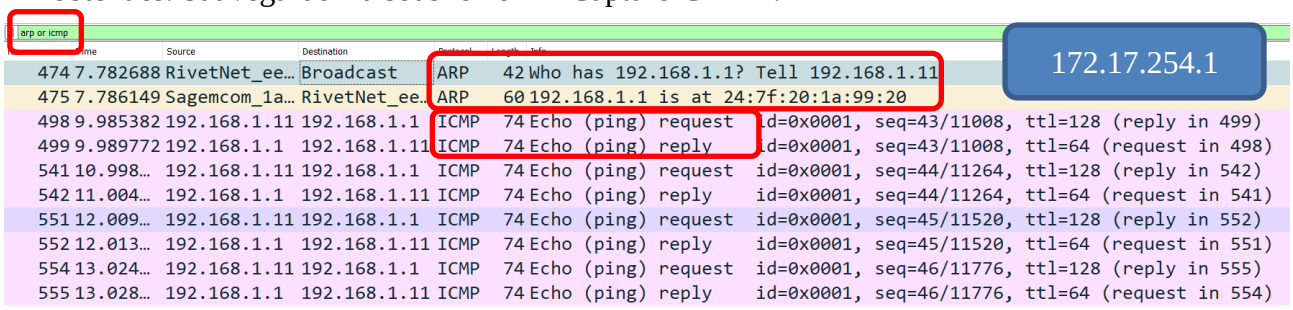
Sommaire

4.1. Capture de trames ARP et ICMP.

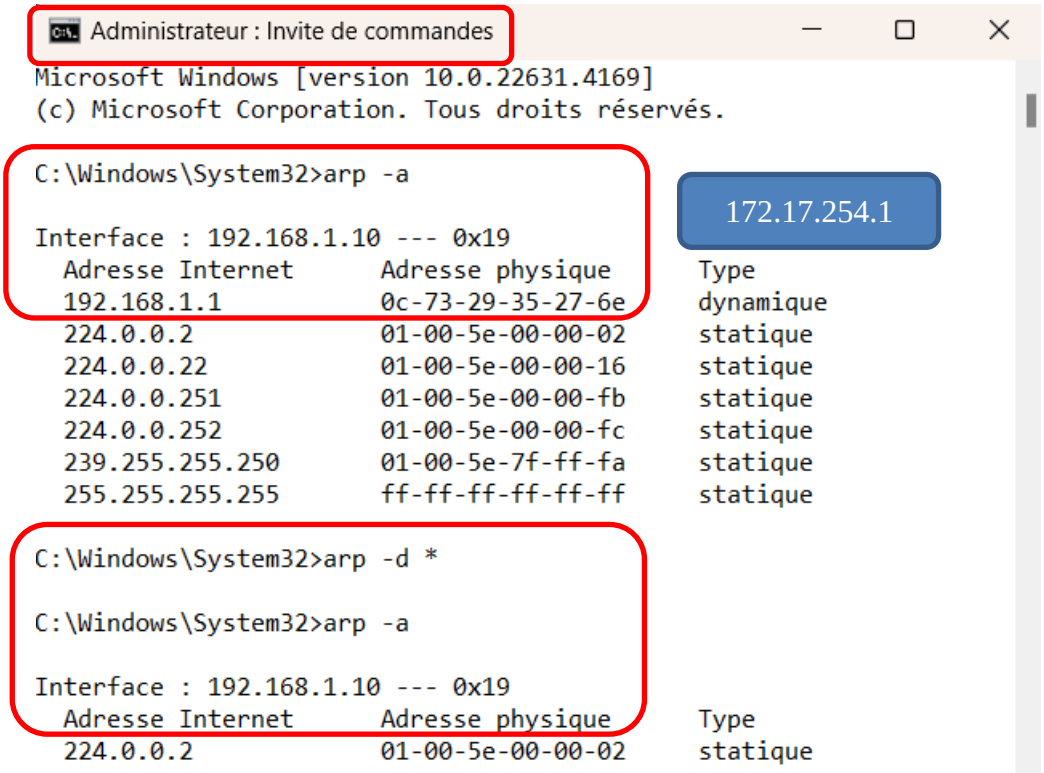
Vous allez capturer les trames ICMP générées par la saisie d'une commande **ping** depuis votre machine physique.

