Extraction des certificats à partir d’une trace wireshark.

• Lors de l’utilisation du protocole SSL/TLS, l’échange de certificat se fait de façon non chiffrée.

Il est donc possible d’extraire le certificat à partir d’une trace de trafic.

• Le projet consiste à :

-> Programmer un script python qui permet d’extraire les certificats d’une trace.

-> Pour chaque certificat, il faut lui associer l’adresse IP du serveur ayant transmis ce certificat.

-> Lorsque possible, il faut associer le nom de domaine associé à cette IP (i.e., si une requête DNS se trouve dans la trace ou si le client fait explicitement la demande avec SNI).

Objectif Initial :

1. Programmer un script python/scapy qui lira les traces Wiresharks (.pcap).

2. Par la suite le script repèrera les certificats et l’extraire (faire un dissecteur dans scapy) voir scapy SSL/TLS

3. Pour chaque certificat, le scripte fera l'association IP/Certificat, si un nom de domaine est associé à une adresse IP il fera l'association IP/Certificat/Nom de domaine

-> 2 option soit en DNS ou SSL (champ SNI).

4. Une fois ces association faite le script enregistrera le tout dans un nouveau document pour lecture ultérieur.