

---

# PLANIFICACIÓN Y ADMINISTRACIÓN DE REDES



CENTRO TRES CANTOS

Grado Superior en Administración de Sistemas  
Informáticos en Red

Autor: Edison Gabriel Vaca Cifuentes

Madrid, 11 de marzo de 2022

---

## CONTENIDO

Realización de la Actividad .....	3
Enumera y explica la función de cada protocolo que a parecen en la grabación: .....	3
Indica las capas que tiene y explica los datos más relevantes e interesantes que aparecen: ..	4
Mira como vienen los datos de las páginas que has solicitado: .....	35
Realiza filtros con cadenas y con regular expresión: .....	36



## REALIZACIÓN DE LA ACTIVIDAD

Enumera y explica la función de cada protocolo que a parecen en la grabación:

**MDNS (Multicast DNS)** Es un servicio en el que se encarga de la resolución de nombres de host en direcciones IP sin la necesidad de una configuración predeterminada.

**SSDP (Simple Service Discovery Protocol)** Es un protocolo en el que nos sirve para la búsqueda de los dispositivos UPnP (Universal Plug and Play) en una red.

**Nota:** un UPNP es un protocolo que nos permite que los dispositivos que se encuentren en la red y que sean compatibles, puedan poder detectar la presencia de otro dispositivo como consecuencia crean canales de comunicación directa con Internet

**LLDP (Link Layer Discovery Protocol)** Es un protocolo de detección de vecino que se encuentra en la capa 2 con la finalidad de que los dispositivos transmitan información de los dispositivos pares que se encuentran conectados directamente.

**UDP (User Datagram Protocol)** Es un protocolo mínimo que se encuentra en el nivel de transporte con la finalidad del intercambio de datagramas. Con la finalidad de que se pueda enviar datagramas en la red sin que se haya establecido una conexión anteriormente.

**DNS (Domain Name System)** Es un Sistema descentralizado para los dispositivos conectados a redes IP o una red privada. Es como una “agenda telefónica” que se encuentra en la web donde organiza e identifica dominios.

**TLSV1.2(Transport Layer Security)** Es un protocolo de Internet con perfil de seguridad que se encuentra en la capa de transporte en el que son protocolos criptográficos con la finalidad de que nos proporciones comunicaciones seguras por una red.

**TCP (Transfer Control Protocol)** Es un protocolo de red importante que nos permite que entre dos hosts se puedan conectar y que puedan conectar e intercambio el flujo de datos.

**QUIC (Quick UDP Internet Connections)** Es un protocolo de red en perfil experimental sobre la capa de transporte. Nos proporciona una base para nuevas aplicaciones como HTTP.

**ARP (Address Resolution Protocol)** Es un protocolo de comunicaciones que se encuentra en la capa de enlace de datos en la que es responsable de poder encontrar dirección MAC que corresponda a una dirección IP.

**IGMP V3 (Internet Group Management Protocol)** Es un protocolo de comunicaciones que permite poder intercambiar información sobre el estado que se encuentra los enrutadores de IP sobre la multidifusión o miembros de grupos de multidifusión.

**ICMPV3(Internet Control Message Protocol)** Es un protocolo en el que nos permite enviar mensajes de error e información operativas indicando por ejemplo un host deslocalizado o un servicio que no se encuentras activo.

Indica las capas que tiene y explica los datos más relevantes e interesantes que aparecen:

- MDNS

En este caso nosotros vamos a elegir el número 15 donde vamos a explicar posteriormente sus capas:

10	0.005071	192.168.0.16	239.255.255.250	SSDP	211 M-SEARCH * HTTP/1.1
11	0.013238	192.168.0.15	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
12	0.013800	192.168.0.15	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
13	0.014268	fe80::f870:921a:850... ff02::fb		MDNS	102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
14	0.014652	fe80::f870:921a:850... ff02::fb		MDNS	102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
15	0.015152	192.168.0.15	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
16	0.015740	192.168.0.15	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
17	0.016355	fe80::f870:921a:850... ff02::fb		MDNS	102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
18	0.016730	fe80::f870:921a:850... ff02::fb		MDNS	102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question

Nos encontramos con que tiene 5 capas:

```
> Frame 15: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0DED249}, id 0
> Ethernet II, Src: IntelCor_48:6a:7a (70:9c:d1:48:6a:7a), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
> Internet Protocol Version 4, Src: 192.168.0.15, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)

0000  01 00 5e 00 00 fb 70 9c d1 48 6a 7a 08 00 45 00  --^--p--Hjz--E-
0010  00 44 08 5f 00 00 01 11 0f 98 c0 a8 00 0f e0 00  --D- - - - -
0020  00 fb 14 e9 14 e9 00 30 e9 f0 00 00 00 00 00 01  -- - - - -0 - - - -
0030  00 00 00 00 00 00 0b 5f 67 6f 6f 67 6c 65 63 61  -- - - - -_googleca
0040  73 74 04 5f 74 63 70 05 6c 6f 63 61 6c 00 00 0c  st-_tcp- local-
0050  00 01
```

### Frame15: 82 bytes on wire

Tipo de encapsulación: Ethernet (1)

Hora de llegada: Mar 11, 2022 21:17:12

Número de cuadro: 15

Longitud de cuadro: 82 bytes (656 bits)

```
▼ Frame 15: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0DED249}, id 0
  ▼ Interface id: 0 (\Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0DED249})
    Interface name: \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0DED249}
    Interface description: Ethernet
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 11, 2022 21:17:12.056202000 Hora estándar romance
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1647029832.056202000 seconds
    [Time delta from previous captured frame: 0.000500000 seconds]
    [Time delta from previous displayed frame: 0.000500000 seconds]
    [Time since reference or first frame: 0.015152000 seconds]
    Frame Number: 15
    Frame Length: 82 bytes (656 bits)
    Capture Length: 82 bytes (656 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:mdns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
```

## Ethernet II

Destinación: IPv4mcast\_fb(01:00:5e:00:00:fb)

Fuente: IntelCor 48:6a 7a (70:9c:d1:48:6a:7a)

Tipo: IPv4

```
▼ Ethernet II, Src: IntelCor_48:6a:7a (70:9c:d1:48:6a:7a), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
  ▼ Destination: IPv4mcast_fb (01:00:5e:00:00:fb)
    Address: IPv4mcast_fb (01:00:5e:00:00:fb)
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 1. .... = IG bit: Group address (multicast/broadcast)
  ▼ Source: IntelCor_48:6a:7a (70:9c:d1:48:6a:7a)
    Address: IntelCor_48:6a:7a (70:9c:d1:48:6a:7a)
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

## Internet Protocol Versión 4

Versión :4

Identificación: 0x0x85f (2143)

Longitud de cuadro : 68

Protocolo: UDP (17)

```
▼ Internet Protocol Version 4, Src: 192.168.0.15, Dst: 224.0.0.251
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... 000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 68
  Identification: 0x085f (2143)
  ▼ Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  ▼ Time to Live: 1
    > [Expert Info (Note/Sequence): "Time To Live" != 255 for a packet sent to the Local Network Control Block (see RFC 3171)]
    Protocol: UDP (17)
    Header Checksum: 0x0f98 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.15
    Destination Address: 224.0.0.251
```

### User Datagram Protocol

Puerto de origen: 5353

Puerto de destino: 5353

Longitud: 48

Suma de control: Inconfirmado

```

User Datagram Protocol, Src Port: 5353, Dst Port: 5353
  Source Port: 5353
  Destination Port: 5353
  Length: 48
  Checksum: 0xe9f0 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 4]
  [Timestamps]
    [Time since first frame: 0.001914000 seconds]
    [Time since previous frame: 0.001352000 seconds]
  UDP payload (40 bytes)

```

### Multicast Domain Name System

ID de la transición: 0x0000

Queries: \_googlecast.\_tcp.local: type PTR, class IN "QM" question

```

Multicast Domain Name System (query)
  Transaction ID: 0x0000
    > [Expert Info (Warning/Protocol): DNS query retransmission. Original request in frame 11]
  Flags: 0x0000 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    .... ..0. .... = Truncated: Message is not truncated
    .... ..0 .... = Recursion desired: Don't do query recursively
    .... ..0... .. = Z: reserved (0)
    .... ..0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    > _googlecast._tcp.local: type PTR, class IN, "QM" question
    [Retransmitted request. Original request in: 11]
    [Retransmission: True]

```

- SSDP

En este caso nosotros vamos a elegir el número 31 donde vamos a explicar posteriormente sus capas:

26 0.461725	192.168.0.16	224.0.0.251	MDNS	87 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
27 0.461905	fe80::b165:5d30:b4d...	ff02::fb	MDNS	107 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
28 0.464815	192.168.0.15	224.0.0.251	MDNS	87 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
29 0.465290	fe80::f870:921a:850...	ff02::fb	MDNS	107 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
30 0.693231	192.168.0.16	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1
31 0.697499	192.168.0.1	192.168.0.16	SSDP	356 HTTP/1.1 200 OK
32 1.003965	192.168.0.16	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
33 1.003965	192.168.0.16	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
34 1.004152	fe80::b165:5d30:b4d...	ff02::fb	MDNS	102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
35 1.004153	fe80::b165:5d30:b4d...	ff02::fb	MDNS	102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question

Nos encontramos con que tiene 5 capas:

```
> Frame 31: 356 bytes on wire (2848 bits), 356 bytes captured (2848 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0ED249}, id 0
> Ethernet II, Src: Sagecom_Bc:8d:f4 (34:49:5b:8c:8d:f4), Dst: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.16
> User Datagram Protocol, Src Port: 1900, Dst Port: 52793
> Simple Service Discovery Protocol

