# Compte rendu TP 3 SR73

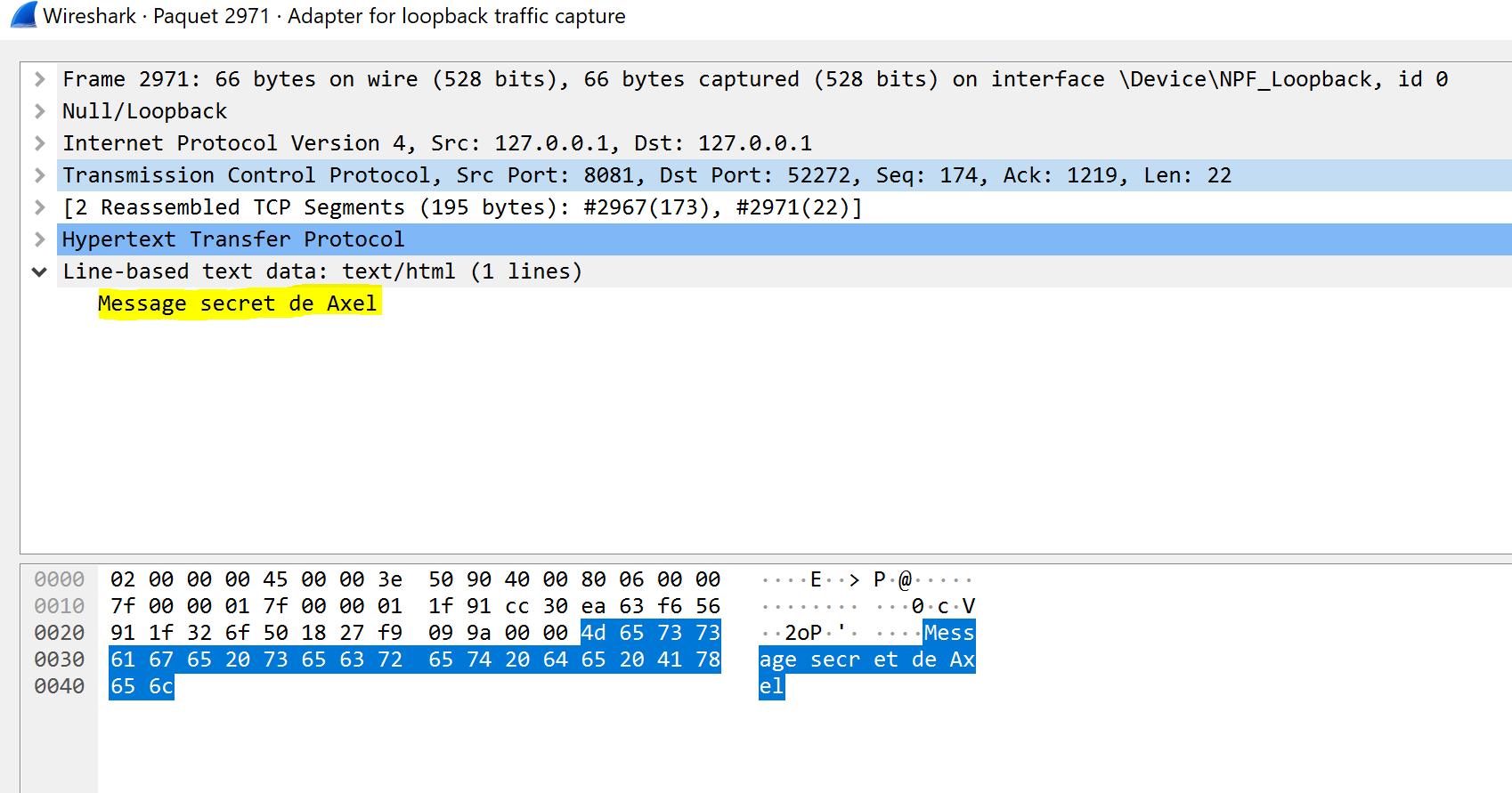
# PARTIE 1

On peut changer le message secret dans « run\_server.py ». La variable à modifier est SECRET\_MESSAGE.

Une image contenant texte

Description générée automatiquement

Ensuite dans wireshark, on retrouve notre clé secrète dans le paquet html en réponse 200 OK en format text/html



# PARTIE 2

Mot de passe : « privatePassword »

Données intégrées : CA\_CONFIGURATION = Configuration("FR", "Territoire de Belfort", "Sevenans", "UTBM\_CA", "localhost")

Une image contenant texte, plaque, capture d’écran, document

Description générée automatiquement

# PARTIE 3

Mot de passe : « publicPassword »

Une image contenant texte

Description générée automatiquement

# PARTIE 4

Après avoir généré les certificats et les avoir intégrés au lancement du programme :

Une image contenant texte

Description générée automatiquement

Lorsqu’on attaque <https://localhost:8081> on voit qu’il y a une alerte sur la sécurité de la page web. C’est tout simplement parce que le certificat utilisé n’est pas connu par le navigateur. Le navigateur considère qu’il y potentiellement un risque. Néanmoins, on peut accepter de prendre les risques et y accéder.

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

Pour remédier à ce problème, une solution serait d’installer le certificat sur le navigateur. Nous n’aurions alors plus l’erreur.

# PARTIE 5

On peut augmenter la taille de la clé RSA dans la fonction « generate\_private\_key ». Nous avons passé l’élément « key\_size=2048 » à 4096.

Une image contenant texte

Description générée automatiquement

Le nouveau certificat :

Une image contenant texte

Description générée automatiquement