Relazione Esplorazione Traffico DNS

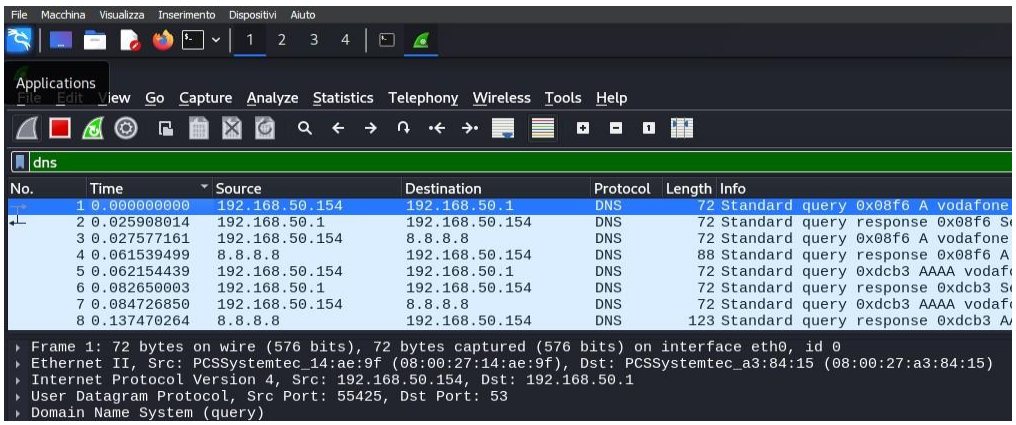
Nella prima immgine utilizzo il comando specifico per l'interrogazione del **Server DNS** e per la richiesta delle informazioni specifiche su un certo Dominio, in questo caso Vodafone, e successivamente con il comando specifico mi metto in ascolto sulla porta che voglio scansionare con **Wireshark** come illustrato di seguito:

- **nslookup vodafone.com**
- **sudo tcpdump -i eth0 port 53**

```
┌──(kali㉿kali)-[~]
└─$ nslookup vodafone.com

;; Got SERVFAIL reply from 192.168.50.1, trying next server
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   vodafone.com
Address: 147.75.40.150
;; Got SERVFAIL reply from 192.168.50.1, trying next server
```

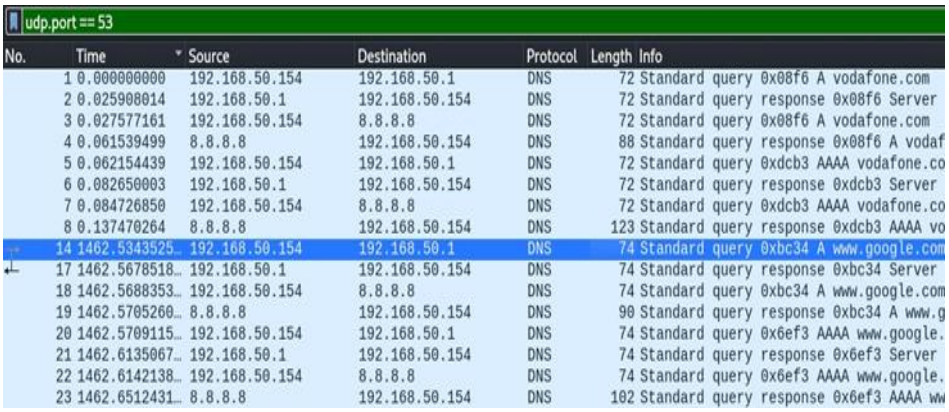
```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth0 port 53

[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
08:59:58.374096 IP 192.168.50.154.38960 > pfSense.home.arpa.domain: 54770+ A? contile.services.mozilla.com. (46)
08:59:58.374155 IP 192.168.50.154.38960 > pfSense.home.arpa.domain: 4851+ AAAA? contile.services.mozilla.com. (46)
08:59:58.429382 IP pfSense.home.arpa.domain > 192.168.50.154.38960: 54770 ServFail 0/0/0 (46)
08:59:58.430476 IP pfSense.home.arpa.domain > 192.168.50.154.38960: 4851 ServFail 0/0/0 (46)
08:59:58.430732 IP 192.168.50.154.36571 > dns.google.domain: 54770+ A? contile.services.mozilla.com. (46)
08:59:58.430789 IP 192.168.50.154.36571 > dns.google.domain: 4851+ AAAA? contile.services.mozilla.com. (46)
08:59:58.440348 IP 192.168.50.154.58548 > pfSense.home.arpa.domain: 48098+ PTR? 1.50.168.192.in-addr.arpa. (43)
08:59:58.441091 IP pfSense.home.arpa.domain > 192.168.50.154.58548: 48098* 1/0/0 PTR pfSense.home.arpa. (70)
08:59:58.441250 IP 192.168.50.154.53454 > pfSense.home.arpa.domain: 57040+ PTR? 154.50.168.192.in-addr.arpa. (45)
08:59:58.441922 IP pfSense.home.arpa.domain > 192.168.50.154.53454: 57040 NXDomain* 0/1/0 (104)
08:59:58.443266 IP 192.168.50.154.48397 > pfSense.home.arpa.domain: 17952+ PTR? 8.8.8.8.in-addr.arpa. (38)
08:59:58.468545 IP dns.google.domain > 192.168.50.154.36571: 54770 1/0/0 A 34.117.188.166 (62)
08:59:58.468546 IP dns.google.domain > 192.168.50.154.36571: 4851 0/1/0 (127)
```

