

Documentation - LabWireshark



Classe : BTS SIO 25.1A

Nom : Aries Smail

Table des matières

1- Définition

2- Prérequis

3- Installation

4- Fonctionnement

1- Définition

TCP : Le protocole TCP est une norme de communication qui permet aux programmes d'application et aux dispositifs informatiques d'échanger des messages sur un réseau. Il permet d'envoyer des paquets sur Internet et d'assurer la transmission effective des données et des messages via les réseaux.

ICMP : Le protocole ICMP (Internet Control Message Protocol) est un protocole de la couche réseau utilisé par les appareils du réseau pour diagnostiquer les problèmes de communication du réseau. ICMP est principalement utilisé pour déterminer si les données atteignent ou non leur destination en temps voulu.

FTP : Comme son nom l'indique, le File Transfer Protocol (FTP) est un protocole de transfert de fichiers par Internet. Il permet l'échange de commandes et de données entre un ordinateur ou un logiciel, le client FTP, et un serveur, l'hôte FTP. Ce serveur FTP est un répertoire distant.

HTTP : HTTP est un protocole qui permet de récupérer des ressources telles que des documents HTML. Il est à la base de tout échange de données sur le Web. C'est un protocole de type client-serveur, ce qui signifie que les requêtes sont initiées par le destinataire (qui est généralement un navigateur web)

Wireshark : Wireshark est un outil de capture et d'analyse de paquets. Il capture le trafic du réseau local et stocke les données ainsi obtenues pour permettre leur analyse hors ligne. Wireshark est capable de capturer le trafic Ethernet, Bluetooth, sans fil, Token Ring, et plus encore.

Paquet : Un paquet, ou paquet réseau, est un bloc de données formaté envoyé sur un réseau. Les principaux composants d'un paquet réseau sont les données utilisateur et les informations de contrôle.

Trame : Une trame est composée d'un en-tête (header), des informations que l'on veut transmettre, et d'un postambule (trailer). Un paquet (dans le cas d'IP par exemple) ne peut transiter directement sur un réseau : il est encapsulé à l'intérieur d'une trame.

2- Prérequis

Hyperviseur de Type 2 : Utilisez VirtualBox ou tout autre hyperviseur de type 2. Ces hyperviseurs s'exécutent comme une application au sein de votre système d'exploitation hôte.

ISO Ubuntu Labtainer : Vous aurez besoin de l'image disque ISO spécifique pour Ubuntu Labtainer. Cette version d'Ubuntu est préconfigurée pour inclure Labtainer, un ensemble d'outils de laboratoire pour les cours de cybersécurité.

(Disponible au téléchargement ici :

<https://nps.box.com/shared/static/dn636n6h2d556nwqezx5w6cfc4cfeacl.ova>)

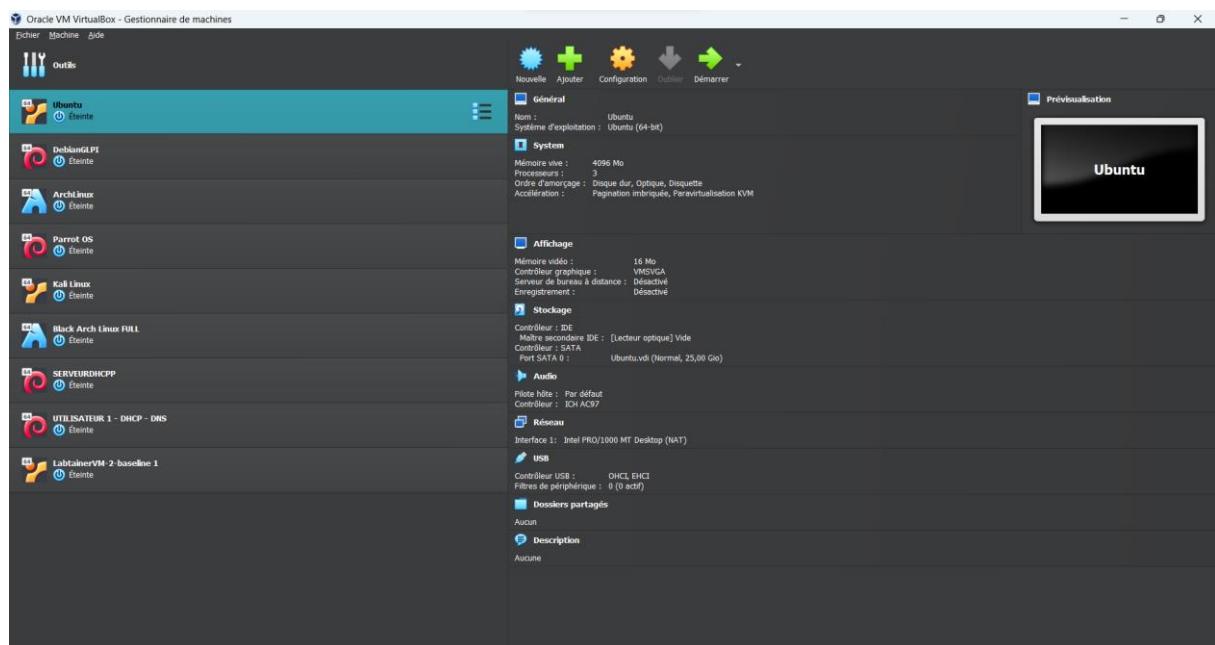
Wireshark : Un analyseur de protocole réseau indispensable pour examiner les paquets réseau et effectuer des analyses de trafic.

3- Installation

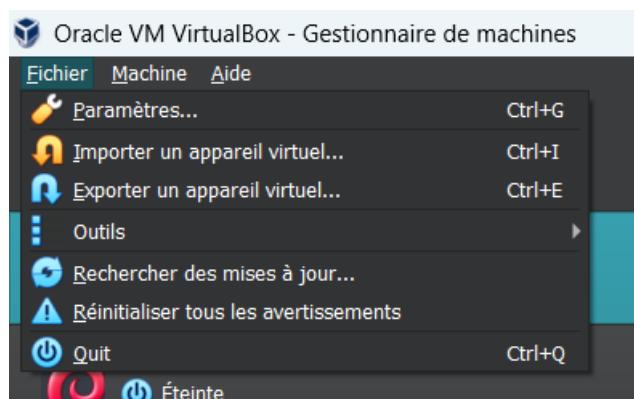
Premièrement nous allons installer l'iso préconfigurée via le lien donné dans « prérequis »

Maintenant que l'iso installé et sur votre bureau, vous pouvez lancer Virtuabox (si vous ne l'avez pas installé, vous pouvez l'installer via le lien suivant : <https://www.virtualbox.org/wiki/Downloads>)

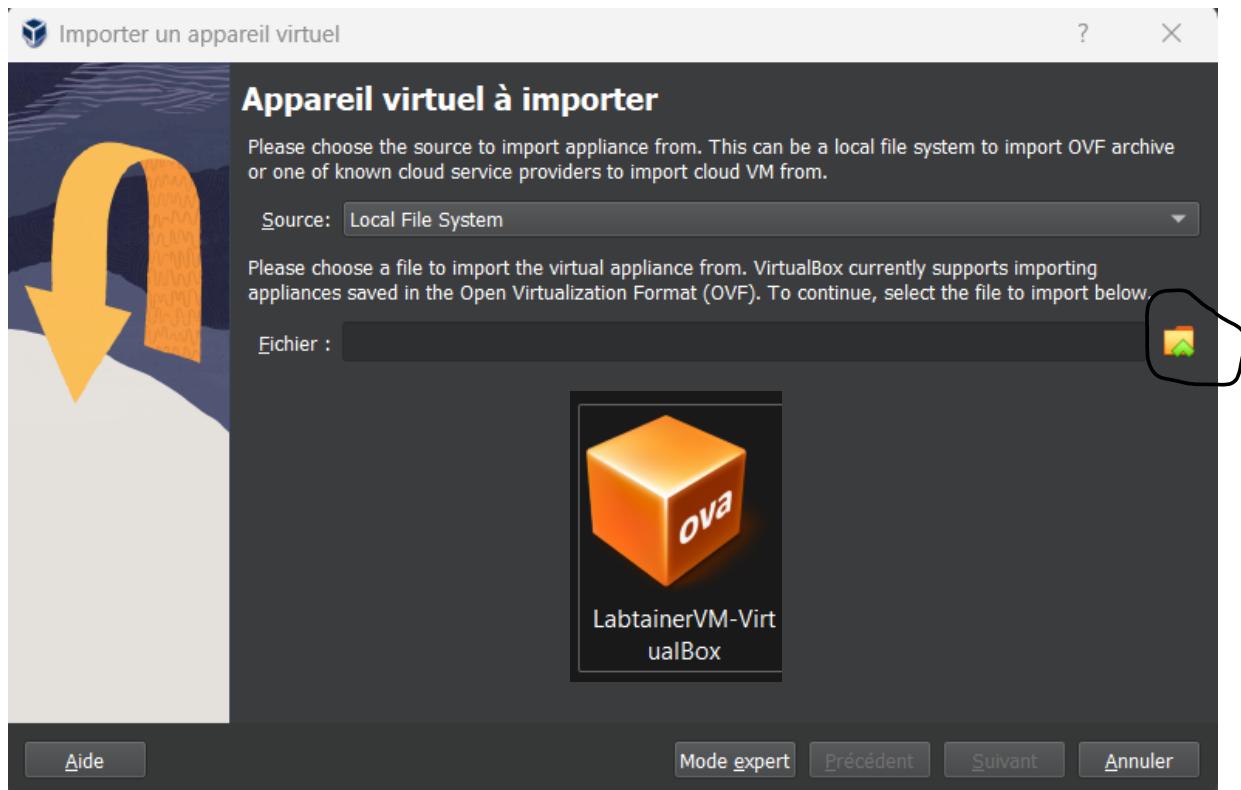
Maintenant, vous voici sur cette interface.



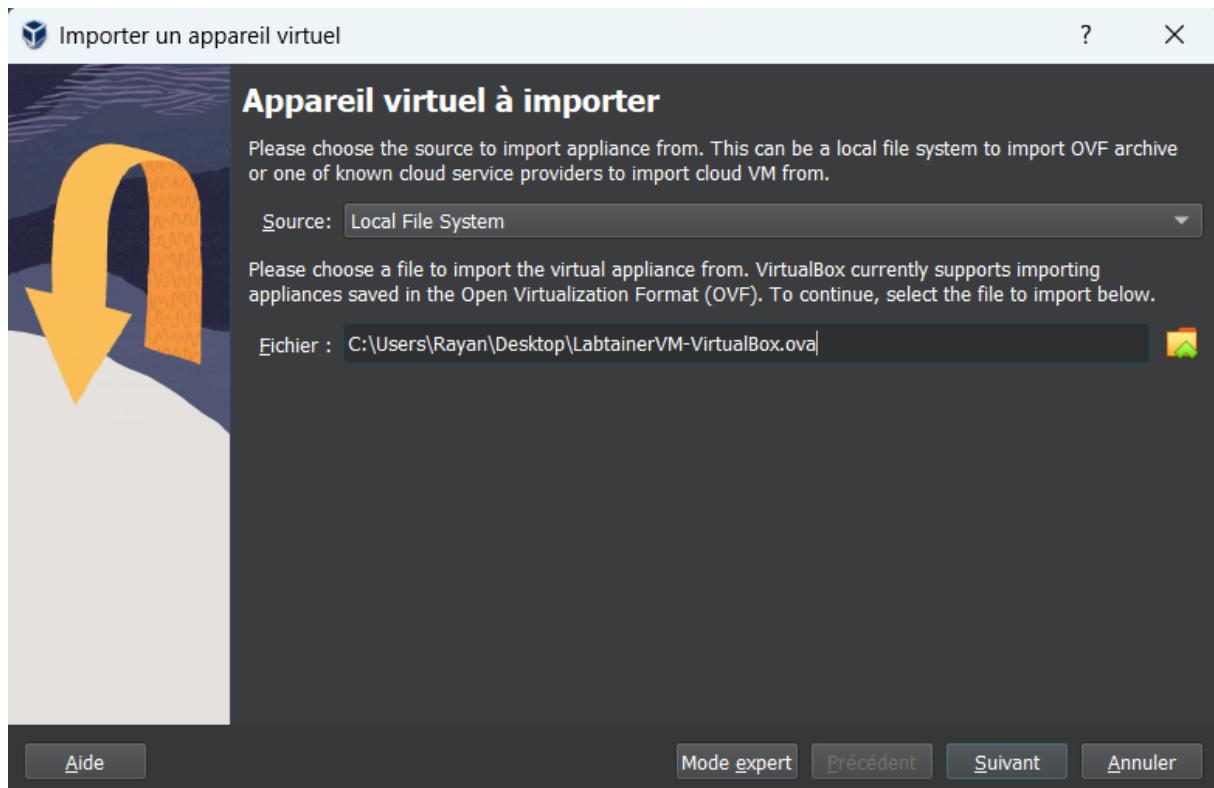
Cliquer sur « Fichier » en haut à gauche et cliquer sur « Importer un appareil virtuel... ».



