
Cyber Security

Lab 2 - Exploring DNS Traffic

Fullscreen: Amangeldi Zhanserik

ID: 22B030301

E-mail: zha_amangeldi@kbtu.kz

Date of submission: February 21, 2025

Class time: Thursday, 15:00–18:00

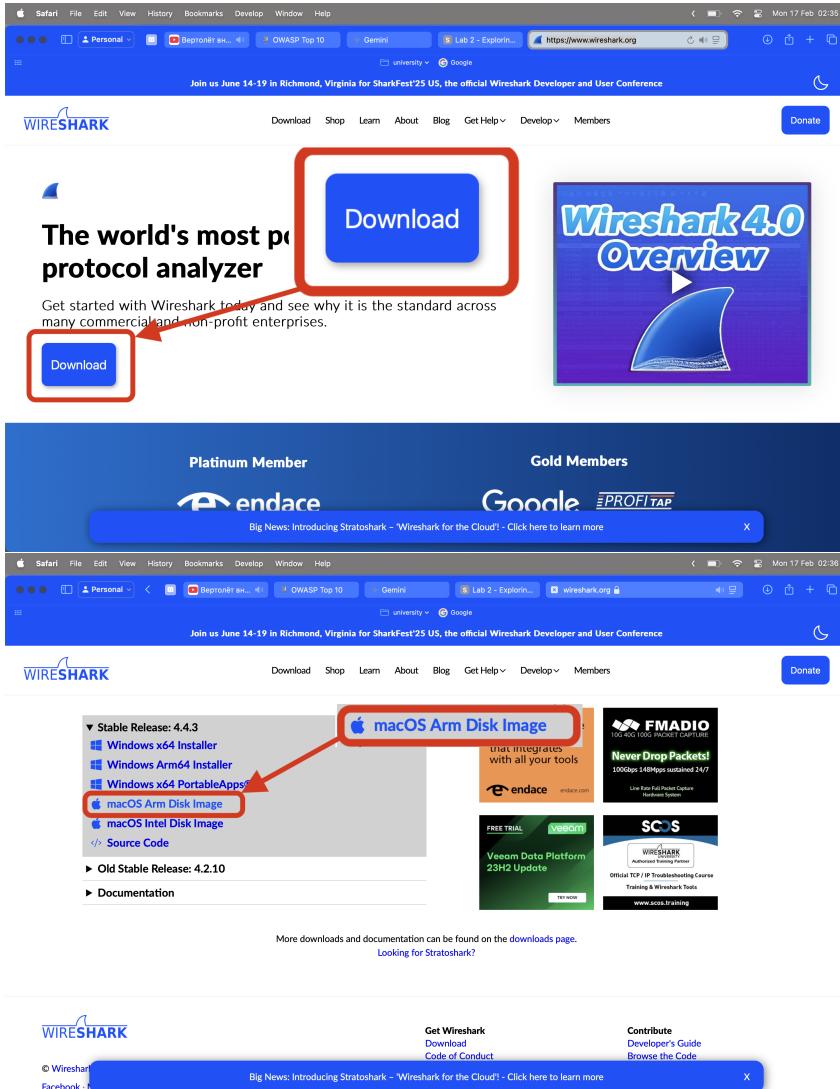


School of Information System and Engineering
Kazakh-British Technical University
Academic Year 2024-2025

