

Encadré Par :

Pr : FARISS Meriam

Présenté Par :

MAFTOUH Omar

KHADIM Mohamed Hamza

Université Sultan Moulay Slimane Faculté Polydisciplinaire Béni Mellal

Département INFORMATIQUE (MIP)

Filière : Science de données et sécurité des systèmes d’information

A.U : 2023-2024

Module : Réseaux Informatiques

Sujet

**Rapport TP01**

**Partie Pratique1 : ICMP**

**Commande ping :**

* Command **ping -n 10** [**www.google.fr**](http://www.google.fr)

C:\Users\HP>ping -n 10 www.google.fr

Envoi d’une requête 'ping' sur www.google.fr [172.217.168.163] avec 32 octets de données :

Réponse de 172.217.168.163 : octets=32 temps=227 ms TTL=116

Réponse de 172.217.168.163 : octets=32 temps=194 ms TTL=116

Réponse de 172.217.168.163 : octets=32 temps=92 ms TTL=116

Réponse de 172.217.168.163 : octets=32 temps=223 ms TTL=116

Réponse de 172.217.168.163 : octets=32 temps=203 ms TTL=116

Réponse de 172.217.168.163 : octets=32 temps=112 ms TTL=116

Réponse de 172.217.168.163 : octets=32 temps=160 ms TTL=116

Délai d’attente de la demande dépassé.

Réponse de 172.217.168.163 : octets=32 temps=144 ms TTL=116

Réponse de 172.217.168.163 : octets=32 temps=295 ms TTL=116

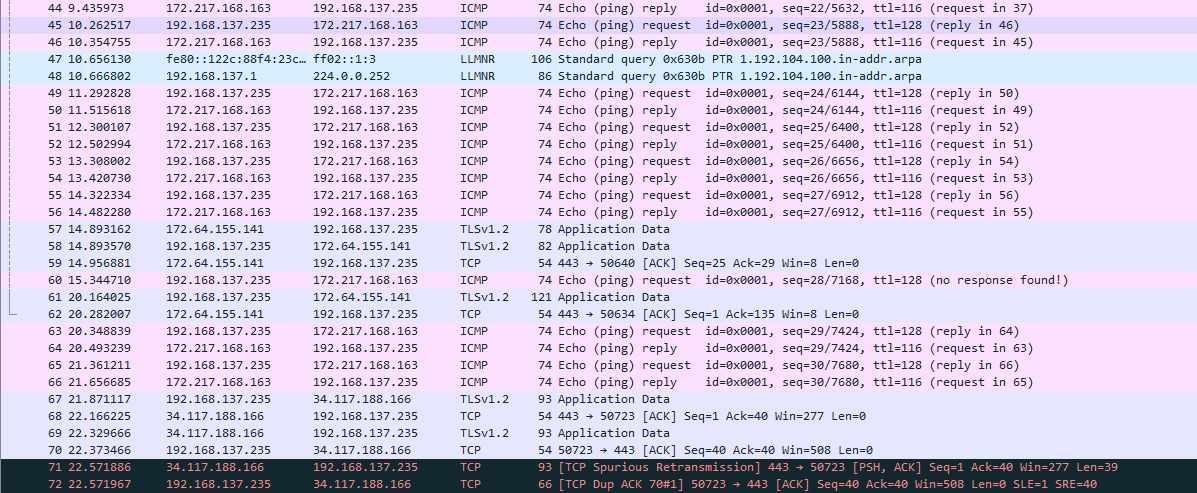
Statistiques Ping pour 172.217.168.163:

Paquets : envoyés = 10, reçus = 9, perdus = 1 (perte 10%),

Durée approximative des boucles en millisecondes :

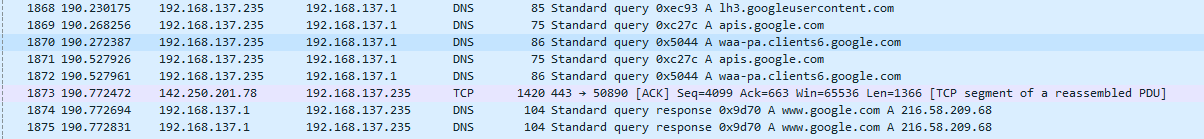
Minimum = 92ms, Maximum = 295ms, Moyenne = 183ms