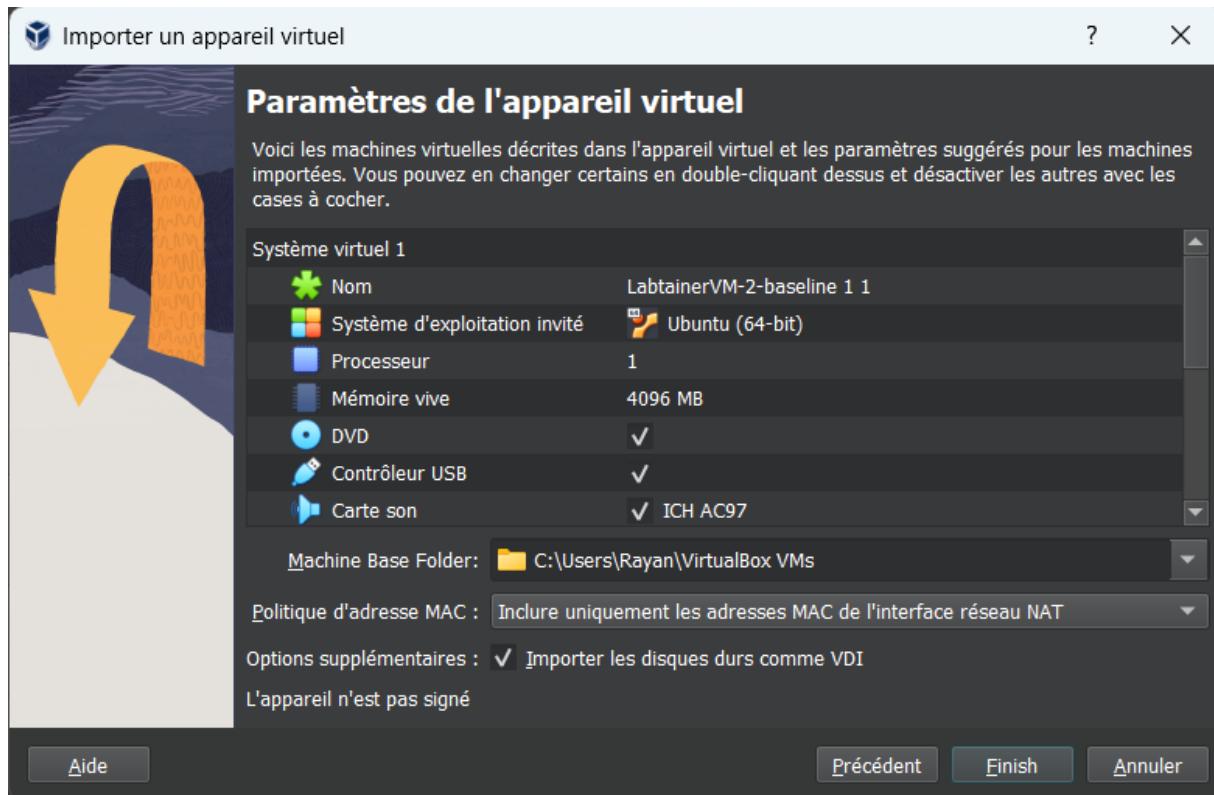
Arriver sur cette interface, sélectionner votre iso qui est sur votre bureau.



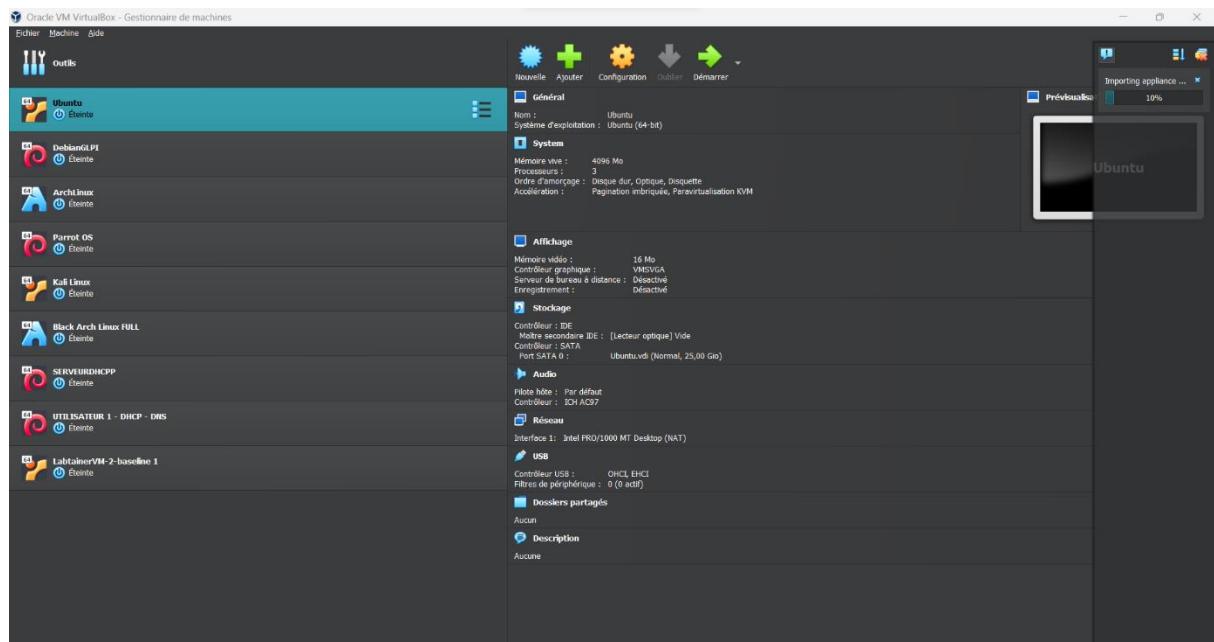
Si le chemin du fichier qui mène vers l'iso est correct, vous pouvez cliquer sur suivant.



Vous pouvez configurer votre machine et changer le processeur par exemple (je vous conseille de le mettre à 2). Après cela cliquer sur « finish ».



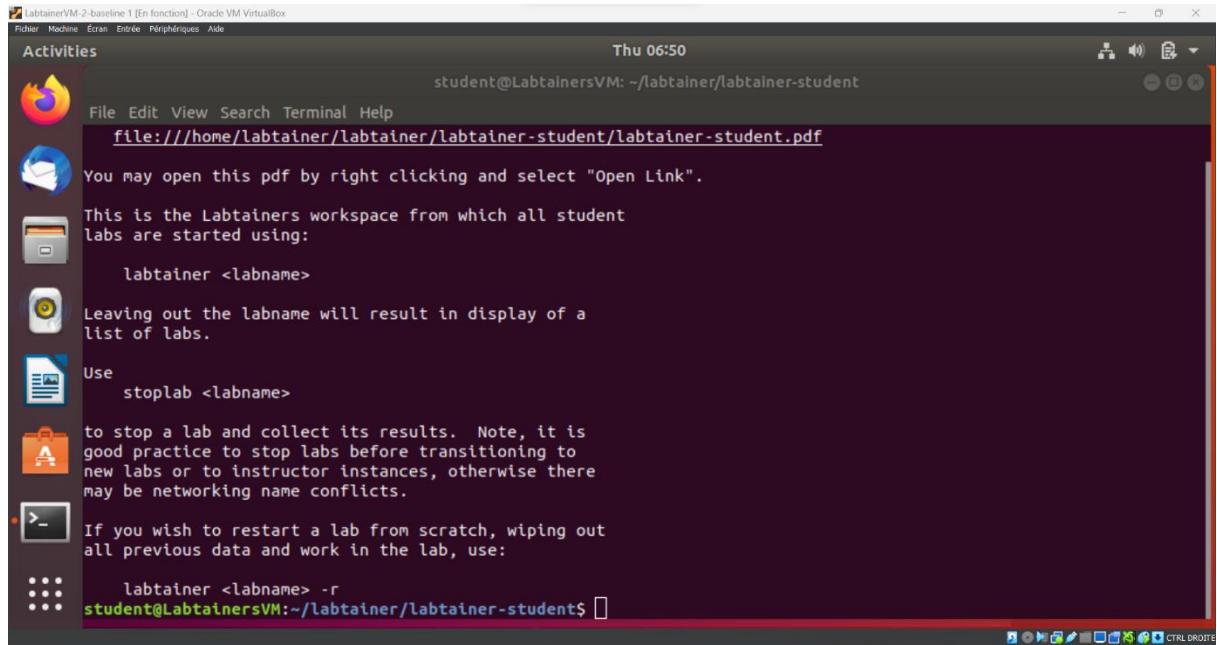
En haut à droite l'iso s'installe, attendez la fin de l'installation.



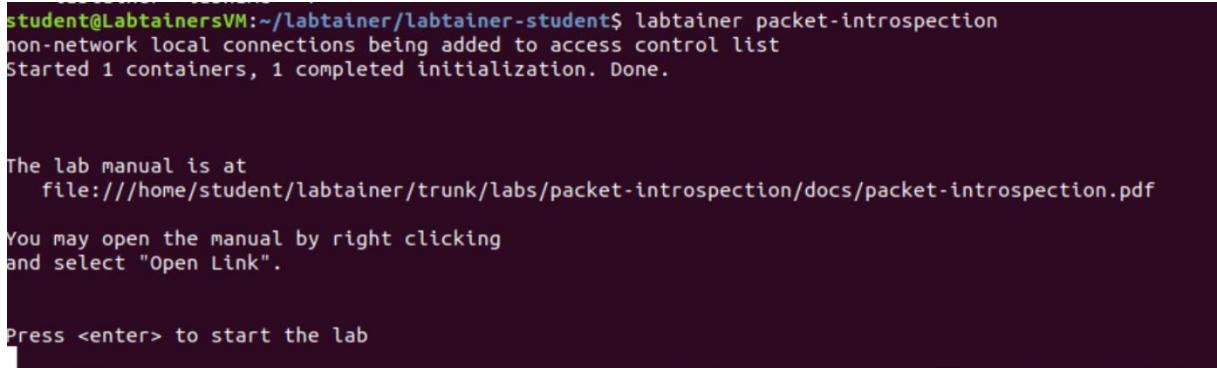
Et voilà vous pouvez lancer votre ISO.



