Pt3 – Wireshark

Nom de l'alumne: Marc Villalobos Figueras

ENUNCIAT

Es tracta d'utilitzar el programa wireshark per capturar els paquets de dades relacionats amb una navegació web.

Per fer-ho utilitzarem un navegador web qualsevol per visualitzar el web http://www.iesmontilivi.cat cal capturar tant la petició DNS i resposta, com la petició web i resposta del servidor web.

Detectar l'establiment i finalització de la connexió al web mostrat.

Tot seguit farem clic a sobre d'un dels articles que contingui un vídeo, secció Extraescolars de l'institut. Iniciar el vídeo de youtube i cercar si ho fa via TCP/UDP.

Si és via TCP. Demostrar que hi ha negociació inicial de la connexió.

Si és via UDP. Demostrar que no hi ha negociació i que comença la transmissió sense fer-ho.

Visualitzar el possible canvis en el Tamany de finestra WS al llarg de la comunicació.

Fer la pràctica des de dos entorns:

1. dins la xarxa del centre

2. des de fora del centre, casa per exemple

Documentar els canvis en les ip's i mac's oportunes en cada cas

.

Cal presentar un document .PDF on es visualitzi clarament els paquets/trames. Cal documentar i justificar els valors.

Puntuació:

Format document (2p):

Contngut (4p);

Desenvolupament (4p):

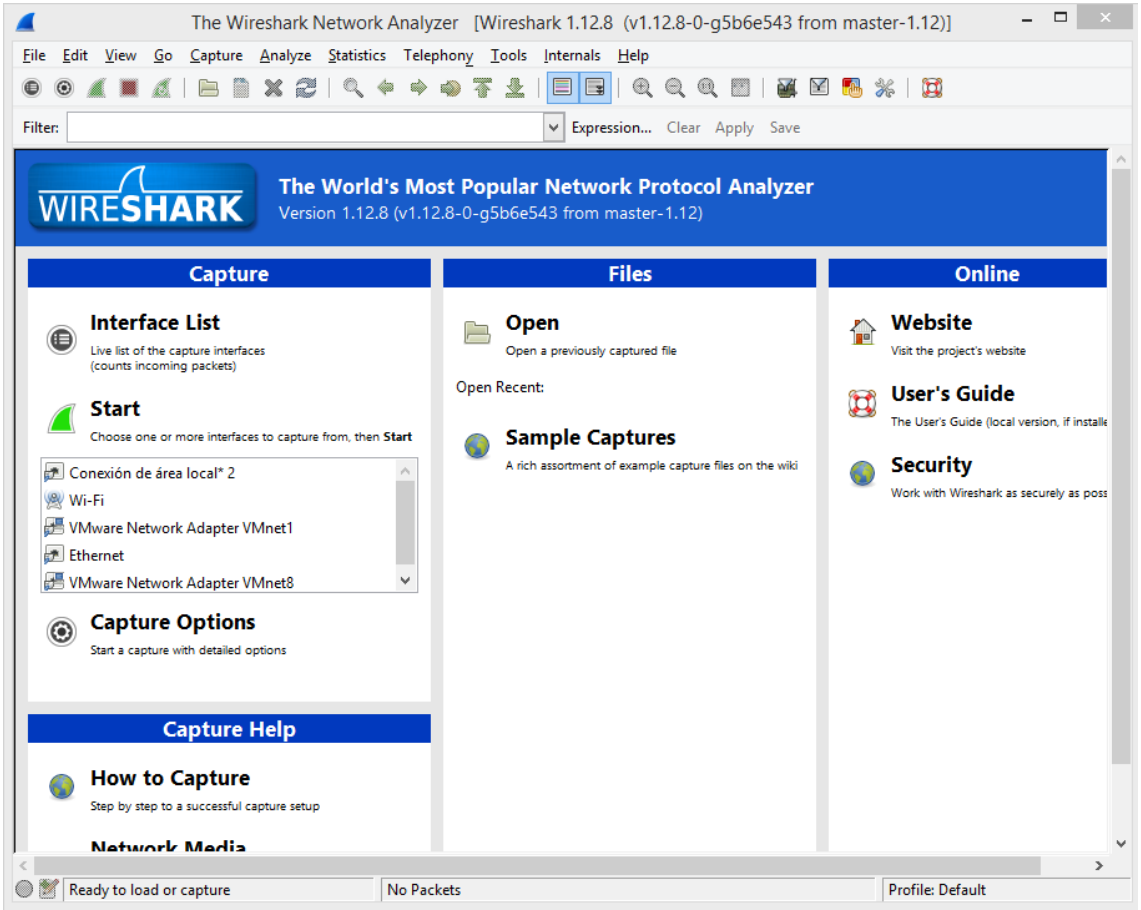
XARXA INSTITUT

En aquesta captura de pantalla, podem veure la configuració ip, que tenim dintre de la xarxa del centre.

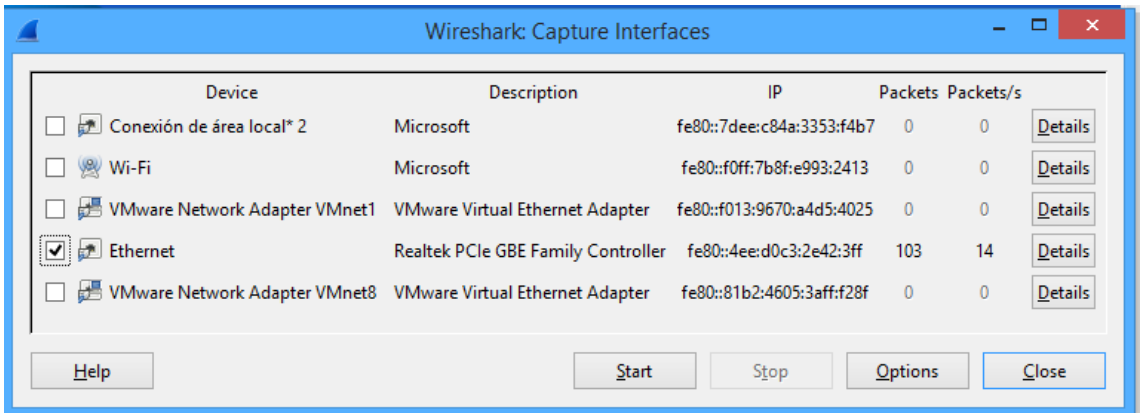
Configuració IP:

```
Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . : iesmontilivi.net
   Vínculo: dirección IPv6 local. . . : fe80::4ee:d0c3:2e42:3ff%3
   Dirección IPv4. . . . . . . . . . . . : 172.17.200.8
   Máscara de subred . . . . . . . . . . : 255.255.0.0
   Puerta de enlace predeterminada . . . . . : 172.17.1.1
```

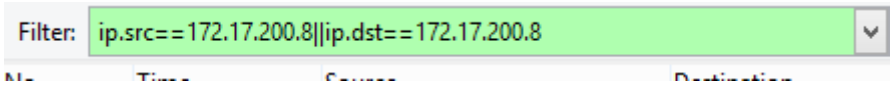
El primer que tenim que fer es entrar al Wireshark.



Tot seguit cliquem sobre *Interficie List*, i triem la nostra interfície de xarxa, que en aquest cas serà *Ethernet*, i tot seguit cliquem sobre *Start*.



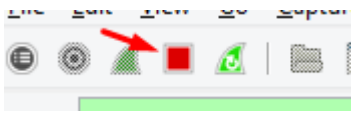
Un cop fet el pas anterior, escrivim el següent:



Un cop hem escrit això, pressionem *Enter*, i ja comença a capturar paquets.

A continuació obrim un navegador i accedim a la pàgina web de l'institut, perquè capturi els paquets que volem.

Després, al cap d'una estona, cliquem aturem la captura de paquets clicant sobre:



Llavors, anem a buscar els paquets que ens interessen.

Primer de tot, busquem les peticions DNS.

Captura de petició DNS:

```
1422 2016-11-11 :172.17.200.8   172.17.1.5      DNS      80 Standard query 0x7fc5  A www.iesmontilivi.cat
1423 2016-11-11 :172.17.1.5     172.17.200.8    DNS      96 Standard query response 0x7fc5  A 172.17.1.5
1459 2016-11-11 :172.17.200.8   172.17.1.5      DNS      85 Standard query 0xf50a  A erp.institutmontilivi.cat
1460 2016-11-11 :172.17.1.5     172.17.200.8    DNS     101 Standard query response 0xf50a  A 172.17.1.6
```

Un cop fet això, busquem i capturem la petició i resposta DNS de iesmontilivi.net, i observem el contingut dels seus paquets, i també mirarem quins són les peticións i quins les respostes.

Pregunta:

iesmontilivi.cat:

Aquí tenim la petició DNS, que li fem a www.iesmontilivi.cat.

```
No.   Time                Source          Destination     Protoco  Length  Info
 1265 2016-11-11 :172.17.200.8   172.17.1.5      DNS        89 Standard query 0xb1db  A statsfe2.update.microsoft.com
 1279 2016-11-11 :172.17.1.5     172.17.200.8    DNS       543 Standard query response 0xb1db  CNAME statsfe2.update.mic
 1422 2016-11-11 :172.17.200.8   172.17.1.5      DNS        80 Standard query 0x7fc5  A www.iesmontilivi.cat
 1423 2016-11-11 :172.17.1.5     172.17.200.8    DNS        96 Standard query response 0x7fc5  A 172.17.1.5
```

```
⊞ Frame 1422: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
⊞ Ethernet II, Src: QuantaCo_b7:55:0c (c4:54:44:b7:55:0c), Dst: DellInc_c0:bf:e8 (00:1c:23:c0:bf:e8)
⊞ Internet Protocol Version 4, Src: 172.17.200.8 (172.17.200.8), Dst: 172.17.1.5 (172.17.1.5)
⊞ User Datagram Protocol, Src Port: 64928 (64928), Dst Port: 53 (53)
⊟ Domain Name System (query)
    [Response In: 1423]
    Transaction ID: 0x7fc5
  ⊟ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.iesmontilivi.cat: type A, class IN
        Name: www.iesmontilivi.cat
        [Name Length: 20]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

iesmontilivi.net:

Aquí tenim la petició DNS, que li fem a www.iesmontilivi.net.

```
Domain Name System (query)
    [Response In: 2163]
    Transaction ID: 0x2e32
  Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    iesmontilivi.net: type A, class IN
        Name: iesmontilivi.net
        [Name Length: 16]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Resposta:

iesmontilivi.cat:

Aquí tenim la resposta del servidor DNS de www.iesmontilivi.cat al nostre ordinador.

```
Domain Name System (response)
    [Request In: 1422]
    [Time: 0.000884000 seconds]
    Transaction ID: 0x7fc5
  Flags: 0x8580 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .1.. .... .... = Authoritative: Server is an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.iesmontilivi.cat: type A, class IN
        Name: www.iesmontilivi.cat
        [Name Length: 20]
        [Label Count: 3]
        Type: A (Host Address) (1)
```

iesmontilivi.net

Aquí tenim la resposta del servidor DNS de www.iesmontilivi.net al nostre ordinador.

```
Domain Name System (response)
    [Request In: 2161]
    [Time: 0.000765000 seconds]
    Transaction ID: 0x2e32
  Flags: 0x8580 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .1.. .... .... = Authoritative: Server is an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  Queries
    iesmontilivi.net: type A, class IN
        Name: iesmontilivi.net
        [Name Length: 16]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  Answers
    iesmontilivi.net: type A, class IN, addr 172.17.1.5
    iesmontilivi.net: type A, class IN, addr 172.17.1.10
    iesmontilivi.net: type A, class IN, addr 172.17.1.16
```

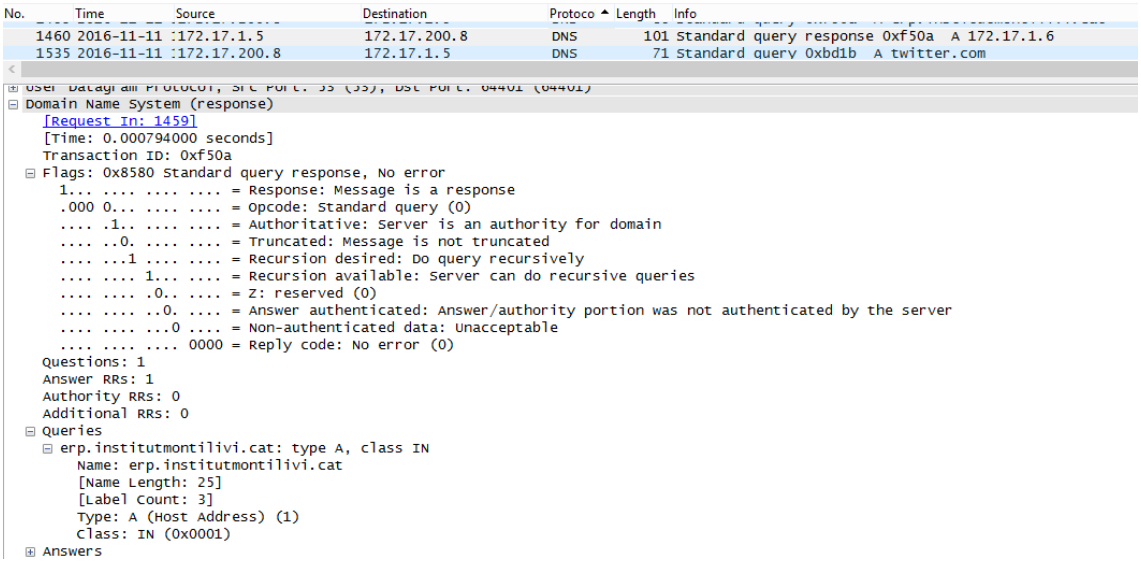
Pregunta:

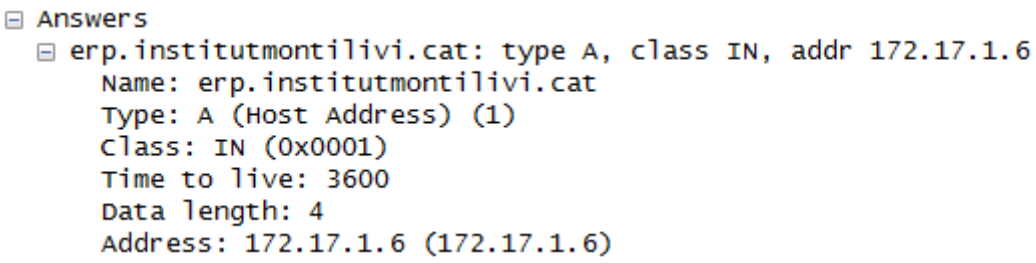
Aquí tenim la petició DNS, que li fem a www.iesmontilivi.cat.

```
Filter: ip.src==172.17.200.8||ip.dst==172.17.200.8   Expression... Clear Apply Save

No.  Time          Source          Destination     Protoco Length Info
1423 2016-11-11 :172.17.1.5      172.17.200.8    DNS        96 Standard query response 0x7fc5  A 172.17.1.5
1459 2016-11-11 :172.17.200.8    172.17.1.5      DNS        85 Standard query 0xf50a  A erp.institutmontilivi.cat
1460 2016-11-11 :172.17.1.5      172.17.200.8    DNS       101 Standard query response 0xf50a  A 172.17.1.6
1535 2016-11-11 :172.17.200.8    172.17.1.5      DNS        71 Standard query 0xbd1b  A twitter.com

Frame 1459: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
Ethernet II, Src: QuantaCo_b7:55:0c (c4:54:44:b7:55:0c), Dst: DellInc_c0:bf:e8 (00:1c:23:c0:bf:e8)
Internet Protocol Version 4, Src: 172.17.200.8 (172.17.200.8), Dst: 172.17.1.5 (172.17.1.5)
User Datagram Protocol, Src Port: 64401 (64401), Dst Port: 53 (53)
Domain Name System (query)
    [Response In: 1460]
    Transaction ID: 0xf50a
  Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    erp.institutmontilivi.cat: type A, class IN
        Name: erp.institutmontilivi.cat
        [Name Length: 25]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Resposta:

Aquí tenim la resposta del servidor DNS de www.iesmontilivi.cat al nostre ordinador.





A continuació, mirarem les peticions que li fem al servidor web, i les respostes que ens dona el servidor a nosaltres.

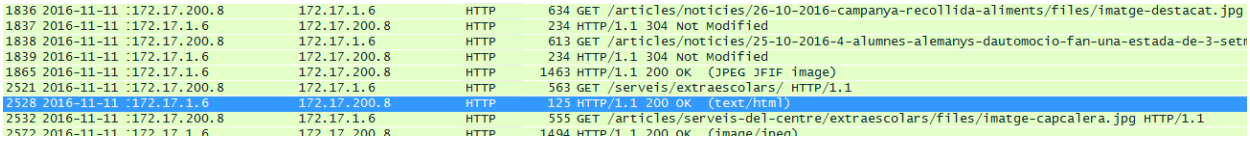
Tot aquest procés, es duu a terme mitjançant el protocol HTTP.

Cada petició de pàgina web (HTTP):

A continuació, podem veure unes captures de pantalla observant la comunicació que establim nosaltres amb el servidor web.

Pregunta:

Aquí tenim una captura de la petició que fem nosaltres al servidor web, per poder establir una connexió.



