

NOM: Romà Sardá Casellas.

DATA 8-11-23

ÀREA/MATÈRIA

m08uf1pr1 - part pràctica

CURS 2DAW

1.- (20% de la nota de la pràctica) Realitza amb **telnet** una petició per demanar la pàgina inicial de **www.binefa.cat** indicant que la teva aplicació client és **telnet** i que la connexió es **tancarà** un cop has rebut la resposta. Mostra clarament:

a) La connexió realitzada amb telnet i el missatge de petició enviat.

```
vadimvolkov@archlinux ~-> telnet www.binefa.cat 80
Trying 51.89.23.164...
Connected to www.binefa.cat.
Escape character is '^]'.
GET / HTTP/1.1
Host: www.binefa.cat
User-Agent: telnet
Connection: close
```

COM ES POT APRECIAR CLARAMENT, HE DEMANAT CONNECTAR-ME PER PODER REBRE LA PÀGINA PRINCIPAL, AIXÍ FENT ÚS DELS CAMPS DE CAPÇALERA INDICATS.

b) La línia d'estat i el camps de la capçalera del missatge de resposta del servidor

```
HTTP/1.1 301 Moved Permanently
Server: nginx/1.21.1
Date: Wed, 08 Nov 2023 16:50:20 GMT
Content-Type: text/html
Content-Length: 169
Connection: close
Location: https://www.binefa.cat/
```

EN AQUEST CAS, EL SERVIDOR ENS HA DIT QUE LA PÀGINA INICIAL HA PASSAT DE FER SERVIR HTTP A HTTPS (COSA QUE ES POT APRECIAR A LA CAPÇALERA DE "Location") QUE ENS HA GENERAT AUTOMÀTICAMENT A CAUSA DE REBRE UN CODI DE RESPOSTA EQUIVALENT A 301. COM ESTIC FENT SERVIR TELNET NO EM REDIRECCIONA AUTOMÀTICAMENT, PERÒ SI ESTIGUÉS AL FIREFOX, DONCS SUPOSADAMENT SÍ QUE EM PORTARIA A LA PÀGINA QUE FA ÚS D'HTTPS.

c) El cos del missatge de resposta del servidor.

```
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.21.1</center>
</body>
</html>
Connection closed by foreign host.
vadimvolkov@archlinux ~-> █
```

ENS RETORNA UN HTML INDICANT QUE LA PÀGINA HA CANVIAT D'UBICACIÓ, AIXÒ APAREIX TANT EN EL TÍTOL COM A LA PÀGINA HTML EN SÍ (LO DE DINS DEL "<body></body>").

d) D'acord amb la resposta mostrada, descriu quin seria el comportament del navegador un cop rebuda la resposta

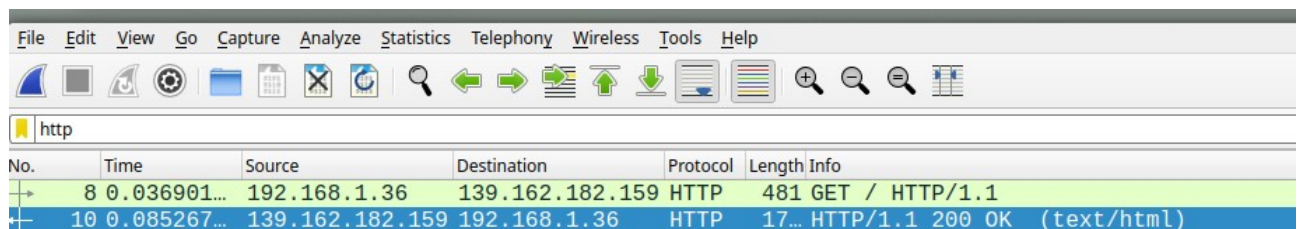
DONCS SUPOSO QUE SI ÉS UN NAVEGADOR MODERN ENS REDIRECCIONARIA A LA VERSIÓ DE LA PÀGINA QUE FA ÚS D'HTTPS AUTOMÀTICAMENT, SINÓ, HO HAURIEM DE FER MANUALMENT.

