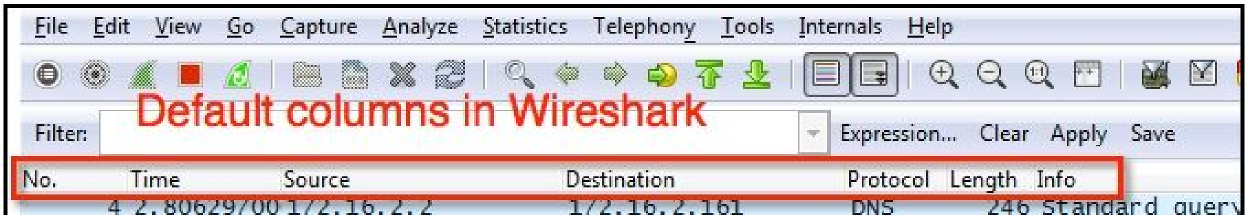
Wireshark Column Display

Source : - MalwareTrafficAnalysis

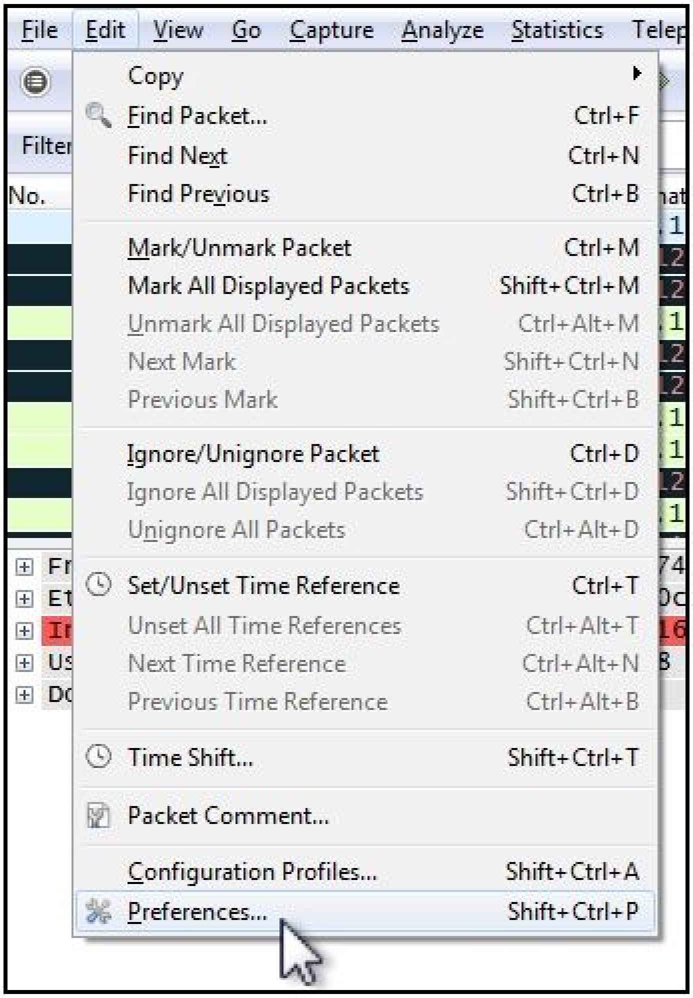
CHANGING THE COLUMN DISPLAY IN WIRESHARK → The default columns for Wireshark are: Packet number, Time, Source, Destination, Protocol, Length, and Info (as shown below):