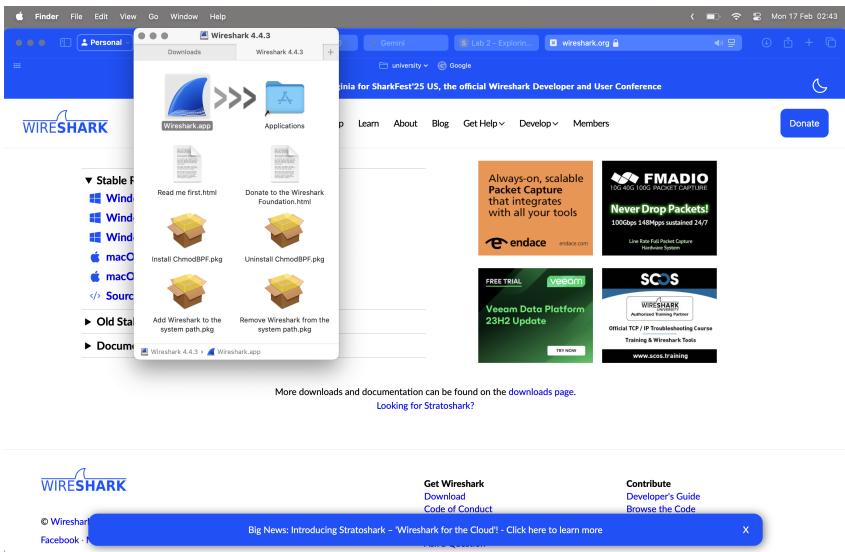
1 Capture DNS Traffic

1.1 Download and install Wireshark.

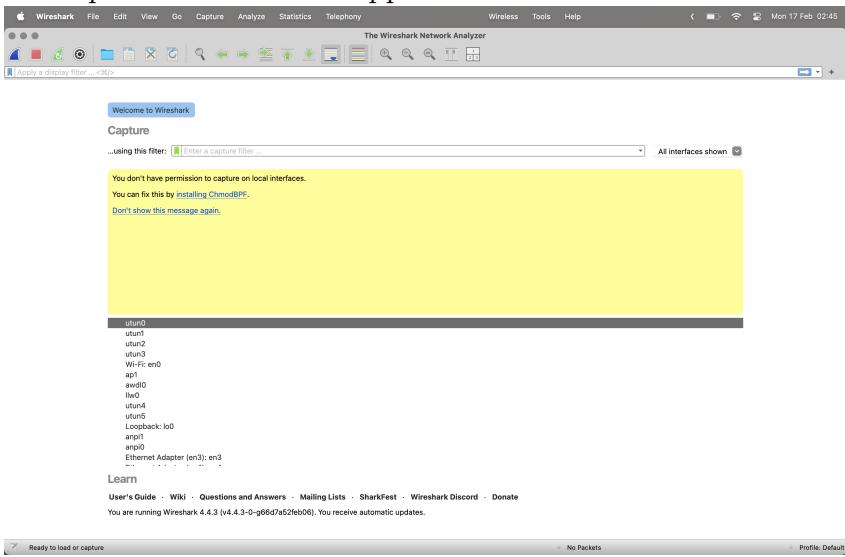
1. I go to the Wireshark website and install version based my own system(MacOS).