- Ouvrez Wireshark et démarrez une capture de trames.
- Pinguez le serveur ROI (172.17.254.1). Effectuez une capture d'écran.
- L'échange démarre avec une requête et une réponse ARP pour obtenir l'adresse MAC du serveur ROI. Ensuite l'échange de trames ICMP a lieu. Arrêtez la capture une fois les 8 trames ICMP obtenues. Sauvegardez la sous le nom « CaptureICMP ».



	Time	Source	Destination	Protocol	Length	Info
474	7.782688	RivetNet_ee…	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.11
475	7.786149	Sagemcom_1a…	RivetNet_ee…	ARP	60	192.168.1.1 is at 24:7f:20:1a:99:20
498	9.985382	192.168.1.11	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=43/11008, ttl=128 (reply in 499)
499	9.989772	192.168.1.1	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=43/11008, ttl=64 (request in 498)
541	10.998…	192.168.1.11	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=44/11264, ttl=128 (reply in 542)
542	11.004…	192.168.1.1	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=44/11264, ttl=64 (request in 541)
551	12.009…	192.168.1.11	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=45/11520, ttl=128 (reply in 552)
552	12.013…	192.168.1.1	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=45/11520, ttl=64 (request in 551)
554	13.024…	192.168.1.11	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=46/11776, ttl=128 (reply in 555)
555	13.028…	192.168.1.1	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=46/11776, ttl=64 (request in 554)

☞ **Si vous ne visualisez pas d'échange ARP**, videz le cache ARP (ouvrir une invite de commandes en tant qu'administrateur et saisir la commande **arp –d ***) puis recommencez une nouvelle capture et ressaisissez la commande ping.



- Après la saisie de la commande ping et la capture des trames ARP/ICMP, arrêtez cette dernière et consultez le contenu du cache ARP : vérifiez la présence de l'association @IP-@MAC correspondant à ROI (capture d'écran à réaliser).
- A l'aide du **Chapitre 5 (page 2)**, analysez l'échange de trames ARP (Request et Reply) précédant l'échange de trames ICMP :

  Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?

  _____

  Quelle est la fonction de la trame ARP Request ?

  _____

  Quelle signification ont les octets de position 0×04 et 0×05 ligne 0010 ?

  _____

  Quelle est la longueur d'un message ARP contenu dans la trame ? _____

  Quelle est la longueur de la trame ARP Request ? _____

  Quelle est la longueur de la trame ARP Reply ? _____

  Combien d'octets sont utilisés pour le padding ? _____

- Complétez les rubriques ci-dessous :

Trame ARP request
@MAC destination = @MAC source = Ethernet Type =
Opcode (valeurs hexa.) = @MAC de la cible = @IP de la cible =

  N'oubliez pas que la « Target MAC address » est la question associée à la trame ARP Request.

- Sélectionnez une trame ICMP Echo Request. A l'aide du **Chapitre 5 (pages 4 et 5)**, répondez aux questions suivantes :

  Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?

  _____

  Quelle signification a l'octet de position 0×07 ligne 0010 ?

  _____

  Quelle est la longueur de la trame ? _____

  Quelle est la longueur du paquet IP ? _____

  Quelle est la longueur du message ICMP ? _____

  Quelle signification a l'octet de position 0×02 ligne 00020 ?

  _____

  A quoi correspondent les octets à partir de l'octet 0×0A, ligne 00020 ? _____

  _____

- Sélectionnez une trame ICMP Echo Reply. Quelle est le nom et la valeur de l'octet de position 0×02 ligne 00020 ?

