|  |  |
| --- | --- |
| formation-informatique-grenoble-cabare  http://[WWW.CABARE.NET](http://WWW.CABARE.NET) **©** | **Protocole TCP-IP & Netbios et Windows 10 – cours & tp -** |
| **Gestion Tcp-ip et réseaux Microsoft**  **Michel Cabaré – Ver 1.6 – déc 2017-** |

**Protocole TCP-IP & Windows10**

**Cours - Travaux Pratiques**

**Michel Cabaré – Ver 1.6 – Déc 2017**

[www.cabare.net](http://www.cabare.net) ©

**table des matiÈres**

Analyse de trame 3

Wireshark installation: 3

Wireshark lancement: 5

Wireshark arp: 6

Wireshark ftp: 6

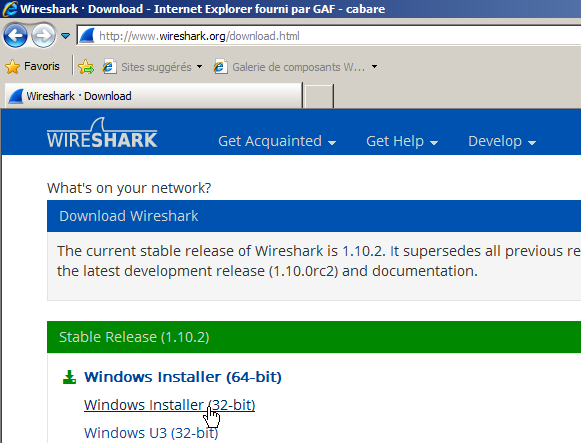
Wireshark dns et nslookup: 7

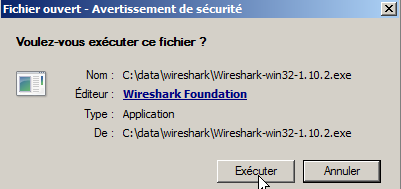
Wireshark statistics: 7

# Analyse de trame

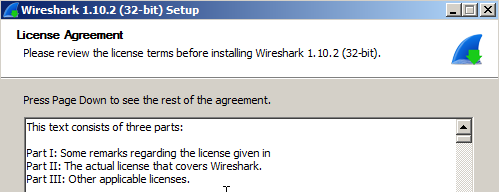
## Wireshark installation:

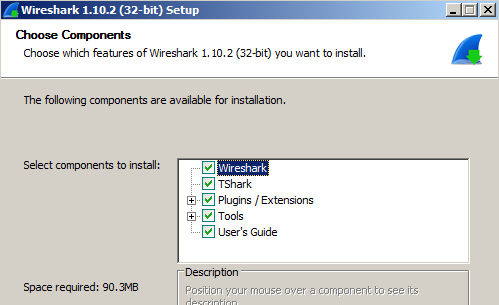
Essayons de télécharger cet utilitaire issu de **ethereal**…

