Wireshark Lab 1: IP

Group Details:

Leting Ni 1006255446
Yuhe Chen 1005689480

Mark:

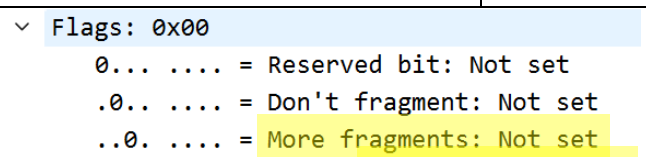
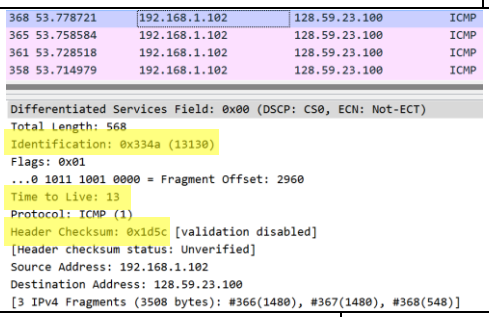
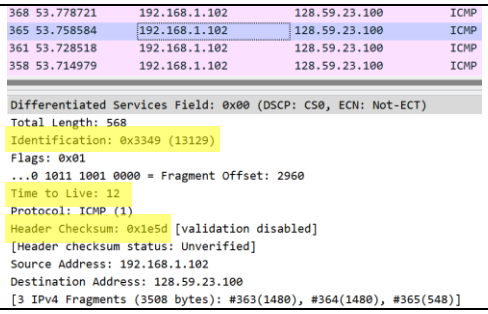
	Question	Answer
1	Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?	192.168.1.102
Annotated Screenshot (if needed)	`Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100`	
2	Within the IP packet header, what is the value in the upper layer protocol field?	ICMP (1)

Annotated Screenshot (if needed)	`Time to Live: 1`
	`Protocol: ICMP (1)`
	`Header Checksum: 0x2d2c [validation disabled]`
	`[Header checksum status: Unverified]`	

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.	Header: 20 bytes Total: 84 bytes Payload: 84 – 20 = 64 bytes

Annotated Screenshot (if needed)	`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)`	

4	Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.	Fragment Offset is 0 and More fragments flag is not set, therefore this IP datagram is not fragmented.

Annotated Screenshot (if needed)		
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.
Annotated Screenshot (if needed)		
6	Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?	**Stay constant:** Version (using IPv4) Header Length (20) Source IP Address (from the same source) Destination IP Address (to the same destination) Upper Layer Protocol (using ICMP) **Must stay constant:** Version (using IPv4) Header Length (20) Source IP Address (from the same source) Destination IP Address (to the same destination) Upper Layer Protocol (using ICMP) **Must change:** Identification (to identify different IP datagrams) Header Checksum (headers are different)
Annotated Screenshot (if needed)		
7	Describe the pattern you see in the values in the Identification field of the IP datagram	Identification decrements by 1 each time as going from one message to 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 status: Unverified] Source Address: 192.168.1.102 Destination Address: 128.59.23.100 [3 IPv4 Fragments (3508 bytes): #366(1480), #367(1480), #368(548)]	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: 0x01 ...0 1011 1001 0000 = Fragment Offset: 2960 Time to Live: 12 Protocol: ICMP (1) Header Checksum: 0x1e5d [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.102 Destination Address: 128.59.23.100 [3 IPv4 Fragments (3508 bytes): #363(1480), #364(1480), #365(548)]
8	What is the value in the Identification field and the TTL field?	Identification: 0x4fcd (20429) TTL: 243
Annotated Screenshot (if needed)	377 54.774816 128.59.1.41 192.168.1.102 ICMP 70 Time-to-live exceeded 320 49.770176 128.59.1.41 192.168.1.102 ICMP 70 Time-to-live exceeded Identification: 0x4fcd (20429) Flags: 0x00 ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 243	
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)	92 28.441511 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) 93 28.442185 192.168.1.102 128.59.23.100 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 Screenshot (if needed)	92 28.441511 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, 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) Flags: 0x20, More fragments 0... .... = Reserved bit: Not set .0.. .... = Don't fragment: Not set ..1. .... = More fragments: Set ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 1 Protocol: ICMP (1)	
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?	Fragment Offset is 1480, therefore it is not the first fragment. More fragments flag is not set, therefore there are no more fragments.
Annotated Screenshot (if needed)	92 28.441511 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol 93 28.442185 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id 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	
13	What fields change in the IP header between the first and second fragment?	Total Length, Flags, More fragments, Fragment Offset, and Header Checksum.
Annotated Screenshot (if needed)	92 28.441511 192.168.1.102 128.59.23.100 IPv4 93 28.442185 192.168.1.102 128.59.23.100 ICMP 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 ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 1 Protocol: ICMP (1) Header Checksum: 0x077b [validation disabled] 92 28.441511 192.168.1.102 128.59.23.100 IPv4 93 28.442185 192.168.1.102 128.59.23.100 ICMP Total Length: 548 Identification: 0x32f9 (13049) 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: 1 Protocol: ICMP (1) Header Checksum: 0x2a7a [validation disabled]	
14	How many fragments were created from the original datagram?	2 fragments.
Annotated Screenshot (if needed)	92 28.441511 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) 93 28.442185 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=30467/887, ttl=1	
15	What fields change in the IP header among the fragments?	Fragment Offset and Header Checksum should always change for all fragments.

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