

INF4032 – Réseaux IP HTTP et Système de fichiers



1) Pratique

Exercice 1 : Mise en place et étude des protocoles historiques

Arrêtez le service de gestion automatique du réseau de Kali (la distribution linux installée sur votre PC).
Exécutez la commande : `# service network-manager stop`

Vérifiez que le service est arrêté. Exécutez la commande : `# service network-manager status`

En utilisant uniquement la commande `ifconfig`, mettez une adresse IP sur votre interface réseau reliée dont le câble est relié au mur. Les adresses IP des machines vous sont données par le chargé de TP pour éviter tout conflit.

```
(user@kali)-[~]
$ systemctl status NetworkManager
● NetworkManager.service - Network Manager
   Loaded: loaded (/lib/systemd/system/NetworkManager.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Fri 2021-09-17 16:35:55 CEST; 6min ago
     Docs: man:NetworkManager(8)
   Process: 492 ExecStart=/usr/sbin/NetworkManager --no-daemon (code=exited, status=0/SUCCESS)
    Main PID: 492 (code=exited, status=0/SUCCESS)
      CPU: 1.033s

Warning: some journal files were not opened due to insufficient permissions.

(user@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
```

```
(user@kali)-[~]
$ ip a del 10.0.2.10/24 dev eth0
RTNETLINK answers: Operation not permitted

(user@kali)-[~]
$ sudo ip a del 10.0.2.10/24 dev eth0

(user@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 90:3e:aa:14:5f:90 brd ff:ff:ff:ff:ff:ff
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 90:3e:aa:13:16:f7 brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 0c:b1:d7:31:2b:a0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.10/24 scope global eth2
        valid_lft forever preferred_lft forever
    inet6 fe80::e0b1:d7ff:fe31:2ba0/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(user@kali)-[~]
$ ping 10.0.2.254
PING 10.0.2.254 (10.0.2.254) 56(84) bytes of data:
64 bytes from 10.0.2.254: icmp_seq=1 ttl=64 time=0.335 ms
64 bytes from 10.0.2.254: icmp_seq=2 ttl=64 time=0.180 ms
64 bytes from 10.0.2.254: icmp_seq=3 ttl=64 time=0.201 ms
64 bytes from 10.0.2.254: icmp_seq=4 ttl=64 time=0.165 ms
64 bytes from 10.0.2.254: icmp_seq=5 ttl=64 time=0.162 ms
^C
--- 10.0.2.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4075ms
rtt min/avg/max/mdev = 0.162/0.208/0.335/0.064 ms

(user@kali)-[~]
$ vim /etc/resolv.conf
```

2 http

Exercice 2 : A la découverte du protocole http

En vous appuyant sur la capture que vous venez de réaliser, tracez, sur un graphe de séquence, les étapes de la connexion au site du CNRS. Faites apparaître les couches du modèle OSI concernées.

Wireshark - Packet 128 eth2

Frame 128: 426 bytes on wire (3408 bits), 426 bytes captured (3408 bits) on interface eth2, id 0

Ethernet II, Src: Hewlett-Packard (08:00:27:00:00:00), Dst: Hewlett-Packard (08:00:27:00:00:00)

Internet Protocol Version 4, Src: 10.0.2.33, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 48808, Dst Port: 80, Seq: 1, Ack: 360, Len: 360

Hypertext Transfer Protocol

GET /kurose/cover.jpg HTTP/1.1

Request Method: GET

Request URI: /kurose/cover.jpg

Request Version: HTTP/1.1

Host: manic.cs.umass.edu

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: keep-alive

Referer: http://gaia.cs.umass.edu/ethereal-labs/lab2-4.html

Cache-Control: no-cache

Full request URI: http://manic.cs.umass.edu/~kurose/cover.jpg

HTTP request 1/1

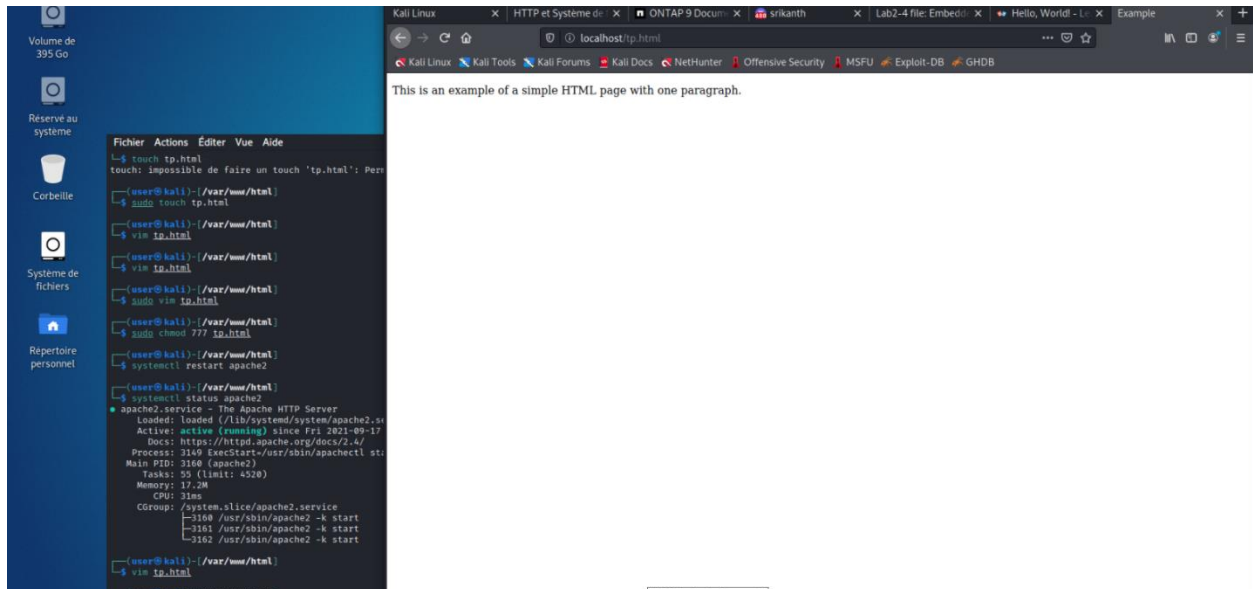
Response in frame 197

2) La requête utilise et la requête GET

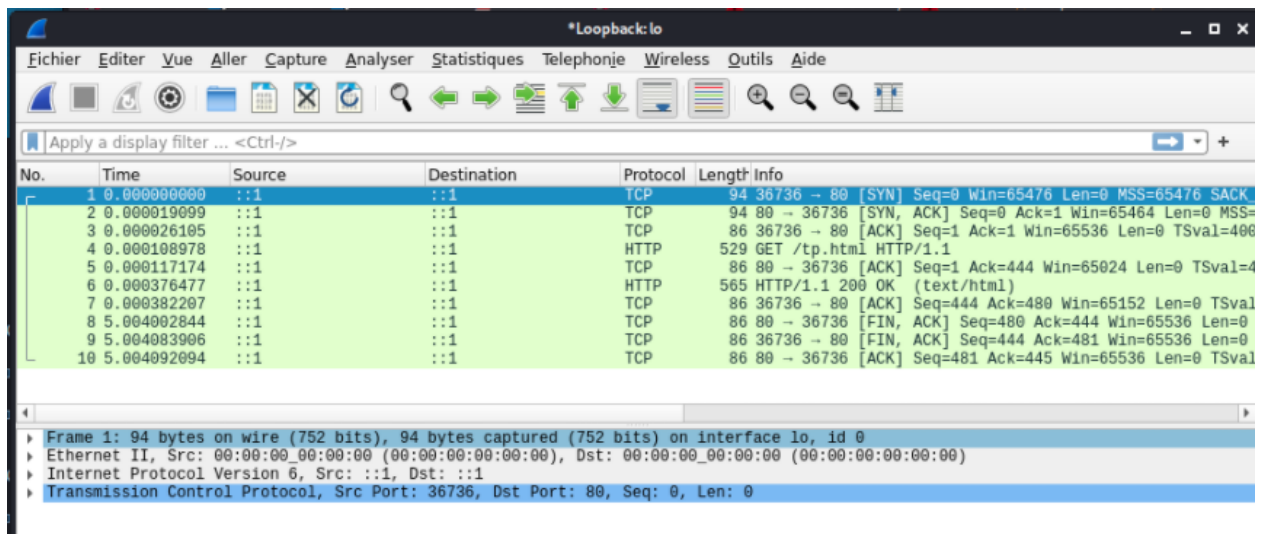
ip.addr == 128.119.245.12 and http					
No.	Time	Source	Destination	Protocol	Length Info
123	6.383330986	10.0.2.33	128.119.245.12	HTTP	462 GET /ethereal-labs/lab2-4.html HTTP/1.1
125	6.458172202	128.119.245.12	10.0.2.33	HTTP	1114 HTTP/1.1 200 OK (text/html)
128	6.468831865	10.0.2.33	128.119.245.12	HTTP	426 GET /~kurose/cover.jpg HTTP/1.1
160	6.670598174	10.0.2.33	128.119.245.12	HTTP	358 GET /favicon.ico HTTP/1.1
189	6.745080142	128.119.245.12	10.0.2.33	HTTP	550 HTTP/1.1 404 Not Found (text/html)
197	6.773463378	128.119.245.12	10.0.2.33	HTTP	662 HTTP/1.1 200 OK (JPEG JFIF image)