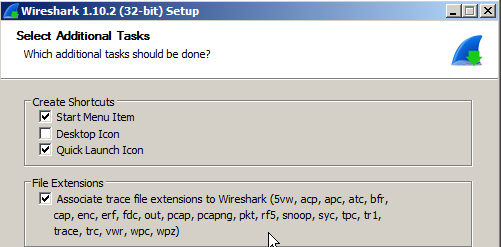


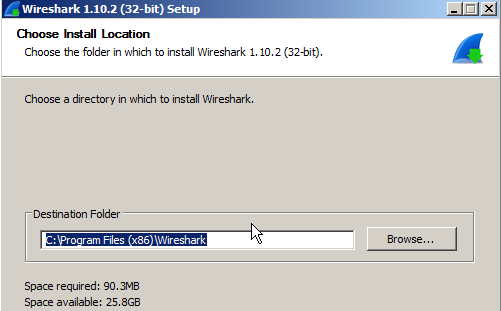


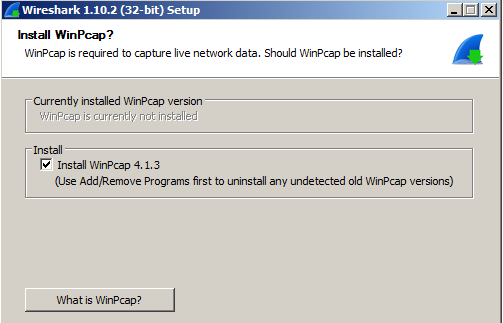


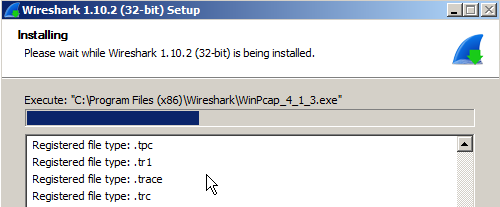


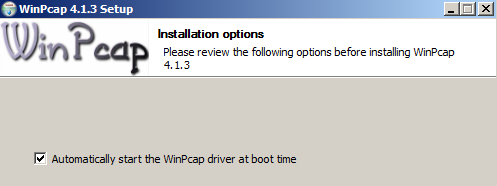










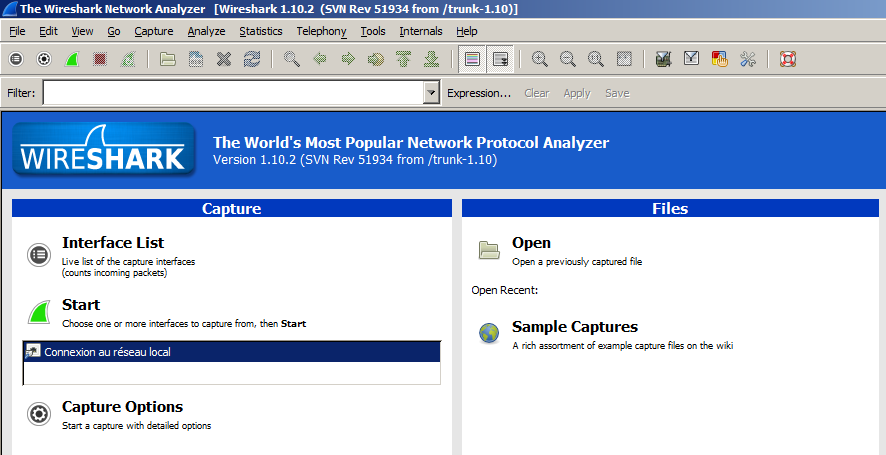


## Wireshark lancement:

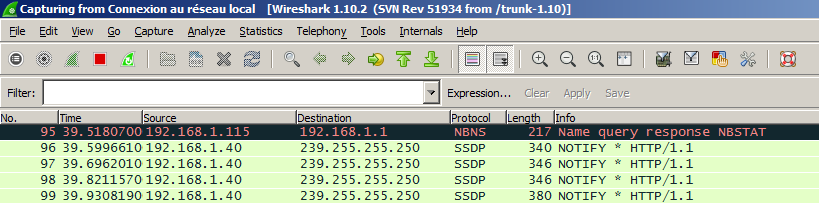
**N.B** : on ne peut auditer que la carte réseau d’un poste, donc on ne voit que les trames qui nous sont destinées, oui sont destinées à tous les postes (broadcast…). On devra donc :

* Se placer sur la machine voulue
* installer un hub (à la place d’un switch)
* mettre un port en mirroir sur le switch sur lequel on branchera notre carte réseau

On indique la carte réseau que l’on souhaite auditer, puis **Start**



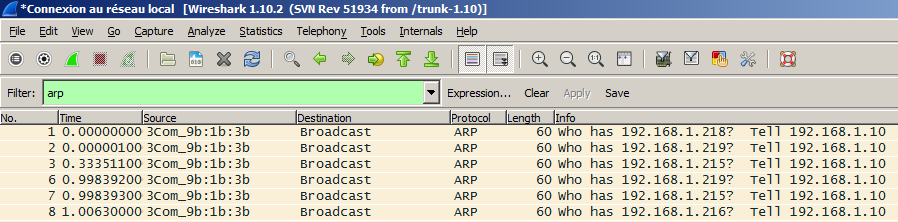
Puis **Start**



## Wireshark arp:

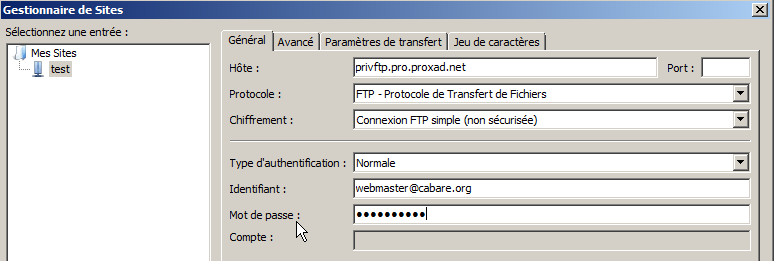
On peut filtrer selon un protocole précis

