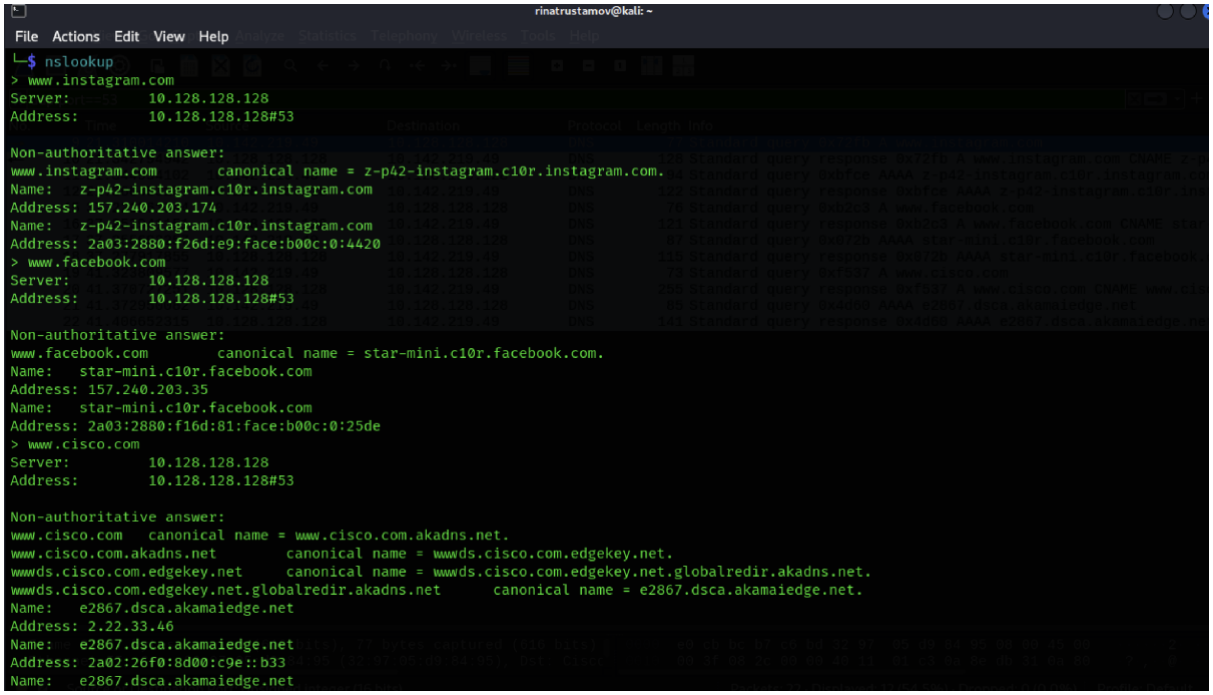
# RAPPORTO

## Catturare il traffico DNS

Ho deciso di riavviare il sistema per cancellare tutte le cache, incluso il DNS, poiché Kali Linux ha risposto negativamente a ciascuno dei seguenti comandi:

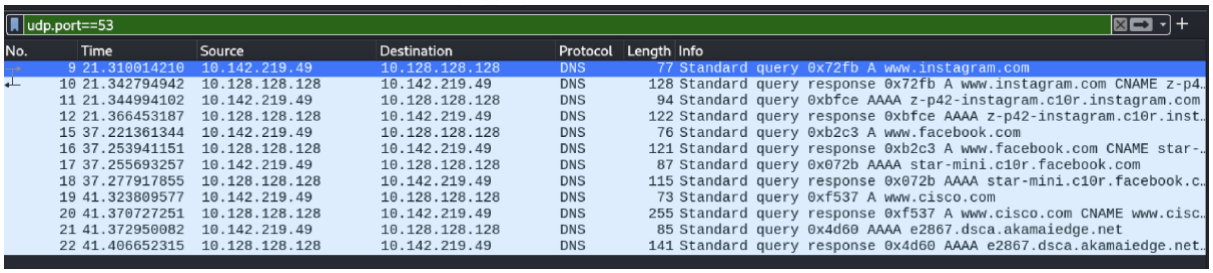
- sudo systemctl restart systemd-resolved.service
- sudo systemctl restart dnsmasq.service
- sudo systemctl restart nscd.service

Dopo il riavvio, ho prima abilitato Wireshark e poi ho comandato nslookup nel terminale Linux e ho cercato www.instagram.com e altri siti web. Poi ho chiuso nslookup e sono tornato a Wireshark per analizzare il traffico catturato:



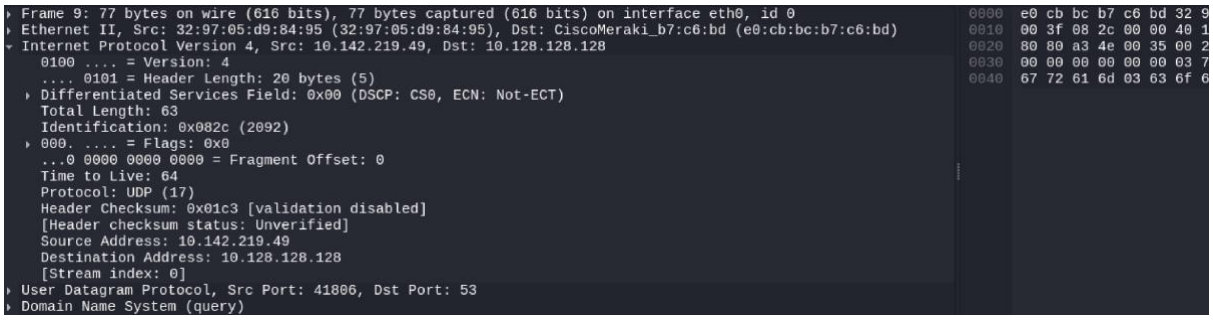

## Esplorare il traffico delle query DNS

Ho filtrato la porta 53 (DNS) per UDP:

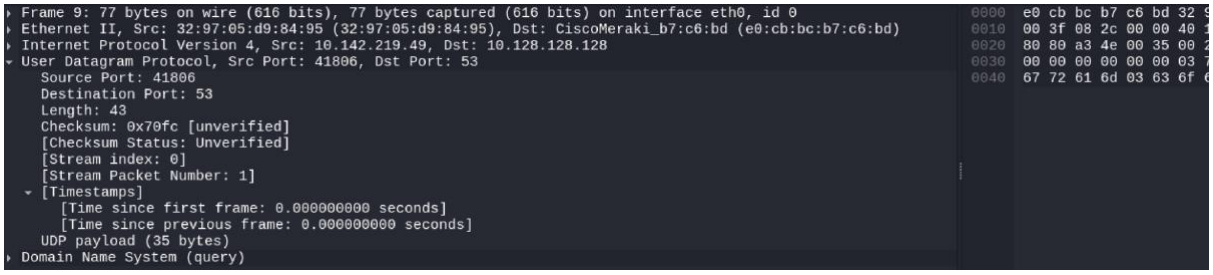


Ho scelto la prima cattura da analizzare. Ethernet II mostra gli indirizzi MAC sia del dispositivo sorgente (in questo caso Linux VM) sia del dispositivo di destinazione (il router):

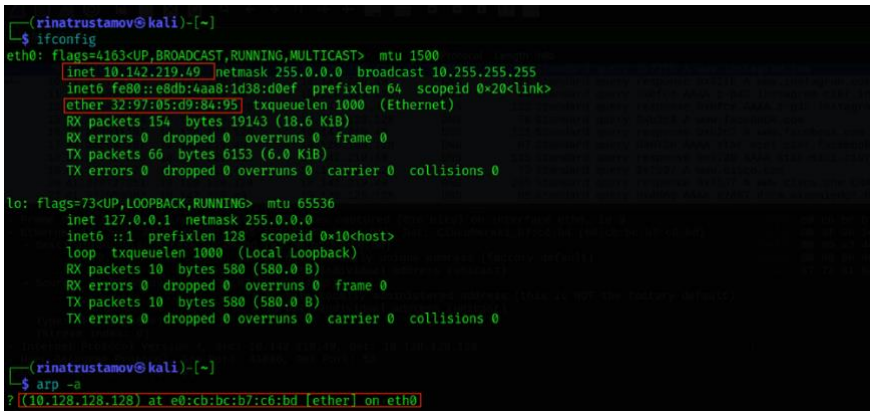

Il protocollo Internet versione 4 mostra gli indirizzi IP di origine e destinazione. L'indirizzo IP di destinazione è il gateway in questo caso:




In User Datagram Protocol (UDP), possiamo vedere le porte di origine e di destinazione. La porta di origine è 41806, mentre quella di destinazione è 53:

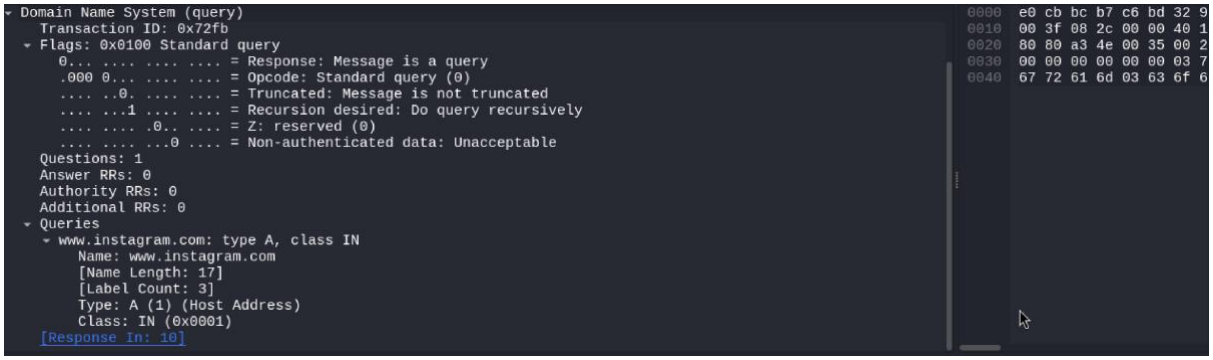



Possiamo verificare se le informazioni fornite in Wireshark corrispondono a quelle effettive scrivendo nel terminale arp -a e ifconfig:




E sì, corrispondono.

Nella sezione DNS del traffico catturato, possiamo vedere i flag. Tutti i flag sono stati impostati su 0, eccetto la ricorsione. Esegue query ricorsivamente:




## Esplorare il traffico delle risposte DNS

Ora scelgo il pacchetto di risposta corrispondente al primo caso che abbiamo analizzato. Tutti gli IP di destinazione e di origine, le porte, gli indirizzi MAC sono stati sostituiti rispetto al caso precedente. Inoltre, anche la query ricorsiva del server è impostata su 1. Ora vengono visualizzate le sezioni delle risposte in DNS, che sono identiche a quelle visualizzate sul terminale quando è stato richiesto nslookup: