Wireshark : analyseur de trafic réseau

- Objet : Observer le trafic réseau de sa machine avec WireShark
- Niveau requis :
  débutant, avisé
- Commentaires : *Que se passe-t-il réellement lorsque vous vous connectez à une machine, à un site, etc. ? Tout est là :)*
- Débutant, à savoir : Utiliser GNU/Linux en ligne de commande, tout commence là !.
- Suivi :
  à-compléter
  à-tester
  - Création par MaTTuX_ le 05/07/2007
  - Testé par <...> le <...>
- Commentaires sur le forum : ici[1)]

Résumé

Wireshark est un analyseur de protocole de réseau. Il examine les données à partir d'un réseau en direct ou à partir d'une capture de fichier sur disque. Vous pouvez naviguer de façon interactive sur les données capturées, visionner le résumé et l'information détaillée pour chaque ensemble. Wireshark possède quelques fonctions puissantes, incluant un affichage de langage filtré et la possibilité de visionner le flux reconstitué de la session TCP.

Installation

Il suffit de taper en console root

```
apt-get update && apt-get install wireshark gksu
```

Utilisation

```
gksu wireshark
```

ou

```
gksudo wireshark
```

Screenshot

Lien utile

- http://blog.rom1v.com/2012/06/utiliser-wireshark-sous-debian/

[1)]

N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !