Lab packet-introspection

Démarrer le laboratoire
Le laboratoire est lancé à partir du répertoire de travail labtainer sur votre hôte sur votre hôte ou votre machine virtuelle Linux. Exécutez la commande:

```
labtainer packet-introspection
```

Un lien vers ce manuel de laboratoire sera affiché.
Le terminal virtuel résultant comprend : un terminal (shell bash) connecté à un ordinateur **client** "ws".

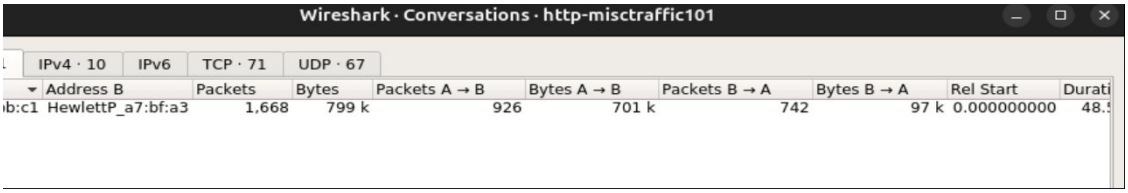
Tâches

1 Trouver le flux TCP le plus actif

Une tâche d'analyse de réseau commune consiste à déterminer les principaux contributeurs au trafic réseau et à la potentielle congestion. Dans cette partie, vous allez isoler et examiner le plus grand débit TCP dans une capture de paquets. Réaliser les étapes suivantes et répondez aux questions.

1. Lancez **wireshark** et ouvrez le fichier `pcaps/http-misctraffic101.pcapng`

2. Sélectionnez **Statistics — Conversations.** Cliquez sur l'onglet **Ethernet**; remarquez qu'il n'y a qu'une paire d'hôtes qui communiquent sur le réseau local. Cochez la case de résolution de nom **« Name resolution »**.
   L'adresse MAC indiquée comme *Cadant* est celle du routeur local.
   L'hôte *HewlettP* est le client à partir duquel le trafic a été capturé.



Cadant → routeur local (MAC du routeur)
HewlettP → machine cliente

3. Cliquez sur l'onglet **IPv4** pour examiner les conversations IPv4 dans ce fichier de trace. En vous basant sur le comptage des octets, identifiez les adresses IP qui participent à la conversation IPv4 la plus active.

Ethernet · 1 | IPv4 · 10 | IPv6 | TCP · 71 | UDP · 67

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
24.6.173.220	209.177.86.18	982	655 k	371	65 k	611	589 k	9.727620000	30.592006	17 k	154 k
24.6.173.220	50.23.252.178	63	52 k	21	1932	42	50 k	11.138355000	19.857303	778	20 k
24.6.173.220	75.75.75.75	152	20 k	76	5915	76	14 k	9.700260000	22.238250	2127	5368
24.6.173.220	210.72.21.12	99	19 k	57	5468	42	13 k	11.119240000	26.916819	1625	4037

Conversation IPv4 la plus active identifiée dans Wireshark à partir du comptage des octets.

- Cliquez sur l'onglet TCP pour identifier la conversation TCP la plus active. Trier par octets en cliquant sur l'entête de colonne des octets « Bytes ».

- Lorsque vous regardez le flux le plus actif, vous voyez que l'hôte Source 24.6.173.220 utilise un port aléatoire (61598) et l'hôte Destination: 209.177.86.18 utilise le port HTTP (80).
  (Si vous voyez des noms de service, vous pouvez décocher la zone de résolution de noms pour afficher les Numéros de port.)
-

Ethernet · 1 | IPv4 · 10 | IPv6 | TCP · 71 | UDP · 67

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B
24.6.173.220	61619	209.177.86.18	80	103	100 k	33	2117	70	98 k	11.393133000	8.757697	1
24.6.173.220	61604	209.177.86.18	80	112	94 k	40	4940	72	89 k	10.758501000	9.394069	4
24.6.173.220	61599	209.177.86.18	80	99	89 k	31	4224	68	85 k	9.727620000	11.416123	2

Analyse des conversations TCP dans Wireshark : la conversation entre 24.6.173.220 (client) et 209.177.86.18 (serveur web) est la plus active, avec une communication HTTP sur le port 80.

