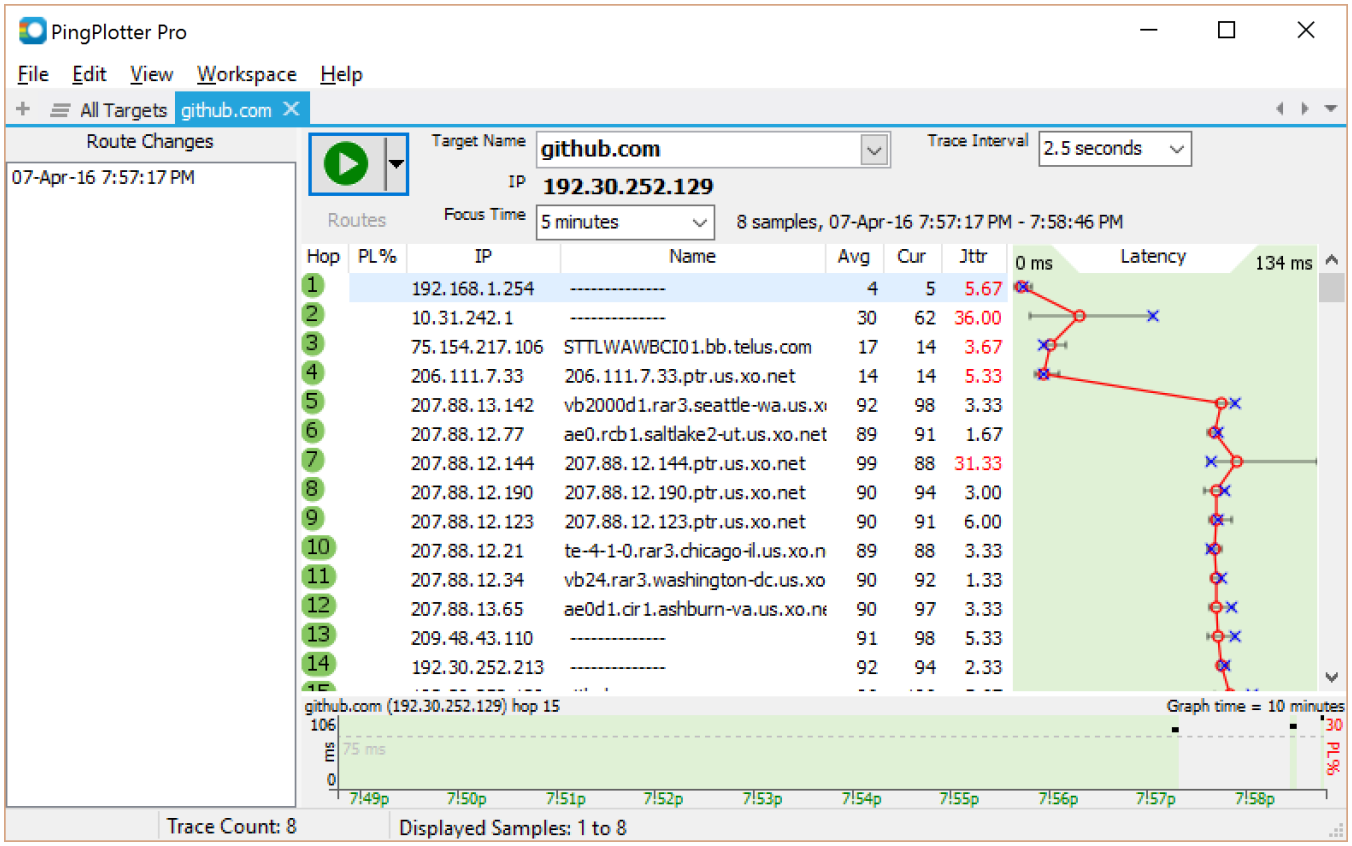
Assignment 3 - Wireshark Lab: IP v6.0

1. Capturing packets from an execution of traceroute

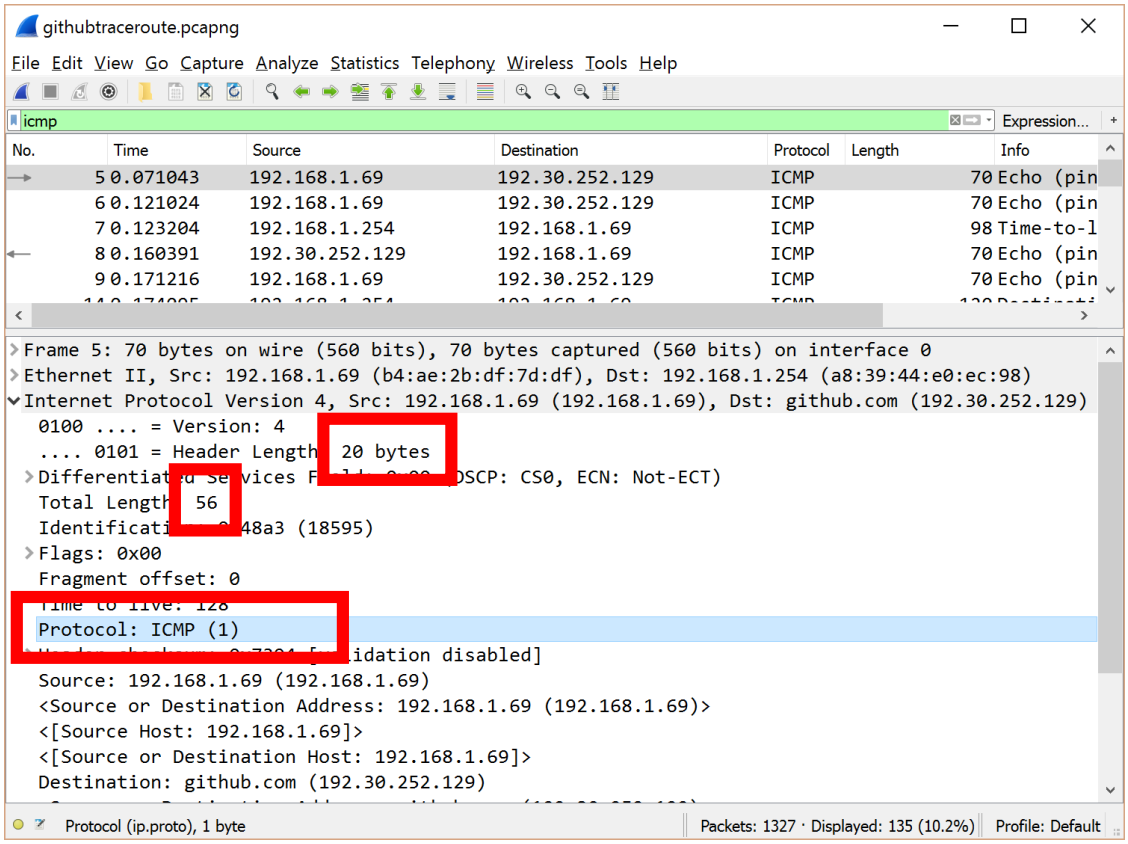
I am using a Windows operating system, so I used a tree trial of the pro version of pingplotter and I traced the site *github.com.*



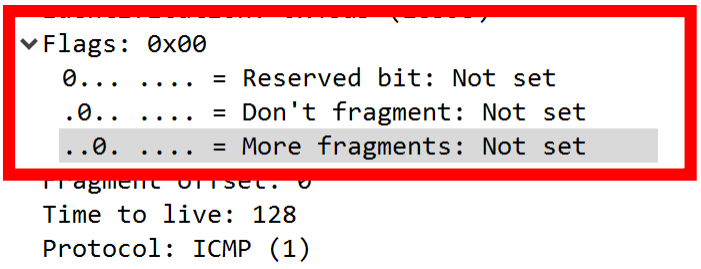
1. The IP address of my computer is **192.168.1.69**

2. The value of the upper-layer protocol field is **ICMP**

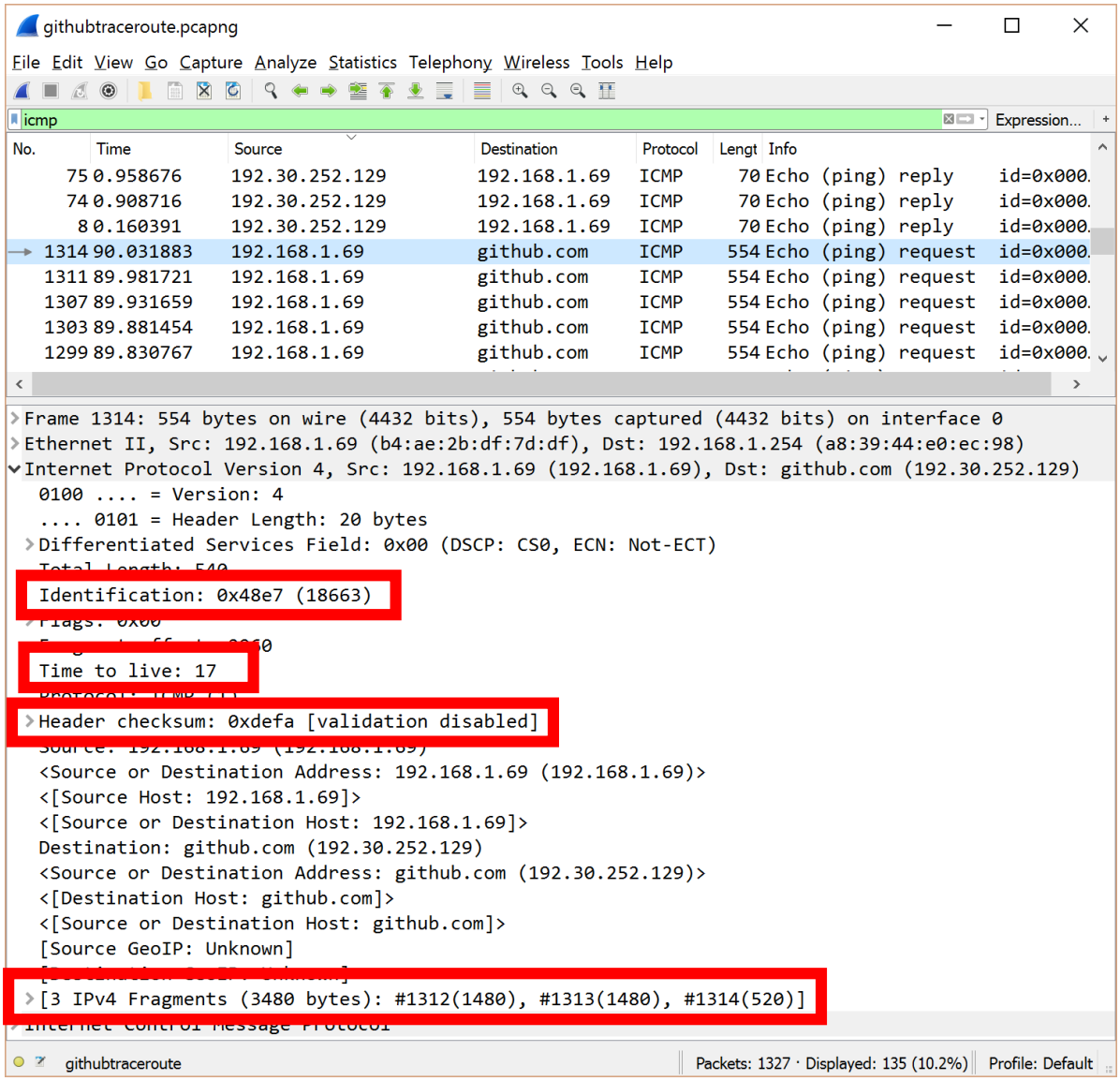
3. The IP header length is **20 bytes**. The total length of the packet is 56 bytes, so the payload is 56-20=**36 bytes**.



