

---

# S11-L3

## Analisi traffico DNS con Wireshark

Emanuele Benedetti | 19 febbraio 2025

---

### Consegna

Il laboratorio è dedicato all'esplorazione del traffico DNS.

Tramite l'utilizzo di Wireshark verranno completati i seguenti obiettivi:

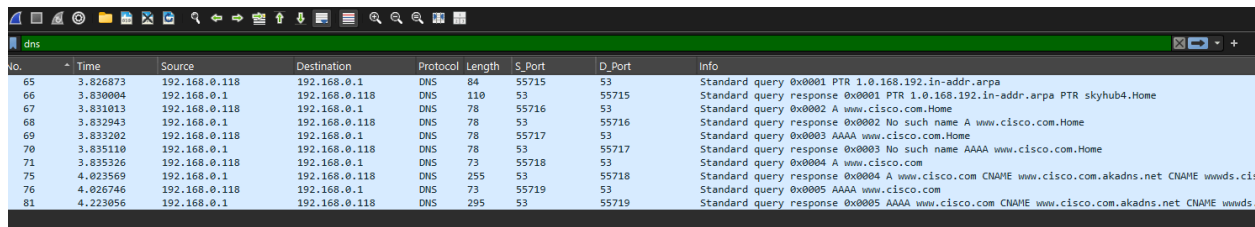
1. Cattura del traffico DNS
2. Esplorazione del traffico delle query DNS
3. Esplorazione del traffico delle risposte DNS

### Svolgimento

#### Cattura del traffico DNS con Wireshark

Per visualizzare correttamente tutto il traffico DNS generato dal nostro PC procediamo innanzitutto con l'eliminazione della cache DNS. Apriamo quindi un prompt dei comandi con *Start > cmd* ed eseguiamo il comando *ipconfig /flushdns*.

Avviamo la cattura del traffico di rete con Wireshark per visualizzare i pacchetti DNS che generiamo inserendo nel terminale il comando *nslookup www.cisco.com*.

