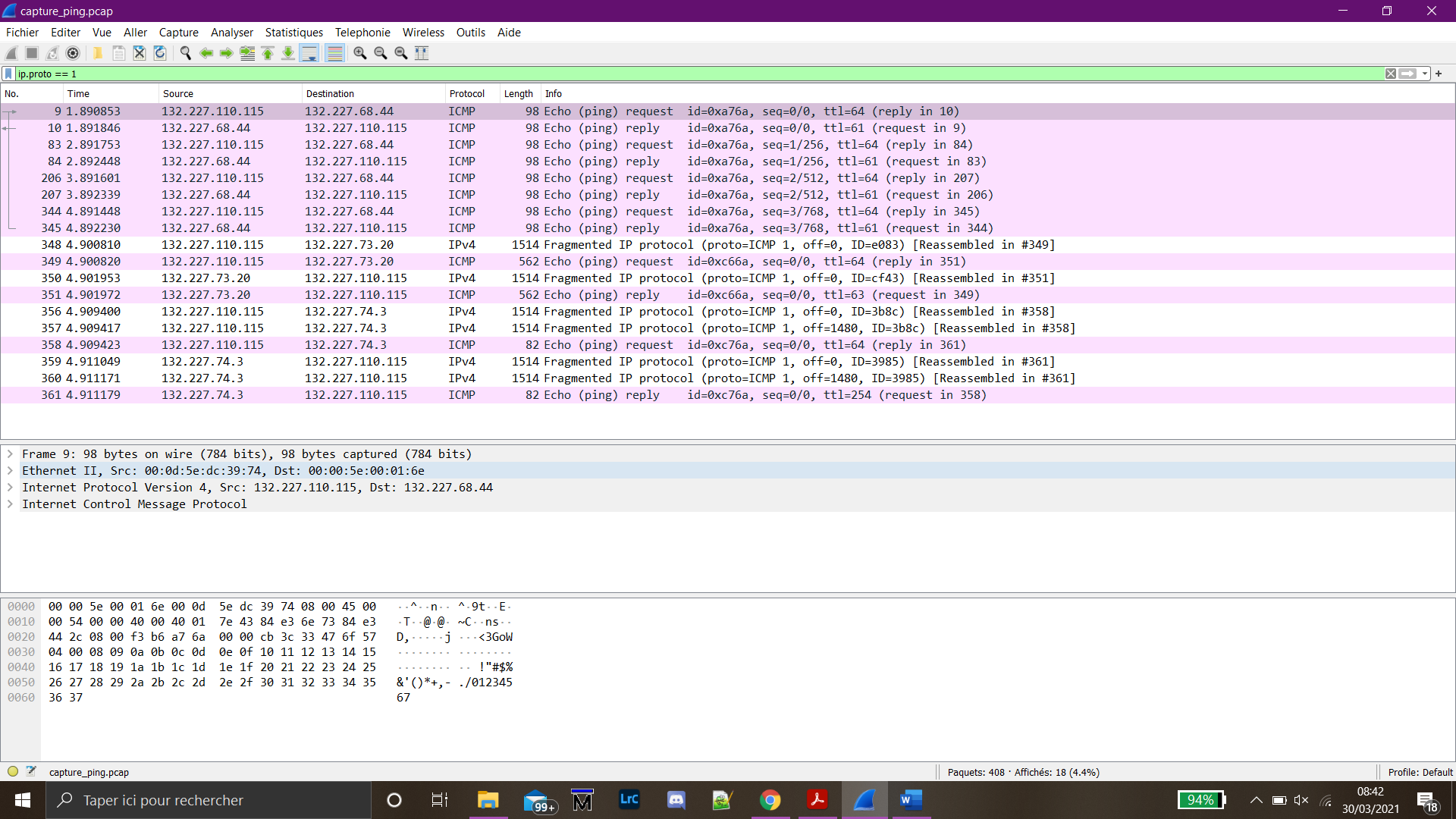
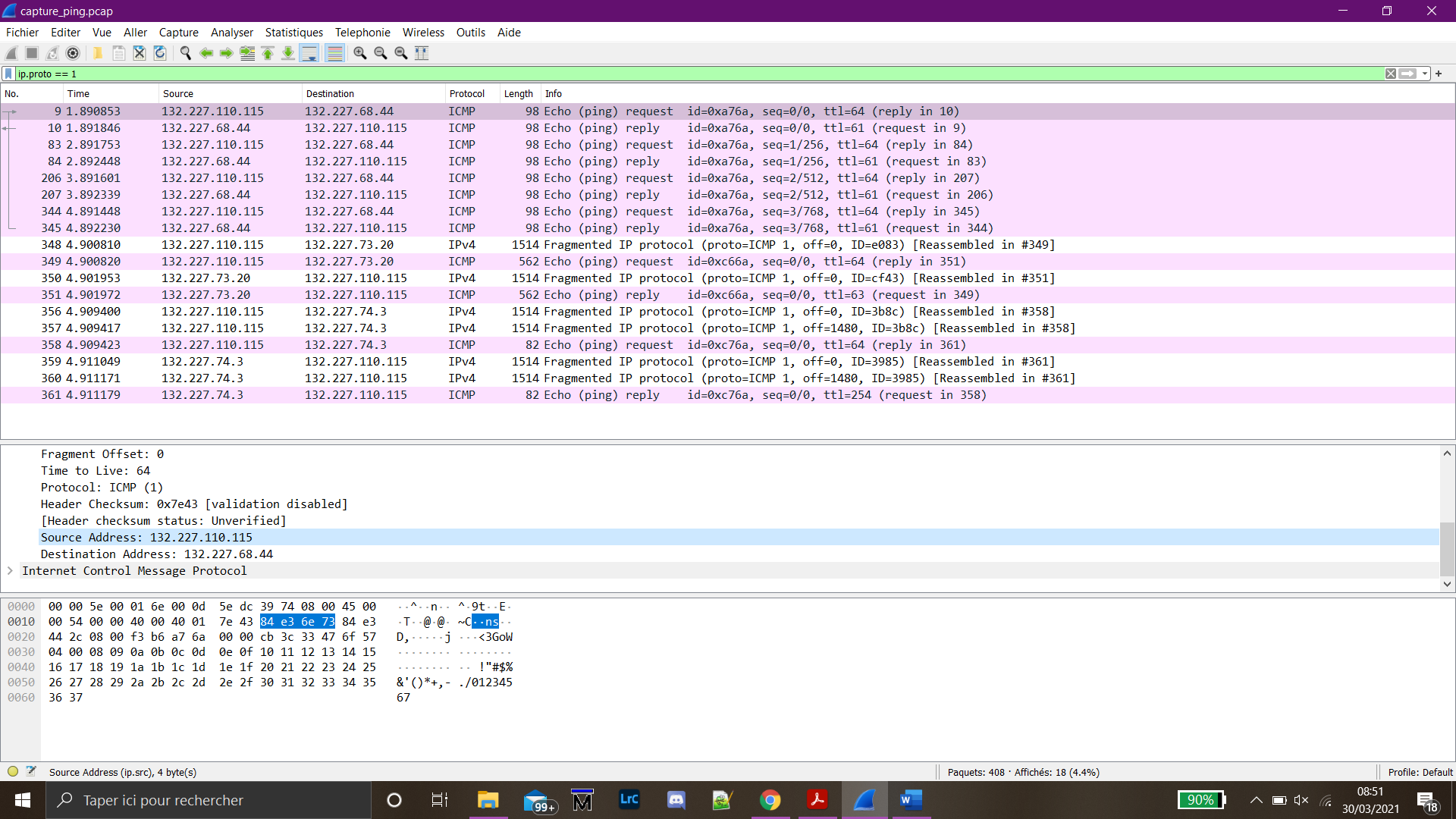
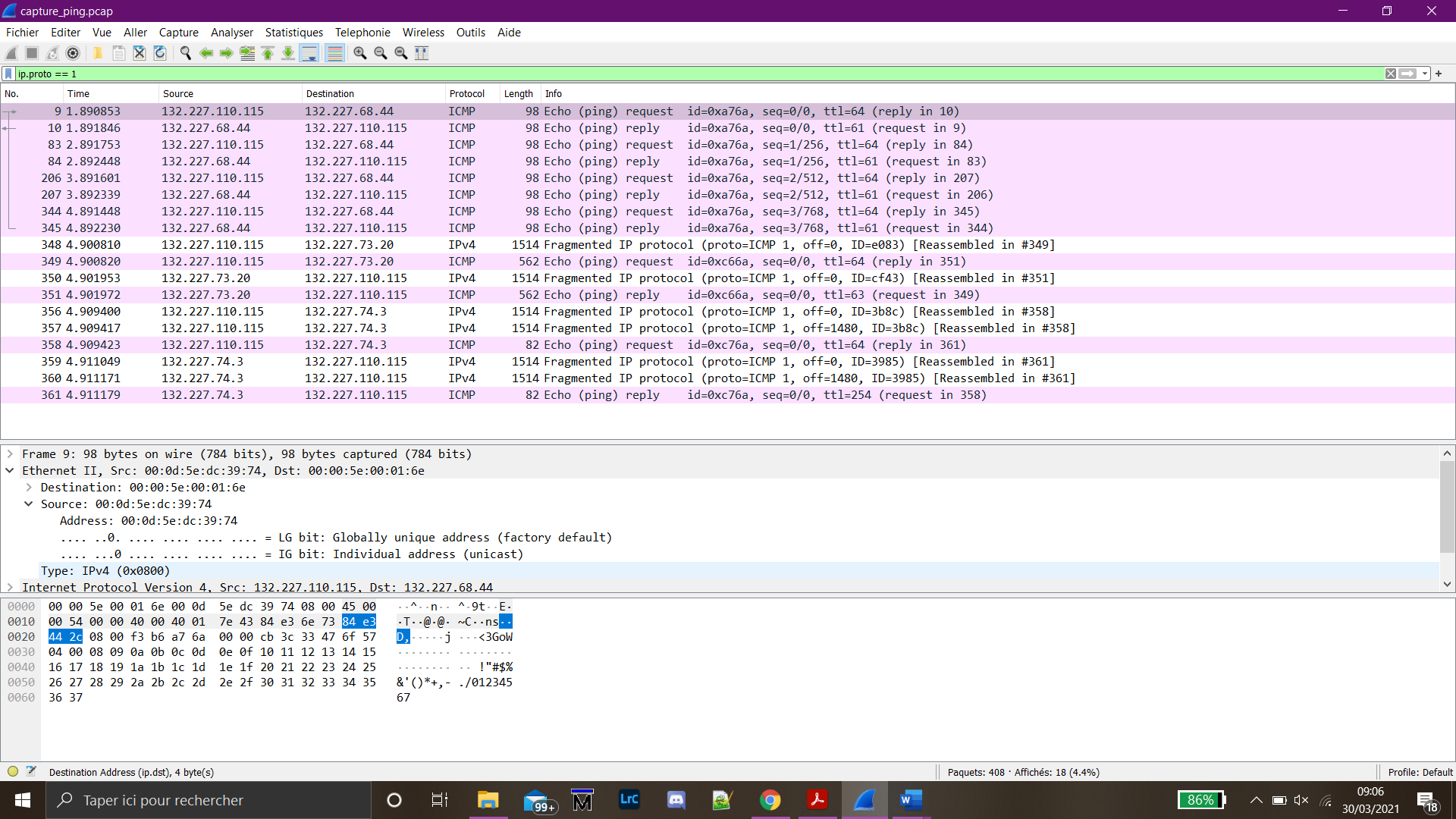
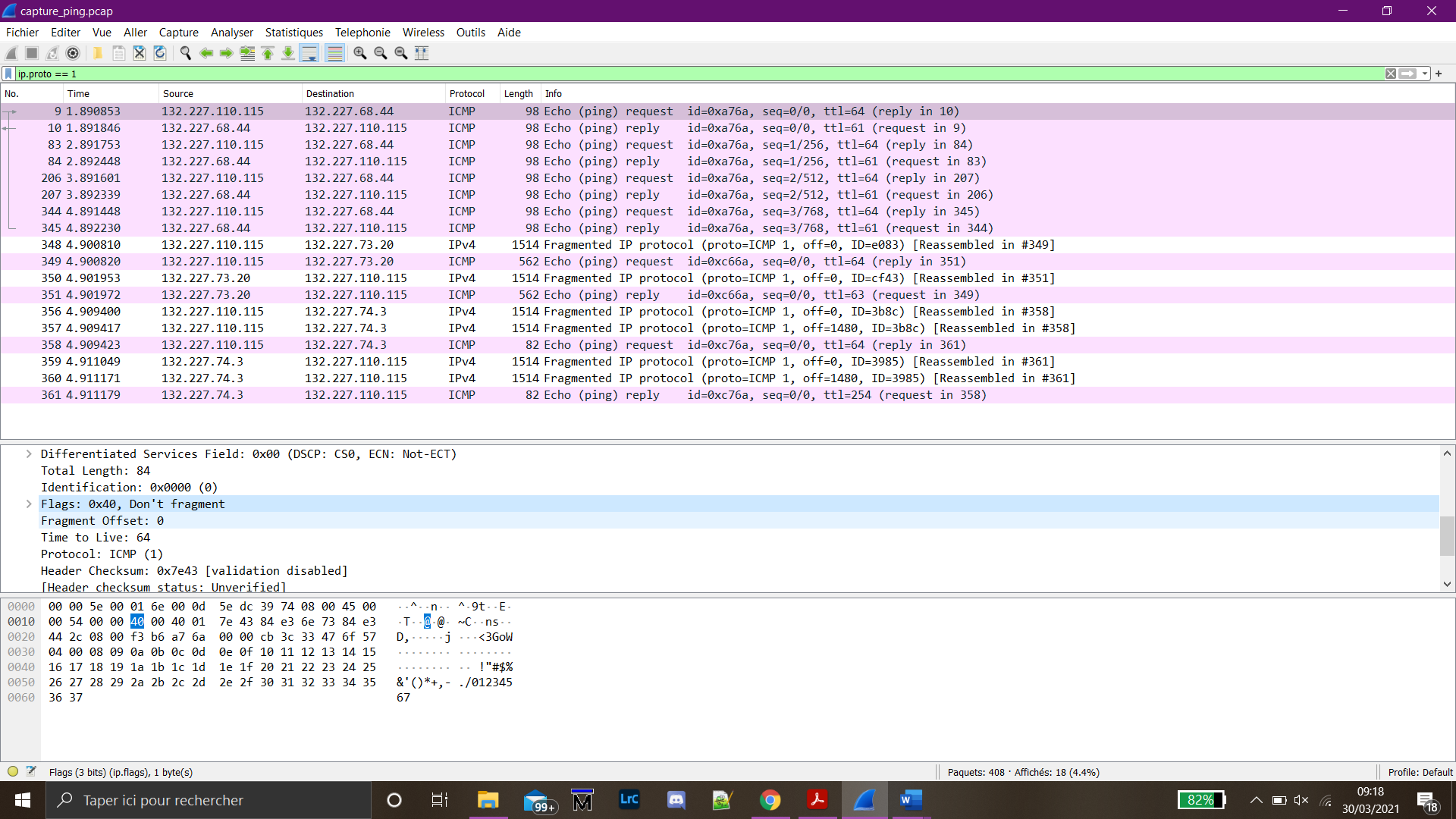
**TP3**

