

Esercizio L11S3

Esplorazione del Traffico DNS

1. Cattura traffico DNS

A. Pulire la cache DNS e avviare Wireshark

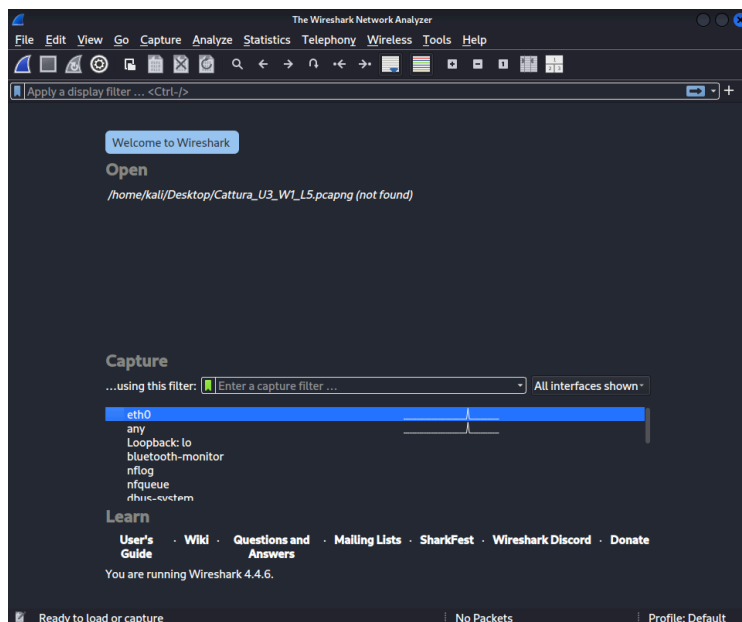
- Per pulire la cache apriamo il terminale e mandiamo il comando **<cat /etc/resolv.conf>** per vedere quale servizio è attivo [Fig.1]
- Avviamo Wireshark e selezioniamo la NIC attiva[Fig.2]

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.

```
(kali@kali)-[~]  
$ cat /etc/resolv.conf  
# Generated by NetworkManager  
search home.arpa  
nameserver 192.168.10.1
```

[Fig.1]

Aperto Wireshark selezioneremo la scheda attiva chiamata “eth0”



[Fig.2]

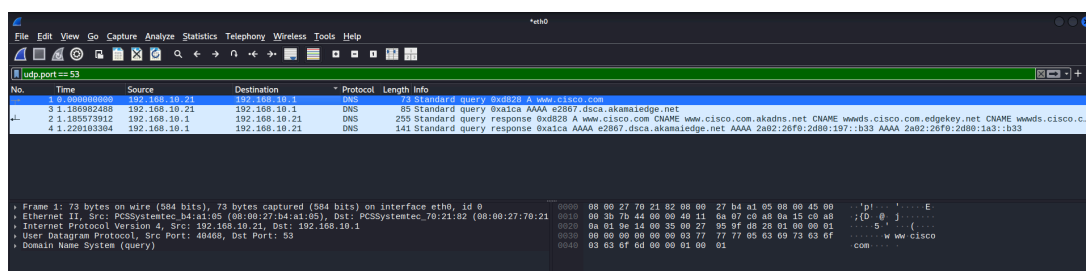
B. Generazione traffico DNS

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

```
(kali㉿kali)-[~]
$ nslookup
> www.cisco.com
Server:      192.168.10.1
Address:     192.168.10.1#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: 2a02:26f0:2d80:197::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d80:1a3::b33
> exit
```

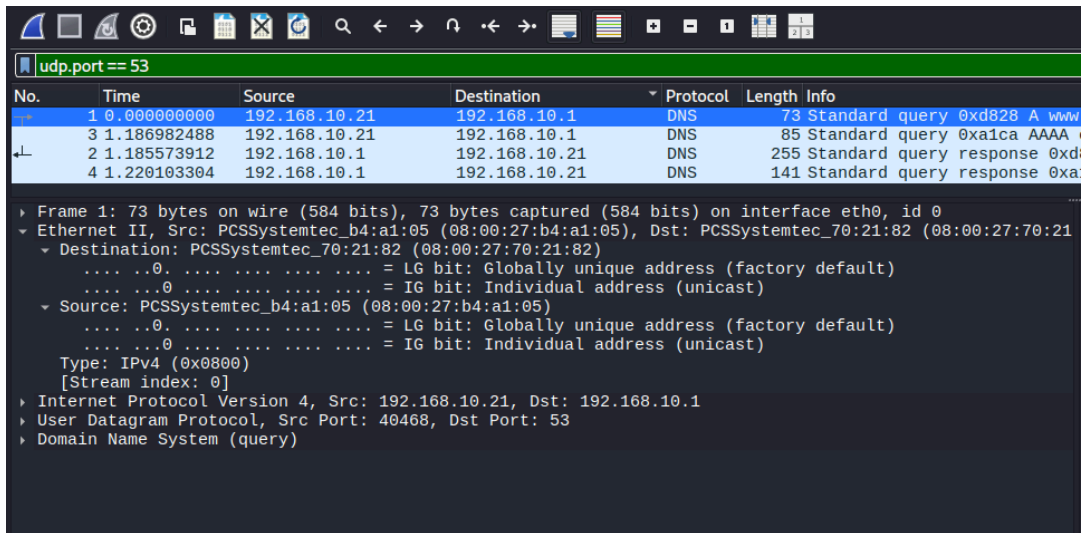
[Fig.3]



[Fig.4]

2. Esplorazione traffico query DNS

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



[Fig.5]

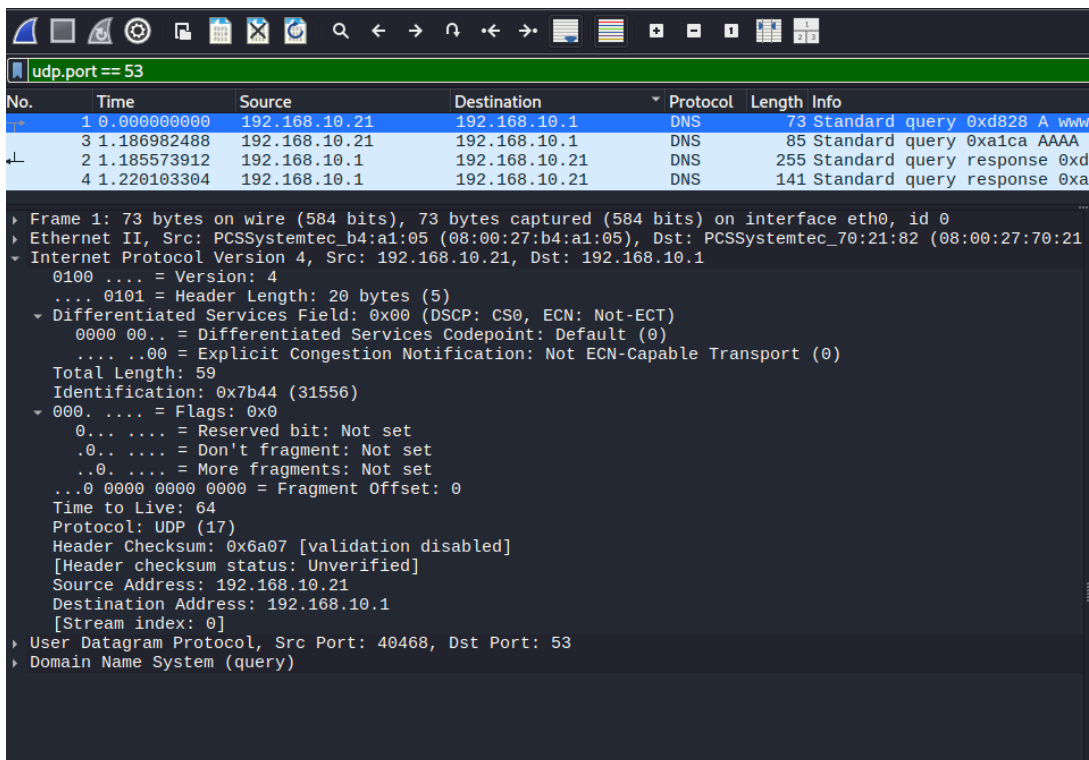
1. Quali sono gli indirizzi MAC di origine e destinazione?

- 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]

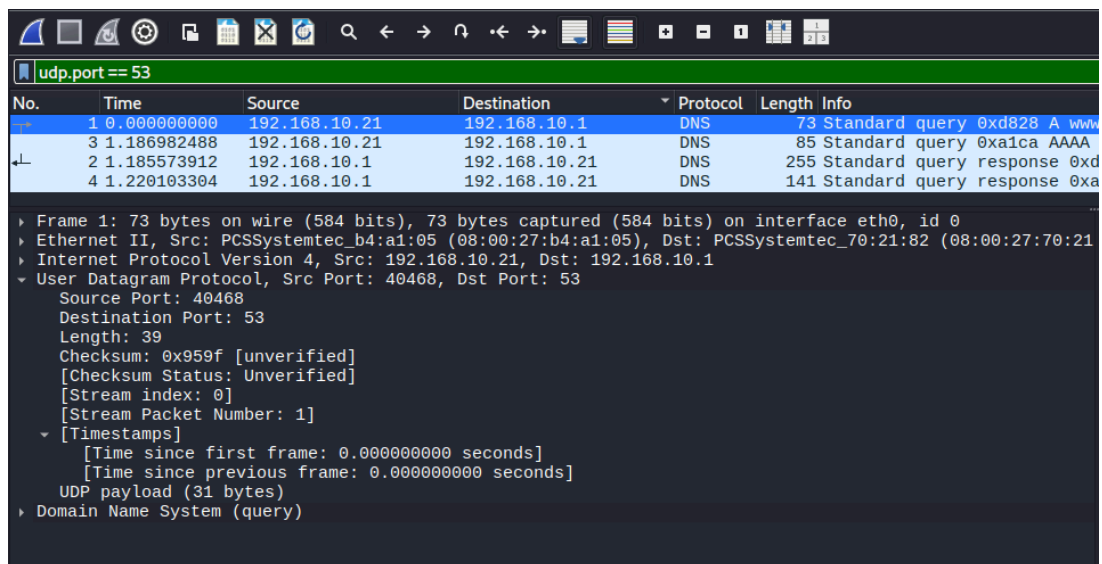
1. Quali sono gli indirizzi IP di origine e destinazione?

- 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

udp.port == 53

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.10.21	192.168.10.1	DNS	73	Standard query 0xd828 A www
3	1.186982488	192.168.10.21	192.168.10.1	DNS	85	Standard query 0xa1ca AAAA
2	1.185573912	192.168.10.1	192.168.10.21	DNS	255	Standard query response 0xa1ca
4	1.220103304	192.168.10.1	192.168.10.21	DNS	141	Standard query response 0xa1ca

▼ Frame 2: 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on interface eth0, id 0

Section number: 1

- Interface id: 0 (eth0)
 - Interface name: eth0
 - Encapsulation type: Ethernet (1)
 - Arrival Time: Jun 11, 2025 08:59:42.904257278 EDT
 - UTC Arrival Time: Jun 11, 2025 12:59:42.904257278 UTC
 - Epoch Arrival Time: 1749646782.904257278
 - [Time shift for this packet: 0.000000000 seconds]
 - [Time delta from previous captured frame: 1.185573912 seconds]
 - [Time delta from previous displayed frame: 1.185573912 seconds]
 - [Time since reference or first frame: 1.185573912 seconds]
 - Frame Number: 2
 - Frame Length: 255 bytes (2040 bits)
 - Capture Length: 255 bytes (2040 bits)
 - [Frame is marked: False]
 - [Frame is ignored: False]
 - [Protocols in frame: eth:ethertype:ip:udp:dns]
 - [Coloring Rule Name: UDP]
 - [Coloring Rule String: udp]
- Ethernet II, Src: PCSSystemtec_70:21:82 (08:00:27:70:21:82), Dst: PCSSystemtec_b4:a1:05 (08:00:27:b4:a1:05)
 - Destination: PCSSystemtec_b4:a1:05 (08:00:27:b4:a1:05)
 - Source: PCSSystemtec_70:21:82 (08:00:27:70:21:82)
 - Type: IPv4 (0x0800)
 - [Stream index: 0]
- Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.21
- User Datagram Protocol, Src Port: 53, Dst Port: 40468
- Domain Name System (response)

[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?

- Sì, 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