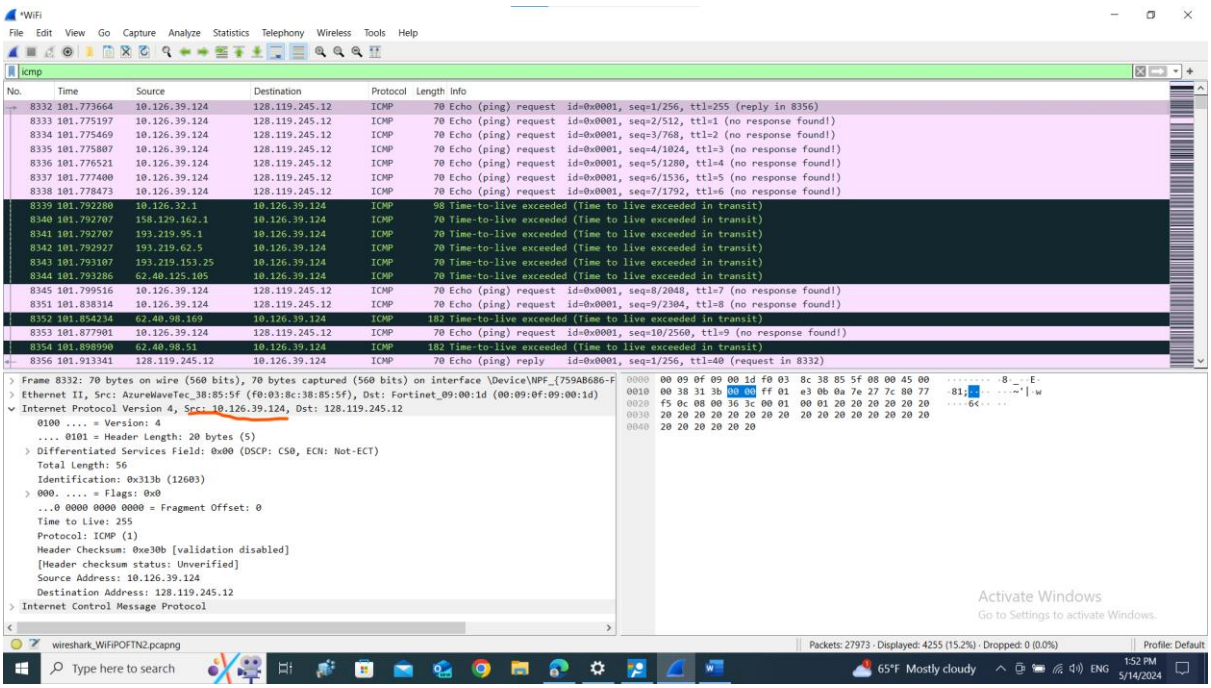
Lab Work 4 : IP

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.

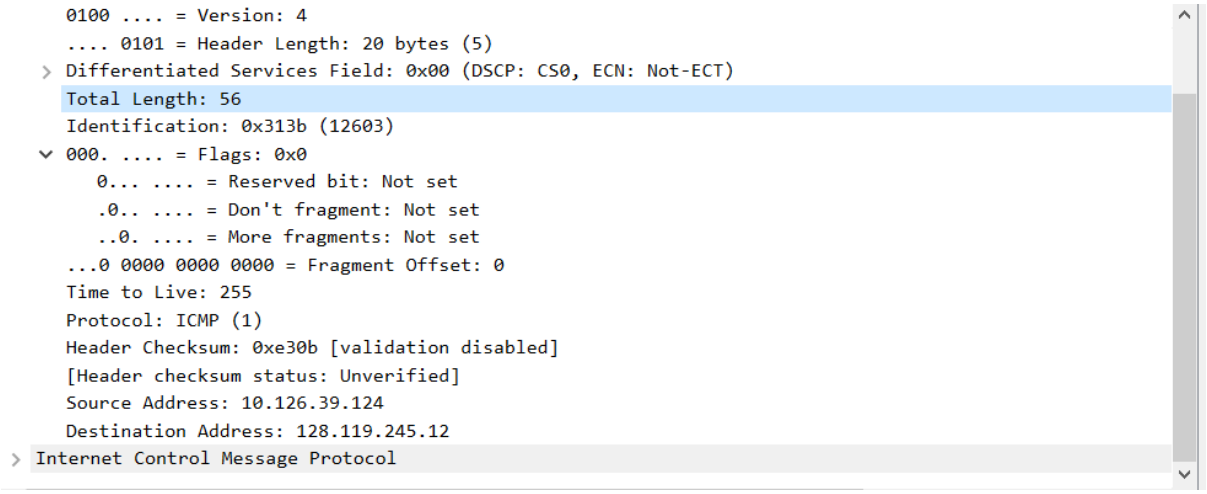
   Ans. Header length : 20;

   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.