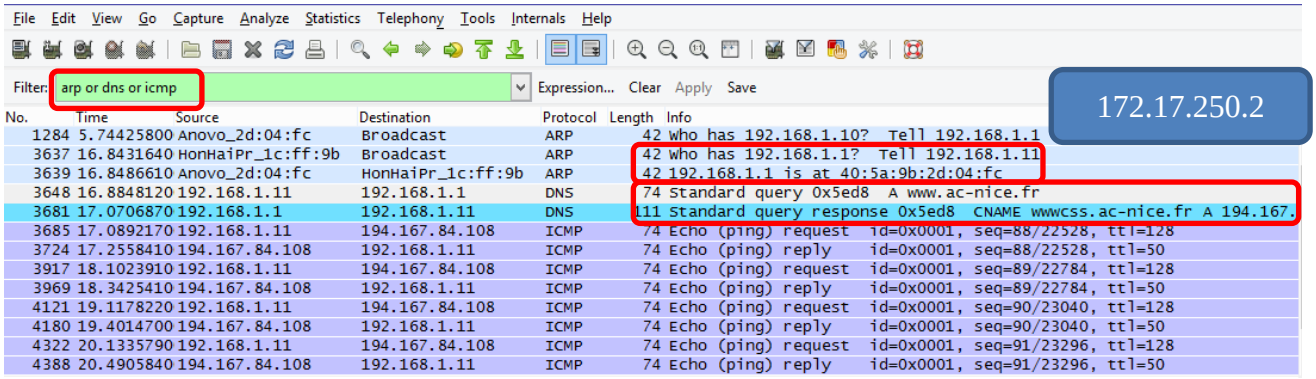
  _____

4.2. Capture de trames ARP, DNS et ICMP.

- Démarrez une capture de trames depuis votre machine physique.
- Ouvrez une invite de commandes, videz le cache ARP (commande **arp -d ***) puis effectuez une requête ping vers le serveur web www.**ac-nice.fr** (ping « nom » et non plus ping « @IP ») :

```
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.22631.4169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\System32>ping www.ac-nice.fr

Envoi d'une requête 'ping' sur cs234.wpc.alphacdn.net [93.184.221.161] avec 32 octets de données :
Réponse de 93.184.221.161 : octets=32 temps=17 ms TTL=55
Réponse de 93.184.221.161 : octets=32 temps=20 ms TTL=55
Réponse de 93.184.221.161 : octets=32 temps=22 ms TTL=55
Réponse de 93.184.221.161 : octets=32 temps=20 ms TTL=55

Statistiques Ping pour 93.184.221.161:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 17ms, Maximum = 22ms, Moyenne = 19ms

C:\Windows\System32>
```

- Arrêtez la capture et sauvegardez la sous le nom « CaptureIcmpDns » :



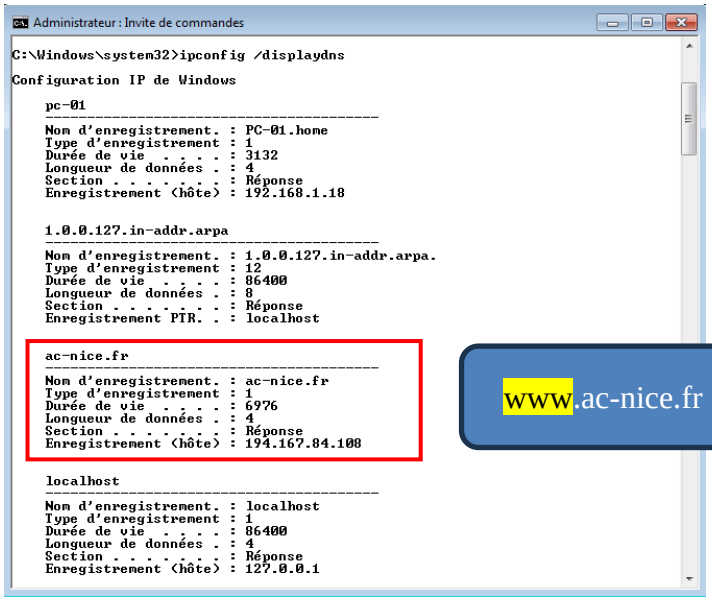
- La liste des trames commence par une requête et une réponse ARP. Quelle est l'adresse MAC recherchée ? _____
- Complétez les rubriques ci-dessous :

Trame ARP request
@MAC destination = @MAC source = Ethernet Type =
Opcode (valeurs hexa.) = @MAC de la cible = @IP de la cible =

