

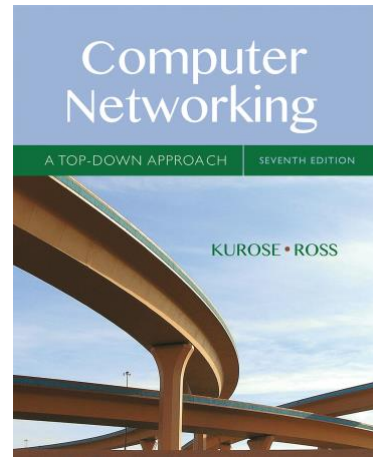
Name: ___Jamie Marini Loebe_____

Wireshark Lab: IP v7.0

Supplement to *Computer Networking: A Top-Down Approach*, 7th ed., J.F. Kurose and K.W. Ross

“Tell me and I forget. Show me and I remember. Involve me and I understand.” Chinese proverb

© 2005-2016, J.F Kurose and K.W. Ross, All Rights Reserved



In this lab, we'll investigate the IP protocol, focusing on the IP datagram. We'll do so by analyzing a trace of IP datagrams sent and received by an execution of the `traceroute` program (the `traceroute` program itself is explored in more detail in the Wireshark ICMP lab). We'll investigate the various fields in the IP datagram, and study IP fragmentation in detail.

Before beginning this lab, you'll probably want to review sections 1.4.3 in the text¹ and section 3.4 of RFC 2151 [[ftp://ftp.rfc-editor.org/in-notes/rfc2151.txt](http://ftp.rfc-editor.org/in-notes/rfc2151.txt)] to update yourself on the operation of the `traceroute` program. You'll also want to read Section 4.3 in the text, and probably also have RFC 791 [[ftp://ftp.rfc-editor.org/in-notes/rfc791.txt](http://ftp.rfc-editor.org/in-notes/rfc791.txt)] on hand as well, for a discussion of the IP protocol.

1. Capturing packets from an execution of `traceroute`

In order to generate a trace of IP datagrams for this lab, we'll use the `traceroute` program to send datagrams of different sizes towards some destination, *X*. Recall that `traceroute` operates by first sending one or more datagrams with the time-to-live (TTL) field in the IP header set to 1; it then sends a series of one or more datagrams towards the same destination with a TTL value of 2; it then sends a series of datagrams towards the same destination with a TTL value of 3; and so on. Recall that a router must decrement the TTL in each received datagram by 1 (actually, RFC 791 says that the router must decrement the TTL by *at least* one). If the TTL reaches 0, the router returns an ICMP message (type 11 – TTL-exceeded) to the sending host. As a result of this behavior, a datagram with a TTL of 1 (sent by the host executing `traceroute`) will cause the router one hop away from the sender to send an ICMP TTL-exceeded message back to the sender; the datagram sent with a TTL of 2 will cause the router two hops

¹ References to figures and sections are for the 7th edition of our text, *Computer Networks, A Top-down Approach*, 7th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2016.

away to send an ICMP message back to the sender; the datagram sent with a TTL of 3 will cause the router three hops away to send an ICMP message back to the sender; and so on. In this manner, the host executing `tracert` can learn the identities of the routers between itself and destination X by looking at the source IP addresses in the datagrams containing the ICMP TTL-exceeded messages.