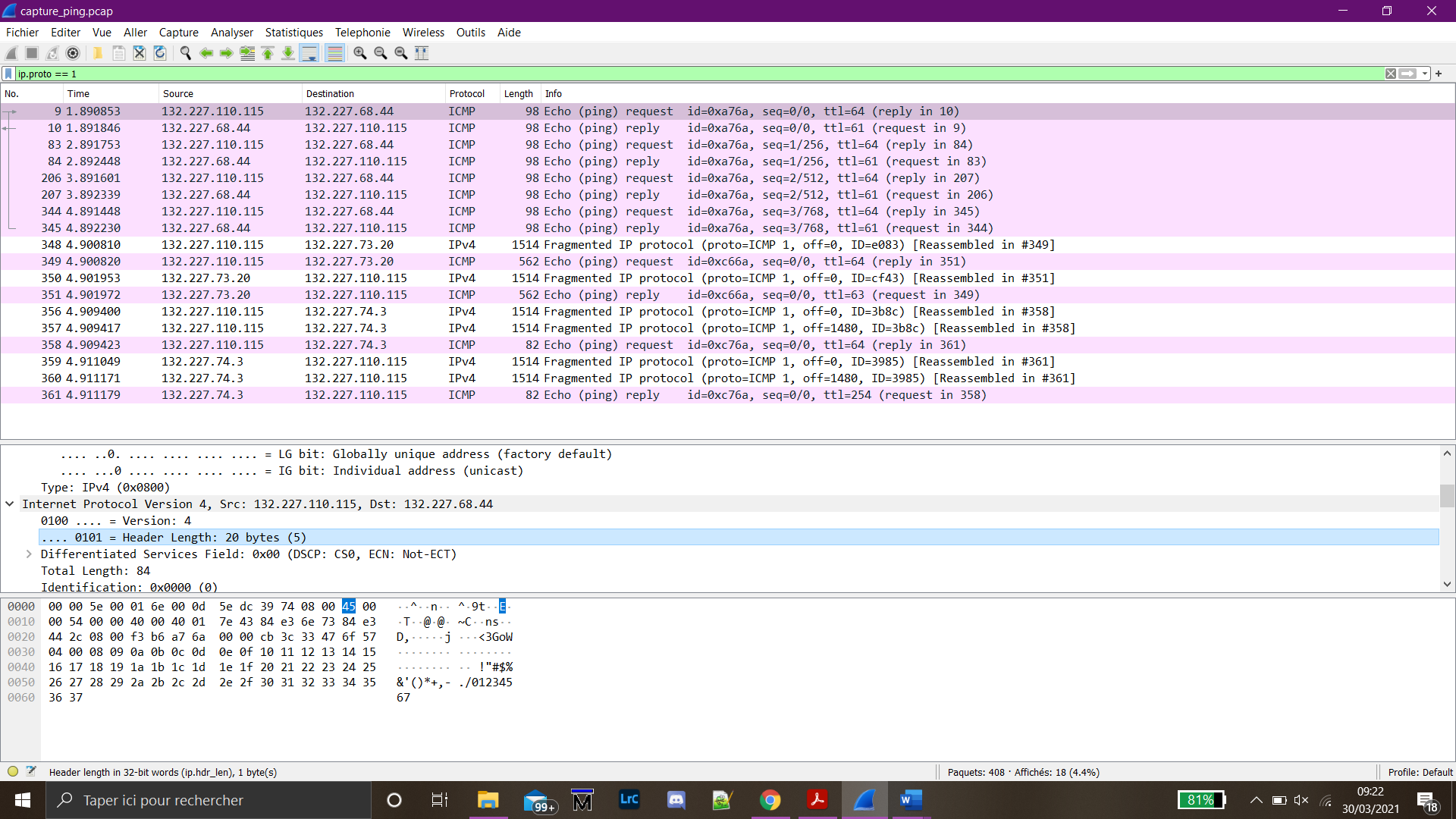
**Julian BARKOUDEH**

1. **Ping et ICMP** 
   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. 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. 

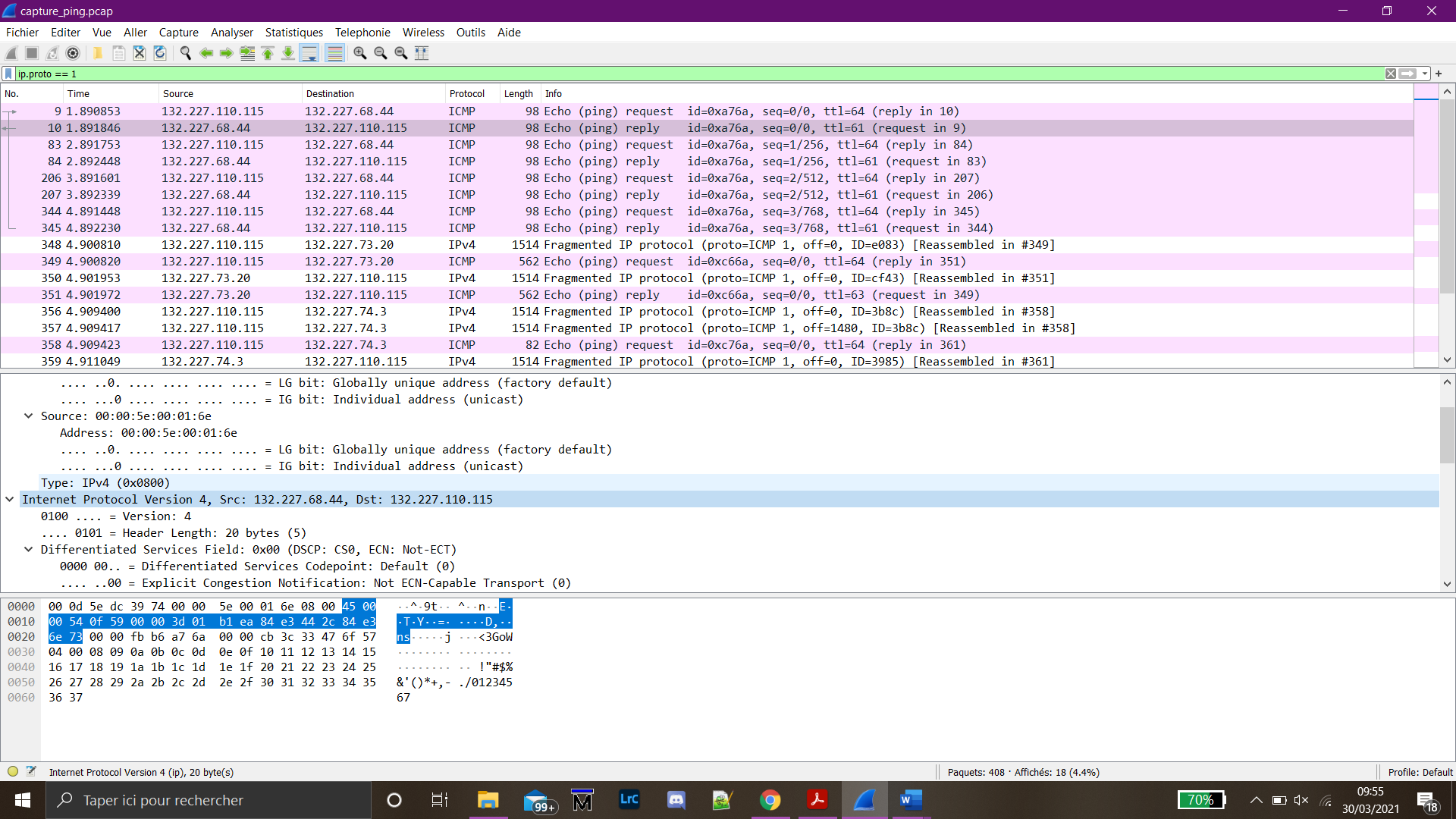
En observant la case d’Ethernet, on remarque que l’adresse MAC est de « 00 :0d :5e : dc :39 :74 » ce qui correspon0d à l’adresse IP source.

* 1. L’adresse MAC de la destination est de « 00 :00 :5e :00 :01 :6e » qui correspond à l’adresse IP destination.
  2. 

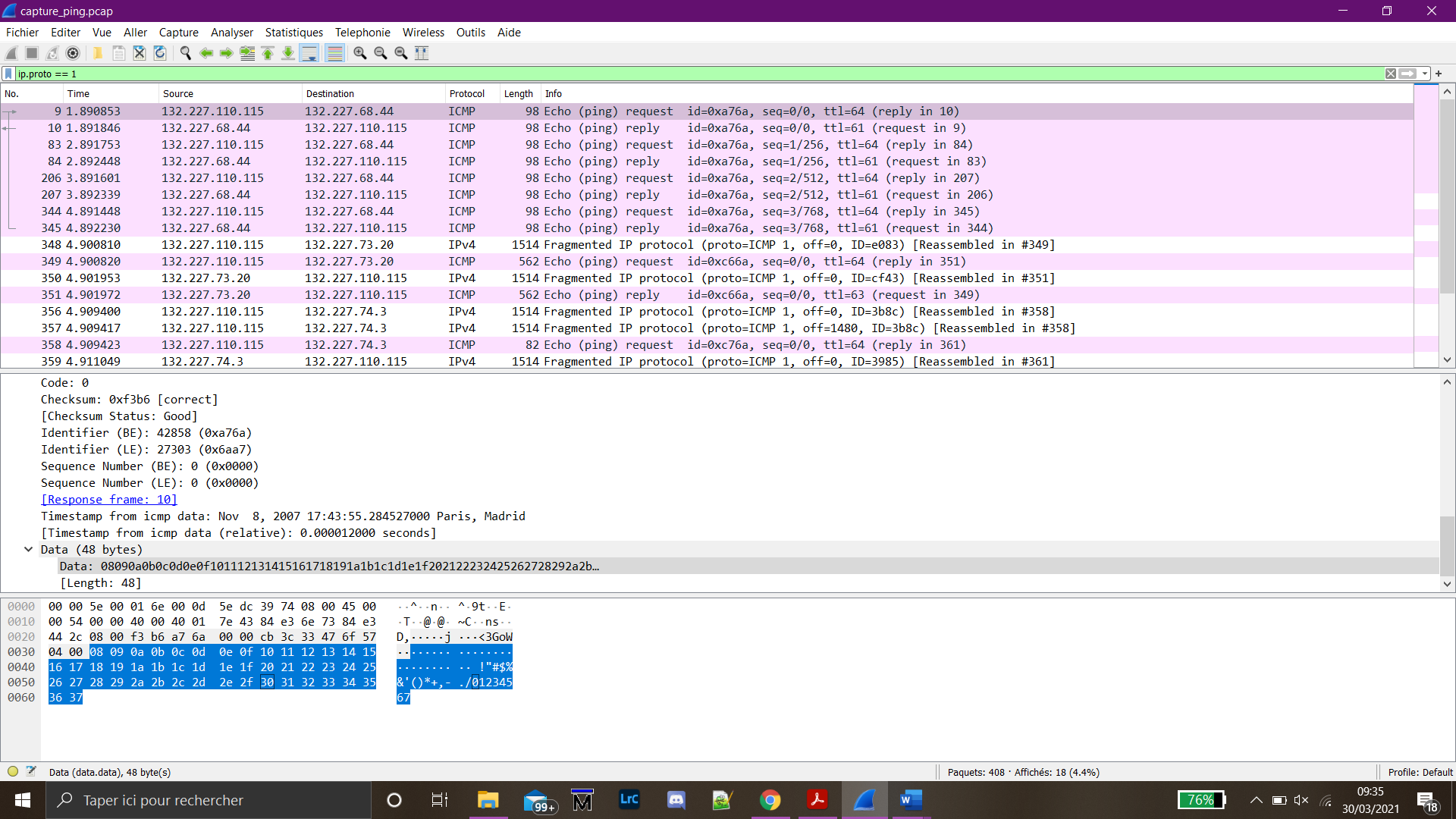
D’après les annexes, la partie Flags de l’entête permet de déterminer si le message a été fragmenté ou pas. Dans ce cas, on remarque que le message n’a pas été fragmenté.

* 1. 

