

Corrigé du laboratoire 1 : découvrir HTTP et FTP avec Wireshark

I. HTTP

Partie A

1. Quelle version de HTTP utilise votre navigateur? Quelle est celle utilisée par le serveur?
2. Quelles langues sont acceptées par votre navigateur?
3. Quelle sont les adresses IP de votre ordinateur et du serveur gaia.cs.umass.edu?
4. Quel est le code d'état retourné par le serveur?
5. Quand est ce que le fichier HTML demandé a été modifié pour la dernière fois?
6. Combien d'octets sont-ils envoyés au serveur?

3. Adresse IP du client

3. Adresse IP du serveur

1. Version HTTP

2. Langues supportées

4. Réponse

5. Dernière mise à jour

6. Taille du contenu

Partie B

No.	Time	Source	Destination	Protocol	Length	Info
1495	216.975471	192.168.1.6	91.228.167.103	HTTP	397	POST / HTTP/1.1
1676	257.767842	192.168.1.6	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
1681	257.929361	128.119.245.12	192.168.1.6	HTTP	1127	HTTP/1.1 200 OK (text/html)
1684	258.028514	192.168.1.6	128.119.245.12	HTTP	483	GET /pearson.png HTTP/1.1
1689	258.191772	128.119.245.12	192.168.1.6	HTTP	941	HTTP/1.1 200 OK (PNG)
1697	258.607604	192.168.1.6	128.119.245.12	HTTP	457	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
1832	260.131035	128.119.245.12	192.168.1.6	HTTP	584	HTTP/1.1 200 OK (JPEG JFIF image)

1. Combien de requêtes HTTP GET sont envoyées par votre navigateur?

Réponse : trois requêtes GET ont été envoyées, la première pour récupérer le fichier html de base, la deuxième pour récupérer l'image png et la troisième pour récupérer l'image jpeg.

2. Quelle est la destination de vos requêtes GET?
Réponse : Chacune des requêtes a été envoyée vers le serveur http ayant l'adresse 128.119.245.12.
3. Donnez les codes des réponses HTTP contenus dans les paquets envoyés par le serveur.
Réponse : Le code des réponses http est 200 OK.

Partie C

No.	Time	Source	Destination	Protocol	Length	Info
147	49.702152	192.168.1.3	128.119.245.12	HTTP	566	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.h
160	49.864905	128.119.245.12	192.168.1.3	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
235	80.005292	192.168.1.3	128.119.245.12	HTTP	651	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.h
240	80.227452	128.119.245.12	192.168.1.3	HTTP	583	HTTP/1.1 404 Not Found (text/html)

>	Frame 235: 651 bytes on wire (5208 bits), 651 bytes captured (5208 bits) on interface \Device\NPF_{2CAE4845-6B5F-4108-A6E7-3012946578}
>	Ethernet II, Src: LiteonTe_e2:53:fd (30:10:b3:e2:53:fd), Dst: HuaweiTe_d6:50:62 (c4:07:2f:d6:50:62)
>	Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
>	Transmission Control Protocol, Src Port: 52612, Dst Port: 80, Seq: 1, Ack: 1, Len: 597
▼	Hypertext Transfer Protocol
>	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
	Host: gaia.cs.umass.edu\r\n
	Connection: keep-alive\r\n
	Cache-Control: max-age=0\r\n
>	Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcmcs=\r\n
	Upgrade-Insecure-Requests: 1\r\n
	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36\r\n
	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange\r\n
	Accept-Encoding: gzip, deflate\r\n
	Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
	\r\n
	[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html]
	[HTTP request 1/1]
	[Response in frame: 240]

1. Quelle a été la réponse du serveur à la première requête GET du navigateur?
Réponse : La réponse du serveur contient le code 401 qui demande une authentification du client (401 Authorization required).
2. Le deuxième GET du navigateur contient un nouveau champ, lequel?
Réponse : Il contient le champ « Authorization » qui contient les informations d'authentification fournies par le client.
3. Le nom d'utilisateur ainsi que le mot de passe que vous avez fourni sont-ils chiffrés? (indice : essayez de vérifier l'encodage du contenu du nouveau champ sur le site <https://www.base64decode.org/>).
Réponse : Les informations d'authentification ne sont pas chiffrées, elles sont seulement encodées en base64. En copiant le contenu du champ sur le décodeur disponible à l'adresse fournie, il est possible de récupérer les informations en ASCII.

Decode from Base64 format

Simply enter your data then push the decode button.

d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms

i For encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page.

▼

Source character set.

☐ Decode each line separately (useful for multiple entries).

Live mode OFF

Decodes in real-time when you type or paste (supports only UTF-8 character set).

