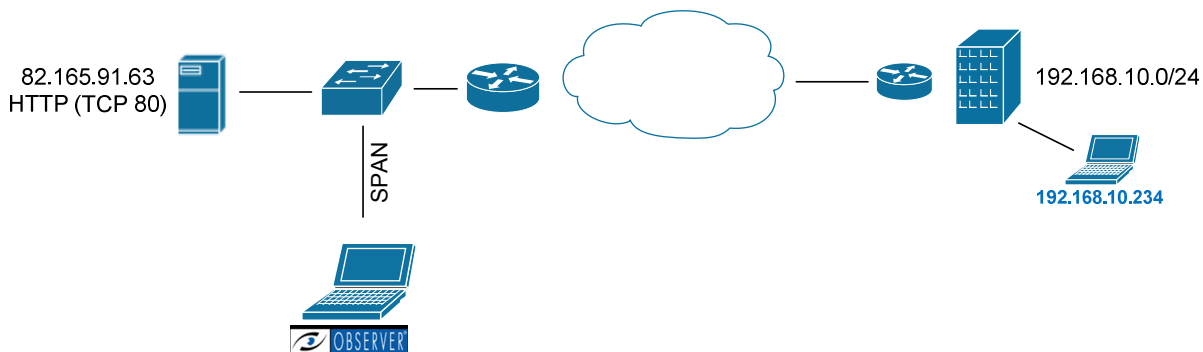


This document outlines the steps to create a filter for syn and syn-ack packets being captured by Observer from Network Instruments.

In my scenario, I want to verify SYN and SYN/ACK packets between those two hosts.



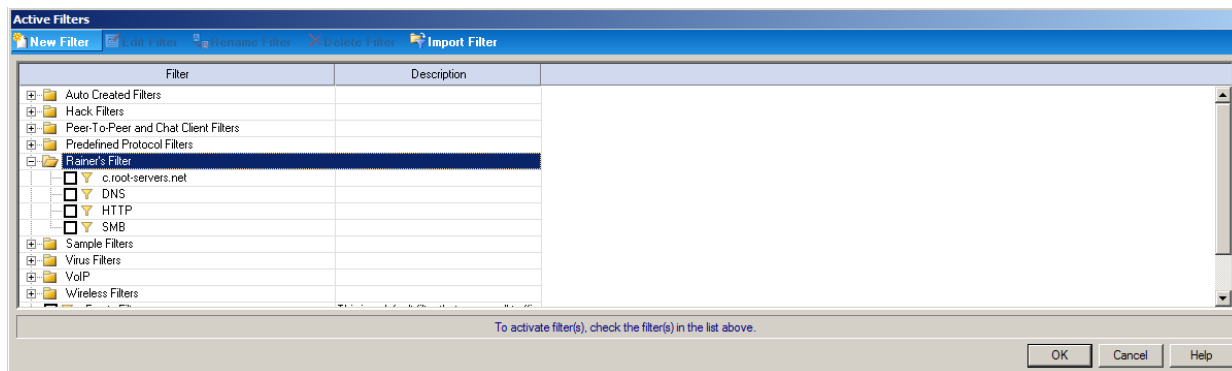
I am not interested in capturing all kind of data, just the two of them.

Start Observer and make sure you are connected with the SPAN port.

