Matthew Krueger – Communication Networks Lab 2

PART A: First Look at the Captured Trace

1.

IP:

Source: 192.168.0.138

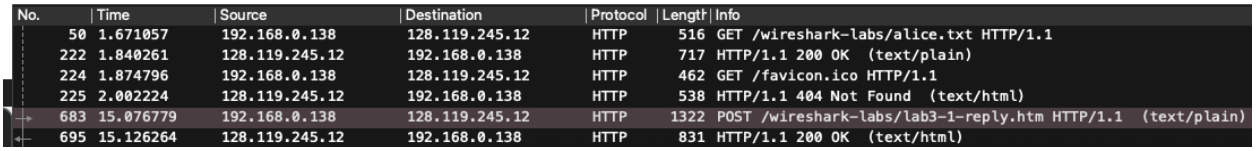
Dest: 128.119.245.12

Port:

Source: 49402

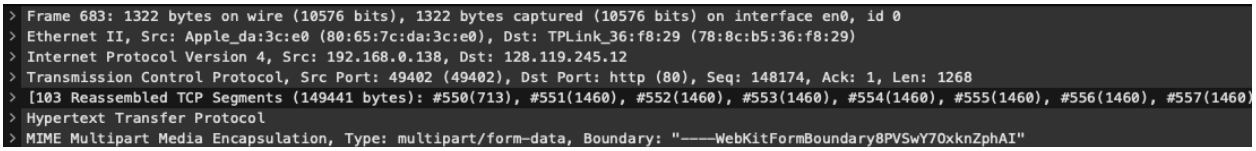
Dest: 80

Picture reference:



No.	Time	Source	Destination	Protocol	Length	Info
50	1.671057	192.168.0.138	128.119.245.12	HTTP	516	GET /wireshark-labs/alice.txt HTTP/1.1
222	1.840261	128.119.245.12	192.168.0.138	HTTP	717	HTTP/1.1 200 OK (text/plain)
224	1.874796	192.168.0.138	128.119.245.12	HTTP	462	GET /favicon.ico HTTP/1.1
225	2.002224	128.119.245.12	192.168.0.138	HTTP	538	HTTP/1.1 404 Not Found (text/html)
683	15.076779	192.168.0.138	128.119.245.12	HTTP	1322	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
695	15.126264	128.119.245.12	192.168.0.138	HTTP	831	HTTP/1.1 200 OK (text/html)

Clicked into:



```
> Frame 683: 1322 bytes on wire (10576 bits), 1322 bytes captured (10576 bits) on interface en0, id 0
> Ethernet II, Src: Apple_da:3c:e0 (80:65:7c:da:3c:e0), Dst: TPLink_36:f8:29 (78:8c:b5:36:f8:29)
> Internet Protocol Version 4, Src: 192.168.0.138, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49402 (49402), Dst Port: http (80), Seq: 148174, Ack: 1, Len: 1268
> [103 Reassembled TCP Segments (149441 bytes): #550(713), #551(1460), #552(1460), #553(1460), #554(1460), #555(1460), #556(1460), #557(1460)
> Hypertext Transfer Protocol
> MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundary8PVSwY7OxknZphAI"
```

2.

Gaia.cs.umass.edu:

IP:

Source: 128.119.245.12

Port:

Sending: 80

Receiving: 80

Server uses same port to send and receive data (port #80)

TCP Basics

3.

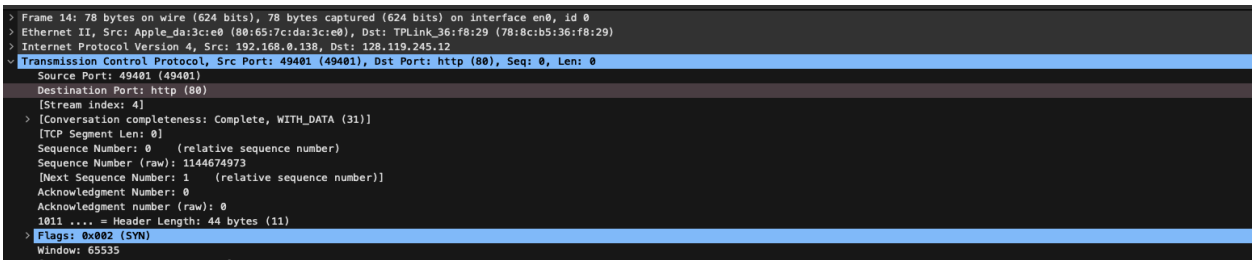
Raw Sequence number:

SYN: 1144674973

Inside of the segment, the SYN flag identifies segment as SYN (see blue selected ‘Flags’)

Picture Reference:

Clicked into:



4.

Raw Sequence Number:

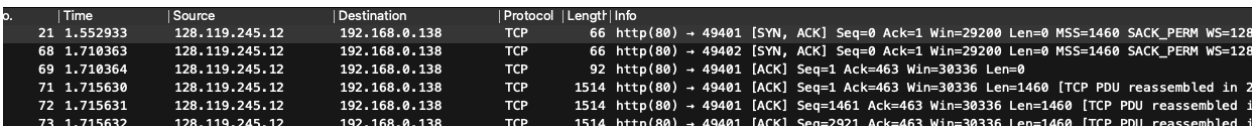
SYN/ACK: 1378621287

Acknowledgement field:

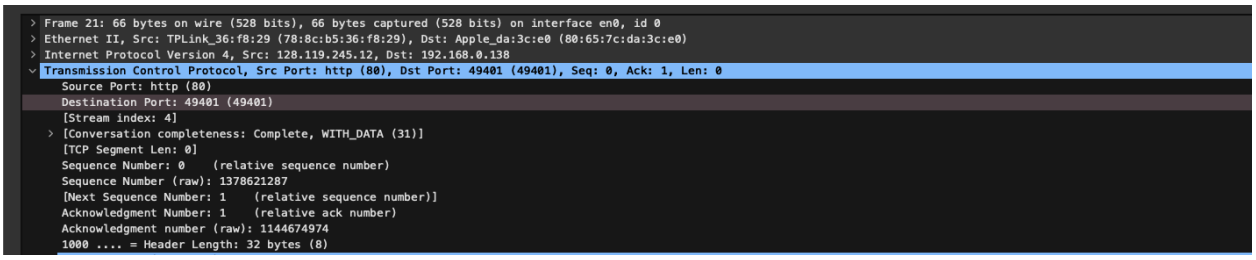
1 (relative ack number)

Inside of the segment, the SYN & ACK flags identify segment as SYN/ACK (see blue selected ‘Flags’)

Picture Reference:



Clicked into:



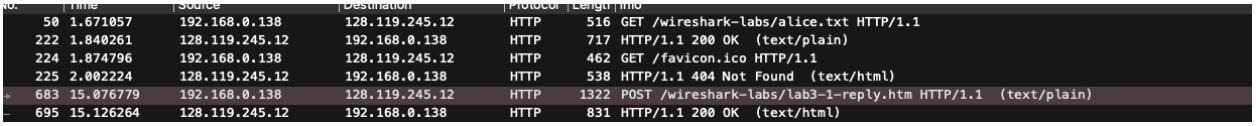
5.

Sequence Numbers:

Raw: 53641098

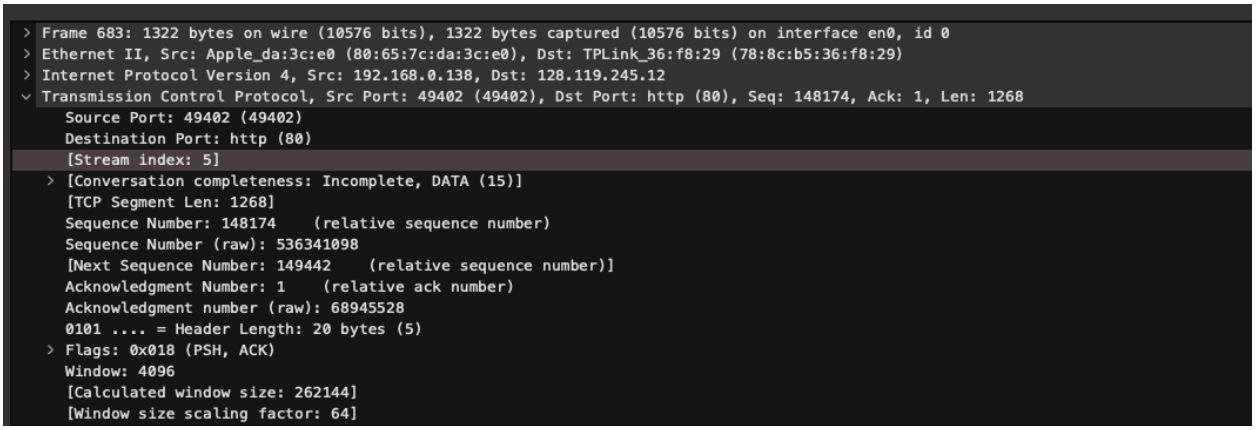
Relative: 148174

Picture Reference:



No.	Time	Source	Destination	Protocol	Length	Info
50	1.671057	192.168.0.138	128.119.245.12	HTTP	516	GET /wireshark-labs/alice.txt HTTP/1.1
222	1.840261	128.119.245.12	192.168.0.138	HTTP	717	HTTP/1.1 200 OK (text/plain)
224	1.874796	192.168.0.138	128.119.245.12	HTTP	462	GET /favicon.ico HTTP/1.1
225	2.002224	128.119.245.12	192.168.0.138	HTTP	538	HTTP/1.1 404 Not Found (text/html)
683	15.076779	192.168.0.138	128.119.245.12	HTTP	1322	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
695	15.126264	128.119.245.12	192.168.0.138	HTTP	831	HTTP/1.1 200 OK (text/html)

Clicked into:



```
> Frame 683: 1322 bytes on wire (10576 bits), 1322 bytes captured (10576 bits) on interface en0, id 0
> Ethernet II, Src: Apple_da:3c:e0 (80:65:7c:da:3c:e0), Dst: TPLink_36:f8:29 (78:8c:b5:36:f8:29)
> Internet Protocol Version 4, Src: 192.168.0.138, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 49402 (49402), Dst Port: http (80), Seq: 148174, Ack: 1, Len: 1268
    Source Port: 49402 (49402)
    Destination Port: http (80)
    [Stream index: 5]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 1268]
    Sequence Number: 148174    (relative sequence number)
    Sequence Number (raw): 536341098
    [Next Sequence Number: 149442    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 68945528
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 4096
    [Calculated window size: 262144]
    [Window size scaling factor: 64]
```

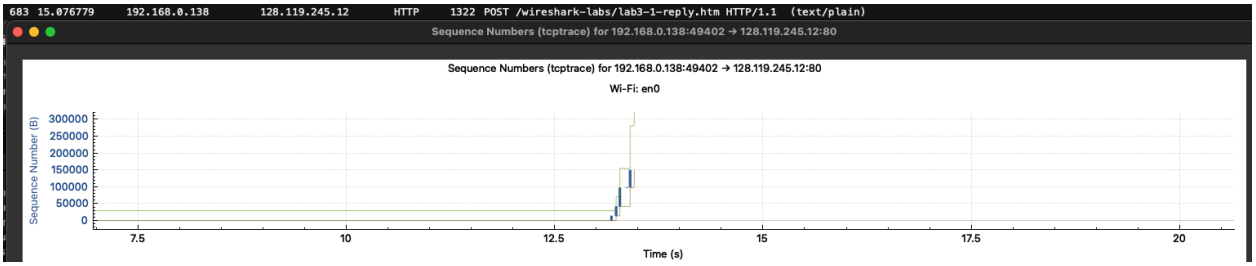
6.

