Architecture des réseaux – TP2 Encadré par PG

Jonathan Morgado-Samagaio Groupe : 3A

**Compte-rendu de TP réseau**

**Wireshark et HTTP**

Table des matières

[Réponses aux questions : 1](#_Toc68880444)

[Exercice 1 : Capture 1](#_Toc68880445)

[Exercice 2 : Pile réseau 1](#_Toc68880446)

[Exercice 3 : Dialogue http 3](#_Toc68880447)

[Conclusion : 4](#_Toc68880448)

# Réponses aux questions :

## Exercice 1 : Capture

Nous commençons par récupérer l’adresse IP de notre machine et le nom de l’interface réseau.

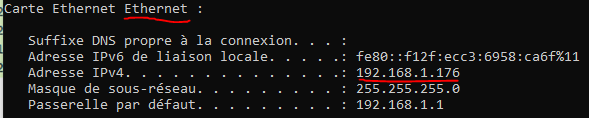


Figure : Résultat de ipconfig /all

Mon adresse est 192.168.1.176 et le nom de l’interface est Ethernet. En ayant la capture Wireshark d’activé, nous ouvrons le site et obtenons :

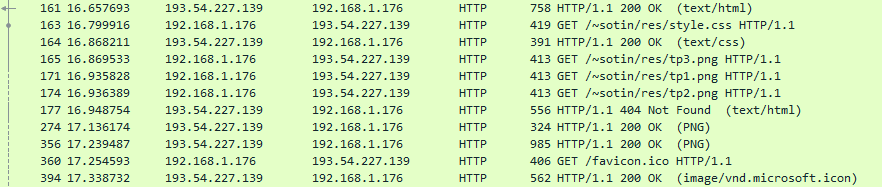


Figure : Résultat de la capture Wireshark

## Exercice 2 : Pile réseau

Nous allons examiner les différents éléments de la pile réseau.



Figure : Protocole TCP

Pour le protocole TCP, nous avons comme port source le port 49860 et comme port de destination le port 80.



Figure : Protocole IP

Pour le protocole IP, l’identifiant source est le : 192.168.1.176 et l’identifiant de destination est le : 193.54.227.139. Ce sont des adresses IP.

Nous savons que la source est mon pc avec le résultat de ipconfig /all du premier exercice.

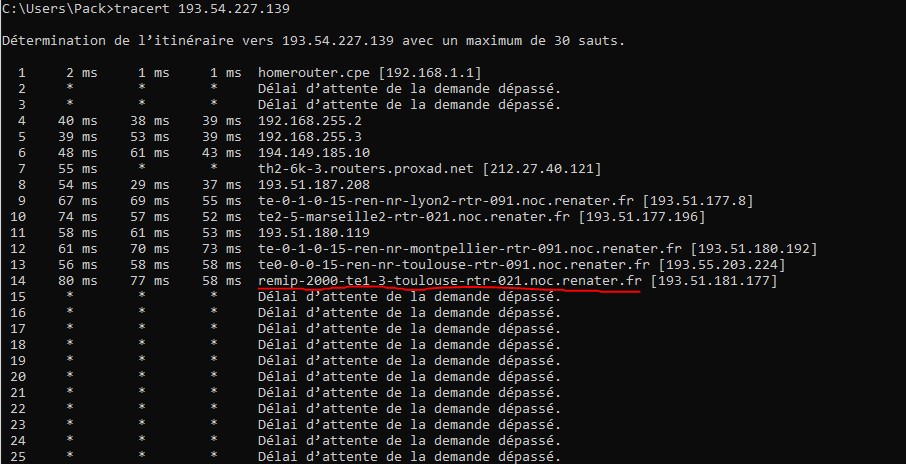


Figure : Résultat tracert 193.54.227.139

Nous pouvons voir que la source se trouve à Toulouse. Ca doit être le serveur de l’IUT que nous ne pouvons pas voir à cause des sécurités.



Figure : Couche Ethernet

Pour le protocole Ethernet, l’identifiant source est le : d0:27:88 :86:15:bb et l’identifiant de destination est le : 04:79:70:72:7d:5f. Ce sont des adresses MAC.

