

## **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):**

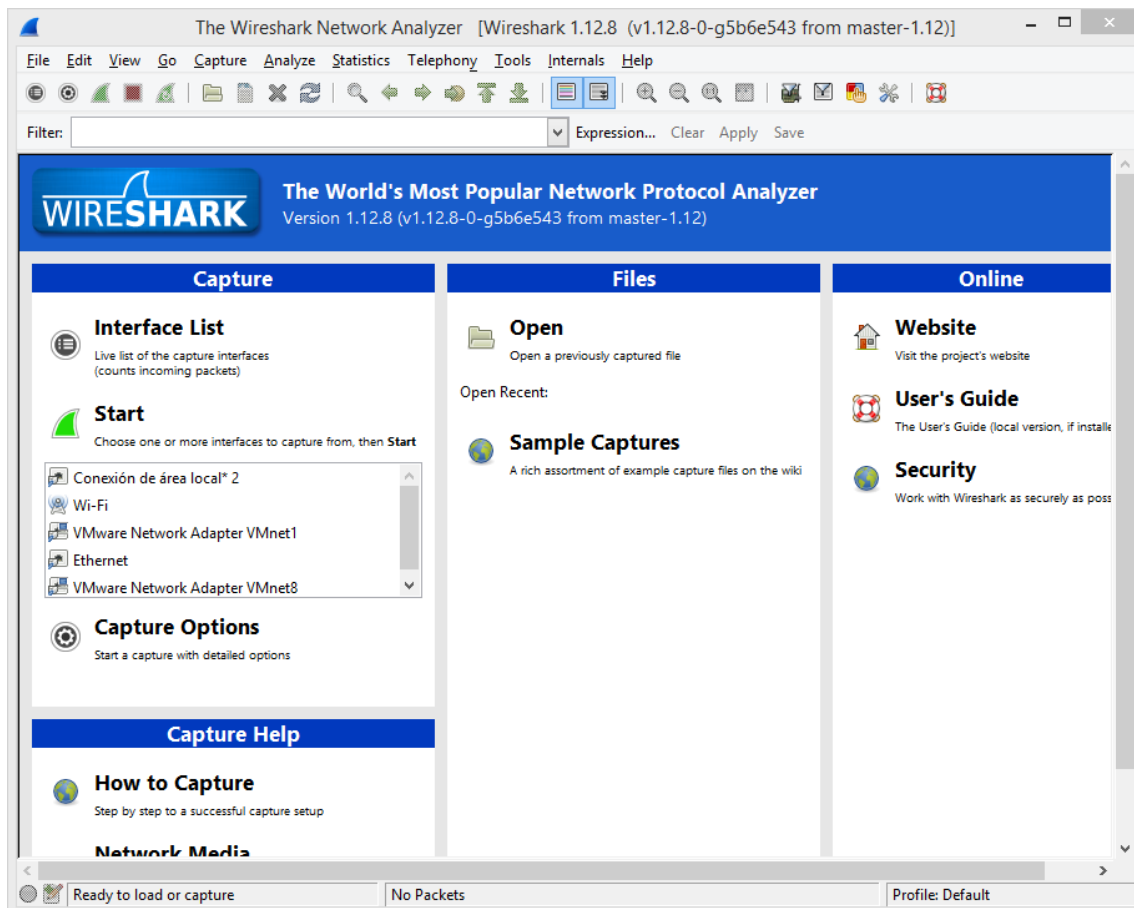
## XARXA INSTITUT

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

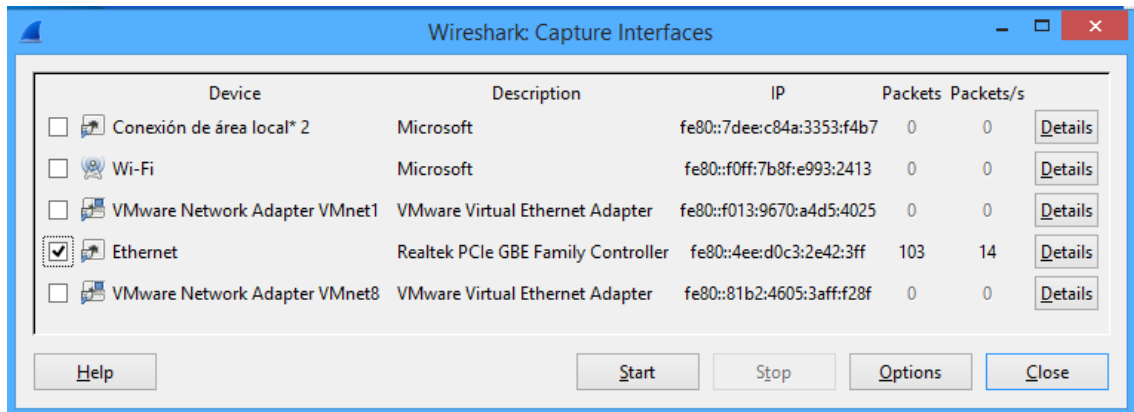
### Configuració IP:

```
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
```

