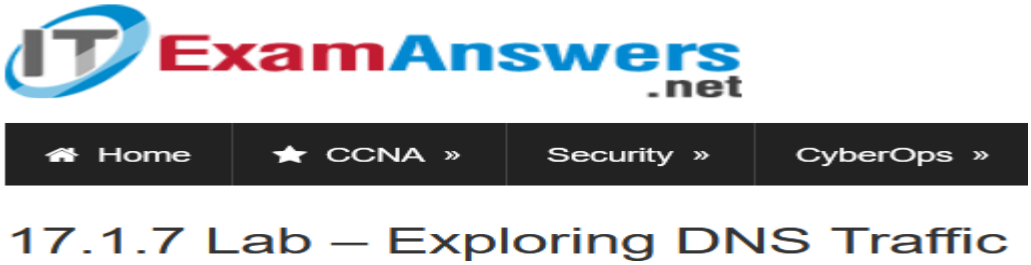
LABORATORIO 19 FEBBRAIO 2025 S11-L3

Laboratorio - Esplorazione del Traffico DNS

In questo laboratorio, completa i seguenti obiettivi:

- Catturare il traffico DNS
- Esplorare il traffico delle query DNS
- Esplorare il traffico delle risposte DNS

https://itexamanswers.net/17-1-7-lab-exploring-dns-traffic-answers.html



Lo scopo del laboratorio è utilizzare Wireshark per filtrare i pacchetti DNS e visualizzare i dettagli dei pacchetti di query e di risposta DNS.

L'unico requisito è un PC con accesso a internet e col tool Wireshark installato al suo interno. Utilizzerò Kali Linux.

Step 2: Capture DNS traffic.

a. Start Wireshark. Select an active interface with traffic for packet capture.

b. Clear the DNS cache.

1) In Windows, enter **ipconfig /flushdns** in Command Prompt.

2) For the majority of Linux distributions, one of the following utilities is used for DNS caching: Systemd -Resolved, DNSMasq, and NSCD. If your Linux distribution does not use one of the listed utilities, please perform an internet search for the DNS caching utility for your Linux distribution.

(i) Identify the utility used in your Linux distribution by checking the status:

Systemd-Resolved: **systemctl status systemd-resolved.service**
DNSMasq: **systemctl status dnsmasq.service**
NSCD: **systemctl status nscd.service**

(ii) If you are using system-resolved, enter systemd-resolve –flush-caches to flush the cache for Systemd-Resolved before restarting the service. The following commands restart the associated service using elevated privileges:

Systemd-Resolved: **sudo systemctl restart systemd-resolved.service**
DNSMasq: **sudo systemctl restart dnsmasq.service**
NSCD: **sudo systemctl restart nscd.service**

3) For the macOS, enter **sudo killall -HUP mDNSResponder** to clear the DNS cache in the Terminal. Perform an internet search for the commands to clear the DNS cache for an older OS.

c. At a command prompt or terminal, type **nslookup** enter the interactive mode.

d. Enter the domain name of a website. The domain name www.cisco.com is used in this example.

Innanzitutto avviamo Wireshark e selezioniamo un'interfaccia attiva per acquisirne i pacchetti.

Da terminale utilizziamo il comando **nslookup** per accedere alla modalità interattiva e inseramo il dominio scelto. Optiamo per www.cisco.com e inseriamo quindi 8.8.8.8. Una volta finito chiudiamo il terminale e interrompiamo l'acquisizione dei pacchetti su Wireshark.

```
┌──(kali㉿kali)-[~]
└─$ nslookup
> www.cisco.com
Server:         10.0.2.3
Address:        10.0.2.3#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: 92.123.44.98
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d80:1a3::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d80:1b9::b33
> exit
```

