

STUDENT NO.: SKSVPX001

3b)

The SYN flag is set to 1, indicating that it is a SYN segment.

The screenshot shows the Wireshark interface with a packet capture of a SYN segment. The packet list shows three packets: a SYN segment (Seq=0, Win=64240, Len=0, MSS=1460, SACK_PERM=1, TSval=706768507, TSecr=0, WS=128), a SYN-ACK segment (Seq=0, Ack=1, Win=14480, Len=0, MSS=1386, SACK_PERM=1, TSval=1000026074, TSecr=706768507), and a TCP Reset segment (RST=1, Seq=1, Win=0, Len=0, TSval=706768510, TSecr=1000026074). The packet details pane shows the structure of the SYN segment, including the source and destination ports, sequence number, and flags. The flags field shows the SYN flag set to 1.

Activities Wireshark Apr 1 03:50

tcptrace.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.130.33.149	128.119.245.12	TCP	74	57876 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=706768507 TSecr=0 WS=128
2	0.002222	128.119.245.12	10.130.33.149	TCP	74	80 → 57876 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1386 SACK_PERM=1 TSval=1000026074 TSecr=706768507
3	0.002242	10.130.33.149	128.119.245.12	TCP	66	57876 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=706768510 TSecr=1000026074

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Ethernet II, Src: IntelCor_4b:40:3d (0c:7a:15:4b:40:3d), Dst: Fortinet_c8:5b:d8 (e8:1c:ba:c8:5b:d8)

Internet Protocol Version 4, Src: 10.130.33.149, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 57876, Dst Port: 80, Seq: 0, Len: 0

Source Port: 57876

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 1789836220

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 0

Acknowledgment number (raw): 0

1010 ... = Header Length: 40 bytes (10)

Flags: 0x002 (SYN)

000. = Reserved: Not set

...0. = Nonce: Not set

...0. = Congestion Window Reduced (CWR): Not set

...0. = ECN-Echo: Not set

...0. = Urgent: Not set

...0. = Acknowledgment: Not set

...0. = Push: Not set

...0. = Reset: Not set

...1. = Syn: Set

...0. = Fin: Not set

[TCP Flags:S.]

Window: 64240

[Calculated window size: 64240]

Checksum: 0x8a09 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale

[Timestamps]

0000 e8 1c ba c8 5b d8 0c 7a 15 4b 40 3d 00 00 45 00 ...[...z...K@...E]

tcptrace.pcap Packets: 854 · Displayed: 854 (100.0%) Profile: Default

4b)

The SYN flag is set to 1 and Acknowledgment flag is set to 1, indicating that this segment is a SYNACK segment.

The screenshot shows the Wireshark interface with a packet capture of a SYNACK segment. The packet list shows three packets: a SYN segment (Seq=0, Win=64240, Len=0, MSS=1460, SACK_PERM=1, TSval=706768507, TSecr=0, WS=128), a SYN-ACK segment (Seq=0, Ack=1, Win=14480, Len=0, MSS=1386, SACK_PERM=1, TSval=1000026074, TSecr=706768507), and a TCP Reset segment (RST=1, Seq=1, Win=0, Len=0, TSval=706768510, TSecr=1000026074). The packet details pane shows the structure of the SYNACK segment, including the source and destination ports, sequence number, and flags. The flags field shows the SYN and ACK flags set to 1.

Activities Wireshark Apr 1 03:56

tcptrace.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.130.33.149	128.119.245.12	TCP	74	57876 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=706768507 TSecr=0 WS=128
2	0.002222	128.119.245.12	10.130.33.149	TCP	74	80 → 57876 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1386 SACK_PERM=1 TSval=1000026074 TSecr=706768507
3	0.002242	10.130.33.149	128.119.245.12	TCP	66	57876 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=706768510 TSecr=1000026074

Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Ethernet II, Src: Fortinet_c8:5b:d8 (e8:1c:ba:c8:5b:d8), Dst: IntelCor_4b:40:3d (0c:7a:15:4b:40:3d)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.130.33.149

Transmission Control Protocol, Src Port: 80, Dst Port: 57876, Seq: 0, Ack: 1, Len: 0

