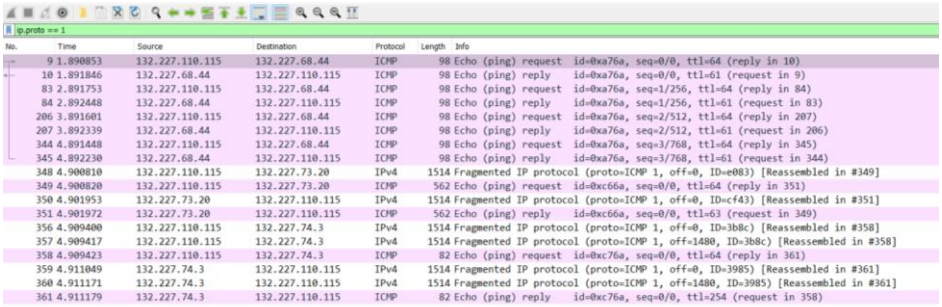
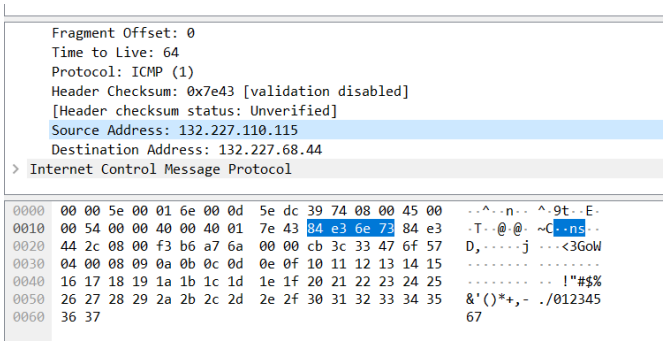
TP3

Julian BARKOUDEH

1) Ping et ICMP

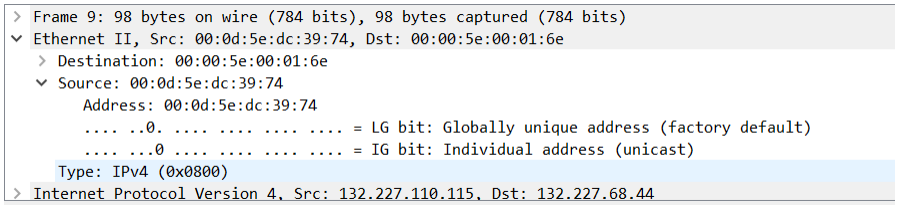


No.	Time	Source	Destination	Protocol	Length	Info
9	1.890853	132.227.110.115	132.227.68.44	ICMP	98	Echo (ping) request id=0xa76a, seq=0/0, ttl=64 (reply in 10)
10	1.891846	132.227.68.44	132.227.110.115	ICMP	98	Echo (ping) reply id=0xa76a, seq=0/0, ttl=61 (request in 9)
83	2.891753	132.227.110.115	132.227.68.44	ICMP	98	Echo (ping) request id=0xa76a, seq=1/256, ttl=64 (reply in 84)
84	2.892448	132.227.68.44	132.227.110.115	ICMP	98	Echo (ping) reply id=0xa76a, seq=1/256, ttl=61 (request in 83)
206	3.891601	132.227.110.115	132.227.68.44	ICMP	98	Echo (ping) request id=0xa76a, seq=2/512, ttl=64 (reply in 207)
207	3.892339	132.227.68.44	132.227.110.115	ICMP	98	Echo (ping) reply id=0xa76a, seq=2/512, ttl=61 (request in 206)
344	4.891448	132.227.110.115	132.227.68.44	ICMP	98	Echo (ping) request id=0xa76a, seq=3/768, ttl=64 (reply in 345)
345	4.892230	132.227.68.44	132.227.110.115	ICMP	98	Echo (ping) reply id=0xa76a, seq=3/768, ttl=61 (request in 344)
348	4.900810	132.227.110.115	132.227.73.20	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=e083) [Reassembled in #349]
349	4.900820	132.227.110.115	132.227.73.20	ICMP	562	Echo (ping) request id=0xc66a, seq=0/0, ttl=64 (reply in 351)
350	4.901953	132.227.73.20	132.227.110.115	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=cf43) [Reassembled in #351]
351	4.901972	132.227.73.20	132.227.110.115	ICMP	562	Echo (ping) reply id=0xc66a, seq=0/0, ttl=63 (request in 349)
356	4.909400	132.227.110.115	132.227.74.3	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3b8c) [Reassembled in #358]
357	4.909417	132.227.110.115	132.227.74.3	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3b8c) [Reassembled in #358]
358	4.909423	132.227.110.115	132.227.74.3	ICMP	82	Echo (ping) request id=0xc76a, seq=0/0, ttl=64 (reply in 361)
359	4.911049	132.227.74.3	132.227.110.115	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3985) [Reassembled in #361]
360	4.911171	132.227.74.3	132.227.110.115	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3985) [Reassembled in #361]
361	4.911179	132.227.74.3	132.227.110.115	ICMP	82	Echo (ping) reply id=0xc76a, seq=0/0, ttl=254 (request in 358)