0000  2c f0 5d b6 83 5f 34 49 5b 8c 8d f4 00 00 45 00  ,...4E [.....E
0010  01 58 de ad 00 00 04 11 55 88 c0 a8 00 01 c0 a8  -V.....U.....
0020  00 10 07 6c ce 39 01 42 b3 4b 48 54 54 50 2f 31  --1 0 8 .XHTTP/1
0030  2e 31 20 32 30 30 20 ff 4b 0d 0a 43 61 63 68 65  .1 200 0 K .Cache
0040  24 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67  -Control : max-ag
0050  65 3d 31 39 30 30 0d 0a 4c 6f 63 61 74 69 6f 6e  e=1900 Location
0060  3a 20 68 74 74 70 3a 2f 2f 31 39 32 2e 31 36 38  : http://192.168
0070  2a 30 2e 31 3a 38 30 2f 52 6f 6f 74 44 65 76 69  .0.180/RootDevi
0080  63 65 2e 78 6d 6c 0d 0a 53 65 72 76 65 72 3a 20  ce.xml Server:
0090  55 50 6e 50 2f 31 2e 30 20 55 50 6e 50 2f 31 2e  UPnP/1.0 UPnP/1
00a0  30 20 55 50 6e 50 2d 44 65 76 69 63 65 2d 48 6f  0 UPnP-D evice-Ho
00b0  73 74 2f 31 2e 30 0d 0a 53 54 3a 75 72 6e 3a 73  st/1.0 STurnis
00c0  63 68 65 6d 63 73 2d 75 70 6e 70 2d 6f 72 67 3a  cheap-u pnp-org:
00d0  64 65 76 69 63 65 3a 49 6e 74 65 72 6e 65 74 47  device:I nternetD
00e0  61 74 65 77 61 79 44 65 76 69 63 65 3a 31 0d 0a  atewayDe vice:I
00f0  55 53 4e 3a 20 75 75 69 64 3a 75 70 6e 70 2d 49  USBC uci drupnp-I
0100  6e 74 65 72 6e 65 74 47 61 74 65 77 61 79 44 65  nternetD atewayDe
0110  76 69 63 65 2d 31 5f 30 2d 33 34 34 39 35 62 38  vice-I 0 -3449508
0120  63 30 64 66 34 3a 75 72 6e 3a 73 63 68 65 6d  cbff4:u rnschem
0130  61 73 2d 75 70 6e 70 2d 6f 72 67 3a 64 65 76 69  as-upnp- org:devi
0140  63 65 3a 49 6e 74 65 72 6e 65 74 47 61 74 65 77  ceInter netDew
0150  61 79 44 65 76 69 63 65 3a 31 0d 0a 45 58 54 3a  ayDevice :I EXT:
0160  0d 0a 0d 0a  ....
```

### Frame31: 356 bytes on wire

Tipo de encapsulación: Ethernet (1)

Hora de llegada: Mar 11, 2022 21:17:12

Número de cuadro: 31

Longitud de cuadro: 356 bytes(2824bit)

```
▼ Frame 31: 356 bytes on wire (2848 bits), 356 bytes captured (2848 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0ED249}, id 0
  Interface id: 0 (\Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0ED249})
    Interface name: \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0ED249}
    Interface description: Ethernet
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 11, 2022 21:17:12.738549000 Hora estándar romance
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1647029832.738549000 seconds
    [Time delta from previous captured frame: 0.004268000 seconds]
    [Time delta from previous displayed frame: 0.004268000 seconds]
    [Time since reference or first frame: 0.697499000 seconds]
    Frame Number: 31
    Frame Length: 356 bytes (2848 bits)
    Capture Length: 356 bytes (2848 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:ssdp]
    [Coloring Rule Name: TTL low or unexpected]
    [Coloring Rule String: ( ! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl !
```



## Ethernet II

Destino: Micro-St\_b6:83:5f

Fuente: Sagemcom\_8c:0d:f4

Tipo: IPV4 (0x800)

```

Ethernet II, Src: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4), Dst: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
  Destination: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
    Address: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    Address: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)

```

## Internet Protocol Versión 4

Versión :4

Identificación: 0xdead (57005)

Longitud de cuadro: 342

Protocolo: UDP (17)

Dirección de la fuente: 192.168.0.1

Dirección de destino: 192.168.0.16

```

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.16
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 342
  Identification: 0xdead (57005)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 4
    > [Expert Info (Note/Sequence): "Time To Live" only 4]
  Protocol: UDP (17)
  Header Checksum: 0x5588 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.1
  Destination Address: 192.168.0.16

```

### User Datagram Protocol

Puerto de origen: 1900

Puerto de destino: 52793

Longitud: 322

Suma de control: Inconfirmado

```
▼ User Datagram Protocol, Src Port: 1900, Dst Port: 52793
  Source Port: 1900
  Destination Port: 52793
  Length: 322
  Checksum: 0xb34b [unverified]
  [Checksum Status: Unverified]
  [Stream index: 14]
  ▼ [Timestamps]
    [Time since first frame: 0.000000000 seconds]
    [Time since previous frame: 0.000000000 seconds]
  UDP payload (314 bytes)
```

### Simple Service Discovery Protocol

Versión: HTTP/1.1

Código de estado: 200

Control de Caché: max-age= 1900\r\n

Localización: <http://192.168.0.1:80>

Servidor: UPnP/1.0UPnP-Device-Host/1.0\r\n

ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n

EXT:\r\n

```
▼ Simple Service Discovery Protocol
  ▼ HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Cache-Control: max-age=1900\r\n
      Location: http://192.168.0.1:80/RootDevice.xml\r\n
      Server: UPnP/1.0 UPnP/1.0 UPnP-Device-Host/1.0\r\n
      ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n
      USN: uuid:upnp-InternetGatewayDevice-1_0-34495b8c0df4::urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n
      EXT:\r\n
      \r\n
      [HTTP response 1/3]
      [Next response in frame: 2138]
```

- LLDP

En este caso nosotros vamos a elegir el número 49 donde vamos a explicar posteriormente sus capas:

45	1.012357	192.168.0.15	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
46	1.012776	fe80::f870:921a:850...	ff02::fb	MDNS	102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
47	1.013155	fe80::f870:921a:850...	ff02::fb	MDNS	102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
48	1.830233	Sagemcom_8c:0d:f4	IEEE-1905.1-Control	ieee19...	60 Topology discovery
49	1.830233	Sagemcom_8c:0d:f4	LLDP_Multicast	LLDP	60 MA/34:49:5b:8c:0d:f4 MA/34:4d:5b:8c:0d:f4 180
50	1.889405	192.168.0.1	239.255.255.250	SSDP	342 NOTIFY * HTTP/1.1
51	1.889563	192.168.0.1	239.255.255.250	SSDP	398 NOTIFY * HTTP/1.1
52	1.889625	192.168.0.1	239.255.255.250	SSDP	326 NOTIFY * HTTP/1.1

Nos encontramos con que tiene 3 capas:

```
> Frame 49: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0ED249}, id 0
> Ethernet II, Src: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
> Link Layer Discovery Protocol
```

```
0000  01 80 c2 00 00 0e 34 49 5b 8c 0d f4 88 cc 02 07  ....4I[.....
0010  04 34 49 5b 8c 0d f4 04 07 03 34 4d 5b 8c 0d f4  4I[.....4M[...
0020  06 02 00 b4 00 00 a8 c6 9e 22 a1 6f 83 52 8f bb  ......."o.R...
0030  d2 b5 44 d5 c5 7b 14 4d 02 78 42 c3  ..D..{.M.xB.
```

### Frame15: 82 bytes on wire

Tipo de encapsulación: Ethernet (1)

Hora de llegada: Mar 11, 2022 21:17:13

Número de cuadro: 49

Longitud de cuadro: 60bytes (480 bits)

```
▼ Frame 49: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0ED249}, id 0
  > Interface id: 0 (\Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0ED249})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 11, 2022 21:17:13.871283000 Hora estándar romance
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1647029833.871283000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 1.830233000 seconds]
    Frame Number: 49
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:lldp]
    [Coloring Rule Name: Broadcast]
    [Coloring Rule String: eth[0] & 1]
```

## Ethernet II

Destinación: LLDP\_Multicast(01:80:c2:00:00:0e)

Fuente: Sagemcom\_8c:0d:f4

Tipo: 802.1(LLDP)(0x88cc)

- ▼ Ethernet II, Src: Sagemcom\_8c:0d:f4 (34:49:5b:8c:0d:f4), Dst: LLDP\_Multicast (01:80:c2:00:00:0e)
  - ▼ Destination: LLDP\_Multicast (01:80:c2:00:00:0e)
    - Address: LLDP\_Multicast (01:80:c2:00:00:0e)
    - .... ..0. .... = LG bit: Globally unique address (factory default)
    - .... ...1. .... = IG bit: Group address (multicast/broadcast)
  - ▼ Source: Sagemcom\_8c:0d:f4 (34:49:5b:8c:0d:f4)
    - Address: Sagemcom\_8c:0d:f4 (34:49:5b:8c:0d:f4)
    - .... ..0. .... = LG bit: Globally unique address (factory default)
    - .... ...0. .... = IG bit: Individual address (unicast)
  - Type: 802.1 Link Layer Discovery Protocol (LLDP) (0x88cc)
  - ▼ Trailer: b40000a8c69e22a16f83528fbbd2b544d5c57b144d027842c3

## Link Layer Discovery Protocol

Subtipo de Chasis: MAC address, Id: 34:49:5b:8c:0d:f4

Subtipo de puertos: MAC address, Id: 34:4d:5b:8c:0d:f4

Tiempo activo: 180 segundos

- ▼ Link Layer Discovery Protocol
  - ▼ Chassis Subtype = MAC address, Id: 34:49:5b:8c:0d:f4
    - 0000 001. .... = TLV Type: Chassis Id (1)
    - .... ...0 0000 0111 = TLV Length: 7
    - Chassis Id Subtype: MAC address (4)
    - Chassis Id: Sagemcom\_8c:0d:f4 (34:49:5b:8c:0d:f4)
  - ▼ Port Subtype = MAC address, Id: 34:4d:5b:8c:0d:f4
    - 0000 010. .... = TLV Type: Port Id (2)
    - .... ...0 0000 0111 = TLV Length: 7
    - Port Id Subtype: MAC address (3)
    - Port Id: 34:4d:5b:8c:0d:f4 (34:4d:5b:8c:0d:f4)
  - ▼ Time To Live = 180 sec
    - 0000 011. .... = TLV Type: Time to Live (3)
    - .... ...0 0000 0010 = TLV Length: 2
    - Seconds: 180
  - ▼ End of LLDPDU
    - 0000 000. .... = TLV Type: End of LLDPDU (0)
    - .... ...0 0000 0000 = TLV Length: 0

- UDP

En este caso nosotros vamos a elegir el número 89 donde vamos a explicar posteriormente sus capas:

86	2.641925	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321	Len=1357
87	2.641990	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321	Len=1357
88	2.641990	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321	Len=1357
89	2.641990	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321	Len=1357
90	2.641990	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321	Len=1357
91	2.641990	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321	Len=1357

Nos encontramos con que tiene 5 capas:

```
> Frame 89: 1399 bytes on wire (11192 bits), 1399 bytes captured (11192 bits) on interface \Device\NPF_{36438583-DF7C-4460-8798-2733F80ED249}, Id 0
> Ethernet II, Src: Sagemcom_Rc:0d:f4 (34:49:5b:8c:0d:f4), Dst: Mikro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
> Internet Protocol Version 4, Src: 77.227.215.15, Dst: 192.168.0.16
> User Datagram Protocol, Src Port: 443, Dst Port: 52321
> Data (1357 bytes)
```

```
0000  2c f0 5d b6 83 5f 34 49 5b 8c 0d f4 08 00 45 00  .,]...41 [.....E
0010  05 69 00 0f 40 00 7b 11 14 ca 4d e3 d7 0f c0 a8  .i.@{...H.....
0020  00 10 01 b0 cc c1 95 55 a7 96 54 58 70 e3 57 52  ...pU...TxxUR
0030  c6 59 f7 69 21 13 a0 64 8f c0 53 53 8e eb c6 ba  .y:ll...d..SS....
0040  dd 36 c8 28 5d 3d c3 ad ab 70 5b b1 ce 86 d2 b3  .6.()...p[.....
0050  48 85 d5 77 8b 9e 8f 59 85 39 e6 3a f8 ef a7 75  H+mm...Y..9...u
0060  a6 00 d7 38 a6 69 52 66 04 7d 6d 63 f2 6f 1d 4a  ...0-LRF...jmc...3
0070  36 15 a2 1a f7 75 a6 4a 3f 79 f9 d8 9a 2c f8 c5  6...u...3y.....
0080  6e cf 58 88 7a 03 df e9 b5 9c b1 c6 05 f3 bc ce  nXz... ..
0090  c2 fc c6 79 ed 9d 95 22 6f 4e 4a 44 32 75 a0 e9  ...y...m002u...
00a0  45 2f 82 03 89 a9 e9 76 f4 2d 9e 8e 42 93 80 01  E/...I...v...8...
00b0  0c 9f be 91 3c 26 25 d9 ed 9e 76 30 44 68 32 f3  ....<8%...v00h2.
00c0  02 40 ba 58 3b 0d b5 29 f6 f0 bf 04 6f ae 5c 85  .@Xj... ..
00d0  09 85 a5 58 f3 05 e4 26 fa 10 5d a4 22 ec 0f cd  ...P...8...
00e0  fe a8 84 33 e8 3a eb 54 9f e3 a7 d6 99 87 9f 20  ...3...T...c....
00f0  09 92 dd 1e 07 47 ee d2 2d e7 0f a1 41 75 df 8e  ....G...Au...
0100  0f 8d f7 a8 8a ae 66 61 c4 2d 9d 5e 09 d1 f3 ad  ....fa...
0110  64 8f d3 56 96 a0 11 b3 3f a9 70 ae bf 35 49 57  d-VX...2-pr-SB
0120  2e 1a 59 1a 4e 76 66 14 f2 da ed ea a9 a0 70 a9  .Y-Nvf... ..p
0130  e8 3b 15 a7 b1 62 1a 20 43 79 e5 55 1a ea 5e d4  .j...b...Cy-U...
0140  3a 81 90 97 c9 52 c4 08 aa a4 32 8e 66 bf 2b a6  ....R...2-f...
0150  11 b0 3f 00 8b 3a 77 f3 97 e5 c5 af 01 5f 35 35  ...3...aw...55
0160  56 c3 d7 ac 2e 34 38 02 ac 6f 0f b3 a0 23 cb da  V...48...p...#...
0170  61 4b 67 a1 9e b8 f5 2b 8b c1 d8 c8 14 1e b6 47  aKg...+...G
0180  00 d3 7f e7 5b b0 01 80 c7 01 75 97 f0 e7 3b 5c  ...[... ..
0190  31 fa 7b 6b 79 81 16 a5 88 81 41 20 5a ae 32 10  1-[ky...A(2.2.
01a0  74 e6 bd af 13 f1 e9 5b 2a 5d 4a 9a ca d9 30 c8  t.....[ ]2...0
01b0  56 ca ed 1c b6 a6 88 f6 17 d6 67 09 16 06 41 91  V.....g...A
01c0  ca 46 33 55 a5 da 3b 29 9e 69 93 4c 48 96 64 be  ^F3U...j...i-LH-d
```

**Frame89: 1399 bytes on wire**

Tipo de encapsulación: Ethernet (1)

Hora de llegada: Mar 11, 2022 21:17:14

Número de cuadro: 89

Longitud de cuadro: 1399bytes(11192bits)

```
> Interface id: 0 (\Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0DED249})
Encapsulation type: Ethernet (1)
Arrival Time: Mar 11, 2022 21:17:14.683040000 Hora estándar romance
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1647029834.683040000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 2.641990000 seconds]
Frame Number: 89
Frame Length: 1399 bytes (11192 bits)
Capture Length: 1399 bytes (11192 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:data]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
```

## Ethernet II

Destinación: Micro-St\_b6:83:5f

Fuente Micro-St\_b6:83:5f

Tipo: IPv4 (0x0800)

```
▼ Ethernet II, Src: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
  ▼ Destination: LLDP_Multicast (01:80:c2:00:00:0e)
    Address: LLDP_Multicast (01:80:c2:00:00:0e)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ...1 .... = IG bit: Group address (multicast/broadcast)
  ▼ Source: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    Address: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ...0 .... = IG bit: Individual address (unicast)
    Type: 802.1 Link Layer Discovery Protocol (LLDP) (0x88cc)
  ▼ Trailer: b40000a8c69e22a16f83528fbbd2b544d5c57b144d027842c3
```

## Internet Protocol Versión 4

Versión :4

Identificación: 0xec2 (52930)

Longitud de cuadro: 342

Protocolo: UDP (17)

Dirección de la fuente: 192.168.0.1

Dirección de destino: 192.168.0.16

```

  ▾ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.16
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 342
    Identification: 0xdead (57005)
    ▾ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment Offset: 0
    ▾ Time to Live: 4
      > [Expert Info (Note/Sequence): "Time To Live" only 4]
    Protocol: UDP (17)
    Header Checksum: 0x5588 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.1
    Destination Address: 192.168.0.16

```

### User Datagram Protocol

Puerto de origen: 52574

Puerto de destino: 53

Longitud: 45

Suma de control: Inconfirmado

```

  ▾ User Datagram Protocol, Src Port: 52574, Dst Port: 53
    Source Port: 52574
    Destination Port: 53
    Length: 45
    Checksum: 0x67ee [unverified]
    [Checksum Status: Unverified]
    [Stream index: 30]
    ▾ [Timestamps]
      [Time since first frame: 0.000000000 seconds]
      [Time since previous frame: 0.000000000 seconds]
    UDP payload (37 bytes)

```

### Domain Name System

ID de la transición: 0x9d1f

Queries: campusonline.ifp.es: type A, class IN

```

v Domain Name System (query)
  Transaction ID: 0x9d1f
  v 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
  v Queries
    > campusonline.ifp.es: type A, class IN
    [Response In: 2223]

```

- DNS

En este caso nosotros vamos a elegir el número 2221 donde vamos a explicar posteriormente

sus capas:

No.	Time	Source	Destination	Protocol	Length	Info
2219	8.203527	192.168.0.16	212.166.210.80	DNS	91	Standard query 0x6cf7 A learn.content.blackboardcdn.com
2220	8.203527	192.168.0.16	212.166.210.80	DNS	81	Standard query 0x6d31 A js-agent.newrelic.com
2221	8.203550	192.168.0.16	212.166.210.80	DNS	79	Standard query 0x9d1f A campusonline.ifp.es
2222	8.214897	212.166.210.80	192.168.0.16	DNS	134	Standard query response 0x6d31 A js-agent.newrelic.com CNAME k.sni.

Nos encontramos con que tiene 3 capas:

```

> Frame 2221: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-8798-2733F0ED249}, id
> Ethernet II, Src: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f), Dst: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
> Internet Protocol Version 4, Src: 192.168.0.16, Dst: 212.166.210.80
> User Datagram Protocol, Src Port: 52574, Dst Port: 53
> Domain Name System (query)

```

```

0000 34 49 5b 8c 0d f4 2c f0 5d b6 83 5f 08 00 45 00 4I[...].E-
0010 00 41 ce c2 00 00 80 11 00 00 c0 a8 00 10 d4 a6 .A.....
0020 d2 50 cd 5e 00 35 00 2d 67 ee 9d 1f 01 00 00 01 .P^5- g.....
0030 00 00 00 00 00 0c 63 61 6d 70 75 73 6f 6e 6c .....campusonl
0040 69 6e 65 03 69 66 70 02 65 73 00 00 01 00 01 ine-ifp.es....

```

**Frame2221: 79 bytes on wire**

Tipo de encapsulación: Ethernet (1)

Hora de llegada: Mar 11, 2022 21:17:20

Número de cuadro: 221



Longitud de cuadro: 79bytes (632 bits)

```

✓ Frame 2221: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0DED249}, id 0
  > Interface id: 0 (\Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0DED249})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 11, 2022 21:17:20.244600000 Hora estándar romance
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1647029840.244600000 seconds
    [Time delta from previous captured frame: 0.000023000 seconds]
    [Time delta from previous displayed frame: 0.000023000 seconds]
    [Time since reference or first frame: 8.203550000 seconds]
    Frame Number: 2221
    Frame Length: 79 bytes (632 bits)
    Capture Length: 79 bytes (632 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]

```

### Ethernet II

Destinación: Sagemcom\_8c:0d:f4

Fuente: Micro-St\_b6:83:5f

Tipo: IPv4 (0x0800)

```

✓ Ethernet II, Src: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f), Dst: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
  ✓ Destination: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    Address: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0 .... = IG bit: Individual address (unicast)
  ✓ Source: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
    Address: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0 .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)

```

### Internet Protocol Versión 4

Versión :4

Identificación: 0xec2(52930)

Longitud de cuadro: 65

Protocolo: UDP (17)

Dirección de la fuente: 192.168.0.16

Dirección de destino: 212.166.210.80

```
Internet Protocol Version 4, Src: 192.168.0.16, Dst: 212.166.210.80
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 65
  Identification: 0xcec2 (52930)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.16
  Destination Address: 212.166.210.80
```

### User Datagram Protocol

Puerto de origen:52574

Puerto de destino: 53

Longitud:45

Suma de control 0x67ee Incorfirmado

```
User Datagram Protocol, Src Port: 52574, Dst Port: 53
  Source Port: 52574
  Destination Port: 53
  Length: 45
  Checksum: 0x67ee [unverified]
  [Checksum Status: Unverified]
  [Stream index: 30]
  [Timestamps]
    [Time since first frame: 0.000000000 seconds]
    [Time since previous frame: 0.000000000 seconds]
  UDP payload (37 bytes)
```

### Domain Name System

ID de la transición: 0x9d1f

Queries: campusonline.ifp.es: type A, class IN