Source Port: 80

Destination Port: 57876

[Stream index: 0]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 2816422859

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 1789836221

1010 ... = Header Length: 40 bytes (10)

Flags: 0x012 (SYN, ACK)

000. = Reserved: Not set

...0. = Nonce: Not set

...0. = Congestion Window Reduced (CWR): Not set

...0. = ECN-Echo: Not set

...0. = Urgent: Not set

...1. = Acknowledgment: Set

...0. = Push: Not set

...0. = Reset: Not set

...1. = Syn: Set

...0. = Fin: Not set

[TCP Flags:A..S.]

Window: 14480

[Calculated window size: 14480]

Checksum: 0x8582 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale

[SEQ/ACK analysis]

[Timestamps]

0020 21 95 00 50 e2 14 a7 df 33 cb 6a ae bb bd a0 12 !...P....3...]

Acknowledgment (tcp.flags.ack), 1 byte Packets: 854 · Displayed: 854 (100.0%) Profile: Default

4d)

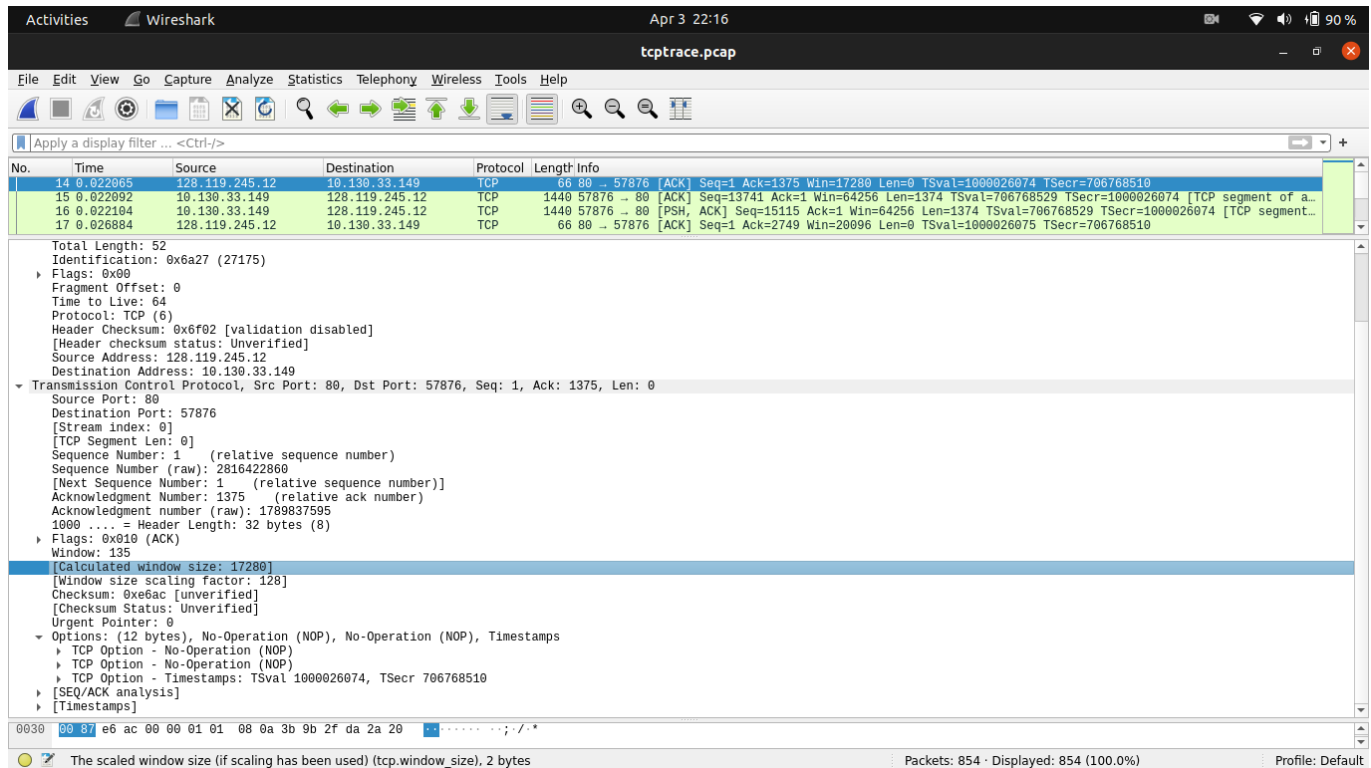
By adding 1 to the initial sequence number of SYN segment from the client computer (the sequence number of the SYN segment initiated by the client computer is 1789836220)

$$1789836220 + 1 = 1789836221$$

8b)

No, the receiver window increases in size from 14480 to 17280 in the next TCP segment sent from gaia.cs.umass.edu to client after the first four data carrying TCP segments advertising amount buffer space, in frame 14.

The sender not is throttled.



9)

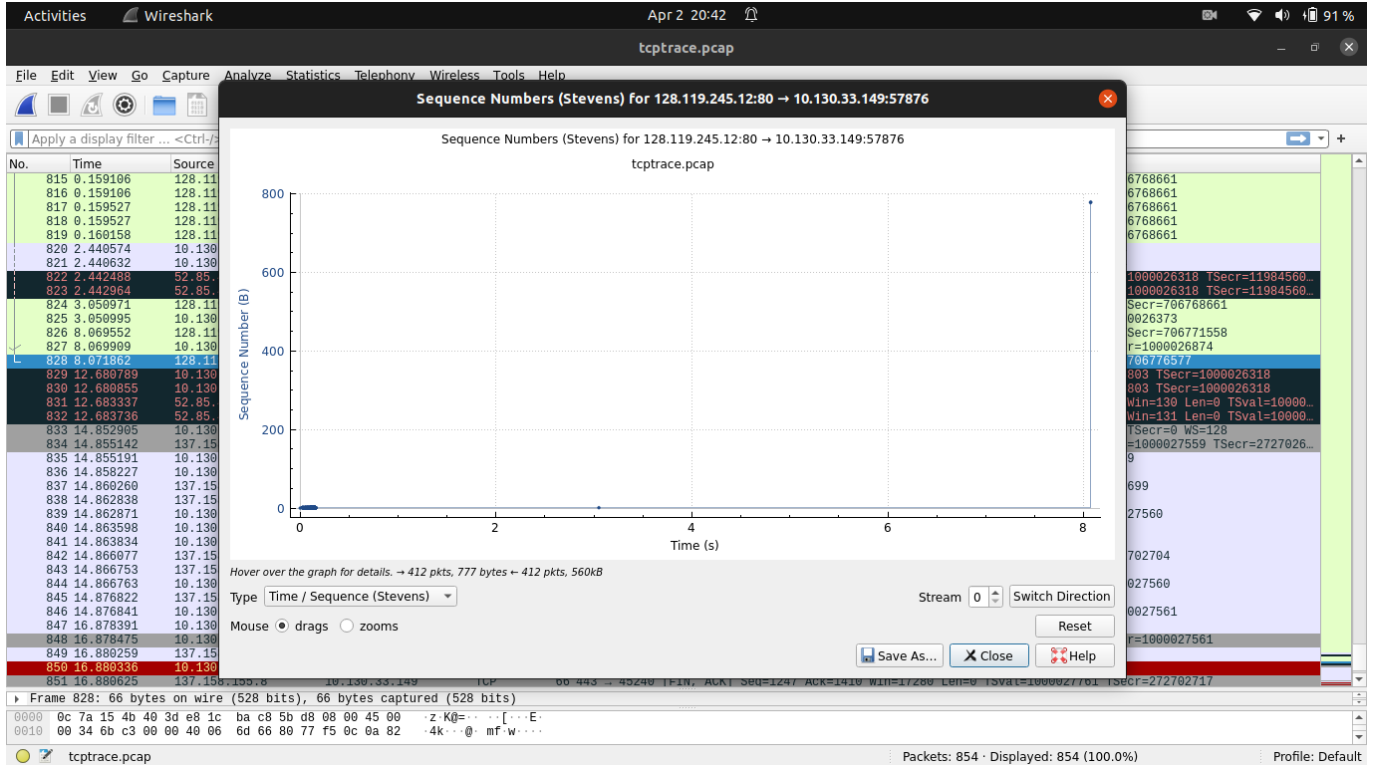
No, there is no retransmitted segments.

All sequence numbers are increasing in the time sequence graph (Stevens).

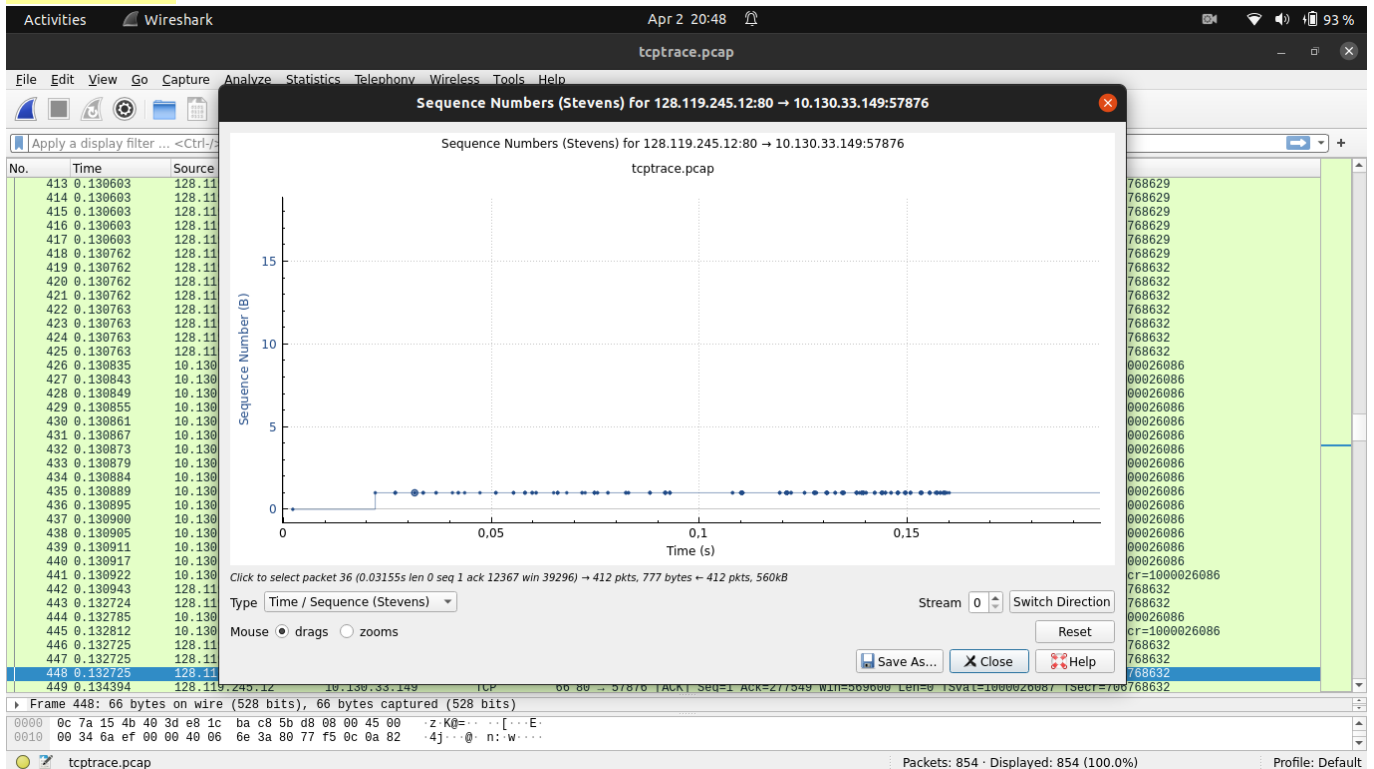
Each dot represents a TCP segment sent, plotting the sequence number of the segment versus the time at which it was sent. A set of dots stacked above each other represents a series of packets that were sent back-to-back by the sender.