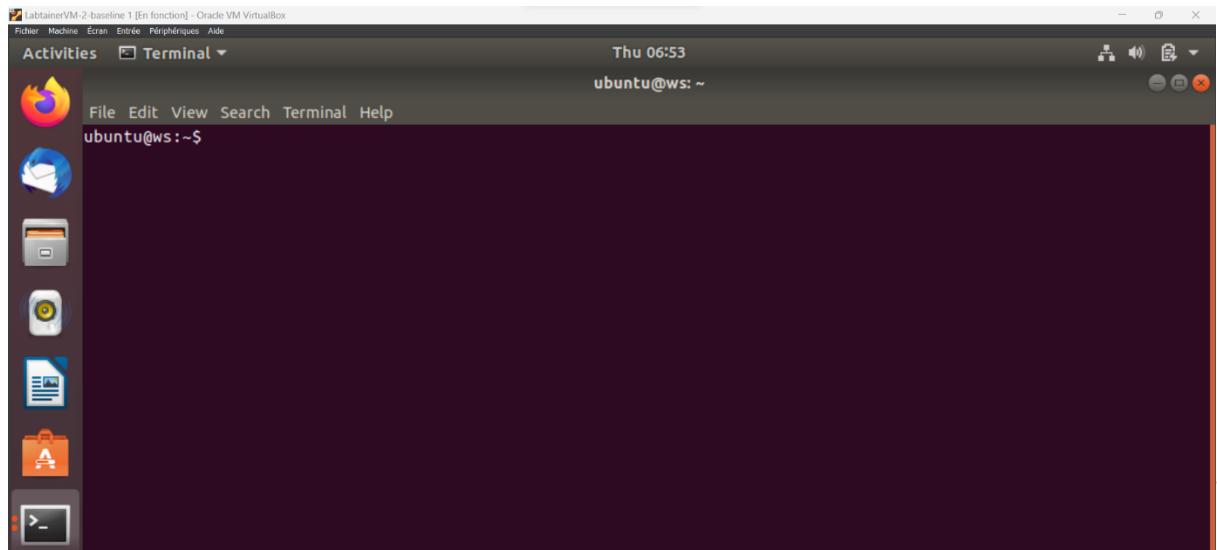
Après avoir double cliquer sur l'iso, vous arriverais sur cette interface avec un terminale



Pour lancer wireshark, vous allez effectuer la commande suivante « labtainer packet-introspection ».



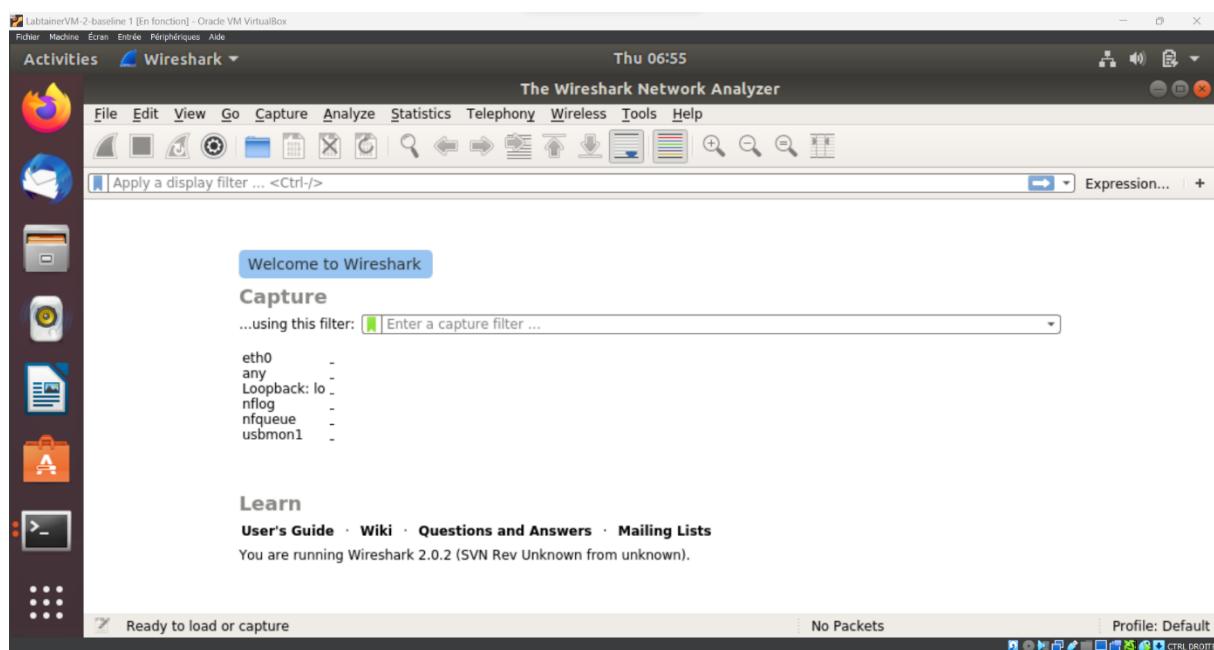
Arriver sur un nouveau terminal...



Vous pouvez taper cette commande suivante « wireshark »

```
ubuntu@ws:~/pcaps$ wireshark
```

Et vous voici sur wireshark



Vous pouvez maintenant commencer le TP

4- Fonctionnement

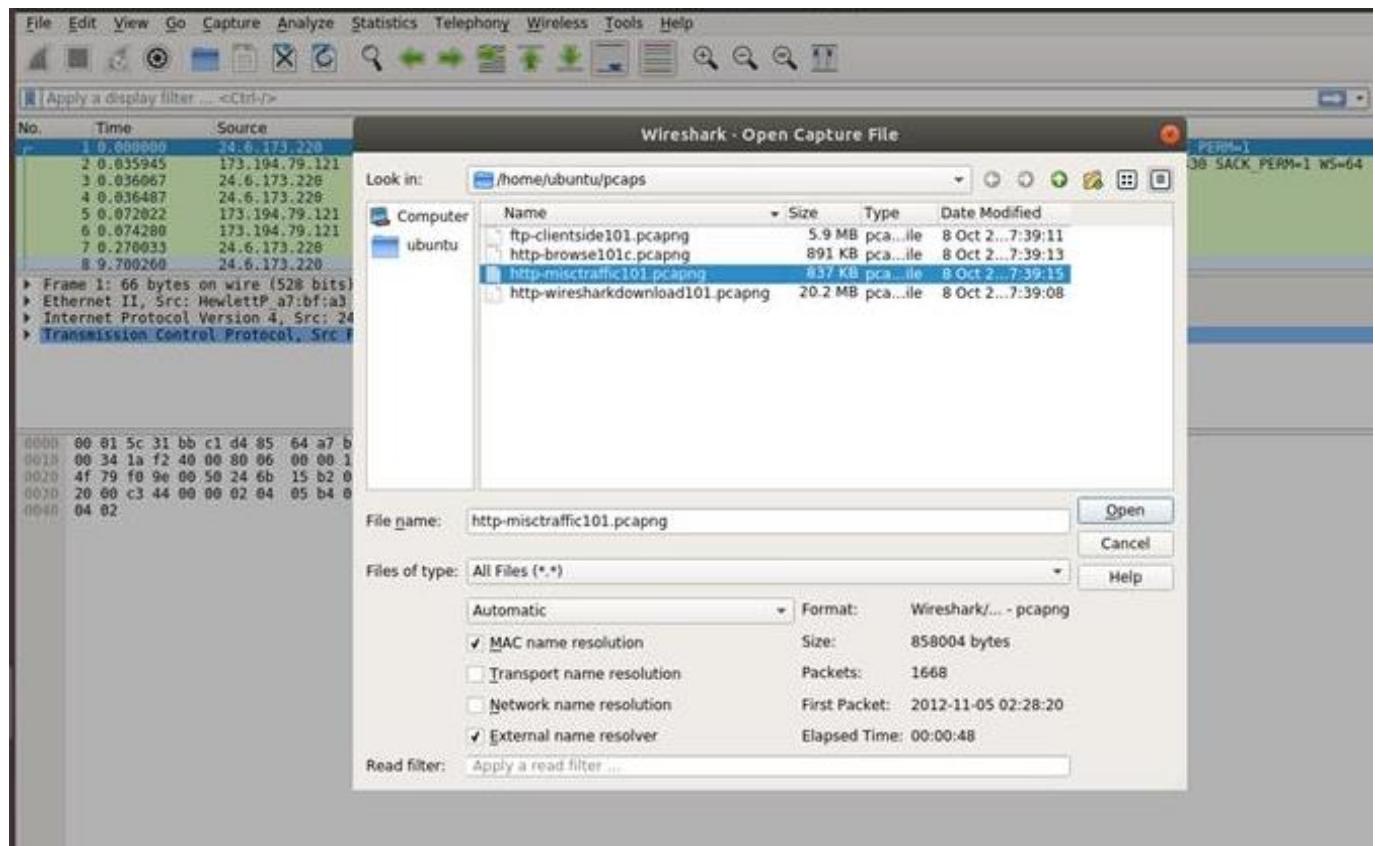
Partie 1 : Trouver le flux TCP le plus actif

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

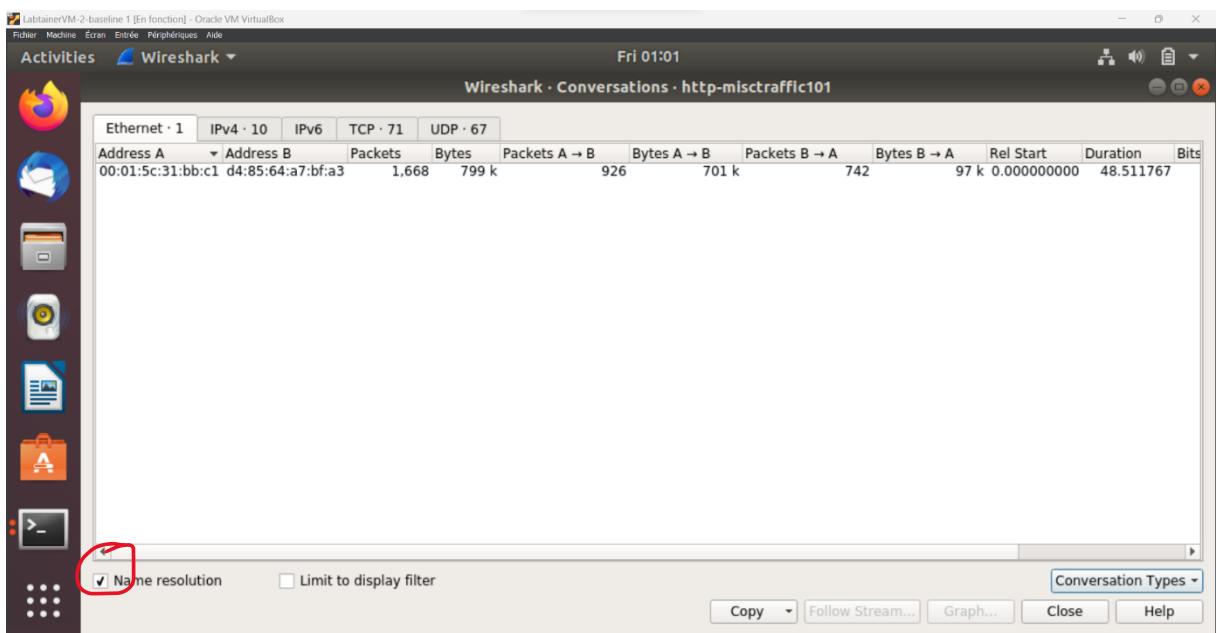
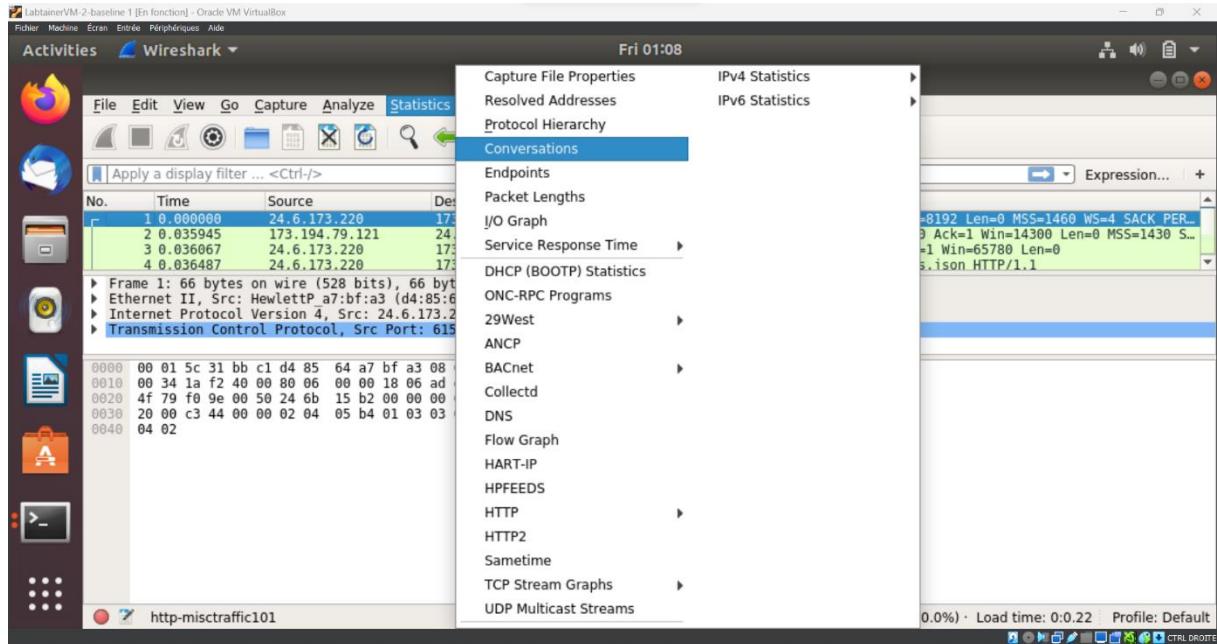
```
labtainer <labname> -r
student@LabtainersVM:~/labtainer/labtainer-student$ labtainer packet-introspection
latest: Pulling from labtainers/packet-introspection.ws.student
3fdfbb760d3e: Pull complete
24636a235964: Pull complete
ecf4c2718065: Pull complete
fc4f3cb439a3: Pull complete
4d80400a1583: Pull complete
556d49b3591a: Pull complete
1be4a963b3f6: Pull complete
8c3c11dc4a82: Pull complete
Digest: sha256:fa5c129eba5fcf089d6811523af6eabcf9220b76f1544fec148401a78af9b802
Status: Downloaded newer image for labtainers/packet-introspection.ws.student:latest
non-network local connections being added to access control list

Please enter your e-mail address: [ppppiiidkdkdd@gmail.com]
```