* Capture lorsque l’invite de commande réapparait à la console

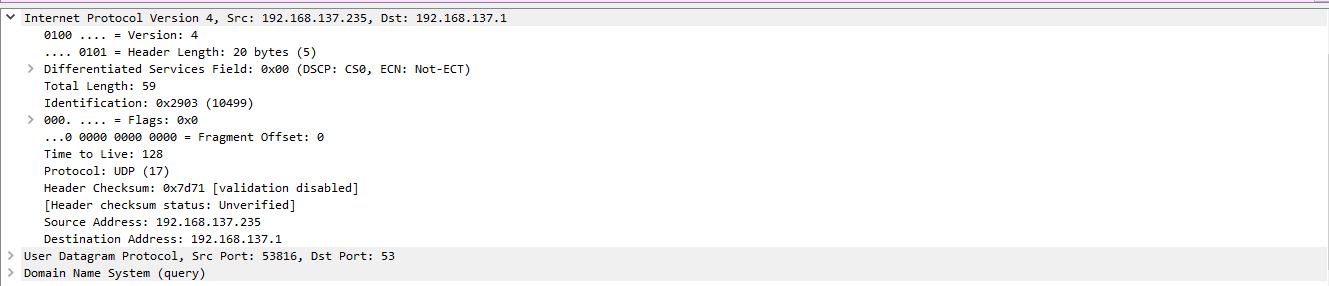


**Analyse avec ping :**

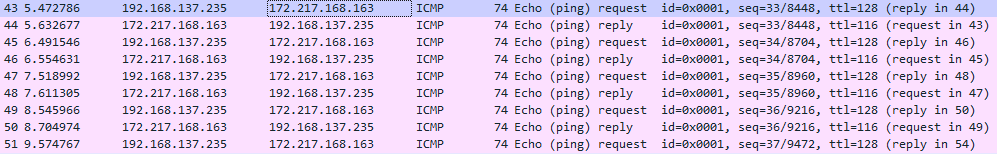
1. Les protocoles indiqués dans la colonne Protocol de la fenêtre de liste des trames capturées

sont comme suit :

Il est possible que les paquets ICMP soient précédés par un échange de requêtes et de réponses DNS.

1. L’adresse IP renvoyée avec la réponse DNS

**Message ICMP « Echo Request »**



Question 01 :

* L’adresse IP de destination du paquet est : **172.217.168.163**
* La valeur du champ Protocol Type et la valeur du champ Time to Live :

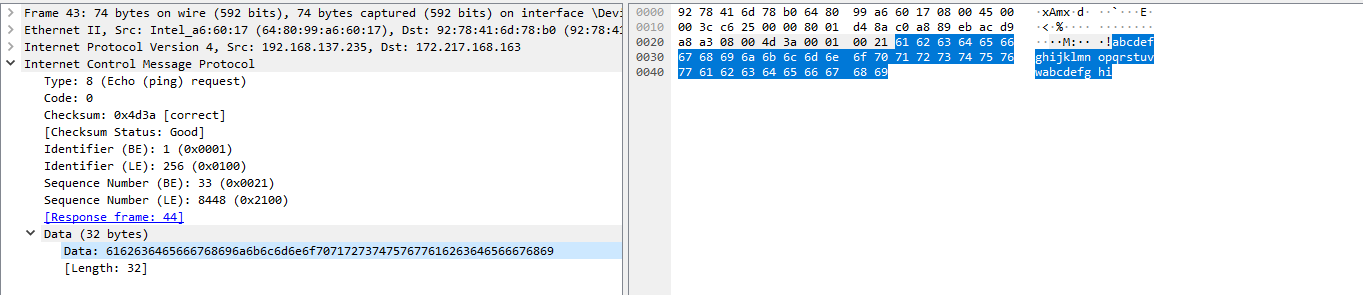


Question 02 :

* Le type de message ICMP est octale, l’identificateur de message 0x0001 et le numéro de séquence 1/256

Question 03 :

* Utilisez la souris pour sélectionner les octets de données du message de requête, puis comparez-les avec les données affichées dans la fenêtre d'affichage brut

