

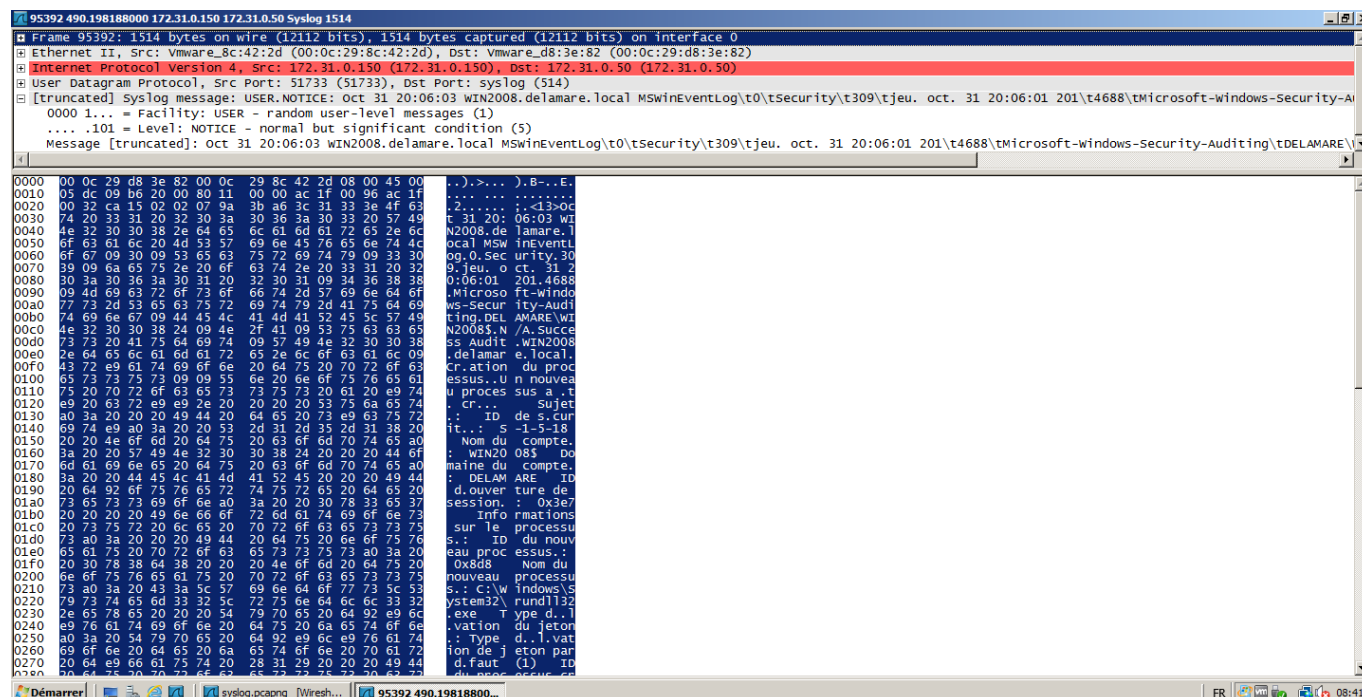
# Syslog exercice : Améliorer le paramétrage des applicatifs émetteurs de traces

En vous aidant des documents ci-dessous répondez aux questions suivantes :

- 1) Donner l'adresse du serveur syslog récepteur, l'adresse du serveur émetteur, le port d'écoute utilisé par le serveur de syslog et le protocole utilisé pour le transfert.
- 2) Dire quelle est la priorité du message (en base 10).
- 3) Préciser à quelle date et à quelle heure ce message a été transmis.
- 4) Donner le nom du serveur ayant émis ce message.
- 5) Conclure sur la difficulté d'analyse des messages syslog en cas d'émetteurs différents situés à la même adresse.
- 6) Proposer, devant l'abondance des messages émis, des modifications dans le paramétrage de Snare afin de faciliter l'analyse.
- 7) En faisant une synthèse des parties 1 et 2, retrouver sur le diagramme de déploiement les parcours possibles des messages syslog.