Lancer wireshark et ouvrir le fichier pcaps/http-misctrace101.pcapng



Sélectionner Statistic — Conversations. Cliquer sur l'onglet Ethernet ; remarquez qu'il n'y a qu'une paire d'hôtes qui communiquent sur le réseau local. Cocher la case de résolution de nom « Name résolution »



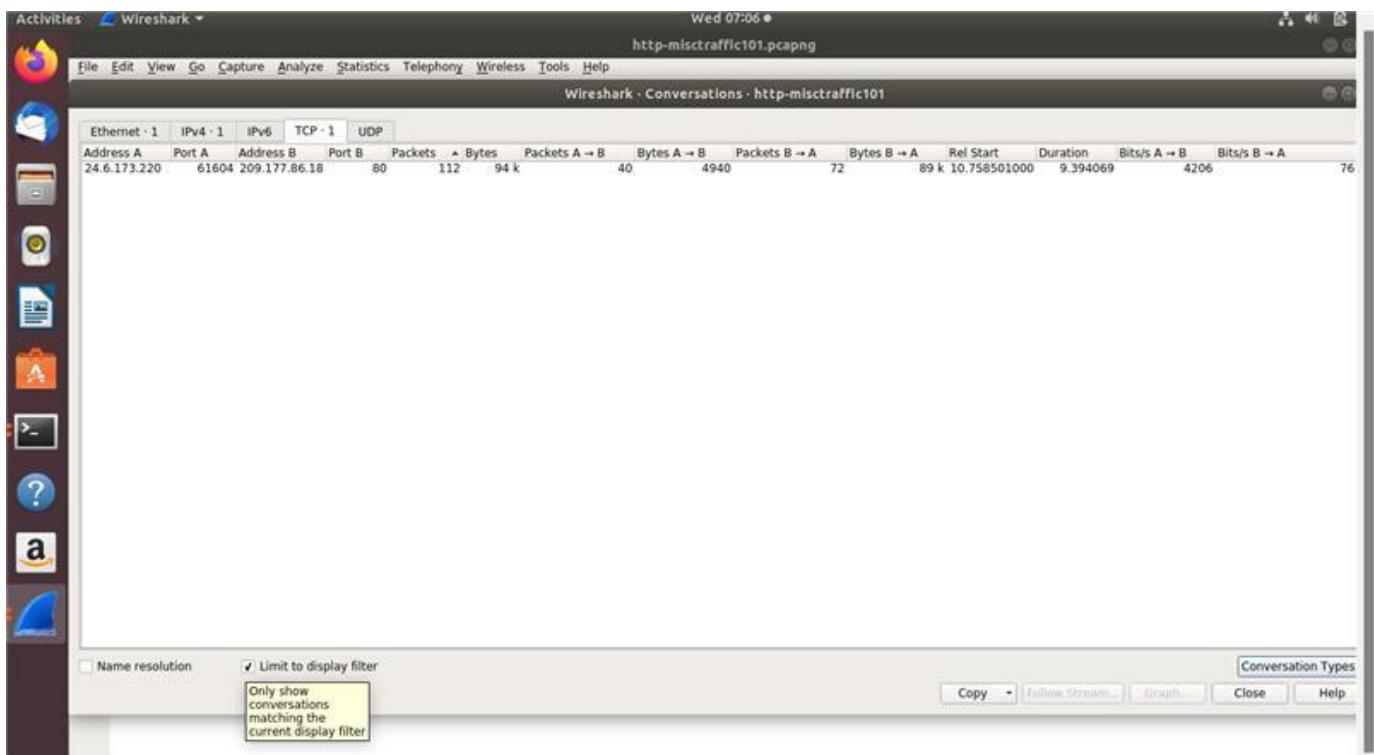
Cliquez sur l'onglet IPv4 pour examiner les conversations IPv4 dans ce fichier de trace. En vous basant sur le comptage des octets, identifiez les adresses IP qui participent à la conversation IPv4 la plus active.

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	658k	371	541	611	589 k	9.700260000	22.330250	2127	5368
24.6.173.220	210.72.21.12	99	20 k	7	5915	46	700260000	9.700260000	1080	4037	
24.6.173.220	123.125.115.126	82	14 k	57	5468	42	13 k	11.119240000	26.916819	1625	2016
24.6.173.220	210.72.21.87	73	7710	42	3408	31	4302	11.119731000	25.920122	1051	1327
24.6.173.220	210.72.21.79	79	72 k	42	3140	59	6945	11.119731000	25.920165	972	1266
24.6.173.220	210.72.21.42	71	7391	42	3246	29	4145	11.120195000	25.920609	1001	1279
24.6.173.220	210.72.21.11	64	10 k	36	3455	28	7191	10.174741000	26.865263	1028	2141
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	173.194.79.121	10	2024	6	658	4	1366	0.000000000	46.519803	113	234

Cliquer avec le bouton droit de la souris sur la conversation TCP la plus active et sélectionner “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. Cocher la case « Limit to display filter »

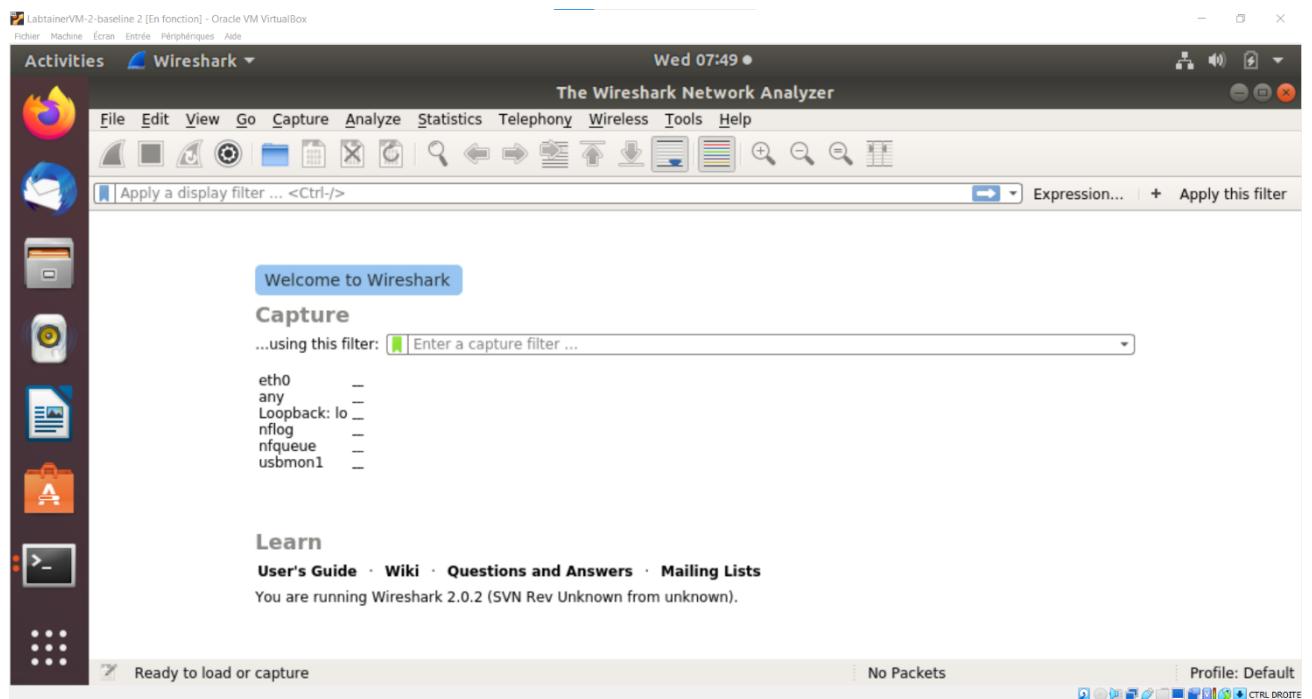
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
24.6.173.220	61619	209.177.86.18	80	103	100 k	33	2117	70	98 k				
24.6.173.220	61604	209.177.86.18	80	112	94 k	40	4940	72	89 k				
24.6.173.220	61599	209.177.86.18	80	99	89 k	31	4224	68	85 k				
24.6.173.220	61603	209.177.86.18	80	104	88 k	36	4375	68	83 k				
24.6.173.220	61607	209.177.86.18	80	86	65 k	31	4718	55	60 k				
24.6.173.220	61606	209.177.86.18	80	86	60 k	33	4882	53	55 k				
24.6.173.220	61608	209.177.86.18	80	79	52 k	31	5094	48	46 k				
24.6.173.220	61613	50.23.252.178	80	53	51 k	16	1203	37	50 k				
24.6.173.220	61605	209.177.86.18	80	78	50 k	30	5089	48	45 k				
24.6.173.220	61609	210.72.21.12	80	27	14 k	12	2822	15	11 k				
24.6.173.220	61651	209.177.86.18	80	33	8581	14	4882	19	3699				
24.6.173.220	61654	209.177.86.18	80	32	8525	14	4895	18	3630				
24.6.173.220	61652	209.177.86.18	80	33	8482	14	4780	19	3702				
24.6.173.220	61665	209.177.86.18	80	31	7783	13	4410	18	3373				
24.6.173.220	61655	209.177.86.18	80	30	7648	13	4343	17	3305				
24.6.173.220	61640	123.125.115.126	80	15	7384	6	634	9	6750				
24.6.173.220	61666	209.177.86.18	80	79	6054	12	3677	16	3683				