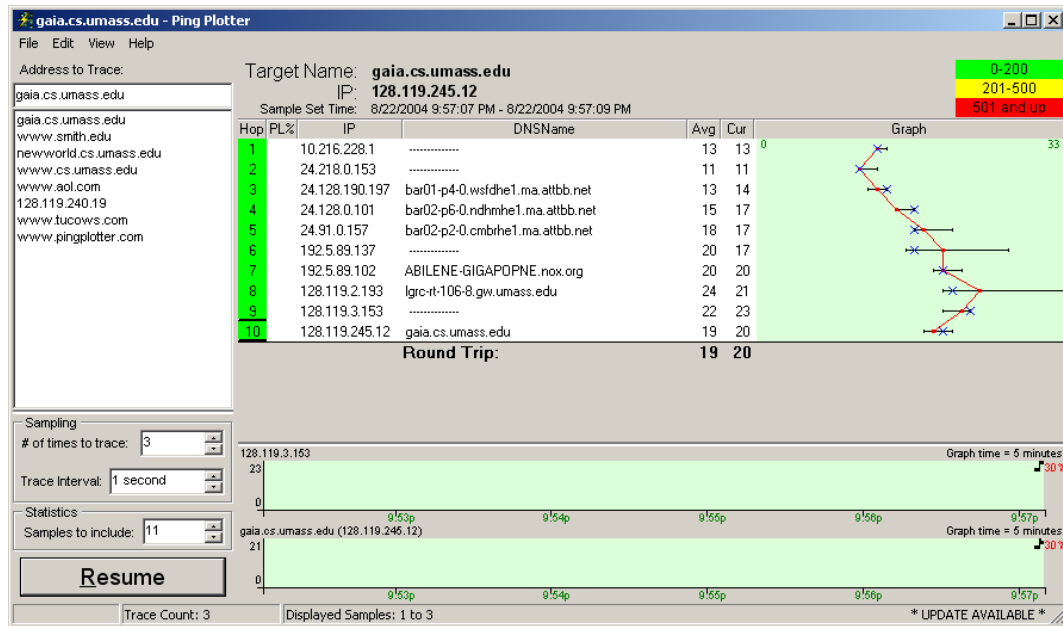
We'll want to run `tracert` and have it send datagrams of various lengths.

- **Windows.** The `tracert` program (used for our ICMP Wireshark lab) provided with Windows does not allow one to change the size of the ICMP echo request (ping) message sent by the `tracert` program. A nicer Windows `tracert` program is *pingplotter*, available both in free version and shareware versions at <http://www.pingplotter.com>. Download and install *pingplotter*, and test it out by performing a few traceroutes to your favorite sites. The size of the ICMP echo request message can be explicitly set in *pingplotter* by selecting the menu item *Edit->Options->Packet Options* and then filling in the *Packet Size* field. The default packet size is 56 bytes. Once *pingplotter* has sent a series of packets with the increasing TTL values, it restarts the sending process again with a TTL of 1, after waiting *Trace Interval* amount of time. The value of *Trace Interval* and the number of intervals can be explicitly set in *pingplotter*.
- **Linux/Unix/MacOS.** With the Unix/MacOS `tracert` command, the size of the UDP datagram sent towards the destination can be explicitly set by indicating the number of bytes in the datagram; this value is entered in the `tracert` command line immediately after the name or address of the destination. For example, to send `tracert` datagrams of 2000 bytes towards `gaia.cs.umass.edu`, the command would be:

```
%tracert gaia.cs.umass.edu 2000
```

Do the following:

- Start up Wireshark and begin packet capture (*Capture->Start*) and then press *OK* on the Wireshark Packet Capture Options screen (we'll not need to select any options here).
- If you are using a Windows platform, start up *pingplotter* and enter the name of a target destination in the "Address to Trace Window." Enter 3 in the "# of times to Trace" field, so you don't gather too much data. Select the menu item *Edit->Advanced Options->Packet Options* and enter a value of 56 in the *Packet Size* field and then press *OK*. Then press the *Trace* button. You should see a *pingplotter* window that looks something like this:



Next, send a set of datagrams with a longer length, by selecting *Edit->Advanced Options->Packet Options* and enter a value of 2000 in the *Packet Size* field and then press OK. Then press the Resume button.

Finally, send a set of datagrams with a longer length, by selecting *Edit->Advanced Options->Packet Options* and enter a value of 3500 in the *Packet Size* field and then press OK. Then press the Resume button.

Stop Wireshark tracing.

- If you are using a Unix or Mac platform, enter three `traceroute` commands, one with a length of 56 bytes, one with a length of 2000 bytes, and one with a length of 3500 bytes.

Stop Wireshark tracing.

If you are unable to run Wireshark on a live network connection, you can download a packet trace file that was captured while following the steps above on one of the author's Windows computers². You may well find it valuable to download this trace even if you've captured your own trace and use it, as well as your own trace, when you explore the questions below.

² Download the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> and extract the file *ip-ethereal-trace-1*. The traces in this zip file were collected by Wireshark running on one of the author's computers, while performing the steps indicated in the Wireshark lab. Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the *ip-ethereal-trace-1* trace file.