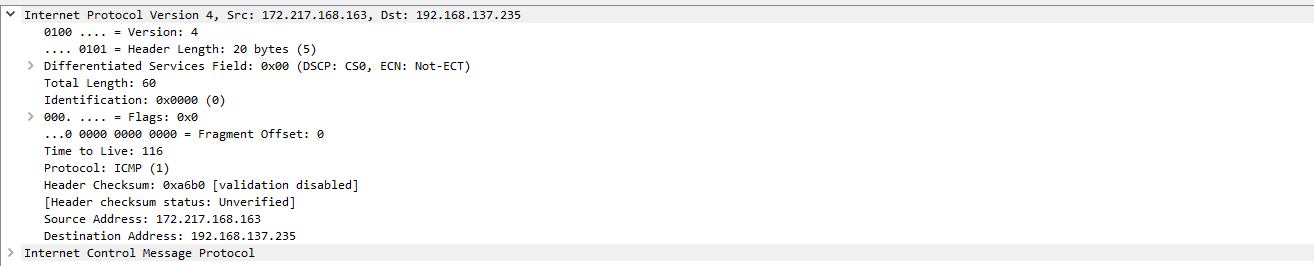


**Message ICMP « Echo Reply «**

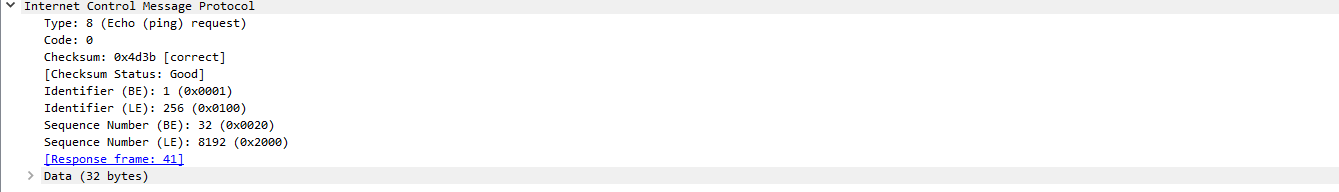
Question 01 :

* L’adresse IP source du paquet : **172.217.168.163**
* L’adresse IP destination du paquet : **192.168.137.235**
* La valeur du champ Protocol Type : **ICMP**

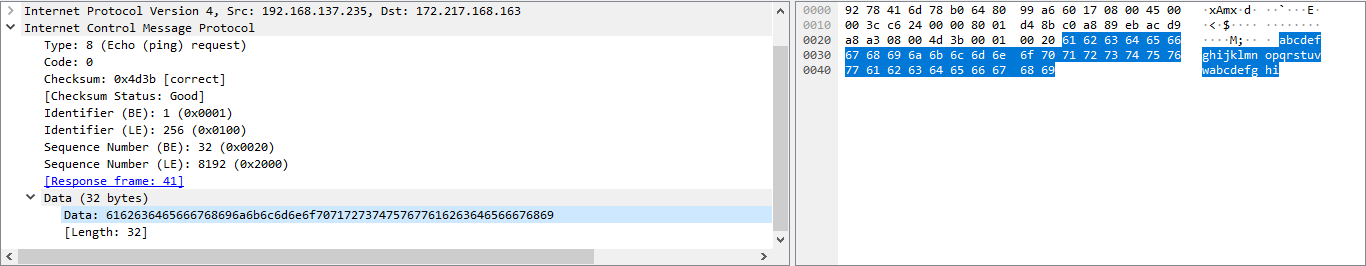
Question 02 :

* La valeur du champ Time to Live du message ICMP : **116**

Question 03 :



Question 04 :



**Commande tracer**

Commande **tracer** [**www.google.fr**](http://www.google.fr)

C:\Users\HP>tracert www.google.fr

Détermination de l’itinéraire vers www.google.fr [172.217.168.163]

avec un maximum de 30 sauts :

  1     2 ms     \*        2 ms  DESKTOP-HGSEJA0.mshome.net [192.168.137.1]

  2     \*        \*        \*     Délai d’attente de la demande dépassé.

  3    24 ms    12 ms     7 ms  100.104.192.1

  4    19 ms    17 ms     4 ms  172.31.253.1

  5    26 ms    14 ms    17 ms  192.168.100.1

  6    28 ms    27 ms    93 ms  105.73.33.158

  7    49 ms    58 ms    39 ms  172.20.14.198

  8    31 ms    29 ms    42 ms  142.250.174.134

  9    92 ms    32 ms    59 ms  142.250.213.243

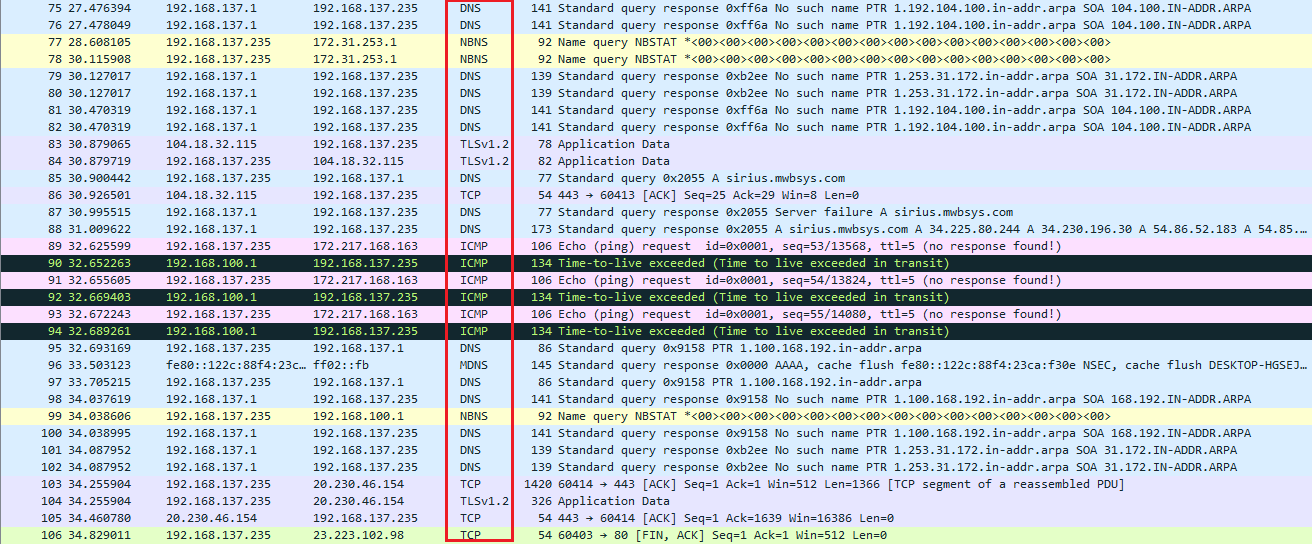
 10    40 ms    66 ms   104 ms  74.125.253.201

 11    32 ms    29 ms    42 ms  mad07s10-in-f3.1e100.net [172.217.168.163]

Itinéraire déterminé.

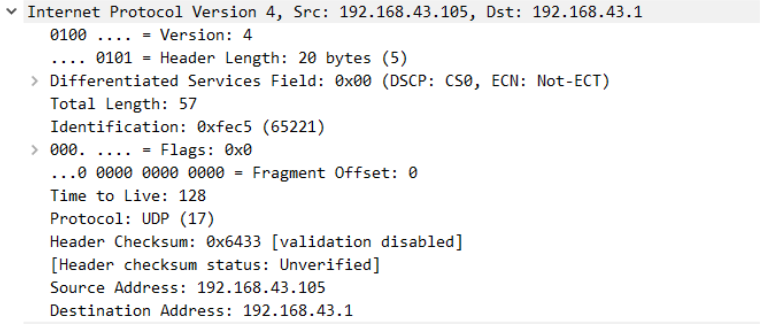
**Protocoles capturés**

1. Les protocoles indiqués dans la colonne protocol de la fenetre de la list des trames capturées sont : **DNS , TCP , NBNS , ICMP , TLSv1.2 , TLSv1.3 , DHCPv6 , UDP**

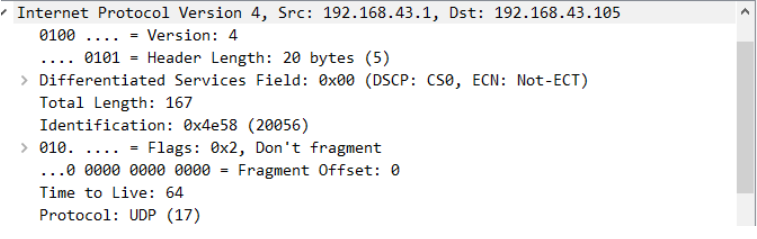
****

**Message UDP**

1. L'adresse IP destination du premier paquet contenant le message UDP : 192.168.43.1 , et les valeurs des champs sont avec Protocol Type et Time to Live :



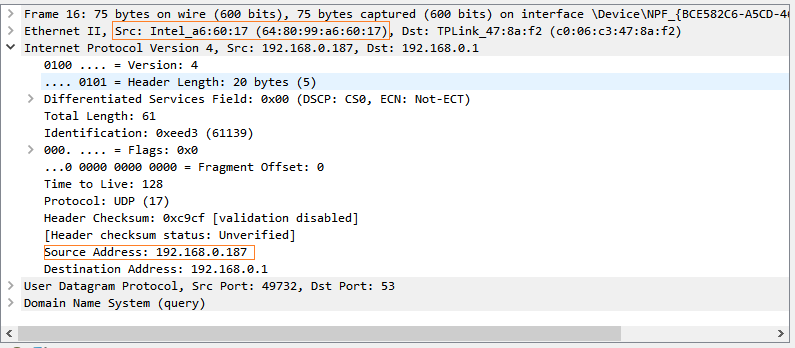
1. L’adresse IP relevée : 192.168.43.1 est différent à celle de la réponse DNS : **192.168.43.105**
2. Combien d'octets de données sont présents dans ce message de requête ?



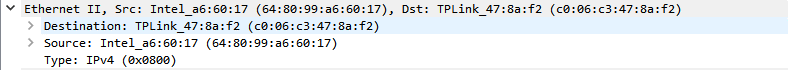
**Partie Pratique 2 : HTTP**

**Trame Ethernet , paquet IP et datagramme UD**

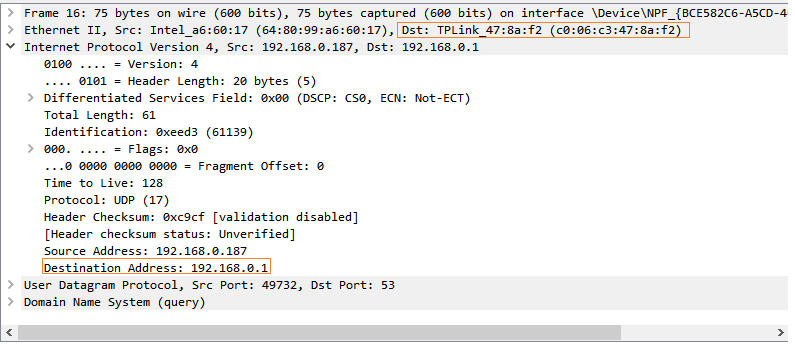
1. Les adresses MAC & IP du client :



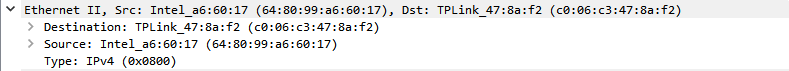
1. Le contenu du champ type de la trame ethernet :



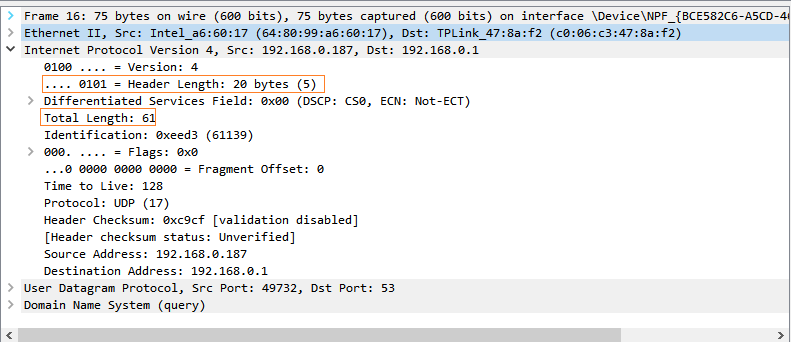
1. Les adresses MAC & IP du destination :



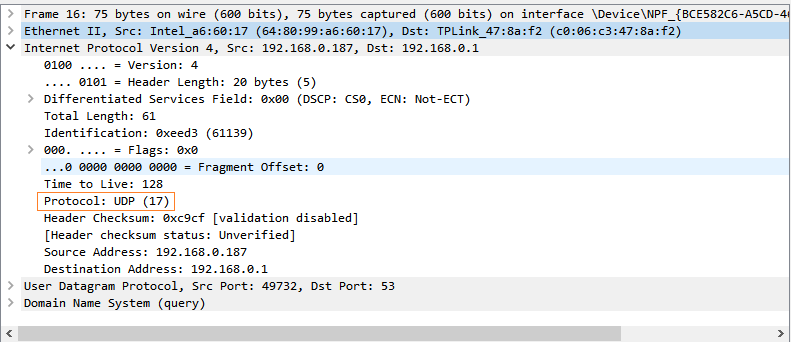
1. Les machines correspondent ces adresses :