4. The IP datagram has **not been fragmented** because the more fragments flag has not been set.



5. The IP fields **Time to live**, **Identification**, **Header checksum** always change. And although it's not an IP field **[3 IPv4 Fragments (3480 bytes):]** always changes as well.



Fields that always change

6. a) Fields that stay constant are the **Version**, the **Header length**, the **Differentiated services field**, the upper-layer **Protocol**, the **Source Address**, and the **Destination Address**.

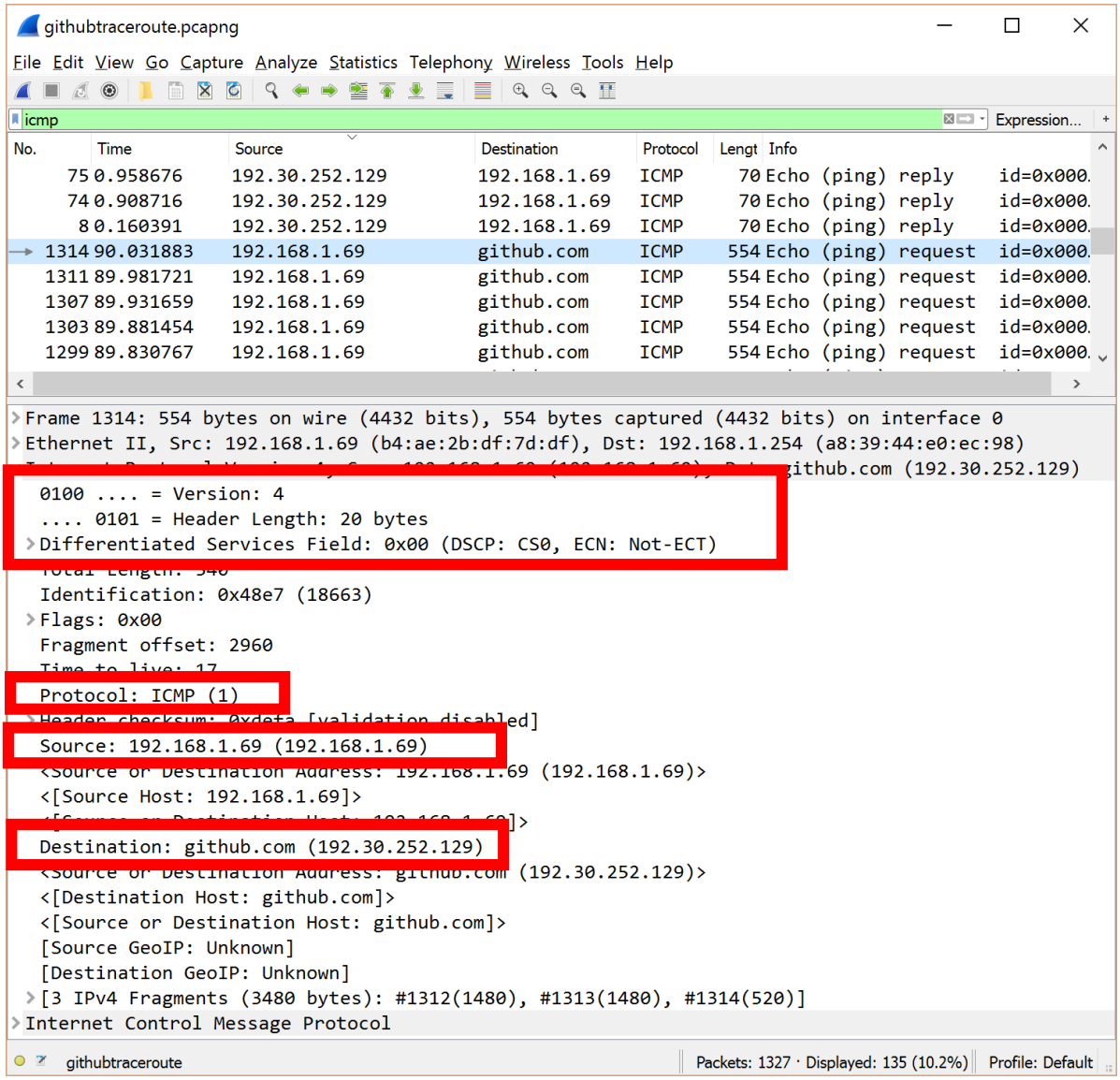
   b) The fields that must stay constant are the **Differentiated services field,** the **Source Address**, the **Destination Address**, and the upper-layer **Protocol**. To be consistent in our transmissions **Version** and **Header Length** also must remain consistent.

   The addresses need to stay the same so that the ICMP messages are sent through the same path to identify the route.

The differentiated services field, protocol, and header fields must stay consistent because all the packets are ICMP packets.

The version number must stay the same so that the messages are consistent, if they were varying between IP versions the packets may travel different routes or experience tunneling which could change our path.

