TP3 TCP et Wireshark

Pour ce TP, vous chargerez le fichier de capture *Big_capture.pcapng*.

Ce fichier comprend environ 4 minutes de capture, et, entre autres le chargement d'un gros fichier, téléchargé sur un site distant.

Dans un premier temps, vous indiquerez combien de connexions TCP sont initiées dans les 10 premières seconde de la capture. Pour chacune de ces connexions, vous essayerez de trouver quels sont les protagonistes de la connexion, et quel est le type, et potentiellement, le nom, de serveur (distant ou pas).

Pour ce faire, dans Wireshark, les filtres de type *tcp.flags.syn==1*, *tcp.flags.fin==1*, peuvent être utile, de même que le menu « Analyze → Follow → TCP Stream » et le menu « Statistics → TCP Streams »

En particulier,

- trouvez le nom de ma « chaîne hi-fi », et le type de protocole de niveau applicatif utilisé
- le nom du site sur lequel j'ai téléchargé le gros fichier
- la taille du fichier (approximative, indiquez pourquoi vous ne pouvez pas donner la taille exacte du fichier)
- quel est le type de sécurité utilisé, numéro de port utilisé (vérifiez sur gogol)
- affichez le débit « throughput – Goodput ». Concentrez vous sur les endroits où les deux sont significativement différents, indiquez ce qui c'est passé.
- Sur ces courbes indiquez clairement ce qui s'est passé au niveau du protocole TCP
- Sur base des captures, quelles sont les tailles d'un PDU ?
- Quel est l'effet des Dup Acks sur la mise à jour des tailles de fenêtre (ou l'inverse)

Quelques problèmes

P1

Soit un client A qui initie une session Telnet avec le serveur S. Au même moment, le client B initie une session Telnet avec le serveur S. Donner les ports (potentiels) de source et de destination pour :

1. les segments envoyés de A à S
2. de B à S
3. de S à A
4. de S à B
5. Si A et B sont différents, est-il possible que le numéro de port source de A→S soit le même que de B→S ?
6. Et si A et B sont les mêmes machines ?