2.- (30% de la nota de la pràctica) Descarrega el fitxer:

- **GRUP 1:** <http://www.collados.org/daw2/m08/uf1/m08uf1pr1v1.pcapng>
- **GRUP 2:** <http://www.collados.org/daw2/m08/uf1/m08uf1pr1v2.pcapng>
- **GRUP 3:** <http://www.collados.org/daw2/m08/uf1/m08uf1pr1v3.pcapng> → EL MEU GRUP.
- **GRUP 4:** <http://www.collados.org/daw2/m08/uf1/m08uf1pr1v4.pcapng>

Obre'l amb **wireshark**. Mostra clarament i indica:

a) L'adreça IP del servidor d'acord amb el primer missatge de resposta del servidor.

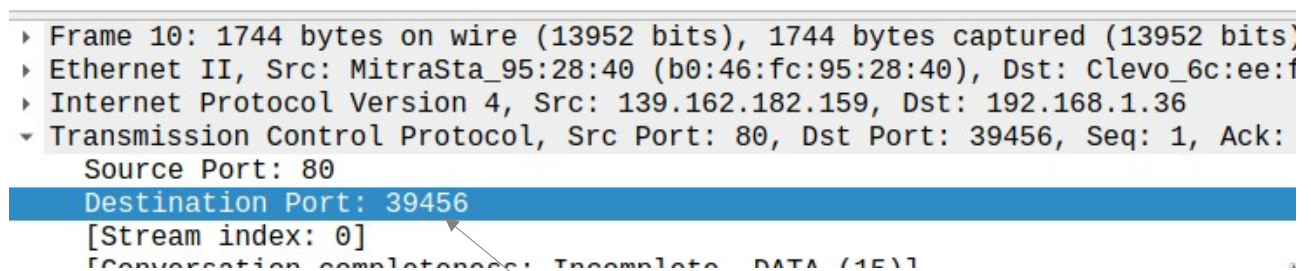


No.	Time	Source	Destination	Protocol	Length	Info
8	0.036901...	192.168.1.36	139.162.182.159	HTTP	481	GET / HTTP/1.1
10	0.085267...	139.162.182.159	192.168.1.36	HTTP	17...	HTTP/1.1 200 OK (text/html)

ADREÇA IP DEL SERVIDOR.

ES POR VEURE QUE L'IP DEL SERVIDOR ÉS: 139.162.182.159, MENTRES QUE LA DEL CLIENT ÉS: 192.168.1.36.

b) El port utilitzat pel programa client d'acord amb el primer missatge de resposta del servidor.



▶ Frame 10: 1744 bytes on wire (13952 bits), 1744 bytes captured (13952 bits)
▶ Ethernet II, Src: MitraSta_95:28:40 (b0:46:fc:95:28:40), Dst: Clevo_6c:ee:f
▶ Internet Protocol Version 4, Src: 139.162.182.159, Dst: 192.168.1.36
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 39456, Seq: 1, Ack:
Source Port: 80
Destination Port: 39456
[Stream index: 0]
[Conversation completeness: Incomplete DATA (15)]

PORT DEL NAVEGADOR DEL CLIENT

ES POT VEURE QUE PORT EL DEL PROGRAMA CLIENT ÉS: 39456, MENTRES QUE LA DEL SERVIDOR ÉS: 80, AMB LA QUAL COSA VOL DIR QUE SEGURAMENT ESTÀ FENT SERVIR APACHE.

