

Universidade Federal de Uberlândia – UFU

Bacharelado em Sistemas de Informação - Campus Monte Carmelo

GS1524 - Redes de computadores - 2021/1

RENAN JUSTINO REZENDE SILVA - 11921BSI223

Atividade 7 IP

- O objetivo desta atividade é entender melhor o protocolo IP. Leia o texto e execute os passos que estão no arquivo (Wireshark IP.pdf). Durante os passos no arquivo, serão indicados itens para serem respondidos. As perguntas a seguir referem-se à atividade no arquivo (Wireshark IP.pdf).

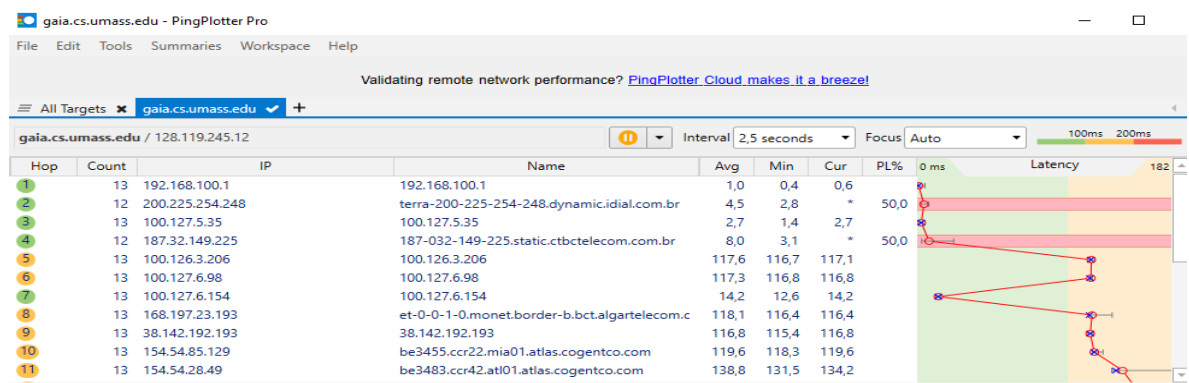


Figura 1: pingplotter gaia.cs.umass.edu

1. Selecione a primeira mensagem de solicitação de eco ICMP enviada pelo seu computador e expanda a parte do protocolo da Internet do pacote na janela de detalhes do pacote. Qual é o endereço IP do seu computador?