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

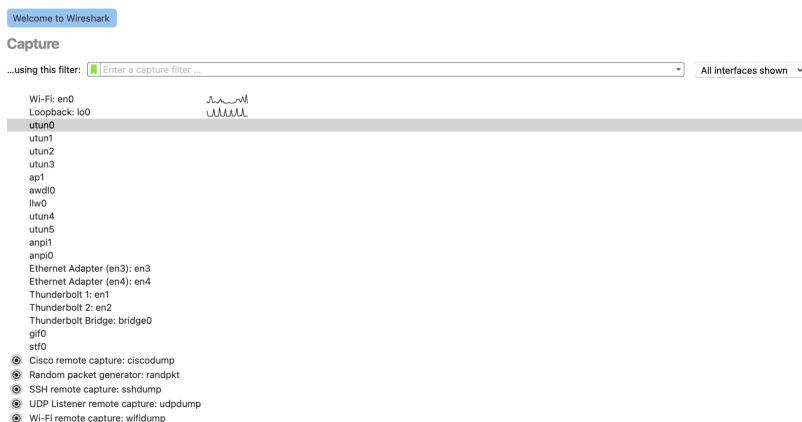


3. And open the Wireshark application.



1.2 Step 2: Capture DNS traffic.

- 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.
```

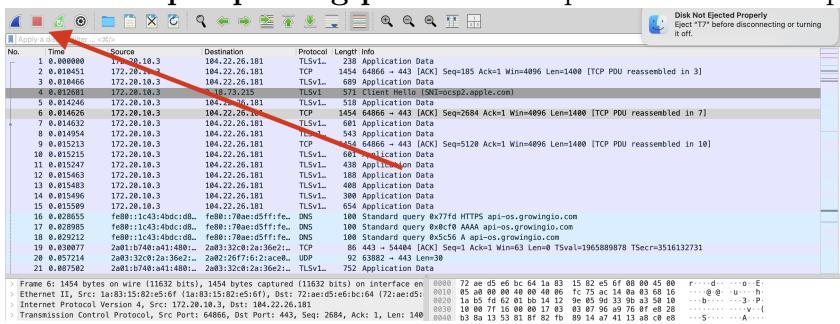
```
zhangs@Zhanseriks-Laptop ~ » sudo killall -HUP mDNSResponder && echo macOS DNS Cache Reset
Password:
macOS DNS Cache Reset
zhangs@Zhanseriks-Laptop ~ » nslookup
> www.cisco.com
```

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

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

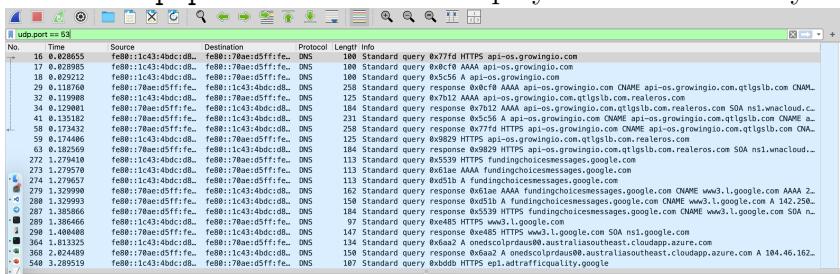
Non-authoritative answer:
www.cisco.com canonical name = www.cisco.com.akadns.net.
www.cisco.com.akadns.net canonical name = wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net canonical name = wwwds.cisco.com.edgekey.net.globalredir.akadns.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net canonical name = e2867.dsca.akamaiedge.net.
Name: e2867.dsca.akamaiedge.net
Address: 23.40.125.28
> exit
```

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.

2713 114.443239 fe80::1c43:40dc:db.. fe80::78ae:c5ffff:fe.. DNS 94 Standard query 0xd483 AAAA op.google.com
6485 183.128198 fe80::1c43:40dc:db.. fe80::78ae:c5ffff:fe.. DNS 114 Standard query 0xd311 A configuration.apple.com.akadns.net
1746 110.321560 fe80::1c43:40dc:db.. fe80::78ae:c5ffff:fe.. DNS 91 Standard query 0xd1b5 HTTPS://tinytng.com
1738 110.265393 fe80::1c43:40dc:db.. fe80::78ae:c5ffff:fe.. DNS 188 Standard query 0xd3d3 A ogad-pa.clients6.google.com
189 259.324544 fe80::1c43:40dc:db.. fe80::78ae:c5ffff:fe.. DNS 93 Standard query 0xc027 A www.cisco.com
186. 213.914568 fe80::1c43:40dc:db.. fe80::78ae:c5ffff:fe.. DNS 97 Standard query 0xcc24 AAA metrics.hotjar.io
186. 213.964518 fe80::1c43:40dc:db.. fe80::78ae:c5ffff:fe.. DNS 119 Standard query 0xc4f3 AAAA pacman-metrics-live.eks.hotjar.com
8031 172.20.10.45 fe80::1c43:40dc:db.. fe80::78ae:c5ffff:fe.. DNS 180 Standard query 0xd401 AAA maxcdn.maxcdn.bootstrapcdn.com
542 3.289795 fe80::1c43:40dc:db.. fe80::78ae:c5ffff:fe.. DNS 187 Standard query 0xc841 A cdn.adraffricafrica.google

3. Details

```
> Frame 10954: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface en0, id 0
> Ethernet II, Src: 1a:83:15:82:e5:6f (1a:83:15:82:e5:6f), Dst: 72:ae:d5:e6:bc:64 (72:ae:d5:e6:bc:64)
> Internet Protocol Version 4, Src: 172.20.10.3, Dst: 172.20.10.1
> User Datagram Protocol, Src Port: 49832, Dst Port: 53
> Domain Name System (query)
```

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

```
> Frame 10954: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface en0, id 0
  Section number: 1
  > Interface id: 0 (en0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 19, 2025 17:19:53.492049000 +05
  ...
```

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.

```
> Internet Protocol Version 4, Src: 172.20.10.3, Dst: 172.20.10.1
  ... 0100 .... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 52
  Identification: 0xedde (64792)
  ... 0000 ... = Flags: 0x0
  ... 0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 60
  Protocol: UDP (17)
  Header Checksum: 0x2117 [validation disabled]
  Header checksum status: unverified
  Source Address: 172.20.10.3
  Destination Address: 172.20.10.1
  [Stream index: 14]
  > User Datagram Protocol, Src Port: 49832, Dst Port: 53
```

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.

```
> User Datagram Protocol, Src Port: 49832, Dst Port: 53
  Source Port: 49832
  Destination Port: 53
  Length: 39
  Checksum: 0x4068 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 284]
  [Stream packet number: 1]
  > [Timestamps]
  UDP payload (31 bytes)
  > Domain Name System (tauvr)
```

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.

```
zsh: command not found: ifconfig
0: flags=4095UP,BROADCAST,NOARP,SMART,RUNNING,MULTICAST mtu 1500
    options=68000<NOARP,BROADCAST,SMART,RUNNING,MULTICAST>
    ether 00:0c:29:14:0d:01 brd ff:ff:ff:ff:ff:ff
    netmask 0xffffffff<0xffffffff>
    broadcast ff:ff:ff:ff:ff:ff
    nd6 options=281<PERFORMNUD,DAD>
    nd6 optplen=4<4> nd6_ifindex=1<1> nd6_lladdr=00:0c:29:14:0d:01
    nd6_ifscope=44<44> nd6_iflink=1<1>
giga0: flags=4095UP,BROADCAST,SMART,RUNNING,MULTICAST mtu 1500
    options=68000<NOARP,BROADCAST,SMART,RUNNING,MULTICAST>
    ether 00:0c:29:14:0d:01 brd ff:ff:ff:ff:ff:ff
    netmask 0xffffffff<0xffffffff>
    broadcast ff:ff:ff:ff:ff:ff
    nd6 options=281<PERFORMNUD,DAD>
    nd6 optplen=4<4> nd6_ifindex=2<2> nd6_lladdr=00:0c:29:14:0d:01
    nd6_ifscope=44<44> nd6_iflink=1<1>
eth0: flags=4095UP,BROADCAST,SMART,RUNNING,MULTICAST mtu 1500
    options=68000<NOARP,BROADCAST,SMART,RUNNING,MULTICAST>
    ether 00:0c:29:14:0d:01 brd ff:ff:ff:ff:ff:ff
    netmask 0xffffffff<0xffffffff>
    broadcast ff:ff:ff:ff:ff:ff
    nd6 options=281<PERFORMNUD,DAD>
    nd6 optplen=4<4> nd6_ifindex=3<3> nd6_lladdr=00:0c:29:14:0d:01
    nd6_ifscope=44<44> nd6_iflink=1<1>
status: inactive
en0: flags=4095UP,BROADCAST,SMART,RUNNING,MULTICAST mtu 1500
    options=68000<NOARP,BROADCAST,SMART,RUNNING,MULTICAST>
    ether 00:0c:29:14:0d:01 brd ff:ff:ff:ff:ff:ff
    netmask 0xffffffff<0xffffffff>
    broadcast ff:ff:ff:ff:ff:ff
    nd6 options=281<PERFORMNUD,DAD>
    nd6 optplen=4<4> nd6_ifindex=4<4> nd6_lladdr=00:0c:29:14:0d:01
    nd6_ifscope=44<44> nd6_iflink=1<1>
status: inactive
en1: flags=4095UP,BROADCAST,SMART,RUNNING,MULTICAST mtu 1500
    options=68000<NOARP,BROADCAST,SMART,RUNNING,MULTICAST>
    ether 00:0c:29:14:0d:01 brd ff:ff:ff:ff:ff:ff
    netmask 0xffffffff<0xffffffff>
    broadcast ff:ff:ff:ff:ff:ff
    nd6 options=281<PERFORMNUD,DAD>
    nd6 optplen=4<4> nd6_ifindex=5<5> nd6_lladdr=00:0c:29:14:0d:01
    nd6_ifscope=44<44> nd6_iflink=1<1>
status: inactive
en2: flags=4095UP,BROADCAST,SMART,RUNNING,MULTICAST mtu 1500
    options=68000<NOARP,BROADCAST,SMART,RUNNING,MULTICAST>
    ether 00:0c:29:14:0d:01 brd ff:ff:ff:ff:ff:ff
    netmask 0xffffffff<0xffffffff>
    broadcast ff:ff:ff:ff:ff:ff
    nd6 options=281<PERFORMNUD,DAD>
    nd6 optplen=4<4> nd6_ifindex=6<6> nd6_lladdr=00:0c:29:14:0d:01
    nd6_ifscope=44<44> nd6_iflink=1<1>
status: inactive
en3: flags=4095UP,BROADCAST,SMART,RUNNING,MULTICAST mtu 1500
    options=68000<NOARP,BROADCAST,SMART,RUNNING,MULTICAST>
    ether 00:0c:29:14:0d:01 brd ff:ff:ff:ff:ff:ff
    netmask 0xffffffff<0xffffffff>
    broadcast ff:ff:ff:ff:ff:ff
    nd6 options=281<PERFORMNUD,DAD>
    nd6 optplen=4<4> nd6_ifindex=7<7> nd6_lladdr=00:0c:29:14:0d:01
    nd6_ifscope=44<44> nd6_iflink=1<1>
status: inactive
en4: flags=4095UP,BROADCAST,SMART,RUNNING,MULTICAST mtu 1500
    options=68000<NOARP,BROADCAST,SMART,RUNNING,MULTICAST>
    ether 00:0c:29:14:0d:01 brd ff:ff:ff:ff:ff:ff
    netmask 0xffffffff<0xffffffff>
    broadcast ff:ff:ff:ff:ff:ff
    nd6 options=281<PERFORMNUD,DAD>
    nd6 optplen=4<4> nd6_ifindex=8<8> nd6_lladdr=00:0c:29:14:0d:01
    nd6_ifscope=44<44> nd6_iflink=1<1>
status: inactive
bridge0: flags=4095UP,BROADCAST,SMART,RUNNING,MULTICAST mtu 1500
    options=3&RCVBUF,TXCSUM,TSD4,TSO4,TBOS+
    ether 00:0c:29:14:0d:01 brd ff:ff:ff:ff:ff:ff
    netmask 0xffffffff<0xffffffff>
    broadcast ff:ff:ff:ff:ff:ff
    nd6 options=281<PERFORMNUD,DAD>
    nd6 optplen=4<4> nd6_ifindex=9<9> nd6_lladdr=00:0c:29:14:0d:01
    nd6_ifscope=44<44> nd6_iflink=1<1>
Configuration:
  id 0x80800 priority 0 holdtime 0 lifetime 0
  maxmtu 1500 queueing discipline pfifo_fast
  root id 0@0@0@0@0 priority 0 ifcost 0 port 0
  ipfilter disabled flags 0x0
.
```

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.