c) Quantes cookies ha enviat el servidor al client d'acord amb el primer missatge de resposta del servidor?

```
› Ethernet II, Src: MitraSta_95:28:40 (b0:46:fc:95:28:40), Dst: Clevo_6c:ee:f2 (80:fa:5b:6c:ee:f2)
› Internet Protocol Version 4, Src: 139.162.182.159, Dst: 192.168.1.36
› Transmission Control Protocol, Src Port: 80, Dst Port: 39456, Seq: 1, Ack: 416, Len: 1678
› Hypertext Transfer Protocol
  › HTTP/1.1 200 OK\r\n
    Date: Wed, 27 Oct 2021 11:23:58 GMT\r\n
    Server: Apache\r\n
    Content-Encoding: gzip\r\n
    Vary: Accept-Encoding\r\n
  › Set-Cookie: compt=38; expires=Fri, 26-Nov-2021 11:23:58 GMT; Max-Age=2592000; path=/; domain=collados.org\r\n
  › Set-Cookie: datahora=27%2F10%2F2021+11%3A23%3A58; expires=Fri, 26-Nov-2021 11:23:58 GMT; Max-Age=2592000; path=/; domain=collados.org\r\n
    Strict-Transport-Security: max-age=31536000; includeSubdomains;\r\n
```

COM ES POT APRECIAR CLARAMENT, EL SERVIDOR HA ENVIAT 2 COOKIES, UNA ANOMENADA “compt” I TÉ UN VALOR DE 38, I UNA ALTRA AMB NOM: “datahora”, I TÉ UN VALIR MOLT LLARG QUE NO PENSO ESCRIURE.

d) Indica el nom i valor de la primera cookie enviada pel servidor al client.

```
› Hypertext Transfer Protocol
  › HTTP/1.1 200 OK\r\n
    Date: Wed, 27 Oct 2021 11:23:58 GMT\r\n
    Server: Apache\r\n
    Content-Encoding: gzip\r\n
    Vary: Accept-Encoding\r\n
  › Set-Cookie: compt=38; expires=Fri, 26-Nov-2021 11:23:58
  › Set-Cookie: datahora=27%2F10%2F2021+11%3A23%3A58; expire
```

COM ANTERIORMENT HE INDICAT, LA PRIMERA COOKIE TÉ EL NOM DE “compt” I TÉ UN VALOR EQUIVALENT A 38.

e) Indica dins de quin domini seria vàlida la segona cookie enviada pel servidor al client.

```
› Ethernet II, Src: MitraSta_95:28:40 (b0:46:fc:95:28:40), Dst: Clevo_6c:ee:f2 (80:fa:5b:6c:ee:f2)
› Internet Protocol Version 4, Src: 139.162.182.159, Dst: 192.168.1.36
› Transmission Control Protocol, Src Port: 80, Dst Port: 39456, Seq: 1, Ack: 416, Len: 1678
› Hypertext Transfer Protocol
  › HTTP/1.1 200 OK\r\n
    Date: Wed, 27 Oct 2021 11:23:58 GMT\r\n
    Server: Apache\r\n
    Content-Encoding: gzip\r\n
    Vary: Accept-Encoding\r\n
  › Set-Cookie: compt=38; expires=Fri, 26-Nov-2021 11:23:58 GMT; Max-Age=2592000; path=/; domain=collados.org\r\n
  › Set-Cookie: datahora=27%2F10%2F2021+11%3A23%3A58; expires=Fri, 26-Nov-2021 11:23:58 GMT; Max-Age=2592000; path=/; domain=collados.org\r\n
    Strict-Transport-Security: max-age=31536000; includeSubdomains;\r\n
```

COM ES POT APRECIAR, AL COSTAT DE path=/, HI HA UN CAMP QUE ES DIU “domain=collados.org”, I SEGONS LO QUE HE APRÈS A PHP, AIXÒ INDICA EL DOMINI EN EL QUAL AQUESTA COOKIE TÉ AFECTE.

ENVIAMENT DE LA PART PRÀCTICA:

a) Genera un fitxer PDF amb la resposta de nom **daw2_cognom_nom_m08uf1pr1.pdf** a on **cognom** és le teu **primer cognom real** i **nom** és el teu **nom real**.

b) Envia el fitxer adjunt a un missatge que s'ha d'enviar a **cf@collados.org** amb l'assumpte **daw2_cognom_nom_m08uf1pr1** a on **cognom** és le teu **primer cognom real** i **nom** és el teu **nom real**.