

## PULIZIA CACHE DNS

Essendo non funzionanti le utility consigliate, ho installato per la mia distribuzione quella che segue, prima controllando l'effettiva presenza all'interno del mio sistema operativo e poi a seguire l'installazione fino al restart e la pulizia della cache DNS.

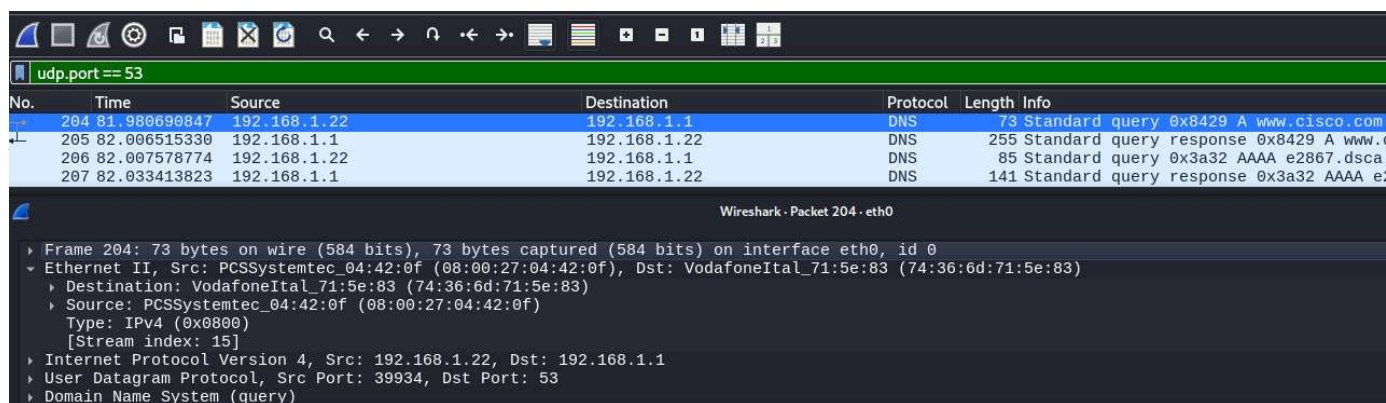
```
(kali㉿kali)-[~]
$ dpkg -s resolvconf
dpkg-query: package 'resolvconf' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.

(kali㉿kali)-[~]
$ sudo apt update

(kali㉿kali)-[~]
$ sudo apt install resolvconf

(kali㉿kali)-[~]
$ sudo systemctl restart NetworkManager
```

## ESPLORARE IL TRAFFICO DELLE QUERY DNS



No.	Time	Source	Destination	Protocol	Length	Info
204	81.980690847	192.168.1.22	192.168.1.1	DNS	73	Standard query 0x8429 A www.cisco.com
205	82.006515330	192.168.1.1	192.168.1.22	DNS	255	Standard query response 0x8429 A www.cisco.com
206	82.007578774	192.168.1.22	192.168.1.1	DNS	85	Standard query 0x3a32 AAAA e2867.dsca.com
207	82.033413823	192.168.1.1	192.168.1.22	DNS	141	Standard query response 0x3a32 AAAA e2867.dsca.com

Wireshark - Packet 204 - eth0

- Frame 204: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
- Ethernet II, Src: PCSSystemtec\_04:42:0f (08:00:27:04:42:0f), Dst: VodafoneItal\_71:5e:83 (74:36:6d:71:5e:83)
  - Destination: VodafoneItal\_71:5e:83 (74:36:6d:71:5e:83)
  - Source: PCSSystemtec\_04:42:0f (08:00:27:04:42:0f)
  - Type: IPv4 (0x0800)
- [Stream index: 15]
- Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 39934, Dst Port: 53
- Domain Name System (query)

### 1) Quali sono gli indirizzi MAC di origine e destinazione?

L'indirizzo MAC di origine è (08:00:27:04:42:0f)

L'indirizzo MAC di destinazione è (74:36:6d:71:5e:83)

### 2) A quali interfacce di rete sono associati questi indirizzi MAC?

L'indirizzo MAC di origine è associata a l'interfaccia di rete PCSSystemtec\_04:42:0f

L'indirizzo MAC di destinazione è associato a l'interfaccia di rete VodafoneItal\_71:5e:83

### 3) Quali sono gli indirizzi IP di origine e destinazione?

L'indirizzo IP di origine è 192.168.1.22

L'indirizzo IP di destinazione è 192.168.1.1

### 4) A quali interfacce di rete sono associati questi indirizzi IP?

L'indirizzo IP di origine 192.168.1.22 è associato all'interfaccia eth0.

