# REPORT S11/L3

# Cisco CyberOps 3

## Traccia

**Esplorazione del Traffico DNS**

In questo laboratorio, completa i seguenti obiettivi:

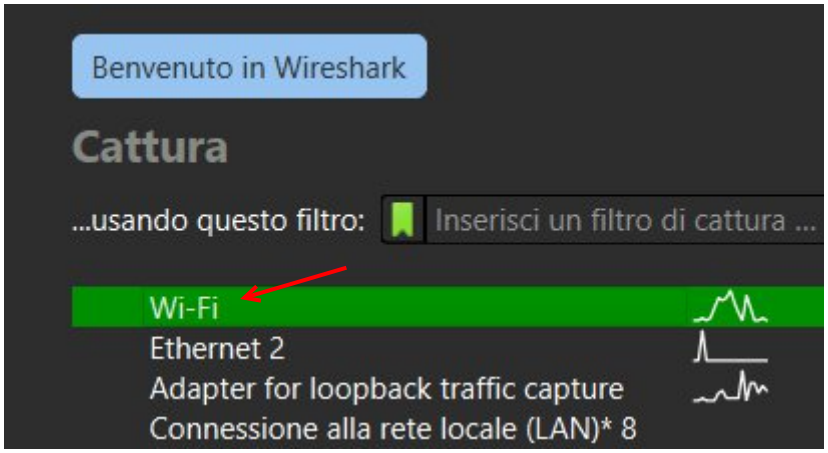
- Catturare il traffico DNS
- Esplorare il traffico delle query DNS
- Esplorare il traffico delle risposte DNS

## Svolgimento

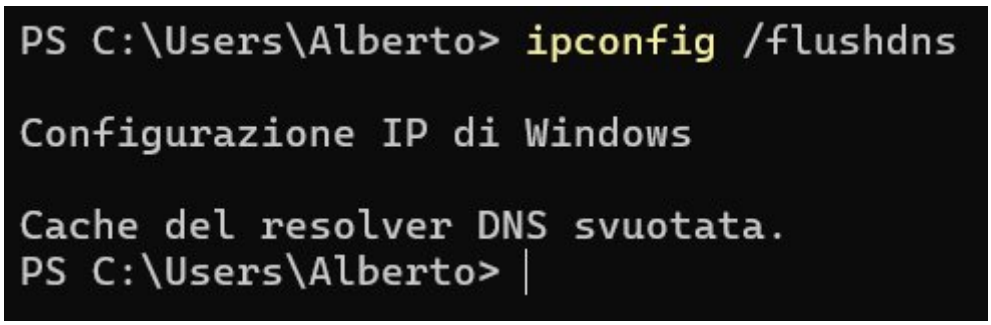
Wireshark è uno strumento di acquisizione e analisi di pacchetti open source. Consente di filtrare il traffico per la risoluzione dei problemi di rete, indagare sui problemi di sicurezza e analizzare i protocolli di rete. Poiché Wireshark ti consente di visualizzare i dettagli del pacchetto, può essere utilizzato come strumento di ricognizione per un utente malintenzionato.

### Parte 1: Cattura il traffico DNS

Per catturare il traffico DNS con Wireshark avviamo il programma e selezioniamo un'interfaccia attiva con il traffico per l'acquisizione dei pacchetti.




Poi svuotiamo la chache dns tramite il comando ***ipconfig /flushdns***

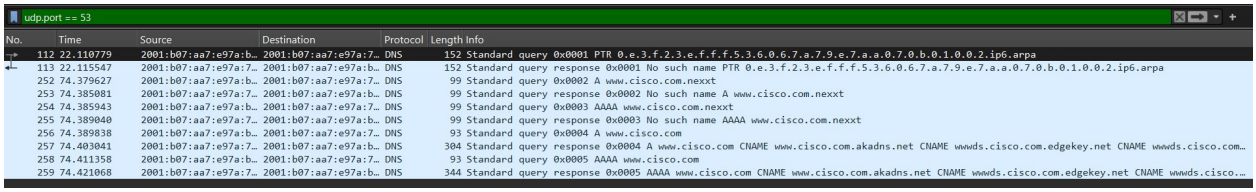


A questo punto avviamo la cattura dei pacchetti facendo doppio click sull'interfaccia scelta e contemporaneamente in una nuova finestra del terminale avviamo uno strumento utilizzato per interrogare server DNS (Domain Name System) e ottenere informazioni dettagliate riguardo ai nomi di dominio. Nel nostro caso questro strumento è **nslookup**, mentre il server (in questo caso sito) che prendiamo come esempio sarà **www.cisco.com**

```
PS C:\Users\Alberto> nslookup
Server predefinito:  UnKnown
Address:  2001:b07:aa7:e97a:7606:35ff:fe32:f3e0

> |
```

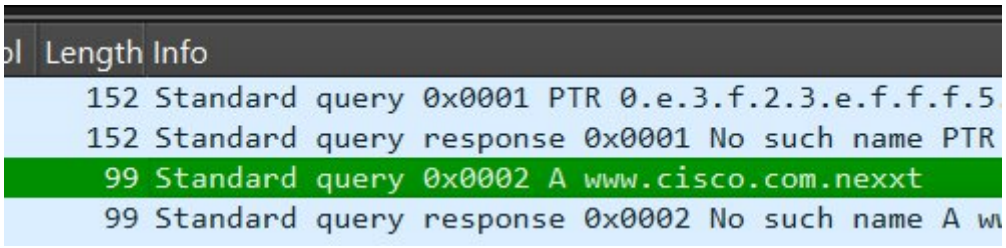
```
> www.cisco.com
Server:  UnKnown
Address:  2001:b07:aa7:e97a:7606:35ff:fe32:f3e0

Risposta da un server non autorevole:
Nome:    e2867.dsca.akamaiedge.net
Addresses:  2a02:26f0:8d00:ca9::b33
          2a02:26f0:8d00:c9e::b33
          23.209.77.25
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net

>
```

I risultati che otteniamo così su Wireshark sono decine, pertanto applichiamo un filtro per concentrarci sui pacchetti di nostro interesse. Il filtro sarà: **udp.port == 53** e quelli che vediamo sono i pacchetti di nostro interesse.