Index	Source MAC	Source IP	Dest MAC	Dest IP	Protocol	Info
186.	00:0c:29:14:0d:01	172.20.10.1	00:0c:29:14:0d:01	172.20.10.3	DNS	129 Standard query response 0xc001 AAAA www.cisco.com.0x00000000000000000000000000000000
186.	00:0c:29:14:0d:01	172.20.10.1	00:0c:29:14:0d:01	172.20.10.3	DNS	130 Standard query response 0xc001 AAAA www.cisco.com.0x00000000000000000000000000000000
186.	00:0c:29:14:0d:01	172.20.10.1	00:0c:29:14:0d:01	172.20.10.3	DNS	131 Standard query response 0xc001 AAAA www.cisco.com.0x00000000000000000000000000000000
186.	00:0c:29:14:0d:01	172.20.10.1	00:0c:29:14:0d:01	172.20.10.3	DNS	132 Standard query response 0xc001 AAAA www.cisco.com.0x00000000000000000000000000000000
186.	00:0c:29:14:0d:01	172.20.10.1	00:0c:29:14:0d:01	172.20.10.3	DNS	133 Standard query response 0xc001 AAAA www.cisco.com.0x00000000000000000000000000000000
186.	00:0c:29:14:0d:01	172.20.10.1	00:0c:29:14:0d:01	172.20.10.3	DNS	134 Standard query response 0xc001 AAAA www.cisco.com.0x00000000000000000000000000000000
186.	00:0c:29:14:0d:01	172.20.10.1	00:0c:29:14:0d:01	172.20.10.3	DNS	135 Standard query response 0xc001 AAAA www.cisco.com.0x00000000000000000000000000000000
186.	00:0c:29:14:0d:01	172.20.10.1	00:0c:29:14:0d:01	172.20.10.3	DNS	136 Standard query response 0xc001 AAAA www.cisco.com.0x00000000000000000000000000000000
186.	00:0c:29:14:0d:01	172.20.10.1	00:0c:29:14:0d:01	172.20.10.3	DNS	137 Standard query response 0xc001 AAAA www.cisco.com.0x00000000000000000000000000000000
186.	00:0c:29:14:0d:01	172.20.10.1	00:0c:29:14:0d:01	172.20.10.3	DNS	138 Standard query response 0xc001 AAAA www.cisco.com.0x00000000000000000000000000000000
186.	00:0c:29:14:0d:01	172.20.10.1	00:0c:29:14:0d:01	172.20.10.3	DNS	139 Standard query response 0xc001 AAAA www.cisco.com.0x00000000000000000000000000000000
186.	00:0c:29:14:0d:01	172.20.10.1	00:0c:29:14:0d:01	172.20.10.3	DNS	140 Standard query response 0xc001 AAAA www.cisco.com.0x00000000000000000000000000000000
186.	00:0c:29:14:0d:01	172.20.10.1	00:0c:29:14:0d:01	172.20.10.3	DNS	141 Standard query response 0xc001 AAAA www.cisco.com.0x00000000000000000000000000000000
186.	00:0c:29:14:0d:01	172.20.10.1	00:0c:29:14:0d:01	172.20.10.3	DNS	142 Standard query response 0xc001 AAAA www.cisco.com.0x00000000000000000000000000000000
186.	00:0c:29:14:0d:01	172.20.10.1	00:0c:29:14:0d:01	172.20.10.3	DNS	143 Standard query response 0xc001 AAAA www.cisco.com.0x00000000000000000000000000000000

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**.

```

    ✓ Domain Name System (response)
      Transaction Id: 0xcd27
      Flags: 0x8180 Standard query response, No error
      1... 0..1. .... = Response: Message is a response
      ...00. 0..1. .... = Standard query message
      .... ..0. .... = Authoritative: Server is not an authority for domain
      .... ..1. .... = Truncated: Message is not truncated
      .... ..1. .... = Recursion desired: Do query recursively
      .... ..1. .... = Recursion available: Server can do recursive queries
      .... ..0.. .... = Z1: 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
    Answers RRs: 5
    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)
    ✓ 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 www.cisco.com.edgekey.net.globalredir.akadns.net
      > e2867.dsca.akamaiedge.net type CNAME, class IN, cname e2867.dsca.akamaiedge.net
      > e2867.dsca.akamaiedge.net type A, class IN, addr 23.40.125.28
      [Request In: 10954]
      [Time: 1.292017000 seconds]

```

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.

```

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

[zhang@Zhangseriks-Laptop ~ » ip add_ip:40: command not found: ip
r
[zhang@Zhangseriks-Laptop ~ » ip address
138 ↵

    ✓ 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 23.40.125.28
      [Request In: 10954]

```

7. Question: How do the results compare to nslookup results?

Answer: The same path, but with more details.

4 Reflection

- 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.

- 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.