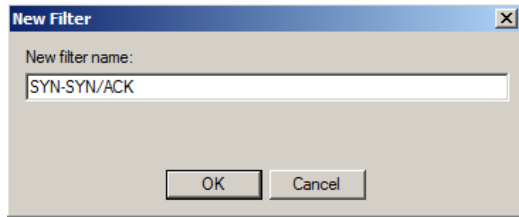
Click on Filter



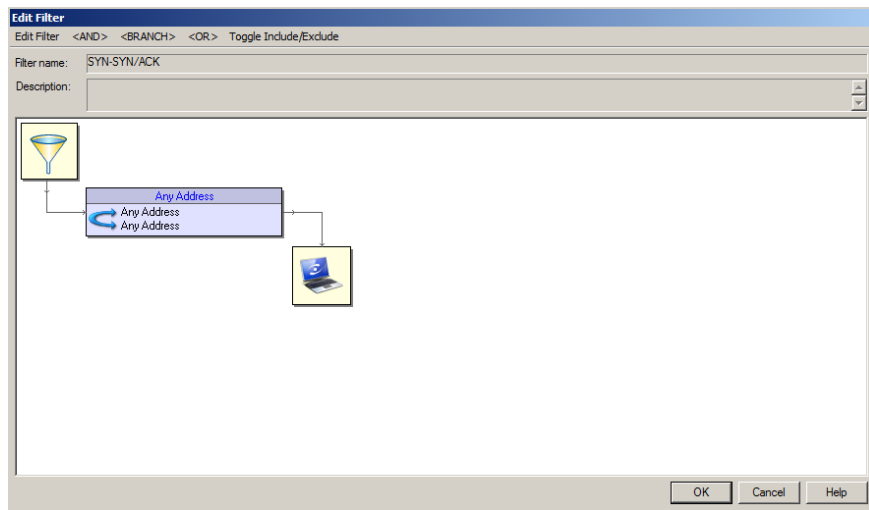
Click on New Filter (you may want to choose predefined Folder)



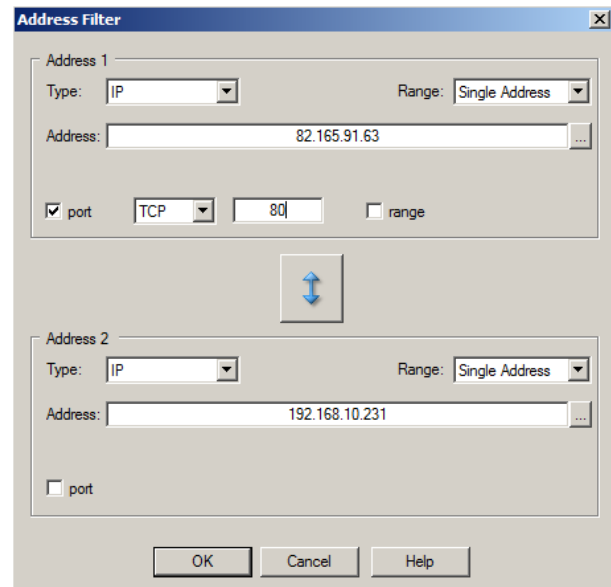
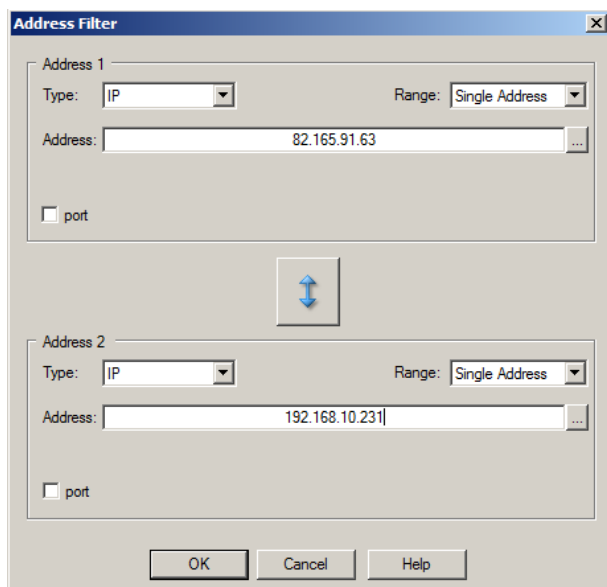
Give it a descriptive name



