

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

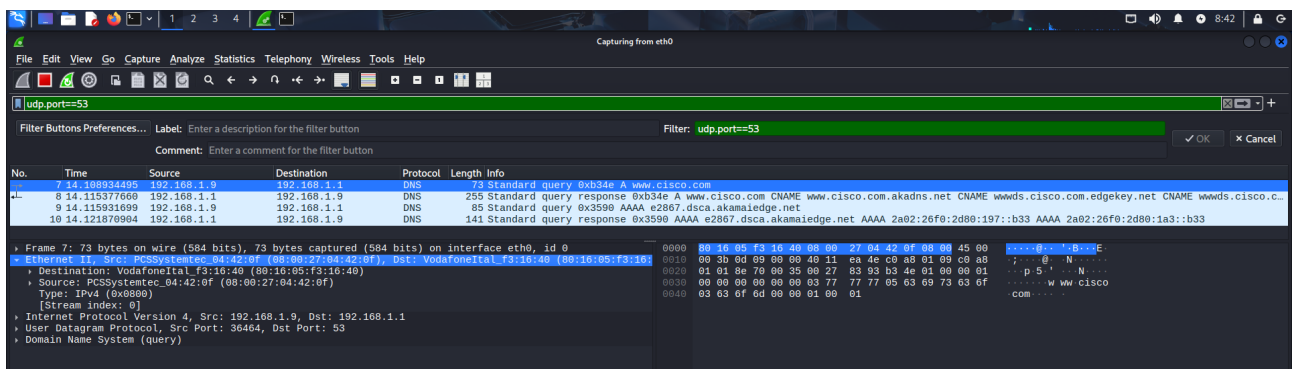
Indirizzi MAC:

- MAC di origine: 08:00:27:04:42:0f
- MAC di destinazione: 80:16:05:f3:16:40

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

Associazione interfacce rete:

- MAC di origine: certamente l'interfaccia della macchina virtuale
- MAC di destinazione (80:16:05:f3:16:40): l'interfaccia del router (in questo caso Vodafone).



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

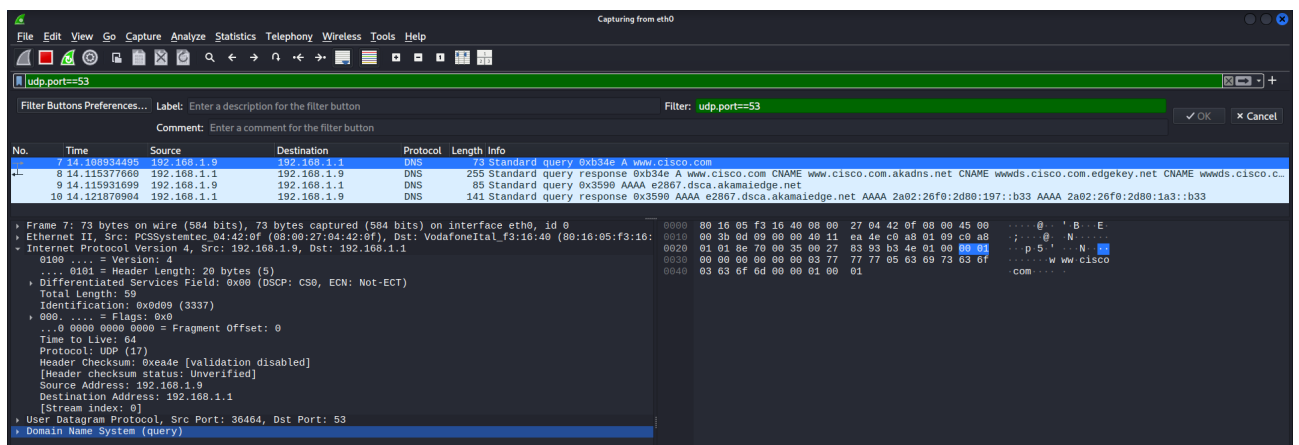
Indirizzi IP:

- Indirizzo IP di origine: 192.168.1.9
- Indirizzo IP di destinazione: 192.168.1.1

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

Associazione con le interfacce di rete:

- Indirizzo IP di origine: È l'indirizzo IP della macchina virtuale
- Indirizzo IP di destinazione: È l'indirizzo IP del gateway locale o del router



