

Travaux pratiques – Utiliser Wireshark pour examiner le trafic HTTP et HTTPS

Objectifs

Partie 1 : capturer et afficher le trafic HTTP

Partie 2 : capturer et afficher le trafic HTTPS

Contexte/scénario

Le protocole HTTP (HyperText Transfer Protocol) est un protocole de couche application qui présente des données via un navigateur web. Avec HTTP, aucune mesure de protection n'est appliquée pour les données échangées entre deux appareils qui communiquent.

Avec HTTPS, le chiffrement est assuré par un algorithme mathématique. Cet algorithme cache la véritable signification des données échangées. Pour cela des certificats, présentés ultérieurement dans ces travaux pratiques, sont utilisés.

Qu'il s'agisse de HTTP ou de HTTPS, il est recommandé d'échanger des données uniquement avec des sites web de confiance. Car même si un site utilise HTTPS cela ne signifie pas qu'il est sécurisé. Les hackers utilisent couramment HTTPS pour cacher leurs activités.

Au cours de ces travaux pratiques, vous allez explorer et capturer le trafic HTTP et HTTPS à l'aide de Wireshark.

Ressources requises

- Poste de travail virtuel CyberOps
- Connexion Internet

Partie 1 : Capture et affichage du trafic HTTP

Dans cette partie, vous allez utiliser **tcpdump** pour capturer le contenu du trafic HTTP. Vous allez utiliser des options de commande pour enregistrer le trafic dans un fichier de capture (pcap) de paquets. Les enregistrements peuvent ensuite être analysés à l'aide de différentes applications qui lisent les fichiers pcap comme Wireshark.

Étape 1 : Démarrez la machine virtuelle et connectez-vous.

Démarrez le poste de travail virtuel CyberOps. Utilisez les informations d'identification d'utilisateur suivantes :

Nom d'utilisateur : **analyst** Mot

de passe : **cyberops**

Étape 2 : Ouvrez un terminal et lancez tcpdump.

- Ouvrez une application de terminal et saisissez la commande **ifconfig**.

```
[analyst@secOps ~]$ ifconfig
```

- Répertoriez les interfaces et leurs adresses IP affichées dans la sortie d'ifconfig.

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.203.101.223 netmask 255.255.0.0 broadcast 10.203.255.255
    inet6 fe80::a00:27ff:fe82:d498 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:82:d4:98 txqueuelen 1000 (Ethernet)
    RX packets 47128 bytes 3700818 (3.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 140 bytes 16081 (15.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- c. Dans l'application de terminal, saisissez la commande **sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap**. Saisissez le mot de passe **cyberops** pour l'utilisateur analyst lorsque vous y êtes invité.

```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap [sudo]
password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size
262144 bytes
```

```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 b
ytes
```

Cette commande démarre tcpdump et enregistre le trafic réseau sur l'interface **enp0s3**.

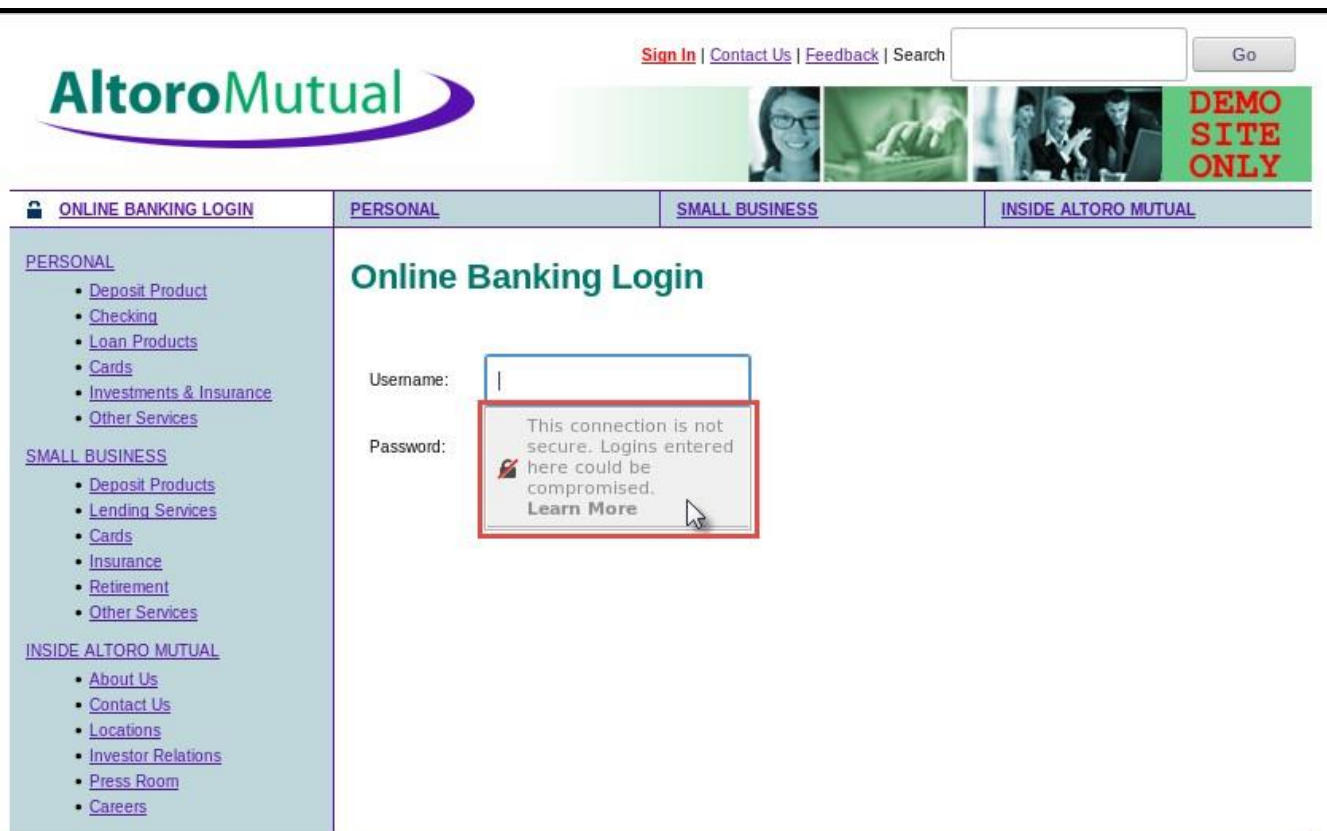
L'option de commande **-i** permet de spécifier l'interface. Si cette option n'est pas spécifiée, la commande tcpdump capturera tout le trafic sur toutes les interfaces.