1. En observant les résultats après avoir appliqué le filtre, on remarque que seules les requêtes faites en ICMP apparaissent. En effet, d'après les annexes, ce filtre consiste à afficher les protocoles avec le code 1, qui correspond bien au protocole ICMP.
2. En reprenant la commande effectuée, le paramètre « -c » permet de spécifier le nombre de paquets à envoyer. Dans ce cas 4 paquets sont envoyés. « Ufr-info-p6.jussieu.fr », cette partie concerne l'adresse IP auquel adresser les paquets.
3. 

```
    Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x7e43 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 132.227.110.115
    Destination Address: 132.227.68.44
> Internet Control Message Protocol
```

```
0000  00 00 5e 00 01 6e 00 0d  5e dc 39 74 08 00 45 00   ··^··n·· ^·9t··E·
0010  00 54 00 00 40 00 40 01  7e 43 84 e3 6e 73 84 e3   ·T··@·@· ~C··ns··
0020  44 2c 08 00 f3 b6 a7 6a  00 00 cb 3c 33 47 6f 57   D,·····j ···<3GoW
0030  04 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                             67
```

En sélectionnant la première requête, on peut en déduire que l'adresse IP source sur son réseau est « 132.227.110.115 », avec la partie « 132.227.110 »
4. L'adresse IP de la machine distante est de « 132.227.68.44 », on en déduite que les deux machines ne sont pas sur le même réseau.
5. 

```
> Frame 9: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
v Ethernet II, Src: 00:0d:5e:dc:39:74, Dst: 00:00:5e:00:01:6e
    > Destination: 00:00:5e:00:01:6e
    v Source: 00:0d:5e:dc:39:74
        Address: 00:0d:5e:dc:39:74
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 132.227.110.115, Dst: 132.227.68.44
```

En observant la case d'Ethernet, on remarque que l'adresse MAC est de « 00 :0d :5e : dc :39 :74 » ce qui correspon0d à l'adresse IP source.
6. L'adresse MAC de la destination est de « 00 :00 :5e :00 :01 :6e » qui correspond à l'adresse IP destination.

7.
```
Total Length: 84
Identification: 0x0000 (0)
> Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x7e43 [validation disabled]
[Header checksum status: Unverified]
```
D’après les annexes, la partie Flags de l’entête permet de déterminer si le message a été fragmenté ou pas. Dans ce cas, on remarque que le message n’a pas été fragmenté.

8.
```
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 132.227.110.115, Dst: 132.227.68.44
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x0000 (0)
```
En observant la case Internet Protcole, on en déduit que ma longueur de l’entête est de 20 octets.

```
Internet Protocol Version 4, Src: 132.227.68.44, Dst: 132.227.110.115
    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)
```

```
0000  00 0d 5e dc 39 74 00 00  5e 00 01 6e 08 00 45 00   ··^·9t·· ^··n··E·
0010  00 54 0f 59 00 00 3d 01  b1 ea 84 e3 44 2c 84 e3   ·T·Y··=· ····D,··
0020  6e 73 00 00 fb b6 a7 6a  00 00 cb 3c 33 47 6f 57   ns·····j ···<3GoW
0030  04 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                             67
```

En comptants le nombres d’octets présents dans l’entête IP (souligné en bleu), on compte aussi 20 octets. En plus l’entête se termine par l’adresse de destination (Avant la partie ICMP encadré en rouge), donc d’après les annexes il n’y pas d’options.