```
Hypertext Transfer Protocol
  GET /serveis/extraescolars/ HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /serveis/extraescolars/ HTTP/1.1\r\n]
       [GET /serveis/extraescolars/ HTTP/1.1\r\n]
       [Severity level: Chat]
       [Group: Sequence]
     Request Method: GET
     Request URI: /serveis/extraescolars/
     Request Version: HTTP/1.1
  Host: erp.institutmontilivi.cat:8888\r\n
  Connection: keep-alive\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.86 Safari/537.36\r\n
  Referer: http://erp.institutmontilivi.cat:8888/\r\n
  Accept-Encoding: gzip, deflate, sdch\r\n
  Accept-Language: es-ES,es;q=0.8\r\n
  Cookie: PHPSESSID=cu5b689umfn0cramhujlur5a71\r\n
    Cookie pair: PHPSESSID=cu5b689umfn0cramhujlur5a71
  \r\n
  [Full request URI: http://erp.institutmontilivi.cat:8888/serveis/extraescolars/]
  [HTTP request 5/5]
  [Prev request in frame: 965]
  [Response in frame: 974]
```

Resposta:

Aquí podem observar, la resposta que ens dona el servidor web, per poder establir la connexió.

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Fri, 11 Nov 2016 10:07:59 GMT\r\n
  Server: Apache/2.4.7 (Ubuntu)\r\n
  Last-Modified: Thu, 10 Nov 2016 22:05:33 GMT
  ETag: "23300-540f99288c714"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 144128\r\n
  Keep-Alive: timeout=5, max=99\r\n
  Connection: Keep-Alive\r\n
  Content-Type: image/jpeg\r\n
  \r\n
  [HTTP response 2/2]
  [Time since request: 0.045917000 seconds]
  [Prev request in frame: 1484]
  [Prev response in frame: 1532]
  [Request in frame: 1565]
JPEG File Interchange Format
```

A continuación, podem veure una captura de pantlla de tots els paquets HTTP.

Captura peticions de pàgina web (HTTP):

```
1685 2016-11-11 :172.17.1.6      172.17.200.8     HTTP      191 HTTP/1.1 200 OK  (JPEG JFIF image)
1687 2016-11-11 :172.17.200.8    172.17.1.6       HTTP      562 GET /articles/noticies/09-11-2016-convocatoria-deleccions-al-consell-escolar/files/imatge-
1688 2016-11-11 :172.17.200.8    172.17.1.6       HTTP      579 GET /articles/noticies/08-11-2016-reconeixement-al-centre-per-la-recollida-selectiva-de-pi
1697 2016-11-11 :172.17.200.8    172.17.1.6       HTTP      662 GET /articles/noticies/03-11-2016-nova-convocatoria-del-concurs-els-anuncis-que-xerriquen/
1724 2016-11-11 :172.17.1.6      172.17.200.8     HTTP     1391 HTTP/1.1 200 OK  (JPEG JFIF image)
1754 2016-11-11 :172.17.1.6      172.17.200.8     HTTP      603 HTTP/1.1 200 OK  (PNG)
1755 2016-11-11 :172.17.1.6      172.17.200.8     HTTP      235 HTTP/1.1 304 Not Modified
1825 2016-11-11 :172.17.1.6      172.17.200.8     HTTP      661 HTTP/1.1 200 OK  (JPEG JFIF image)
1835 2016-11-11 :172.17.200.8    172.17.1.6       HTTP      702 GET /articles/noticies/02-11-2016-alumnes-deducacio-i-control-ambiental-del-institut-monti
1836 2016-11-11 :172.17.200.8    172.17.1.6       HTTP      634 GET /articles/noticies/26-10-2016-campanya-recollida-aliments/files/imatge-destacat.jpg HT
1837 2016-11-11 :172.17.1.6      172.17.200.8     HTTP      234 HTTP/1.1 304 Not Modified
1838 2016-11-11 :172.17.200.8    172.17.1.6       HTTP      613 GET /articles/noticies/25-10-2016-4-alumnes-alemanys-dautomocio-fan-una-estada-de-3-setman
1839 2016-11-11 :172.17.1.6      172.17.200.8     HTTP      234 HTTP/1.1 304 Not Modified
1865 2016-11-11 :172.17.1.6      172.17.200.8     HTTP     1463 HTTP/1.1 200 OK  (JPEG JFIF image)
2521 2016-11-11 :172.17.200.8    172.17.1.6       HTTP      563 GET /serveis/extraescolars/ HTTP/1.1
2528 2016-11-11 :172.17.1.6      172.17.200.8     HTTP      125 HTTP/1.1 200 OK  (text/html)
2532 2016-11-11 :172.17.200.8    172.17.1.6       HTTP      555 GET /articles/serveis-del-centre/extraescolars/files/imatge-capcalera.jpg HTTP/1.1
2572 2016-11-11 :172.17.1.6      172.17.200.8     HTTP     1494 HTTP/1.1 200 OK  (image/jpeg)
```

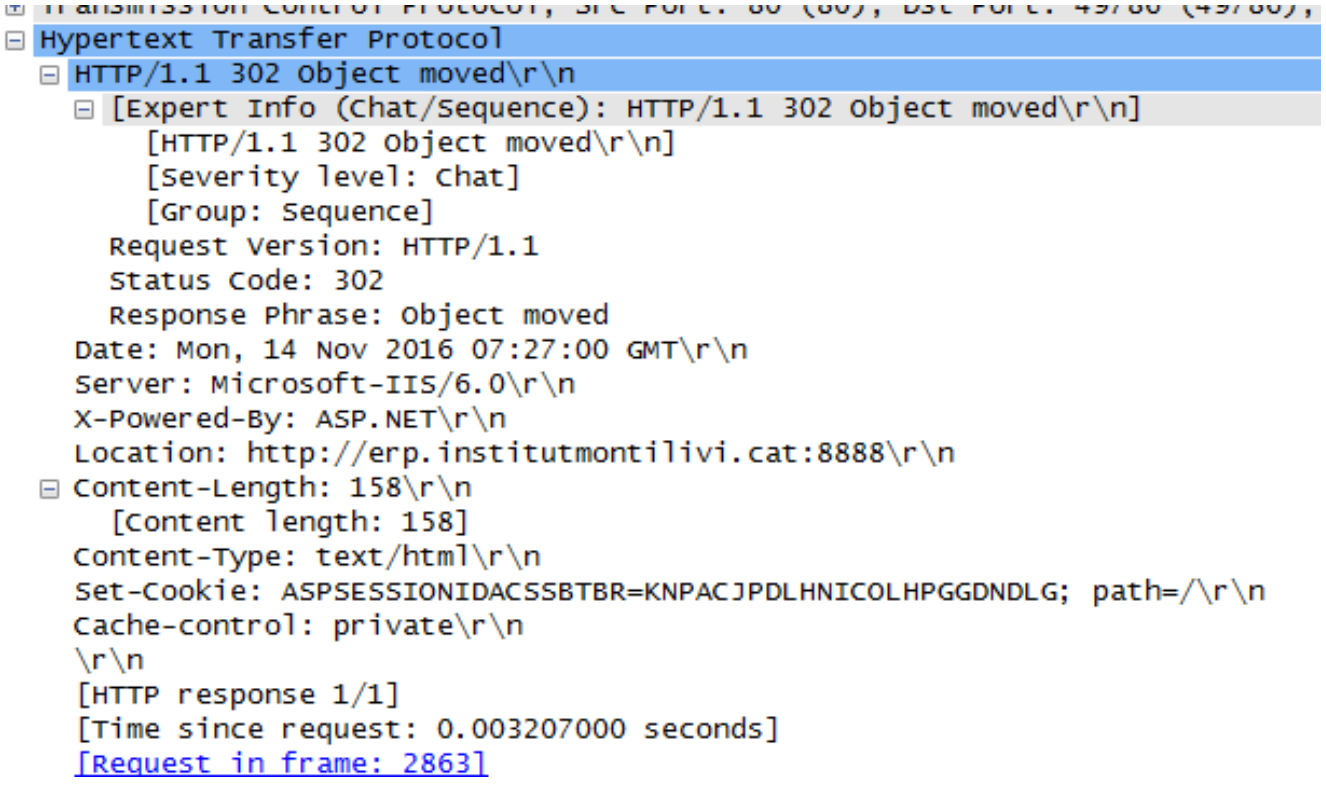
Tot seguit, podem veure el contingut dels paquets (petició web i resposta) que estableixen la comunicació entre el servidor web i el nostre ordinador, utilitzant les URL's www.iesmontilivi.net i www.iesmontilivi.cat.

