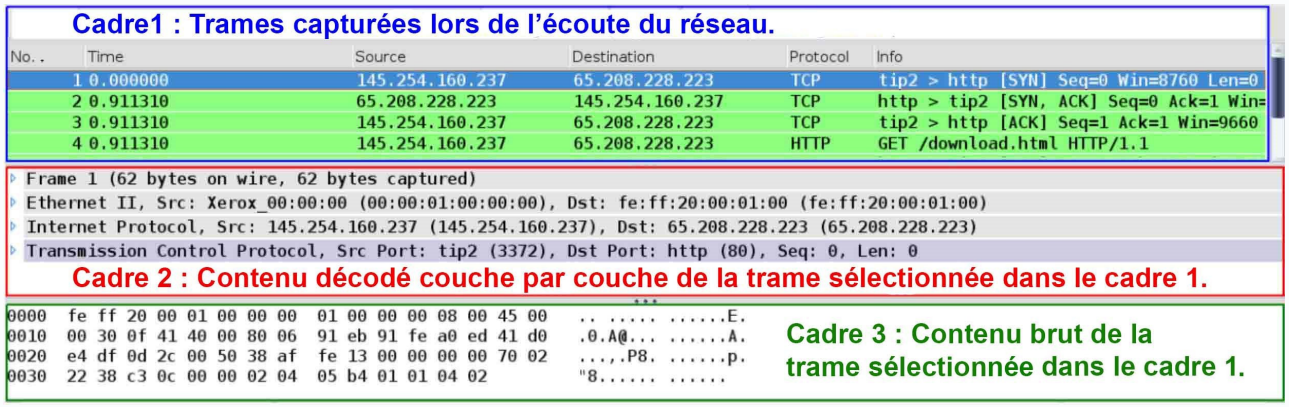
ARSE06-ACT1 UTILISATION DE WIRESHARK

Wireshark est un logiciel de sniffing, c'est-à-dire un analyseur qui permet d'écouter le réseau auquel est connecté l'ordinateur. Il enregistre tous les transferts de données (toutes les trames) du réseau. Ce logiciel de surveillance est un outil puissant et il est interdit de l'utiliser pour surveiller un réseau sans autorisation. Pour cette raison, seul un précédent enregistrement sera utilisé, mais vous pourrez le tester intégralement chez vous, sur votre propre réseau.

Vous pouvez télécharger Wireshark à l'adresse suivante : `https://www.wireshark.org/download.html`.

L'interface de Wireshark

- La partie supérieure affiche la liste des paquets capturés, avec des informations telles que le numéro du paquet, l'heure de capture, l'adresse source, l'adresse de destination, le protocole utilisé et une brève description du contenu du paquet.
- La partie centrale affiche les détails du paquet sélectionné dans la partie supérieure. Elle montre les différentes couches du modèle TCP/IP et les informations spécifiques à chaque couche.
- La partie inférieure affiche les données brutes du paquet sélectionné, souvent en format hexadécimal et ASCII.



Exercice 1 : Analyse d'une capture Wireshark

1. Récupérer le fichier de capture act11.pcap et l'ouvrir avec le logiciel Wireshark.
2. À quelle heure a eu lieu cette connexion ? Pour cela explorer une des trames (Frame).
3. Quels sont les différents protocoles utilisés et à quelle couche du modèle TCP/IP simplifié appartiennent-ils ?
4. Dans la suite nous étudierons la trame 3.
5. Quelle est la taille (en octets) de cette trame ?
6. Faire un clic droit dans le cadre 3 et choisir l'affichage hexadécimal.
7. Qu'indiquent les six premiers octets de cette trame ainsi que les six octets suivants ?
8. Quel est le constructeur de la carte réseau du destinataire ?
9. À quelle couche (Accès Réseau, Internet, Transport ou Application) appartiennent les informations à partir du 15ième octet ?
10. À quelle couche (Accès Réseau, Internet, Transport ou Application) appartiennent les informations à partir du 35ième octet ?
11. Trouver l'adresse logique IP à laquelle l'ordinateur essaie de se connecter.
12. Copier cette adresse IP dans la barre d'adresse d'un navigateur pour trouver à quel site l'utilisateur essayait de se connecter.
13. Maintenant, étudions ce qui se passe dans les deux premières trames.
14. Décrire ce qui se passe ? Que réalise le protocole ARP ?