Based off my graph, I would assume no retransmissions during my POST request.

Inside of my trace, I looked for anything suggesting that there was an error or retransmission in the process of POSTING data.

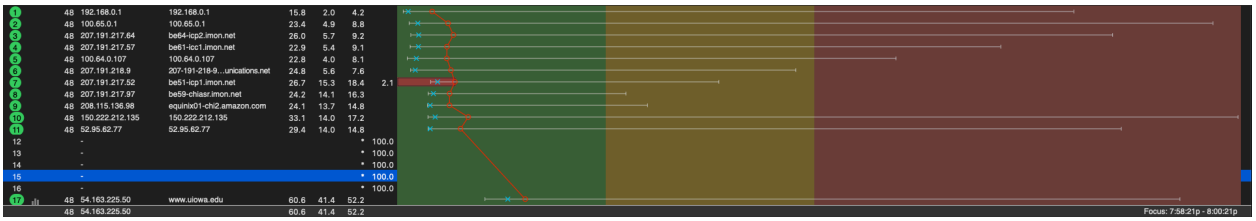
As this is the only POST message in my trace & the shape of my graph is as expected, I believe there is no retransmission… on my machine at least…

Graph Reference: POST to gaia.umass

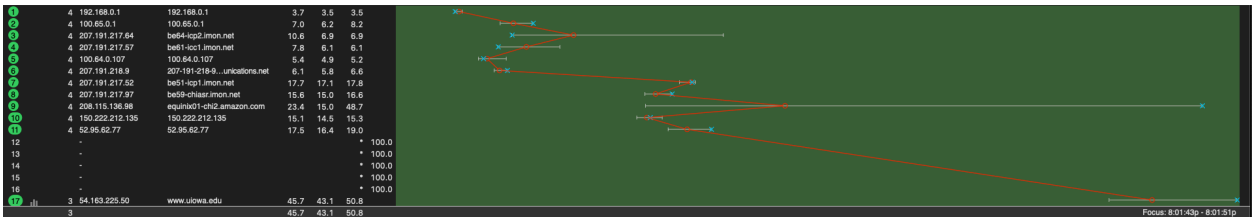


PART B: Using Wireshark to Investigate IP Behavior

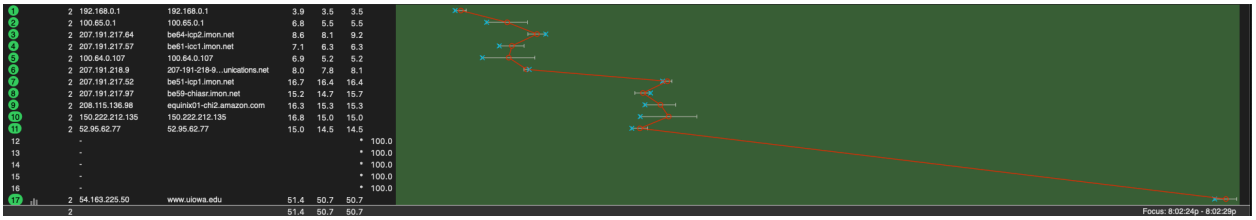
56 packet size (www.uiowa.edu)



2000 packet size (www.uiowa.edu)

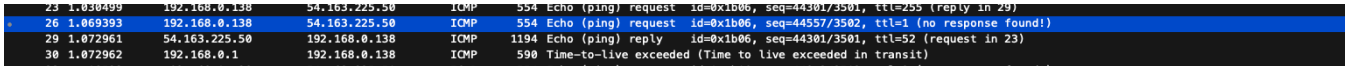


3500 packet size (www.uiowa.edu)



1.

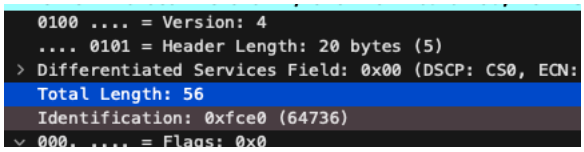
Picture Reference: First message



Upper Layer Protocol Field: ICMP (1)

2.

