

TP 1

INTRODUCTION A WIRESHARK

Les TP de cette UE ont pour but de comprendre le fonctionnement d'un réseau. Pour ce faire, nous allons observer le fonctionnement des protocoles qui résultent de l'activité de diverses applications telles que votre navigateur web.

L'exécution de ces protocoles ont des effets que nous nous proposons d'observer en utilisant Wireshark. Wireshark est un logiciel libre distribué pour la plupart des systèmes d'exploitation, compatible avec un grand nombre d'interfaces réseau telles qu'Ethernet ou Wifi.

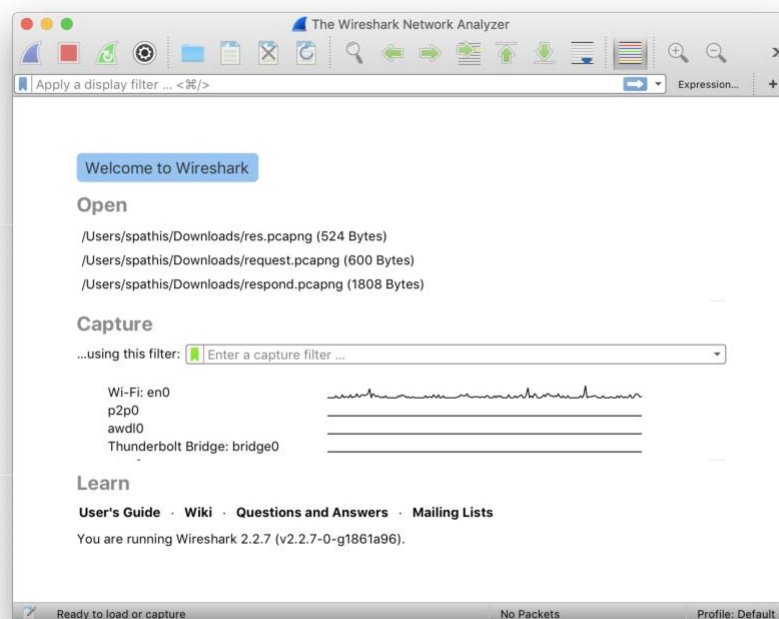
1. PRESENTATION

Wireshark est un analyseur de trafic (*packet sniffer*) qui permet 1) la capture des messages envoyés et reçus par votre machine et 2) l'analyse des entêtes (et enqueues) de ces messages.

- Capturer le trafic consiste à récupérer une copie des messages au niveau le plus bas (couche 2). On récupère la plupart du temps des trames Ethernet ainsi que l'ensemble des autres entêtes situées à la suite de l'entête Ethernet.
- Analyser le trafic consiste à décoder l'ensemble des entêtes en listant le nom des champs et leurs valeurs respectives. Wireshark est capable de décoder les entêtes de plusieurs centaines de protocoles tels que IP, TCP, UDP, DNS, ou HTTP.

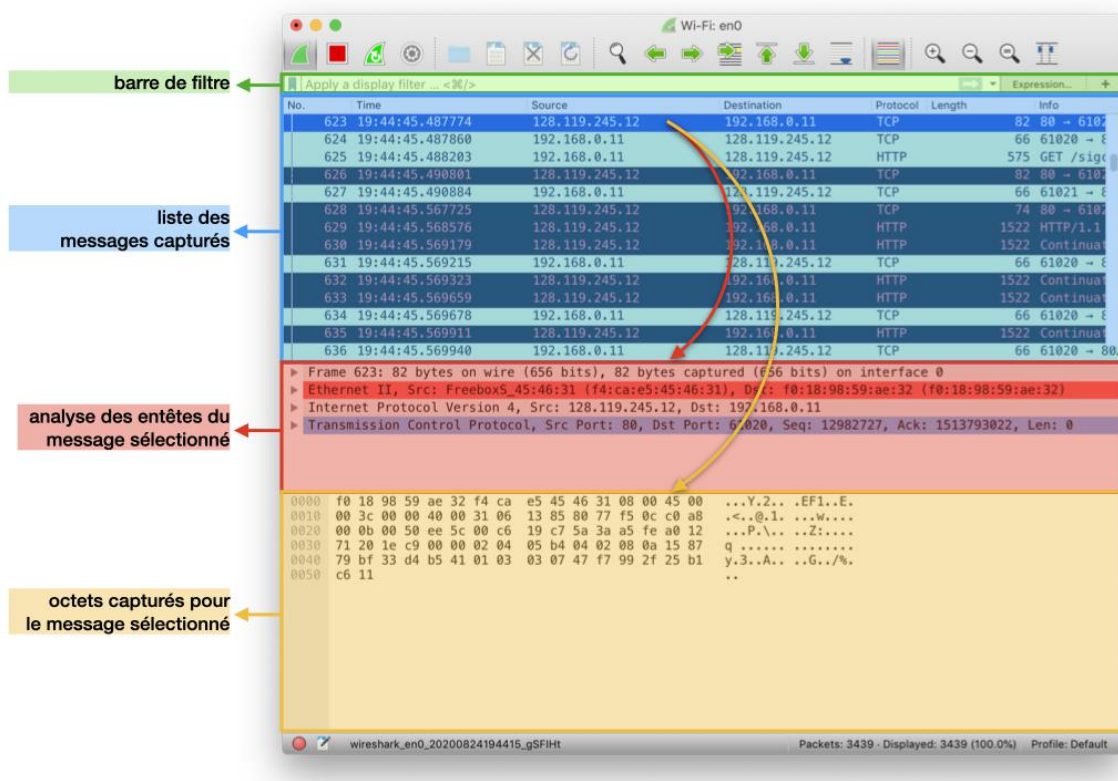
Pour installer Wireshark, visitez la page <https://www.wireshark.org/> et téléchargez la version adaptée à votre système d'exploitation.

Au démarrage de Wireshark, la première fenêtre contient les trois sections 'Open', 'Capture' et 'Learn'. La section 'Capture' liste les interfaces réseau installées sur votre machine parmi lesquelles vous devez sélectionner celle sur laquelle le trafic sera capturé.



2. FENETRE WIRESHARK

Une fois une interface réseau sélectionnée, une seconde fenêtre apparaît, indiquant que Wireshark a débuté la capture du trafic réseau observé sur cette interface. Vous pouvez à tout moment interrompre, redémarrer ou relancer la capture dans le menu 'Capture'. Le menu 'File' vous permet de sauvegarder les messages capturés dans un fichier pcap ou d'ouvrir un fichier pcap contenant une capture précédemment sauvegardée.



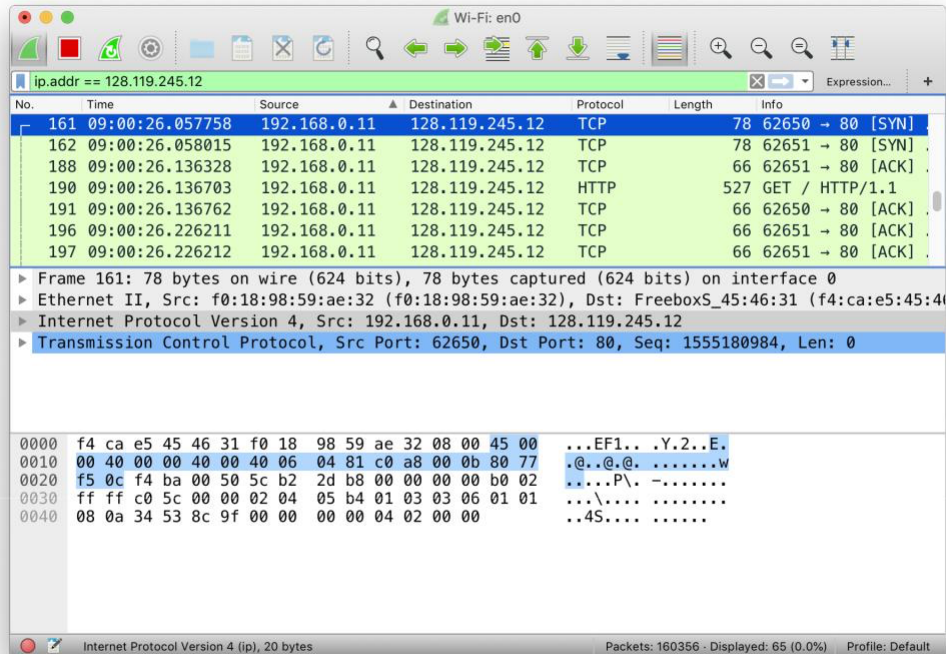
Cette nouvelle fenêtre est composée de plusieurs panneaux. Les informations présentées dans chaque panneau dépendent de la sélection effectuée dans le panneau précédent.

- La barre de filtre qui permet de soumettre des expressions pour filtrer les messages listés dans le panneau suivant.
- Le panneau où sont listés les messages capturés (en accord avec l'expression filtrante soumise dans la barre de filtre précédente).
- Le panneau contenant l'analyse des entêtes du message sélectionné dans la liste précédente.
- Le panneau montrant les octets tels que capturés pour le message sélectionné.

La suite de ce document présente le détail de chaque panneau.

2.1. Barre de filtre

La barre de filtre permet de soumettre des expressions permettant de sélectionner les messages à afficher dans le panneau suivant. Ces expressions portent sur la valeur des protocoles et/ou les valeurs des champs d'entête pertinentes du point des messages que l'on souhaite afficher et étudier.