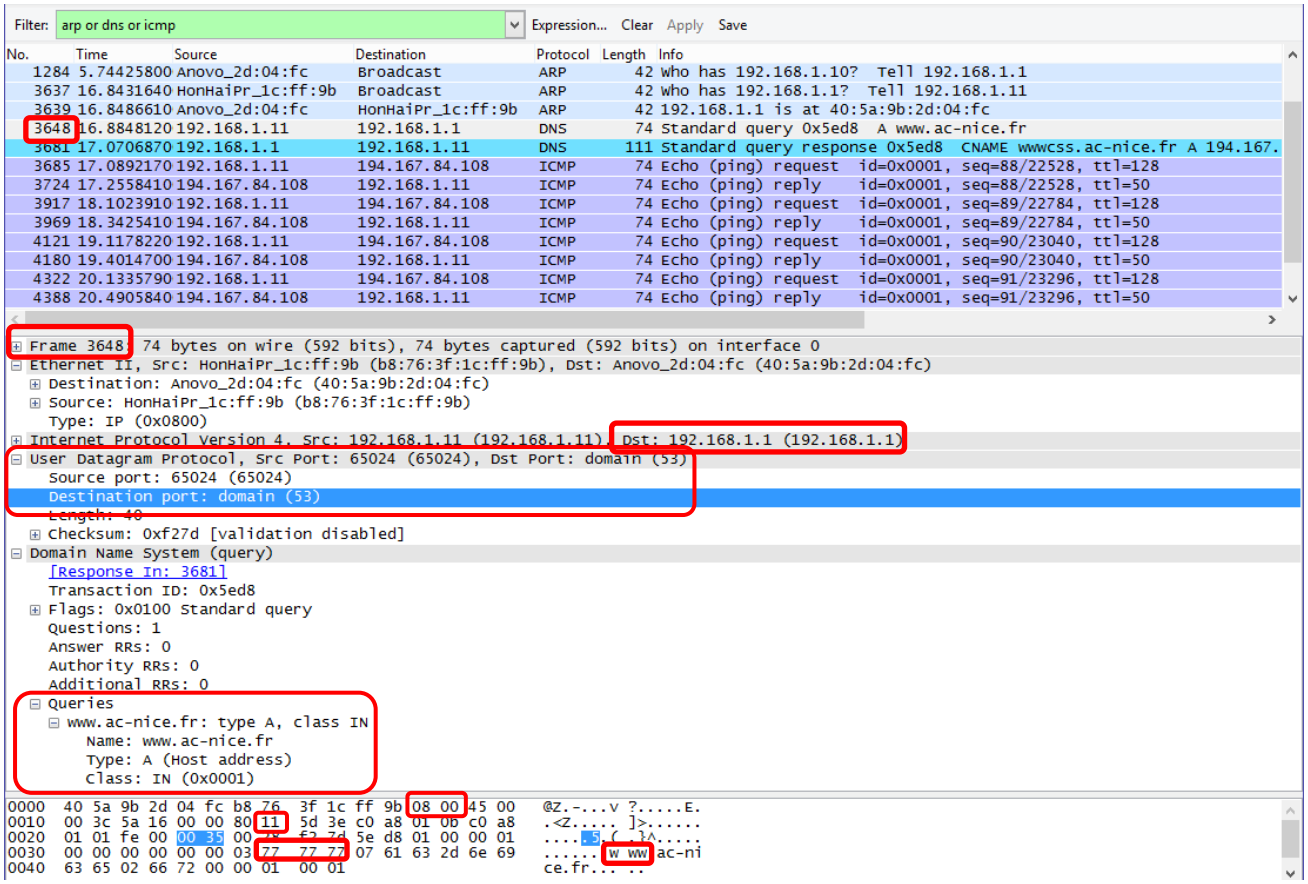
- Pour quelle raison trouve-t-on ensuite une requête DNS avant l'échange de trames ICMP suite à l'exécution de la commande ping proprement dite ?

_____

- Consultez le cache DNS à l'aide de la commande **ipconfig /displaydns** et vérifiez la présence de l'**enregistrement DNS** ac-nice.fr et de l'adresse IP associée :



- Démarrez une nouvelle capture et ressaisissez la commande **ping www.ac-nice.fr** dans l'invite de commandes. Vous ne devriez pas constater de requête DNS puisque l'enregistrement est présent dans le cache DNS.
- Videz le cache DNS à l'aide de la commande **ipconfig /flushdns** et redémarrez une nouvelle capture afin de visualiser de nouveau une requête DNS (capture d'écran à faire) :



- Quels sont les différents protocoles encapsulés dans une trame DNS ?

_____

- Quelle est la machine destinataire de la requête DNS ? Quelle est son IP (en-tête IP) ?

