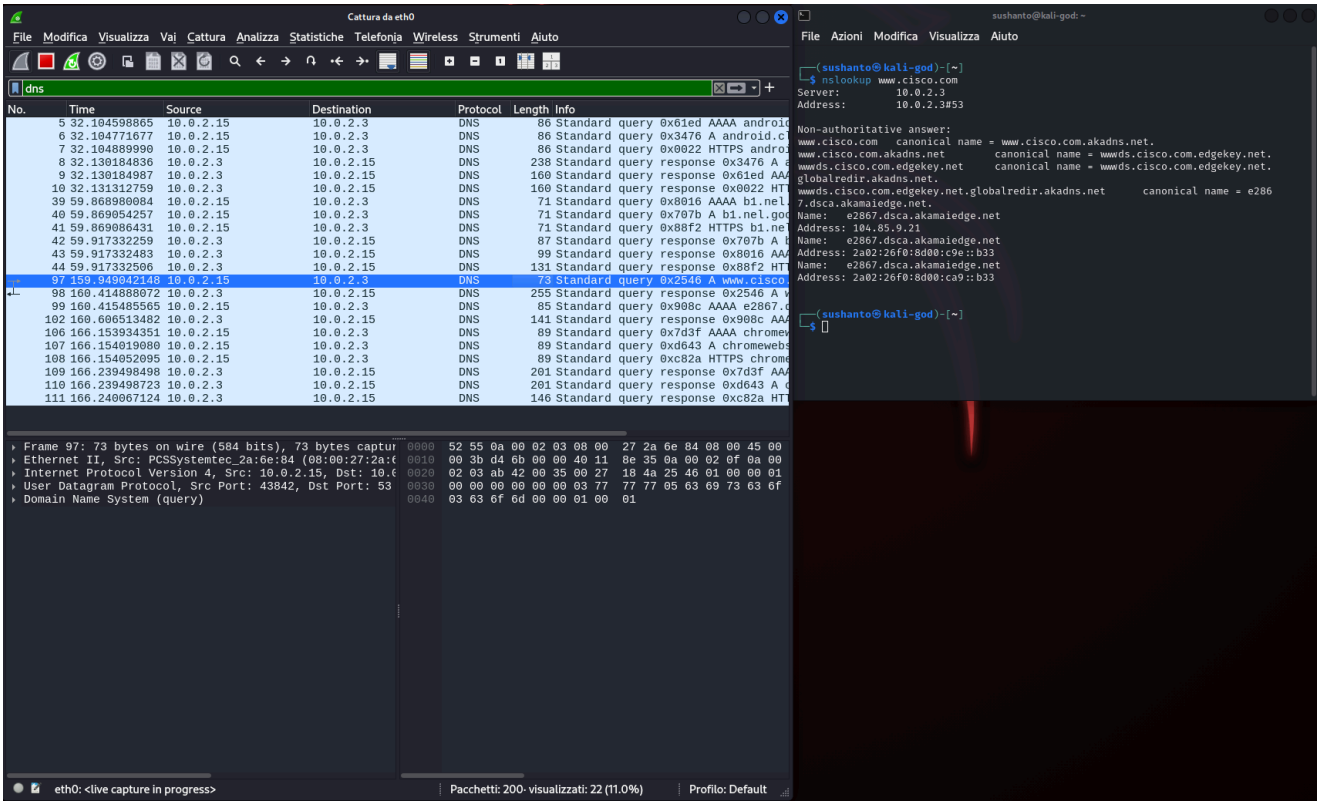
Es. S11-L4 Relazione sull'analisi del traffico DNS

