

Guide utilisation wireshark et expérimentations

Contenu

Introduction	2
Présentation de l'interface Wireshark	3
Applications pratiques de Wireshark (HTTPS, Telnet)	5
Protocole HTTPS	5
Protocole Telnet	8
<i>Analyse détaillée</i>	8
Conclusion	12

Liste des figures

Figure 1 : Fenêtre principale de l'interface de Wireshark.....	3
Figure 2 : Page principale de l'interface de Wireshark.....	4
Figure 3 : Interface Wireshark – protocole HTTPS	5
Figure 4 : Algorithme de cryptage pour la trame « Server Hello ».....	6
Figure 5 : Capture de paquets avec Wireshark	7
Figure 6 : Interface Wireshark – protocole Telnet	8
Figure 7 : Installation du Telnet.....	9
Figure 8 : Connexion à l'ordinateur Windows (client) via Telnet.....	10
Figure 9 : Affichage du Raspberry Pi sur le client Telnet	10
Figure 10 : Interface Wireshark – protocole Telnet – analyse des paquets (1/2)	11
Figure 11 : Interface Wireshark – protocole Telnet – analyse des paquets (2/2)	11

Introduction

Ce document sert à illustrer le comportement en réseau de certains protocoles à l'aide de captures de paquets spécifiques à chaque protocole, grâce au programme « sniffer » Wireshark.

Présentation de l'interface Wireshark

Le téléchargement de Wireshark 2.2.2 (version française) se fait à partir du site suivant : <http://telecharger.tomsguide.fr/Ethereal-Wireshark,0301-20912.html>.

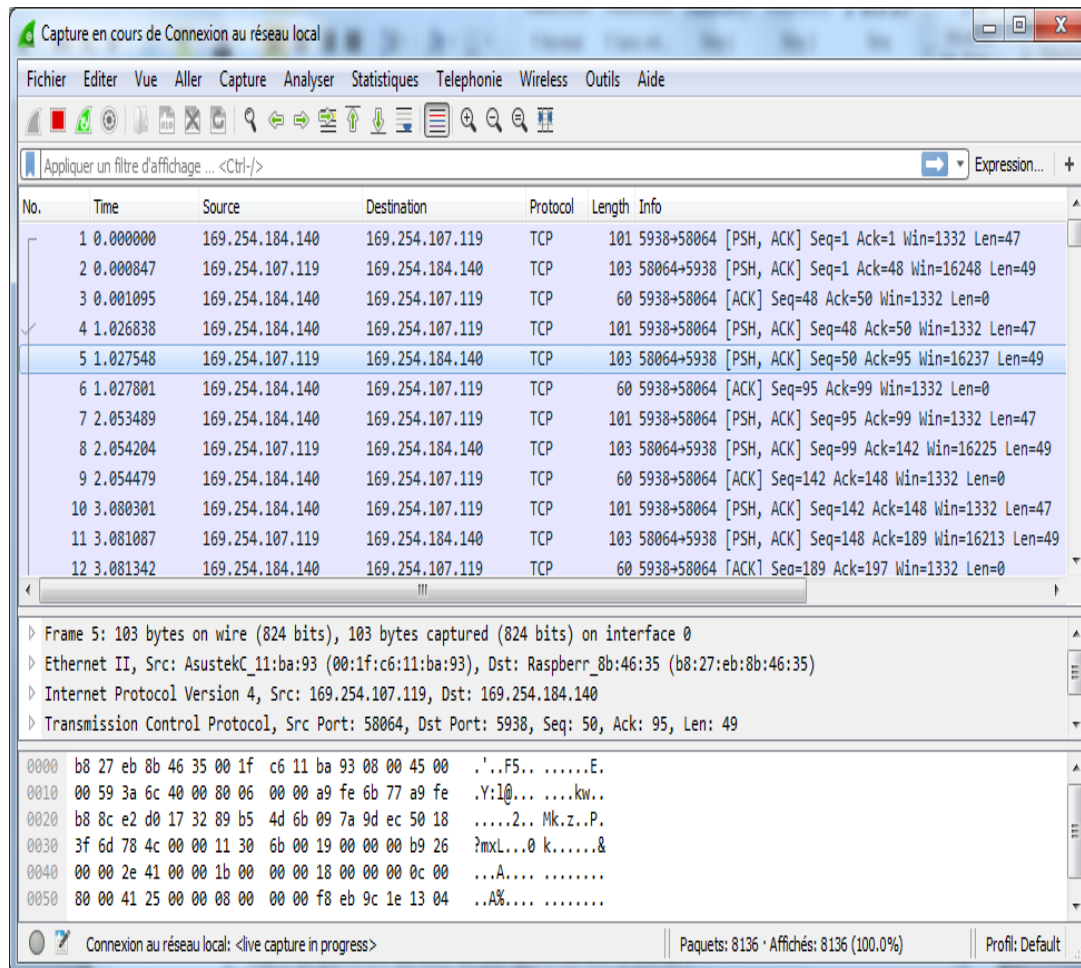


Figure 1 : Fenêtre principale de l'interface de Wireshark

La fenêtre principale de l'interface de Wireshark est divisée en trois sections :

- la première, en haut, affiche la liste des paquets capturés;
- la deuxième, au milieu, donne des détails sur le paquet sélectionné de la liste du haut (le paquet surligné);
- la troisième reproduit le contenu en hexadécimal, du même paquet.