4. Cliquez avec le bouton droit de la souris sur la conversation TCP la plus active et sélectionnez Appliquer en tant que filtre « **Apply as a Filter—Selected—A<->B** ». Wireshark crée et applique automatiquement un filtre d'affichage pour cette conversation TCP. Cochez la case « **Limit to display filter** ».
   Combien de paquets correspondent à ce filtre? Il y a 103 paquets filtrés

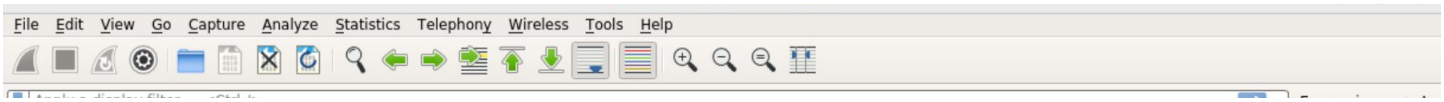
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	B
24.6.173.220	61619	209.177.86.18	80	103	100 k	33	
24.6.173.220	61604	209.177.86.18	80	112	94 k	40	
24.6.173.220	61599	209.177.86.18	80	99	89 k	31	

Filtrage de la conversation TCP la plus active dans Wireshark à l'aide de la fonction "Apply as Filter A<->B", montrant que 103 paquets correspondent à ce flux.

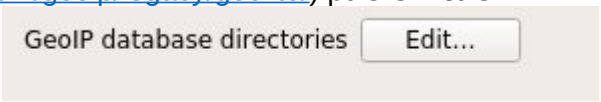
2. Géolocaliser des Adresses IP

Faire la corrélation entre les adresses IP des interfaces réseau et leurs emplacements physiques est souvent une tâche utile. Wireshark comprend une fonctionnalité de base à cet égard, qui utilise les versions gratuites de la base de données MaxMind2. Il est important de reconnaître qu'aucune base de données de Géolocalisation IP n'est sans erreur. En effet, diverses approches permettent de géolocaliser des adresses IP et ces processus ont des complexités associées plus importantes que nous n'étudierons pas ici.