The filter editor will open and a standard filter is being provided

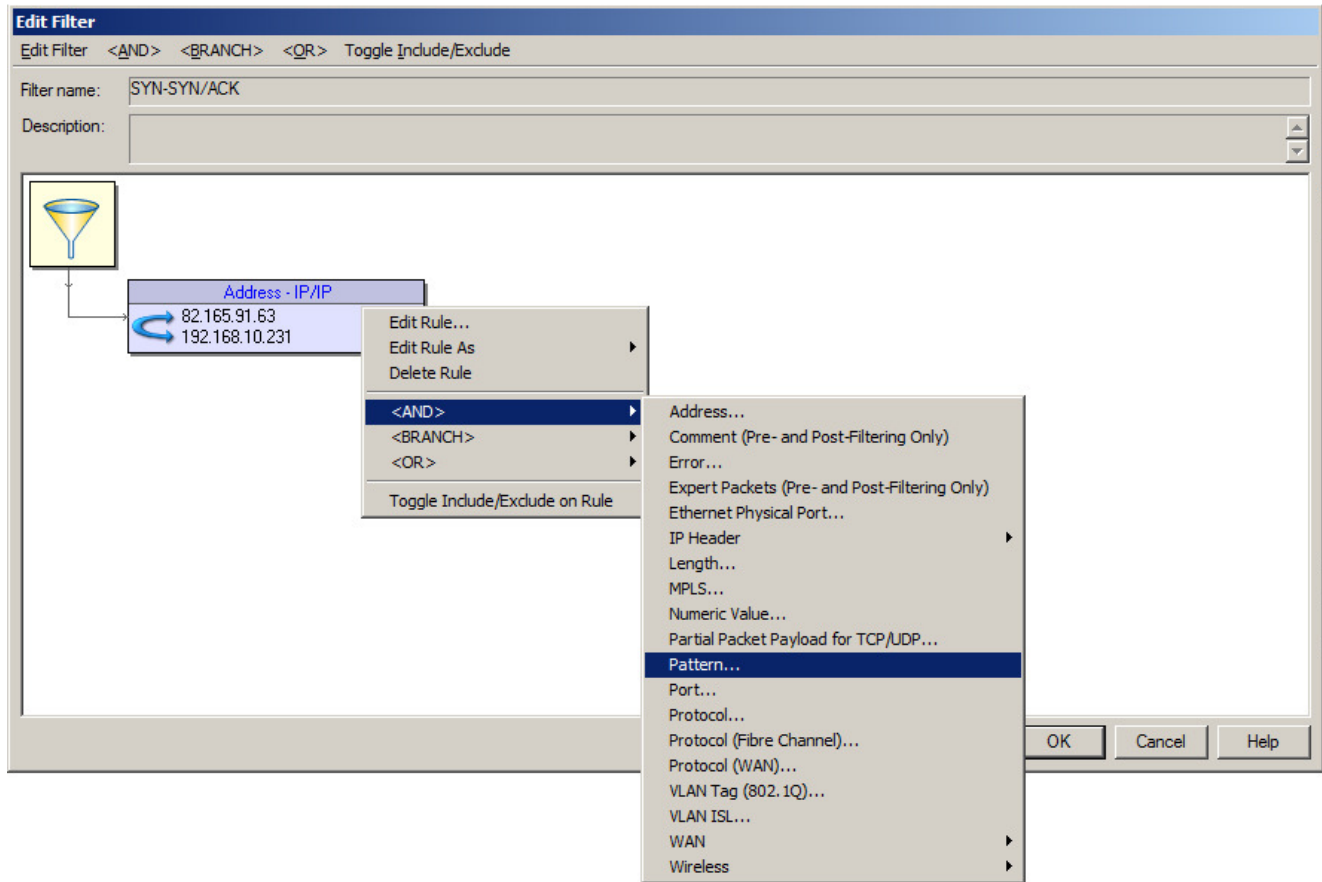


Change the Type from Hardware to IP and provide IP address pair, you want to monitor.

