.23.100 ICMP
Screenshot	365 53.758584 192.168.1.102 128.59. 361 53.728518 192.168.1.102 128.59. 358 53.714979 192.168.1.102 128.59.	.23.100 ICMP	361 53.728518 192.168.1.102 128.59.23.100 ICMP 358 53.714979 192.168.1.102 128.59.23.100 ICMP
(if needed)	Differentiated Services Field: 0x00 (DSCP: CS0,		Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
(II liceacu)	Total Length: 568 Identification: 0x334a (13130)	ecn. Not-ect)	Total Length: 568 Identification: 0x3349 (13129)
	Flags: 0x01 0 1011 1001 0000 = Fragment Offset: 2960		Flags: 0x01 0 1011 1001 0000 = Fragment Offset: 2960
	Time to Live: 13 Protocol: ICMP (1)		Time to Live: 12 Protocol: ICMP (1)
	Header Checksum: 0x1d5c [validation disabled] [Header checksum status: Unverified]		Header Checksum: 0x1e5d [validation disabled] [Header checksum status: Unverified]
	Source Address: 192.168.1.102 Destination Address: 128.59.23.100		Source Address: 192.168.1.102 Destination Address: 128.59.23.100
6	[3 IPv4 Fragments (3508 bytes): #366(1480), #367		[3 IPv4 Fragments (3508 bytes): #363(1480), #364(1480), #365(548)]
0	Which fields stay constant? Which of the	Stay cons	using IPv4)
	fields must stay	Header Le	9 ,
	constant? Which fields		Address (from the same source)
	must change? Why?		,
	must change? Why? Destination IP Address (to the same destination) Upper Layer Protocol (using ICMP)		·
		opper Ea	yer rrotocor (using reivir)
		Must stay	y constant:
		•	using IPv4)
		Header Le	<u> </u>
	Source IP Address (from the same source) Destination IP Address (to the same destination)		
			` /
			yer Protocol (using ICMP)
			, ,
		Must cha	inge:
			tion (to identify different IP datagrams)
			hecksum (headers are different)
Annotated			
Screenshot			
(if needed)			
7	Describe the pattern you see in the Identification decrements by 1 each		
	values in the Identification	n field of	time as going from one message to
	the IP datagram		the next. (Packet No. is in decreasing
			order.)

Annotated Screenshot (if needed)	368 53.778721 [192.168.1.102 128.59.23.100 ICMP 365 53.758584 192.168.1.102 128.59.23.100 ICMP 361 53.728518 192.168.1.102 128.59.23.100 ICMP 358 53.714979 192.168.1.102 128.59.23.100 ICMP Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 568 Identification: 0x334a (13130) Flags: 0x01 0 1011 1001 0000 = Fragment Offset: 2960 Time to Live: 13 Protocol: ICMP (1) Header checksum: 0x1d5c [validation disabled] Header checksum: 0x1d5c [validation disabled] Source Address: 192.168.1.102 Destination Address: 128.59.23.100 [3 IPv4 Fragments (3508 bytes): #366(1480), #367(1480), #368(548)] What is the value in the Identification field and the TTL field?	368 53.778721 192.168.1.102 128.59.23.100 ICMP 365 53.758584 192.168.1.102 128.59.23.100 ICMP 361 53.728518 192.168.1.102 128.59.23.100 ICMP 358 53.714979 192.168.1.102 128.59.23.100 ICMP Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 568 Identification: 0x3349 (13129) Flags: 0x010 1011 1001 0000 = Fragment Offset: 2960 Time to Live: 12 Protocol: ICMP (1) Header Checksum: 0x165d [validation disabled] [Header checksum status: Univerified] Source Address: 192.168.1.102 Destination Address: 128.59.23.100 [3 IPv4 Fragments (3508 bytes): #363(1480), #364(1480), #365(548)] Identification: Ox4fcd (20429)
Annotated Screenshot (if needed)	377 54.774816 128.59.1.41 192.168 320 49.770176 128.59.1.41 192.168 Identification: 0x4fcd (20429) Flags: 0x00	
	0 0000 0000 0000 = Fragment Offset: 0	
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?	Values of Identification change since Identification is unique for each IP datagram (if it is not fragmented). Values of TTL are unchanged since they are all TTL of the nearest router.
Annotated Screenshot (if needed)		
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 is fragmented.
Annotated Screenshot (if needed)		1Pv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) ICMP 562 Echo (ping) request id=0x0300, seq=30467/887, ttl=1
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?	More fragments flag is set, therefore the IP datagram is fragmented. Fragment Offset is 0, therefore it is the first fragment. The total length is 1500 bytes.