2. A look at the captured trace

In your trace, you should be able to see the series of ICMP Echo Request (in the case of Windows machine) or the UDP segment (in the case of Unix) sent by your computer and the ICMP TTL-exceeded messages returned to your computer by the intermediate routers. In the questions below, we'll assume you are using a Windows machine; the corresponding questions for the case of a Unix machine should be clear. Whenever possible, when answering a question below you should include a screenshot of the packet(s) within the trace that you used to answer the question asked. When you submit your assignment, annotate the output so that it's clear where in the output you're getting the information for your answer (e.g., for our class, we ask that students annotate electronic copies with text in a colored font). Make sure to include in your screenshot ALL and ONLY the minimum amount of packet detail that you need to answer the question.

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.

The screenshot displays the Wireshark 1.6.7 interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The first packet (No. 1) is an ARP request. Subsequent packets (No. 2-7) are UDP segments. Packets 8-13 are ICMP Echo (ping) requests. Packet 8 is selected, and its details are shown in the packet details pane.
- Packet Details:** Shows the hierarchical structure of the selected packet (No. 8). The selected packet is an ICMP Echo (ping) request. The details pane shows the following information:
 - Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
 - Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
 - Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.59.23.100 (128.59.23.100)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
 - Total Length: 84
 - Identification: 0x32d0 (13008)
 - Flags: 0x00
 - Fragment offset: 0
- Packet Bytes:** Shows the raw data of the selected packet in hexadecimal and ASCII. The data starts with 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00, which corresponds to the Ethernet II header.

The status bar at the bottom indicates: Frame (frame), 98 bytes | Packets: 380 Displayed: 380 Marked: 0 Load time: 0:00.006 | Profile: Default

What is the IP address of your computer?

--My IP Address: 192.168.1.102 (Per Wireshark Trace ZIP file provided)

1	20:47:56.658352	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
2	20:48:01.525219	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
3	20:48:01.526499	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
4	20:48:02.021888	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
5	20:48:02.023151	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
6	20:48:02.522780	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	20:48:02.523813	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
8	20:48:02.821397	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
9	20:48:02.835178	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	20:48:02.846981	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
11	20:48:02.861309	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	20:48:02.866949	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
13	20:48:02.892857	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	20:48:02.897047	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
15	20:48:02.916024	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
16	20:48:02.917102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
17	20:48:02.944369	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
0100 = Version: 4
... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x32d0 (13008)
> Flags: 0x00
Fragment Offset: 0
> Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x2d2c [validation disabled]

2. Within the IP packet header, what is the value in the upper layer protocol field?

--The value in upper layer protocol field is ICMP(1)

No.	Time	Source	Destination	Protocol	Length	Info
1	20:47:56.658352	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
2	20:48:01.525219	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
3	20:48:01.526499	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
4	20:48:02.021888	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
5	20:48:02.023151	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
6	20:48:02.522780	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	20:48:02.523813	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
8	20:48:02.821397	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
9	20:48:02.835178	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	20:48:02.846981	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
11	20:48:02.861309	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	20:48:02.866949	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
13	20:48:02.892857	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	20:48:02.897047	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
15	20:48:02.916024	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
16	20:48:02.917102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
17	20:48:02.944369	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

> Flags: 0x00
0... = Reserved bit: Not set
0... = Don't fragment: Not set
..0... = More fragments: Not set
Fragment Offset: 0
> Time to Live: 1
> [Expert Info (Note/Sequence): "Time To Live" only 1]
Protocol: ICMP (1)
Header Checksum: 0x2d2c [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
> Internet Control Message Protocol

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.

--IP Header: 20 bytes

--Payload: 64.

--Explanation: Payload = (Total size – 20) thus 84 – 20 = 64

See Screenshow Below

No.	Time	Source	Destination	Protocol	Length	Info
1	20:47:56.658352	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
2	20:48:01.525219	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
3	20:48:01.526499	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
4	20:48:02.021888	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
5	20:48:02.023151	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
6	20:48:02.522780	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	20:48:02.523813	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
8	20:48:02.821397	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
9	20:48:02.835178	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	20:48:02.846981	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
11	20:48:02.861309	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	20:48:02.866949	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
13	20:48:02.892857	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	20:48:02.897047	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
15	20:48:02.916024	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
16	20:48:02.917102	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
17	20:48:02.944369	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)	
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100	
0100 ... = Version: 4	
... 0101 = Header Length: 20 bytes (5)	
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	
Total Length: 84	
Identification: 0x32d0 (13008)	
Flags: 0x00	
Fragment Offset: 0	
Time to Live: 1	
[Expert Info (Note/Sequence): "Time To Live" only 1]	
Protocol: ICMP (1)	

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
--Per above screenshots, no. There are no IPv4 fragments, and also MORE_FRAGMENTS flag is not set.