Avant de commencer la capture de paquets, on doit en préciser les options. Pour ce faire :

- choisir dans le menu, l'option « Capture>Options »;
- appuyer sur le bouton « Options de capture » de la barre d'outils principale;

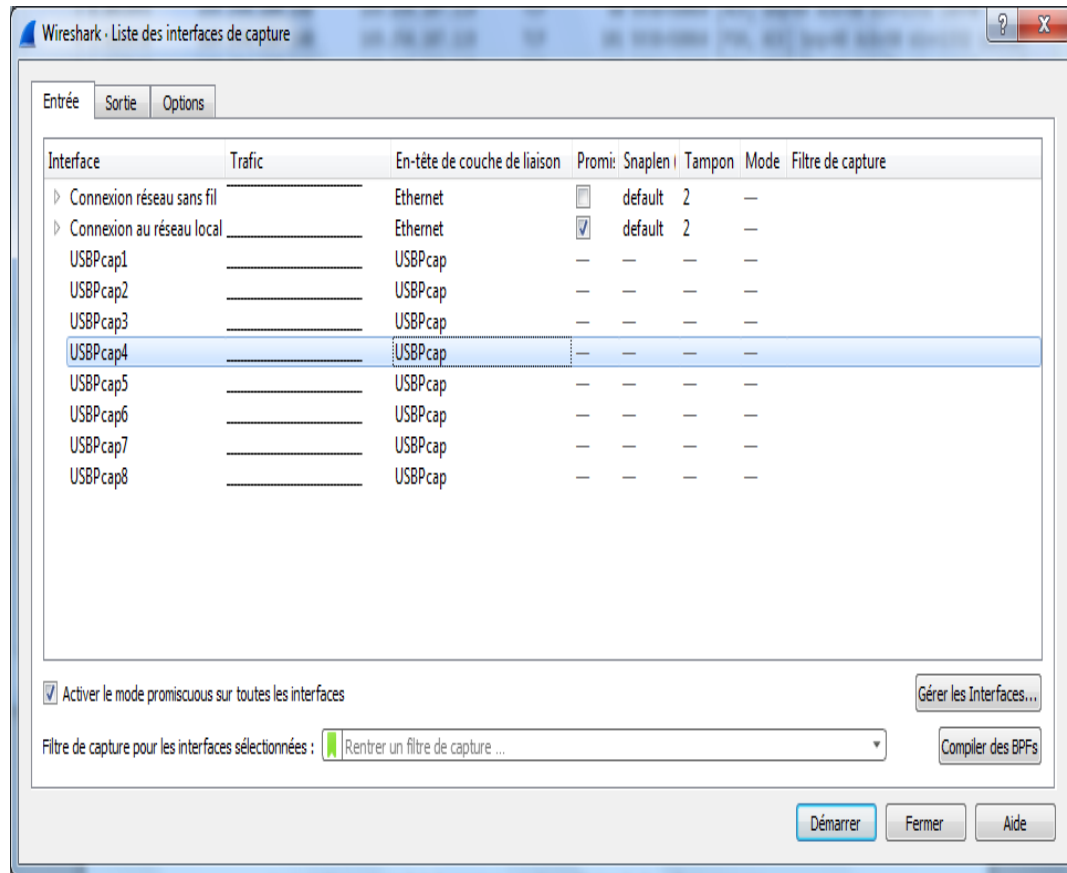


Figure 2 : Page principale de l'interface de Wireshark

- sélectionner l'interface à surveiller (USBP) sous l'onglet « Entrée »;
- préciser le filtre qui raffine la capture d'écran;
- préciser également les autres options sous les onglets « Sortie » et « Options »;
- cliquer sur le bouton « Démarrer »;
- après un délai de 30 secondes, arrêter la capture en appuyant sur le bouton correspondant de la barre d'outils principale ou à partir du menu (commande « Capture>Arrêt »).

