TP 11: Wireshark Lab sur les applications:

Basé sur : Computer Networks, A Top-down Approach, 8th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2020.

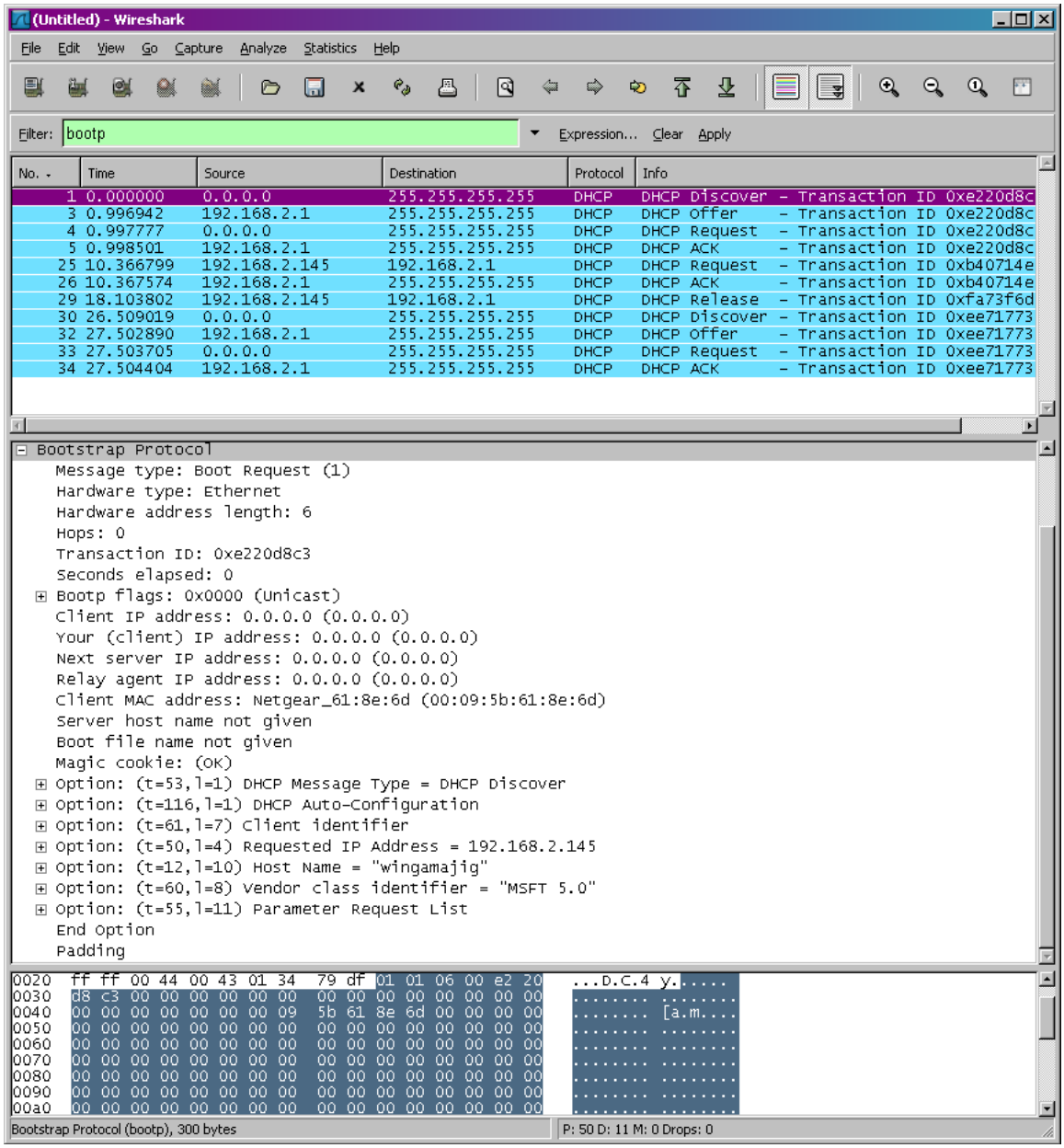
DHCP

Ce TP sur DHCP suppose que vous pouvez activer DHCP … les commandes données ici supposent un PC-Windows.