1. Lancez **wireshark** et ouvrez le fichier `pcaps/http-browse101c.pcapng`



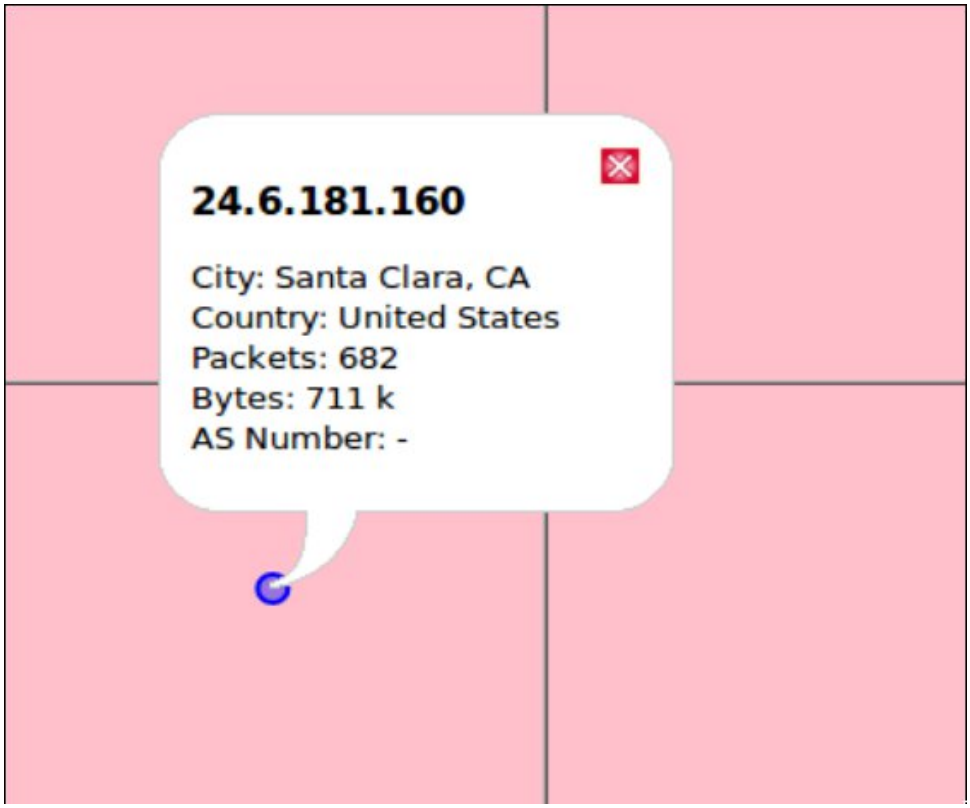
2. Sélectionnez **Edit — Preferences — Name Resolution** et cliquez le bouton modifier **Edit** des
3. répertoires de base de données GeoIP, cliquez sur *Nouveau*  et pointez sur le répertoire `/home/ubuntu/MaxMind` (qui dispose de fichiers de base de données téléchargés à partir de :http://dev.maxmind.com/geoip/legacy/geolite/) puis **OK** et **OK**.



4. Sélectionnez **Statistics — Endpoints** et cliquez sur l'onglet IPv4. Vous devriez voir des informations dans les colonnes pays, ville, latitude et longitude (**Country, City, Latitude,** et **Longitude**).

Informations de géolocalisation des adresses IPv4 affichées dans Wireshark (Endpoints IPv4).

5. Cliquez sur le bouton **Map**, Wireshark lancera une vue cartographique dans votre navigateur avec les adresses IP connues tracées sous forme de points sur la carte. Cliquez sur l'un des points pour trouver plus d'informations sur l'adresse IP.



➢ **Combien de trafic agrégé est allé à / provient de Santa Clara, CA? 682 paquets 7**

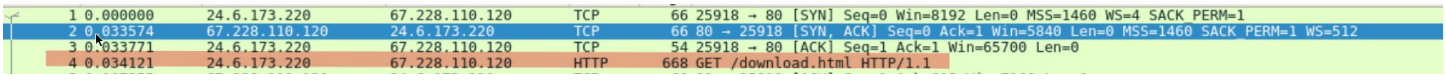
3. Réassembler un texte à partir du flux TCP capturé

En tant que protocole orienté « flux d'octets », les données de segments TCP sont basées sur ses MSS, et non sur la sémantique de la langue anglaise, voire même sur le formatage des données d'application. Ainsi, il peut être utile de réassembler ces données avant de les inspecter manuellement.

1. Lancez **wireshark** et ouvrez le fichier `pcaps/http-wiresharkdownload101.pcapng`

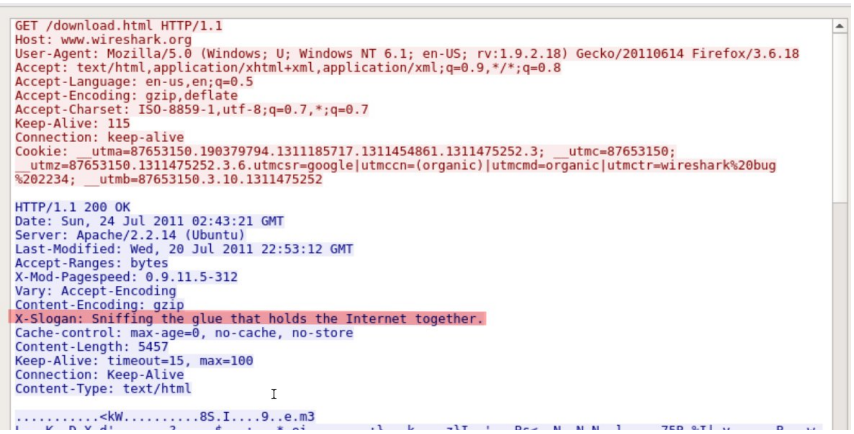
Les trois premiers paquets sont la poignée de main ou « handshake TCP » pour la connexion au Server Web. La trame 4 contient les requêtes GET des clients pour la page *download.html*.

