

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.

Cadre1 : Trames capturées lors de l'écoute du réseau.

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	145.254.160.237	65.208.228.223	TCP	tip2 > http [SYN] Seq=0 Win=8760 Len=0
2	0.911310	65.208.228.223	145.254.160.237	TCP	http > tip2 [SYN, ACK] Seq=0 Ack=1 Win=
3	0.911310	145.254.160.237	65.208.228.223	TCP	tip2 > http [ACK] Seq=1 Ack=1 Win=9660
4	0.911310	145.254.160.237	65.208.228.223	HTTP	GET /download.html HTTP/1.1

```

▶ Frame 1 (62 bytes on wire, 62 bytes captured)
▶ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
▶ Internet Protocol, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
▶ Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 0, Len: 0

```

Cadre 2 : Contenu décodé couche par couche de la trame sélectionnée dans le cadre 1.

```

0000  fe ff 20 00 01 00 00 00 01 00 00 00 08 00 45 00  . . . . .E.
0010  00 30 0f 41 40 00 00 06 91 eb 91 fe a0 ed 41 d0  .0.A@... .A.
0020  e4 df 0d 2c 00 50 38 af fe 13 00 00 00 70 02  . . . .P8. . . .p.
0030  22 38 c3 0c 00 00 02 04 05 b4 01 01 04 02      "8. . . . .

```

Cadre 3 : Contenu brut de la trame sélectionnée dans le cadre 1.

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?