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?

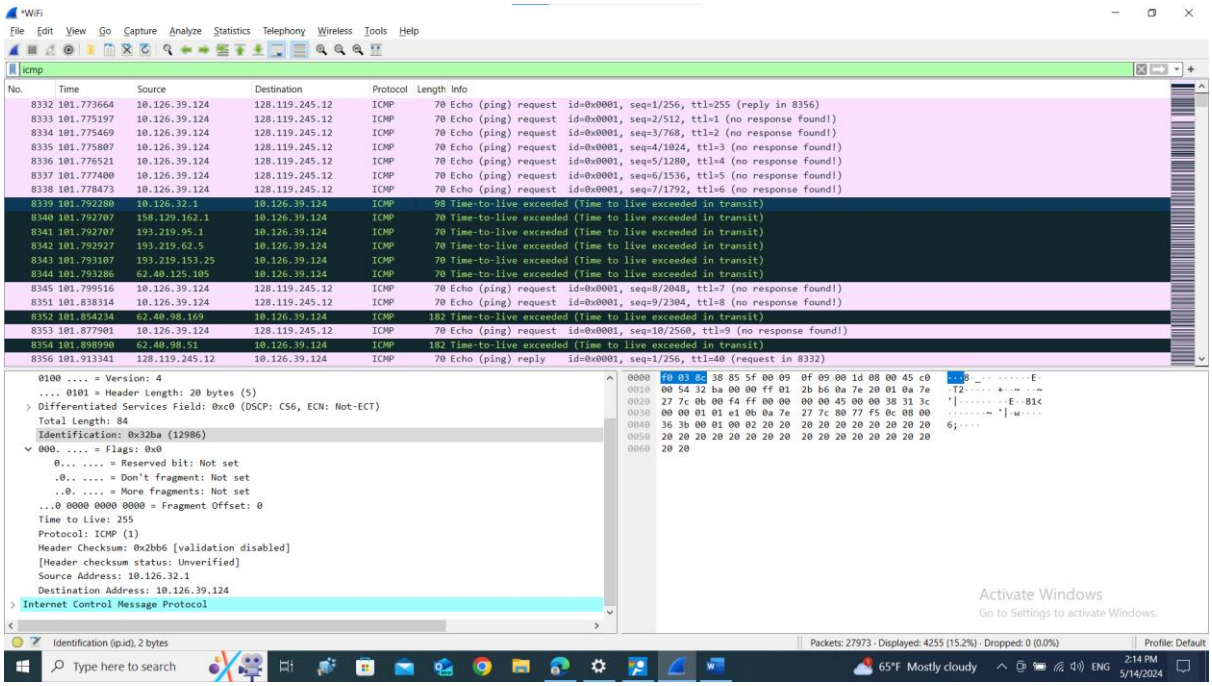
   Ans. Not change : i)version
   ii)header length
   iii)flag
   iv)fragmentation of set

