

# Es. S11-L4 Relazione sull'analisi del traffico DNS

## Relazione sull'analisi del traffico DNS



Tag:

#analisiRete

#dns

#wireshark

#kaliLinux

## Introduzione

L'analisi del traffico DNS è stata eseguita tramite Wireshark per osservare le richieste e risposte DNS durante le query verso vari domini, in particolare verso `www.cisco.com`. I pacchetti DNS sono stati esaminati e confrontati utilizzando `nslookup` per verificare i risultati.

The screenshot displays a Wireshark capture of DNS traffic on the interface `eth0`. The packet list shows several DNS queries and responses. The selected packet (No. 73) is a standard query for `www.cisco.com`. The packet details pane shows the query structure, including the question section with `www.cisco.com` and the answer section with `www.cisco.com.akadns.net`. The packet bytes pane shows the raw data of the DNS query.

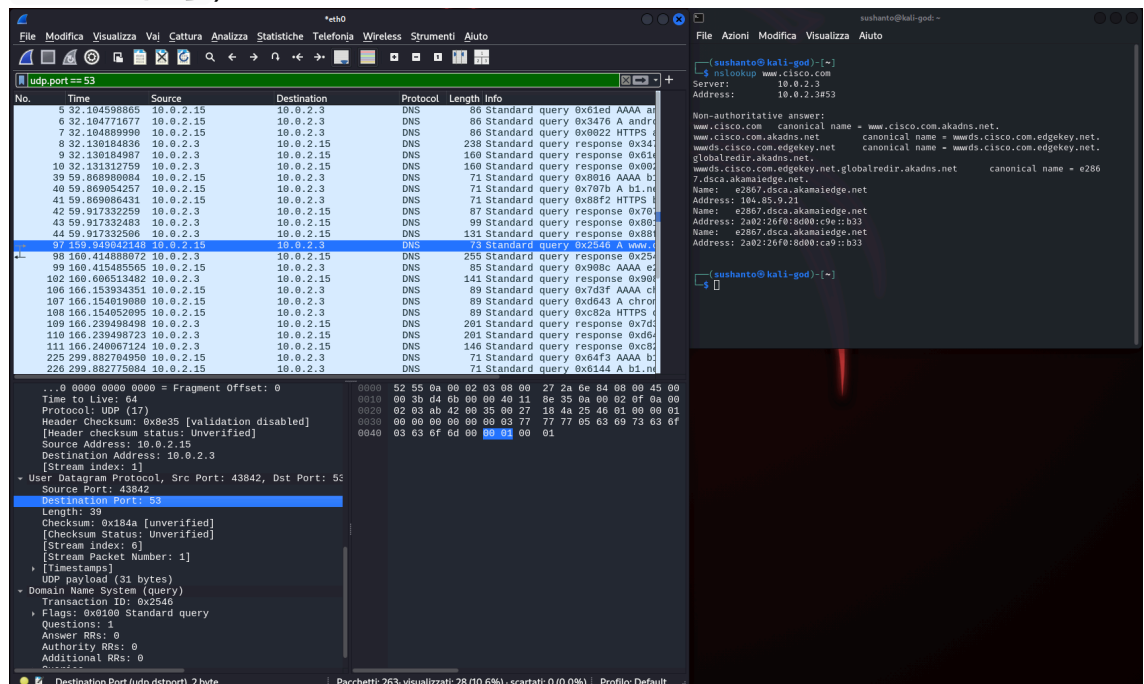
On the right, a terminal window shows the output of the `nslookup` command:

```
sushanto@kali-god: ~  
$ nslookup www.cisco.com  
Server: 10.0.2.3  
Address: 10.0.2.3#53  
  
Non-authoritative answer:  
www.cisco.com canonical name = www.cisco.com.akadns.net.  
www.cisco.com.akadns.net canonical name = wwwds.cisco.com.edgekey.net.  
wwwds.cisco.com.edgekey.net canonical name = wwwds.cisco.com.edgekey.net.  
globalredir.akadns.net.  
wwwds.cisco.com.edgekey.net.globalredir.akadns.net canonical name = e2867.dsca.akamaledge.net.  
7.dsca.akamaledge.net.  
Name: e2867.dsca.akamaledge.net  
Address: 104.85.9.21  
Name: e2867.dsca.akamaledge.net  
Address: 2a02:26f0:8d00:c9e::b33  
Name: e2867.dsca.akamaledge.net  
Address: 2a02:26f0:8d00:ca9::b33
```

