

# Wireshark



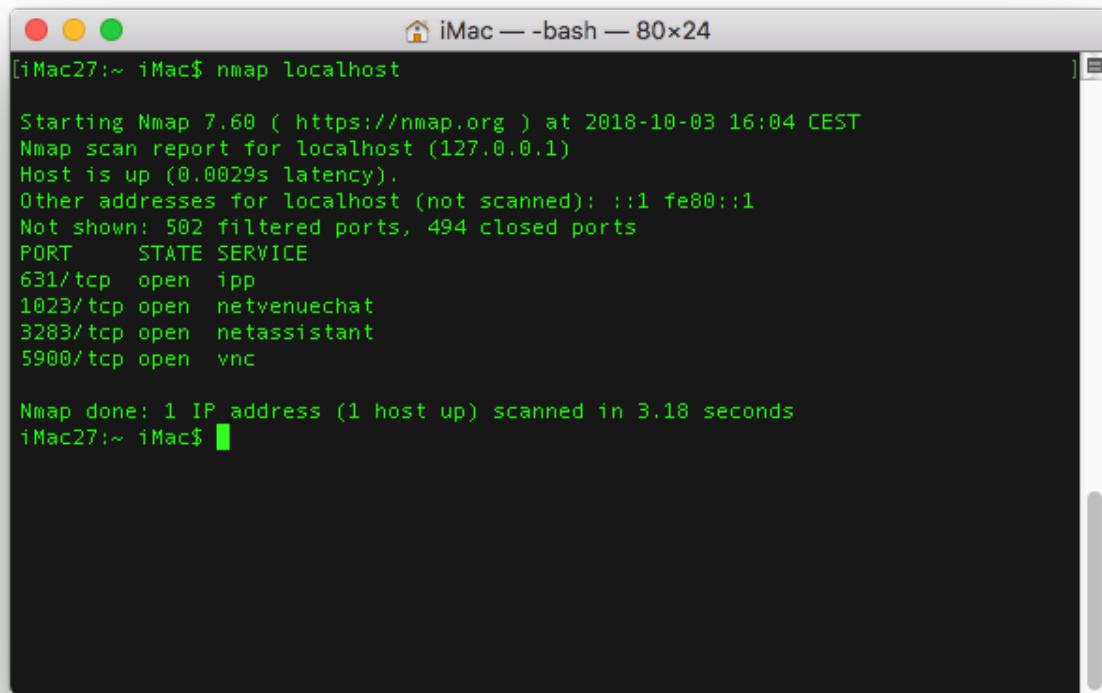
Les 2 26/09/2019

M. DIMA



# Poorten

- nmap localhost



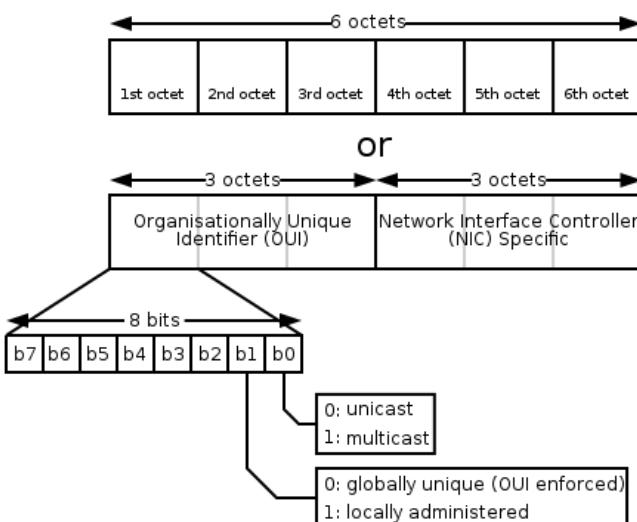
```
iMac — -bash — 80x24
[iMac27:~ iMac$ nmap localhost

Starting Nmap 7.60 ( https://nmap.org ) at 2018-10-03 16:04 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0029s latency).
Other addresses for localhost (not scanned): ::1 fe80::1
Not shown: 502 filtered ports, 494 closed ports
PORT      STATE SERVICE
631/tcp    open  ipp
1023/tcp   open  netvenuechat
3283/tcp   open  netassistant
5900/tcp   open  vnc

Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
iMac27:~ iMac$
```

# MAC Adres

- Media Access Control address  
**00:0C:6E:D2:11:E6**
- Broadcast  
**FF:FF:FF:FF:FF:FF**



```
iMac — bash — 80x41
[iMac27:~ iMac$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xffffffff
    inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
EHCI253: flags=0<> mtu 0
EHCI250: flags=0<> mtu 0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=b<RXCSUM,TXCSUM,VLAN_HWTAGGING>
    ether c4:2c:03:04:bc:28
    inet6 fe80::183b:edda:d77f:278b%en0 prefixlen 64 secured scopeid 0x6
    inet 192.168.31.124 netmask 0xffffffff broadcast 192.168.31.255
    nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (1000baseT <full-duplex,flow-control>)
        status: active
en1: flags=8823<UP,BROADCAST,SMART,SIMPLEX,MULTICAST> mtu 1500
    ether d8:30:62:56:10:c6
    nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (<unknown type>)
        status: inactive
p2p0: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 2304
    ether 0a:30:62:56:10:c6
    media: autoselect
    status: inactive
fw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 4078
    lladdr e8:06:88:fe:e7:f5:80
    nd6 options=201<PERFORMNUD,DAD>
        media: autoselect <full-duplex>
        status: inactive
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
    inet6 fe80::6c67:7baa:dab0:ad19%utun0 prefixlen 64 scopeid 0xa
    inet6 fd21:b223:9479:23b2:6c67:7baa:dab0:ad19 prefixlen 64
    nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
    inet6 fe80::abb2:d8f7:ded4:7b54%utun1 prefixlen 64 scopeid 0xb
    nd6 options=201<PERFORMNUD,DAD>
iMac27:~ iMac$
```

# Protocol

- Set voorgedefinieerde regels over hoe iets moet gebeuren  
bv TCP-IP Transmission Control Protocol / Internet Protocol

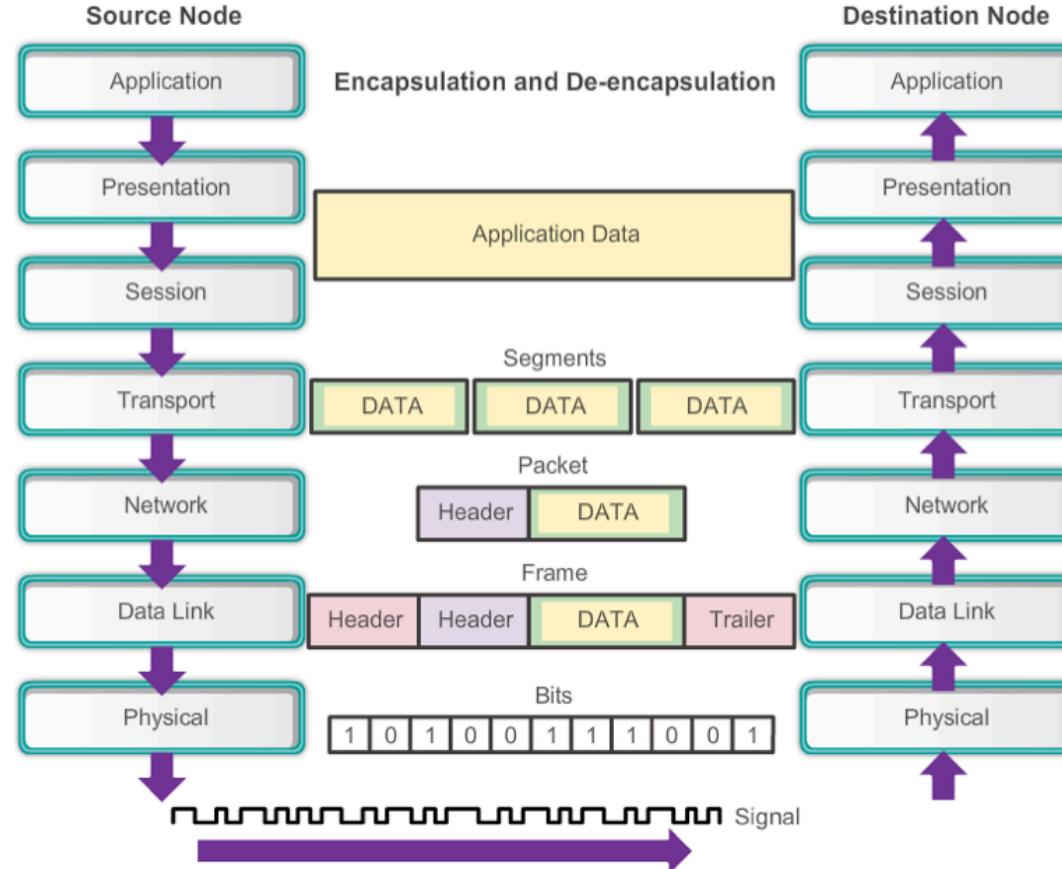
	<b>OSI Layer</b>	<b>TCP/IP</b>	<b>Datagrams are called</b>
<b>Software</b>	<b>Layer 7</b> Application	HTTP, SMTP, IMAP, SNMP, POP3, FTP	<b>Upper Layer Data</b>
	<b>Layer 6</b> Presentation	ASCII Characters, MPEG, SSL, TSL, Compression (Encryption & Decryption)	
	<b>Layer 5</b> Session	NetBIOS, SAP, Handshaking connection	
	<b>Layer 4</b> Transport	TCP, UDP	<b>Segment</b>
	<b>Layer 3</b> Network	IPv4, IPv6, ICMP, <u>IPSec</u> , MPLS, ARP	<b>Packet</b>
<b>Hardware</b>	<b>Layer 2</b> Data Link	Ethernet, 802.1x, PPP, ATM, <u>Fiber</u> Channel, MPLS, FDDI, MAC Addresses	<b>Frame</b>
	<b>Layer 1</b> Physical	Cables, Connectors, Hubs (DLS, RS232, 10BaseT, 100BaseTX, ISDN, T1)	<b>Bits</b>

apps zelf  
converters data  
app -> network  
manages connections  
  
transfer data h -> h +  
data integriteit  
switching & routing  
  
MAC & LLC

## Doele van de fysieke laag

# De fysieke laag

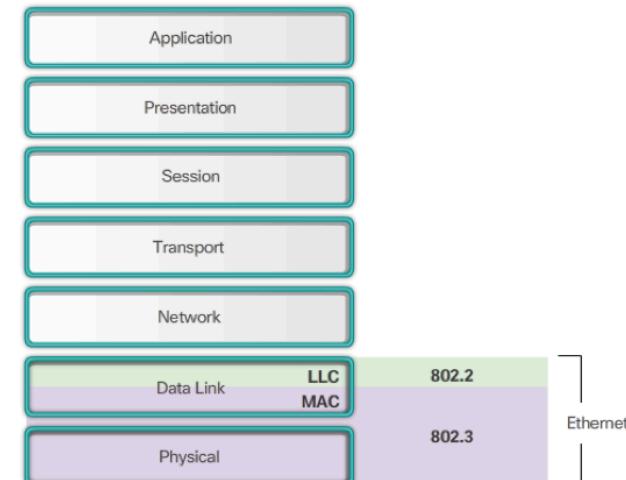
De fysieke laag biedt de middelen om de bits van een frame gevormd door de datalinklaag over het netwerk medium te sturen.



# LLC en MAC Sublagen

### Ethernet

- Eén van de meest gebruikte LAN-technologieën
- Werkt in de datalinklaag en de fysieke laag
- Familie van netwerktechnologieën die zijn gedefinieerd in de IEEE 802.2 en 802.3 standaarden.
- Ondersteunt data bandbreedtes van 10, 100, 1 000, 10 000, 40 000 en 100 000 Mbps (100 Gbps)



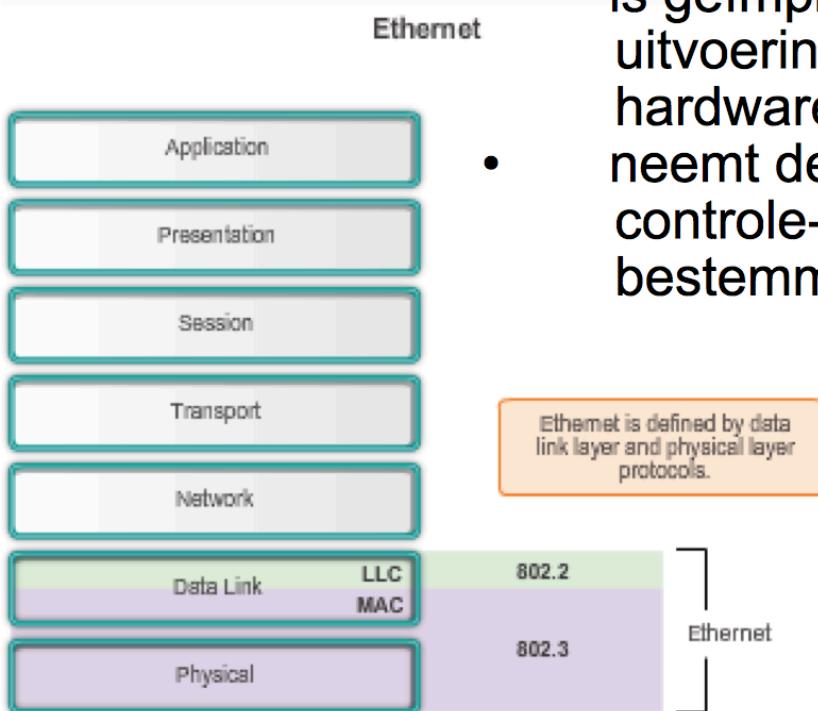
### Ethernet standaarden

- Definiëren laag 2 protocollen en laag 1 technologieën.
- Twee afzonderlijke sublagen van de datalinklaag om het te laten werken - **Logical Link Control (LLC)** en de **MAC** sublagen.

