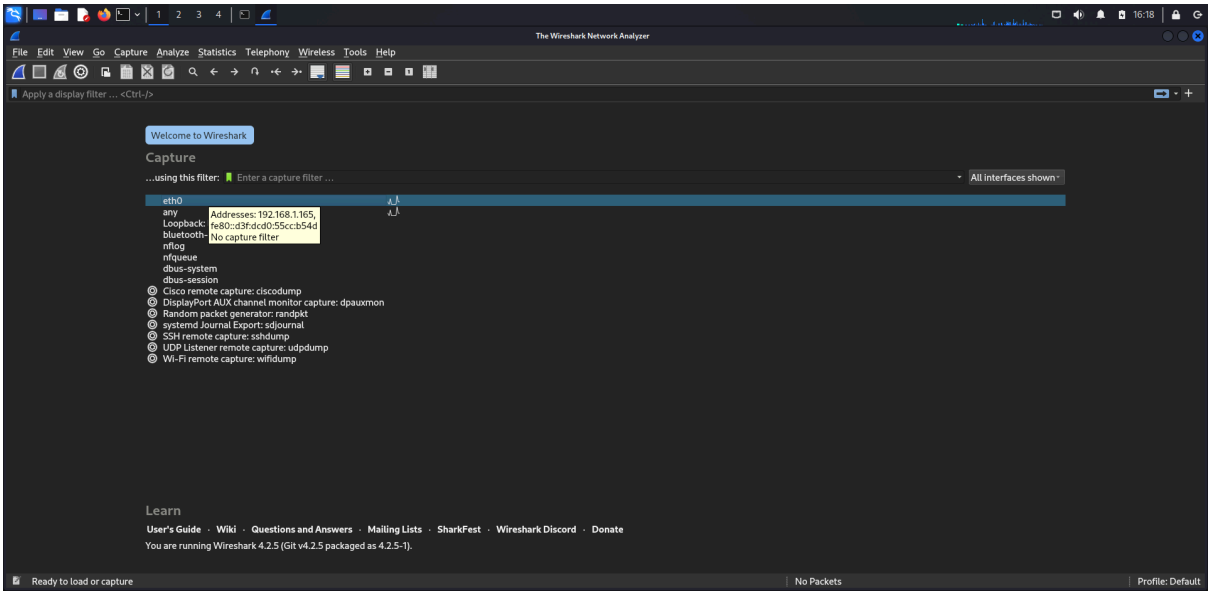
Obiettivi esercizio:

1. Catturare il traffico DNS.
2. Esplorare il traffico delle query DNS.
3. Esplorare il traffico delle risposte DNS.

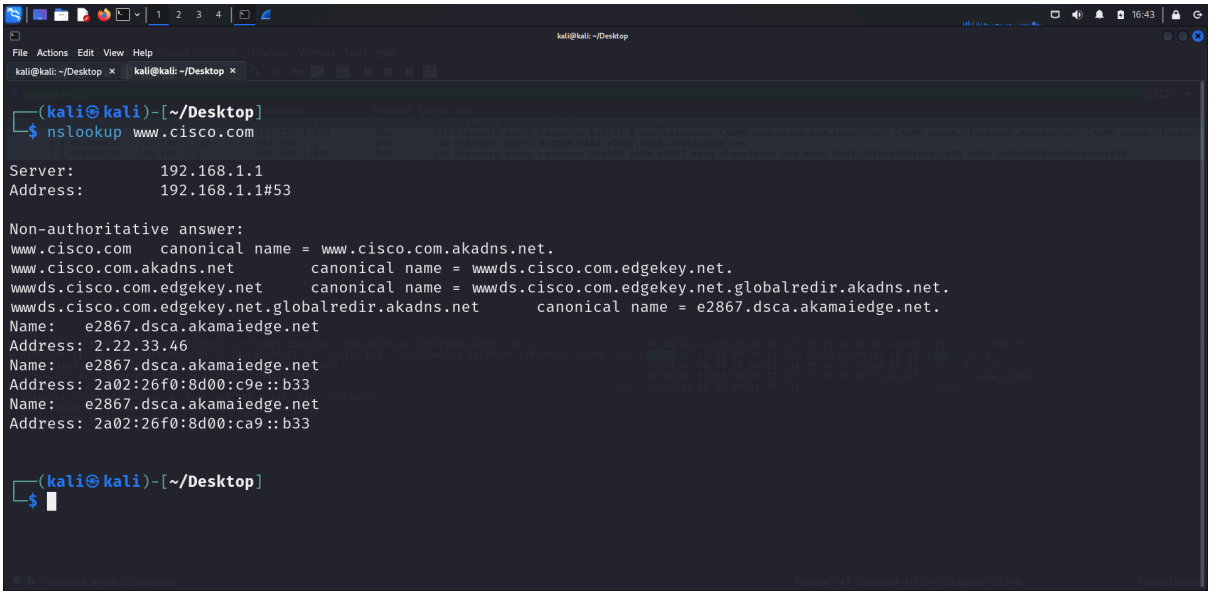
Catturare il traffico DNS:

- Avviare Wireshark e selezionare un'interfaccia attiva per la cattura dei pacchetti.

