

Département de génie informatique et génie logiciel

INF3405

Réseaux Informatiques

Hiver 2019

Rapport du TP3 : Analyse d’applications client-serveur avec WireShark

Soumis à Émilie Dion-Paquin

Julien Legault 1847125

Abdellah Rahmani 1965352

Le XXXXXXXX

# 7. Analyse de l’application client/serveur du laboratoire 1 (10 points)

**C) Analyse du flot de données de l’application de gestion de fichier**

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

(Ip.src==192.168.79.143 and ip.dst==192.168.79.145) || (Ip.src==192.168.79.145 and ip.dst==192.168.79.143)

Ce filtre masque toutes les communications n’allant pas du client (192.168.79.143) au serveur (192.168.79.145) ou du serveur au client.

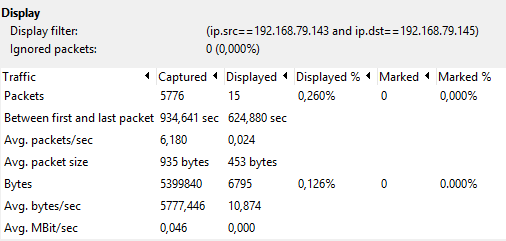
1. À la lumière de vos observations, dites quel protocole de la couche 4 est utilisé pour la communication entre le client et le serveur. **(0.5 point)**



Le protocole permettant la communication est le protocole TCP.

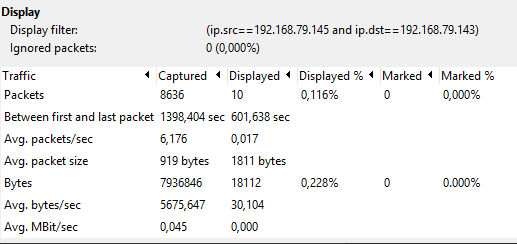
1. Combien de paquets et d’octets de données ont été envoyés du client vers le serveur et du serveur vers le client? **(2 points)**

Client → Serveur :



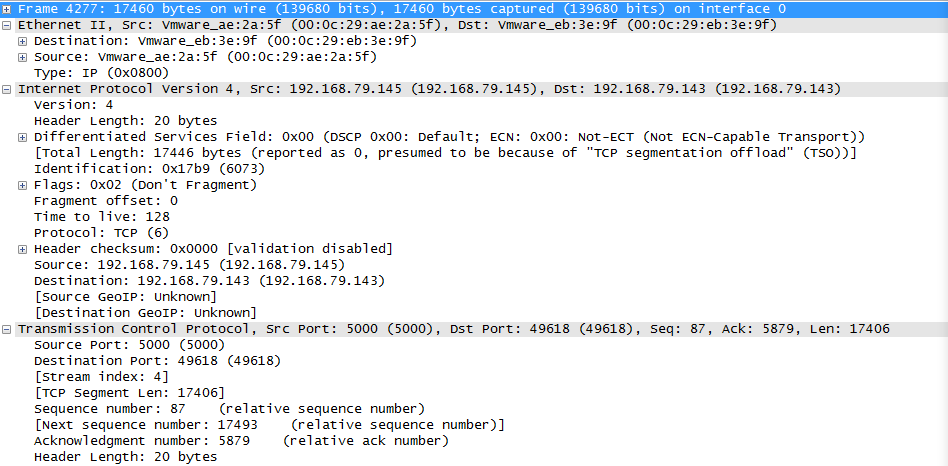
Du client au serveur, 15 paquets ont été envoyés pour un total de 6795 octets.

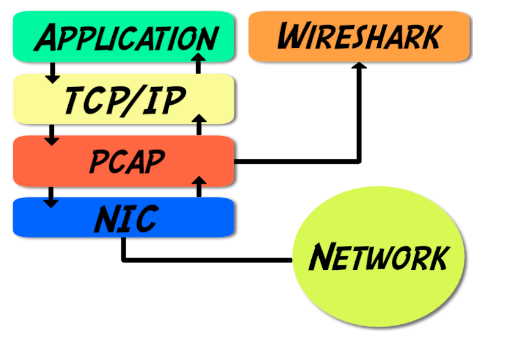
Serveur → Client :



Du serveur au client, 1 paquets ont été envoyés pour un total de 18112 octets.

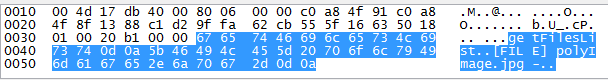
1. Normalement, le standard IEEE 802.3 limite la taille d’une trame Ethernet à 1518 octets. Dans votre capture Wireshark, existe-t-il des paquets ayant une taille supérieure à 1518 octets? Si oui, expliquez pourquoi et comment ce paquet réussit à transiger sur le réseau alors que sa taille est plus grande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



Oui, La capture ci-haut montre un paquet faisant plus de 1518 octets. La raison est que le paquet n’a pas été encore fragmenté afin de répondre au standard imposé par la norme IEEE 802.3. La raison pourquoi il n’a pas encore été fragmenté est que wireshark intercepte les paquets entre le TCP/IP et la carte réseau (NIC) qui fragmente les paquets avant de les envoyer sur le réseau. 