L'option de commande **-s** spécifie la longueur de la capture pour chaque paquet. Vous devez limiter la longueur de la capture (snaplen) avec la plus petite valeur possible de manière à capturer les informations de protocole qui vous intéressent. Lorsque la longueur est définie sur 0, elle est en fait définie avec la valeur par défaut 262144, pour des raisons de rétrocompatibilité avec les versions plus anciennes de tcpdump.

L'option de commande **-w** sert à écrire le résultat de la commande tcpdump dans un fichier. En ajoutant l'extension .pcap, les systèmes d'exploitation et les applications pourront lire ce fichier. Tout le trafic enregistré sera enregistré dans le fichier httpdump.pcap dans le répertoire de base de l'utilisateur analyst.

Utilisez les pages man de la commande tcpdump pour connaître l'utilisation des options de commande **-s** et **-w**.

- d. Ouvrez un navigateur web à partir de la barre de lancement dans le poste de travail Linux. Accédez à www.altoromutual.com/bank/login.aspx



Étant donné que ce site web utilise le protocole HTTP, le trafic n'est pas chiffré. Cliquez sur le champ de nom d'utilisateur pour afficher le message d'avertissement.

- e. Saisissez le nom d'utilisateur **Admin** avec le mot de passe **Admin** et cliquez sur **Login**. f.

Fermez le navigateur web virtuel.

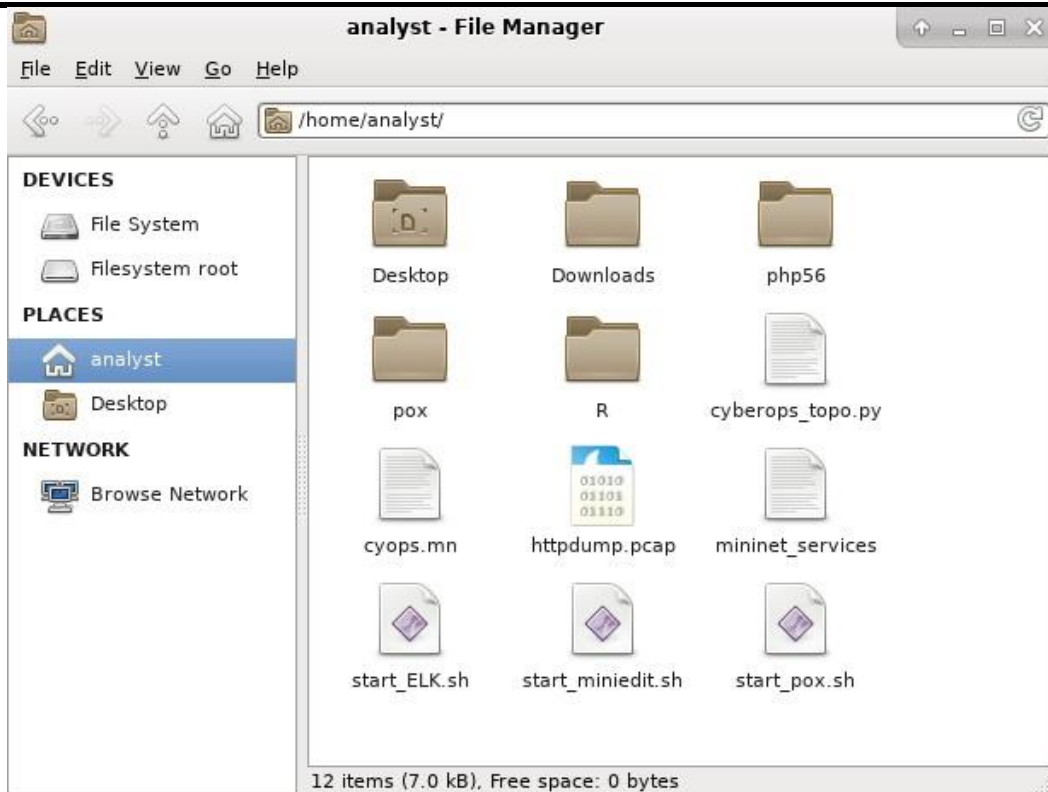
- g. Revenez à la fenêtre de terminal où tcpdump est en cours d'exécution. Appuyez sur **Ctrl+C** pour arrêter la capture des paquets.