Pregunta a www.iesmontilivi.net:

En aquesta captura de pantalla, podem veure el paquet que fa la petició web a www.iesmontilivi.net.

Resposta de www.iesmontilivi.net:

En aquesta captura de pantalla, podem veure el paquet que duu la resposta del servidor web www.iesmonitilivi.net al nostre ordinador.

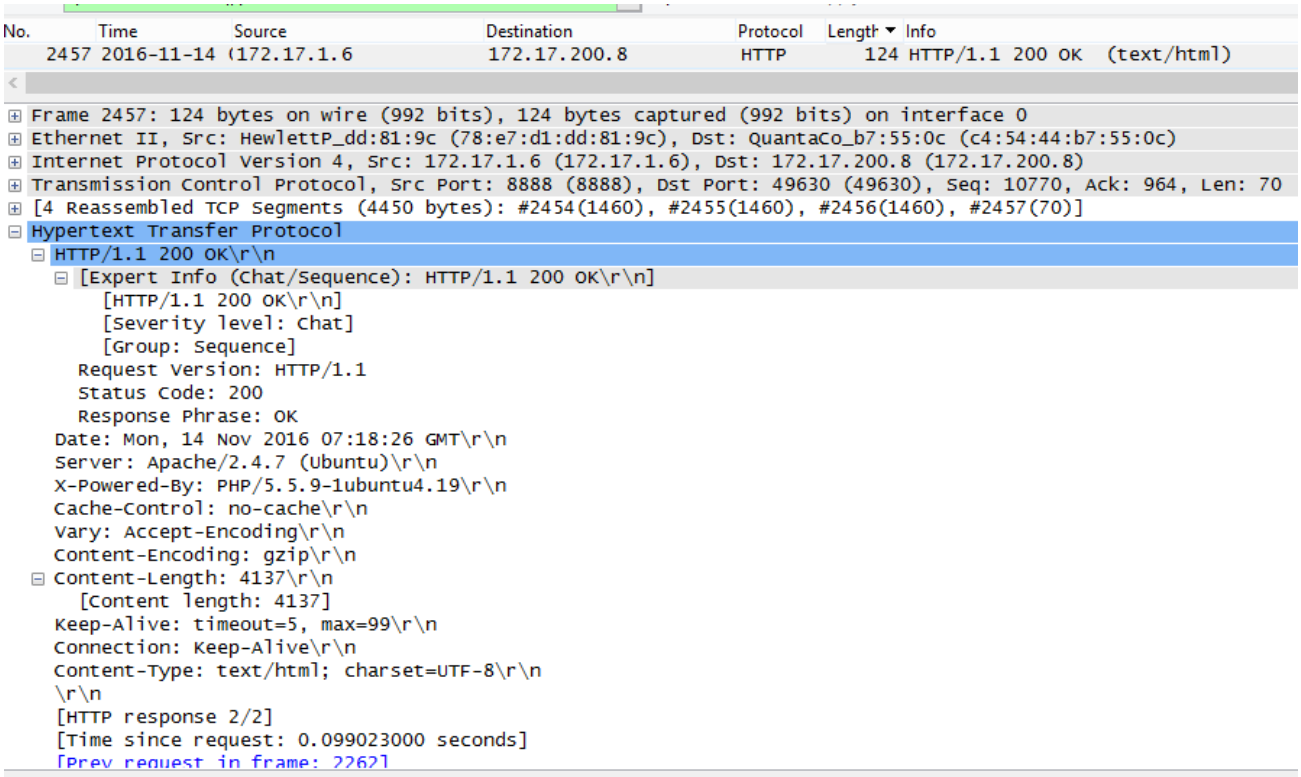


Pregunta de http://erp.institutmontilivi.cat:8888/:

En aquesta captura de pantalla, podem veure el paquet que fa la petició web a www.iesmontilivi.cat.

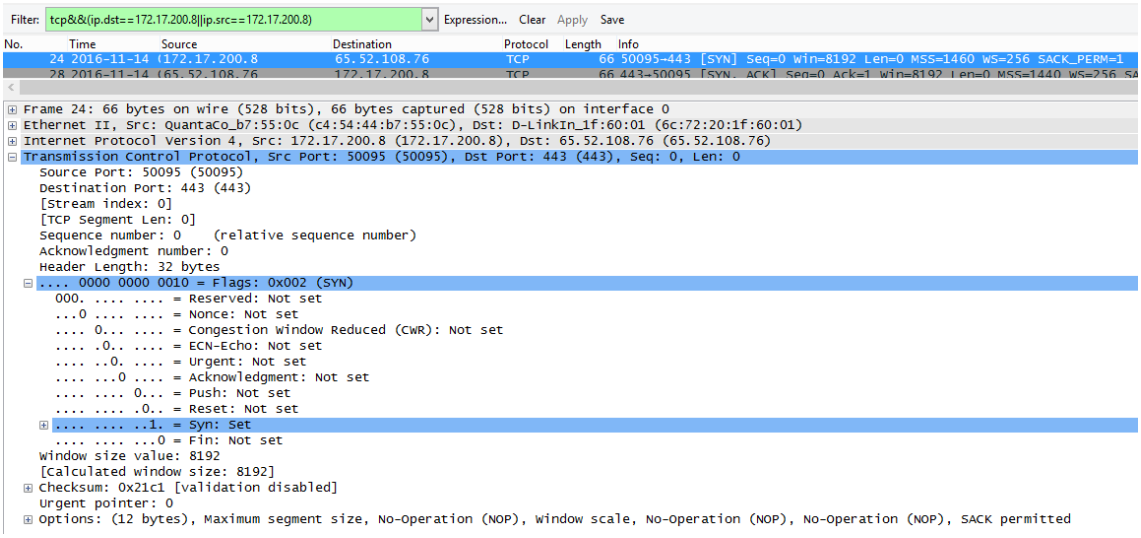
Resposta:

En aquesta captura de pantalla, podem veure el paquet que duu la resposta del servidor web www.iesmonitilivi.cat al nostre ordinador.



Establiment de la connexió:

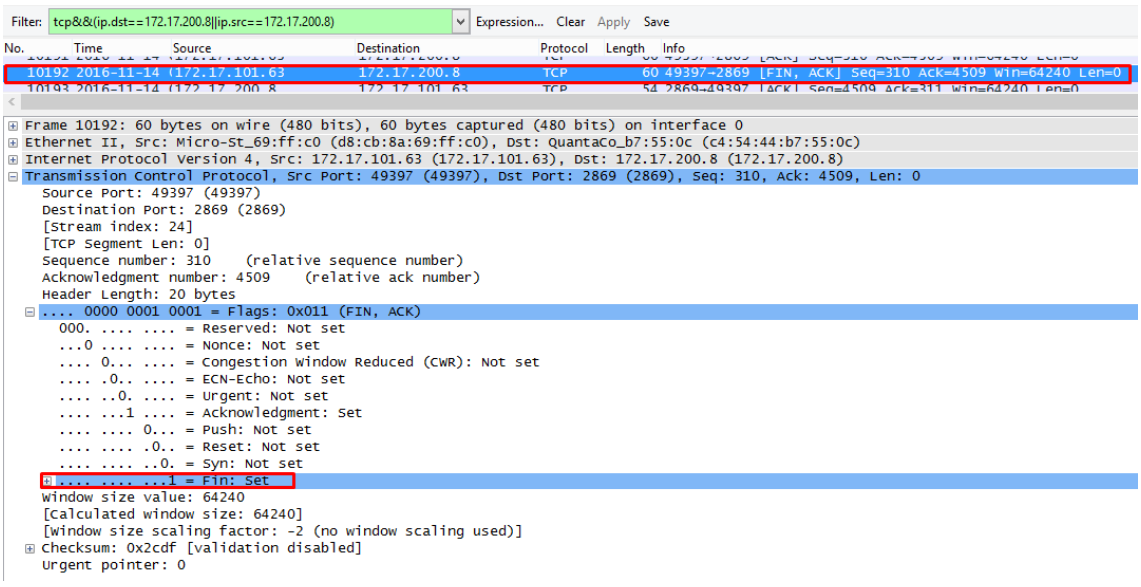
A continuació, podem veure una captura de pantalla del paquet i del seu contingut que estableix la connexió entre el servidor web i el nostre ordinador.