Next, sort the traced packets according to IP source address by clicking on the *Source* column header; a small downward pointing arrow should appear next to the word *Source*. If the arrow points up, click on the *Source* column header again. Select the first ICMP Echo Request message sent by your computer and expand the Internet Protocol portion in the “details of selected packet header” window. In the “listing of captured packets” window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent by other protocols running on your computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by your computer.

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?
--Identification, TTL, Header Checksum
6. Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?

Do NOT change:

- **Version** – Always using IP4V
- **Header Length**
- **Total Length** – Each message still is part of larger data being sent
- **Fragment Offset** – Each ICMP message is not a fragment itself
- **Protocol + Differentiated services** – Protocol does not change
- **Source** – Computer IP address does not change
- **Destination Addresses** -- gaia.cs.umass.edu IP address does not change

Do change:

- **Identification** – Each IP datagram has different ID
- **TTL** – With each IP datagram received, traceroute increments the TTL value by 1
- **Header Checksum** – ****Validation is disabled****

The screenshot shows a Wireshark packet capture. The packet list pane displays several ICMP Echo (ping) requests. The selected packet is packet 368, an ICMP Echo (ping) request from 192.168.1.102 to 128.59.23.100. The packet details pane shows the following information:

- Frame 368: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)
- Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 568
 - Identification: 0x334a (13130)
 - Flags: 0x01
 - Fragment Offset: 2960
 - Time to Live: 13
 - Protocol: ICMP (1)
 - Header Checksum: 0x1d5c [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.1.102
 - Destination Address: 128.59.23.100
 - [3 IPv4 Fragments (3508 bytes): #366(1480), #367(1480), #368(548)]
- Internet Control Message Protocol

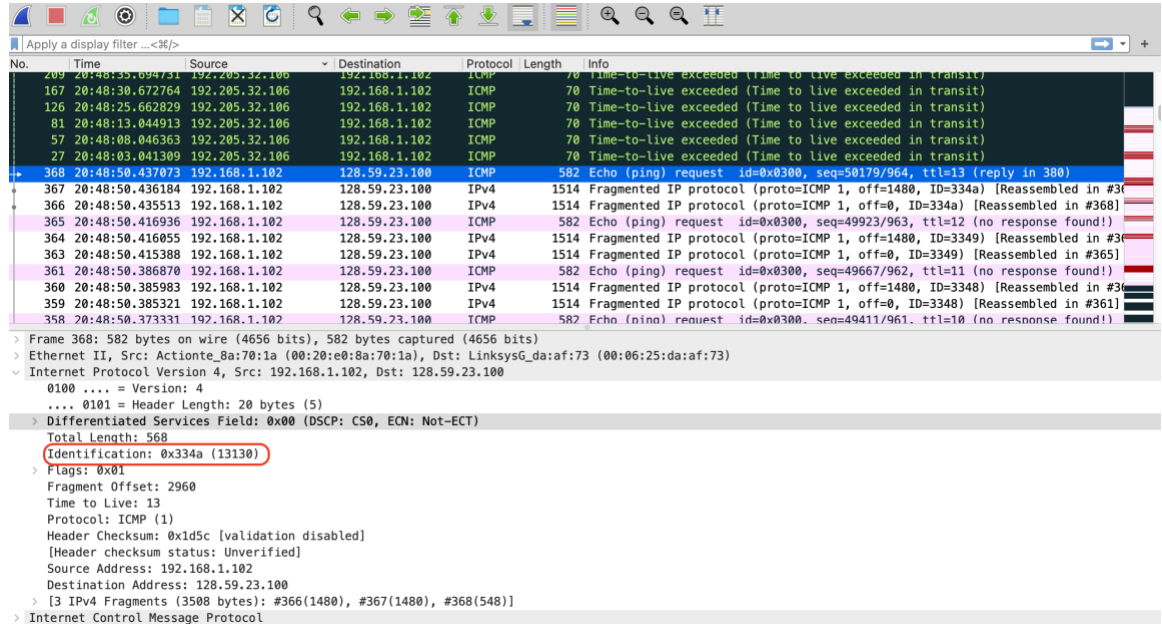
The screenshot shows a Wireshark packet capture. The packet list pane displays several ICMP Echo (ping) requests. The selected packet is packet 365, an ICMP Echo (ping) request from 192.168.1.102 to 128.59.23.100. The packet details pane shows the following information:

- Frame 365: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)
- Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 568
 - Identification: 0x3349 (13129)
 - Flags: 0x01
 - Fragment Offset: 2960
 - Time to Live: 12
 - Protocol: ICMP (1)
 - Header Checksum: 0x1e5d [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.1.102
 - Destination Address: 128.59.23.100
 - [3 IPv4 Fragments (3508 bytes): #363(1480), #364(1480), #365(548)]
- Internet Control Message Protocol

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

--The Identification value is incrementing with each datagram

**Please see time stamps on screenshots, as newest data is at top



No.	Time	Source	Destination	Protocol	Length	Info
209	20:48:35.694731	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
167	20:48:30.672764	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
126	20:48:25.662829	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
81	20:48:13.044913	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
57	20:48:08.046363	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
27	20:48:03.041389	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
368	20:48:50.437073	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=50179/964, ttl=13 (reply in 380)
367	20:48:50.436184	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]
366	20:48:50.435513	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
365	20:48:50.416936	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49923/963, ttl=12 (no response found!)
364	20:48:50.416055	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
363	20:48:50.415388	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
361	20:48:50.386870	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49667/962, ttl=11 (no response found!)
360	20:48:50.385983	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3348) [Reassembled in #361]
359	20:48:50.385321	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3348) [Reassembled in #361]
358	20:48:50.373331	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49411/961, ttl=10 (no response found!)

> Frame 368: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)

> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)

> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 568

Identification: 0x334a (13130)

> Flags: 0x01

Fragment Offset: 2960

Time to Live: 13

Protocol: ICMP (1)

Header Checksum: 0x1d5c [validation disabled]

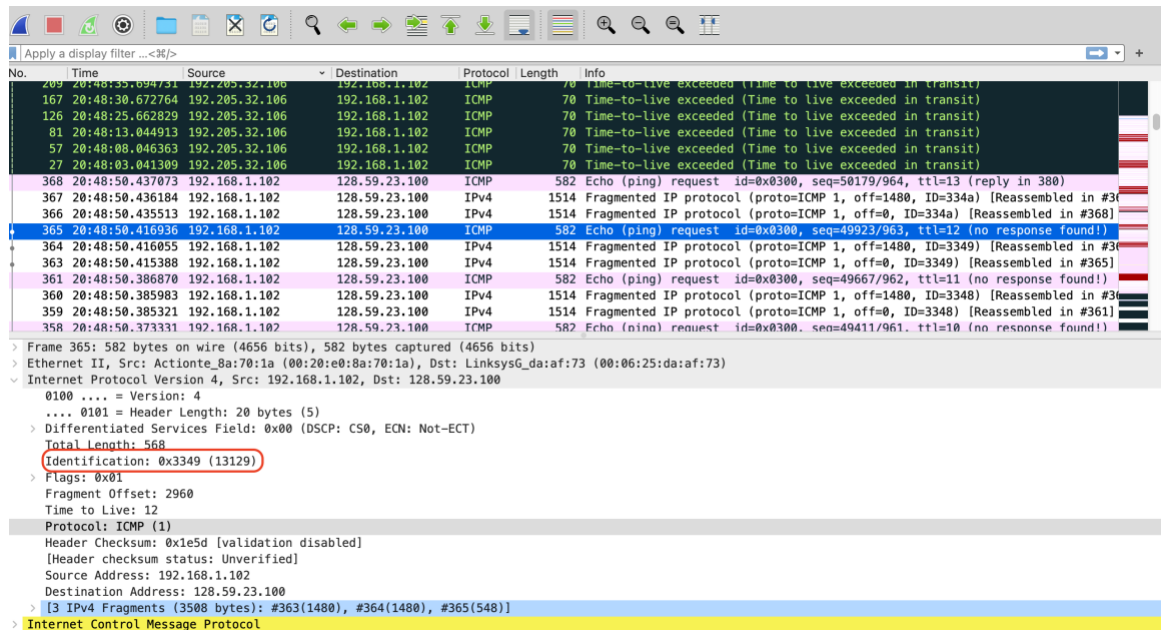
[Header checksum status: Unverified]