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

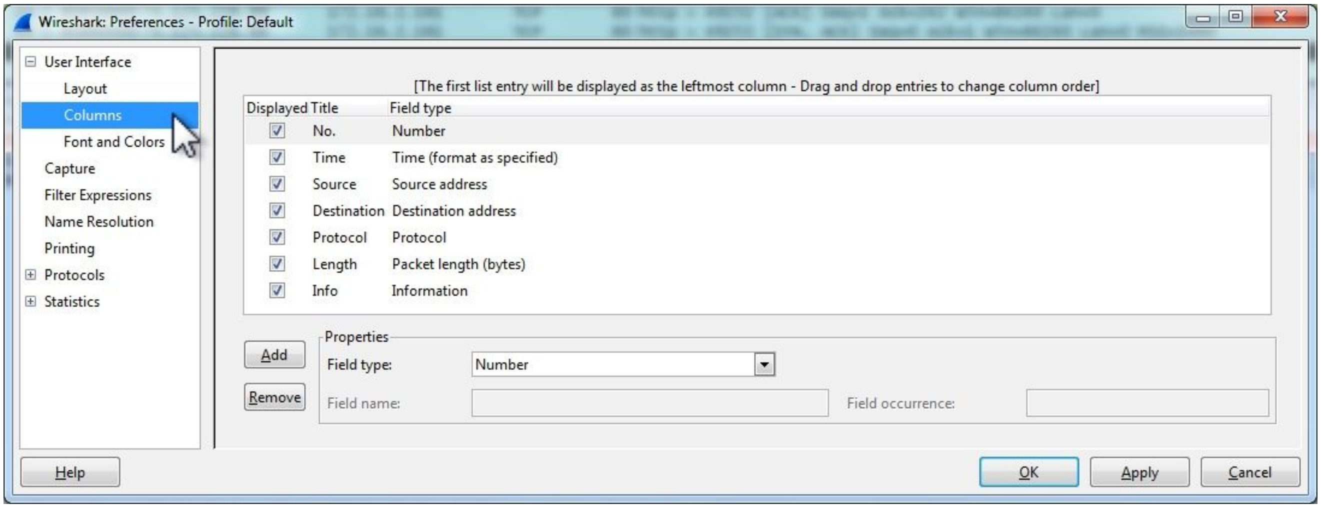
Default columns in Wireshark

```
No.      Time         Source          Destination          Protocol Length Info
   4 2.80629700 172.16.2.2     172.16.2.161         DNS       246 Standard query
```

Let's change this by editing our preferences (edit --> Preferences):


File Edit View Go Capture Analyze Statistics Telep
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet Ctrl+M
Mark All Displayed Packets Shift+Ctrl+M
Unmark All Displayed Packets Ctrl+Alt+M
Next Mark Shift+Ctrl+N
Previous Mark Shift+Ctrl+B
Ignore/Unignore Packet Ctrl+D
Ignore All Displayed Packets Shift+Ctrl+D
Unignore All Packets Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Shift+Ctrl+T
Packet Comment...
Configuration Profiles... Shift+Ctrl+A
Preferences... Shift+Ctrl+P
Filter
No.

From the Wireshark Preferences menu, select columns:



[The first list entry will be displayed as the leftmost column - Drag and drop entries to change column order]

Displayed	Title	Field type
☑	No.	Number
☑	Time	Time (format as specified)
☑	Source	Source address
☑	Destination	Destination address
☑	Protocol	Protocol
☑	Length	Packet length (bytes)
☑	Info	Information

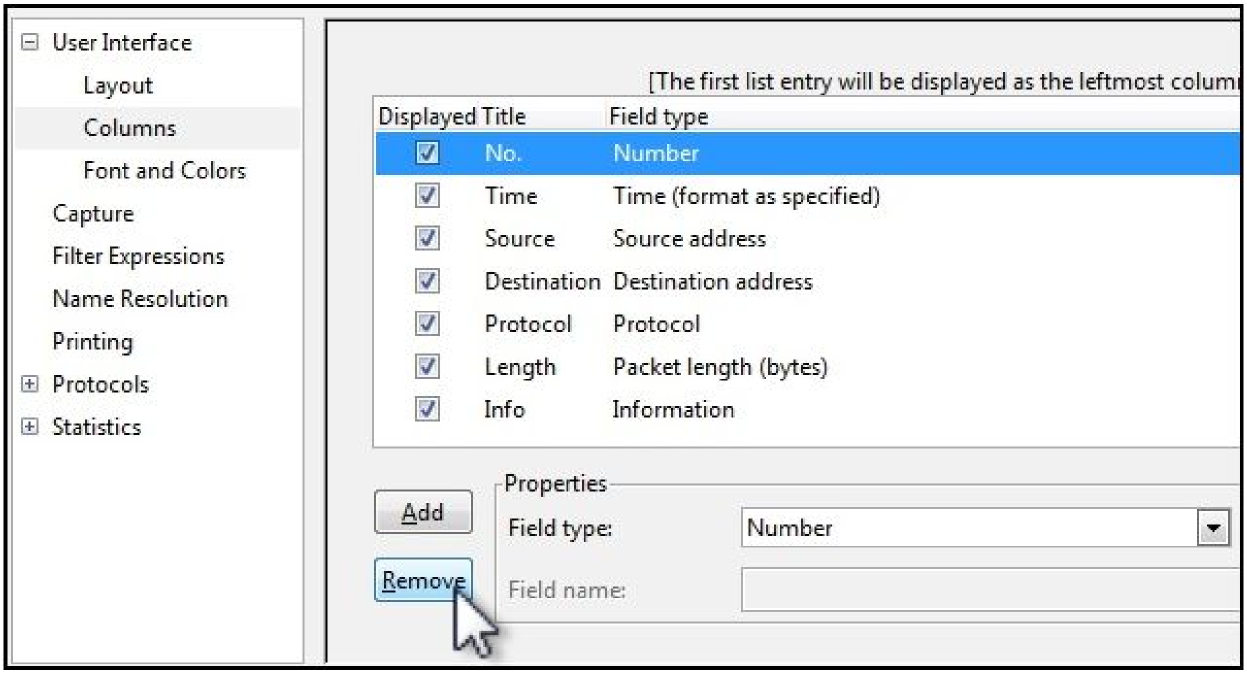
Properties

Field type: Number

Field name:

Field occurrence:

From there, we're going to remove the first column, which is the "Number" (lists the current packet number you're viewing in the PCAP):



[The first list entry will be displayed as the leftmost colum

Displayed	Title	Field type
☑	No.	Number
☑	Time	Time (format as specified)
☑	Source	Source address
☑	Destination	Destination address
☑	Protocol	Protocol
☑	Length	Packet length (bytes)
☑	Info	Information

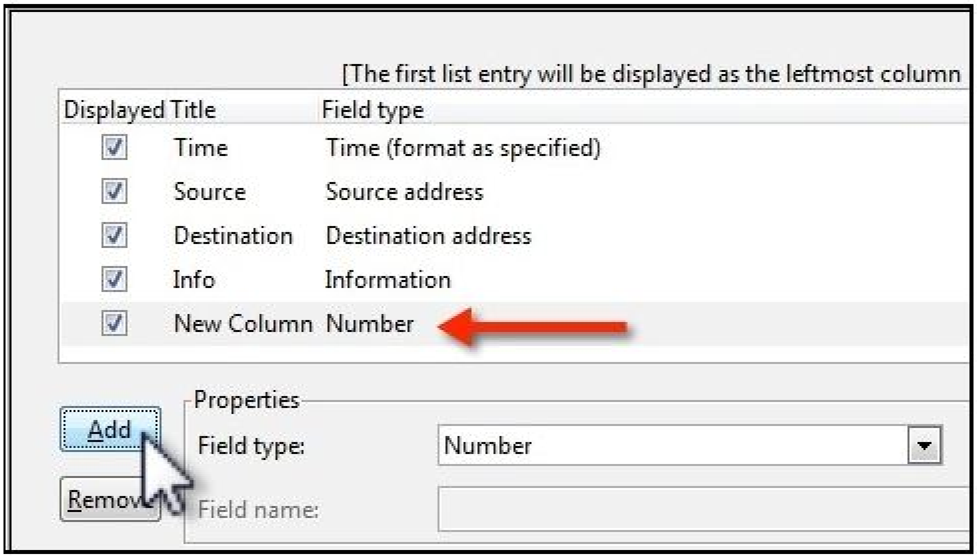
Properties

Field type: Number

Field name:

After that, I also remove Protocol and Length columns.

Next, we'll add some new columns, as shown below:



[The first list entry will be displayed as the leftmost column

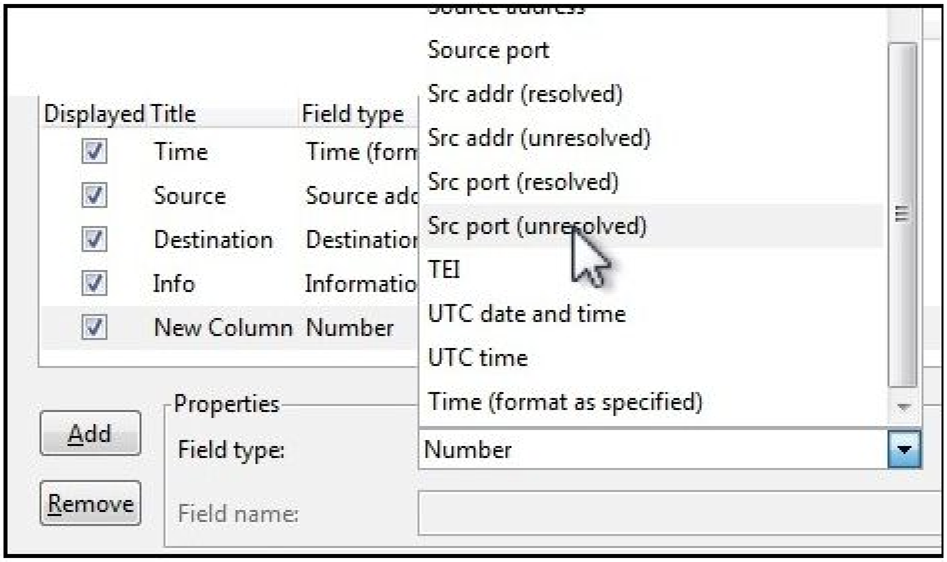
Displayed	Title	Field type
☑	Time	Time (format as specified)
☑	Source	Source address
☑	Destination	Destination address
☑	Info	Information
☑	New Column	Number

Properties

Field type: Number

Field name:

The first new column to add is the source port. You'll want to select ***Src port (unresolved)*** so you can see the port number. Otherwise, it'll show whatever server is associated with that port instead of the number.



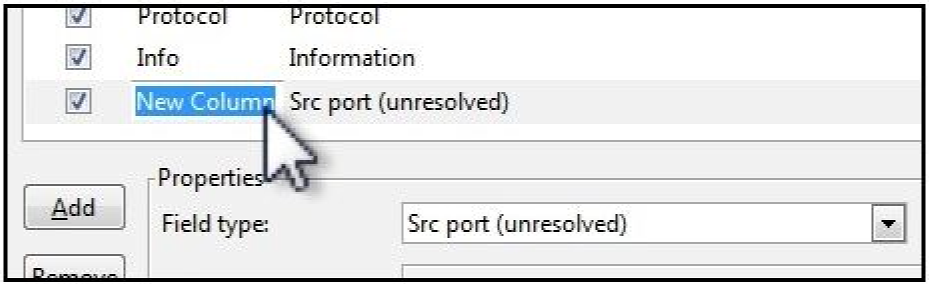
Displayed	Title	Field type
☑	Time	Time (form
☑	Source	Source adc
☑	Destination	Destinatior
☑	Info	Informatio
☑	New Column	Number

Properties

Field type: Number

Field name:

The default name of any new columns is "New Column", so change the name of that new column.

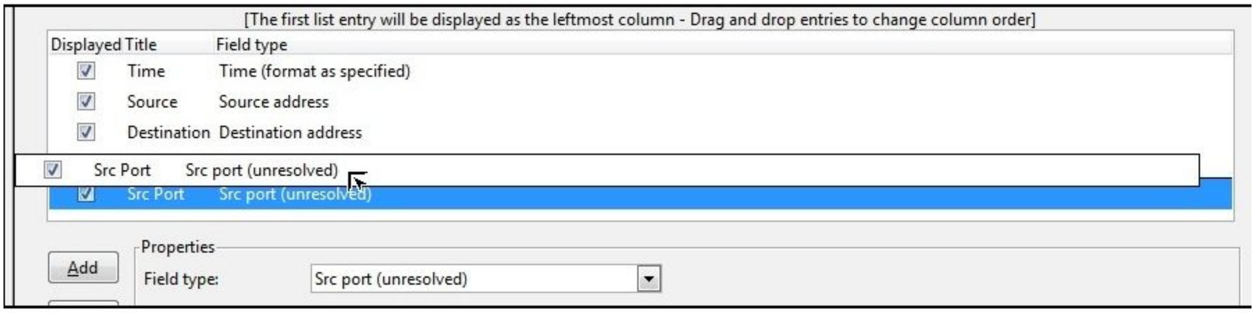


☑	Protocol	Protocol
☑	Info	Information
☑	New Column	Src port (unresolved)

Properties

Field type: Src port (unresolved)

Once you've changed the name, you can left-click and drag that column to the location you choose. We'll put it after the Source address.



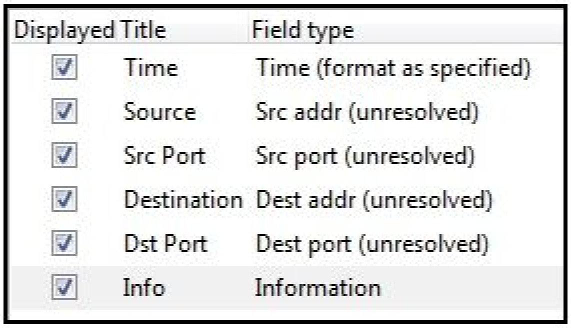
[The first list entry will be displayed as the leftmost column - Drag and drop entries to change column order]

	Displayed Title	Field type
☑	Time	Time (format as specified)
☑	Source	Source address
☑	Destination	Destination address
☑	Src Port	Src port (unresolved)
☑	Src Port	Src port (unresolved)

