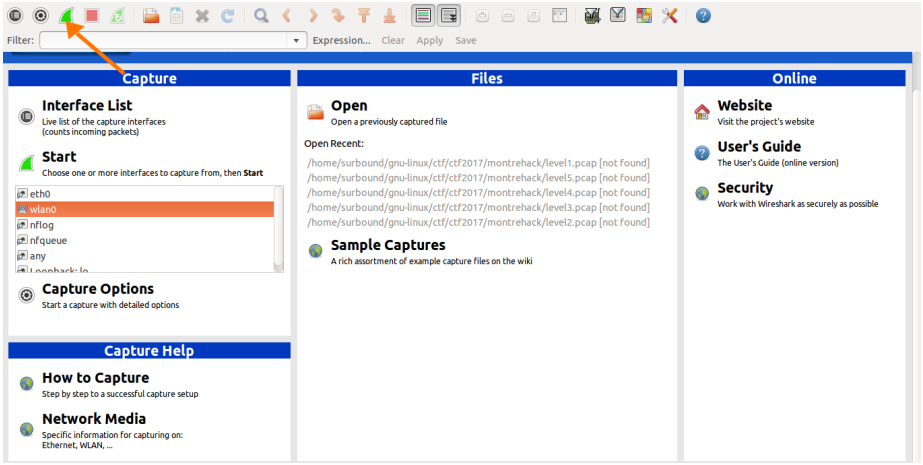
FTP: Comment capturer les données

Cet exemple servira à montrer comment capter du traffic. Plus particulièrement, celeui d'une connexion FTP. Les captures se feront de manière analogue pour les autres types de connections. Pour faire des captures, plutôt que d'utiliser 'gksudo', il est conseillé d'ajouter l'utilisateur au groupe wireshark. Ce n'est seulement qu'avec ces droits, qu'il sera possible de - capturer - des données.

Étape 1:

Ouvrir wireshark, sélectionner l'interface et lancer la capture. (wlan0 pour du wifi)

```
$ wireshark
```



Étape 2:

Connection via l'application FTP sur un serveur. Dans cet example, la connection se fera sur un serveur qui sert à tester. L'utilisateur pourra s'authentifier avec n'importe quel identifiant et mot de passe.

```
$ ftp ftp.freebsd.org
Connected to ftp.geo.freebsd.org.
220 This is ftp0.nyi.freebsd.org - hosted at NYI.net.
Name (ftp.freebsd.org:surbound): anonymous
331 Please specify the password.
Password:
```

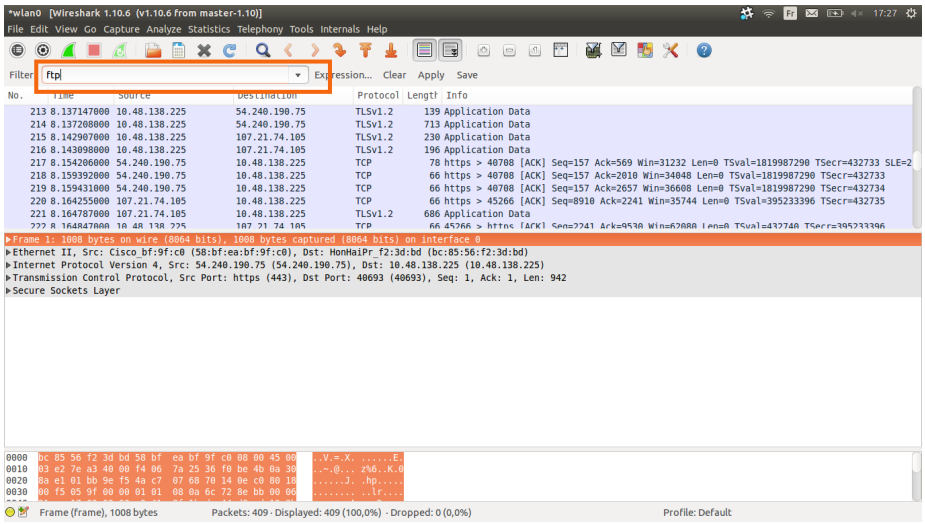
```
230-
230-This is ftp0.nyi.FreeBSD.org, graciously hosted by
230-New York Internet - NYI.net
230-
230-FreeBSD files can be found in the /pub/FreeBSD directory.
230-
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp          5430 Jul 18  2014 favicon.ico
-rw-r--r--    1 ftp      ftp           682 Nov 02  2015 index.html
drwxr-xr-x    3 ftp      ftp             3 Jul 18  2014 pub
226 Directory send OK.
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> get index.html
local: index.html remote: index.html
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for index.html (682 bytes).
#
226 Transfer complete.
682 bytes received in 0.00 secs (4970.3 kB/s)
ftp> exit
221 Goodbye.
```

Étape 3:

Revenir à wireshark et arreter la capture - carré rouge -. Les outils essentiels dans wireshark sont les suivants:

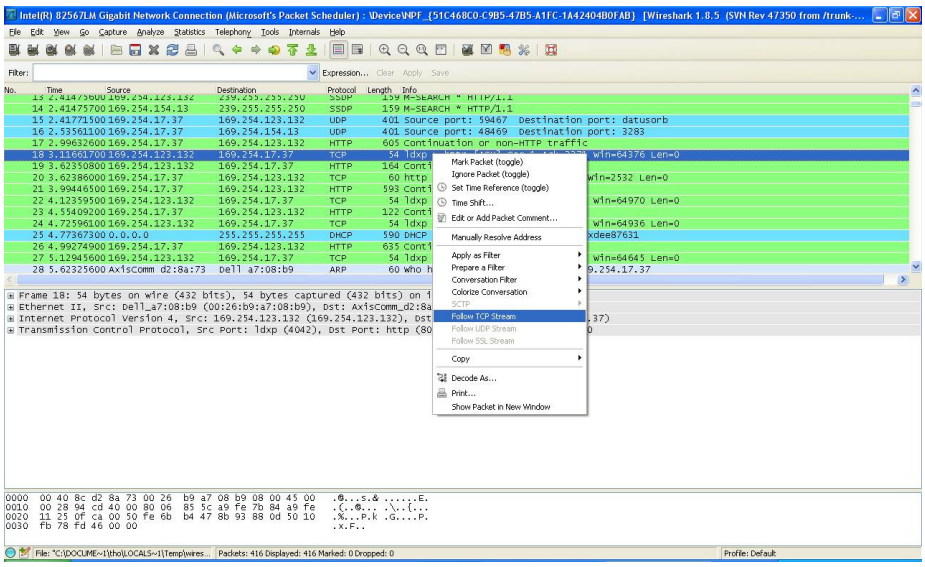
filtrer:

Dans cet exemple, il faut filtrer pour ne garder que le FTP



follow stream:

Dans cet exemple, il faut follow le TCP stream -de cette connection-



Remarque:

La photo n'est pas celle de la capture. Elle ne sert qu'a montrer comment accéder au 'follow TCP stream'

L'intégralité de la conversation de cette connexion ftp qui à utilisé le protocole de transport TCP s'affiche dans une nouvelle fenetre. Le changement de couleur -bleu-rouge- dans le 'follow TCP stream' sert à indiquer le changement d'interlocuteur.

Lien du tutoriel: http://opcode.ninja/sharif-ctf-2016-network-forensics/