Relazione sull'analisi del traffico DNS

⚜️ **Tag:** #analisiRete #dns #wireshark #kaliLinux

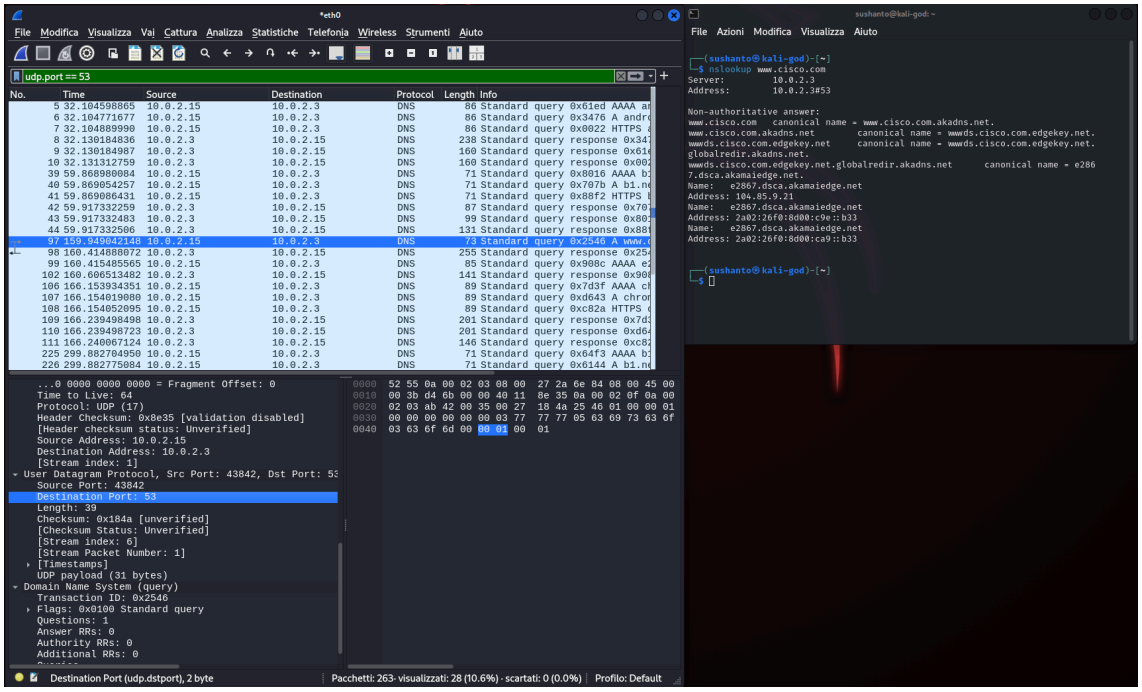
Introduzione

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.



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`).