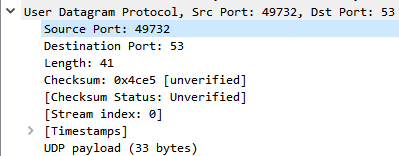
1. La taille de l’en-tête & longueur total du paquet :



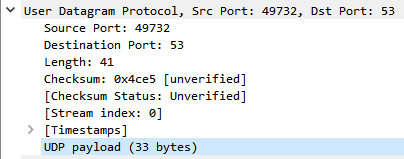
1. Type de protocole & numéro du type de protocole :



1. Les numéros ports du client/serveur , particularités & le protocole :



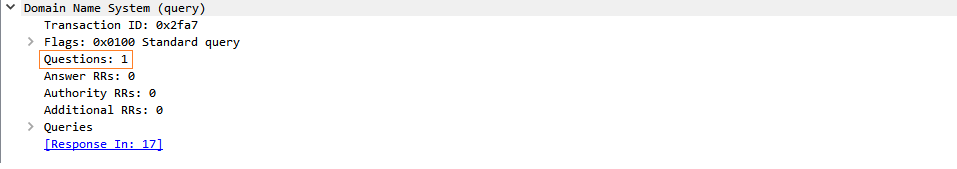
1. Longueur de l’en-tête UDP :



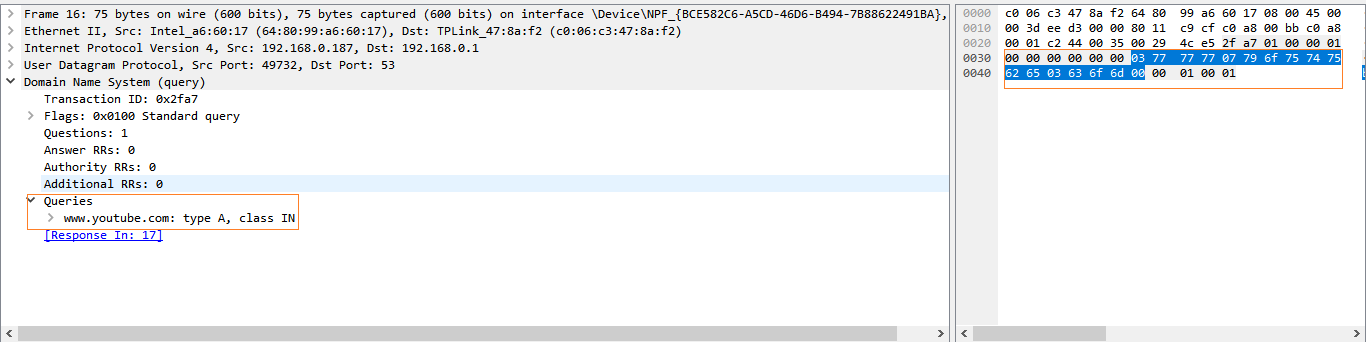
**Les deux valeurs sont différentes**

**Services DNS**

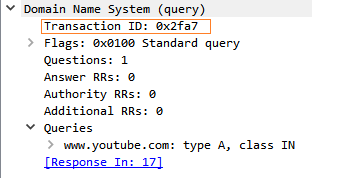
1. Le champ qu’indique que le message et une requête ou une réponse :



1. Les informations transposées dans le corps de la requête & le type et la classe de la requête :



1. L’identification de transaction de la requête :

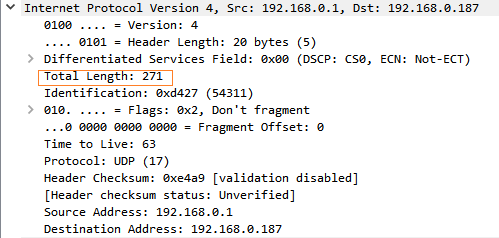


1. Les adresses MAC|Ethernet & IP du paquet :
   1. Adresse Source : **192.168.0.1**
   2. Adresse Déstination : **192.168.0.187**