```

▼ Domain Name System (query)
  Transaction ID: 0x9d1f
  ▼ 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
    > campusonline.ifp.es: type A, class IN
    [Response In: 2223]

```

- TLSV.2

En este caso nosotros vamos a elegir el número 2249 donde vamos a explicar posteriormente sus capas:

2240	8.252731	192.168.0.16	18.158.76.148	TLSv1.2	571 Client Hello
2242	8.285577	18.158.76.148	192.168.0.16	TLSv1.2	1514 Server Hello
2248	8.287156	18.158.76.148	192.168.0.16	TLSv1.2	677 Certificate, Server Key Exchange, Server Hello Done
2249	8.290044	192.168.0.16	18.158.76.148	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2250	8.321432	18.158.76.148	192.168.0.16	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
2251	8.321667	192.168.0.16	18.158.76.148	TLSv1.2	1012 Application Data
2253	8.359771	18.158.76.148	192.168.0.16	TLSv1.2	81 Application Data

Nos encontramos con que tiene 5 capas:

```

> Frame 2249: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0ED249}, id 6
> Ethernet II, Src: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f), Dst: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
> Internet Protocol Version 4, Src: 192.168.0.16, Dst: 18.158.76.148
> Transmission Control Protocol, Src Port: 61028, Dst Port: 443, Seq: 518, Ack: 6180, Len: 126
> Transport Layer Security

```

```

0000  34 49 5b 8c 0d f4 2c f0 5d b6 83 5f 08 00 45 00 4I[... ]...E
0010  00 a6 ce bf 40 00 80 06 00 00 c0 a8 00 10 12 9e ...@:.....
0020  4c 94 ee 64 01 bb 3b ef 7a f2 7b 3c 49 f5 50 18 L...;...z{<I-P
0030  04 00 20 83 00 00 16 03 03 00 46 10 00 00 42 41 .....F...BA
0040  04 98 eb 6b 33 67 45 6d c0 7a 22 2a 39 04 8d 5f ...k3gEm...z"*9...
0050  0f 47 a4 b4 12 1e 49 40 e5 89 d1 3f a4 83 97 ed ...G...I@...?...
0060  59 8a 8c 08 9f f7 54 6b 43 41 68 8d 5e 52 b7 8a Y...Tk CAh^R...
0070  0c c2 db 58 00 6c 83 6d f3 81 85 f3 05 c8 95 5f ...X:l:m .....
0080  e5 14 03 03 00 01 01 16 03 03 00 28 00 00 00 00 .....(.....
0090  00 00 00 00 68 f3 d9 87 4c cb 75 26 97 b4 14 32 ...h...L'u&...2
00a0  b0 93 73 19 69 cc 1a 5f 90 1f 63 f7 67 a9 8c 4d ...s.i...c:g...M
00b0  67 91 e1 6c                                     g...l

```

### Frame2249: 180 bytes on wire

Tipo de encapsulación: Ethernet (1)

Hora de llegada: Mar 11, 2022 21:17:20

Número de cuadro: 2249

Longitud de cuadro: 180bytes (1440 bits)

```
▼ Frame 2249: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0ED249}, id
  > Interface id: 0 (\Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0ED249})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 11, 2022 21:17:20.331094000 Hora estándar romance
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1647029840.331094000 seconds
    [Time delta from previous captured frame: 0.002888000 seconds]
    [Time delta from previous displayed frame: 0.002888000 seconds]
    [Time since reference or first frame: 8.290044000 seconds]
    Frame Number: 2249
    Frame Length: 180 bytes (1440 bits)
    Capture Length: 180 bytes (1440 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
```

### Ethernet II

Destinación: Sagemcom\_8c:0d:f4

Fuente: Micro-St\_b6:83:5f

Tipo: IPv4 (0x0800)

```
✓ Ethernet II, Src: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f), Dst: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
  ▼ Destination: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    Address: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
    Address: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

### Internet Protocol Versión 4

Versión :4

Identificación: 0xec2(52927)

Longitud de cuadro: 166

Protocolo: UDP (17)

Dirección de la fuente: 192.168.0.16

Dirección de destino: 212.166.76.148

```

  ▾ Internet Protocol Version 4, Src: 192.168.0.16, Dst: 18.158.76.148
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 166
    Identification: 0xcebf (52927)
    ▾ Flags: 0x40, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.16
    Destination Address: 18.158.76.148

```

### Transmission Control Protocol:

Puerto de Origen:61028

Puerto de destino: 443

Secuencia de números: 518

Window 1024

Calculo de tamaño de Window:262144

Suma de control: 0x2083

Factor de escala del tamaño de Windows:256

```

  ▾ Transmission Control Protocol, Src Port: 61028, Dst Port: 443, Seq: 518, Ack: 6180, Len: 126
    Source Port: 61028
    Destination Port: 443
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 126]
    Sequence Number: 518 (relative sequence number)
    Sequence Number (raw): 1005550322
    [Next Sequence Number: 644 (relative sequence number)]
    Acknowledgment Number: 6180 (relative ack number)
    Acknowledgment number (raw): 2067548661
    0101 .... = Header Length: 20 bytes (5)
    ▸ Flags: 0x018 (PSH, ACK)
    Window: 1024
    [Calculated window size: 262144]
    [Window size scaling factor: 256]
    Checksum: 0x2083 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    ▸ [Timestamps]
    ▸ [SEQ/ACK analysis]
    TCP payload (126 bytes)

```

### Transport Layer Security:

Edison Gabriel Vaca Cifuentes

Tipo de Contenido: Handshake (22)

Versión: TLS 1.2 (0X0303)

Longitud: 70

Ec Diffie-Hellam Client Params:

Longitud de Pubkey : 65

Pubkey:0498eb6b3367456dc07a222a39048d5f0f47a4b4121e4940e589d13fa48397ed598a8c08...

```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 70
  Handshake Protocol: Client Key Exchange
    Handshake Type: Client Key Exchange (16)
    Length: 66
  EC Diffie-Hellman Client Params
    Pubkey Length: 65
    Pubkey: 0498eb6b3367456dc07a222a39048d5f0f47a4b4121e4940e589d13fa48397ed598a8c08...
```

- TCP

En este caso nosotros vamos a elegir el número 2266 donde vamos a explicar posteriormente sus capas:

2259	8.445553	18.158.76.148	192.168.0.16	TCP	60 443 → 61028 [ACK] Seq=7718 Ack=2936 Win=32768 Len=0
2264	8.534744	18.158.76.148	192.168.0.16	TLSv1.2	1105 Application Data
2265	8.543327	192.168.0.16	18.158.76.148	TLSv1.2	1417 Application Data
2266	8.575393	18.158.76.148	192.168.0.16	TCP	60 443 → 61028 [ACK] Seq=8769 Ack=4299 Win=35328 Len=0
2267	8.861485	18.158.76.148	192.168.0.16	TCP	1514 443 → 61028 [ACK] Seq=8769 Ack=4299 Win=35328 Len=1460 [TCP segment of a reassembled PD
2268	8.861485	18.158.76.148	192.168.0.16	TCP	1514 443 → 61028 [ACK] Seq=10229 Ack=4299 Win=35328 Len=1460 [TCP segment of a reassembled PD
2269	8.861553	192.168.0.16	18.158.76.148	TCP	54 61028 → 443 [ACK] Seq=4299 Ack=11689 Win=262656 Len=0
2270	8.861580	18.158.76.148	192.168.0.16	TCP	1514 443 → 61028 [ACK] Seq=11689 Ack=4299 Win=35328 Len=1460 [TCP segment of a reassembled PD

Nos encontramos con que tiene 5 capas:

```
> Frame 2266: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0ED249}, id 0
> Ethernet II, Src: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4), Dst: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
> Internet Protocol Version 4, Src: 18.158.76.148, Dst: 192.168.0.16
> Transmission Control Protocol, Src Port: 443, Dst Port: 61028, Seq: 8769, Ack: 4299, Len: 0
```

```
0000  2c f0 5d b6 83 5f 34 49 5b 8c 0d f4 08 00 45 00  ,.].._4I [.....E.
0010  00 28 37 f8 40 00 ed 06 35 ed 12 9e 4c 94 c0 a8  .(7.@...5...L...
0020  00 10 01 bb ee 64 7b 3c 54 12 3b ef 89 b7 50 10  ....d{<T;...P.
0030  00 8a 0a 4b 00 00 00 00 00 00 00 00 00 00 00  ...K.....
```

**Frame2260: 60 bytes on wire**

Tipo de encapsulación: Ethernet (1)

Hora de llegada: Mar 11, 2022 21:17:20

Número de cuadro: 2266

Longitud de cuadro: 60bytes (480 bits)

```

▼ Frame 2249: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0ED249}, id
  > Interface id: 0 (\Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0ED249})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 11, 2022 21:17:20.331094000 Hora estándar romance
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1647029840.331094000 seconds
    [Time delta from previous captured frame: 0.002888000 seconds]
    [Time delta from previous displayed frame: 0.002888000 seconds]
    [Time since reference or first frame: 8.290044000 seconds]
    Frame Number: 2249
    Frame Length: 180 bytes (1440 bits)
    Capture Length: 180 bytes (1440 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]

```

**Ethernet II**

Destinación: Micro-St\_b6:83:5f

Fuente: Micro-St\_b6:83:5f

Tipo: IPv4 (0x0800)

```

▼ Ethernet II, Src: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4), Dst: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
  ▼ Destination: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
    Address: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  ▼ Source: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    Address: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    Padding: 000000000000

```

**Internet Protocol Versión 4**

Versión: 4

Identificación: 0x37F8(14328)

Longitud de cuadro: 40

Protocolo: UDP (6)

Dirección de la fuente: 18.158.76.148

Dirección de destino: 192.168.0.16

```
▼ Internet Protocol Version 4, Src: 18.158.76.148, Dst: 192.168.0.16
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 40
  Identification: 0x37f8 (14328)
  ▼ Flags: 0x40, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 237
  Protocol: TCP (6)
  Header Checksum: 0x35ed [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 18.158.76.148
  Destination Address: 192.168.0.16
```

### Transmission Control Protocol:

Puerto de Origen:61028

Puerto de destino: 443

Secuencia de números: 518

Window 1024

Calculo de tamaño de Window:262144

Suma de control: 0x2083

Factor de escala del tamaño de Windows:256

```
▼ Transmission Control Protocol, Src Port: 61028, Dst Port: 443, Seq: 518, Ack: 6180, Len: 126
  Source Port: 61028
  Destination Port: 443
  [Stream index: 0]
  [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 126]
  Sequence Number: 518 (relative sequence number)
  Sequence Number (raw): 1005550322
  [Next Sequence Number: 644 (relative sequence number)]
  Acknowledgment Number: 6180 (relative ack number)
  Acknowledgment number (raw): 2067548661
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
  Window: 1024
  [Calculated window size: 262144]
  [Window size scaling factor: 256]
  Checksum: 0x2083 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
  TCP payload (126 bytes)
```