# LLC en MAC Sublagen (vervolg)

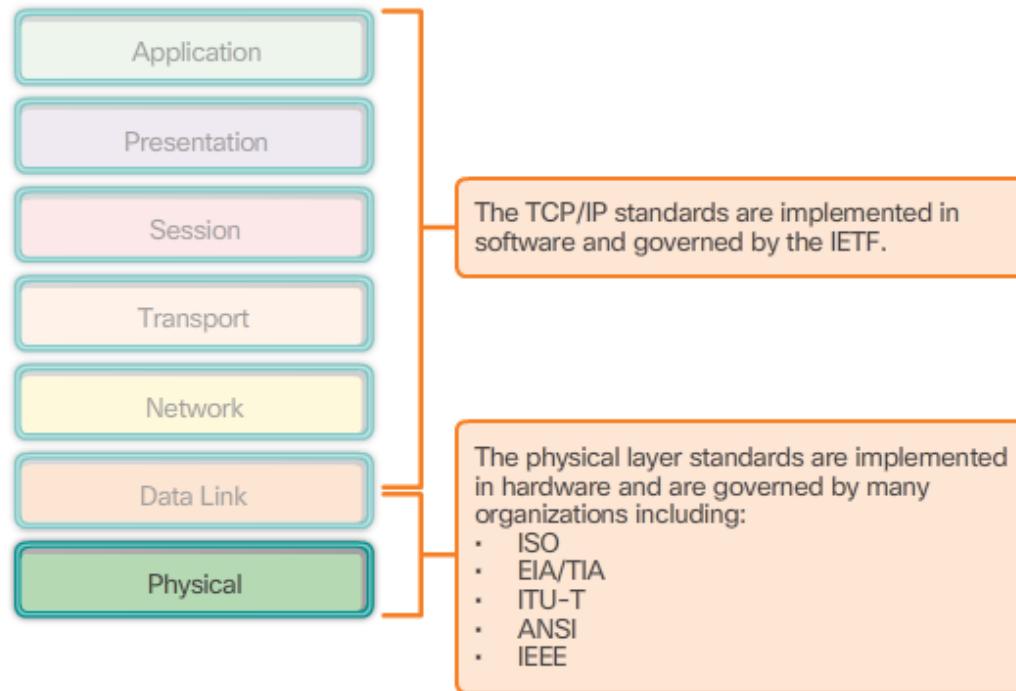
## De Ethernet **LLC** sublaag

- verzorgt de communicatie tussen de netwerksoftware en de apparaat hardware
- is geïmplementeerd in de software, en de uitvoering ervan is onafhankelijk van de hardware
- neemt de netwerkprotocolgegevens en voegt controle-informatie toe om het pakket naar de bestemming te helpen



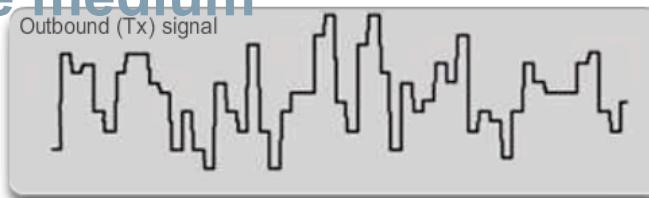
De **MAC** sublaag vormt de onderste sublaag van de datalink-laag. MAC wordt uitgevoerd door de hardware, meestal in de computer NIC. De details worden gespecificeerd in de IEEE 802.3-normen.

# Standaarden van de fysieke laag



Doel van de fysieke laag

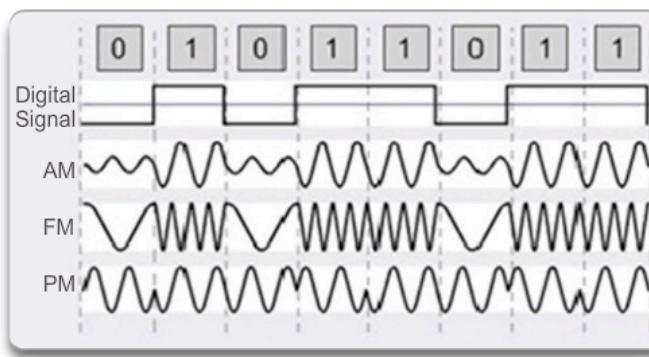
## Het fysieke medium



Electrical Signals -  
Copper cable



Light Pulse -  
Fiber-optic cable



Microwave Signals -  
Wireless

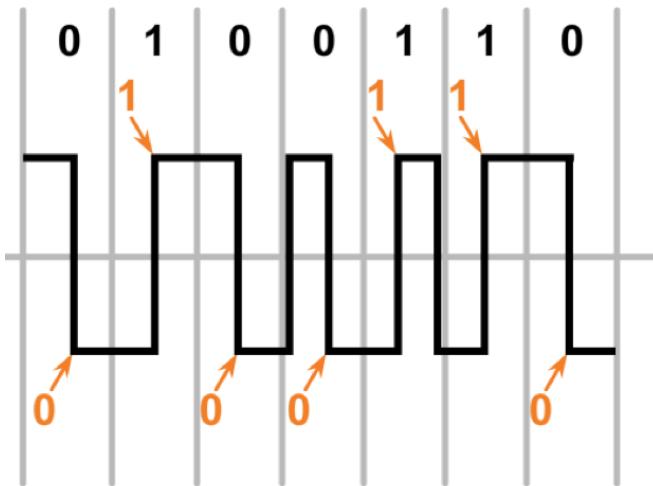
## Fundamentele principes van laag 1

# Fundamentele principes van de fysieke laag

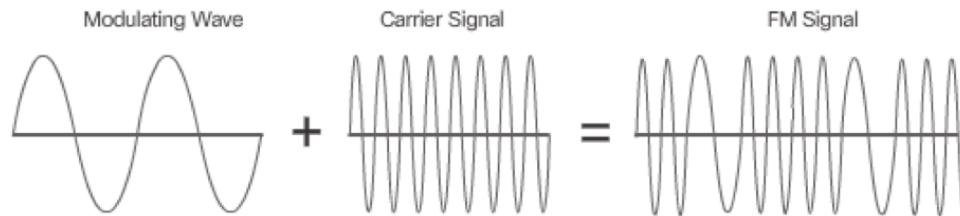
Media	Physical Components	Frame Encoding Technique	Signalling Method
Copper Cable	UTP Coaxial Connectors NICs Ports Interfaces	Manchester Encoding Non-Return to Zero (NRZ) techniques 4B/5B codes are used with Multi-Level Transition Level 3 (MLT-3) signaling 8B/10B PAM5	Changes in the electromagnetic field Intensity of the electromagnetic field Phase of the electromagnetic wave
Fiber Optic Cable	Single-mode Fiber Multimode Fiber Connectors NICs Interfaces Lasers and LEDs Photoreceptors	Pulses of light Wavelength multiplexing using different colors	A pulse equals 1. No pulse is 0.
Wireless Media	Access Points NICs Radio Antennae	DSSS (direct-sequence spread-spectrum) OFDM (orthogonal frequency division multiplexing)	Radio waves

# Coderingstechniek – transmissie techniek

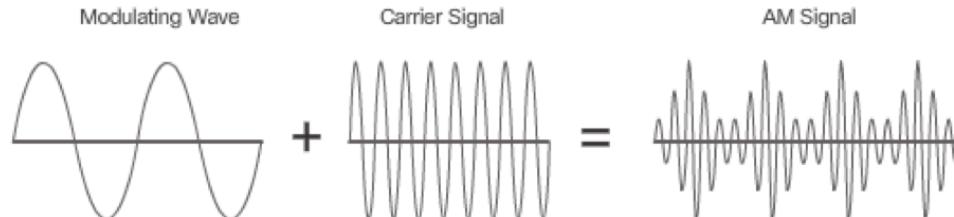
Manchester Encoding

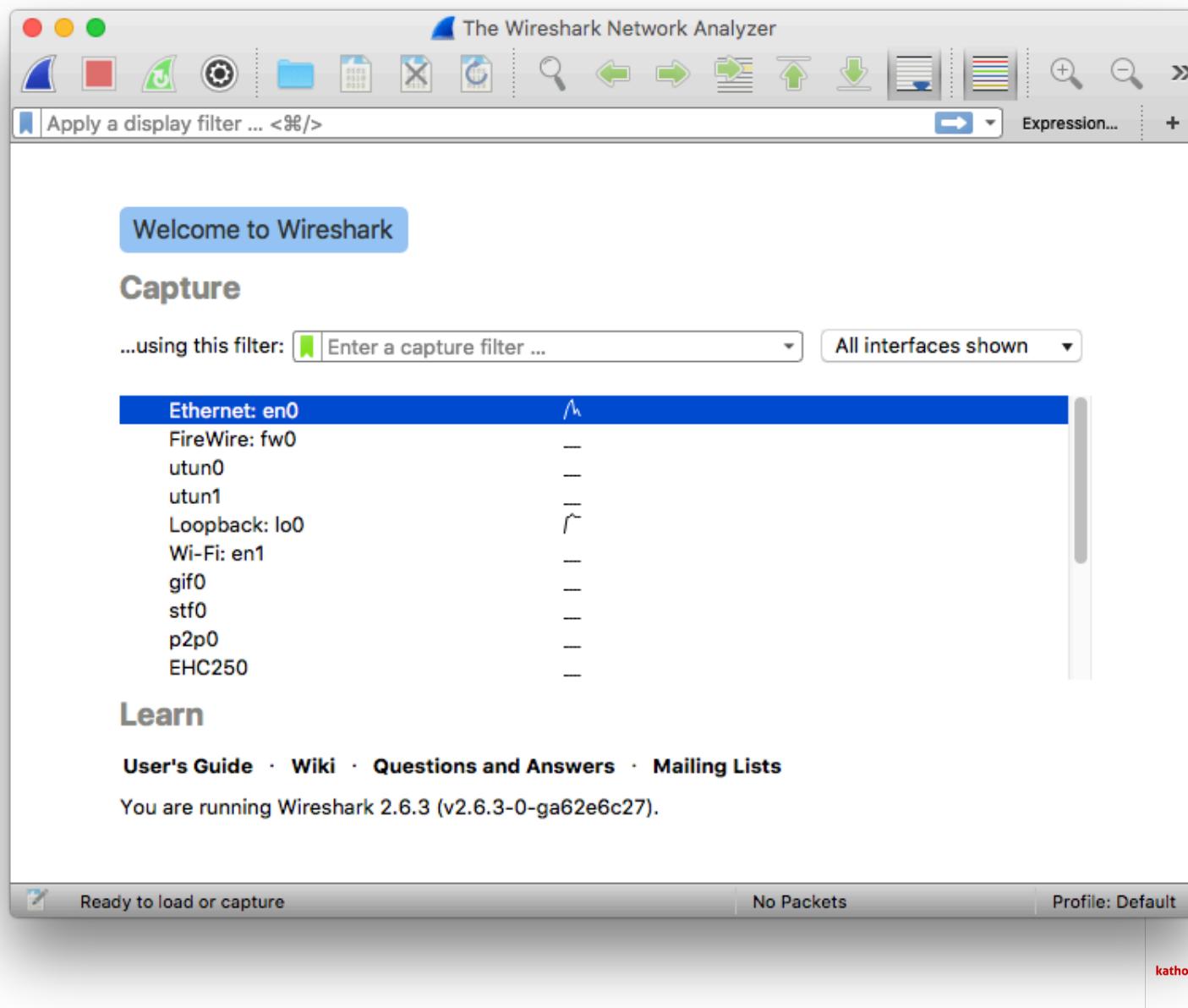


Frequency Modulation (FM)



Amplitude Modulation (AM)





Wireshark

Appearance

Columns

Font and Colors

Layout

Capture

Expert

Filter Buttons

Name Resolution

Protocols

Statistics

Advanced

Displayed	Title	Type
<input type="checkbox"/>	No.	Number
<input checked="" type="checkbox"/>	Time	Time
<input checked="" type="checkbox"/>	Source	Source
<input checked="" type="checkbox"/>	Destination	Destination
<input checked="" type="checkbox"/>	Protocol	Protocol
<input checked="" type="checkbox"/>	Length	Packet length
<input type="checkbox"/>	Info	Information
<input checked="" type="checkbox"/>	New Column	Number