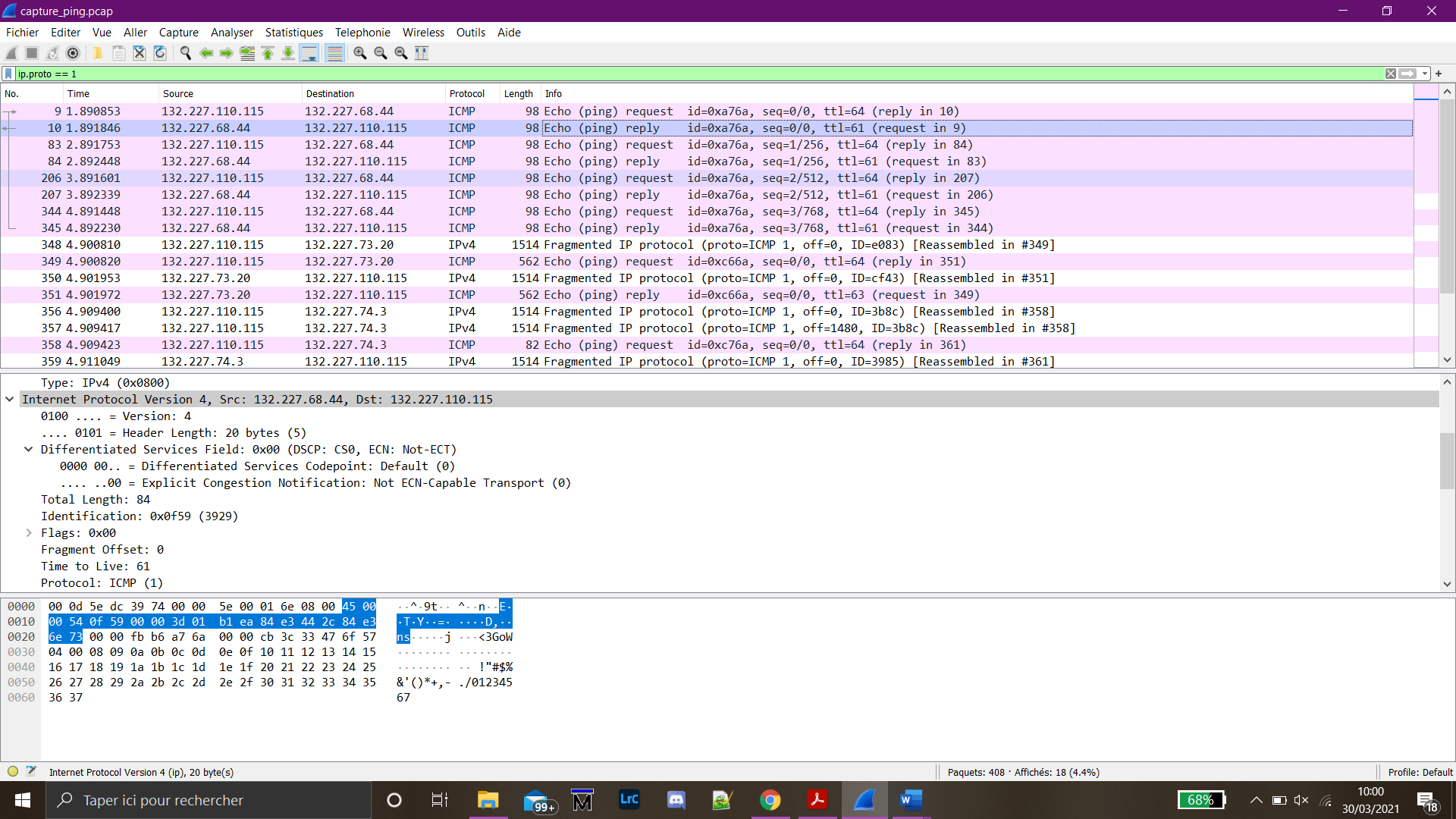
En observant la case Internet Protcole, on en déduit que ma longueur de l’entête est de 20 octets.



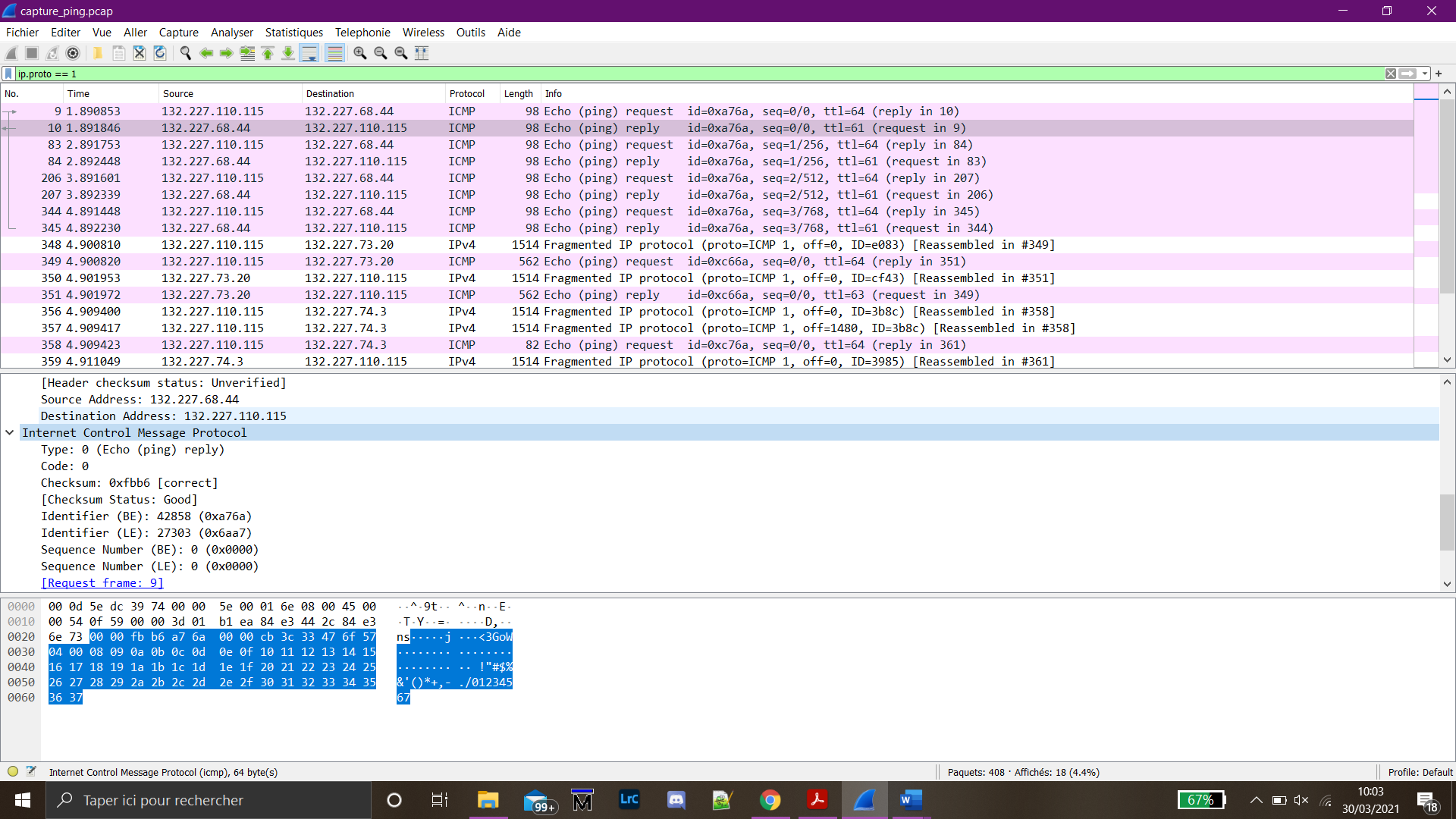
En comptants le nombres d’octets présents dans l’entête IP (souligné en bleu), on compte aussi 20 octets. En plus l’entête se termine par l’adresse de destination (Avant la partie ICMP encadré en rouge), donc d’après les annexes il n’y pas d’options.

* 1. 

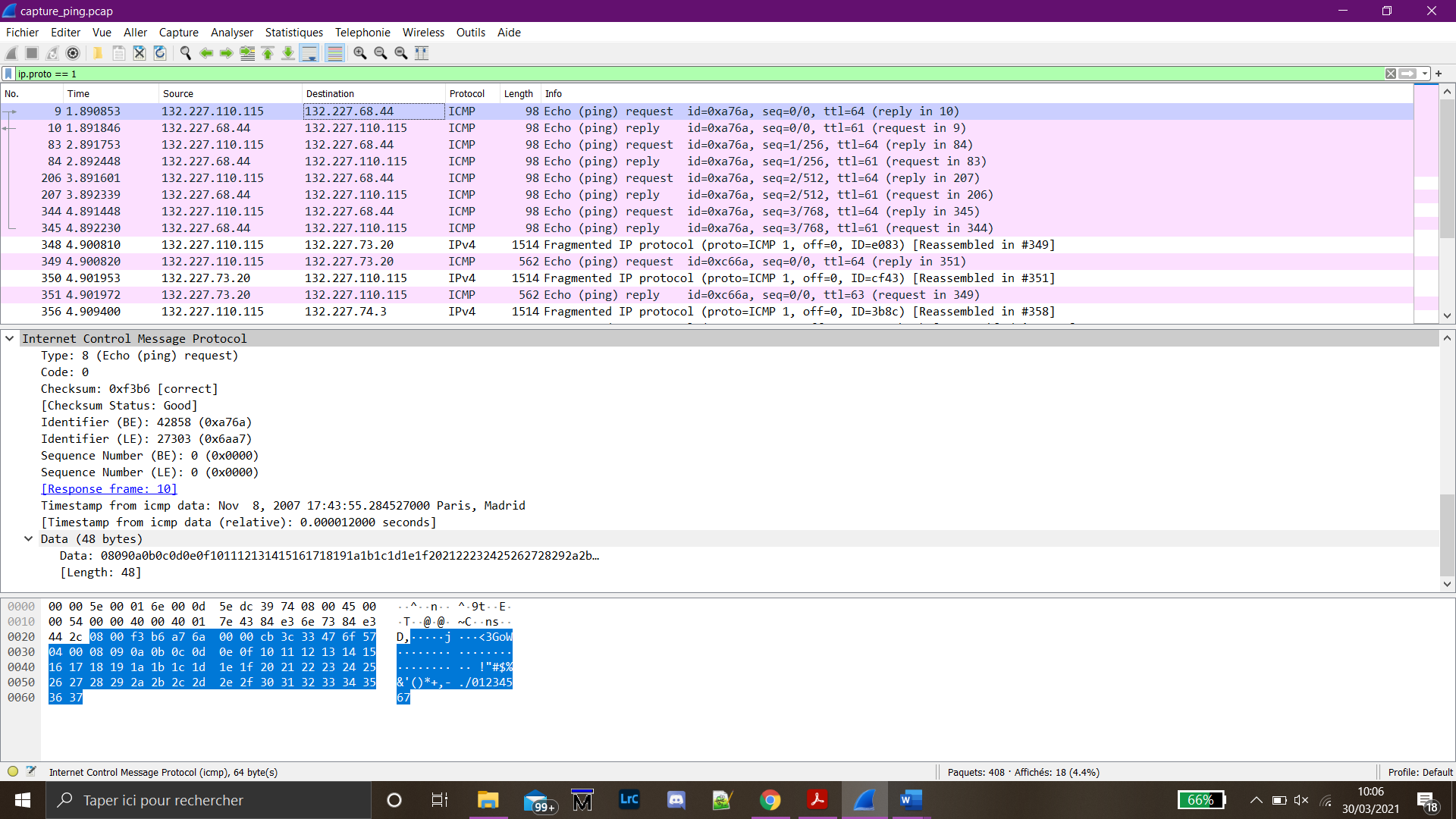
En sélectionnant la partie de Data, et en observant dans la case de ICMP, on remarque que le Data contient 64 octets.

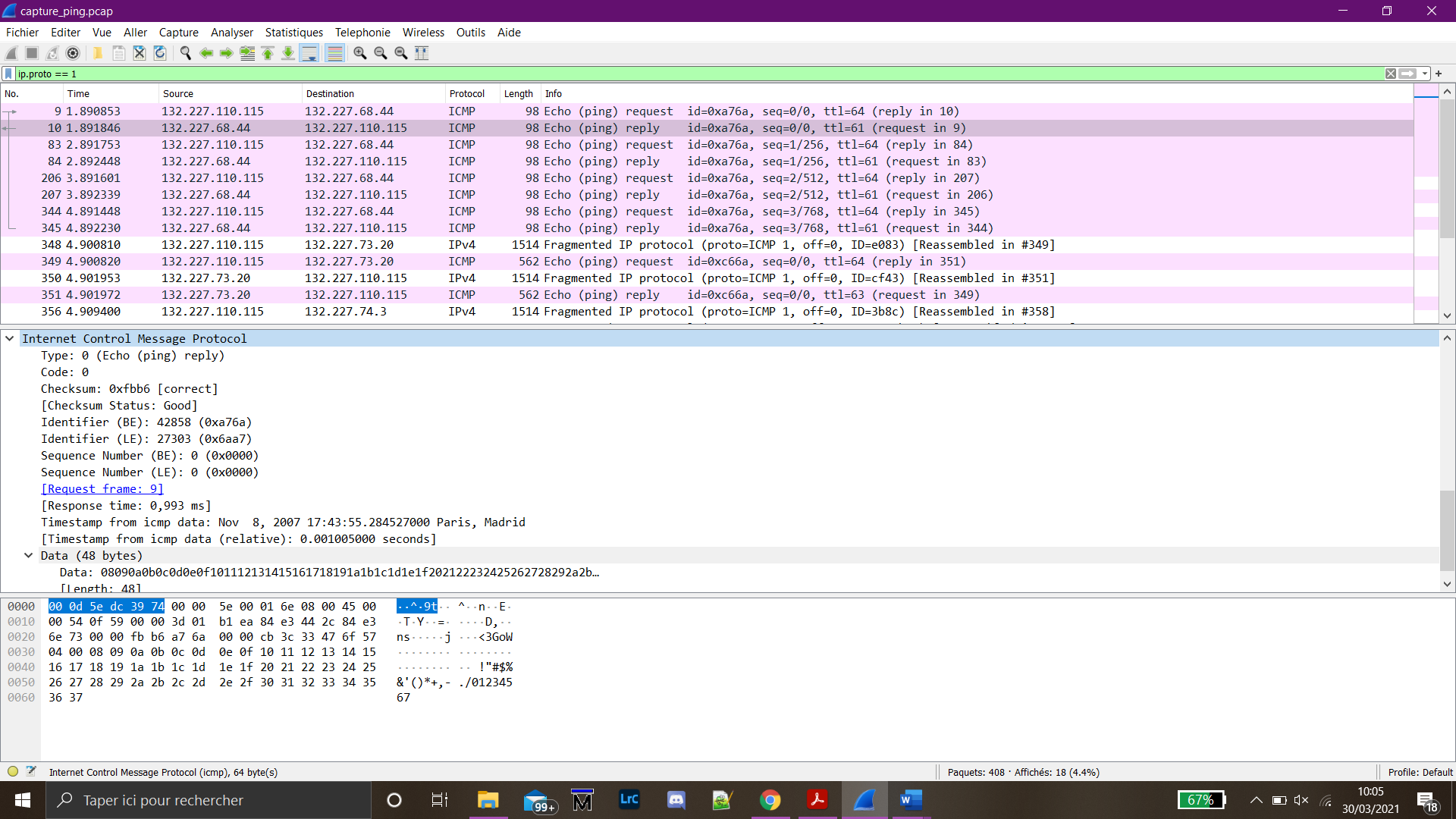
* 1. En se basant sur les annexes, on remarque qu’il n’y que 8 octets. Donc, il n’y a pas d’options dans l’entête du message ICMP.
  2. En regardant le manuel de la commande PING, on en déduit que les data de ICMP sont encapsuler dans une trame de 56 octets, avec 8 octets pour l’entête. Donc 64 octets de partie ICMP. Or, dans notre cas nous avons 8 octets pour l’entête et 56 pour les données.
  3. 

