

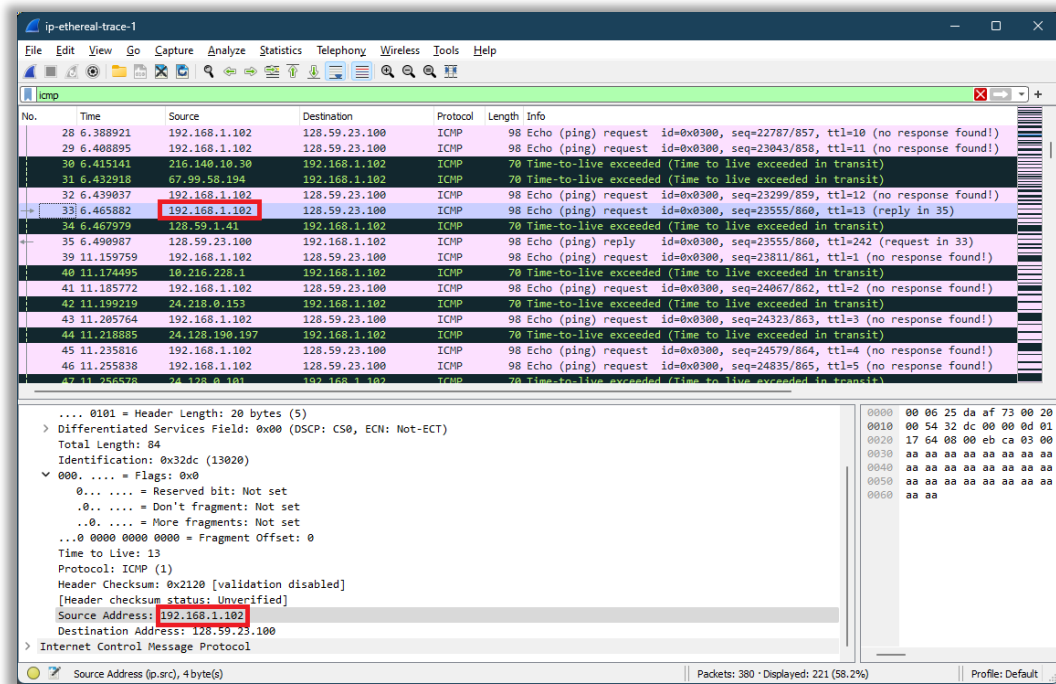
Wireshark Lab 06 - IP v7.0

Igor Augusto Reis Gomes – 12011BSI290 – igor.augusto@ufu.br

Heitor Guimarães Da Fonseca Filho – 12011BSI203 – heitor.filho@ufu.br

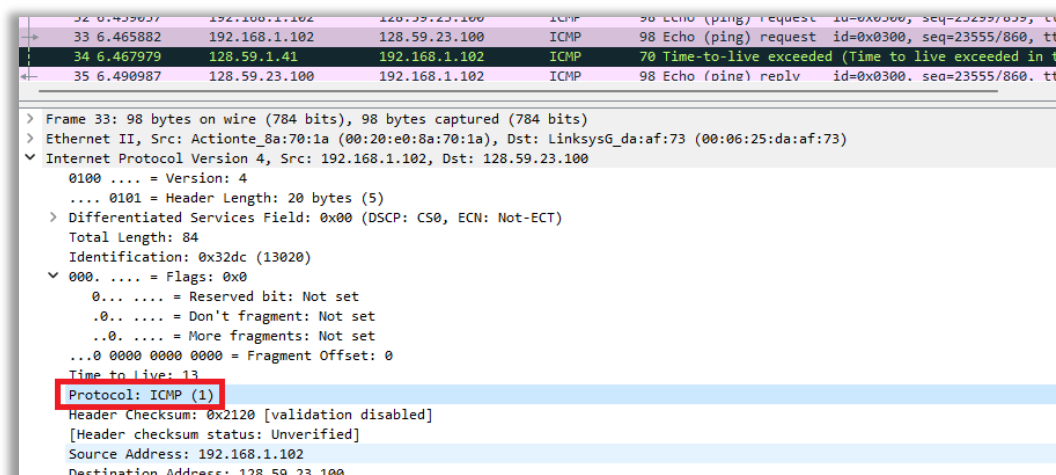
- 1) Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

O endereço de IP do arquivo de exemplo é 192.168.1.102, o meu é 192.168.12.1.