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	Bits/s B → A
24.6.173.220	61619	209.177.86.18	80	103	100 k	33	2117	70	98 k				
24.6.173.220	61604	209.177.86.18	80	112	94 k	40	4940	72	89 k				
24.6.173.220	61599	209.177.86.18	80	99	89 k	31	4224	68	85 k				
24.6.173.220	61603	209.177.86.18	80	104	88 k	36	4375	68	83 k				
24.6.173.220	61607	209.177.86.18	80	86	65 k	31	4718	55	60 k				
24.6.173.220	61606	209.177.86.18	80	86	60 k	33	4882	53	55 k				
24.6.173.220	61608	209.177.86.18	80	79	52 k	31	5094	48	46 k				
24.6.173.220	61613	50.23.252.178	80	53	51 k	16	1203	37	50 k				
24.6.173.220	61605	209.177.86.18	80	78	50 k	30	5089	48	45 k				
24.6.173.220	61609	210.72.21.12	80	27	14 k	12	2822	15	11 k				
24.6.173.220	61651	209.177.86.18	80	33	8581	14	4882	19	3699				
24.6.173.220	61654	209.177.86.18	80	32	8525	14	4895	18	3630				
24.6.173.220	61652	209.177.86.18	80	33	8482	14	4780	19	3702				
24.6.173.220	61665	209.177.86.18	80	31	7783	13	4410	18	3373				
24.6.173.220	61655	209.177.86.18	80	30	7648	13	4343	17	3305				
24.6.173.220	61640	123.125.115.126	80	15	7384	6	634	9	6750				
24.6.173.220	61610	210.72.21.87	80	12	2212	6	667	6	1545	11.119731000	5.974681	893	2068
24.6.173.220	61651	210.72.21.42	80	12	3187	6	696	6	2499	11.120195000	5.896654	941	3382
24.6.173.220	61652	210.72.21.97	80	12	3518	6	746	6	2499	11.120195000	5.896654	890	3179
24.6.173.220	61614	209.177.86.18	80	12	2050	6	882	6	1368	11.218233000	8.919195	610	1225
24.6.173.220	61623	209.177.86.18	80	12	2444	6	882	6	1762	11.4464751000	8.686932	628	1622
24.6.173.220	61661	210.72.21.87	80	12	2522	6	977	6	1545	30.805080000	5.810525	1345	2127
24.6.173.220	61662	202.96.25.95	80	12	3506	6	724	6	2782	30.806906000	6.179892	837	3601
24.6.173.220	61663	210.72.21.86	80	12	3441	6	1020	5	548	30.806906000	6.179892	954	1579
24.6.173.220	61653	210.72.21.11	80	11	1211	6	724	5	487	30.483236000	5.813467	996	679
24.6.173.220	61636	210.72.21.11	80	11	1293	6	706	5	586	30.504956000	6.133210	920	764
24.6.173.220	61662	210.72.21.42	80	11	1288	6	788	5	500	30.806024000	5.815511	2083	687
24.6.173.220	61598	173.194.79.121	80	10	2024	6	855	5	378	30.806024000	46.519803	113	234
24.6.173.220	61616	123.125.115.126	80	10	3250	5	955	5	378	30.806024000	46.519803	4424	5178
24.6.173.220	61649	123.125.115.126	80	10	3175	5	691	5	484	30.2175486000	1.706660	3299	2268
24.6.173.220	61657	123.125.115.126	80	10	1181	5	806	5	575	30.527278000	1.854728	3476	2480
24.6.173.220	61664	123.125.115.126	80	10	1165	5	729	5	436	30.212259000	0.173399	33 k	20 k
24.6.173.220	61658	123.125.115.126	80	10	1349	5	788	5	575	30.813103000	0.049085	5467	4393
24.6.173.220	61654	210.72.21.11	80	9	548	5	294	4	252	31.135870000	0.342033	370	317

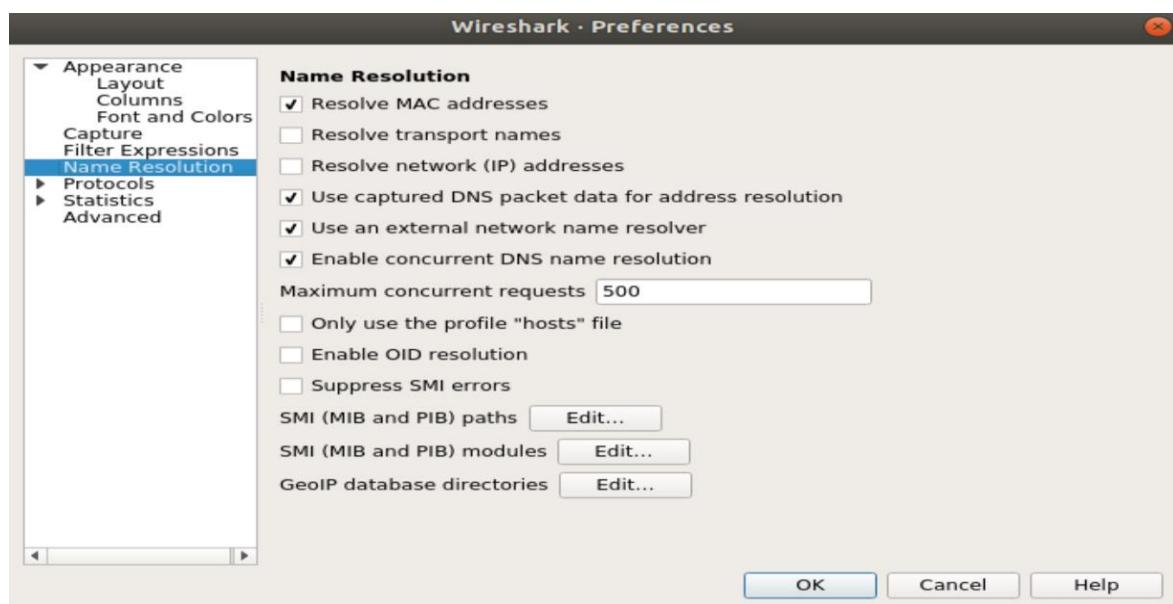


Partie 2 : Géolocaliser des Adresses IP

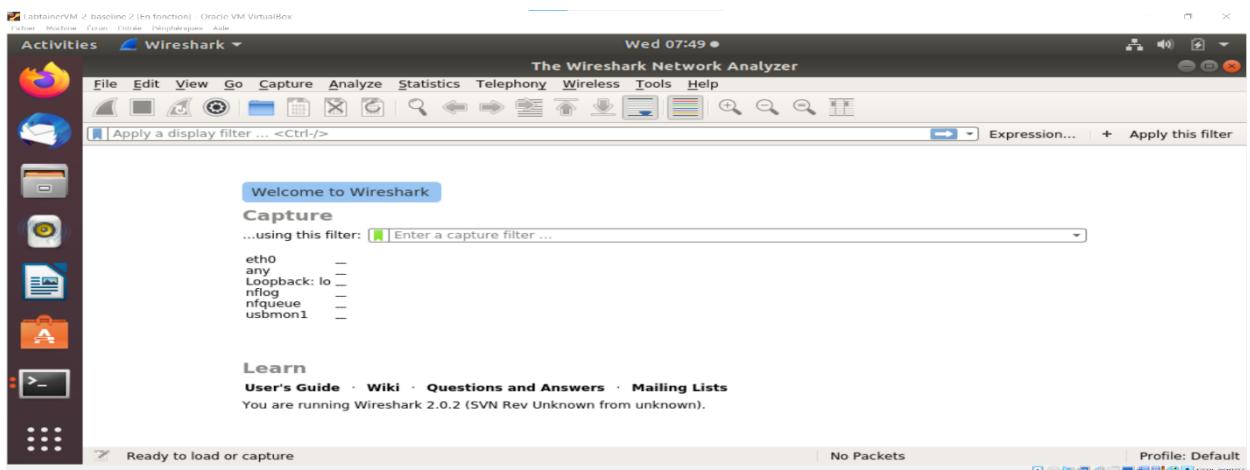
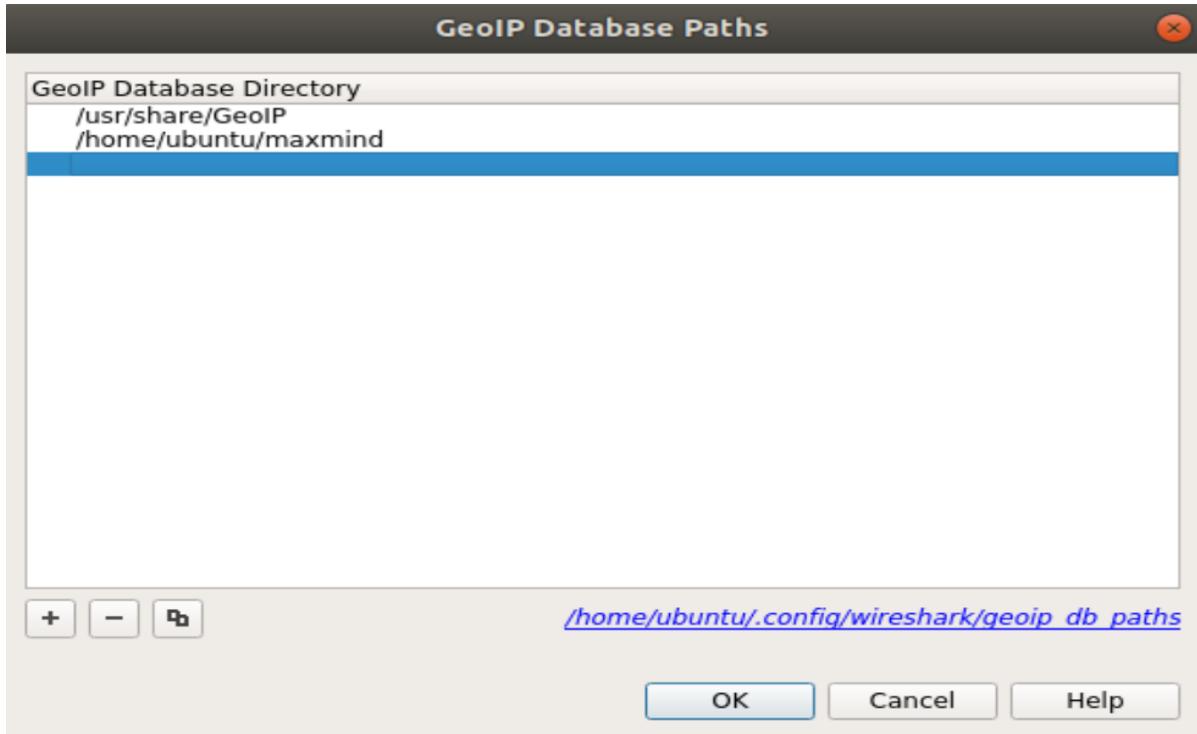
Lancer Wireshark :



Sélectionnez Edit — Préférences — Name Resolution et cliquez le bouton modifier Edit des 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.



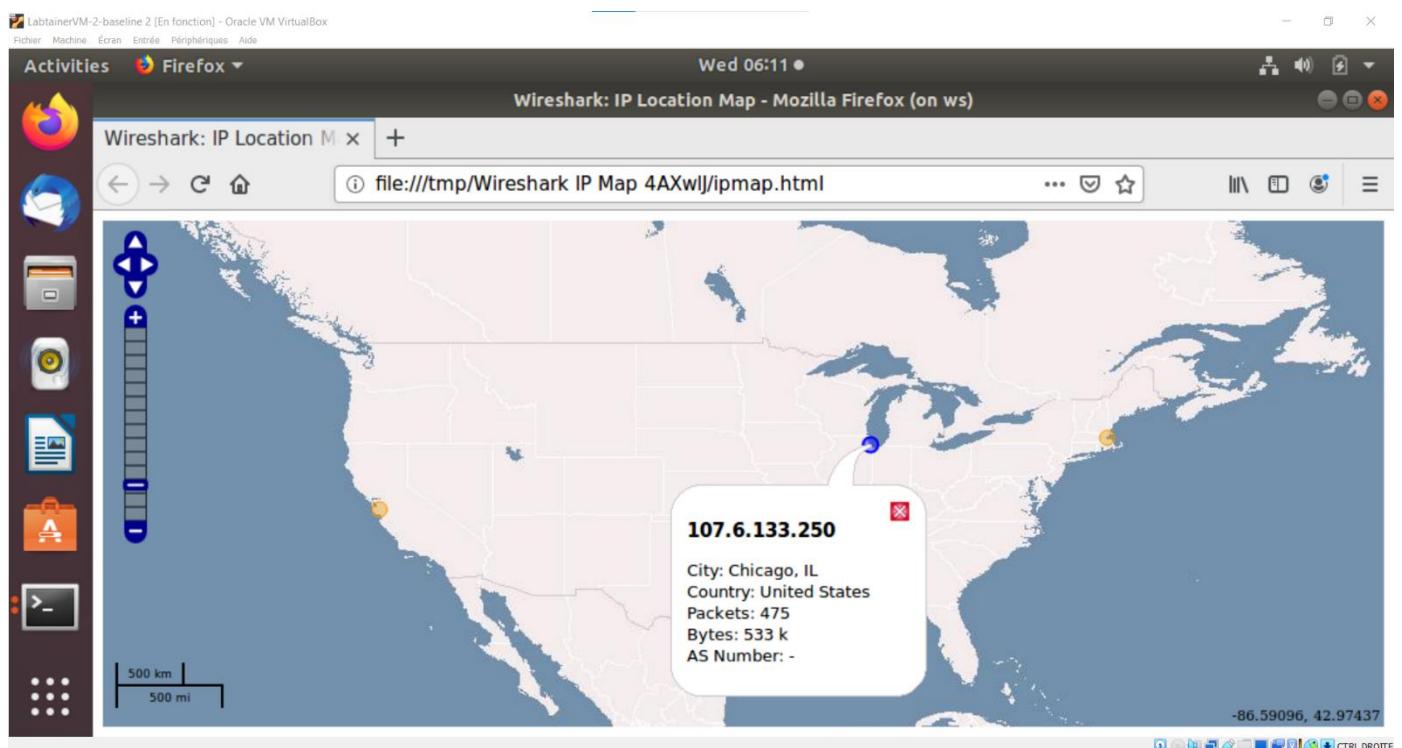
Sélectionnez Statistics — Endpoints et cliquez sur l'onglet IPv4. Vous devriez voir des informations dans les colonnes pays, ville, latitude et longitude (Country, City, Latitude, et Longitude).

