Cyber Security

Lab 2 - Exploring DNS Traffic

Fullname: Amangeldi Zhanserik
ID: 22B030301
E-mail: zha_amangeldi@kbtu.kz
Date of submission: February 21, 2025
Class time: Thursday, 15:00–18:00

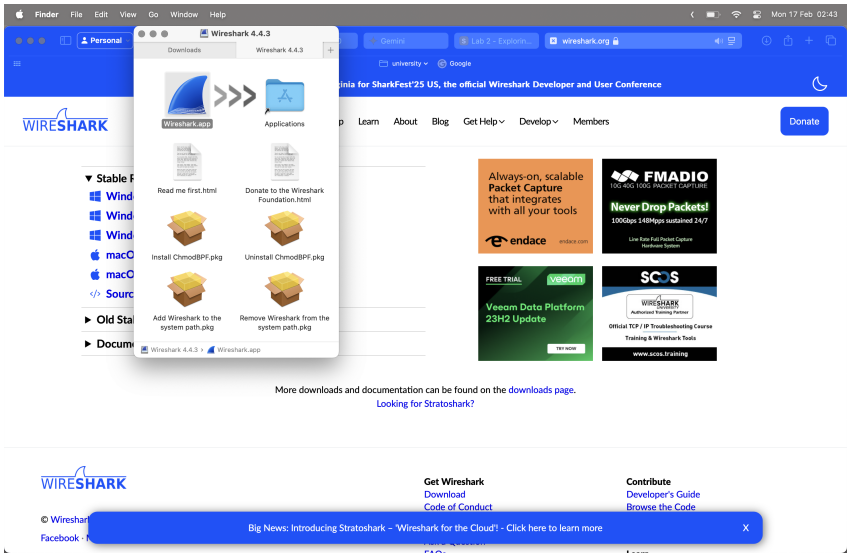
School of Information System and Engineering
Kazakh-British Technical University
Academic Year 2024-2025

1 Capture DNS Traffic

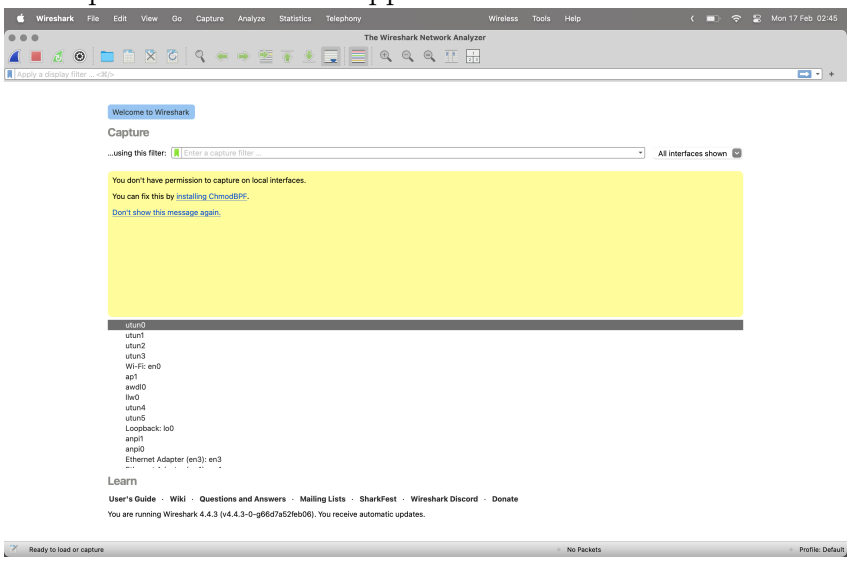
1.1 Download and install Wireshark.

1. I go to the Wireshark website and install version based my own system(MacOS).

2. After downloading it, I open the downloaded file and install it.

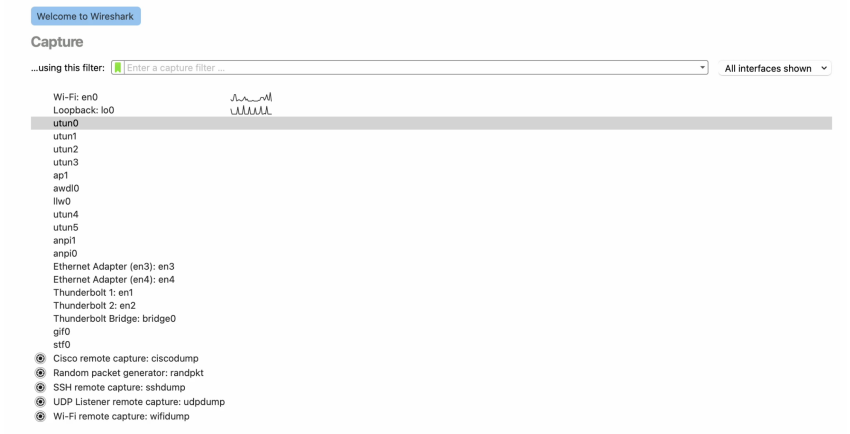


3. And open the Wireshark application.



1.2 Step 2: Capture DNS traffic.

1. Started Wireshark and click on the network interface to capture packets.



2. Clear the DNS cache.

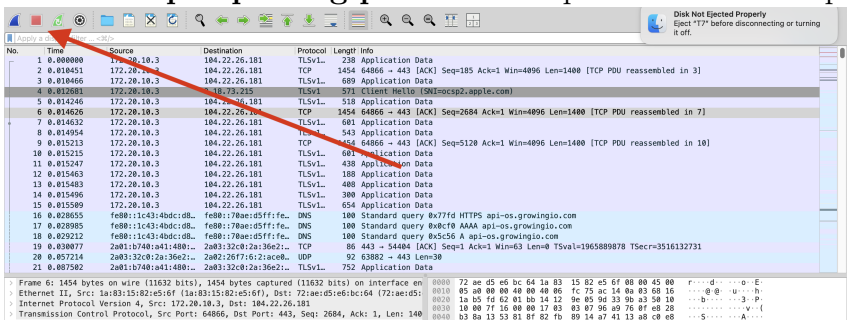
   (a) Because of I have MacOS I entered the following command in the terminal: `sudo killall -HUP mDNSResponder`.

```
mdns options=201<PERFORMNOD,DAD>
zhans@Zhanseriks-Laptop ~ » sudo killall -HUP mDNSResponder && echo macOS DNS Cache Reset
Password:
macOS DNS Cache Reset
zhans@Zhanseriks-Laptop ~ » nslookup
> www.cisco.com
```

3. After that wrote command lookup for the domain name `www.cisco.com` in the terminal, after end of the process wrote exit.

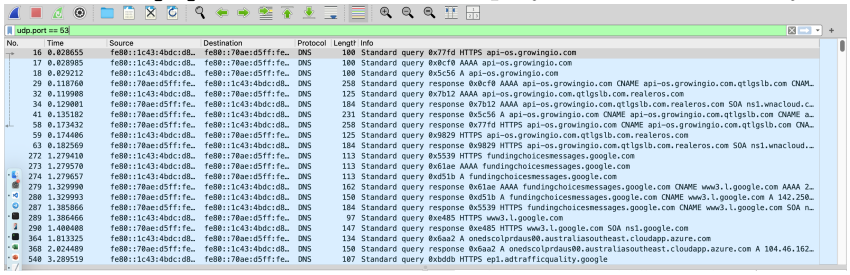
```
zhans@Zhanseriks-Laptop ~ » nslookup
> www.cisco.com
Server:         172.20.10.1
Address:        172.20.10.1#53

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: 23.40.125.28
> exit

zhans@Zhanseriks-Laptop ~ »
```

4. Clicked **Stop capturing packets** to stop the Wireshark capture.



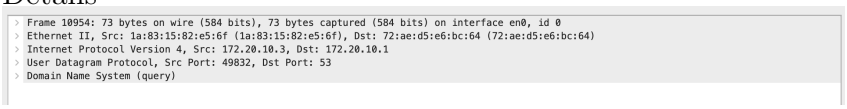
2 Explore DNS Query Traffic

1. Entered `udp.port == 53` in the display filter to show only DNS traffic.

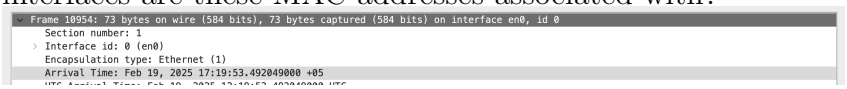


2. Selected the DNS packet contains **Standard query** and **A www.cisco.com** in the Info column.

3. Details

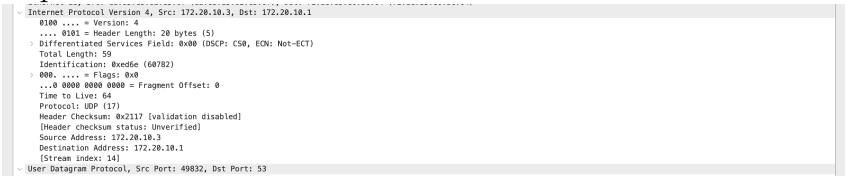


4. **Question**: What are the source and destination MAC addresses? Which network interfaces are these MAC addresses associated with?



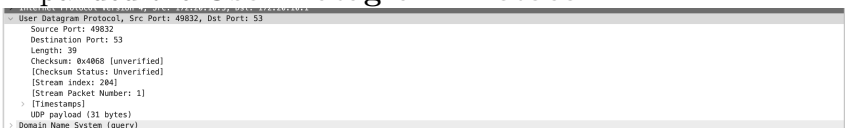
Answer: src: 1a:83:15:82:e5:6f, dst: 72:ae:d5:e6:bc:64, network interface en0.

5. Expanded the **Internet Protocol Version 4**.



6. **Question**: What are the source and destination IP addresses? Which network interfaces are these IP addresses associated with?
Answer: src: 172.20.10.3, dst: 172.20.10.1, with the interface en0.