As time progresses sequence numbers increase, being larger than those of its previous segments.

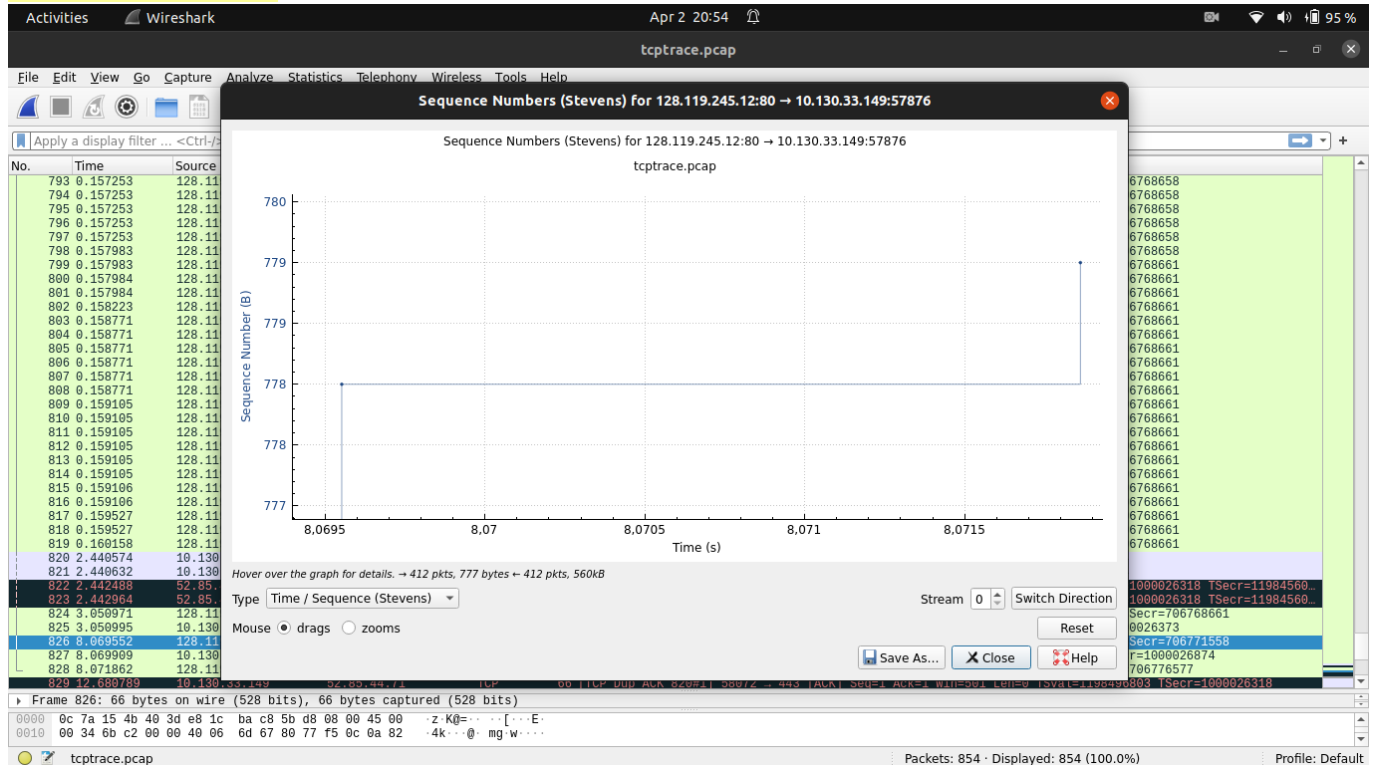
The entire graph



From 0s to 0.16s (ZOOMED IN)



From 8.0695s to 8.07185s (ZOOMED IN)



15

The more fragments bit flag is set to zero, meaning the IP datagram is not fragmented.

16

- Identification
- Header checksum
- Time to live

17

- Version, because we are using IPv4 for all packets
- Source IP, because all UDP segments are sent from the same client.
- Header length, because they are UDP segments.
- Destination IP, because all UDP segments are sent to the same destination.
- Differentiated Services, because all segments are of UDP protocol, they use the same Type of Service class.
- Protocol, because all segments are of UDP.