Finalització de la connexió:

Tot seguit, podem veure una captura de pantalla del paquet que s'encarrega de finalitzar la connexió entre el servidor web i el nostre servidor.

Ens donem compte, que el paquet es aquest perquè veiem que el *FIN: Set* és igual a *1*.



Tot seguit farem clic a sobre d'un dels articles que contingui un vídeo, secció Extraescolars de l'institut. Iniciar el vídeo de youtube i cercar si ho fa via TCP/UDP.

Ho fa per via TCP.

24	2016-11-14 (172.17.200.8	65.52.108.76	TCP	54 49758→443 [ACK] Seq=1 Ack=550 Win=254 Len=0
69	2016-11-14 (172.17.200.8	40.113.94.88	TCP	54 49757→443 [ACK] Seq=86 Ack=70 Win=258 Len=0
104	2016-11-14 (172.17.200.8	40.77.226.249	TCP	54 49820→443 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
106	2016-11-14 (40.77.226.249	172.17.200.8	TCP	60 443→49820 [FIN, ACK] Seq=1 Ack=2 Win=513 Len=0
107	2016-11-14 (172.17.200.8	40.77.226.249	TCP	54 49820→443 [ACK] Seq=2 Ack=2 Win=256 Len=0
168	2016-11-14 (40.101.44.138	172.17.200.8	TCP	60 443→49681 [ACK] Seq=1 Ack=2 Win=65535 Len=0
399	2016-11-14 (172.17.200.8	172.17.1.6	TCP	66 49824→8888 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
400	2016-11-14 (172.17.200.8	172.17.1.5	TCP	66 49825→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
401	2016-11-14 (172.17.200.8	172.17.1.5	TCP	66 49826→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
402	2016-11-14 (172.17.200.8	172.17.1.5	TCP	66 49827→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
403	2016-11-14 (172.17.1.6	172.17.200.8	TCP	66 8888→49824 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
404	2016-11-14 (172.17.1.5	172.17.200.8	TCP	66 80→49825 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
405	2016-11-14 (172.17.1.5	172.17.200.8	TCP	66 80→49826 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
406	2016-11-14 (172.17.1.5	172.17.200.8	TCP	66 80→49827 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
407	2016-11-14 (172.17.200.8	172.17.1.5	TCP	66 49828→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
408	2016-11-14 (172.17.200.8	172.17.1.6	TCP	54 49824→8888 [ACK] Seq=1 Ack=1 Win=65536 Len=0
409	2016-11-14 (172.17.200.8	172.17.1.5	TCP	54 49825→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
410	2016-11-14 (172.17.200.8	172.17.1.5	TCP	54 49827→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
411	2016-11-14 (172.17.200.8	172.17.1.5	TCP	54 49826→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
412	2016-11-14 (172.17.200.8	172.17.1.5	TCP	66 49829→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
413	2016-11-14 (172.17.200.8	172.17.1.5	TCP	66 49830→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
414	2016-11-14 (172.17.1.5	172.17.200.8	TCP	66 80→49829 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
415	2016-11-14 (172.17.1.5	172.17.200.8	TCP	66 80→49828 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
416	2016-11-14 (172.17.1.5	172.17.200.8	TCP	66 80→49830 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
417	2016-11-14 (172.17.200.8	172.17.1.5	TCP	54 49829→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
418	2016-11-14 (172.17.200.8	172.17.1.5	TCP	54 49828→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
419	2016-11-14 (172.17.200.8	172.17.1.5	TCP	54 49830→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
425	2016-11-14 (172.17.200.8	172.17.1.6	TCP	66 49831→8888 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
426	2016-11-14 (172.17.200.8	172.17.1.6	TCP	66 49832→8888 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

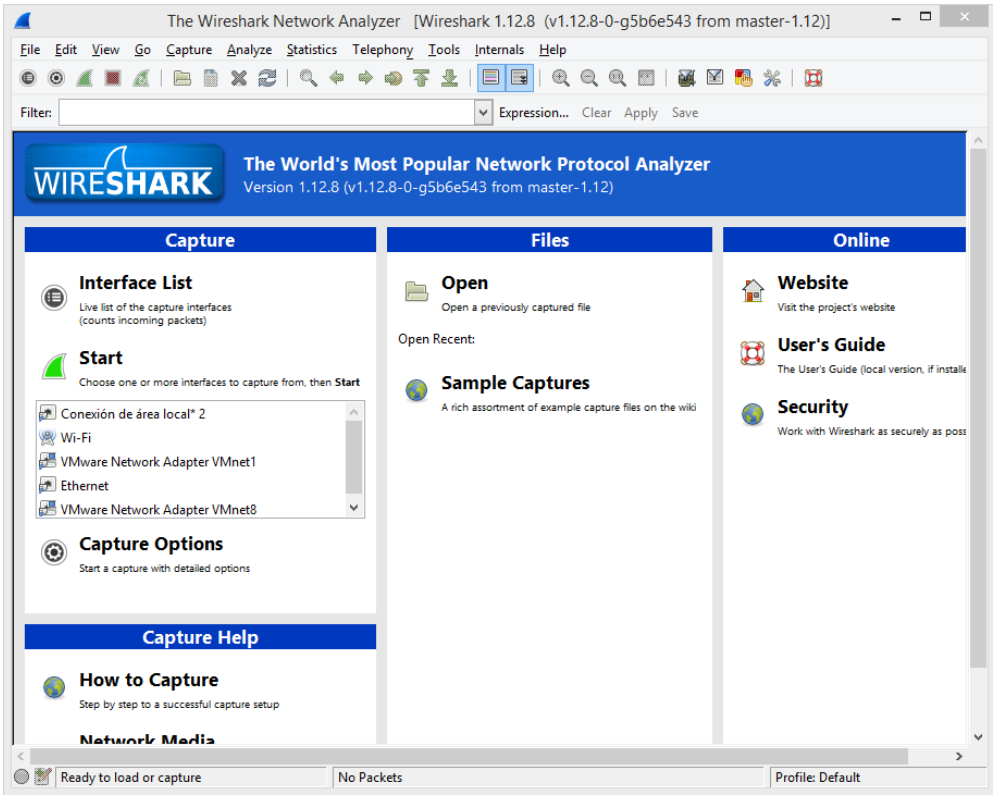
XARXA CASA

En aquesta captura de pantalla, podem veure la configuració ip, que tenim dintre de la xarxa de casa.

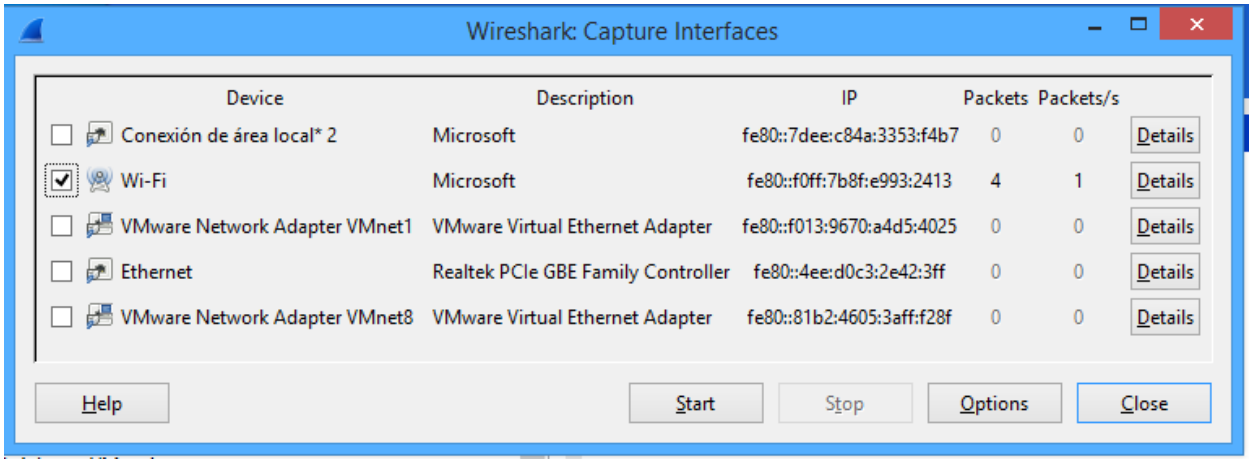
Configuració IP:

```
Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . : homestation
   Vínculo: dirección IPv6 local. . . : fe80::f0ff:7b8f:e993:2413%6
   Dirección IPv4. . . . . . . . . . . . : 192.168.1.38
   Máscara de subred . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::da61:94ff:fef2:b862%6
                                       192.168.1.1
```

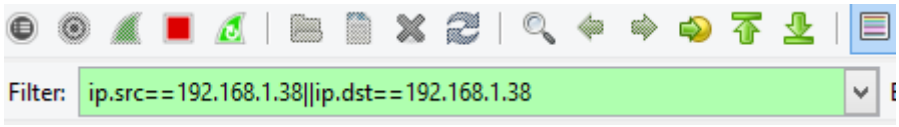
El primer que tenim que fer es entrar al Wireshark.



