

Introduction à Wireshark

Objectifs d'apprentissage

1. Savoir utiliser les fonctions de base de Wireshark : capture de paquets et analyse de protocoles.
2. Savoir dessiner un diagramme en flèches.
3. Savoir utiliser Wireshark pour analyser du trafic de réseau.

Contenu

Ce laboratoire vous permet de vous familiariser avec l'analyser de protocoles Wireshark.

1. Wireshark pour la capture et l'analyse de trafic de réseau
2. Diagramme en flèches pour illustrer le fonctionnement d'un protocole
3. Analyses de trafic réseau.

Rapport à fournir

Remplir le formulaire sur Cyberlearn.

Délai

Avant le début du prochain laboratoire.

1 Introduction

L'objectif premier du cours RXI est de vous permettre de comprendre le fonctionnement, de savoir configurer et de dépanner des réseaux informatiques.

Que se passe-t-il quand on envoie des données à travers un réseau complexe ? Vous allez voir que beaucoup de mécanismes comme DHCP, DNS, le routage, les retransmissions, etc., sont nécessaires pour rendre ça possible.

Dans ce laboratoire, vous allez apprendre à utiliser un outil précieux : Wireshark. Wireshark est un analyseur de protocoles. Il capture les données envoyées sur le réseau, les analyse et les affiche d'une manière structurée. Ainsi il nous permet de comprendre ce qui se passe sur le réseau. Wireshark est précieux pour comprendre le fonctionnement de protocoles et pour le dépannage.

2 Matériel

Lors de l'installation d'EVE-NG, Wireshark a été installé sur votre ordinateur. Nous allons l'utiliser pour ce laboratoire. Vous n'avez pas besoin de démarrer EVE-NG.

3 Exercices

Objectif 1 : Wireshark

L'objectif de cette partie est d'apprendre à effectuer une capture Wireshark simple et de documenter les résultats.

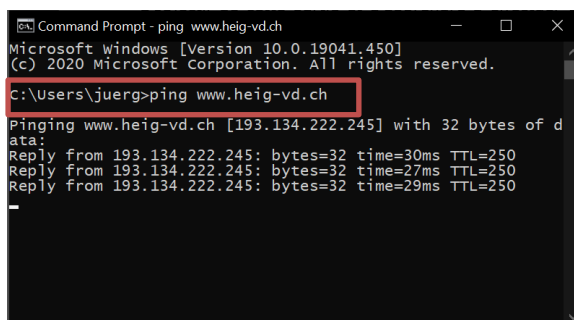
L'objectif est atteint si vous savez :

- effectuer une capture Wireshark
- utiliser un filtre d'affichage
- réaliser un diagramme en flèche.

Pour commencer à utiliser Wireshark, lisez le document « Annexe – Wireshark » et regardez la vidéo Wireshark sur Cyberlearn.

Puis, suivez les instructions :

1. Sur votre ordinateur, démarrer Wireshark.
2. Choisir l'interface de capteur qui est connecté à Internet (« Wi-Fi » ou « Local Area Connection »). Si vous êtes connecté au VPN lors de cette étape, tout le trafic est chiffré et vous ne serez pas en mesure de faire les étapes suivantes. Il vous faut alors soit vous déconnecter du VPN, soit choisir l'interface du client GlobalProtect dans Wireshark (différent selon votre OS)
3. Utiliser un filtre d'affichage « icmp ».
4. Dans un terminal de votre ordinateur (sur Windows : cmd, sur Mac : Terminal) effectuer un ping, qui envoie des messages de test au serveur Web de la HEIG-VD :



```
Command Prompt - ping www.heig-vd.ch
Microsoft Windows [Version 10.0.19041.450]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\juerg>ping www.heig-vd.ch

Pinging www.heig-vd.ch [193.134.222.245] with 32 bytes of data:
Reply from 193.134.222.245: bytes=32 time=30ms TTL=250
Reply from 193.134.222.245: bytes=32 time=27ms TTL=250
Reply from 193.134.222.245: bytes=32 time=29ms TTL=250


```

5. Analyser les paquets capturés et complétez le diagramme en flèches ci-dessous (dessiner à la main, ne fait pas partie des éléments à rendre sur Cyberlearn).