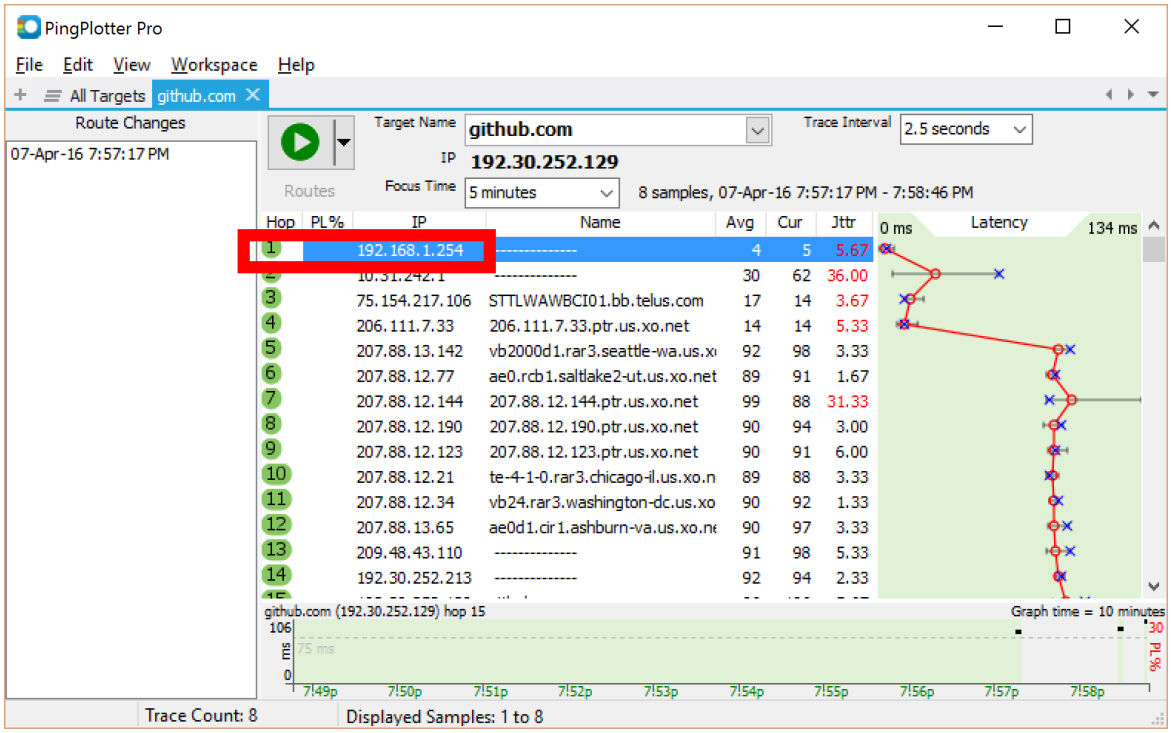
c) The fields that must change are **Identification**, **Time to live,** and **Header checksum**. Identification changes because all the packets in this exchange must have different identification numbers. Time to live changes because traceroute operates by resending a similar packet with incrementing TTL values to learn the identities of each router along the path by the notification of TTL expiring.



Fields that must stay constant

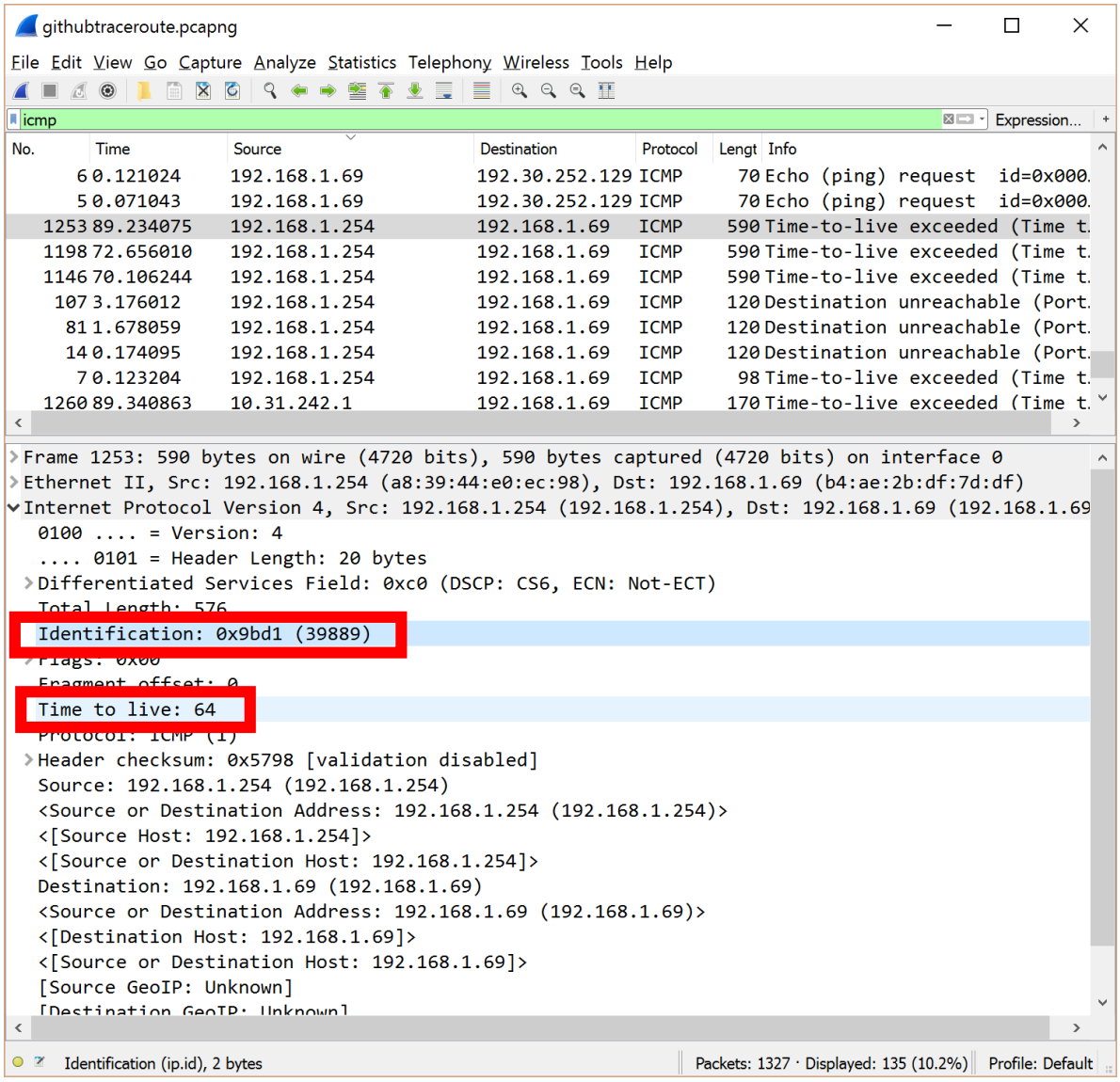
7. As I go down the list of “Echo (ping) request” send by my computer, sorted by source in descending order, the IP header identification number decrements by one with each request. So **as the packet number increases, each Echo (ping) request’s identification number is incremented by one.**