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

O valor no campo de protocolo da camada superior é: ICMP (1).



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.

O cabeçalho IP tem tamanho de 20 bytes, e 84 de tamanho total, resultando em uma carga útil (payload) de 64 bytes do datagrama IP, ou seja, Total Length – Header Length.

No.	Time	Source	Destination	Protocol	Length	Info
30	6.415141	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
31	6.432918	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
32	6.439037	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=23299/859, ttl=12 (no response)
33	6.465882	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=23555/860, ttl=13 (reply to 32)
34	6.467979	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
35	6.490987	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=23555/860, ttl=242 (request 33)

> Frame 33: 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: 0x32dc (13020)

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

Esse datagrama IP não está fragmentado. É possível determinar com o sinalizador (flag) “More fragments”, se não estiver definido, o datagrama não será fragmentado, caso contrário, será fragmentado.

33	6.465882	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=23555/860, ttl=13 (reply to 32)
34	6.467979	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
35	6.490987	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=23555/860, ttl=242 (request 33)
39	11.159759	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=23811/861, ttl=13 (reply to 38)
40	11.174495	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

> Frame 33: 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: 0x32dc (13020)
> 0000 = 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: 13

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?

Os campos os quais sempre mudam são: identificação (*Identification*), tempo de vida (*Time to live*) e verificação de soma de cabeçalho (*Header checksum*).

8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=12 (no response)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=13 (reply to 9)
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=12 (no response)
13	6.234505	24.128.190.197	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)
> 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)
> 0000 = 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
Protocol: 1 (ICMP)
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

8	6.163045	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=20483/848, t
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=20739/849, t
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=20995/850, t
13	6.234505	24.128.190.197	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in


```

> Frame 10: 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: 0x32d1 (13009)
  > 0000 .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 = Fragment Offset: 0
  > Time to Live: 2
  Protocol: ICMP (1)
  Header Checksum: 0x2c2b [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.102
  Destination Address: 128.59.23.100
  > Internet Control Message Protocol

```

6) Which fields stay constant? Which of the fields must stay constant? Why?

Os campos que permanecem e devem permanecer constantes são:

- Version, pois estamos usando IPv4 para todos os pacotes.
- Header Length, pois esses pacotes são ICMP.
- Source Address (IP), pois estamos mandando da mesma origem.
- Destination Address (IP), pois estamos mandando para o mesmo destino.
- Differentiated Services, pois dado que todos os pacotes são since all packets are ICMP eles usam a mesma classe Type of Service).
- Upper Layer Protocol, pois esses pacotes são ICMP.

No.	Time	Source	Destination	Protocol	Length	Info
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, t
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in t
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, t
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in t
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, t
13	6.234505	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in t


```

> Frame 10: 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: 0x32d1 (13009)
  > 0000 .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 = Fragment Offset: 0
  > Time to Live: 2
  Protocol: ICMP (1)
  Header Checksum: 0x2c2b [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.102
  Destination Address: 128.59.23.100
  > Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0

```

Which fields must change? Why?

Os campos que devem mudar são:

- Identification, pois os pacotes devem ter ids diferentes.
- Time to live, pois o traceroute incrementa cada pacote subsequente.
- Header checksum, pois a verificação de soma do cabeçalho deve mudar à medida que o cabeçalho é alterado.

*economizando print, pois o da questão 5 já serve para essa parte.