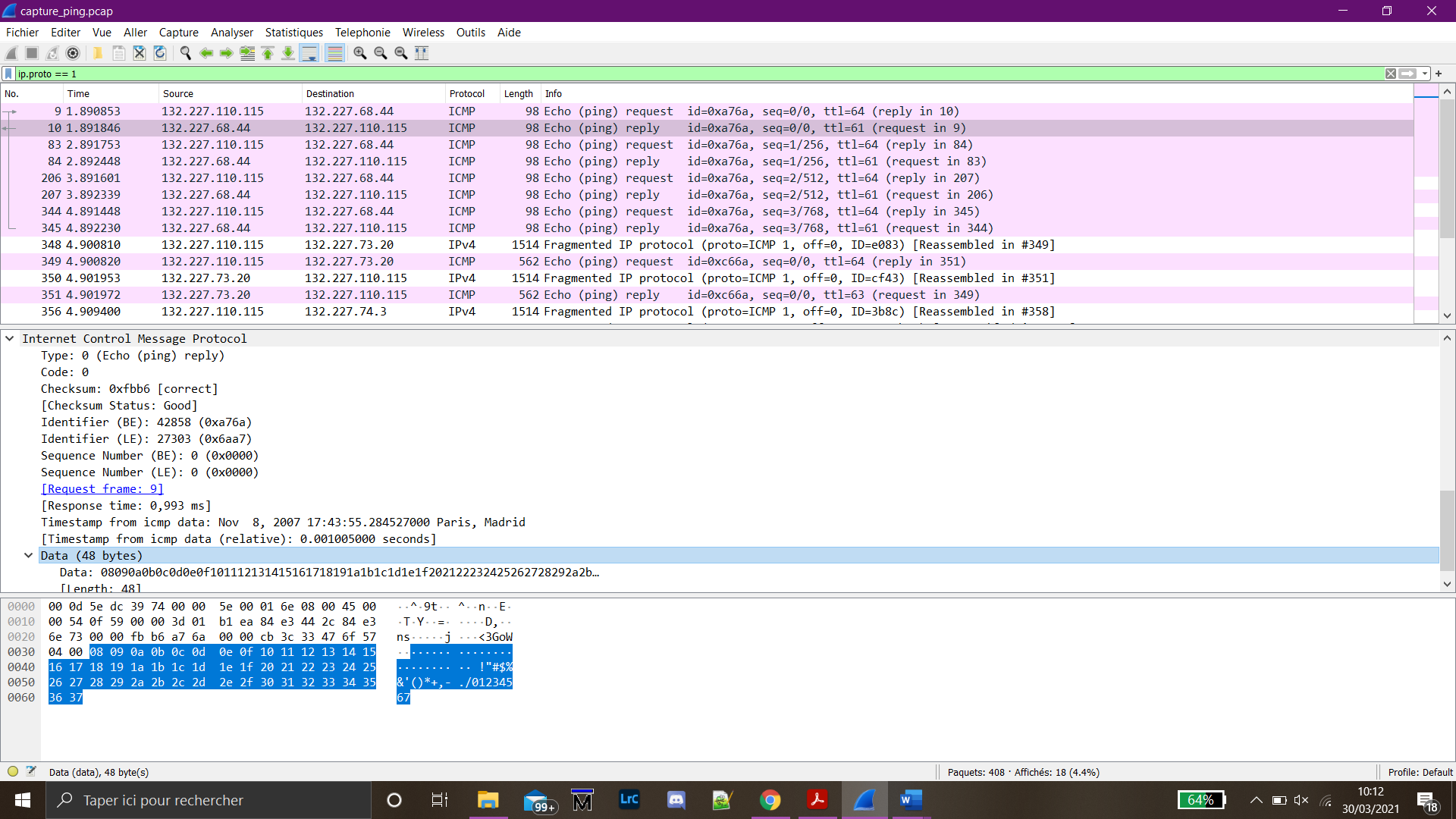
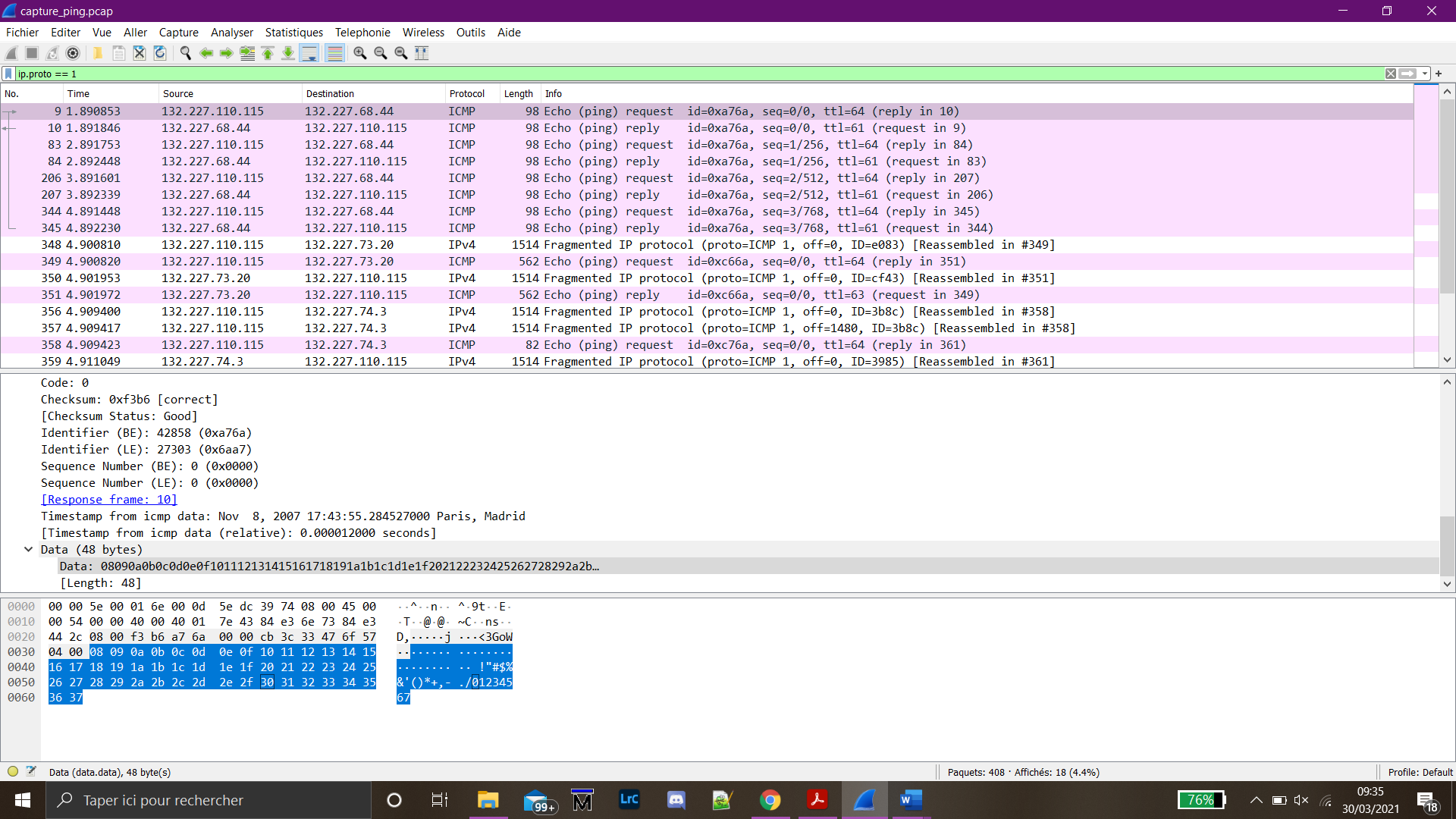
L’entête IP pour la deuxième requête compte 20 octets.

* 1. 