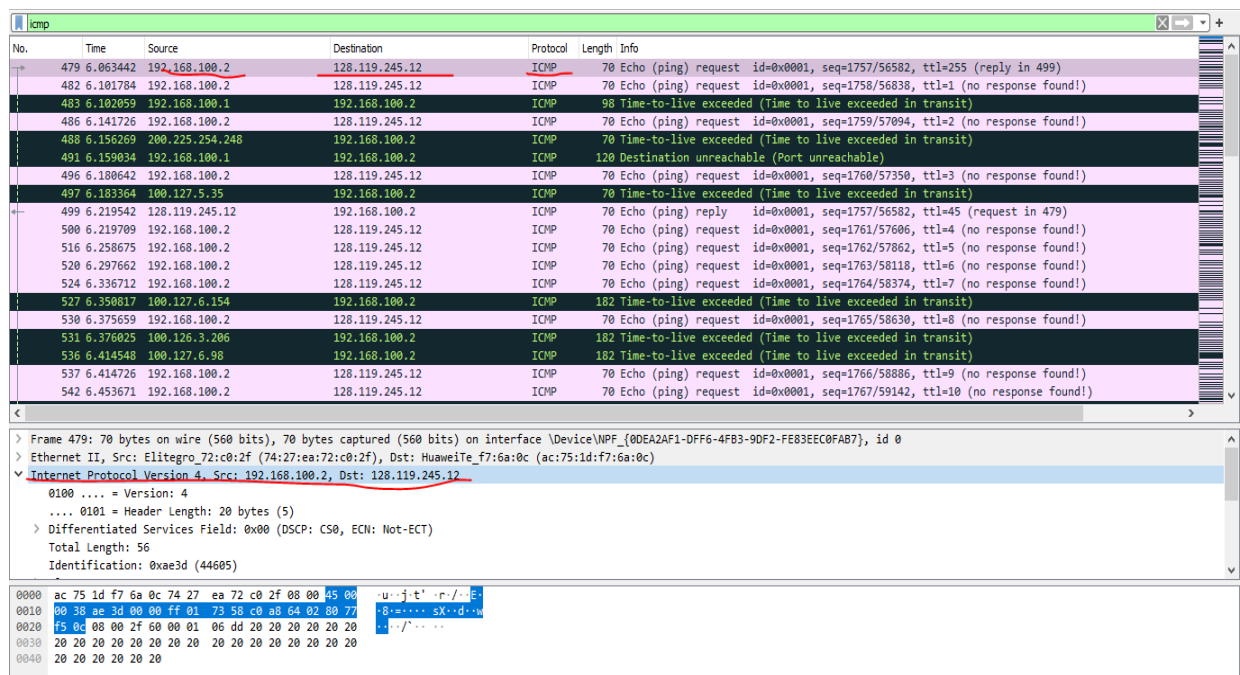


Figura 2: Endereço meu computador, mensagem ICMP ECO

R = O endereço IP do meu computador é 192.168.100.2

2. Dentro do cabeçalho do pacote IP, qual é o valor no campo do protocolo da camada

superior?

```
Internet Protocol Version 4, Src: 192.168.100.2, Dst: 128.119.245.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 56
  Identification: 0xae3d (44605)
  Flags: 0x00
    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: 255
  Protocol: ICMP (1)
```

Figura 3: Protocol field ICMP

R = Protocolo ICMP (1).

3. Quantos bytes existem no cabeçalho IP? Quantos bytes existem na carga útil do datagrama IP? Explique como você determinou o número de bytes de carga útil.

```
Internet Protocol Version 4, Src: 192.168.100.2, Dst: 128.119.245.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 56
  Identification: 0xae3d (44605)
  Flags: 0x00
    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: 255
  Protocol: ICMP (1)
  Header Checksum: 0x7258 [validation disabled]

0000  ac 75 1d f7 6a 0c 74 27 ea 72 c0 2f 08 00 45 00  .u..j..t'..r../..E.
0010  00 38 ae 3d 00 00 ff 01 73 58 c0 a8 64 02 80 77  .8.=.....sX..d..w
0020  f5 0c 08 00 2f 60 00 01 06 dd 20 20 20 20 20 20  ..../^.....
```

Figura 4: Datagrama IP

R = Existem 20 bytes no cabeçalho IP, pelo header length e inspecionando o IP. O total length equivale a 56 bytes total, então $56 - 20 = 36$ bytes de payload ou carga útil do datagrama IP.

4. Este datagrama IP foi fragmentado? Explique como você determinou se o datagrama foi fragmentado ou não.

```
Internet Protocol Version 4, Src: 192.168.100.2, Dst: 128.119.245.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 56
  Identification: 0xae3d (44605)
  Flags: 0x00
    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: 255
  Protocol: ICMP (1)
  Header Checksum: 0x7258 [validation disabled]

0000  ac 75 1d f7 6a 0c 74 27 ea 72 c0 2f 08 00 45 00  .u..j..t'..r../..E.
0010  00 38 ae 3d 00 00 ff 01 73 58 c0 a8 64 02 80 77  .8.=.....sX..d..w
0020  f5 0c 08 00 2f 60 00 01 06 dd 20 20 20 20 20 20  ..../^.....
```

Figura 5: Fragment Offset 0

R = O datagrama IP não foi fragmentado. Pois o Fragment Offset está setado em 0.

5. Quais campos no datagrama IP sempre mudam de um datagrama para o próximo dentro desta série de mensagens ICMP enviadas pelo seu computador?

```

> Frame 483: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{0DEA2AF1-DFF6-4FB3-9DF2-FE83EEC0FAB7}, id
> Ethernet II, Src: HuaweiTe_f7:6a:0c (ac:75:1d:f7:6a:0c), Dst: Elitegro_72:c0:2f (74:27:ea:72:c0:2f)
> Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.100.2
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    1100 00.. = Differentiated Services Codepoint: Class Selector 6 (48)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 84
  Identification: 0x5a68 (23144)
  > Flags: 0x00
    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: 64
  Protocol: ICMP (1)
  Header Checksum: 0xd63e (validation disabled)
0010 00 54 5a 68 00 00 40 01 d6 2c c0 a8 64 01 c0 a8 72 c0 2f 74 27 ea 72 c0 2f
0020 64 02 0b 00 f4 ff 00 00 00 00 45 00 00 38 ae 3e d.....E..8>
0030 00 00 01 01 71 58 c0 a8 64 02 80 77 f5 0c 08 00 ....qX..d..w...

```

Figura 6: Outro frame IP

R = Os campos que sempre mudam são: TTL (time to live), Identification que é o código de identificação e o header checksum que é o cabeçalho da soma de verificação.

6. Quais campos permanecem constantes? Qual dos campos deve permanecer constante? Quais campos devem ser alterados? Por quê?

R = De acordo com as imagens já postadas e com outros frames, os campos que permanecem constantes são: Versão (IPV4), header length que é 20 bytes, IP de Origem (Source), IP de destino (Destination), e o ICMP protocolo. Os campos que devem permanecer constante são os mesmos pois não pode alterar. Os campos que devem ser alterados são: Identificação pois os pacotes precisam ser verificados e os números são diferentes, header checksum pois os cabeçalhos mudam e então as somas são alteradas.

7. Descreva o padrão que você vê nos valores no campo Identification do datagrama IP.

483	6.102059	192.168.100.1	192.168.100.2	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)
486	6.141726	192.168.100.2	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=1759/57094, ttl=2 (no response)
488	6.156269	200.225.254.248	192.168.100.2	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
491	6.159034	192.168.100.1	192.168.100.2	ICMP	120 Destination unreachable (Port unreachable)
496	6.180642	192.168.100.2	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=1760/57350, ttl=3 (no response)
497	6.183364	100.127.5.35	192.168.100.2	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
499	6.219542	128.119.245.12	192.168.100.2	ICMP	70 Echo (ping) reply id=0x0001, seq=1757/56582, ttl=45 (request ir)
500	6.219709	192.168.100.2	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=1761/57606, ttl=4 (no response)
516	6.258675	192.168.100.2	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=1762/57862, ttl=5 (no response)
520	6.297662	192.168.100.2	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=1763/58118, ttl=6 (no response)


```

0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 56
Identification: 0xae3f (44607)

```

Figura 7: Identification

R = A cada frame de ping ECHO request, o campo identification foi incrementando em 1, estava em 44605, depois 44606 e neste printado em 44607.

8. Qual é o valor no campo Identificação e no campo TTL?

483	6.102059	192.168.100.1	192.168.100.2	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)
486	6.141726	192.168.100.2	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=1759/57094, ttl=2 (no response found!)
488	6.156369	200.225.254.248	192.168.100.2	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
491	6.159034	192.168.100.1	192.168.100.2	ICMP	120 Destination unreachable (Port unreachable)
496	6.180642	192.168.100.2	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=1760/57350, ttl=3 (no response found!)
497	6.183364	100.127.5.35	192.168.100.2	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
499	6.219542	128.119.245.12	192.168.100.2	ICMP	70 Echo (ping) reply id=0x0001, seq=1757/56582, ttl=45 (request in 479)
500	6.219709	192.168.100.2	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=1761/57606, ttl=4 (no response found!)
516	6.258675	192.168.100.2	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=1762/57862, ttl=5 (no response found!)
520	6.297662	192.168.100.2	128.119.245.12	ICMP	70 Echo (ping) request id=0x0001, seq=1763/58118, ttl=6 (no response found!)