Endpoints · http-browse101c								
IPv4 · 3	Ethernet · 2	IPv6	TCP · 9	UDP	Bytes A → B	Packets B → A	Bytes B → A	Country City AS Number Latitude Longitude
17 k	485	693 k	United States	Santa Clara, CA	AS7922 Comcast Cable Communications, LLC	37.350101	-121.985397	
525 k	126	8261	United States	Chicago, IL	AS32475 SingleHop LLC	41.877602	-87.627197	
168 k	71	9483	United States	Boston, MA	AS27552 TowardEX Technologies International, Inc.	42.358398	-71.059799	

Name resolution Limit to display filter Endpoint Types

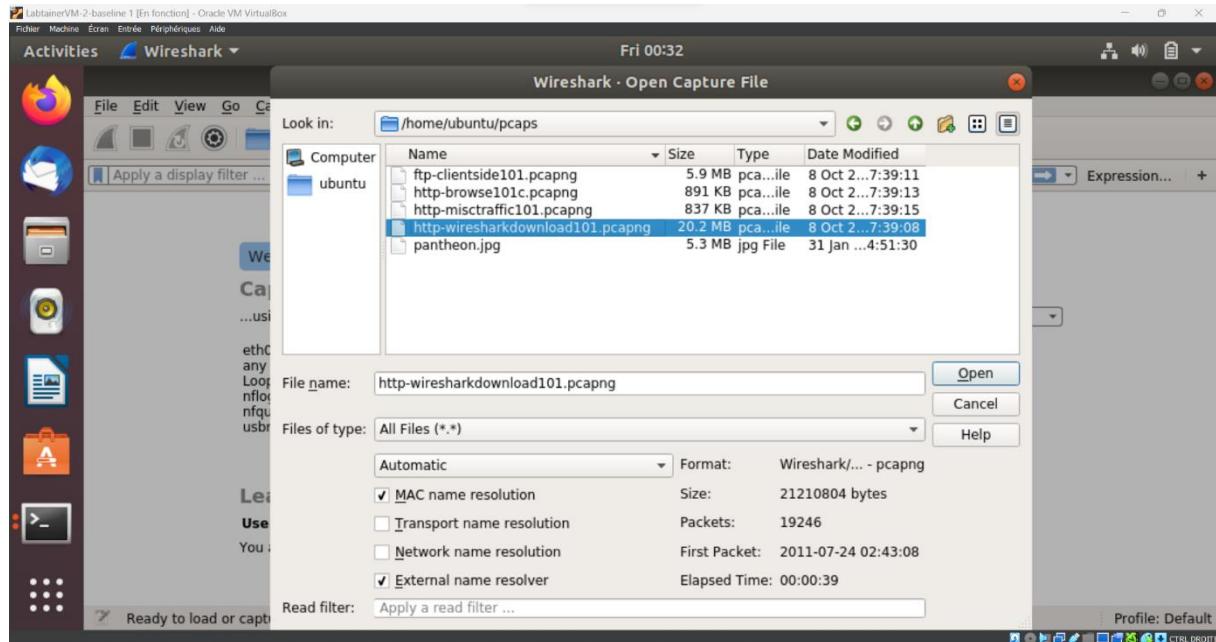
Copy Map Close Help

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.

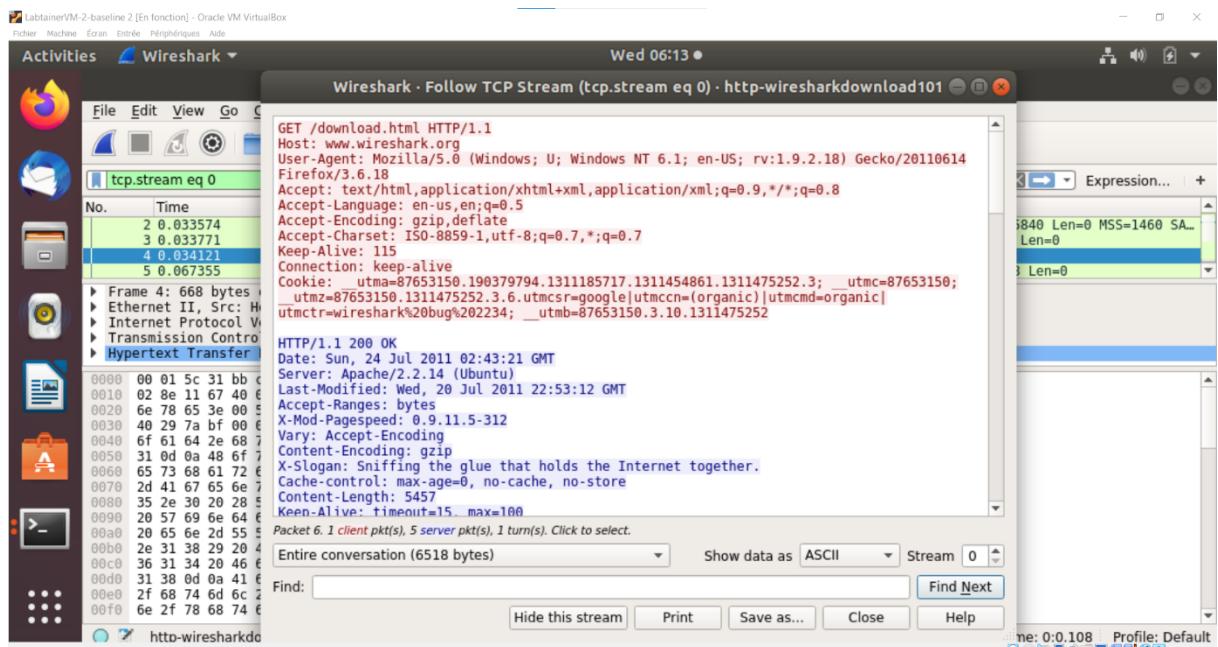


Partie 3 : Réassembler un texte à partir du flux TCP capturé

Pour commencer, nous avons lancé Wireshark et ouvert le fichier via Fichier → Ouvrir → pcaps/http-wiresharkdownload101.pcapng.



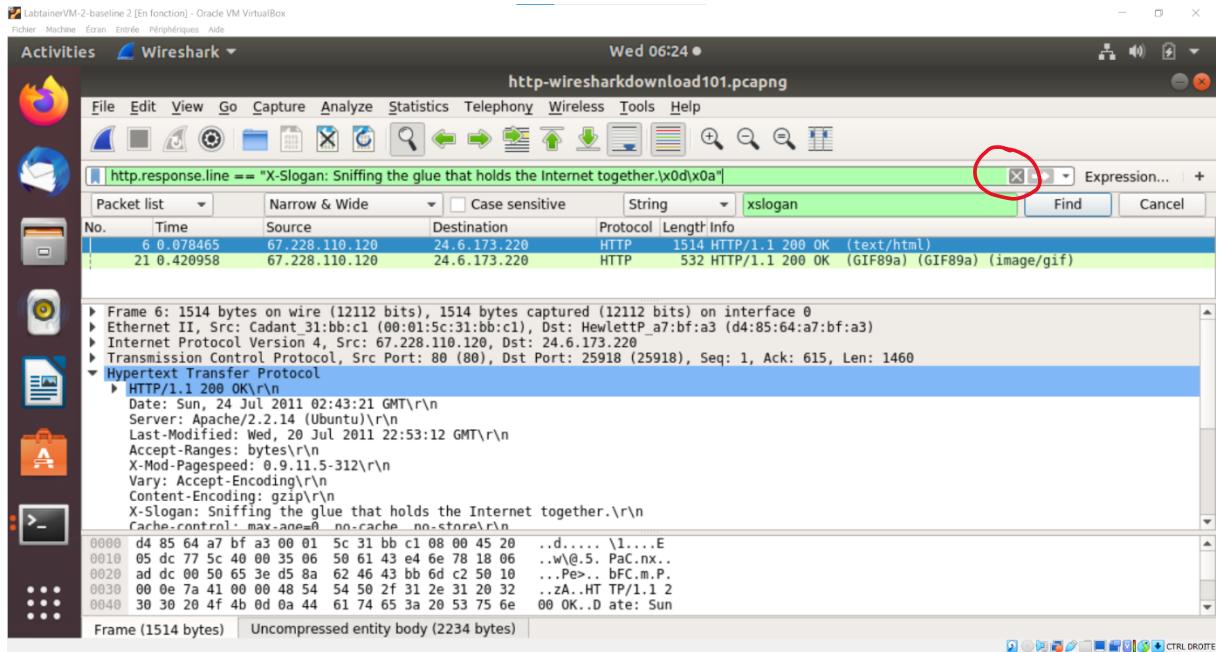
Plusieurs trames sont apparues. Nous avons cliqué sur la trame 4, puis sélectionné Analysis → Follow → TCP Stream pour suivre le flux TCP.



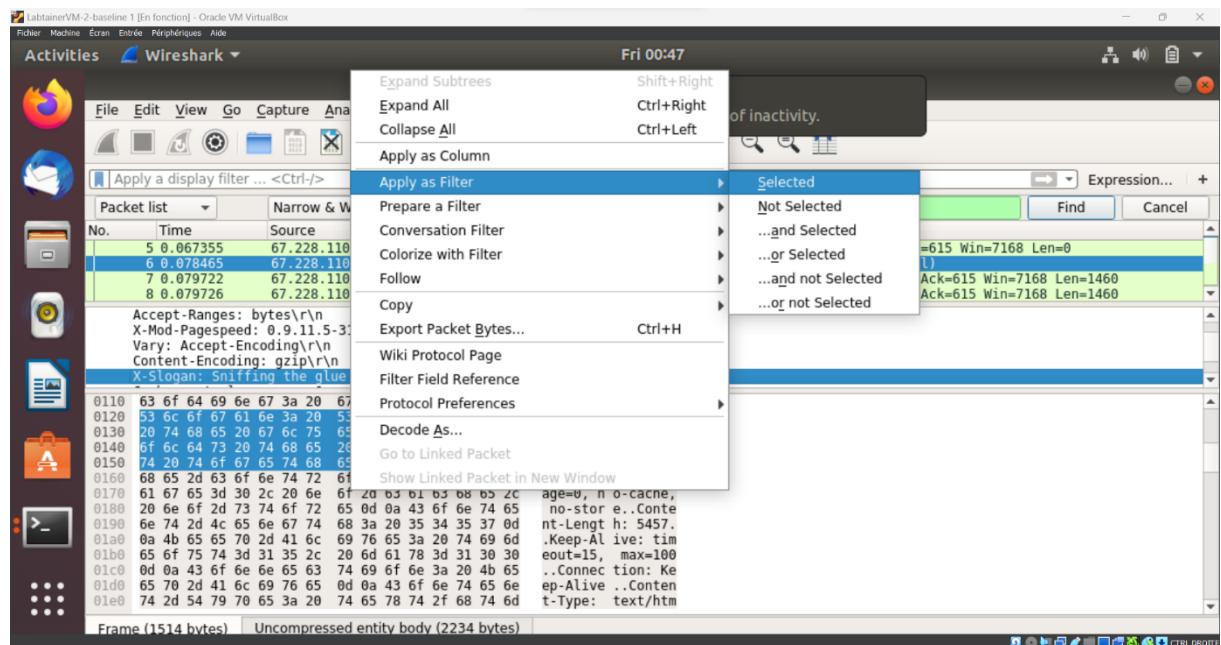
En défilant dans le flux, nous avons cherché le message caché de Gerald Combs, (le créateur de Wireshark). Ce message commence par X-Slogan.