L'indirizzo IP di destinazione 192.168.1.1 è associato all'interfaccia di rete del server DNS (il mio router).

## 5) Quali sono le porte di origine e destinazione?

No.	Time	Source	Destination	Protocol	Length	Info
204	81.980690847	192.168.1.22	192.168.1.1	DNS	73	Standard query 0x8429 A www.cisco.com
205	82.006515330	192.168.1.1	192.168.1.22	DNS	255	Standard query response 0x8429 A www.cisc
206	82.007578774	192.168.1.22	192.168.1.1	DNS	85	Standard query 0x3a32 AAAA e2867.dsca.aka
207	82.033413823	192.168.1.1	192.168.1.22	DNS	141	Standard query response 0x3a32 AAAA e2867

Wireshark - Packet 204 - eth0	
▶ Frame 204: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0	
▶ Ethernet II, Src: PCSSystemtec_04:42:0f (08:00:27:04:42:0f), Dst: VodafoneIta_71:5e:83 (74:36:6d:71:5e:83)	
▶ Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.1	
▼ User Datagram Protocol, Src Port: 39934, Dst Port: 53	
Source Port: 39934	
Destination Port: 53	

La porta di origine è la 39934. La porta di destinazione è la 53.

## 6) Qual è il numero di porta DNS predefinito?

Il numero predefinito della porta dedicata al DNS è la 53

## 7) Confrontare gli indirizzi MAC e IP nei risultati di Wireshark con gli indirizzi IP e MAC. Qual è la tua osservazione?

Gli indirizzi IP e gli indirizzi MAC sono coerentemente associati per identificare i dispositivi sorgente e destinazione nella rete locale. Il traffico di livello 2 (Ethernet, che usa i MAC address) trasporta il traffico di livello 3 (IP, che usa gli IP address) per stabilire la comunicazione tra i dispositivi.

In questo specifico scenario, si sta osservando una tipica comunicazione tra un client (la mia Kali Linux con IP 192.168.1.22 e un MAC virtuale) e il suo gateway/server DNS (il mio router Vodafone con IP 192.168.1.1 e un MAC Vodafone).

## 8) Quali sono gli indirizzi MAC e IP e i numeri di porta di origine e destinazione?

Time	Source	Destination	Protocol	Length	Info
204	81.980690847	192.168.1.22	192.168.1.1	DNS	73 Standard query 0x8429 A www.cisco.com
205	82.006515330	192.168.1.1	192.168.1.22	DNS	255 Standard query response 0x8429 A www.cisc
206	82.007578774	192.168.1.22	192.168.1.1	DNS	85 Standard query 0x3a32 AAAA e2867.dsca.aka
207	82.033413823	192.168.1.1	192.168.1.22	DNS	141 Standard query response 0x3a32 AAAA e2867

Wireshark - Packet 205 - eth0	
▶ Frame 205: 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on interface eth0, id 0	
▶ Ethernet II, Src: VodafoneIta_71:5e:83 (74:36:6d:71:5e:83), Dst: PCSSystemtec_04:42:0f (08:00:27:04:42:0f)	
▶ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.22	
▼ User Datagram Protocol, Src Port: 53, Dst Port: 39934	
Source Port: 53	
Destination Port: 39934	

### ORIGINE:

MAC: (74:36:6d:71:5e:83)

IP: 192.168.1.1

PORTA: 53

### DESTINAZIONE:

MAC: (08:00:27:04:42:0f)

IP: 192.168.1.22

PORTA: 39934

## 9) Come si confrontano con gli indirizzi nei pacchetti di query DNS?

udp.port == 53					
Time	Source	Destination	Protocol	Length	Info
204 81.980690847	192.168.1.22	192.168.1.1	DNS	73	Standard query 0x8429 A www.cisco.com
205 82.006515330	192.168.1.1	192.168.1.22	DNS	255	Standard query response 0x8429 A www.cisco.com
206 82.007578774	192.168.1.22	192.168.1.1	DNS	85	Standard query 0x3a32 AAAA e2867.dsca.akam
207 82.033413823	192.168.1.1	192.168.1.22	DNS	141	Standard query response 0x3a32 AAAA e2867.dsca.akam

Wireshark - Packet 205 - eth0

- Ethernet II, Src: VodafoneItal\_71:5e:83 (74:36:6d:71:5e:83), Dst: PCSSystemtec\_04:42:0f (08:00:27:04:42:0f)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.22
- User Datagram Protocol, Src Port: 53, Dst Port: 39934
- Domain Name System (response)
  - Transaction ID: 0x8429
  - 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
    - [\[Request In: 204\]](#)
    - [Time: 0.025824483 seconds]

I pacchetti di risposta DNS riflettono l'esatto scambio inverso degli indirizzi di sorgente e destinazione (sia IP che MAC) rispetto ai pacchetti di query corrispondenti, indicando un flusso di comunicazione DNS standard e di successo.

## 10) Il server DNS può fare query ricorsive?

udp.port == 53					
No.	Time	Source	Destination	Protocol	Length Info
204	81.980690847	192.168.1.22	192.168.1.1	DNS	73 Standard query 0x8429 A www.cisco.com
205	82.006515330	192.168.1.1	192.168.1.22	DNS	255 Standard query response 0x8429 A www.cisco.com
206	82.007578774	192.168.1.22	192.168.1.1	DNS	85 Standard query 0x3a32 AAAA e2867.dsca.akam
207	82.033413823	192.168.1.1	192.168.1.22	DNS	141 Standard query response 0x3a32 AAAA e2867.dsca.akam

Wireshark - Packet 205 - eth0

- Ethernet II, Src: VodafoneItal\_71:5e:83 (74:36:6d:71:5e:83), Dst: PCSSystemtec\_04:42:0f (08:00:27:04:42:0f)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.22
- User Datagram Protocol, Src Port: 53, Dst Port: 39934
- Domain Name System (response)
  - Transaction ID: 0x8429
  - 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
    - [\[Request In: 204\]](#)
    - [Time: 0.025824483 seconds]

Alla sezione “Domain Name System (query)” del pacchetto, alla voce “Flags” trovo:

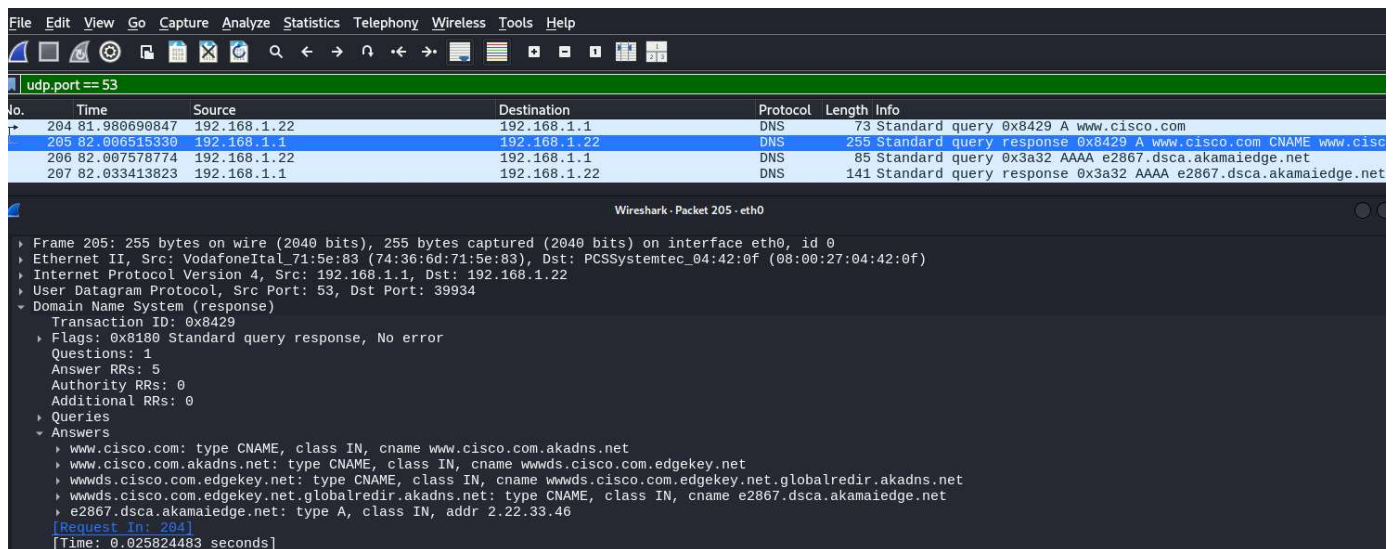
```
.... 1... = Recursion available: Server can do recursive queries
```