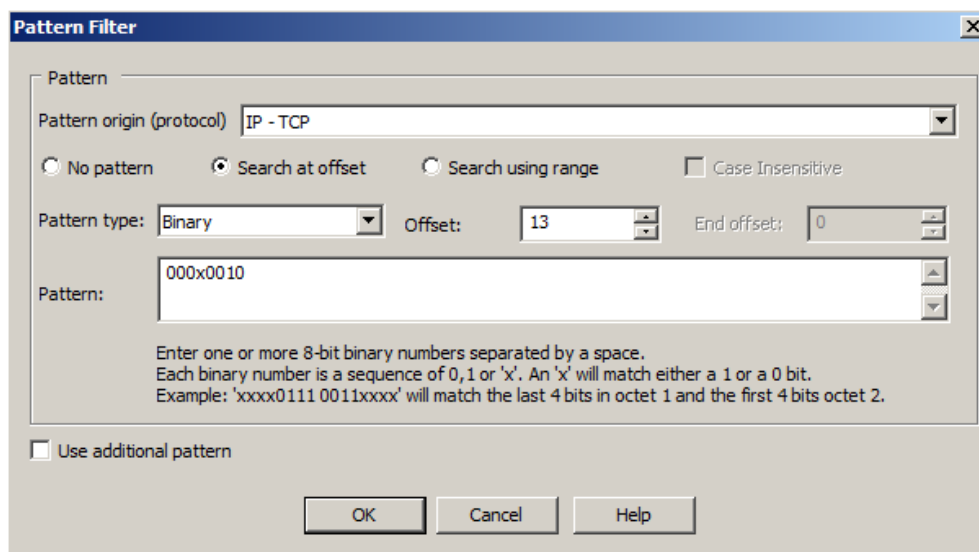


I also active the port on the server side and added TCP port 80 for HTTP Traffic

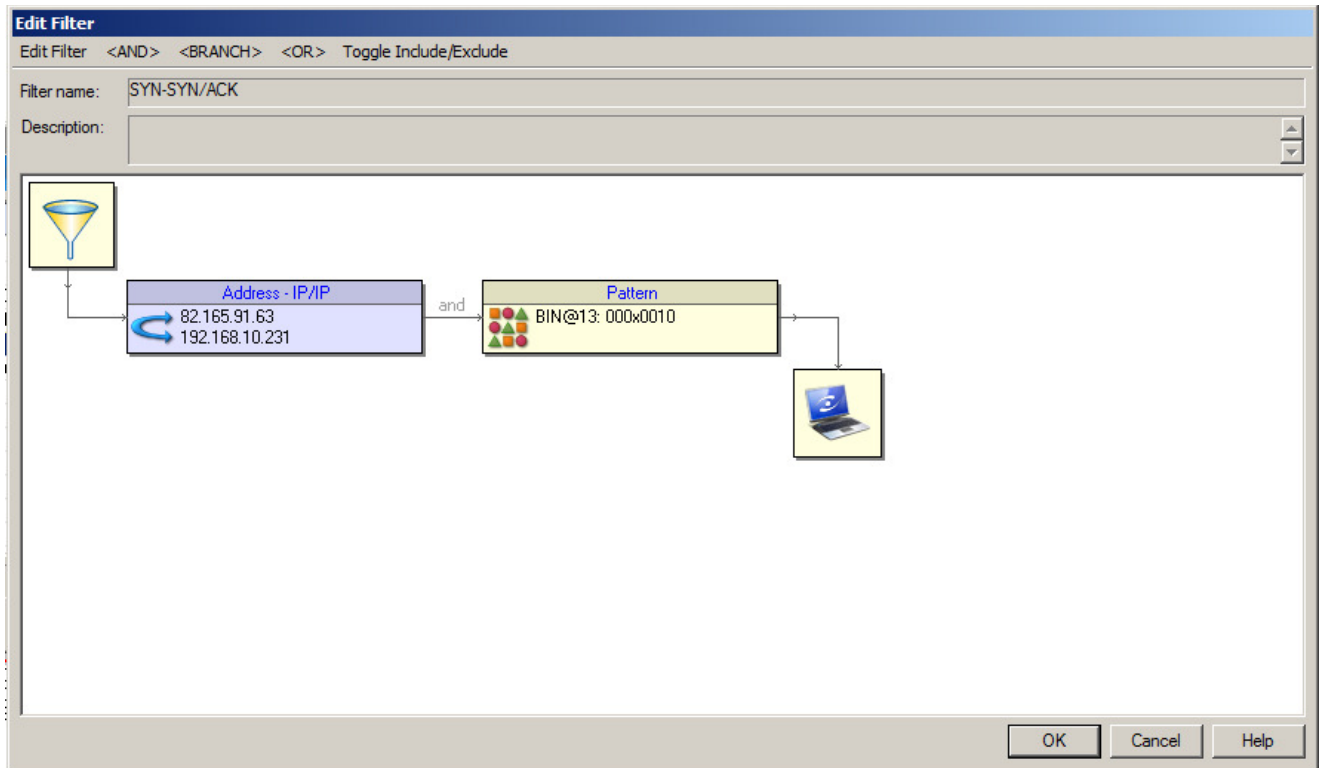
The filter has been created. Now roll-over with the mouse pointer on the filter and right-click to add another filter



