Esercizio L11S3

Esplorazione del Traffico DNS

1. Cattura traffico DNS

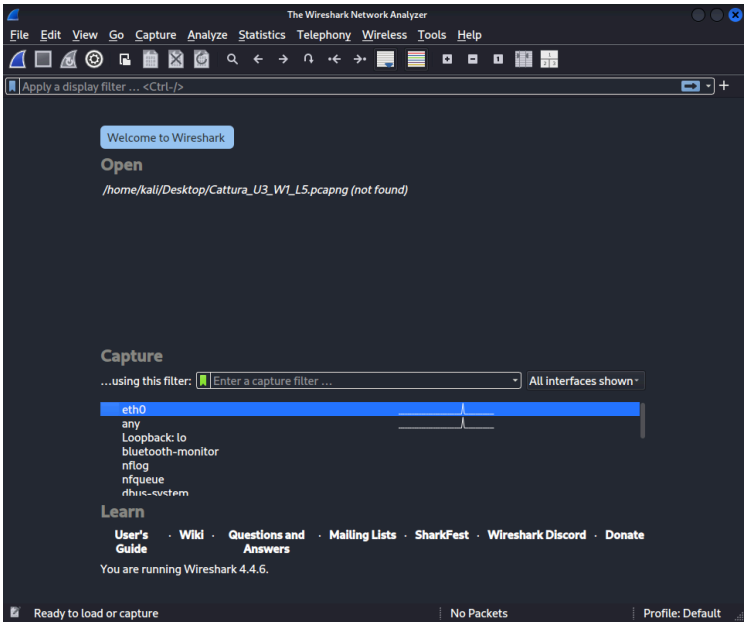
A. Pulire la cache DNS e avviare Wireshark

- Per pulire la cache apriamo il terminale e mandiamo il comando **<cat /etc/resolv.conf>** per vedere quale servizio è attivo [Fig.1]
- Avviamo Wireshark e selezioniamo la NIC attiva[Fig.2]

Il terminale risponde mostrandoci il servizio utilizzato da Kali (NetworkManager) e l'indirizzo del server DNS, non è presente in questo caso una cache DNS quindi non servirà pulirla.

[Fig.1]

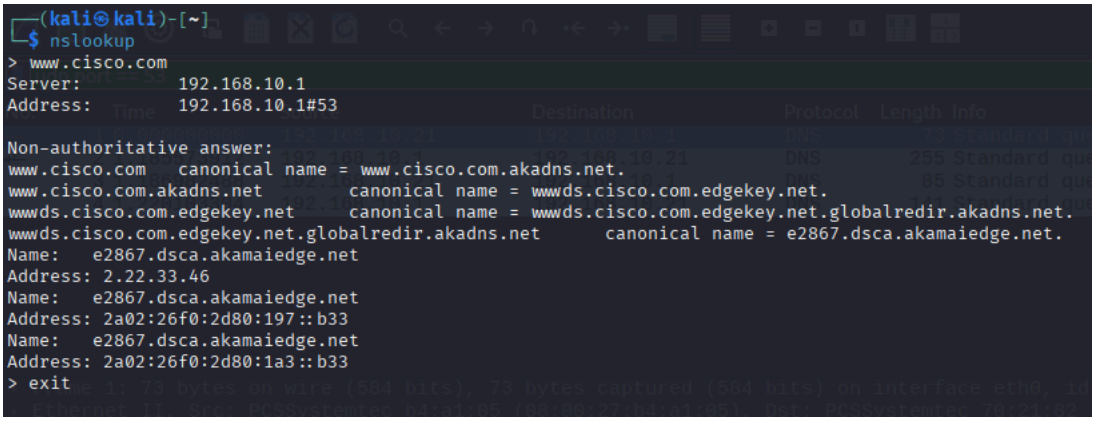
Aperto Wireshark selezioneremo la scheda attiva chiamata "eth0"



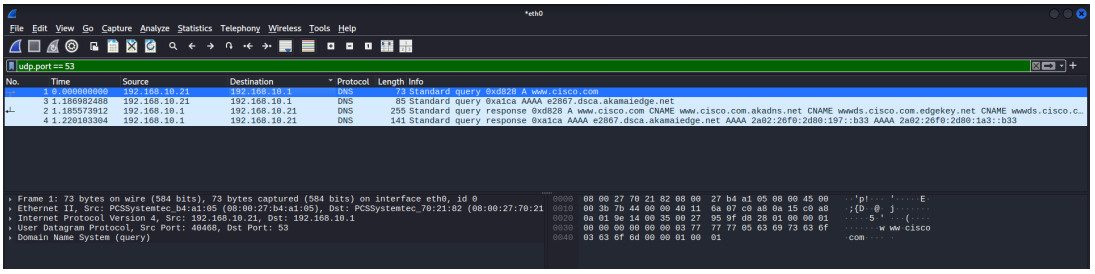
[Fig.2]