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

Replay Request

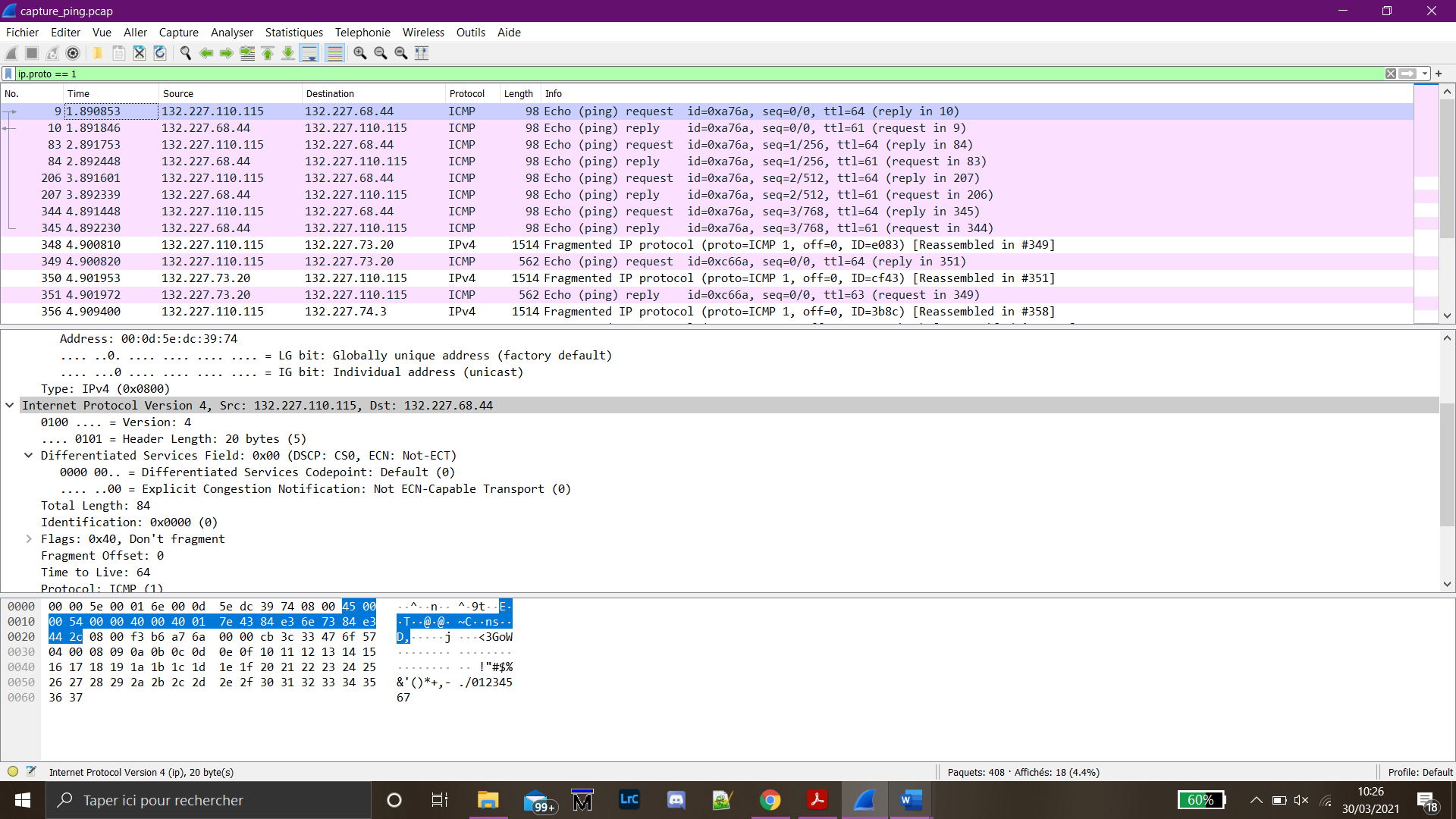
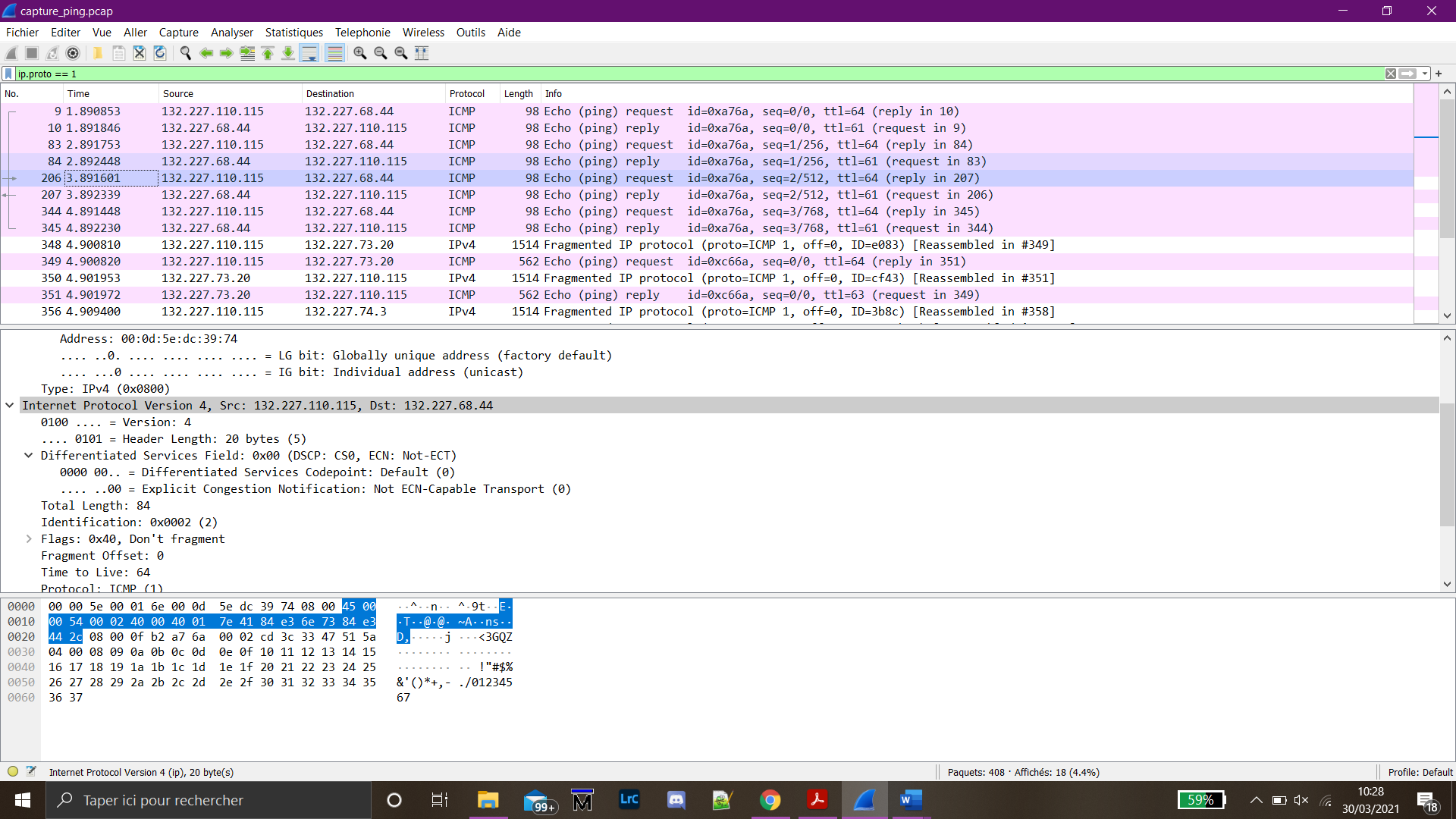
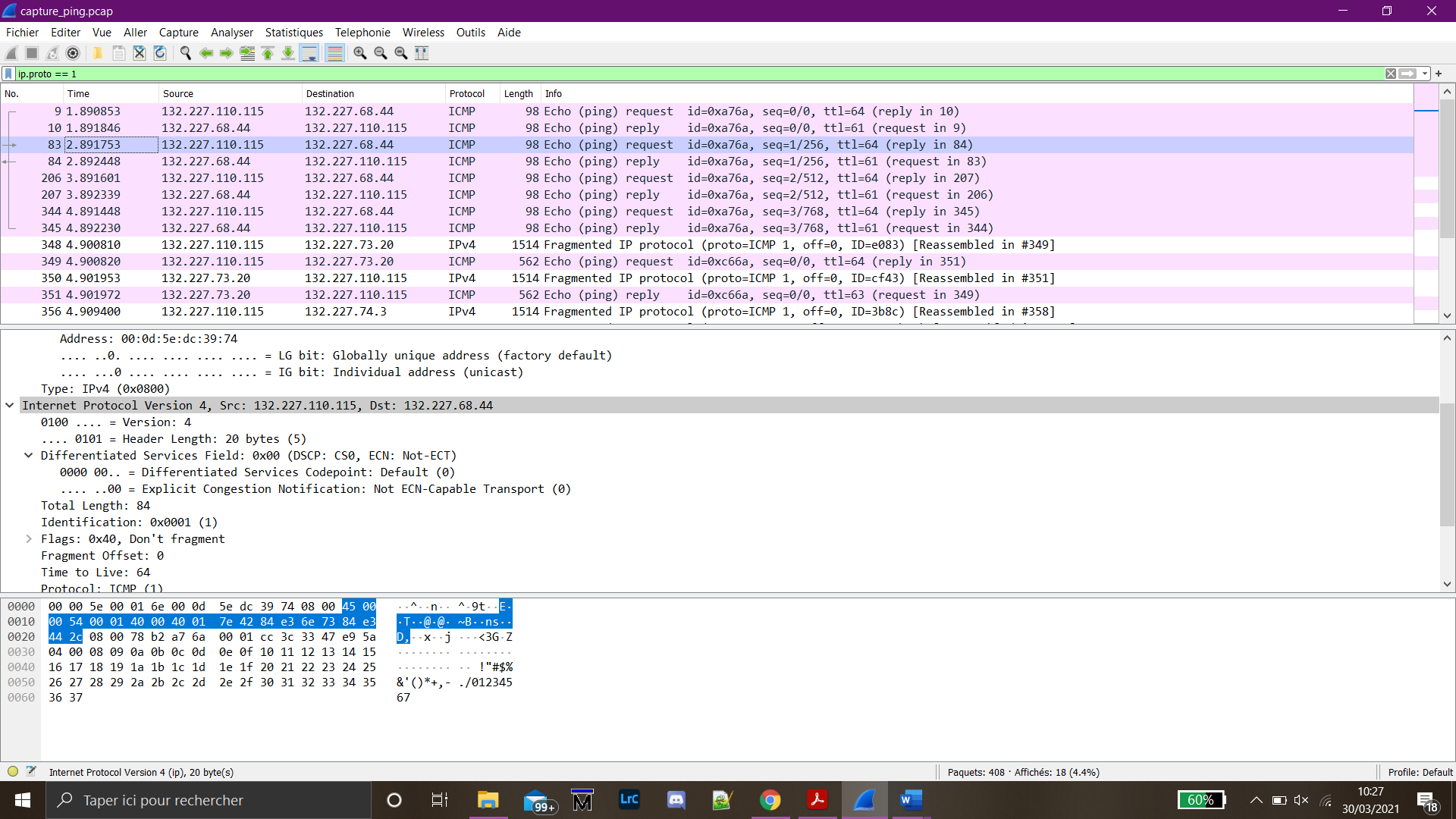
On remarque tout d’abord une différence dans la case Type, qui dans la réponse est de 0. Cela correspond d’après les annexes à Echo Reply. La case Code ne change pas, car il s’agit toujours du protocole ICMP. On remarque aussi que les Timestamp sont quasiment identiques.

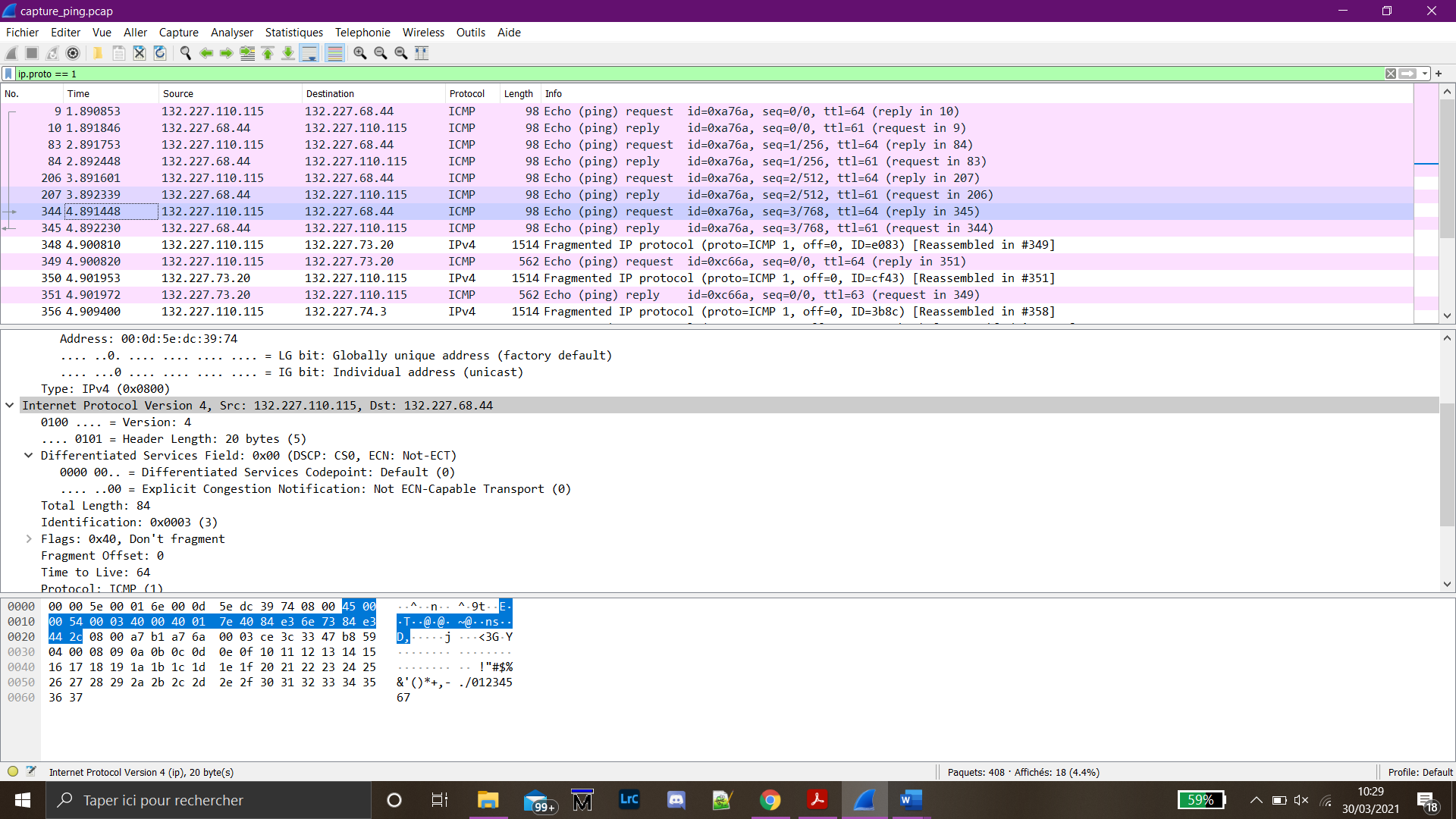


En comparant les deux cases de data ( Reply à gauche et Request à droite) , on remarque que les deux blocs sont exactement identiques. Ceci vient de la nature de la deuxième trame (Reply) qui consiste à renvoyer les paquets de données reçus par un utilisateur.



