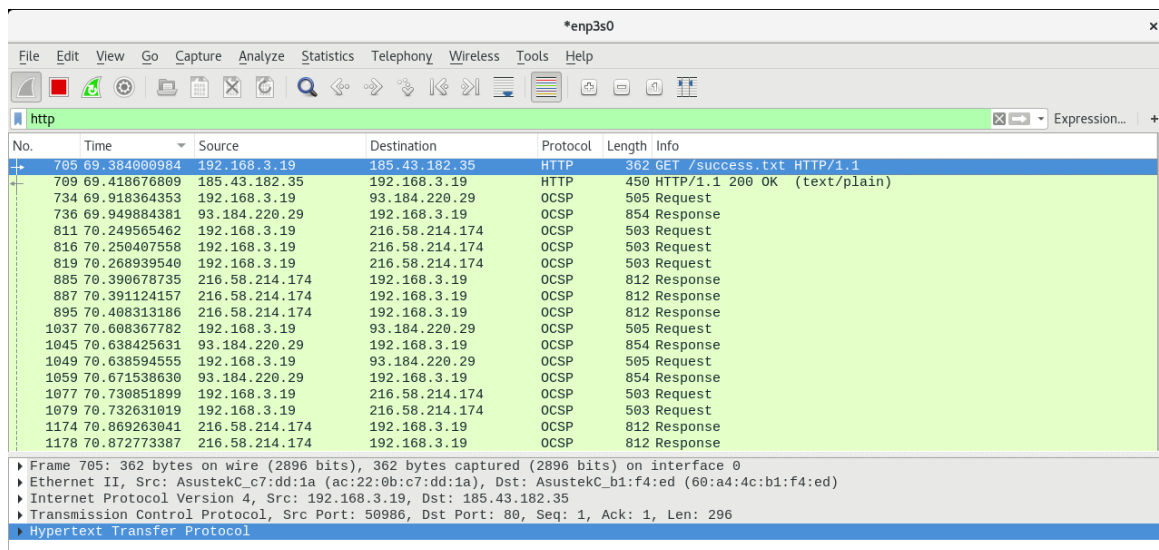


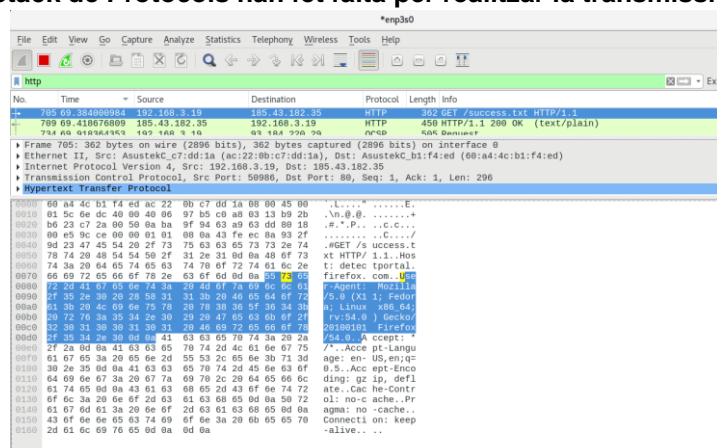
Carregueu la pàgina del Moodle de l'Escola Del Treball (<http://moodle.escoladeltreball.org/>) i, capturant amb el Wireshark, identifiqueu el paquet de protocol HTTP que fa la petició GET / HTTP/1.1.



El paquet identificat per el protocol es el “success.txt”

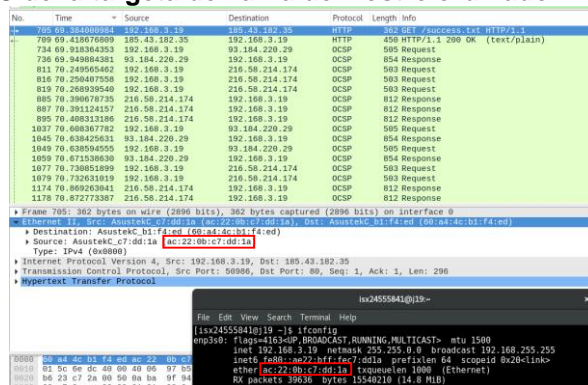
1. Un cop el tingueu localitzat, completeu els següents punts:

1. Quina Pila o Stack de Protocols han fet falta per realitzar la transmissió d'aquestes dades?



El protocol “Hypertext Trasnfer Protocol”

2. Feu una captura de les dades referents a la Capa d'Accés a la Xarxa. Quin protocol utilitza? Indiqueu les adreces MAC d'origen i destí de la trama. Quina d'aquestes dues adreces correspon a la MAC de la targeta de xarxa del vostre ordinador?