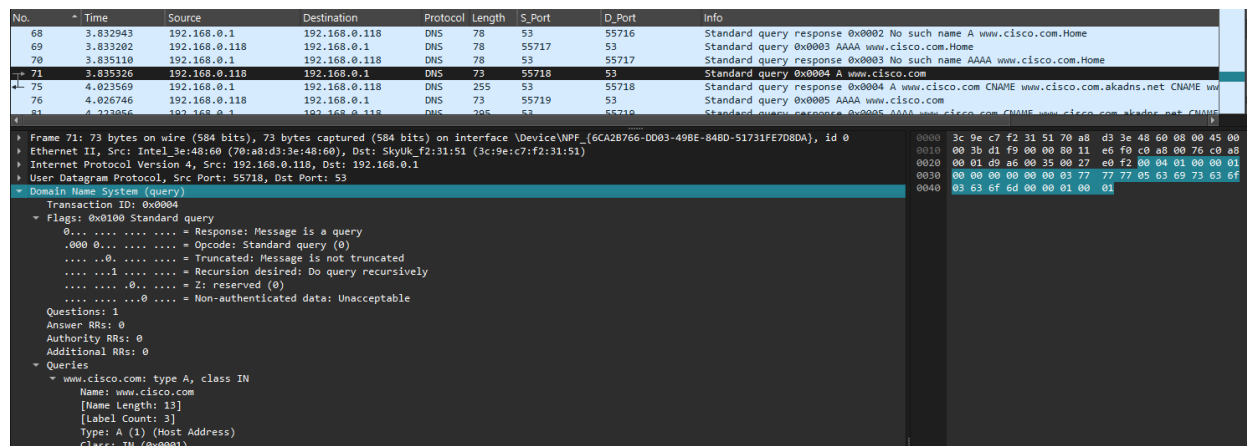


No.	Time	Source	Destination	Protocol	Length	S.Port	D.Port	Info
65	3.826873	192.168.0.118	192.168.0.1	DNS	84	55715	53	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
66	3.830004	192.168.0.1	192.168.0.118	DNS	110	53	55715	Standard query response 0x0001 PTR 1.0.168.192.in-addr.arpa PTR skyhub4.Home
67	3.831013	192.168.0.118	192.168.0.1	DNS	78	55716	53	Standard query 0x0002 A www.cisco.com.Home
68	3.832943	192.168.0.1	192.168.0.118	DNS	78	53	55716	Standard query response 0x0002 No such name A www.cisco.com.Home
69	3.833202	192.168.0.118	192.168.0.1	DNS	78	55717	53	Standard query 0x0003 AAAA www.cisco.com.Home
70	3.835110	192.168.0.1	192.168.0.118	DNS	78	53	55717	Standard query response 0x0003 No such name AAAA www.cisco.com.Home
71	3.835326	192.168.0.118	192.168.0.1	DNS	73	55718	53	Standard query 0x0004 A www.cisco.com
75	4.023569	192.168.0.1	192.168.0.118	DNS	255	53	55718	Standard query response 0x0004 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com
76	4.026746	192.168.0.118	192.168.0.1	DNS	73	55719	53	Standard query 0x0005 AAAA www.cisco.com
81	4.223056	192.168.0.1	192.168.0.118	DNS	295	53	55719	Standard query response 0x0005 AAAA www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com

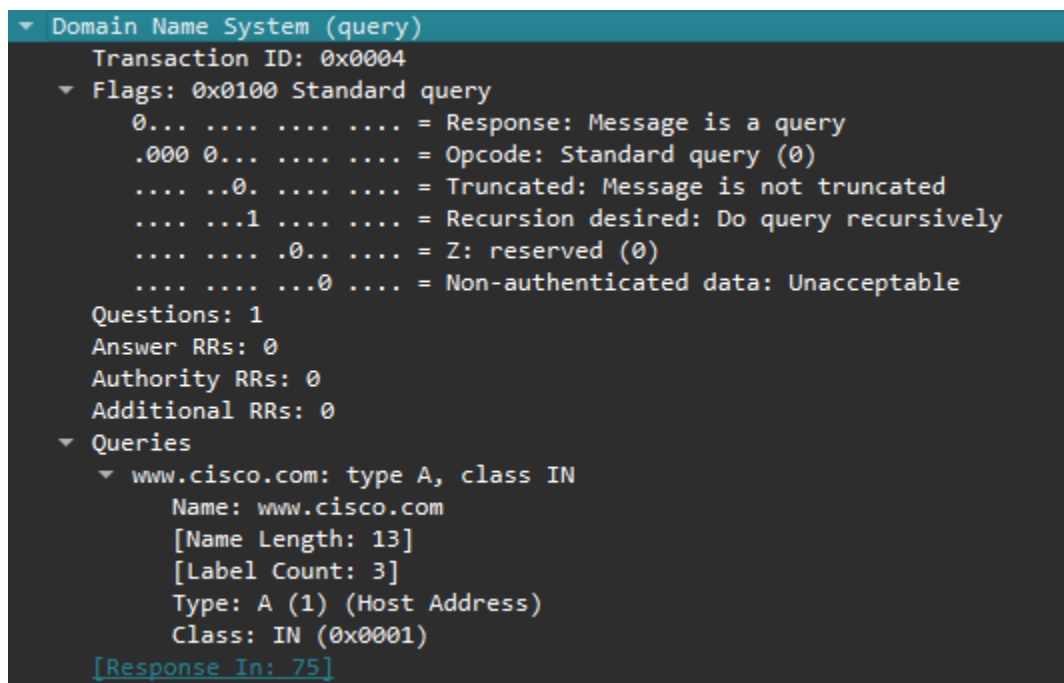
## Esplorazione delle query DNS con wireshark

Nello screenshot precedente ho utilizzato il filtro *dns* per visualizzare solamente i pacchetti dns catturati.

Selezioniamo il pacchetto 71, relativo alla *Standard query A www.cisco.com* ed analizziamo tutti i dettagli tramite la sezione informazioni in basso.