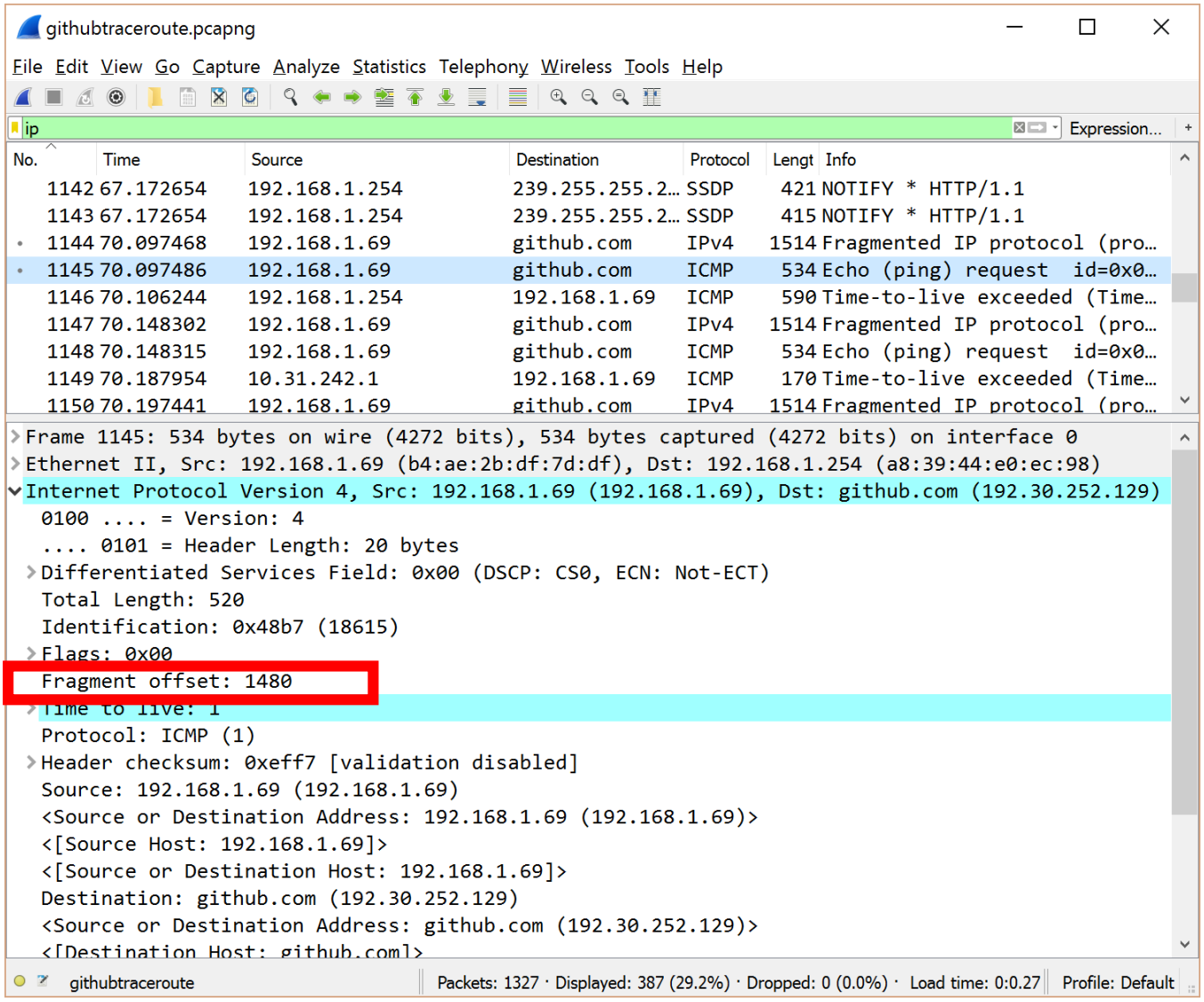
8. According to PingPlotter the first hop router is 192.168.1.254:



In the Wireshark capture (see next page). The value in the TTL field of the first TTL-exceeded message in **64** and the value in the first TTL-exceeded message is **39889**.