_____

- Quelle signification ont les octets de position 0×0C, 0×0D ligne 0000 et 0×07 ligne 0010 ?

  _____

- Quelle signification ont les octets de position 0×04 et 0×05 ligne 0020 ?

  _____

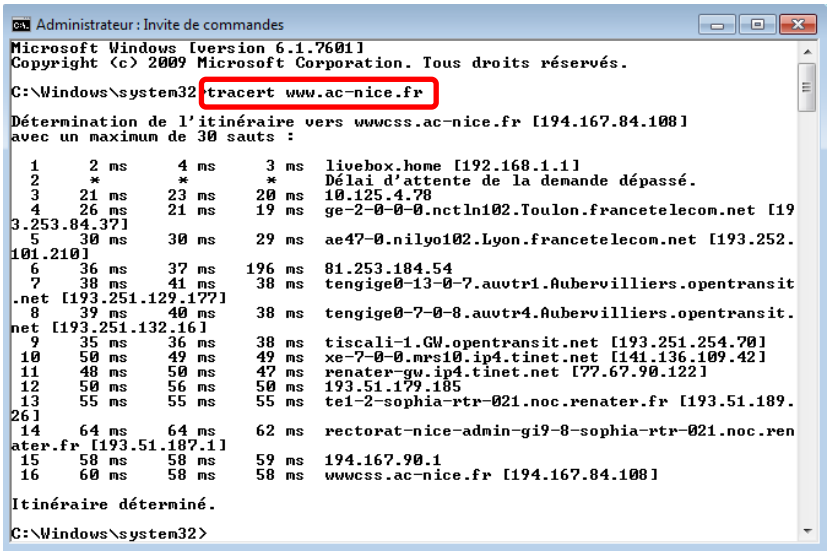
- Développez la section **Domain Name System (query)** et plus précisément la rubrique **Queries**. Quels sont les valeurs hexadécimales des octets correspondant au nom de domaine internet ac-nice.fr ? _____

- Sélectionnez la trame comportant la réponse à la requête DNS et développez la section **Domain Name System (response)** et plus particulièrement la rubrique **Answers**. Recherchez les valeurs hexadécimales et décimales de l'adresse IP du serveur web hébergeant le site de l'académie de Nice. _____

4.3. Commande Tracert et capture de trames ICMP.

→ On a vu que la commande **ping** génère deux types de message ICMP : une machine émet une trame **Echo request** (type 8) à laquelle répond la machine destinataire avec un message **Echo reply** (type 0). Lorsque l'on arrive à pinguer une autre machine, on en déduit que les couches 1, 2 et 3 sont opérationnelles sur toutes les machines participant à l'échange de trames (ICMP est un protocole de la couche 3) et que, en conséquence, le routage est fonctionnel dans les deux sens.

→ La commande **tracert** permet de connaître tous les routeurs entre la machine locale et une destination donnée, par exemple le site web de l'Académie de Nice (**tracert www.ac-nice.fr**) :



Elle génère l'envoi de messages ICMP **Echo request** dans le but de recevoir en retour un **message automatique** ICMP **TTL exceeded** de la part des différents routeurs rencontrés **permettant ainsi d'obtenir leur adresse IP**.