Tot seguit cliquem sobre *Interficie List*, i triem la nostra interfície de xarxa, que en aquest cas serà *Wi-Fi*, i tot seguit cliquem sobre *Start*.



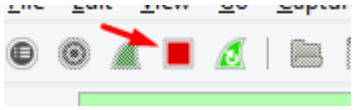
Un cop fet el pas anterior, escrivim el següent:



Un cop hem escrit això, pressionem *Enter*, i ja comença a capturar paquets.

A continuació obrim un navegador i accedim a la pàgina web de l'institut, perquè capturi els paquets que volem.

Després, al cap d'una estona, cliquem aturem la captura de paquets clicant sobre:



Llavors, anem a buscar els paquets que ens interessen.

Primer de tot, busquem les peticions DNS.

Captura de petició DNS:

Un cop fet això, busquem i capturem la petició i resposta DNS de iesmontilivi.net, i observem el contingut dels seus paquets, i també mirarem quins són les peticións i quins les respostes.

58	2016-11-11 :192.168.1.38	80.58.61.250	DNS	82	Standard query 0xc210	A ensenyament.gencat.cat
59	2016-11-11 :192.168.1.38	80.58.61.250	DNS	87	Standard query 0xad39	A montiliviplus.wordpress.com
60	2016-11-11 :192.168.1.38	80.58.61.250	DNS	74	Standard query 0x0a34	A web.gencat.cat
61	2016-11-11 :192.168.1.38	80.58.61.254	DNS	87	Standard query 0xad39	A montiliviplus.wordpress.com
62	2016-11-11 :192.168.1.38	80.58.61.254	DNS	82	Standard query 0xc210	A ensenyament.gencat.cat
63	2016-11-11 :192.168.1.38	80.58.61.254	DNS	74	Standard query 0x0a34	A web.gencat.cat
64	2016-11-11 :80.58.61.250	192.168.1.38	DNS	190	Standard query response 0xc210	CNAME gecoplus.gencat.cat.edgesuite.net CNAME a2000.b.akam
65	2016-11-11 :80.58.61.250	192.168.1.38	DNS	136	Standard query response 0xad39	CNAME lb.wordpress.com A 192.0.78.13 A 192.0.78.12
66	2016-11-11 :80.58.61.250	192.168.1.38	DNS	182	Standard query response 0x0a34	CNAME gecoplus.gencat.cat.edgesuite.net CNAME a2000.b.akam
67	2016-11-11 :80.58.61.254	192.168.1.38	DNS	136	Standard query response 0xad39	CNAME lb.wordpress.com A 192.0.78.13 A 192.0.78.12
68	2016-11-11 :80.58.61.254	192.168.1.38	DNS	190	Standard query response 0xc210	CNAME gecoplus.gencat.cat.edgesuite.net CNAME a2000.b.akam
69	2016-11-11 :80.58.61.254	192.168.1.38	DNS	182	Standard query response 0x0a34	CNAME gecoplus.gencat.cat.edgesuite.net CNAME a2000.b.akam

Pregunta:

Aquí tenim la petició DNS, que li fem a www.iesmontilivi.cat.

```
⊟ Domain Name System (query)
    [Response In: 816]
    Transaction ID: 0xef11
  ⊟ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ erp.institutmontilivi.cat: type A, class IN
        Name: erp.institutmontilivi.cat
        [Name Length: 25]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Resposta:

Aquí tenim la resposta del servidor DNS de www.iesmontilivi.cat al nostre ordinador.

```
Domain Name System (response)
    [Request In: 809]
    [Time: 0.192856000 seconds]
    Transaction ID: 0xef11
  Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 0
  Queries
    erp.institutmontilivi.cat: type A, class IN
        Name: erp.institutmontilivi.cat
        [Name Length: 25]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  Answers
    erp.institutmontilivi.cat: type A, class IN, addr 85.192.70.85
        Name: erp.institutmontilivi.cat
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 3600
        Data length: 4
        Address: 85.192.70.85 (85.192.70.85)
```

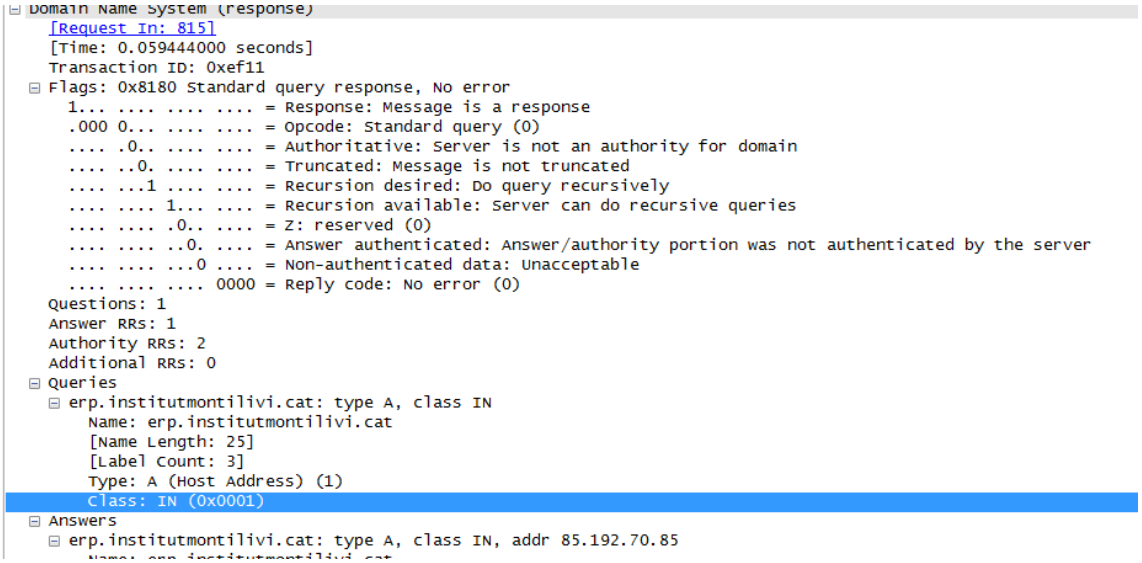
Pregunta:

Aquí tenim la petició DNS, que li fem a www.iesmontilivi.cat.

```
Domain Name System (query)
    [Response In: 817]
    Transaction ID: 0xef11
  Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    erp.institutmontilivi.cat: type A, class IN
        Name: erp.institutmontilivi.cat
        [Name Length: 25]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Resposta:

Aquí tenim la resposta del servidor DNS de www.iesmontilivi.cat al nostre ordinador.

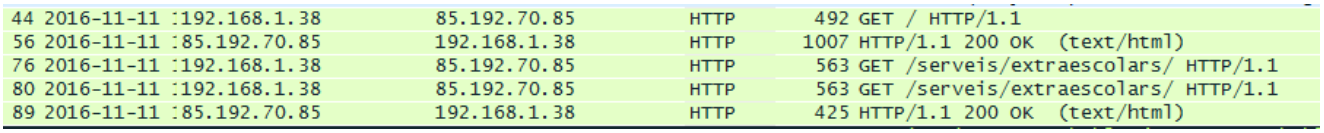


Cada petició de pàgina web (HTTP):

A continuació, podem veure unes captures de pantalla observant la comunicació que establim nosaltres amb el servidor web.

