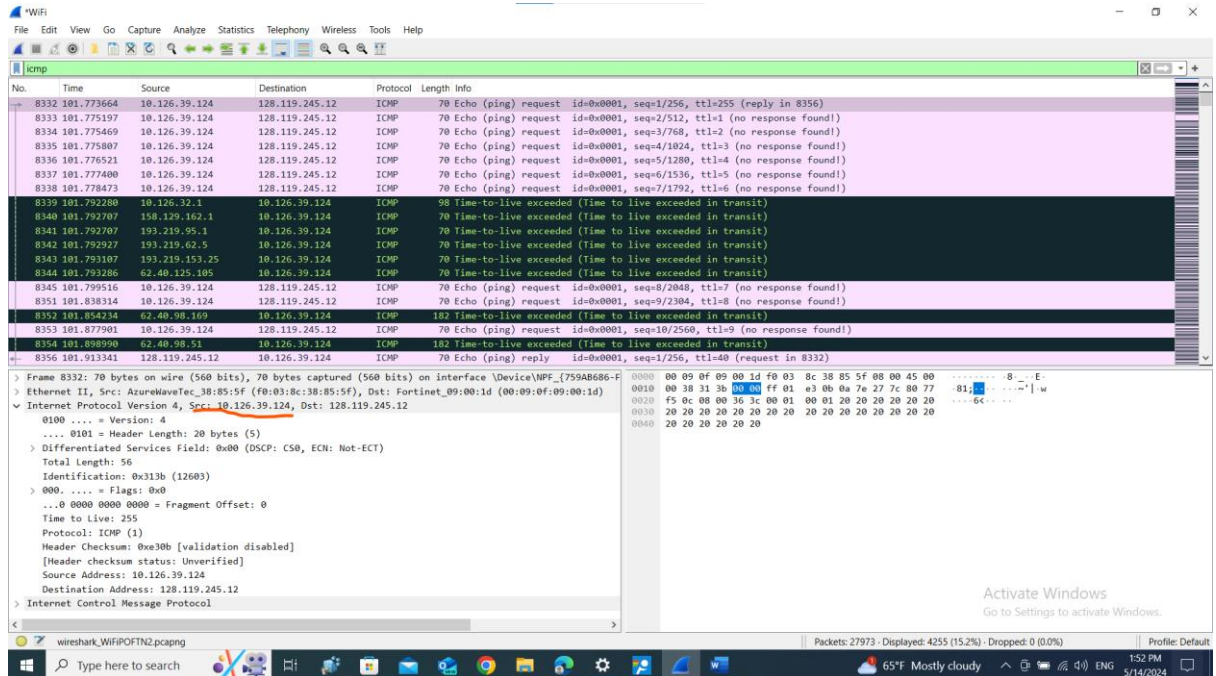


Lab Work 4 : IP

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?

Ans .



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

Ans. ICMP(1)

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.

Ans. Header length : 20;

Total length : 56;

payload bytes : 56-20;