Dopo aver utilizzato il comando illustrato e descritto in precedenza, utilizzo il comando nel filtro di ricerca di **Wireshark**, per ricercare il traffico specifico di rete **DNS** (**Domain Name System**), come illustrato di seguito:



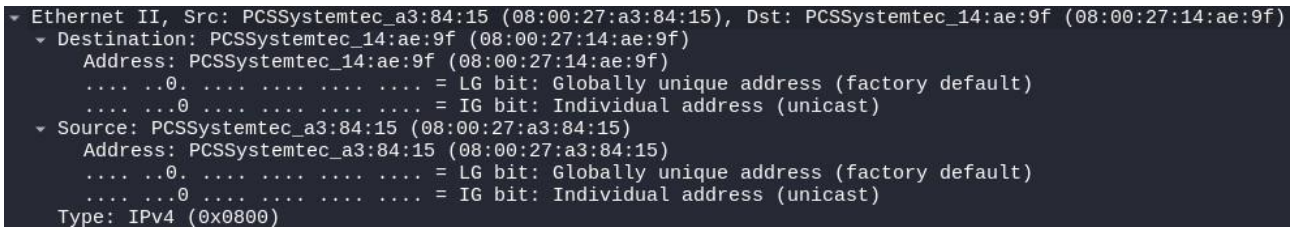
Nella prossima immagine e passaggio sul tool di cattura di rete Wireshark, sempre nel filtro di ricerca, scrivo il comando per il solo traffico di rete DNS e come illustrato di seguito, seleziono riga (blue scuro), la **Standard query** (**www.google.com**)

- **udp.port == 53**

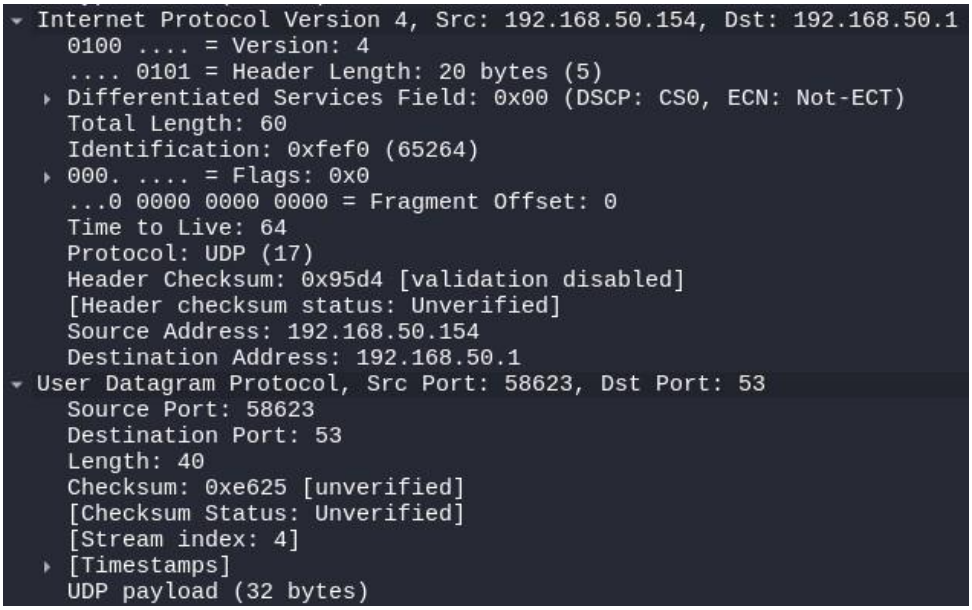


Nel prossimo passaggio ed immagine, clicco ed espando la voce **Ethernet II** nel quale posso visualizzare tutti i dettagli della comunicazione, e nello specifico, campi di origine e di destinazione.

