ESPLORAZIONE DEL TRAFFICO DNS

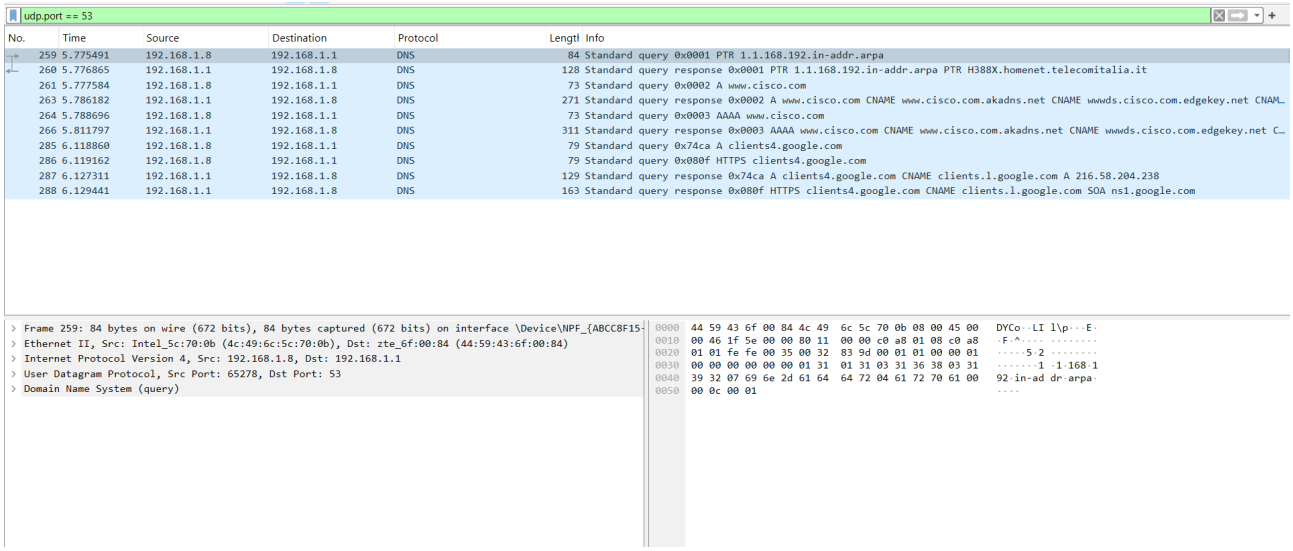
Dopo aver installato Wireshark, cancelliamo la cache DNS inserendo nel terminale comando specifico per Windows “ipconfig /flushdns”.

```
Microsoft Windows [Versione 10.0.26100.3775]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\andre>ipconfig /flushdns

Configurazione IP di Windows

Cache del resolver DNS svuotata.

C:\Users\andre>
```

Avviamo Wireshark e attiviamo la cattura del traffico dei pacchetti. Sul terminale inseriamo il comando”nslookup www.cisco.com” per interrogare il dominio.

```
Microsoft Windows [Versione 10.0.26100.3775]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\andre>ipconfig /flushdns

Configurazione IP di Windows

Cache del resolver DNS svuotata.

C:\Users\andre>nslookup www.cisco.com
Server:  UnKnown
Address:  10.2.0.1

Risposta da un server non autorevole:
Nome:    e2867.dsca.akamaiedge.net
Addresses:  2001:41a8:47:a83::b33
          2001:41a8:47:a81::b33
          2.18.1.94
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.
net


C:\Users\andre>
```

Su Wireshark stoppiamo la cattura ed inseriamo il filtro “udp.port == 53”. Tra i pacchetti che vi vengono proposti, andiamo a selezionare la stringa che ha “Standard query 0x0002 A www.cisco.com” tra le info.



Qui notiamo nel riquadro Packet Details che questo pacchetto ha:

Ethernet II, Internet Protocol Version 4, User Datagram Protocol e Domain Name System (query). Andando ad espandere la sezione Ethernet II noteremo gli indirizzi MAC di origine (4c:49:6c:5c:70:0b riferito alla NIC del PC) e di destinazione (44:59:43:6f:00:84 riferito al Gateway).

