Travaux pratiques 11.5.6 : Étude de cas finale : Analyse de datagrammes à l'aide de Wireshark

Objectifs pédagogiques

À l'issue de cet exercice, les participants seront en mesure de montrer comment effectuer les opérations suivantes :

- Construire un segment TCP et décrire les champs du segment
- Construire un paquet IP et décrire les champs du paquet
- Construire une trame Ethernet II et décrire les champs de la trame
- Décrire le contenu d'une REQUÊTE ARP et d'une RÉPONSE ARP

Contexte

Ces travaux pratiques nécessitent deux fichiers de paquets capturés et Wireshark, analyseur de protocole réseau. Téléchargez les fichiers suivants sur le serveur Eagle, puis installez Wireshark sur votre ordinateur, si ce n'est déjà fait :

- eagle1_web_client.pcap (décrit)
- eagle1_web_server.pcap (référence uniquement) ;
- wireshark.exe.

Scénario

Cet exercice décrit la séquence de datagrammes créés et transmis au sein d'un réseau entre un client Web (PC_client) et un serveur Web (eagle1.example.com). C'est en maîtrisant l'insertion séquentielle de paquets sur le réseau que les participants pourront logiquement traiter les pannes. Pour plus de concision et de clarté, les interférences des paquets réseau ont été omises dans les captures. Avant d'exécuter un analyseur de protocole réseau sur un réseau qui appartient à un tiers, veillez à vous procurer une autorisation écrite.

La figure 1 illustre la topologie de ces travaux pratiques.

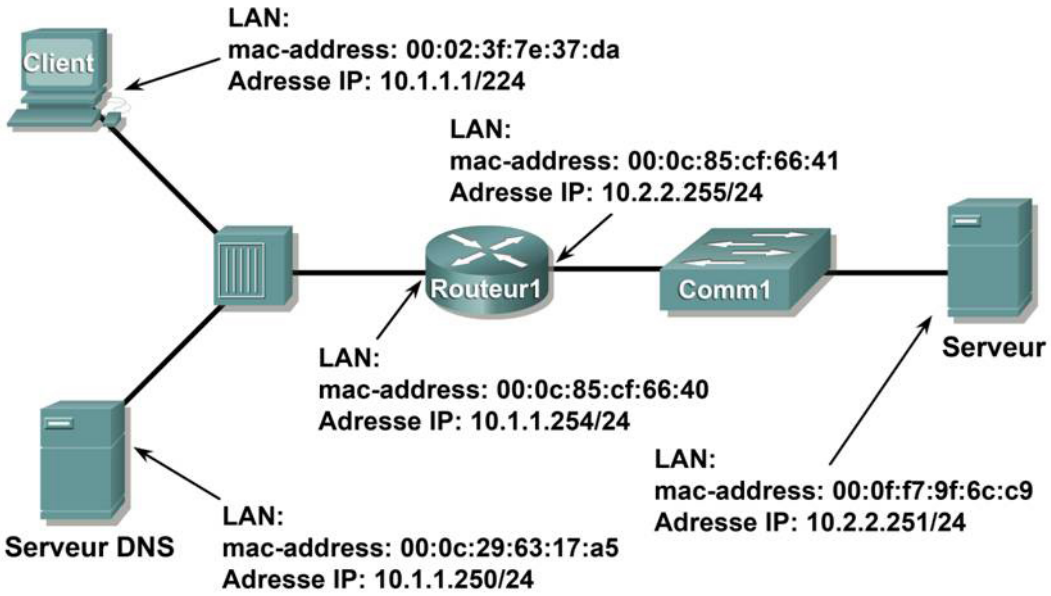

Figure 1. Topologie de réseau

Les paramètres de configuration IP et le contenu de la mémoire cache ARP sont affichés à l'aide des outils de ligne de commande Microsoft ®. Reportez-vous à la figure 2.

```
C: > ipconfig / all
Windows IP Configuration
Ethernet adapter Local Area Connection:
     Connection-specific DNS Suffix  . :
     Description . . . . . . . . . . . : Intel(R) PRO/1000 MT
                                          Network Connection
     Physical Address. . . . . . . . . : 00:02:3f:7e:37:da
     Dhcp Enabled. . . . . . . . . . . : No
     IP Address. . . . . . . . . . . . : 10.1.1.1
     Subnet Mask . . . . . . . . . . . : 255.255.255.0
     Default Gateway . . . . . . . . . : 10.1.1.254
     DNS Servers . . . . . . . . . . . : 10.1.1.250
C: > arp -a
No ARP Entries Found
C: >
```

Figure 2. État initial du réseau sur le PC Client.

Comme l'indique la figure 3, on active un client Web et on saisit l'URL eagle1.example.com. Cela permet d'établir une communication avec le serveur Web et de capturer les paquets.

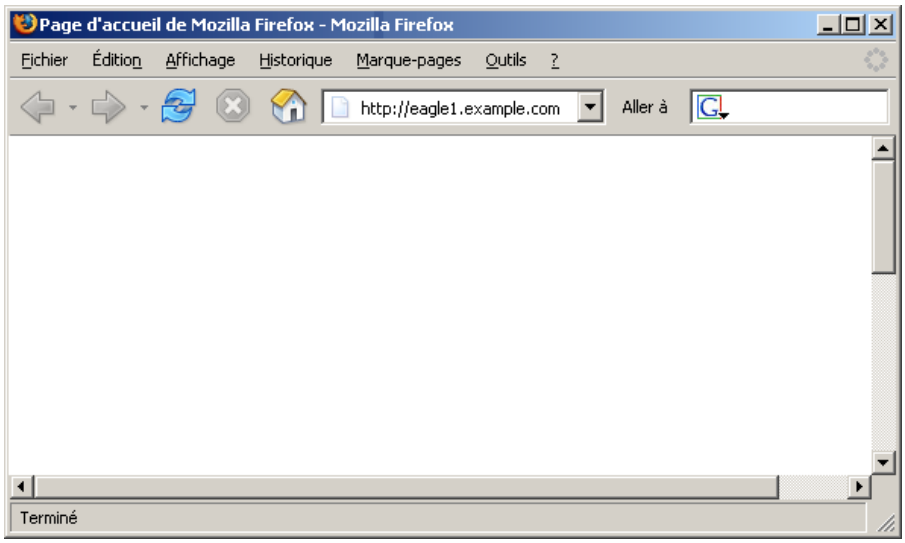

Figure 3. Navigateur Web sur le PC Client.

Tâche 1 : préparation des travaux pratiques

Étape 1 : démarrage de Wireshark sur votre ordinateur

Reportez-vous à la figure 4 pour visualiser les différences par rapport à l'affichage par défaut. Désactivez `Main toolbar`, `Filter toolbar` et `Packet Bytes`. Vérifiez que `Packet List` et `Packet Details` sont activés. Pour éviter toute traduction automatique des adresses MAC, désélectionnez `Name Resolution` pour `MAC layer` et `Transport Layer`.

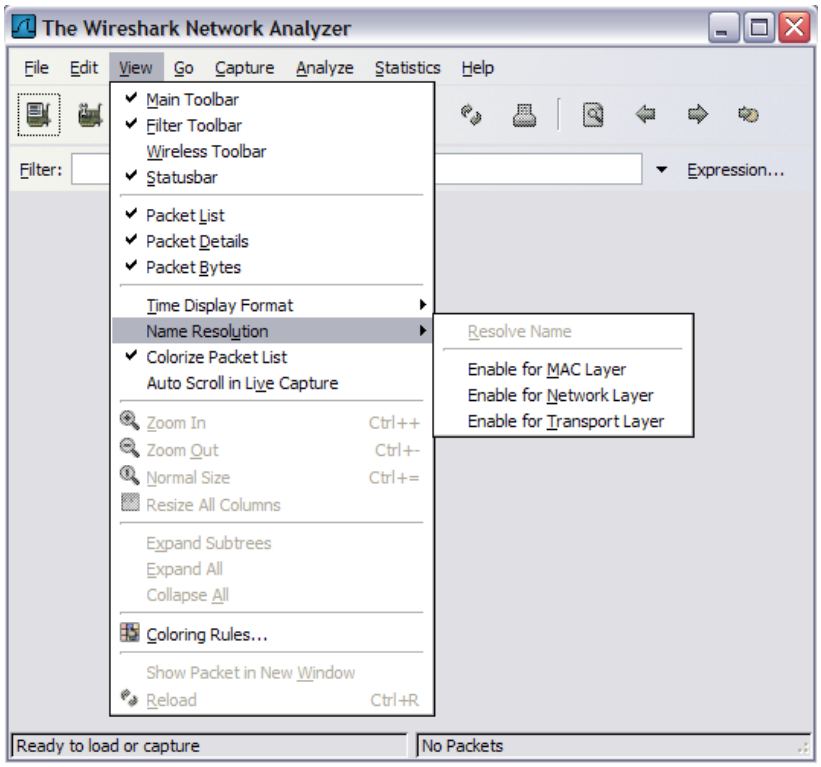

Figure 4. Modifications de l'affichage par défaut de Wireshark.

Étape 2 : importation de la capture du client Web, `eagle1_web_client.pcap`

Un écran similaire à la figure 5 apparaît. Plusieurs menus et sous-menus déroulants sont disponibles. Vous distinguez également deux fenêtres de données distinctes. La fenêtre supérieure de Wireshark répertorie tous les paquets capturés. La fenêtre du bas contient les détails des paquets. Dans la fenêtre du bas, chaque ligne contient une case à cocher ; ☒ indique la présence d'informations supplémentaires.

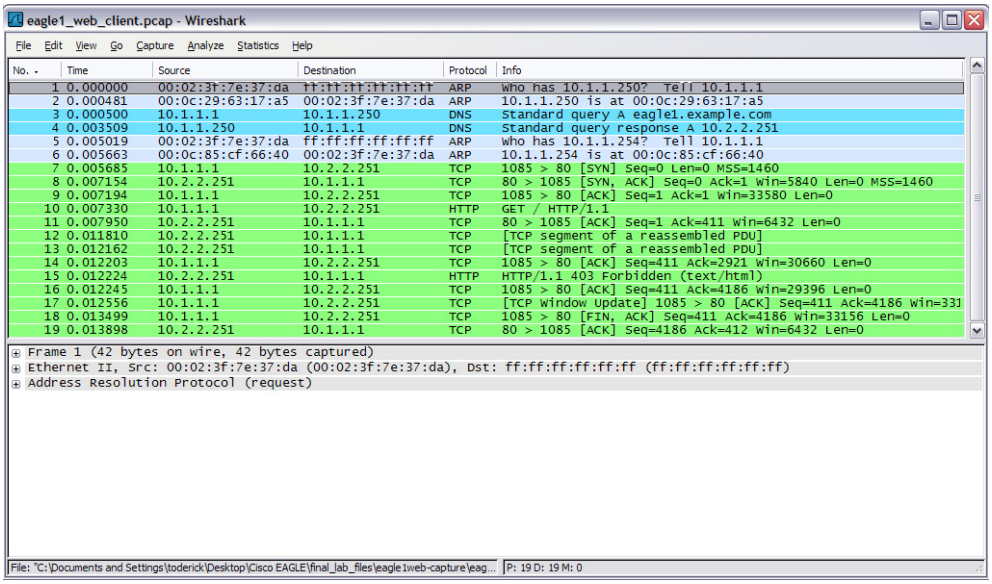

Figure 5. Wireshark après le chargement du fichier eagle1_web_client.pcap.

Tâche 2 : analyse du flux de données transitant par le réseau

Étape 1 : analyse du fonctionnement de la couche transport

Lorsque PC_Client construit le datagramme pour une connexion avec eagle1.example.com, celui-ci transite par les différentes couches réseau. À chaque couche, des informations d'en-tête importantes sont ajoutées. Cette communication ayant pour origine un client Web, le protocole de la couche transport est TCP. Observez le segment TCP illustré dans la figure 6. Le PC_Client génère une adresse de port TCP interne, 1085 dans cette conversation, et connaît l'adresse du port du serveur Web, à savoir 80. De même, le système crée un numéro de séquence en interne. Des données fournies par la couche application sont incluses. Certaines informations n'étant pas connues de PC_Client, elles doivent être obtenues via d'autres protocoles réseau.

Il n'y a pas de numéro d'accusé de réception. Pour que ce segment puisse atteindre la couche réseau, la connexion TCP en trois étapes doit être établie.

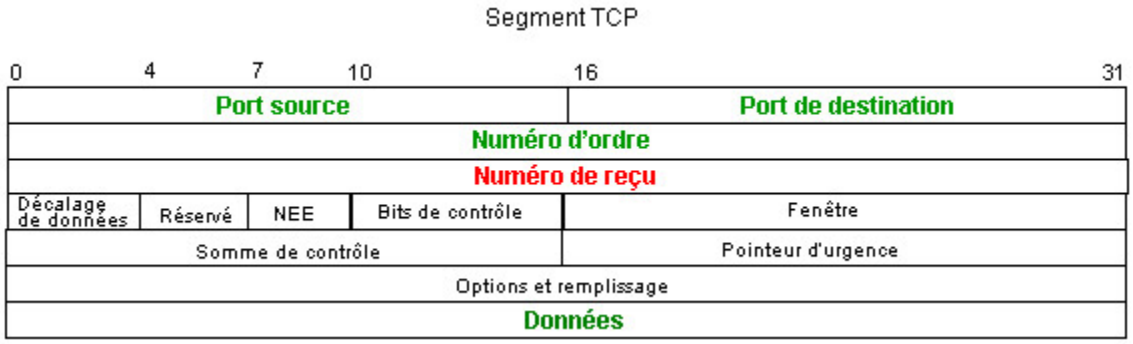

Figure 6. Champs du segment TCP.

Étape 2 : analyse du fonctionnement de la couche réseau

Au niveau de la couche réseau, le paquet IPv4 (IP) comporte plusieurs champs renseignés. Reportez-vous à la figure 7. Par exemple, la version (IPV4) pour ce paquet est connue, tout comme l'adresse IP source.

eagle1.example.com est la destination de ce paquet. L'adresse IP correspondante doit être identifiée via DNS (Domain Name Services). Tant que le datagramme de la couche supérieure n'a pas été reçu, les champs associés aux protocoles de couche supérieure sont vides.

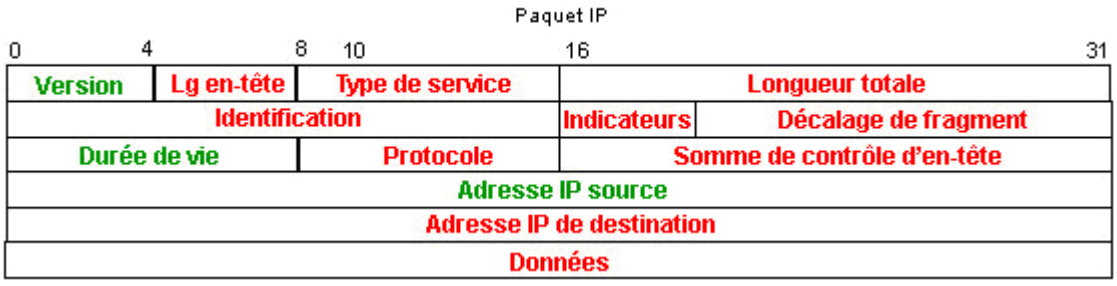

Figure 7. Champs du paquet IP.

Étape 3 : analyse du fonctionnement de la couche liaison de données

Avant d'être inséré sur le support physique, le datagramme doit être encapsulé à l'intérieur d'une trame. Reportez-vous à la figure 8. Si PC_Client connaît l'adresse MAC source, il doit en revanche trouver l'adresse MAC de destination.

Celle-ci doit être identifiée.

Structure de trame Ethernet II

Préambule	Adresse de destination	Adresse source	Type de trame	Données	CRC
8 Octets	6 Octets	6 Octets	2 Octets	46-1500 Octets	4 Octets

Figure 8. Champs d'une trame Ethernet II

Tâche 3 : analyse des paquets capturés

Étape 1 : analyse des étapes parcourues par le flux de données

Une analyse des informations manquantes s'avèrera utile pour suivre les étapes parcourues par les paquets capturés :

a. Le segment TCP ne peut pas être construit, car le champ d'accusé de réception est vide. Une connexion TCP en trois étapes doit d'abord être établie avec eagle1.example.com.

b. La connexion TCP en trois étapes n'est pas possible, car PC_Client ne connaît pas l'adresse IP de eagle1.example.com. Il faut donc que PC_Client envoie une requête DNS au serveur DNS.

c. Le serveur DNS ne peut pas être interrogé, car l'adresse MAC du serveur DNS n'est pas connue. Le protocole ARP est diffusé sur le réseau local pour identifier l'adresse MAC du serveur DNS.

d. L'adresse MAC du serveur eagle1.example.com est inconnue. Le protocole ARP est diffusé sur le réseau local pour identifier l'adresse MAC de destination du serveur eagle1.example.com.

Étape 2 : analyse de la requête ARP

Reportez-vous à l'élément n°1 de la liste de paquets Wireshark. La trame capturée est une requête ARP (Address Resolution Protocol). Le contenu de la trame Ethernet II s'affiche si vous cochez la case située dans la deuxième ligne de la fenêtre Packet Details. Il est possible d'afficher le contenu de la requête ARP en cliquant sur la ligne ARP Request dans la fenêtre Packet Details.

1. Quelle est l'adresse MAC source de la requête ARP ? _____
2. Quelle est l'adresse MAC de destination de la requête ARP ? _____
3. Quelle est l'adresse IP inconnue dans la requête ARP ? _____
4. Quel est le type de la trame Ethernet II ? _____

Étape 3 : examen de la réponse ARP

Reportez-vous à l'élément n°2 de la liste de paquets Wireshark. Le serveur DNS a envoyé une réponse ARP.

1. Quelle est l'adresse MAC source de la réponse ARP ? _____
2. Quelle est l'adresse MAC de destination de la requête ARP ? _____
3. Quel est le type de la trame Ethernet II ? _____
4. Quelle est l'adresse IP de destination dans la réponse ARP ? _____
5. Après observation du protocole ARP, que pouvez-vous déduire d'une adresse de requête ARP et d'une adresse de destination de réponse ARP ?
   _____
   _____
   _____
6. Pourquoi le serveur DNS n'a pas envoyé de requête ARP pour l'adresse MAC du PC_Client ?
   _____
   _____

Étape 4 : analyse de la requête DNS

Reportez-vous à l'élément n°3 de la liste de paquets Wireshark. PC_Client a envoyé une requête DNS au serveur. En vous aidant de la fenêtre Packet Details, répondez aux questions suivantes :

1. Quel est le type de la trame Ethernet II ? _____
2. Quel est le protocole de la couche transport, et quel est le numéro de port de destination ?
   _____

Étape 5 : analyse de la réponse à la requête DNS

Reportez-vous à l'élément n°4 de la liste de paquets Wireshark. Le serveur DNS a envoyé une réponse à PC_Client. En vous aidant de la fenêtre Packet Details, répondez aux questions suivantes :

1. Quel est le type de la trame Ethernet II ? _____
2. Quel est le protocole de la couche transport, et quel est le numéro de port de destination ?
   _____
3. Quelle est l'adresse IP du serveur eagle1.example.com ? _____
4. L'un de vos collègues, administrateur de pare-feu, vous demande s'il y a une raison de ne pas empêcher l'entrée de tous les paquets UDP sur le réseau interne. Quelle est votre réponse ?
   _____
   _____
   _____
   _____

Étape 6 : analyse de la requête ARP

Reportez-vous aux éléments n°5 et 6 de la liste de paquets Wireshark. PC_Client a envoyé une requête ARP à l'adresse IP 10.1.1.254.

1. Cette adresse IP est-elle différente de l'adresse IP du serveur eagle1.example.com ? Expliquez.
   _____
   _____

Étape 7 : analyse de la connexion TCP en trois étapes

Reportez-vous aux éléments n°7, 8 et 9 de la liste de paquets Wireshark. Ces captures décrivent la connexion TCP en trois étapes entre PC_Client et eagle1.example.com. Au départ, seul l'indicateur TCP SYN est associé au datagramme transmis par PC_Client, (numéro d'ordre 0). eagle1.example.com répond avec les indicateurs TCP ACK et SYN avec 1 accusé de réception et 0 séquence. Dans la liste de paquets, une valeur est inconnue : **MSS=1460**. Il s'agit de la taille maximale d'un segment. Lorsqu'un segment TCP est transporté sur IPv4, la valeur de MSS correspond à la taille maximale d'un datagramme IPv4 moins 40 octets. Cette valeur est envoyée au début de la connexion. C'est également à ce moment que les fenêtres dynamiques TCP sont définies.

1. Si la valeur initiale de séquence TCP du PC_Client est égale à 0, pourquoi le serveur eagle1.example a-t-il répondu avec un accusé de réception de 1 ?
   _____
   _____

2. Dans eagle1.example.com, à la ligne n°8, que signifie la valeur 0x04 d'indicateur IP ?
   _____

3. Lorsque le PC_Client termine la connexion TCP en 3 étapes (ligne n° 9 dans la fenêtre Packet List de Wireshark), quels sont les états des indicateurs TCP renvoyés à eagle1.example.com ?
   _____

Tâche 4 : analyse finale

Étape 1 : résultats de Wireshark par rapport au processus

Il a fallu neuf datagrammes transmis entre PC_Client, le serveur DNS, la passerelle et eagle1.example.com pour que PC_Client obtienne suffisamment de paramètres pour envoyer la requête initiale à eagle1.example.com. La liste de paquets Wireshark n°10 montre que PC_Client a envoyé une requête GET.

1. Indiquez le numéro de l'élément dans la fenêtre « Packet List » de Wireshark qui satisfait à chacune des entrées manquantes suivantes :

   a. Le segment TCP ne peut pas être construit, car le champ d'accusé de réception est vide. Une connexion TCP en trois étapes doit d'abord être établie avec eagle1.example.com. _____

b. La connexion TCP en trois étapes n'est pas possible, car PC_Client ne connaît pas l'adresse IP de eagle1.example.com. Il faut donc que PC_Client envoie une requête DNS au serveur DNS. _____

c. Le serveur DNS ne peut pas être interrogé, car l'adresse MAC du serveur DNS n'est pas connue. Le protocole ARP est diffusé sur le réseau local pour identifier l'adresse MAC du serveur DNS. _____

d. L'adresse MAC permettant à la passerelle d'atteindre eagle1.example.com est inconnue. Le protocole ARP est diffusé sur le réseau local pour découvrir l'adresse MAC de destination de la passerelle. _____

2. La ligne n° 11 de la fenêtre Packet List de Wireshark est un accusé de réception du serveur eagle1.example.com à la demande GET du PC_Client (ligne n° 10 de la fenêtre Packet List de Wireshark).

3. Les éléments n°12, 13 et 15 de la liste de paquets Wireshark affichent des segments TCP transmis par eagle1.example.com. Les éléments n°14 et 16 de cette liste sont des datagrammes ACK transmis par PC_Client.

4. Pour vérifier les datagrammes ACK, sélectionnez l'élément n°14 de la liste de paquets. Ensuite, faites défiler l'écran jusqu'au bas de la liste détaillée, puis développez la trame [SEQ/ACK]. À quel datagramme du serveur eagle1.example.com le datagramme ACK de la ligne n° 14 de la fenêtre Packet List de Wireshark répond-il ? _____

5. PC_Client transmet le paquet n°17 (dans la liste) à eagle1.example.com. Analysez les paramètres de la trame [analyse SEQ/ACK]. À quoi sert ce datagramme ? _____

6. Lorsque PC_Client a terminé, les indicateurs TCP ACK et FIN sont transmis et figurent dans la liste de paquets Wireshark n°18. eagle1.example.com répond avec un datagramme TCP ACK et met fin à la session TCP.