3)

Création de la page html



Sur wireshark on configure sur l'interface loopback



2.2 Questions

1. En vous appuyant sur la capture Wireshark que vous venez de réaliser, tracez, sur un graphe de séquence, les étapes de la connexion à votre page. Faites apparaître les couches du modèle OSI concernées.

1	0.000000000	:::1	:::1	TCP	94 36736 → 80 [SYN] Seq=0 Win=65476 Len=0 MSS=65476 SACK
2	0.000019099	:::1	:::1	TCP	94 80 → 36736 [SYN, ACK] Seq=0 Ack=1 Win=65464 Len=0 MSS=
3	0.000026105	:::1	:::1	TCP	86 36736 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=400
4	0.000108978	:::1	:::1	HTTP	529 GET /tp.html HTTP/1.1
5	0.000117174	:::1	:::1	TCP	86 80 → 36736 [ACK] Seq=1 Ack=444 Win=65024 Len=0 TSval=4
6	0.000376477	:::1	:::1	HTTP	565 HTTP/1.1 200 OK (text/html)
7	0.000382207	:::1	:::1	TCP	86 36736 → 80 [ACK] Seq=444 Ack=480 Win=65152 Len=0 TSval
8	5.004002844	:::1	:::1	TCP	86 80 → 36736 [FIN, ACK] Seq=480 Ack=444 Win=65536 Len=0
9	5.004003906	:::1	:::1	TCP	86 36736 → 80 [FIN, ACK] Seq=444 Ack=481 Win=65536 Len=0
10	5.004092094	:::1	:::1	TCP	86 80 → 36736 [ACK] Seq=481 Ack=445 Win=65536 Len=0 TSval

2. Quel(s) est (sont) le(s) type(s) de requêtes (GET, POST, HEAD, OPTION, etc.) utilisé(s) ?

les requêtes les plus utilisées et la requête GET

1	0.000000000	:::1	:::1	TCP	94 36736 → 80 [SYN] Seq=0 Win=65476 Len=0 MSS=65476 SACK
2	0.000019099	:::1	:::1	TCP	94 80 → 36736 [SYN, ACK] Seq=0 Ack=1 Win=65464 Len=0 MSS=
3	0.000026105	:::1	:::1	TCP	86 36736 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=400
4	0.000108978	:::1	:::1	HTTP	529 GET /tp.html HTTP/1.1
5	0.000117174	:::1	:::1	TCP	86 80 → 36736 [ACK] Seq=1 Ack=444 Win=65024 Len=0 TSval=4
6	0.000376477	:::1	:::1	HTTP	565 HTTP/1.1 200 OK (text/html)
7	0.000382207	:::1	:::1	TCP	86 36736 → 80 [ACK] Seq=444 Ack=480 Win=65152 Len=0 TSval
8	5.004002844	:::1	:::1	TCP	86 80 → 36736 [FIN, ACK] Seq=480 Ack=444 Win=65536 Len=0
9	5.004003906	:::1	:::1	TCP	86 36736 → 80 [FIN, ACK] Seq=444 Ack=481 Win=65536 Len=0
10	5.004092094	:::1	:::1	TCP	86 80 → 36736 [ACK] Seq=481 Ack=445 Win=65536 Len=0 TSval

3. Toujours en vous appuyant sur la capture Wireshark, décrire de manière exhaustive la première requête à partir de votre appui sur le bouton "Envoyer" sur votre page de formulaire : il s'agit d'une requête de type POST ; ainsi que la première réponse du serveur à cette requête. On attachera une attention particulière au type mime et au status http

sur la capture on a bien la requête POST et le type MIME est /myPage.php

Fichier Editor Vue Aller Capture Analyser Statistiques Téléphone Wireless Outils Aide												
Apply a display filter ... <input type="text" value=""/> <input type="button" value="OK"/> <input type="button" value="+"/>												
io.	Time	Source	Destination	Protocol	Length	Info						
-	11.87.888708121	:::1	:::1	TCP	94	37008 → 80	[SYN]	Seq=0	Win=65476	Len=0	MSS=65476	SAC
-	12.87.888720943	:::1	:::1	TCP	94	80 → 37008	[SYN, ACK]	Seq=0	Ack=1	Win=65464	Len=0	MS
-	13.87.888728975	:::1	:::1	TCP	86	37008 → 80	[ACK]	Seq=1	Ack=1	Win=65536	Len=0	TSval=4
-	14.87.888803028	:::1	:::1	HTTP	530	GET /tp2.html HTTP/1.1						
-	15.87.888820070	:::1	:::1	TCP	86	80 → 37008	[ACK]	Seq=1	Ack=445	Win=65024	Len=0	TSval
-	16.87.889130305	:::1	:::1	HTTP	574	HTTP/1.1 200 OK (text/html)						
-	17.87.889136259	:::1	:::1	TCP	86	37008 → 80	[ACK]	Seq=445	Ack=489	Win=65152	Len=0	Tsv
-	18.92.889111059	:::1	:::1	TCP	86	37008 → 80	[FIN, ACK]	Seq=445	Ack=489	Win=65536	Len=	
-	19.92.889193139	:::1	:::1	TCP	86	80 → 37008	[FIN, ACK]	Seq=489	Ack=446	Win=65536	Len=	
-	20.92.889199391	:::1	:::1	TCP	86	37008 → 80	[ACK]	Seq=446	Ack=490	Win=65536	Len=0	Tsv
-	21.93.848545842	:::1	:::1	TCP	94	37010 → 80	[SYN]	Seq=0	Win=65476	Len=0	MSS=65476	SAC
-	22.93.848556763	:::1	:::1	TCP	94	80 → 37010	[SYN, ACK]	Seq=0	Ack=1	Win=65464	Len=0	MS

Le statut http est bien le numéro 200.

2.3 LiveHTTPheaders

2.4 Questions

1. Qu'observez-vous ?

On voit que les requête sont de type POST et GET.