+ -

Help

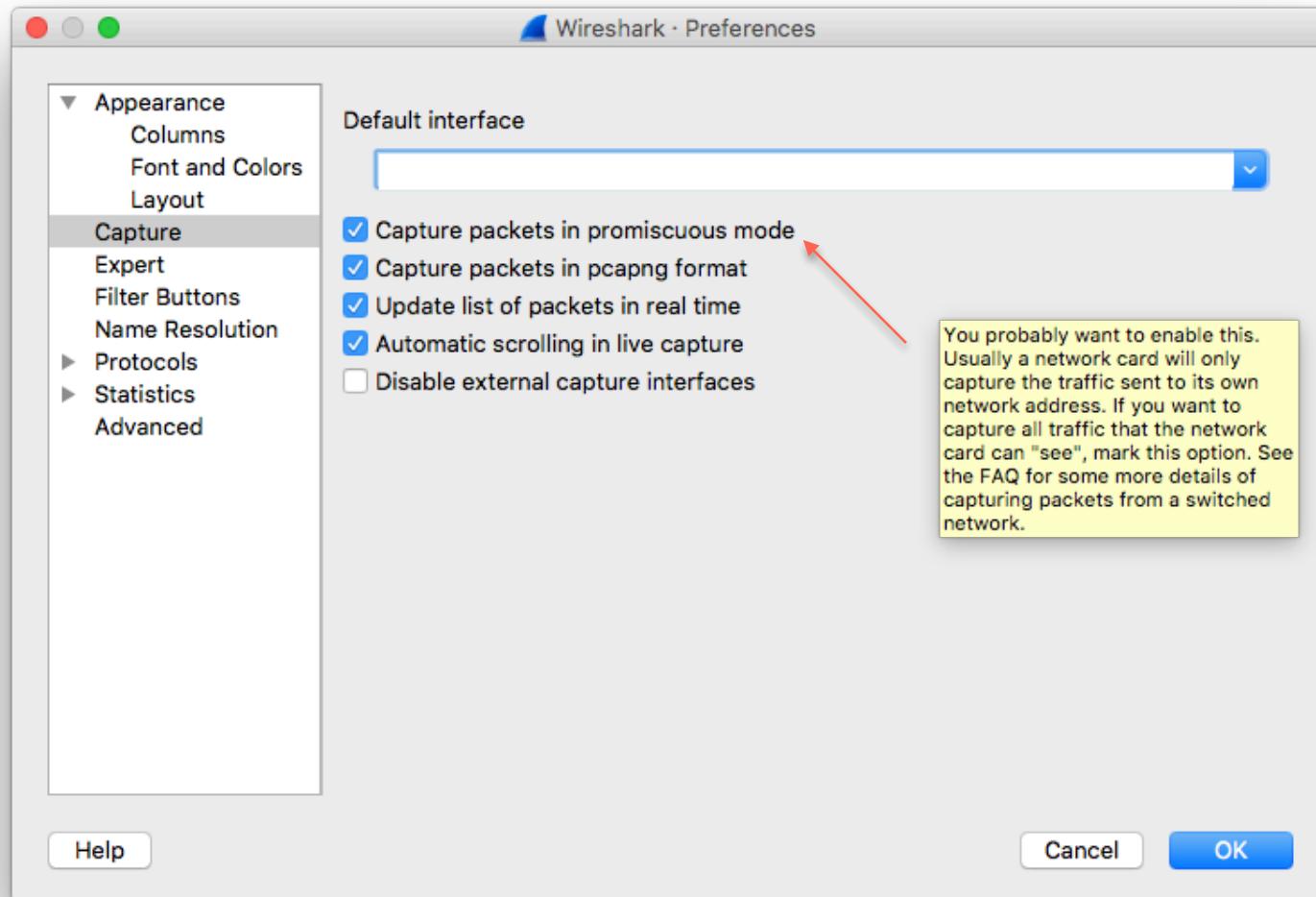
802.1Q VLAN id  
Absolute date, as YYYY-MM-DD, and time  
Absolute date, as YYYY/DOY, and time  
Absolute time  
Cisco VSAN  
Cumulative Bytes  
Custom  
DCE/RPC call (cn\_call\_id / dg\_seqnum)  
Delta time  
Delta time displayed  
Dest addr (resolved)  
Dest addr (unresolved)  
Dest port (resolved)  
Dest port (unresolved)  
Destination address  
Destination port  
Expert Info Severity  
FW-1 monitor if/direction  
Frequency/Channel  
Hardware dest addr  
Hardware src addr  
Hw dest addr (resolved)  
Hw dest addr (unresolved)  
Hw src addr (resolved)  
Hw src addr (unresolved)  
IEEE 802.11 RSSI  
IEEE 802.11 TX rate  
IP DSCP Value  
Information  
Net dest addr (resolved)  
Net dest addr (unresolved)  
Net src addr (resolved)  
Net src addr (unresolved)  
Network dest addr  
Network src addr  
 Number  
Packet length (bytes)  
Protocol  
Relative time  
Source address  
Source port  
Src addr (resolved)  
Src addr (unresolved)  
Src port (resolved)  
Src port (unresolved)  
TEI  
UTC date, as YYYY-MM-DD, and time  
UTC date, as YYYY/DOY, and time  
UTC time  
Time (format as specified)

Field

OK

katholieke hogeschool  
associatie KU Leuven

vives



Ethernet: en0

Apply a display filter ... <%> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1022	25.708348	192.168.31.124	104.40.147.142	TCP	66	61220 → 443 [ACK] Seq=39 Ack=8591 Wi...
1023	25.730722	104.40.147.142	192.168.31.124	TLSv1...	247	Application Data
1024	25.730813	192.168.31.124	104.40.147.142	TCP	66	61220 → 443 [ACK] Seq=39 Ack=8772 Wi...
1025	25.733327	192.168.31.124	8.8.8.8	DNS	91	Standard query 0xd489 A lp-push-serv...
<b>1026</b>	<b>25.755508</b>	<b>8.8.8.8</b>	<b>192.168.31.124</b>	<b>DNS</b>	<b>107</b>	<b>Standard query response 0xd489 A lp...</b>
1027	25.756064	192.168.31.124	192.241.181.178	TCP	78	63469 → 443 [SYN] Seq=0 Win=65535 Le...
1028	25.849826	192.241.181.178	192.168.31.124	TCP	74	443 → 63469 [SYN, ACK] Seq=0 Ack=1 W...
1029	25.849933	192.168.31.124	192.241.181.178	TCP	66	63469 → 443 [ACK] Seq=1 Ack=1 Win=13...
1030	25.850504	192.168.31.124	192.241.181.178	TLSv1	588	Client Hello
1031	25.999522	192.168.31.124	192.168.31.44	AFP	88	FPGetVolParms request: Vol=9
1032	25.999838	192.168.31.44	192.168.31.124	AFP	116	FPGetVolParms reply
1033	25.999920	192.168.31.124	192.168.31.11	TCP	66	64625 → 542 [ACK] Seq=505 Ack=1254 Wi...

▶ Frame 1026: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface 0

▶ Ethernet II, Src: BelkinIn\_88:a2:20 (94:10:3e:88:a2:20), Dst: Apple\_04:bc:28 (c4:2c:03:04:bc:28)

▶ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.31.124

▶ User Datagram Protocol, Src Port: 53, Dst Port: 24806

▶ Domain Name System (response)

Offset	Hex	Dec	Printable
0000	c4 2c 03 04 bc 28 94 10 3e 88 a2 20 08 00 45 00	205 44 3 4 20 44 148 16 58 136 168 170 32 8 0 69 0	, . . . ( . . > . . E .
0010	00 5d 81 6a 00 00 79 11 cf f1 08 08 08 08 c0 a8	0 93 131 106 0 0 125 17 251 241 8 8 8 8 192 168	. ] j . y . . . . . .
0020	1f 7c 00 35 60 e6 00 49 99 1c d4 89 81 80 00 01	31 124 0 53 96 234 15 209 193 136 205 137 129 128 0 1	.   5' . I . . . . . .
0030	00 01 00 00 00 00 12 6c 70 2d 70 75 73 68 2d 73	0 1 0 0 0 0 0 0 18 14 112 17 117 115 113 110 175 115	. . . . . l p-push-s
0040	65 72 76 65 72 2d 38 38 37 08 6c 61 73 74 70 61	101 114 118 101 114 141 102 102 102 102 102 102 102 102 102 102 102 102	erver-88 7 lastpa
0050	73 73 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00	115 115 103 99 102 104 0 0 0 1 0 1 192 168 170 128 115 115	ss . com . . . . . .
0060	01 00 00 01 7e 00 04 c0 f1 b5 b2	1 0 0 0 126 0 4 192 168 170 128 115 115	. . . ~ . . . . . .

Ethernet (eth), 14 bytes

Packets: 1066 · Displayed: 1066 (100.0%) · Dropped: 0 (0.0%) · Profile: Default



Ethernet: en0

dns Expression...

No.	Time	Source	Destination	Protocol	Length	Info
20	1.076600	192.168.31.124	8.8.8.8	DNS	88	Standard query 0x7ffd A 20.client-channel...
21	1.097643	8.8.8.8	192.168.31.124	DNS	104	Standard query response 0x7ffd A 20.client...
954	24.587099	192.168.31.124	8.8.8.8	DNS	80	Standard query 0x8942 A adfarm.mediaplex.c...
958	24.664392	192.168.31.124	8.8.8.8	DNS	80	Standard query 0xbc9f A adfarm.mediaplex.c...
959	24.692671	8.8.8.8	192.168.31.124	DNS	255	Standard query response 0xbc9f A adfarm.me...
984	24.732391	8.8.8.8	192.168.31.124	DNS	255	Standard query response 0x8942 A adfarm.me...
1025	25.733327	192.168.31.124	8.8.8.8	DNS	91	Standard query 0xd489 A lp-push-server-887...
1026	25.755508	8.8.8.8	192.168.31.124	DNS	107	Standard query response 0xd489 A lp-push-s...

Frame 1026: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface 0

Ethernet II, Src: BelkinIn\_88:a2:20 (94:10:3e:88:a2:20), Dst: Apple\_04:bc:28 (c4:2c:03:04:bc:28)

Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.31.124

User Datagram Protocol, Src Port: 53, Dst Port: 24806

Domain Name System (response)

Hex	Dec	Text
0000	c4 2c 03 04 bc 28 94 10 3e 88 a2 20 08 00 45 00	. , ... ( . . > . . . E
0010	00 5d 81 6a 00 00 79 11 cf f1 08 08 08 08 c0 a8	: j . y . . . . . . . .
0020	1f 7c 00 35 60 e6 00 49 99 1c d4 89 81 80 00 01	:   . 5 ' . I . . . . . . .
0030	00 01 00 00 00 00 12 6c 70 2d 70 75 73 68 2d 73	: . . . . . l p - push - s
0040	65 72 76 65 72 2d 38 38 37 08 6c 61 73 74 70 61	er ver - 88 7 . lastpa
0050	73 73 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00	ss . com . . . . . . . .
0060	01 00 00 01 7e 00 04 c0 f1 b5 b2	.... ~ . . . . . . . .

Domain Name System: Protocol

Packets: 1066 · Displayed: 8 (0.8%) · Dropped: 0 (0.0%) · Profile: Default



Ethernet: en0

ip.src == 192.168.31.1

No.	Time	Source	Destination	Protocol	Length	Info
136	4.810945	192.168.31.1	224.0.1.60	IGMPv2	60	Membership Query, specific for group 224.0...
137	4.811266	192.168.31.1	224.0.1.60	IGMPv2	60	Membership Query, specific for group 224.0...
138	4.811526	192.168.31.1	224.0.1.60	IGMPv2	60	Membership Query, specific for group 224.0...
454	9.981564	192.168.31.1	224.0.0.22	IGMPv2	60	Membership Query, specific for group 224.0...
455	9.982255	192.168.31.1	224.0.0.2	IGMPv2	60	Membership Query, specific for group 224.0...
483	10.636227	192.168.31.1	224.0.0.2	IGMPv2	60	Membership Report group 224.0.0.2
486	10.866153	192.168.31.1	224.0.0.22	IGMPv2	60	Membership Report group 224.0.0.22

► Frame 486: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
► Ethernet II, Src: BelkinIn\_88:a2:20 (94:10:3e:88:a2:20), Dst: IPv4mcast\_16 (01:00:5e:00:00:16)  
► Internet Protocol Version 4, Src: 192.168.31.1, Dst: 224.0.0.22  
► Internet Group Management Protocol

0000	01 00 5e 00 00 16 94 10 3e 88 a2 20 08 00 46 c0	..^..... >... F.
0010	00 20 00 00 40 00 01 02 24 58 c0 a8 1f 01 e0 00	. . @... \$X.....
0020	00 16 94 04 00 00 16 00 09 e9 e0 00 00 16 00 00	..... .... .....
0030	00 00 00 00 00 00 00 00 77 2c 25 e8	..... w,%.

# Operators

## Comparison operators:

English format:	C like format:	Meaning:
Six comparison operators are available:		
eq	==	Equal
ne	!=	Not equal
gt	>	Greater than
lt	<	Less than
ge	>=	Greater or equal
le	<=	Less or equal

## Logical expressions:

English format:	C like format:	Meaning:
and	&&	Logical AND
or		Logical OR
xor	^^	Logical XOR
not	!	Logical NOT

Examples:

**snmp || dns || icmp** Display the SNMP or DNS or ICMP traffics.

**ip.addr == 10.1.1.1**

Displays the packets with source or destination IP address equals to 10.1.1.1.

**ip.src != 10.1.2.3 or ip.dst != 10.4.5.6**

Displays the packets with a source IP address different from 10.1.2.3 or with a destination IP different from 10.4.5.6.

In other words, the displayed packets will have:

Source IP address: anything but 10.1.2.3, destination IP address: anything  
and

Source IP address: anything, destination IP address: anything but 10.4.5.6

**ip.src != 10.1.2.3 and ip.dst != 10.4.5.6**

Displays the packets with source IP different from 10.1.2.3 and in the same time with destination IP different from 10.4.5.6

In other words, the displayed packets will have:

Source IP address: anything but 10.1.2.3 and destination IP address: anything but 10.4.5.6

**tcp.port == 25** Display packets with TCP source or destination port 25.

**tcp.dstport == 25** Display packets with TCP destination port 25.

**tcp.flags** Display packets having a TCP flags

**tcp.flags.syn == 0x02** Display packets with a TCP SYN flag.

If the filter syntax is correct, it will be highlighted in green, otherwise if there is a syntax mistake it will be highlighted in red.

Filter: `tcp.port == 100`

Correct syntax

Filter: `tcp.port = 100`

Wrong syntax

## Ethernet address

6 bytes separated by a colon (:), dot (.) or dash (-) with one or two bytes between separators:

```
eth.dst == ff:ff:ff:ff:ff:ff  
eth.dst == ff-ff-ff-ff-ff-ff  
eth.dst == ffff.ffff.ffff
```

## IPv4 address

```
ip.addr == 192.168.0.1
```

Classless InterDomain Routing (CIDR) notation can be used to test if an IPv4 address is in a certain subnet. For example, this display filter will find all packets in the 129.111 Class-B network:

```
ip.addr == 129.111.0.0/16
```

## IPv6 address

```
ip6.addr == ::1
```

#### 6.4.4. Slice Operator

Wireshark allows you to select subsequences of a sequence in rather elaborate ways. After a label you can place a pair of brackets [] containing a comma separated list of range specifiers.

```
eth.src[0:3] == 00:00:83
```

The example above uses the n:m format to specify a single range. In this case n is the beginning offset and m is the length of the range being specified.

```
eth.src[1-2] == 00:83
```

The example above uses the n-m format to specify a single range. In this case n is the beginning offset and m is the ending offset.

```
eth.src[:4] == 00:00:83:00
```

The example above uses the :m format, which takes everything from the beginning of a sequence to offset m. It is equivalent to 0:m

```
eth.src[4:] == 20:20
```

The example above uses the n: format, which takes everything from offset n to the end of the sequence.

```
eth.src[2] == 83
```

The example above uses the n format to specify a single range. In this case the element in the sequence at offset n is selected. This is equivalent to n:1.

```
eth.src[0:3,1-2,:4,4:,2] ==
00:00:83:00:83:00:00:83:00:20:20:83
```

Wireshark allows you to string together single ranges in a comma separated list to form compound ranges as shown above.



## 6.4.5. Membership Operator

Wireshark allows you to test a field for membership in a set of values or fields. After the field name, use the in operator followed by the set items surrounded by braces {}.

```
tcp.port in {80 443 8080}
```

This can be considered a shortcut operator, as the previous expression could have been expressed as:

```
tcp.port == 80 || tcp.port == 443 || tcp.port == 8080
```

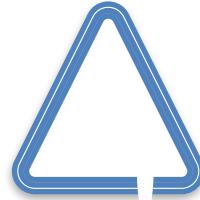
The set of values can also contain ranges:

```
tcp.port in {443 4430..4434}
```

This is not merely a shortcut for `tcp.port == 443 || (tcp.port >= 4430 && tcp.port <= 4434)`. Comparison operators are usually satisfied when any field matches the filter, and thus a packet with ports 80 and 56789 would match this alternative display filter since `56789 >= 4430 && 80 <= 4434` is true. The membership operator instead tests the same field against the range condition.

Sets are not just limited to numbers, other types can be used as well:

```
http.request.method in {"HEAD" "GET"}  
ip.addr in {10.0.0.5 .. 10.0.0.9 192.168.1.1..192.168.1.9}  
frame.time_delta in {10 .. 10.5}
```



#### 6.4.7. A Common Mistake

Using the `!=` operator on combined expressions like `eth.addr`, `ip.addr`, `tcp.port`, and `udp.port` will probably not work as expected. Wireshark will show the warning “`"!="` is deprecated or may have unexpected results” when you use it.

Often people use a filter string to display something like `ip.addr == 1.2.3.4` which will display all packets containing the IP address 1.2.3.4.

Then they use `ip.addr != 1.2.3.4` to see all packets not containing the IP address 1.2.3.4 in it. Unfortunately, this does *not* do the expected.

Instead, that expression will even be true for packets where either source or destination IP address equals 1.2.3.4. The reason for this, is that the expression `ip.addr != 1.2.3.4` must be read as “the packet contains a field named `ip.addr` with a value different from 1.2.3.4”. As an IP datagram contains both a source and a destination address, the expression will evaluate to true whenever at least one of the two addresses differs from 1.2.3.4.

If you want to filter out all packets containing IP datagrams to or from IP address 1.2.3.4, then the correct filter is `!(ip.addr == 1.2.3.4)` as it reads “show me all the packets for which it is not true that a field named `ip.addr` exists with a value of 1.2.3.4”, or in other words, “filter out all packets for which there are no occurrences of a field named `ip.addr` with the value 1.2.3.4”.

## Extra voorbeelden filters

<https://networksecuritytools.com/list-wireshark-filters>



▶ Frame 1: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0

▼ Ethernet II, Src: BelkinIn\_88:a2:20 (94:10:3e:88:a2:20), Dst: Apple\_04:bc:28 (c4:2c:03:04:bc:28)

- ▶ Destination: Apple\_04:bc:28 (c4:2c:03:04:bc:28)
- ▶ Source: BelkinIn\_88:a2:20 (94:10:3e:88:a2:20)
- Type: IPv4 (0x0800)

▶ Internet Protocol Version 4, Src: 217.148.93.160, Dst: 192.168.31.124

▶ Transmission Control Protocol, Src Port: 443, Dst Port: 59173, Seq: 1, Ack: 1, Len: 31

▶ Secure Sockets Layer

0000	c4 2c 03 04 bc 28 94 10 3e 88 a2 20 08 00 45 00	. ,...(... >... ..E.
0010	00 53 79 12 40 00 35 06 b5 39 d9 94 5d a0 c0 a8	.Sy @ 5 . 9 ...] ...
0020	1f 7c 01 bb e7 25 47 44 43 85 0b 5b 22 30 80 18	.   ...%GD C ["0 ..
0030	00 fd ad 96 00 00 01 01 08 0a c5 86 7e 9a 4b af	..... . .~K.
0040	12 91 17 03 03 00 1a fd 7d 2e a9 3e 14 4a 4d ec	..... }..>.JM.
0050	50 88 67 d4 be cf eb 0d d2 2d 24 2c 0d dc bf fd	P.g..... -\$,...
0060	89	

▶ Frame 1: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0

▼ Ethernet II, Src: BelkinIn\_88:a2:20 (94:10:3e:88:a2:20), Dst: Apple\_04:bc:28 (c4:2c:03:04:bc:28)

- ▶ Destination: Apple\_04:bc:28 (c4:2c:03:04:bc:28)
- ▶ Source: BelkinIn\_88:a2:20 (94:10:3e:88:a2:20)
- Type: IPv4 (0x0800)

▶ Internet Protocol Version 4, Src: 217.148.93.160, Dst: 192.168.31.124

▶ Transmission Control Protocol, Src Port: 443, Dst Port: 59173, Seq: 1, Ack: 1, Len: 31

▶ Secure Sockets Layer

0000	c4 2c 03 04 bc 28 94 10 3e 88 a2 20 08 00 45 00	. ,...(... >... ..E.
0010	00 53 79 12 40 00 35 06 b5 39 d9 94 5d a0 c0 a8	.Sy @ 5 . 9 ...] ...
0020	1f 7c 01 bb e7 25 47 44 43 85 0b 5b 22 30 80 18	.   ...%GD C ["0 ..
0030	00 fd ad 96 00 00 01 01 08 0a c5 86 7e 9a 4b af	..... . .~K.
0040	12 91 17 03 03 00 1a fd 7d 2e a9 3e 14 4a 4d ec	..... }..>.JM.
0050	50 88 67 d4 be cf eb 0d d2 2d 24 2c 0d dc bf fd	P.g..... -\$,...
0060	89	



tcp

No.	Time	Source	Destination	Protocol	Length	Info
91	5.671099	192.168.31.124	104.40.147.142	TCP	66	65018 → 443 [ACK] Seq=1 Ack=1440 Win=4089 Len=0 TSval...
99	6.051383	104.40.147.142	192.168.31.124	TLSv1...	208	Application Data
100	6.051475	192.168.31.124	104.40.147.142	TCP	66	65018 → 443 [ACK] Seq=1 Ack=1582 Win=4091 Len=0 TSval...
101	6.325604	104.40.147.142	192.168.31.124	TLSv1...	265	Application Data
102	6.325739	192.168.31.124	104.40.147.142	TCP	66	65018 → 443 [ACK] Seq=1 Ack=1781 Win=4089 Len=0 TSval...
105	6.459147	108.177.126.189	192.168.31.124	TLSv1...	124	Application Data
106	6.459264	192.168.31.124	108.177.126.189	TCP	66	55047 → 443 [ACK] Seq=1 Ack=59 Win=4094 Len=0 TSval=1...
107	6.466372	192.168.31.124	192.168.31.44	AFP	88	FPGetVolParms request: Vol=9
108	6.466704	192.168.31.44	192.168.31.124	AFP	116	FPGetVolParms reply
109	6.466767	192.168.31.124	192.168.31.44	TCP	66	54625 → 548 [ACK] Seq=89 Ack=201 Win=11482 Len=0 TSva...

Frame 127: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface 0

Ethernet II, Src: BelkinIn\_88:a2:20 (94:10:3e:88:a2:20), Dst: Apple\_04:bc:28 (c4:2c:03:04:bc:28)

- ▶ Destination: Apple\_04:bc:28 (c4:2c:03:04:bc:28)
- ▶ Source: BelkinIn\_88:a2:20 (94:10:3e:88:a2:20)
- Type: IPv4 (0x0800)
- ▶ Internet Protocol Version 4, Src: 185.82.210.189, Dst: 192.168.31.124
- ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 64970, Seq: 124, Ack: 356, Len: 70
- ▶ Secure Sockets Layer

```

0000 c4 2c 03 04 bc 28 94 10 3e 88 a2 20 08 00 45 00 . , ... ( .. > .. E .
0010 00 7a 1d 3a 40 00 35 06 bc 0f b9 52 d2 bd c0 a8 . z : @ 5 . . . R . .
0020 1f 7c 01 bb fd ca 7b e7 06 6a 7f 1c 68 72 80 18 . | . . . { . j . hr . .
0030 00 b6 dd 0d 00 00 01 01 08 0a c7 3f 31 26 4b af . . . . . . ? 1 & K .
0040 8d 9f 17 03 03 00 41 59 6e 8b 1c 86 3e 7a 50 59 . . . . A Y n . . > z P Y
0050 90 07 ac 9b 49 ad 58 61 b7 3b a8 ca 1d 60 b6 ab . . . . I X a . ; . . .
0060 4b 94 cf 2f 87 bf 42 61 3d da 08 11 0a a6 36 ad K . / . Ba = . . . . 6 .
0070 7e f0 29 94 54 56 5f f8 19 d9 50 a4 42 a4 ec c5 ~ . ) . T V _ . . P B . .
0080 dc 72 08 36 12 3e 0f 91 . r 6 . > . .

```

Packets: 6134 · Displayed: 5325 (86.8%) · Dropped: 0 (0.0%) · Profile: Default

# ICMP = ping

Ethernet: en0

No.	Time	Source	Destination	Protocol	Length	Info
184	7.116482	192.168.31.124	8.8.8.8	ICMP	70	Destination unreachable (Port unreachable)
384	8.757787	192.168.31.124	172.217.17.110	ICMP	98	Echo (ping) request id=0xa8b2, seq=0/0, ttl=64 (reply in ...)
385	8.787625	172.217.17.110	192.168.31.124	ICMP	98	Echo (ping) reply id=0xa8b2, seq=0/0, ttl=51 (request i...)
539	9.761021	192.168.31.124	172.217.17.110	ICMP	98	Echo (ping) request id=0xa8b2, seq=1/256, ttl=64 (reply i...)
540	9.787157	172.217.17.110	192.168.31.124	ICMP	98	Echo (ping) reply id=0xa8b2, seq=1/256, ttl=51 (request...)
589	10.764882	192.168.31.124	172.217.17.110	ICMP	98	Echo (ping) request id=0xa8b2, seq=2/512, ttl=64 (reply i...)
590	10.796414	172.217.17.110	192.168.31.124	ICMP	98	Echo (ping) reply id=0xa8b2, seq=2/512, ttl=51 (request...)
4590	44.831304	192.168.31.1	192.168.31.124	ICMP	130	Destination unreachable (Port unreachable)

► Frame 385: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

▼ Ethernet II, Src: BelkinIn\_88:a2:20 (94:10:3e:88:a2:20), Dst: Apple\_04:bc:28 (c4:2c:03:04:bc:28)

► Destination: Apple\_04:bc:28 (c4:2c:03:04:bc:28)

► Source: BelkinIn\_88:a2:20 (94:10:3e:88:a2:20)

Type: IPv4 (0x0800)

► Internet Protocol Version 4, Src: 172.217.17.110, Dst: 192.168.31.124

► Internet Control Message Protocol

0000 c4 2c 03 04 bc 28 94 10 3e 88 a2 20 08 00 45 00  
0010 00 54 00 00 00 00 33 01 e9 3d ac d9 11 6e c0 a8  
0020 1f 7c 00 00 9c 0b a8 b2 00 00 5b b5 0d ee 00 01  
0030 66 9a 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  
0060 36 37

iMac27:~ iMac\$ ping google.com  
PING google.com (172.217.17.110): 56 data bytes  
64 bytes from 172.217.17.110: icmp\_seq=0 ttl=51 time=31.319 ms  
64 bytes from 172.217.17.110: icmp\_seq=1 ttl=51 time=27.952 ms  
64 bytes from 172.217.17.110: icmp\_seq=2 ttl=51 time=30.248 ms  
64 bytes from 172.217.17.110: icmp\_seq=3 ttl=51 time=33.228 ms  
^C >-- google.com ping statistics ---  
4 packets transmitted, 4 packets received, 0.0% packet loss  
round-trip min/avg/max/stddev = 27.952/30.687/33.228/1.906 ms  
iMac27:~ iMac\$

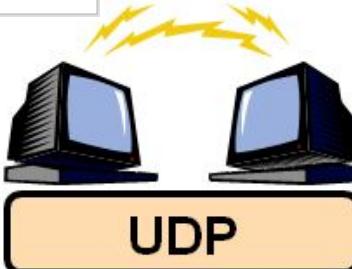
Packets: 5393 · Displayed: 8 (0.1%) · Dropped: 0 (0.0%) · Profile: Default  
associate KU Leuven Waves

Ethernet: en0

udp.port == 53

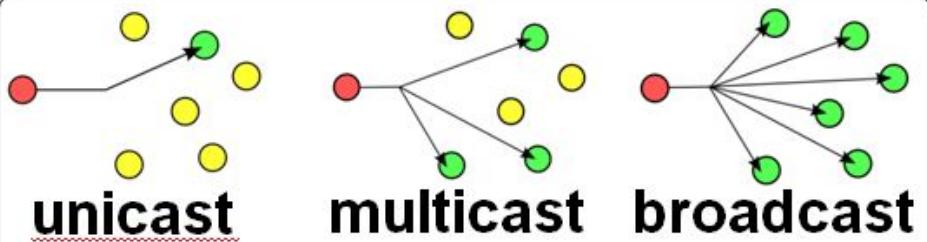
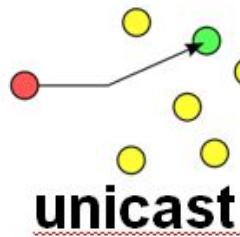
No.	Time	Source	Destination	Protocol	Length	Info
14	0.136677	192.168.31.124	8.8.8.8	DNS	83	Standard query 0x13be A col.eum-appdynamics.com
15	0.169169	8.8.8.8	192.168.31.124	DNS	211	Standard query response 0x13be A col.eum-appdynamics...
174	7.094961	192.168.31.124	8.8.8.8	DNS	74	Standard query 0xeaf8 A www.google.com
183	7.116396	8.8.8.8	192.168.31.124	DNS	90	Standard query response 0xeaf8 A www.google.com A 17...
184	7.116482	192.168.31.124	8.8.8.8	ICMP	70	Destination unreachable (Port unreachable)
256	7.386716	192.168.31.124	8.8.8.8	DNS	80	Standard query 0xaa8e A adfarm.mediaplex.com
269	7.432291	8.8.8.8	192.168.31.124	DNS	255	Standard query response 0xaa8e A adfarm.mediaplex.co...
382	8.735099	192.168.31.124	8.8.8.8	DNS	70	Standard query 0x5e95 A google.com
383	8.757068	8.8.8.8	192.168.31.124	DNS	86	Standard query response 0x5e95 A google.com A 172.21...
628	11.119230	192.168.31.124	8.8.8.8	DNS	81	Standard quer 0xd8eb A outlook.office365.com
► Frame 383: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0						
▼ Ethernet II, Src: BelkinIn_88:a2:20 (94:10:3e:88:a2:20), Dst: Apple_04:bc:28 (c4:2c:03:04:bc:28)						
► Destination: Apple_04:bc:28 (c4:2c:03:04:bc:28)						
► Source: BelkinIn_88:a2:20 (94:10:3e:88:a2:20)						
Type: IPv4 (0x0800)						
► Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.31.124						
► User Datagram Protocol, Src Port: 53, Dst Port: 63382						
► Domain Name System (response)						
0000	c4 2c 03 04 bc 28 94 10 3e 88 a2 20 08 00 45 00	. , . . ( . . > . . E .				
0010	00 48 36 94 00 00 79 11 1a dd 08 08 08 08 c0 a8	. H 6 . . y . . . . . . .				
0020	1f 7c 00 35 f7 96 00 34 a5 30 5e 95 81 80 00 01	.   . 5 . . 4 . 0 ^ . . . .				
0030	00 01 00 00 00 00 06 67 6f 6f 67 6c 65 03 63 6f	. . . . . g o o g l e . c o				
0040	6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 01 2b	m . . . . . . . . . . + . .				
0050	00 04 ac d9 11 6e	. . . . n . . . . . . . . .				

Application	WWW	FTP	E-mail	NFS	VoIP	DNS
Transport	TCP		UDP			
Network	IP					
Physical	Ethernet	AAL-5	HDLC			



- Slower but reliable transfers
- Typical applications:
  - Email
  - Web browsing

- Fast but non-guaranteed transfers (“best effort”)
- Typical applications:
  - VoIP
  - Music streaming



# Help

ip.  
No. ip.src == 192.168.31.1  
ip.addr == 192.0.2.1 and not tcp.port in {80 25}  
ip.addr == 192.0.2.1  
ip.addr  
ip.bogus\_ip\_length  
ip.bogus\_ip\_version  
ip.checksum  
ip.checksum.status  
ip.checksum\_bad.expert  
ip.checksum\_calculated  
ip.cipso.categories  
ip.cipso.doi  
ip.cipso.malformed  
ip.cipso.sensitivity\_level  
ip.cipso.tag\_data  
ip.cipso.tag\_type  
ip.cur\_rt  
ip.cur\_rt\_host  
ip.dsfield  
ip.dsfield.dsdp  
User Datagram Protocol, Src Port: 53, Dst Port: 63  
Domain Name System (response)

No.	Destination
	8.8.8
	192.168.31.
	8.8.8
	192.168.31.
	<b>8.8.8</b>
	8.8.8
	192.168.31.
	8.8.8
	192.168.31.
	8.8.8
	86 bytes o
	:10:3e:88:a
	:04:bc:28)
	8:a2:20)

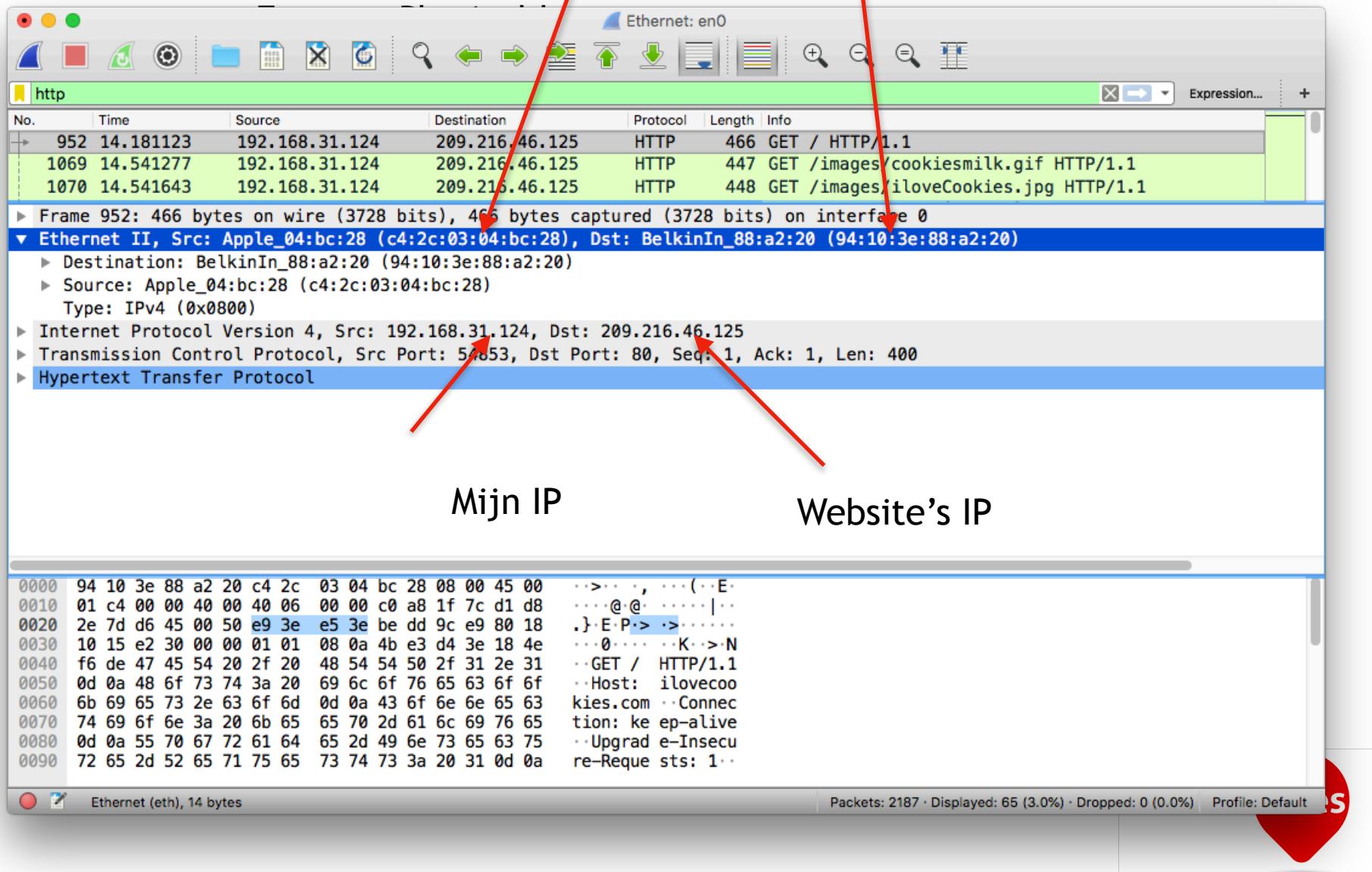
No.	Time	Source
14	0.136677	192.168.31.124
15	0.169169	8.8.8.8
174	7.094961	192.168.31.124
183	7.116396	8.8.8.8
<b>184</b>	<b>7.116482</b>	<b>192.168.31.124</b>
256	7.386716	192.168.31.124

No.	Time	Source
14	0.136677	192.168.31.124
15	0.169169	8.8.8.8

# Packet Analysis

## Mijn MAC

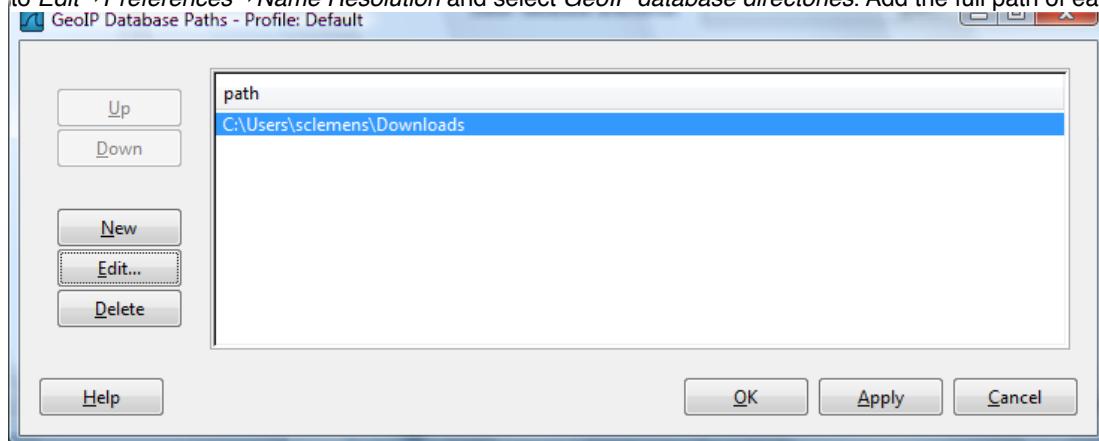
## Router's MAC



Wireshark does not ship with any GeoIP or GeoLite databases, so you have to download them yourself. You can get them at the following locations:

- GeoLite City, Country, and ASNum: <http://geolite.maxmind.com/download/geoip/database/> (free download)

It's more convenient if you put all of the databases in the same directory. Once you've downloaded your databases, you must tell Wireshark where they are. Go to *Edit→Preferences→Name Resolution* and select *GeoIP database directories*. Add the full path of each database directory, as shown below:



## Filtering Traffic

You can use the `ip.geoip` display filters to filter traffic.

Exclude U.S.-based traffic:

```
ip and not ip.geoip.country == "United States"
```

Show address above the arctic circle:

```
ip.geoip.lat > "66.5"
```

Ethernet: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
428	5.411763	192.168.31.124	145.239.69.56	HTTP	462	GET / HTTP/1.1
432	5.434108	145.239.69.56	192.168.31.124	HTTP	703	HTTP/1.1 301 Moved Permanently (text/html)
1568	6.398795	192.168.31.124	2.22.55.123	HTTP	341	GET /MFYwVKADAgEAME0wSzBJMAkGBSs0AwIaBQAEF...