Ci-dessous quelques exemples de filtres :

<code>ip.addr == 128.119.245.12</code>	Filtrer tous les paquets provenant ou à destination de la machine numérotée avec l'adresse IP 128.119.245.12
<code>(ip.addr == 132.227.0.0/16) or (ip.addr == 134.157.0.0/16)</code>	Filtrer tous les paquets provenant ou à destination de Sorbonne Université
<code>tcp.port == 80</code>	Filtrer tous les paquets résultant d'une activité web
<code>eth.dst == ff:ff:ff:ff:ff:ff</code>	Filtrer les messages envoyés en broadcast Ethernet
<code>eth.src[:3] == f0:18:98</code>	Filtrer les messages provenant d'une interface réseau dont l'adresse mac commence par f0:18:98

2.2. Liste des messages capturés

Ce panneau contient la liste des messages capturés par ordre chronologique ou le sous-ensemble des messages correspondant à l'expression filtrante soumise dans la barre de filtre. Chaque ligne correspond à un message et pour chaque message, Wireshark fournit un résumé des informations principales concernant ce message organisées par colonne.

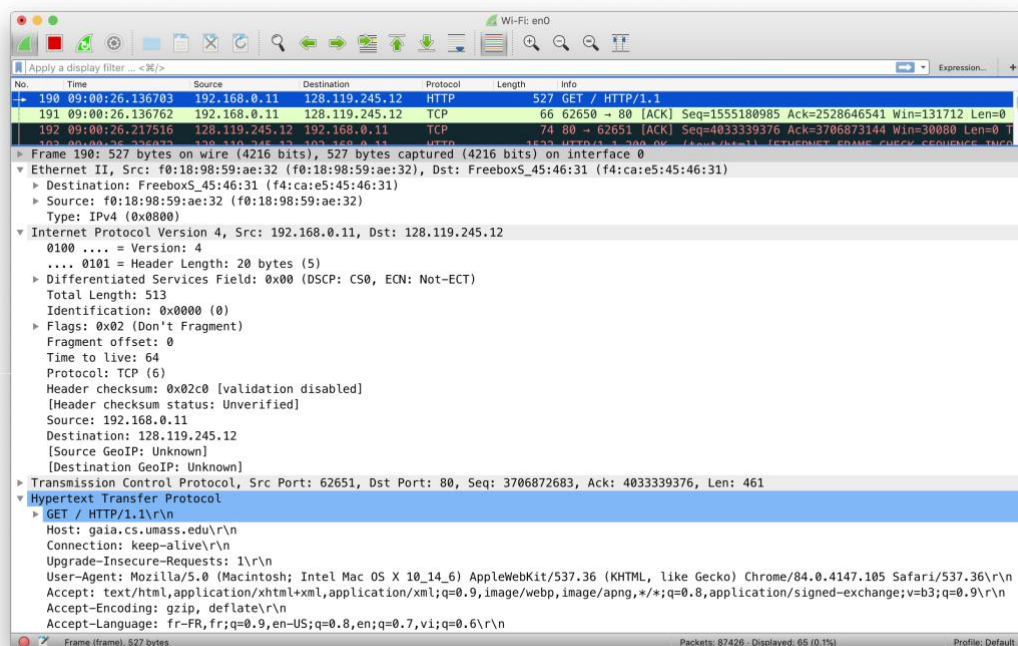
No.	Time	Source	Destination	Protocol	Length	Info
190	09:00:26.136703	192.168.0.11	128.119.245.12	HTTP	527	GET / HTTP/1.1

Ces informations consistent du numéro du message dans la liste des messages capturés (hors filtre), l'instant de sa capture, ses adresses IP source et destination, le nom du protocole encapsulé de plus haut niveau, la longueur totale du message, et un résumé des informations contenues dans l'entête de ce protocole.

Dans la capture ci-dessus, le message est le 190^e à avoir été capturé, les adresses IP source et destination sont respectivement 192.168.0.11 et 128.119.245.12, le dernier entête du message a été ajoutée par HTTP. Il s'agit d'une requête GET utilisant la version 1.1 de HTTP.

2.3. Liste des entêtes de message

Pour tout message sélectionné dans la liste des messages capturées, le panneau d'analyse des entêtes fournit pour chaque entête présente dans le message, le détail des champs d'entête et leur valeur.



Dans la capture ci-dessus, le message contient 4 entêtes consécutives présentées dans leur ordre d'apparition dans le message :

- Ethernet II ;
- Internet Protocol Version 4 ;
- Transmission Control Protocol ;
- Hypertext Transfer Protocol.

Pour chaque entête, les champs sont présentés sous la forme d'une liste déroulante (dévoilée en cliquant le triangle précédant le nom de l'entête). Pour chaque champ, Wireshark fournit le nom du champ suivi de sa valeur. Les valeurs de certains champs sont converties en décimal, d'autres sont laissées au format hexadécimal (valeurs précédées par '0x'). Si une valeur est interprétable, Wireshark donne l'interprétation de cette valeur. Par exemple, Wireshark convertit la valeur 0x06 du champ Protocol de l'entête IP en décimal et indique que cette valeur signifie que le protocole encapsulé dans ce paquet IP est TCP.

2.4. Liste des octets capturés

Le dernier panneau de la fenêtre Wireshark contient la liste des octets du message tels que capturés par Wireshark. En sélectionnant un entête dans le panneau précédent, Wireshark met en surbrillance les octets correspondants à cet entête.

