

UNIVERSITE DE PARIS 8 SAINT-DENIS

UFR STN – MASTER 1 MATHÉMATIQUES

PARCOURS CYBER SECURITE ET SCIENCES DES DONNEES

COURS DE RESEAUX INFORMATIQUES

RAPPORT TP : WIRESHARK

ENCADRE PAR L. BOUBCHIR

NOVEMBRE 2020

**RALAINARIVO
N. T. THIERRY**

November 21, 2020

TP-WIRESHARK

Contents

1	Introduction	2
2	Préparation du TP	3
3	Première capture du trafic	4
4	Capture et analyse d'une trame	7
5	Conclusion	8

1 Introduction

Wireshark est un logiciel open source utilisé pour "sniffer" le réseau. Il permet de voir en temps réel le flux internet qui voyage entre une source et la destination de la requête. Plusieurs protocoles sont installés sur Wireshark. Cela permet de faire un tri rapide en tant que filtre dans la pratique lors de l'analyse d'une trame internet.

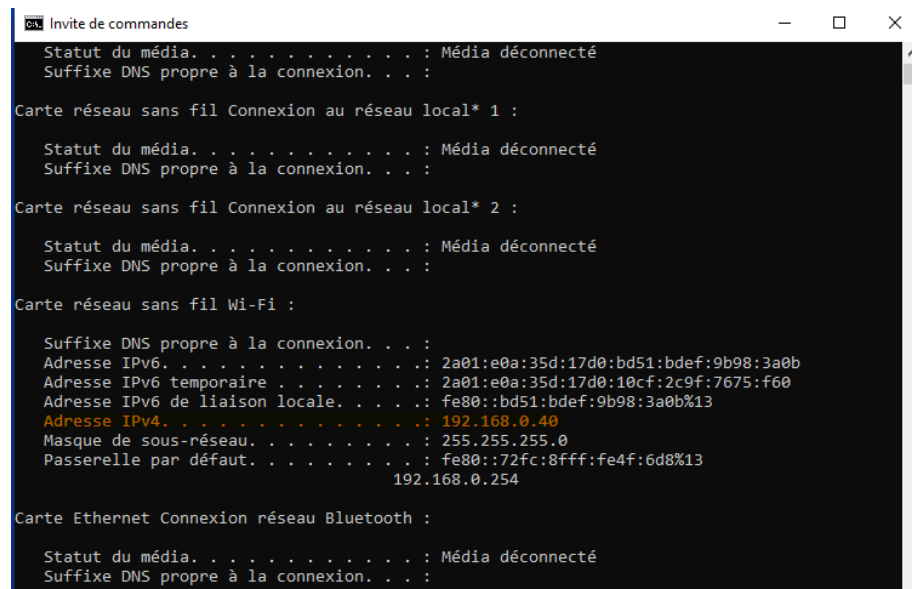
Faisons les étapes proposées dans le TP-Wireshark pour voir certains avantages et inconvénients de cet outil utile à l'opérateur réseaux.

Ce TP sera réalisé sur Windows 10.

2 Préparation du TP

J'ai téléchargé la version Wireshark-win64-3.4.0.