Frame 428: 462 bytes on wire (3696 bits), 462 bytes captured (3696 bits) on interface 0  
Ethernet II, Src: Apple\_04:bc:28 (c4:2c:03:04:bc:28), Dst: BelkinIn\_88:a2:20 (94:10:3e:88:a2:20)  
Internet Protocol Version 4, Src: 192.168.31.124, Dst: 145.239.69.56  
Transmission Control Protocol, Src Port: 59094, Dst Port: 80, Seq: 1, Ack: 1, Len: 396

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n
Host: www.miras.be\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_13\_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,nl;q=0.8\r\n
\r\n
[Full request URI: http://www.miras.be/]
[HTTP request 1/1]
[Response in frame: 432]

0020	45 38 e6 d6 00 50 0d 00	01 ca 65 0a 00 8e 80 18	E8 ..P...e.....
0030	10 15 b8 fe 00 00 01 01	08 0a 4b f1 db ae 18 2d	.....K....-
0040	8e f0 47 45 54 20 2f 20	48 54 54 50 2f 31 2e 31	..GET / HTTP/1.1
0050	0d 0a 48 6f 73 74 3a 20	77 77 77 2e 6d 69 72 61	..Host: www.mira
0060	73 2e 62 65 0d 0a 43 6f	6e 6e 65 63 74 69 6f 6e	s.be..Co nnection
0070	3a 20 6b 65 65 70 2d 61	6c 69 76 65 0d 0a 55 70	: keep-a live..Up
0080	67 72 61 64 65 2d 49 6e	73 65 63 75 72 65 2d 52	grade-In secure-R
0090	65 71 75 65 73 74 73 3a	20 31 0d 0a 55 73 65 72	equests: 1..User
00a0	2d 41 67 65 6e 74 3a 20	4d 6f 7a 69 6c 6c 61 2f	-Agent: Mozilla/
00b0	35 2e 30 20 28 4d 61 63	69 6e 74 6f 73 68 3b 20	5.0 (Mac intosh;
00c0	49 6e 74 65 6c 20 4d 61	63 20 4f 53 20 58 20 31	Intel Ma c OS X 1

Transmission Control Protocol (tcp), 32 bytes

Packets: 11171 - Displayed: 4 (0.0%) - Dropped: 0 (0.0%) Profile: Default

# HTTP Request

Ethernet: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
428	5.411763	192.168.31.124	145.239.69.56	HTTP	462	GET / HTTP/1.1
432	5.434108	145.239.69.56	192.168.31.124	HTTP	703	HTTP/1.1 301 Moved Permanently (text/html)
1568	6.398795	192.168.31.124	2.22.55.123	HTTP	341	GET /MFYwVKADAgEAME0wSzBJMAkGBSs0AwIaBQAEF..

Frame 428: 462 bytes on wire (3696 bits), 462 bytes captured (3696 bits) on interface 0  
Ethernet II, Src: Apple\_04:bc:28 (c4:2c:03:04:bc:28), Dst: BelkinIn\_88:a2:20 (94:10:3e:88:a2:20)  
Internet Protocol Version 4, Src: 192.168.31.124, Dst: 145.239.69.56  
Transmission Control Protocol, Src Port: 59094, Dst Port: 80, Seq: 1, Ack: 1, Len: 396

Hypertext Transfer Protocol

GET / HTTP/1.1\r\nHost: www.miras.be\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_13\_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9,nl;q=0.8\r\n\r\n[Full request URI: http://www.miras.be/]  
[HTTP request 1/1]  
[Response in frame: 432]

0020 45 38 e6 d6 00 50 0d 00 01 ca 65 0a 00 8e 80 18 E8...P...e.....  
0030 10 15 b8 fe 00 00 01 01 08 0a 4b f1 db ae 18 2d .....K....-  
0040 8e f0 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 .GET / HTTP/1.1  
0050 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 69 72 61 .Host: www.mira  
0060 73 2e 62 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e s.be..Co nnection  
0070 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 : keep-a live..Up  
0080 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 grade-In secur-R  
0090 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 equests: 1..User  
00a0 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/  
00b0 35 2e 30 20 28 4d 61 63 69 6e 74 6f 73 68 3b 20 5.0 (Mac intosh;  
00c0 49 6e 74 65 6c 20 4d 61 63 20 4f 53 20 58 20 31 Intel Ma c OS X 1

Transmission Control Protocol (tcp), 32 bytes

Packets: 11171 · Displayed: 4 (0.0%) · Dropped: 0 (0.0%) · Profile: Default

## About Chrome



Google Chrome



Google Chrome is up to date

Version 69.0.3497.100 (Official Build) (64-bit)

# HTTP

Ethernet: en0

No.	Time	Source	Destination	Protocol	Length	Info
328	15.106684	192.168.31.124	192.195.77.80	HTTP	955	POST /login-form/ HTTP/1.1 (application/x-www-f...)
334	15.238931	192.195.77.80	192.168.31.124	HTTP	257	HTTP/1.1 200 OK (text/html)

▶ Content-Length: 49\r\nCache-Control: max-age=0\r\nOrigin: http://www.demo.amitjakhu.com\r\nUpgrade-Insecure-Requests: 1\r\nContent-Type: application/x-www-form-urlencoded\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_13\_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Sa...Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/...Referer: http://www.demo.amitjakhu.com/login-form/\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9,nl;q=0.8\r\n▶ Cookie: \_\_utma=262906265.776638764.1538595062.1538595062.1538595062.\r\n\r\n[\[Full request URI: http://www.demo.amitjakhu.com/login-form/\]](http://www.demo.amitjakhu.com/login-form/)  
[HTTP request 1/1]  
[Response in frame: 334]  
File Data: 49 bytes

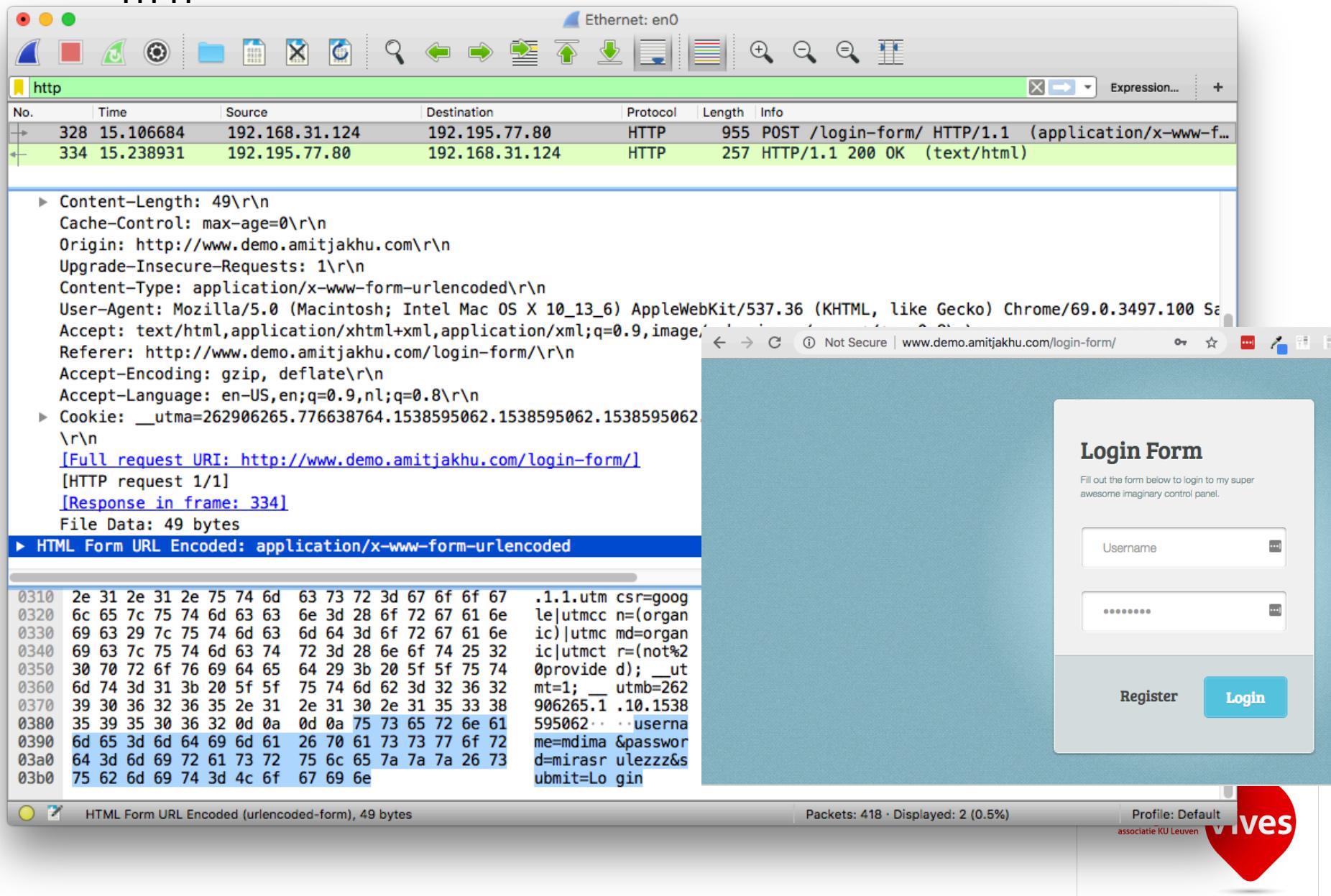
▶ HTML Form URL Encoded: application/x-www-form-urlencoded

0310	2e 31 2e 31 2e 75 74 6d 63 73 72 3d 67 6f 6f 67 .1.1.utm csr=goog
0320	6c 65 7c 75 74 6d 63 63 6e 3d 28 6f 72 67 61 6e le utmcc n=(organ
0330	69 63 29 7c 75 74 6d 63 6d 64 3d 6f 72 67 61 6e ic) utmcc md=organ
0340	69 63 7c 75 74 6d 63 74 72 3d 28 6e 6f 74 25 32 ic utmct r=(not%2
0350	30 70 72 6f 76 69 64 65 64 29 3b 20 5f 5f 75 74 0provide d); __ut
0360	6d 74 3d 31 3b 20 5f 5f 75 74 6d 62 3d 32 36 32 mt=1; __utmb=262
0370	39 30 36 32 36 35 2e 31 2e 31 30 2e 31 35 33 38 906265.1 .10.1538
0380	35 39 35 30 36 32 0d 0a 0d 0a 75 73 65 72 6e 61 595062 .. userna
0390	6d 65 3d 6d 64 69 6d 61 26 70 61 73 73 77 6f 72 me=mdima &passwor
03a0	64 3d 6d 69 72 61 73 72 75 6c 65 7a 7a 7a 26 73 d=mirasr ulezzz&s
03b0	75 62 6d 69 74 3d 4c 6f 67 69 6e ubmit=Lo gin

HTML Form URL Encoded (urlencoded-form), 49 bytes

Packets: 418 - Displayed: 2 (0.5%)

Profile: Default  
associaté KU Leuven vives



# HTTPS

Ethernet: en0

Apply a display filter ... <%> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
539	12.060370	104.40.147.142	192.168.31.124	TLSv1...	240	Application Data
540	12.060478	192.168.31.124	104.40.147.142	TCP	66	65018 → 443 [ACK] Seq=39 Ack=4925 Win=4090...
541	12.136752	192.168.31.124	8.8.8.8	DNS	75	Standard query 0xea33 A www.twitter.com
542	12.152407	8.8.8.8	192.168.31.124	DNS	121	Standard query response 0xea33 A www.twimg...
543	12.155657	192.168.31.124	63.215.202.158	TCP	54	64018 → 443 [RST, ACK] Seq=1 Ack=1 Win=409...
544	12.155805	192.168.31.124	93.184.220.66	TCP	66	63295 → 443 [FIN, ACK] Seq=1 Ack=1 Win=409...
545	12.156148	192.168.31.124	104.244.42.65	TCP	78	64234 → 443 [SYN] Seq=0 Win=65535 Len=0 MS...
546	12.156288	192.168.31.124	104.244.42.65	TCP	78	64235 → 443 [SYN] Seq=0 Win=65535 Len=0 MS...
547	12.175414	93.184.220.66	192.168.31.124	TCP	60	443 → 63295 [RST] Seq=1 Win=0 Len=0
548	12.185173	104.244.42.65	192.168.31.124	TCP	74	443 → 64235 [SYN, ACK] Seq=0 Ack=1 Win=289...
549	12.185321	192.168.31.124	104.244.42.65	TCP	66	64235 → 443 [ACK] Seq=1 Ack=1 Win=131744 L...
550	12.185816	192.168.31.124	104.244.42.65	TLSv1...	583	Client Hello
551	12.186359	104.244.42.65	192.168.31.124	TCP	74	443 → 64234 [SYN, ACK] Seq=0 Ack=1 Win=289...
552	12.186417	192.168.31.124	104.244.42.65	TCP	66	64234 → 443 [ACK] Seq=1 Ack=1 Win=131744 L...
553	12.186773	192.168.31.124	104.244.42.65	TLSv1...	583	Client Hello
554	12.189005	192.168.31.124	8.8.8.8	DNS	97	Standard query 0x0021 A www.twimg...

► Frame 553: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0

► Ethernet II, Src: Apple\_04:bc:28 (c4:2c:03:04:bc:28), Dst: BelkinIn\_88:a2:20 (94:10:3e:88:a2:20)

► Internet Protocol Version 4, Src: 192.168.31.124, Dst: 104.244.42.65

► Transmission Control Protocol, Src Port: 64234, Dst Port: 443, Seq: 1, Ack: 1, Len: 517

▼ Secure Sockets Layer

► TLSv1.2 Record Layer: Handshake Protocol: Client Hello

0000 94 10 3e 88 a2 20 c4 2c 03 04 bc 28 08 00 45 00 ..> . , .( E

0010 02 39 00 00 40 00 40 06 00 00 c0 a8 1f 7c 68 f4 .9 @ @ . | h

0020 2a 41 fa ea 01 bb 7a a6 e1 dc 12 aa 26 0f 80 18 \*A z &

0030 10 15 75 85 00 00 01 01 08 0a 4c 02 66 ed 13 29 ..u ..L.f )

0040 c5 8c 16 03 01 02 00 01 00 01 fc 03 03 7b 05 7a .....{z

0050 9b 55 b5 f7 2f 75 2c 02 ae 45 86 c1 f4 ea e1 dd ..U..u, E

0060 91 59 39 7c 1c 7c ad 8c 19 09 81 08 92 20 b5 8a .Y9| ..