2. Grâce à un schéma, et en faisant apparaître toutes les requêtes, tracez le déroulement de ce qu'il se passe.



```

K-XSS-Protection: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443";
X-Firefox-Spdy: h2

https://googleads.g.doubleclick.net/adsid/google/si?gadsid=A0RoGNR-y3s38Ll53rZ7aJwU60gzFZxSi5Q8-spFipUXN8qU2oBs-11CNKlgXx9cFw6rtU8nQ0_8hRAwmssvuYvD
Host: googleads.g.doubleclick.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.google.fr/
Connection: keep-alive

GET: HTTP/2.0 204 No Content
p3p: CP="This is not a P3P policy! See http://support.google.com/accounts/answer/151657 for more info."
timing-Allow-Origin: *
cross-origin-resource-policy: cross-origin
cache-control: private, max-age=15
content-type: text/html; charset=UTF-8
x-content-type-options: nosniff
date: Fri, 17 Sep 2021 16:27:31 GMT
server: cafe
content-length: 0
X-XSS-Protection: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443";
X-Firefox-Spdy: h2

https://www.google.fr/gen_204?atyp=i&r=1&ei=88FEYzr5F8eUa85QLJAI&ct=slh&v=t1&m=HV6pv=0.8009446027176936&me=1:1631896051342,x:4,V:0,0,1010,839:0,N:1
Host: www.google.fr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.google.fr/
Origin: https://www.google.fr
Connection: keep-alive
Cookie: CONSENT=YES+shp.gws-20210902-0-RC2.fr+FX+476; NID=511~XPz0HR9tn07IN7-eGqChxRMl3uX0m5GZfPpRkH7H1evvcYLqNuf1onHr3M1JchQoRXNEeW9zWahge5nEr8xmck7U5mr54H38j0Q58KJ_qRhlriUJ_85;
POST: HTTP/2.0 204 No Content
content-type: text/html; charset=UTF-8
date: Fri, 17 Sep 2021 16:27:32 GMT
server: gws
content-length: 0
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443";
X-Firefox-Spdy: h2

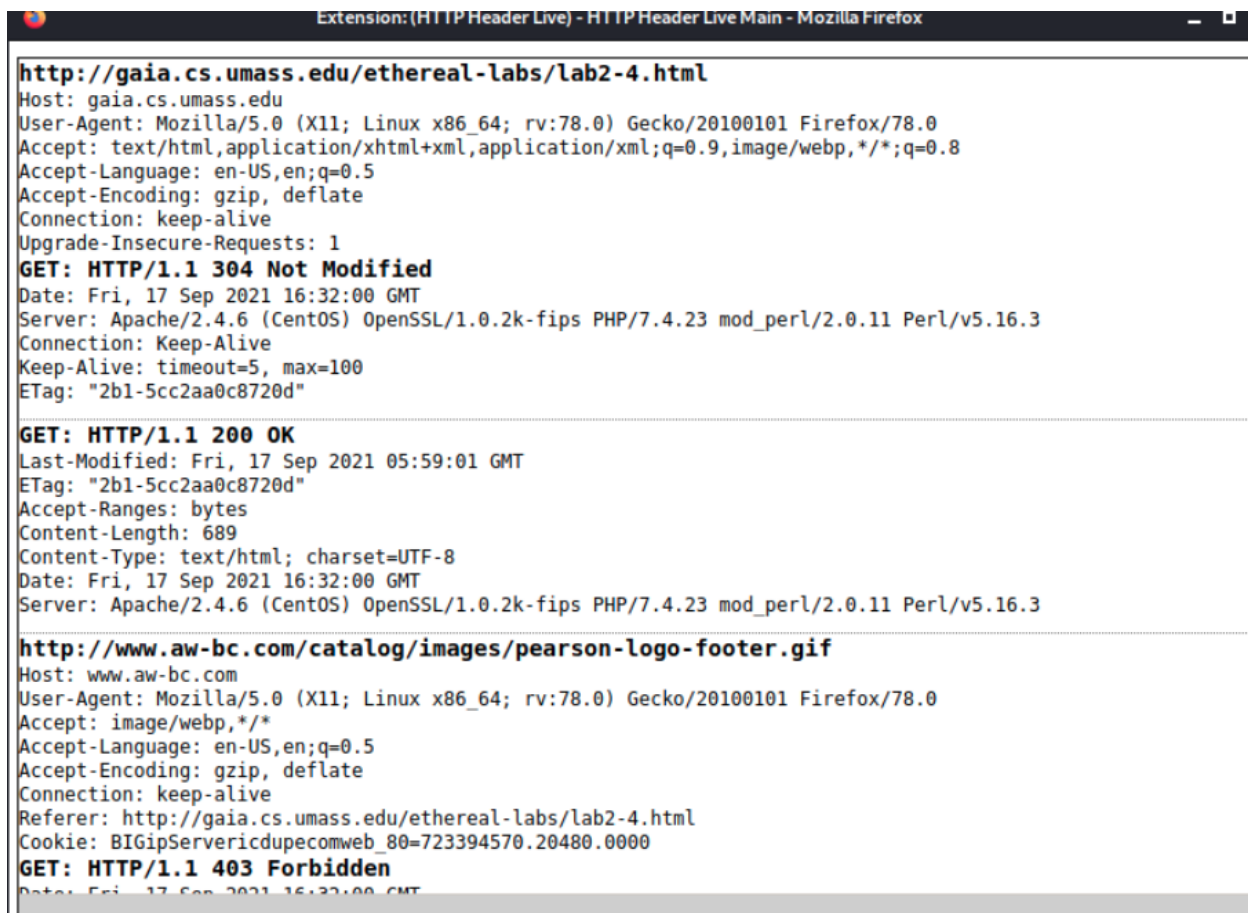
https://www.google.fr/gen_204?atyp=i&r=1&ei=88FEYzr5F8eUa85QLJAI&ct=slh&v=t1&m=M6pv=0.8009446027176936&me=7:1631896051831,V:0,0,0,0:5928,h:1,1,1,i:3
Host: www.google.fr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br

```

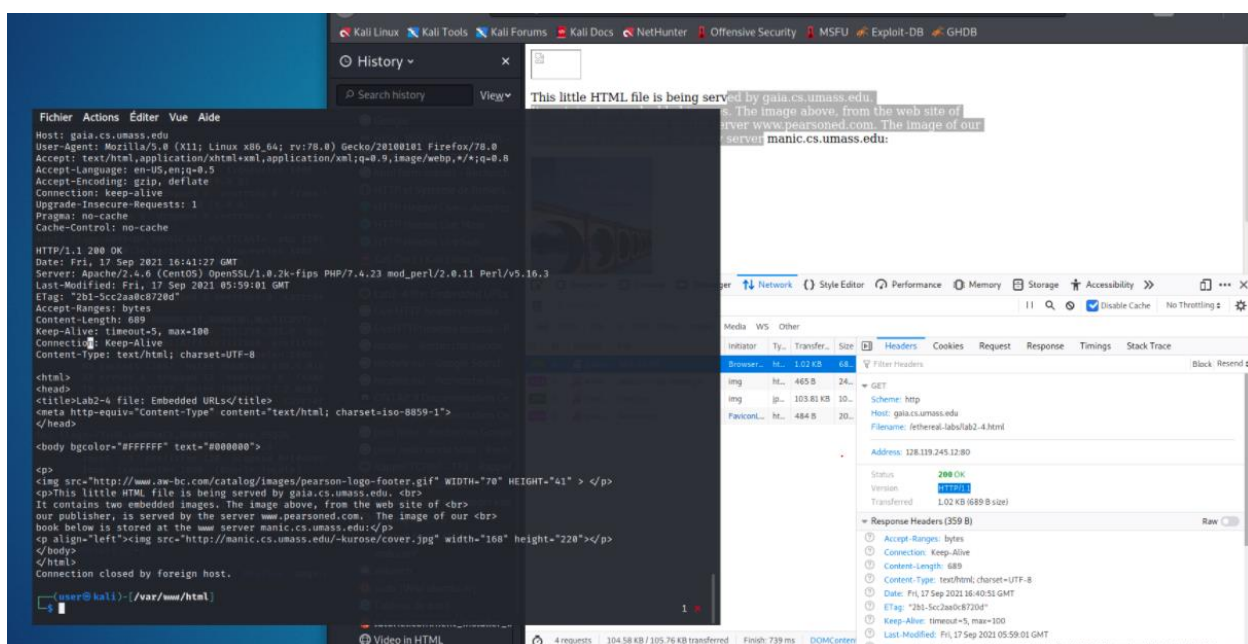
```
Extension: (HTTP Header Live) - HTTP Header Live Main - Mozilla Firefox
COOKIE: CONSENT=YES+shp.gws-20210902-0-RC2.fr+FX+476; NID=511=XP20hR9tn07IN7-eGqCHxRML3uXQwm5GZFpRKH7H1evcY
Upgrade-Insecure-Requests: 1
GET: HTTP/2.0 200 OK
date: Fri, 17 Sep 2021 16:29:49 GMT
expires: -1
cache-control: private, max-age=0
content-type: text/html; charset=UTF-8
strict-transport-security: max-age=31536000
content-encoding: br
server: gws
content-length: 34984
x-xss-protection: 0
x-frame-options: SAMEORIGIN
set-cookie: 1P_JAR=2021-09-17-16; expires=Sun, 17-Oct-2021 16:29:49 GMT; path=/; domain=.google.fr; Secure;
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000
X-Firefox-Spdy: h2
https://www.google.fr/gen_204?atyp=i&r=1&ei=88FEYZrSF8eUa8SQLJAI&ct=slh&v=t1&im=M&pv=0.800
Host: www.google.fr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.google.fr/
Origin: https://www.google.fr
Connection: keep-alive
Cookie: CONSENT=YES+shp.gws-20210902-0-RC2.fr+FX+476; NID=511=XP20hR9tn07IN7-eGqCHxRML3uXQwm5GZFpRKH7H1evcY
POST: HTTP/2.0 204 No Content
content-type: text/html; charset=UTF-8
date: Fri, 17 Sep 2021 16:29:49 GMT
server: gws
content-length: 0
x-xss-protection: 0
x-frame-options: SAMEORIGIN
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000
```

3. Effacez la capture précédente, puis rendez-vous sur www.cnrs.fr. Qu'observez-vous ? Est-ce que ce que vous observez est conforme avec les observations faites par la capture Wireshark ?