Properties

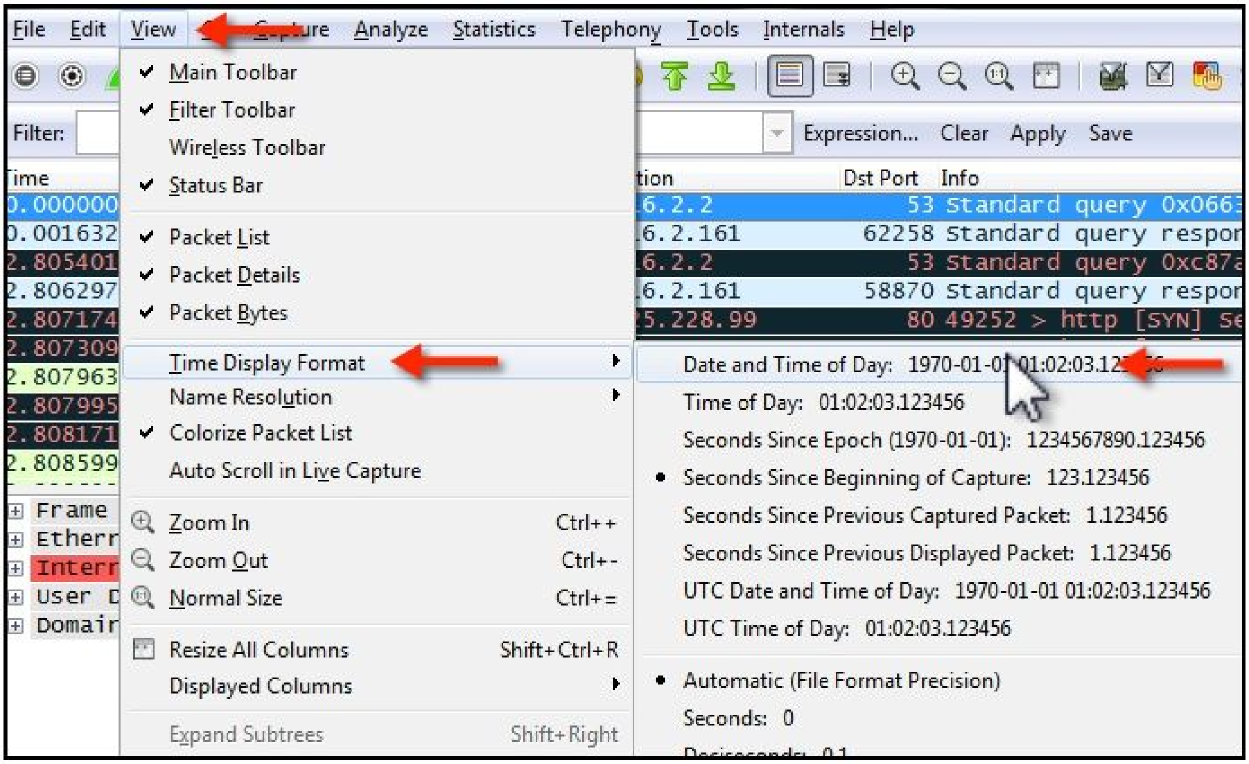
Field type: Src port (unresolved)

After a few additions and column changes, here's the setup that I use. Notice how the Source and Destination addresses are changed to an "unresolved" field type.



	Displayed Title	Field type
☑	Time	Time (format as specified)
☑	Source	Src addr (unresolved)
☑	Src Port	Src port (unresolved)
☑	Destination	Dest addr (unresolved)
☑	Dst Port	Dest port (unresolved)
☑	Info	Information