Pour observer le fonctionnement de DHCP, vous allez effectuer les opérations suivantes:

1. Effectuez un "*ipconfig /release*" dans le fenêtre de commande. Cette commande relâche votre adresse IP, qui devrait devenir 0.0.0.0
2. Lancez Wireshark
3. Effectuez un "*ipconfig /renew*". Ca demandera une nouvelle adresse IP à votre serveur DHCP
4. Dès que une adresse a été allouée (verifiez avec "*ipconfig*"), effectuez un deuxième "*ipconfig /renew*".
5. Effectuez "*ipconfig/release*"
6. Réeffectuez "*ipconfig /renew*"
7. Stoppez Wireshark.

Filtrez les paquets DHCP, en entrant “dhcp” comme filtre. DHCP utilise les ports, 67 et 68. Sur d’anciennes versions de Wireshark, ça pourrait être le filtre « bootp »
Vous devriez obtenir un trace du type :



Faites une capture d'écran et répondez aux questions suivantes :

1. DHCP utilise t'il UDP ou TCP ?
2. Faites un diagramme illustrant la séquence des quatre premiers paquets Discover/Offer/Request/ACK DHCP échangés entre client et server. Pour chaque paquet, indiquez la source (IP/port) et la destination. Ces ports seront-ils les mêmes si vous réeffectuer une trace ?
3. Quelle est l'adresse Ethernet de votre hôte ?
4. Quelle valeurs, dans le message DHCP discover, le différencient du message DHCP request ?
5. Quelle est la valeur du Transaction-ID dans chacun des 4 premiers paquets (Discover/Offer/Request/ACK) DHCP messages? Et dans le deuxième groupe ? Quelle est l'utilité du Transaction-ID?
6. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.
7. Quelle est l'adresse de votre serveur DHCP ?
8. Quelle adresse IP vous est proposée dans le message DHCP Offer ? Quels sont les messages qui contiennent cette adresse IP.
9. Dans la capture d'écrant donnée en exemple, il n'y a pas de relais entre l'hôte et le serveur DHCP. Quelles valeurs indiquent l'absence de relais ? Si c'est le cas chez vous, quelle est l'adresse du relais ?
10. Quel est l'objectif du masque dans le message DHCP offer.
11. Quel est l'objectif du « lease time ». Combien vaut-il dans votre cas ?
12. Quel est l'objectif du message DHCP release? Le serveur DHCP émet-il un accusé de réception au DHCP request du client ? Que se passerait-il si le DHCP release était perdu ?
13. Désactivez le filtre *bootp*. Y a-t-il eu des échanges ARP pendant l'échange DHCP. Si oui, pourquoi ?

DNS

NSLOOKUP

Dans ce TP, nous utiliserons largement l'outil *nslookup*, qui est actuellement disponible sur la plupart des plateformes Linux / Unix et Microsoft, en ligne de commande.

Dans son fonctionnement le plus basique, l'outil nslookup permet à l'hôte exécutant l'outil d'interroger un serveur DNS spécifié pour un enregistrement DNS. Le serveur DNS interrogé peut être un serveur DNS racine, un serveur DNS de domaine de premier niveau, un serveur DNS faisant autorité ou un serveur DNS intermédiaire. Pour accomplir cette tâche, nslookup envoie une requête DNS au serveur DNS spécifié, reçoit une réponse DNS de ce même serveur DNS et affiche le résultat.