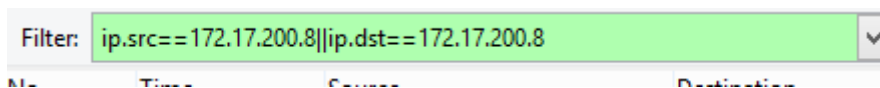
El primer que tenim que fer es entrar al Wireshark.



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:

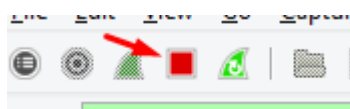


Un cop hem escrit això, pressionem *Enter*, i ja comença a capturar paquets.

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 interessin.

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 peticions i quins les respostes.

### Pregunta:

iesmontilivi.cat:

Aquí tenim la petició DNS, que li fem a [www.iesmontilivi.cat](http://www.iesmontilivi.cat).

No.	Time	Source	Destination	Protocol	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
1459	2016-11-11	:172.17.200.8	172.17.1.5	DNS	85	Standard query 0xf50a A erp.institutmontilivi.cat

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)
.... .. = 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](http://iesmontilivi.net):

Aquí tenim la petició DNS, que li fem a [www.iesmontilivi.net](http://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](http://iesmontilivi.cat):

Aquí tenim la resposta del servidor DNS de [www.iesmontilivi.cat](http://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](http://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](http://www.iesmontilivi.cat).

```

Filter: ip.src==172.17.200.8||ip.dst==172.17.200.8
No. Time Source Destination Protocol 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
1536 2016-11-11 172.17.200.8 172.17.1.5 DNS 81 Standard query 0x3bca A www.iesmontilivi.net

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](http://www.iesmontilivi.cat) al nostre ordinador.

No.	Time	Source	Destination	Protocol	Length	Info
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

User Datagram Protocol, Src Port: 3535, Dst Port: 54401 (54401)

Domain Name System (response)

[Request In: 1459]

[Time: 0.000794000 seconds]

Transaction ID: 0xf50a

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

- 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 172.17.1.6
  - Name: erp.institutmontilivi.cat
  - Type: A (Host Address) (1)
  - Class: IN (0x0001)
  - Time to live: 3600
  - Data length: 4
  - Address: 172.17.1.6 (172.17.1.6)

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.

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
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-dautomicio-fan-una-estada-de-3-set
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)



```

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 continuació, podem veure una captura de pantalla 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](http://www.iesmontilivi.net) i [www.iesmontilivi.cat](http://www.iesmontilivi.cat).

Pregunta a [www.iesmontilivi.net](http://www.iesmontilivi.net):

En aquesta captura de pantalla, podem veure el paquet que fa la petició web a [www.iesmontilivi.net](http://www.iesmontilivi.net).

```

Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      [GET / HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
    Host: www.iesmontilivi.net\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.3; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.87 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: es-ES,es;q=0.8\r\n
    \r\n
    [Full request URI: http://www.iesmontilivi.net/]
    [HTTP request 1/1]
    [Response in frame: 2864]

```

Resposta de [www.iesmontilivi.net](http://www.iesmontilivi.net):

En aquesta captura de pantalla, podem veure el paquet que duu la resposta del servidor web [www.iesmontilivi.net](http://www.iesmontilivi.net) al nostre ordinador.

```

Hypertext Transfer Protocol
  HTTP/1.1 302 Object moved\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 302 Object moved\r\n]
      [HTTP/1.1 302 Object moved\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 302
    Response Phrase: Object moved
    Date: Mon, 14 Nov 2016 07:27:00 GMT\r\n
    Server: Microsoft-IIS/6.0\r\n
    X-Powered-By: ASP.NET\r\n
    Location: http://erp.institutmontilivi.cat:8888\r\n
    Content-Length: 158\r\n
      [Content length: 158]
    Content-Type: text/html\r\n
    Set-Cookie: ASPSESSIONIDACSSBTBR=KNPACJPD LHNICOLHPGGDNDLG; path=/\r\n
    Cache-control: private\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.003207000 seconds]
    [Request in frame: 2863]

```

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](http://www.iesmontilivi.cat).