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

Percebo que valor deste campo é incrementado por 1 (um) a cada ICMP Echo (ping) request:

Pacote 8: Identification: 0x32d0 (13008)

Pacote 9: Identification: 0x32d1 (13009)

Pacote 10: Identification: 0x32d2 (13010)

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

Identification: 0xa60b (42507)

Time to Live: 244

No.	Time	Source	Destination	Protocol	Length	Info
128	29.140439	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live excee
169	34.147910	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live excee
211	39.164169	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live excee
265	44.655324	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live excee
321	49.827260	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live excee
376	54.659995	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live excee

> Frame 321: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

> 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: 67.99.58.194, Dst: 192.168.1.102

0100 = Version: 4

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

> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)

Total Length: 56

Identification: 0xa5e3 (42467)

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: 244

Protocol: ICMP (1)

Header Checksum: 0xdfed [validation disabled]

[Header checksum status: Unverified]

Source Address: 67.99.58.194

Destination Address: 192.168.1.102

> Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)

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?

Como é possível observar na captura de tela abaixo, o campo de identificação muda para todas as respostas ICMP TTL excedidas porque o campo de identificação é um valor exclusivo. Dessa forma, quando dois ou mais datagramas IP têm o mesmo valor de identificação, isso significa que esses datagramas IP são fragmentos de um único datagrama IP grande.

O campo TTL permanece inalterado porque o TTL do roteador de primeiro salto (first hop) é sempre o mesmo.

No.	Time	Source	Destination	Protocol	Length	Info
128	29.140439	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded)
169	34.147910	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded)
211	39.164169	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded)
265	44.655324	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded)
321	49.827260	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded)
376	54.659995	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded)

> Frame 321: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

> Ethernet II, Src: Linksys6 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: 67.99.58.194, Dst: 192.168.1.102

0100 = Version: 4

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

> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)

Total Length: 56

Identification: 0xa5e3 (42467)

0000 = 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: 244

Protocol: ICMP (1)

Header Checksum: 0xdf [validation disabled]

[Header checksum status: Unverified]

Source Address: 67.99.58.194

Destination Address: 192.168.1.102

Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)

10) 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?

Sim, esse pacote foi fragmentado em mais de um datagrama IP.

[illegible]

11) Print out the first fragment of the fragmented IP datagram.

```
No.    Time    Source          Destination      Protocol  Length  Info
---
88 16.468603 128.59.1.41     192.168.1.102   ICMP      70      Time-to-live exceeded (Time to live exceeded in transit)
89 16.499919 128.59.23.100   192.168.1.102   ICMP      98      Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (request in 87)
90 22.928093 192.168.1.102   128.119.245.12  SSH       74      Client: Encrypted packet (len=20)
91 22.952738 128.119.245.12  192.168.1.102   TCP       60      22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
92 28.441511 192.168.1.102   128.59.23.100   IPv4      1514     Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93 28.442185 192.168.1.102   128.59.23.100   ICMP      562      Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)
94 28.462264 10.216.228.1    192.168.1.102   ICMP      70      Time-to-live exceeded (Time to live exceeded in transit)

> Frame 92: 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: 0x32f9 (13049)
  > 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
  > 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]
  Data (1480 bytes)
  [Length: 1480]
  Data: 0800d0c603007703373620aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa..
```

What information in the IP header indicates that the datagram been fragmented?

O sinalizador (flag) *more fragments* indica se o datagrama foi fragmentado ou não, sendo que neste caso está com valor 1 de bit definido, isto é, está fragmentado.

What information in the IP header indicates whether this is the first fragment versus a latter fragment?

É indicado pelo campo *Fragment offset*, sendo que está definido como 0, indicando que este é o primeiro fragmento.

How long is this IP datagram?

O datagrama IP tem tamanho de 1480 bytes.

12) 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?