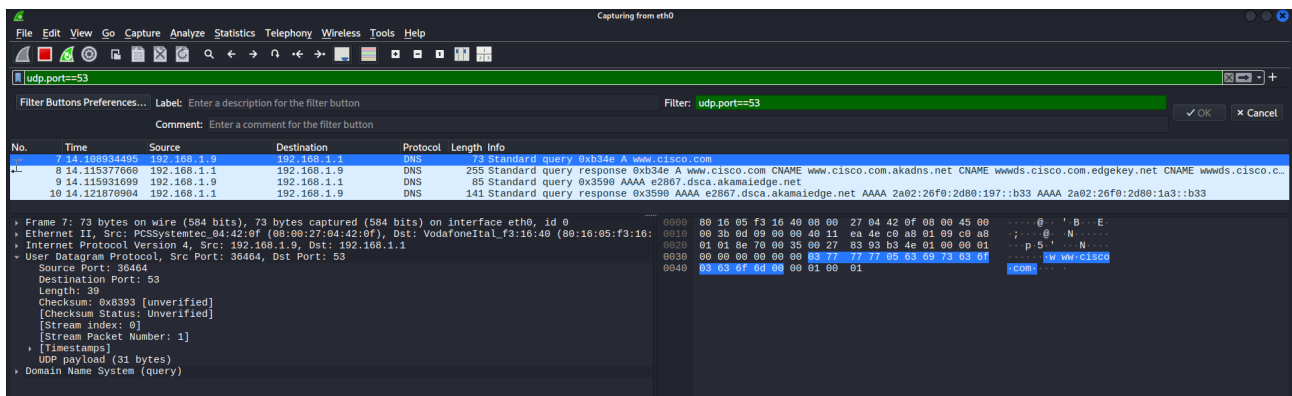
# Domanda 5: Quali sono le porte di origine e destinazione?

Porte:

- Porta di origine: 36464
- Porta di destinazione: 53

# Domanda 6: Qual è il numero di porta DNS predefinito?

- Porta DNS predefinita = 53 (UDP/TCP)



## Domanda 7: **Determinare l'indirizzo IP e MAC del PC. Confrontare gli indirizzi MAC e IP nei risultati di Wireshark con gli indirizzi IP e MAC. Qual è la tua osservazione?**

```
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.9 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::3ff9:c122:b3f2:7d48 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:04:42:0f txqueuelen 1000 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- **Indirizzo IP:** 192.168.1.9
- **Indirizzo MAC:** 08:00:27:04:42:0f

Gli indirizzi IP e MAC rilevati dal comando ifconfig **corrispondono** agli indirizzi IP e MAC presenti nel **pacchetto DNS** visualizzato in Wireshark. Questo conferma che il pacchetto DNS è stato **generato dalla nostra VM**

**Domanda 8: Selezionare il corrispondente pacchetto DNS di risposta che ha Standard query response e A www.cisco.com nella colonna Info. Quali sono gli indirizzi MAC e IP e i numeri di porta di origine e destinazione?**

**Indirizzi MAC:**

- **MAC Sorgente:** 80:16:05:f3:16:40
- **MAC Destinazione:** 08:00:27:04:42:

**Indirizzi IP:**

- **IP Sorgente:** 192.168.1.1
- **IP Destinazione:** 192.168.1.9

**Porte:**

- **Porta Sorgente:** 53
- **Porta Destinazione:** 36464

Nella **query DNS**, tutti questi valori saranno **invertiti**. Questo è il normale comportamento **request-response** del protocollo DNS

## Domanda 10: Il server DNS può fare query ricorsive?

Si, osservando i flag nella risposta DNS:

- Recursion desired: **Do query recursively**
- Recursion available: **Server can do recursive queries**

# Domanda 11: Osservare i record CNAME e A nei dettagli delle Risposte (Answers). Come si confrontano i risultati con quelli di nslookup?

```
(kali@kali)-[~] on wire (2840 bits), 288 bytes captured (2840 bits) on interface eth0, id 0
$ nslookup
> www.cisco.com
Server: 192.168.1.1
Address: 192.168.1.1#53

** server can't find www.cisco.com: NXDOMAIN
> 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: 2a02:26f0:2d80:197::b33
Name: e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d80:1a3::b33
>
Answers
www.cisco.com: type A, class IN
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: 7]
[Time: 0.006443165 seconds]
```

I risultati sono **uguali**. Questo dimostra che l'analisi del traffico DNS con **Wireshark** fornisce gli stessi dati che ottieni con strumenti da riga di comando come **nslookup**

## **Domanda 12: Come può un attaccante usare Wireshark per compromettere la sicurezza della tua rete?**

### **Analisi del Traffico Sensibile**

- Intercettazione di comunicazioni aziendali
- Cattura di dati personali o finanziari

### **Ricognizione Network**

- Identificazione di servizi attivi e versioni software
- Scoperta di indirizzi IP interni e struttura della rete

### **Dirottamento di sessione**

- Cattura dei cookie di sessione non protetti
- Furto di session ID per impersonare utenti legittimi

## **Domanda 13: Dai risultati di Wireshark, cos'altro puoi imparare sulla rete quando rimuovi il filtro?**



**Rimuovendo il filtro potremo vedere:**

- **Protocolli di Rete Utilizzati:** TCP, HTTP, ARP, UDP
- **Performance della Rete**
- **Potenziati Problemi di Sicurezza:** Traffico non crittografato, Porte aperte e servizi esposti, Comunicazioni sospette verso IP esterni