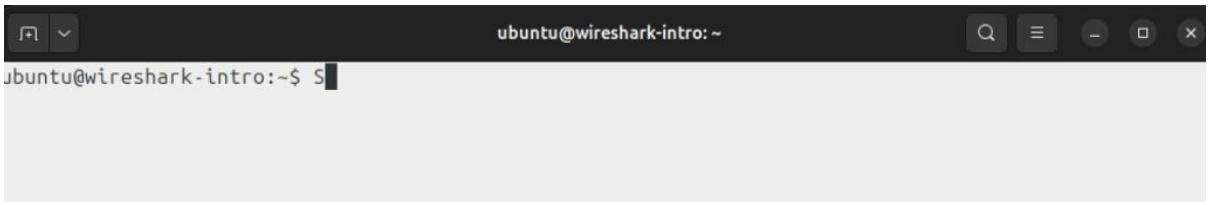
TP WireShark

Pour commencer notre Tp nous allons tout d'abord ouvrir notre Lab en éxécutant la commande ***:***

Labtainer wireshark-intro

```
student@LabtainerVMware:~/labtainer/labtainer-student$ labtainer wireshark-intro
```

Cela va ouvrir un terminal qui nous permettra d'exécuter les commandes demandées



Nous allons ensuite pour afficher le contenu du répertoire utilisez la commande : ***ls-l.***

```
ubuntu@wireshark-intro:~$ ls -l
```

Un fichier s'affiche, nous allons afin de percevoir les détails du fichier utilisez la commande : ***file telnet-pcap***

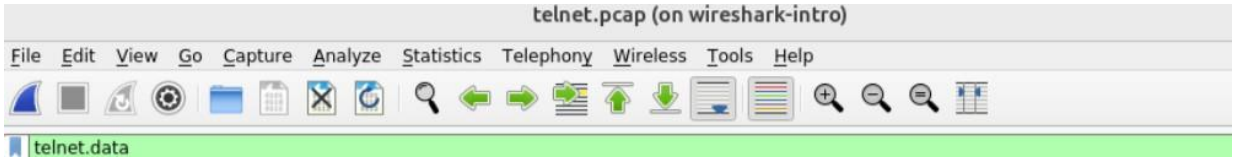
```
ubuntu@wireshark-intro:~$ file telnet.pcap
```

On va ensuite utilisez la commande : *wireshark* afin de lancer wireshark et d'exécuter une analyse PCAP du fichier.

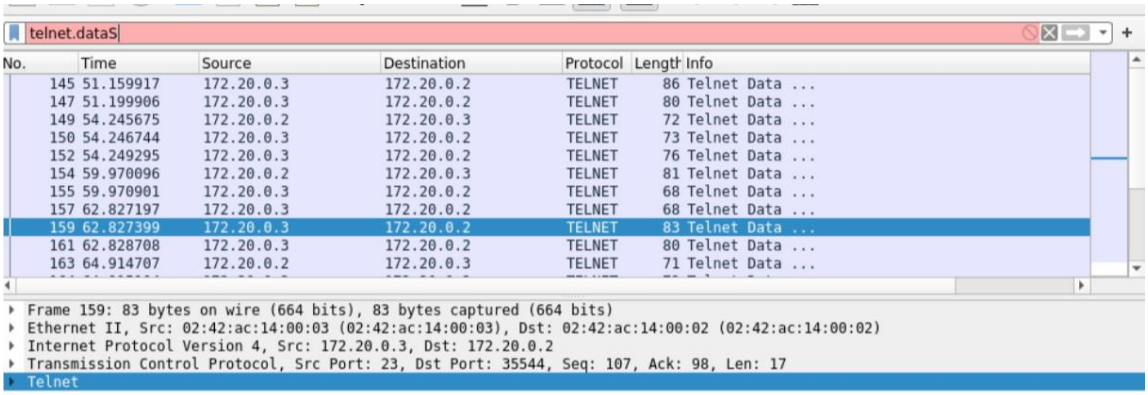
```
ubuntu@wireshark-intro:~$ wireshark
```

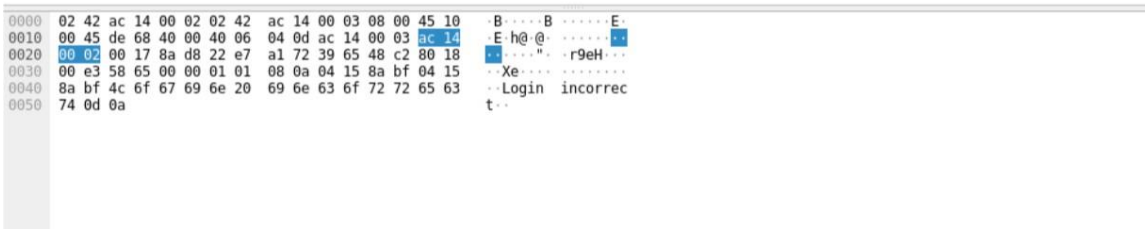
Nous allons ensuite ouvrir le fichier telnet.pcap

Puis taper la commande telnet.data afin de filtrer et d'afficher seulement les paquets de données Telnet.

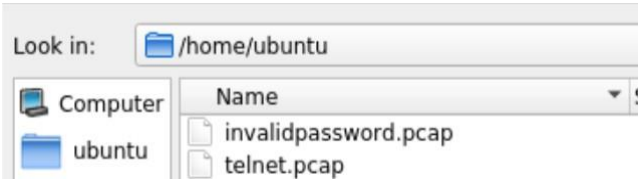


Nous allons ensuite localisez le paquet qui contient le Mdp fourni lorsque l'utilisateur John a tenté d'utiliser telnet.





Nous allons ensuite enregistrer le packet unique en utilisant : ***File =>Export specified packets*** sous le nom de **invalidepassword.pcap.**



Nous pouvons ensuite suivre l'exploration en observant d'autre paquets et en experimentants des filtres.

Puis arreter le Lab en tapant la commande : *stoplab*