   change : I) identification
   ii) header Checksum
   iii)Time to Live

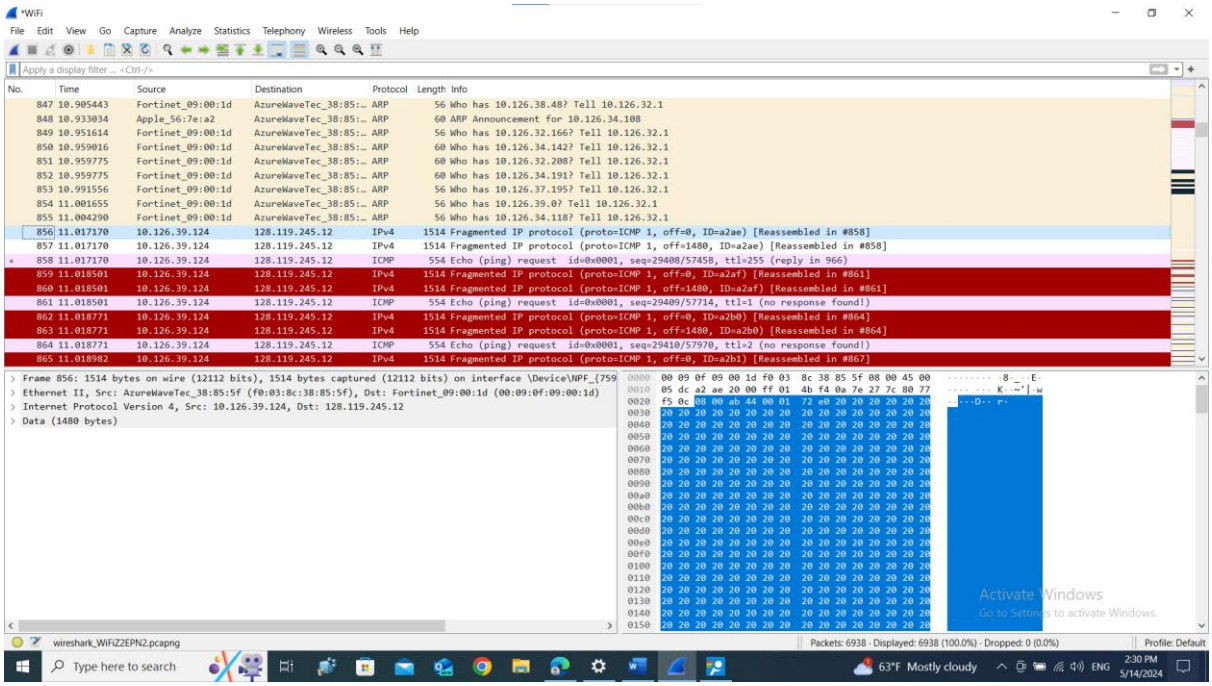
7. Describe the pattern you see in the values in the Identification field of the IP datagram?

   Ans. I can see a incrementing pattern.

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

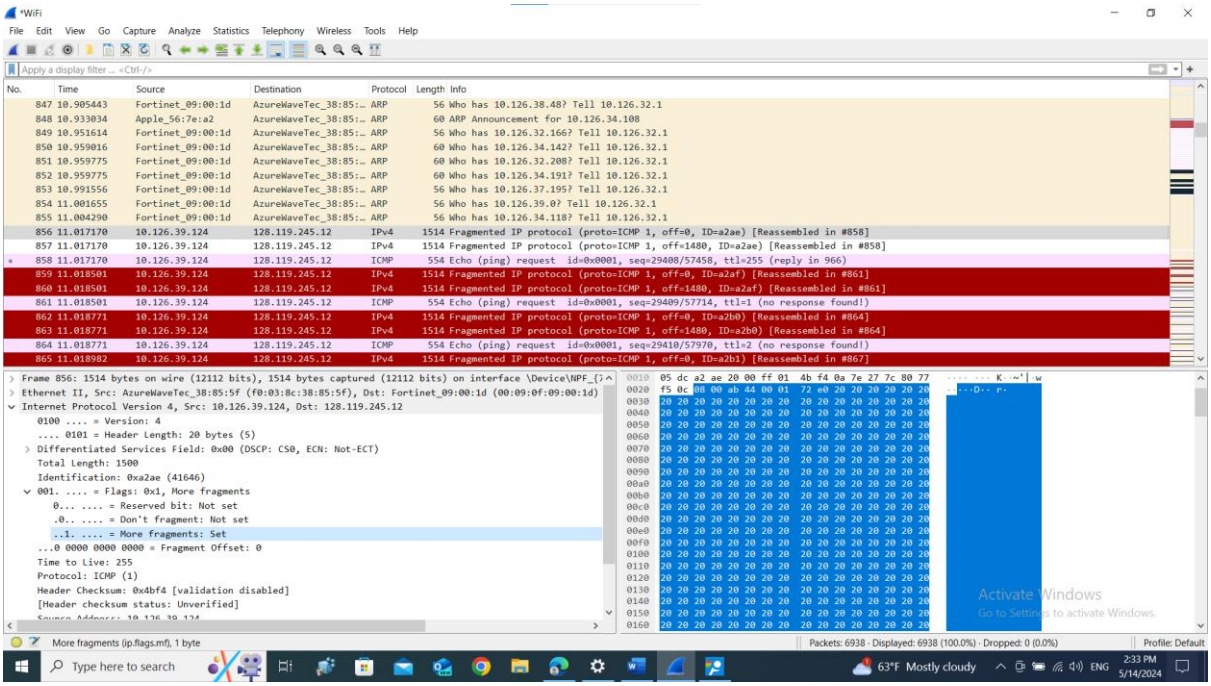


9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?
   Ans. Identification field is changing and TTL is decreasing
10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