Dans la capture ci-dessous le statut http est 200, et on obtient les même informations que sur wireshark.



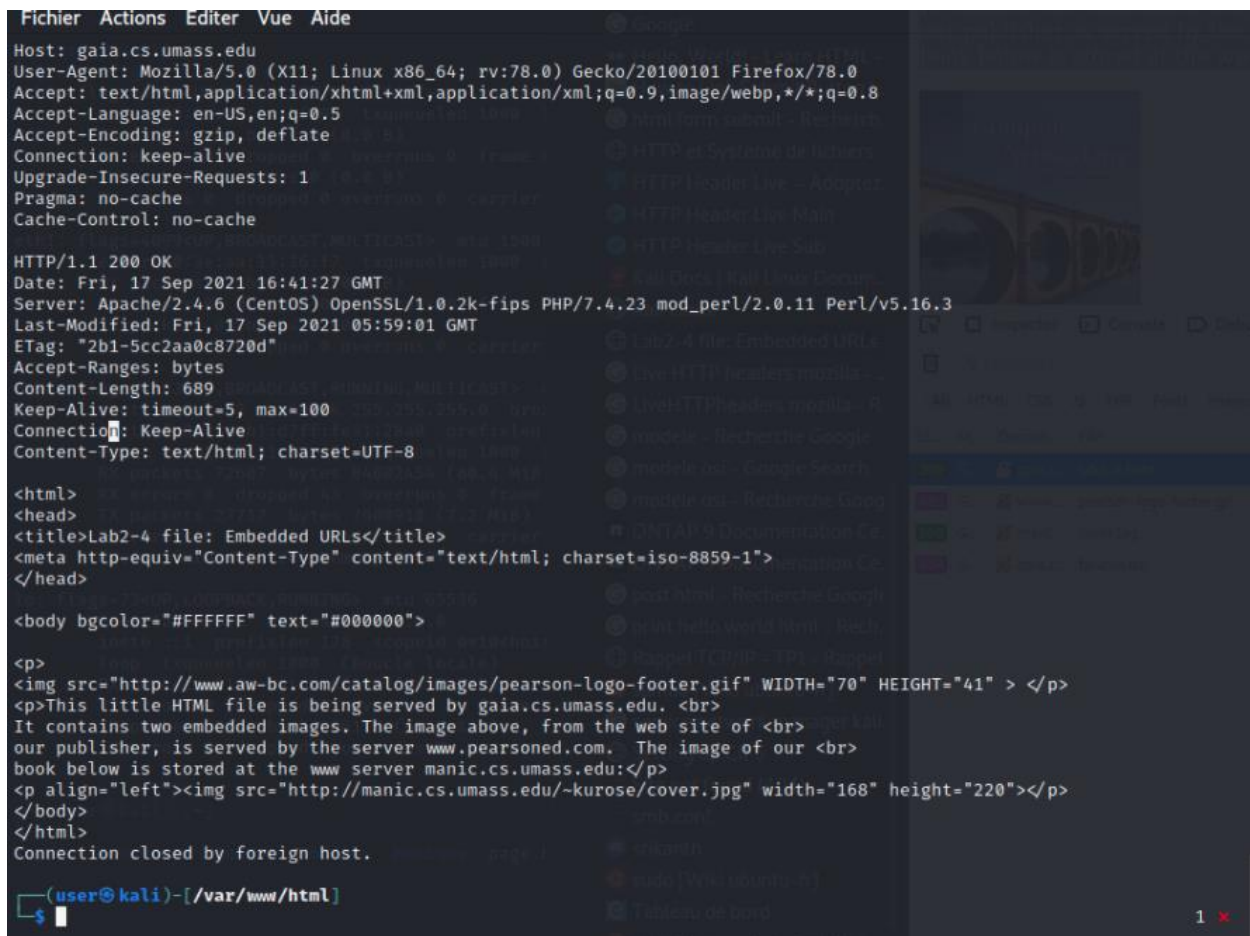
Avec la commande telnet



2.5 Questions

1. Qu'est-ce que vous observez ?

On peut voir la page html, avec la date de connexion, et le serveur.



```
Fichier Actions Editor Vue Aide
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Fri, 17 Sep 2021 16:41:27 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.23 mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Fri, 17 Sep 2021 05:59:01 GMT
ETag: "2b1-5cc2aa0c8720d"
Accept-Ranges: bytes
Content-Length: 689
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
<head>
<title>Lab2-4 file: Embedded URLs</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>

<body bgcolor="#FFFFFF" text="#000000">

<p>
 </p>
<p>This little HTML file is being served by gaia.cs.umass.edu. <br>
It contains two embedded images. The image above, from the web site of <br>
our publisher, is served by the server www.pearsoned.com. The image of our <br>
book below is stored at the www server manic.cs.umass.edu:</p>
<p align="left"></p>
</body>
</html>
Connection closed by foreign host.

(user@kali)-[/var/www/html]
$
```

2. En supprimant des éléments de l'en-tête HTTP de votre requête, cela modifie-t'il la réponse du serveur ? (vous pouvez itérer en supprimant à chaque fois la dernière ligne de l'en-tête). Il s'agit ici de déterminer quels sont les éléments indispensables au sein des en-têtes d'une requête HTTP pour qu'un serveur HTTP puisse y répondre.

```
(user@kali)-[/var/www/html]
$ telnet 128.119.245.12 80
Trying 128.119.245.12...
Connected to 128.119.245.12.
Escape character is '^]'.
GET /ethereal-labs/lab2-4.html HTTP/1.1Host: gaia.cs.umass.eduUser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8Accept-Language: en-US,en;q=0.5Accept-Encoding: gzip, deflateConnection
HTTP/1.1 400 Bad Request
Date: Fri, 17 Sep 2021 16:52:55 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.23 mod_perl/2.0.11 Perl/v5.16.3
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
</body></html>
Connection closed by foreign host.

(user@kali)-[/var/www/html]
$
```

on supprimeant l'en tete , on remarque q'il y a des changement , dans la capture on peut voir le BAD REQUEST.

Supprimez votre capture et retournez sur votre page de formulaire qui est en local. Commencez la capture.

```

Fichier Actions Éditer Vue Aide
Traitement des actions différées (« triggers ») pour kali-menu (2021.3.3) ... [1/1]
[user@kali]~/var/www/html$ vim /etc/exports
[user@kali]~/var/www/html$ telnet 127.0.0.1 80
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
GET /tp.html HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
HTTP/1.1 200 OK
Date: Fri, 17 Sep 2021 17:08:07 GMT
Server: Apache/2.4.48 (Debian)
Last-Modified: Fri, 17 Sep 2021 16:15:00 GMT
ETag: "ef-5cc333bb8582e-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 182
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
Connection closed by foreign host.
[user@kali]~/var/www/html$

```

2.6 Questions

1. Qu'observez-vous ?

Pour notre site web : sur notre site web on reçoit bien une réponse on peut voir qu'il y a une partie crypter.

On retrouver bien les informations vu précédemment

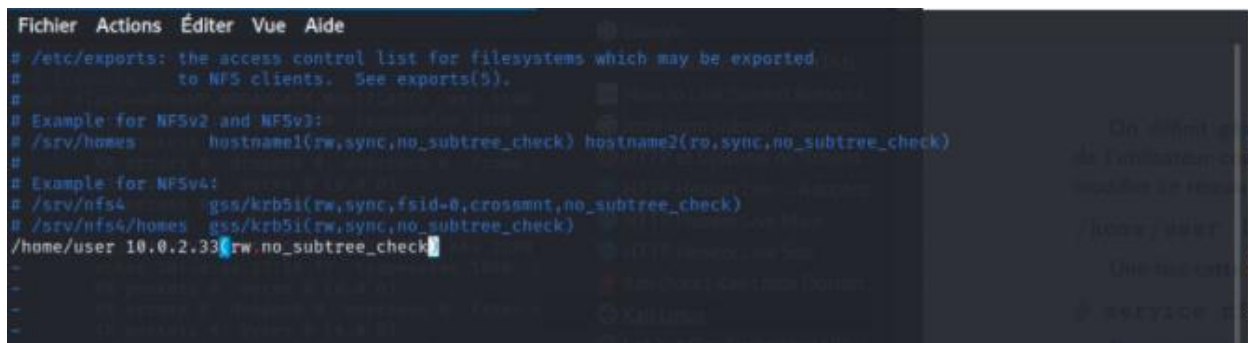
2. Grâce à un schéma, et en faisant apparaître toutes les requêtes, tracez le déroulement de ce qu'il se passe.