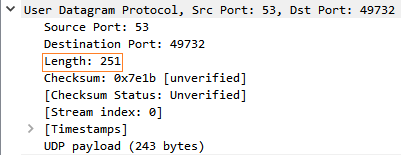


1. Taille du paquet IP du message UDP :

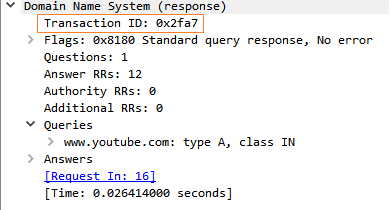
* Paquet IP :



* Message UDP :

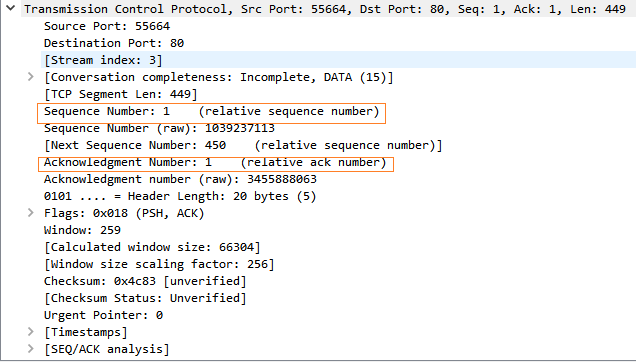


1. L’identification de transaction de la réponse :

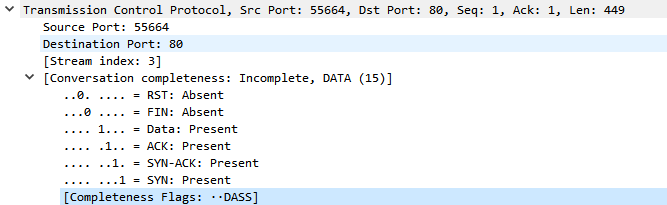


**Requête HTTP GET**

1. Numéro du séquence & acquittement de l’en-tête TCP :

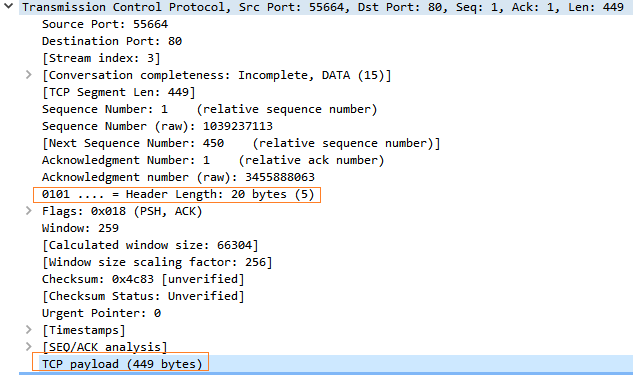


1. Les indicateurs d’état actif dans l’en-tête TCP :



* **Aucune réinitialisation de connexion (RST) ou demande de fermeture (FIN) n'est présente.**
* **Le segment contient des données et un numéro d'acquittement valide (ACK).**
* **Il s'agit d'une réponse SYN-ACK dans le processus d'établissement de connexion.**

1. La longueur de l’en-tête & la charge du message TCP :

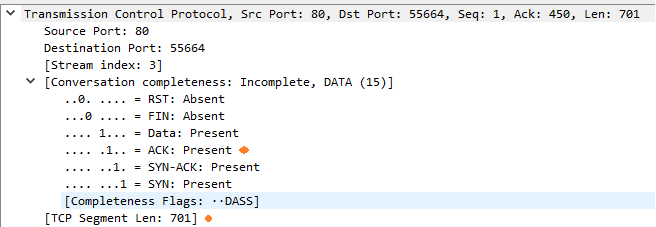


**Réponse HTTP**

1. Temps écoulé entre la capture du message GET & message de réponse :



1. Le serveur répond par un segment TCP ACK :



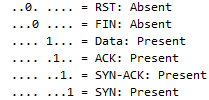
1. Le numéro de séquence émis par le serveur http :



1. La longueur de la charge dans l’en-tête TCP :



1. Les indicateurs d’état actifs de l’en-tête TCP :



* Le drapeau DATA indique la présence de données dans le segment TCP.
* ACK signifie que le segment contient un numéro d'acquittement valide.
* SYN-ACK indique une réponse au processus d'établissement de connexion TCP.
* SYN signifie qu'une demande de connexion a été initiée.

1. Le prochain numéro de séquence est **2** .