9.
```
Data (48 bytes)
    Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f20212223242526272
    [Length: 48]
```

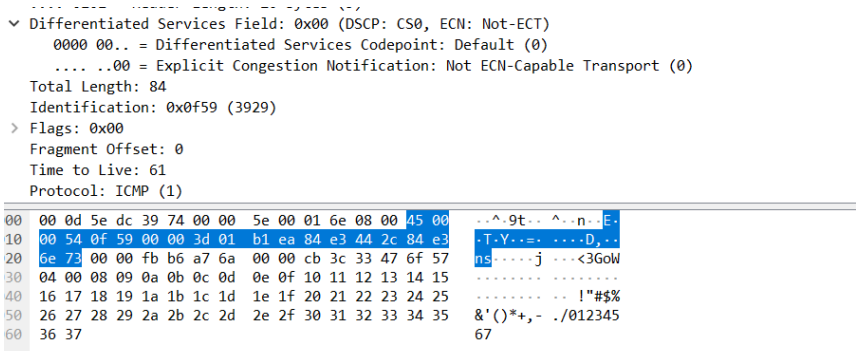
```
0000  00 00 5e 00 01 6e 00 0d  5e dc 39 74 08 00 45 00   ··^··n·· ^·9t··E·
0010  00 54 00 00 40 00 40 01  7e 43 84 e3 6e 73 84 e3   ·T··@·@· ~C··ns··
0020  44 2c 08 00 f3 b6 a7 6a  00 00 cb 3c 33 47 6f 57   D,·····j ···<3GoW
0030  04 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ·····  ·· ·····
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ·····  ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                             67
```

En sélectionnant la partie de Data, et en observant dans la case de ICMP, on remarque que le Data contient 64 octets.

10. En se basant sur les annexes, on remarque qu’il n’y que 8 octets. Donc, il n’y a pas d’options dans l’entête du message ICMP.

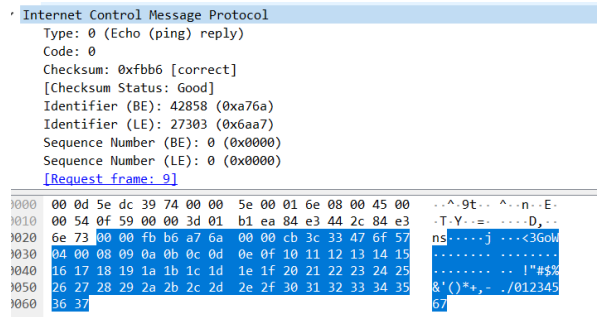
11. En regardant le manuel de la commande PING, on en déduit que les data de ICMP sont encapsuler dans une trame de 56 octets, avec 8 octets pour

l'entête. Donc 64 octets de partie ICMP. Or, dans notre cas nous avons 8 octets pour l'entête et 56 pour les données.



12.

L'entête IP pour la deuxième requête compte 20 octets.

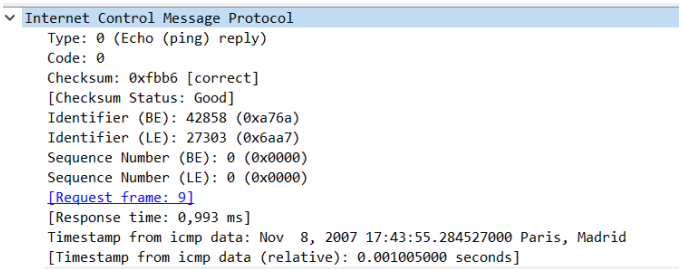


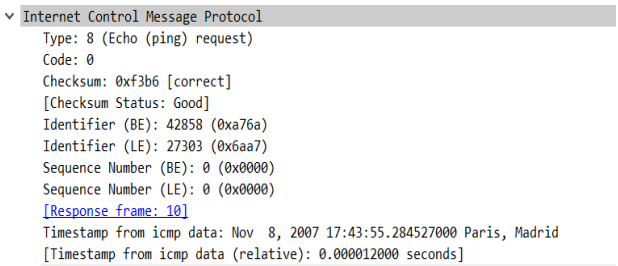
13.

