Fiche Exercices pratiques 12 – Dissection d'une capture réseau

Laurent Signac – CC-BY-SA – 08-06-21 1407 7fcb9ae0f5d6e49edaeb

La capture réseau `requete_http_simple.pcap` (téléchargement[1]) a été obtenue lors de l'affichage d'une page Web dans un navigateur.

Chargez cette capture dans Wireshark et identifiez les différents éléments.

Lors de la consultation de la page Web, plusieurs actions, transparentes pour l'utilisateur ont été réalisées par la machine cliente.

Voici la liste des opérations que la machine observée a dû effectuer (dans le désordre)

- réception de la réponse du DNS : quelle est l'IP recherchée ?
- recherche de l'adresse MAC de 172.16.111.252
- calcul d'une route vers 193.55.138.46
- communication selon le protocole HTTP
- connexion TCP sur le port 80 de la machine 194.254.43.242. Quelles est l'adresse MAC de destination ?
- envoi d'une requête DNS. Recherchez les adresses IP et MAC, ainsi que le nom de la machine recherchée.
- recherche d'une route vers 194.254.43.242.

Remettez cette liste dans l'ordre. Attention, certains éléments de la liste ne correspondent pas forcément à des trames visibles dans la communication. Répondez aussi aux questions indiquées dans cette liste.

Dressez la liste des machines mises en jeu : noms, IP, MAC, pouvez-vous donner des indications sur les masques de sous-réseaux de certaines machines ?

[1] https://deptinfo-ensip.univ-poitiers.fr/pygit/g/pub/reseaux/FILES/requete_http_simple.pcap