ANALISI DEGLI INDIRIZZI IP E PORTE

ELEMENTO	ORIGINE	DESTINAZIONE
INDIRIZZO MAC	NIC DEL PC	GATEWAY PREDEFINITO
INDIRIZZO IP	192.168.1.8	192.168.1.1
PORTA	65279	53

Come controprova sul terminale sul terminale inseriamo i comandi “arp -a” e “ipconfig /all” Noteremo che l'indirizzo MAC del nostro PC è lo stesso catturato da Wireshark

```
Scheda LAN wireless Wi-Fi:

   Suffisso DNS specifico per connessione: homenet.telecomitalia.it
   Descrizione . . . . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX101
   Indirizzo fisico. . . . . . . . . . . . : 4C-49-6C-5C-70-0B
   DHCP abilitato. . . . . . . . . . . . . : Sì
   Configurazione automatica abilitata   : Sì
   Indirizzo IPv4. . . . . . . . . . . . . : 192.168.1.8(Preferenziale)
   Subnet mask . . . . . . . . . . . . . . : 255.255.255.0
   Lease ottenuto. . . . . . . . . . . . . : mercoledì 9 aprile 2025 21:07:32
   Scadenza lease . . . . . . . . . . . . . : venerdì 11 aprile 2025 08:32:35
   Gateway predefinito . . . . . . . . . . : 192.168.1.1
   Server DHCP . . . . . . . . . . . . . . : 192.168.1.1
   Server DNS . . . . . . . . . . . . . . . : 192.168.1.1
   NetBIOS su TCP/IP . . . . . . . . . . . : Attivato
```

DETTAGLI DELLA QUERY DNS

Analisi Domain Name System (query)

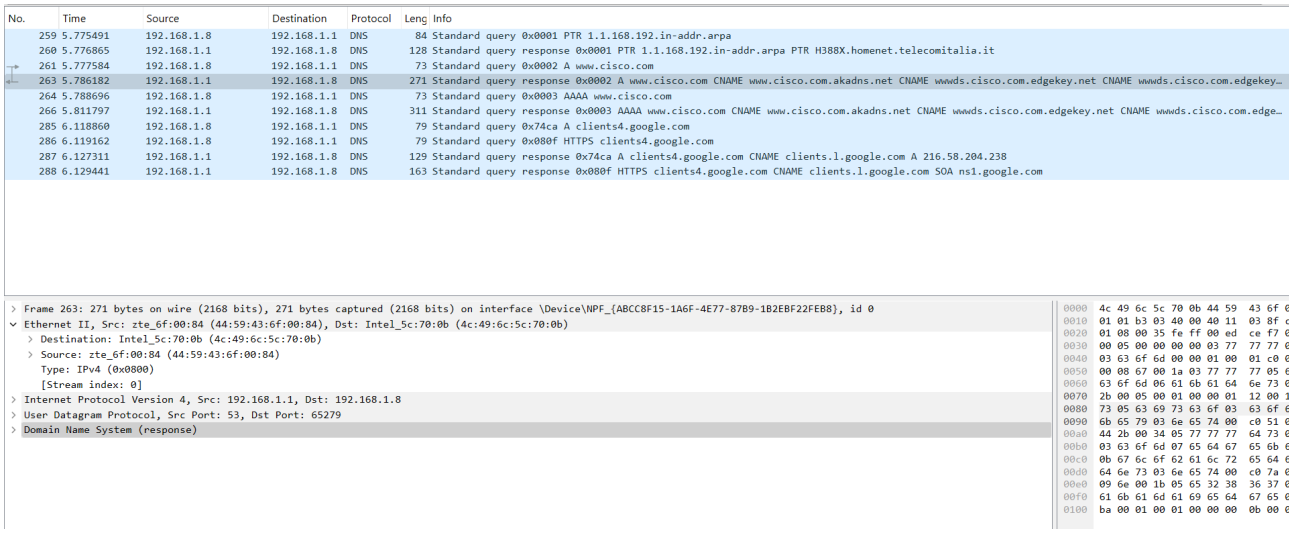
```
> User Datagram Protocol, Src Port: 65279, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.cisco.com: type A, class IN
    [Response In: 263]
```

Espandendo Domain Name System (query), ed espandere Flags e Queries, possiamo notare che la query DNS contiene:

- Identificatore della transazione
- Flag per la query ricorsiva
- Dominio richiesto (www.cisco.com)
- Tipo di record richiesto (A)

ESPLORAZIONE DEL TRAFFICO DI RISPOSTA DNS

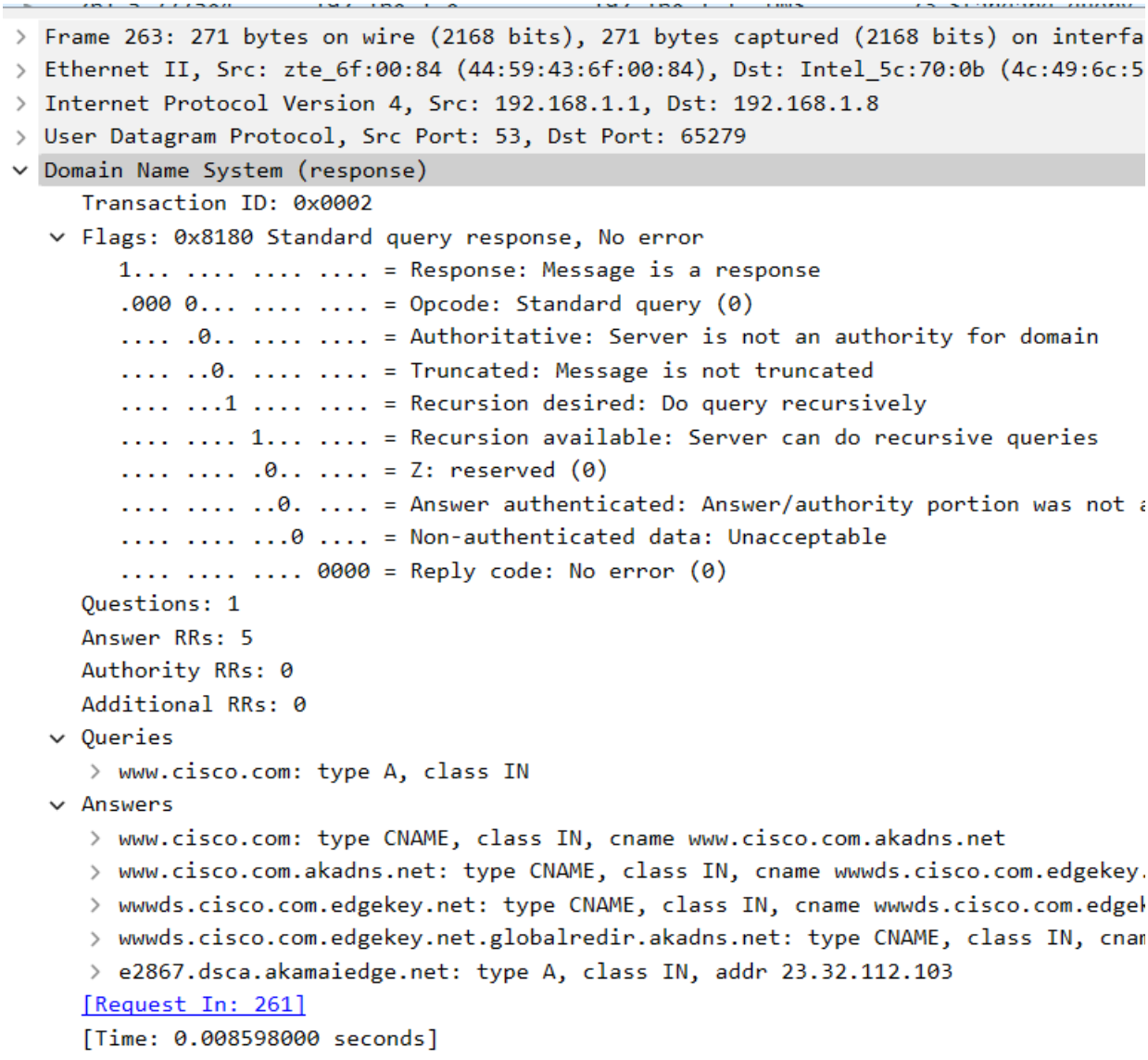
Per questo passaggio prendiamo in esame il pacchetto DNS di risposta che ha “Standard query response – A www.cisco.com” nella colonna info



ANALISI DEGLI INDIRIZZI IP E PORTE

ELEMENTO	ORIGINE	DESTINAZIONE
INDIRIZZO MAC	GATEWAY PREDEFINITO	NIC DEL PC
INDIRIZZO IP	192.168.1.1	192.168.1.8
PORTA	53	65279

Espandendo Domain Name System (response), poi Flags, Queries e Answers potremmo vedere quanto segue



Possiamo notare che il DNS può gestire query ricorsive.