Par exemple :

```
nslookup www.unice.fr
```

la réponse de cette commande fournit deux informations: (1) le nom et l'adresse IP du serveur DNS qui fournit la réponse; et (2) la réponse elle-même, qui est le nom d'hôte et l'adresse IP de www.mit.edu. Bien que la réponse provienne du serveur DNS local de l'Université polytechnique, il est fort possible que ce serveur DNS local ait contacté de manière itérative plusieurs autres serveurs DNS pour obtenir la réponse.

La commande

```
nslookup –type=NS unice.fr
```

demandant spécifiquement les DNS liés à unice.fr.

A noter que nslookup peut également être exécuté en mode interactif (il suffit d'exécuter nslookup sans argument, et vous aurez un « prompt », et il faut alors entrer des commandes).

On notera également que sur Windows, les commandes

```
ipconfig /displaydns
ipconfig /flushdns
```

permettent d'afficher les DNS et également de les effacer de la configuration.

Explorer DNS avec Wireshark

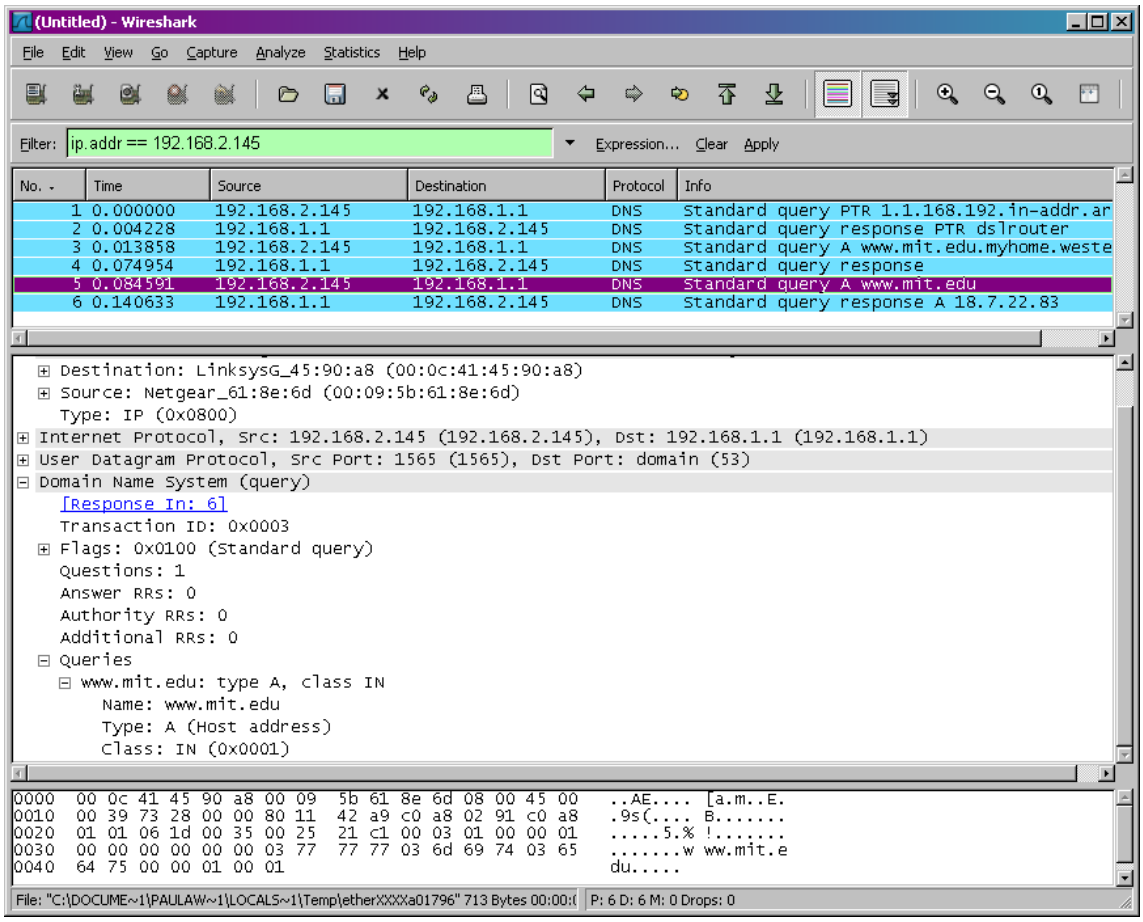
- Utilisez ipconfig pour vider le cache DNS de votre hôte.
- Ouvrez votre navigateur et videz le cache de votre navigateur.
- Ouvrez Wireshark et entrez «ip.addr == your_IP_address» dans le filtre, où vous obtenez votre_IP_address avec ipconfig. Ce filtre supprime tous les paquets qui ne proviennent ni ne sont destinés à votre hôte.
- Démarrez la capture de paquets dans Wireshark.
- Avec votre navigateur, visitez la page Web: http://www.ietf.org
- Arrêtez la capture de paquets.