B. Generazione traffico DNS

- Apriamo un nuovo terminale, mandiamo il comando **<nslookup>**
- Inseriamo “www.cisco.com” come dominio [Fig.3]
- Inseriamo “udp.port==53” come filtro [Fig.4]



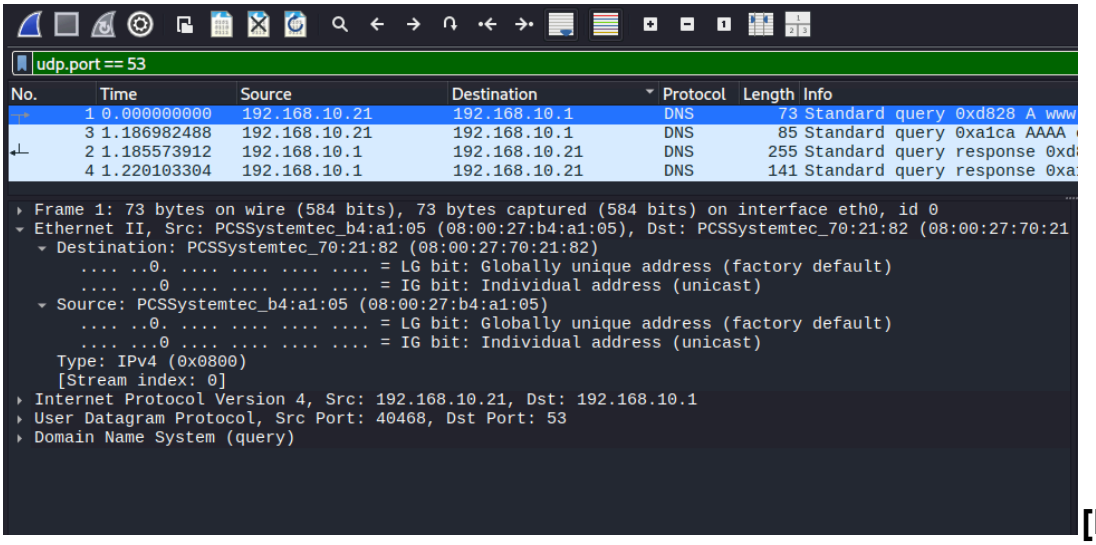
[Fig.3]



[Fig.4]

2. Esplorazione traffico query DNS

A. Apriamo il primo pacchetto e visualizziamo “Ethernet II”



[Fig.5]

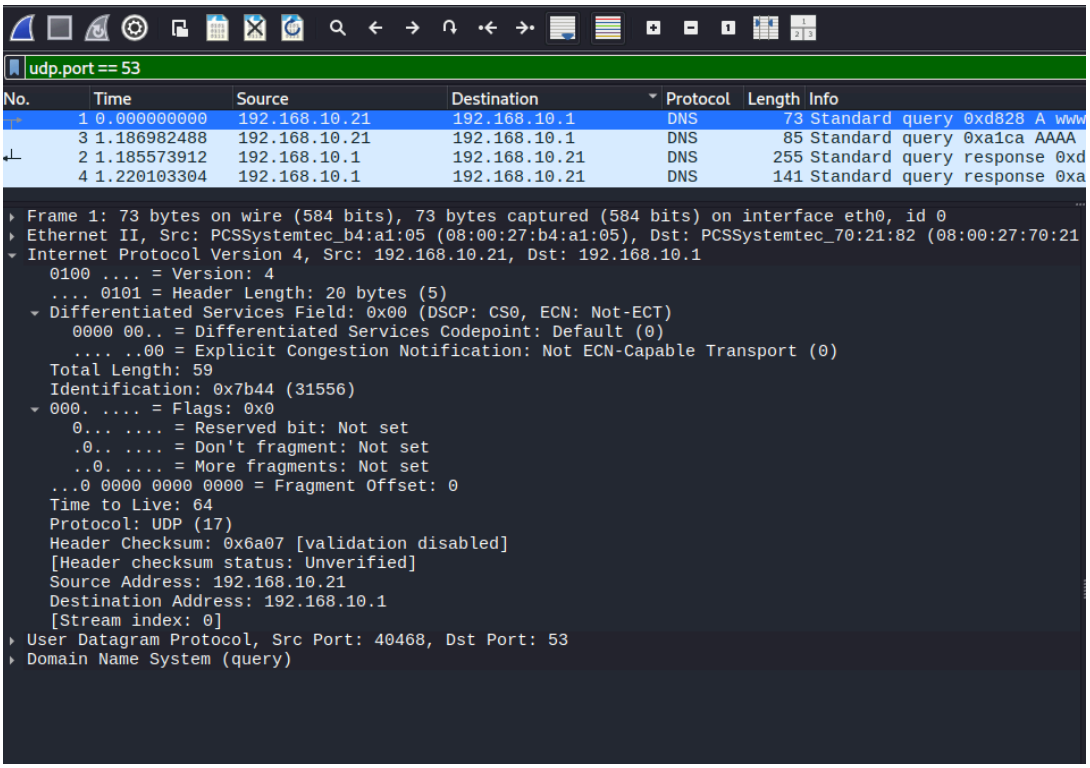
1. Quali sono gli indirizzi MAC di origine e destinazione?

