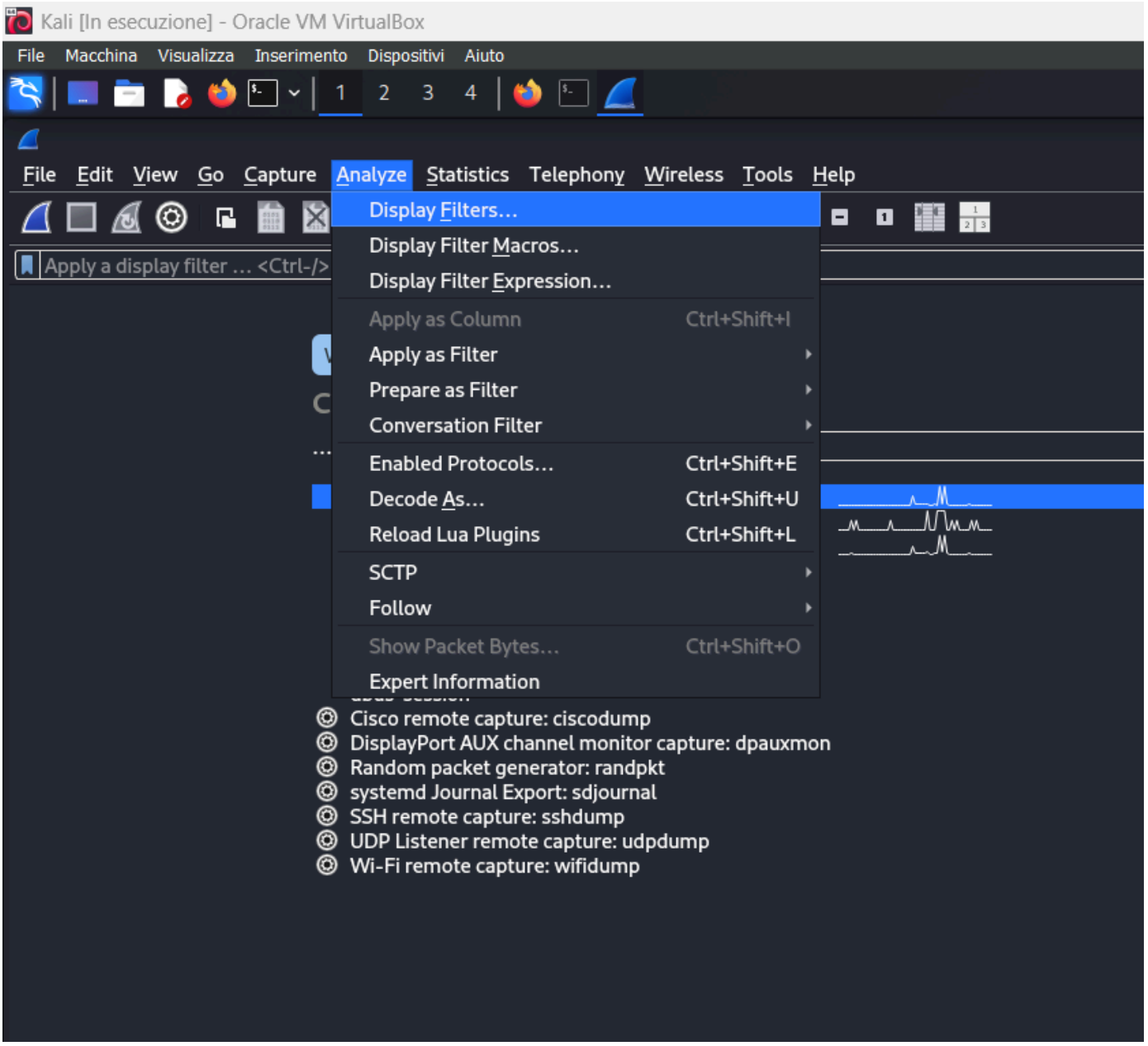
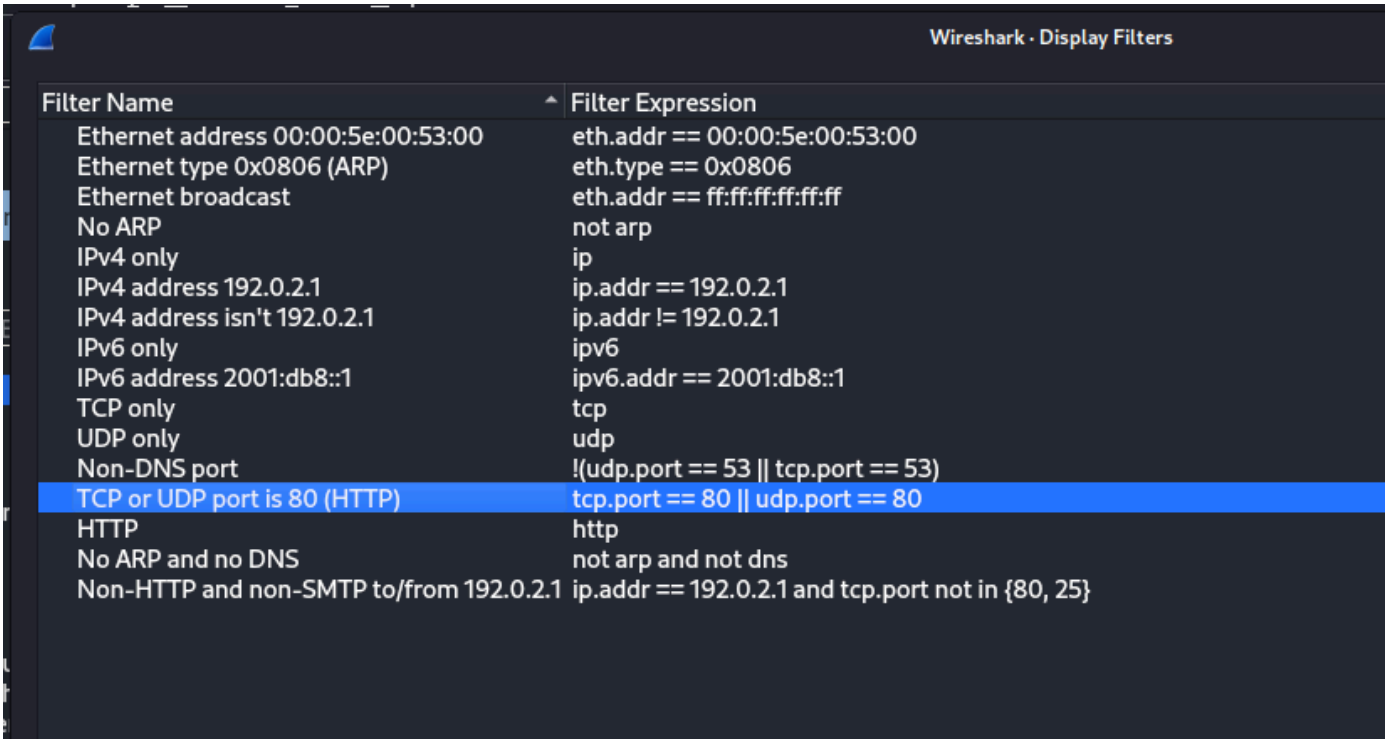