Étape 2 : utilisation du flux TCP de Wireshark

L'analyse du contenu des paquets est parfois fastidieuse et peut vous amener à faire des erreurs. Wireshark intègre une option qui construit le flux TCP dans une fenêtre distincte. Pour utiliser cette fonctionnalité, sélectionnez d'abord un datagramme TCP dans la fenêtre Packet List de Wireshark. Ensuite, sélectionnez les options de menu Wireshark Analyze | Follow TCP Stream. Une fenêtre similaire à la figure 9 s'affiche à l'écran.

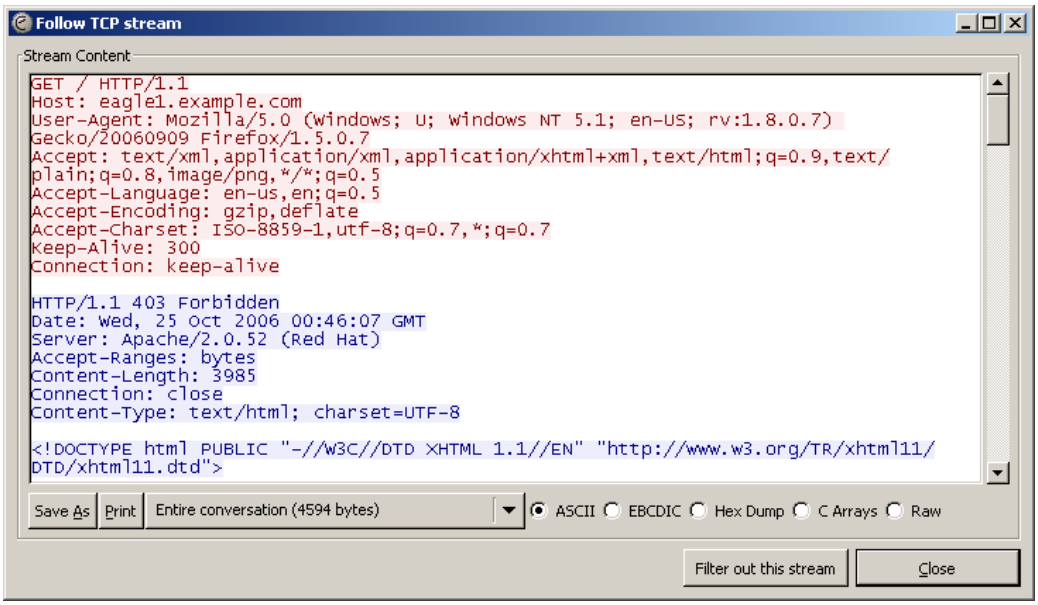

Figure 9. Aperçu de la fenêtre de flux TCP.

Tâche 5 : conclusion

L'utilisation d'un analyseur de protocole est souvent un outil d'apprentissage efficace pour assimiler les éléments importants qui constituent la communication réseau. Dès lors que l'administrateur réseau s'est familiarisé avec les protocoles de communication, ce même analyseur de protocole peut devenir un outil de dépannage efficace en cas de panne réseau. Par exemple, plusieurs raisons peuvent empêcher un navigateur Web de se connecter à un serveur Web. Un analyseur de protocole désignera les requêtes ARP et DNS infructueuses, ainsi que les paquets non reconnus.

Tâche 6 : résumé

Au cours de cet exercice, le participant a compris comment un client et un serveur Web communiquent. Les protocoles en arrière-plan, notamment DNS et ARP, sont utilisés pour combler les parties manquantes des paquets IP et des trames Ethernet. Pour qu'une session TCP puisse démarrer, la connexion TCP en 3 étapes doit créer un chemin d'accès fiable et fournir aux deux extrémités communicantes les paramètres d'en-tête TCP d'origine. Au final, la session TCP est détruite de façon ordonnée, dès lors que le client émet un indicateur TCP FIN.