No.	Time	Source	Destination	Protocol	Length	Info
2401	2016-11-14	(104.24.111.80)	172.17.200.8	HTTP	60	HTTP/1.1 200 OK (application/javascript)
2449	2016-11-14	(172.17.200.8)	172.17.1.6	HTTP	571	GET /serveis/extraescolars/ HTTP/1.1

Frame 2449: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0 Ethernet II, Src: QuantaCo_b7:55:0c (c4:54:44:b7:55:0c), Dst: HewlettP_dd:81:9c (78:e7:d1:dd:81:9c) Internet Protocol Version 4, Src: 172.17.200.8 (172.17.200.8), Dst: 172.17.1.6 (172.17.1.6) Transmission Control Protocol, Src Port: 49630 (49630), Dst Port: 8888 (8888), Seq: 447, Ack: 6390, Len: 517 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 Upgrade-Insecure-Requests: 1\r\n User-Agent: Mozilla/5.0 (Windows NT 6.3; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.87 Safari/537.36\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\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=q8if1788c4j7i07pii9itqbk00; mipu=1\r\n Cookie pair: PHPSESSID=q8if1788c4j7i07pii9itqbk00 Cookie pair: mipu=1 \r\n [Full request URI: http://erp.institutmontilivi.cat:8888/serveis/extraescolars/] [HTTP request 2/2] [Prev request in frame: 2262]
---	--

Resposta:

En aquesta captura de pantalla, podem veure el paquet que duu la resposta del servidor web [www.iesmontilivi.cat](http://www.iesmontilivi.cat) al nostre ordinador.

No.	Time	Source	Destination	Protocol	Length	Info
2457	2016-11-14	(172.17.1.6)	172.17.200.8	HTTP	124	HTTP/1.1 200 OK (text/html)

Frame 2457: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0 Ethernet II, Src: HewlettP_dd:81:9c (78:e7:d1:dd:81:9c), Dst: QuantaCo_b7:55:0c (c4:54:44:b7:55:0c) Internet Protocol Version 4, Src: 172.17.1.6 (172.17.1.6), Dst: 172.17.200.8 (172.17.200.8) Transmission Control Protocol, Src Port: 8888 (8888), Dst Port: 49630 (49630), Seq: 10770, Ack: 964, Len: 70 [4 Reassembled TCP Segments (4450 bytes): #2454(1460), #2455(1460), #2456(1460), #2457(70)] Hypertext Transfer Protocol	HTTP/1.1 200 OK\r\n [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n] [HTTP/1.1 200 OK\r\n] [Severity level: chat] [Group: Sequence] Request Version: HTTP/1.1 Status Code: 200 Response Phrase: OK Date: Mon, 14 Nov 2016 07:18:26 GMT\r\n Server: Apache/2.4.7 (Ubuntu)\r\n X-Powered-By: PHP/5.5.9-1ubuntu4.19\r\n Cache-Control: no-cache\r\n Vary: Accept-Encoding\r\n Content-Encoding: gzip\r\n Content-Length: 4137\r\n [Content length: 4137] Keep-Alive: timeout=5, max=99\r\n Connection: Keep-Alive\r\n Content-Type: text/html; charset=UTF-8\r\n \r\n [HTTP response 2/2] [Time since request: 0.099023000 seconds] [Prev request in frame: 2262]
--	--

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.

No.	Time	Source	Destination	Protocol	Length	Info
24	2016-11-14 17:21:14.141	172.17.200.8	65.52.108.76	TCP	66	50095→443 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
28	2016-11-14 16:52:108.76	172.17.200.8	172.17.200.8	TCP	66	443→50095 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

<p>Frame 24: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0</p> <p>Ethernet II, Src: QuantaCo_b7:55:0c (c4:54:44:b7:55:0c), Dst: D-LinkIn_1f:60:01 (6c:72:20:1f:60:01)</p> <p>Internet Protocol Version 4, Src: 172.17.200.8 (172.17.200.8), Dst: 65.52.108.76 (65.52.108.76)</p> <p><b>Transmission Control Protocol, Src Port: 50095 (50095), Dst Port: 443 (443), Seq: 0, Len: 0</b></p> <p>Source Port: 50095 (50095)</p> <p>Destination Port: 443 (443)</p> <p>[Stream index: 0]</p> <p>[TCP Segment Len: 0]</p> <p>Sequence number: 0 (relative sequence number)</p> <p>Acknowledgment number: 0</p> <p>Header Length: 32 bytes</p> <p>... 0000 0000 0010 = Flags: 0x002 (SYN)</p> <p>000. .... = Reserved: Not set</p> <p>...0 .... = Nonce: Not set</p> <p>.... 0... = Congestion window Reduced (CWR): Not set</p> <p>.... .0.. = ECN-Echo: Not set</p> <p>.... ..0. = Urgent: Not set</p> <p>.... ...0 = Acknowledgment: Not set</p> <p>.... .... 0.. = Push: Not set</p> <p>.... ..... 0. = Reset: Not set</p> <p>... ..1. = Syn: Set</p> <p>.... .... 0 = Fin: Not set</p> <p>Window size value: 8192</p> <p>[Calculated window size: 8192]</p> <p>Checksum: 0x21c1 [validation disabled]</p> <p>Urgent pointer: 0</p> <p>Options: (12 bytes), Maximum segment size, No-operation (NOP), window scale, No-operation (NOP), No-operation (NOP), SACK permitted</p>
---

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.

No.	Time	Source	Destination	Protocol	Length	Info
10192	2016-11-14 17:21:14.141	172.17.101.63	172.17.200.8	TCP	60	49397→2869 [FIN, ACK] Seq=310 Ack=4509 Win=64240 Len=0

<p>Frame 10192: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0</p> <p>Ethernet II, Src: Micro-ST_69:ff:c0 (d8:cb:8a:69:ff:c0), Dst: QuantaCo_b7:55:0c (c4:54:44:b7:55:0c)</p> <p>Internet Protocol Version 4, Src: 172.17.101.63 (172.17.101.63), Dst: 172.17.200.8 (172.17.200.8)</p> <p><b>Transmission Control Protocol, Src Port: 49397 (49397), Dst Port: 2869 (2869), Seq: 310, Ack: 4509, Len: 0</b></p> <p>Source Port: 49397 (49397)</p> <p>Destination Port: 2869 (2869)</p> <p>[Stream index: 24]</p> <p>[TCP Segment Len: 0]</p> <p>Sequence number: 310 (relative sequence number)</p> <p>Acknowledgment number: 4509 (relative ack number)</p> <p>Header Length: 20 bytes</p> <p>... 0000 0001 0001 = Flags: 0x011 (FIN, ACK)</p> <p>000. .... = Reserved: Not set</p> <p>...0 .... = Nonce: Not set</p> <p>.... 0... = Congestion window Reduced (CWR): Not set</p> <p>.... .0.. = ECN-Echo: Not set</p> <p>.... ..0. = Urgent: Not set</p> <p>.... ...1 = Acknowledgment: Set</p> <p>.... .... 0.. = Push: Not set</p> <p>.... ..... 0. = Reset: Not set</p> <p>.... .... 0. = Syn: Not set</p> <p>... ..1. = Fin: Set</p> <p>Window size value: 64240</p> <p>[Calculated window size: 64240]</p> <p>[window size scaling factor: -2 (no window scaling used)]</p> <p>Checksum: 0x2cdf [validation disabled]</p> <p>Urgent pointer: 0</p>
---

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:

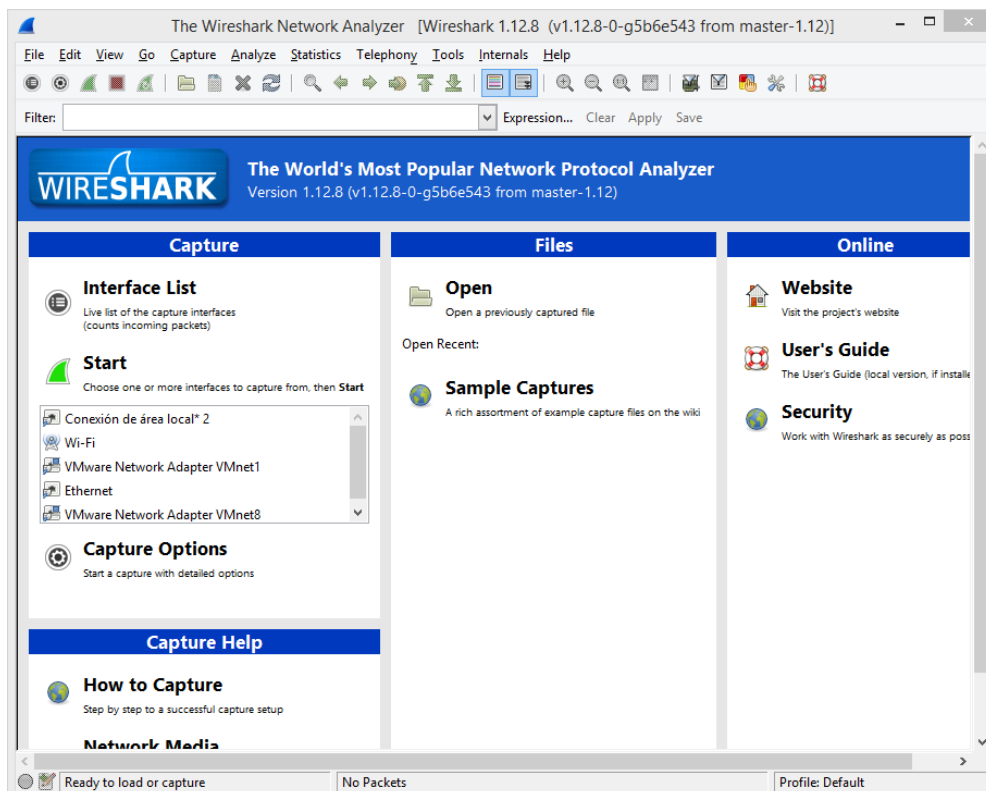
```

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

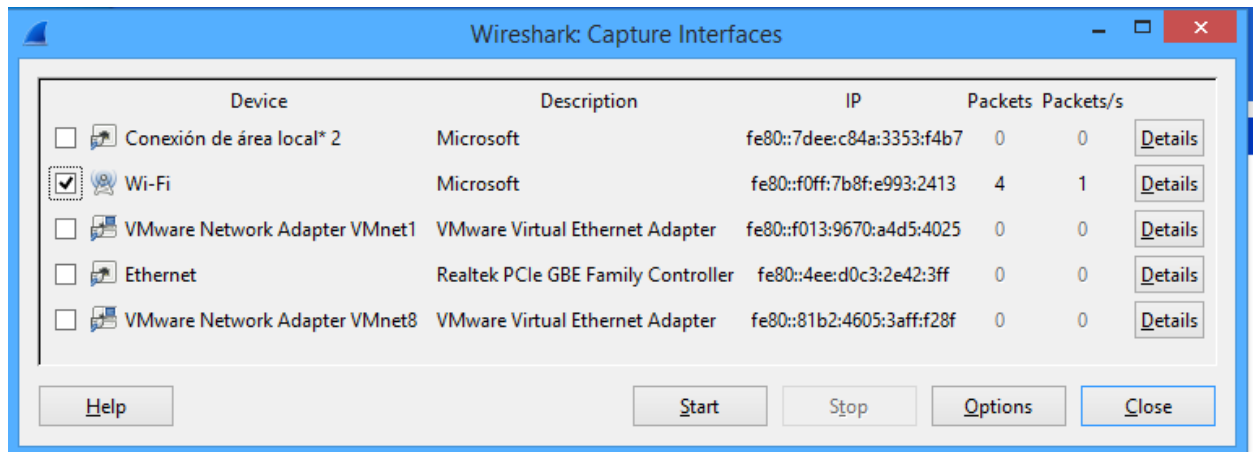
```

El primer que tenim que fer es entrar al Wireshark.

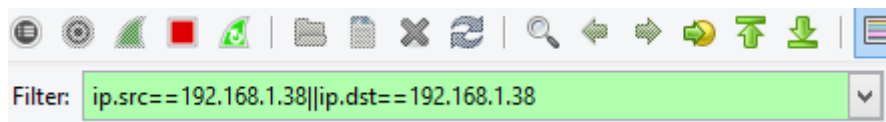




Tot seguit cliquem sobre *Interfície List*, i triem la nostra interfície de xarxa, que en aquest cas serà *Wi-Fi*, i tot seguit cliquem sobre *Start*.



Un cop fet el pas anterior, escrivim el següent:

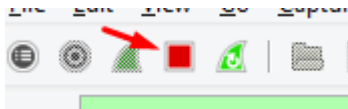


Un cop hem escrit això, pressionem *Enter*, i ja comença a capturar paquets.

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 interessin.

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 peticions 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 0xa34	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 0xa34	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 0xa34	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 0xa34	CNAME gecoplus.gencat.cat.edgesuite.net CNAME a2000.b.akam

### Pregunta:

Aquí tenim la petició DNS, que li fem a [www.iesmontilivi.cat](http://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](http://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](http://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](http://www.iesmontilivi.cat) al nostre ordinador.

```

domain Name System (response)
[Request In: 815]
[Time: 0.059444000 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

```

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.

44	2016-11-11	192.168.1.38	85.192.70.85	HTTP	492 GET / HTTP/1.1
56	2016-11-11	85.192.70.85	192.168.1.38	HTTP	1007 HTTP/1.1 200 OK (text/html)
76	2016-11-11	192.168.1.38	85.192.70.85	HTTP	563 GET /serveis/extraescolars/ HTTP/1.1
80	2016-11-11	192.168.1.38	85.192.70.85	HTTP	563 GET /serveis/extraescolars/ HTTP/1.1
89	2016-11-11	85.192.70.85	192.168.1.38	HTTP	425 HTTP/1.1 200 OK (text/html)

```

Hypertext Transfer Protocol
GET /serveis/extraescolars/ HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /serveis/extraescolars/ HTTP/1.1\r\n]
Request Method: GET
Request URI: /serveis/extraescolars/
Request Version: HTTP/1.1
Host: erp.institutmontilivi.cat:8888\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.87 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\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=dbig9r0u0bandhe603b1dru2b2\r\n
Cookie pair: PHPSESSID=dbig9r0u0bandhe603b1dru2b2\r\n
[Full request URI: http://erp.institutmontilivi.cat:8888/serveis/extraescolars/]
[HTTP request 2/2]
[Prev request in frame: 44]

```

Resposta:

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

44	2016-11-11	192.168.1.38	85.192.70.85	HTTP	492 GET / HTTP/1.1
56	2016-11-11	85.192.70.85	192.168.1.38	HTTP	1007 HTTP/1.1 200 OK (text/html)
76	2016-11-11	192.168.1.38	85.192.70.85	HTTP	563 GET /serveis/extraescolars/ HTTP/1.1
80	2016-11-11	192.168.1.38	85.192.70.85	HTTP	563 GET /serveis/extraescolars/ HTTP/1.1
89	2016-11-11	85.192.70.85	192.168.1.38	HTTP	425 HTTP/1.1 200 OK (text/html)

[-]	Hypertext Transfer Protocol
[-]	HTTP/1.1 200 OK\r\n
+	[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
	Request Version: HTTP/1.1
	Status Code: 200
	Response Phrase: OK
	Date: Fri, 11 Nov 2016 14:13:35 GMT\r\n
	Server: Apache/2.4.7 (Ubuntu)\r\n
	X-Powered-By: PHP/5.5.9-1ubuntu4.19\r\n
	Cache-Control: no-cache\r\n
	Vary: Accept-Encoding\r\n
	Content-Encoding: gzip\r\n
[-]	Content-Length: 6079\r\n
	[Content length: 6079]
	Keep-Alive: timeout=5, max=100\r\n
	Connection: Keep-Alive\r\n
	Content-Type: text/html; charset=UTF-8\r\n
	\r\n
	[HTTP response 1/2]
	[Time since request: 0.997754000 seconds]
	[Request in frame: 44]
	[Next request in frame: 76]
	Content-encoded entity body (gzip): 6079 bytes -> 26389 bytes
[-]	Line-based text data: text/html
	<!DOCTYPE html>\n
	<html lang="ca">\n

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](http://www.iesmontilivi.cat).

44	2016-11-11	192.168.1.38	85.192.70.85	HTTP	492 GET / HTTP/1.1
56	2016-11-11	85.192.70.85	192.168.1.38	HTTP	1007 HTTP/1.1 200 OK (text/html)
76	2016-11-11	192.168.1.38	85.192.70.85	HTTP	563 GET /serveis/extraescolars/ HTTP/1.1
80	2016-11-11	192.168.1.38	85.192.70.85	HTTP	563 GET /serveis/extraescolars/ HTTP/1.1
89	2016-11-11	85.192.70.85	192.168.1.38	HTTP	425 HTTP/1.1 200 OK (text/html)

Pregunta a [www.iesmontilivi.net](http://www.iesmontilivi.net):

En aquesta captura de pantalla, podem veure el paquet que fa la petició web a [www.iesmontilivi.net](http://www.iesmontilivi.net).

```

[ ] Domain Name System (query)
    [Response In: 6562]
    Transaction ID: 0x5918
    [ ] 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)

[ ] Transmission Control Protocol, Src Port: 4353 (4353), Dst Port: 8088 (8088), Seq: 435, Len: 60
[ ] 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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.87 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\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=dbig9r0u0bandhe603b1dru2b2\r\n
        Cookie pair: PHPSESSID=dbig9r0u0bandhe603b1dru2b2
    \r\n
    [Full request URI: http://erp.institutmontilivi.cat:8888/serveis/extraescolars/]
    [HTTP request 2/2]
    [Prev request in frame: 44]

```

Resposta de [www.iesmontilivi.net](http://www.iesmontilivi.net):

En aquesta captura de pantalla, podem veure el paquet que duu la resposta del servidor web [www.iesmontilivi.net](http://www.iesmontilivi.net) al nostre ordinador.

```

Domain Name System (response)
  [Request in: 6554]
  [Time: 0.052681000 seconds]
  Transaction ID: 0x5918
  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
    [iesmontilivi.net: type A, class IN]
  Answers
  Authoritative nameservers

```

Pregunta de [http://erp.institutmontilivi .cat:8888/](http://erp.institutmontilivi.cat:8888/):

En aquesta captura de pantalla, podem veure el paquet que fa la petició web a [www.iesmontilivi.cat](http://www.iesmontilivi.cat).

```

Hypertext Transfer Protocol
  GET /serveis/extraescolars/ HTTP/1.1\r\n
  Host: erp.institutmontilivi.cat:8888\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.87 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\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=tj308rr0ts1df71hlqa0hsvdi4\r\n
  Cookie pair: PHPSESSID=tj308rr0ts1df71hlqa0hsvdi4\r\n
  [Full request URI: http://erp.institutmontilivi.cat:8888/serveis/extraescolars/]
  [HTTP request 1/1]
  [Response in frame: 173]

```

Resposta:

En aquesta captura de pantalla, podem veure el paquet que duu la resposta del servidor web [www.iesmonitilivi.cat](http://www.iesmonitilivi.cat) al nostre ordinador.

```

[4] Reassembled TCP segments (4711 bytes): #103(1300), #170(1300), #171(1300), #173(1317)
[+] Hypertext Transfer Protocol
  [+] HTTP/1.1 200 OK\r\n
    [Expert Info (chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
      Date: Sun, 13 Nov 2016 10:41:03 GMT\r\n
      Server: Apache/2.4.7 (Ubuntu)\r\n
      X-Powered-By: PHP/5.5.9-1ubuntu4.19\r\n
      Cache-Control: no-cache\r\n
      Vary: Accept-Encoding\r\n
      Content-Encoding: gzip\r\n
    [Content-Length: 4137\r\n]
      [Content length: 4137]
      Keep-Alive: timeout=5, max=100\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=UTF-8\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.159051000 seconds]
      [Request in frame: 167]
    Content-encoded entity body (gzip): 4137 bytes -> 15364 bytes

```

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.

```

Filter: tcp&&(ip.dst==192.168.1.36||ip.src==192.168.1.36) Expression... Clear Apply Save
No.    Time    Source                Destination            Protocol Length  Info
6561  2016-11-14 192.168.1.36        104.24.111.80          TCP                66  50406->443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
6562  2016-11-14 104.24.111.80        192.168.1.36          TCP                66  443->50406 [ACK] Seq=0 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
<----->
[+] Frame 6561: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
[+] Ethernet II, Src: IntelCor_a0:43:62 (30:3a:64:a0:43:62), Dst: Objetivo_f2:b8:62 (d8:61:94:f2:b8:62)
[+] Internet Protocol Version 4, Src: 192.168.1.36 (192.168.1.36), Dst: 104.24.111.80 (104.24.111.80)
[+] Transmission Control Protocol, Src Port: 50406 (50406), Dst Port: 443 (443), Seq: 0, Len: 0
  Source Port: 50406 (50406)
  Destination Port: 443 (443)
  [Stream index: 77]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Acknowledgment number: 0
  Header Length: 32 bytes
[+] .... 0000 0000 0010 = Flags: 0x002 (SYN)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  .... 0... = Congestion Window Reduced (CWR): Not set
  .... 0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...0 = Acknowledgment: Not set
  .... .... 0.. = Push: Not set
  .... .... .0.. = Reset: Not set
[+] .... .... .1. = Syn: Set
  .... .... ...0 = Fin: Not set
  window size value: 8192
  [Calculated window size: 8192]
[+] Checksum: 0xf7b9 [validation disabled]
  Urgent pointer: 0
[+] Options: (12 bytes), Maximum segment size, No-Operation (NOP), window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted

```

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.

Filter: tcp&&(ip.dst==192.168.1.36  ip.src==192.168.1.36)						
No.	Time	Source	Destination	Protocol	Length	Info
7153	2016-11-14	192.168.1.36	104.197.47.161	TCP	54	50421->443 [FIN, ACK] Seq=1258 Ack=4408 win=16384 Len=0
<div> <div>Frame 7153: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0</div> <div> <div>Ethernet II, Src: IntelCor_a0:43:62 (30:3a:64:a0:43:62), Dst: Objetivo_f2:b8:62 (d8:61:94:f2:b8:62)</div> <div>Internet Protocol Version 4, Src: 192.168.1.36 (192.168.1.36), Dst: 104.197.47.161 (104.197.47.161)</div> <div> <div>Transmission Control Protocol, Src Port: 50421 (50421), Dst Port: 443 (443), Seq: 1258, Ack: 4408, Len: 0</div> <div> <div>Source Port: 50421 (50421)</div> <div>Destination Port: 443 (443)</div> <div>[Stream index: 92]</div> <div>[TCP segment Len: 0]</div> <div>Sequence number: 1258 (relative sequence number)</div> <div>Acknowledgment number: 4408 (relative ack number)</div> <div>Header Length: 20 bytes</div> <div> <div>0000 0001 0001 = Flags: 0x011 (FIN, ACK)</div> <div> <div>000. .... = Reserved: Not set</div> <div>...0 .... = Nonce: Not set</div> <div>...0 .... = Congestion Window Reduced (CWR): Not set</div> <div>.... 0. .... = ECN-Echo: Not set</div> <div>.... 0. .... = Urgent: Not set</div> <div>.... ..1 .... = Acknowledgment: Set</div> <div>.... .... 0. .... = Push: Not set</div> <div>.... .... 0. .... = Reset: Not set</div> <div>.... .... 0. .... = Syn: Not set</div> <div>.... .... ..1 = Fin: Set</div> </div> <div>Window size value: 64</div> <div>[calculated window size: 16384]</div> <div>[window size scaling factor: 256]</div> <div>Checksum: 0x5cd7 [validation disabled]</div> <div>urgent pointer: 0</div> </div> </div> </div> </div></div>						

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.

27	2016-11-14	192.168.1.36	40.77.226.250	TCP	54	50457->443 [ACK] Seq=2 Ack=2 win=64 Len=0
57	2016-11-14	192.168.1.36	216.58.210.174	TCP	54	50447->443 [FIN, ACK] Seq=1 Ack=1 win=62 Len=0
58	2016-11-14	192.168.1.36	216.58.210.174	TCP	54	50447->443 [RST, ACK] Seq=2 Ack=1 win=0 Len=0
59	2016-11-14	192.168.1.36	216.58.210.174	TCP	54	50449->443 [FIN, ACK] Seq=1 Ack=1 win=62 Len=0
60	2016-11-14	192.168.1.36	216.58.210.174	TCP	54	50449->443 [RST, ACK] Seq=2 Ack=1 win=0 Len=0
61	2016-11-14	192.168.1.36	216.58.210.174	TCP	54	50450->443 [FIN, ACK] Seq=1 Ack=1 win=63 Len=0
62	2016-11-14	192.168.1.36	216.58.210.174	TCP	54	50450->443 [RST, ACK] Seq=2 Ack=1 win=0 Len=0
64	2016-11-14	192.168.1.36	216.58.210.174	TCP	54	50448->443 [FIN, ACK] Seq=1 Ack=1 win=63 Len=0
65	2016-11-14	192.168.1.36	216.58.210.174	TCP	54	50448->443 [RST, ACK] Seq=2 Ack=1 win=0 Len=0
67	2016-11-14	192.168.1.36	216.58.210.174	TCP	54	50451->443 [FIN, ACK] Seq=1 Ack=1 win=63 Len=0
68	2016-11-14	192.168.1.36	216.58.210.174	TCP	54	50451->443 [RST, ACK] Seq=2 Ack=1 win=0 Len=0
71	2016-11-14	192.168.1.36	85.192.70.85	TCP	66	50458->8888 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
72	2016-11-14	192.168.1.36	85.192.70.85	TCP	66	50459->8888 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
73	2016-11-14	192.168.1.36	85.192.70.85	TCP	66	50460->8888 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
74	2016-11-14	192.168.1.36	85.192.70.85	TCP	66	50461->8888 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
75	2016-11-14	192.168.1.36	85.192.70.85	TCP	66	50462->8888 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
76	2016-11-14	192.168.1.36	85.192.70.85	TCP	66	50463->8888 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
82	2016-11-14	192.168.1.36	151.101.120.133	TCP	66	50464->443 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
83	2016-11-14	192.168.1.36	151.101.120.133	TCP	66	50465->443 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
84	2016-11-14	192.168.1.36	104.31.92.211	TCP	66	50466->443 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
87	2016-11-14	85.192.70.85	192.168.1.36	TCP	66	8888->50459 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1360 SACK_PERM=1
88	2016-11-14	85.192.70.85	192.168.1.36	TCP	66	8888->50458 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1360 SACK_PERM=1
89	2016-11-14	192.168.1.36	85.192.70.85	TCP	54	50459->8888 [ACK] Seq=1 Ack=1 win=16384 Len=0
90	2016-11-14	192.168.1.36	85.192.70.85	TCP	54	50458->8888 [ACK] Seq=1 Ack=1 win=16384 Len=0
91	2016-11-14	192.168.1.36	104.24.111.80	TCP	66	50467->80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
92	2016-11-14	85.192.70.85	192.168.1.36	TCP	66	8888->50460 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1360 SACK_PERM=1
93	2016-11-14	192.168.1.36	104.24.111.80	TCP	66	50468->80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
94	2016-11-14	192.168.1.36	85.192.70.85	TCP	54	50460->8888 [ACK] Seq=1 Ack=1 win=16384 Len=0