[← DECODE →](#)

Decodes your data into the textarea below.

wireshark-students:network

wireshark-students:network

II. FTP

1. Quel est le protocole de couche transport utilisé par FTP.

ftp						
No.	Time	Source	Destination	Protocol	Length	Info
71	9.272545	209.51.188.20	192.168.1.6	FTP	81	Response: 220 GNU FTP server ready.
72	9.273634	192.168.1.6	209.51.188.20	FTP	64	Request: AUTH TLS
74	9.424167	209.51.188.20	192.168.1.6	FTP	92	Response: 530 Please login with USER and PASS.
75	9.424573	192.168.1.6	209.51.188.20	FTP	64	Request: AUTH SSL
76	9.572492	209.51.188.20	192.168.1.6	FTP	92	Response: 530 Please login with USER and PASS.
77	9.595534	192.168.1.6	209.51.188.20	FTP	70	Request: USER anonymous

> Frame 77: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{2CAE4845-6B5F-4108-A6E7-3012946578EB}, id 0
> Ethernet II, Src: LiteonTe_e2:53:fd (30:10:b3:e2:53:fd), Dst: HuaweiTe_d6:50:62 (c4:07:2f:d6:50:62)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 209.51.188.20
> Transmission Control Protocol, Src Port: 55798, Dst Port: 21, Seq: 21, Ack: 104, Len: 16
> File Transfer Protocol (FTP)
[Current working directory:]

Réponse : Le protocole de couche transport utilisé par FTP est TCP (Transmission Control Protocol).

2. D'après les paquets échangés, déterminez l'adresse IP du client et l'adresse IP du serveur.

Réponse : L'adresse IP du client est 192.168.1.6 et l'adresse IP du serveur est 209.51.188.20.

3. Est-ce que le client a utilisé un nom d'utilisateur pour se connecter? Si oui lequel?

Réponse : Le client utilise un accès anonyme lors de l'authentification auprès du serveur. Par conséquent, le nom d'utilisateur utilisé est « anonymous ». (Voir le paquet 77 de la capture ci-haut, qui contient la commande ftp « USER ».)

4. Est-ce que le client a utilisé un mot de passe pour se connecter? Si oui lequel?

Réponse : Non, le client n'utilise pas un mot de passe pour se connecter.

5. En analysant les paquets FTP, quels sont les numéros de port utilisés par le serveur? Quels sont ceux utilisés par le client?

ip.addr == 209.51.188.20						
No.	Time	Source	Destination	Protocol	Length	Info
125	10.782104	209.51.188.20	192.168.1.6	FTP	85	Response: 200 Switching to Binary mode.
126	10.782421	192.168.1.6	209.51.188.20	FTP	60	Request: PASV
127	10.927412	209.51.188.20	192.168.1.6	FTP	105	Response: 227 Entering Passive Mode (209,51,188,20,105,41).
128	10.928808	192.168.1.6	209.51.188.20	FTP	60	Request: LIST
129	10.930265	192.168.1.6	209.51.188.20	TCP	66	55799 → 26921 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
130	11.077003	209.51.188.20	192.168.1.6	TCP	66	26921 → 55799 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1362 SACK_PERM=1 WS=128
131	11.077253	192.168.1.6	209.51.188.20	TCP	54	55799 → 26921 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
132	11.112759	209.51.188.20	192.168.1.6	TCP	54	21 → 55798 [ACK] Seq=1597 Ack=74 Win=29312 Len=0
133	11.223114	209.51.188.20	192.168.1.6	FTP	93	Response: 150 Here comes the directory listing.
134	11.228509	209.51.188.20	192.168.1.6	FTP-DA...	1388	FTP Data: 1334 bytes (PASV) (LIST)
135	11.228852	209.51.188.20	192.168.1.6	TCP	54	26921 → 55799 [FIN, ACK] Seq=1335 Ack=1 Win=29312 Len=0
136	11.228999	192.168.1.6	209.51.188.20	TCP	54	55799 → 26921 [ACK] Seq=1 Ack=1335 Win=4192896 Len=0
137	11.229030	192.168.1.6	209.51.188.20	TCP	54	55799 → 26921 [ACK] Seq=1 Ack=1336 Win=4192896 Len=0
138	11.229950	192.168.1.6	209.51.188.20	TCP	54	55799 → 26921 [FIN, ACK] Seq=1 Ack=1336 Win=4192896 Len=0
139	11.264122	192.168.1.6	209.51.188.20	TCP	54	55798 → 21 [ACK] Seq=74 Ack=1636 Win=131840 Len=0
140	11.378649	209.51.188.20	192.168.1.6	FTP	78	Response: 226 Directory send OK.

Réponse : Les numéros de port utilisés par le serveur sont 21 et 26921. Les numéros de port utilisés par le client sont 55798 et 55799.

6. Est-ce que les données contenues dans les messages FTP sont en clair ou chiffrées?

Réponse : Les données contenues dans les messages FTP sont clair.

7. Après quelle(s) commande(s), le serveur initie-t-il une connexion pour l'échange de données?

Réponse : Après la commande « LIST », le serveur initie une connexion de données.