- QUIC

En este caso nosotros vamos a elegir el número 42338 donde vamos a explicar posteriormente sus capas:

42338	263.346807	192.168.0.16	162.159.136.232	QUIC	1392 Initial, DCID=3e7326c1caa10067, PKN: 1, CRYPTO, PADDING
42339	263.346950	192.168.0.16	162.159.136.232	QUIC	119 0-RTT, DCID=3e7326c1caa10067
42343	263.359944	162.159.136.232	192.168.0.16	QUIC	1242 Protected Payload (KP0)
42344	263.360492	192.168.0.16	162.159.136.232	QUIC	132 Handshake, DCID=01d6848cd910bbd77bd7eb8cf410b8120bdb7d73
42345	263.360675	192.168.0.16	162.159.136.232	QUIC	1386 Protected Payload (KP0), DCID=01d6848cd910bbd77bd7eb8cf410b8120bdb7d73
42346	263.360699	192.168.0.16	162.159.136.232	QUIC	532 Protected Payload (KP0), DCID=01d6848cd910bbd77bd7eb8cf410b8120bdb7d73

Nos encontramos con que tiene 5 capas:

```
> Frame 42338: 1392 bytes on wire (11136 bits), 1392 bytes captured (11136 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-273F0DEDE249}
> Ethernet II, Src: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f), Dst: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
> Internet Protocol Version 4, Src: 192.168.0.16, Dst: 162.159.136.232
> User Datagram Protocol, Src Port: 64618, Dst Port: 443
> QUIC IETF
```

```
0000 34 49 5b 8c 0d f4 2c f0 5d b6 83 5f 08 00 45 00 4I[...].E
0010 05 62 cd 13 40 00 80 11 00 00 c0 a8 00 10 a2 9f b@...
0020 88 e8 fc 6a 01 bb 05 4e f1 9f c5 ff 00 00 1d 08 j...N
0030 3e 73 26 c1 ca a1 00 67 00 00 45 34 94 37 11 b2 >s&...gE4.7..
0040 2f 3a 9b ca ae 01 7c fc 0d 7d 0a 64 5d af 86 2a /:....|.d).*
0050 a8 2f 4d 35 b9 ba 3e 70 89 11 ba 3d c9 78 15 d5 ./M5...p...x..
0060 f4 8b 29 52 1b 4c 6e 89 ac 7c d1 a6 6c b4 41 82 ..)R.Ln..|..l.A.
0070 83 d2 ad 16 e8 53 f3 6d 53 14 bc 9b 6b 87 20 02 .....S.m S...k..
0080 25 85 df 78 93 e0 6d c4 f1 35 b1 cf 78 ca 2e 5a %..x..m..5..x..Z
0090 f8 6a 29 2a 2f 6d d4 ad d1 42 f9 09 7e 38 99 0e .j)*./m..B...8..
00a0 a3 d4 31 3f fc ca 35 c8 bf 88 11 6b c3 88 49 bb ..1?...5..k..I.
00b0 fe 2a 47 b8 3a 9a 35 86 7f cc ff 97 11 24 66 12 *G...5..$f.
00c0 3b 43 26 46 c5 b3 65 7a 1d fc 07 8e 2e 5f 07 58 ;C&F...ez....X
```

### Frame 42338: 1392 bytes on wire

Tipo de encapsulación: Ethernet (1)

Hora de llegada: Mar 11, 2022 21:17:14

Número de cuadro: 42338

Longitud de cuadro: 1392 bytes (11136 bits)

```
> Interface id: 0 (\Device\NPF_{3E43B5B3-DF7C-4460-879B-273F0DEDE249})
Encapsulation type: Ethernet (1)
Arrival Time: Mar 11, 2022 21:17:14.683040000 Hora estándar romance
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1647029834.683040000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 2.641990000 seconds]
Frame Number: 89
Frame Length: 1399 bytes (11192 bits)
Capture Length: 1399 bytes (11192 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:data]
[Coloring Rule Name: UDP]
[Coloring Rule String: udnl]
```

## Ethernet II

Destinación: Micro-St\_b6:0d:f4

Fuente Micro-St\_b6:0d:f4

Tipo: IPv4 (0x0800)

```
▼ Ethernet II, Src: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f), Dst: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
  ▼ Destination: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    Address: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0 .... = IG bit: Individual address (unicast)
  ▼ Source: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
    Address: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0 .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

## Internet Protocol Versión 4

Versión :4

Identificación: 0xcec13 (52499)

Longitud de cuadro: 1378

Protocolo: UDP (17)

Dirección de la fuente: 192.168.0.16

Dirección de destino: 192.159.136.232

```
▼ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.16
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 342
  Identification: 0xdead (57005)
  ▼ Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  ▼ Time to Live: 4
    > [Expert Info (Note/Sequence): "Time To Live" only 4]
  Protocol: UDP (17)
  Header Checksum: 0x5588 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.1
  Destination Address: 192.168.0.16
```

### User Datagram Protocol

Puerto de origen: 64618

Puerto de destino: 443

Longitud: 1358

Suma de control: 0xf194 Inconfirmado

```

User Datagram Protocol, Src Port: 64618, Dst Port: 443
  Source Port: 64618
  Destination Port: 443
  Length: 1358
  Checksum: 0xf19f [unverified]
  [Checksum Status: Unverified]
  [Stream index: 168]
  > [Timestamps]
  UDP payload (1350 bytes)

```

### QUIC IETF

Longitud de paquete :1350

Versión: draft-29

Conexión de Id de longitud de destino: 8

Conexión de Id de destino 3e7326c1caa10067

Número de paquetes :1

Payload:3711b22f3a9bcaae017cfc0d7d0a645daf862aa82f4d35b9ba3e708911ba3dc97815d5f4

...

```

QUIC IETF
  QUIC Connection information
    [Connection Number: 0]
    [Packet Length: 1350]
    1... .... = Header Form: Long Header (1)
    .1.. .... = Fixed Bit: True
    ..00 .... = Packet Type: Initial (0)
    .... 00.. = Reserved: 0
    .... ..00 = Packet Number Length: 1 bytes (0)
    Version: draft-29 (0xff00001d)
    Destination Connection ID Length: 8
    Destination Connection ID: 3e7326c1caa10067
    Source Connection ID Length: 0
    Token Length: 0
    Length: 1332
    Packet Number: 1
    Payload: 3711b22f3a9bcaae017cfc0d7d0a645daf862aa82f4d35b9ba3e708911ba3dc97815d5f4...

```

- ARP

En este caso nosotros vamos a elegir el número 47604 donde vamos a explicar posteriormente sus capas:

24771	195.452662	HuaweiTe_1d:58:6e	Broadcast	ARP	60 Who has 192.168.0.1? Tell 192.168.0.13
32582	225.584855	HuaweiTe_1d:58:6e	Broadcast	ARP	60 Who has 192.168.0.1? Tell 192.168.0.13
40600	255.708063	HuaweiTe_1d:58:6e	Broadcast	ARP	60 Who has 192.168.0.1? Tell 192.168.0.13
47604	285.793199	HuaweiTe_1d:58:6e	Broadcast	ARP	60 Who has 192.168.0.1? Tell 192.168.0.13
55524	315.877950	HuaweiTe_1d:58:6e	Broadcast	ARP	60 Who has 192.168.0.1? Tell 192.168.0.13
63378	346.027598	HuaweiTe_1d:58:6e	Broadcast	ARP	60 Who has 192.168.0.1? Tell 192.168.0.13
69232	370.214793	Sagemcom_8c:0d:f4	Broadcast	ARP	60 Who has 172.31.255.40? Tell 192.168.0.1
69604	372.211210	Sagemcom_8c:0d:f4	Broadcast	ARP	60 Who has 172.31.255.45? Tell 192.168.0.1

Nos encontramos con que tiene 3 capas:

```
> Frame 47604: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0DED2}
> Ethernet II, Src: HuaweiTe_1d:58:6e (34:12:f9:1d:58:6e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

### Frame42338: 13923 bytes on wire

Tipo de encapsulación: Ethernet (1)

Hora de Llegada: Mar 11, 2022 21:17:14

Número de cuadro: 89

Longitud de cuadro: 1399bytes(11192bits)

```
> Interface id: 0 (\Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0DED249})
  Encapsulation type: Ethernet (1)
  Arrival Time: Mar 11, 2022 21:17:14.683040000 Hora estándar romance
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1647029834.683040000 seconds
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 2.641990000 seconds]
  Frame Number: 89
  Frame Length: 1399 bytes (11192 bits)
  Capture Length: 1399 bytes (11192 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:data]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
```

## Ethernet II

Destinación: Micro-St\_b6:0d:5f

Fuente Micro-St\_b6:0d:f4

Tipo: IPv4 (0x0800)

```

Ethernet II, Src: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f), Dst: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
  Destination: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    Address: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
    Address: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)

```

## Internet Protocol Versión 4

Versión :4

Identificación: 0xcec13 (52499)

Longitud de cuadro: 1378

Protocolo: UDP (17)

Dirección de la fuente: 192.168.0.16

Dirección de destino: 192.159.136.232

```

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.16
  0100 .... = Version: 4
  ....0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    ....0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 342
  Identification: 0xdead (57005)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 4
    > [Expert Info (Note/Sequence): "Time To Live" only 4]
  Protocol: UDP (17)
  Header Checksum: 0x5588 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.1
  Destination Address: 192.168.0.16

```

- IGMP V3

En este caso nosotros vamos a elegir el número 47604 donde vamos a explicar posteriormente sus capas:

36641	240.926689	192.168.0.11	224.0.0.22	IGMPv3	60 Membership Report / Join group 224.0.0.251 for any sources
47484	285.341168	192.168.0.1	224.0.0.1	IGMPv3	60 Membership Query, general
47485	285.342698	192.168.5.1	224.0.0.1	IGMPv3	60 Membership Query, general
47563	285.628064	192.168.0.16	224.0.0.22	IGMPv3	54 Membership Report / Join group 224.0.0.251 for any sources
47794	286.632254	192.168.0.16	224.0.0.22	IGMPv3	54 Membership Report / Join group 224.0.0.252 for any sources
48598	290.121374	192.168.0.16	224.0.0.22	IGMPv3	54 Membership Report / Join group 239.255.255.250 for any sources
48800	290.880946	192.168.0.10	224.0.0.22	IGMPv3	64 Membership Report / Join group 239.255.255.250 for any sources

Nos encontramos con que tiene 4 capas:

```
> Frame 47563: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0DED249}, id 0
> Ethernet II, Src: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
> Internet Protocol Version 4, Src: 192.168.0.16, Dst: 224.0.0.22
> Internet Group Management Protocol

0000  01 00 5e 00 00 16 2c f0 5d b6 83 5f 08 00 46 00  ..^... ]...F.
0010  00 28 06 b4 00 00 01 02 00 00 c0 a8 00 10 e0 00  ..(.....
0020  00 16 94 04 00 00 22 00 fb 02 00 00 00 01 02 00  ....."-.....
0030  00 00 e0 00 00 fb                                .....