Applications pratiques de Wireshark (HTTPS, Telnet)

Les expérimentations que vous effectuerez portent sur le fonctionnement normal des protocoles SSL/TLS, HTTP, SSH. Les captures que vous ferez pour ces protocoles devraient être similaires aux captures suivantes :

Protocole HTTPS

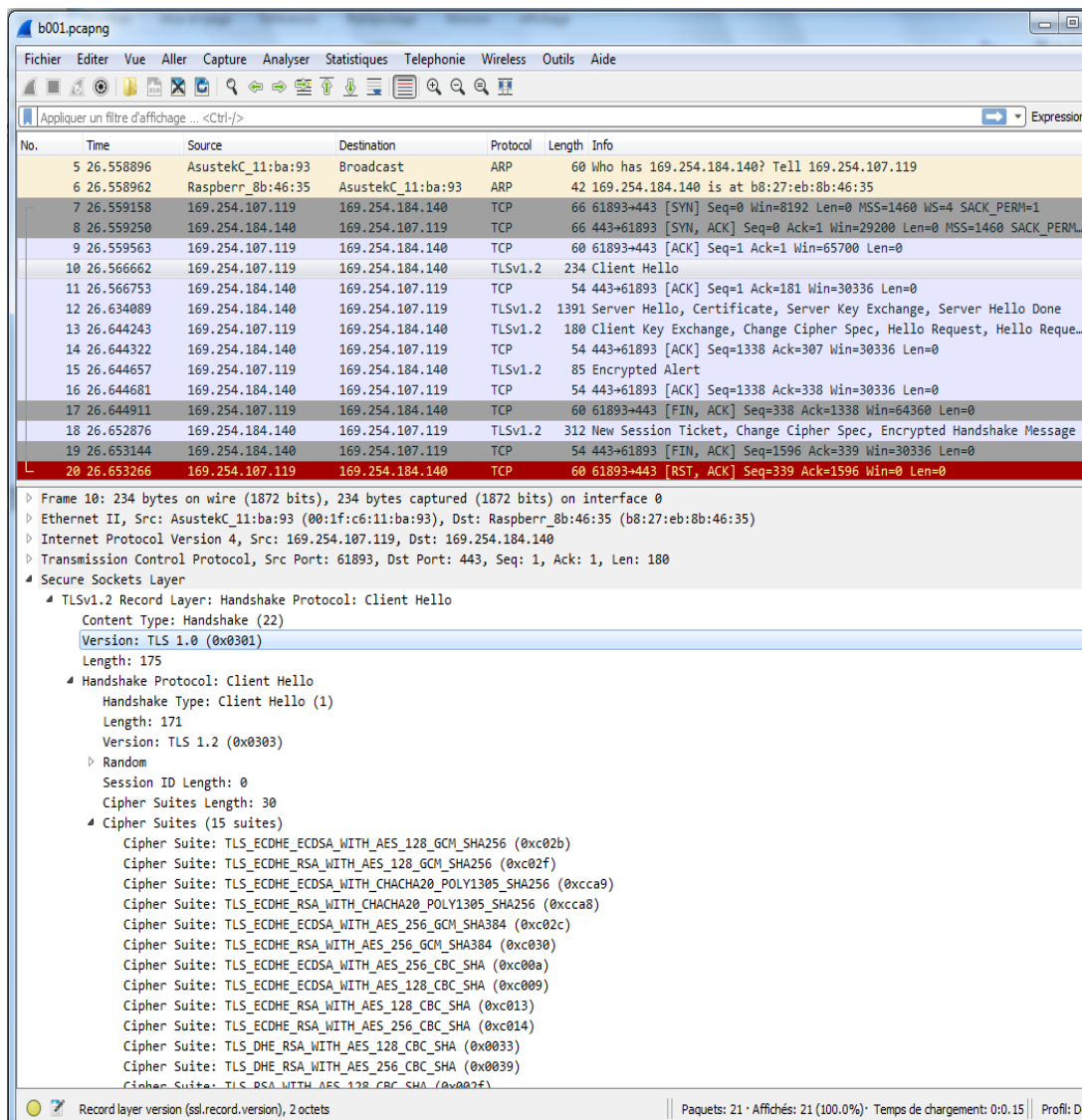


Figure 3 : Interface Wireshark – protocole HTTPS

Voici comment se négocie la future transmission chiffrée entre le client navigateur (sur l'ordinateur Windows) et le serveur SSL sur Raspberry Pi (voir Figure 3)¹ :

¹ Voir également le document [Expérimentation site Web sécurisé par certificat de sécurité.](#)

- a) les deux premières lignes (lignes numérotées 5 et 6) constituent le dialogue au niveau du protocole ARP qui informera l'ordinateur Windows de l'adresse Ethernet correspondant à l'adresse IP 169.254.184.140 du Raspberry Pi;
- b) les lignes numérotées 7 à 9 sont des paquets qui constituent le dialogue au niveau « Transport » du réseau, protocole TCP. Ces trois paquets (« messages ») établissent une connexion sûre entre les deux dispositifs du réseau par l'intermédiaire des signaux (bits) SYN et ACK;
- c) pour que la connexion soit sécuritaire, à partir de la ligne numérotée 10, les deux dispositifs négocient l'algorithme précis de cryptage qui sera utilisé (voir la section du bas). Cette section affiche les détails de la pile des protocoles, décodés pour la trame sélectionnée : une liste de « Cypher Suite » y est présentée, le premier choix étant : TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b);
- d) le serveur répond dans la trame (ligne numérotée 12) avec quatre enregistrements TLS, dont « Server Hello », qui choisit également TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256 comme algorithme de cryptage :

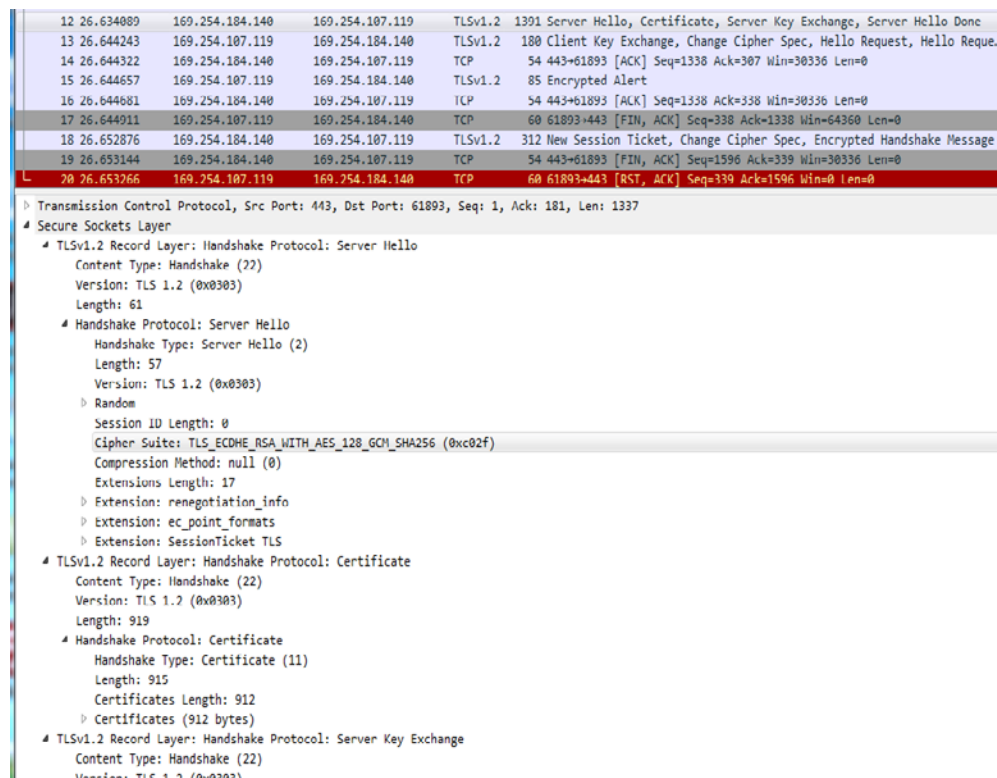


Figure 4 : Algorithme de cryptage pour la trame « Server Hello ».

L'enregistrement « Certificates » de la même trame contient le certificat X.509 qui comprend : la clé publique du serveur, des informations sur le propriétaire et sur l'autorité qui a émis le certificat (voir Figure 4).

De plus, le certificat contient la signature digitale obtenue par le chiffrement du *checksum* ou du hachage de l'information contenue par le certificat avec la clé privée de l'émetteur.

Voici ce qui est capturé avec Wireshark ou un autre « sniffer » quand le dialogue sous protocole est chiffré (http over tls v.1.2) :

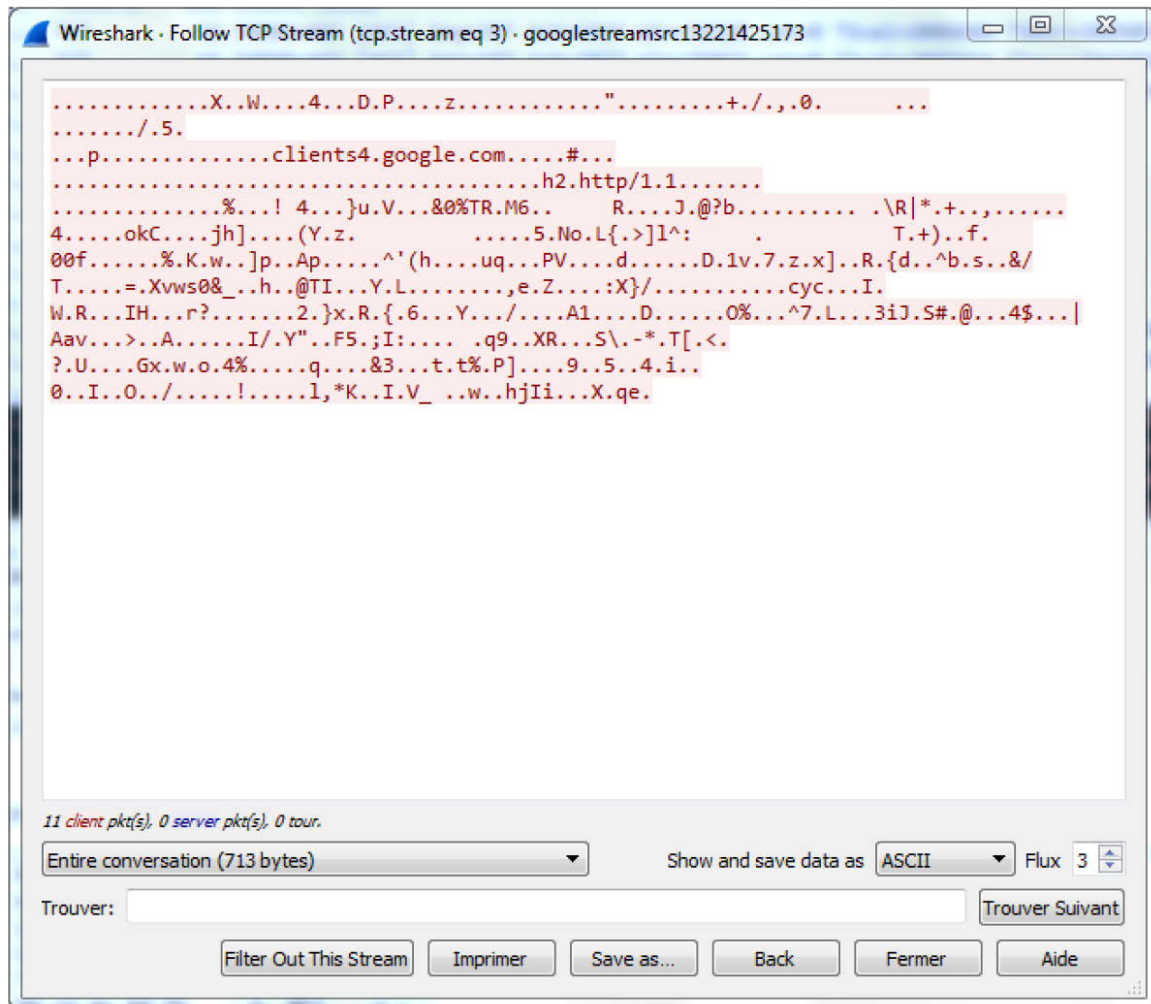


Figure 5 : Capture de paquets avec Wireshark

Protocole Telnet

Aux fins de comparaison, prenons l'exemple du protocole « Telnet », qui n'est pas chiffré. À la suite de l'exécution de la commande « Analyser/Suivre/Flux TCP » de Wireshark, on obtient :

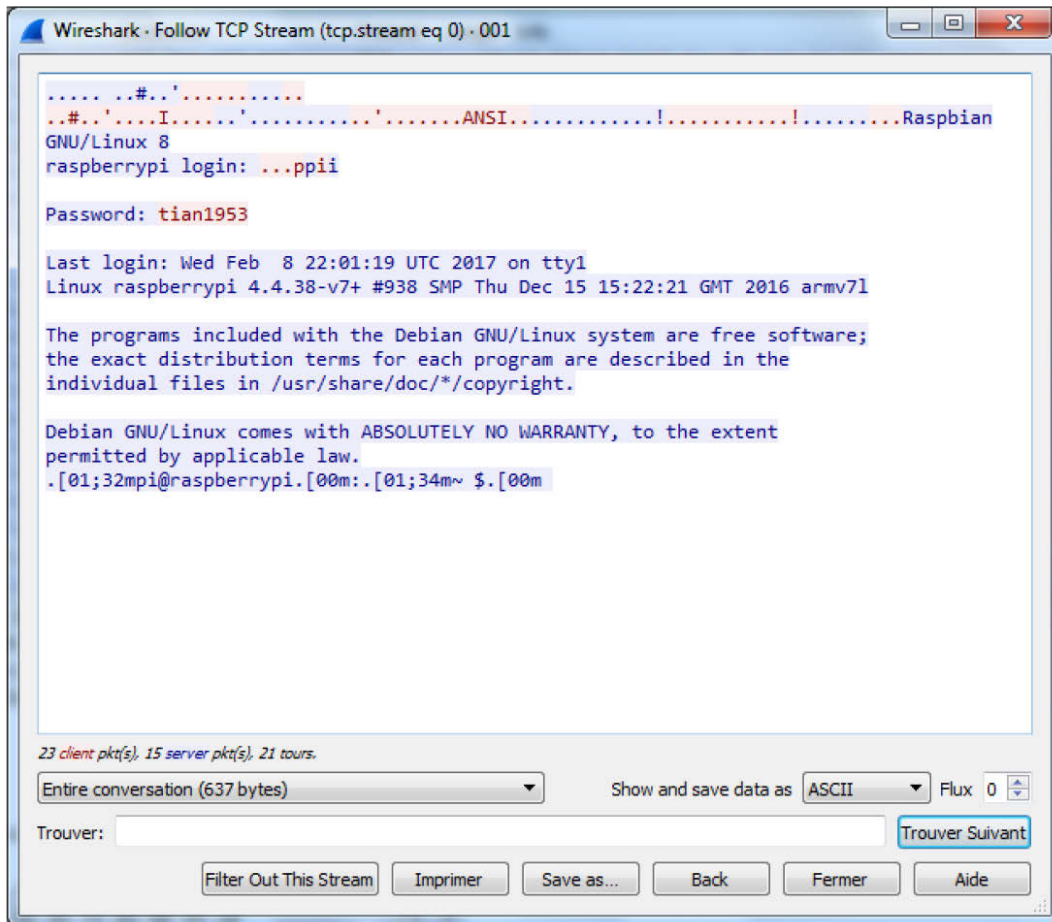


Figure 6 : Interface Wireshark – protocole Telnet

Dans ce cas, le texte est en clair, incluant le « login » et le « mot de passe » du Raspberry Pi.