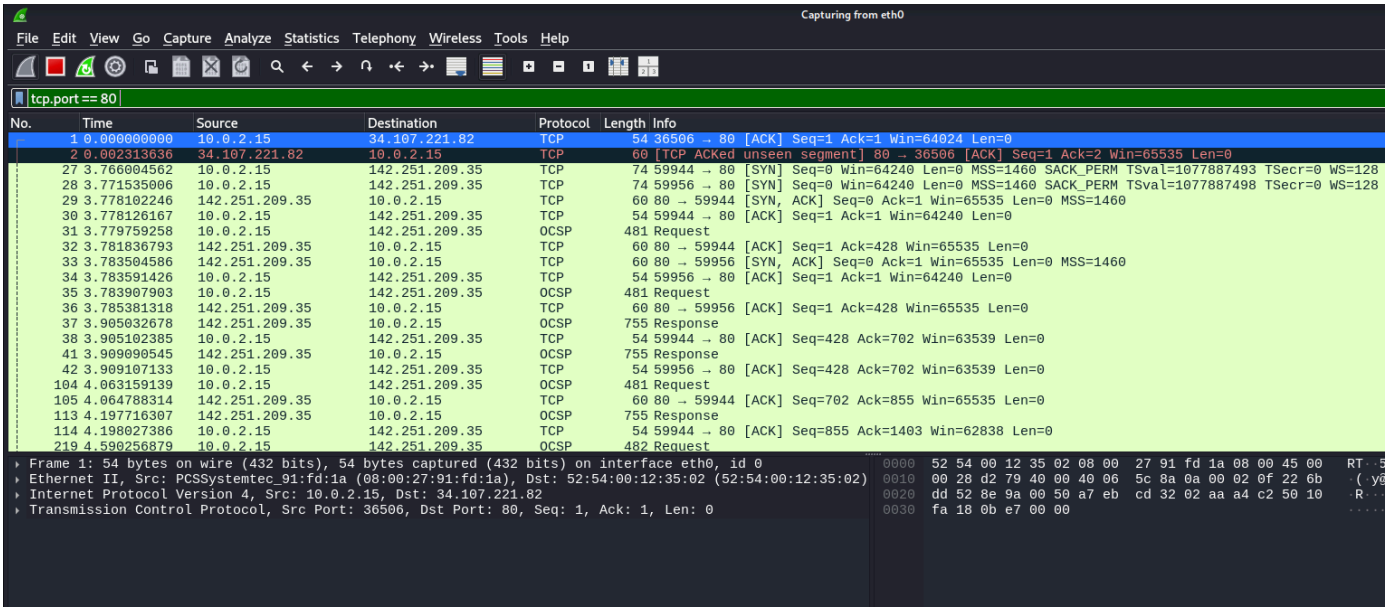
Analizziamo pacchetti TCP con Wire shark