1100	00.. = Differentiated Services Codepoint: Class Selector 6 (48)
....	00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length:	84
Identification:	0x5a68 (23144)
Flags:	0x00
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:	64
Protocol:	ICMP (1)
Header Checksum:	0xd62c [validation disabled]
[Header checksum status:	Unverified]
Source Address:	192.168.100.1
Destination Address:	192.168.100.2
Internet Control Message Protocol	
Type:	11 (Time-to-live exceeded)
Code:	0 (Time to live exceeded in transit)
0	00 54 5a 68 00 00 40 01 d6 2c c0 a8 64 01 c0 a8
0	64 02 0b 00 f4 ff 00 00 00 00 45 00 00 38 ae 3e
0	00 00 01 01 71 58 c0 a8 64 02 80 77 f5 0c 00 00

Figura 8: TTL e Identificação

R = O valor do campo identificação é 23144 e o TTL (Time to Live) de 64 para a mensagem TTL-exceeded.

9. Esses valores permanecem inalterados para todas as respostas ICMP TTL-exceeded enviadas ao seu computador pelo roteador mais próximo (primeiro salto)? Por quê?

R = O campo de identificação é diferente para todas as respostas ICMP de TTL, tempo excedido, pois o campo de identificação é único. Se dois datagramas possuírem este mesmo valor, então são fragmentos de um de um único maior. O campo TTL não altera pois o TTL do roteador do primeiro salto é sempre o mesmo.

10. Encontre a primeira mensagem ICMP Echo Request que foi enviada pelo seu computador depois que você alterou o tamanho do pacote no pingplotter para 2000. Essa mensagem foi fragmentada em mais de um datagrama IP? [Nota: se você achar que seu pacote não foi fragmentado, você deve baixar o arquivo ip-ethereal-trace-1. Se o seu computador tiver uma interface Ethernet, um tamanho de pacote de 2.000 deve causar fragmentação.]

85	16.438258	67.99.58.194	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
86	16.443310	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (no response found!)
87	16.463382	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (reply in 89)
88	16.468693	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)
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!)
97	28.490663	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
98	28.491323	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found!)
99	28.520729	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #100]
100	28.521393	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id=0x0300, seq=31235/890, ttl=4 (no response found!)
101	28.530213	24.218.0.153	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
102	28.540758	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fd) [Reassembled in #103]
103	28.541476	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id=0x0300, seq=31491/891, ttl=5 (no response found!)

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
...0	0101 1100 1000 = Fragment Offset: 1480
Time to Live:	1
Protocol:	ICMP (1)
Header Checksum:	0x2a7a [validation disabled]
[Header checksum status:	Unverified]

Figura 9: ICMP Echo Request

R = Sim, fragmentada em mais de um.

11. Imprima o primeiro fragmento do datagrama IP fragmentado. Quais informações no cabeçalho IP indicam que o datagrama foi fragmentado? Quais informações no cabeçalho IP indicam se este é o primeiro fragmento versus um fragmento posterior? Qual a extensão deste datagrama IP?

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!)
97	28.490663	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
98	28.491323	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found!)
99	28.520729	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #100]
100	28.521393	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=31235/890, ttl=4 (no response found!)
101	28.530213	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
102	28.540758	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fd) [Reassembled in #103]
103	28.541476	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=31491/891, ttl=5 (no response found!)
104	28.570848	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fe) [Reassembled in #105]
105	28.571603	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=31747/892, ttl=6 (no response found!)
106	28.590801	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32ff) [Reassembled in #107]


```

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
...0 0000 0000 0000 = Fragment Offset: 0

```



```

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00  ..%..s..p...E:
0010 05 dc 32 f9 20 00 01 01 07 7b c0 a8 01 66 80 3b  --2....{...f;
0020 17 64 08 00 d0 c6 03 00 77 03 37 36 20 aa aa aa  -d.....w76...

```

Figura 10: Fragmento info

R = As informações que indicam que houve fragmento: Fragment Offset, 2 IPV4 fragments. O primeiro fragmento possui fragment offset 0. O length tbm de 1480 para 2000 bytes. A extensão é de 1500 bytes, 1480 bytes + 20 do header (cabeçalho).

