README

- ZHANG zhile 21201131 Groupe5
- ZHANG jiawen 21117173 Groupe5

Notre structure de code est très simple, il n'y a que deux fichiers de programmation au total, tous deux écrits en python.

L'un s'appelle **analyse.py**, qui est spécialement utilisé pour analyser ces protocoles, ce que nous appelons communément le décodage. Il contient quatre fonctions principales(analyserMAC, analyserIP, analyseTCP, analyseHTTP). Selon les signatures des fonctions, nous pouvons savoir chaque fonction elle est dédiée à l'analyse de quel protocole, et chaque fonction renverra les informations dont nous avons besoin sur ce protocole.

L'autre fichier s'appelle **graph.py**. Bien qu'il ne s'agisse que d'une interface visuelle, ce fichier contient beaucoup de travail. Premièrement, nous devons convertir un fichier qui n'est pas en codage brut (*tcp.txt*) en codage brut (*trame. txt*), puis on filtre toutes les trames qui sont des tcp et http trames, et on filtre les trames tcp et http envoyées depuis l'adresse ip locale, de même, nous attribuons également différentes couleurs de fond à la trame des différents ports à afficher, tout comme dans wireshark. Puis on appelle chacune de ces tcp et http trames à la fonction en **analyse.py** pour obtenir les informations, et enfin, une fenêtre de visualisation est créée avec des informations (et des flèches) pour chaque trame, aussi mettre en place la fonction de filtrage les protocoles et filtrage les adresses ip et enregistrer les résultats d'analyse dans *trame_analyse.txt*