

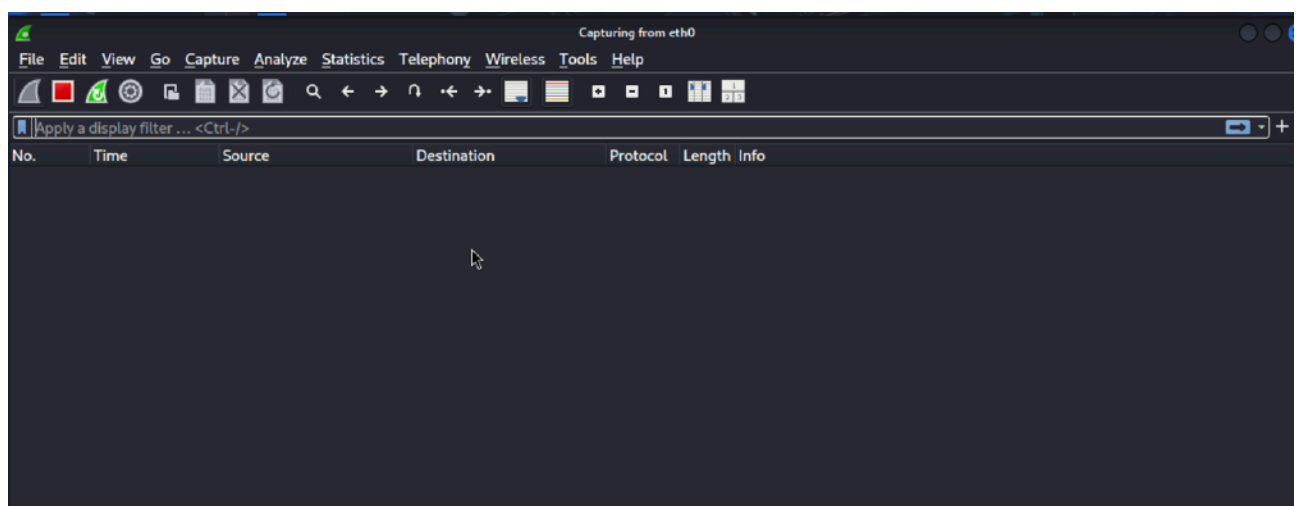
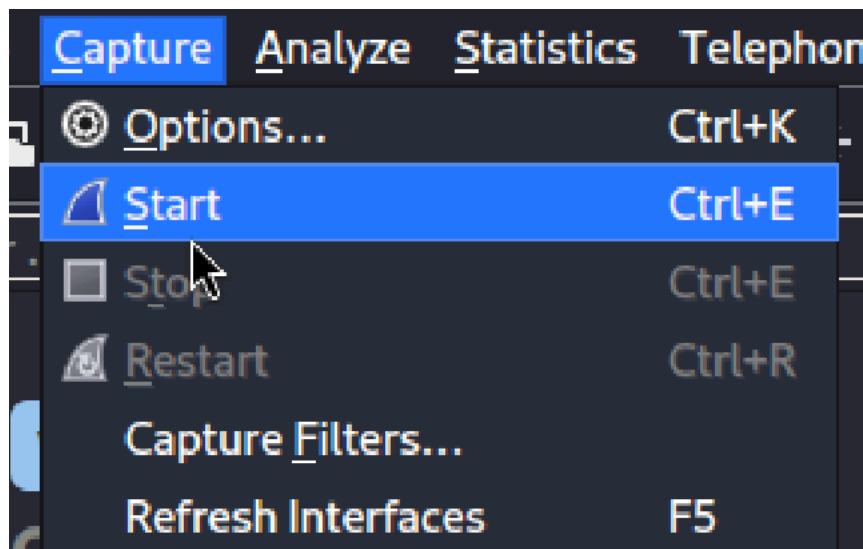
S11L3

Obiettivi:

- Parte 1 [?] Catturare il Traffico DNS
- • Parte 2 [?] Esplorare il Traffico delle Query DNS
- • Parte 3 [?] Esplorare il Traffico delle Risposte DNS

Fase1.

Entro sulla macchina kali ed apro Wireshark, dopo di che seleziono una interfaccia attiva con traffico per la cattura dei pacchetti



Tramite il terminale inserisco il comando “nslookup” sulla pagina web di Epicode.

```
(kali@kali)-[~]
$ nslookup www.epicode.com
Server:      192.168.64.1
Address:     192.168.64.1#53

Non-authoritative answer:
www.epicode.com canonical name = epicode.com.
Name: www.epicode.com
Address: 35.207.141.200
```

