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)

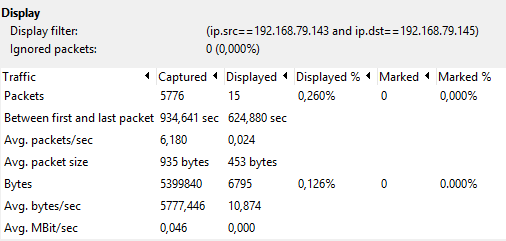
1. À la lumière de vos observations, dites quel protocole de la couche 4 est utilisé pour la communication entre le client et le serveur. (0.5 point)

Le protocole permettant la communication est le protocol TCP.



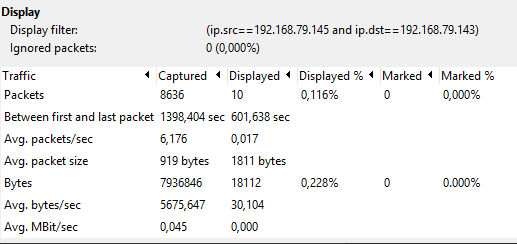
1. Combien de paquets et d’octets de données ont été envoyés du client vers le serveur et du serveur vers le client? (2 points)

Client –> Serveur

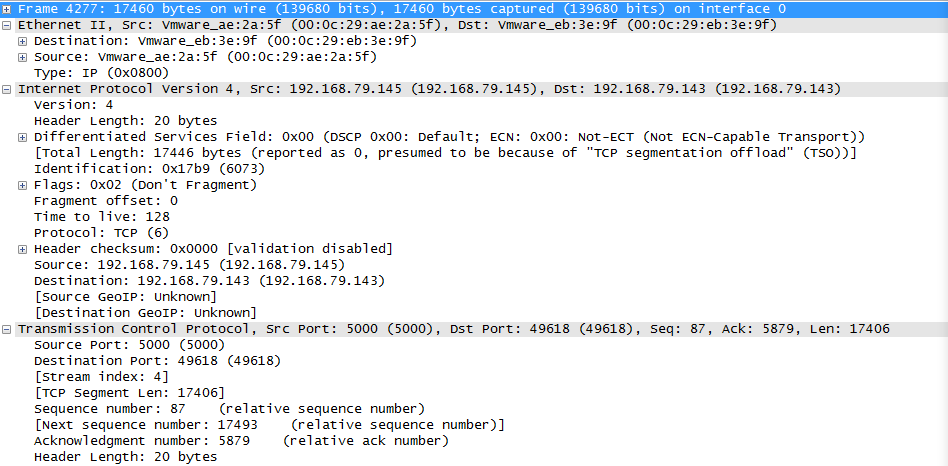




Serveur -> Client

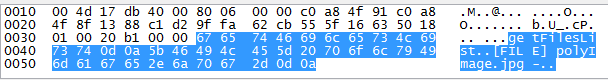


1. Normalement, le standard IEEE 802.3 limite la taille d’une trame Ethernet à 1518 octets. Dans votre capture Wireshark, existe-t-il des paquets ayant une taille supérieure à 1518 octets? Si oui, expliquez pourquoi et comment ce paquet réussit à transiger sur le réseau alors que sa taille est plus grande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