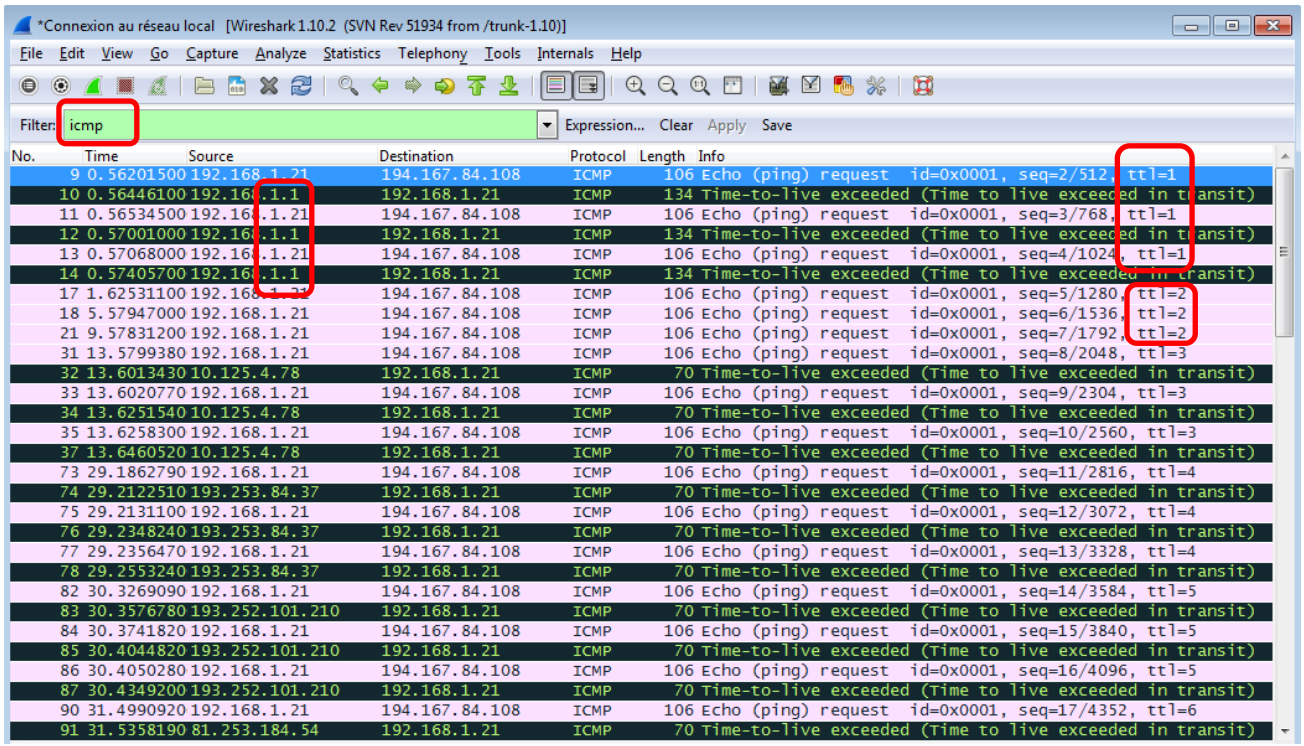
Comment faire pour provoquer l'envoi de ce message d'erreur par le premier routeur ? Il suffit de mettre le TTL à 1 dans la trame **Echo request** adressée au serveur web de l'Académie de Nice. Le premier routeur rencontré (le routeur Cisco 172.17.250.2 ou la box chez vous) décrémente le TTL de 1 et le met donc à 0. Il supprime en conséquence le paquet reçu et renvoie un message d'erreur **TTL exceeded**. Ainsi, obtenons-nous son adresse IP.

Pour connaître l'adresse du second routeur, il suffit de mettre le TTL à 2 dans le message **Echo request** à destination du serveur web. Le TTL sera décrémenté de 1 lors du passage du premier routeur qui routera le paquet reçu vers le second routeur. Celui-ci décrémente à son tour le TTL

de 1 et le met donc à 0. Il supprime en conséquence le paquet reçu et renvoie un message d'erreur **TTL exceeded**. Ainsi, obtenons-nous également son adresse IP.

Et ainsi de suite jusqu'à la destination finale.

- Démarrez une capture de trames depuis votre machine physique.
- Ouvrez une invite de commandes et saisissez la commande **tracert www.ac-nice.fr.**
- Une fois l'itinéraire déterminé, arrêtez la capture et sauvegardez la sous le nom « CaptureTracert ».
- Limitez l'affichage des trames à celles encapsulant le protocole ICMP (zone **Filter**) :



- Sélectionnez la première trame ICMP **Echo request**. Développez l'**en-tête IP**. Quelle est l'adresse IP **Destination** (valeurs déci. et hexa.) ? _____
- Sélectionnez le champ **TTL**. Quelle est la valeur portée par ce champ (valeurs déci. et hexa.) ?

  _____
- Développez la section correspondant au message ICMP. Quelle est la valeur portée par le champ **Type** (valeurs déci. et hexa.) ? _____
- Sélectionnez la trame, comportant un message d'erreur ICMP **Time-to-live exceeded**, envoyée par le premier routeur rencontré. Développez la section correspondant au message ICMP. Quelle est la valeur portée par le champ **Type** (valeurs déci. et hexa.) ?

  _____