École Polytechnique de Montréal



INF3405

Réseaux informatiques

Hiver 2020 laboratoire 3

Soumis par

Roman Zhornytskiy (1899786) et

# [Hakim Payman](https://www.facebook.com/hakim.sakhawat) (1938609)

Soumis à Esther Guerrier

15 avril 2020

1) Quel filtre appliqueriez-vous afin d’afficher uniquement les échanges entre le client et le serveur? **(1 point)**

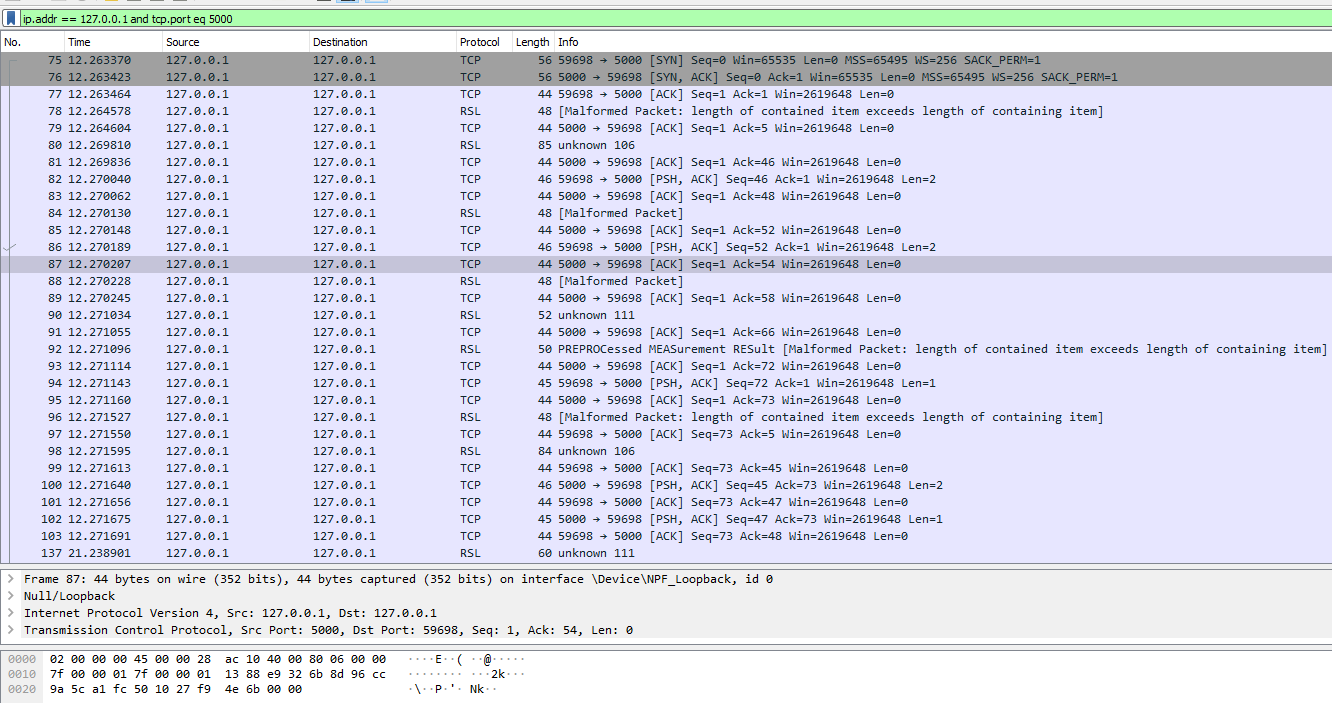
(pas sûr)

ip.addr == 127.0.0.1 and tcp.port eq 5000

2) À la lumière de vos observations, dites quel protocole de la couche 4 est utilisé pour la communication entre le client et le serveur. **(0.5 point)**

**Pas sûr non plus, car ca peut êre RSL (radio signalling link), mais je pense pas. Par contre le protocol OML (transmission control protocol) contient tous les données à mon avis, car il contient beaucoup de données.**