12. Imprima o segundo fragmento do datagrama IP fragmentado. Quais informações no cabeçalho IP indicam que este não é o primeiro fragmento de datagrama? São mais fragmentos? Como você sabe?

No.	Time	Source	Destination	Protocol	Length	Info
82	16.393260	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29443/883, ttl=10 (no response found!)
83	16.413273	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29699/884, ttl=11 (no response found!)
84	16.418067	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	16.438258	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	16.443310	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (no response found!)
87	16.463382	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (reply in 89)
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)
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!)
97	28.490663	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
98	28.491323	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found!)
99	28.520729	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #100]
100	28.521393	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=31235/890, ttl=4 (no response found!)


```

> Flags: 0x00
...0 0101 1100 1000 = Fragment Offset: 1480
> Time to Live: 1
> [Expert Info (Note/Sequence): "Time To Live" only 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)]

```



```

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00  ..%..s..p...E:
0010 02 24 32 f9 00 b9 01 01 2a 7a c0 a8 01 66 80 3b  --$2.....*z...f;

```

Figura 11: Fragmento 2 info

```

0... .... = Reserved bit: Not set
...0... .... = Don't fragment: Not set
...0... .... = More fragments: Not set

```

Figura 12: More fragments

R = Fragment Offset 1480, ou seja, o fragmento não é o primeiro. Ele é o último fragmento pois o more fragments não está setado.

13. Quais campos mudam no cabeçalho IP entre o primeiro e o segundo fragmento?

```

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

```

Figura 13: Fragmento 2 total length

```

[Expert Info (Note/Sequence): Time To Live on
Protocol: ICMP (1)
Header Checksum: 0x2a7a [validation disabled]
[Header checksum status: Unverified]

```

Figura 14: Fragmento 2 checksum

R = De acordo com as imagens dos fragmentos, os campos que mudam no cabeçalho IP entre o primeiro e segundo fragmento são: Total length, os flags que setam diferentes, pois um está more fragments outro não, fragment offset e o checksum.

14. Quantos fragmentos foram criados a partir do datagrama original?

[Length: 3500]

Figura 15: Fragmento contendo 3500

```

> [3 IPv4 Fragments (3508 bytes): #327(1480), #328(1480), #329(548)]
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
0010  02 38 33 3e 01 72 01 01 29 68 c0 a8 01 66 80 3b 83>...h...f;
0020  17 64 aa aa aa aa aa aa aa aa aa aa aa aa aa aa d.....
Frame (582 bytes)   Reassembled IPv4 (3508 bytes)
Header Checksum (ip.checksum), 2 byte(s)
Packets: 380 · Displayed: 380 (100.0%)

```

Figura 16: 3 fragments

R = Após mudar para 3500, 3 fragmentos foram criados a partir do datagrama original.

15. Quais campos mudam no cabeçalho IP entre os fragmentos?

```

.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 568
Identification: 0x333e (13118)
< Flags: 0x01
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
  ...0 1011 1001 0000 = Fragment Offset: 2960
< Time to Live: 1

```

Figura 17: Campos

```

Identification: 0x333e (13118)
< Flags: 0x20, More fragments
  0... .... = Reserved bit: Not set
  .0... .... = Don't fragment: Not set
  ..1. .... = More fragments: Set
  ...0 0101 1100 1000 = Fragment Offset: 1480
< Time to Live: 1
> [Expert Info (Note/Sequence): "Time To Live" only 1]
Protocol: ICMP (1)
Header Checksum: 0x067d [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[Reassembled IPv4 in frame: 329]
Data (1480 bytes)

```

Figura 18: Campos de outro fragmento exemplo

R = O fragment offset, de um está 2960, outro 1480 e outro 0. Checksum é diferente entre os fragmentos, o menor fragmento possui total length menor e não possui o more fragments setado enquanto os outros fragmentos possuem total length maior e o more fragments setado.