## Analisi dei pacchetti DNS

## 1. Richieste DNS (Query):

- Le query DNS sono state catturate utilizzando il filtro `udp.port == 53`.
- Ogni pacchetto conteneva una richiesta di risoluzione del nome per `www.cisco.com`.
- Il pacchetto catturato mostrava indirizzi IP di origine `10.0.2.15` e destinazione `10.0.2.3` con porta di destinazione 53, come illustrato nell'immagine allegata ( `udp_port_53_2024-10-24_14-27-35.png` ).



## 2. Risposte DNS (Response):

- Le risposte corrispondenti alle richieste DNS sono state identificate nel traffico e contenevano le informazioni sul nome risolto (CNAME e record A).
- L'indirizzo IP di risposta confermava la corrispondenza con i risultati ottenuti da `nslookup`, come evidenziato nelle immagini.

## Indirizzi MAC e IP

L'indirizzo MAC e IP di origine nella richiesta DNS diventano gli indirizzi di destinazione nella risposta DNS, e viceversa. Questo comportamento è visibile nei pacchetti catturati:

- **Indirizzo MAC e IP nella richiesta:** PCSYSstemtec\_2a:6e:84 (08:00:27:2a:6e:84) con IP 10.0.2.15
- **Indirizzo MAC e IP nella risposta:** 52:55:0a:00:02:03 con IP 10.0.2.3 ( mac\_compare\_2024-10-24\_14-43-58.png ).

The screenshot displays a Wireshark capture of network traffic on the eth0 interface. The packet list shows a series of DNS queries and responses. The selected packet is a DNS query from 10.0.2.15 to 10.0.2.3, with a source MAC of 08:00:27:2a:6e:84 and a destination MAC of 52:55:0a:00:02:03. The packet details show the query for 'www.4' with flags indicating it's a recursive query. The packet bytes show the raw data of the query.

## Query Ricorsive

I pacchetti mostrano che il server DNS è configurato per gestire query ricorsive. Questo è confermato dall'analisi dei flag nei pacchetti DNS ( flags\_query\_2024-10-24\_14-45-26.png ).

Wireshark interface showing network traffic analysis. The main pane displays a list of captured packets, with packet 97 selected (UDP port 53). The packet details pane shows the structure of the DNS query, including the transaction ID (0x2540) and the query type (Standard query). The packet bytes pane shows the raw data of the packet.

Packet 97 details:

- Source Port: 43842
- Destination Port: 53
- Length: 39
- Checksum: 0x184a [unverified]
- Stream Status: Unverified
- Stream index: 6
- Stream Packet Number: 1
- Time: 0.000000
- UDP payload (31 bytes)
- Domain Name System (query)
- Transaction ID: 0x2540
- Flags: 0x0100 Standard query
- 0... .. = Response: Message is a query
- 0000... .. = Opcode: Standard query (0)
- ... .. = Truncated: Message is not truncated
- ... .. = Recursion desired: Do query recursively
- ... .. = Z: reserved (0)
- ... .. = Non-authenticated data: Unacceptable
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries
- www.cisco.com: type A, class IN
- Response In: 98

Packet 97 bytes:

```
0000 52 55 08 00 02 03
0010 00 3b d4 6b 00 00
0020 02 03 ab 42 00 35
0030 00 00 00 00 00 00
0040 03 63 6f 6d 00 00
```

 **Chiavi:**  
[analisi traffico DNS, Wireshark, nslookup, porta 53, query DNS ricorsiva]