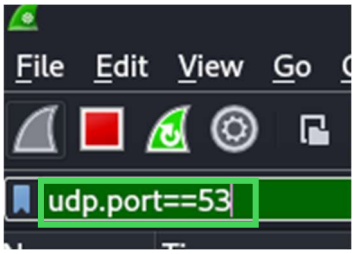
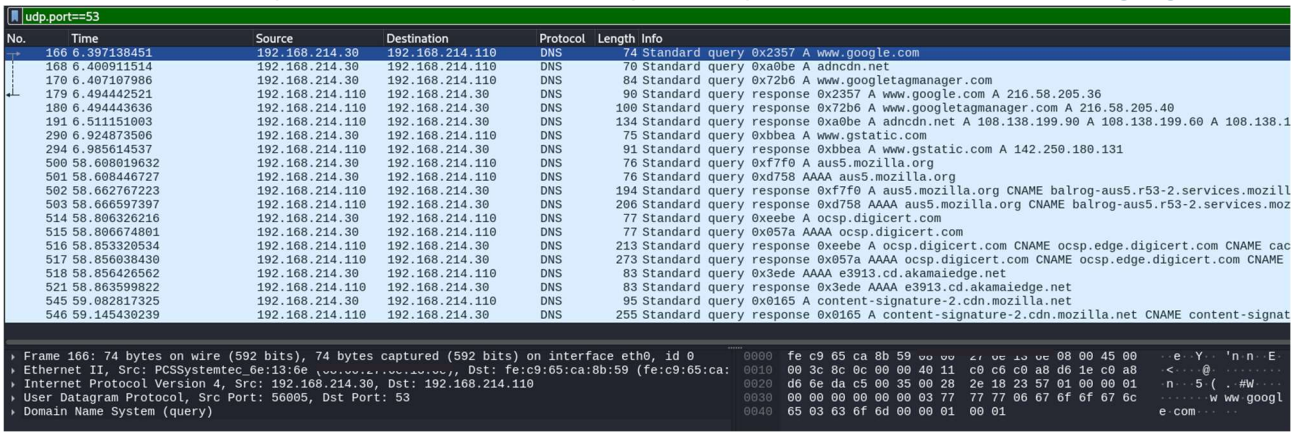
https://itexamanswers.net/17-1-7-lab-exploring-dns-traffic-answers.html

```
sudo systemctl status systemd-resolved
● systemd-resolved.service - Network Name Resolution
     Loaded: loaded (/usr/lib/systemd/system/systemd-resolved.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-02-19 10:00:48 EST; 1min 43s ago
 Invocation: bf45db7d000942a08c9f8c13172a98b3
       Docs: man:systemd-resolved.service(8)
             man:org.freedesktop.resolve1(5)
             https://systemd.io/WRITING_NETWORK_CONFIGURATION_MANAGERS
             https://systemd.io/WRITING_RESOLVER_CLIENTS
   Main PID: 18374 (systemd-resolve)
     Status: "Processing requests..."
      Tasks: 1 (limit: 2211)
     Memory: 3.5M (peak: 4M)
        CPU: 86ms
     CGroup: /system.slice/systemd-resolved.service
             └─18374 /usr/lib/systemd/systemd-resolved
```

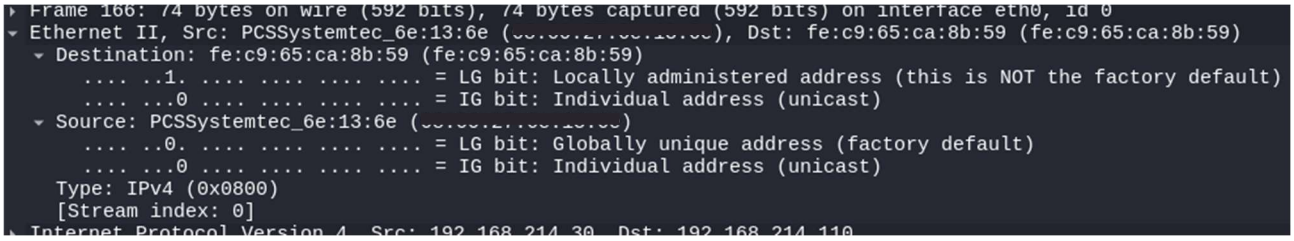
Applico il filtro su wireshark:



Nella cattura non era presente www.cisco.com e quindi ho preso come riferimento www.google.com

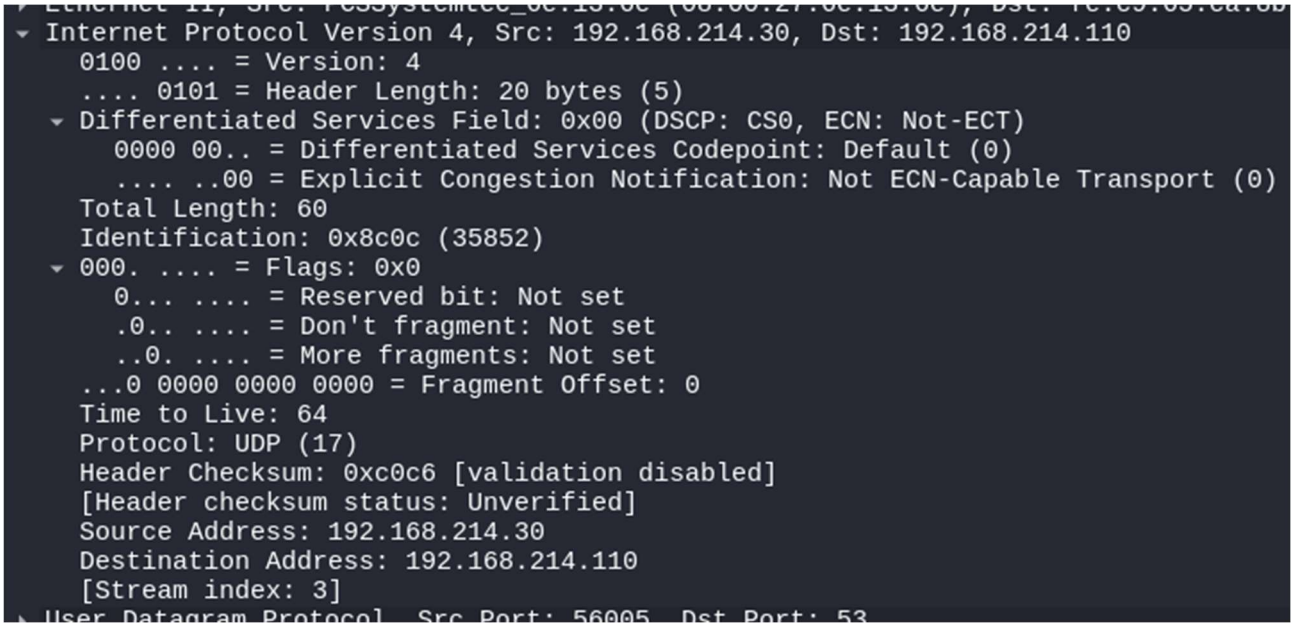


Da notare che nella sezione in basso, è presente la dicitura Ethernet II che se la espando:



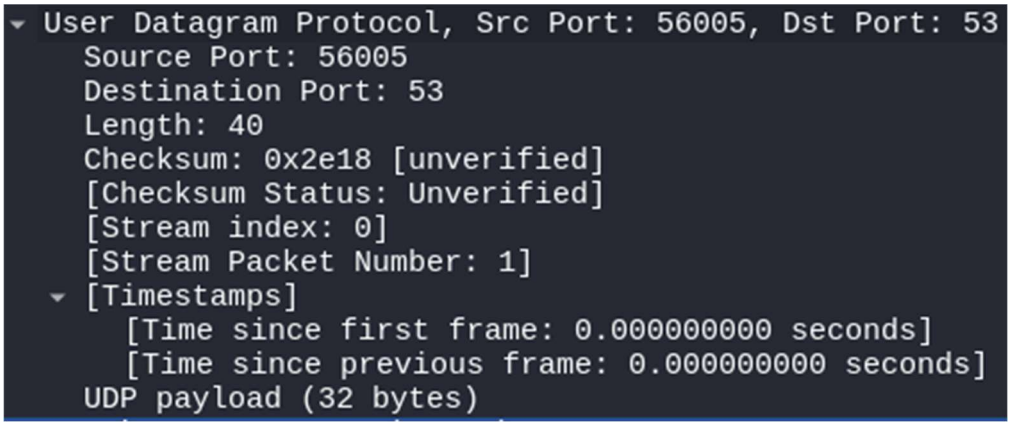
Possiamo notare come sono presenti informazioni riguardo gli indirizzi mac sorgente e destinazione.