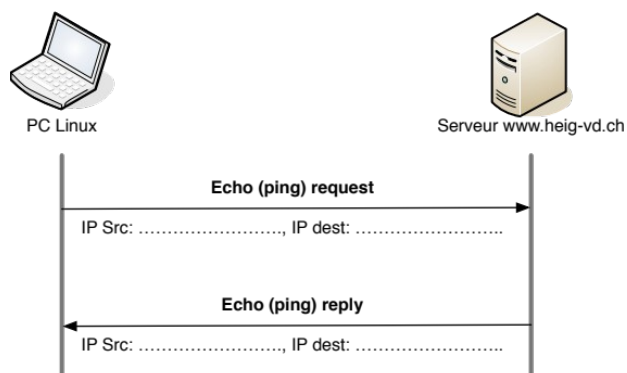


Diagramme en flèches

Les diagrammes en flèches montrent de manière claire les paquets échangés entre différents nœuds. Ils permettent ainsi d'illustrer le fonctionnement d'un protocole.

Dans cet exercice, vous devez dessiner un diagramme en flèches selon une capture Wireshark.

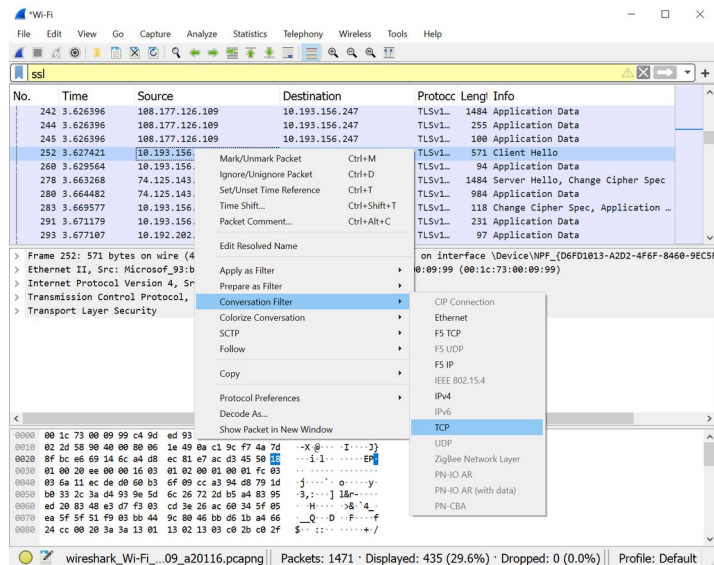
Vous pouvez utiliser par exemple les logiciels suivants pour dessiner un diagramme en flèches :

- Microsoft Visio (Windows)
- Omnigraffle (Mac)
- Microsoft Powerpoint
- OpenOffice/LibreOffice Drawing
- Draw.io
- Dia (open source, multi-plateforme, <http://projects.gnome.org/dia/>)

Suivez les instructions suivantes :

1. Lancer une nouvelle capture Wireshark.
2. Utiliser un filtre d'affichage « ssl »¹.
3. Pendant la capture Wireshark, connectez-vous au site <https://www.gmail.com> (https, donc crypté).
4. Utiliser la fonction de recherche de chaînes de caractères avec Ctrl-F, choisir le type « String » et chercher un paquet de type « Client Hello ».
5. Avec le bouton droit sur ce paquet, choisir « *Conversation filter* » -> « TCP ».

¹ SSL est un protocole de sécurité qui permet de crypter des connexions. Une connexion HTTP transmet les informations en clair, une connexion HTTPS chiffre les données.



6. Dessiner un diagramme en flèches des 6 paquets (3 paquets TCP + 3 paquets TLS) qui illustrent la négociation TLS (TLS Handshake) . Indiquer les informations suivantes :
 - o Adresses IP source et destination
 - o Type du paquet (par exemple « Client Hello »)
 - o L'instant d'envoi, en secondes (temps affiché par Wirkeshawk)
7. Sauvegarder le diagramme en format PDF comme élément à rendre sur Cyberlearn.



Puis complétez le formulaire Cyberlearn.

Objectif 2 : trouver l'image cachée

L'objectif de cette partie est d'apprendre à utiliser Wireshark pour analyser le trafic réseau.

L'objectif est atteint si vous trouvez les indices et l'image cachés.

Wireshark peut aussi être utile dans des analyses de sécurité. Votre tâche est maintenant de trouver une image cachée.