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

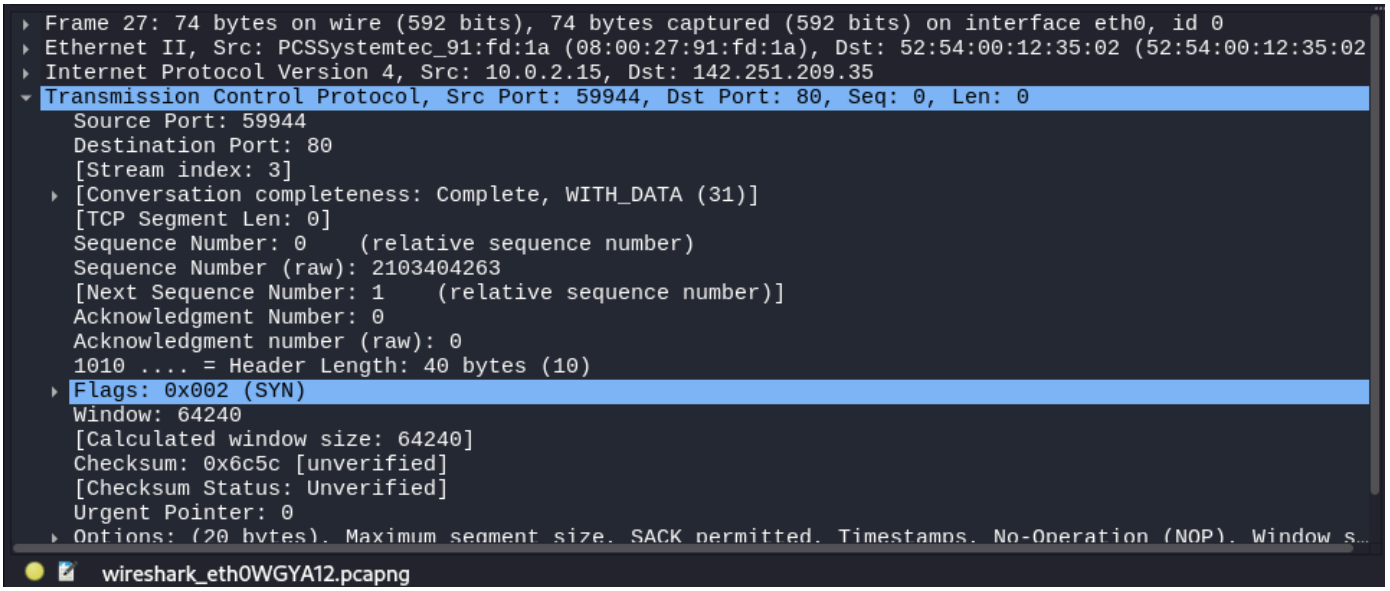




Dopo aver individuato il filtro piu' adatto alla nostra esigenza procediamo ad applicarlo nella barra di Wire shark.



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.



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