3. Est-ce que c'est conforme à ce que vous avez observé avec Wireshark ? 4. Peut-on rejouer la capture comme précédemment ? Pourquoi ?

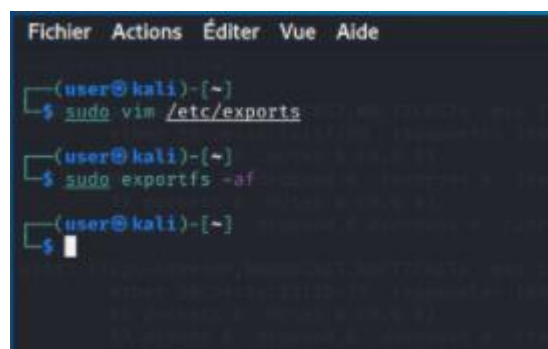
Cela n'est pas conforme, sur Wireshark on a POST et GET en temps réel, et sur telnet on obtient que le GET sur l'instant présent. On n'a pas l'en-tête du POST.

3 Système de fichiers

3.1 Configuration NFS

A screenshot of a text editor window showing the contents of the /etc/exports file. The file contains comments and several export rules for NFSv2, NFSv3, and NFSv4. The last line of the file is being edited, showing the path /home/user 10.0.2.33 with a cursor at the end of the line.

```
Fichier Actions Éditer Vue Aide
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
/home/user 10.0.2.33(rw,no_subtree_check)
```

A screenshot of a terminal window showing a series of commands being executed to configure NFS. The user is at a kali machine. The commands are: sudo vim /etc/exports, sudo exportfs -af, and a final prompt.

```
Fichier Actions Éditer Vue Aide
(user@kali)-[~]
$ sudo vim /etc/exports
(user@kali)-[~]
$ sudo exportfs -af
(user@kali)-[~]
$
```


3.2 Questions

1. Quelles sont les modifications à apporter au fichier de configuration pour que cette dernière soit correcte ?

La modification a apporté au fichier de configuration c'est de mettre la bonne adresse ip.

```
srikanth@srikanth-VirtualBox:~$ sudo cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes          hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4           gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes     gss/krb5i(rw,sync,no_subtree_check)
#
/home/srikanth 10.0.2.15/24(rw,sync,no_subtree_check)
srikanth@srikanth-VirtualBox:~$
```

```
srikanth@srikanth-VirtualBox:~$ showmount -e 172.17.0.1
Export list for 172.17.0.1:
/home/srikanth 10.0.2.15/24
srikanth@srikanth-VirtualBox:~$
```

Une fois la configuration correcte, connectez-vous sur une seconde machine, dans le réseau autorisé pour le partage NFS, et faites le montage NFS.

```
srikanth@srikanth-VirtualBox:~$ sudo mount -t nfs 172.17.0.1:/home/srikanth /mnt
srikanth@srikanth-VirtualBox:~$ dh -f
Command 'dh' not found, but can be installed with:
sudo apt install debhelper
srikanth@srikanth-VirtualBox:~$ df -h

```

Filesystem	Size	Used	Avail	Use%	Mounted on
tmpfs	457M	1,4M	456M	1%	/run
/dev/sda3	148G	10G	131G	8%	/
tmpfs	2,3G	0	2,3G	0%	/dev/shm
tmpfs	5,0M	4,0K	5,0M	1%	/run/lock
tmpfs	4,0M	0	4,0M	0%	/sys/fs/cgroup
/dev/sda2	512M	5,3M	507M	2%	/boot/efi
tmpfs	457M	108K	457M	1%	/run/user/1000
172.17.0.1:/home/srikanth	148G	10G	131G	8%	/mnt

```
srikanth@srikanth-VirtualBox:~$
```

Ecrivez un fichier dans le partage réseau avec le client et vérifiez que ce fichier apparaît bien sur le serveur.

The image shows two terminal windows side-by-side. The left window is the client's terminal, and the right window is the server's terminal. Both are running Ubuntu in a VirtualBox environment.

Left Terminal (Client):

```
srikanth@srikanth-VirtualBox: ~
RX packets 171 bytes 14491 (14.4 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 171 bytes 14491 (14.4 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collision:0
srikanth@srikanth-VirtualBox:~$ exportfs -af
exportfs: could not open /var/lib/nfs/.etab.lock for locking: Permission denied
exportfs: could not open /var/lib/nfs/.etab.lock for locking: Permission denied
exportfs: can't lock /var/lib/nfs/etab for writing
srikanth@srikanth-VirtualBox:~$ sudo exportfs -af
[sudo] password for srikanth:
srikanth@srikanth-VirtualBox:~$ service nfs-kernel-server restart
srikanth@srikanth-VirtualBox:~$ ls
Desktop Music prog.xml 'Untitled Dc/dev/sda3
Documents new_rep Public USER
Downloads nohup.out ss.txt user.sh
File part Templates Videos
File part-3-2.c test.html w.html /dev/sda2
File Pictures testtp3.txt xml.xml
File lex.html prog test.xml
File prog LAB3_collaty.c tp2reseau.txt
srikanth@srikanth-VirtualBox:~$
```

Right Terminal (Server):

```
srikanth@srikanth-VirtualBox: ~
mount: /mnt: can't find in /etc/fstab.
srikanth@srikanth-VirtualBox:~$ sudo mount -t 10.0.2.15:/home/srikanth /mnt
mount: /mnt: can't find in /etc/fstab.
srikanth@srikanth-VirtualBox:~$ sudo mount -t 127.0.0.1:/home/srikanth /mnt
mount: /mnt: can't find in /etc/fstab.
srikanth@srikanth-VirtualBox:~$ sudo mount -t 172.17.0.1:/home/srikanth /mnt
mount: /mnt: can't find in /etc/fstab.
srikanth@srikanth-VirtualBox:~$ sudo mount -t nfs 172.17.0.1:/home/srikanth /mnt
srikanth@srikanth-VirtualBox:~$ dh -f
Command 'dh' not found, but can be installed with:
sudo apt install debhelper
srikanth@srikanth-VirtualBox:~$ df -h
Filesystem Size Used Avail Use% Mounted on
tmpfs 457M 1,4M 456M 1% /run
/dev/sda3 148G 10G 131G 8% /
/dev/shm 2,3G 0 2,3G 0% /dev/shm
/run/lock 5,0M 4,0K 5,0M 1% /run/lock
/sys/fs/cgroup 4,0M 0 4,0M 0% /sys/fs/cgroup
/boot/efi 512M 5,3M 507M 2% /boot/efi
/run/user/1000 457M 108K 457M 1% /run/user/1000
172.17.0.1:/home/srikanth 148G 10G 131G 8% /mnt
srikanth@srikanth-VirtualBox:~$ touch tp2reseau.txt
srikanth@srikanth-VirtualBox:~$
```

A gauche nous avons le serveur et a droite nous avoir le serveur, pour voir si le nfs fonctionne, à partir du client j'ai créé un fichier tp2reseau.txt et dans le serveur on peut voir que le fichier a bien était créer.

