DNS 1 and DNS2

Question 1: Open the `dns2.pcap` file in Wireshark

1. Launch **Wireshark**.
2. Open the provided **`dns2.pcap`** file (`File` > `Open` > Select `dns2.pcap`).

Question 2: Locate DNS Query and Response Messages

In Wireshark's **Filter bar**, type:

```
dns
```

- Press **Enter** to filter only DNS packets.
- Identify the **DNS query** and **DNS response** packets.

Are DNS messages sent over UDP or TCP?

- In the **Protocol** column, check if the packets are **UDP** or **TCP**.
- Most DNS queries are sent over **UDP (port 53)**, but large responses may use **TCP**.

Question 3: Check the Destination and Source Ports

What is the destination port for the DNS query? What is the source port of the DNS response?

- Click on a **DNS query** packet.
- In the **Packet Details pane**, expand the **User Datagram Protocol (UDP)** or **Transmission Control Protocol (TCP)** section.
- Check the **Destination Port** (should be `53` for queries).
- Now, select the **DNS response** packet and check the **Source Port** (should be `53`).

Question 4: Identify the DNS Server IP

To what IP address is the DNS query sent?

- Click on a **DNS query** packet.
- In the **Packet Details pane**, expand the **Internet Protocol (IP)** section.
- Look at the **Destination IP** (this is the DNS server).

Find your local DNS server using `nm-tool` (Linux)
Open a terminal and run:

```
Nm-tool
```

Look for the **DNS Server IP** under `IP4.DNS` or use:

Linux user : `nmcli dev show | grep 'IP4.DNS'`
`Windows User : Get-DnsClientServerAddress`

- Compare it with the DNS query **destination IP** from Wireshark. Are they the same?

Question 5: Examine the DNS Query Message

What “Type” of DNS query is it? Does it contain any answers?

- Click on a **DNS query** packet.
- Expand the **Domain Name System (DNS)** section.
- Look for **Query Type** (A, AAAA, NS, CNAME, etc.).
- Does it contain an **Answer section**? (Typically, queries do not contain answers.)

Question 6: Examine the DNS Response Message

How many "answers" are provided? What do they contain?

- Click on a **DNS response** packet.
- Expand the **DNS section**.
- Look for **Answer RRs (Resource Records)**.
- Each **answer** may contain an **IP address (A record), alias (CNAME), or other DNS information**.

Question 7: Check the TCP SYN Packet

Does the destination IP of the TCP SYN match any IP from the DNS response?

- After the DNS response, look for a **TCP SYN** packet.

Set Wireshark's filter to:

```
tcp.flags == 0x02
```

- Compare the **Destination IP** in this TCP packet with the **IP addresses from the DNS response**. They should match.

Question 8: Check DNS Queries for Images

Does the host issue new DNS queries for images?

- Look at packets following the initial page load.
- Are there **additional DNS queries** for domains like `cdn.example.com` or `images.example.com`?
- If yes, your browser is resolving image URLs separately.

Question 9: Run `nslookup` and Analyze the Result

To what IP is the `nslookup` query sent? Is it your default DNS server?

Open a terminal and run:

```
nslookup -type=NS mit.edu
```

In Wireshark, filter:

```
dns
```

- Find the **DNS query packet** for `mit.edu` and check the **Destination IP**.
- Compare this with your **default DNS server**

Question 10: Examine the `nslookup` Response

What "Type" of DNS query is it? Does the query contain answers?

- Look at the **Query Type** in the DNS request.
- Since we used `-type=NS`, it should be a **Nameserver (NS) query**.
- Does the query contain any **answers**?

What MIT nameservers are provided? Do they include IPs?

- Look at the **DNS response**.
  Check the **Answer Section** for names like:
- `ns1.mit.edu`
- `ns2.mit.edu`