Voici les instructions :

1. Lancer une capture Wireshark
2. Visiter le site Web <http://iict-space.heig-vd.ch/jer/wschallenge/>.
3. Choisir un filtre d'affichage pour montrer le trafic Web.
4. Analyser le contenu des paquets, notamment le contenu du paquet « HTTP/1.1 200 OK » après le message « GET /jer/wschallenge/ HTTP/1.1 ».
5. Est-ce que vous trouvez l'indice et l'image ? L'indice se trouve vers la fin du contenu du paquet « 200 OK ».
6. Sauvegarder l'image comme élément à rendre sur Cyberlearn.



Puis complétez le formulaire Cyberlearn.

Objectif 3 : analyse forensique

L'objectif de cette partie est d'apprendre à utiliser des fonctions avancées (conversations, flux) de Wireshark.

L'objectif est atteint si vous arrivez à effectuer l'analyse ci-dessous et à répondre aux questions.

Wireshark ne permet pas seulement d'effectuer des captures en temps réel, mais aussi d'enregistrer une capture dans un fichier .pcap et de l'utiliser après-coup.

Votre tâche est d'analyser un email envoyé d'Ann à son amant secret.

Voici les instructions :

1. Télécharger le fichier PCAP evidence02.pcap de Cyberlearn.
2. Ouvrir le fichier PCAP avec Wireshark.
3. Utilisez comme filtre d'affichage « smtp »
(le protocole pour l'échange d'emails).
4. Utilisez le menu « Statistics » → « Conversations » pour afficher les connexions.
5. Sélectionnez les connexions TCP.
6. Puis analysez chacune des connexions TCP à l'aide du bouton « Follow stream ».
7. Vous verrez les données envoyées entre le client email d'Ann et un serveur mail.



Répondez aux questions sur Cyberlearn.

Objectif 4 - analyse forensiques avec des outils

Nous pouvons encore aller plus loin dans l'analyse des données comprises dans la capture Wireshark.

- Quel est le mot de passe d'Anne ?
- Dans quelle ville est le rendez-vous (nécessite l'extraction de l'attachement du mail) ?

Essayez de répondre à ces questions ! Voici quelques pistes :

Le login et le mot de passe d'Ann sont transmis lors de l'échange avec le serveur email. Ils apparaissent de manière codée dans les textes générés par « Follow TCP stream ». Ces textes sont marqués en gras ci-dessous.

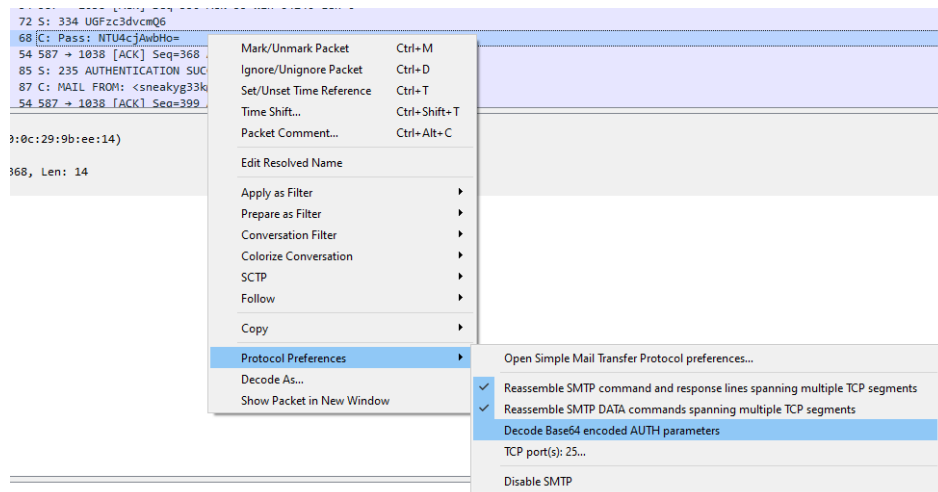
Ces textes semblent encryptés, mais en réalité ils ne sont que codés et peuvent être décodés facilement.