2. Cliquez sur la **trame 4** et sélectionnez **Analysis - Follow — TCP stream** pour suivre le flux TCP. Le trafic du premier hôte vu dans le fichier de trace, le **client** dans notre cas, est coloré en **rouge**. Le trafic du deuxième hôte vu dans le fichier de trace, le **serveur** dans notre cas est coloré en **bleu**.



Suivi du flux TCP à partir de la trame 4 (HTTP GET) dans Wireshark.

3. Wireshark affiche la conversation sans les en-têtes Ethernet, IP ou TCP. Faites défiler le flux pour
4. rechercher le message caché de Gerald Combs, créateur de Wireshark. Il est situé dans le flux du serveur et commence par **X-Slogan**.



5. Quel est le message? **Sniffing the glue that holds the Internet Together**

Ce n'est pas le seul message masqué dans la session de navigation sur le Web. Maintenant que vous savez que le message commence par X-slogan, vous pouvez afficher dans WireShark chaque trame comprenant cette chaîne ASCII. Cliquez sur le bouton **Close** pour fermer, puis sur le bouton **Clear** pour supprimer le filtre de flux TCP.

6. Appliquer le filtre d'affichage qui contient " **X-Slogan**" sur les trames.

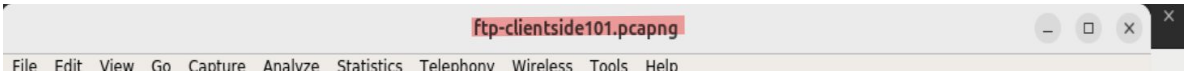
Astuce : repérez dans la zone Hypertext Transfer Protocol, le texte xslogan, cliquez avec le bouton droit et sélectionnez **Apply as Filter—Selected** afin de voir la syntaxe du filtre et le modifier.

7. Cliquez avec le bouton droit sur les deux autres trames affichées et sélectionnez **Follow — TCP stream** pour examiner les en-têtes HTTP échangés entre les hôtes. Avez-vous trouvé l'autre message? Notez que vous ne pouvez suivre qu'un seul flux à la fois en utilisant cette méthode de clic droit. Vous devrez effacer votre filtre d'affichage avant de suivre le prochain flux.
   Quel autre message avez-vous trouvé (différent de Q3)? **Snif free or die**

4. Extraire un fichier binaire d’une session FTP

Dans la section précédente, nous avons extrait des messages ASCII-text des paquets. Qu'en est-il des données binaires? Wireshark a également des outils pour cela.

1. Lancez **wireshark** et ouvrez le fichier `pcaps/ftp-clientside101.pcapng`



2. Faites défiler le début du fichier de trace. Vous verrez de nombreuses commandes **FTP** utilisées pour se connecter, demander un répertoire, définir un numéro de port pour le transfert de données et récupérer un fichier.
   Il existe deux connexions de données dans ce fichier de trace : une pour la liste des répertoires et une autre pour le transfert de fichier. Nous ne sommes intéressés que par ces deux flux de données et non par le flux de canal de commandes.
   - Choisissez une trame de flux de canal de commandes puis cliquez avec le bouton droit **Follow — TCP stream**, cliquez sur le bouton **Hide This Stream**. Ceci ferme la fenêtre du flux TCP et applique un filtre d'exclusion.

   Maintenant, vous ne voyez que le trafic de canal de données. Les trames 16 à 18 et 22 à 24 sont des paquets de poignée de main ou « handshake TCP » pour établir les deux canaux de données requis.