Étape 3 : Affichez la capture HTTP.

La commande tcpdump, exécutée à l'étape précédente, a enregistré la sortie dans un fichier nommé httpdump.pcap. Ce fichier se trouve dans le répertoire de base de l'utilisateur **analyst**.

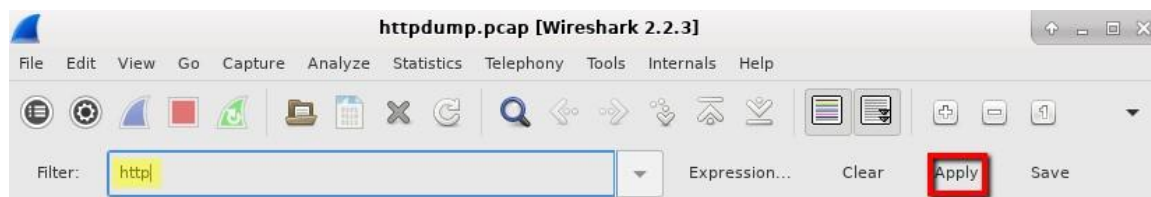
- a. Cliquez sur l'icône du gestionnaire de fichiers sur le bureau et accédez au dossier de base pour l'utilisateur **analyst**. Double-cliquez sur le fichier **httpdump.pcap** pour l'ouvrir dans Wireshark.

Travaux pratiques – Utiliser Wireshark pour examiner le trafic HTTP et HTTPS

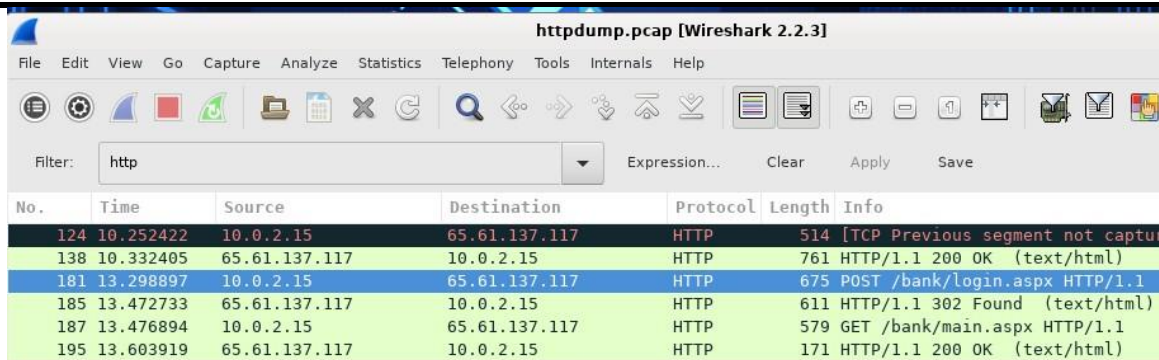


Filter:		http		Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info	
55	88.809921	192.168.1.21	34.107.221.82	HTTP	354	GET /success.txt HTTP/1.1	
57	88.818444	34.107.221.82	192.168.1.21	HTTP	282	HTTP/1.1 200 OK (text/plain)	
101	90.319803	192.168.1.21	96.17.206.24	OCSP	496	Request	
104	90.324629	192.168.1.21	96.17.206.24	OCSP	496	Request	
106	90.332680	96.17.206.24	192.168.1.21	OCSP	954	Response	

- b. Dans l'application Wireshark, recherchez **http** et cliquez sur **Apply**.

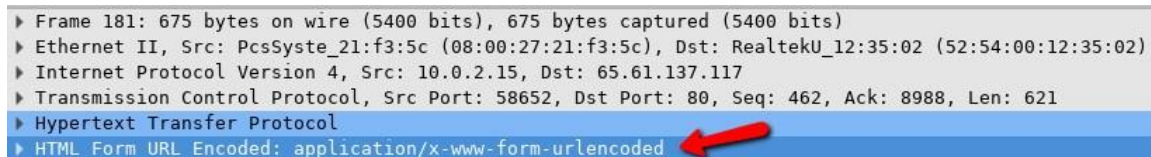


- c. Naviguez dans les différents messages HTTP, puis sélectionnez le message **POST**.