Source Address: 192.168.1.102

Destination Address: 128.59.23.100

> [3 IPv4 Fragments (3508 bytes): #366(1480), #367(1480), #368(548)]

> Internet Control Message Protocol



No.	Time	Source	Destination	Protocol	Length	Info
209	20:48:35.694731	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
167	20:48:30.672764	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
126	20:48:25.662829	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
81	20:48:13.044913	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
57	20:48:08.046363	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
27	20:48:03.041389	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
368	20:48:50.437073	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=50179/964, ttl=13 (reply in 380)
367	20:48:50.436184	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]
366	20:48:50.435513	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
365	20:48:50.416936	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49923/963, ttl=12 (no response found!)
364	20:48:50.416055	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
363	20:48:50.415388	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
361	20:48:50.386870	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49667/962, ttl=11 (no response found!)
360	20:48:50.385983	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3348) [Reassembled in #361]
359	20:48:50.385321	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3348) [Reassembled in #361]
358	20:48:50.373331	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49411/961, ttl=10 (no response found!)

> Frame 365: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)

> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)

> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 568

Identification: 0x3349 (13129)

> Flags: 0x01

Fragment Offset: 2960

Time to Live: 12

Protocol: ICMP (1)

Header Checksum: 0x1e5d [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.102

Destination Address: 128.59.23.100

> [3 IPv4 Fragments (3508 bytes): #363(1480), #364(1480), #365(548)]

> Internet Control Message Protocol

Next (with the packets still sorted by source address) find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router.

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

-- **Identification:** 0x4fcd (20429)

-- **TTL:** 243

No.	Time	Source	Destination	Protocol	Length	Info
63	20:48:08.138415	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=26883/873, ttl=242 (request in 61)
35	20:48:03.149339	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=23555/860, ttl=242 (request in 33)
377	20:48:51.433168	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
320	20:48:46.428528	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
266	20:48:41.422315	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
212	20:48:35.886001	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
170	20:48:30.870459	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
129	20:48:25.865519	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
88	20:48:13.126955	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
62	20:48:08.125388	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
34	20:48:03.126331	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
326	20:48:49.650523	128.119.245.12	192.168.1.102	TCP	60	22 → 1170 [ACK] Seq=1 Ack=41 Win=35040 Len=0
91	20:48:19.611090	128.119.245.12	192.168.1.102	TCP	60	22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
370	20:48:50.632316	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
314	20:48:45.621996	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 377: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
Internet Protocol Version 4, Src: 128.59.1.41, Dst: 192.168.1.102
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0x4fcd (20429)
> Flags: 0x00
> Fragment Offset: 0
Time to Live: 243
Protocol: ICMP (1)
Header Checksum: 0x3485 [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.59.1.41
Destination Address: 192.168.1.102
> Internet Control Message Protocol

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?

--**The Identification field changes each time, as this is a unique value. If they were the same, then it would mean they belong to one larger packet**

-- **TTL field does not change, as it is always the same for the first hop router.**

Fragmentation

Sort the packet listing according to time again by clicking on the *Time* column.

- 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? [Note: if you find your packet has not been fragmented, you should download the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> and extract the *ip-ethereal-trace-1* packet trace. If your computer has an Ethernet interface, a packet size of 2000 *should* cause fragmentation.³]

--Yes, see below.

The image shows a Wireshark packet capture interface. The packet list pane on the left shows a series of ICMP Echo (ping) requests. Packet 92 is highlighted, showing it is a fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]. The packet details pane on the right shows the structure of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and ICMP Echo (ping) request. The ICMP Echo (ping) request section is expanded, showing the payload as a list of IPv4 fragments. The fragments are listed as follows:

- [Frame 92, payload: 0-1479 (1480 bytes)]
- [Frame 93, payload: 1480-2007 (528 bytes)]
- [Fragment count: 2]

The fragments are shown as a single list, indicating they are part of the same datagram. The total length of the fragments is 2008 bytes, which is the size of the original datagram.