L'installation est très simple et rapide, il suffit de lancer l'exécutable. Avec la commande "**ipconfig**", l'adresse IP de ma machine est : 192.168.0.40.



```
Invite de commandes

Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . :

Carte réseau sans fil Connexion au réseau local* 1 :

Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . :

Carte réseau sans fil Connexion au réseau local* 2 :

Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . :

Carte réseau sans fil Wi-Fi :

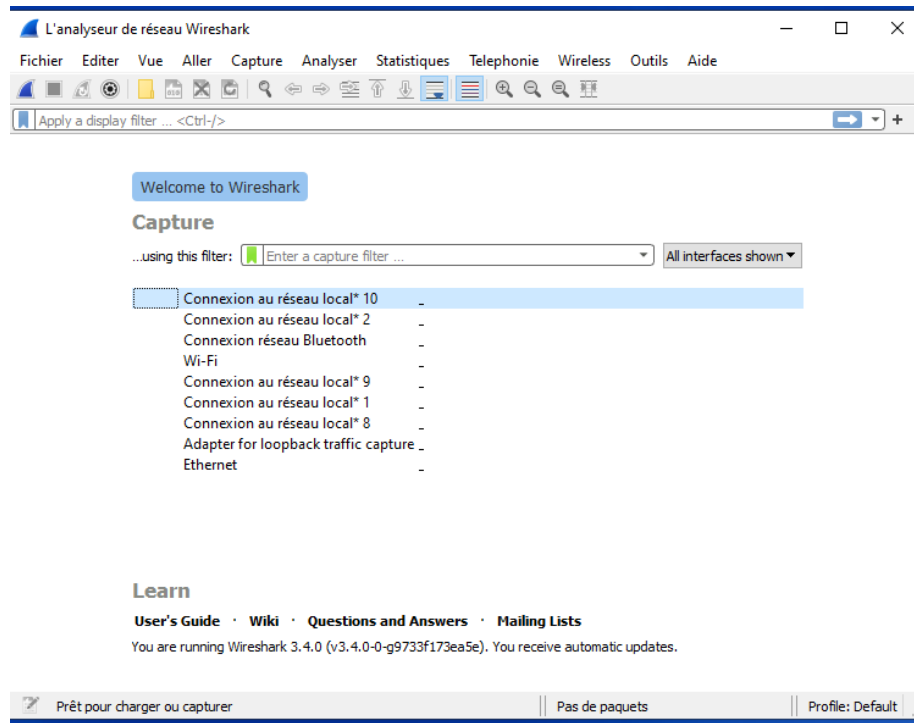
Suffixe DNS propre à la connexion. . . :
Adresse IPv6. . . . . : 2a01:e0a:35d:17d0:bd51:bdef:9b98:3a0b
Adresse IPv6 temporaire . . . . . : 2a01:e0a:35d:17d0:10cf:2c9f:7675:f60
Adresse IPv6 de liaison locale. . . . : fe80::bd51:bdef:9b98:3a0b%13
Adresse IPv4. . . . . : 192.168.0.40
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : fe80::72fc:8fff:fe4f:6d8%13
                                192.168.0.254

Carte Ethernet Connexion réseau Bluetooth :

Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . :
```

3 Première capture du trafic

1. Lancement de Wireshark



2. Paramétrage du logiciel.
3. L'adresse IP de l'Université Paris 8 est : **193.54.174.19**.
4. Le nombre de trames échangées et reçues est de **721**.

The image shows a Wireshark capture of a TLS connection. The packet list on the left shows a series of packets from 447 to 721, all from source 192.168.0.40 to destination 193.54.174.19. The packet details pane on the right shows the structure of the captured data, including the TLS handshake and application data. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
447	8.876295	192.168.0.40	193.54.174.19	TLSv1.2	571	Client Hello
452	8.892887	192.168.0.40	193.54.174.19	TCP	54	58875 → 443 [ACK] Seq=511
453	8.911528	192.168.0.40	193.54.174.19	TLSv1.2	180	Client Key Exchange, Cha
455	8.918241	192.168.0.40	193.54.174.19	TLSv1.2	638	Application Data
469	9.111557	192.168.0.40	193.54.174.19	TCP	54	58875 → 443 [ACK] Seq=12
470	9.118214	192.168.0.40	193.54.174.19	TCP	54	58875 → 443 [ACK] Seq=12
477	9.282817	192.168.0.40	193.54.174.19	TLSv1.2	584	Application Data
488	9.332418	192.168.0.40	193.54.174.19	TCP	54	58875 → 443 [ACK] Seq=17
699	9.881818	192.168.0.40	193.54.174.19	TLSv1.2	618	Application Data
721	9.932156	192.168.0.40	193.54.174.19	TCP	54	58875 → 443 [ACK] Seq=23