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.2.3	DNS	73	Standard query 0xd0e9 A www.cisco.com
2	0.014950900	fe80::2	ff02::1	ICMPv6	134	Router Advertisement from 52:56:00:00:00:02
3	0.026694514	fe80::2890:30e9:a35…	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
4	0.027125785	10.0.2.3	10.0.2.15	DNS	255	Standard query response 0xd0e9 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME wwwds.cisco.c…
5	0.028575936	10.0.2.15	10.0.2.3	DNS	85	Standard query 0xdef2 AAAA e2867.dsca.akamaiedge.net
6	0.045331492	10.0.2.3	10.0.2.15	DNS	141	Standard query response 0xdef2 AAAA e2867.dsca.akamaiedge.net AAAA 2a02:26f0:2d80:1a3::b33 AAAA 2a02:26f0:2d80:1b9::b33
7	1.038371298	fe80::2890:30e9:a35…	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
8	5.166287741	PCSSystemtec_11:f8:…	52:55:0a:00:02:03	ARP	42	Who has 10.0.2.3? Tell 10.0.2.15
9	5.166545202	52:55:0a:00:02:03	PCSSystemtec_11:f8:…	ARP	64	10.0.2.3 is at 52:55:0a:00:02:03

Part 2: Explore DNS Query Traffic

a. Observe the traffic captured in the Wireshark Packet List pane. Enter **udp.port == 53** in the filter box and click the arrow (or press enter) to display only DNS packets.

A questo punto osserviamo il traffico catturato. Inseriamo il filtro **udp.port == 53** per vedere solo i pacchetti relativi al **DNS.**

udp.port == 53

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.2.3	DNS	73	Standard query 0xd0e9 A www.cisco.com
4	0.027125785	10.0.2.3	10.0.2.15	DNS	255	Standard query response 0xd0e9 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME wwwds.cisco.c…
5	0.028575936	10.0.2.15	10.0.2.3	DNS	85	Standard query 0xdef2 AAAA e2867.dsca.akamaiedge.net
6	0.045331492	10.0.2.3	10.0.2.15	DNS	141	Standard query response 0xdef2 AAAA e2867.dsca.akamaiedge.net AAAA 2a02:26f0:2d80:1a3::b33 AAAA 2a02:26f0:2d80:1b9::b33

b. Select the DNS packet contains **Standard query** and **A www.cisco.com** in the Info column.

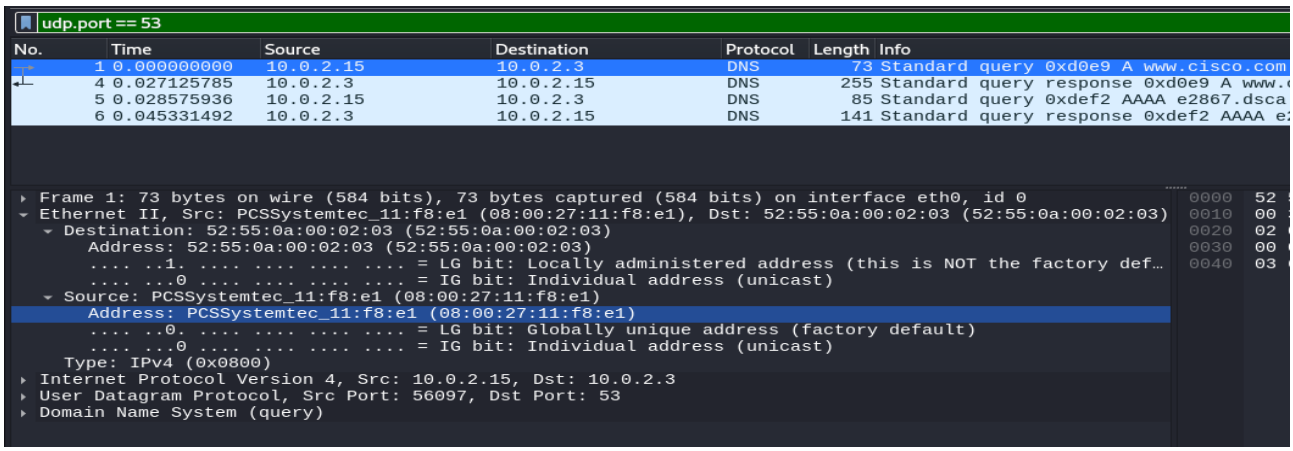
c. In the Packet Details pane, notice this packet has Ethernet II, Internet Protocol Version 4, User Datagram Protocol and Domain Name System (query).

d. Expand **Ethernet II** to view the details. Observe the source and destination fields.