El protocol que utilitza la Capa d'Accés a la Xarxa es el Ethernet II.

Adreça MAC d'origen: ac:22:0b:c7:dd:1a

Adreça MAC de destí: 60:a4:4c:b1:f4:ed

En vermell esta marcat la adreça MAC que correspon a la mateixa adreça MAC de la targeta de xarxa de

l'ordinador, amb l'ordre "ifconfig" he pogut saber quina es.

**3. Feu una captura de les dades referents a la Capa d'Internet. Quin protocol utilitza? Indiqueu les adreces IP d'origen i destí del paquet.**

No.	Time	Source	Destination	Protocol	Length	Info
705	69.384000984	192.168.3.19	185.43.182.35	HTTP	362	GET /success.txt HTTP/1.1
709	69.418676809	185.43.182.35	192.168.3.19	HTTP	450	HTTP/1.1 200 OK (text/plain)
734	69.918364353	192.168.3.19	93.184.229.29	OCSP	505	Request
736	69.949884381	93.184.229.29	192.168.3.19	OCSP	854	Response
811	70.249565462	192.168.3.19	216.58.214.174	OCSP	503	Request
816	70.259497558	192.168.3.19	216.58.214.174	OCSP	503	Request
819	70.268939548	192.168.3.19	216.58.214.174	OCSP	503	Request
885	70.390678735	216.58.214.174	192.168.3.19	OCSP	812	Response
887	70.391124157	216.58.214.174	192.168.3.19	OCSP	812	Response
895	70.408313186	216.58.214.174	192.168.3.19	OCSP	812	Response
1037	70.608367782	192.168.3.19	93.184.229.29	OCSP	505	Request
1045	70.638425611	93.184.229.29	192.168.3.19	OCSP	854	Response
1049	70.638594555	192.168.3.19	93.184.229.29	OCSP	505	Request
1059	70.671538638	93.184.229.29	192.168.3.19	OCSP	854	Response
1077	70.730851899	192.168.3.19	216.58.214.174	OCSP	503	Request
1079	70.732631819	192.168.3.19	216.58.214.174	OCSP	503	Request
1174	70.869263041	216.58.214.174	192.168.3.19	OCSP	812	Response
1178	70.872773387	216.58.214.174	192.168.3.19	OCSP	812	Response

Internet Protocol Version 4, Src: 192.168.3.19, Dst: 185.43.182.35

0100 ... = Version: 4

... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 348

Identification: 0x6edc (28380)

Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 64

Protocol: TCP (6)

Header checksum: 0x97b5 [validation disabled]

Source: 192.168.3.19

Destination: 185.43.182.35

[Source GeoIP: Unknown]

En la Capa d'internet el protocol utilitzat es el Protocol de internet la versió num. 4  
Les adreces IP de origen i destí son:

- Origen: 192.168.3.19
- Destí: 185.43.182.35

**4. Feu una captura de les dades referents a la Capa de Transport. Quin protocol utilitza? Indiqueu el port d'origen i destí del segment.**

No.	Time	Source	Destination	Protocol	Length	Info
705	69.384000984	192.168.3.19	185.43.182.35	HTTP	362	GET /success.txt HTTP/1.1
709	69.418676809	185.43.182.35	192.168.3.19	HTTP	450	HTTP/1.1 200 OK (text/plain)
734	69.918364353	192.168.3.19	93.184.229.29	OCSP	505	Request

Frame 705: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits) on interface 0

Ethernet II, Src: AsustekC\_c7:dd:1a (ac:22:0b:c7:dd:1a), Dst: AsustekC\_b1:f4:ed (60:a4:4c:b1:f4:ed)