³ The packets in the *ip-ethereal-trace-1* trace file in <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> are all less than 1500 bytes. This is because the computer on which the trace was gathered has an Ethernet card that limits the length of the maximum IP packet to 1500 bytes (40 bytes of TCP/IP header data and 1460 bytes of upper-layer protocol payload). This 1500 byte value is the standard maximum length allowed by Ethernet. If your trace indicates a datagram longer 1500 bytes, and your computer is using an Ethernet connection, then Wireshark is reporting the wrong IP datagram length; it will likely also show only one large IP datagram rather than multiple smaller datagrams.. This inconsistency in reported lengths is due to the interaction between the Ethernet driver and the Wireshark software. We recommend that if you have this inconsistency, that you perform this lab using the *ip-ethereal-trace-1* trace file.

11. Screenshot the first fragment of the fragmented IP datagram (with sufficient details to answer these questions). 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?

-- More fragments flag set, Fragment offset = 0.

Apply a display filter ...<[?]>

No.	Time	Source	Destination	Protocol	Length	Info
88	20:48:13.126955	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	20:48:13.158271	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x8300, seq=30211/886, ttl=242 (request in 87)
90	20:48:19.586445	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (Len=20)
91	20:48:19.611090	128.119.245.12	192.168.1.102	TCP	60	22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
92	20:48:25.099863	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93	20:48:25.100537	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x8300, seq=30467/887, ttl=1 (no response found!)
94	20:48:25.120616	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	20:48:25.129020	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
96	20:48:25.129690	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x8300, seq=30723/888, ttl=2 (no response found!)
97	20:48:25.149015	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
98	20:48:25.149675	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x8300, seq=30979/889, ttl=3 (no response found!)
99	20:48:25.179081	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #100]
100	20:48:25.179745	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x8300, seq=31235/890, ttl=4 (no response found!)
101	20:48:25.188565	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
102	20:48:25.199110	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fd) [Reassembled in #103]

> Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

> Ethernet II, Src: Actionte_Ba:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)

> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 1500

Identification: 0x32f9 (13049)

> Flags: 0x20, More fragments

0... = Reserved bit: Not set

.0.. = Don't fragment: Not set

..1. = More fragments: Set

Fragment Offset: 0

> Time to Live: 1

> [Expert Info (Note/Sequence): "Time To Live" only 1]

Protocol: ICMP (1)

Header Checksum: 0x077b [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.102

Destination Address: 128.59.23.100

[Reassembled IPv4 in frame: 93]

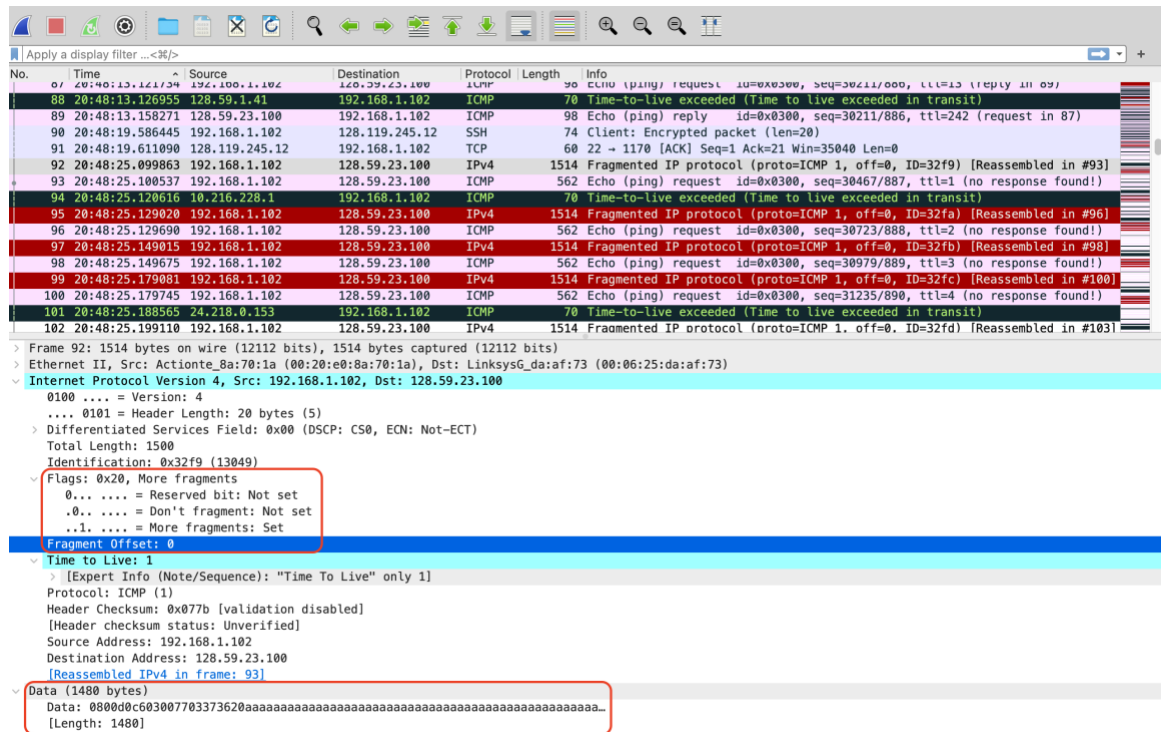
> Data (1480 bytes)