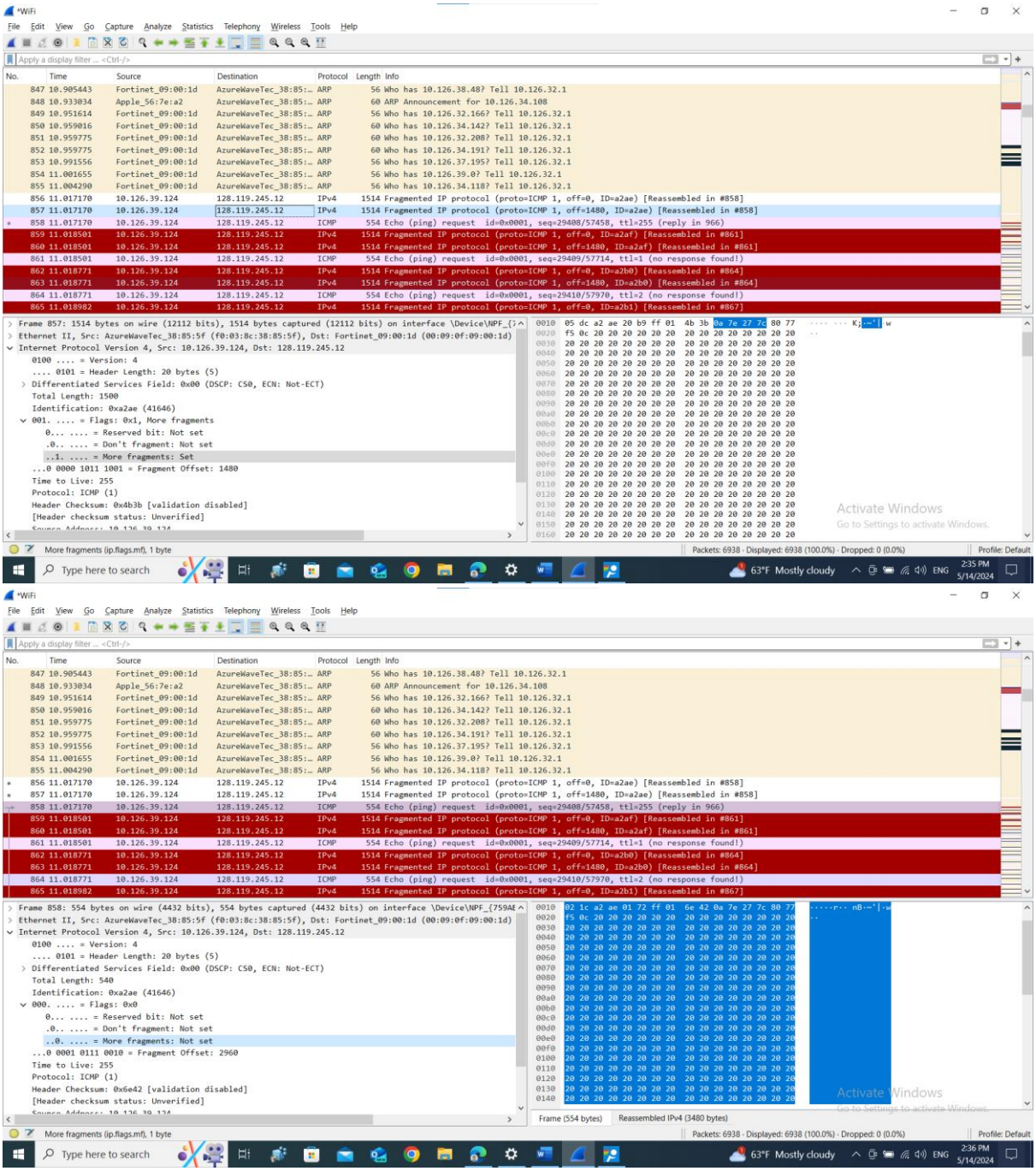


11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter

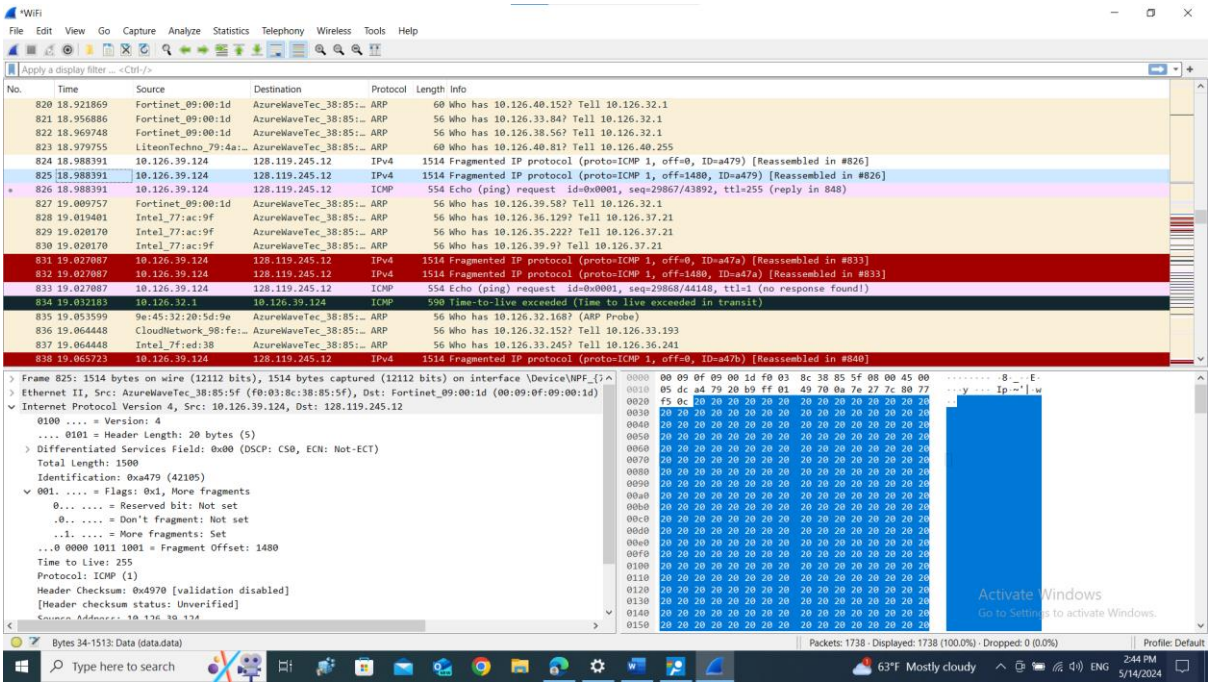
fragment? How long is this IP datagram?



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?



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-/>
No. Time Source Destination Protocol Length Info
820 18.921869 Fortinet_09:00:1d AzureWaveTec_38:85:... ARP 60 Who has 10.126.40.152? Tell 10.126.32.1
821 18.956886 Fortinet_09:00:1d AzureWaveTec_38:85:... ARP 56 Who has 10.126.33.84? Tell 10.126.32.1
822 18.969748 Fortinet_09:00:1d AzureWaveTec_38:85:... ARP 56 Who has 10.126.38.56? Tell 10.126.32.1
823 18.979755 LiteonTechno_79:4a:... AzureWaveTec_38:85:... 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:... ARP 56 Who has 10.126.39.58? Tell 10.126.32.1
828 19.019401 Intel_77:ac:9f AzureWaveTec_38:85:... ARP 56 Who has 10.126.36.129? Tell 10.126.37.21
829 19.020170 Intel_77:ac:9f AzureWaveTec_38:85:... ARP 56 Who has 10.126.35.222? Tell 10.126.37.21
830 19.020170 Intel_77:ac:9f AzureWaveTec_38:85:... 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 590 Time-to-live exceeded (Time to live exceeded in transit)
835 19.053599 9e:45:32:20:5d:9e AzureWaveTec_38:85:... ARP 56 Who has 10.126.32.168? (ARP Probe)
836 19.064448 CloudNetwork_98:fe:... AzureWaveTec_38:85:... ARP 56 Who has 10.126.32.152? Tell 10.126.33.193
837 19.064448 Intel_7f:ed:38 AzureWaveTec_38:85:... 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 (f0:03:8c: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)
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: 0x4970 [validation disabled]
[Header checksum status: Unverified]
0000 00 09 0f 09 00 1d f0 03 8c 38 85 5f 08 00 45 00
0010 05 dc a4 79 20 b9 ff 01 49 70 0a 7e 27 7c 80 77
0020 f5 0c 20 20 20 20 20 20 20 20 20 20 20 20 20 20
Activate Windows
Go to Settings to activate Windows.
Bytes 34-1513: Data (data.data)
Packets: 1738 · Displayed: 1738 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
63°F Mostly cloudy
ENG
2:44 PM
5/14/2024