Analyse détaillée

Voici comment implémenter et utiliser le protocole Telnet (l'ordinateur Windows) :

- 1) s'assurer que l'option Client Telnet est active (dans Windows sous Panneau de Configuration -> Programmes et fonctionnalités -> Activer ou désactiver des fonctionnalités Windows -> Client Telnet);
- 2) télécharger et installer un serveur « Telnetd » sur le Raspberry Pi :

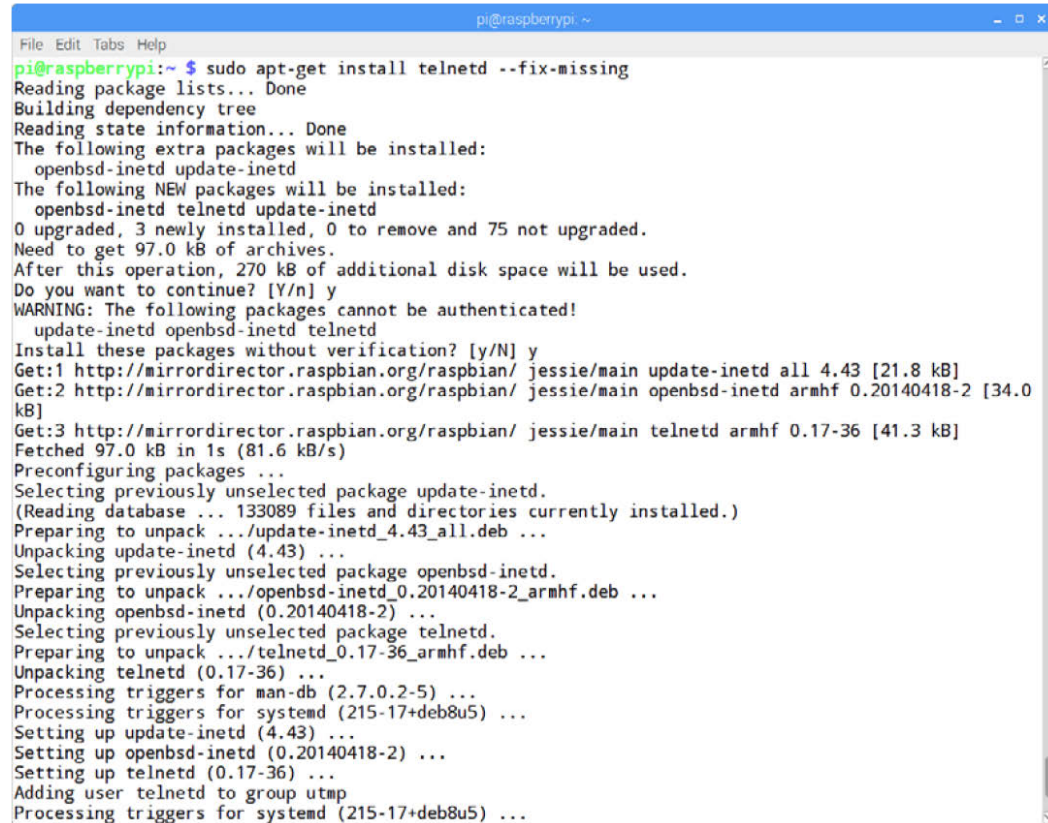
- a. pour ce faire, il faut enlever le signe de commentaire « # » de la dernière ligne du fichier « /etc/apt/sources.list » avec un éditeur de texte (nano, par ex.) :

Cette ligne est :

deb-src <http://archive.raspbian.org/raspbian/> jessie main contrib non-fri rpi

- b. installer « Telnetd » avec la commande :

sudo apt-get install telnetd --fix-missing



```

pi@raspberrypi: ~
File Edit Tabs Help
pi@raspberrypi:~$ sudo apt-get install telnetd --fix-missing
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  openbsd-inetd update-inetd
The following NEW packages will be installed:
  openbsd-inetd telnetd update-inetd
0 upgraded, 3 newly installed, 0 to remove and 75 not upgraded.
Need to get 97.0 kB of archives.
After this operation, 270 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
WARNING: The following packages cannot be authenticated!
  update-inetd openbsd-inetd telnetd
Install these packages without verification? [y/N] y
Get:1 http://mirrordirector.raspbian.org/raspbian/ jessie/main update-inetd all 4.43 [21.8 kB]
Get:2 http://mirrordirector.raspbian.org/raspbian/ jessie/main openbsd-inetd armhf 0.20140418-2 [34.0 kB]
Get:3 http://mirrordirector.raspbian.org/raspbian/ jessie/main telnetd armhf 0.17-36 [41.3 kB]
Fetched 97.0 kB in 1s (81.6 kB/s)
Preconfiguring packages ...
Selecting previously unselected package update-inetd.
(Reading database ... 133089 files and directories currently installed.)
Preparing to unpack .../update-inetd_4.43_all.deb ...
Unpacking update-inetd (4.43) ...
Selecting previously unselected package openbsd-inetd.
Preparing to unpack .../openbsd-inetd_0.20140418-2_armhf.deb ...
Unpacking openbsd-inetd (0.20140418-2) ...
Selecting previously unselected package telnetd.
Preparing to unpack .../telnetd_0.17-36_armhf.deb ...
Unpacking telnetd (0.17-36) ...
Processing triggers for man-db (2.7.0.2-5) ...
Processing triggers for systemd (215-17+deb8u5) ...
Setting up update-inetd (4.43) ...
Setting up openbsd-inetd (0.20140418-2) ...
Setting up telnetd (0.17-36) ...
Adding user telnetd to group utmp
Processing triggers for systemd (215-17+deb8u5) ...

```

Figure 7 : Installation du Telnet

Il est maintenant possible de se connecter sur le Raspberry Pi à l'aide de Telnet (c'est-à-dire à partir de l'ordinateur Windows) :

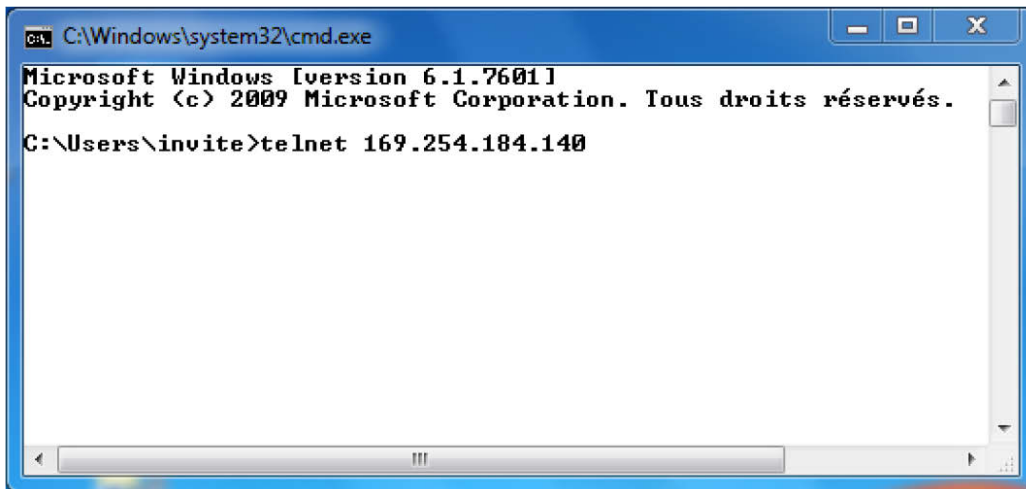


Figure 8 : Connexion à l'ordinateur Windows (client) via Telnet

Et voici le résultat pour l'utilisateur Pi :

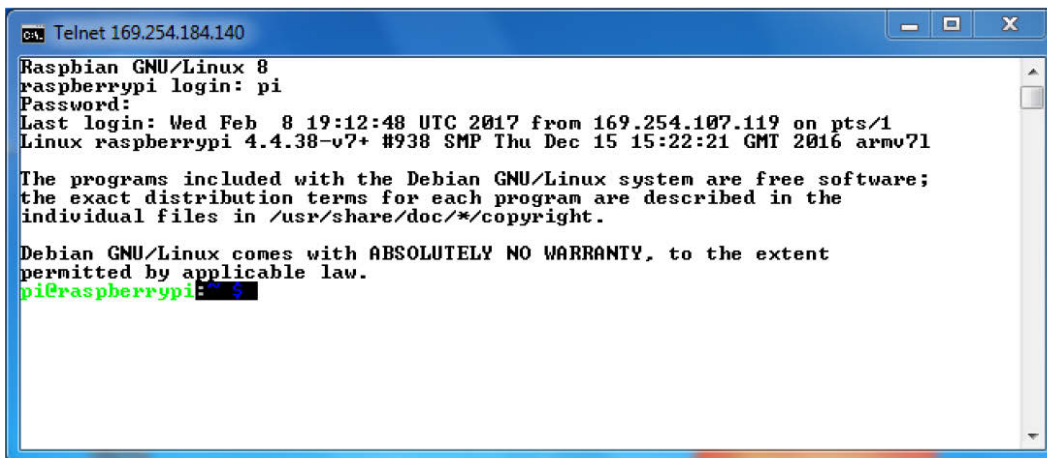


Figure 9 : Affichage du Raspberry Pi sur le client Telnet

L'analyse détaillée des paquets Telnet permet d'obtenir les valeurs du nom d'utilisateur (lignes numérotées 32 à 36) :

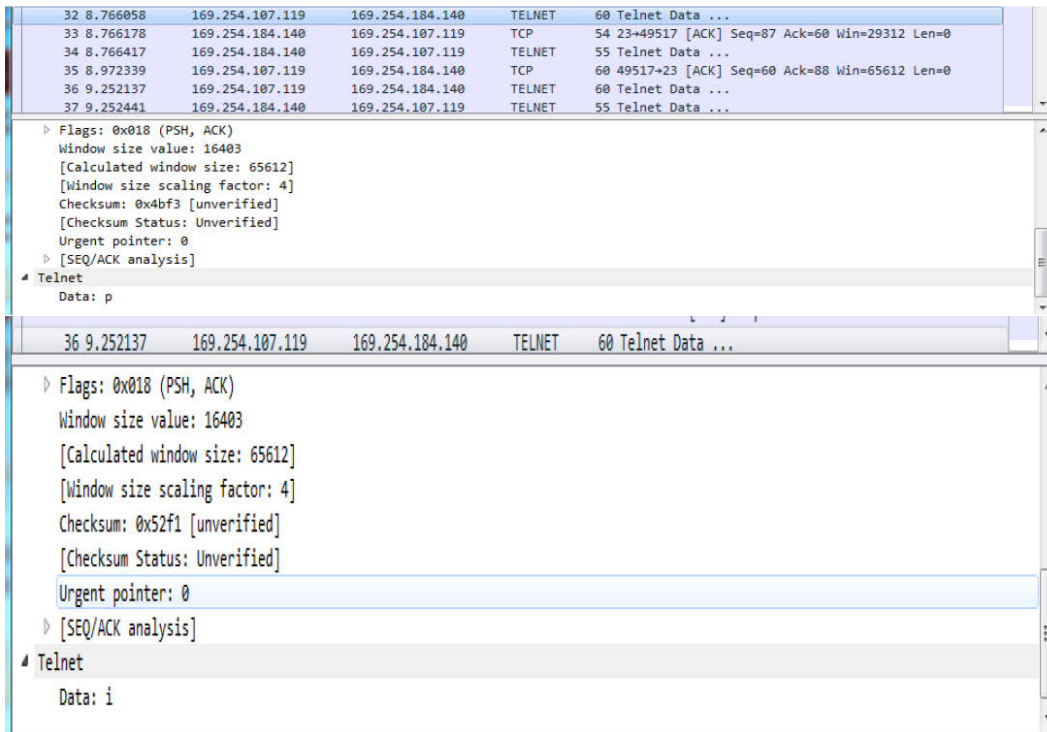


Figure 10 : Interface Wireshark – protocole Telnet – analyse des paquets (1/2)

... et de son mot de passe (lignes numérotées 42-64) :

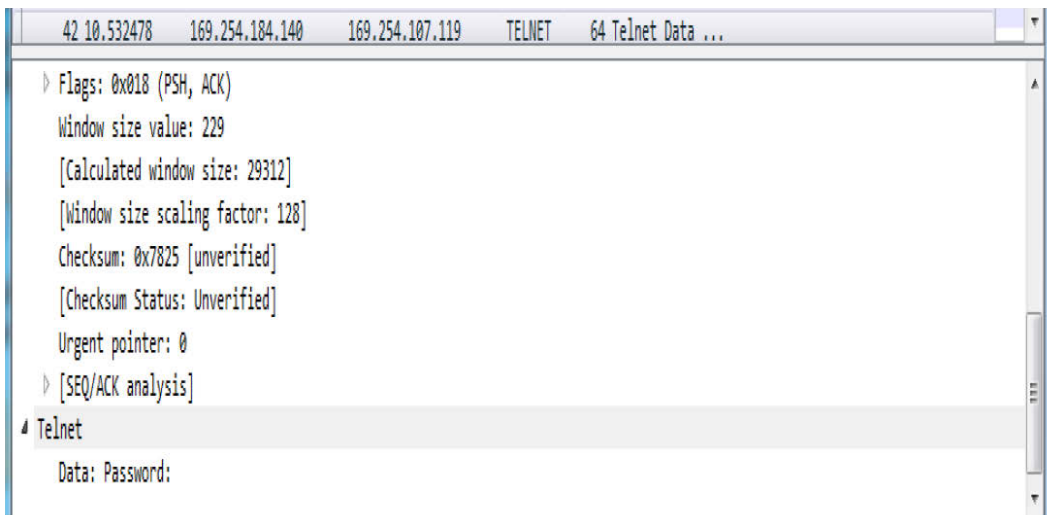


Figure 11 : Interface Wireshark – protocole Telnet – analyse des paquets (2/2)

Conclusion

Pour plus d'informations, consultez le guide [*Mastering Wireshark – Analyze data network like a professional by mastering Wireshark – from 0 to 1137*](#) de Charit Mishra.