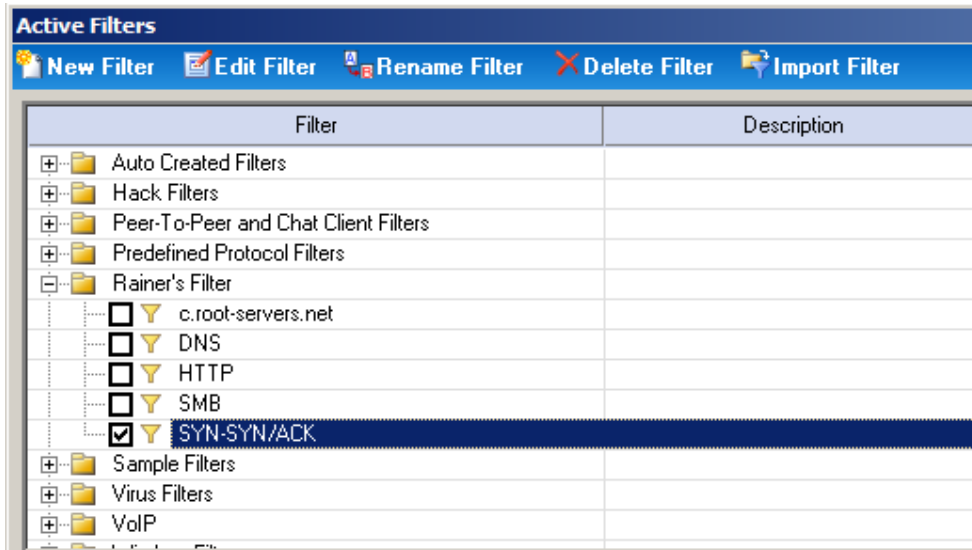
To capture SYN and SYN/ACK Packets you need to add following Pattern to the previous filter



The complete filter looks like that



Now, you want to use the newly created filter. To activate the filter, mark the checkbox



Click on Start. The yellow indicate captured packets.



The screenshot shows the 'Decode and Analysis from Probe - Instance 1 / Local Observer' window. It displays a list of 24 selected packets. The columns include Pkt, Source, Destination, Size, Date, Day Time, Diff Time, Relative Time, and Summary. An arrow points from the highlighted packet in the table to the summary view below.