Picture Reference: Length of packet



Bytes:

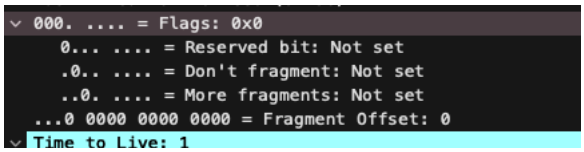
IP Datagram Header: 20 bytes

IP Datagram Payload: Total Length – Header = 36 bytes

(20 + 36 == 56 (as expected))

3.

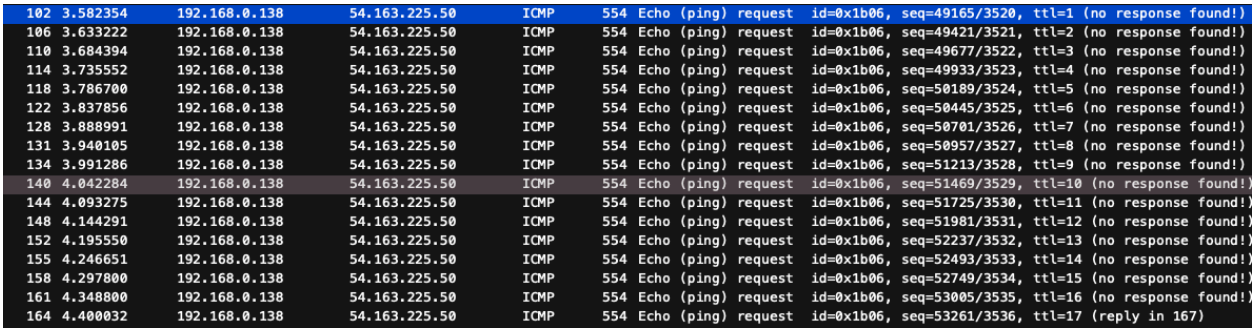
Picture Reference: Fragments (none as 56 is small enough to be unfragmented)



No, the IP Datagram IS NOT fragmented. This is indicated by the 'Flags' set to 0. Refer to picture

**** the sorting of 'Source' column is very vague, and it does not say which direction it should be sorted. I have answered the following using the sorting arrow pointing up ****

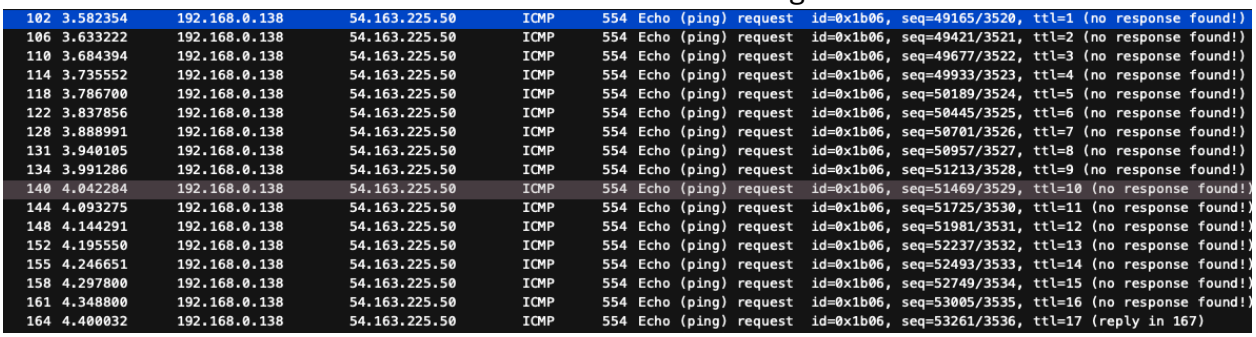
Picture Reference: top of sorted list.