No.	Time	Source	Destination	Protocol	Length	Info
124	10.252422	10.0.2.15	65.61.137.117	HTTP	514	[TCP Previous segment not captured]
138	10.332405	65.61.137.117	10.0.2.15	HTTP	761	HTTP/1.1 200 OK (text/html)
181	13.298897	10.0.2.15	65.61.137.117	HTTP	675	POST /bank/login.aspx HTTP/1.1
185	13.472733	65.61.137.117	10.0.2.15	HTTP	611	HTTP/1.1 302 Found (text/html)
187	13.476894	10.0.2.15	65.61.137.117	HTTP	579	GET /bank/main.aspx HTTP/1.1
195	13.603919	65.61.137.117	10.0.2.15	HTTP	171	HTTP/1.1 200 OK (text/html)

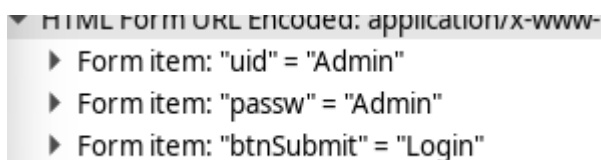
- d. Le message s'affiche dans la fenêtre inférieure. Développez la section **HTML Form URL Encoded: application/x-www-form-urlencoded**.



```

▶ Frame 181: 675 bytes on wire (5400 bits), 675 bytes captured (5400 bits)
▶ Ethernet II, Src: PcsSyste_21:f3:5c (08:00:27:21:f3:5c), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 65.61.137.117
▶ Transmission Control Protocol, Src Port: 58652, Dst Port: 80, Seq: 462, Ack: 8988, Len: 621
▶ Hypertext Transfer Protocol
▶ HTML Form URL Encoded: application/x-www-form-urlencoded
    
```

Quelles sont les deux informations affichées ? **les identifiants ainsi que le mot de passe**



```

▶ HTML Form URL Encoded: application/x-www-
▶ Form item: "uid" = "Admin"
▶ Form item: "passwd" = "Admin"
▶ Form item: "btnSubmit" = "Login"
    
```

- e. Fermez l'application Wireshark.

Partie 2 : Capturer et afficher le trafic HTTPS

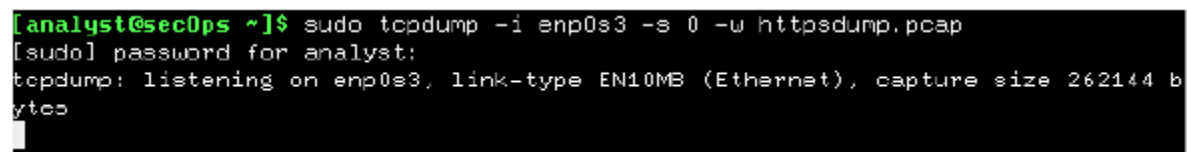
Vous allez maintenant utiliser tcpdump depuis la ligne de commande d'un poste de travail Linux pour capturer le trafic HTTPS. Après avoir démarré tcpdump, vous allez générer le trafic HTTPS et tcpdump enregistrera le contenu du trafic réseau. Ce contenu sera également analysé à l'aide de Wireshark.

Étape 1 : Lancez tcpdump dans un terminal.

- a. Dans l'application de terminal, saisissez la commande **sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap**. Saisissez le mot de passe **cyberops** pour l'utilisateur analyst lorsque vous y êtes invité.

```

[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size
262144 bytes
    
```



```

[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
    
```

Cette commande démarre tcpdump et enregistre le trafic réseau sur l'interface **enp0s3** du poste de travail Linux. Si votre interface est différente de celle d'enp0s3, modifiez-la lorsque vous utilisez la commande ci-dessus.