En sélectionnant la partie ICMP, qui correspond à la partie Data de datagramme IP, on compte 64 octets.

14.

Replay Request





On remarque tout d'abord une différence dans la case Type, qui dans la réponse est de 0. Cela correspond d'après les annexes à Echo Reply. La case Code ne change pas, car il s'agit toujours du protocole ICMP. On remarque aussi que les Timestamp sont quasiment identiques.

15.

```
[Length: 48]
0000  00 0d 5e dc 39 74 00 00  5e 00 01 6e 08 00 45 00   ··^·9t·· ^··n··E·
0010  00 54 0f 59 00 00 3d 01  b1 ea 84 e3 44 2c 84 e3   ·T·Y··=· ····D,··
0020  6e 73 00 00 fb b6 a7 6a  00 00 cb 3c 33 47 6f 57   ns·····j ···<3GoW
0030  04 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                             67
```

```
0000  00 00 5e 00 01 6e 00 0d  5e dc 39 74 08 00 45 00   ··^··n·· ^·9t··E·
0010  00 54 00 00 40 00 40 01  7e 43 84 e3 6e 73 84 e3   ·T··@·@· ~C··ns··
0020  44 2c 08 00 f3 b6 a7 6a  00 00 cb 3c 33 47 6f 57   D,·····j ···<3GoW
0030  04 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                             67
```

En comparant les deux cases de data (Reply à gauche et Request à droite) , on remarque que les deux blocs sont exactement identiques. Ceci vient de la nature de la deuxième trame (Reply) qui consiste à renvoyer les paquets de données reçus par un utilisateur.

16.

Ententes IP :

9

```
Address: 00:0d:5e:dc:39:74
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 132.227.110.115, Dst: 132.227.68.44
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: 84
Identification: 0x0000 (0)
```

83

```
Internet Protocol Version 4, Src: 132.227.110.115, Dst: 132.227.68.44
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: 84
Identification: 0x0001 (1)
Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 64
```

206

```
Internet Protocol Version 4, Src: 132.227.110.115, Dst: 132.227.68.44
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: 84
Identification: 0x0002 (2)
Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
```

344

```
Internet Protocol Version 4, Src: 132.227.110.115, Dst: 132.227.68.44
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: 84
Identification: 0x0003 (3)
Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 64
```

En comparant les 4 ententes IP de ces requêtes, on remarque que seulement le champ Identification qui change. En effet, il s'agit que le champ Identification s'incrémente avec chaque requête.

Ententes ICMP :

9

```
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf3b6 [correct]
[Checksum Status: Good]
Identifier (BE): 42858 (0xa76a)
Identifier (LE): 27303 (0x6aa7)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
```

83

```
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x78b2 [correct]
[Checksum Status: Good]
Identifier (BE): 42858 (0xa76a)
Identifier (LE): 27303 (0x6aa7)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100)
```

206

```
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x0fb2 [correct]
[Checksum Status: Good]
Identifier (BE): 42858 (0xa76a)
Identifier (LE): 27303 (0x6aa7)
Sequence Number (BE): 2 (0x0002)
Sequence Number (LE): 512 (0x0200)
```

344

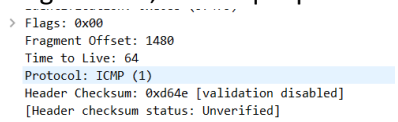
```
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xa7b1 [correct]
[Checksum Status: Good]
Identifier (BE): 42858 (0xa76a)
Identifier (LE): 27303 (0x6aa7)
Sequence Number (BE): 3 (0x0003)
Sequence Number (LE): 768 (0x0300)
```

On remarque que le champ Checksum.

17. Le champs Flags dans l'entête de l'IP, indique More fragments. Cela vaut dire que le message a été fragmenté. On remarque que ce fragment prend la taille maximum de 1500 octets.

