

Computer Networks 1

Lab 4a

Wireshark Lab: IP v8.0

Student Name: Nguyễn Quý Hải

Student No.: 2052974

I. Objectives

In this lab, we'll explore several aspects of the HTTP protocol:

- Investigate the IP protocol
- Focusing on the IP datagram
- Investigate the various fields in the IP datagram
- Study IP fragmentation in detail

II. Content

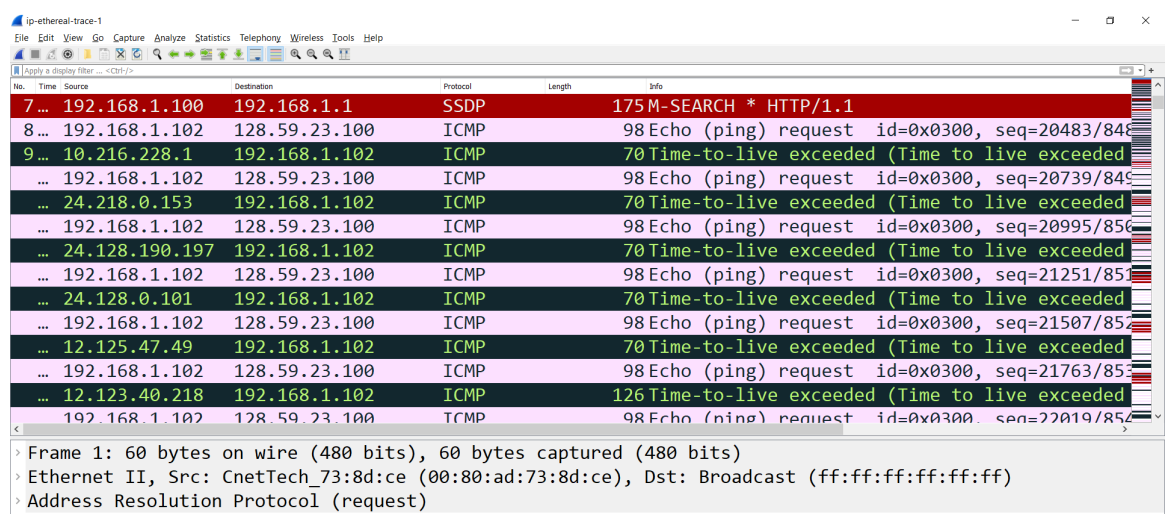
1. Capturing packets from an execution of traceroute

- Following the lab's guide.

2. A look at the captured trace

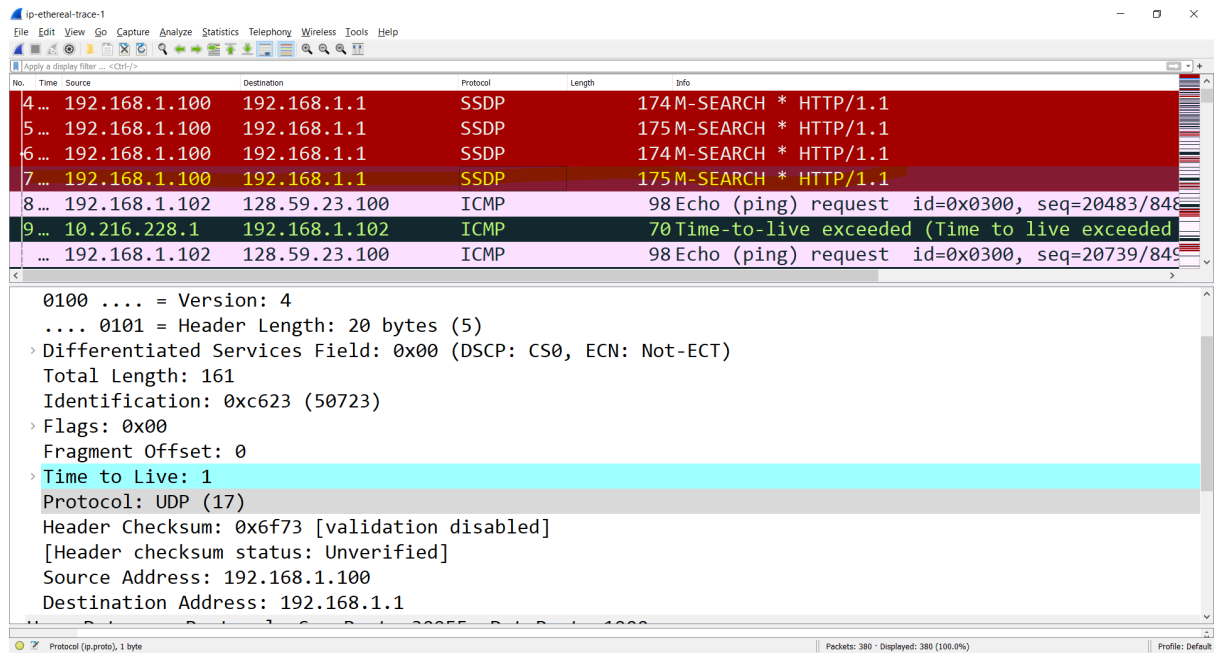
- Q1: Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