- Recherchez la requête DNS et les messages de réponse. Sont-ils envoyés via UDP ou TCP?
- Quel est le port de destination du message de requête DNS? Quel est le port source du message de réponse DNS?
- À quelle adresse IP le message de requête DNS est-il envoyé? Utilisez ipconfig pour déterminer l'adresse IP de votre serveur DNS local. Ces deux adresses IP sont-elles identiques?
- Examinez le message de requête DNS. De quel «type» de requête DNS s'agit-il? Le message de requête contient-il des «réponses»?
- Examinez le message de réponse DNS. Combien de «réponses» sont fournies? Que contient chacune de ces réponses?
- Considérez le paquet TCP SYN envoyé par votre hôte. L'adresse IP de destination du paquet SYN correspond-elle à l'une des adresses IP fournies dans le message de réponse DNS?
- Cette page Web contient des images. Avant de récupérer chaque image, votre hôte émet-il de nouvelles requêtes DNS?

Jouons maintenant avec nslookup.

• Démarrez la capture de paquets.
• Faites un nslookup sur www.mit.edu
• Arrêtez la capture de paquets.

Vous devriez obtenir une trace qui ressemble à ce qui suit:



Nous voyons dans la capture d'écran ci-dessus que nslookup a en fait envoyé trois requêtes DNS et reçu trois réponses DNS. Dans le cadre de cette tâche, en répondant aux questions suivantes, ignorez les deux premiers ensembles de requêtes / réponses, car ils sont spécifiques à nslookup et ne sont normalement pas générés par des applications Internet standard. Vous devriez plutôt vous concentrer sur les derniers messages de requête et de réponse.

- Quel est le port de destination du message de requête DNS? Quel est le port source du message de réponse DNS?
- À quelle adresse IP le message de requête DNS est-il envoyé? Est-ce l'adresse IP de votre serveur DNS local par défaut?
- Examinez le message de requête DNS. De quel «type» de requête DNS s'agit-il? Le message de requête contient-il des «réponses»?
- Examinez le message de réponse DNS. Combien de «réponses» sont fournies? Que contient chacune de ces réponses?
- Fournissez une capture d'écran.

Maintenant, répétez l'expérience précédente, mais émettez plutôt la commande:

nslookup –type = NS mit.edu
remplacer par dig nslookup www.aiit.or.kr bitsy.mit.edu

