

# 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: "-----WebKitFormBoundary8PVSwY70xknZphAI"
```

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:

13	1.514139	192.168.0.138	172.217.0.164	TCP	66	49385 → https(443) [FIN, ACK] Seq=1 Ack=1 Win=2048 Len=0 TSval=3464030398 TSecr=1730716376
14	1.514326	192.168.0.138	128.119.245.12	TCP	78	49401 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2812997685 TSecr=0 SACK_PERM
16	1.532664	192.168.0.138	142.250.191.163	TCP	66	49331 → https(443) [ACK] Seq=2 Ack=2 Win=2048 Len=0 TSval=3323321977 TSecr=2767662569

Clicked into:

>	Frame 14: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en0, id 0
>	Ethernet II, Src: Apple_dai3cie0 (08:65:7c: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: 49401 (49401), Dst Port: http (80), Seq: 0, Len: 0
	Source Port: 49401 (49401)
	Destination Port: http (80)
	[Stream index: 4]
>	[Conversation completeness: Complete, WITH_DATA (31)]
>	[TCP Segment Len: 0]
	Sequence Number: 0 (relative sequence number)
	Sequence Number (raw): 1144674973
	[Next Sequence Number: 1 (relative sequence number)]
	Acknowledgment Number: 0
	Acknowledgment number (raw): 0
	1011 .... = Header Length: 44 bytes (11)
>	Flags: 0x002 (SYN)
	Window: 65535

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:

No.	Time	Source	Destination	Protocol	Length	Info
21	1.552933	128.119.245.12	192.168.0.138	TCP	66	http(80) → 49401 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
68	1.710363	128.119.245.12	192.168.0.138	TCP	66	http(80) → 49402 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
69	1.710364	128.119.245.12	192.168.0.138	TCP	92	http(80) → 49401 [ACK] Seq=1 Ack=463 Win=30336 Len=0
71	1.715630	128.119.245.12	192.168.0.138	TCP	1514	http(80) → 49401 [ACK] Seq=1 Ack=463 Win=30336 Len=1460 [TCP PDU reassembled in 2]
72	1.715631	128.119.245.12	192.168.0.138	TCP	1514	http(80) → 49401 [ACK] Seq=1461 Ack=463 Win=30336 Len=1460 [TCP PDU reassembled in 2]
73	1.715632	128.119.245.12	192.168.0.138	TCP	1514	http(80) → 49401 [ACK] Seq=2921 Ack=463 Win=30336 Len=1460 [TCP PDU reassembled in 2]

Clicked into:

>	Frame 21: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
>	Ethernet II, Src: TPLink_36:f8:29 (78:8c:b5:36:f8:29), Dst: Apple_dai3cie0 (08:65:7c:da:3c:e0)
>	Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.138
>	Transmission Control Protocol, Src Port: http (80), Dst Port: 49401 (49401), Seq: 0, Ack: 1, Len: 0
	Source Port: http (80)
	Destination Port: 49401 (49401)
	[Stream index: 4]
>	[Conversation completeness: Complete, WITH_DATA (31)]
>	[TCP Segment Len: 0]
	Sequence Number: 0 (relative sequence number)
	Sequence Number (raw): 1378621287
	[Next Sequence Number: 1 (relative sequence number)]
	Acknowledgment Number: 1 (relative ack number)
	Acknowledgment number (raw): 1144674974
	1000 .... = Header Length: 32 bytes (8)

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
> 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]
```

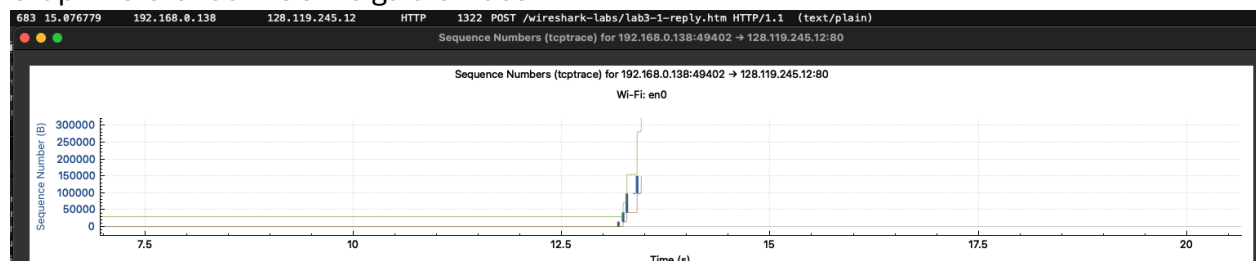
6.

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.

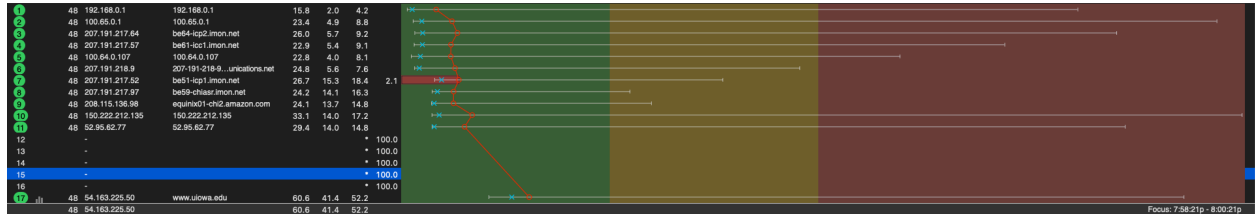
As this is the only POST message in my trace & the shape of my graph is as expected, I believe there is no retransmission... on my machine at least...