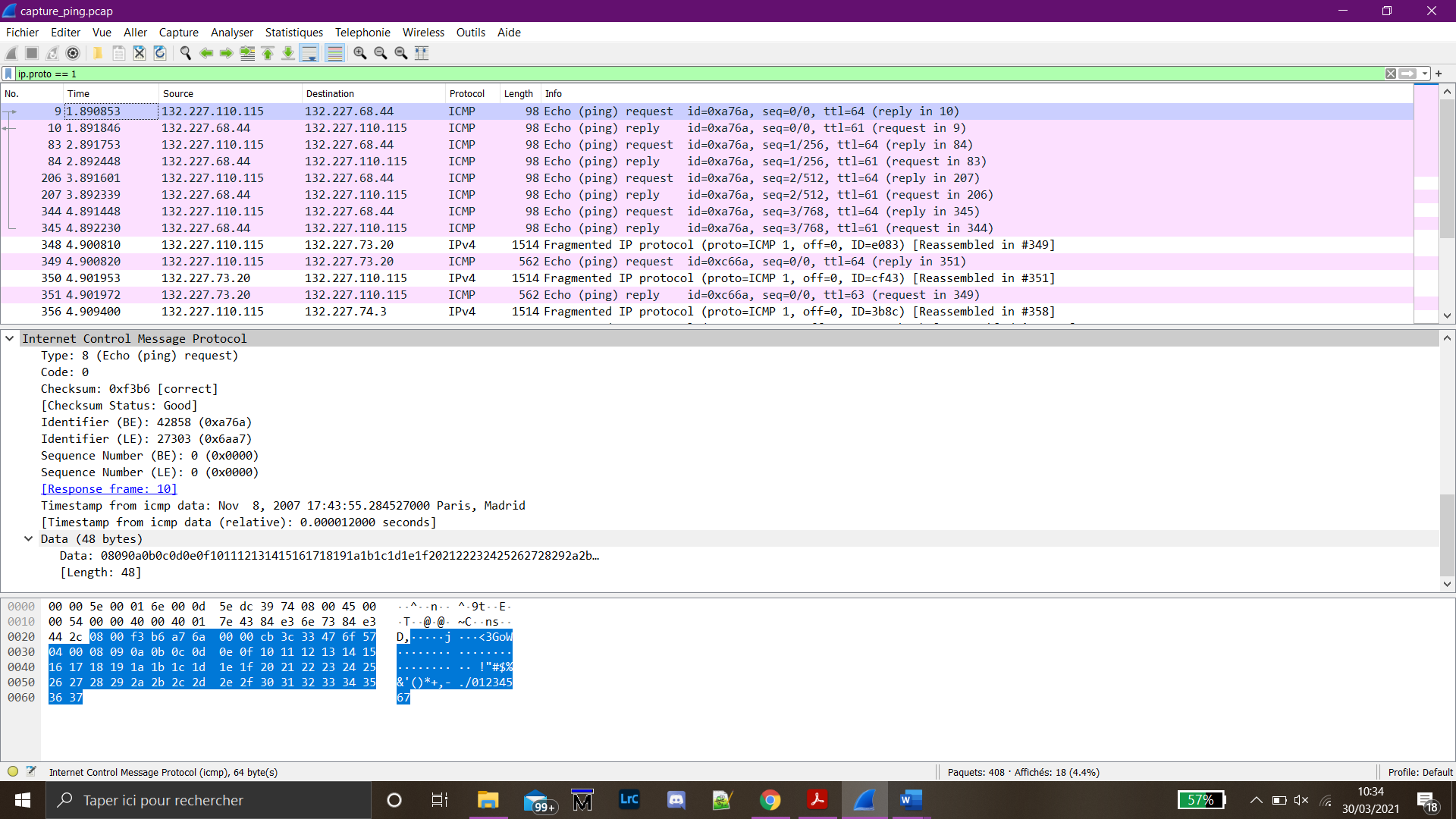
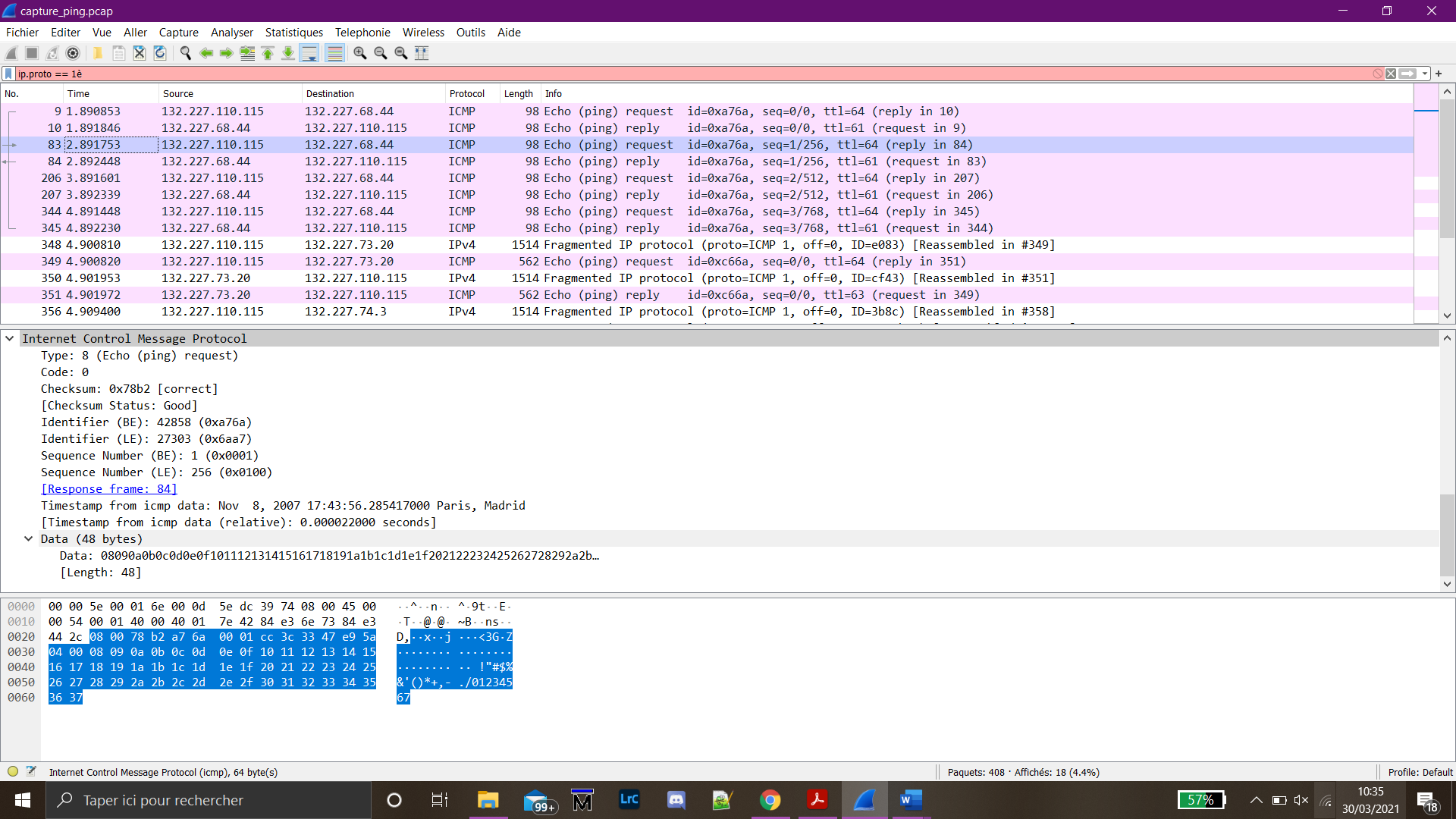
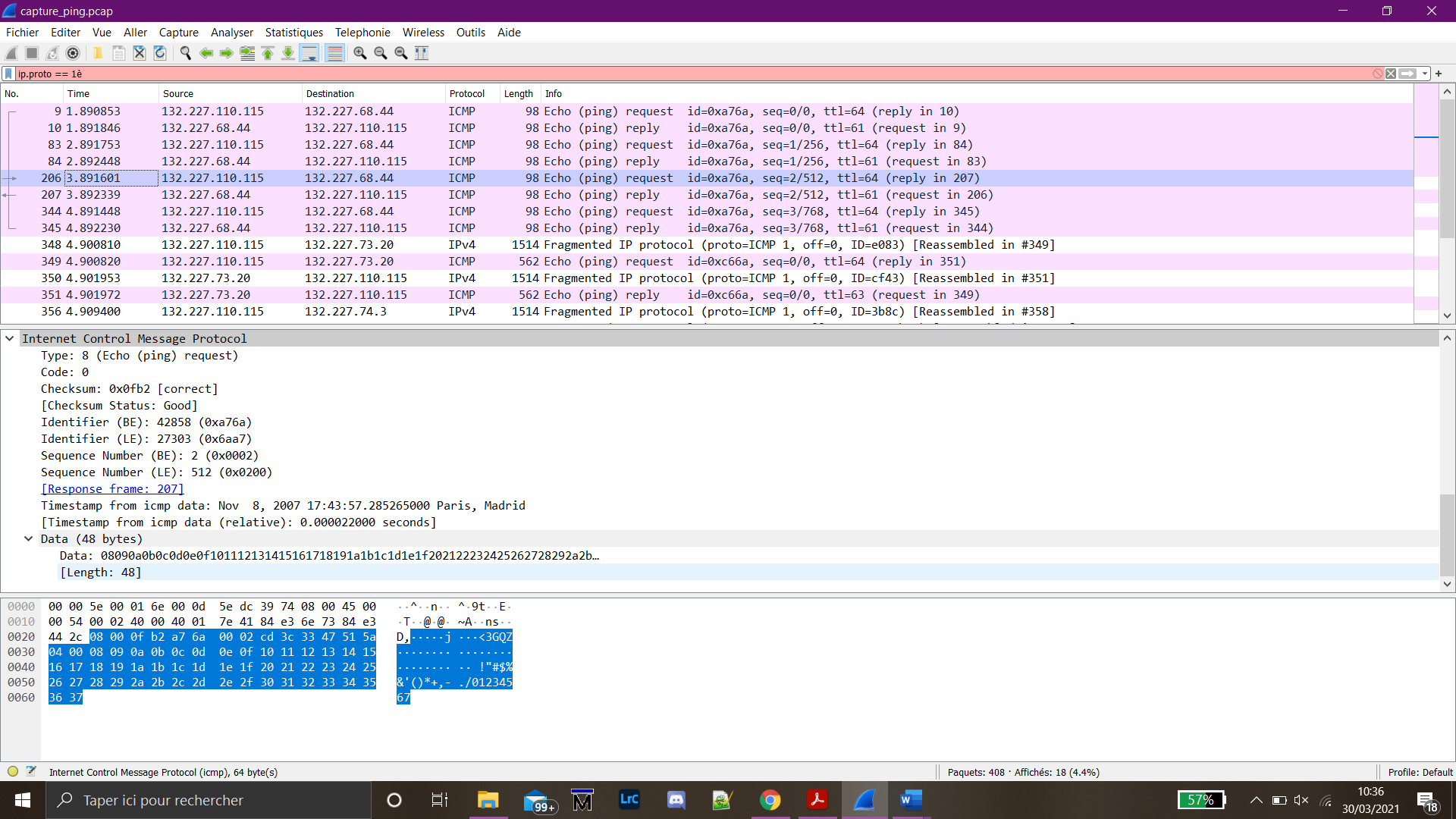
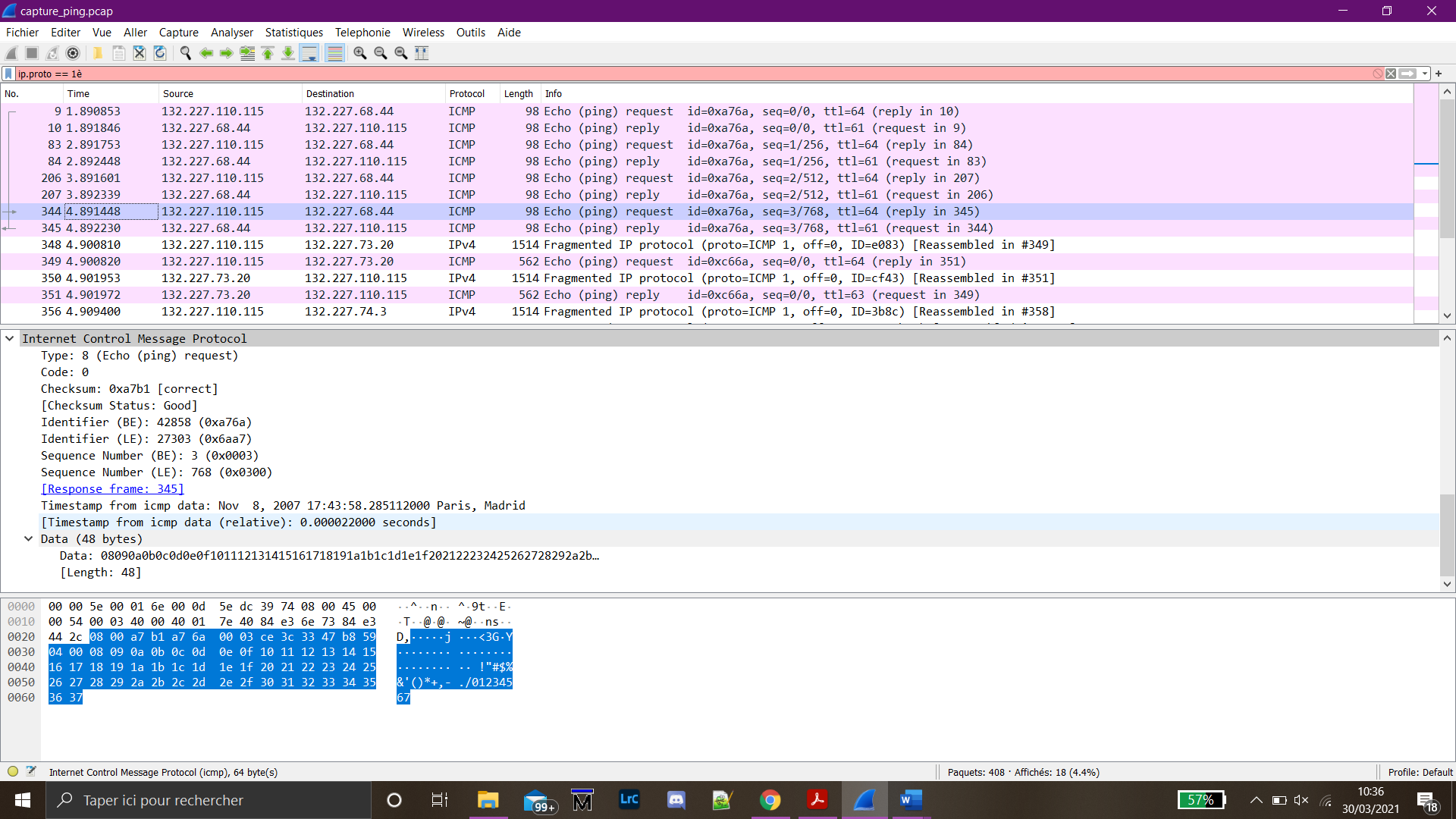
Ententes IP :

9 83 206

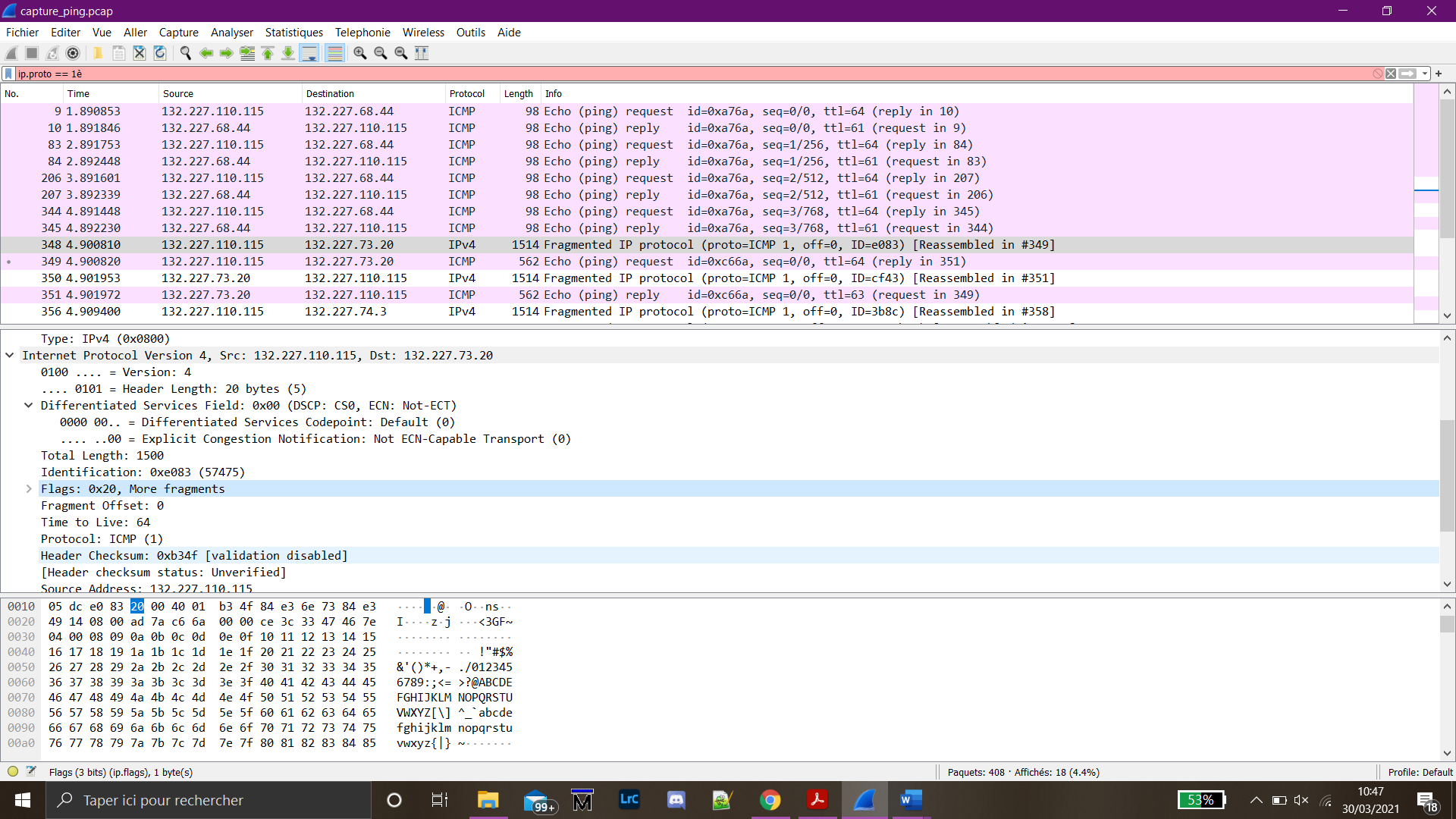
344

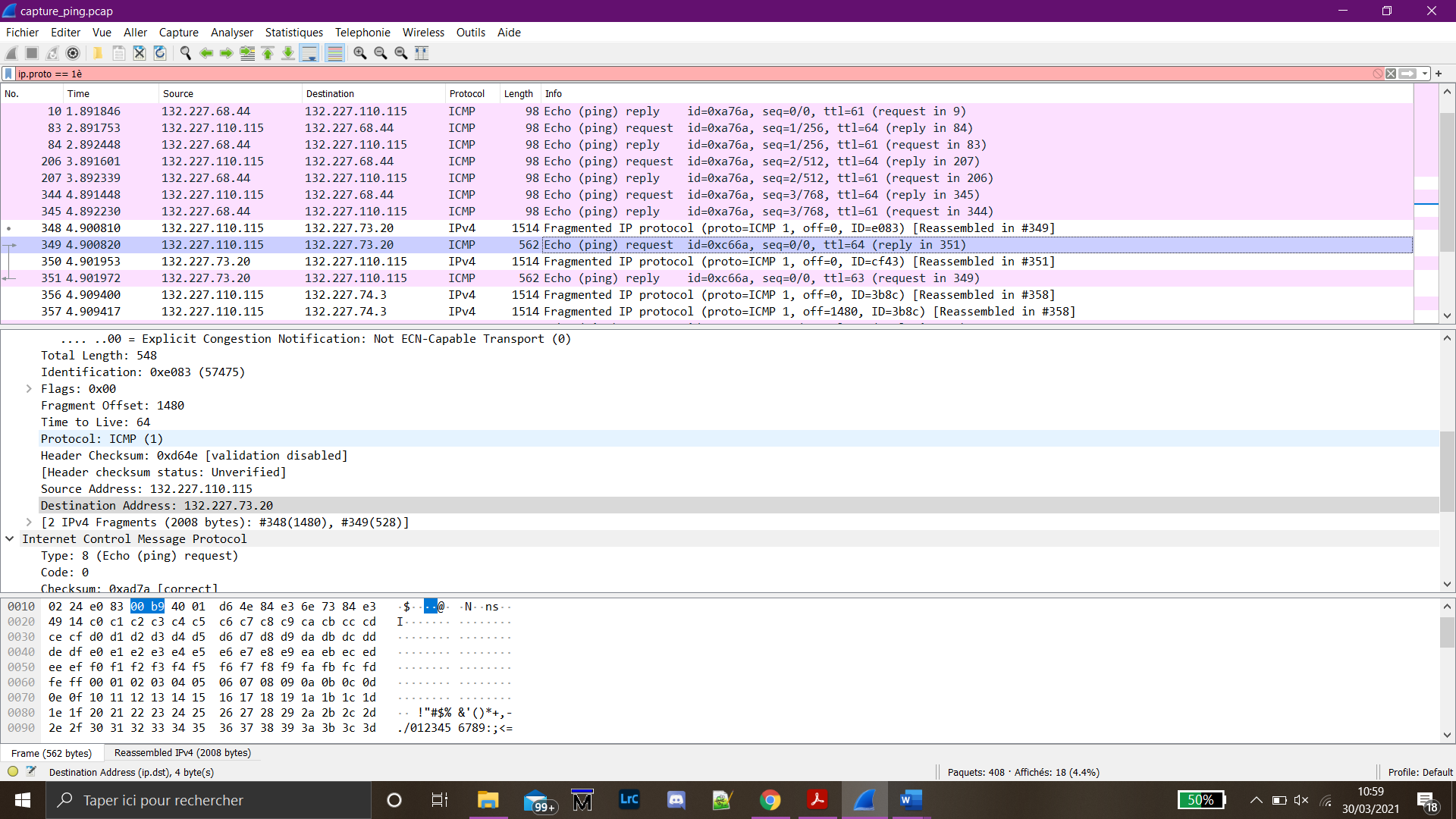
En comparant les 4 ententes IP de ces requêtes, on remarque que seulement le champ Identification qui change. En effet, il s’agit que le champ Identification s’incrémente avec chaque requête.

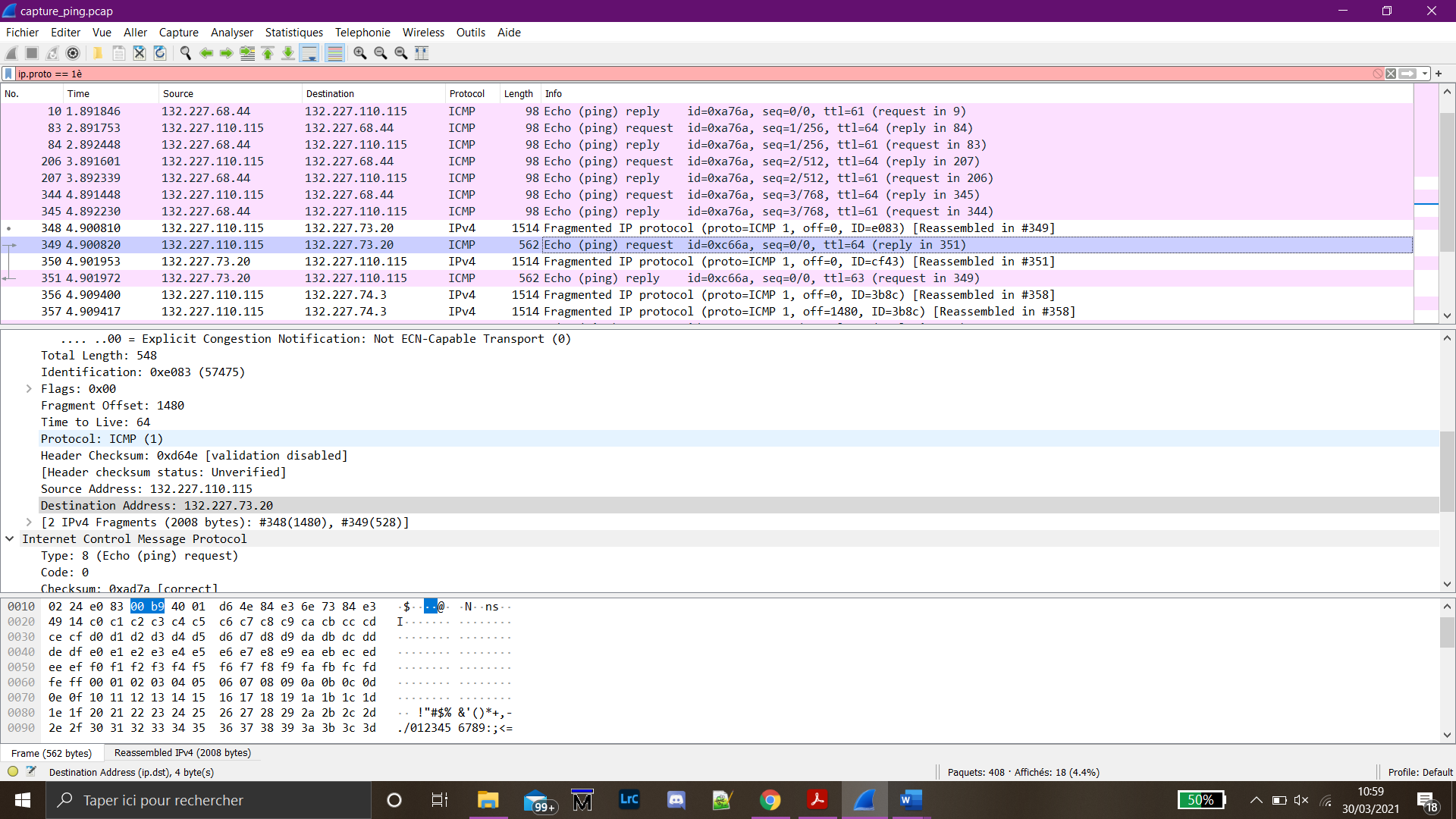
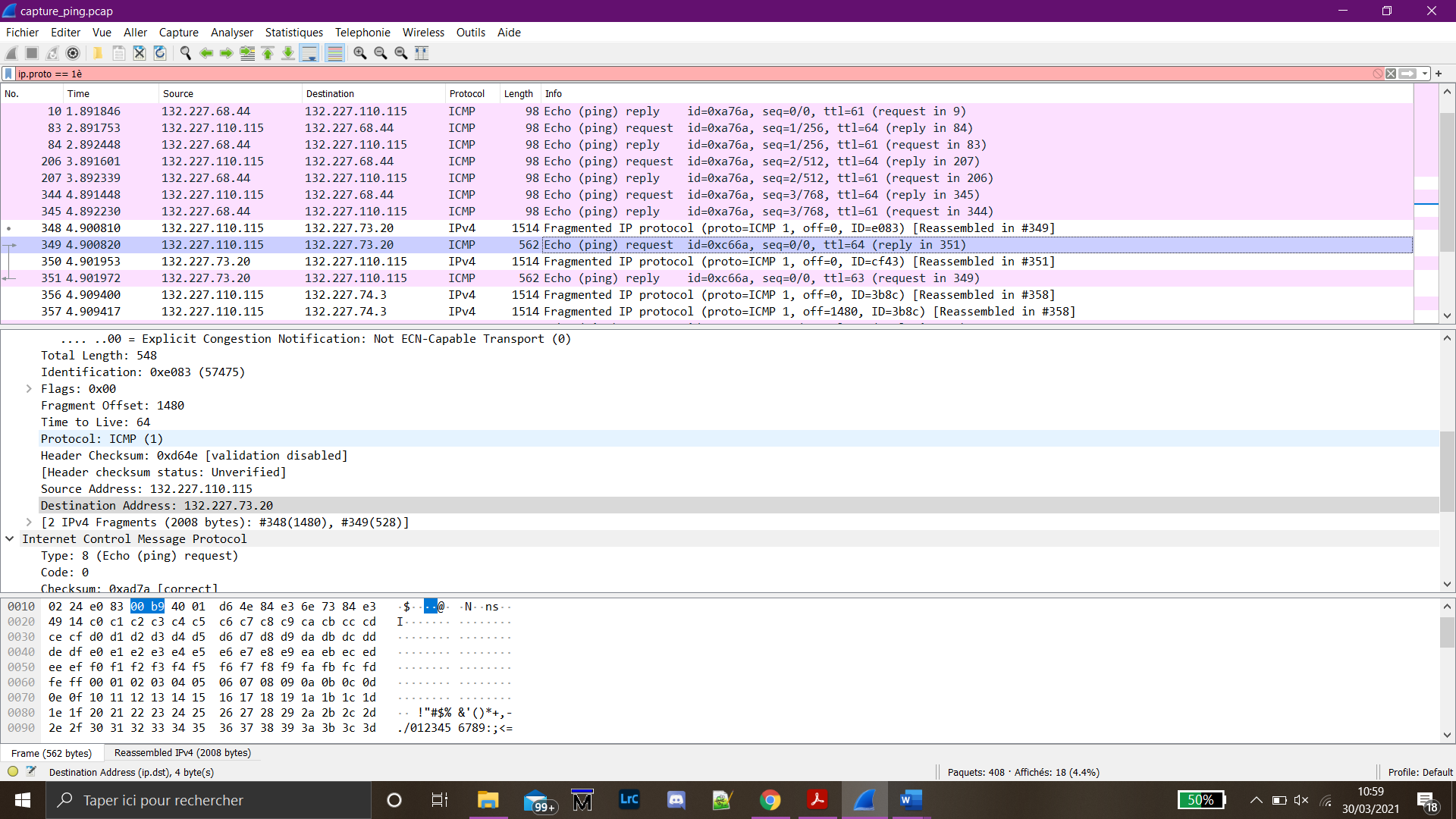
Ententes ICMP :

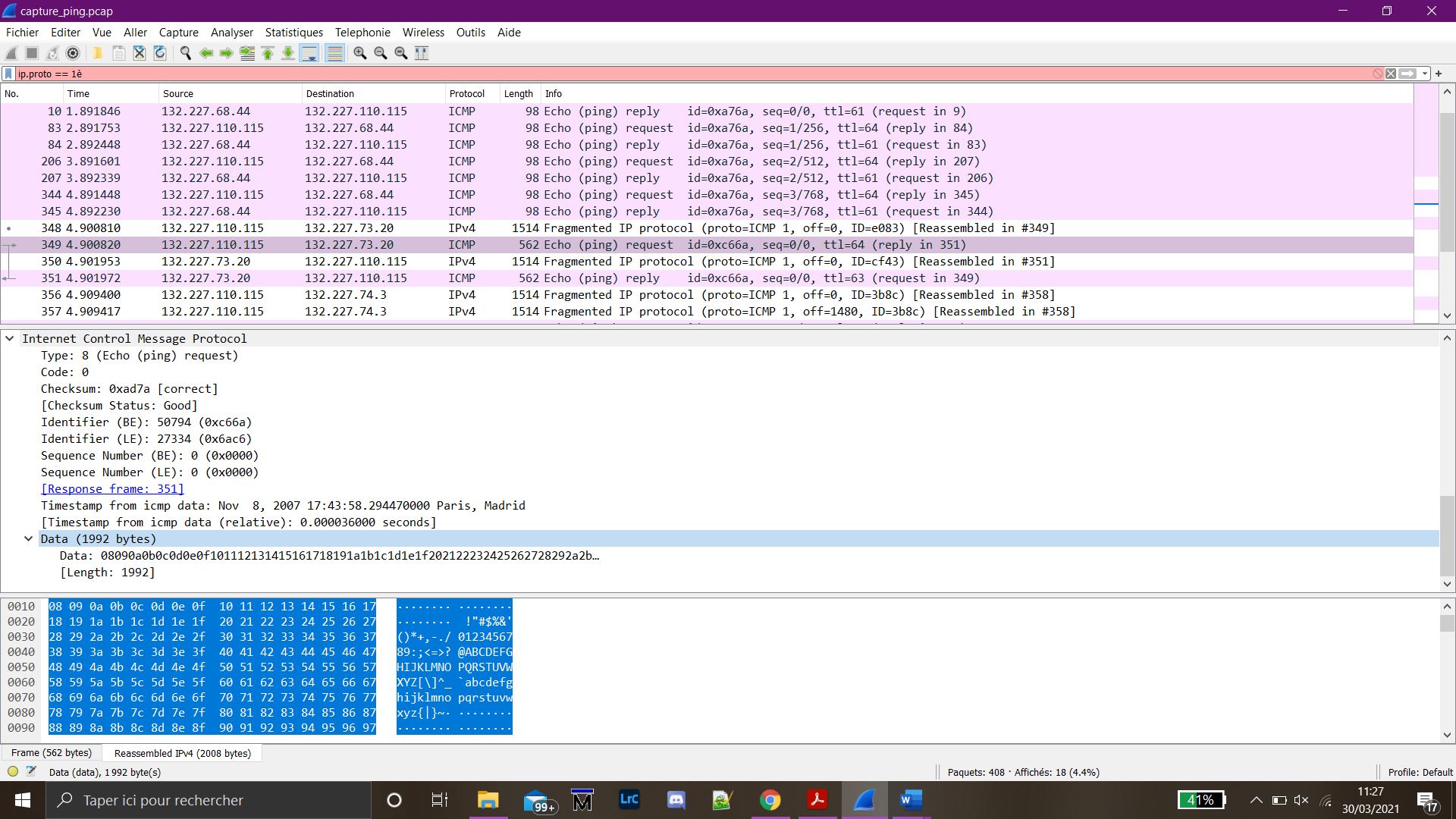
9 83 206 344

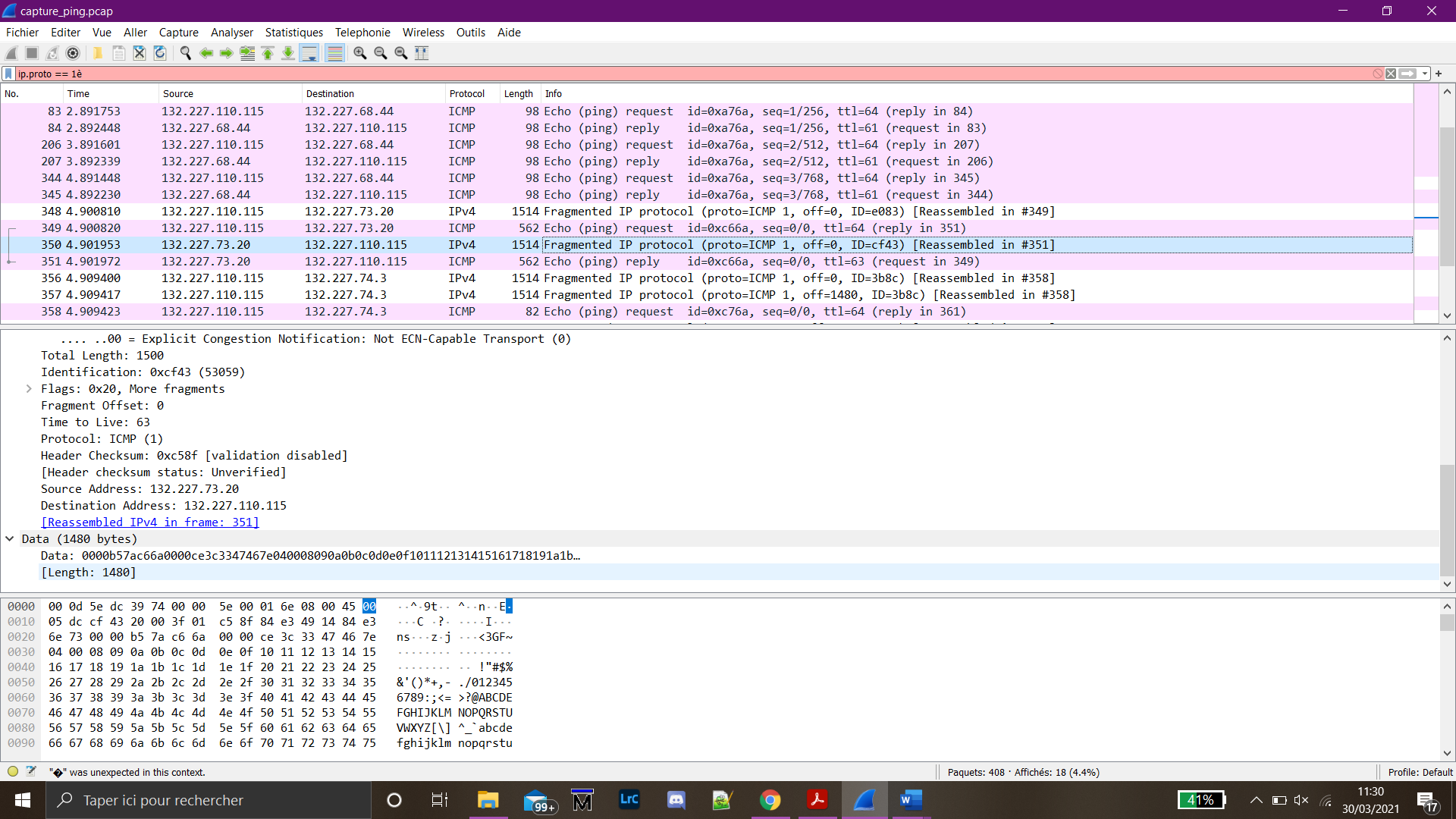
On remarque que le champ Checksum.

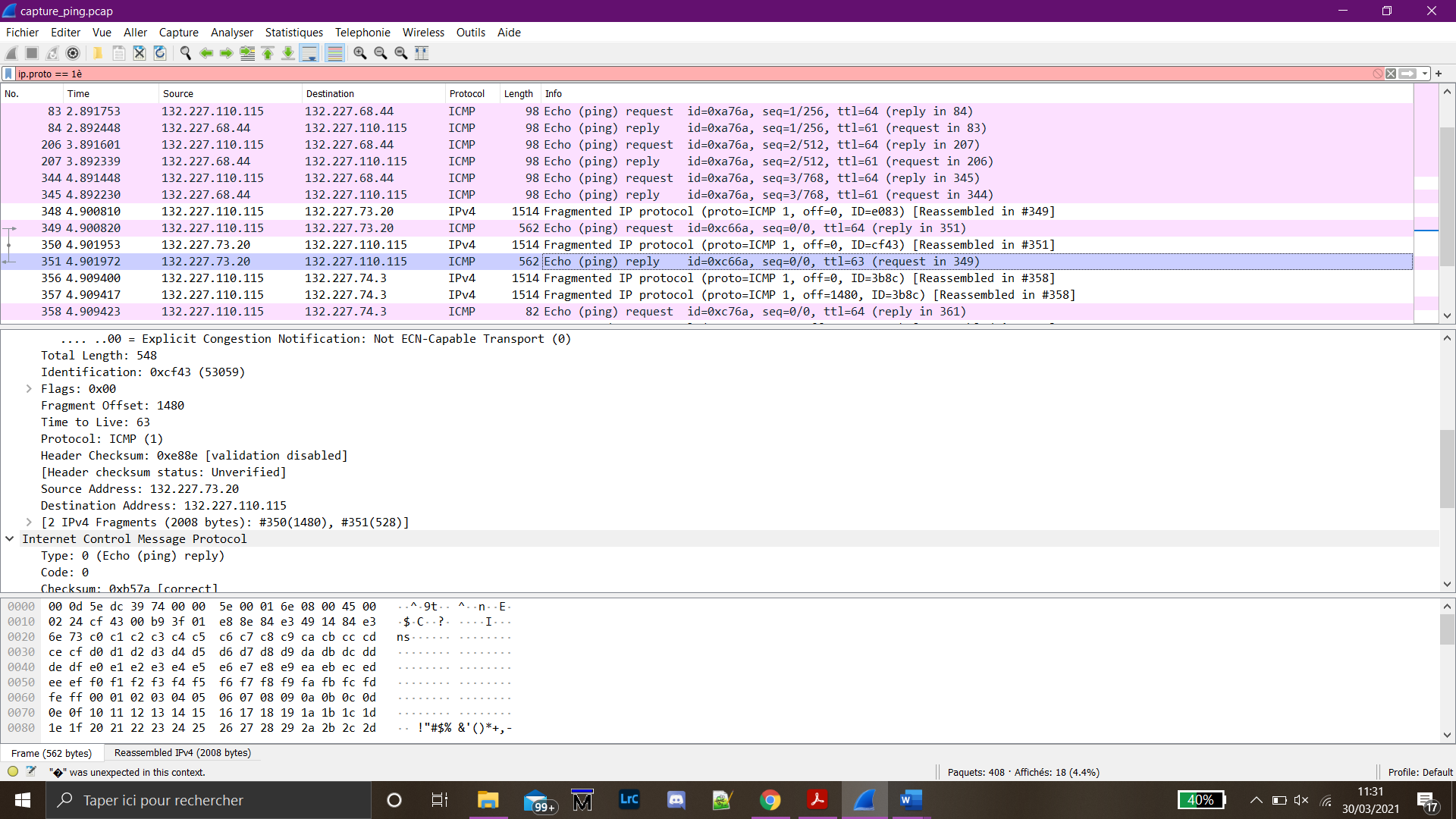
* 1. Le champs Flags dans l’entête de l’IP, indique More fragments. Cela vaut dire que le message a été fragmenté. On remarque que ce fragment prend la taille maximum de 1500 octets.
  2. Le champs Fragment Offset indique le numéro de fragment. Dans ce cas, le champ indique 0. En regardant le champ Flags 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.



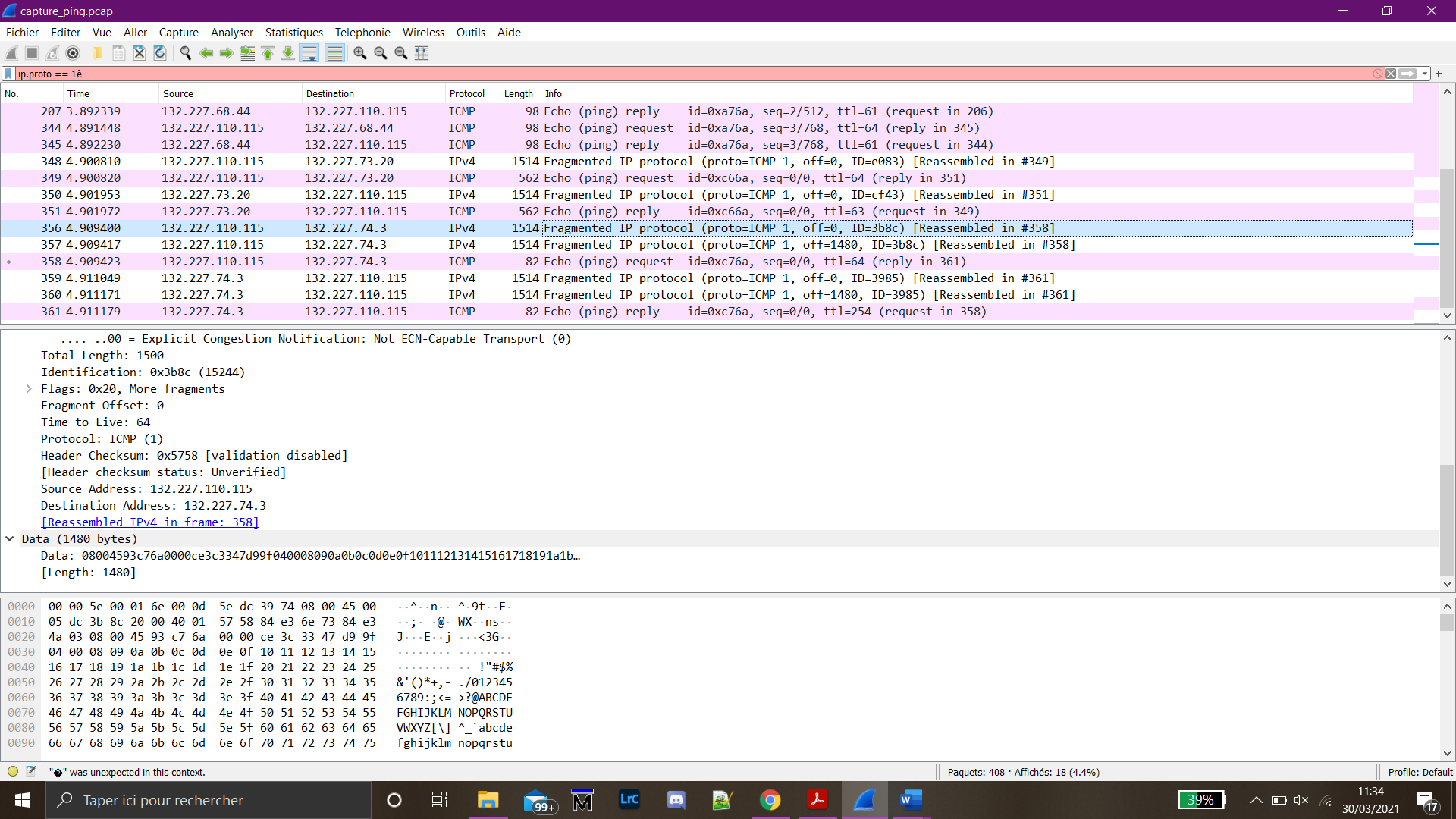
* 1. La longueur totale de ce fragment sera de 1500-20, donc de 1480 octets.
  2.  L’adresse de destination est de « 132.227.73.20 »
  3. Dans l’entête le champ Fragment Offset indique la valeur 1480, donc il commence à partir d’un grand paquet. Ceci indique qu’une partie de ce paquet a été déjà envoyé dans des trames précédentes. Donc ce n’est pas la première trame.
  4.  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.
  5. Ce fragment est de 548 octets
  6. 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.

* 1. 



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.

* 1. 

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.