Pkt	Source	Destination	Size	Date	Day Time	Diff Time	Relative Time	Summary
24	cupertino	kundenserver.de	70	2/20/2012	17h:26m 38.273 673s	0.0273374	12.645324	TCP SYN [53385 -> 80] ---- IP [192.168.10.231 -> 82.165.91.63] ---- ETHERTYPE
25	cupertino	kundenserver.de	70	2/20/2012	17h:26m 38.273 893s	0.000 009	12.645333	TCP SYN [53384 -> 80] ---- IP [192.168.10.231 -> 82.165.91.63] ---- ETHERTYPE
26	kundenserver.de	cupertino	66	2/20/2012	17h:26m 38.291 182s	0.017 300	12.667233	TCP SYN ACK [80 -> 53385] ---- IP [82.165.91.63 -> 192.168.10.231] ---- ETHERTYPE
27	kundenserver.de	cupertino	66	2/20/2012	17h:26m 38.291 191s	0.000 009	12.667242	TCP SYN ACK [80 -> 53384] ---- IP [82.165.91.63 -> 192.168.10.231] ---- ETHERTYPE
28	cupertino	kundenserver.de	70	2/20/2012	17h:26m 38.320 462s	0.029 271	12.696513	TCP SYN [53388 -> 80] ---- IP [192.168.10.231 -> 82.165.91.63] ---- ETHERTYPE
29	cupertino	kundenserver.de	70	2/20/2012	17h:26m 38.324 458s	0.003 996	12.700509	TCP SYN [53389 -> 80] ---- IP [192.168.10.231 -> 82.165.91.63] ---- ETHERTYPE
30	cupertino	kundenserver.de	70	2/20/2012	17h:26m 38.324 465s	0.000 007	12.700516	TCP SYN [53390 -> 80] ---- IP [192.168.10.231 -> 82.165.91.63] ---- ETHERTYPE
31	kundenserver.de	cupertino	66	2/20/2012	17h:26m 38.333 798s	0.009 323	12.709330	TCP SYN ACK [80 -> 53388] ---- IP [82.165.91.63 -> 192.168.10.231] ---- ETHERTYPE
32	kundenserver.de	cupertino	66	2/20/2012	17h:26m 38.336 438s	0.002 651	12.712489	TCP SYN ACK [80 -> 53389] ---- IP [82.165.91.63 -> 192.168.10.231] ---- ETHERTYPE
33	kundenserver.de	cupertino	66	2/20/2012	17h:26m 38.344 429s	0.007 990	12.720480	TCP SYN ACK [80 -> 53390] ---- IP [82.165.91.63 -> 192.168.10.231] ---- ETHERTYPE

Summary

```
TCP SYN [53385 -> 80] ---- IP [192.168.10.231 -> 82.165.91.63] ---- ETHERTYPE
TCP SYN [53384 -> 80] ---- IP [192.168.10.231 -> 82.165.91.63] ---- ETHERTYPE
TCP SYN ACK [80 -> 53385] ---- IP [82.165.91.63 -> 192.168.10.231] ---- ETHERTYPE
TCP SYN ACK [80 -> 53384] ---- IP [82.165.91.63 -> 192.168.10.231] ---- ETHERTYPE
TCP SYN [53388 -> 80] ---- IP [192.168.10.231 -> 82.165.91.63] ---- ETHERTYPE
TCP SYN [53389 -> 80] ---- IP [192.168.10.231 -> 82.165.91.63] ---- ETHERTYPE
TCP SYN [53390 -> 80] ---- IP [192.168.10.231 -> 82.165.91.63] ---- ETHERTYPE
TCP SYN ACK [80 -> 53388] ---- IP [82.165.91.63 -> 192.168.10.231] ---- ETHERTYPE
TCP SYN ACK [80 -> 53389] ---- IP [82.165.91.63 -> 192.168.10.231] ---- ETHERTYPE
TCP SYN ACK [80 -> 53390] ---- IP [82.165.91.63 -> 192.168.10.231] ---- ETHERTYPE
```