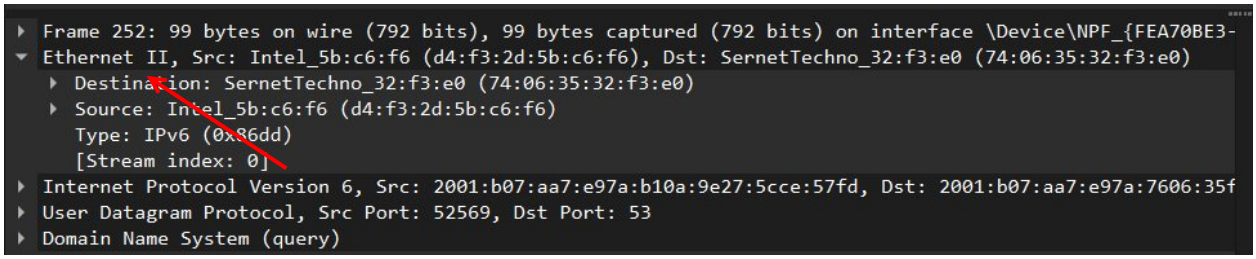


## Parte 1: Esplorare il traffico delle query DNS

Analizziamo ora in particolare il pacchetto che riporta la dicitura **Query standard** e **A www.cisco.com**

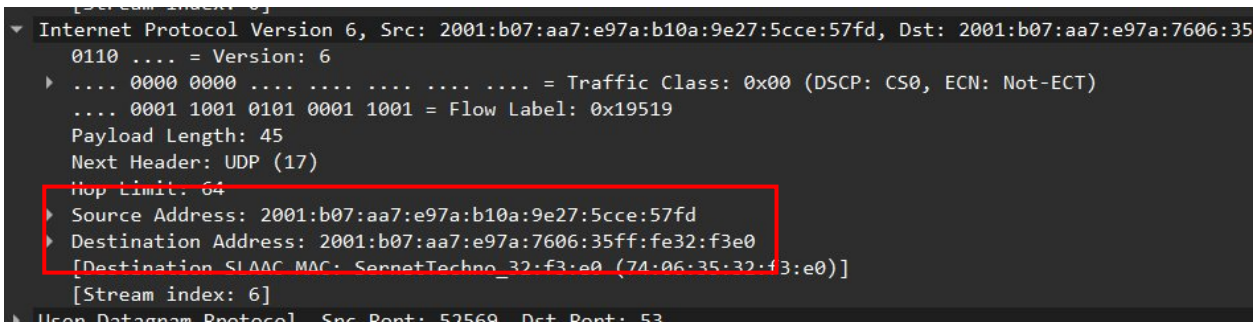



Dal **Riquadro Dettaglio** in basso possiamo estrarre delle informazioni interessanti, sopratuttto espandendo la voce **Ethernet II**.

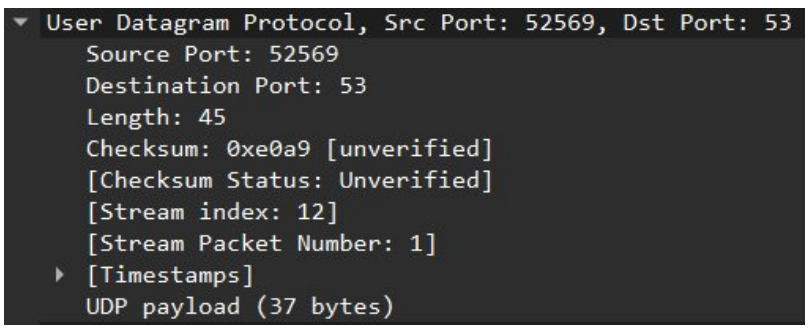



Nel nostro esempio, l'indirizzo MAC di origine è associato alla NIC sul PC e l'indirizzo MAC di destinazione è associato al gateway predefinito. Se è presente un server DNS locale, l'indirizzo MAC di destinazione sarebbe l'indirizzo MAC del server DNS locale.

Espandendo l'**Internet Protocol Version 6** possiamo estrarre gli indirizzi IP di origine e destinazione, che nel nostro caso sono indirizzi IPv6.




Dallo **User Datagram Protocol** vediamo quali sono state le porte usate per questa comunicazione:



## Parte 3: Esplorare il traffico delle risposte DNS

Selezioniamo la risposta corrispondente che presenta **Standard query response** e **A www.cisco.com** nella colonna Informazioni.

Come ci potremmo aspettare adesso l'IP di origine, l'indirizzo MAC e il numero di porta nel pacchetto di query sono ora indirizzi di destinazione, mentre quello di destinazione, l'indirizzo MAC e il numero di porta nel pacchetto di query sono ora indirizzi di origine.