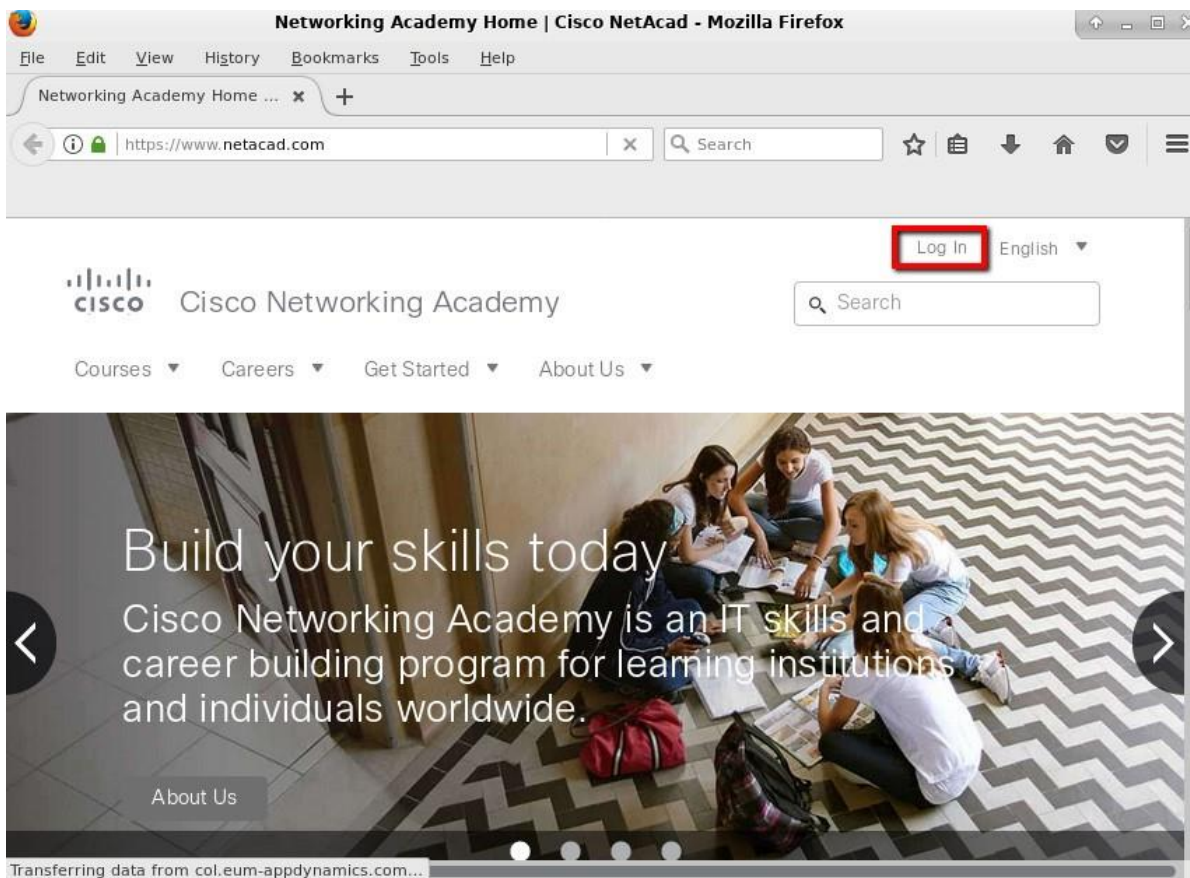
Travaux pratiques – Utiliser Wireshark pour examiner le trafic HTTP et HTTPS

Tout le trafic enregistré sera enregistré dans le fichier **httpsdump.pcap** dans le répertoire de base de l'utilisateur analyst.

- b. Ouvrez un navigateur web à partir de la barre de lancement dans le poste de travail Linux. Accédez à www.netacad.com.

Que remarquez-vous à propos de l'URL du site web ? On remarque que celle-ci est protégé/chiffé avec le symbole cadenas vert car elle est en https

- c. Cliquez sur **Log in**.



- d. Saisissez votre nom d'utilisateur et votre mot de passe pour NetAcad. Cliquez sur **Log In**.

Cisco Networking Academy Log In

Email address or screen name

your_username

Password

●●●●●●●●

Cancel Log In

[Forgot Password](#) [Resend Activation Email](#) [Redeem Seat Token](#)

e.

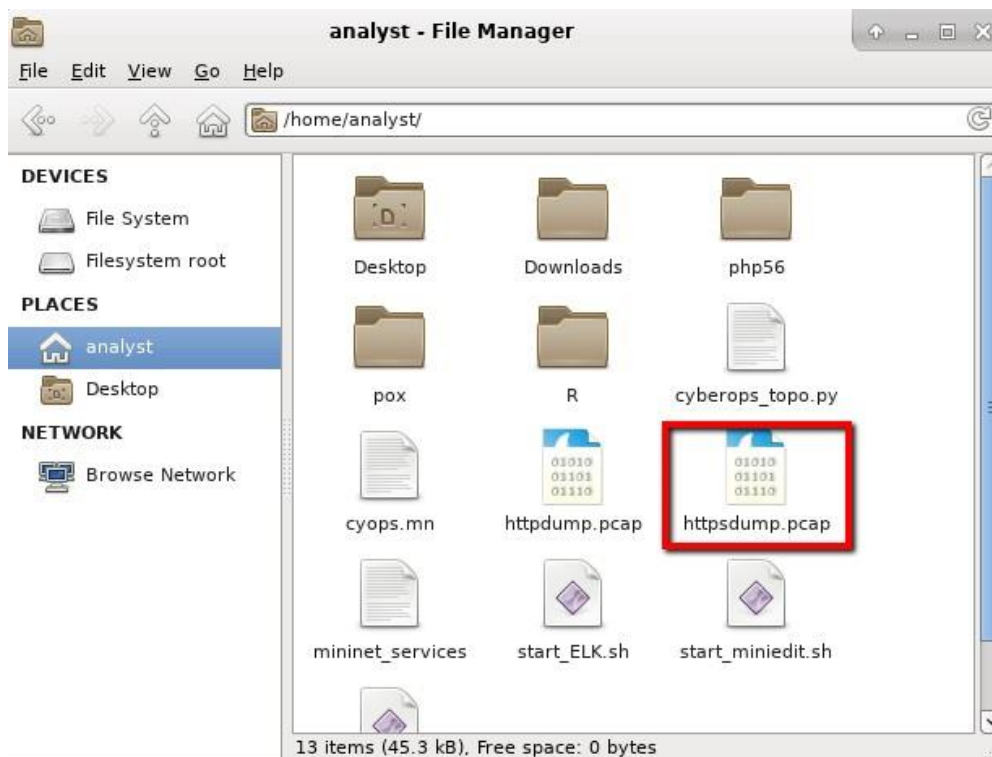
Fermez le navigateur web virtuel.