   - Cliquez avec le bouton droit de la souris sur la trame 16 et sélectionnez **Follow — TCP stream**. Cette liste de flux indique qu'il n'y a qu'un seul fichier dans le répertoire.
     Quel est son nom? **pantheon.jpg**

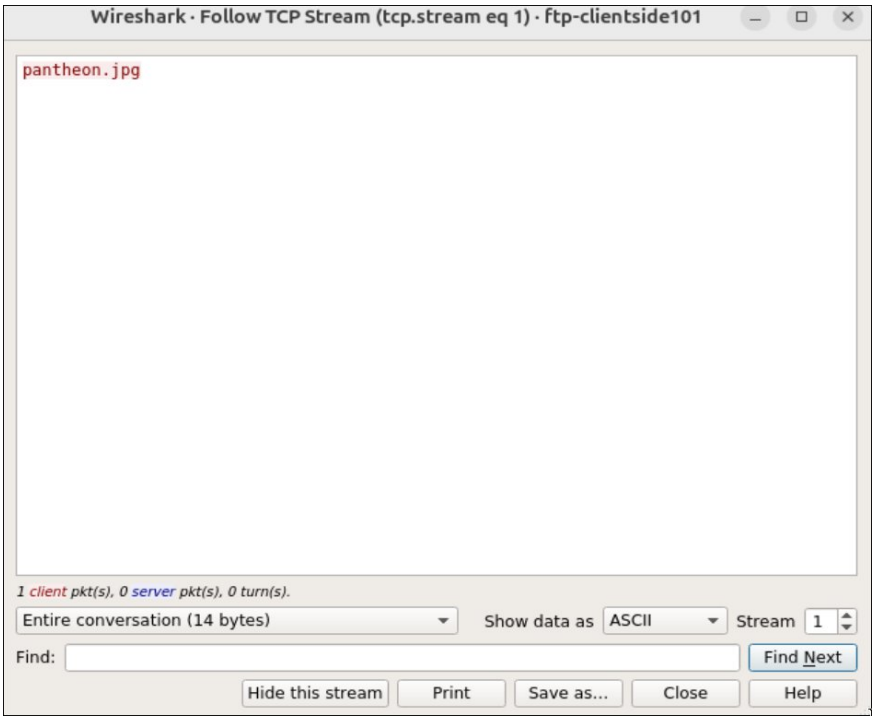
```
220 (vsFTPd 2.0.3)
USER anonymous
331 Please specify the password.
PASS anypwd
230 Login successful.
PORT 192,168,0,101,206,177
200 PORT command successful. Consider using PASV.
NLST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 192,168,0,101,206,178
200 PORT command successful. Consider using PASV.
RETR pantheon.jpg
150 Opening BINARY mode data connection for pantheon.jpg (5544612 bytes).
226 File send OK.
QUIT
221 Goodbye.
```

   - Cliquez sur le bouton **Hide This Stream**. Ceci ferme la fenêtre du flux TCP et l’ajoute au filtre d'exclusion existant.

   Le seul trafic restant affiché est le trafic de transfert de fichier.
   - Cliquez avec le bouton droit de la souris sur n'importe quelle trame et sélectionnez **Follow — TCP stream**.

Vous pouvez afficher l'identifiant de fichier qui indique qu'il s'agit d'un fichier .jpg (JFIF) et des métadonnées contenues dans le fichier graphique.

- Pour réassembler l'image graphique transférée dans cette communication FTP, dans la liste déroulante **Show and save data** choisissez le format **RAW**, puis cliquez sur le bouton **Save As**, sélectionnez un répertoire cible pour le fichier et définissez le nom du fichier avec celui que vous avez trouvé quelques étapes plus haut. Cliquez sur **Save** pour l'enregistrer.



- Accédez au répertoire cible et ouvrez le fichier que vous avez enregistré à l'étape précédente à l'aide du navigateur firefox installé sur le client **ws**. Inclure l'image dans votre rapport.