=36

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

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0x313b (12603)
v 000. .... = Flags: 0x0
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0xe30b [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.126.39.124
Destination Address: 128.119.245.12
> Internet Control Message Protocol
```

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?

Ans. I) identification
ii) header Checksum
iii) Time to Live

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

Ans. Not change : i) version
ii) header length
iii) flag
iv) fragmentation of set
change : I) identification
ii) header Checksum
iii) Time to Live

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

Ans. I can see an incrementing pattern.

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

Wireshark packet capture showing ICMP Echo (ping) requests and replies. The packet list shows several ICMP Echo (ping) requests from 10.126.39.124 to 128.119.245.12. The packet details pane shows the ICMP Echo (ping) request packet with the Identification field set to 0x32ba (12986) and the Time to Live field set to 255. The packet bytes pane shows the raw data of the ICMP Echo (ping) request.

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?

Ans. Identification field is changing and TTL is decreasing

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?

Wireshark packet capture showing ICMP Echo (ping) requests and replies. The packet list shows several ICMP Echo (ping) requests from 10.126.39.124 to 128.119.245.12. The packet details pane shows the ICMP Echo (ping) request packet with the Identification field set to 0x32ba (12986) and the Time to Live field set to 255. The packet bytes pane shows the raw data of the ICMP Echo (ping) request.

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?

The image shows a Wireshark packet capture of a network interface. The packet list on the left shows several ARP requests and a fragmented IP datagram (packet 856). The packet details pane on the right shows the structure of the fragmented IP datagram, including the Ethernet II header, Internet Protocol Version 4 header, and ICMP Echo (ping) request. The packet bytes pane on the right shows the raw data of the packet, which is a fragmented IP datagram. The packet list shows that the fragmented IP datagram is composed of multiple fragments, with the first fragment being 1514 bytes long and the second fragment being 1514 bytes long. The packet details pane shows that the fragmented IP datagram is an ICMP Echo (ping) request, with the destination IP address being 10.126.32.1. The packet bytes pane shows the raw data of the packet, which is a fragmented IP datagram.

No.	Time	Source	Destination	Protocol	Length	Info
847	10.905443	Fortinet_09:00:1d	AzureWaveTec_38:85:1d	ARP	56	Who has 10.126.38.48? Tell 10.126.32.1
848	10.933034	Apple_56:7e:a2	AzureWaveTec_38:85:1d	ARP	60	ARP Announcement for 10.126.34.108
849	10.951614	Fortinet_09:00:1d	AzureWaveTec_38:85:1d	ARP	56	Who has 10.126.32.166? Tell 10.126.32.1
850	10.959016	Fortinet_09:00:1d	AzureWaveTec_38:85:1d	ARP	60	Who has 10.126.34.142? Tell 10.126.32.1
851	10.959775	Fortinet_09:00:1d	AzureWaveTec_38:85:1d	ARP	60	Who has 10.126.32.208? Tell 10.126.32.1
852	10.959775	Fortinet_09:00:1d	AzureWaveTec_38:85:1d	ARP	60	Who has 10.126.34.191? Tell 10.126.32.1
853	10.991556	Fortinet_09:00:1d	AzureWaveTec_38:85:1d	ARP	56	Who has 10.126.37.195? Tell 10.126.32.1
854	11.001655	Fortinet_09:00:1d	AzureWaveTec_38:85:1d	ARP	56	Who has 10.126.39.0? Tell 10.126.32.1
855	11.004290	Fortinet_09:00:1d	AzureWaveTec_38:85:1d	ARP	56	Who has 10.126.34.118? Tell 10.126.32.1
856	11.017170	10.126.39.124	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=a2ae) [Reassembled in #858]
857	11.017170	10.126.39.124	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=a2ae) [Reassembled in #858]
858	11.017170	10.126.39.124	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=29488/57458, ttl=255 (reply in 966)
859	11.018501	10.126.39.124	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=a2af) [Reassembled in #861]
860	11.018501	10.126.39.124	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=a2af) [Reassembled in #861]
861	11.018501	10.126.39.124	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=29489/57714, ttl=1 (no response found!)
862	11.018771	10.126.39.124	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=a2b0) [Reassembled in #864]
863	11.018771	10.126.39.124	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=a2b0) [Reassembled in #864]
864	11.018771	10.126.39.124	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=29410/57970, ttl=2 (no response found!)
865	11.018802	10.126.39.124	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=a2b1) [Reassembled in #867]

Frame 856: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF...
> Ethernet II, Src: AzureWaveTec_38:85:1d (f0:03:8c:85:1d), Dst: Fortinet_09:00:1d (00:09:0f:09:00:1d)
> Internet Protocol Version 4, Src: 10.126.39.124, Dst: 128.119.245.12
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0xa2ae (41646)
0001 = Flags: 0x1, 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: 255
Protocol: ICMP (1)
Header Checksum: 0x4bf4 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.126.39.124

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?

The top screenshot shows a packet capture with a filter 'Apply a display filter -> <Ctrl>'. The bottom screenshot shows the same capture with a different filter applied. Both screenshots show a list of packets and a detailed view of a selected packet.

Top Screenshot:

- Filter: Apply a display filter -> <Ctrl>
- Packet 857: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF... (00:09:0F:09:00:1D)
- Protocol: Internet Protocol Version 4, Src: 10.126.39.124, Dst: 128.119.245.12
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 1500
- Identification: 0xa2ae (41646)
- 001. = Flags: 0x1, More fragments
- 0... = Reserved bit: Not set
- ..0... = Don't fragment: Not set
- ...1. = More fragments: Set
- ...0 0000 1011 1001 = Fragment Offset: 1480
- Time to Live: 255
- Protocol: ICMP (1)
- Header Checksum: 0x4b3b [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 10.126.39.124

Bottom Screenshot:

- Filter: Apply a display filter -> <Ctrl>
- Packet 857: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface \Device\NPF... (759A2...)
- Ethernet II, Src: AzureWaveTec_38:85:5f (f8:03:8c:38:85:5f), Dst: Fortinet_09:00:1d (00:09:0f:09:00:1d)
- Internet Protocol Version 4, Src: 10.126.39.124, Dst: 128.119.245.12
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 540
- Identification: 0xa2ae (41646)
- 000. = Flags: 0x0
- 0... = Reserved bit: Not set
- ..0... = Don't fragment: Not set
- ...0 0001 0111 0010 = Fragment Offset: 2960
- Time to Live: 255
- Protocol: ICMP (1)
- Header Checksum: 0x6e42 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 10.126.39.124

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

Ans. More fragments fields are changed.

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

Ans. 3 fragments

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

Ans. More fragments and fragment offset field.

WiFi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl>F

No.	Time	Source	Destination	Protocol	Length	Info
820	18.921869	Fortinet_09:00:1d	AzureWaveTec_38:85:12	ARP	60	Who has 10.126.40.152? Tell 10.126.32.1
821	18.956896	Fortinet_09:00:1d	AzureWaveTec_38:85:12	ARP	56	Who has 10.126.33.84? Tell 10.126.32.1
822	18.969748	Fortinet_09:00:1d	AzureWaveTec_38:85:12	ARP	56	Who has 10.126.38.56? Tell 10.126.32.1
823	18.979755	LiteonTechno_79:4a:12	AzureWaveTec_38:85:12	ARP	60	Who has 10.126.40.81? Tell 10.126.40.255
824	18.988391	10.126.39.124	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=a479) [Reassembled in #826]
825	18.988391	10.126.39.124	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=a479) [Reassembled in #826]
826	18.988391	10.126.39.124	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=29867/43892, ttl=255 (reply in 848)
827	19.009757	Fortinet_09:00:1d	AzureWaveTec_38:85:12	ARP	56	Who has 10.126.39.58? Tell 10.126.32.1
828	19.019401	Intel_77:ac:9f	AzureWaveTec_38:85:12	ARP	56	Who has 10.126.36.129? Tell 10.126.37.21
829	19.020170	Intel_77:ac:9f	AzureWaveTec_38:85:12	ARP	56	Who has 10.126.35.222? Tell 10.126.37.21
830	19.020170	Intel_77:ac:9f	AzureWaveTec_38:85:12	ARP	56	Who has 10.126.39.9? Tell 10.126.37.21
831	19.027087	10.126.39.124	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=a47a) [Reassembled in #833]
832	19.027087	10.126.39.124	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=a47a) [Reassembled in #833]
833	19.027087	10.126.39.124	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=29868/44148, ttl=1 (no response found)
834	19.032183	10.126.32.1	10.126.39.124	ICMP	598	Time-to-live exceeded (Time to live exceeded in transit)
835	19.053599	9e:45:32:20:5d:9e	AzureWaveTec_38:85:12	ARP	56	Who has 10.126.32.168? (ARP Probe)
836	19.064448	CloudNetwork_98:fe:12	AzureWaveTec_38:85:12	ARP	56	Who has 10.126.32.152? Tell 10.126.33.193
837	19.064448	Intel_7f:ed:38	AzureWaveTec_38:85:12	ARP	56	Who has 10.126.33.245? Tell 10.126.36.241
838	19.065723	10.126.39.124	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=a47b) [Reassembled in #840]

> Frame 825: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF...
> Ethernet II, Src: AzureWaveTec_38:85:5f (f8:03:8c:38:85:5f), Dst: Fortinet_09:00:1d (00:09:0f:09:00:1d)
> Internet Protocol Version 4, Src: 10.126.39.124, Dst: 128.119.245.12
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0xa479 (42105)
0001 = Flags: 0x1, More fragments
0... = Reserved bit: Not set
..0... = Don't fragment: Not set
...1.... = More fragments: Set
...0 0000 1011 1001 = Fragment Offset: 1480
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0xa470 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.126.39.124

0000 00 09 0f 09 00 1d f0 03 8c 38 85 5f 08 00 45 00 8...E.
0010 09 4c a4 79 20 19 ff 01 49 70 0a 7a 27 7c 80 77 ...y...Ip...W
0020 f5 0c 20 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 20
0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0060 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0070 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0080 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0090 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00a0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00b0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00c0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00d0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00e0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00f0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0100 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0110 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0120 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0130 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0140 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0150 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Bytes 34-1513: Data (data.data)

Packets: 1738 - Displayed: 1738 (100.0%) - Dropped: 0 (0.0%)

Profile: Default

63°F Mostly cloudy 2:44 PM 5/14/2024