Graph Reference: POST to gaia.umass

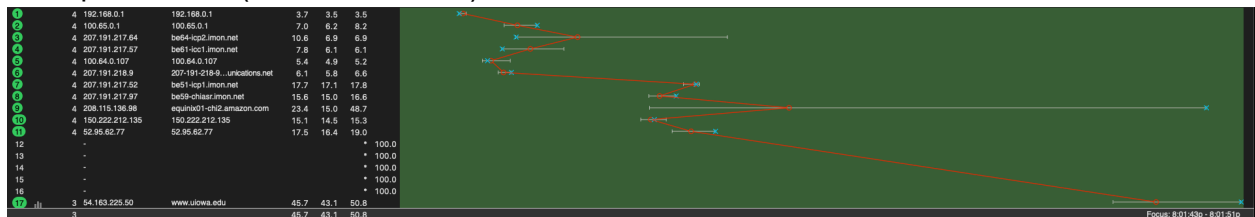


## PART B: Using Wireshark to Investigate IP Behavior

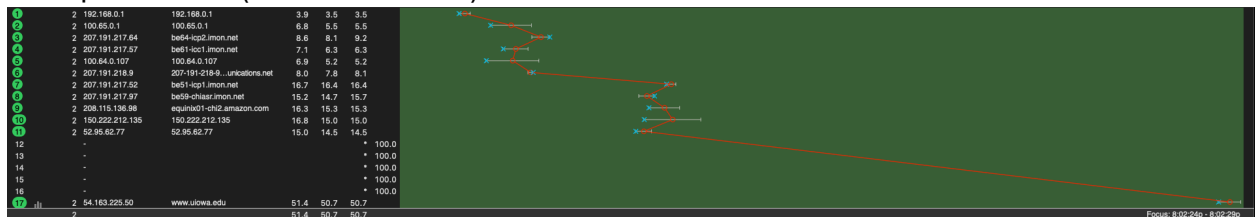
### 56 packet size (www.uiowa.edu)



### 2000 packet size (www.uiowa.edu)



### 3500 packet size (www.uiowa.edu)



1.

#### Picture Reference: First message

23	1.870439	192.168.0.138	54.163.225.50	ICMP	554 Echo (ping) request id=0x1b06, seq=44301/3501, ttl=255 (reply in 29)
26	1.869393	192.168.0.138	54.163.225.50	ICMP	554 Echo (ping) request id=0x1b06, seq=44557/3502, ttl=1 (no response found!)
29	1.872961	54.163.225.50	192.168.0.138	ICMP	1194 Echo (ping) reply id=0x1b06, seq=44301/3501, ttl=52 (request in 23)
30	1.872962	192.168.0.1	192.168.0.138	ICMP	590 Time-to-live exceeded (Time to live exceeded in transit)

#### Upper Layer Protocol Field: ICMP (1)

2.

#### Picture Reference: Length of packet

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN:
Total Length: 56
Identification: 0xfcfe0 (64736)
< 0000 .... = Flags: 0x0
```

#### 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)

```

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: 1

```

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:

```
> Ethernet II, Src: Apple_da:3c:e0 (80:65:7c:da:3c:e0), Dst: TPLink_36:f8:29 (78:8c:b5:36:
  > Internet Protocol Version 4, Src: 192.168.0.138, Dst: 54.163.225.50
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 540
  Identification: 0xbce4 (48356)
  > 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0001 0111 0010 = Fragment Offset: 2960
  > Time to Live: 1
  > [Expert Info (Note/Sequence): "Time To Live" only 1]
```

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 IPv4 Fragments (1980 bytes): #1(1480), #2(500)]
[Stream index: 0]
```

2 fragments:

1<sup>st</sup>: 1480 bytes

2<sup>nd</sup>: 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 additional fragments awaiting.

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

#### Picture Reference:

```
Identification: 0x4010 (16024)
  001. .... = 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
```

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:

```
000. .... = Flags: 0x0
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
  ...0 0000 1011 1001 = Fragment Offset: 1480
```

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

8	5.522967	192.168.0.138	54.163.225.50	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=e3a7) [Reassembled in #10]
9	5.522989	192.168.0.138	54.163.225.50	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=e3a7) [Reassembled in #10]
10	5.522992	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request id=0x1b06, seq=25358/3683, ttl=1 (no response found!)
15	5.562052	192.168.0.138	54.163.225.50	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=f11e) [Reassembled in #17]
16	5.562077	192.168.0.138	54.163.225.50	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=f11e) [Reassembled in #17]
17	5.562081	192.168.0.138	54.163.225.50	ICMP	554	Echo (ping) request id=0x1b06, seq=25614/3684, ttl=2 (no response found!)

Picture Reference: Fragments

```
[ 3 IPv4 Fragments (3480 bytes): #8(1480), #9(1480), #10(520)]
[Frame: 8, payload: 0-1479 (1480 bytes)]
[Frame: 9, payload: 1480-2959 (1480 bytes)]
[Frame: 10, payload: 2960-3479 (520 bytes)]
[Fragment count: 3]
[Reassembled IPv4 length: 3480]
```

The datagram is split into 3 fragments

1<sup>st</sup>: 1480

2<sup>nd</sup>: 1480

3<sup>rd</sup>: 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