Commencez par démonter le montage existant sur le client :

```
srikanth@srikanth-VirtualBox:~$ sudo umount /mnt
[sudo] password for srikanth:
srikanth@srikanth-VirtualBox:~$
```

— Sur le serveur, lancez Wireshark

```
srikanth@srikanth-VirtualBox:~$ sudo wireshark &
[1] 3703
srikanth@srikanth-VirtualBox:~$ 23:56:31.870 Main Warn QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

— Sur le client, recommencez l'opération de montage

Capturing from enp0s3					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
Apply a display filter ... <Ctrl-/>					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	10.0.2.15	192.168.1.254	DNS	100 Standard query 0xba37 AAAA connectivity-check.ubuntu
2	0.012644978	192.168.1.254	10.0.2.15	DNS	161 Standard query response 0xba37 AAAA connectivity-check.ubuntu
3	0.014062948	10.0.2.15	192.168.1.254	DNS	100 Standard query 0x9bc5 AAAA connectivity-check.ubuntu
4	0.023303199	192.168.1.254	10.0.2.15	DNS	161 Standard query response 0x9bc5 AAAA connectivity-check.ubuntu
5	5.023349574	PcsCompu_91:39:97	RealtekU_12:35:02	ARP	42 Who has 10.0.2.2? Tell 10.0.2.15
6	5.024160178	RealtekU_12:35:02	PcsCompu_91:39:97	ARP	60 10.0.2.2 is at 52:54:00:12:35:02
7	110.504050033	10.0.2.15	34.122.121.32	TCP	74 38706 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
8	110.616250393	34.122.121.32	10.0.2.15	TCP	60 80 → 38706 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS
9	110.616396994	10.0.2.15	34.122.121.32	TCP	54 38706 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	110.620562901	10.0.2.15	34.122.121.32	HTTP	141 GET / HTTP/1.1
11	110.622280872	34.122.121.32	10.0.2.15	TCP	60 80 → 38706 [ACK] Seq=1 Ack=88 Win=65535 Len=0
12	110.800049519	34.122.121.32	10.0.2.15	HTTP	202 HTTP/1.1 204 No Content
13	110.800142497	10.0.2.15	34.122.121.32	TCP	54 38706 → 80 [ACK] Seq=88 Ack=149 Win=64092 Len=0

— Sur le client, faites un ls dans le partage.

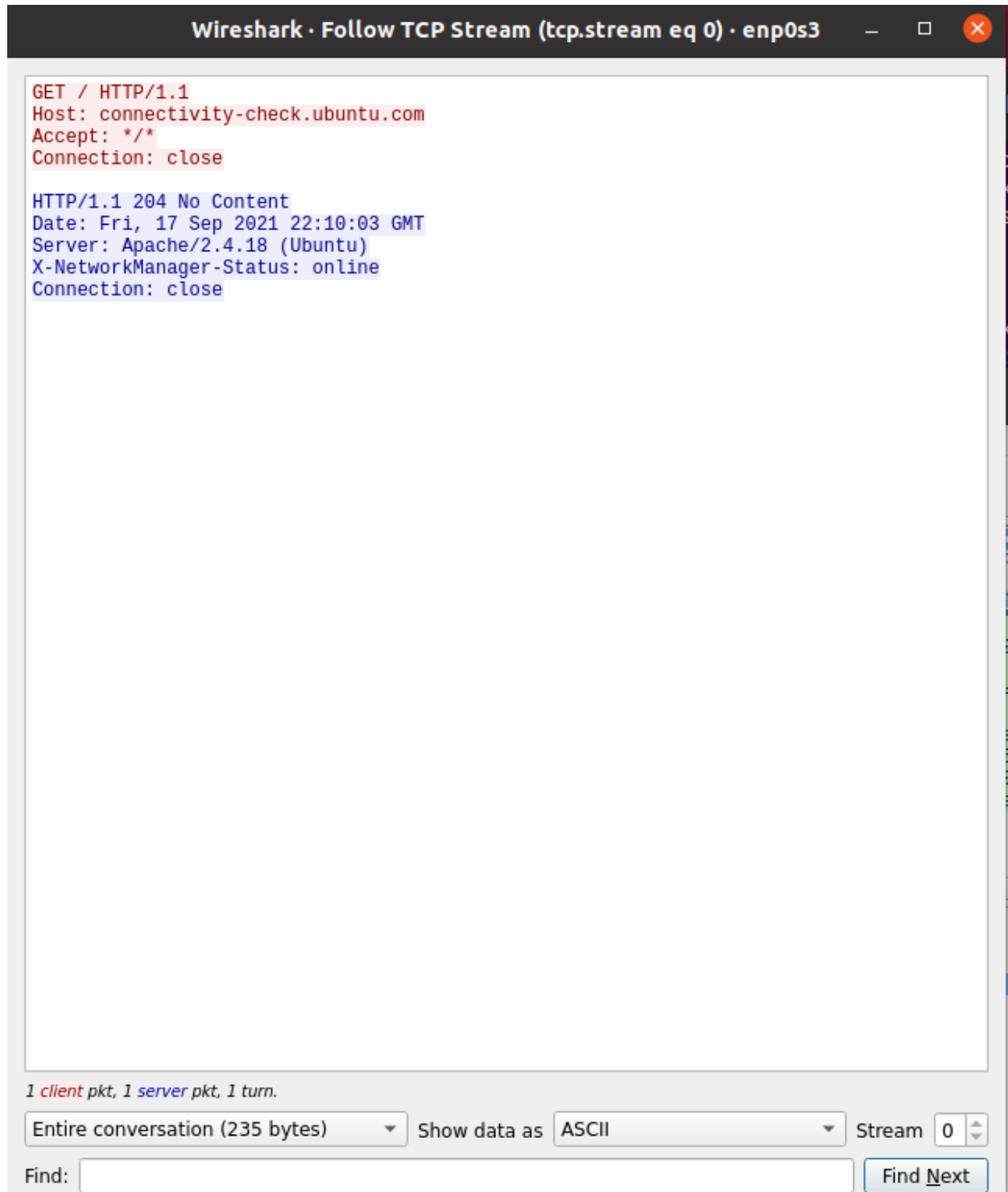
Capturing from enp0s3					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
Apply a display filter ... <Ctrl-/>					
No.	Time	Source	Destination	Protocol	Length Info
5	5.082118676	PcsCompu_91:39:97	RealtekU_12:35:02	ARP	42 Who has 10.0.2.2? Tell 10.0.2.15
6	5.083544189	RealtekU_12:35:02	PcsCompu_91:39:97	ARP	60 10.0.2.2 is at 52:54:00:12:35:02
7	110.493087343	10.0.2.15	34.122.121.32	TCP	74 38710 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
8	110.599370850	34.122.121.32	10.0.2.15	TCP	60 80 → 38710 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS
9	110.599440084	10.0.2.15	34.122.121.32	TCP	54 38710 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	110.600173094	10.0.2.15	34.122.121.32	HTTP	141 GET / HTTP/1.1
11	110.600700721	34.122.121.32	10.0.2.15	TCP	60 80 → 38710 [ACK] Seq=1 Ack=88 Win=65535 Len=0
12	110.773460495	34.122.121.32	10.0.2.15	HTTP	202 HTTP/1.1 204 No Content
13	110.773508558	10.0.2.15	34.122.121.32	TCP	54 38710 → 80 [ACK] Seq=88 Ack=149 Win=64092 Len=0
14	110.773460871	34.122.121.32	10.0.2.15	TCP	60 80 → 38710 [FIN, ACK] Seq=149 Ack=88 Win=65535 Len=0
15	110.775180659	10.0.2.15	34.122.121.32	TCP	54 38710 → 80 [FIN, ACK] Seq=88 Ack=150 Win=64091 Len=0
16	110.775755084	34.122.121.32	10.0.2.15	TCP	60 80 → 38710 [ACK] Seq=150 Ack=89 Win=65535 Len=0

3.3 Questions

1. Sur quels protocoles s'appuie NFS ?

Le NFS s'appuie sur le protocole RPC.

2. En faisant un clic-droit, puis en cliquant sur Follow TCP Stream sur le premier paquet, inspectez le contenu du flux. Que remarquez-vous ?



On voit qu'on a un GET et un POST, on a les informations sur la date et l'heure de connexion, le nom du serveur.

3. En vous basant sur la capture, expliquez le fonctionnement des RPC. Faites-le à base de schéma.

Un client contacte par exemple un serveur de base de données central lors de la recherche d'une pièce de rechange. Le serveur situé à distance vérifie ensuite les données disponibles et envoie le résultat au client. Ce dernier traite les données obtenues et affiche par exemple une liste des données disponibles dans le logiciel de gestion.

3.4 Configuration CIFS

Installation de samba

```
srikanth@srikanth-VirtualBox:~$ sudo apt-get install samba
[sudo] password for srikanth:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm11
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  attr ibverbs-providers libcephfs2 libibverbs1 librados2 librdmacm1 liburing1
  python3-dnspython python3-ecdsa python3-gpg python3-markdown
  python3-pycryptodome python3-pygments python3-samba python3-tdb samba-common
  samba-common-bin samba-dsdb-modules samba-vfs-modules tdb-tools
Suggested packages:
  python-markdown-doc python-pygments-doc ttf-bitstream-vera bind9 bind9utils
  ctdb ldb-tools ntp | chrony smbldap-tools winbind heimdal-clients
The following NEW packages will be installed:
  attr ibverbs-providers libcephfs2 libibverbs1 librados2 librdmacm1 liburing1
  python3-dnspython python3-ecdsa python3-gpg python3-markdown
  python3-pycryptodome python3-pygments python3-samba python3-tdb samba
  samba-common samba-common-bin samba-dsdb-modules samba-vfs-modules tdb-tools
```