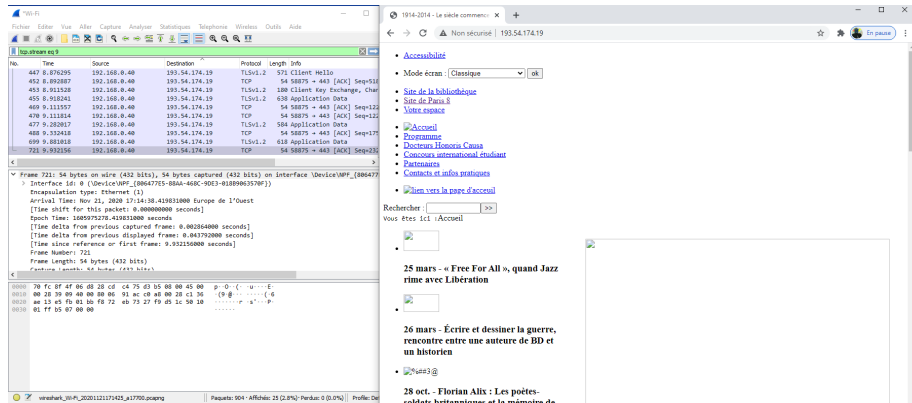
Frame 721: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on Interface \Device\NPF_{086477E5-8...} Interface id: 0 (Device\NPF_{086477E5-8...}) Encapsulation type: Ethernet (1) Arrival Time: Nov 21, 2020 17:14:38.419831000 Europe de l'Ouest [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1605975278.419831000 seconds [Time delta from previous captured frame: 0.002864000 seconds] [Time delta from previous displayed frame: 0.045792000 seconds] [Time since reference or first frame: 9.932156000 seconds] Frame Number: 721 Frame Length: 54 bytes (432 bits) Capture Length: 54 bytes (432 bits)

0000 70 fc 0f 4f 06 d8 28 cd c4 75 d3 b5 08 00 45 00 p:O-(-u-E-
0010 00 28 39 09 40 00 00 06 91 ac c0 a8 00 28 c1 36 (9@-(-(-6
0020 ac 13 e5 fb 01 b0 f8 72 eb 73 27 f9 d5 1c 50 10r's'-P
0030 01 ff b5 07 00 00

5. Pourquoi envoie-t-on plusieurs trames?

Il est utile d'envoyer plusieurs trames pour garantir l'intégrité du message complet.