X-Slogan: Sniffing the glue that holds the Internet together.

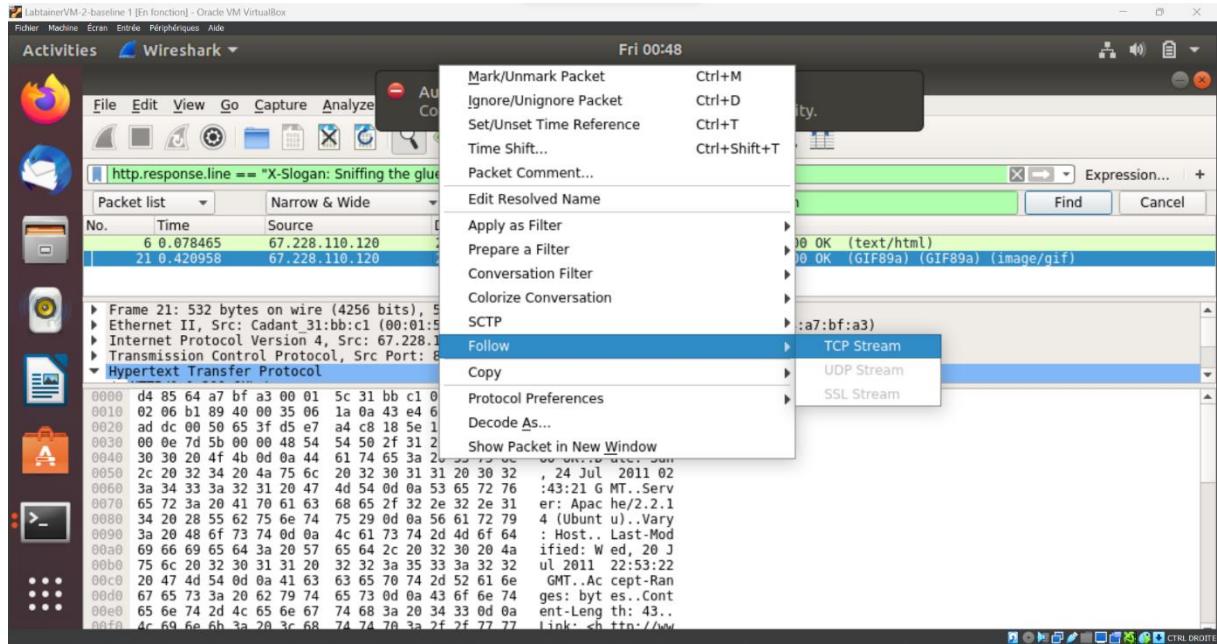
Après avoir trouvé le message, nous avons fermé (bouton close) cette page et enlevé le filtre appliqué précédemment.



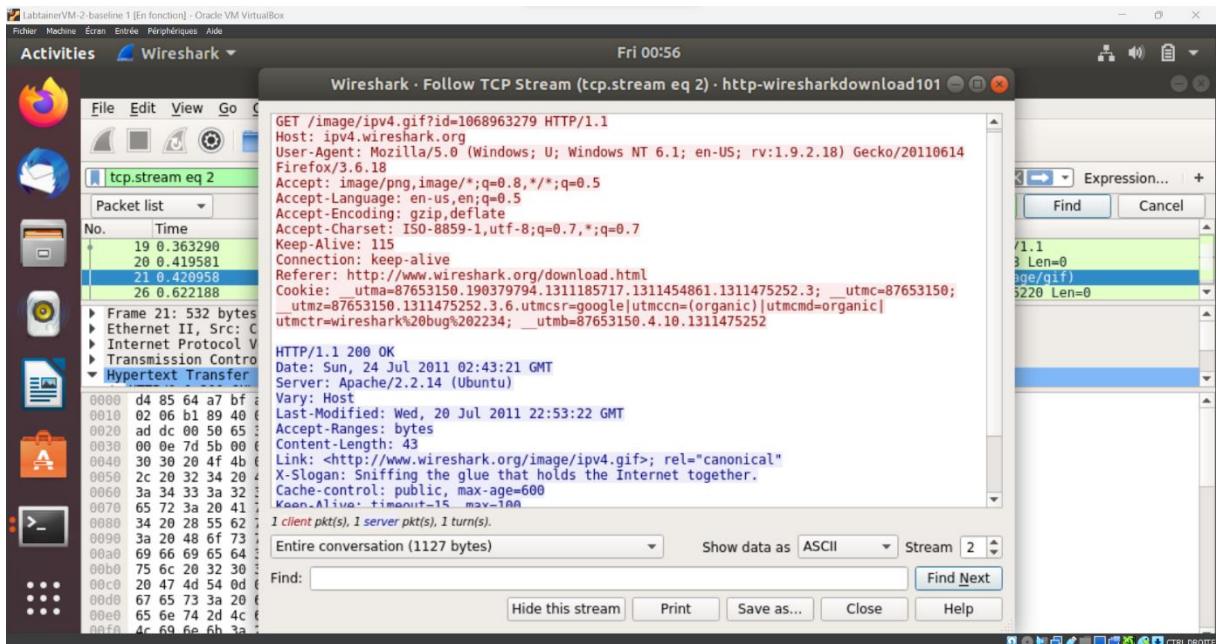
Nous avons ensuite appliqué un nouveau filtre d'affichage "xslogan" pour sélectionner uniquement les trames contenant xslogan. Après avoir sélectionné la trame, nous avons choisi Apply as Filter → Selected.



Seules deux trames sont alors affichées sur Wireshark, chacune avec un message différent. Nous avons pris l'une d'entre elles et fait Follow → TCP Stream pour examiner les en-têtes HTTP échangés entre les hôtes.



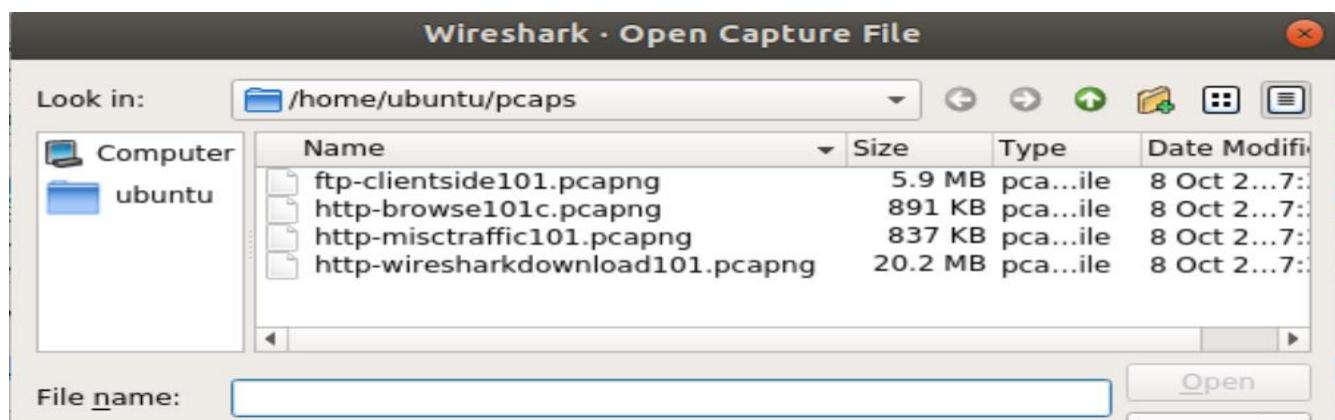
Normalement le message n'ai pas le même et on devrais avoir trois trames, du a une erreur sur la machine virtuel.



Partie 4 :

Extraire un fichier binaire d'une session FTP

Lancer Wireshark et ouvrez le fichier : pcaps/http-misctraffic101.pcapng



Choisissez une trame de flux de canal de commandes puis cliquez avec le bouton droit Follow —TCPstream, cliquez sur le bouton HideThis Stream. Ceci ferme la fenêtre du flux TCP et applique un filtre d'exclusion.

The screenshot shows a Wireshark window titled "Wireshark · Follow TCP Stream (tcp.stream eq 0) · ftp-clientside101". The main pane displays a sequence of ASCII text representing an FTP session. The server (vsFTPD) initiates the session with a 220 response. The client (anonymous user) responds with a USER command. The server prompts for a password with a 331 response. The client responds with a PASS command. The server confirms login with a 230 response. The client then issues a PORT command to the server's IP address (192.168.0.101) and port 206. The server responds with a 200 PORT command successful message, suggesting the use of PASV. The client performs an NLST command to request a directory listing, which the server responds to with a 150 message. The client then switches to Binary mode with a TYPE I command, followed by a 200 response. The client issues a RETR command for the file "pantheon.jpg", and the server responds with a 150 message indicating the opening of a binary connection for the file. The client sends the file with a 226 File send OK message, and the server responds with a 221 Goodbye message. At the bottom of the window, there are controls for "Entire conversation (505 bytes)", "Show data as ASCII", "Stream 0", a search bar for "Find:", and buttons for "Hide this stream", "Print", "Save as...", "Close", and "Help".

```
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.
```

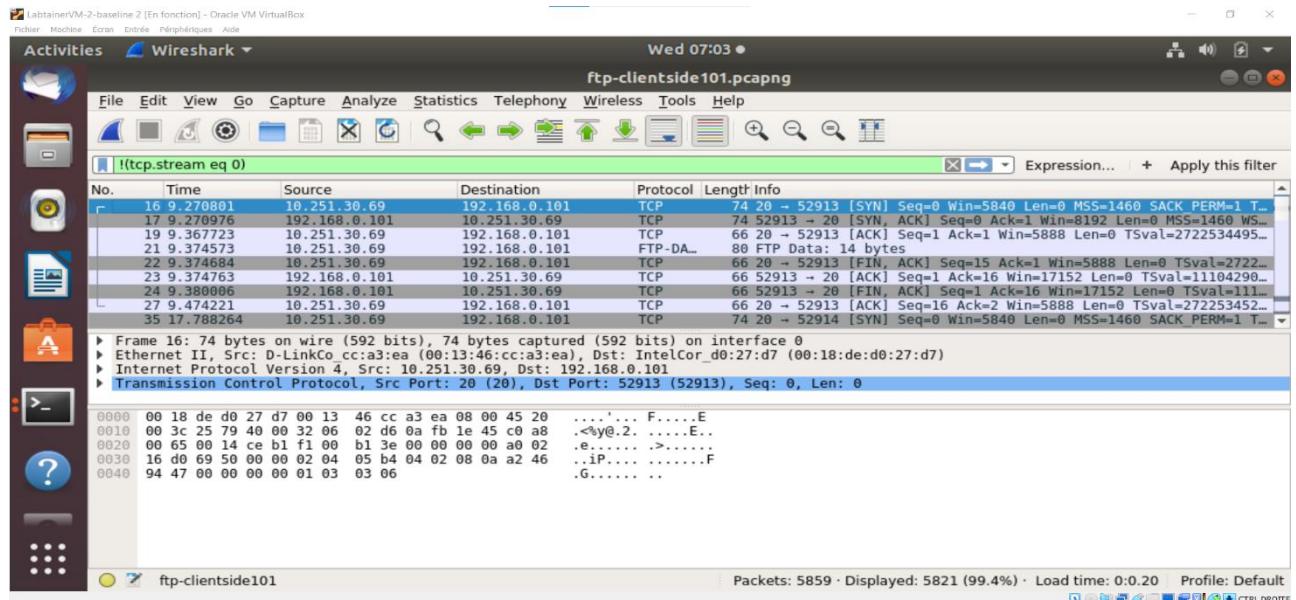
8 client pkt(s), 11 server pkt(s), 16 turn(s).