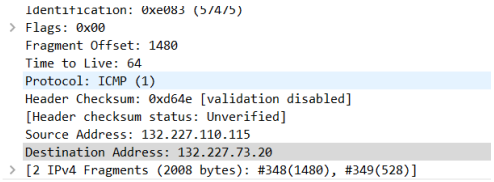
```
Internet Protocol Version 4, Src: 132.227.110.115, Dst: 132.227.73.20
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 1500
Identification: 0xe083 (57475)
Flags: 0x20, More fragments
Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0xb34f [validation disabled]
[Header checksum status: Unverified]
Source Address: 132.227.110.115
```

18. Le champs Fragment Offset indique le numéro de fragment. Dans ce cas, le champ indique 0. En regardant le champ Flags de la trame d'après, on voit que le flag est devenu à 0. Donc le premier Flag du premier fragment doit indiquer « More Fragments », tandis que pour les autres fragment le flag change.



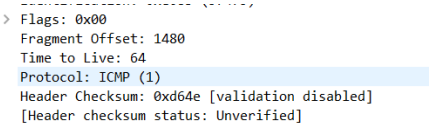
19. La longueur totale de ce fragment sera de 1500-20, donc de 1480 octets.

20. L'adresse de destination est de « 132.227.73.20 »



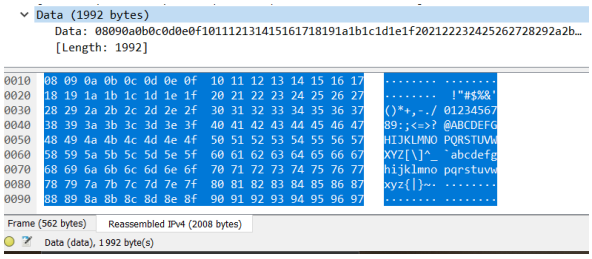
21. Dans l'entête le champ Fragment Offset indique la valeur 1480, donc il commence à partir d'un grand paquet. Ceci indique qu'une partie de ce paquet a été déjà envoyé dans des trames précédentes. Donc ce n'est pas la première trame.

22. Dans l'entête de la deuxième trame, on remarque que le champ Flags indique la valeur 0. Cela vaut dire qu'il n'y aura plus de fragments qui vont être envoyés. On en déduit qu'il s'agit de deuxième et dernier fragment.



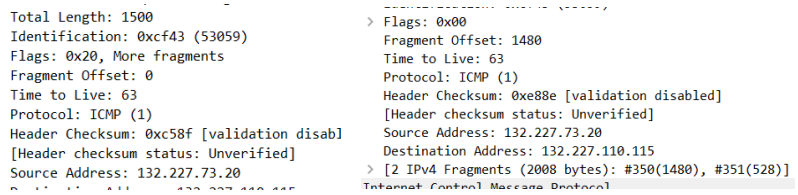
23. Ce fragment est de 548 octets

24. En additionnant les deux fragments on obtient : 1480+528 = 2008 octets.



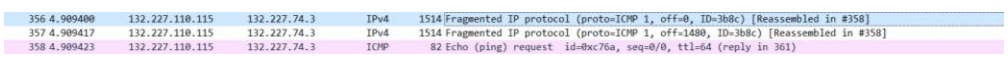
En regardant les données envoyés on observe 1992 octets. Donc le paquet de 2008 octets correspond à 1992 octets + 8 octets pour le timestamp + 8 octets pour l'entête ICMP.

25.

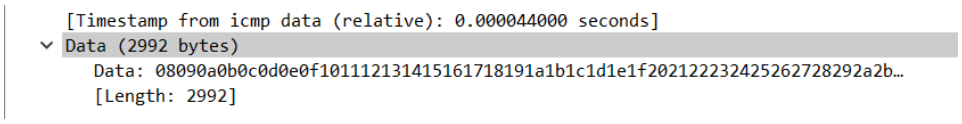


On sélectionne les trames 350(à gauche) et 351(à droite). Le champ Flags de 350 indique bien qu'il y aura plus de fragments, or la trame 351 après indique qu'il n'y aura plus de fragments. Donc 2 fragments sont nécessaires pour ce paquet.

26.



On observe 3 fragments, avec les deux premiers qui porte le champ Flags de « More fragments » et le dernier fragment la valeur 0 pour le champ Flags.
Longueur totale : 1480 + 1480 + (68-20) = 3008. Avec 8 octets qui comptent pour le Timestamp et 8 octets pour l'entête ICMP.


[Timestamp from icmp data (relative): 0.000044000 seconds]
Data (2992 bytes)
Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b…
[Length: 2992]