18

The IP header Identification field increments with each UDP segment.

19

Internet Control Message Protocol (ICMP), with value 1.

20

No,

21

No, they are different.

Examples a (random)

Activities Wireshark Apr 3 16:49

iptrace.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 10.130.33.149 and icmp

No.	Time	Source	Destination	Protocol	Length	Info
40	0.277945	154.66.247.148	10.130.33.149	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
41	0.278629	154.66.247.148	10.130.33.149	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
68	1.609230	154.66.247.148	10.130.33.149	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
69	1.609979	154.66.247.71	10.130.33.149	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
70	1.610369	154.66.247.71	10.130.33.149	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
71	1.610369	154.66.247.71	10.130.33.149	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
72	1.610369	193.251.141.13	10.130.33.149	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
73	1.610369	193.251.141.13	10.130.33.149	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
74	1.610370	193.251.141.13	10.130.33.149	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
77	1.618926	193.251.151.35	10.130.33.149	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
78	1.619287	193.251.151.35	10.130.33.149	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
79	1.620100	193.251.151.35	10.130.33.149	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
80	1.620921	193.251.249.40	10.130.33.149	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)

Frame 71: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
 Ethernet II, Src: Fortinet_c8:5b:d8 (e8:1c:ba:c8:5b:d8), Dst: IntelCor_4b:40:3d (0c:7a:15:4b:40:3d)
 Internet Protocol Version 4, Src: 154.66.247.71, Dst: 10.130.33.149
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 56
 Identification: 0x0000 (0)
 Flags: 0x00
 Fragment Offset: 0
 Time to Live: 249
 Protocol: ICMP (1)
 Header Checksum: 0x0424 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 154.66.247.71
 Destination Address: 10.130.33.149
 Internet Control Message Protocol

0010 00 38 00 00 00 00 00 01 04 24 9a 42 f7 47 0a 82 ..8... ..\$B 6..

Time to Live (ip.ttl), 1 byte

Packets: 490 · Displayed: 121 (24.7%) Profile: Default

Example b (random)

Activities Wireshark Apr 3 16:50

iptrace.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 10.130.33.149 and icmp

No.	Time	Source	Destination	Protocol	Length	Info
118	3.453127	96.110.42.14	10.130.33.149	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
119	3.453127	96.110.42.14	10.130.33.149	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
120	3.453127	162.151.53.214	10.130.33.149	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
121	3.453127	162.151.53.214	10.130.33.149	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
122	3.453128	162.151.53.214	10.130.33.149	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
123	3.453128	50.222.38.42	10.130.33.149	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
124	3.453128	50.222.38.42	10.130.33.149	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
125	3.453128	50.222.38.42	10.130.33.149	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
126	3.453224	96.108.44.226	10.130.33.149	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
127	3.453224	96.108.44.226	10.130.33.149	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
128	3.453225	96.108.44.226	10.130.33.149	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
129	3.453225	192.80.83.113	10.130.33.149	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
130	3.453225	192.80.83.113	10.130.33.149	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
131	3.453227	192.80.83.113	10.130.33.149	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 128: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
 Ethernet II, Src: Fortinet_c8:5b:d8 (e8:1c:ba:c8:5b:d8), Dst: IntelCor_4b:40:3d (0c:7a:15:4b:40:3d)
 Internet Protocol Version 4, Src: 96.108.44.226, Dst: 10.130.33.149
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 96
 Identification: 0xf958 (63832)
 Flags: 0x00
 Fragment Offset: 0
 Time to Live: 242
 Protocol: ICMP (1)
 Header Checksum: 015df [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 96.108.44.226
 Destination Address: 10.130.33.149
 Internet Control Message Protocol
 Data (28 bytes)

0010 00 60 f9 58 00 00 00 01 15 df 60 6c 2c e2 0a 82 ...X... ..l...

Time to Live (ip.ttl), 1 byte

Packets: 490 · Displayed: 121 (24.7%) Profile: Default