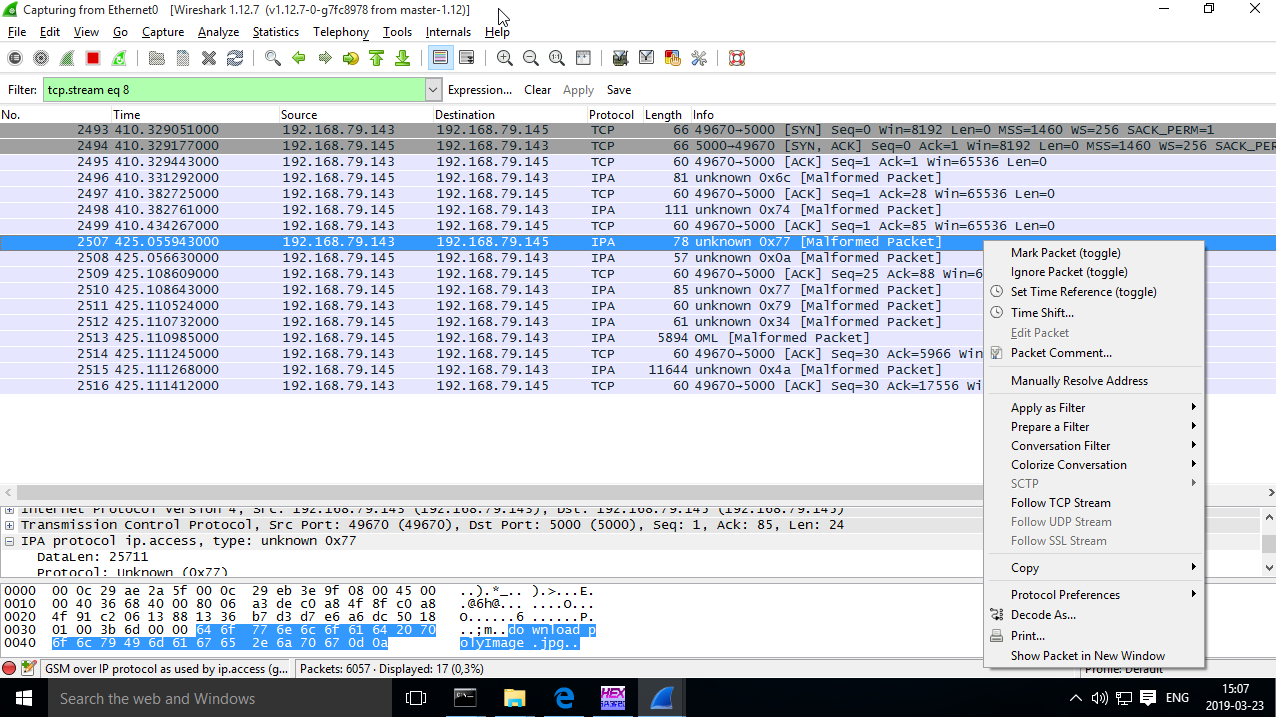


Oui, paquet non fragmente.

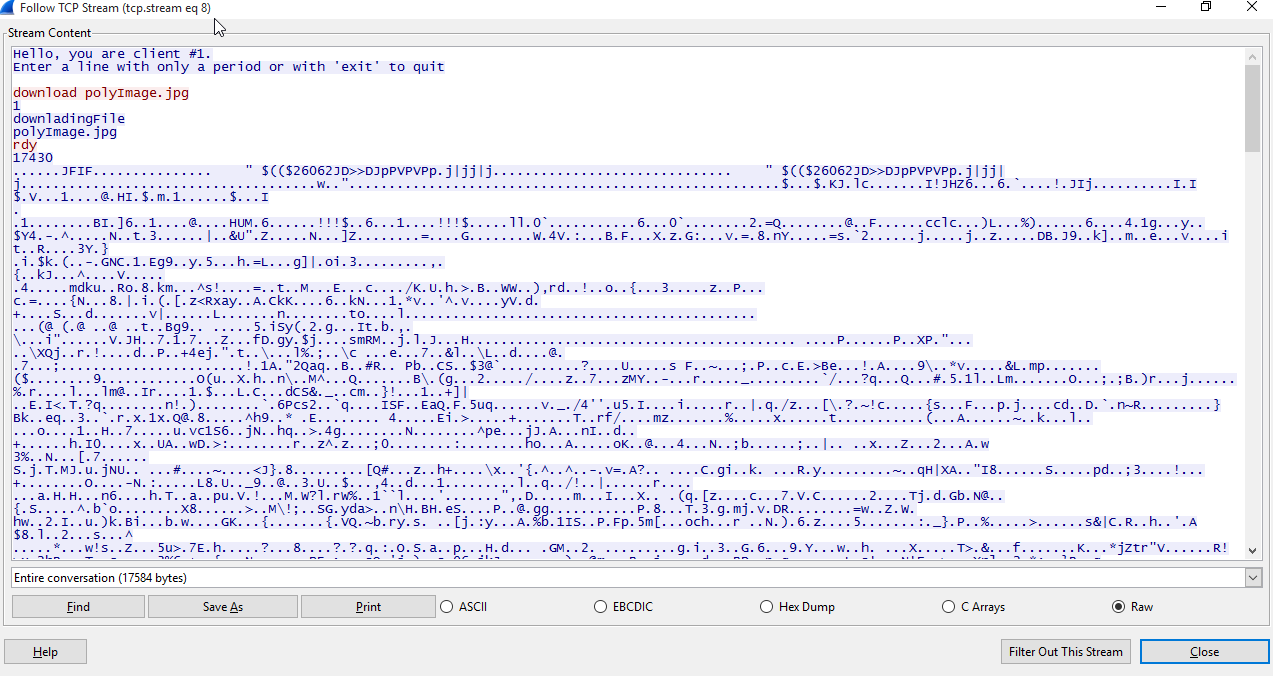
1. Quel type d’information êtes-vous capables d’extraire de Wireshark en lien l’exécution de la commande « ls » ? Montrer vos résultats (1 point)