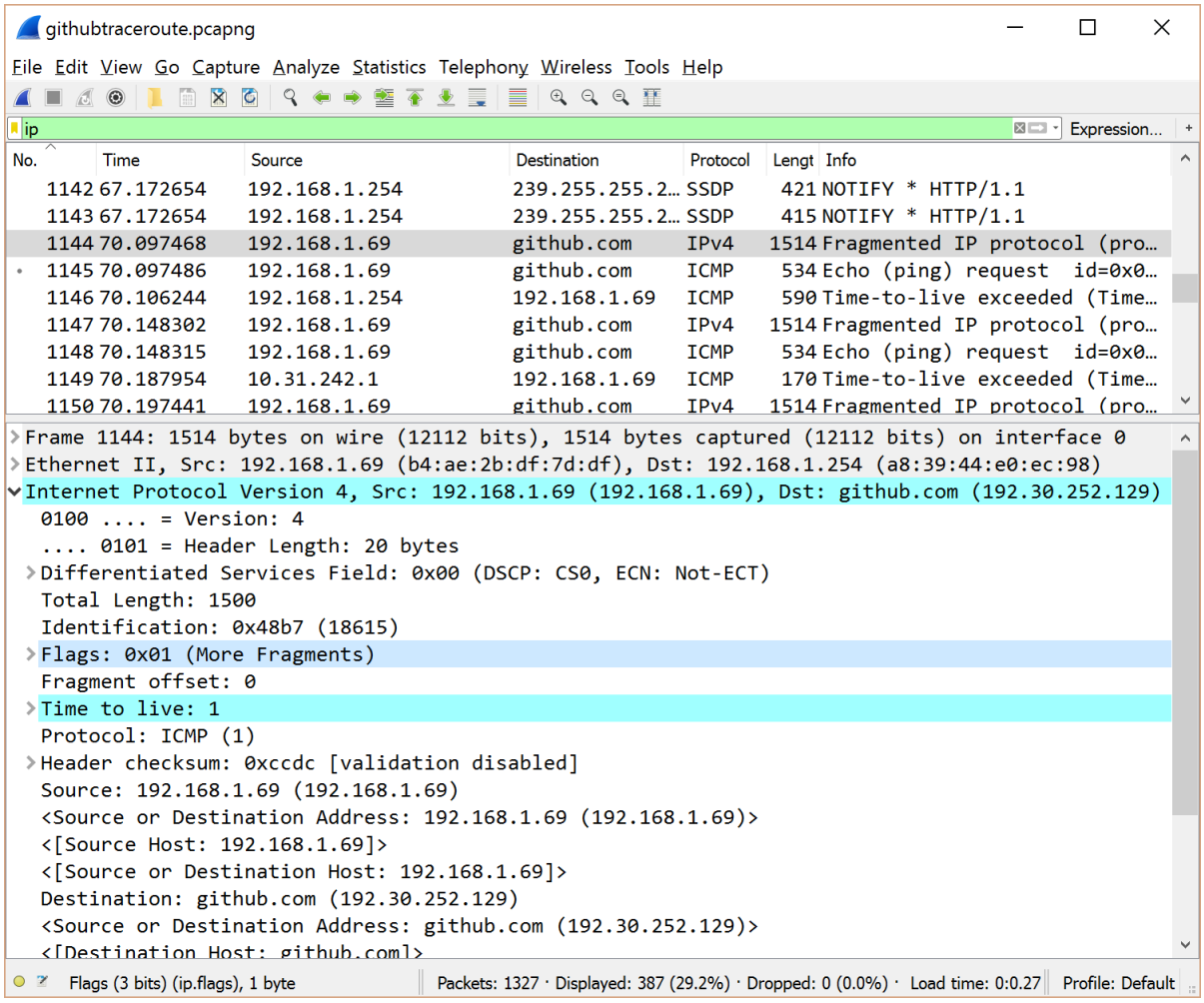
9. The TTL value of each TTL-exceeded message from the first hop router is same, because the message always originates from that router. However, the identification number is not the same in each message because unless they’re fragments of an original message, each new datagram gets a different identification value.


githubtraceroute.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...
No. Time Source Destination Protocol Lengt Info
6 0.121024 192.168.1.69 192.30.252.129 ICMP 70 Echo (ping) request id=0x000.
5 0.071043 192.168.1.69 192.30.252.129 ICMP 70 Echo (ping) request id=0x000.
1253 89.234075 192.168.1.254 192.168.1.69 ICMP 590 Time-to-live exceeded (Time t.
1198 72.656010 192.168.1.254 192.168.1.69 ICMP 590 Time-to-live exceeded (Time t.
1146 70.106244 192.168.1.254 192.168.1.69 ICMP 590 Time-to-live exceeded (Time t.
107 3.176012 192.168.1.254 192.168.1.69 ICMP 120 Destination unreachable (Port.
81 1.678059 192.168.1.254 192.168.1.69 ICMP 120 Destination unreachable (Port.
14 0.174095 192.168.1.254 192.168.1.69 ICMP 120 Destination unreachable (Port.
7 0.123204 192.168.1.254 192.168.1.69 ICMP 98 Time-to-live exceeded (Time t.
1260 89.340863 10.31.242.1 192.168.1.69 ICMP 170 Time-to-live exceeded (Time t.
Frame 1253: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
Ethernet II, Src: 192.168.1.254 (a8:39:44:e0:ec:98), Dst: 192.168.1.69 (b4:ae:2b:df:7d:df)
Internet Protocol Version 4, Src: 192.168.1.254 (192.168.1.254), Dst: 192.168.1.69 (192.168.1.69
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes
Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
Total Length: 576
Identification: 0x9bd1 (39889)
Flags: 0x00
Fragment offset: 0
Time to live: 64
Protocol: ICMP (1)
Header checksum: 0x5798 [validation disabled]
Source: 192.168.1.254 (192.168.1.254)
<Source or Destination Address: 192.168.1.254 (192.168.1.254)>
<[Source Host: 192.168.1.254]>
<[Source or Destination Host: 192.168.1.254]>
Destination: 192.168.1.69 (192.168.1.69)
<Source or Destination Address: 192.168.1.69 (192.168.1.69)>
<[Destination Host: 192.168.1.69]>
<[Source or Destination Host: 192.168.1.69]>
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Identification (ip.id), 2 bytes
Packets: 1327 · Displayed: 135 (10.2%)
Profile: Default



10. Yes, this ICMP echo request has been fragmented across IP datagrams.

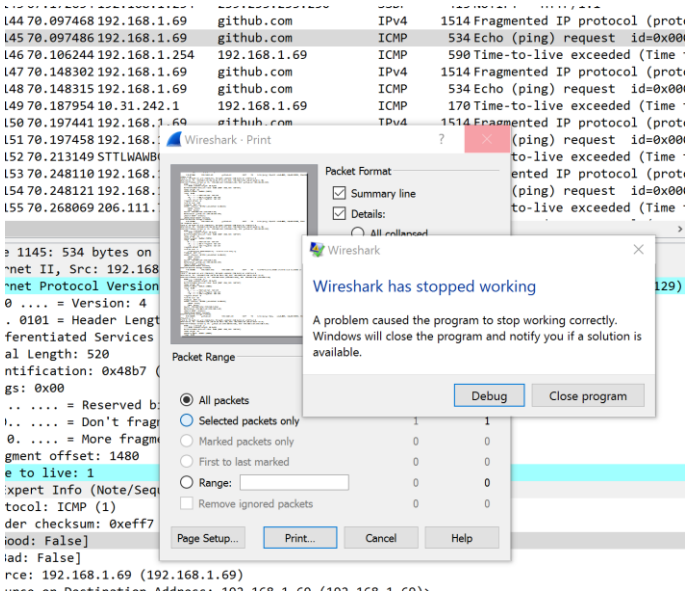
11. The first fragment of the fragmented IP datagram (see next page) has clearly been fragmented because the **More fragments** flag has been set, and it can be seen to be the first fragment because the **fragmentation offset** has a value of 0. The IP datagram has a **total length of 1500 bytes**, with a 20 byte header, so a **payload of 1480 bytes**.


githubtraceroute.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip
Expression...
No. Time Source Destination Protocol Lengt Info
1142 67.172654 192.168.1.254 239.255.255.2... SSDP 421 NOTIFY * HTTP/1.1
1143 67.172654 192.168.1.254 239.255.255.2... SSDP 415 NOTIFY * HTTP/1.1
1144 70.097468 192.168.1.69 github.com IPv4 1514 Fragmented IP protocol (pro...
1145 70.097486 192.168.1.69 github.com ICMP 534 Echo (ping) request id=0x0...
1146 70.106244 192.168.1.254 192.168.1.69 ICMP 590 Time-to-live exceeded (Time...
1147 70.148302 192.168.1.69 github.com IPv4 1514 Fragmented IP protocol (pro...
1148 70.148315 192.168.1.69 github.com ICMP 534 Echo (ping) request id=0x0...
1149 70.187954 10.31.242.1 192.168.1.69 ICMP 170 Time-to-live exceeded (Time...
1150 70.197441 192.168.1.69 github.com IPv4 1514 Fragmented IP protocol (pro...
Frame 1144: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Ethernet II, Src: 192.168.1.69 (b4:ae:2b:df:7d:df), Dst: 192.168.1.254 (a8:39:44:e0:ec:98)
Internet Protocol Version 4, Src: 192.168.1.69 (192.168.1.69), Dst: github.com (192.30.252.129)
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x48b7 (18615)
Flags: 0x01 (More Fragments)
Fragment offset: 0
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0xccdc [validation disabled]
Source: 192.168.1.69 (192.168.1.69)
<Source or Destination Address: 192.168.1.69 (192.168.1.69)>
<[Source Host: 192.168.1.69]>
<[Source or Destination Host: 192.168.1.69]>
Destination: github.com (192.30.252.129)
<Source or Destination Address: github.com (192.30.252.129)>
<[Destination Host: github.com]>
Flags (3 bits) (ip.flags), 1 byte
Packets: 1327 · Displayed: 387 (29.2%) · Dropped: 0 (0.0%) · Load time: 0:0.27
Profile: Default