NSLOOKUP-

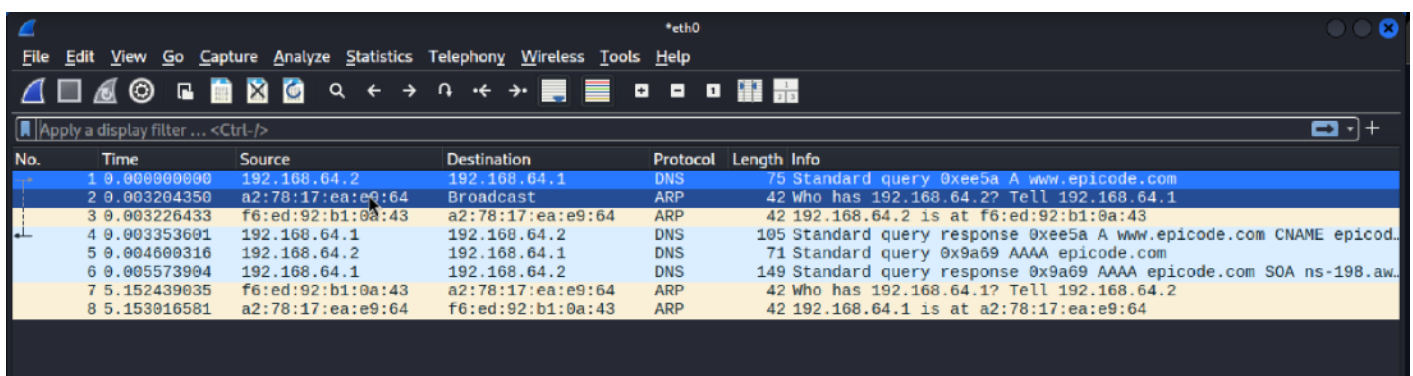
Verificare la risoluzione DNS: Permette di confermare che un nome di dominio si risolva nell'indirizzo IP corretto.

Risoluzione inversa: Ti consente di scoprire il nome di dominio associato a un determinato indirizzo IP.

Analisi dei record DNS: Può essere utilizzato per interrogare specifici tipi di record DNS, come i record **MX** (per i server di posta), **NS** (per i server dei nomi), o **TXT**.

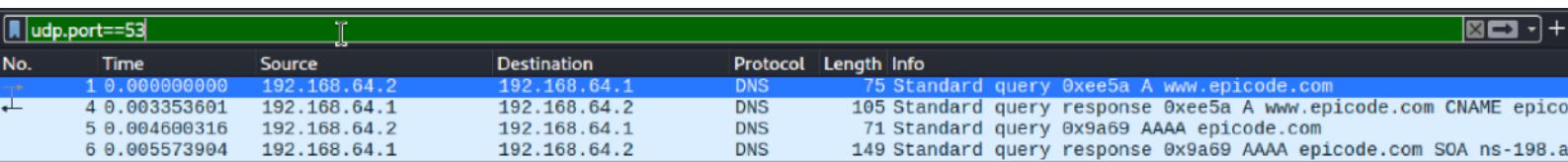
Risoluzione dei problemi: È uno strumento fondamentale per gli amministratori di rete per diagnosticare problemi di connettività, come l'impossibilità di raggiungere un sito web a causa di una configurazione DNS errata.

Ora interrompo la cattura su Wireshark ed analizzo i risultati.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.64.2	192.168.64.1	DNS	75	Standard query 0xee5a A www.epicode.com
2	0.003204350	a2:78:17:ea:e9:64	Broadcast	ARP	42	Who has 192.168.64.2? Tell 192.168.64.1
3	0.003226433	f6:ed:92:b1:0a:43	a2:78:17:ea:e9:64	ARP	42	192.168.64.2 is at f6:ed:92:b1:0a:43
4	0.003353601	192.168.64.1	192.168.64.2	DNS	105	Standard query response 0xee5a A www.epicode.com CNAME epicode.com
5	0.004600316	192.168.64.2	192.168.64.1	DNS	71	Standard query 0x9a69 AAAA epicode.com
6	0.005573904	192.168.64.1	192.168.64.2	DNS	149	Standard query response 0x9a69 AAAA epicode.com SOA ns-198.aw
7	5.152439035	f6:ed:92:b1:0a:43	a2:78:17:ea:e9:64	ARP	42	Who has 192.168.64.1? Tell 192.168.64.2
8	5.153016581	a2:78:17:ea:e9:64	f6:ed:92:b1:0a:43	ARP	42	192.168.64.1 is at a2:78:17:ea:e9:64

In questo caso voglio analizzare solo i pacchetti DNS quindi sulla casella del filtro inserisco udp.port==53



The screenshot shows the Wireshark interface with a packet list table. The filter bar at the top contains 'udp.port==53'. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. It displays six packets, all of which are DNS queries or responses between 192.168.64.1 and 192.168.64.2.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.64.2	192.168.64.1	DNS	75	Standard query 0xee5a A www.epicode.com
4	0.003353601	192.168.64.1	192.168.64.2	DNS	105	Standard query response 0xee5a A www.epicode.com CNAME epico
5	0.004600316	192.168.64.2	192.168.64.1	DNS	71	Standard query 0x9a69 AAAA epicode.com
6	0.005573904	192.168.64.1	192.168.64.2	DNS	149	Standard query response 0x9a69 AAAA epicode.com SOA ns-198.a

Domande:

1. Quali sono gli indirizzi MAC di origine e destinazione?
a2:78:17:ea:e9:64 Destinazione
f6:ed:92:b1:0a:43 Origine
2. A quali interfacce di rete sono associati questi indirizzi MAC?
Destinazione Cliente
Origine server DNS
3. Quali sono gli indirizzi IP di origine e destinazione?
Destinazione 192.168.64.1
Origine 192.168.64.2
4. Quali sono le porte di origine e destinazione?
Source Port: 53370
Destination Port: 53
5. Qual è il numero di porta DNS predefinito?
53
6. Confrontare gli indirizzi MAC e IP nei risultati di Wireshark con gli indirizzi IP e MAC. Qual è la tua osservazione?
7. Quali sono gli indirizzi MAC e IP e i numeri di porta di origine e destinazione?
Si alternano tra Destinazione 192.168.64.1
Origine 192.168.64.2