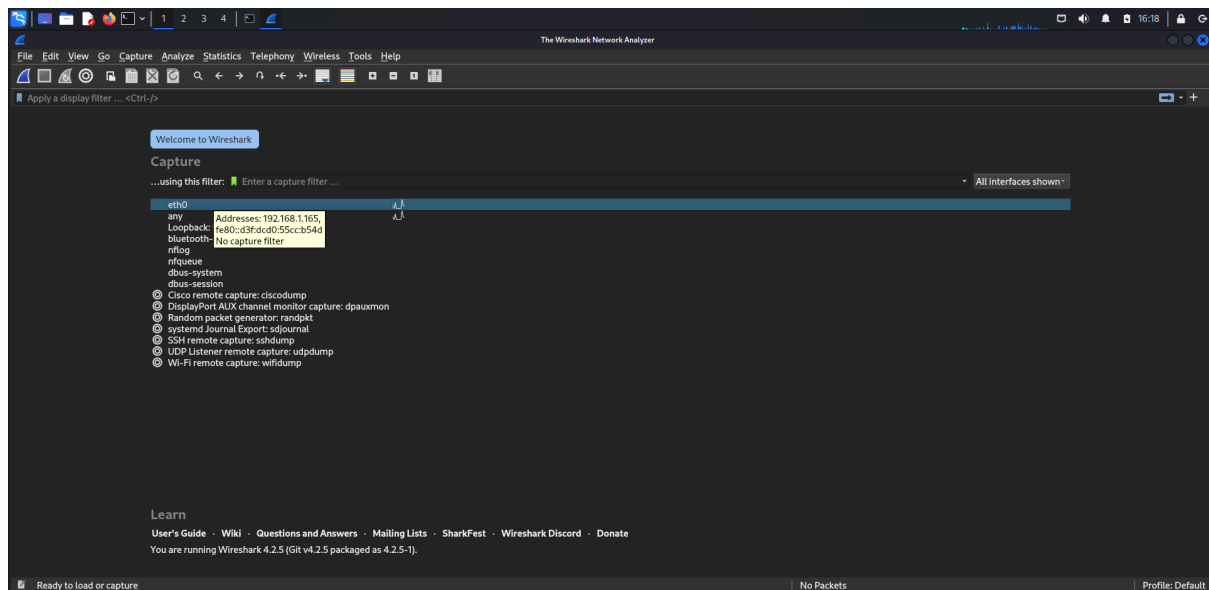


Obiettivi esercizio:

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

```
(kali@kali)-[~/Desktop]
$ 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: 2a02:26f0:8d00:c9e::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:8d00:ca9::b33

(kali@kali)-[~/Desktop]
$
```

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

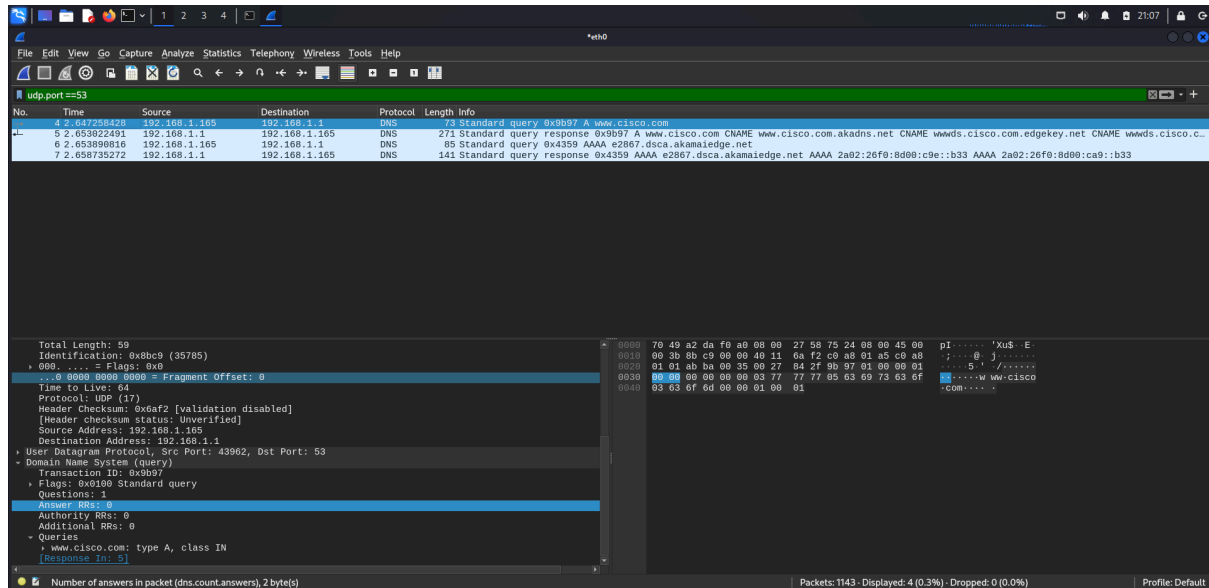
```

No.  Time  Source          Destination      Protocol  Length  Info
--  -
5  2.653022491  192.168.1.1    192.168.1.105   DNS      271     Standard query response 0x9b97 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME wwwds.cisco.com
6  2.653998816  192.168.1.105  192.168.1.1     DNS      85      Standard query 0x4359 AAAA e2867.dsca.akamaiedge.net
7  2.658735272  192.168.1.1    192.168.1.105   DNS      141     Standard query response 0x4359 AAAA e2867.dsca.akamaiedge.net AAAA 2a02:26f0:8d00:c9e::b33 AAAA 2a02:26f0:8d00:ca9::b33

Frame 4: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
  Ethernet II, Src: PCSysstemec_58:75:24 (08:00:27:58:75:24), Dst: ZyxelCommuni_da:f0:a0 (70:49:a2:da:f0:a0)
    Destination: ZyxelCommuni_da:f0:a0 (70:49:a2:da:f0:a0)
      Address: ZyxelCommuni_da:f0:a0 (70:49:a2:da:f0:a0)
        ....0.. = IG bit: Globally unique address (factory default)
        ....0.. = IG bit: Individual address (unicast)
      Source: PCSysstemec_58:75:24 (08:00:27:58:75:24)
        Address: PCSysstemec_58:75:24 (08:00:27:58:75:24)
        ....0.. = IG bit: Globally unique address (factory default)
        ....0.. = IG bit: Individual address (unicast)
      Type: IPv4 (0x0800)
    Internet Protocol Version 4, Src: 192.168.1.105, Dst: 192.168.1.1
      0100... = Version: 4
      ...0101 = Header Length: 20 bytes (5)
      Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 59
      Identification: 0xbbc9 (35785)
      000... = Flags: 0x0
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 64
      Protocol: UDP (17)

```

- 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.