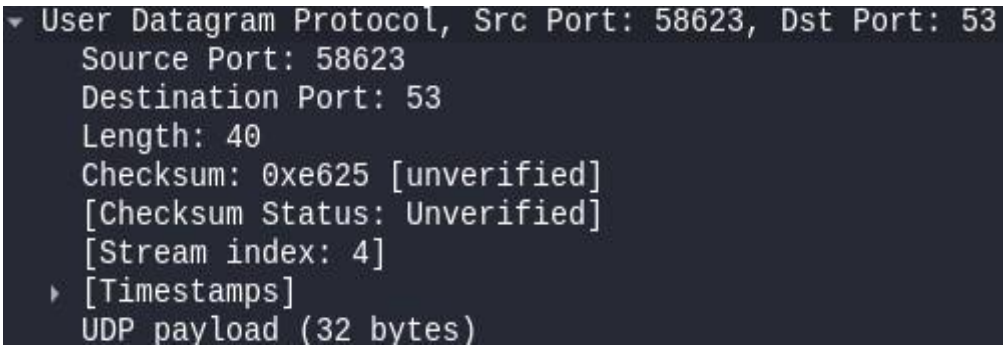
Nel seguente passaggio l'indirizzo MAC sorgente viene associato alla NIC sul PC e l'indirizzo MAC della destinazione viene associato al Gateway predefinito.
Se è presente un Server DNS locale, l'indirizzo MAC di destinazione sarebbe l'indirizzo MAC del server DNS locale.



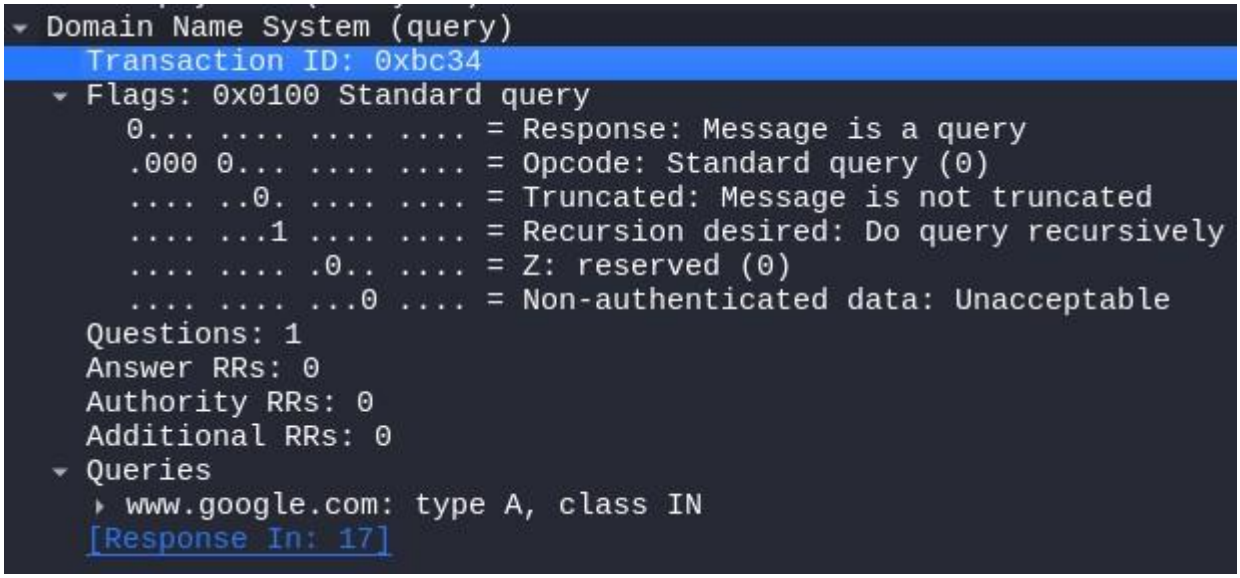
Dopo aver analizzato la scheda **Ethernet II**, vado ad analizzare, espandendo, la scheda **Internet Protocol Version 4,** nel quale posso notare che l'indirizzo **IP sorgente** (di origine) viene associato alla scheda di rete del mio PC, e l'indirizzo **IP di destinazione**, viene associato al Gateway predefinito, come possiamo vedere di seguito:



Nella seguente immagine dopo aver analizzato nei dettagli **Internet Protocol Version 4** possiamo notare la **Source Port**: **58623** e come visto in precedenza e come agito prima, tramite specifico comando per l'ascolto su una determinata porta: **53** (**Destination Port**), come illustrato di seguito:



Successivamente all'analisi effettuata sulla **Source Port** (**58623**) e la **Destination Port** (**53**), posso notare nell'analisi del Domain Name System, che il flag delle query è settato per un'interrogazione ricorsiva sull'indirizzo **www.google.com**, come possiamo notare di seguito:



Nella seguente immagine vado ad identificare il traffico di risposta del DNS con il comando specifico che mi restituisca la risposta:

- **dns.flags.response ==1**