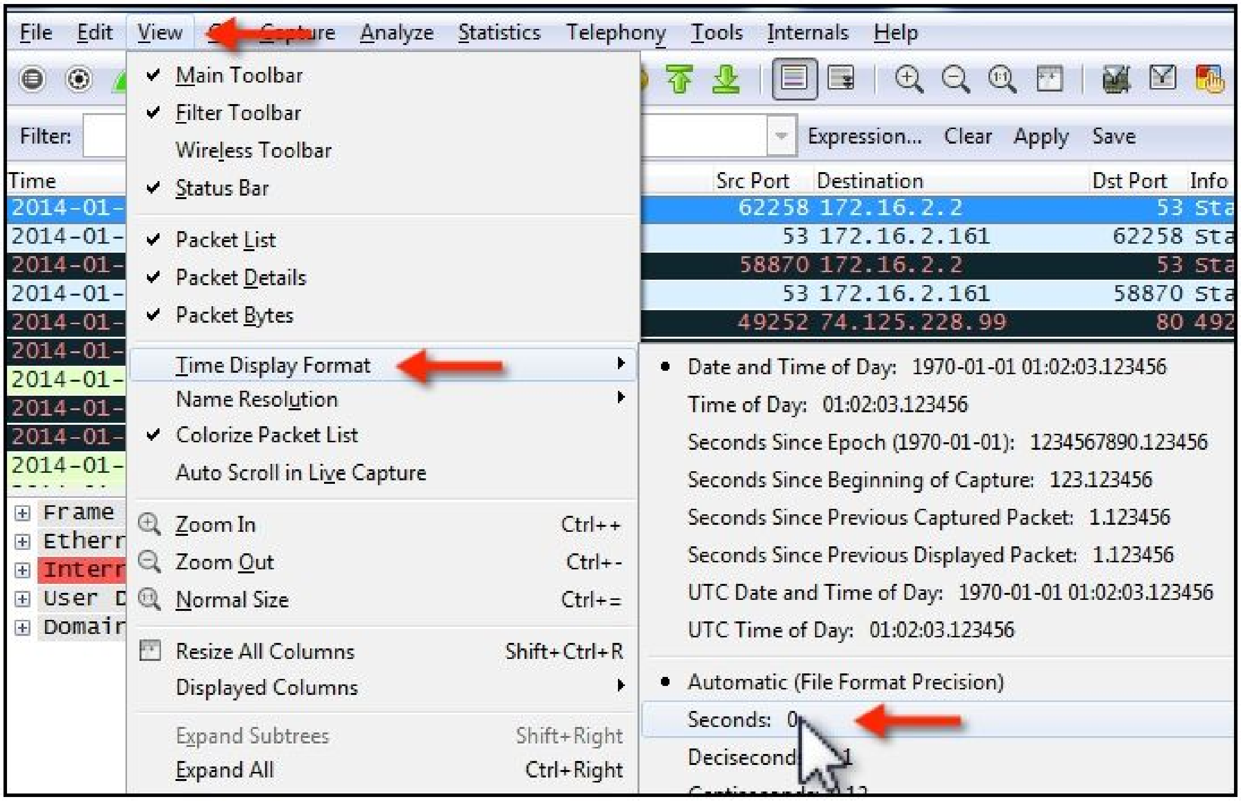
Now let's fix the time. The default format is "Seconds Since Beginning Capture". Let's change it to "Date and Time of Day". Go to: View --> Time Display Format --> Date and Time of Day.



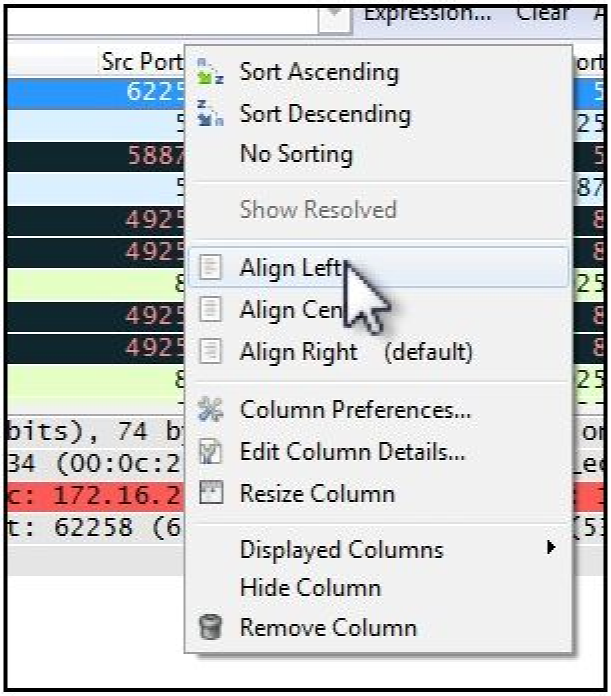
File
Edit
View
Capture
Analyze
Statistics
Telephony
Tools
Internals
Help
Filter:
Expression...
Clear
Apply
Save
Main Toolbar
Filter Toolbar
Wireless Toolbar
Status Bar
Packet List
Packet Details
Packet Bytes
Time Display Format
Name Resolution
Colorize Packet List
Auto Scroll in Live Capture
Zoom In Ctrl++
Zoom Out Ctrl+-
Normal Size Ctrl+=
Resize All Columns Shift+Ctrl+R
Displayed Columns
Expand Subtrees Shift+Right
Date and Time of Day: 1970-01-01 01:02:03.123456
Time of Day: 01:02:03.123456
Seconds Since Epoch (1970-01-01): 1234567890.123456
Seconds Since Beginning of Capture: 123.123456
Seconds Since Previous Captured Packet: 1.123456
Seconds Since Previous Displayed Packet: 1.123456
UTC Date and Time of Day: 1970-01-01 01:02:03.123456
UTC Time of Day: 01:02:03.123456
Automatic (File Format Precision)
Seconds: 0
Deciseconds: 0.1
Time
tion
Dst Port
Info
Frame
Etherr
Interr
User D
Domair

```
0.000000   6.2.2        53 Standard query 0x066
0.001632   6.2.161   62258 Standard query respon
2.805401   6.2.2        53 Standard query 0xc87a
2.806297   6.2.161   58870 Standard query respon
2.807174   5.228.99     80 49252 > http [SYN] Se
2.807309
2.807963
2.807995
2.808171
2.808599
```