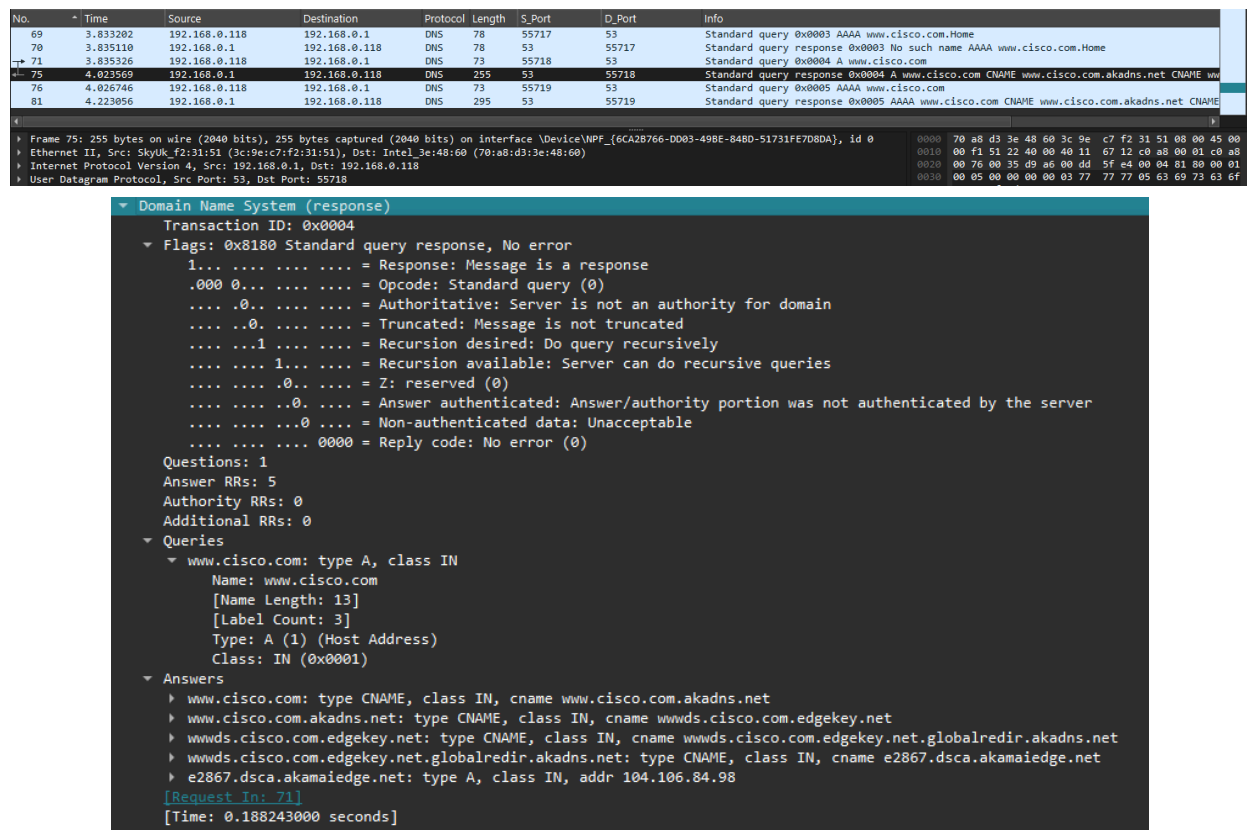


Di seguito ho ingrandito la sezione *Domain Name System (query)*



## Esplorazione delle risposte DNS con wireshark

Selezioniamo ora il pacchetto successivo relativo alla *Standard query response* A *www.cisco.com*.



Domain Name System (response)

Transaction ID: 0x0004

Flags: 0x8180 Standard query response, No error

- 1... .. = Response: Message is a response
- .000 0... .. = Opcode: Standard query (0)
- .... .0.. .. = Authoritative: Server is not an authority for domain
- .... .0.. .. = Truncated: Message is not truncated
- .... .1... .. = Recursion desired: Do query recursively
- .... .1... .. = Recursion available: Server can do recursive queries
- .... .0.. .. = Z: reserved (0)
- .... .0.. .. = Answer authenticated: Answer/authority portion was not authenticated by the server
- .... .0.. .. = Non-authenticated data: Unacceptable
- .... .0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 5

Authority RRs: 0

Additional RRs: 0

Queries

- www.cisco.com: type A, class IN
  - Name: www.cisco.com
  - [Name Length: 13]
  - [Label Count: 3]
  - Type: A (1) (Host Address)
  - Class: IN (0x0001)

Answers

- www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
- www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net
- wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredir.akadns.net
- wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
- e2867.dsca.akamaiedge.net: type A, class IN, addr 104.106.84.98

[Request In: 71]

[Time: 0.188243000 seconds]

Come possiamo vedere dagli screenshot l'indirizzo IP, MAC e numero delle porte sorgente sono ora diventati IP, MAC e numero delle porte di destinazione.

Verificando la risposta del comando *nslookup www.cisco.com* fornita dal terminale possiamo verificare che le informazioni corrispondono

```
C:\Users\personale>nslookup www.cisco.com
Server: skyhub4.Home
Address: 192.168.0.1

Risposta da un server non autorevole:
Nome: e2867.dsca.akamaiedge.net
Addresses: 2a02:26f0:8d00:ca9::b33
           2a02:26f0:8d00:c9e::b33
           104.106.84.98
Aliases: www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```