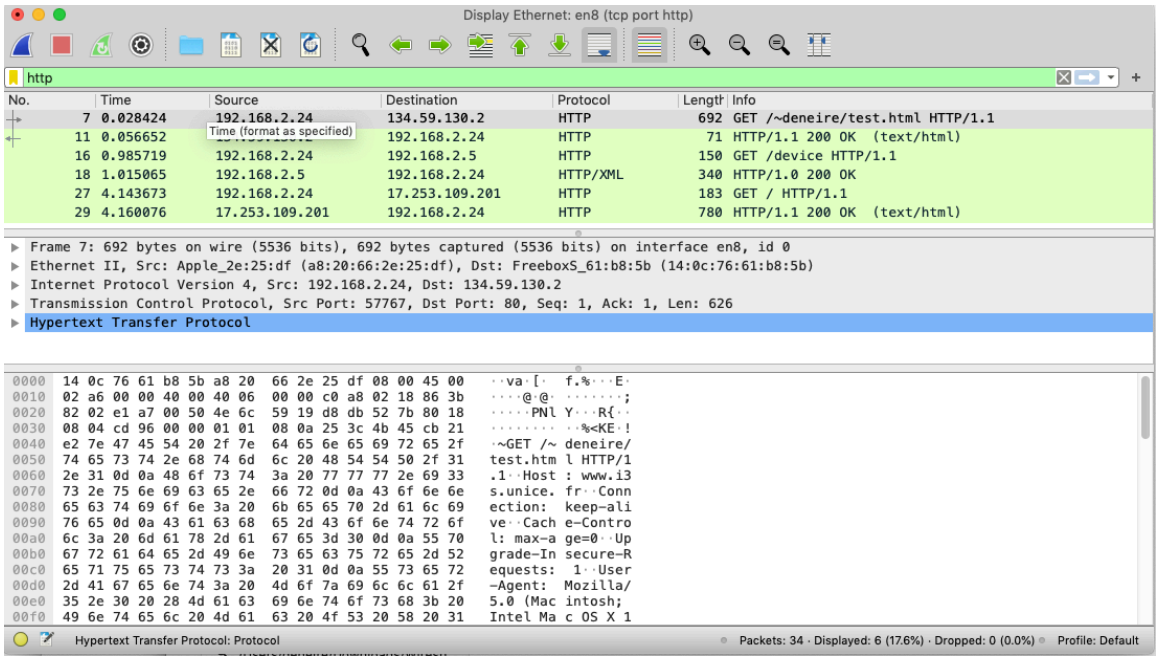
HTTP

1. L'interaction de base HTTP GET / réponse

Commençons notre exploration de HTTP en téléchargeant un fichier HTML très simple, très court et ne contenant aucun objet incorporé. Procédez comme suit:

1. Démarrez votre navigateur Web.
2. Démarrez Wireshark, Entrez «tcp port http» dans la fenêtre de spécification du filtre d'affichage.
3. Attendez un peu plus d'une minute puis commencez la capture de paquets Wireshark.
4. Entrez ce qui suit dans votre navigateur : http://www.i3s.unice.fr/~deneire/test.html vous devriez avoir un résultat simple …
5. Arrêtez la capture de paquets Wireshark.

Votre fenêtre Wireshark doit ressembler à la fenêtre illustrée



L'exemple de la figure 1 montre dans la fenêtre de liste des paquets que deux messages HTTP ont été capturés: le message GET et le message de réponse du serveur à votre navigateur. La fenêtre du contenu des paquets affiche les détails du message sélectionné (dans ce cas, le message HTTP OK).

En examinant les informations contenues dans HTTP GET et les messages de réponse, répondez aux questions suivantes. Lorsque vous répondez aux questions suivantes, vous devez imprimer les messages GET et de

1. Votre navigateur exécute-t-il la version 1.0 ou 1.1 de HTTP? Quelle version de HTTP le serveur exécute-t-il?
2. Quelles langues (le cas échéant) votre navigateur indique-t-il qu'il peut accepter le serveur?
3. Quelle est l'adresse IP de votre ordinateur? Du serveur?
4. Quel est le code d'état renvoyé par le serveur à votre navigateur?
5. Quand le fichier HTML que vous récupérez a-t-il été modifié pour la dernière fois sur le serveur?
6. Combien d'octets de contenu sont renvoyés à votre navigateur?
7. En inspectant les données brutes dans la fenêtre de contenu des paquets, voyez-vous des en-têtes dans les données qui ne sont pas affichés dans la fenêtre de liste des paquets? Si oui, nommez-en un.