Questo flag indica che il server DNS (192.168.1.1) supporta e può eseguire query ricorsive. La presenza di questo flag nella risposta significa che il server ha la capacità di offrire il servizio di risoluzione ricorsiva ai client.

## 11) Come si confrontano i risultati con quelli di nslookup?

```
(kali@kali)-[~]
$ nslookup
> www.cisco.com
Server:      192.168.1.1
Address:     192.168.1.1#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.akamaiedge.net.
Name:   e2867.dsca.akamaiedge.net
Address: 2.22.33.46
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d80:1a3::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d80:197::b33
```



Wireshark - Packet 205 - eth0

Frame 205: 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on interface eth0, id 0

Ethernet II, Src: VodafoneIta1\_71:5e:83 (74:36:6d:71:5e:83), Dst: PCSSystemtec\_04:42:0f (08:00:27:04:42:0f)

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.22

User Datagram Protocol, Src Port: 53, Dst Port: 39934

Domain Name System (response)

Transaction ID: 0x8429

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 5

Authority RRs: 0

Additional RRs: 0

Queries

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 2.22.33.46

[Request In: 204]

[Time: 0.025824483 seconds]

I risultati di Wireshark e nslookup sono coerenti e forniscono le stesse informazioni logiche sulla risoluzione del nome di dominio ([www.cisco.com](http://www.cisco.com) che punta a 2.22.33.46) tramite CNAMEs). La differenza sta nel livello di dettaglio e nel formato di presentazione. Wireshark mostra gli elementi grezzi del pacchetto e il loro assemblaggio, mentre nslookup interpreta questi elementi e presenta il risultato della risoluzione in un formato più leggibile per l'utente finale.



# RIFLESSIONE

## 1) Dai risultati di Wireshark, cos'altro puoi imparare sulla rete quando rimuovi il filtro?

Rimuovendo il filtro ho una visione più ampia di analisi che mi permette di monitorare le attività del traffico. Nel caso preso in esame, vedo un ventaglio di protocolli più sfaccettato tra cui:

- MDNS: trova dispositivi locali per nome senza server DNS centrale
- STP: Previene loop in reti con switch.
- UDP: Trasporto dati veloce ma non garantito.
- ICMP: Messaggi di errore e diagnostica.
- ICMPv6: ICMP per reti IPv6.
- DHCP: Assegna automaticamente indirizzi IP ai dispositivi.
- ARP: Mappa indirizzi IP a MAC address su rete locale.
- DNS: Traduce nome di dominio in indirizzi IP.
- SSDP: Scopre servizi e dispositivi UpnP sulla rete locale.

## 2) Come può un attaccante usare Wireshark per compromettere la sicurezza della tua rete?

Wireshark è uno strumento potente per la diagnostica di rete, ma nelle mani di un attaccante diventa un messo efficace per la ricognizione, l'intercettazione di dati sensibili e l'identificazione di punti deboli sfruttando la mancanza di crittografia o un'architettura di rete non sicura.