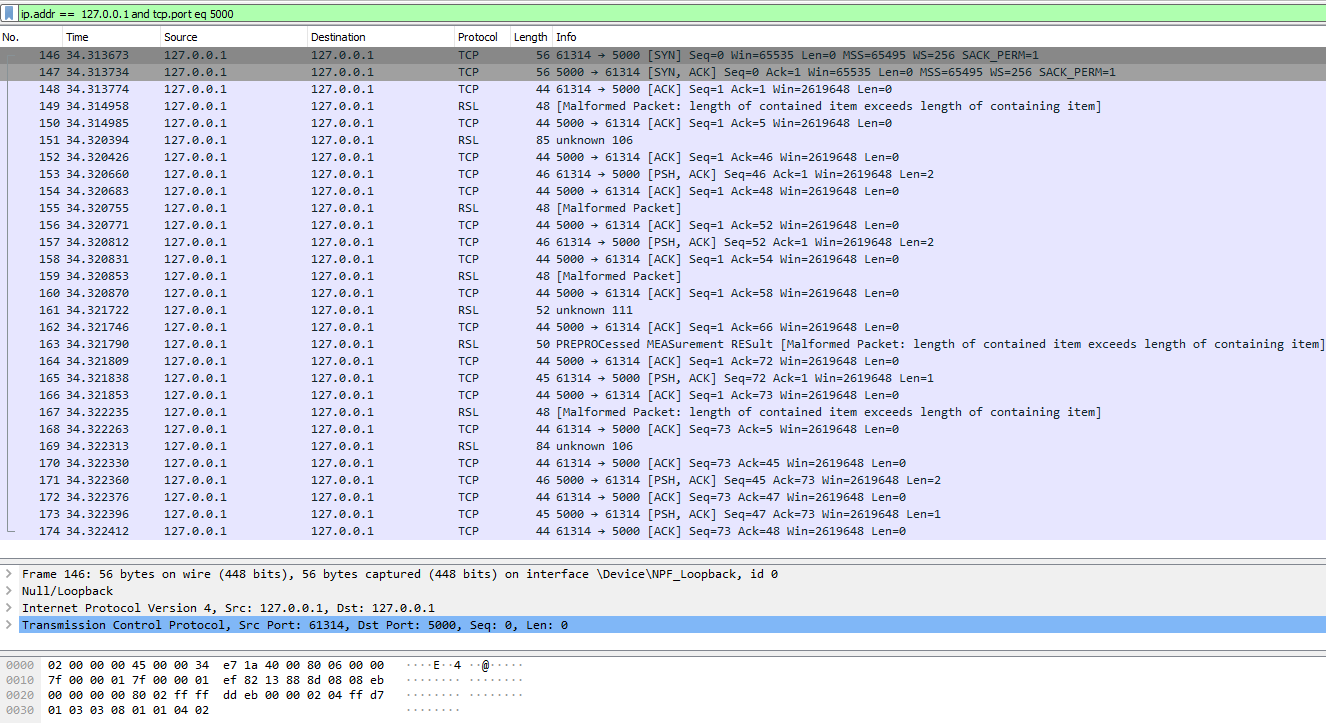
TCP



3) Combien de paquets et d’octets de données ont été envoyés du client vers le serveur et du serveur vers le client ? **(2 points)**