- **Indirizzo MAC dI origine:** 08:00:27:b4:a1:05
- **Indirizzo MAC destinazione:** 08:00:27:70:21:82

2. A quali interfacce di rete sono associati questi indirizzi MAC?

- **MAC d'origine:** fa riferimento all'indirizzo MAC della VM
- **MAC destinazione:** fa riferimento all'indirizzo MAC del Router

B. Ora visualizziamo "Internet Protocol Version 4"



[Fig.6]

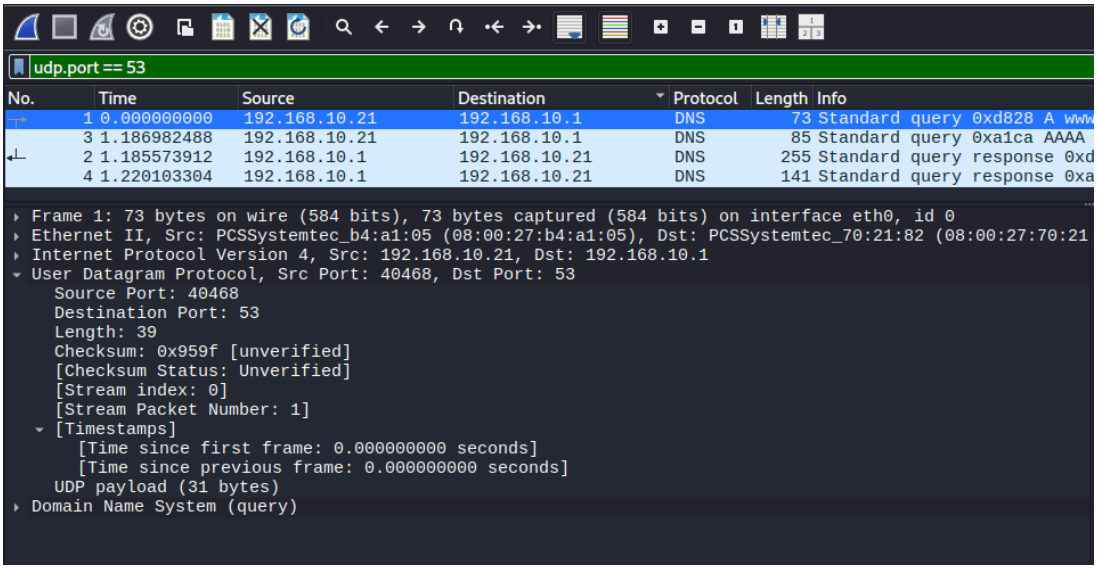
1. Quali sono gli indirizzi IP di origine e destinazione?

- **IP di origine:** 192.168.10.21
- **IP destinazione:** 192.168.10.1

2. A quali interfacce di rete sono associati questi indirizzi IP?

- **IP di origine:** IP associato alla VM
- **IP destinazione:** IP associato al server DNS

C. Ora visualizziamo “User Datagram Protocol”



[Fig.7]

1. Quali sono le porte di origine e destinazione?

- **Porte di origine:** 40468
- **Porte di destinazione:** 53

2. Qual è il numero di porta DNS predefinito?

- La porta di default utilizzata è la 53

D. Determinare l'indirizzo IP e MAC del PC col comando <ip a>

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b4:a1:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.21/24 brd 192.168.10.255 scope global dynamic noprefixroute eth0
       valid_lft 3673sec preferred_lft 3673sec
    inet6 fe80::a229:2da8:1cd1:3e9f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

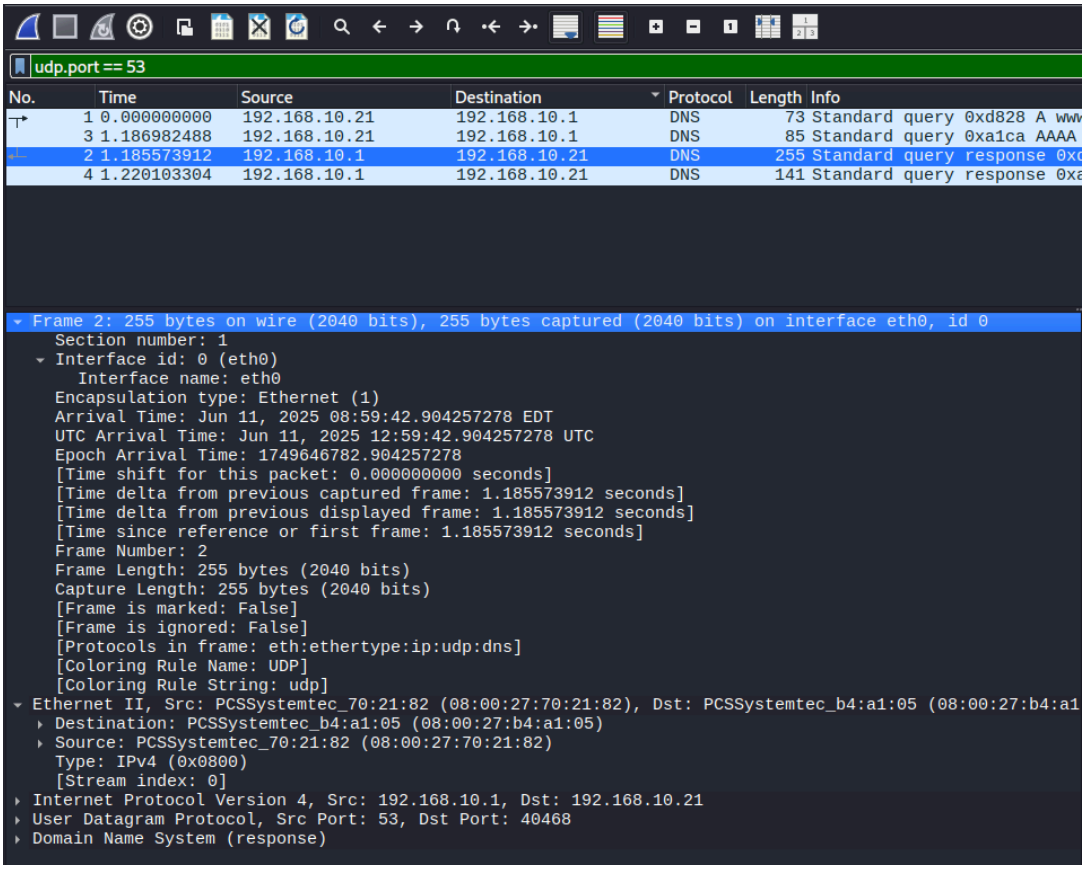
[Fig.8]

3. Confrontare gli indirizzi MAC e IP nei risultati di Wireshark con gli indirizzi IP e MAC. Qual è la tua osservazione?

- Gli indirizzi MAC e IP presenti dal report di Wireshark e quelli stampati nel terminali corrispondono

3. Esplorazione Traffico delle Risposte DNS

A. Visualizziamo il terzo pacchetto



[Fig.9]

1. Quali sono gli indirizzi MAC e IP e i numeri di porta di origine e destinazione?

- **Indirizzo MAC di origine:** 08:00:27:70:21:82
- **Indirizzo MAC destinazione:** 08:00:27:b4:a1:05
- **IP di origine:** 192.168.10.1
- **IP destinazione:** 192.168.10.21
- **Porte di origine:** 53
- **Porte di destinazione:** 40468

2. Come si confrontano con gli indirizzi nei pacchetti di query DNS?

- ***QUERY* MAC di origine e destinazione:** Dal PC al Gateway
- ***RESPONSE* MAC di origine e destinazione:** Dal Gateway al PC
- ***QUERY* IP di origine e destinazione:** Dal PC al Server DNS
- ***RESPONSE* IP di origine e destinazione:** Dal Server DNS al PC
- ***QUERY* PORTA di origine e destinazione:** Dalla porta 40468 alla 53
- ***RESPONSE* PORTA di origine e destinazione:** Dalla 53 alla 40468

3. Il server DNS può fare query ricorsive?

- Si, nella sezione Flag dice “Server can do recursive queries”

4. Come si confrontano i risultati con quelli di nslookup?

Anche in questo caso i risultati di Wireshark corrispondono con quelli di <nslookup>

4. Riflessione

1. Dai risultati di Wireshark, cos'altro puoi imparare sulla rete quando rimuovi il filtro?

Rimuovendo il filtro potremo vedere:

- **Protocolli vari di rete:** ARP, ICMP, DHCP, UDP
- **Protocolli non crittografati:** FTTP, HTTP
- **Metadati vari:** Indirizzi IP, Volume del traffico

2. Come può un attaccante usare Wireshark per compromettere la sicurezza della tua rete?

Un attaccante potrà:

- Intercettare varie comunicazioni
- Catturare dati personali o finanziari
- Identificare servizi attivi e versioni software
- Scoprire indirizzi IP interni e la struttura di rete
- Dirottare la sessione
- Catturare cookie di sessione non protetti