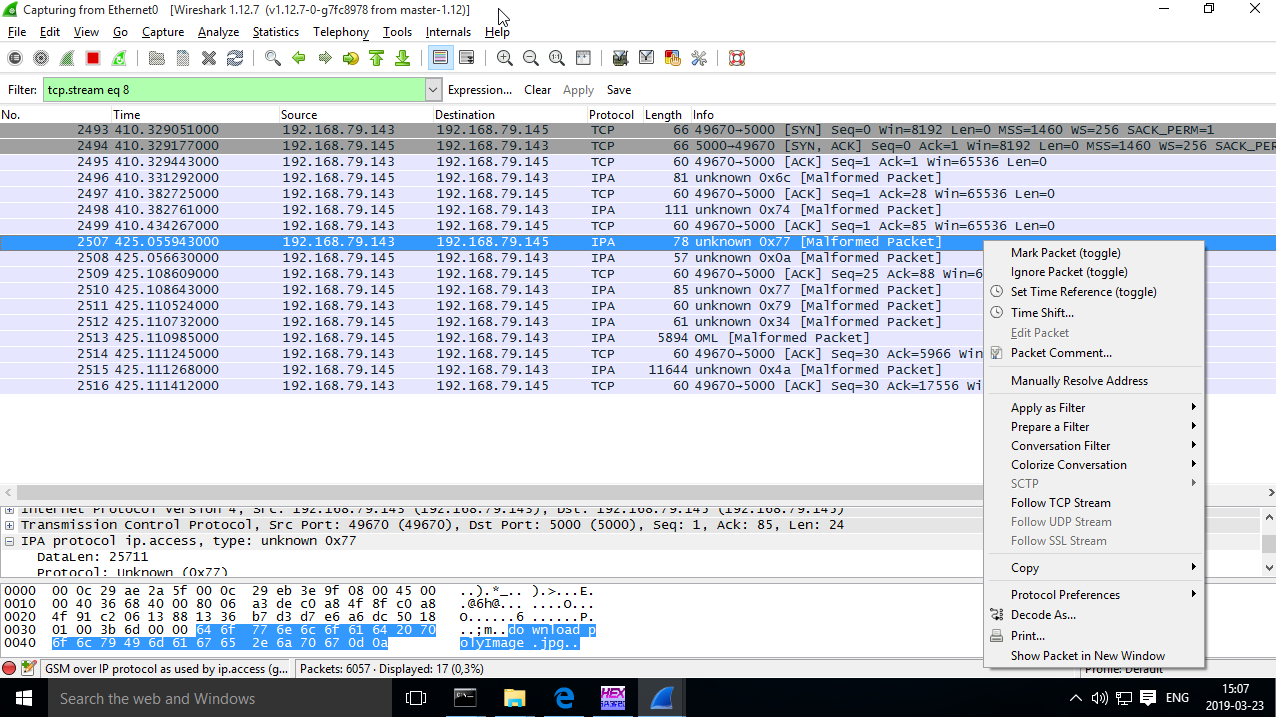
<http://packetbomb.com/how-can-the-packet-size-be-greater-than-the-mtu/>

1. Quel type d’information êtes-vous capables d’extraire de Wireshark en lien l’exécution de la commande « ls » ? Montrer vos résultats **(1 point)**