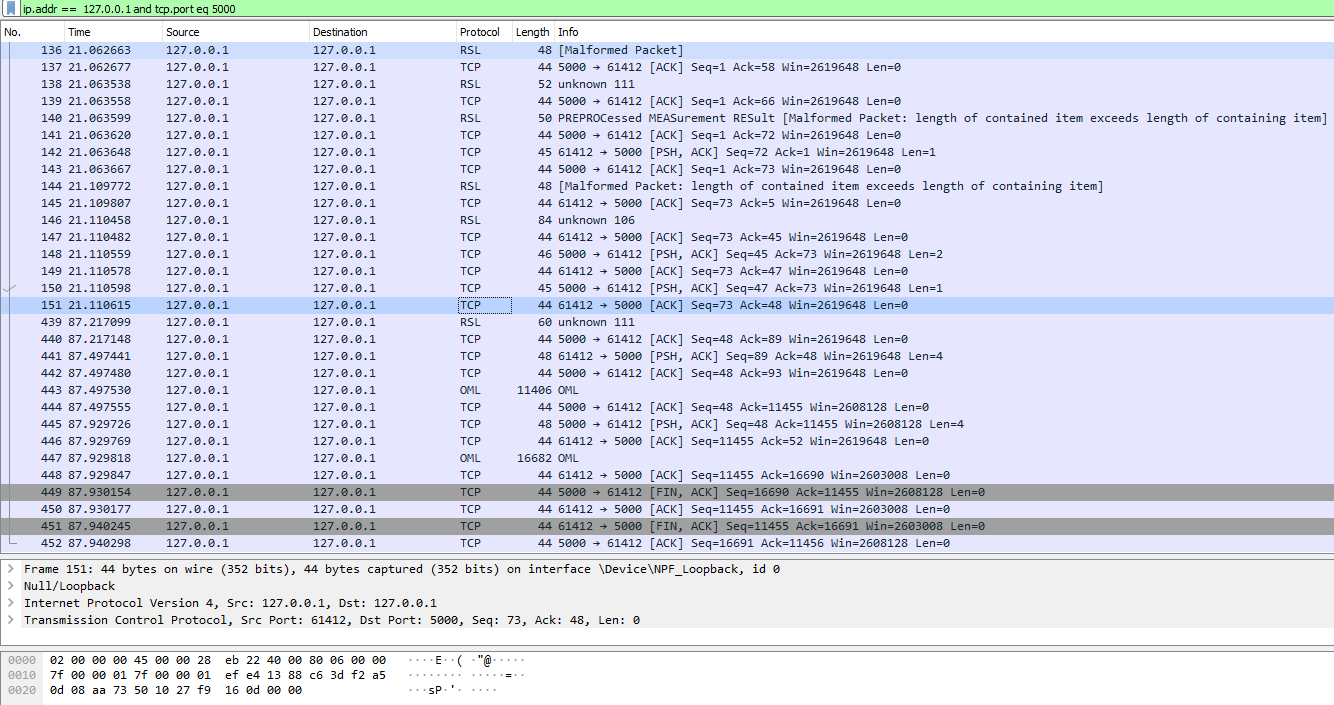
**Pas sûr**

Image lors de connexion du client au serveur :



Il y a 21 paquets TCP et 8 RSL (5 malformé et 3 inconnues)

Image après la réception de l’image sobelisé



Il y a 11 nouveaux paquets TCP, ce qui donne un total de 32 paquets TCP.

Note à effacer **: \*quand Dst port : 5000**\* cela veut dire que le client envoie au serveur.

Les 21 premiers paquets TCP établies la connexion entre le client et le serveur. Parmi ceux-là, le client envoie au serveur 9 paquets TCP et 6 RSL et le serveur envoie 12 paquets TCP et 2 RSL au client.

Ensuite, le client envoie un paquet RSL, 5 paquets TCP et un paquet OML (image originale).

Le serveur envoie 6 paquets TCP et un paquet OML (image sobelisé).

Alors, le client a envoyé 14 paquets TCP, 7 paquets RSL et 1 paquet OML, ce qui donne un total de 9 (données TCP) + 83 (données RSL incluant les malformés et les inconnues) + 11362 (données OML) = 11454 données.

Le serveur a envoyé 18 paquets TCP, 2 paquets RSL et 1 paquet OML, ce qui donne un total de 7 (données TCP) + 44 (données RSL incluant les malformés et les inconnues) + 16638 (données OML) = 16689 données.

4) Normalement, le standard IEEE 802.3 limite la taille d’une trame *Ethernet* à 1518 octets. Dans votre capture Wireshark, existe-t-il des paquets ayant une taille supérieure à 1518 octets? Si oui, expliquez pourquoi et comment ce paquet réussit à transiger sur le réseau alors que sa taille est plus grande que celle spécifiée par le standard. **(2.5 points)**

5) Quel type d’information êtes-vous capables d’extraire de Wireshark en lien avec l’authentification au serveur de traitement d’images? **(1 point)**

6) Il est possible, avec Wireshark, d’extraire l’image envoyée par le client ou l’image traitée. Donnez les étapes à suivre, incluant des captures d’écran montrant chaque étape permettant l’extraction de l’image envoyée du client vers le serveur. Servez-vous des propriétés du fichier.jpg énoncées plus haut. Indice: utilisez le programme *WinHex* après avoir sauvegardé le flot de données en format “ *Raw* ”. **(2 points)**

7) Suite à toute cette analyse que pouvez-vous conclure quant à la sécurité de l’application de traitement d’images que vous avez développé lors du travail pratique no.2. **(1 point)**

**3.6. Vérifier les hypothèses et argumenter**

1) Quel protocole de la couche transport est utilisé? Dans le cas de TCP, montrer le tout premier échange entre le client et le serveur lors de l’initialisation de la connexion, comment ce nomme cet échange? Dans le cas d'UDP, est-ce que ce même échange à lieu? Pourquoi? **(0.5 point)**

2) En vous basant sur les informations recueillies par Wireshark, indiquez les ports source et destination utilisés par la couche 4. **(0.5 point)**

3) Combien de paquets et d’octets contenant des données ont été envoyés par le client vers le serveur? Par le serveur vers le client? Montrer où vous avez trouvé cette information. **(0.5 point)**

4) À la lumière de votre analyse, que fait le client? Selon vous, combien d’itérations le client a-t-il faites pour envoyer ces données? **(0.5 point)**

**C) Analyse des performances et protocole TCP (2 points)**

1) Comparez la performance des envois de données pour le mode 1 et le mode 2. Qu’est-ce qui diffère entre ces deux modes? Lequel est le plus performant selon vous et pourquoi? **(0.5 point)**

2) Comparer la performance des envois de données pour le mode 3 et le mode 4. Qu’est-ce qui diffère entre ces deux modes? Lequel est le plus performant selon vous et pourquoi? **(0.5 point)**

3) Discutez de la fiabilité de chaque mode. Selon vous, quel(s) mode(s) est le plus fiable? **(0.5 point)**

4) Pour les modes secrets utilisant le protocole TCP, vous avez certainement remarqué à la fin de la communication un échange FIN, ACK. Expliquez en quoi consiste cet échange. **(0.5 point)**