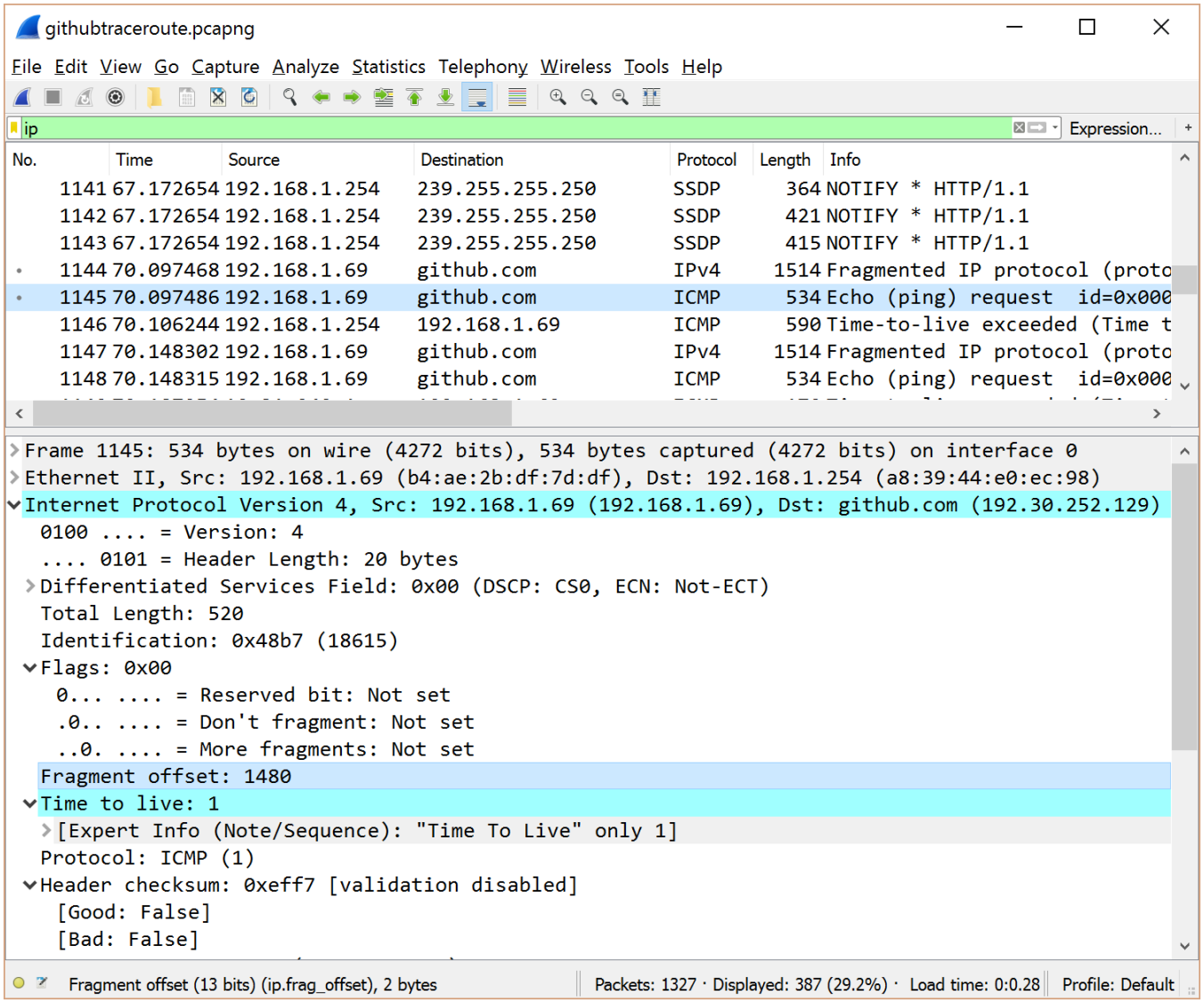
First fragment

```
> Frame 1144: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: 192.168.1.69 (b4:ae:2b:df:7d:df), Dst: 192.168.1.254 (a8:39:44:e0:ec:98)
v Internet Protocol Version 4, Src: 192.168.1.69 (192.168.1.69), Dst: github.com (192.30.252.129)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x48b7 (18615)
  v Flags: 0x01 (More Fragments)
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment offset: 0
  v Time to live: 1
    > [Expert Info (Note/Sequence): "Time To Live" only 1]
    Protocol: ICMP (1)
  v Header checksum: 0xccdc [validation disabled]
      [Good: False]
      [Bad: False]
    Source: 192.168.1.69 (192.168.1.69)
    <Source or Destination Address: 192.168.1.69 (192.168.1.69)>
    <[Source Host: 192.168.1.69]>
    <[Source or Destination Host: 192.168.1.69]>
    Destination: github.com (192.30.252.129)
    <Source or Destination Address: github.com (192.30.252.129)>
    <[Destination Host: github.com]>
    <[Source or Destination Host: github.com]>
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    [Reassembled IPv4 in frame: 1145]
> Data (1480 bytes)
```

Note: I tried to print this using File -> Print -> Selected Packets, but it would crash Wireshark, so I have opted to just take screenshots.



12. The second fragment can be found because the **fragmentation offset is 1480**, meaning that the previous fragment delivered a payload of 1480 bytes and this is where the second fragment fits in. You can tell it is the last fragment because the **More fragments** bit has not been set, indicating to the receiving host that it has received the last fragment.



Second fragment:

```
> Frame 1145: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0
> Ethernet II, Src: 192.168.1.69 (b4:ae:2b:df:7d:df), Dst: 192.168.1.254 (a8:39:44:e0:ec:98)
v Internet Protocol Version 4, Src: 192.168.1.69 (192.168.1.69), Dst: github.com (192.30.252.129)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 520
    Identification: 0x48b7 (18615)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 1480
  v Time to live: 1
    > [Expert Info (Note/Sequence): "Time To Live" only 1]
    Protocol: ICMP (1)
  v Header checksum: 0xeff7 [validation disabled]
      [Good: False]
      [Bad: False]
    Source: 192.168.1.69 (192.168.1.69)
    <Source or Destination Address: 192.168.1.69 (192.168.1.69)>
    <[Source Host: 192.168.1.69]>
    <[Source or Destination Host: 192.168.1.69]>
    Destination: github.com (192.30.252.129)
    <Source or Destination Address: github.com (192.30.252.129)>
    <[Destination Host: github.com]>
    <[Source or Destination Host: github.com]>
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  > [2 IPv4 Fragments (1980 bytes): #1144(1480), #1145(500)]
> Internet Control Message Protocol
```

13. The fields that are different between the first and second fragment are the **total length**, **flags**, **fragmentation offset**, and **checksum**. Everything else stays the same.

14. When the size is set to 3500 bytes, the datagram is fragmented into **3 fragments**.

```
192.168.1.69   192.30.252.129  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=48d7) [Reassembled in #1252]
192.168.1.69   192.30.252.129  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=48d7) [Reassembled in #1252]
192.168.1.69   192.30.252.129  ICMP      554 Echo (ping) request  id=0x0001, seq=131/33536, ttl=1 (no response found!)
```

15. The fields that change between all the three fragments of the 3500 datagram are the **fragmentation offset** and **checksum.** The first two fragments both have a total **length of 1500 bytes**, however the last fragment has a **total length of 540 bytes**. The first two fragments also have the **more fragments** flag set, but the last one does not. Everything else stays the same.

Last fragment of three