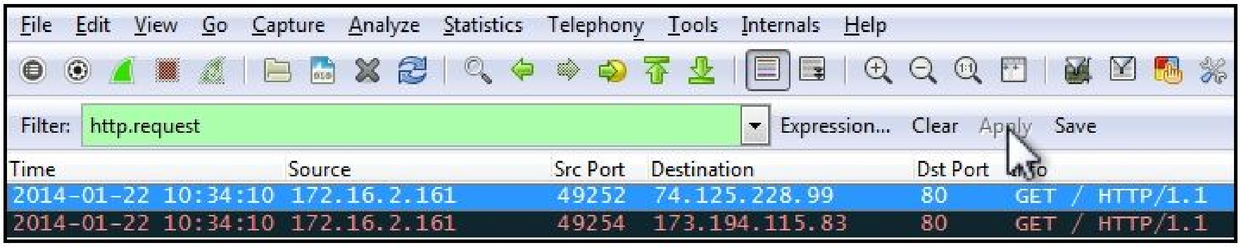
After that, we'll change the precision of the displayed time from automatic to "Seconds", as shown below (View --> Time Display Format --> select "Seconds: 0"):


File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Internals
Help
✓ Main Toolbar
✓ Filter Toolbar
Wireless Toolbar
✓ Status Bar
✓ Packet List
✓ Packet Details
✓ Packet Bytes
Time Display Format
Name Resolution
✓ Colorize Packet List
Auto Scroll in Live Capture
Zoom In Ctrl++
Zoom Out Ctrl+-
Normal Size Ctrl+=
Resize All Columns Shift+Ctrl+R
Displayed Columns
Expand Subtrees Shift+Right
Expand All Ctrl+Right
● Date and Time of Day: 1970-01-01 01:02:03.123456
Time of Day: 01:02:03.123456
Seconds Since Epoch (1970-01-01): 1234567890.123456
Seconds Since Beginning of Capture: 123.123456
Seconds Since Previous Captured Packet: 1.123456
Seconds Since Previous Displayed Packet: 1.123456
UTC Date and Time of Day: 1970-01-01 01:02:03.123456
UTC Time of Day: 01:02:03.123456
● Automatic (File Format Precision)
Seconds: 0
Deciseconds: 0.1
Filter:
Expression...
Clear
Apply
Save
Time
Src Port
Destination
Dst Port
Info
2014-01-
62258 172.16.2.2 53 Sta
53 172.16.2.161 62258 Sta
58870 172.16.2.2 53 Sta
53 172.16.2.161 58870 Sta
49252 74.125.228.99 80 492
Frame
Etherr
Interr
User D
Domair

Some of the columns are aligned to the right, which we can fix by right-clicking on the column and selecting the proper alignment:



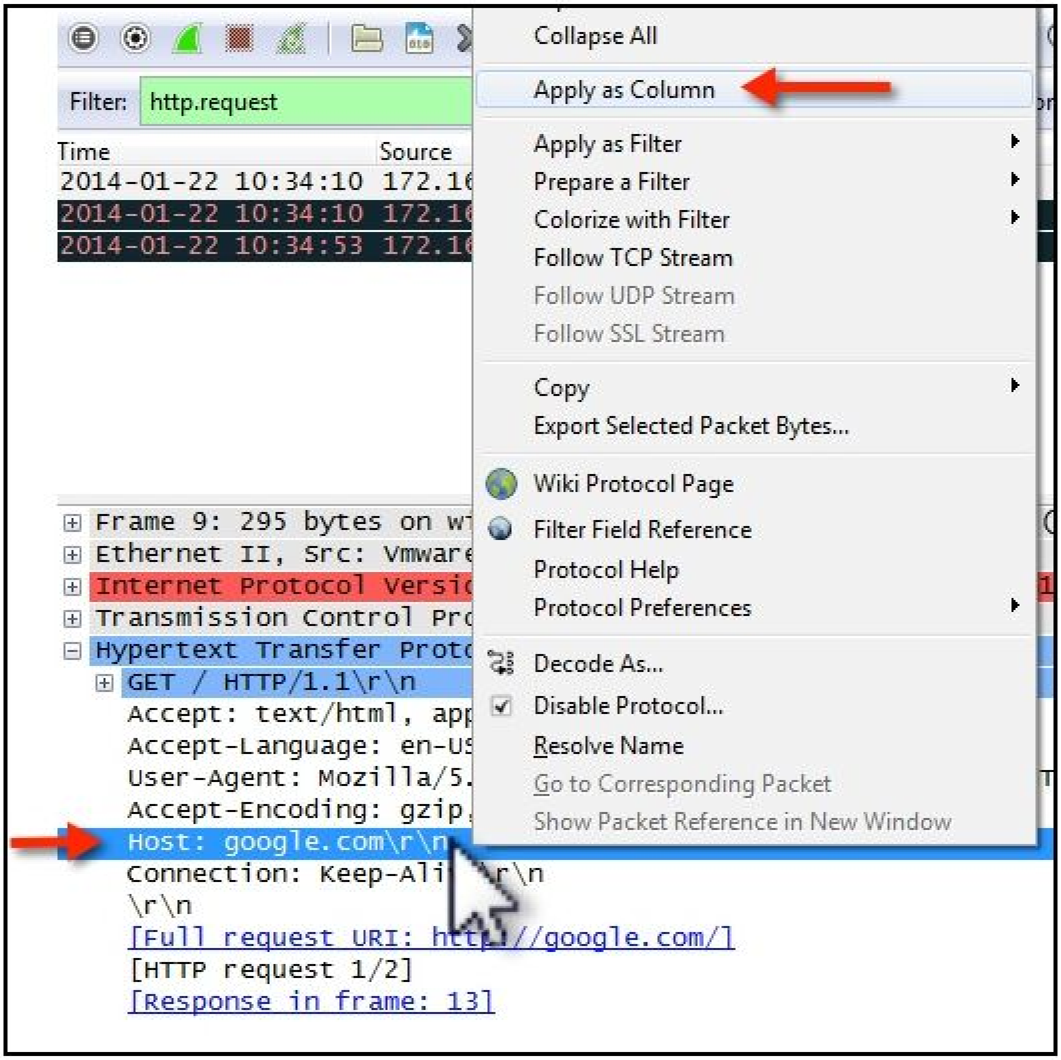
Now we have everything, but I also want to see the **http.host** name as one of the columns. To do that, let's filter on **http.request**, so we're only seeing the HTTP requests.


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: http.request

```
Time                 Source        Src Port  Destination     Dst Port  Info
2014-01-22 10:34:10  172.16.2.161  49252     74.125.228.99   80        GET / HTTP/1.1
2014-01-22 10:34:10  172.16.2.161  49254     173.194.115.83  80        GET / HTTP/1.1
```

Expand the breakout in the middle section, so you see the Host: line in the HTTP header. Right-click on that, and select "Apply as Column" from the menu.

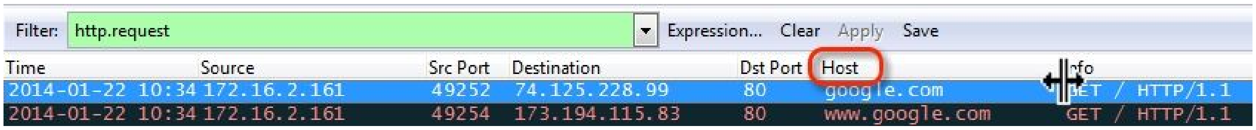


Filter: http.request

```
Time                 Source
2014-01-22 10:34:10  172.16
2014-01-22 10:34:10  172.16
2014-01-22 10:34:53  172.16
```

```
⊞ Frame 9: 295 bytes on wi
⊞ Ethernet II, Src: Vmware
⊞ Internet Protocol Versio
⊞ Transmission Control Pro
⊟ Hypertext Transfer Proto
  ⊞ GET / HTTP/1.1\r\n
    Accept: text/html, app
    Accept-Language: en-US
    User-Agent: Mozilla/5.
    Accept-Encoding: gzip,
    Host: google.com\r\n
    Connection: Keep-Ali  \r\n
    \r\n
    [Full request URI: http://google.com/]
    [HTTP request 1/2]
    [Response in frame: 13]
```

You'll notice now that the HTTP host from the GET or POST requests is now shown as a column. You might have to widen the column to see the whole name.



Filter: http.request

Time	Source	Src Port	Destination	Dst Port	Host	Info
2014-01-22 10:34	172.16.2.161	49252	74.125.228.99	80	google.com	GET / HTTP/1.1
2014-01-22 10:34	172.16.2.161	49254	173.194.115.83	80	www.google.com	GET / HTTP/1.1