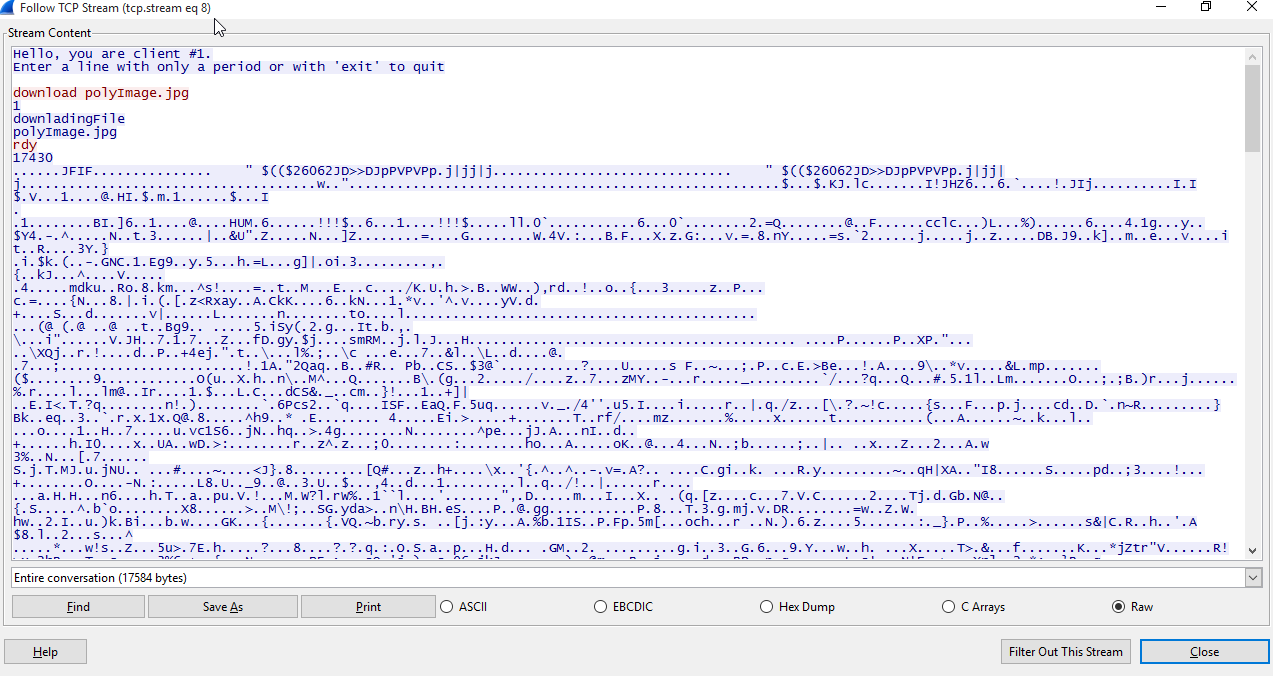


On peut voir que la commande « ls » envoi une valeur encodé sur 37 octets effectuant un « getFiles » du côté serveur retournant ainsi tous les fichiers présents. Dans notre cas, seul l’image « polyImage.jpg ».

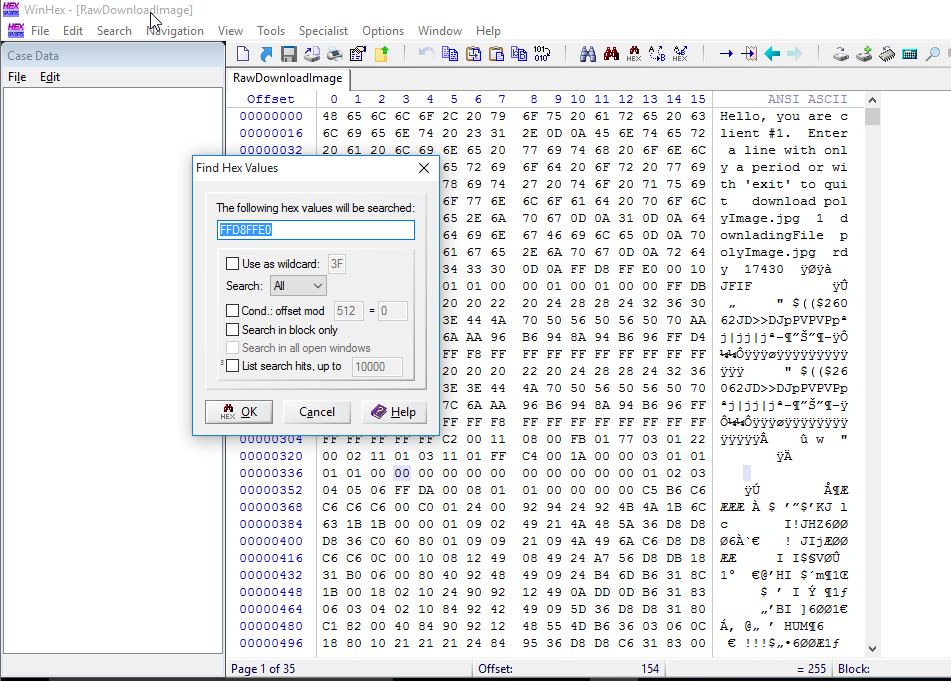
1. Il est possible, avec Wireshark, d’extraire l’image envoyée par le client ou l’image envoyer par le serveur vers le client. Donnez les étapes à suivre, incluant des captures d’écran montrant chaque étape permettant l’extraction de l’image envoyée du client vers le serveur. Servez-vous des propriétés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



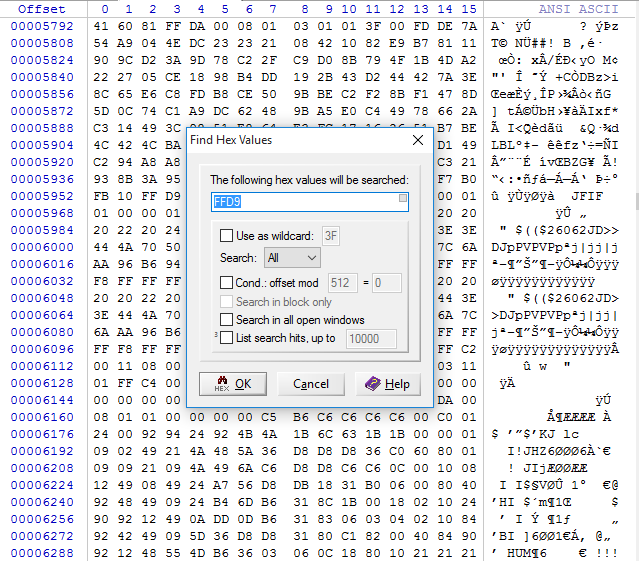
1. Trouvons l’instruction nous intéressant, soit un download PolyImage.jpg et effectuons un Follow TCP Stream pour sauvegarder le paquet.



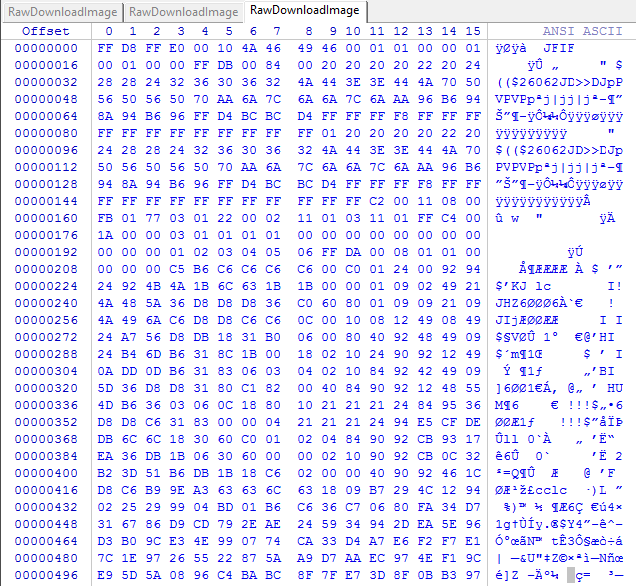
1. Enregistrons le fichier en .Raw pour modifier les données avec le logiciel WinHex.



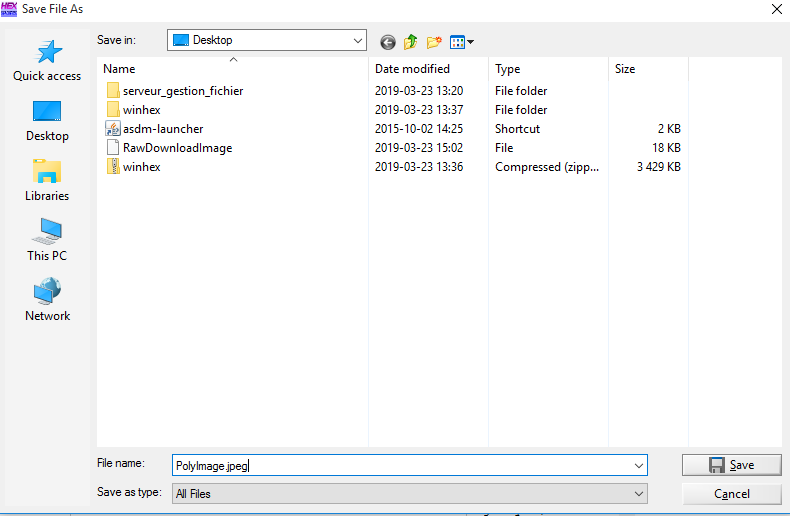
1. Cherche l’entête de début de l’image avec FFD8E0 pour retirer tous les entêtes antécédentes identifiant les protocoles de transport utilisés.



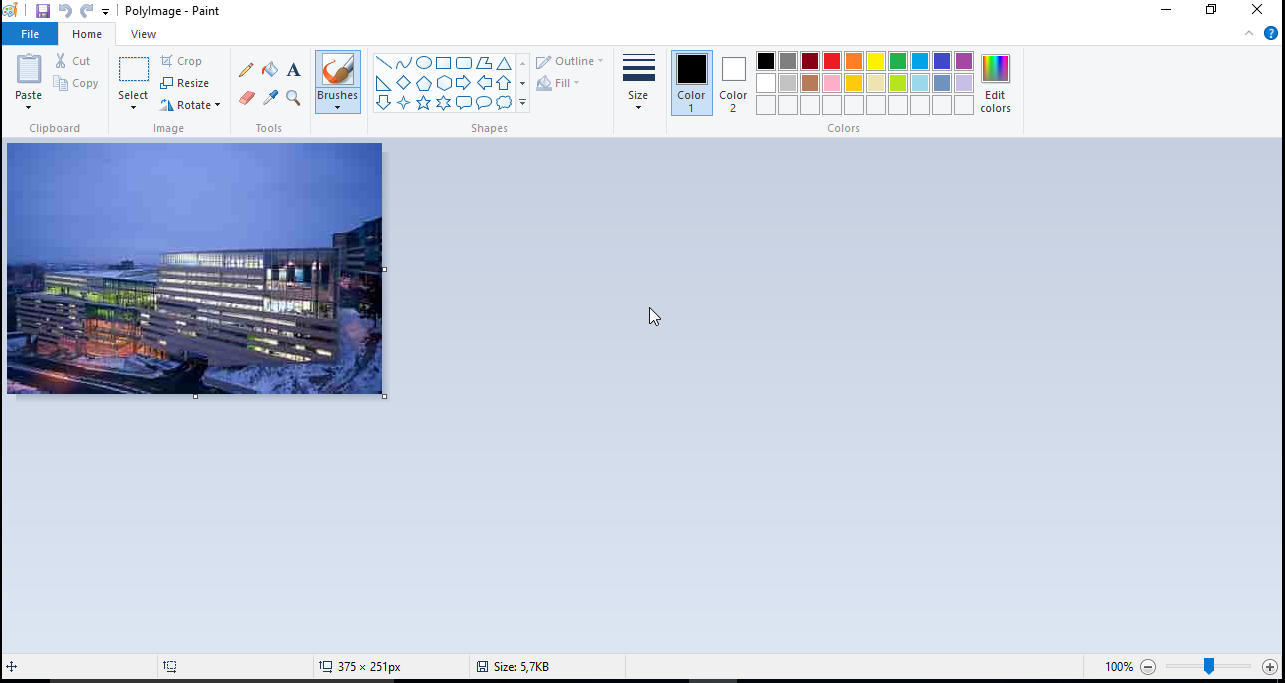
1. Cherche l’entête de fin de l’image avec FFD9 pour retirer toutes les données ne faisant pas partie de l’image.



1. Une fois que nous avons les données ne représentant que l’image, nous pouvons aller choisir l’option Save As.



1. On enregistre les données sous forme jpeg



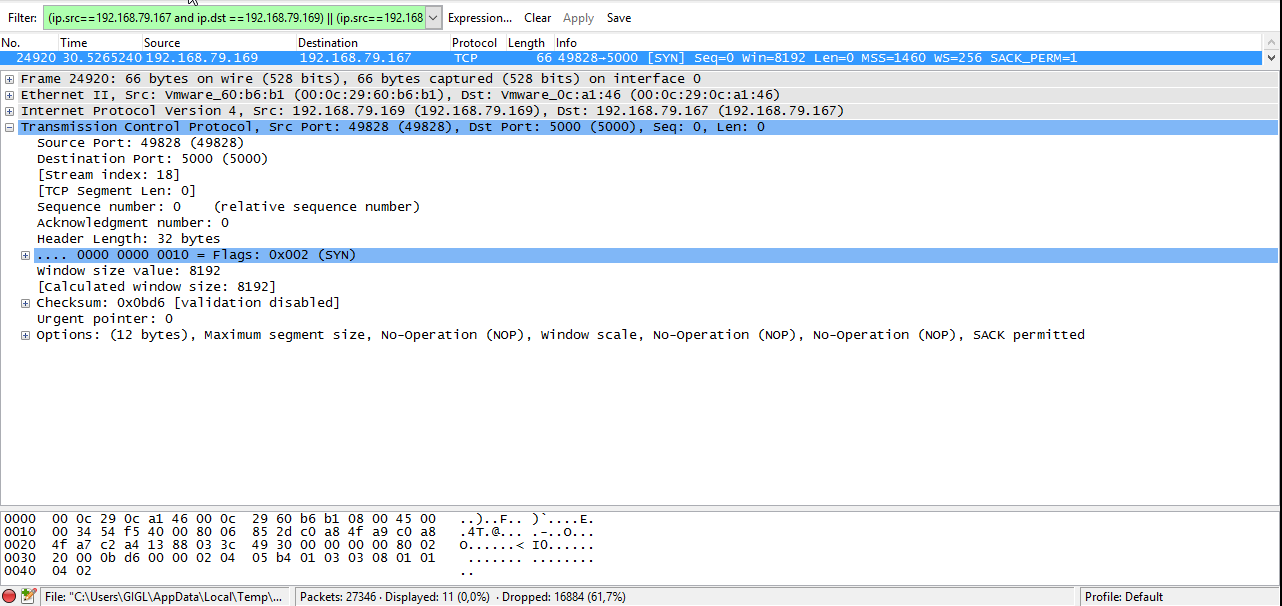
1. On Ouvre l’image avec Paint pour voir que nous avons bien notre image initiale.
2. Suite à toute cette analyse que pouvez-vous conclure quant à la sécurité de l’application de gestion de fichier que vous avez développé lors du travail pratique no.1 **(1 point)**

Nous constatons que nos données ne sont pas du tout protégées et que si quelqu’un intercepte l’envoi des données, il sera alors très facile de récupérer son contenu.

Partie 8

Mode 1 :

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)

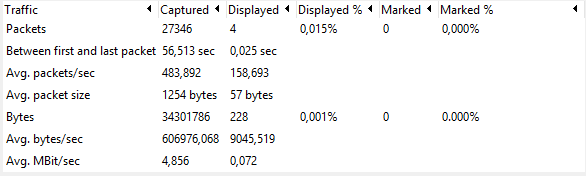


1. En vous basant sur les informations recueillies par Wireshark, indiquez les ports source et destination utilisés par la couche 4. (0.5 point)

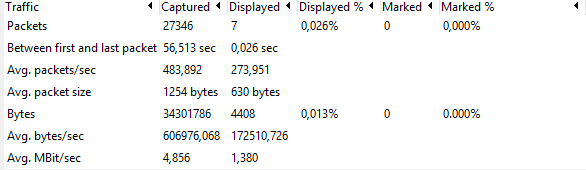


1. Combien de paquets et d’octets contenant des données ont été envoyés par le client vers le serveur? Par le serveur vers le client? Montrer où vous avez trouvé cette information. (0.5 point)

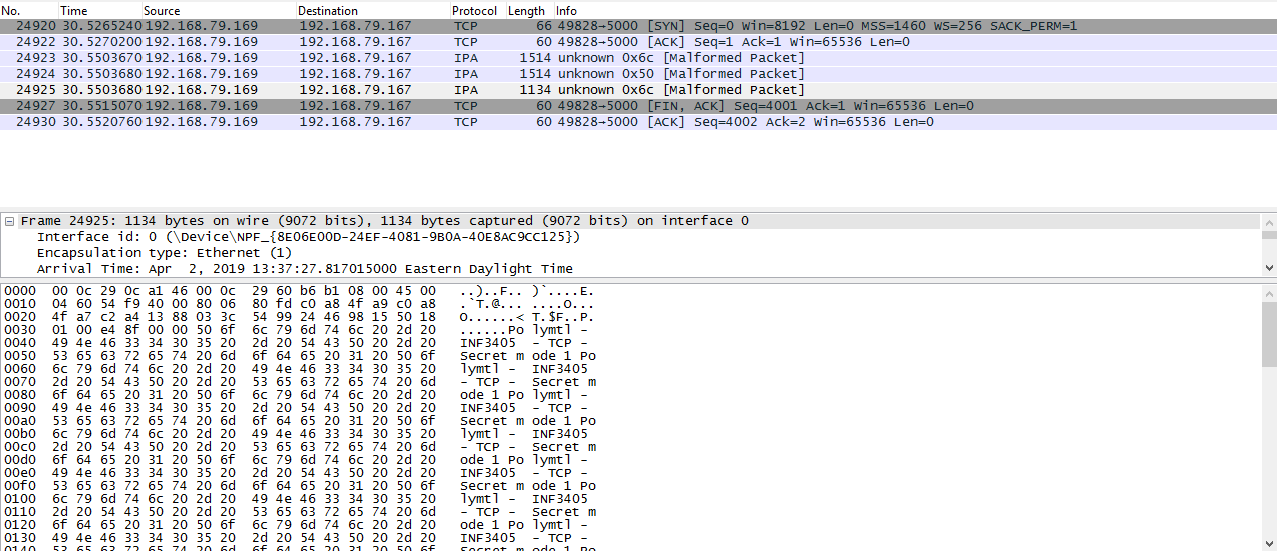
SERVEUR A CLIENT



CLIENT A SERVEUR



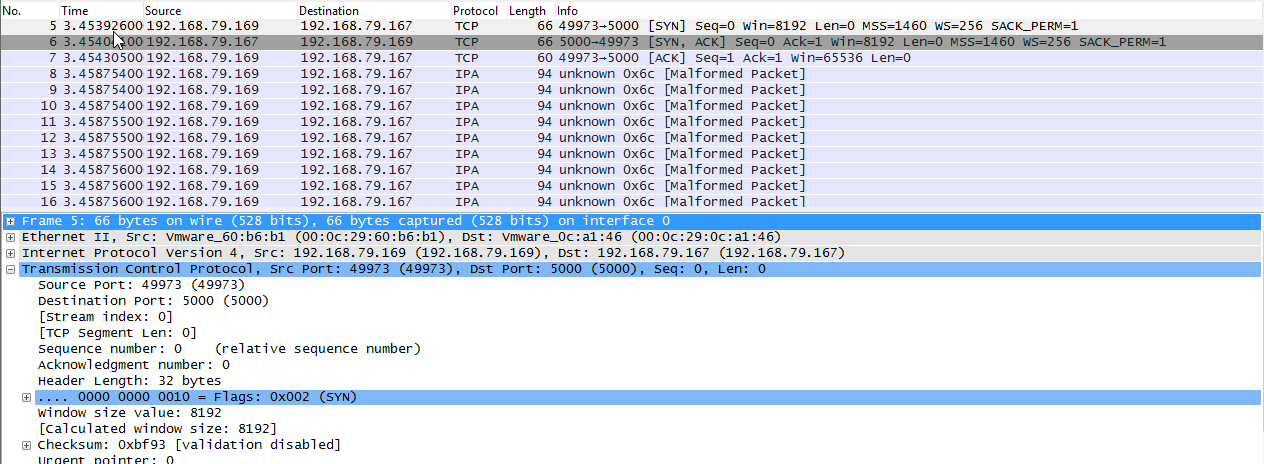
1. À la lumière de votre analyse, que fait le client? Selon vous, combien d’itérations le client a-t-il faites pour envoyer ces données? (0.5 point)



1 Seule puisque les paquets de type TCP ne sont que les entêtes alors que IPA contient les données avec le message secret << Polymtl – INF3405 – TCP – Secret – mode 1 …>>

Mode 2 :

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)

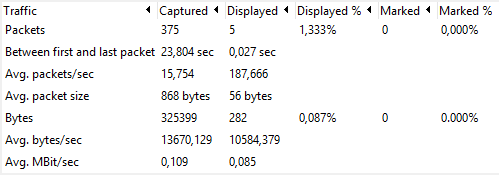


1. En vous basant sur les informations recueillies par Wireshark, indiquez les ports source et destination utilisés par la couche 4. (0.5 point)

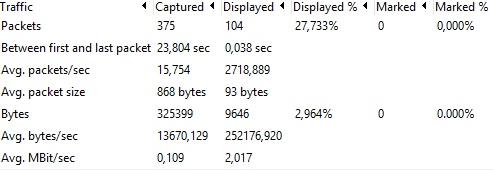


1. Combien de paquets et d’octets contenant des données ont été envoyés par le client vers le serveur? Par le serveur vers le client? Montrer où vous avez trouvé cette information. (0.5 point)

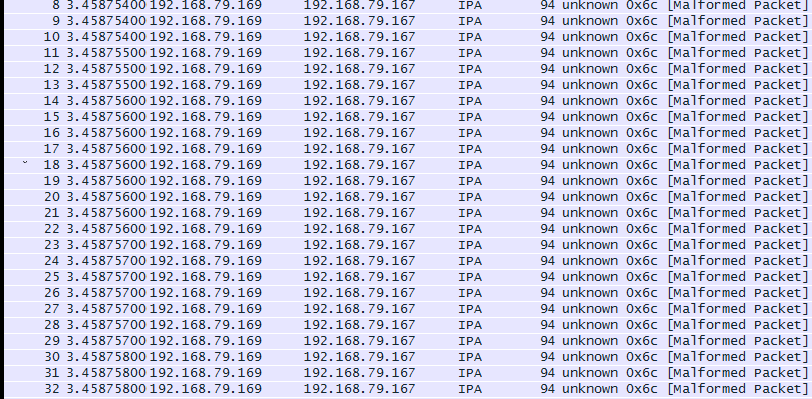
SERVEUR A CLIENT



CLIENT A SERVEUR

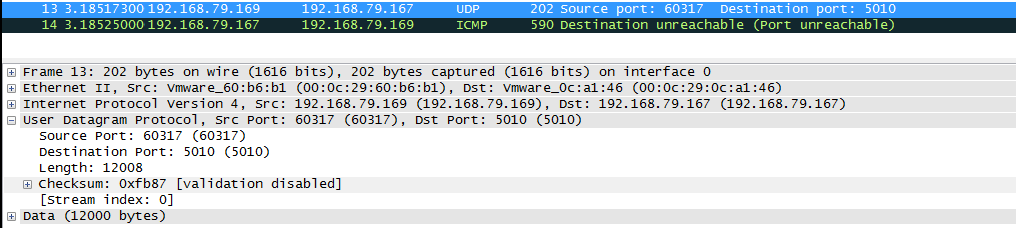


4) À la lumière de votre analyse, que fait le client? Selon vous, combien d’itérations le client a-t-il faites pour envoyer ces données? (0.5 point)



Mode 3 :

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)



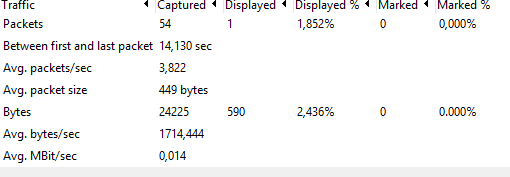
UDP pas de SYN pour la synchro.

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

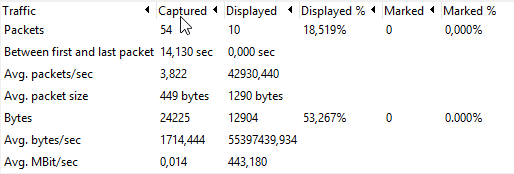


1. Combien de paquets et d’octets contenant des données ont été envoyés par le client vers le serveur? Par le serveur vers le client? Montrer où vous avez trouvé cette information. (0.5 point)

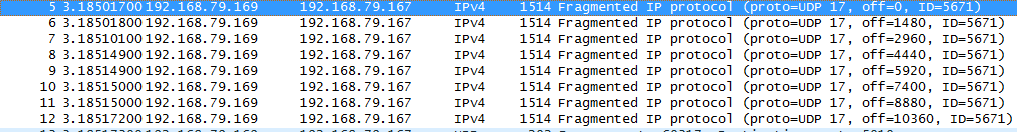
SERVEUR A CLIENT



CLIENT A SERVEUR



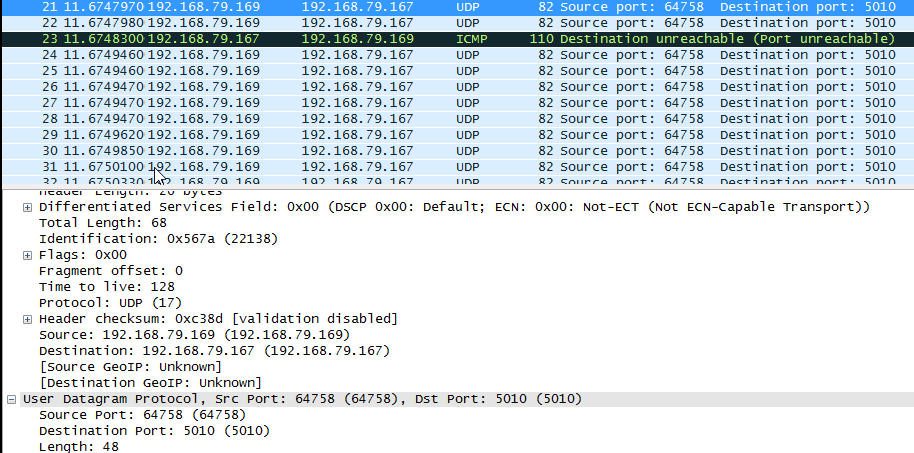
1. À la lumière de votre analyse, que fait le client? Selon vous, combien d’itérations le client a-t-il faites pour envoyer ces données? (0.5 point)



Une seule

Mode 4 :

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)



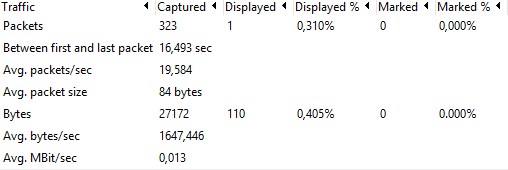
Pas de sync

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

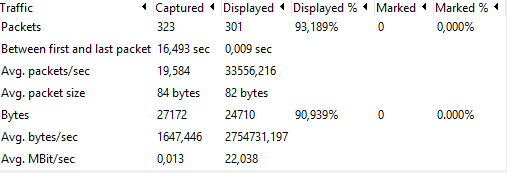


1. Combien de paquets et d’octets contenant des données ont été envoyés par le client vers le serveur? Par le serveur vers le client? Montrer où vous avez trouvé cette information. (0.5 point)

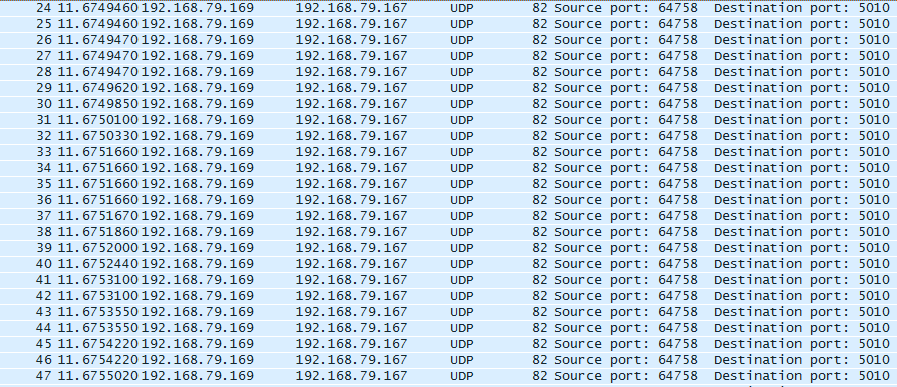
SERVEUR A CLIENT



CLIENT A SERVEUR



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)

1. 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)
2. Discutez de la fiabilité de chaque mode. Selon vous, quel(s) mode(s) est le plus fiable? (0.5 point)

TCP plus fiable mais plus long

1. 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)

Le principe de TCP qui sert à valider l’envoi de chaque paquet.