Esplorazione del traffico DNS

Obiettivi

- **Parte 1 Catturare il Traffico DNS**
- **Parte 2 Esplorare il Traffico delle Query DNS**
- **Parte 3 Esplorare il Traffico delle Risposte DNS**

Cattura DNS

Avviamo wireshark.

```
C:\Windows\system32>ipconfig /flushdns

Configurazione IP di Windows

Cache del resolver DNS svuotata.

C:\Windows\system32>nslookup
Server predefinito:  one.one.one.one
Address:  1.1.1.1

> www.cisco.com
Server:  one.one.one.one
Address:  1.1.1.1

Risposta da un server non autorevole:
Nome:    e2867.dsca.akamaiedge.net
Addresses:  2a02:26f0:8d00:cb6::b33
          2a02:26f0:8d00:c9e::b33
          23.49.196.116
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

Stoppiamo la cattura di wireshark.

Esplorazione traffico DNS:

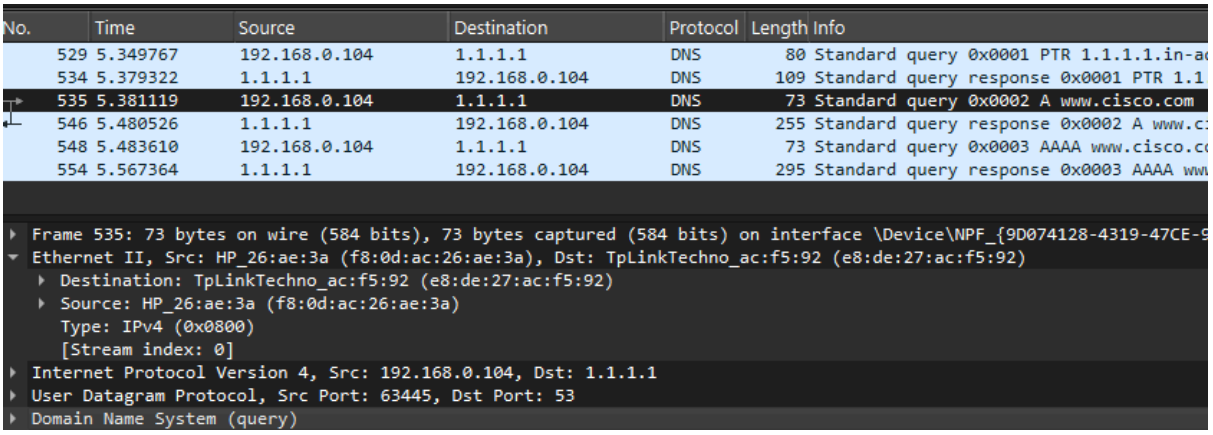
Nell'immagine sottostante si puo' verificare la richiesta fatta per CISCO:

udp.port == 53

No.	Time	Source	Destination	Protocol	Length	Info
529	5.349767	192.168.0.104	1.1.1.1	DNS	80	Standard query 0x0001 PTR 1.1.1.1.in-addr.arpa
534	5.379322	1.1.1.1	192.168.0.104	DNS	109	Standard query response 0x0001 PTR 1.1.1.1.in-add
535	5.381119	192.168.0.104	1.1.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
546	5.480526	1.1.1.1	192.168.0.104	DNS	255	Standard query response 0x0002 A www.cisco.com CN
548	5.483610	192.168.0.104	1.1.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
554	5.567364	1.1.1.1	192.168.0.104	DNS	295	Standard query response 0x0003 AAAA www.cisco.com

Analisi dettagli ETHERNET II

A livello Ethernet, il pacchetto viaggia dal PC (MAC `f8:0d:ac:26:ae:3a`, HP) verso il CPE domestico (MAC `e8:de:27:ac:f5:92`, TP-Link), che poi si occuperà di inoltrarlo su internet.



MAC sorgente: `f8:0d:ac:26:ae:3a`

Appartiene al computer HP, come indicato dal prefisso OUI `f8:0d:ac` registrato a **HP Inc.**

MAC destinazione: `e8:de:27:ac:f5:92`

Appartiene al **CPE/router TP-Link**, come indicato dal prefisso OUI `e8:de:27`, registrato a **TP-LINK TECHNOLOGIES.**

Analisi dettagli IPv4

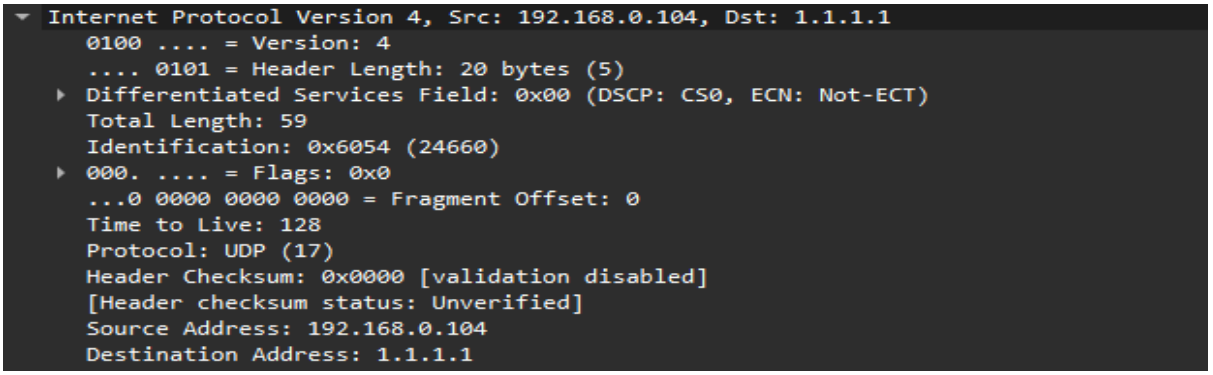
Gli indirizzi IP riportati nell'intestazione del pacchetto sono:

- **IP origine:** `192.168.0.104`

Questo e' l'indirizzo IPv4 privato locale assegnato dinamicamente alla scheda di rete del computer.

- **IP destinazione:** `1.1.1.1`

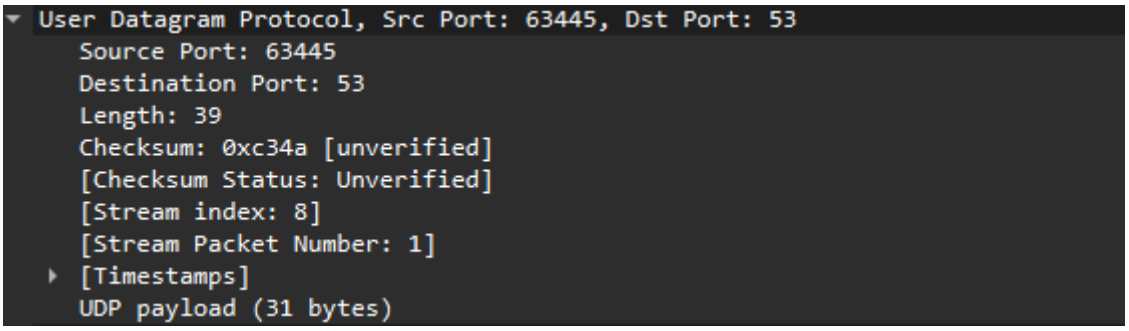
Questo IP pubblico e' assegnato staticamente alla scheda di rete del server DNS gestito da CloudFlare.



Analisi dettagli protocollo UDP

La comunicazione è avvenuta dalla porta **sorgente 63445** verso la porta di **destinazione 53.**

La porta **63445** è stata scelta casualmente dall'host tra quelle effimere (libere e non assegnate a servizi specifici), mentre la porta **53** è quella predefinita per il servizio **DNS** fornito da **Cloudflare.**



Determinazione indirizzi IP e MAC del pc

Indirizzi raccolti da wireshark:

(host HP)

MAC Sorgente: `f8-0d-ac-26-ae-3a`

IPv4 Sorgente: `192.168.0.114`

(gateway)

MAC Destinatario: `e8-de-27-ac-f5-92`

IPv4 Destinatario: `192.168.0.1`

ARP -A

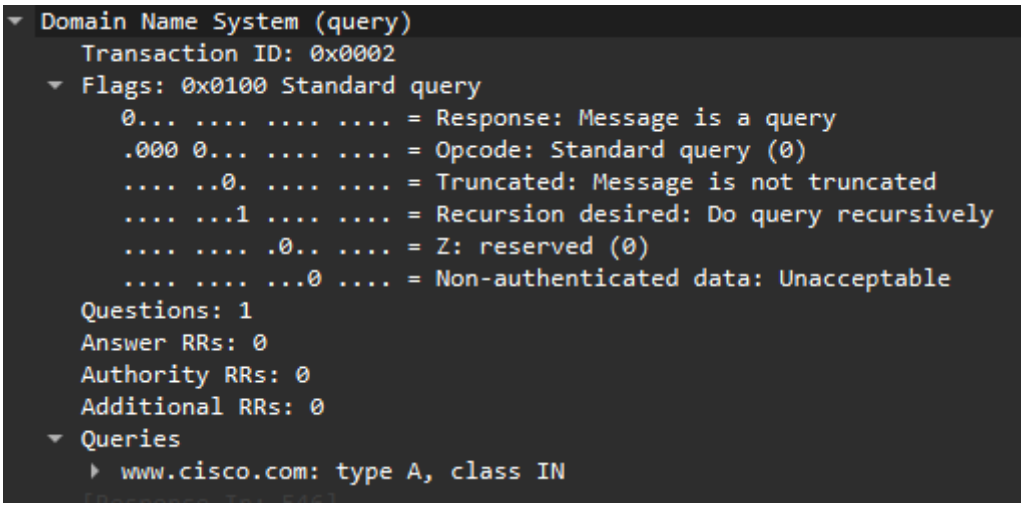
```
Interfaccia: 192.168.0.104 --- 0x11
  Indirizzo Internet    Indirizzo fisico      Tipo
  192.168.0.1           e8-de-27-ac-f5-92     dinamico
```

ifconfig /all

```
Suffisso DNS specifico per connessione:
Descrizione . . . . . . . . . . . . . . : Realtek Gaming GbE Family Controller
Indirizzo fisico. . . . . . . . . . . . : F8-0D-AC-26-AE-3A
DHCP abilitato. . . . . . . . . . . . . : Sì
Configurazione automatica abilitata   : Sì
Indirizzo IPv6 locale rispetto al collegamento . : fe80::efe4:5d64:e8dd:93ce%1
Indirizzo IPv4. . . . . . . . . . . . . : 192.168.0.104(Preferenziale)
Subnet mask . . . . . . . . . . . . . . : 255.255.255.0
Lease ottenuto. . . . . . . . . . . . . : giovedì 12 giugno 2025 08:51:05
Scadenza lease . . . . . . . . . . . .  : giovedì 12 giugno 2025 13:51:03
Gateway predefinito . . . . . . . . . . : fe80::8f3:92ff:fe9b:5d34%17
                                          192.168.0.1
Server DHCP . . . . . . . . . . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . . . . . . . . . . : 167251372
DUID Client DHCPv6. . . . . . . . . . . : 00-01-00-01-27-77-BC-27-F8-0D-AC-26-AE-3A
Server DNS . . . . . . . . . . . . . . .  : 1.1.1.1
```

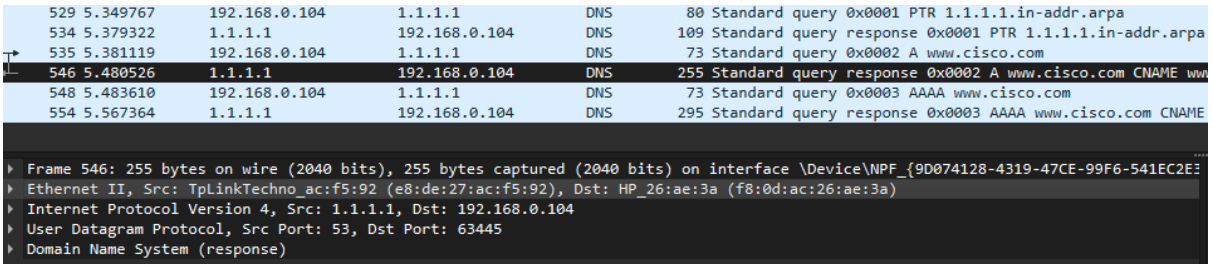
Confrontando i dati acquisiti da Wireshark con le informazioni ottenute tramite il command prompt, è possibile verificare la correttezza degli indirizzi rilevati.
In particolare, si osserva che gli indirizzi **MAC e IP dell'host** corrispondono a quelli restituiti dai comandi `ipconfig /all` e `arp -a`. Analogamente, anche gli indirizzi **MAC e IP del gateway** risultano coerenti con quelli riportati nella tabella ARP. Infine, si conferma la correttezza dell'indirizzo del server DNS, visibile nell'ultima riga dell'output di `ipconfig /all`.

Scheda Domain Name System



Parte 3 Esplorare il Traffico delle Risposte DNS

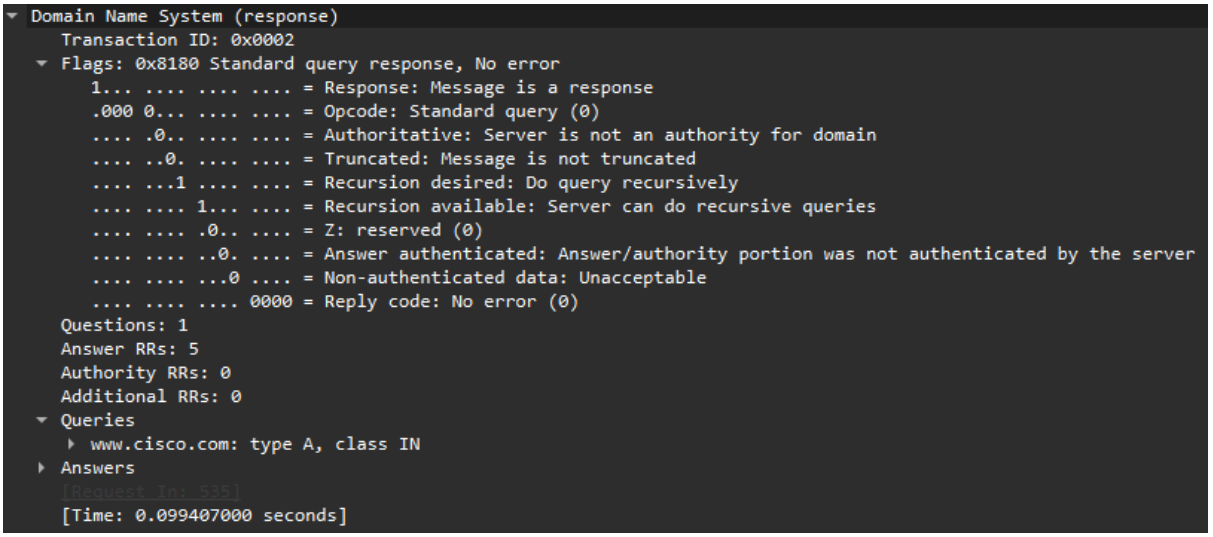
Risposta DNS:



Gli indirizzi MAC e IP e i numeri di porta di destinazione e di sorgente sono uguali ai precedenti, ma essendo questa la risposta alla richiesta fatta prima, saranno invertiti, nel modo seguente:

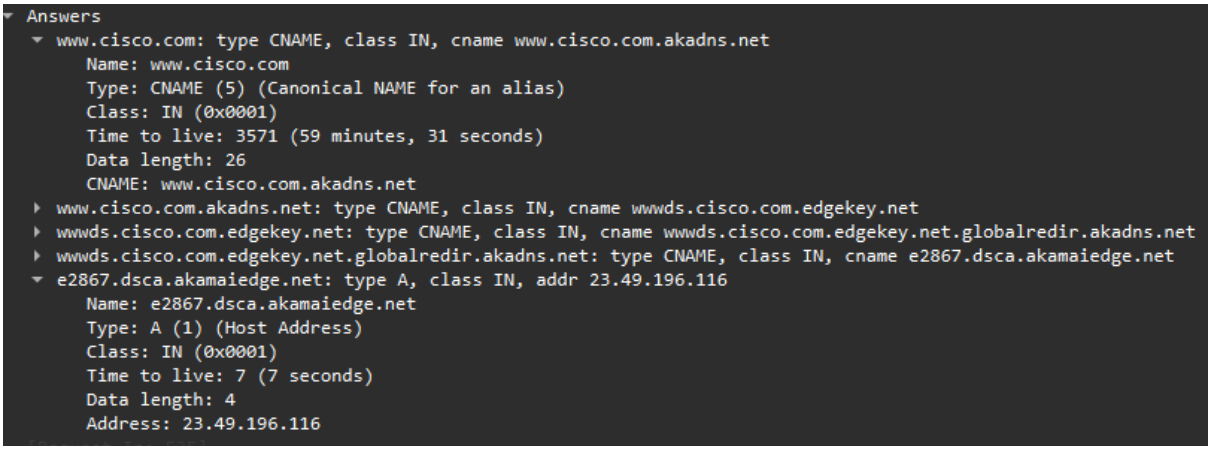
Sorgente:
(gateway locale)
e8:de:27:ac:f5:92
1.1.1.1 → 192.168.0.1
port 53
Destinazione:
(host HP)
f8:0d:ac:26:ae:3a
192.168.0.104
port 63445

Scheda DNS della risposta:



Nella sotto-scheda **Flags** e' impostato ad 1 (True) il flag descritto come
`"Recursion available: server can do recursive queries"`
Quindi si, **il server puo' fare query ricorsive.**

Scheda Answers:



Wireshark consente di vedere **tutti i passaggi della risoluzione DNS**, inclusi i **CNAME intermedi**, che mostrano come il dominio `www.cisco.com` venga instradato attraverso diversi alias (tipicamente legati a CDN come Akamai).

Nslookup, invece, mostra solitamente solo l'indirizzo IP finale o, al massimo, un solo alias CNAME.

Riflessione

1. Dai risultati di Wireshark, cos'altro puoi imparare sulla rete quando rimuovi il filtro?
2. Come può un attaccante usare Wireshark per compromettere la sicurezza della tua rete?

1. Rimuovendo i filtri da Wireshark è possibile osservare l'intero traffico di rete in tempo reale, il che consente di raccogliere informazioni utili per comprendere la topologia della rete, individuare i dispositivi connessi, i protocolli utilizzati e identificare eventuali traffici sospetti o non cifrati. Questa visione globale è utile per analisi di sicurezza e diagnostica.

2. Se un attaccante ha accesso alla rete locale e utilizza Wireshark, può intercettare traffico non cifrato (es. HTTP, DNS, FTP) e raccogliere informazioni sensibili come credenziali, token di sessione, o dettagli sull'infrastruttura. Può inoltre analizzare il comportamento dei dispositivi in rete e pianificare attacchi mirati come ARP spoofing o man-in-the-middle.