```

### Frame 47563: 56 bytes on wire

Tipo de encapsulación: Ethernet (1)

Hora de llegada: Mar 11, 2022 22:22:05

Número de cuadro: 47563

Longitud de cuadro: 54bytes(11192bits)

```
> Interface id: 0 (\Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0DED249})
Encapsulation type: Ethernet (1)
Arrival Time: Mar 11, 2022 21:17:14.683040000 Hora estándar romance
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1647029834.683040000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 2.641990000 seconds]
Frame Number: 89
Frame Length: 1399 bytes (11192 bits)
Capture Length: 1399 bytes (11192 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:data]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

```

**Ethernet II**

Destinación: IPv4mcast\_16

Fuente IPv4mcast\_16

Tipo: IPv4 (0x0800)

```

Ethernet II, Src: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f), Dst: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
  Destination: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    Address: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
    Address: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)

```

**Internet Protocol Versión 4**

Versión :4

Identificación: 0xcec13 (52499)

Longitud de cuadro: 40

Protocolo: IGMP(2)

Dirección de la fuente: 192.168.0.16

Dirección de destino: 224.0.0.22

```

Internet Protocol Version 4, Src: 192.168.0.16, Dst: 224.0.0.22
  0100 .... = Version: 4
  ....0110 = Header Length: 24 bytes (6)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x06b4 (1716)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 1
    Protocol: IGMP (2)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.16
    Destination Address: 224.0.0.22
  > Options: (4 bytes), Router Alert

```

### Internet Group Management Protocol

Versión: 3

Tipo: Reporte de Afiliación(0x22)

Suma de control: 0xfb02 (correcto)

Estado de Suma de Control: Buena

```
Internet Group Management Protocol
  [IGMP Version: 3]
  Type: Membership Report (0x22)
  Reserved: 00
  Checksum: 0xfb02 [correct]
  [Checksum Status: Good]
  Reserved: 0000
  Num Group Records: 1
```



- ICMP

En este caso nosotros vamos a elegir el número 2399 donde vamos a explicar posteriormente sus capas:

2378...	1119.696228	192.168.0.16	212.145.41.82	ICMP	106 Echo (ping) request	id=0x0001, seq=9/2304, ttl=3 (no response found!)
2389...	1123.625996	192.168.0.16	212.145.41.82	ICMP	106 Echo (ping) request	id=0x0001, seq=10/2560, ttl=3 (no response found!)
2399...	1127.631398	192.168.0.16	212.145.41.82	ICMP	106 Echo (ping) request	id=0x0001, seq=11/2816, ttl=3 (no response found!)
2409...	1131.624643	192.168.0.16	212.145.41.82	ICMP	106 Echo (ping) request	id=0x0001, seq=12/3072, ttl=4 (no response found!)

Nos encontramos con que tiene 4 capas:

```
> Frame 239954: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0DED249}, id 0
> Ethernet II, Src: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f), Dst: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
> Internet Protocol Version 4, Src: 192.168.0.16, Dst: 212.145.41.82
> Internet Control Message Protocol

0000  34 49 5b 8c 0d f4 2c f0 5d b6 83 5f 08 00 45 00  4I[...].E
0010  00 5c 0d 5b 00 00 03 01 00 00 c0 a8 00 10 d4 91  .\[...]
0020  29 52 08 00 f7 f3 00 01 00 0b 00 00 00 00 00 00  )R.....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

### Frame 2399: 56 bytes on wire

Tipo de encapsulación: Ethernet (1)

Hora de llegada: Mar 11, 2022 22:36:07

Número de cuadro: 239954

Longitud de cuadro: 106 bytes (848 bits)

```
▼ Frame 239954: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0DED249}, id 0
  > Interface id: 0 (\Device\NPF_{3E43B5B3-DF7C-4460-879B-2733F0DED249})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 11, 2022 22:36:07.186732000 Hora estándar romance
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1647034567.186732000 seconds
    [Time delta from previous captured frame: 0.004476000 seconds]
    [Time delta from previous displayed frame: 4.005402000 seconds]
    [Time since reference or first frame: 1127.631398000 seconds]
    Frame Number: 239954
    Frame Length: 106 bytes (848 bits)
    Capture Length: 106 bytes (848 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
```

## Ethernet II

Destinación: Sagemcom\_8c:0d:f4

Fuente Micro-St\_b6:83:5f

Tipo: IPv4 (0x0800)

```
▼ Ethernet II, Src: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f), Dst: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
  ▼ Destination: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    Address: Sagemcom_8c:0d:f4 (34:49:5b:8c:0d:f4)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
    Address: Micro-St_b6:83:5f (2c:f0:5d:b6:83:5f)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

## Internet Protocol Versión 4

Versión :4

Identificación: 0x0d5b(3419)

Longitud de cuadro: 92

Protocolo: ICMP(1)

Dirección de la fuente: 192.168.0.16

Dirección de destino: 212.145.41.82

```
▼ Internet Protocol Version 4, Src: 192.168.0.16, Dst: 212.145.41.82
  0100 .... = Version: 4
  ....0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x0d5b (3419)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 3
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.16
    Destination Address: 212.145.41.82
```

Internet Group Management Protocol

Tipo :8

Checksum: 0xf7f3

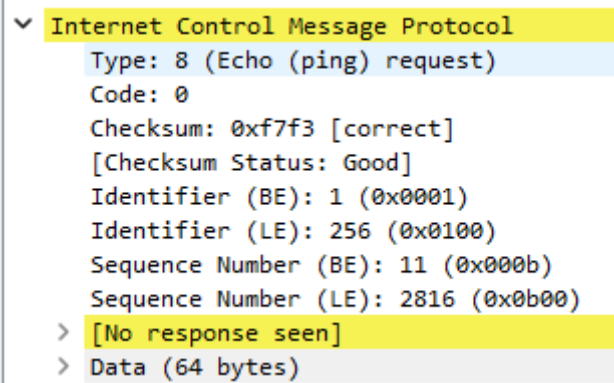
Estado de Checksum: Correcto

Identificador (BE) 1 (0x0001)

Identificador (LE) 1 (0x0100)

Secuencia de números (BE): 11 (0x000b)

Secuencia de números (LE): 2816 (0x0b00)



Mira como vienen los datos de las páginas que has solicitado:

Al realizar el análisis de nuestra red mediante Ethernet y haber guardado el archivo, nos mostrará la información recogida donde está dividido la información en diferentes secciones.

No.	Time	Source	Destination	Protocol	Length	Info
41675	73.912031	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1036123 Ack=4722 Win=0 Len=0
41676	73.912031	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1037583 Ack=4722 Win=0 Len=0
41677	73.912066	192.168.0.16	104.26.5.248	TCP	54	54 54551 → 443 [ACK] Seq=4722 Ack=1039843 Win=0 Len=0
41678	73.912091	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1039843 Ack=4722 Win=0 Len=0
41679	73.912091	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1040503 Ack=4722 Win=0 Len=0
41680	73.912091	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1041963 Ack=4722 Win=0 Len=0
41681	73.912091	104.26.5.248	192.168.0.16	TLSv1.3	945	Application Data
41682	73.912135	192.168.0.16	104.26.5.248	TCP	54	54 54551 → 443 [ACK] Seq=4722 Ack=1044314 Win=0 Len=0
41683	73.912286	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1044314 Ack=4722 Win=0 Len=0
41684	73.912286	104.26.5.248	192.168.0.16	TLSv1.3	1452	Application Data
41685	73.912286	104.26.5.248	192.168.0.16	TLSv1.3	102	Application Data
41686	73.912327	192.168.0.16	104.26.5.248	TCP	54	54 54551 → 443 [ACK] Seq=4722 Ack=1047220 Win=0 Len=0
41687	73.916966	192.168.0.16	179.60.193.60	TLSv1.3	192	Application Data
41688	73.917574	192.168.0.16	179.60.193.60	TLSv1.3	339	Application Data
41689	73.925859	179.60.193.60	192.168.0.16	TCP	60	443 → 54569 [ACK] Seq=711 Ack=1687 Win=711 Len=0
41690	73.928893	192.168.0.16	34.107.221.82	TCP	55	[TCP Keep-Alive] 61131 → 80 [ACK] Seq=324 Len=0
41691	73.937917	34.107.221.82	192.168.0.16	TCP	66	[TCP Keep-Alive ACK] 80 → 61131 [ACK] Seq=324 Len=0
41692	73.938644	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1047220 Ack=4722 Win=0 Len=0
41693	73.938644	104.26.5.248	192.168.0.16	TLSv1.3	1443	Application Data
41694	73.938700	192.168.0.16	104.26.5.248	TCP	54	54 54551 → 443 [ACK] Seq=4722 Ack=1050069 Win=0 Len=0
41695	73.942135	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1050069 Ack=4722 Win=0 Len=0
41696	73.942135	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1051529 Ack=4722 Win=0 Len=0
41697	73.942174	192.168.0.16	104.26.5.248	TCP	54	54 54551 → 443 [ACK] Seq=4722 Ack=1052989 Win=0 Len=0
41698	73.942198	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1052989 Ack=4722 Win=0 Len=0
41699	73.942263	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1054449 Ack=4722 Win=0 Len=0
41700	73.942263	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1055909 Ack=4722 Win=0 Len=0
41701	73.942263	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1057369 Ack=4722 Win=0 Len=0
41702	73.942263	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1058829 Ack=4722 Win=0 Len=0
41703	73.942263	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1060289 Ack=4722 Win=0 Len=0
41704	73.942309	192.168.0.16	104.26.5.248	TCP	54	54 54551 → 443 [ACK] Seq=4722 Ack=1061749 Win=0 Len=0
41705	73.942329	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1061749 Ack=4722 Win=0 Len=0
41706	73.942329	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1063209 Ack=4722 Win=0 Len=0
41707	73.942329	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1064669 Ack=4722 Win=0 Len=0
41708	73.942329	104.26.5.248	192.168.0.16	TLSv1.3	400	Application Data
41709	73.942329	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1066475 Ack=4722 Win=0 Len=0
41710	73.942329	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1067935 Ack=4722 Win=0 Len=0
41711	73.942329	104.26.5.248	192.168.0.16	TCP	54	1514 443 → 54551 [ACK] Seq=1069395 Ack=4722 Win=0 Len=0

Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF\_{3E43B5B3-DF7C-4460-879B-2733F0ED249}, id 0  
 Ethernet II, Src: Mikro-St\_b6:83:5f (2c:f0:5d:b6:83:5f), Dst: IPv4mcast\_fb (01:00:5e:00:00:fb)  
 Internet Protocol Version 4, Src: 192.168.0.16, Dst: 224.0.0.251  
 User Datagram Protocol, Src Port: 5353, Dst Port: 5353  
 Multicast Domain Name System (auerv)

```

0000  01 00 5e 00 00 fb 2c f0 5d b6 83 5f 00 00 45 00  ..E..
0010  00 44 05 d0 00 01 11 00 00 c0 a8 00 10 e0 00  ....D.....
0020  00 fb 14 e9 14 e9 00 30 e9 ef 00 00 00 00 01  ....0.....
0030  00 00 00 00 00 00 5f 67 6f 6f 67 6c 65 63 61  ...._googleca
0040  73 74 04 5f 74 63 70 05 6c 6f 63 61 6c 00 0c  st.tcp.local..
0050  00 01  ..
  
```

**No.** Es el número de frame que ha sido recogida.

**Time** Es el tiempo en segundos en el que ha sido capturado.

**Source** La IP de origen que ha sido recogido por el análisis.

**Destination** La IP de destino que ha sido recogido por el análisis.

**Protocol** El protocolo que es involucrado.

**Length** El tamaño del frame que ha sido recogido

**Info** Por terminar tenemos el campo de información en la que Wireshark a decodificado.

En la parte Intermedia de la ventana podemos encontrar las capas que contiene cada línea, al seleccionarlo.

Y en la parte Final de la ventana podemos encontrar contenido/información sobre el protocolo, capas etc pero encriptado.

Realiza filtros con cadenas y con regular expresión:

### Cadena:

**ip.addr == 192.168.0.1**

Nos muestra los paquetes de la cadena que en este caso es de al IP 192.168.0.1

No.	Time	Source	Destination	Protocol	Length	Info
31	0.697499	192.168.0.1	192.168.0.16	SSDP	356	HTTP/1.1 200 OK
50	1.889405	192.168.0.1	239.255.255.250	SSDP	342	NOTIFY * HTTP/1.1
51	1.889563	192.168.0.1	239.255.255.250	SSDP	398	NOTIFY * HTTP/1.1
52	1.889625	192.168.0.1	239.255.255.250	SSDP	326	NOTIFY * HTTP/1.1
53	1.889688	192.168.0.1	239.255.255.250	SSDP	318	NOTIFY * HTTP/1.1
54	1.889767	192.168.0.1	239.255.255.250	SSDP	362	NOTIFY * HTTP/1.1
55	1.889856	192.168.0.1	239.255.255.250	SSDP	338	NOTIFY * HTTP/1.1
56	1.889947	192.168.0.1	239.255.255.250	SSDP	392	NOTIFY * HTTP/1.1
57	1.890035	192.168.0.1	239.255.255.250	SSDP	390	NOTIFY * HTTP/1.1
58	1.890126	192.168.0.1	239.255.255.250	SSDP	394	NOTIFY * HTTP/1.1
59	1.890224	192.168.0.1	239.255.255.250	SSDP	386	NOTIFY * HTTP/1.1
2138	3.179426	192.168.0.1	192.168.0.16	SSDP	356	HTTP/1.1 200 OK
2150	6.169737	192.168.0.1	192.168.0.16	SSDP	356	HTTP/1.1 200 OK
6089	19.481827	192.168.0.1	239.255.255.250	SSDP	381	NOTIFY * HTTP/1.1
6098	19.483583	192.168.0.1	239.255.255.250	SSDP	326	NOTIFY * HTTP/1.1
6112	19.486425	192.168.0.1	239.255.255.250	SSDP	317	NOTIFY * HTTP/1.1
6156	19.490630	192.168.0.1	239.255.255.250	SSDP	391	NOTIFY * HTTP/1.1
8303	22.807566	192.168.0.1	192.168.0.16	SSDP	356	HTTP/1.1 200 OK
8327	22.993569	192.168.0.1	192.168.0.16	SSDP	356	HTTP/1.1 200 OK
11622	26.802497	192.168.0.1	192.168.0.16	SSDP	356	HTTP/1.1 200 OK
11624	26.804595	192.168.0.1	192.168.0.16	SSDP	356	HTTP/1.1 200 OK
12038	28.821753	192.168.0.1	192.168.0.16	SSDP	356	HTTP/1.1 200 OK
14307	31.833494	192.168.0.1	192.168.0.16	SSDP	356	HTTP/1.1 200 OK
14308	31.893131	192.168.0.1	239.255.255.250	SSDP	342	NOTIFY * HTTP/1.1
14309	31.893332	192.168.0.1	239.255.255.250	SSDP	398	NOTIFY * HTTP/1.1
14310	31.893332	192.168.0.1	239.255.255.250	SSDP	326	NOTIFY * HTTP/1.1
14311	31.893441	192.168.0.1	239.255.255.250	SSDP	318	NOTIFY * HTTP/1.1
14312	31.893501	192.168.0.1	239.255.255.250	SSDP	362	NOTIFY * HTTP/1.1
14313	31.893571	192.168.0.1	239.255.255.250	SSDP	338	NOTIFY * HTTP/1.1
14314	31.893666	192.168.0.1	239.255.255.250	SSDP	392	NOTIFY * HTTP/1.1
14315	31.893754	192.168.0.1	239.255.255.250	SSDP	390	NOTIFY * HTTP/1.1
14316	31.893844	192.168.0.1	239.255.255.250	SSDP	394	NOTIFY * HTTP/1.1
14317	31.893932	192.168.0.1	239.255.255.250	SSDP	386	NOTIFY * HTTP/1.1
15520	34.837556	192.168.0.1	192.168.0.16	SSDP	356	HTTP/1.1 200 OK
15683	37.842605	192.168.0.1	192.168.0.16	SSDP	356	HTTP/1.1 200 OK
19436	47.849648	192.168.0.1	239.255.255.250	SSDP	381	NOTIFY * HTTP/1.1

**tcp contains "google.com"**

Nos ayuda a realizar una búsqueda de segmentos TCP contenido a la cadena Google.com

No.	Time	Source	Destination	Protocol	Length	Info
14347	32.950744	192.168.0.16	142.250.184.174	TLSv1.3	571	Client Hello
94813	188.502643	192.168.0.16	142.250.201.69	TLSv1.3	571	Client Hello
96398	191.924456	192.168.0.16	74.125.133.189	TLSv1.3	571	Client Hello

udp.port == 53

Nos permite visualizar el tráfico UDPP del puerto 53

udp.port == 53							
Listado de paquetes Reducido & ampliado Mayúsculas y minúsculas Cadena							
No.	Time	Source	Destination	Protocol	Length	Info	
95160	196.371982	192.168.0.16	212.166.218.80	DNS	79	Standard query 0x770a A clients2.google.com	
95161	196.383340	212.166.218.80	192.168.0.16	DNS	119	Standard query response 0x770a A clients2.google.com CNAME clients1.google.com A 1	
95162	196.383847	192.168.0.16	212.166.218.80	DNS	80	Standard query 0x0880b A clients1.google.com	
95165	196.394556	212.166.218.80	192.168.0.16	DNS	96	Standard query response 0x0880b A clients1.google.com A 172.217.17.14	
95166	196.394845	192.168.0.16	212.166.218.80	DNS	80	Standard query 0x3cf5 AAAA clients1.google.com	
95167	196.407780	212.166.218.80	192.168.0.16	DNS	108	Standard query response 0x3cf5 AAAA clients1.google.com AAAA 2a00:1450:4003:802::2	
95707	196.827609	192.168.0.16	212.166.218.80	DNS	79	Standard query 0x28d3 A hangouts.google.com	
95708	196.836519	212.166.218.80	192.168.0.16	DNS	116	Standard query response 0x28d3 A hangouts.google.com CNAME www3.l.google.com A 142.	
95949	191.253583	192.168.0.16	212.166.218.80	DNS	80	Standard query 0x7be9 A people-pa.clients6.google.com	
95951	191.258060	192.168.0.16	212.166.218.80	DNS	87	Standard query 0x189e A chat-pa.clients6.google.com	
95952	191.264346	212.166.218.80	192.168.0.16	DNS	105	Standard query response 0x7be9 A people-pa.clients6.google.com A 172.217.168.170	
95953	191.264851	192.168.0.16	212.166.218.80	DNS	89	Standard query 0x67c9 A people-pa.clients6.google.com	
95956	191.268512	212.166.218.80	192.168.0.16	DNS	103	Standard query response 0x189e A chat-pa.clients6.google.com A 142.258.178.170	
95957	191.269033	192.168.0.16	212.166.218.80	DNS	87	Standard query 0x04e5 A chat-pa.clients6.google.com	
95989	191.275892	212.166.218.80	192.168.0.16	DNS	105	Standard query response 0x67c9 A people-pa.clients6.google.com A 172.217.168.170	
95990	191.276164	192.168.0.16	212.166.218.80	DNS	89	Standard query 0x3d99 AAAA people-pa.clients6.google.com	
95996	191.288922	212.166.218.80	192.168.0.16	DNS	103	Standard query response 0x04e5 A chat-pa.clients6.google.com A 142.258.178.170	
95997	191.281179	192.168.0.16	212.166.218.80	DNS	87	Standard query 0xc8fc AAAA chat-pa.clients6.google.com	
96004	191.288145	212.166.218.80	192.168.0.16	DNS	117	Standard query response 0x3d99 AAAA people-pa.clients6.google.com AAAA 2a00:1450:4003:802::2	
96005	191.291427	192.168.0.16	212.166.218.80	DNS	79	Standard query 0x2f14 A clients6.google.com	
96006	191.291990	212.166.218.80	192.168.0.16	DNS	115	Standard query response 0xc8fc AAAA chat-pa.clients6.google.com AAAA 2a00:1450:4003:802::2	
96033	191.302208	212.166.218.80	192.168.0.16	DNS	119	Standard query response 0x2f14 A clients6.google.com CNAME clients1.google.com A 1	
96312	191.822300	192.168.0.16	212.166.218.80	DNS	96	Standard query 0x625f AAAA googlehosted1.googleusercontent.com	
96315	191.821830	212.166.218.80	192.168.0.16	DNS	124	Standard query response 0x625f AAAA googlehosted1.googleusercontent.com AAAA 2a00:	
96316	191.833128	192.168.0.16	212.166.218.80	DNS	75	Standard query 0x4387 A chat.google.com	
96320	191.843833	212.166.218.80	192.168.0.16	DNS	91	Standard query response 0x4387 A chat.google.com A 216.58.209.78	
96321	191.844363	192.168.0.16	212.166.218.80	DNS	75	Standard query 0x21be A chat.google.com	
96330	191.854950	212.166.218.80	192.168.0.16	DNS	91	Standard query response 0x21be A chat.google.com A 216.58.209.78	
96331	191.855222	192.168.0.16	212.166.218.80	DNS	75	Standard query 0xa609 AAAA chat.google.com	
96336	191.866209	212.166.218.80	192.168.0.16	DNS	103	Standard query response 0xa609 AAAA chat.google.com AAAA 2a00:1450:4003:80c::200e	
96341	191.871226	192.168.0.16	212.166.218.80	DNS	87	Standard query 0xcd2c A 8.client-channel.google.com	
96363	191.881973	212.166.218.80	192.168.0.16	DNS	103	Standard query response 0xcd2c A 8.client-channel.google.com A 74.125.133.189	
96364	191.882566	192.168.0.16	212.166.218.80	DNS	87	Standard query 0xa6f6 A 8.client-channel.google.com	
96381	191.893678	212.166.218.80	192.168.0.16	DNS	103	Standard query response 0xa6f6 A 8.client-channel.google.com A 74.125.133.189	
96382	191.893909	192.168.0.16	212.166.218.80	DNS	87	Standard query 0x25f4 AAAA 8.client-channel.google.com	