Data: 0800d0c603007703373620aaa...

[Length: 1480]

-- More fragments flag set, fragment offset set to 0

-- This datagram has a size of 1500 (1480 minus header length)



12. Screenshot the second fragment of the fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?
- TTL value is 2, first fragment would be 1.
- Yes. The 'More Fragments' flag is set, and we are expecting 2000 bytes, but this first fragment only has 1480.

No.	Time	Source	Destination	Protocol	Length	Info
84	20:48:13.076419	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	20:48:13.096610	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	20:48:13.101662	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (no response found!)
87	20:48:13.121734	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (reply in 89)
88	20:48:13.126955	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	20:48:13.158271	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (request in 87)
90	20:48:19.586445	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (len=20)
91	20:48:19.611090	128.119.245.12	192.168.1.102	TCP	60	22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
92	20:48:25.099863	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93	20:48:25.100537	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)
94	20:48:25.120616	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	20:48:25.129020	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
96	20:48:25.129690	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response found!)
97	20:48:25.149015	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
98	20:48:25.149675	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found!)

> Frame 95: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x32fa (13050)
> Flags: 0x20, More fragments
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..1. = More fragments: Set
Fragment Offset: 0
> Time to Live: 2
Protocol: ICMP (1)
Header Checksum: 0x067a [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[Reassembled IPv4 in frame: 96]
> Data (1480 bytes)
Data: 0800cfc603007803373620aa...
[Length: 1480]

13. What fields change in the IP header between the first and second fragment?
--Identification, TTL, Header Checksum (Validation disabled)

Now find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 3500.

14. How many fragments were created from the original datagram?
--Three (3).

No.	Time	Source	Destination	Protocol	Length	Info
211	20:48:35.822521	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
212	20:48:35.886001	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
213	20:48:35.972615	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0956) [Reassembled in #214]
214	20:48:35.980918	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in 205)
215	20:48:37.697010	192.168.1.102	199.2.53.206	TCP	62	[TCP Retransmission] 1483 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_D
216	20:48:40.124488	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217	20:48:40.125160	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218	20:48:40.125981	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219	20:48:40.144138	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
220	20:48:40.150636	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221	20:48:40.151305	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
222	20:48:40.152253	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=40707/927, ttl=2 (no response found!)
223	20:48:40.170497	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled in #225]
224	20:48:40.171170	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3325) [Reassembled in #225]
225	20:48:40.172012	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=40963/928, ttl=3 (no response found!)

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 568
Identification: 0x3323 (13091)
Flags: 0x01
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment Offset: 2960
> Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x2983 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
> [3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xa9c3 [correct]
[Checksum Status: Good]

15. What fields change in the IP header among the fragments?

--Fragment Offset (Increases from 0 to 1480 to 2960)

--Flags (Set to More Fragments for first 2, then set to None on 3rd fragment)

--Length: Set to 1500 for first 2, then set to 568 for 3rd fragment