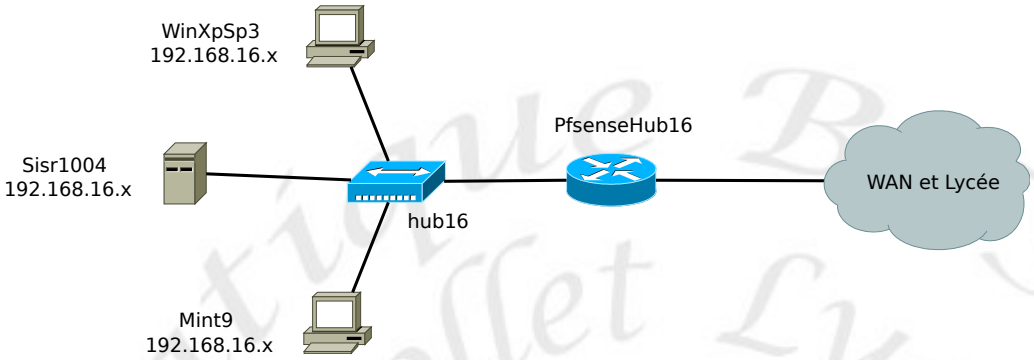
Capture de trames

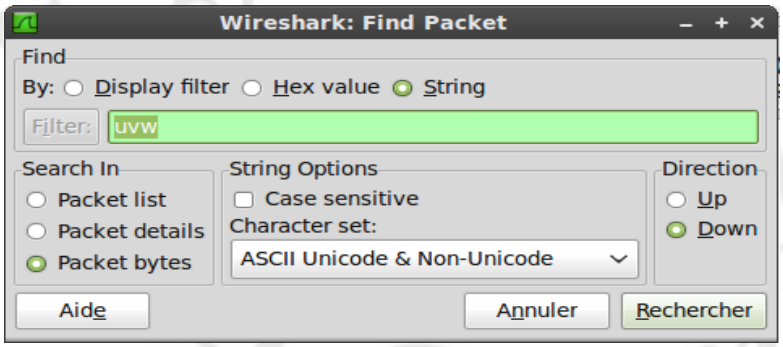
1 Installation



- La carte réseau de la Mint9 doit être en mode "promisc". Pour activer le mode "promisc" sur le système d'exploitation : *ifconfig eth0 promisc*

2 Utilisation de Wireshark

- Lancez Wireshark sur la Mint9. Écoutez eth0.
- A partir de WinXpSp3 :
  - Lancez un ping vers Sisr1004.
  - Naviguez sur "www.google.fr" avec Firefox.
  - Naviguez sur "sio.lgmarras.org" avec Firefox.
- Arrêtez la capture de trame sur Wireshark.
- Wireshark dispose de fonctions de triage :
  - En cliquant sur les intitulés de colonne ❀.
  - En utilisant la fonction recherche : par exemple recherchez si une trame contient la chaîne de caractères (string) "uvw" ❀.



  - En utilisant le filtre d'affichage :
    - Voir uniquement les trames qui utilisent le protocole UDP ❀ : "udp" . Remarquez que la couleur de votre filtre change si il y a des erreurs de syntaxe.
    - Voir uniquement les trames TCP qui pointent vers le port 80 ❀ : "tcp.port==80" (double égal).
    - Voir uniquement les trames qui viennent de PfsenseHub16 ❀ : "ip.src==192.168.16.254"
    - Voir les trames qui viennent du réseau 192.168.16.0 et qui vont au réseau 192.168.11.0 ❀ : "ip.src==192.168.16.0/24 and ip.dst==192.168.11.0/24"
    - Plus de documentation ici : http://wiki.wireshark.org/DisplayFilters

3 Analyse d'une trames de ping

- Réalisez une capture d'écran d'une trame "ping request" ❀.
- Réalisez une capture d'écran d'une trame "ping reply" ❀.
- Autres questions ❀ :
  - Quelles est la taille en octets d'une trame de ping.
  - Quel est le protocole d'un ping.
  - Quel est le nombre de trames générés par un "ping microsoft".
  - Quel est le corps du "message" contenu dans un "ping microsoft".

4 Analyse d'une trame DNS

- Réalisez une capture d'écran d'une trame "dns query" ❀.
- Réalisez une capture d'écran d'une trame "dns response" ❀.
- Dans la trame "dns response" isolez le contenu de la réponse (c'est à dire l'adresse ip) ❀.

5 Analyse d'une trame ARP

- Réalisez une capture d'écran d'une trame "arp request" ❀.
- Réalisez une capture d'écran d'une trame "arp reply" ❀.
- Recherchez une trame "arp request" qui utilise un broadcast ❀, puis réalisé un tableau avec LibreOffice qui explique le rôle de tous les champs qui composent les en-têtes de niveau 2 et de niveau 3 ❀.