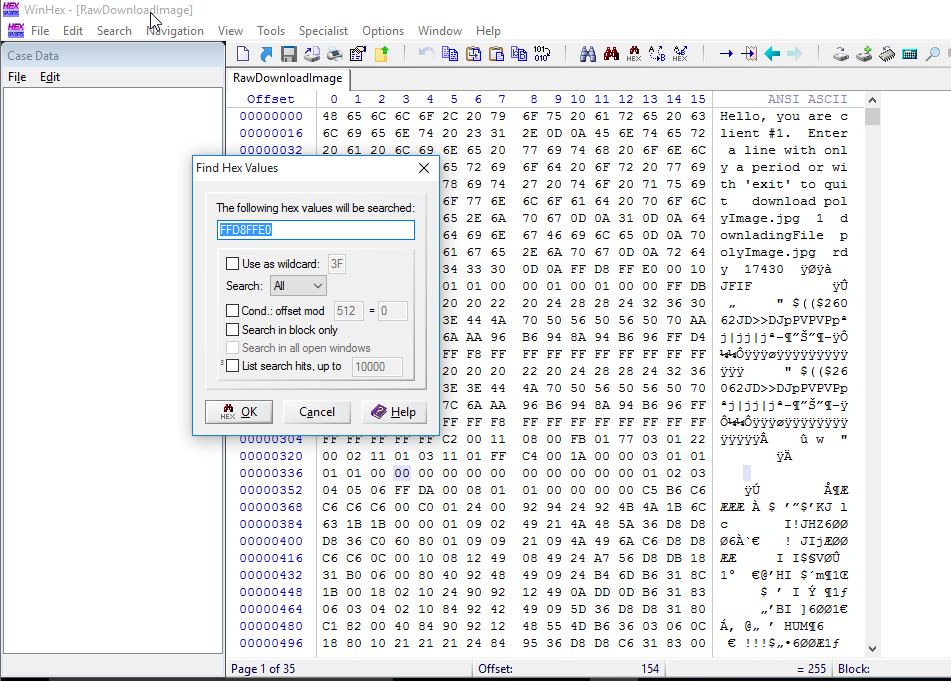
1. Il est possible, avec Wireshark, d’extraire l’image envoyée par le client ou l’image envoyer par le serveur vers le client. Donnez les étapes à suivre, incluant des captures d’écran montrant chaque étape permettant l’extraction de l’image envoyée du client vers le serveur. Servez-vous des propriétés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



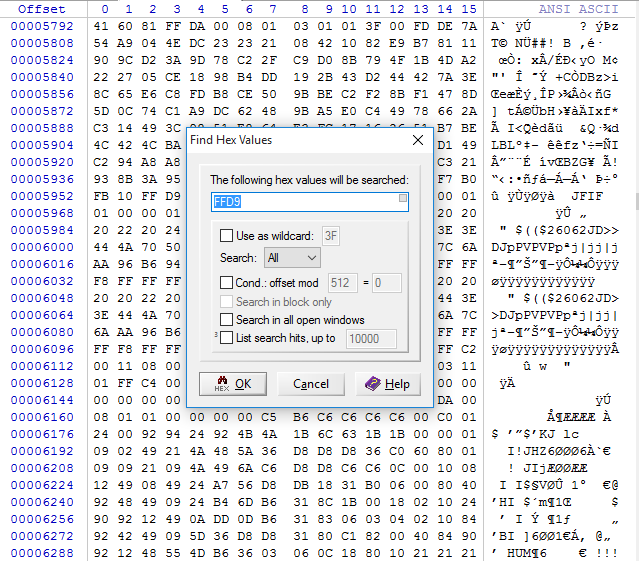
Follow TCP



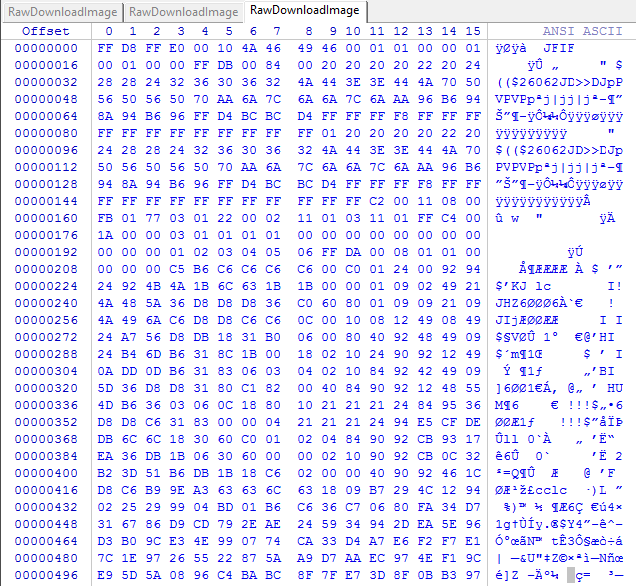
Save As Raw

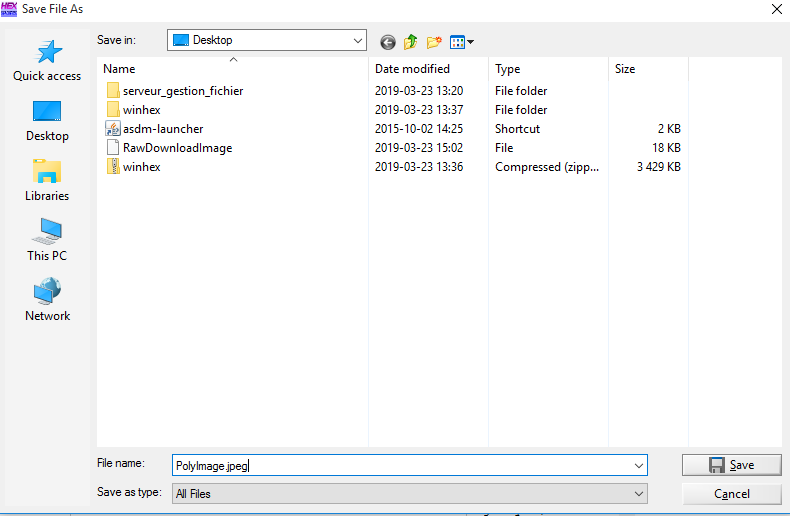


Cherche entête image avec FFD8E0

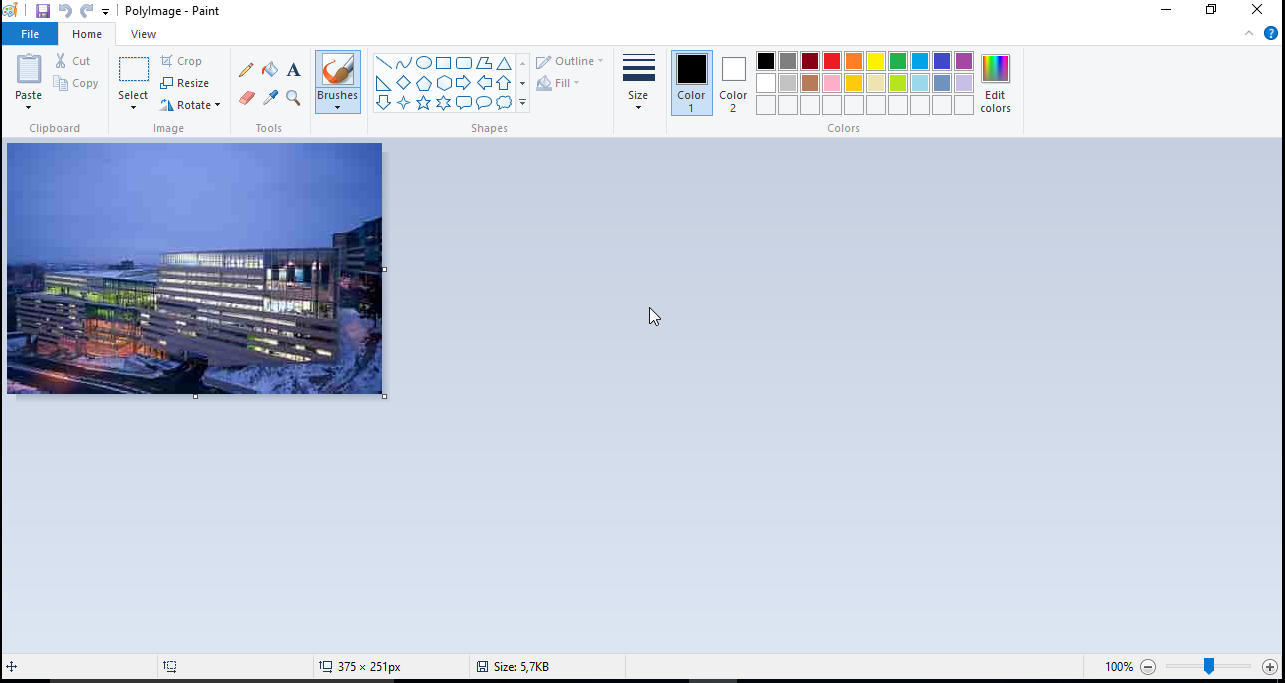


Cherche la fin de limage



On enlève ce qui est avant FFD8DDE0 et après FFD9 pour n’avoir que l’image 

On enregistre les données sous forme jpeg



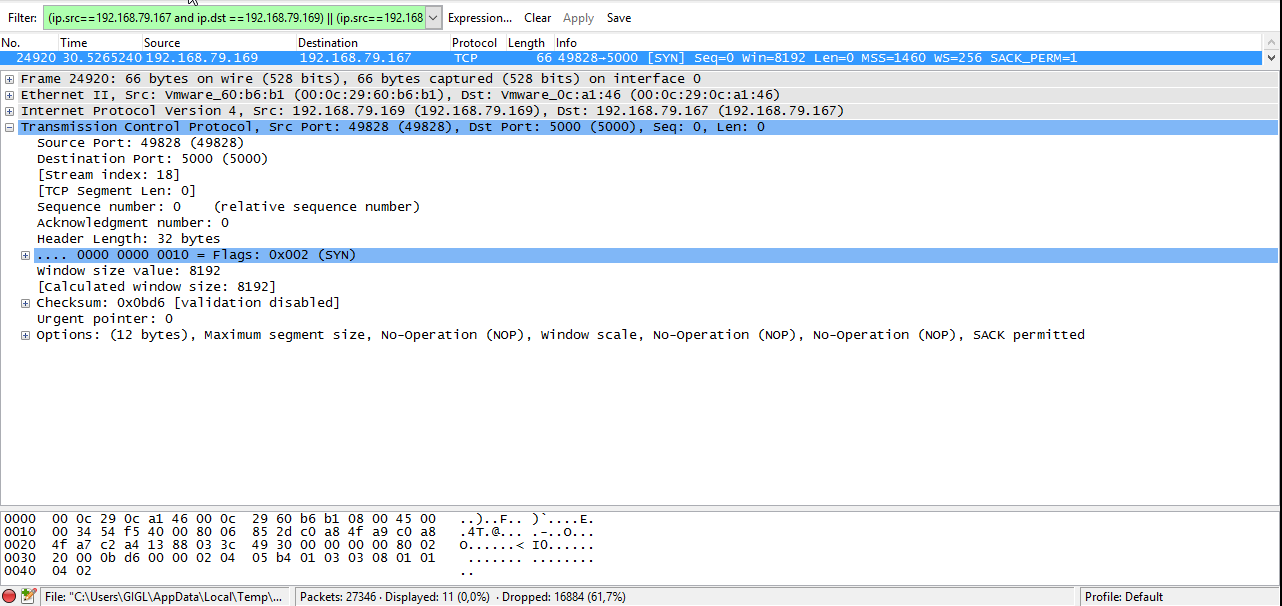
On Ouvre l’image avec Paint

1. 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)

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)

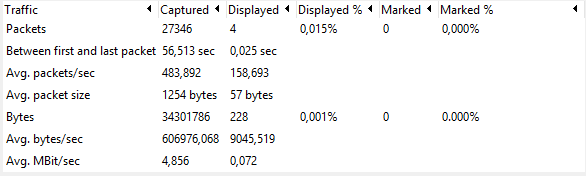


1. En vous basant sur les informations recueillies par Wireshark, indiquez les ports source et destination utilisés par la couche 4. (0.5 point)

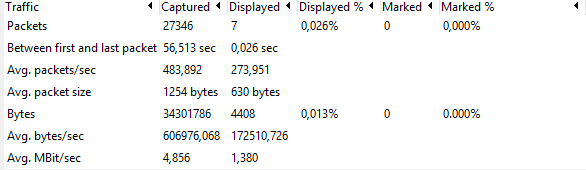


1. Combien de paquets et d’octets contenant des données ont été envoyés par le client vers le serveur? Par le serveur vers le client? Montrer où vous avez trouvé cette information. (0.5 point)

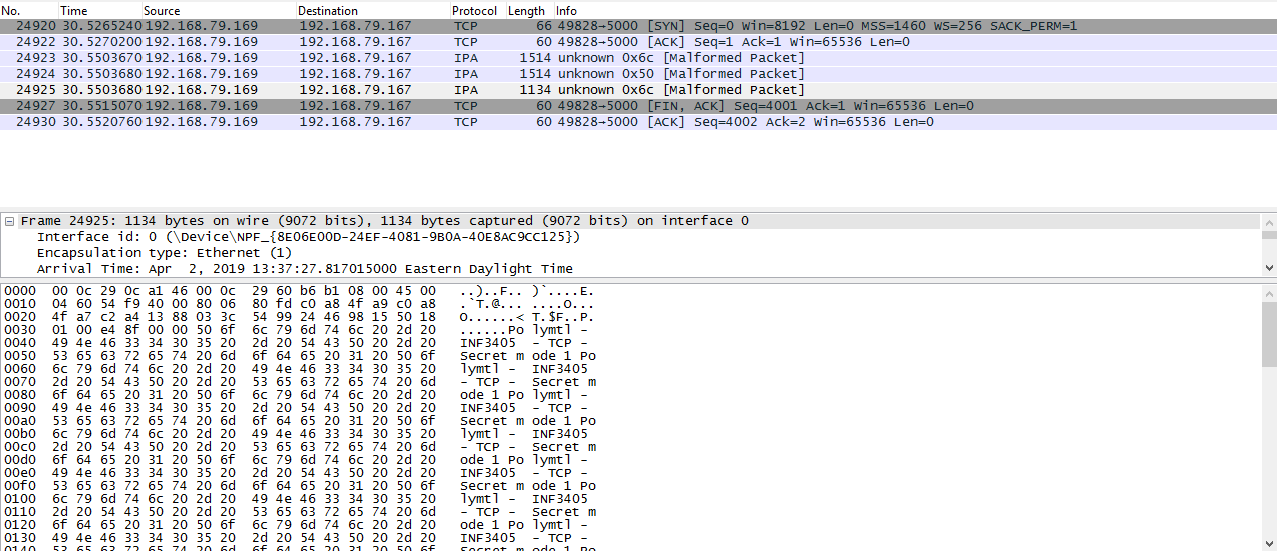
SERVEUR A CLIENT



CLIENT A SERVEUR



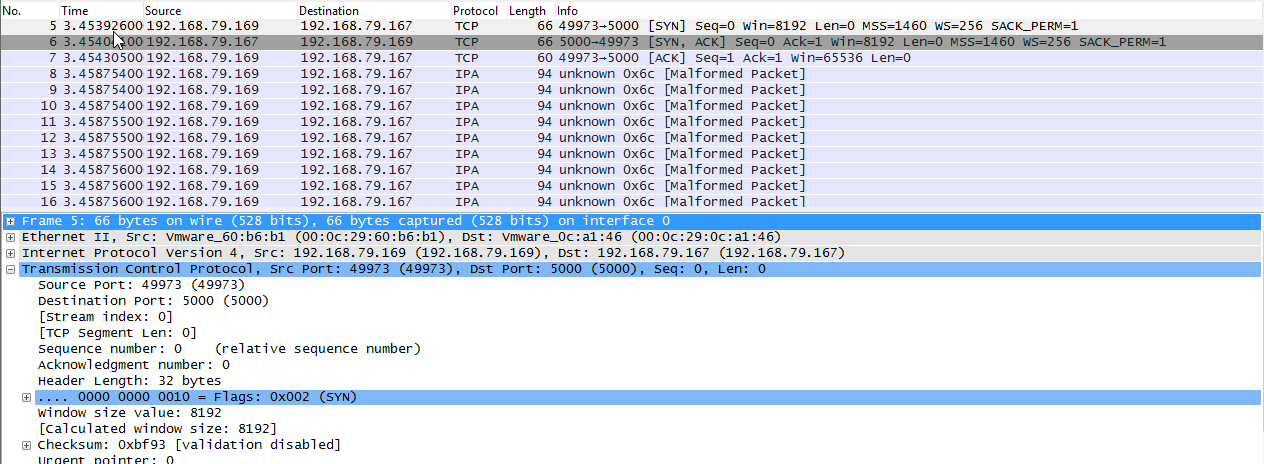
1. À la lumière de votre analyse, que fait le client? Selon vous, combien d’itérations le client a-t-il faites pour envoyer ces données? (0.5 point)