6. Taper l'adresse IP de l'université de Paris 8:

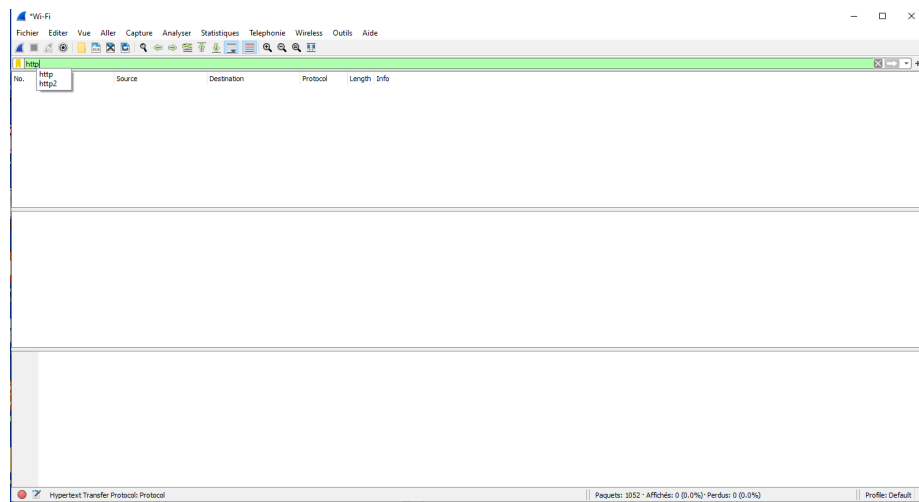


7. Pourquoi ne pas utiliser l'adresse IP directement?

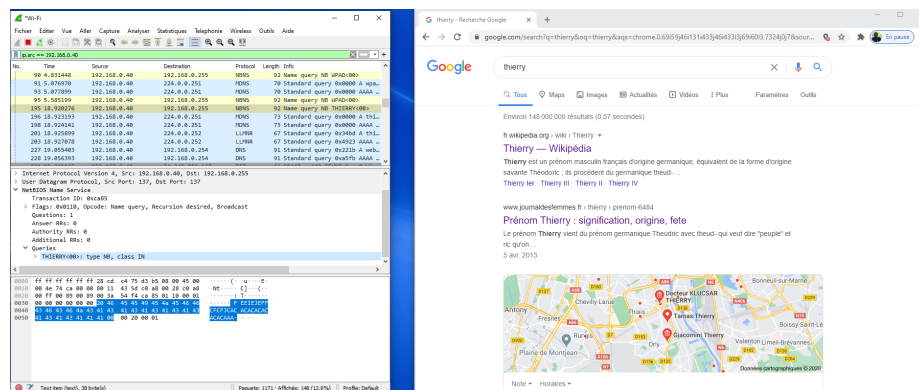
L'accès à un site par son adresse IP est possible. On vient de le voir. Pourtant pour des raisons pratiques, la présence du DNS simplifie largement la tâche pour éviter de mémoriser la combinaison exacte d'une adresse IP.

4 Capture et analyse d'une trame

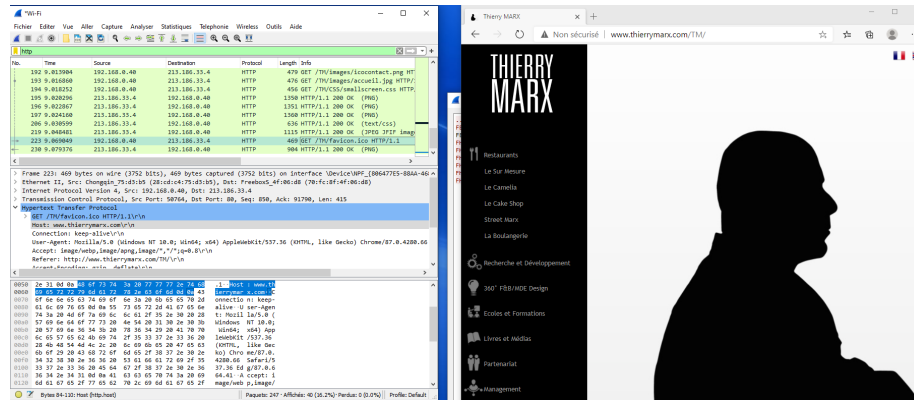
1. Relancez le trafic,
2. Tapez votre prénom: "thierry",
3. Stoppez la capture et sélectionnez la trame dans laquelle apparaît votre prénom: il ne se passe rien.
4. Le filtre "http" ne me donne rien comme information. **Ce qui est normal, car le prénom seul ne dirige pas vers une page web.**



Pour retrouver les échanges concernant la recherche de mon prénom, il est nécessaire de mettre TCP comme filtre:



- La solution "web" pour retrouver le prénom serait de visiter une page web avec le prénom de "thierry" comme titre: Google me propose entre autres celle de "Thierry Marx":



- En aidant du code ASCII, la valeur hexadécimale de "thierry" est: **74 68 69 65 72 72 79**.

On retrouve cette portion de valeur dans la trame analysée ci-dessus.

- La conversion en binaire de "thierry" est: 00110111 00110100 00100000 00110110 00111000 00100000 00110110 00111001 00100000 00110110 00110101 00100000 00110111 00110010 00100000 00110111 00110010 00100000 00110111 00111001.

5 Conclusion

En conclusion, on peut dire que grâce à Wireshark, il est possible de trouver l'adresse IP d'un site web mais aussi de trouver exactement "en texte clair" les informations qu'on a recherché. Cela fait de Wireshark un outil très puissant qui pourrait nuire à la protection de la vie privée.

Voici donc à la fois un avantage pour celui qui fait ses recherches sur internet mais aussi un inconvénient majeur pour celui qui essaie d'être discret sur le web.