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

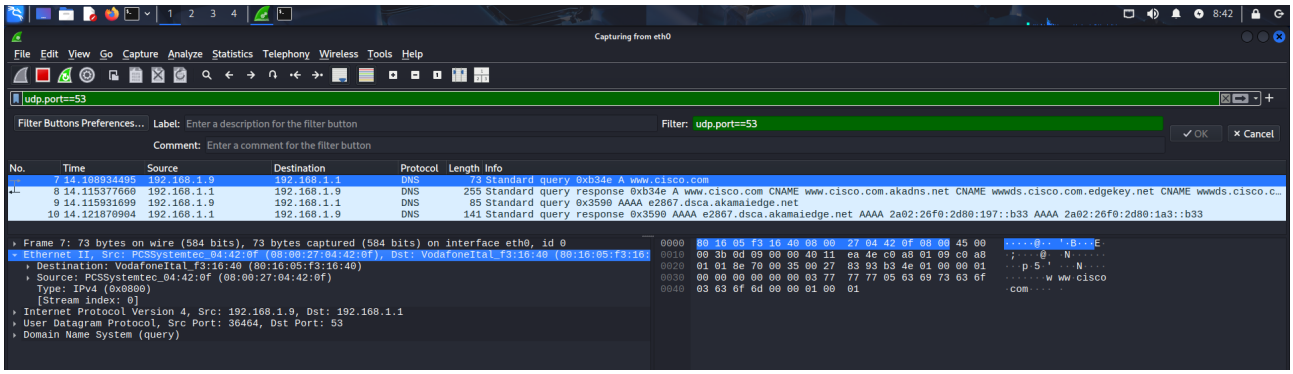
Indirizzi MAC:

- **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?**

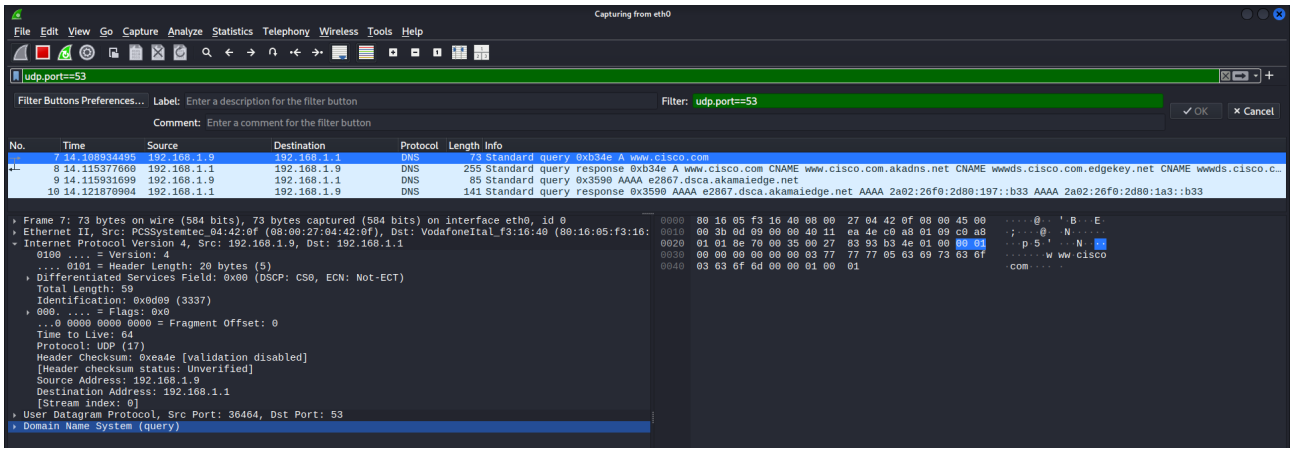
Indirizzi IP:

- **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**



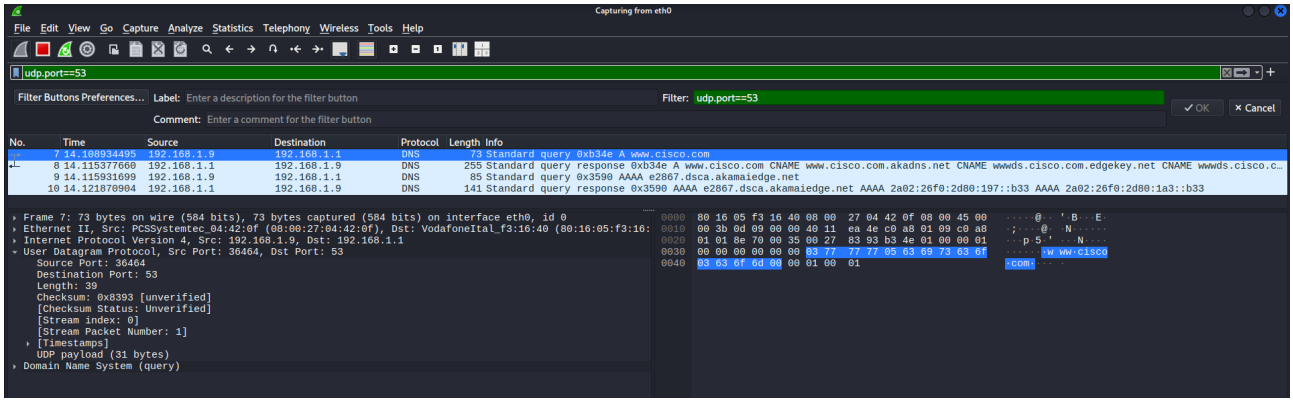
Domanda 5: **Quali sono le porte di origine e destinazione?**