Utilisez la commande `base64` sur Linux ou le site <https://www.base64decode.org/> pour les décoder.

```
220 cia-mc07.mx.aol.com ESMTP mail_cia-mc07.1; Sat, 10 Oct 2009 15:37:56 -0400
EHLO annlaptop
250-cia-mc07.mx.aol.com host-69-140-19-190.static.comcast.net
250-AUTH=LOGIN PLAIN XAOL-UAS-MB
250-AUTH LOGIN PLAIN XAOL-UAS-MB
250-STARTTLS
250-CHUNKING
250-BINARYMIME
250-X-AOL-FWD-BY-REF
250-X-AOL-DIV_TAG
250-X-AOL-OUTBOX-COPY
250 HELP
AUTH LOGIN
334 VXNlcm5hbWU6
c25lYWt5ZzMza0Bhb2wuY29t
334 UGFzc3dvcmQ6
NTU4cjAwbHo=
235 AUTHENTICATION SUCCESSFUL
```

Wireshark offre la possibilité de simplifier le décodage base64 :

- Clic droit sur un des paquets du flux
- Choisir « Protocol preferences », puis « Decode Base64 encoded AUTH parameters ».



Pour extraire le fichier attaché au mail, vous avez deux options : la conversion manuelle ou l'exportation automatique par Wireshark.

Conversion manuelle

Sauvegardez le résultat de la commande « Follow TCP stream » dans un fichier texte. Puis effacez tout sauf le texte codé entre les lignes « -----=_NextPart... », marqués en gras ci-dessous. Il s'agit d'un fichier binaire « secretrendezvous.docx », codé en Base64.

```
<DIV><FONT face=3DArial size=3D2>Hi sweetheart! Bring your fake passport =
and a=20
bathing suit. Address attached. love, Ann</FONT></DIV></BODY></HTML>

-----=_NextPart_001_000E_01CA497C.9DEC1E70--

-----=_NextPart_000_000D_01CA497C.9DEC1E70
Content-Type: application/octet-stream;
    name="secretrendezvous.docx"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
    filename="secretrendezvous.docx"

UESDBBQABgAIAAAAIQDIeUAGfwEAANcFAAATAAgCW0NvbnRlbnRfVHlwZXNdLnhtbCCiBAIooAAC
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
A
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
A
...
... (beaucoup de lignes)
...
NXECAACGCAAAEgAAAAAAAAAAAAAAAAABFIQMA29yZC9mb250VGFiGUEG1sUEsBAi0AFAAGAAgA
AAAhAKVR8wbYAAQAA2QMAABAAAAAAAAAAAAAAAAAA5iMDAGRvY1Byb3BzL2FwcC54bWxQSwUGAAAA
AA0ADQBEAwAA9CYDAAAA

-----=_NextPart_000_000D_01CA497C.9DEC1E70--

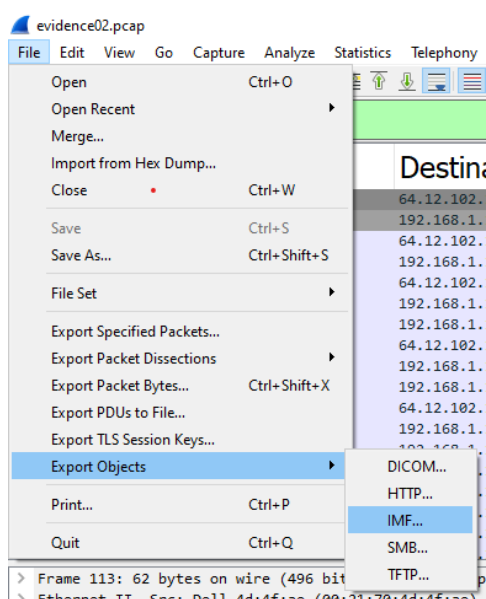
.
250 OK
QUIT
221 SERVICE CLOSING CHANNEL
```

Utilisez la commande `munpack` sur Linux ou la fonction « Decode files from Base64 format » de la page <https://www.base64decode.org/> pour extraire le fichier Word.

Exportation automatique avec Wireshark

Wireshark comprend le format de messagerie. Il vous permet de directement exporter le message :

- Choisir le menu principal « File », puis « Export Objects », puis « IMF... ».
- Choisir le message à exporter.
- Ouvrir le message sauvegardé avec double-clic. Il s'ouvre dans votre client email comme Outlook.



Puis complétez le formulaire Cyberlearn.