**Arp** (en vert s’il connait le protocole, attention, il est sensible à la casse…)

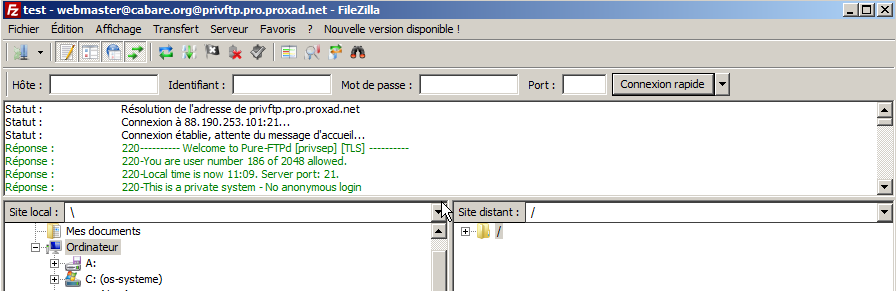


## Wireshark ftp:

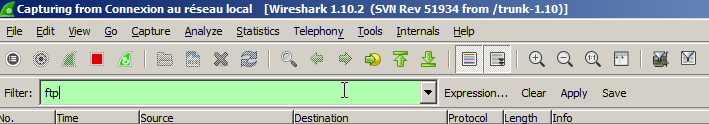
on met en place un client FTP genre filezilla avec les paramètres qui vont biens, par exemple un mot de passe ***ftporgzk28***…



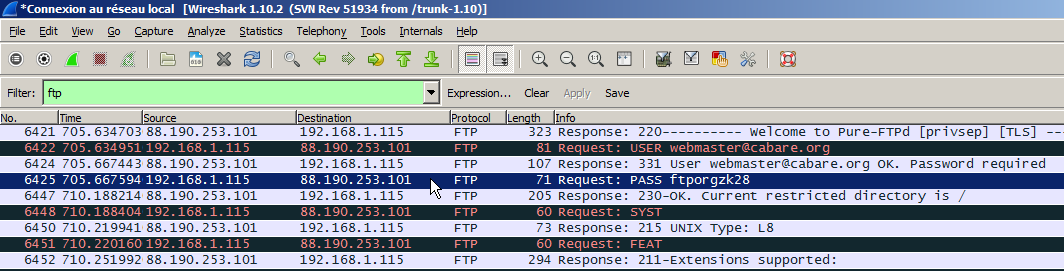
Et on fait une connexion



Parallèlement uis on filtre FTP dans wireshark



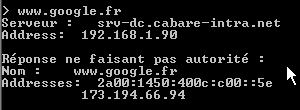
Et le travail est joué !



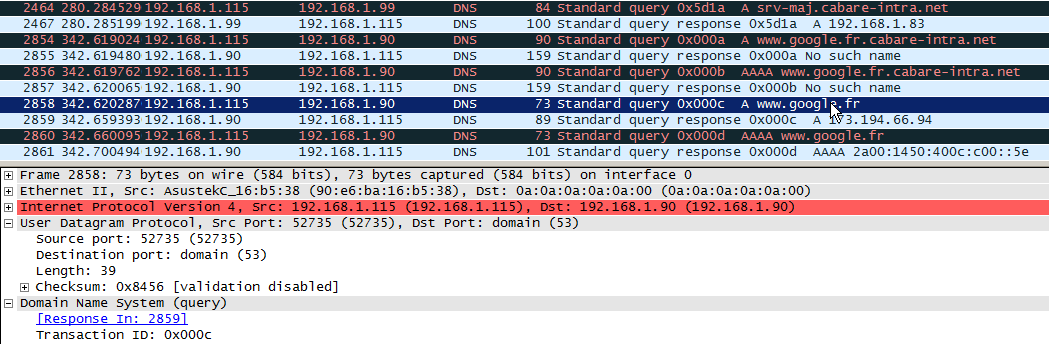
## Wireshark dns et nslookup:

On essaye de voir la résolution dns de nom sur www.google.fr

Donc dans nslookup je demande www.google.fr

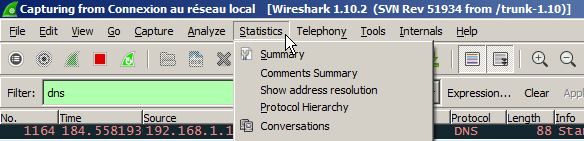


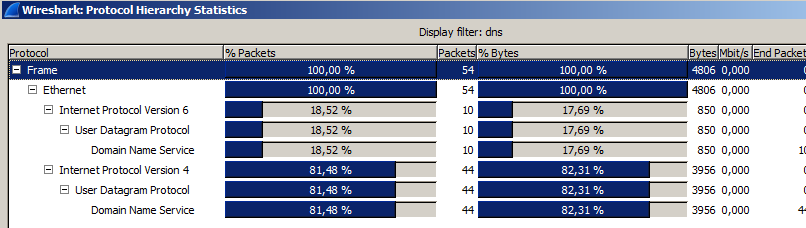
Et wireshark me répond et me donne le n° de la trame contenant la réponse



## Wireshark statistics:

On peut savoir par protocole (détecter un protocole intrus) le taux d’occupation du réseau, **Statistics / Protocol hierarchy**





Ou qui parle avec qui… **Statistics / Conversations**