É possível afirmar que este não é o primeiro fragmento dado já que o deslocamento do fragmento (*Fragment offset*) é 1480. É o último fragmento, já que o sinalizador (*flag*) de mais fragmentos (*More fragments*) não está definido.

```
No.    Time    Source          Destination      Protocol  Length  Info
---
91 22.952738 128.119.245.12  192.168.1.102   TCP       60      22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
92 28.441511 192.168.1.102   128.59.23.100   IPv4      1514     Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93 28.442185 192.168.1.102   128.59.23.100   ICMP      562      Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)
94 28.462264 10.216.228.1    192.168.1.102   ICMP      70      Time-to-live exceeded (Time to live exceeded in transit)
95 28.470668 192.168.1.102   128.59.23.100   IPv4      1514     Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
96 28.471338 192.168.1.102   128.59.23.100   ICMP      562      Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response found!)

> Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 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: 548
    Identification: 0x32f9 (13049)
  > 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
  > 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)]
  [Frame: 92, payload: 0-1479 (1480 bytes)]
  [Frame: 93, payload: 1480-2007 (528 bytes)]
  [Fragment count: 2]
  [Reassembled IPv4 length: 2008]
  [Reassembled IPv4 data: 0800d0c603007703373620aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa..]
```

13) What fields change in the IP header between the first and second fragment?

Os campos que mudam entre o primeiro e segundo fragmento são:

- Total length.
- Flags (*More fragments*).
- Fragment offset
- Checksum.

Primeiro pacote:

```
92 28.441511 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93 28.442185 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)

> Frame 92: 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: 0x32f9 (13049)
  > 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
  > 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
```

Segundo pacote:

```
92 28.441511 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93 28.442185 192.168.1.102 128.59.23.100 ICMP 562 Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)

> Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 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: 548
    Identification: 0x32f9 (13049)
  > 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
  > 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
```

14) How many fragments were created from the original datagram?

Ao usar tamanho de pacote 3500, foram criados 3 fragmentos a partir do datagrama original.

```
No. Time Source Destination Protocol Length Info
212 39.227649 128.59.1.41 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
214 39.322566 128.59.23.100 192.168.1.102 ICMP 562 Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in 205)
218 43.467629 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219 43.485786 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)

> 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
  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)]
  [Frame: 216, payload: 0-1479 (1480 bytes)]
  [Frame: 217, payload: 1480-2959 (1480 bytes)]
  [Frame: 218, payload: 2960-3507 (548 bytes)]
  [Fragment count: 3]
  [Reassembled IPv4 length: 3508]
```


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

Os campos do cabeçalho IP que mudaram entre todos os três fragmentos foram:

- Total length: mudança entre os dois primeiros pacotes (dado que ambos possuem o mesmo número) e o último. Ambos possuem tamanho total de 1500, já o último é de 568.
- Flags (*More fragments*): os dois primeiros estão com valor 1, já o último está com 0.
- Fragment offset: 0, 1480 e 2960, no primeiro, segundo e terceiro, respectivamente.
- Checksum: 0x0751 (1873), 0x0698 (1688) e 0x2983 (10627), respectivamente

Primeiro pacote:

```
216 43.466136 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217 43.466808 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218 43.467629 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)

> Frame 216: 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: 0x3323 (13091)
  > 001. .... = Flags: 0x1, More fragments
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
    ...0 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x0751 [validation disabled]
  [Header checksum status: Unverified]
```

Segundo pacote:

```
216 43.466136 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217 43.466808 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218 43.467629 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)

> Frame 217: 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: 0x3323 (13091)
  > 001. .... = Flags: 0x1, More fragments
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
    ...0 0000 1011 = Fragment Offset: 1480
  > Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x0698 [validation disabled]
  [Header checksum status: Unverified]
```

Terceiro pacote:

```
216 43.466136 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217 43.466808 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218 43.467629 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)

> Frame 218: 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: 0x3323 (13091)
  > 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
  Protocol: ICMP (1)
  Header Checksum: 0x2983 [validation disabled]
  [Header checksum status: Unverified]
```