102	3.582354	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=49165/3520, ttl=1 (no response found!)
106	3.633222	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=49421/3521, ttl=2 (no response found!)
110	3.684394	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=49677/3522, ttl=3 (no response found!)
114	3.735552	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=49933/3523, ttl=4 (no response found!)
118	3.786700	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=50189/3524, ttl=5 (no response found!)
122	3.837856	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=50445/3525, ttl=6 (no response found!)
128	3.888991	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=50701/3526, ttl=7 (no response found!)
131	3.940105	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=50957/3527, ttl=8 (no response found!)
134	3.991286	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=51213/3528, ttl=9 (no response found!)
140	4.042284	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=51469/3529, ttl=10 (no response found!)
144	4.093275	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=51725/3530, ttl=11 (no response found!)
148	4.144291	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=51981/3531, ttl=12 (no response found!)
152	4.195550	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=52237/3532, ttl=13 (no response found!)
155	4.246651	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=52493/3533, ttl=14 (no response found!)
158	4.297800	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=52749/3534, ttl=15 (no response found!)
161	4.348800	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=53005/3535, ttl=16 (no response found!)
164	4.400032	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=53261/3536, ttl=17 (reply in 167)

4.

Picture Reference for 4: these are the ICMP series I investigated.



102	3.582354	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=49165/3520, ttl=1 (no response found!)
106	3.633222	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=49421/3521, ttl=2 (no response found!)
110	3.684394	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=49677/3522, ttl=3 (no response found!)
114	3.735552	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=49933/3523, ttl=4 (no response found!)
118	3.786700	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=50189/3524, ttl=5 (no response found!)
122	3.837856	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=50445/3525, ttl=6 (no response found!)
128	3.888991	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=50701/3526, ttl=7 (no response found!)
131	3.940105	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=50957/3527, ttl=8 (no response found!)
134	3.991286	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=51213/3528, ttl=9 (no response found!)
140	4.042284	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=51469/3529, ttl=10 (no response found!)
144	4.093275	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=51725/3530, ttl=11 (no response found!)
148	4.144291	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=51981/3531, ttl=12 (no response found!)
152	4.195550	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=52237/3532, ttl=13 (no response found!)
155	4.246651	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=52493/3533, ttl=14 (no response found!)
158	4.297800	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=52749/3534, ttl=15 (no response found!)
161	4.348800	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=53005/3535, ttl=16 (no response found!)
164	4.400032	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request	id=0x1b06, seq=53261/3536, ttl=17 (reply in 167)

Constant Fields:

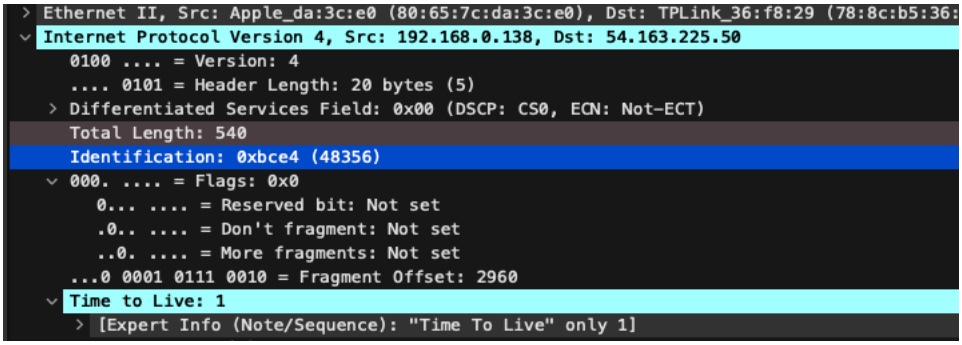
- Src & Dest IP – same src/dest
- Length of datagram – same data sent

Variable Fields:

- Checksum – different packets
- Identification – different packets
- TTL – traceroute shows TTL incrementing by 1

5.

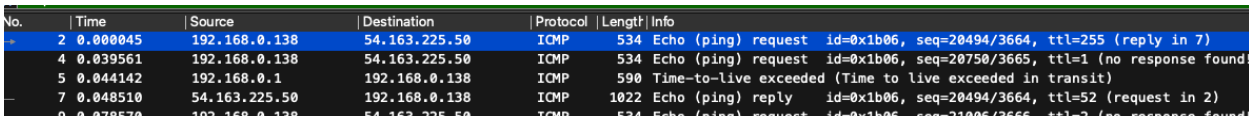
Picture reference:



Identification: 0xbce4 (**48356**)

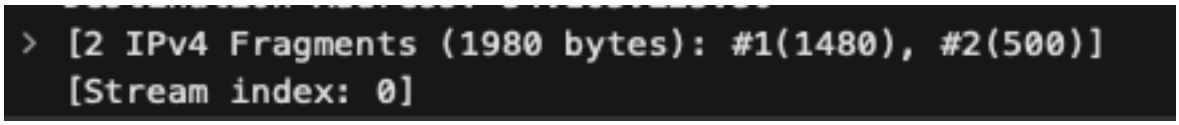
6.

a) Picture Reference: First 'Echo' request message



No.	Time	Source	Destination	Protocol	Length	Info
2	0.000045	192.168.0.138	54.163.225.50	ICMP	534	Echo (ping) request id=0x1b06, seq=20494/3664, ttl=255 (reply in 7)
4	0.039561	192.168.0.138	54.163.225.50	ICMP	534	Echo (ping) request id=0x1b06, seq=20750/3665, ttl=1 (no response found!
5	0.044142	192.168.0.1	192.168.0.138	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
7	0.048510	54.163.225.50	192.168.0.138	ICMP	1022	Echo (ping) reply id=0x1b06, seq=20494/3664, ttl=52 (request in 2)

b) Picture Reference: Yes, the message has been fragmented



2 fragments:

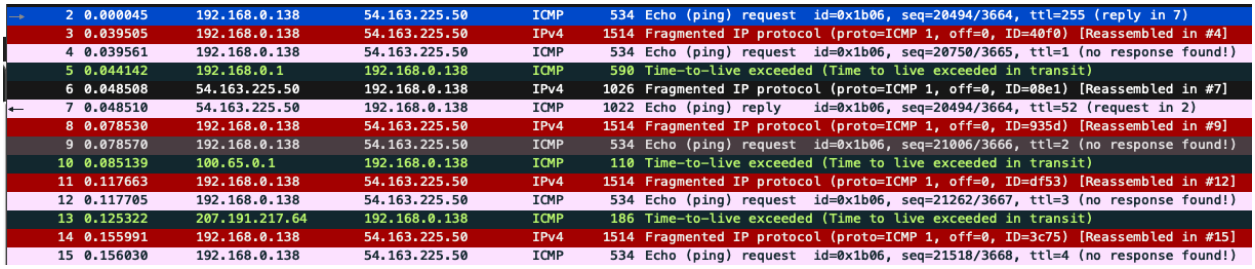
1st: 1480 bytes

2nd: 500 bytes

Note header still 20, so 1480 + 500 + 20 = 2000 (total packet length as expected)

7.

Picture Reference: Fragments (multiple as ttl expired)



→	2	0.000045	192.168.0.138	54.163.225.50	ICMP	534 Echo (ping) request id=0x1b06, seq=20494/3664, ttl=255 (reply in 7)
	3	0.039505	192.168.0.138	54.163.225.50	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=40f0) [Reassembled in #4]
	4	0.039561	192.168.0.138	54.163.225.50	ICMP	534 Echo (ping) request id=0x1b06, seq=20750/3665, ttl=1 (no response found!)
	5	0.044142	192.168.0.1	192.168.0.138	ICMP	590 Time-to-live exceeded (Time to live exceeded in transit)
	6	0.048508	54.163.225.50	192.168.0.138	IPv4	1026 Fragmented IP protocol (proto=ICMP 1, off=0, ID=08e1) [Reassembled in #7]
←	7	0.048510	54.163.225.50	192.168.0.138	ICMP	1022 Echo (ping) reply id=0x1b06, seq=20494/3664, ttl=52 (request in 2)
	8	0.078530	192.168.0.138	54.163.225.50	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=935d) [Reassembled in #9]
	9	0.078570	192.168.0.138	54.163.225.50	ICMP	534 Echo (ping) request id=0x1b06, seq=21006/3666, ttl=2 (no response found!)
	10	0.085139	100.65.0.1	192.168.0.138	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
	11	0.117663	192.168.0.138	54.163.225.50	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=df53) [Reassembled in #12]
	12	0.117705	192.168.0.138	54.163.225.50	ICMP	534 Echo (ping) request id=0x1b06, seq=21262/3667, ttl=3 (no response found!)
	13	0.125322	207.191.217.64	192.168.0.138	ICMP	186 Time-to-live exceeded (Time to live exceeded in transit)
	14	0.155991	192.168.0.138	54.163.225.50	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3c75) [Reassembled in #15]
	15	0.156030	192.168.0.138	54.163.225.50	ICMP	534 Echo (ping) request id=0x1b06, seq=21518/3668, ttl=4 (no response found!)

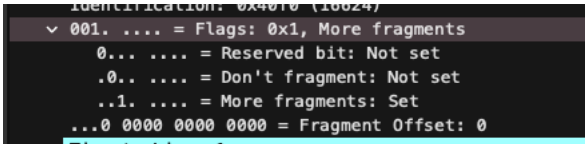
Indication of first fragmentation inside of IP Datagram Header:

Flags:

'More fragments': set to 1, meaning yes fragmented, with additonal fragments awaiting.

'Fragment Offset': set to 0, meaning first fragment.

Picture Reference:



8.

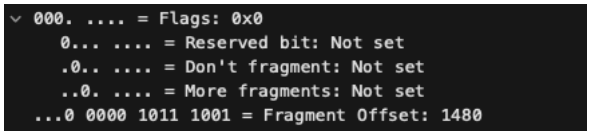
Indication of fragmented datagram not first fragmentation inside of IP Datagram Header:

Flags:

‘More fragments’: set to 0, meaning it is the last of total datagram.

‘Fragment Offset’: NOT 0, meaning not the first fragment.

Picture Reference:



9.

Constant Fields:

Src & Dest IP – same src/dest

TTL – included in same total datagram (to be rebuilt)

Fragment Version - IPv4

Protocol – Fragmented IP Protocol; ICMP 1

Variable Fields:

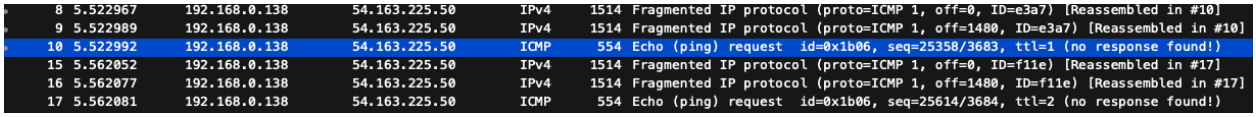
Checksum – different fragment

Identification – different fragment

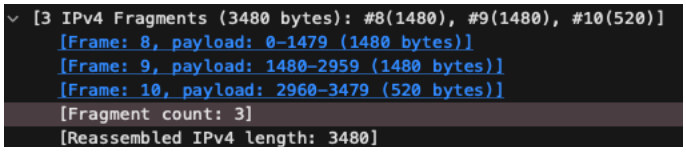
Length of fragment – different fragment (1480 vs 500)

10.

Picture Reference: first message



Picture Reference: Fragments



The datagram is split into 3 fragments

1st: 1480

2nd: 1480

3rd: 520

Header is 20, so 1480 + 1480 + 520 + 20 == 3500 (as expected)

11.

Constant Fields:

Src & Dest IP – same src/dest

TTL – included in same total datagram (to be rebuilt)

Fragment Version - IPv4

Protocol – Fragmented IP Protocol; ICMP 1

Variable Fields:

Checksum – different fragment

Identification – different fragment

Length of fragment – different fragment (1480 vs 520) HOWEVER FIRST 2 ARE EQUAL