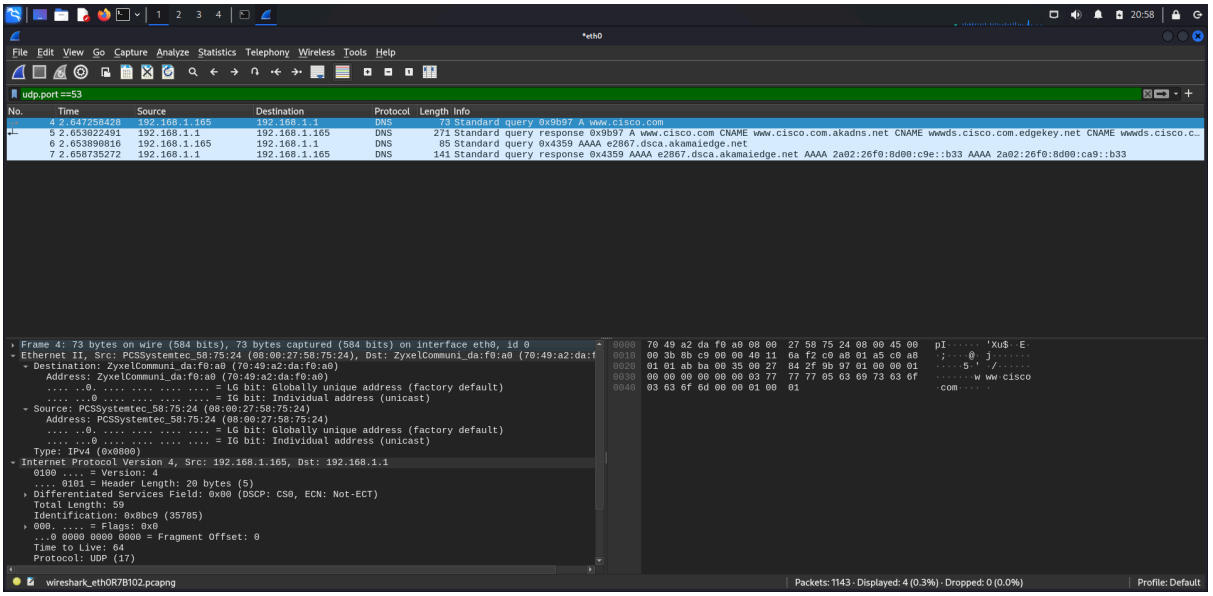


- **Ho eseguito il comando `nslookup www.cisco.com` per inviare una query DNS.**

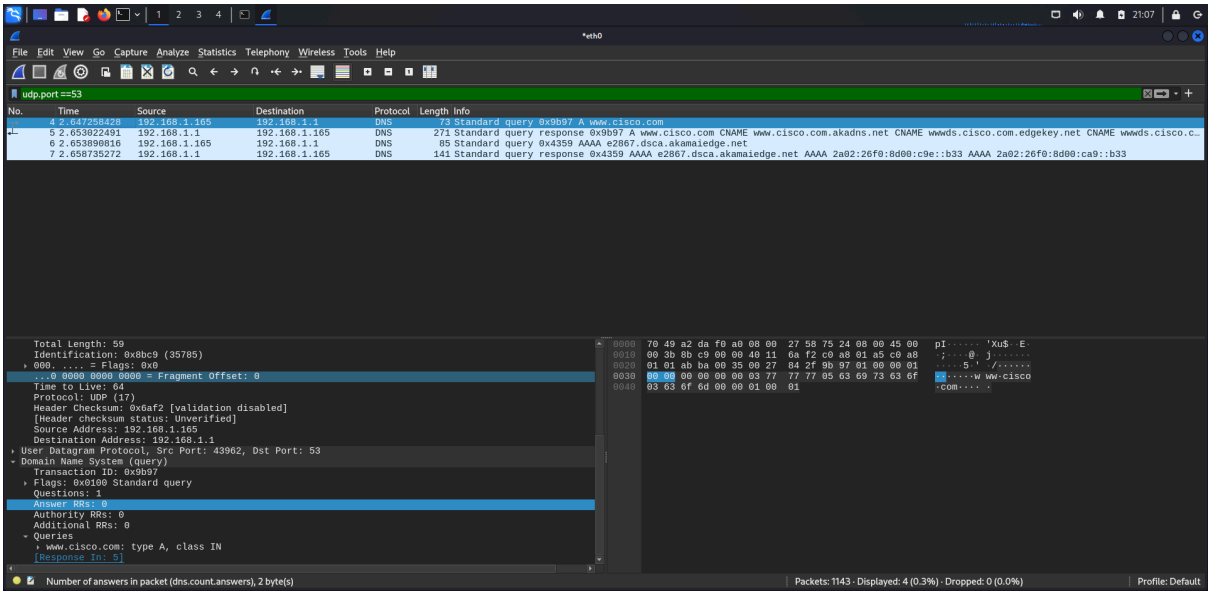
nslookup www.cisco.com



Ho applicato un filtro su Wireshark per visualizzare solo il traffico UDP sulla porta 53, utilizzando il filtro `udp.port == 53`.



- **Ho selezionato un pacchetto di query DNS e ho analizzato le informazioni nelle sezioni Ethernet, IP e UDP, osservando gli indirizzi MAC e IP di origine e destinazione, nonché le porte utilizzate.**



Ho verificato che il dominio richiesto fosse incluso nel campo "Answer" della risposta.

Conclusioni:

- **Il traffico DNS è composto principalmente da pacchetti UDP sulla porta 53.**
- **Le risposte DNS contengono le informazioni di risoluzione del dominio, come gli indirizzi IP associati.**
- **È possibile analizzare dettagliatamente le query e le risposte DNS utilizzando Wireshark, uno strumento utile per il troubleshooting di rete e per la sicurezza.**