## Documents de travail

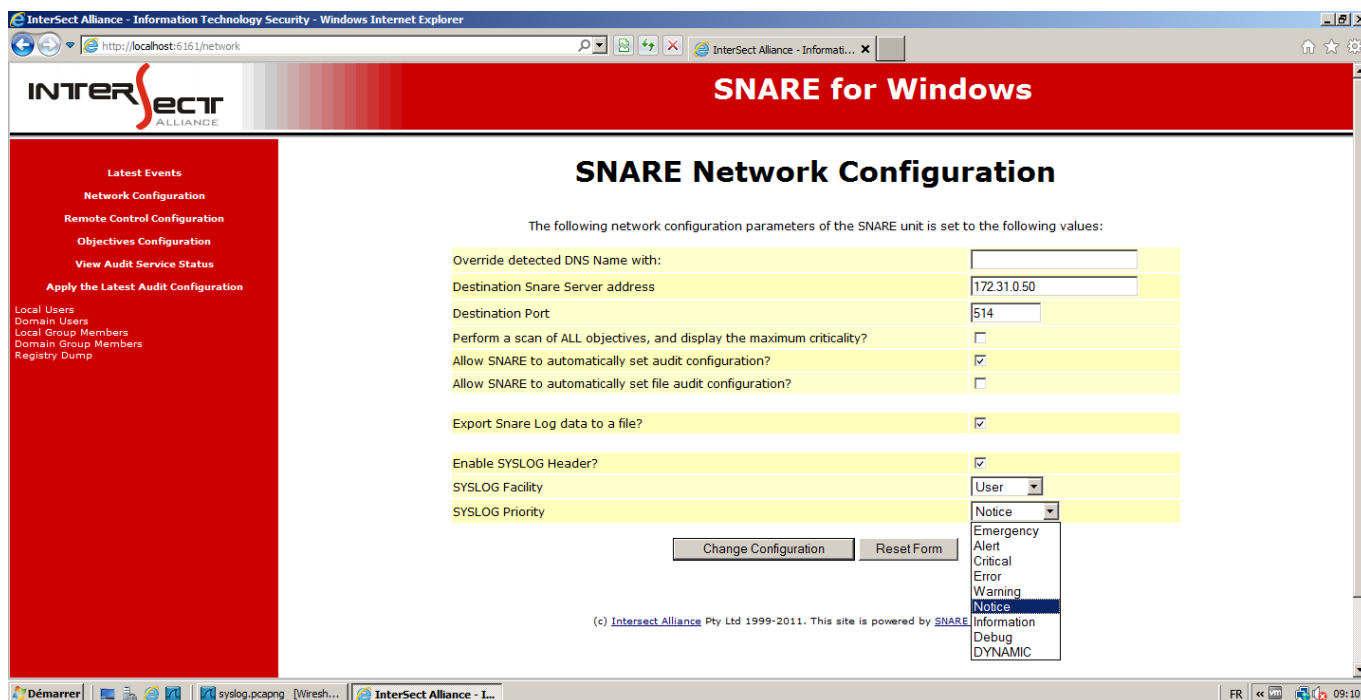
autre message syslog transmis depuis le même serveur et présent dans la même capture de trame



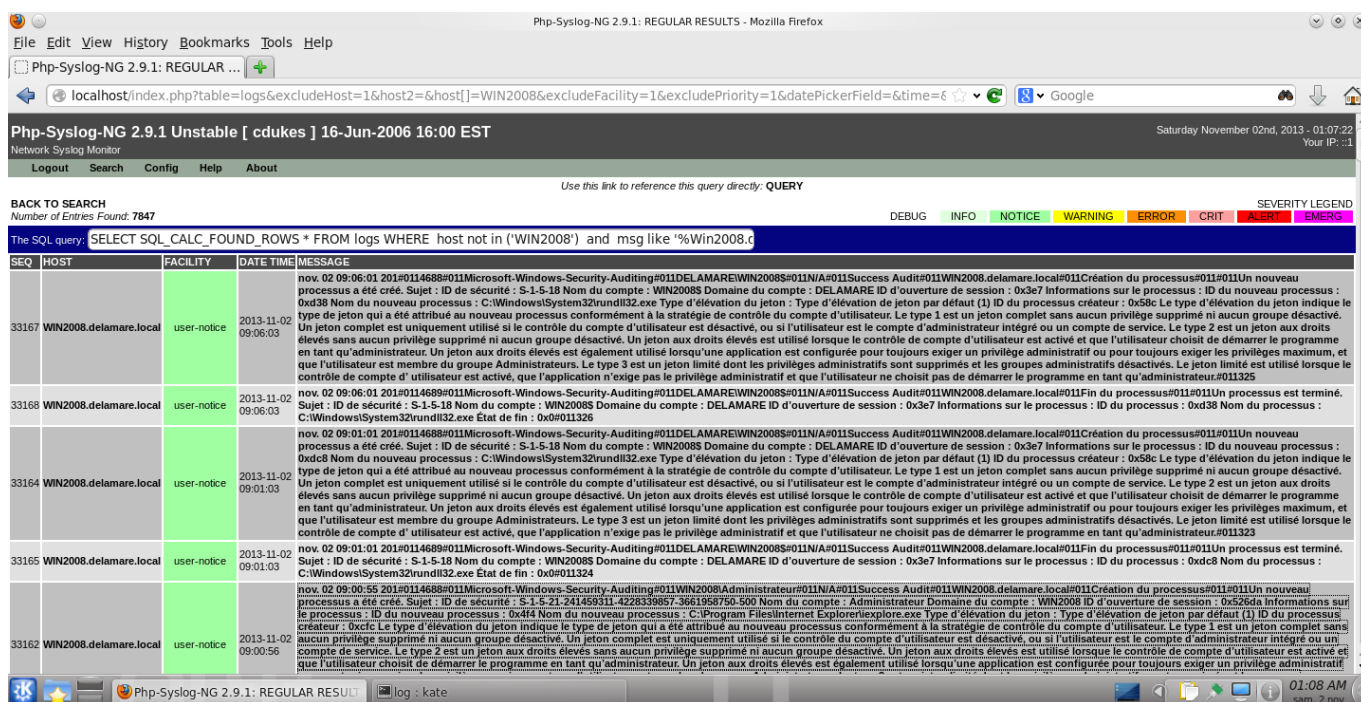
## Paramétrage du logiciel Snare

Les OS Windows ne peuvent pas envoyer les logs générés par l'observateur d'événements vers un serveur syslog.

Le logiciel Open Source **Snare** permet d'envoyer des messages **syslog**.



## La visualisation des messages via l'interface web du serveur de traces centralisé



From:

<https://siocours.lycees.nouvelle-aquitaine.pro/> - Les cours du BTS SIO

Permanent link:

[https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/sisr3/syslog\\_03](https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/sisr3/syslog_03)

Last update: 2014/11/24 10:26