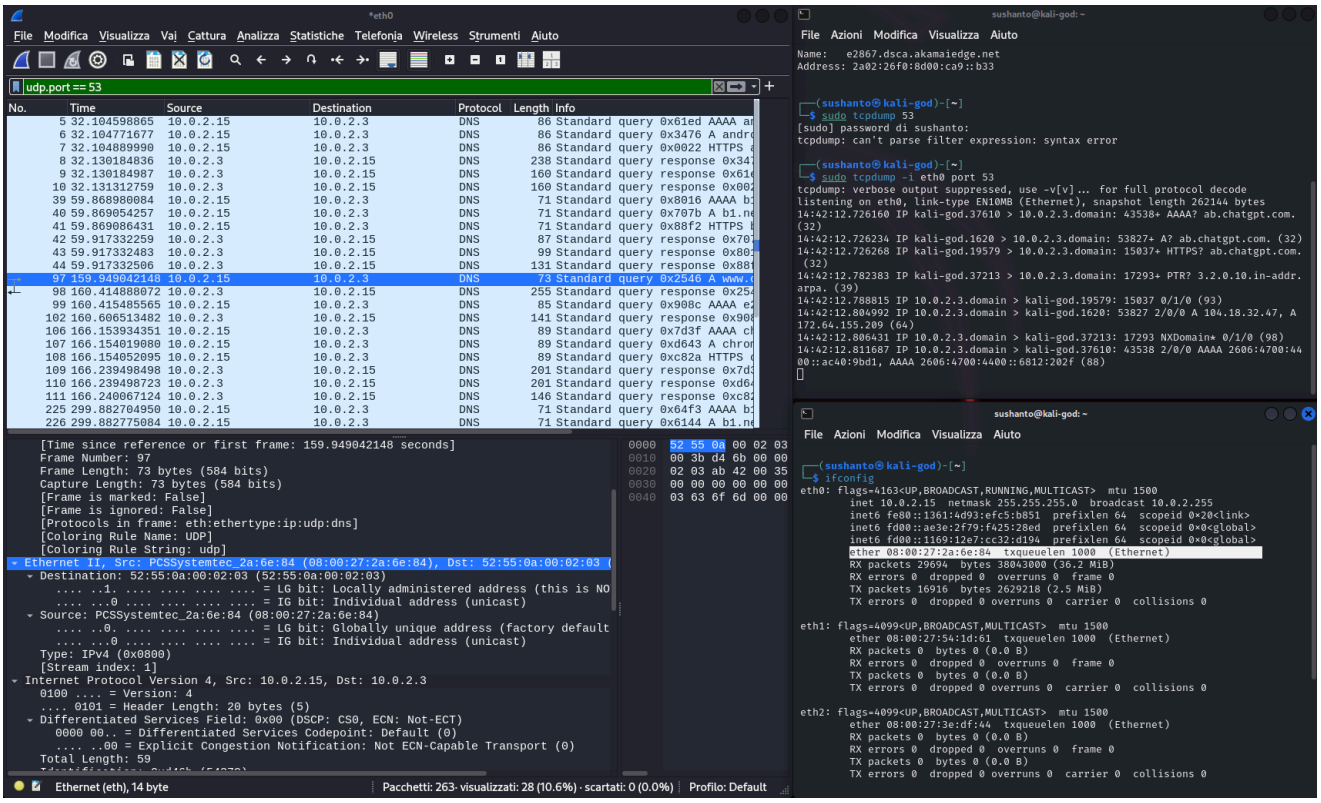


2. **Risposte DNS (Response)**:
    - Le risposte corrispondenti alle richieste DNS sono state identificate nel traffico e contenevano le informazioni sul nome risolto (CNAME e record A).
    - L'indirizzo IP di risposta confermava la corrispondenza con i risultati ottenuti da `nslookup`, come evidenziato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

Indirizzi MAC e IP

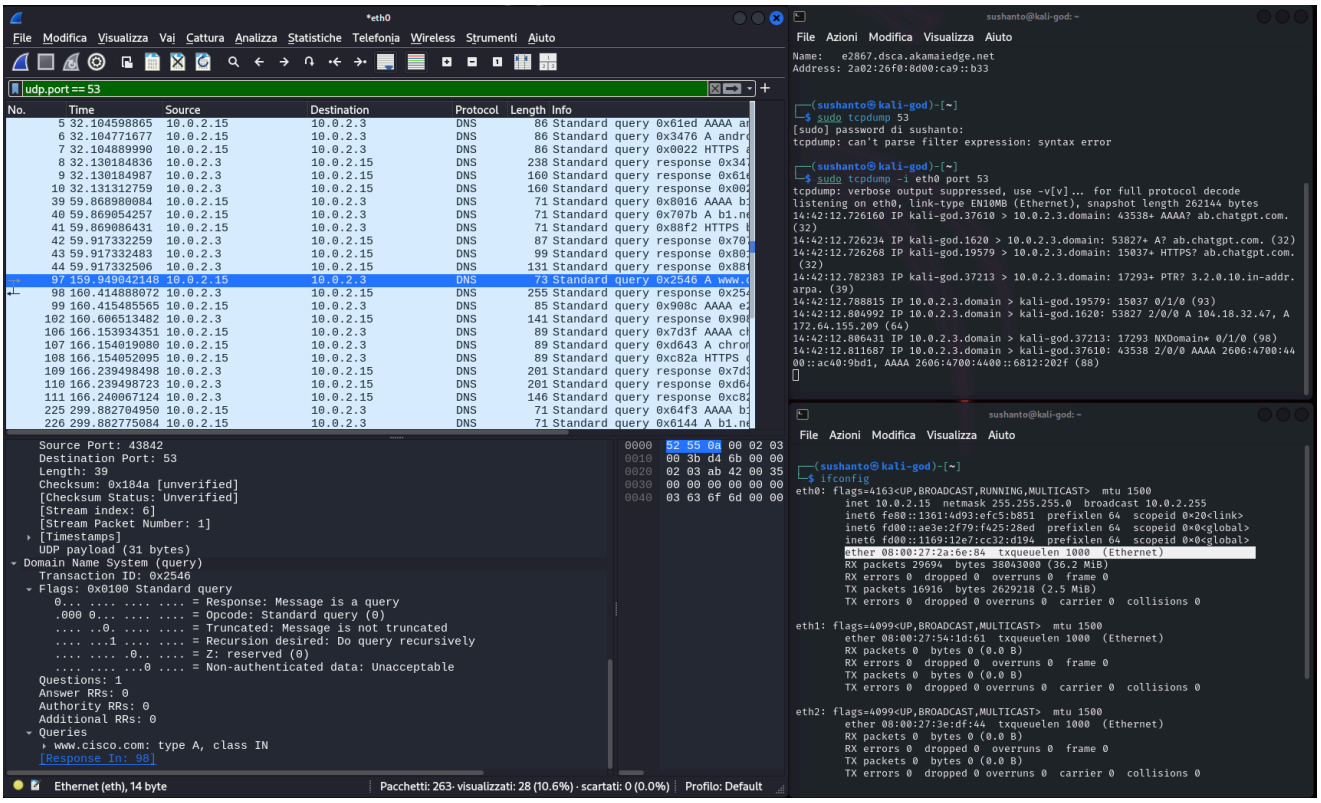
L'indirizzo MAC e IP di origine nella richiesta DNS diventano gli indirizzi di destinazione nella risposta DNS, e viceversa. Questo comportamento è visibile nei pacchetti catturati:

- **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`).



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`).



🔑 **Chiavi**:

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