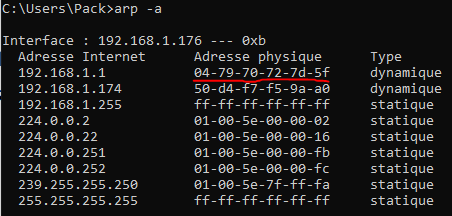


Figure : Résultat de arp –a

Nous pouvons voir que l’adresse de destination est l’adresse de mon routeur.

L’adresse source doit être l’adresse du serveur de l’IUT.

L’encapsulation consiste a mettre les données d’un protocole dans un autre.

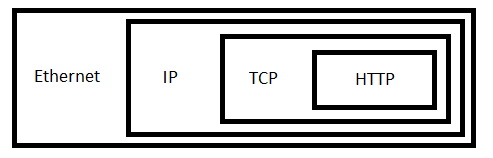


Figure : Croquis de l'encapsulation



Figure : Message PNG sélectionné



Figure : Fragments du message

Nous pouvons voir qu’il y a 33 fragments. La taille maximale est de 1384 octets. La taille totale du message st de 44 558 octets et c’est une image.

## Exercice 3 : Dialogue http

Voici le lien : <http://choregies.iut-blagnac.fr/~sotin/res/reseau.html>

Pour afficher ce lien dans une page HTML, nous utilisons la balise <a>.

Dans cette URL, le champ host est : choregies.iut-blagnac.fr, le port n’étant pas visible, celui par défaut est utilisé: c’est le port 80. Le champ chem\_abs est : /~sotin/res/reseau.html

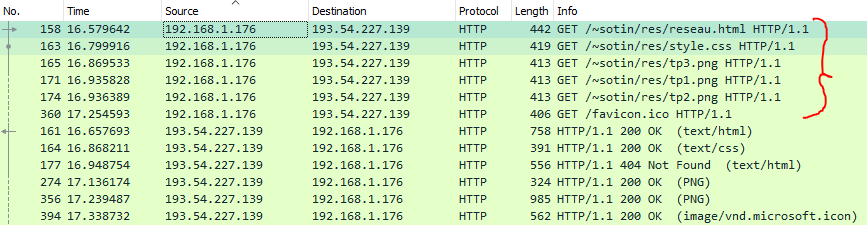


Figure : Résultat de Wireshark trié par sources

L’unique méthode http utilisé par mon navigateur est la méthode GET. Le protocole utilisé est le 1.1.

Format des réponses : Ligne\_état = Version\_HTTP SP Code\_état SP Raison CRLF

Dans les colonnes requête et réponse sont données les numéros des lignes Wireshark.

|  |  |  |
| --- | --- | --- |
| Requête | Réponse | Commentaire |
| 158 | 161 | Demande du corps de la page par le client et réponse positive du serveur. |
| 163 | 164 | Demande de la feuille de style par le client et réponse positive du serveur. |
| 165 | 177 | Demande d’une image par le client et réponse négative du serveur. |
| 171 | 274 | Demande d’une image par le client et réponse positive du serveur. |
| 174 | 356 | Demande d’une image par le client et réponse négative du serveur. |
| 360 | 394 | Demande de l’icône par le client et réponse positive du serveur. |

On nous a demandé de vider le cache avant la capture pour que toutes les requêtes soit effectué et pas que l’on récupère une donnée dans le cache.

Ce qui déclenche la première requête est l’appuie sur le lien qui demande au serveur le corps de la page. Un fois le corps de la page reçu, le client demande chaque information qu’il ne possède pas, donc ici la feuille de style, les images et l’icône.

# Conclusion :

Dans ce TP, nous avons vu comment utiliser Wireshark pour voir toutes les requêtes et réponses effectuées lors du chargement d’une page. Nous avons ensuite vu comment se découpais une requête avec les différents éléments de la pile comme la couche TCP, la couche IP et la couche Ethernet. Nous avons aussi vu que des messages lourds peuvent être fragmentés pour respecter la limite de poids. Nous avons ensuite vu comment se découper une URL et les messages reçu par Wireshark et pourquoi il y a eu toutes ces requêtes.