Porte:

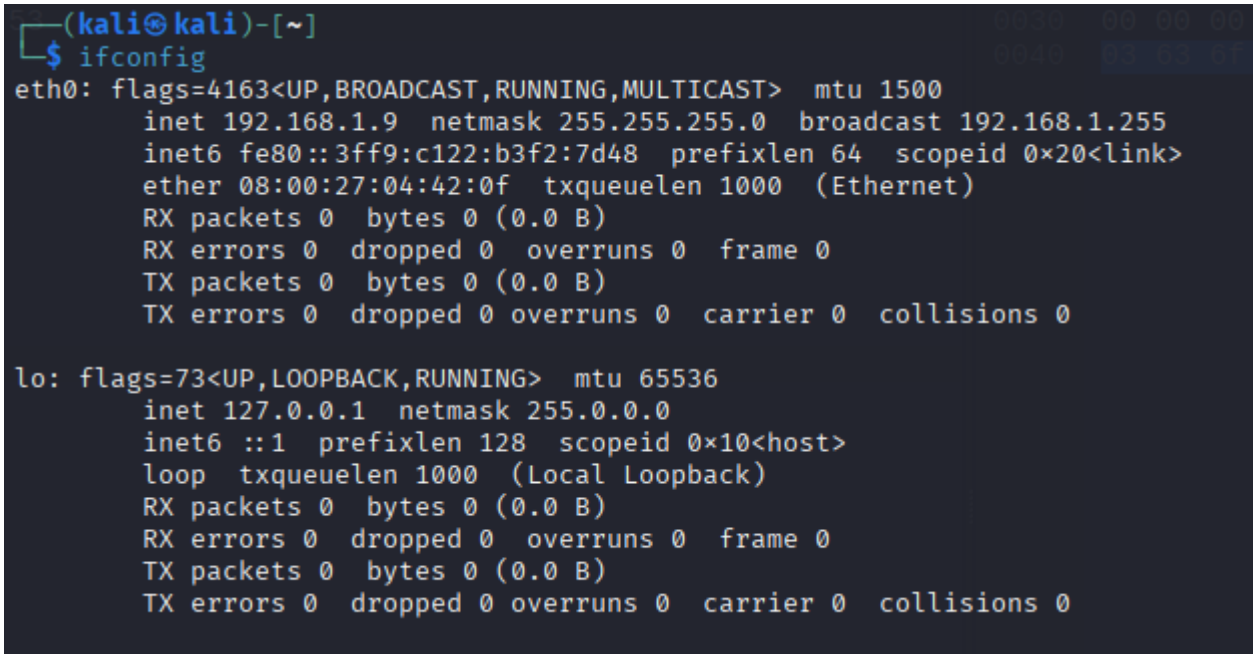
- **Porta di origine:** 36464
- **Porta di destinazione:** 53

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?**



- **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:

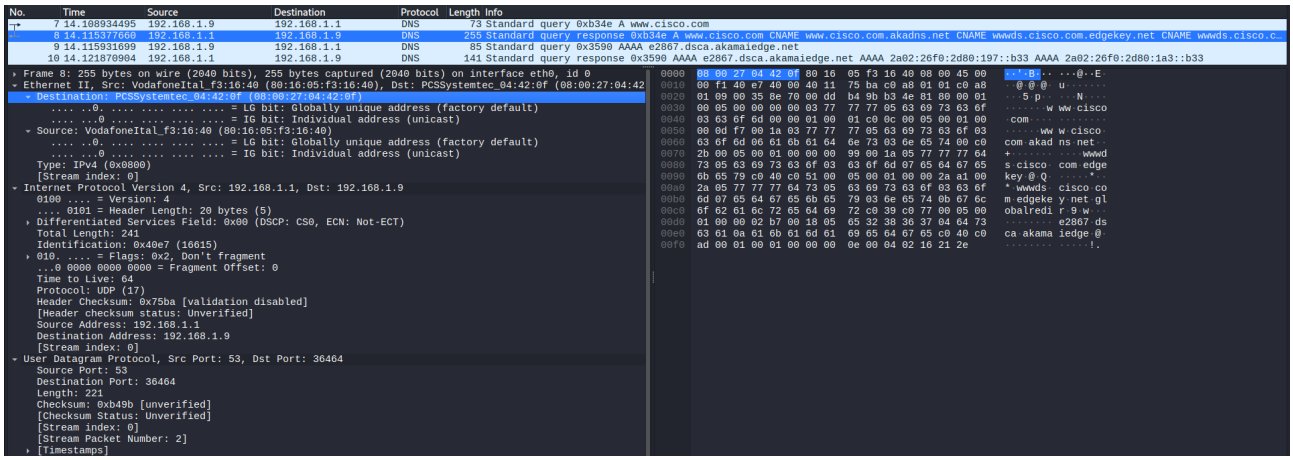
- **IP Sorgente:** 192.168.1.1
- **IP Destinazione:** 192.168.1.9

Porte:

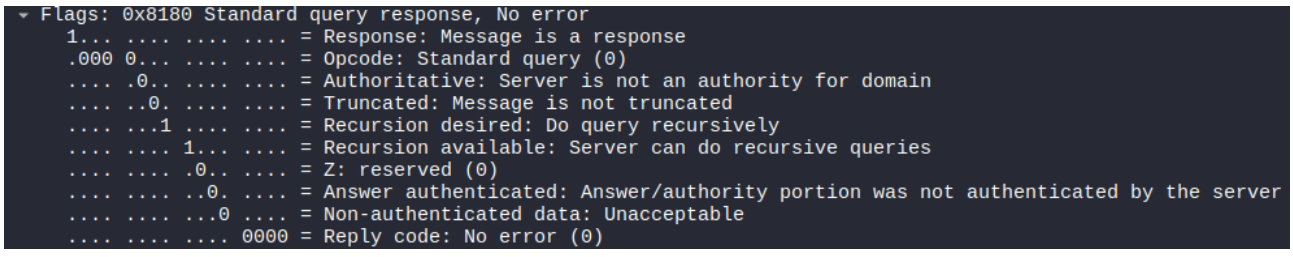
- **Porta Sorgente:** 53
- **Porta Destinazione:** 36464

Domanda 9: **Come si confrontano con gli indirizzi nei pacchetti di query DNS?**

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?**

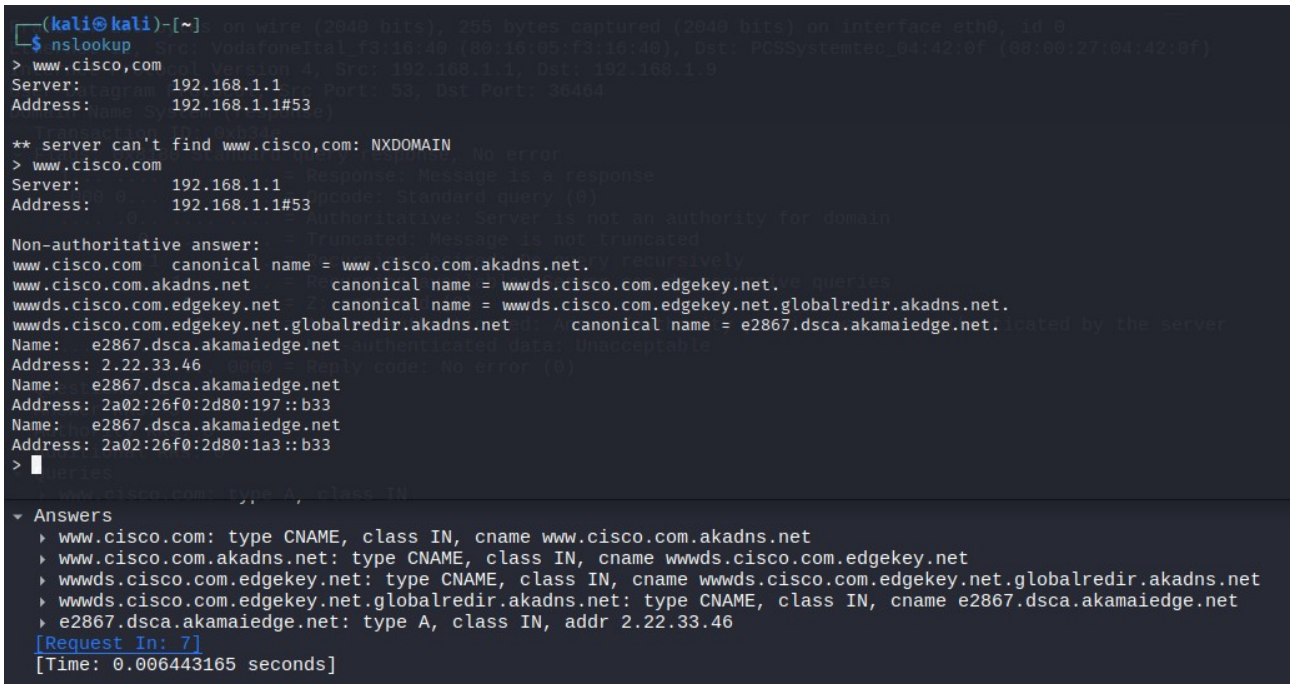


Si, osservando i flag nella risposta DNS:

Nelle Flags:

- 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?**



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**
- **Potenziali Problemi di Sicurezza:** Traffico non crittografato, Porte aperte e servizi esposti**,** Comunicazioni sospette verso IP esterni