Selezionare il pacchetto DNS che contiene la query standard e un www.cisco.com nella colonna Info.

Nel riquadro Dettagli pacchetto, si noti che questo pacchetto contiene Ethernet II, Internet Protocol versione 4, User Datagram Protocol e Domain Name System (query).

Espandere **Ethernet II** per visualizzare i dettagli. Osservare i campi di origine e di destinazione.



What are the source and destination MAC addresses? Which network interfaces are these MAC addresses associated with?

Quali sono gli indirizzi MAC di origine e di destinazione?
L'indirizzo MAC di origine è 08:00:27:11:f8 :e1 e quello di destinazione è 52:55:0a:00:02:03.

A quali interfacce di rete sono associati questi indirizzi MAC? **Eth0**

e. Expand **Internet Protocol Version 4**. Observe the source and destination IPv4 addresses.

```
▸ Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
▸ Ethernet II, Src: PCSSystemtec_11:f8:e1 (08:00:27:11:f8:e1), Dst: 52:55:0a:00:02:03 (52:55:0a:00:02:03)
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 59
    Identification: 0xc1be (49598)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xa0e2 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 10.0.2.3
```

What are the source and destination IP addresses? Which network interfaces are these IP addresses associated with?

Quali sono gli indirizzi IP di origine e di destinazione?
10.0.2.15/10.0.2.3

A quali interfacce di rete sono associati questi indirizzi IP?
L'indirizzo IP di origine è associato alla scheda di interfaccia di rete del PC e l'indirizzo IP di destinazione è associato al gateway predefinito

f. Expand the **User Datagram Protocol**. Observe the source and destination ports.

```
▸ Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
▸ Ethernet II, Src: PCSSystemtec_11:f8:e1 (08:00:27:11:f8:e1), Dst: 52:55:0a:00:02:03 (52:55:0a:00:02:03)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
▾ User Datagram Protocol, Src Port: 56097, Dst Port: 53
    Source Port: 56097
    Destination Port: 53
    Length: 39
    Checksum: 0x184a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  ▸ [Timestamps]
    UDP payload (31 bytes)
▸ Domain Name System (query)
```

What are the source and destination ports? What is the default DNS port number?

Quali sono le porte di origine e di destinazione?

Origine: 56097 Destinazione: 53

Qual è il numero di porta DNS predefinito? **53**

g. Determine the IP and MAC address of the PC.

1. In a Windows command prompt, enter **arp –a** and **ipconfig /all** to record the MAC and IP addresses of the PC.
2. For Linux and macOS PC, enter **ifconfig** or **ip address** in a terminal.

Compare the MAC and IP addresses in the Wireshark results to the IP and MAC addresses. What is your observation?

Determinare l'indirizzo IP e MAC del PC. Confrontare gli indirizzi MAC e IP nei risultati di Wireshark con gli indirizzi IP e MAC.

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::2890:30e9:a35d:385a  prefixlen 64  scopeid 0x20<link>
        inet6 fd00::c042:4ce6:a3bd:8939  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:11:f8:e1  txqueuelen 1000  (Ethernet)
        RX packets 21  bytes 4812 (4.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 45  bytes 5713 (5.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 48  bytes 2480 (2.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 48  bytes 2480 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Indirizzo IP= **10.0.2.15**

Indirizzo MAC**= 08:00:27:11:f8:e1**

Sono gli stessi acquisiti con Wireshark.

h. Expand **Domain Name System (query)** in the Packet Details pane. Then expand the **Flags** and **Queries**.

i. Observe the results. The flag is set to do the query recursively to query for the IP address to www.cisco.com.

Espandere Domain Name System (query) nel riquadro Dettagli pacchetto. Quindi espandere Flag e query.

Osservare i risultati. Il flag è impostato per eseguire la query in modo ricorsivo per eseguire la query per l'indirizzo IP da www.cisco.com.

```
▾ Domain Name System (query)
    Transaction ID: 0xd0e9
  ▾ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.cisco.com: type A, class IN
        Name: www.cisco.com
        [Name Length: 13]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
    [Response In: 4]
```

Part 3: Explore DNS Response Traffic

a. Select the corresponding response DNS packet has **Standard query response** and **A www.cisco.com** in the Info column.

```
udp.port == 53
No.  Time          Source       Destination  Protocol Length Info
1    0.000000000   10.0.2.15    10.0.2.3     DNS      73     Standard query 0xd0e9 A www.cisco.com
4    0.027125785   10.0.2.3     10.0.2.15    DNS      255    Standard query response 0xd0e9 A www.cisco.com
5    0.028575936   10.0.2.15    10.0.2.3     DNS      85     Standard query 0xdef2 AAAA e2867.dsca.akamaiedg
6    0.045331492   10.0.2.3     10.0.2.15    DNS      141    Standard query response 0xdef2 AAAA e2867.dsca.

▸ Frame 4: 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on interface eth0, id 0
▸ Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_11:f8:e1 (08:00:27:11:f8:e1)
▸ Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.0.2.15
▸ User Datagram Protocol, Src Port: 53, Dst Port: 56097
▸ Domain Name System (response)

0000  08
0010  00
0020  02
0030  00
0040  03
0050  00
```

What are the source and destination MAC and IP addresses and port numbers? How do they compare to the addresses in the DNS query packets?

Quali sono gli indirizzi MAC e IP di origine e di destinazione e i numeri di porta? **Origine: 10.0.2.3 Porta 53; Destinazione 10.0.2.15 porta 56097**

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

Quelli che prima erano IP e Porta di Origine ora sono di Destinazione e viceversa.

b. Expand **Domain Name System (response)**. Then expand the **Flags, Queries,** and **Answers.**

c. Observe the results.

Can the DNS server do recursive queries?

```
▾ Domain Name System (response)
    Transaction ID: 0xd0e9
  ▾ Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.cisco.com: type A, class IN
  ▾ Answers
    ▸ www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
    ▸ www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net
    ▸ wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredir.akadns.net
    ▸ wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
    ▸ e2867.dsca.akamaiedge.net: type A, class IN, addr 92.123.44.98
    [Request In: 1]
    [Time: 0.027125785 seconds]
```

Il server DNS può eseguire query ricorsive? **Si, il server DNS, come possiamo vedere dal flag 1, è in grado di esergurle.**

d. Observe the CNAME and A records in the Answers details.

How do the results compare to nslookup results?

Osservare i record CNAME e A nei dettagli delle risposte.

```
┌──(kali㉿kali)-[~]
└─$ nslookup
> www.cisco.com
Server:         10.0.2.3
Address:        10.0.2.3#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: 92.123.44.98
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d80:1a3::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:26f0:2d80:1b9::b33
> exit
```

```
▾ www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
    Name: www.cisco.com
    Type: CNAME (5) (Canonical NAME for an alias)
    Class: IN (0x0001)
    Time to live: 2337 (38 minutes, 57 seconds)
    Data length: 26
    CNAME: www.cisco.com.akadns.net
▾ www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net
    Name: www.cisco.com.akadns.net
    Type: CNAME (5) (Canonical NAME for an alias)
    Class: IN (0x0001)
    Time to live: 69 (1 minute, 9 seconds)
    Data length: 26
    CNAME: wwwds.cisco.com.edgekey.net
▾ wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredir.akadns.net
    Name: wwwds.cisco.com.edgekey.net
    Type: CNAME (5) (Canonical NAME for an alias)
    Class: IN (0x0001)
    Time to live: 19742 (5 hours, 29 minutes, 2 seconds)
    Data length: 42
    CNAME: wwwds.cisco.com.edgekey.net.globalredir.akadns.net
▾ wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
    Name: wwwds.cisco.com.edgekey.net.globalredir.akadns.net
    Type: CNAME (5) (Canonical NAME for an alias)
    Class: IN (0x0001)
    Time to live: 3369 (56 minutes, 9 seconds)
    Data length: 24
    CNAME: e2867.dsca.akamaiedge.net
▾ e2867.dsca.akamaiedge.net: type A, class IN, addr 92.123.44.98
    Name: e2867.dsca.akamaiedge.net
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 20 (20 seconds)
    Data length: 4
    Address: 92.123.44.98
```

Come si confrontano i risultati con i risultati di nslookup?

I risultati devono essere gli stessi, come in questo caso.