# Activité Wireshark : les graphiques de flux réseau

Document réalisé à partir de la page suivante : http://www.it-connect.fr/graphique-de-flux-reseaux-avec-wireshark/

> Vous devez connaitre les base dans l'utilisation de l'analyseur de protocoles wireshark.
>
> - Tutoriel : découverte de l'analyseur de protocoles Wireshark

## Wireshark : outil de capture réseaux et de création de graphiques réseaux

Wireshark est un outil de capture et d'étude de flux réseaux et permet de traiter la plupart des protocoles réseaux. Wireshark permet aussi de tracer des graphiques à partir des captures réseaux.

## Fonction IO Graph de Wireshark

- Lancez une capture durant quelques minutes puis arrêtez la capture.
- A partir du menu **Statistics** puis **IO Graph** :

Une nouvelle fenêtre va alors apparaître avec le graphique de la capture réseau, ce qui peut être plus ou moins long selon la taille de la capture et la puissance de l'ordinateur :

## Utilisation des filtres et paramétrage des axes X,Y

A de cette première courbe, il est possible d'effectuer différentes paramétrages pour mettre en évidence des informations spécifiques :

- en faisant varier les données de temps et de mesure,
- en jouant sur les couleurs des données
- en appliquant des filtres pour **trier** les informations pour permettre par exemple d'évaluer la quantité de flux réseaux entre deux ordinateurs ou sur un protocole précis.

En bas à droite de la fenêtre, il y a le paramétrage des **axe X** (Horizontal) **et Y** (Vertical) :

### X Axis

On gére la précision d'affichage des données en modifiant l'intervalle entre les points formant la courbe affichée et le nombre de pixel entre chaque point par **tranche** (c'est à dire entre deux barres de marquage).

Exemple avec un affichage plus précis en utilisant un intervalle de 0.01 seconde entre deux points consécutifs :

> L'affichage est **par défaut en temps** depuis le début de l'analyse et l'option L'option **View as time of day** permet d'afficher l'heure de la prise de capture s'il est nécessaire de savoir **à quel moment de la journée** un événement doit être identifié.

### Y Axis

L'unité de l'axe vertical qui pourra être :

- **Packets/ticks** : en nombre de paquets
- **Bytes/ticks** : en octets
- **Bits/ticks** : en bits
- **Advanced** : permet d'effectuer des filtrages plus avancés

La gestion de l'échelle permet sur un même graphique d'avoir une vue générale du graphique et également une vue très précise sur des

petites valeurs :

Il est aussi possible de **lisser** la courbe avec par exemple la valeur **M.avg 4** :

### Forme des graphiques

La forme des graphiques peut être :

- une courbe (**Line**),
- des points (**Dot**),
- un histogramme (**FBar** ou **Impulse**)

### Les filtres

Les filtres peuvent être utilisés dans les graphes de la même façon que dans l'utilisation **normale** de Wireshark et permettent de visualiser plusieurs représentations de graphique en même temps :

#### Exemple pour le trafic HTTP

Visualisation du trafic **http** (graph 2) par rapport à l'ensemble du **trafic** (graph 1):

**Conclusion** : l'ensemble du trafic correspond à du trafic http.

#### Exemple pour le trafic DNS

Ajout d'un troisième graphe sur du protocole **DNS** et pour le rendre plus visible, choix d'un graphique en **point**, **réduction** de l'échelle sur **X axis** et **augmentation** de l'échelle sur **Y Axis** :

En changeant l'unité de l'**axe Y** sur **Byte/trick** (octets), on peux déterminer la consommation en bande passante pour un protocole donné :

- à la seconde 140 le protocole http à consommé 488 ko (500 000 octets) :

Ce tour d'horizon des fonctionnalités de **représentation graphique** de Wireshark associées aux **filtres** permet de découvrir une autre manière d'analyser le trafic réseau de manière **statistique**.

### A faire

- réalisez une **capture** de trames d'environ **5 minutes**.
- utilisez les possibilités graphiques de Wireshark pour **mettre en évidence** dans le trafic réseau capturé :
  - le traffic réseau **généré par votre propre ordinateur**, tous protocoles réseaux confondus. Utiliser de préférence un filtre sur l'adresse MAC de votre ordinateur (eth.addr==adresse MAC),
  - le trafic réseau complet des **protocoles http, https et dns**,
  - la **consommation** en bande passante du trafic **http et https** sur le réseau.