- f. Revenez à la fenêtre de terminal où tcpdump est en cours d'exécution. Appuyez sur **Ctrl+C** pour arrêter la capture des paquets.

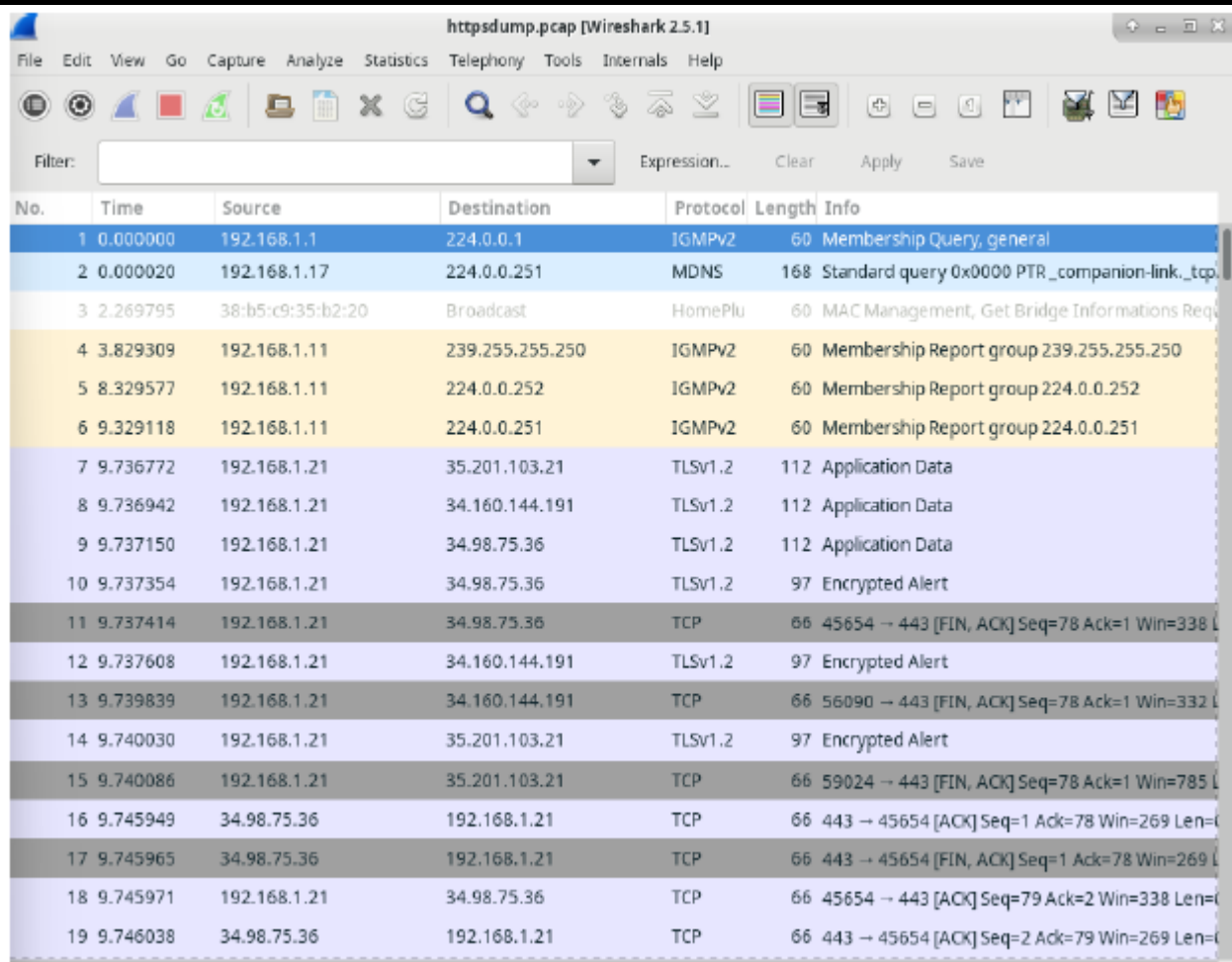
Étape 2 : Affichez la capture HTTPS.