```
srikanth@srikanth-VirtualBox:~$ sudo useradd smbuser1
srikanth@srikanth-VirtualBox:~$ sudo useradd smbuser2
```



```
srikanth@srikanth-VirtualBox:~$ sudo usermod smbuser1 -aG smbgroup
```

```
smbgroup:x:1002:smbuser1
smbuser1:x:1003:
smbuser2:x:1004:
```

Création du mot de passe :

```
srikanth@srikanth-VirtualBox:~$ sudo smbpasswd -a smbuser1
New SMB password:
Retype new SMB password:
Added user smbuser1.
srikanth@srikanth-VirtualBox:~$
```

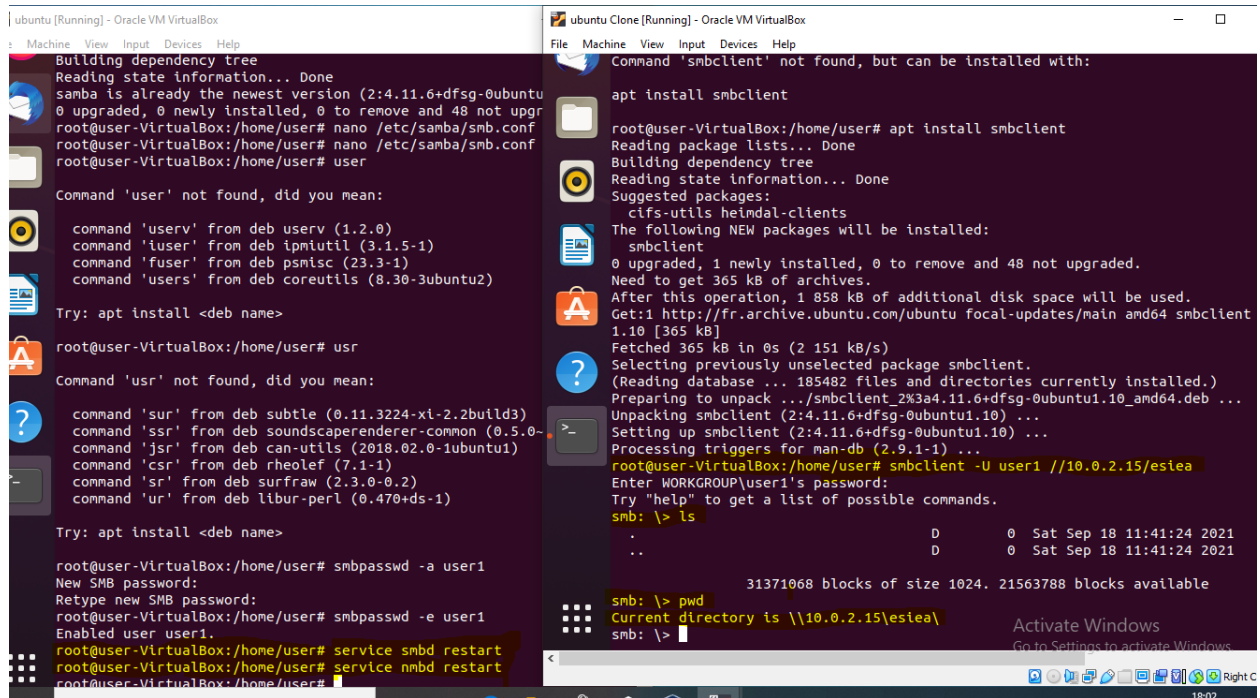
Pour activer l'utilisateur

```
srikanth@srikanth-VirtualBox:~$ sudo smbpasswd -e smbuser1
Enabled user smbuser1.
```

Relancez le service Samba

```
srikanth@srikanth-VirtualBox:~$ service smb restart
srikanth@srikanth-VirtualBox:~$ service nmb restart
srikanth@srikanth-VirtualBox:~$
```

Pour effectuer la connexion avec samba je me suis mis en root et cloner la machine virtuelle qui fait office de client et serveur.



```
ubuntu [Running] - Oracle VM VirtualBox
Machine View Input Devices Help
Building dependency tree
Reading state information... Done
samba is already the newest version (2:4.11.6+dfsg-0ubuntu
0 upgraded, 0 newly installed, 0 to remove and 48 not upgr
root@user-VirtualBox:/home/user# nano /etc/samba/smb.conf
root@user-VirtualBox:/home/user# nano /etc/samba/smb.conf
root@user-VirtualBox:/home/user# user

Command 'user' not found, did you mean:

  command 'userv' from deb userv (1.2.0)
  command 'iuser' from deb ipmiutil (3.1.5-1)
  command 'fuser' from deb psmisc (23.3-1)
  command 'users' from deb coreutils (8.30-3ubuntu2)

Try: apt install <deb name>

root@user-VirtualBox:/home/user# usr

Command 'usr' not found, did you mean:

  command 'sur' from deb subtle (0.11.3224-x1-2.2build3)
  command 'ssr' from deb soundscaperenderer-common (0.5.0-
  command 'jsr' from deb can-utils (2018.02.0-1ubuntu1)
  command 'csr' from deb rheolef (7.1-1)
  command 'sr' from deb surfraw (2.3.0-0.2)
  command 'ur' from deb libur-perl (0.470+ds-1)

Try: apt install <deb name>

root@user-VirtualBox:/home/user# smbpasswd -a user1
New SMB password:
Retype new SMB password:
root@user-VirtualBox:/home/user# smbpasswd -e user1
Enabled user user1.
root@user-VirtualBox:/home/user# service smbd restart
root@user-VirtualBox:/home/user# service nmbd restart
root@user-VirtualBox:/home/user#

ubuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command 'smbclient' not found, but can be installed with:

apt install smbclient

root@user-VirtualBox:/home/user# apt install smbclient
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  cifs-utils heimdal-clients
The following NEW packages will be installed:
  smbclient
0 upgraded, 1 newly installed, 0 to remove and 48 not upgraded.
Need to get 365 kB of archives.
After this operation, 1 858 kB of additional disk space will be used.
Get:1 http://fr.archive.ubuntu.com/ubuntu focal-updates/main amd64 smbclient
1.10 [365 kB]
Fetched 365 kB in 0s (2 151 kB/s)
Selecting previously unselected package smbclient.
(Reading database ... 185482 files and directories currently installed.)
Preparing to unpack .../smbclient_2%3a4.11.6+dfsg-0ubuntu1.10_amd64.deb ...
Unpacking smbclient (2:4.11.6+dfsg-0ubuntu1.10) ...
Setting up smbclient (2:4.11.6+dfsg-0ubuntu1.10) ...
Processing triggers for man-db (2.9.1-1) ...
root@user-VirtualBox:/home/user# smbclient -U user1 //10.0.2.15/esiea
Enter WORKGROUP\user1's password:
Try "help" to get a list of possible commands.
smb: \> ls

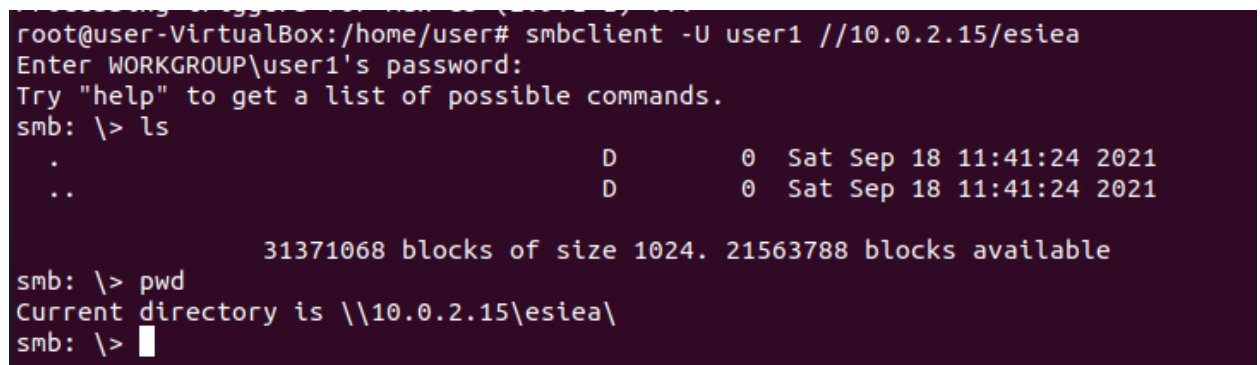
.                D                0    Sat Sep 18 11:41:24 2021
..               D                0    Sat Sep 18 11:41:24 2021