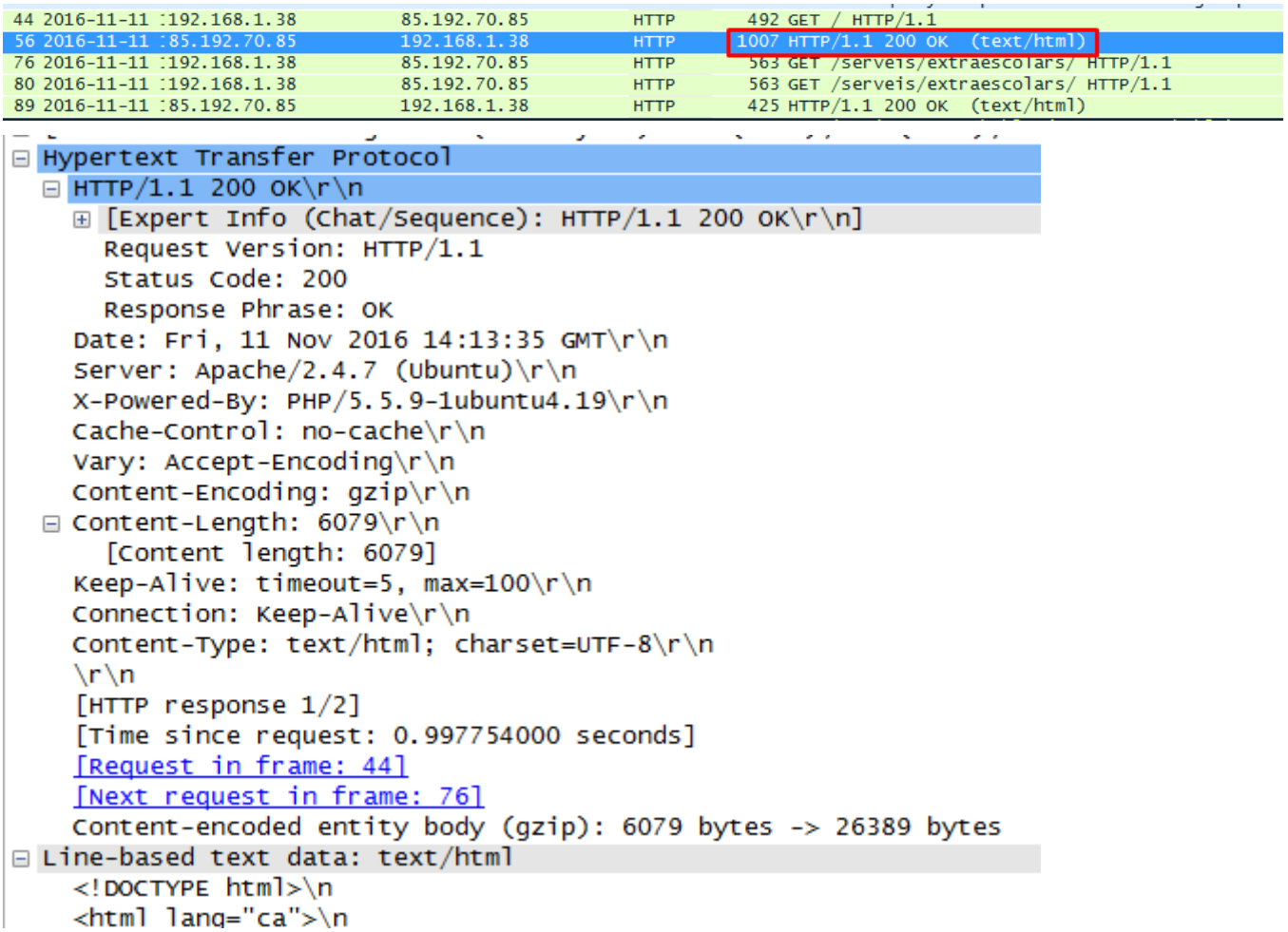
Pregunta:

Aquí tenim una captura de la petició que fem nosaltres al servidor web, per poder establir una connexió.



Resposta:

Aquí podem observar, la resposta que ens dona el servidor web, per poder establir la connexió.

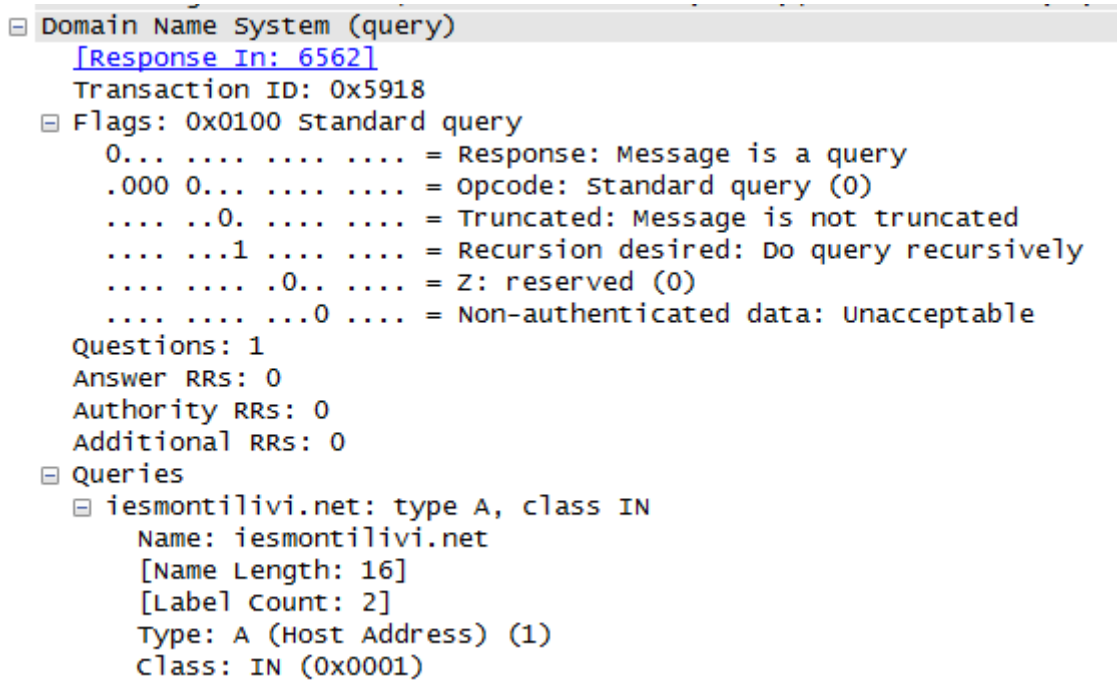


Captura peticions de pàgina web (HTTP):

Tot seguit, podem veure el contingut dels paquets (petició web i resposta) que estableixen la comunicació entre el servidor web i el nostre ordinador, utilitzant les URL's www.iesmontilivi.cat.

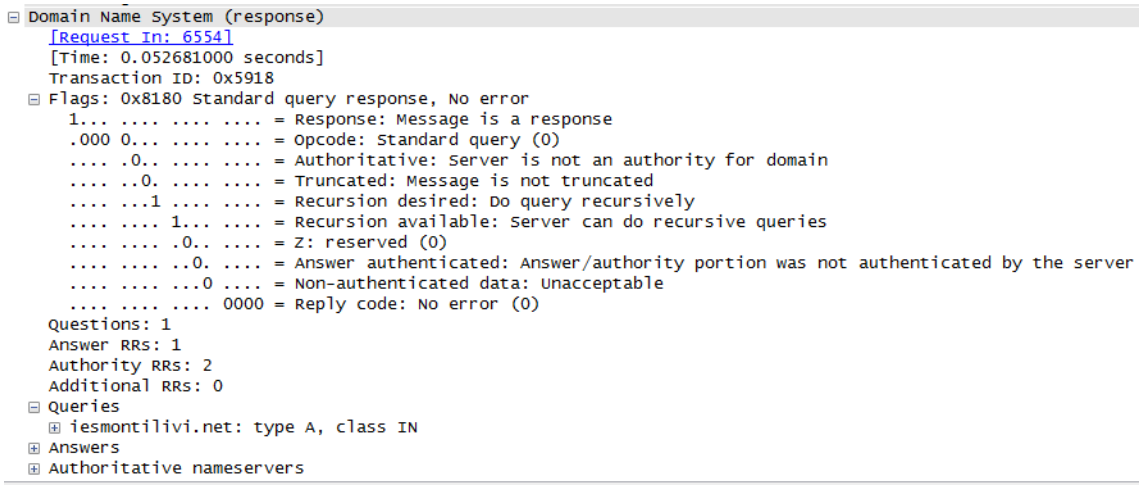
Pregunta a www.iesmontilivi.net:

En aquesta captura de pantalla, podem veure el paquet que fa la petició web a www.iesmontilivi.net.