0070 6c ee e2 f0 0e aa 16 45 da 21 87 dd a2 62 a9 7e l ..E ! ~ b

0080 fe be f6 49 01 13 88 28 a4 79 ed bf b3 49 00 22 ..I ..( y ..I "

0090 ca ca 13 03 13 01 13 02 cc a9 cc a8 c0 2b c0 2f .....+/

00a0 c0 2c c0 30 c0 13 c0 14 00 9c 00 9d 00 2f 00 35 .., 0 .. / 5

00b0 00 0a 01 00 01 91 4a 4a 00 00 ff 01 00 01 00 00 ..JJ ..

00c0 00 00 14 00 12 00 00 0f 77 77 77 2e 74 77 69 74 .....www.twimg

Bytes 166-167: Cipher Suite (ssl.handshake.ciphersuite)

Packets: 1943 · Displayed: 1943 (100.0%) · Dropped: 0 (0.0%) · Profile: Default · tool · associate · vives



# CLI

```
iMac — bash — 80x41
[iMac27:~ iMac$ tshark
Capturing on 'Ethernet'
  1  0.000000 G-ProCom_2a:d0:3d -> Broadcast      ARP 60 Who has 192.168.31.70?
    Tell 192.168.31.146
  2  0.136995 ZyxelCom_5e:45:09 -> Broadcast      0x8899 60 Realtek Layer 2 Protocols
  3  0.298200 192.168.31.124 -> 188.172.219.140 TCP 90 61191 -> 5938 [PSH, ACK]
    Seq=1 Ack=1 Win=4096 Len=24 TSval=1277691568 TSecr=3548010345
  4  0.304935 192.168.31.124 -> 8.8.8.8      DNS 73 Standard query 0x2c77 A www.cisco.com
  5  0.315363 188.172.219.140 -> 192.168.31.124 TCP 90 5938 -> 61191 [PSH, ACK]
    Seq=1 Ack=25 Win=1028 Len=24 TSval=3548060297 TSecr=1277691568
  6  0.315456 192.168.31.124 -> 188.172.219.140 TCP 66 61191 -> 5938 [ACK] Seq=25 Ack=25 Win=4095 Len=0 TSval=1277691584 TSecr=3548060297
  7  0.324106 ZyxelCom_5e:40:63 -> Broadcast      0x8899 60 Realtek Layer 2 Protocols
  8  0.361686      8.8.8.8 -> 192.168.31.124 DNS 255 Standard query response 0x2c77 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME wwwds.cisco.com.edgekey.net.globalredir.akadns.net CNAME e2867.dsca.akamaiedge.net A 23.206.90.16
  9  0.362314 192.168.31.124 -> 23.206.90.16 TCP 78 59148 -> 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1277691630 TSecr=0 SACK_PERM=1
 10  0.376558 23.206.90.16 -> 192.168.31.124 TCP 74 443 -> 59148 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2482571726 TSecr=1277691630 WS=128
 11  0.376666 192.168.31.124 -> 23.206.90.16 TCP 66 59148 -> 443 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=1277691644 TSecr=2482571726
 12  0.377043 192.168.31.124 -> 23.206.90.16 TLSv1 583 Client Hello
 13  0.395007 23.206.90.16 -> 192.168.31.124 TCP 74 [TCP Retransmission] 443 -> 59148 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2482571746 TSecr=1277691630 WS=128
 14  0.395073 192.168.31.124 -> 23.206.90.16 TCP 66 [TCP Dup ACK 11#1] 59148 -> 443 [ACK] Seq=518 Ack=1 Win=131744 Len=0 TSval=1277691661 TSecr=2482571726
 15  0.401000 23.206.90.16 -> 192.168.31.124 TCP 66 443 -> 59148 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=2482571751 TSecr=1277691644
 16  0.401889 23.206.90.16 -> 192.168.31.124 TLSv1.2 204 Server Hello, Change Cipher Spec, Encrypted Handshake Message
 17  0.401972 192.168.31.124 -> 23.206.90.16 TCP 66 59148 -> 443 [ACK] Seq=518 Ack=139 Win=131616 Len=0 TSval=1277691667 TSecr=2482571752
 18  0.402165 192.168.31.124 -> 23.206.90.16 TLSv1.2 109 Change Cipher Spec, Encrypted Handshake Message
```

tshark - -h

wireshark  
extension .

tshark -D

```
[iMac27:~ iMac$ tshark -D
1. en0 (Ethernet)
2. fw0 (FireWire)
3. utun0
4. utun1
5. lo0 (Loopback)
6. en1 (Wi-Fi)
7. gif0
8. stf0
9. p2p0
10. EHC250
11. EHC253
12. ciscodump (Cisco remote capture)
13. randpkt (Random packet generator)
14. sshdump (SSH remote capture)
15. udppdump (UDP Listener remote capture)
iMac27:~ iMac$
```

tshark -i en0 of tshark -i 1tshark -i en0 -i any

```
[iMac27:~ iMac$ tshark -i en0
Capturing on 'Ethernet'
    1  0.000000 129.143.116.10 -> 192.168.31.124 SSL 1514 Continuation Data
    2  0.000121 192.168.31.124 -> 129.143.116.10 TCP 54 61743 -> 443 [ACK] Seq=1
Ack=1461 Win=8146 Len=0
    3  0.000233 129.143.116.10 -> 192.168.31.124 SSL 1514 Continuation Data
    4  0.000344 129.143.116.10 -> 192.168.31.124 SSL 1514 Continuation Data
    5  0.000365 192.168.31.124 -> 129.143.116.10 TCP 54 61743 -> 443 [ACK] Seq=1
Ack=2921 Win=8192 Len=0
    6  0.000466 129.143.116.10 -> 192.168.31.124 SSL 1514 Continuation Data
    7  0.000508 192.168.31.124 -> 129.143.116.10 TCP 54 61743 -> 443 [ACK] Seq=1
Ack=5841 Win=8146 Len=0
    8  0.000646 129.143.116.10 -> 192.168.31.124 SSL 1514 Continuation Data
    9  0.000704 192.168.31.124 -> 129.143.116.10 TCP 54 61743 -> 443 [ACK] Seq=1
Ack=7301 Win=8192 Len=0
   10  0.000716 129.143.116.10 -> 192.168.31.124 SSL 1514 Continuation Data
   11  0.000844 129.143.116.10 -> 192.168.31.124 SSL 1514 Continuation Data
   12  0.000875 192.168.31.124 -> 129.143.116.10 TCP 54 61743 -> 443 [ACK] Seq=1
Ack=10221 Win=8146 Len=0
   13  0.040324 129.143.116.10 -> 192.168.31.124 SSL 1514 Continuation Data
   14  0.040468 192.168.31.124 -> 129.143.116.10 TCP 54 61743 -> 443 [ACK] Seq=1
Ack=11681 Win=8192 Len=0
   15  0.045303 129.143.116.10 -> 192.168.31.124 SSL 1514 Continuation Data
   16  0.045482 129.143.116.10 -> 192.168.31.124 SSL 1514 Continuation Data
   17  0.045541 192.168.31.124 -> 129.143.116.10 TCP 54 61743 -> 443 [ACK] Seq=1
Ack=14601 Win=8146 Len=0
   18  0.045603 129.143.116.10 -> 192.168.31.124 SSL 1514 Continuation Data
   19  0.045657 192.168.31.124 -> 129.143.116.10 TCP 54 61743 -> 443 [ACK] Seq=1
Ack=16061 Win=8192 Len=0
   20  0.045715 129.143.116.10 -> 192.168.31.124 SSL 1514 [TCP Previous segment
not captured], Continuation Data
   21  0.045753 192.168.31.124 -> 129.143.116.10 TCP 66 [TCP Dup ACK 19#1] 61743
- 443 [ACK] Seq=1 Ack=16061 Win=8192 Len=0 SLE=17521 SRE=18981
   22  0.045889 129.143.116.10 -> 192.168.31.124 SSL 1514 Continuation Data
   23  0.045923 192.168.31.124 -> 129.143.116.10 TCP 66 [TCP Dup ACK 19#2] 61743
- 443 [ACK] Seq=1 Ack=16061 Win=8192 Len=0 SLE=17521 SRE=20441
   24  0.081958 129.143.116.10 -> 192.168.31.124 SSL 1514 Continuation Data
   25  0.082045 192.168.31.124 -> 129.143.116.10 TCP 66 [TCP Dup ACK 19#3] 61743
- 443 [ACK] Seq=1 Ack=16061 Win=8192 Len=0 SLE=17521 SRE=21901
   26  0.095008 129.143.116.10 -> 192.168.31.124 TCP 1514 443 -> 61743 [ACK] Seq=
21901 Ack=1 Win=22 Len=1460
```

# tshark luistert enkel naar

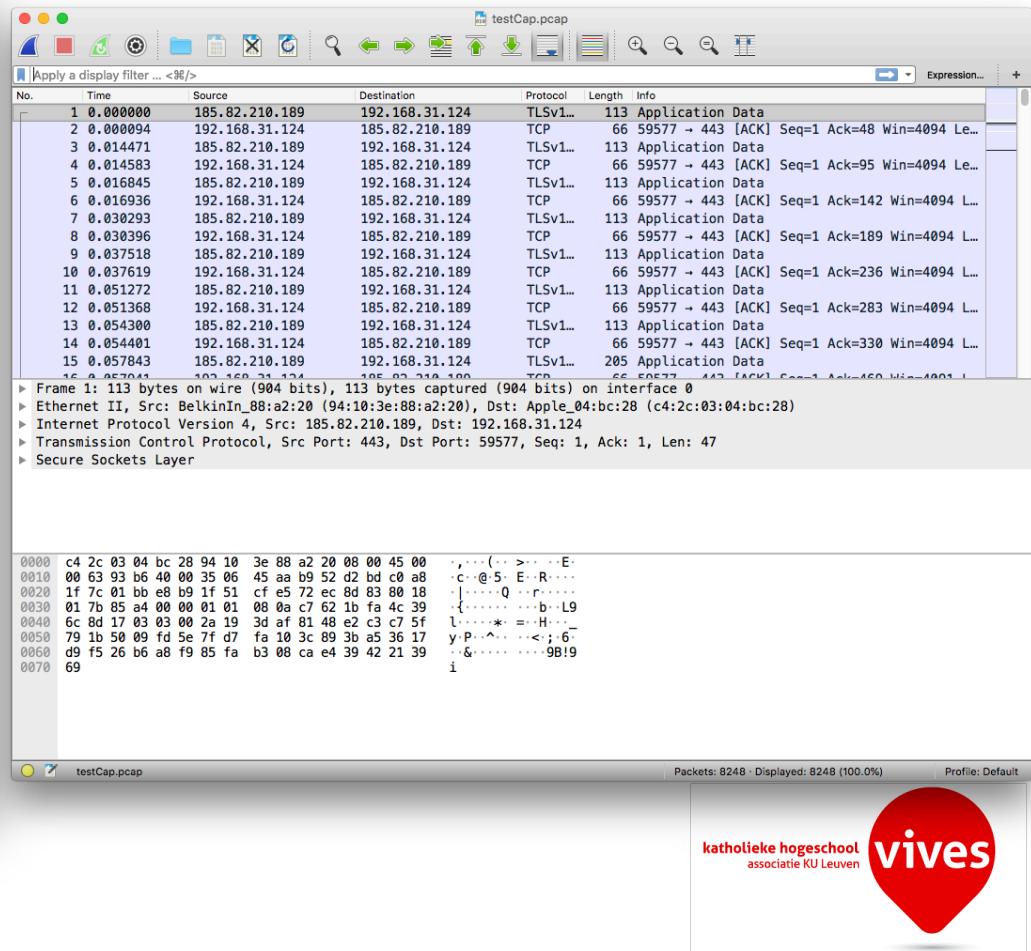
tshark -i en0 -w /hor  
beter  
tshark -i en0 -w /tmp/testCap.pcap

```
iMac — g?|vx{1??/?n{o?}?T? — bash — 80x41
[iMac27:~ iMac$ cat /tmp/testCap.pcap

?M<+????????=Intel(R) Core(TM) i3 CPU      550 @ 3.20GHz (with SSE4.2)-Mac_0
S X 10.13.6, build 17G65 (Darwin 17.7.0).Dumpcap (Wireshark) 2.6.3 (v2.6.3-0-ga6
2e6c27)?en0
-Mac OS X 10.13.6, build 17G65 (Darwin 17.7.0)\?Ywqq?,?(>??Ec??
@5E??Re??|??Q?r歛?({?
?bL91?*=?H??_y      ??<??;6??&?????9B!91?dYvcBB?>?? ?,?E4@??|?Re??r歛Q?
??l[
L9l??bd?Yw?S?qq?,?(>??Ec??@5E?Re??|??Q?r歛?({?
?bL91?*=?H??_B?V?Xj?3s?????V?T?6?0?r ?dYw?S?BB?>?? ?,?E4@??|?Re??r歛Q?C??
[ L9l??bd?Yw?\?qq?,?(>??Ec??@5E?Re??|??Q?Cr歛?({?
?bL91?*=?H??m?]?L?_?D?Fj?Ex?xg??,C??_??dYw-]BB?>?? ?,?E4@??|?Re??r歛Q?r??l [
L9l??bd?YwZ??qq?,?(>??Ec??@5E?Re??|??Q?rr歛?({?
?bL91?*=?H??1&=g?VFQ??k?R??
    Ud?????&ej??dYw???BB?>?? ?,?E4@??|?Re??r歛Q??
?1[
L9l??bd?Yw??qq?,?(>??Ec??@5E?Re??|??Q?r歛?({?
?bL91?*=?H??r??o??"?s?llc?16d?2?D?>dYw??BB?>?? ?,?E4@??|?Re??r歛Q?E?1[
L9l??bd?YwM?qq?,?(>??Ec??@5E?Re??|??Q?rr歛?({?
?bL91?*=?H??PU-S)h2q??>?k?*?d? 7???)??9dYw??BB?>?? ?,?E4@??|?Re??r歛Q??
?1[
L9l??bd?Yw?qq?,?(>??Ec??@5E?Re??|??Q?r歛?({?
?1[?K?d?Yw??qq?,?(>??Ec??@5E?Re??|??Q?r歛?({?
L9l??d?Yw??????,?(>??Ec??@5E?Re??|??Q?r歛?({?
?L91??=?H??c?)?"s????#鍏?>k?();<R????)?z??./@?P?m??"(fr?^?i??R??h?yp??
G?x
????HE??&?#bp?#p?n?=?6-BF??+dYwZ??BB?>?? ?,?E4@??|?Re??r歛Q?y?1[
L9l??d?Yw??????,?(>??Ec??@5E?Re??|??Q?r歛Q?y?m,
?j?n&??(?????9???)?<? ?
?h??~??n??>?P?D??SH??aa#?DJa?N1?????ZJ1W??Q??N?????9?5??&?Y?k??A?u?
??j??=?-8\Yw?
    <<?????#$*#*=?????F\dYw=<?BB?,?(>??Ec??@5E?Re??|??Q?y?V? ??
?b
-L91?d?Yw??\? ,?(>??EN??@5D?Re??|??Q?y?V? ??
?bCL91?=?H??M(N?P?Y(?HwKL??
??F??$?????b2?@?v??CB%55N1?
??Y@?+f??a?A6?^?l?!,t??M?B(US??Ro?y?r??(?S?1??
8?:.VN
    ?(
```

```
[iMac27:~ iMac$ tshark -i en0 -w /home/iMac27/testCap.pcap
Capturing on 'Ethernet'
tshark: The file to which the capture would be saved (""/home/iMac27/testCap.pcap") could not be opened: No such file or directory.

[iMac27:~ iMac$ tshark -i en0 -w /tmp/testCap.pcap
Capturing on 'Ethernet'
8248 ^C
iMac27:~ iMac$
```