Andando ad espandere invece la sezione Internet Protocol Version 4:



Sono presenti informazioni riguardo agli indirizzi IP sorgente e destinazione.

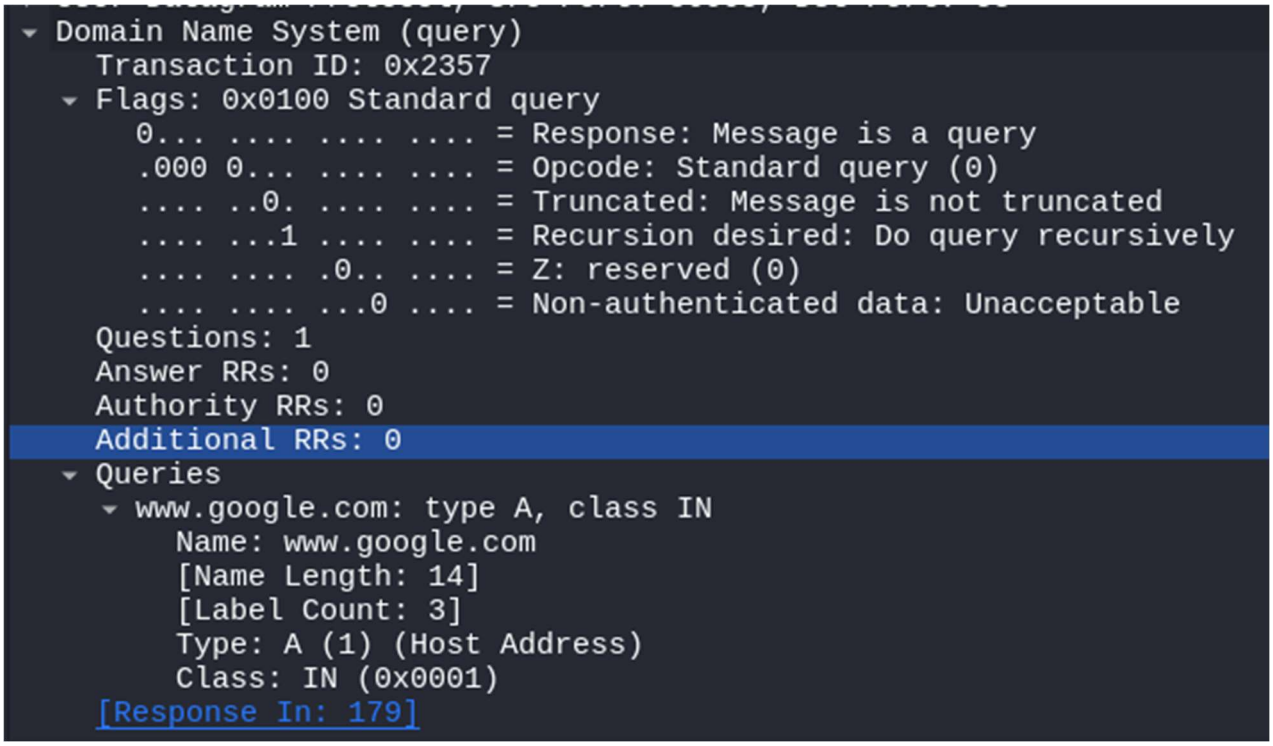
Espandendo poi User Datagram Protocol:



Sono presenti informazioni riguardo le porte di origine e destinazione.

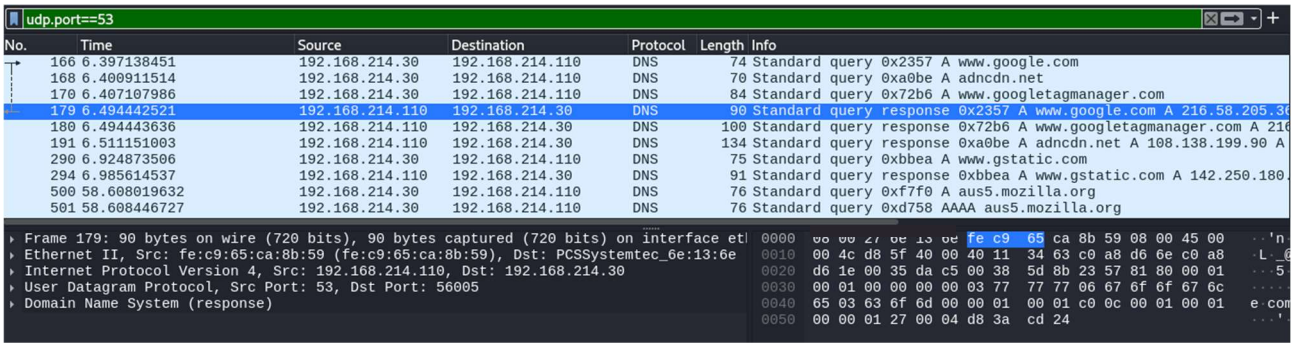
se andiamo a confrontare gli indirizzi indicati, sono gli stessi se andiamo a scrivere sul terminale il comando ip a

espandendo Domain Name System:



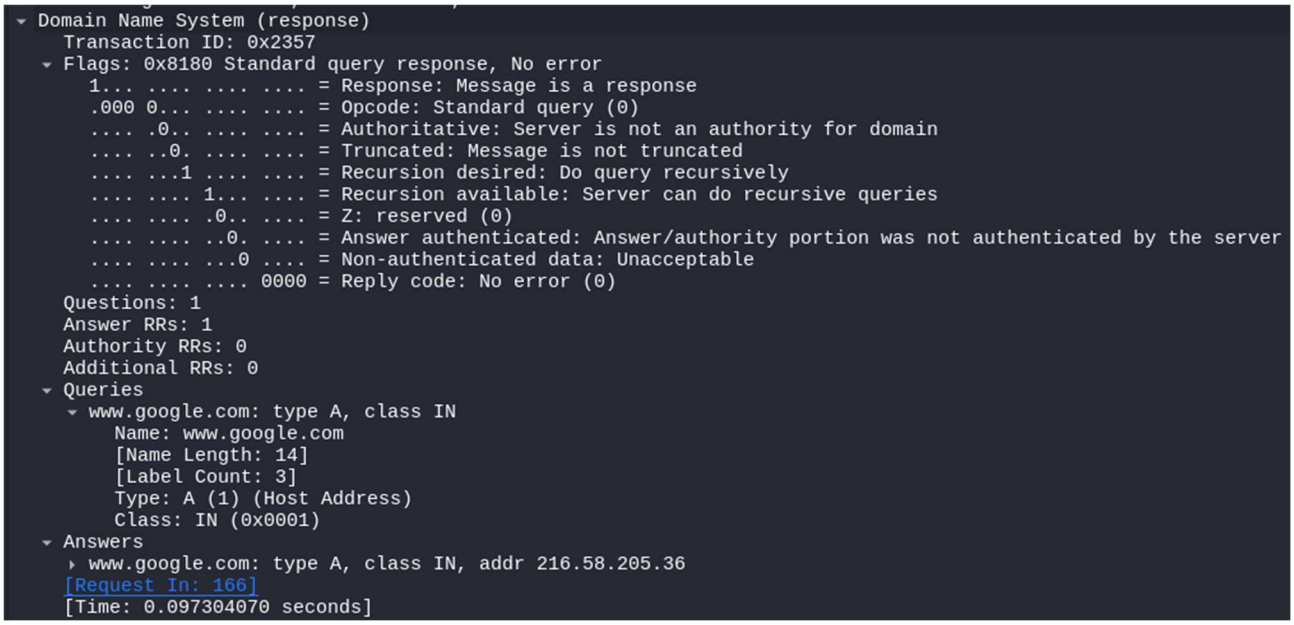
Possiamo notare come il flag è impostato per eseguire la query in maniera ricorsiva.

Adesso analizzo il pacchetto di risposta dal dominio www.google.com



Possiamo notare come gli indirizzi mac sono ora invertiti dato che si tratta di una risposta.

Analizzando Domain Name System:



Possiamo notare che il DNS può gestire le query ricorsive e che il flag di risposta è attivo.