Answer: My computer is 192.168.1.11. And the author's computer in example is 192.168.1.102.



- Q2. Within the IP packet header, what is the value in the upper layer protocol field?

Answer: the upper layer protocol field's value is 17



The screenshot shows a Wireshark capture of network traffic. The packet list pane displays several packets, including SSDP M-SEARCH requests and ICMP Echo (ping) requests. The packet details pane for the selected packet (No. 9) shows the following fields:

- Version: 4
- Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 161
- Identification: 0xc623 (50723)
- Flags: 0x00
- Fragment Offset: 0
- Time to Live: 1
- Protocol: UDP (17)
- Header Checksum: 0x6f73 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.1.100
- Destination Address: 192.168.1.1

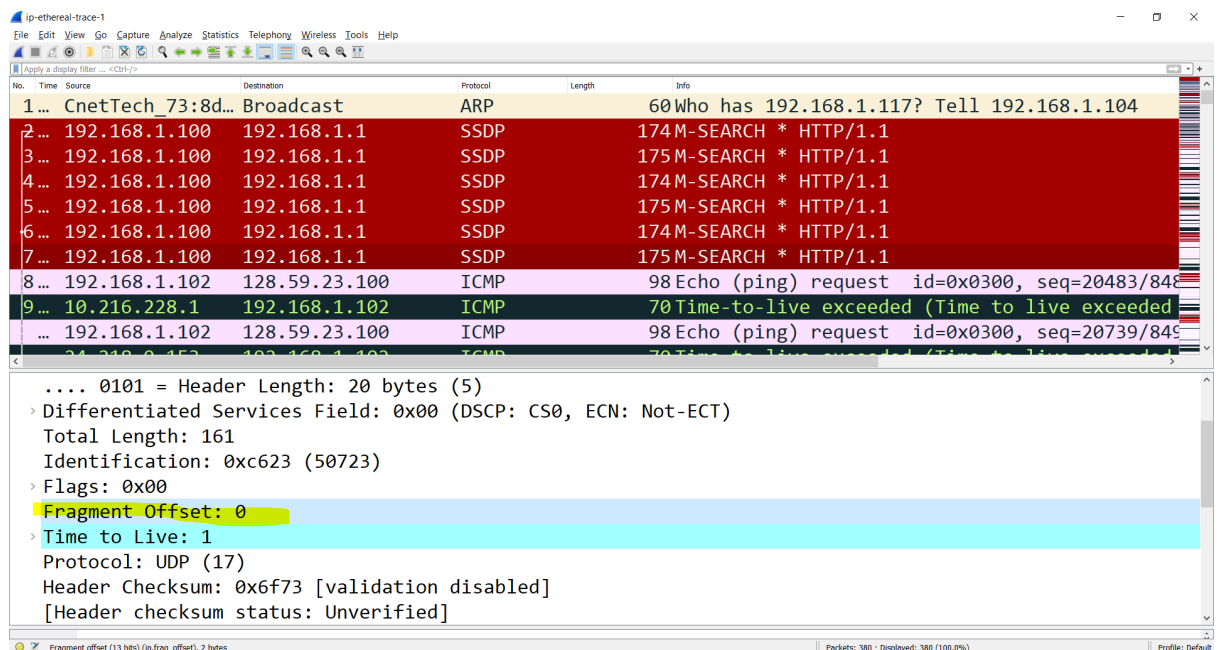
- Q3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

Answer: It is 141 bytes. Total length is 161 bytes and the header length is 20 bytes.

So the payload of IP datagram is 161 - 20 bytes

- Q4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

Answer: No, because fragment offset is 0.



The screenshot shows a Wireshark capture of network traffic. The packet list pane displays several packets, including ARP requests and ICMP Echo (ping) requests. The packet details pane for the selected packet (No. 9) shows the following fields:

- Version: 4
- Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 161
- Identification: 0xc623 (50723)
- Flags: 0x00
- Fragment Offset: 0
- Time to Live: 1
- Protocol: UDP (17)
- Header Checksum: 0x6f73 [validation disabled]
- [Header checksum status: Unverified]

- Q5: Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

Answer: It is header checksum and time to live

ip-ethereal-trace-1

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

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

No.

Time

Source

Destination

Protocol

Length

Info

4...

192.168.1.100

192.168.1.1

SSDP

174

M-SEARCH * HTTP/1.1

5...

192.168.1.100

192.168.1.1

SSDP

175

M-SEARCH * HTTP/1.1

6...

192.168.1.100

192.168.1.1

SSDP

174

M-SEARCH * HTTP/1.1

7...

192.168.1.100

192.168.1.1

SSDP

175

M-SEARCH * HTTP/1.1

8...

192.168.1.102

128.59.23.100

ICMP

98

Echo (ping) request id=0x0300, seq=20483/848

9...

10.216.228.1

192.168.1.102

ICMP

70

Time-to-live exceeded (Time to live exceeded)

...

192.168.1.102

128.59.23.100

ICMP

98

Echo (ping) request id=0x0300, seq=20739/849

...

24.218.0.153

192.168.1.102

ICMP

70

Time-to-live exceeded (Time to live exceeded)

...

192.168.1.102

128.59.23.100

ICMP

98

Echo (ping) request id=0x0300, seq=20995/850

...

24.128.190.197

192.168.1.102

ICMP

70

Time-to-live exceeded (Time to live exceeded)

...

192.168.1.102

128.59.23.100

ICMP

98

Echo (ping) request id=0x0300, seq=21251/851

Identification: 0x32d0 (13008)

> Flags: 0x00

Fragment Offset: 0

> Time to Live: 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

Fragment offset (13 bits) (ip frag offset), 2 bytes

Packets: 380 · Displayed: 380 (100.0%)

Profile: Default

ip-ethereal-trace-1

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

- Q6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Answer:

- +Fields stay constant: IP version, Length of header, Source IP address, Destination IP address, Upper Layer Protocol
- +Fields must stay constant: Same as Fields stay constant
- +Fields must change: Header Checksum, Time to live, Identification

- Q7. Describe the pattern you see in the values in the Identification field of the IP datagram

Answer: Pattern: Identification field increases by one each echo request

ip-ethereal-trace-1

File

Edit

View

Go

Capture

Analyze

Statistics

Telephony

Wireless

Help

Apply a display filter ... <Ctrl>F

No.

Time

Source

Destination

Protocol

Length

Info

5 ...

192.168.1.100

192.168.1.1

SSDP

175

M-SEARCH * HTTP/1.1

6 ...

192.168.1.100

192.168.1.1

SSDP

174

M-SEARCH * HTTP/1.1

7 ...

192.168.1.100

192.168.1.1

SSDP

175

M-SEARCH * HTTP/1.1

8 ...

192.168.1.102

128.59.23.100

ICMP

98

Echo (ping) request id=0x0300, seq=20483/848

9 ...

10.216.228.1

192.168.1.102

ICMP

70

Time-to-live exceeded (Time to live exceeded)

...

192.168.1.102

128.59.23.100

ICMP

98

Echo (ping) request id=0x0300, seq=20739/849

...

24.218.0.153

192.168.1.102

ICMP

70

Time-to-live exceeded (Time to live exceeded)

...

192.168.1.102

128.59.23.100

ICMP

98

Echo (ping) request id=0x0300, seq=20995/850

...

24.128.190.197

192.168.1.102

ICMP

70

Time-to-live exceeded (Time to live exceeded)

...

192.168.1.102

128.59.23.100

ICMP

98

Echo (ping) request id=0x0300, seq=21251/851

...

24.128.0.101

192.168.1.102

ICMP

70

Time-to-live exceeded (Time to live exceeded)

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, 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

ip-ethereal-trace-1

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

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

</

- Q8. What is the value in the Identification field and the TTL field?

Answer: Identification: 0x32d1 (13009). Time to live: 2

| | | | | | |
|------|----------------|---------------|------|-----|---|
| 6... | 192.168.1.100 | 192.168.1.1 | SSDP | 174 | M-SEARCH * HTTP/1.1 |
| 7... | 192.168.1.100 | 192.168.1.1 | SSDP | 175 | M-SEARCH * HTTP/1.1 |
| 8... | 192.168.1.102 | 128.59.23.100 | ICMP | 98 | Echo (ping) request id=0x0300, seq=20483/848 |
| 9... | 10.216.228.1 | 192.168.1.102 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| ... | 192.168.1.102 | 128.59.23.100 | ICMP | 98 | Echo (ping) request id=0x0300, seq=20739/849 |
| ... | 24.218.0.153 | 192.168.1.102 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| ... | 192.168.1.102 | 128.59.23.100 | ICMP | 98 | Echo (ping) request id=0x0300, seq=20995/850 |
| ... | 24.128.190.197 | 192.168.1.102 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| ... | 192.168.1.102 | 128.59.23.100 | ICMP | 98 | Echo (ping) request id=0x0300, seq=21251/851 |

0100 = Version: 4

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

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

Total Length: 84

Identification: 0x32d1 (13009)

Flags: 0x00

Fragment Offset: 0

Time to live: 2

Protocol: ICMP (1)

Header Checksum: 0x2c2b [validation disabled]

- Q9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

Answer:

- The values of identification field changes for all the ICMP TTL-exceeded replies since the identification field is a unique value. If two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram.
- The TTL field was unchanged since the TTL for the nearest router is always the same

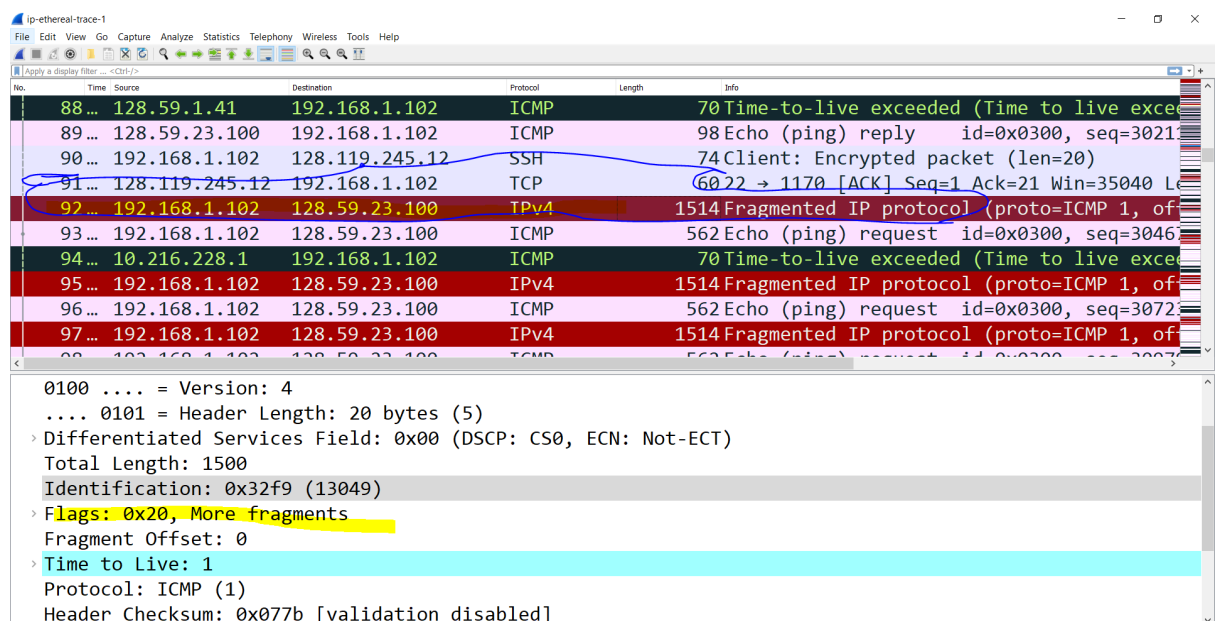
3. Fragmentation

- Q10: 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

ipethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.3]

Answer: No.92 message has been fragmented across more than one IP datagram (in No.93).



The image shows a Wireshark packet capture window titled 'ip-ethereal-trace-1'. The packet list pane shows several packets. Packet 92 is an ICMP Echo (ping) request from 192.168.1.102 to 128.59.23.100. Packet 93 is a fragmented IP datagram (protocol=ICMP 1) from 192.168.1.102 to 128.59.23.100. Packet 94 is another ICMP Echo (ping) request from 192.168.1.102 to 128.59.23.100. Packet 95 is a fragmented IP datagram (protocol=ICMP 1) from 192.168.1.102 to 128.59.23.100. Packet 96 is another ICMP Echo (ping) request from 192.168.1.102 to 128.59.23.100. Packet 97 is a fragmented IP datagram (protocol=ICMP 1) from 192.168.1.102 to 128.59.23.100. The packet details pane for packet 93 shows the following information:

```

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
Fragment Offset: 0
> Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x077b [validation disabled]

```

ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|------|----------------|----------------|----------|--------|--|
| 89... | | 128.59.23.100 | 192.168.1.102 | ICMP | 98 | Echo (ping) reply id=0x0300, seq=3021 |
| 90... | | 192.168.1.102 | 128.119.245.12 | SSH | 74 | Client: Encrypted packet (len=20) |
| 91... | | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0 |
| 92... | | 192.168.1.102 | 128.59.23.100 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, offset=1480) |
| 93... | | 192.168.1.102 | 128.59.23.100 | ICMP | 562 | Echo (ping) request id=0x0300, seq=3046 |
| 94... | | 10.216.228.1 | 192.168.1.102 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| 95... | | 192.168.1.102 | 128.59.23.100 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, offset=1480) |
| 96... | | 192.168.1.102 | 128.59.23.100 | ICMP | 562 | Echo (ping) request id=0x0300, seq=3072 |
| 97... | | 192.168.1.102 | 128.59.23.100 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, offset=1480) |
| 98... | | 192.168.1.102 | 128.59.23.100 | ICMP | 562 | Echo (ping) request id=0x0300, seq=3097 |

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 548
 Identification: 0x32f9 (13049)
 > Flags: 0x00
 Fragment Offset: 1480
 > Time to Live: 1
 Protocol: ICMP (1)
 Header Checksum: 0x2a7a [validation disabled]

- Q11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram has 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?

Answer: First fragment:

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

Fragment Offset: 0

Time to Live: 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]

- Q12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?

Answer: Second fragment:

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: 548

Identification: 0x32f9 (13049)

Flags: 0x00

Fragment Offset: 1480

Time to Live: 1

Protocol: ICMP (1)

Header Checksum: 0x2a7a [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.102

Destination Address: 128.59.23.100

[2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]

=> No more fragments because flags are now 0. This is not the first fragment but is the last one

- Q13. What fields change in the IP header between the first and second fragment?

Answer:

- Total length: 1500 -> 548
- flags: 0x20 -> 0x00
- fragment offset: 0 -> 1480
- checksum: 0x077b -> 0x2a7a

- Q14. How many fragments were created from the original datagram?

Answer: 3 fragments were created from the original datagram

| | | | | |
|--------|---------------|---------------|------|---|
| 269... | 128.59.23.100 | 192.168.1.102 | ICMP | 582 Echo (ping) reply id=0x0300, seq=4352 |
| 270... | 128.59.23.100 | 192.168.1.102 | IPv4 | 1514 Fragmented IP protocol (proto=ICMP 1, of |
| 271... | 192.168.1.102 | 128.59.23.100 | IPv4 | 1514 Fragmented IP protocol (proto=ICMP 1, of |
| 272... | 192.168.1.102 | 128.59.23.100 | IPv4 | 1514 Fragmented IP protocol (proto=ICMP 1, of |
| 273... | 192.168.1.102 | 128.59.23.100 | ICMP | 582 Echo (ping) request id=0x0300, seq=4377 |
| 274... | 10.216.228.1 | 192.168.1.102 | ICMP | 70 Time-to-live exceeded (Time to live exce |
| 275... | 192.168.1.102 | 128.59.23.100 | IPv4 | 1514 Fragmented IP protocol (proto=ICMP 1, of |
| 276... | 192.168.1.102 | 128.59.23.100 | IPv4 | 1514 Fragmented IP protocol (proto=ICMP 1, of |
| 277... | 192.168.1.102 | 128.59.23.100 | ICMP | 582 Echo (ping) request id=0x0300, seq=4403 |
| 278... | 192.168.1.102 | 128.59.23.100 | IPv4 | 1514 Fragmented IP protocol (proto=ICMP 1, of |
| 279... | 192.168.1.102 | 128.59.23.100 | IPv4 | 1514 Fragmented IP protocol (proto=ICMP 1, of |

> Frame 271: 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: 0x3330 (13104)
 > Flags: 0x20, More fragments
 Fragment Offset: 0

- Q15. What fields change in the IP header among the fragments?

Answer: Fragment offset (0->1480->2960), checksum(0x0744->0x068b0->0x2976)