tshark i en0 -a duration: 250 -w /tmp/file.pcap *stopt na 250 seconden*

tshark i en0 -a filesize: 250 -w /tmp/file.pcap *stopt als de file 250KB groot is*

tshark i en0 f “port 80 or port 443 or port 53”-b filesize: 5 -a files: 10 -w /tmp/file.pcap *luistert naar en0 poorten 80,443,53 en stopt als het 10 files van 5KB aangemaakt heeft*

# Capture filters != Display filters

tshark i en0 -f = filter

```
iMac27:~ iMac$ tshark -i en0 -f "
[> port 80
[> or
[> port 443"
Capturing on 'Ethernet'
 1  0.000000 104.40.147.142 -> 192.168.31.124 TLSv1.2 204 Application Data
 2  0.000130 192.168.31.124 -> 104.40.147.142 TCP 66 65018 -> 443 [ACK] Seq=1 Ack=139 Win=4091 Len=0 TS
 3  0.093108 192.168.31.124 -> 198.252.206.25 TCP 54 56439 -> 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
 4  0.164335 104.40.147.142 -> 192.168.31.124 TLSv1.2 251 Application Data
 5  0.164439 192.168.31.124 -> 104.40.147.142 TCP 66 65018 -> 443 [ACK] Seq=1 Ack=324 Win=4090 Len=0 TS
 6  0.186129 192.168.31.124 -> 216.58.211.99 UDP 290 65280 -> 443 Len=248
 7  0.203952 104.40.147.142 -> 192.168.31.124 TLSv1.2 210 Application Data
 8  0.204048 192.168.31.124 -> 104.40.147.142 TCP 66 65018 -> 443 [ACK] Seq=1 Ack=468 Win=4091 Len=0 TS
 9  0.207228 198.252.206.25 -> 192.168.31.124 TCP 66 [TCP ACKed unseen segment] 443 -> 56439 [ACK] Seq=
280344532
10  0.226264 216.58.211.99 -> 192.168.31.124 UDP 62 443 -> 65280 Len=20
11  0.232516 216.58.211.99 -> 192.168.31.124 UDP 584 443 -> 65280 Len=542
12  0.233252 216.58.211.99 -> 192.168.31.124 UDP 317 443 -> 65280 Len=275
13  0.233734 192.168.31.124 -> 216.58.211.99 UDP 70 65280 -> 443 Len=28
14  0.296464 104.40.147.142 -> 192.168.31.124 TLSv1.2 234 Application Data
15  0.296586 192.168.31.124 -> 104.40.147.142 TCP 66 65018 -> 443 [ACK] Seq=1 Ack=636 Win=4090 Len=0 TS
16  0.368822 108.177.126.189 -> 192.168.31.124 TLSv1.2 127 Application Data
17  0.368959 192.168.31.124 -> 108.177.126.189 TCP 66 60333 -> 443 [ACK] Seq=1 Ack=62 Win=4094 Len=0 TS
18  0.427107 192.168.31.124 -> 216.58.211.99 UDP 290 65280 -> 443 Len=248
```

## Filter file

```
tshark -r /tmp/testCap.pcap -T fields -e dns -e ip.src |uniq
```

Master Mode : alle traffic passeert via jou (bv router)

Ad-hoc Mode: p2p

Mash: via andere computers

Repeater Mode: alles wat binnenkomt wordt gerepeat

Monitor Mode: alle traffic wordt onderschept

check compatibiliteit netwerkkaart:

[https://www.aircrack-ng.org/doku.php?id=compatibility\\_drivers](https://www.aircrack-ng.org/doku.php?id=compatibility_drivers)

indien nodig usb netwerkkaart

```
rx packets 334327 bytes 33222372 (300.6 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 265617 bytes 28110199 (26.8 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@localhost ~]# iwconfig wlp2s0 | grep -i mode
Mode:Managed Frequency:2.437 GHz Access Point: 90:F6:52:C1:BB:18
[root@localhost ~]#
```

```
channel freq  key      power
[root@localhost ~]# iwconfig wlp2s0 mode monitor
Error for wireless request "Set Mode" (8B06) :
        SET failed on device wlp2s0 ; Device or resource busy.
[root@localhost ~]# ifconfig wlp2s0 down
```

```
[root@localhost ~]# iwconfig wlp2s0 mode monitor
[root@localhost ~]# ifconfig wlp2s0 up
[root@localhost ~]#
```

```
[root@localhost ~]# iwconfig wlp2s0
wlp2s0      IEEE 802.11bgn  Mode:Monitor
```

# When a problem strikes

- Network engineers check network interfaces, utilization levels, link errors and the wireless environment
- They want to prove it's not the network.



# What should I look for in traces?

- Wireshark has some great error events to flag TCP problems.
- Use the `tcp.analysis.flags` filter to spot them quickly, or the intelligent slide bar.

- TCP Retransmissions
- TCP Out-of-Orders
- Duplicate Acks
- Zero Windows

Wireshark

Apply a display filter ... <%>

No.	Time	DTime	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.31.121	224.0.0.2	IGMPv2	60	Membership Report group 224.0.0.2
2	0.036044	0.036044	G-ProCom_2a:d0:3d	Broadcast	ARP	60	Who has 192.168.31.64? Tell 192.168.31
3	0.051470	0.015426	G-ProCom_2a:d0:3d	Broadcast	ARP	60	Who has 192.168.31.70? Tell 192.168.31
4	0.128241	0.076771	192.168.31.122	224.0.0.22	IGMPv2	60	Membership Report group 224.0.0.22
5	0.128549	0.000308	192.168.31.121	224.0.0.22	IGMPv2	60	Membership Query, specific for group 2
6	0.128552	0.000003	192.168.31.121	224.0.1.60	IGMPv2	60	Membership Query, specific for group 2
7	0.129208	0.000656	192.168.31.1	224.0.0.22	IGMPv2	60	Membership Report group 224.0.0.22
8	0.180513	0.051305	ZyxelCom_5e:45:09	Broadcast	0x8899	60	Realtek Layer 2 Protocols
9	0.304923	0.124410	192.168.31.124	89.207.16.157	TCP	54	50904 → 443 [RST, ACK] Seq=1 Ack=1 Win
10	0.305951	0.001028	192.168.31.124	8.8.8.8	DNS	83	Standard query 0xa8b2 A col.eum-appdyn
11	0.332208	0.0262					
12	0.336292	0.0040					
13	0.336910	0.0006					
14	0.369040	0.0321					
15	0.369191	0.0001					

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0 at 192.168.31.121 (Intel PRO/100 MT Desktop) with driver e1000e at 2019-01-10 10:45:09 UTC

- Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0 at 192.168.31.121 (Intel PRO/100 MT Desktop) with driver e1000e at 2019-01-10 10:45:09 UTC
- Ethernet II, Src: Shenz (192.168.31.121), Dst: 224.0.0.2 (224.0.0.2) [ethertype IPv4 (0x0800), length 480]
- Internet Protocol Version 4 Version: 4 (IPv4 header), Src: Shenz (192.168.31.121), Dst: All nodes (224.0.0.2) [length 40]
- Internet Group Management Version: 2 (IGMP header), Type: Membership Report (0x0001), Group: 224.0.0.2 [length 16]

Wireshark · Preferences

Appearance

Columns

Displayed	Title	Type	Fields	Field
<input checked="" type="checkbox"/>	No.	Number		
<input checked="" type="checkbox"/>	Time	Time (format as specified)		
<input checked="" type="checkbox"/>	DTime	Delta time displayed		
<input checked="" type="checkbox"/>	Source	Source address		
<input checked="" type="checkbox"/>	Destination	Destination address		
<input checked="" type="checkbox"/>	Protocol	Protocol		
<input checked="" type="checkbox"/>	Length	Packet length (bytes)		
<input checked="" type="checkbox"/>	Info	Information		

+ -

Help Cancel OK

## Packet not routed - elke hop TTI -1

No.	Time	Delta	Source	Destination	Protocol	Length	Window size value	Info
1	10.000000	0.000000	10.0.0.102	198.238.212.10	TCP	66	65535	1490
2	10.007276	0.007276	10.0.0.102	198.238.212.10	TCP	66	65535 [TCP]	
3	10.014515	0.014515	198.238.212.10	10.0.0.102	TCP	66	8760	80
4	10.021855	0.000064	10.0.0.102	198.238.212.10	TCP	64	65535	1490
5	10.022128	0.000273	10.0.0.102	198.238.212.10	HTTP	338	65535	GET
6	10.046088	0.023960	198.238.212.10	10.0.0.102	HTTP	308	17240	HTTP
7	10.047936	0.001848	198.238.212.10	10.0.0.102	TCP	600	17240	80
8	10.047957	0.000021	198.238.212.10	10.0.0.102	TCP	64	17240	80
9	10.047994	0.000037	10.0.0.102	198.238.212.10	TCP	64	64743	1490
10	10.050908	0.002914	10.0.0.102	198.238.212.10	TCP	64	64743	1490
11	10.065627	0.014719	198.238.212.10	10.0.0.102	TCP	64	17240	80

▷ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 48  
Identification: 0x310d (12557)  
Flags: 0x02 (Don't Fragment)  
Fragment offset: 0  
Time to live: 128  
Protocol: TCP (6)  
Header checksum: 0x245c [validation disabled]

## Filteren op bad TCP

Ethernet: en0

tcp.analysis.flags

No.	Time	DTime	Source	Destination	Protocol	Length
35	0.850034	0.000000	192.168.31.124	185.82.210.189	TCP	14
45	1.075858	0.225824	192.168.31.124	172.217.19.206	TCP	14
90	1.772926	0.697068	52.114.75.29	192.168.31.124	TCP	14
109	2.092825	0.319899	108.177.126.189	192.168.31.124	TLSv1...	2
112	2.093018	0.000193	192.168.31.124	108.177.126.189	TCP	14
113	2.093018	0.000000	192.168.31.124	108.177.126.189	TCP	14
116	2.095274	0.002256	108.177.126.189	192.168.31.124	TLSv1...	1
119	2.102018	0.006744	108.177.126.189	192.168.31.124	TCP	2
121	2.102336	0.000318	108.177.126.189	192.168.31.124	TCP	7
134	2.711322	0.608986	151.101.2.49	192.168.31.124	TCP	15
137	2.711431	0.000109	192.168.31.124	151.101.2.49	TCP	1
139	2.711562	0.000131	192.168.31.124	151.101.2.49	TCP	1
141	2.711729	0.000167	192.168.31.124	151.101.2.49	TCP	1
142	2.711766	0.000037	151.101.2.49	192.168.31.124	TLSv1...	14
145	2.711944	0.000178	192.168.31.124	151.101.2.49	TCP	15
146	2.712070	0.000125	151.101.2.49	192.168.31.124	TCP	15

► Ethernet II, Src: Apple\_04:bc:28 (c4:2c:03:04:bc:28), Dst: BelkinIn\_88:a2:20 (94:10:...)

▼ Internet Protocol Version 4, Src: 192.168.31.124, Dst: 172.217.19.206  
0100 .... = Version: 4

Retransmission: opnieuw zenden van packets

Out Of order: volgorde packets reversed of packet not captured Dup Ack = Hey server, I'm missing a packet!

KeepAlive = Hey, leef je nog?

Meer informatie:

<https://www.youtube.com/watch?v=15wDU3Wx1h0>



Wireshark oefeningen:

Les 2 Wireshark oefeningen.pdf