Entire conversation (505 bytes) Show data as ASCII Stream 0

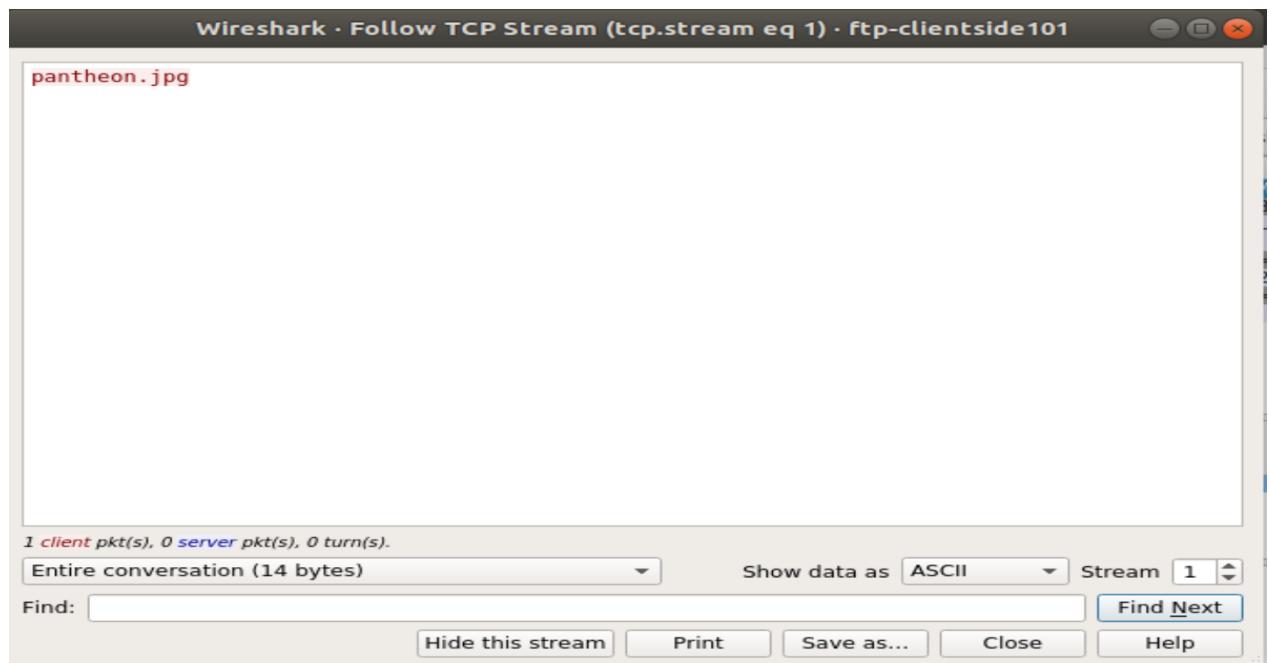
Find: | Find Next

Hide this stream Print Save as... Close Help

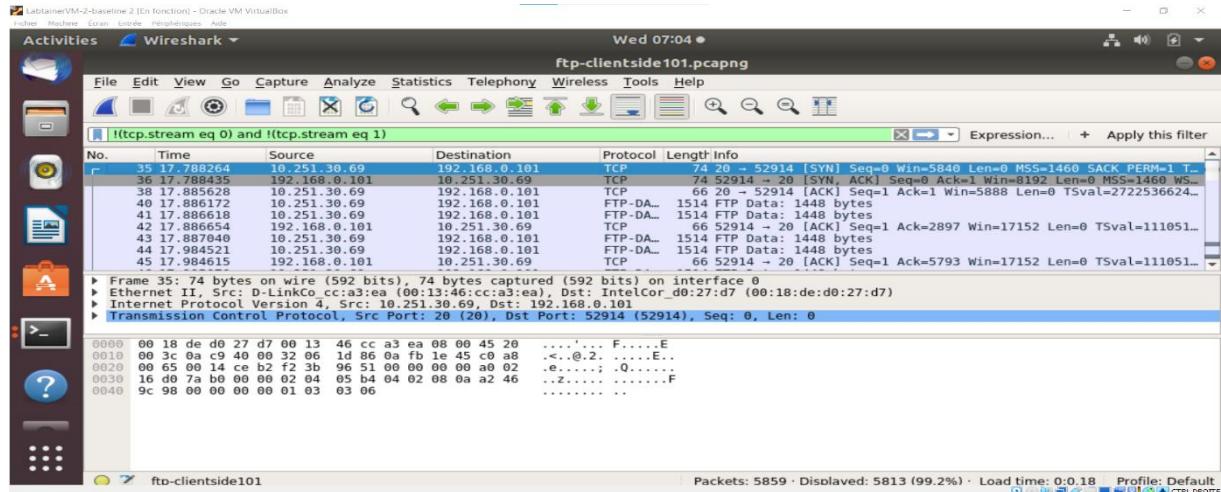
Cliquez avec le bouton droit de la souris sur latrame16 et sélectionnez Follow — TCPstream



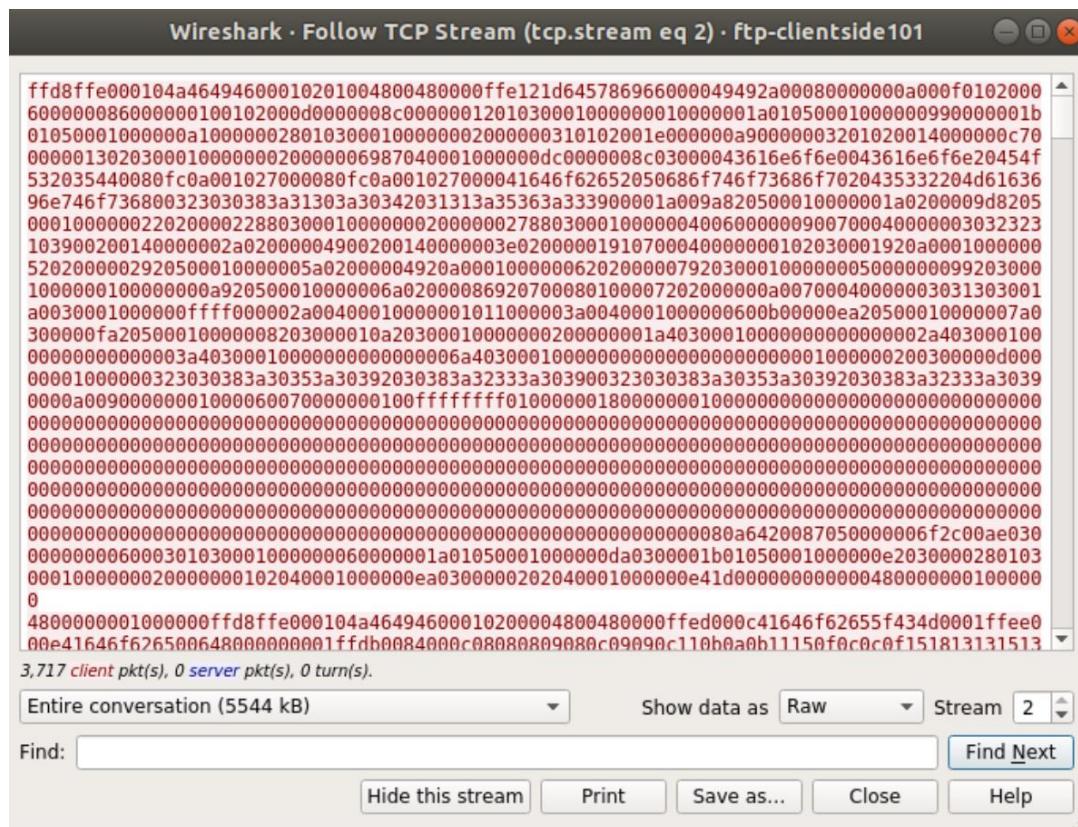
Cette liste de flux indique qu'il n'y a qu'un seul fichier dans le répertoire.

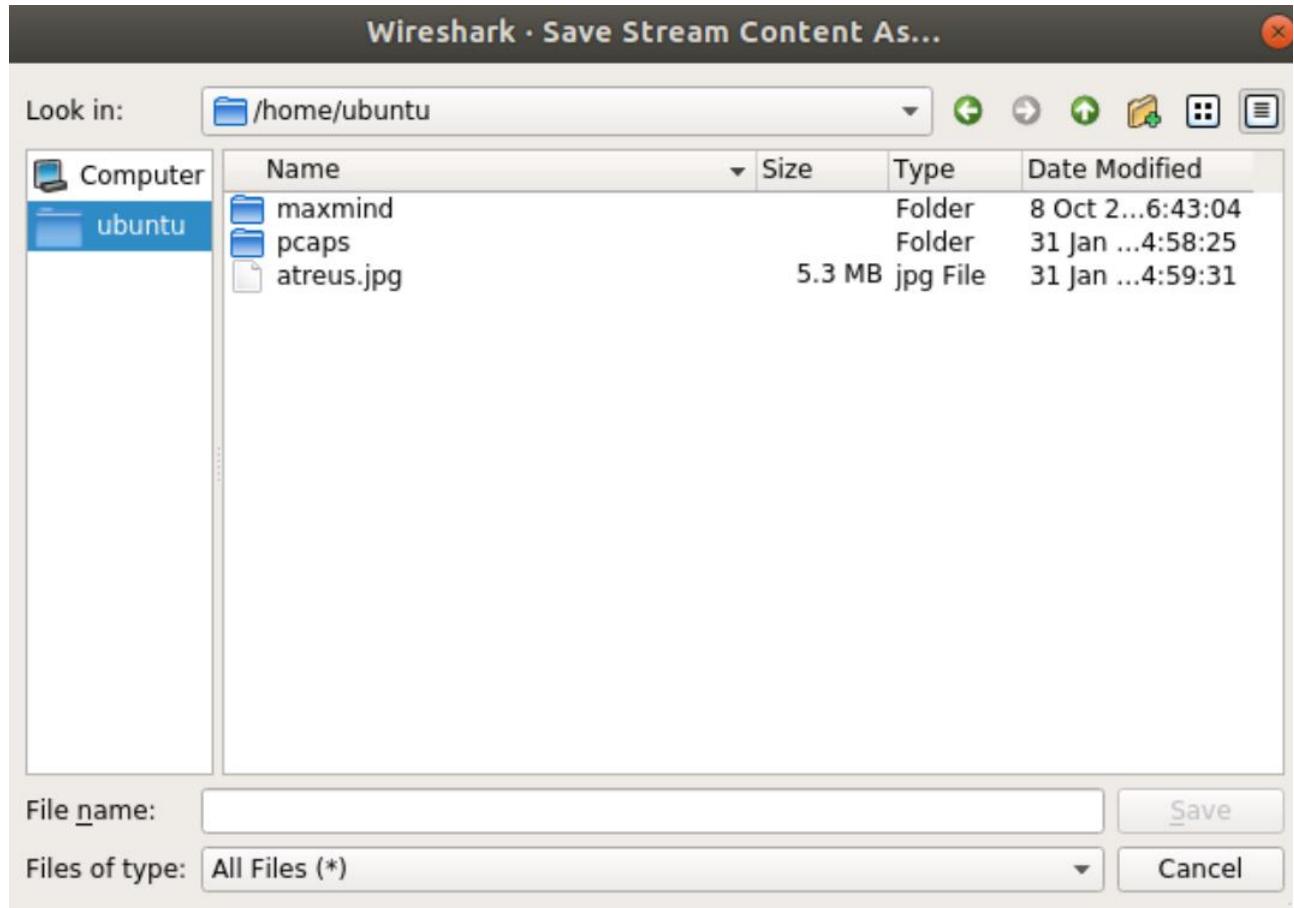


Cliquez avec le bouton droit de la souris sur n'importe quelle trame et sélectionnez Follow —TCP stream.



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





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.

```
ubuntu@ws:~$ ls -l
total 5432
-rw-rw-r-- 1 ubuntu ubuntu 5544612 Jan 31 14:59 atreus.jpg
drwxrwxr-x 1 ubuntu ubuntu    4096 Oct  8  2019 maxmind
drwxr-x--- 1 ubuntu ubuntu    4096 Jan 31 14:58 pcaps
ubuntu@ws:~$ firefox
```

Cela vous affiche alors l'image :