Annotated	92 28.441511 192.168.1.102 128.59.	23.100 IPv4 1514 Fragmented IP protocol	
	S		
Screenshot	0100 Ver 31011. 4		
(if needed)	0101 = Header Length: 20 bytes (5) V Differentiated Services Field: 0x00 (DSCP: CS0, E	ECN: Not-ECT)	
	0000 00 = Differentiated Services Codepoint: Default (0)		
	00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)		
	Total Length: 1500 Identification: 0x32f9 (13049)		
	<pre> Flags: 0x20, More fragments </pre>		
	0 = Reserved bit: Not set		
	.0 = Don't fragment: Not set1 = More fragments: Set		
	0 0000 0000 0000 = Fragment Offset: 0		
	> Time to Live: 1		
12	Print out the second fragment of the	Fragment Offset is 1480, therefore it	
12		1	
	fragmented IP datagram. What	is not the first fragment.	
	information in the IP header		
	indicates that this is not the first	More fragments flag is not set,	
	datagram fragment? Are the more	therefore there are no more fragments.	
	fragments? How can you tell?		
	armenter in the four four terms		
Annotated	92 28.441511 192.168.1.102 128.59.2	3.100 IPv4 1514 Fragmented IP protocol	
Screenshot	93 28.442185 192.168.1.102 128.59.2	3.100 ICMP 562 Echo (ping) request id	
(if needed)	Flags: 0x00 0 = Reserved bit: Not set		
	.0 = Don't fragment: Not set		
	= More fragments: Not set		
13	What fields change in the ID header	Total Length, Flags, More fragments,	
13	What fields change in the IP header		
	between the first and second	Fragment Offset, and Header	
	fragment?	Checksum.	
Annotated	92 28.441511 192.168.1.102 128.59.23.100 IPv4 93 28.442185 192.168.1.102 128.59.23.100 ICMP	92 28.441511 192.168.1.102 128.59.23.100 IPv4 93 28.442185 192.168.1.102 128.59.23.100 ICMP	
Screenshot	Total Length: 1500	Tatal Length, 549	
(if needed)	Identification: 0x32f9 (13049)	Total Length: 548 Identification: 0x32f9 (13049)	
(II liceacu)	Flags: 0x20, More fragments 0 = Reserved bit: Not set	Plags: 0x00 0 = Reserved bit: Not set	
	.0 = Don't fragment: Not set1 = More fragments: Set	.0 = Don't fragment: Not set0 = More fragments: Not set	
	0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 1	0 0101 1100 1000 = Fragment Offset: 1480 Time to Live: 1	
	Protocol: ICMP (1) Header Checksum: 0x077b [validation disabled]	Protocol: ICMP (1) Header Checksum: 0x2a7a [validation disabled]	
14	How many fragments were created	2 fragments.	
1	from the original datagram?	2 magniones.	
	Troni the original datagram:		
	92 28.441511 192.168.1.102 128.59.23.100	IPv4 1514 Fragmented IP protocol (proto=ICMP 1. off=0. ID=32f9)	
Annotated		IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) ICMP 562 Echo (ping) request id=0x0300, seq=30467/887, ttl=1	
Screenshot			
(if needed)			
15	What fields change in the IP header	Fragment Offset and Header	
	among the fragments?	Checksum should always change for	
	among the magnitude.	1	
		all fragments.	

	Total Length and More fragments should only change for the last fragment.
Annotated	1 20 2 2
Screenshot	
(if needed)	