Resposta de www.iesmontilivi.net:

En aquesta captura de pantalla, podem veure el paquet que duu la resposta del servidor web www.iesmonitilivi.net al nostre ordinador.

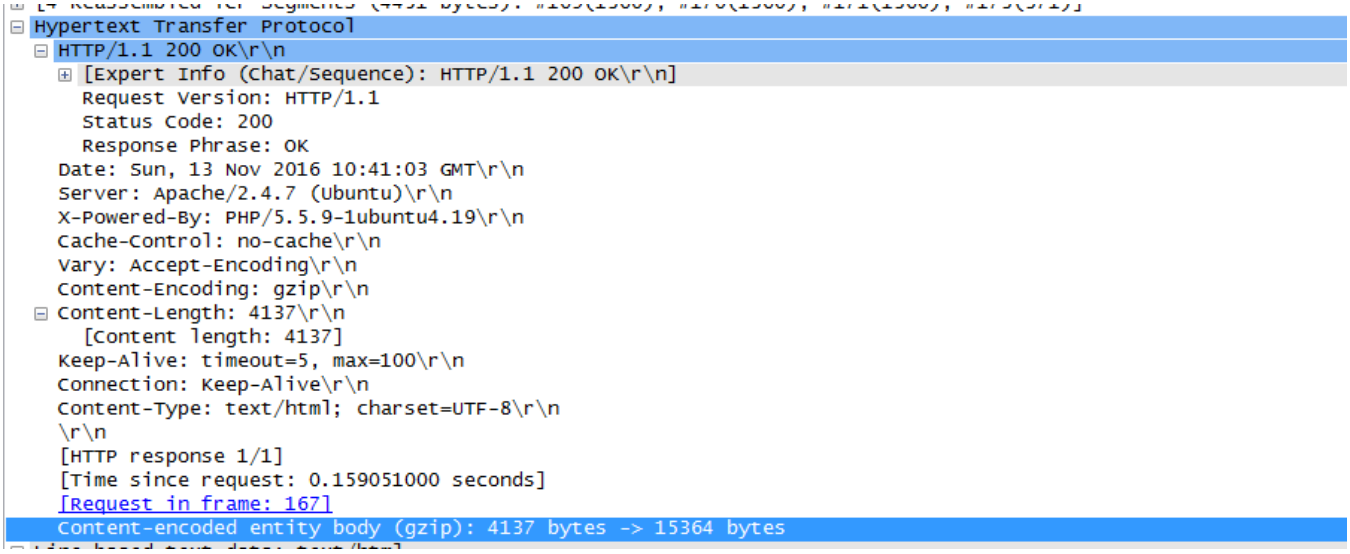


Pregunta de http://erp.institutmontilivi .cat:8888/:

En aquesta captura de pantalla, podem veure el paquet que fa la petició web a www.iesmontilivi.cat.

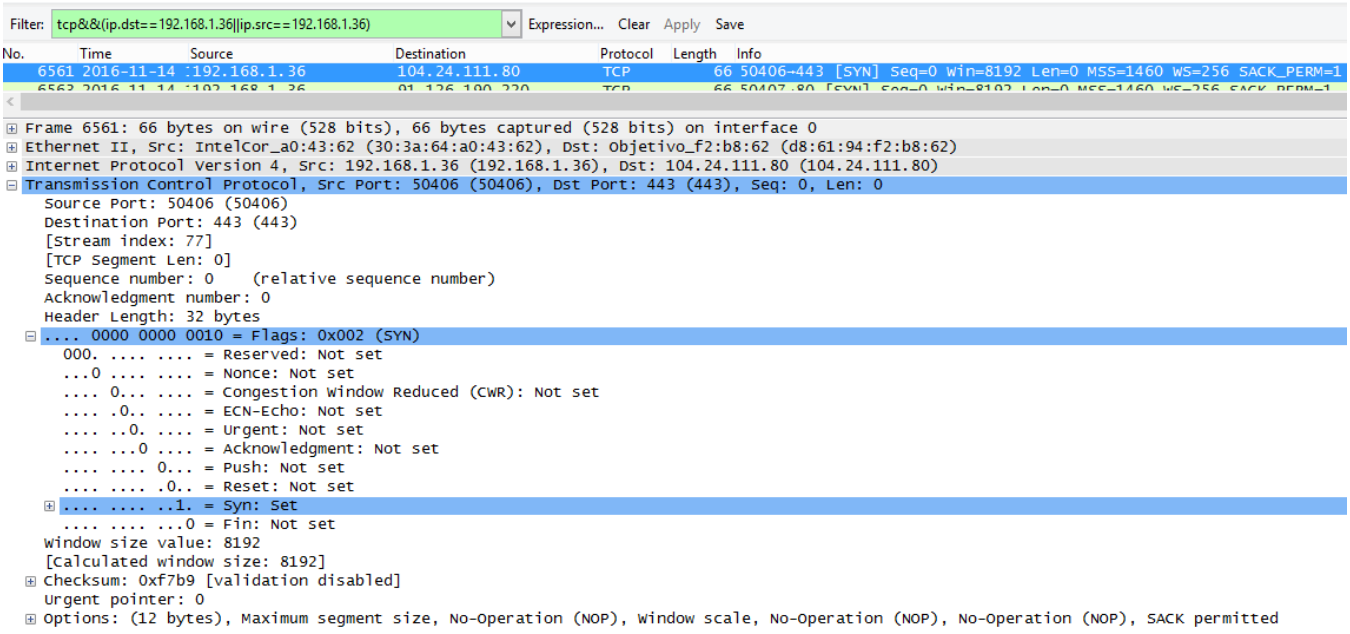
Resposta:

En aquesta captura de pantalla, podem veure el paquet que duu la resposta del servidor web www.iesmonitilivi.cat al nostre ordinador.



Establiment de la connexió:

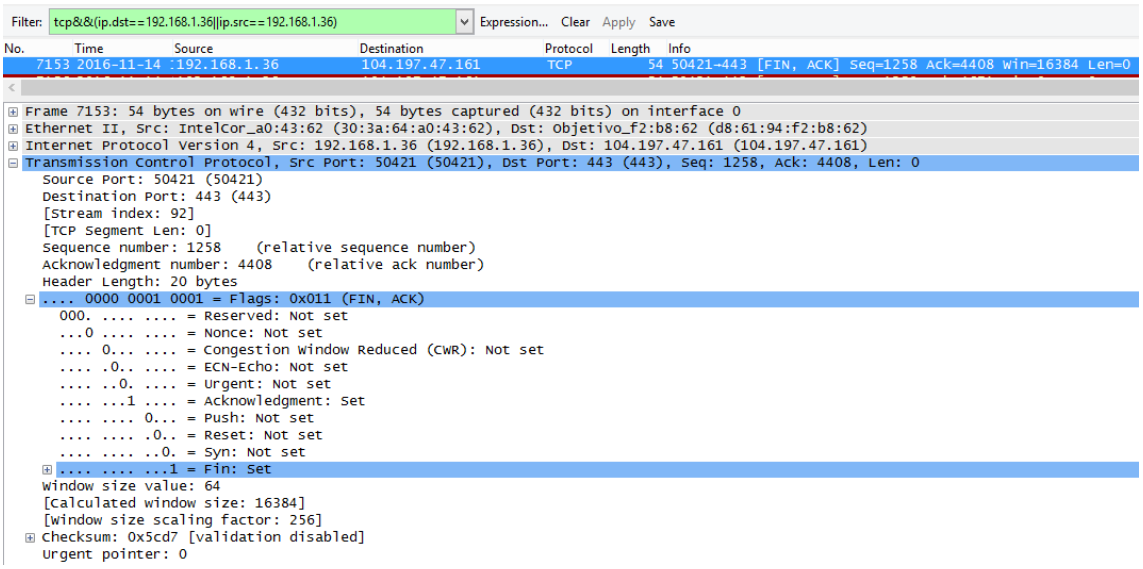
A continuació, podem veure una captura de pantalla del paquet i del seu contingut que estableix la connexió entre el servidor web i el nostre ordinador.



Finalització de la connexió:

Tot seguit, podem veure una captura de pantalla del paquet que s'encarrega de finalitzar la connexió entre el servidor web i el nostre servidor.

Ens donem compte, que el paquet es aquest perquè veiem que el *FIN: Set* és igual a *1*.



Tot seguit farem clic a sobre d'un dels articles que contingui un vídeo, secció Extraescolars de l'institut. Iniciar el vídeo de youtube i cercar si ho fa via TCP/UDP.

Ho fa per via TCP.