La commande tcpdump exécutée à l'étape 1 a enregistré la sortie dans un fichier nommé httpsdump.pcap. Ce fichier se trouve dans le répertoire de base de l'utilisateur **analyst**.

- a. Cliquez sur l'icône du système de fichiers sur le bureau et recherchez le dossier de base de l'utilisateur analyst. Ouvrez le fichier **httpsdump.pcap**.



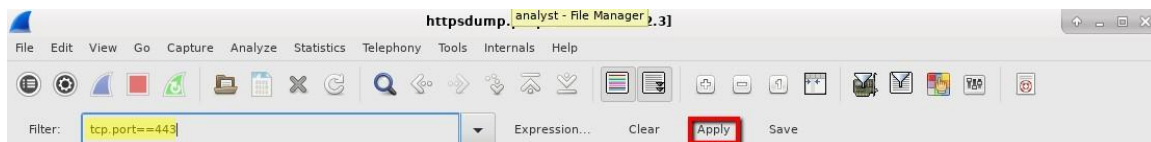
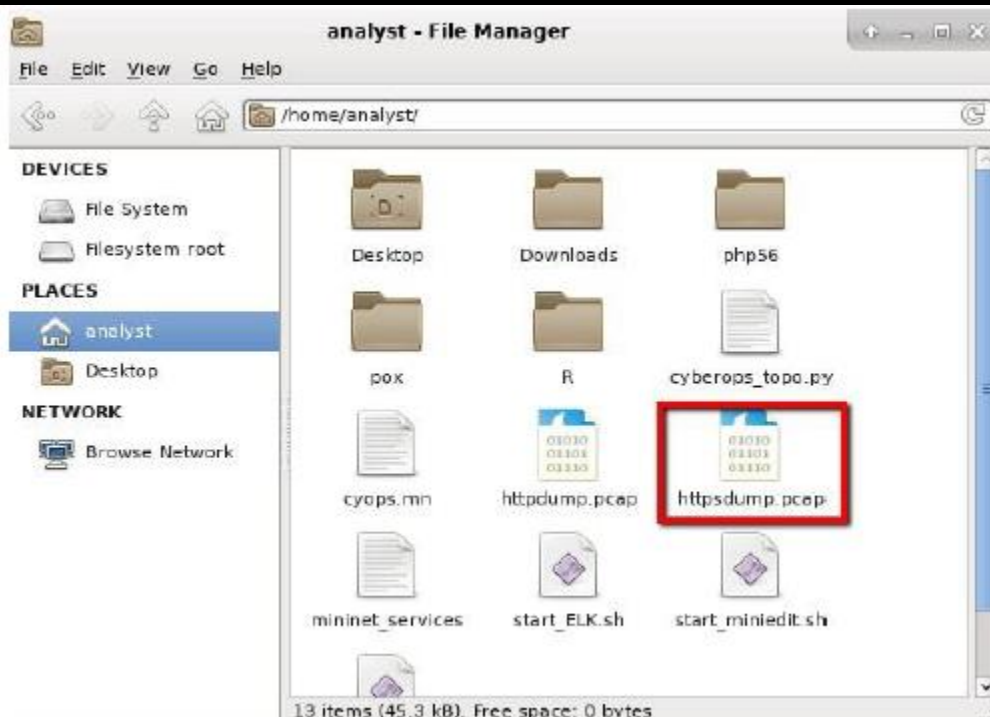
Travaux pratiques – Utiliser Wireshark pour examiner le trafic HTTP et HTTPS