Internet Protocol Version 4, Src: 192.168.3.19, Dst: 185.43.182.35

Transmission Control Protocol, Src Port: 50986, Dst Port: 80, Seq: 1, Ack: 1, Len: 296

Source Port: 50986

Destination Port: 80

[Stream index: 13]

[TCP Segment Len: 296]

Sequence number: 1 (relative sequence number)

[Next sequence number: 297 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Header Length: 32 bytes

Internet Protocol Version 4, Src: 192.168.3.19, Dst: 185.43.182.35

Transmission Control Protocol, Src Port: 50986, Dst Port: 80, Seq: 1, Ack: 1, Len: 296

HyperText Transfer Protocol

GET /success.txt HTTP/1.1\r\n

Request Info (CharSequence): GET /success.txt HTTP/1.1\r\n

Request Method: GET

Request URI: /success.txt

Request Version: HTTP/1.1

User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86\_64; rv:54.0) Gecko/20100101 Firefox/54.0\r\n

Accept: \*/\*\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Cache-Control: no-cache\r\n

Pragma: no-cache\r\n

Connection: keep-alive\r\n

\r\n

Full request URI: http://detectportal.firefox.com/success.txt

Header request [14]

[Response in frame: 709]

[Next request in frame: 2291]

El protocol utilitzat es el protocol de control de transmissió  
Els port que utilitza son:

- Origen: 50986
- Destí: 80

**5. Feu una captura de les dades referents a la Capa d'Aplicació. Quin protocol utilitza? Quina és l'URL de destí de les dades?**

No.	Time	Source	Destination	Protocol	Length	Info
705	69.384000984	192.168.3.19	185.43.182.35	HTTP	362	GET /success.txt HTTP/1.1
709	69.418676809	185.43.182.35	192.168.3.19	HTTP	450	HTTP/1.1 200 OK (text/plain)
734	69.918364353	192.168.3.19	93.184.229.29	OCSP	505	Request

Frame 705: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits) on interface 0

Ethernet II, Src: AsustekC\_c7:dd:1a (ac:22:0b:c7:dd:1a), Dst: AsustekC\_b1:f4:ed (60:a4:4c:b1:f4:ed)

Internet Protocol Version 4, Src: 192.168.3.19, Dst: 185.43.182.35

Transmission Control Protocol, Src Port: 50986, Dst Port: 80, Seq: 1, Ack: 1, Len: 296

HyperText Transfer Protocol

GET /success.txt HTTP/1.1\r\n

Request Info (CharSequence): GET /success.txt HTTP/1.1\r\n

Request Method: GET

Request URI: /success.txt

Request Version: HTTP/1.1

User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86\_64; rv:54.0) Gecko/20100101 Firefox/54.0\r\n

Accept: \*/\*\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Cache-Control: no-cache\r\n

Pragma: no-cache\r\n

Connection: keep-alive\r\n

\r\n

Full request URI: http://detectportal.firefox.com/success.txt

Header request [14]

[Response in frame: 709]

[Next request in frame: 2291]

El protocol que utilitza aquesta ultima capa es el protocol HTTP  
L'URL de destí de dades es http://detectportal.firefox.com/succes.txt

2. Identifiqueu ara el paquet de resposta a aquesta petició (suggeriment: cada paquet que captura Wireshark especifica en quin *frame* podem esperar la resposta).

- Quina Pila o Stack de Protocols han fet falta per realitzar la transmissió d'aquestes dades? Quina diferència hi ha respecte de l'exercici anterior?

No.	Time	Source	Destination	Protocol	Length	Info
705	69.384000984	192.168.3.19	185.43.182.35	HTTP	362	GET /success.txt HTTP/1.1
709	69.418676809	185.43.182.35	192.168.3.19	HTTP	450	HTTP/1.1 200 OK (text/plain)
▶ Frame 709: 450 bytes on wire (3600 bits), 450 bytes captured (3600 bits) on interface 0 ▶ Ethernet II, Src: AsustekC_b1:f4:ed (60:a4:4c:b1:f4:ed), Dst: AsustekC_c7:dd:1a (ac:22:0b:c7:dd:1a) ▶ Internet Protocol Version 4, Src: 185.43.182.35, Dst: 192.168.3.19 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50986, Seq: 1, Ack: 297, Len: 384 ▶ Hypertext Transfer Protocol Line-based text data: text/plain						

Respecte l'exercici anterior s'ha afegir una nova línia anomenada "Line-based text data: text/plain"

- Feu una captura de les dades referents a la Capa d'Accés a la Xarxa. Quin protocol utilitza? Indiqueu les adreces MAC d'origen i destí de la trama. Quina d'aquestes dues adreces correspon a la MAC de la targeta de xarxa del vostre ordinador? Comproveu que les adreces MAC d'origen i destí són les mateixes que en el cas anterior però en l'ordre invertit.

No.	Time	Source	Destination	Protocol	Length	Info
705	69.384000984	192.168.3.19	185.43.182.35	HTTP	362	GET /success.txt HTTP/1.1
709	69.418676809	185.43.182.35	192.168.3.19	HTTP	450	HTTP/1.1 200 OK (text/plain)
▶ Frame 709: 450 bytes on wire (3600 bits), 450 bytes captured (3600 bits) on interface 0 ▶ Ethernet II, Src: AsustekC_b1:f4:ed (60:a4:4c:b1:f4:ed), Dst: AsustekC_c7:dd:1a (ac:22:0b:c7:dd:1a) ▶ Destination: AsustekC_c7:dd:1a (ac:22:0b:c7:dd:1a) Address: AsustekC_c7:dd:1a (ac:22:0b:c7:dd:1a) ..0. .... = LG bit: Globally unique address (factory default) ....0. .... = IG bit: Individual address (unicast) ▶ Source: AsustekC_b1:f4:ed (60:a4:4c:b1:f4:ed) Address: AsustekC_b1:f4:ed (60:a4:4c:b1:f4:ed) ..0. .... = LG bit: Globally unique address (factory default) ....0. .... = IG bit: Individual address (unicast) Type: IPv4 (0x0800) ▶ Internet Protocol Version 4, Src: 185.43.182.35, Dst: 192.168.3.19 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50986, Seq: 1, Ack: 297, Len: 384 ▶ Hypertext Transfer Protocol Line-based text data: text/plain						

Aquesta capa utilitza el protocol "Ethernet II"

Les adreces MAC corresponen al mateix exerci anterior tant com la de origen com la adreça MAC de la targeta de l'ordinador, però la diferencia que hi ha es que la adreça MAC de l'ordinador ara es a de destí.

- Feu una captura de les dades referents a la Capa d'Internet. Quin protocol utilitza? Indiqueu les adreces IP d'origen i destí del paquet. Comproveu que les adreces IP d'origen i destí són les mateixes que en el cas anterior però en l'ordre invertit.

No.	Time	Source	Destination	Protocol	Length	Info
705	69.384000984	192.168.3.19	185.43.182.35	HTTP	362	GET /success.txt HTTP/1.1
709	69.418676809	185.43.182.35	192.168.3.19	HTTP	450	HTTP/1.1 200 OK (text/plain)
714	69.418676852	192.168.3.19	185.43.182.35	HTTP	450	HTTP/1.1 200 OK (text/plain)
▶ Frame 709: 450 bytes on wire (3600 bits), 450 bytes captured (3600 bits) on interface 0 ▶ Ethernet II, Src: AsustekC_b1:f4:ed (60:a4:4c:b1:f4:ed), Dst: AsustekC_c7:dd:1a (ac:22:0b:c7:dd:1a) ▶ Internet Protocol Version 4, Src: 185.43.182.35, Dst: 192.168.3.19						
0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 436 Identification: 0xfe99 (65177) ▶ Flags: 0x02 (Don't Fragment) Fragment offset: 0 Time to live: 55 Protocol: TCP (6) ▶ Header checksum: 0x10a0 [validation disabled] Source: 185.43.182.35 Destination: 192.168.3.19 [Source GeoIP: Unknown] [Destination GeoIP: Unknown] ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50986, Seq: 1, Ack: 297, Len: 384 ▶ Hypertext Transfer Protocol ▶ Line-based text data: text/plain						
0000	ac 22 0b c7 dd 1a 60 a4	4c b1 f4 ed 08 00 45 00	.....L.....			
0010	01 b4 fe 99 40 00 37 06	10 a0 b9 2b b6 23 c0 a8	...0.7. ....#...			
0020	03 13 00 50 c7 2a 63 a9	63 dd 0a ba a0 bc 80 18	...P.*C. ....			
0030	03 ab 85 31 00 00 01 01	08 0a 93 2f 9d 45 43 fe	...1.....//EC.			

La capa d'internet te com a protocol el protocol Internet versió 4. En aquest cas les adreces tan com la de destí i origen són les mateixes però amb l'ordre canviat.

- Feu una captura de les dades referents a la Capa de Transport. Quin protocol utilitza? Indiqueu el port d'origen i destí del segment. Comproveu que els ports estan invertits respecte de l'exercici anterior.

No.	Time	Source	Destination	Protocol	Length	Info
705	69.384000984	192.168.3.19	185.43.182.35	HTTP	362	GET /success.txt HTTP/1.1
709	69.418676809	185.43.182.35	192.168.3.19	HTTP	450	HTTP/1.1 200 OK (text/plain)
714	69.418676852	192.168.3.19	185.43.182.35	HTTP	450	HTTP/1.1 200 OK (text/plain)
▶ Frame 709: 450 bytes on wire (3600 bits), 450 bytes captured (3600 bits) on interface 0 ▶ Ethernet II, Src: AsustekC_b1:f4:ed (60:a4:4c:b1:f4:ed), Dst: AsustekC_c7:dd:1a (ac:22:0b:c7:dd:1a) ▶ Internet Protocol Version 4, Src: 185.43.182.35, Dst: 192.168.3.19 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50986, Seq: 1, Ack: 297, Len: 384						
Source Port: 80 Destination Port: 50986 [Stream index: 13] [TCP Segment Len: 384] Sequence number: 1 (relative sequence number) [Next sequence number: 385 (relative sequence number)] Acknowledgment number: 297 (relative ack number) Header Length: 32 bytes ▶ Flags: 0x018 (PSH, ACK) Window size value: 939 [Calculated window size: 30048] [Window size scaling factor: 32] ▶ Checksum: 0x8531 [validation disabled] Urgent pointer: 0 ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps ▶ [SEQ/ACK analysis] ▶ Hypertext Transfer Protocol ▶ Line-based text data: text/plain						
0020	03 13 00 50 c7 2a 63 a9	63 dd 0a ba a0 bc 80 18	...P.*C. ....			
0030	03 ab 85 31 00 00 01 01	08 0a 93 2f 9d 45 43 fe	...1.....//EC.			
0040	ec 8a 48 54 54 50 2f 31	2e 31 20 32 30 30 20 4f	...HTTP/1.1 200 0			
0050	4b 0d 0a 43 6f 6e 74 65	6e 74 2d 54 79 70 65 3a	K..Content-Type:			
0060	20 74 65 78 74 2f 70 6c	61 69 6e 0d 0a 43 6f 6e	text/plain..Con			
0070	74 65 6e 74 2d 4c 65 6e	67 74 68 3a 20 38 0d 0a	tent-Length: 8..			

Aquesta capa mostrada com la de transport utilitza el protocol de control de transmissió, el ports que mostra són exactament els mateixos però canvia de ordre.

## 5. Feu una captura de les dades referents a la Capa d'Aplicació. Quin protocol utilitza?

http						
No.	Time	Source	Destination	Protocol	Length	Info
705	69.384000984	192.168.3.19	185.43.182.35	HTTP	362	GET /success.txt HTTP/1.1
709	69.418676809	185.43.182.35	192.168.3.19	HTTP	450	HTTP/1.1 200 OK (text/plain)
711	69.418764353	192.168.3.19	185.43.182.35	ICMP	565	Destination unreachable
▶ Frame 709: 450 bytes on wire (3600 bits), 450 bytes captured (3600 bits) on interface 0						
▶ Ethernet II, Src: AsustekC_b1:f4:ed (60:a4:4c:b1:f4:ed), Dst: AsustekC_c7:dd:1a (ac:22:0b:c7:dd:1a)						
▶ Internet Protocol Version 4, Src: 185.43.182.35, Dst: 192.168.3.19						
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50986, Seq: 1, Ack: 297, Len: 384						
Hypertext Transfer Protocol						
▶ HTTP/1.1 200 OK\r\n						
Content-Type: text/plain\r\n						
Content-Length: 8\r\n						
Last-Modified: Mon, 15 May 2017 18:04:40 GMT\r\n						
ETag: "ae780585f49b94ce1444eb7d28906123"\r\n						
Accept-Ranges: bytes\r\n						
Server: AmazonS3\r\n						
X-Amz-Cf-Id: V7j9NpQTXcQtb-ZLBwIn0FqT5kKZifRlFKSiqCXG-auU2ibLI_N7g==\r\n						
Cache-Control: no-cache, no-store, must-revalidate\r\n						
Date: Tue, 17 Oct 2017 10:40:34 GMT\r\n						
Connection: keep-alive\r\n						
\r\n						
[HTTP response 1/2]						
[Time since request: 0.034675825 seconds]						
[Request in frame: 705]						
[Next request in frame: 2291]						
[Next response in frame: 2296]						
File Data: 8 bytes						
Line-based text data: text/plain						
0040	ec 8a 48 54 54 50 2f 31	2e 31 20 32 30 30 20 4f	..HTTP/1.1 200 OK			
0050	4d 0d 0a 43 6f 6e 74 65	6e 74 2d 54 79 70 65 3a	K..Content-Type:			
0060	20 74 65 78 74 2f 79 6c	61 69 6e 0d 0a 43 6f 6e	text/plain..Con			
0070	74 65 6e 74 2d 4c 65 6e	67 74 68 3a 20 38 0d 0a	tent-Length: 8..			
0080	4c 61 73 74 2d 4d 6f 64	69 66 69 65 64 3a 20 4d	Last-Modified: M			
0090	6f 6e 2c 20 31 35 20 4d	61 79 20 32 30 31 37 20	on, 15 May 2017,			
00a0	31 38 3a 30 34 3a 34 30	20 47 4d 54 0d 0a 45 54	18:04:40 GMT..ET			
00b0	61 67 3a 20 22 61 65 37	38 30 35 38 35 66 34 39	ag: "ae7 80585f49			
00c0	62 39 34 63 65 31 34 34	34 65 62 37 64 32 38 39	b94ce144 4eb7d289			
00d0	30 36 31 32 33 22 0d 0a	41 63 63 65 70 74 2d 52	06123".. Accept-R			
00e0	61 6e 67 65 73 3a 20 62	79 74 65 73 0d 0a 53 65	anges: bytes..Se			
00f0	72 76 65 72 3a 20 41 6d	61 7a 6f 6e 53 33 0d 0a	rver: Am azonS3..			
0100	58 2d 41 6d 7a 2d 43 66	2d 49 64 3a 20 56 37 6a	X-Amz-Cf -Id: V7j			
0110	39 4e 70 51 54 58 63 51	74 62 2d 5a 4c 42 77 49	9NpQTXcQ tb-ZLBwI			
0120	6e 30 46 71 54 35 6b 4b	5a 69 66 52 6c 66 4b 53	n0FqT5kK ZifRlFKS			
0130	69 71 43 78 47 2d 5f 61	75 55 32 69 62 4c 49 5f	iqCXG-_a uU2ibLI			
0140	4e 37 67 3d 3d 0d 0a 43	61 63 68 65 2d 43 6f 6e	N7g==..C ache-Con			
0150	74 72 6f 6c 3a 20 6e 6f	2d 63 61 63 68 65 2c 20	trol: no -cache,			
0160	6e 6f 2d 73 74 6f 72 65	2c 20 6d 75 73 74 2d 72	no-store , must-r			

La ultima capa, la capa d'aplicació funciona amb el protocol HTTP

## 6. En aquest cas, el paquet té algun contingut que pugueu identificar? Feu-ne una captura.