ip.ttl == 1

Nos ayuda a visualizar todos los paquetes IP en el que haiga un campo TTL sea igual a 1

ip.ttl == 1							
Listado de paquetes Reducido & ampliado Mayúsculas y minúsculas Cadena							
No.	Time	Source	Destination	Protocol	Length	Info	
12238	30.330645	192.168.0.16	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QI" question	
12240	30.331476	192.168.0.16	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QI" question	
12242	30.345777	192.168.0.16	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QI" question	
12244	30.346385	192.168.0.16	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QI" question	
15445	33.846655	192.168.0.16	224.0.0.251	MDNS	70	Standard query 0x0000 A _wpad.local, "QI" question	
15447	33.847249	192.168.0.16	224.0.0.251	MDNS	70	Standard query 0x0000 A _wpad.local, "QI" question	
15450	33.847661	192.168.0.16	224.0.0.252	LLMNR	64	Standard query 0x9a25 A _wpad	
15451	33.847888	192.168.0.16	224.0.0.251	MDNS	70	Standard query 0x0000 A _wpad.local, "QI" question	
15453	33.847991	192.168.0.16	224.0.0.252	LLMNR	64	Standard query 0xa7e2 A _wpad	
15455	33.848262	192.168.0.16	224.0.0.251	MDNS	70	Standard query 0x0000 A _wpad.local, "QI" question	
15505	34.271476	192.168.0.16	224.0.0.252	LLMNR	64	Standard query 0xa7e2 A _wpad	
15506	34.271485	192.168.0.16	224.0.0.252	LLMNR	64	Standard query 0x9a25 A _wpad	
15521	34.848253	192.168.0.16	224.0.0.251	MDNS	70	Standard query 0x0000 A _wpad.local, "QI" question	
15523	34.849224	192.168.0.16	224.0.0.251	MDNS	70	Standard query 0x0000 A _wpad.local, "QI" question	
15525	34.849985	192.168.0.16	224.0.0.251	MDNS	70	Standard query 0x0000 A _wpad.local, "QI" question	
15527	34.850536	192.168.0.16	224.0.0.251	MDNS	70	Standard query 0x0000 A _wpad.local, "QI" question	
44047	76.583004	192.168.0.11	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.251 for any sources	
44563	78.584746	192.168.0.11	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.251 for any sources	
58180	112.433272	192.168.0.11	224.0.0.1	IGMPv3	60	Membership Query, general	
58181	112.433803	192.168.0.11	224.0.0.1	IGMPv3	60	Membership Query, general	
58182	112.441383	192.168.0.16	224.0.0.22	IGMPv3	62	Membership Report / Join group 224.0.0.252 for any sources / Join group 239.255.255.250 for any sources	
59299	113.776406	192.168.0.19	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sources	
59420	113.941906	192.168.0.16	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources	
64008	119.713140	192.168.0.10	224.0.0.22	IGMPv3	64	Membership Report / Join group 239.255.255.250 for any sources	
84858	144.313312	192.168.0.16	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1	
84970	144.321364	192.168.0.16	239.255.255.250	SSDP	211	M-SEARCH * HTTP/1.1	
87229	145.324407	192.168.0.16	239.255.255.250	SSDP	211	M-SEARCH * HTTP/1.1	
87230	145.324407	192.168.0.16	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1	
87400	146.334872	192.168.0.16	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1	
87401	146.334872	192.168.0.16	239.255.255.250	SSDP	211	M-SEARCH * HTTP/1.1	
87662	147.349504	192.168.0.16	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1	
87663	147.349504	192.168.0.16	239.255.255.250	SSDP	211	M-SEARCH * HTTP/1.1	
90326	163.923841	192.168.0.16	224.0.0.252	LLMNR	64	Standard query 0x8b15 A hola	
90328	163.924092	192.168.0.16	224.0.0.252	LLMNR	64	Standard query 0x70f8 AAAA hola	
90436	164.349696	192.168.0.16	224.0.0.252	LLMNR	64	Standard query 0x70f8 AAAA hola	

**ip.dst == 192.168.0.16**

Podemos visualizar el host destino 192.168.0.16

ip.dst == 192.168.0.16						
Listado de paquetes Reducido & ampliado Mayúsculas y minúsculas Cadena						
No.	Time	Source	Destination	Protocol	Length	Info
21	0.023702	192.168.0.19	192.168.0.16	SSDP	379	HTTP/1.1 200 OK
22	0.023702	192.168.0.19	192.168.0.16	SSDP	379	HTTP/1.1 200 OK
25	0.398333	192.168.0.19	192.168.0.16	SSDP	379	HTTP/1.1 200 OK
31	0.697499	192.168.0.1	192.168.0.16	SSDP	356	HTTP/1.1 200 OK
63	2.443117	192.168.0.19	192.168.0.16	SSDP	379	HTTP/1.1 200 OK
69	2.637986	77.227.215.15	192.168.0.16	UDP	75	443 → 52321 Len=33
70	2.640222	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
72	2.640450	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
73	2.640764	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
75	2.641015	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
76	2.641218	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
78	2.641464	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
79	2.641671	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
80	2.641671	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
82	2.641925	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
83	2.641925	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
84	2.641925	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
85	2.641925	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
86	2.641925	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
87	2.641990	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
88	2.641990	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
89	2.641990	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
90	2.641990	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
91	2.641990	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
92	2.641990	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
93	2.642056	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
94	2.642056	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
95	2.642118	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
97	2.642285	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
98	2.642285	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
99	2.642285	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
100	2.642285	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
101	2.642285	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
102	2.642285	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357
103	2.642285	77.227.215.15	192.168.0.16	UDP	1399	443 → 52321 Len=1357

## Regular Expresión:

**(\w{4})**

Busca una palabra con 4 letras

Current filter: ip.addr == 8.8.8.8

Expresión regular: **(\w{4})** Buscar Cancelar

No.	Time	Source	Destination	Protocol	Length	Info
139	15.939800	100.66.4.43	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001
140	15.941383	8.8.8.8	100.66.4.43	ICMP	74	Echo (ping) reply id=0x0001
146	16.944819	100.66.4.43	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001
147	16.946281	8.8.8.8	100.66.4.43	ICMP	74	Echo (ping) reply id=0x0001
153	17.949674	100.66.4.43	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001
154	17.951247	8.8.8.8	100.66.4.43	ICMP	74	Echo (ping) reply id=0x0001
163	18.956763	100.66.4.43	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001
164	18.958343	8.8.8.8	100.66.4.43	ICMP	74	Echo (ping) reply id=0x0001

< >

> Frame 139: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{170D0408-E113-4C1D-860F-B6B813C35808}

> Ethernet II, Src: Dell\_f2:7c:5b (30:00:42:f2:7c:5b), Dst: Fortinet\_09:00:12 (00:09:0f:09:00:12)

> Internet Protocol Version 4, Src: 100.66.4.43, Dst: 8.8.8.8

> Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x4ce7 [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 116 (0x0074)

Sequence Number (LE): 29696 (0x7400)

< >

```

0000  00 09 0f 09 00 12 30 d0 42 f2 7c 5b 08 00 45 00  ....0 B.[...E
0010  00 3c 6c c5 00 00 01 00 00 64 42 84 2b 08 08 00  <1.....db+...
0020  08 08 00 00 4c e7 00 01 00 74 01 02 03 04 05 06  ....L....4abcdaf
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f  wabcedefgh ijkl
  
```

$\backslash d+$

## Búsqueda de número

Current filter: ip.addr == 8.8.8.8									
Listado de paquetes		Reducido & ampliado	Mayúsculas y minúsculas		Expresión regular	=  id+	Buscar	Cancelar	
No.	Time	Source	Destination	Protocol	Length	Info			
+	139	15.939800	100.66.4.43	8.8.8.8	ICMP	74 Echo (ping) request	id=0x000		
+	140	15.941383	8.8.8.8	100.66.4.43	ICMP	74 Echo (ping) reply	id=0x000		
	146	16.944819	100.66.4.43	8.8.8.8	ICMP	74 Echo (ping) request	id=0x000		
	147	16.946281	8.8.8.8	100.66.4.43	ICMP	74 Echo (ping) reply	id=0x000		
	153	17.949674	100.66.4.43	8.8.8.8	ICMP	74 Echo (ping) request	id=0x000		
	154	17.951247	8.8.8.8	100.66.4.43	ICMP	74 Echo (ping) reply	id=0x000		
	163	18.956763	100.66.4.43	8.8.8.8	ICMP	74 Echo (ping) request	id=0x000		
	164	18.958343	8.8.8.8	100.66.4.43	ICMP	74 Echo (ping) reply	id=0x000		

```
> Frame 139: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF{170D0408-E113-4C1D-860F-B6B813C35B00}
> Ethernet II, Src: Dell_f2:7c:5b (30:d0:42:f2:7c:5b), Dst: Fortinet_09:00:12 (00:09:0f:09:00:12)
> Internet Protocol Version 4, Src: 100.66.4.43, Dst: 8.8.8.8
v Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4ce7 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence (BE): 1 (0x0001)
  Sequence (LE): 256 (0x0100)

0000  00 09 0f 09 00 12 30 d0 42 f2 7c 5b 08 00 45 00  ....0.8.[.E.
0010  3c 6c c5 00 00 80 01 00 00 64 42 04 2b 08 08  <1....db+...
0020  08 08 08 00 64 c7 01 00 74 61 62 63 64 65 66  ....L...tbddef
0030  77 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76  wbcdefghijkl
```