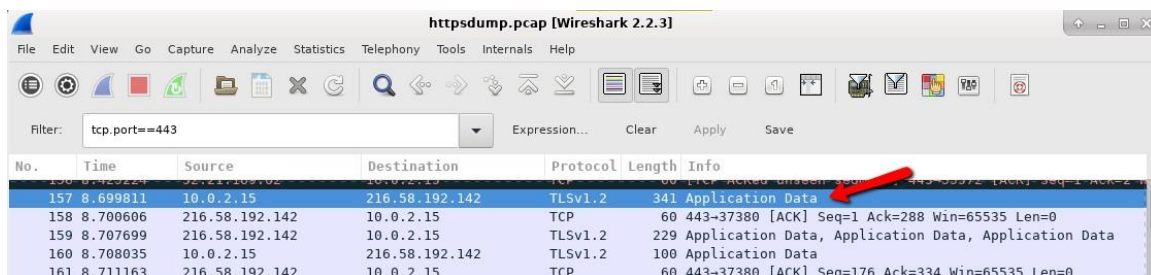
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.1	224.0.0.1	IGMPv2	60	Membership Query, general
2	0.000020	192.168.1.17	224.0.0.251	MDNS	168	Standard query 0x0000 PTR_companion-link._tcp
3	2.269795	38:b5:c9:35:b2:20	Broadcast	HomePlu	60	MAC Management, Get Bridge Informations Req
4	3.829309	192.168.1.11	239.255.255.250	IGMPv2	60	Membership Report group 239.255.255.250
5	8.329577	192.168.1.11	224.0.0.252	IGMPv2	60	Membership Report group 224.0.0.252
6	9.329118	192.168.1.11	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
7	9.736772	192.168.1.21	35.201.103.21	TLSv1.2	112	Application Data
8	9.736942	192.168.1.21	34.160.144.191	TLSv1.2	112	Application Data
9	9.737150	192.168.1.21	34.98.75.36	TLSv1.2	112	Application Data
10	9.737354	192.168.1.21	34.98.75.36	TLSv1.2	97	Encrypted Alert
11	9.737414	192.168.1.21	34.98.75.36	TCP	66	45654 → 443 [FIN, ACK] Seq=78 Ack=1 Win=338 L
12	9.737608	192.168.1.21	34.160.144.191	TLSv1.2	97	Encrypted Alert
13	9.739839	192.168.1.21	34.160.144.191	TCP	66	56090 → 443 [FIN, ACK] Seq=78 Ack=1 Win=332 L
14	9.740030	192.168.1.21	35.201.103.21	TLSv1.2	97	Encrypted Alert
15	9.740086	192.168.1.21	35.201.103.21	TCP	66	59024 → 443 [FIN, ACK] Seq=78 Ack=1 Win=785 L
16	9.745949	34.98.75.36	192.168.1.21	TCP	66	443 → 45654 [ACK] Seq=1 Ack=78 Win=269 Len=0
17	9.745965	34.98.75.36	192.168.1.21	TCP	66	443 → 45654 [FIN, ACK] Seq=1 Ack=78 Win=269 L
18	9.745971	192.168.1.21	34.98.75.36	TCP	66	45654 → 443 [ACK] Seq=79 Ack=2 Win=338 Len=0
19	9.746038	34.98.75.36	192.168.1.21	TCP	66	443 → 45654 [ACK] Seq=2 Ack=79 Win=269 Len=0

- b. Dans l'application Wireshark, agrandissez la fenêtre de capture verticalement, puis filtrez par trafic HTTPS via le port 443.

Saisissez **tcp.port==443** comme filtre, puis cliquez sur **Apply**.



- c. Naviguez parmi les différents messages HTTPS, puis sélectionnez un message **Application Data**.



- d. Le message s'affiche dans la fenêtre inférieure.

Par quoi la section HTTP qui était dans le fichier de capture précédent a-t-elle été remplacée ? La section **http** a été remplacée par la fenêtre « section **Secure Sockets Layer** » avec comme protocole **TLSv1.2**

- e. Développez complètement la section **Secure Sockets Layer**.

Travaux pratiques – Utiliser Wireshark pour examiner le trafic HTTP et HTTPS

```
▶ Frame 157: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on interface 0
▶ Ethernet II, Src: PcsSyste_21:f3:5c (08:00:27:21:f3:5c), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 216.58.192.142
▶ Transmission Control Protocol, Src Port: 37380, Dst Port: 443, Seq: 1, Ack: 1, Len: 287
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 282
    Encrypted Application Data: 0000000000000000bed2031d6dabc4c685ca7854a009a7a56...
```

f.

Cliquez sur **Encrypted Application Data**.

Les données d'application sont-elles en texte clair ou dans un format lisible ? **Non, celle-ci sont cryptées**

g. Fermez toutes les fenêtres et arrêtez la machine virtuelle.

Remarques générales

1. Quels sont les avantages d'utiliser HTTPS plutôt que HTTP ?

HTTPS (Hypertext Transfer Protocol Secure) offre plusieurs avantages par rapport à HTTP (Hypertext Transfer Protocol) non sécurisé. :

- Il assure la sécurité des données grâce au cryptage,
- Garantit l'intégrité des données en transit,
- Améliore la confidentialité des utilisateurs,
- Assure l'authenticité des sites web et peut même améliorer le référencement

En résumé, HTTPS est essentiel pour une communication en ligne sécurisée, offrant une protection contre les attaques et garantissant la confiance des utilisateurs.

2. Tous les sites web qui utilisent le protocole HTTPS sont-ils considérés comme sécurisés ?

L'utilisation du protocole HTTPS ne garantit pas automatiquement la sécurité complète d'un site web. Bien que HTTPS offre une couche de protection en cryptant les données échangées entre le navigateur et le serveur, certains sites peuvent encore présenter des vulnérabilités. Des problèmes tels que des certificats SSL/TLS invalides, des contenus mixtes, des failles de sécurité sur le site ou des attaques de phishing peuvent compromettre la sécurité, même sur des sites HTTPS. Ainsi, il est essentiel pour les propriétaires de sites de prendre des mesures supplémentaires pour identifier et corriger les failles de sécurité afin de garantir la sécurité globale du site.