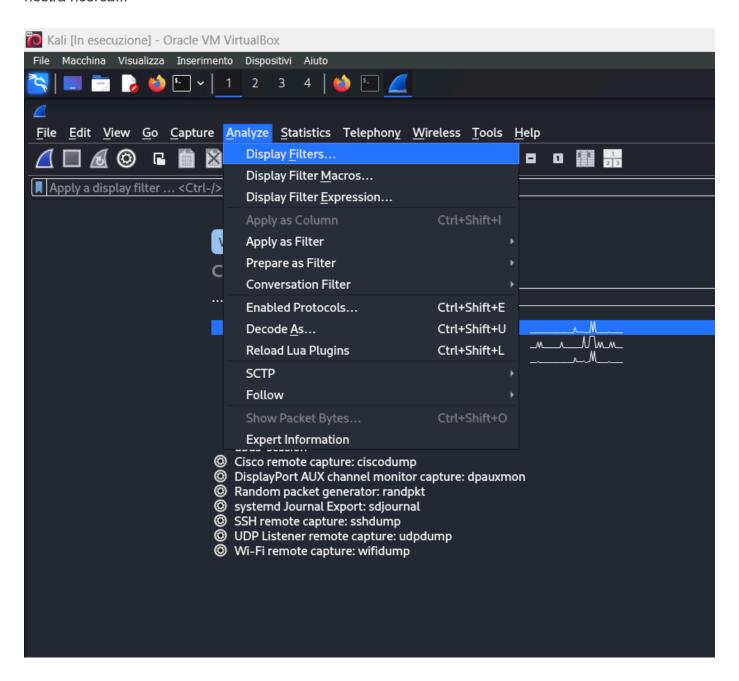
Analizziamo pacchetti TCP con Wire shark

Per prima cosa apriamo Wire shark e facciamoci un' idea di tutti i filtri che possiamo applicare alla nostra ricerca...

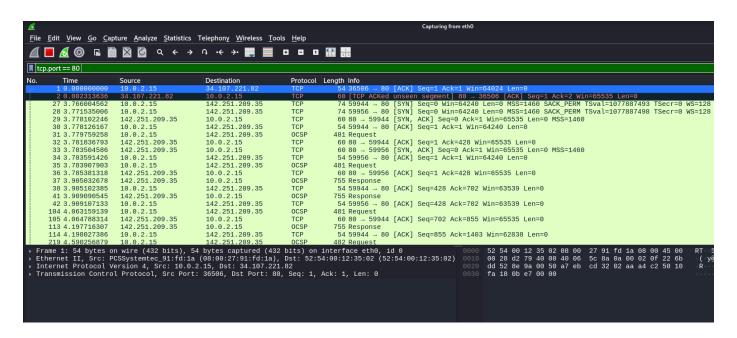


```
Wireshark · Display Filters
Filter Name

    Filter Expression

   Ethernet address 00:00:5e:00:53:00
                                               eth.addr == 00:00:5e:00:53:00
   Ethernet type 0x0806 (ARP)
                                               eth.type == 0x0806
   Ethernet broadcast
                                               eth.addr == ff:ff:ff:ff:ff
  No ARP
                                               not arp
  IPv4 only
  IPv4 address 192.0.2.1
                                               ip.addr == 192.0.2.1
  IPv4 address isn't 192.0.2.1
                                               ip.addr!=192.0.2.1
  IPv6 only
                                               ipv6
  IPv6 address 2001:db8::1
                                               ipv6.addr == 2001:db8::1
   TCP only
                                               tcp
  UDP only
                                               udp
  Non-DNS port
                                               !(udp.port == 53 || tcp.port == 53)
   TCP or UDP port is 80 (HTTP)
                                               tcp.port == 80 || udp.port == 80
   No ARP and no DNS
                                               not arp and not dns
   Non-HTTP and non-SMTP to/from 192.0.2.1 ip.addr == 192.0.2.1 and tcp.port not in {80, 25}
```

Dopo aver individuato il filtro piu' adatto alla nostra esigenza procediamo ad applicarlo nella barra di Wire shark.



In questa casistica particolare ho analizzato il traffico che creo connettendomi semplicemente al mio browser google, per avere info piu' nel dettaglio dei vari pacchetti selezionando la riga interessata e andando in basso a sinistra aprendo la tendina il software ci fornirà una panoramica molto piu' dettagliata dei pacchetti.

```
Frame 27: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_91:fd:1a (08:00:27:91:fd:1a), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.251.209.35

Transmission Control Protocol, Src Port: 59944, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 59944
    Destination Port: 80
    [Stream index: 3]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
    Sequence Number: 0
                                      (relative sequence number)
    Sequence Number (raw): 2103404263
    [Next Sequence Number: 1
Acknowledgment Number: 0
                                               (relative sequence number)]
    Acknowledgment number (raw): 0
   1010 .... = Header Length: 40 bytes (10) Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x6c5c [unverified]
[Checksum Status: Unverified]
    Urgent Pointer: 0
   Options: (20 bytes). Maximum seament size. SACK permitted. Timestamps. No-Operation (NOP). Window s.
 wireshark_eth0WGYA12.pcapng
```

Con questi semplici step potremo analizzare in modo piu' ordinato e aprofondito i nostri pacchetti TCP.