31371068 blocks of size 1024. 21563788 blocks available

smb: \> pwd
Current directory is \\10.0.2.15\esiea\
smb: \>
```

Vous pouvez tester en ligne de commandes que tout fonctionne :

La commande # smbclient -U user // IP_SERVER/esiea fonctionne parfaitement (capture ci-dessous)



```
root@user-VirtualBox:/home/user# smbclient -U user1 //10.0.2.15/esiea
Enter WORKGROUP\user1's password:
Try "help" to get a list of possible commands.
smb: \> ls

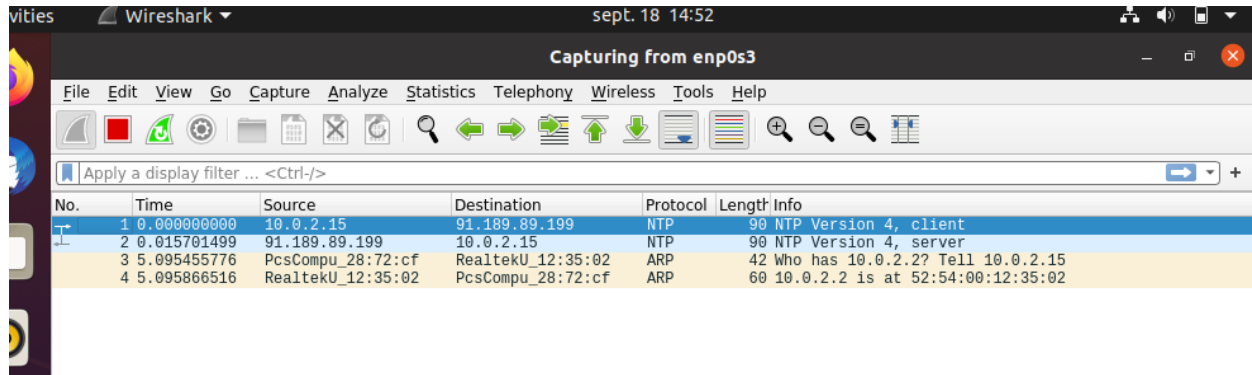
.                D                0    Sat Sep 18 11:41:24 2021
..               D                0    Sat Sep 18 11:41:24 2021

31371068 blocks of size 1024. 21563788 blocks available

smb: \> pwd
Current directory is \\10.0.2.15\esiea\
smb: \>
```

3.5 Questions

1. Lancez Wireshark. Faites un montage à la main sur un poste client.



Ce qu'on obtient quand on utilise samba entre le client et serveur

2. Lors de la phase d'authentification, pouvez-vous voir le mot de passe ?

```
root@user-VirtualBox:/home/user# smbclient -U user1 //10.0.2.15/esiea
Enter WORKGROUP\user1's password:
Try "help" to get a list of possible commands.
smb: \>
```

Lors de l'authentification, on ne peut pas voir le mot de passe

3. Créer un fichier depuis le client sur le partage et écrivez à l'intérieur. Pouvez-vous retrouver le contenu du fichier dans la capture ? Expliquez.

```

root@user-VirtualBox:/home/user# touch test
root@user-VirtualBox:/home/user# nano test
root@user-VirtualBox:/home/user# mv /home/user/test /media/esiea
root@user-VirtualBox:/home/user# cd /media/esiea
root@user-VirtualBox:/media/esiea# ls
test
root@user-VirtualBox:/media/esiea# cat test
tp reseau informatique
root@user-VirtualBox:/media/esiea# smbclient -U user1 //10.0.2.15/esiea
Enter WORKGROUP\user1's password:
Try "help" to get a list of possible commands.
smb: \> ^C
root@user-VirtualBox:/media/esiea# smbclient -U user1 //10.0.2.15/esiea
Enter WORKGROUP\user1's password:
session setup failed: NT_STATUS_LOGON_FAILURE
root@user-VirtualBox:/media/esiea# smbclient -U user1 //10.0.2.15/esiea
Enter WORKGROUP\user1's password:
Try "help" to get a list of possible commands.
smb: \> l

.                               D              0   Sat Sep 18 15:19:35 2021
..                              D              0   Sat Sep 18 11:41:24 2021
test                            N             23   Sat Sep 18 15:19:11 2021

                                31371068 blocks of size 1024. 21402336 blocks available
smb: \>

```

Le fichier est bien créé et partagé dans le dossier de partage.

Voici ce qu'on observe sur Wireshark

The image shows a Wireshark network capture of SMB traffic. The top pane displays a list of packets, with packet 182 selected. The middle pane shows the details of the selected packet, and the bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
21	229.254319432	10.0.2.15	10.0.2.255	BROWSER	281	Local Master Announcement
22	229.254454589	10.0.2.15	10.0.2.255	BROWSER	258	Domain/Workgroup Announcement
111	954.146083816	10.0.2.15	10.0.2.255	BROWSER	281	Local Master Announcement
112	954.146218291	10.0.2.15	10.0.2.255	BROWSER	258	Domain/Workgroup Announcement
181	1674.2221378...	10.0.2.15	10.0.2.255	BROWSER	281	Local Master Announcement
182	1674.2222658...	10.0.2.15	10.0.2.255	BROWSER	258	Domain/Workgroup Announcement

Source name: USER-VIRTUALBOX<00> (Workstation/Redirector)
Destination name: <01><02>__MSBROWSE__<02><01> (Browser)
SMB (Server Message Block Protocol)

- SMB Header
 - Server Component: SMB
 - SMB Command: Trans (0x25)
 - Error Class: Success (0x00)
 - Reserved: 00
 - Error Code: No Error
 - Flags: 0x00
 - Flags2: 0x0000
 - 0... .. = Unicode Strings: Strings are ASCII
 - .0... .. = Error Code Type: Error codes are DOS error codes
 - ..0... .. = Execute-only Reads: Don't permit reads if execute-only

Raw packet data (hex and ASCII):

```

0040 43 43 4e 46 47 45 4a 46 43 46 45 46 46 45 42 45 CCNFGJF CFEFFEBE
0050 4d 45 43 45 50 46 49 41 41 00 20 41 42 41 43 46 MECEPFIA A ABACF
0060 50 46 50 45 4e 46 44 45 43 46 43 45 50 46 48 46 PFPENFDE CFCEPFHF
0070 44 45 46 46 50 46 50 41 43 41 42 00 ff 53 4d 42 DEFFFPFA CAB SMB
0080 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 %.....
0090 00 00 00 00 00 00 00 00 00 00 00 00 11 00 00 30 .....0
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00b0 00 00 00 30 00 56 00 03 00 01 00 01 00 02 00 41 ...0.V...A

```

The image shows a Wireshark packet capture. The top pane displays a list of network packets. Packet 21 is a Browser Protocol announcement from 10.0.2.15 to 10.0.2.255. Packet 22 is a detailed view of this announcement, showing details like 'Command: Domain/Workgroup Announcement (0x0c)', 'Update Count: 3', 'Update Periodicity: 12 minutes', 'Domain/Workgroup: WORKGROUP', 'Windows version: Windows 7 or Windows Server 2008 R2', 'OS Major Version: 6', 'OS Minor Version: 1', 'Server Type: 0x80001000, NT Workstation, Domain Enum', 'Browser Protocol Major Version: 15', 'Browser Protocol Minor Version: 1', 'Signature: 0xaa55', and 'Master Browser Server Name: USER-VIRTUALBOX'. The bottom pane shows the raw hex data of the packet, with a corresponding ASCII representation on the right. The hex data starts with 43 43 4e 46 47 45 4a 46, which corresponds to the ASCII string 'CCNFGEJF CFEFFEBE'.

Mais on n'a pas trouvé le contenu du fichier, mais on voit bien que le protocole smb a bien été effectuée.

4. Sur un schéma, faites apparaître les différents échanges entre le client et le serveur lors de la création et l'écriture dans un fichier.