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)

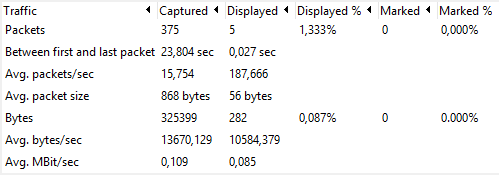


1. En vous basant sur les informations recueillies par Wireshark, indiquez les ports source et destination utilisés par la couche 4. (0.5 point)

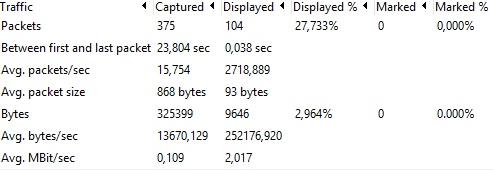


1. Combien de paquets et d’octets contenant des données ont été envoyés par le client vers le serveur? Par le serveur vers le client? Montrer où vous avez trouvé cette information. (0.5 point)

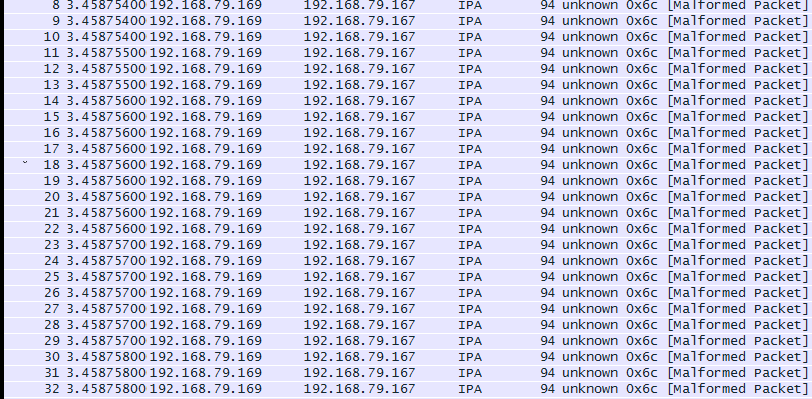
SERVEUR A CLIENT



CLIENT A SERVEUR

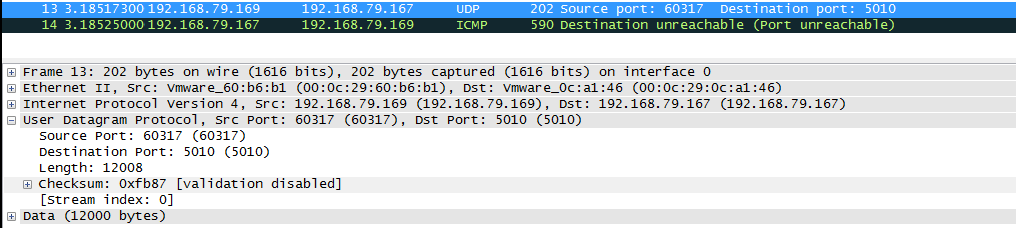


4) À la lumière de votre analyse, que fait le client? Selon vous, combien d’itérations le client a-t-il faites pour envoyer ces données? (0.5 point)



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)



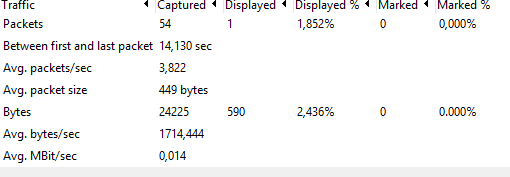
UDP pas de SYN pour la synchro.

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

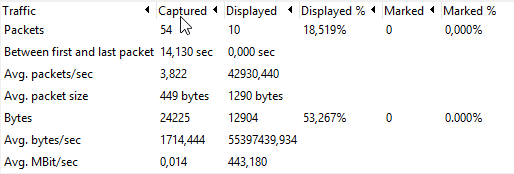


1. Combien de paquets et d’octets contenant des données ont été envoyés par le client vers le serveur? Par le serveur vers le client? Montrer où vous avez trouvé cette information. (0.5 point)

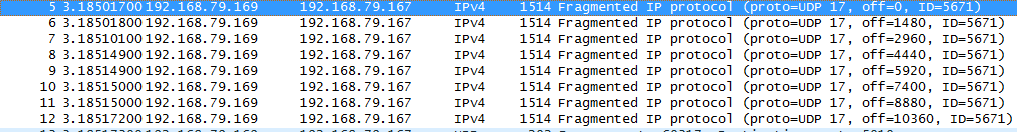
SERVEUR A CLIENT



CLIENT A SERVEUR



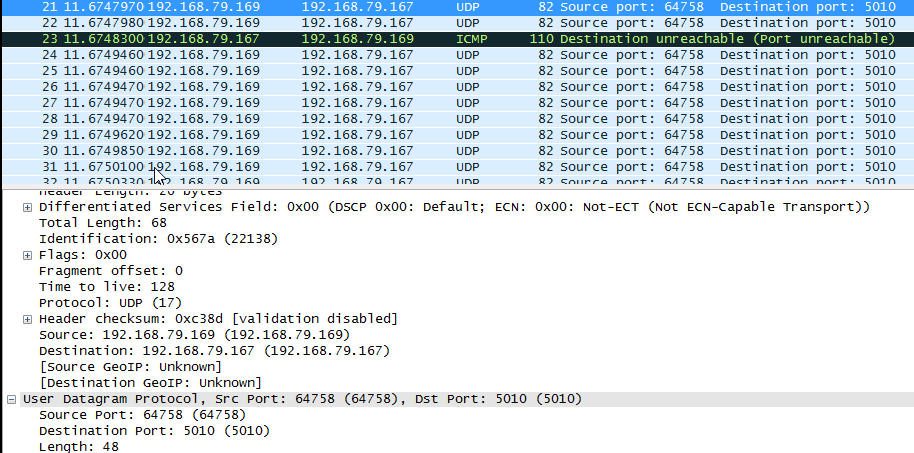
1. À la lumière de votre analyse, que fait le client? Selon vous, combien d’itérations le client a-t-il faites pour envoyer ces données? (0.5 point)



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)



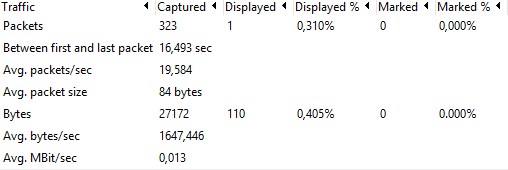
Pas de sync

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

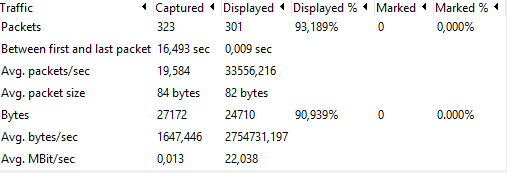


1. Combien de paquets et d’octets contenant des données ont été envoyés par le client vers le serveur? Par le serveur vers le client? Montrer où vous avez trouvé cette information. (0.5 point)

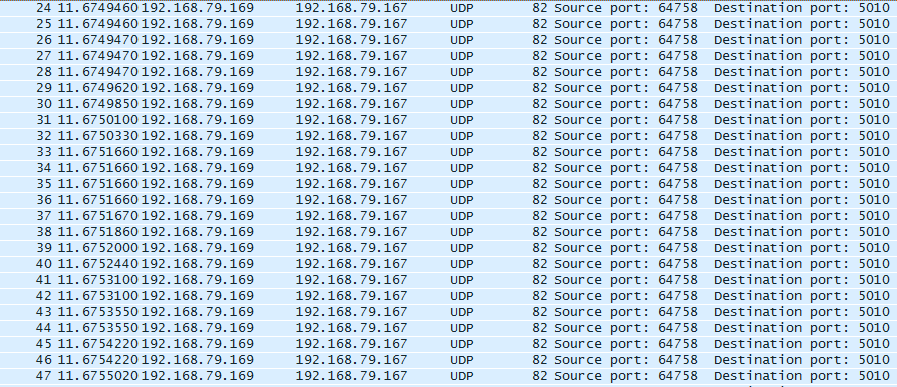
SERVEUR A CLIENT



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.