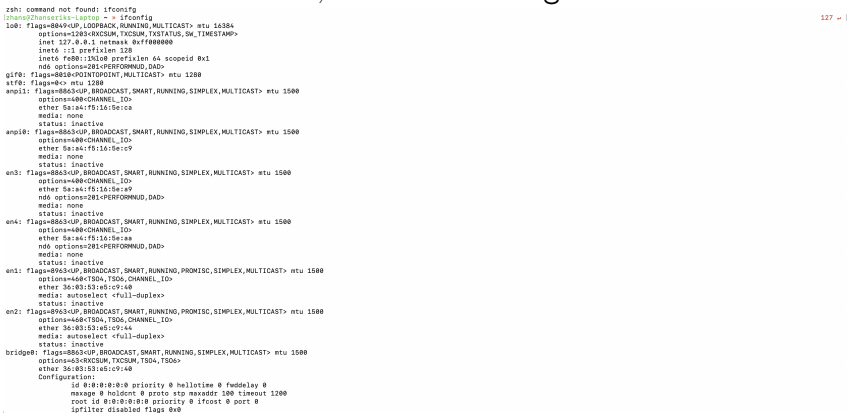
7. Expanded the **User Datagram Protocol**.



8. **Question**: What are the source and destination ports? What is the default DNS port number?
Answer: src port: 49832, dst port: 53, port number 53.

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

   (a) Because I have MacOS, I used `ifconfig` command.

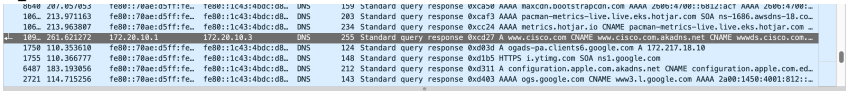


10. **Question**: Compare the MAC and IP addresses in the Wireshark results to the IP and MAC addresses What is your observation?
    Answer: I had difference in Mac addresses, but ip addresses is same.

11. Expanded the **Domain Name System (query)** and all subsections **flags** and **queries**.

3 Explore DNS Response Traffic

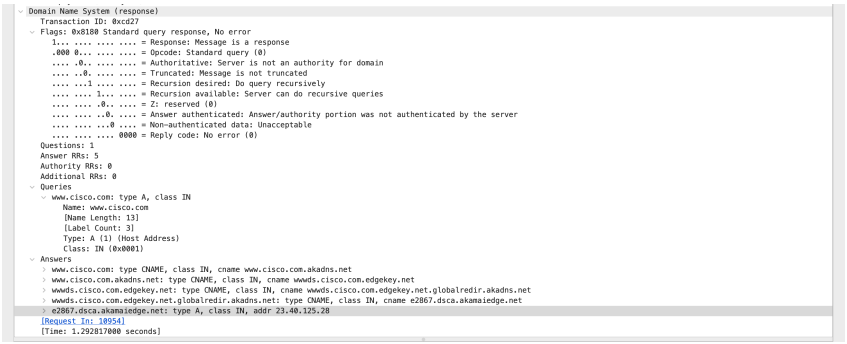
1. Selected the corresponding response DNS packet that has **Standard query response** and **www.cisco.com** in the Info column.



2. **Question**: What are the source and destination MAC and IP addresses and port numbers?
   Answer: Mac src: 72:ae:d5:e6:bc:64 dest: 1a:83:15:82:e5:6f. IP src: 172.20.10.1 dest: 172.20.10.3. Port numbers src: 53, dest: 49832

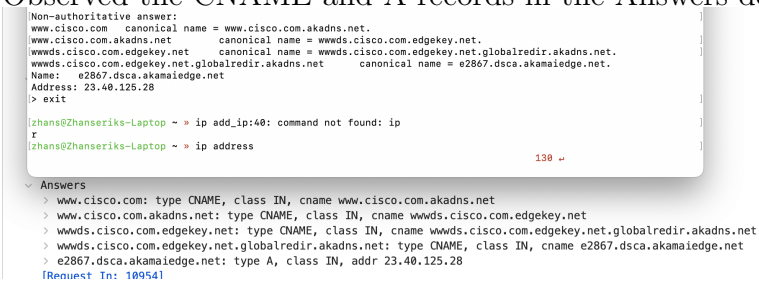
3. How do they compare to the addresses in the DNS query packets? **Answer**: Same but just change the direction(src now is dest, and dest is src).

4. Expanded **Domain Name System (response)**. [cite: 42] Then expanded the **Flags**, **Queries**, and **Answers**.



5. **Question**: Can the DNS server do recursive queries?
   Answer: Yes, dns server can.

6. Observed the CNAME and A records in the Answers details.



7. **Question**: How do the results compare to nslookup results?
   Answer: The same path, but with more details.

4 Reflection

1. From the Wireshark results, what else can you learn about the network when you remove the filter?
   Answer: Without filters, results show other packets like DHCP and ARP, revealing information about other devices and their roles in the LAN.

2. How can an attacker use Wireshark to compromise your network security?
   Answer: An attacker can use Wireshark to capture unencrypted sensitive information on the network.