

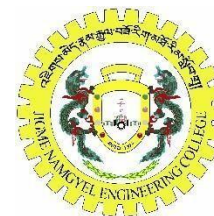
05240133



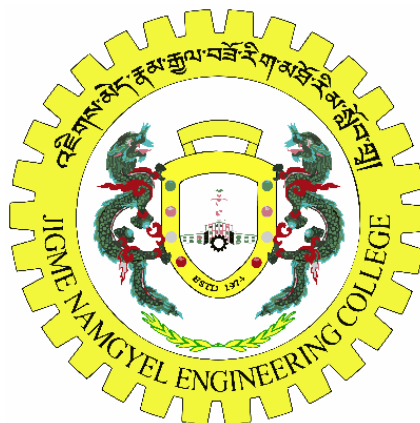
འཇགས་མདེན་རྒྱལ་བཟོ་རྒྱལ་མཐོ་རིམ་སློབ་གྲྭ།

Royal University of Bhutan

Jigme Namgyal Engineering Collage, Dewathang



Lab - Explore DNS Traffic



Submitted by:

Dorji Samdrup (05240133)

DIPLOMA IN COMPUTER SYSTEM AND NETWORK

JIGME NAMGYEL ENGINEERING COLLEGE

ROYAL UNIVERSITY OF BHUTAN

DEWATHANG

(30th August, 2025)

Contents

Background / Scenario.....	3
Part 1: Capture DNS traffic.	3
Part 2: Explore DNS Query Traffic	6
Part 3: Explore DNS Response Traffic.....	10
Reflection Question	11

05240133

Background / Scenario

Wireshark is an opensource packet capture and analysis tool. Wireshark gives a detailed breakdown of the network protocol stack. Wireshark allows you to filter traffic for network troubleshooting, investigate security issues, and analyze network protocols. Because Wireshark allows you to view the packet details, it can be used as a reconnaissance tool for an attacker.

In this lab, you will install Wireshark on a Windows system and use Wireshark to filter for DNS packets and view the details of both DNS query and response packets.

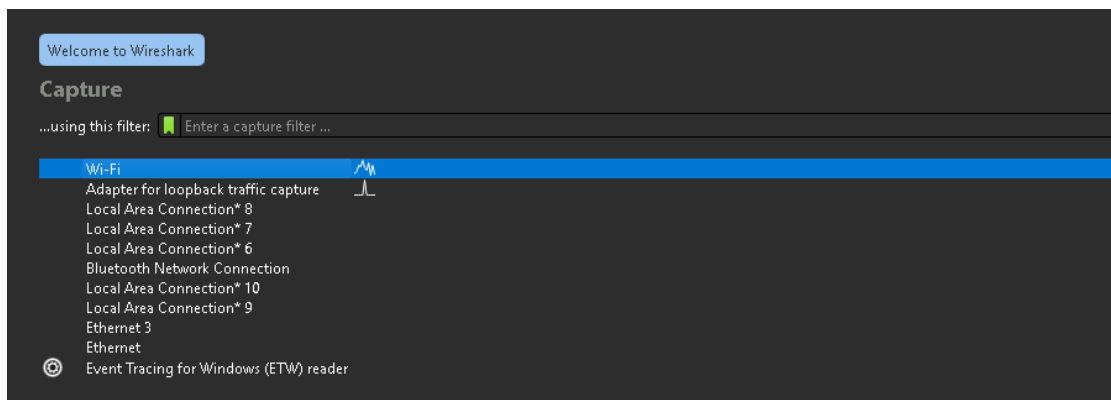
Required Resources

- 1 Windows PC with internet access and Wireshark installed

Instructions

Part 1: Capture DNS traffic.

- a. Open Wireshark and start a Wireshark capture by double clicking a network interface with traffic.



05240133

No.	Time	Source	Destination	Protocol	Length	Info
16	2.035918	192.168.60.166	224.0.0.251	NDNS	119	Standard query 0x00ae PTR_googlecast_tcp.local, "QN" question PTR_674A0243_sub_googlecast_tcp.local, "QN"
17	2.035918	fe80::c4c0:3eff:feb...	ff02::fb	NDNS	139	Standard query 0x00ae PTR_googlecast_tcp.local, "QN" question PTR_674A0243_sub_googlecast_tcp.local, "QN"
18	2.035918	192.168.60.29	224.0.0.251	NDNS	590	Standard query response 0x0000 TXT, cache flush PTR_mi-connect_udp.local PTR {"rm":"Redmi Note 8 Pro","as":["
19	2.035918	fe80::44f1:86a5:9a1...	ff02::fb	NDNS	610	Standard query response 0x0000 TXT, cache flush PTR_mi-connect_udp.local PTR {"rm":"Redmi Note 8 Pro","as":["
20	2.035918	192.168.60.229	224.0.0.251	NDNS	324	Standard query response 0x0000 TXT, cache flush PTR_FC9F5ED42C8A_tcp.local PTR I02KU1b8n14AAA_FC9F5ED42C8A._
21	2.755539	4a:92:cb:42:dd:63	Broadcast	ARP	60	Who has 192.168.60.247? Tell 192.168.60.64
22	2.755539	4a:92:cb:42:dd:63	Broadcast	ARP	60	Who has 192.168.61.98? Tell 192.168.60.64
23	2.755605	23.212.164.226	192.168.60.120	UDP	73	443 → 52237 Len=31
24	2.766496	23.212.164.226	192.168.60.120	UDP	73	443 → 52237 Len=31
25	2.766496	23.212.164.226	192.168.60.120	UDP	73	443 → 52237 Len=31
26	2.766939	192.168.60.120	23.212.164.226	UDP	75	52237 → 443 Len=33
27	2.767083	192.168.60.120	23.212.164.226	UDP	77	52237 → 443 Len=35
28	2.844616	192.168.60.13	255.255.255.255	UDP	506	46386 → 29810 Len=464
29	2.955225	23.212.164.226	192.168.60.120	UDP	66	443 → 52237 Len=24
30	2.955225	23.212.164.226	192.168.60.120	UDP	1494	443 → 52237 Len=1452
31	2.955956	192.168.60.120	23.212.164.226	UDP	77	52237 → 443 Len=35
32	2.956288	192.168.60.120	23.212.164.226	UDP	77	52237 → 443 Len=35
33	3.065048	192.168.60.19	255.255.255.255	UDP	307	54655 → 10001 Len=265

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{...} (4a:92:cb:42:dd:63), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Ethernet II, Src: 4a:92:cb:42:dd:63 (4a:92:cb:42:dd:63), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

- b. At the Command Prompt, enter `ipconfig /flushdns` clear the DNS cache.

```
Microsoft Windows [Version 10.0.26100.5074]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\DELL>
```

- c. Enter `nslookup` at the prompt to enter the `nslookup` interactive mode.

```
C:\Users\DELL>nslookup
Default Server: ns0.jnec.edu.bt
Address: 192.168.255.227
```

- d. Enter the domain name of a website. The domain name `www.cisco.com` is used in this example. Enter `www.cisco.com` at the `>` prompt.

05240133

```
> www.cisco.com
Server: ns0.jnec.edu.bt
Address: 192.168.255.227

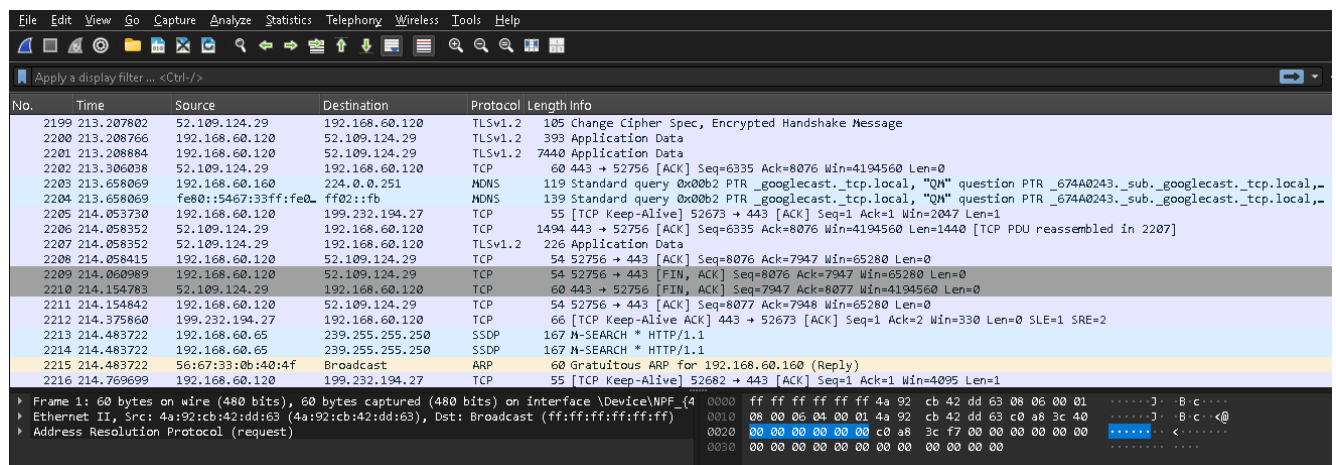
Non-authoritative answer:
Name: e2867.dsca.akamaiedge.net
Addresses: 2600:140f:7:48c::b33
           2600:140f:7:489::b33
           23.204.252.98
Aliases: www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

- e. Enter exit when finished to exit the nslookup interactive mode. Close the command prompt.

```
> exit

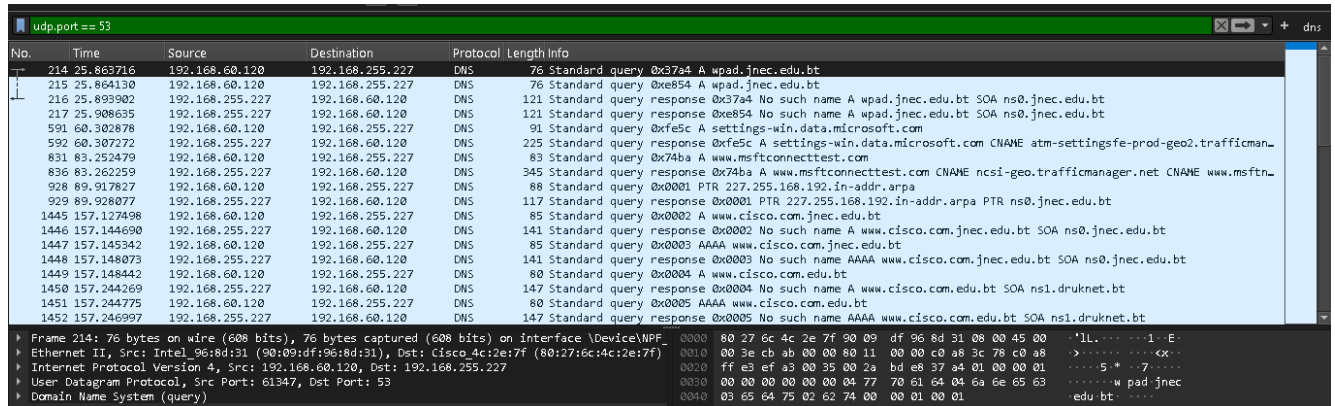
C:\Users\DELL>
```

- f. Click Stop capturing packets to stop the Wireshark capture.

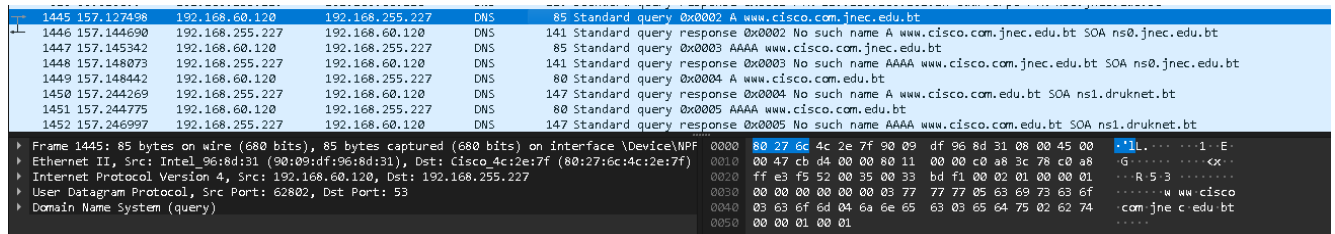


Part 2: Explore DNS Query Traffic

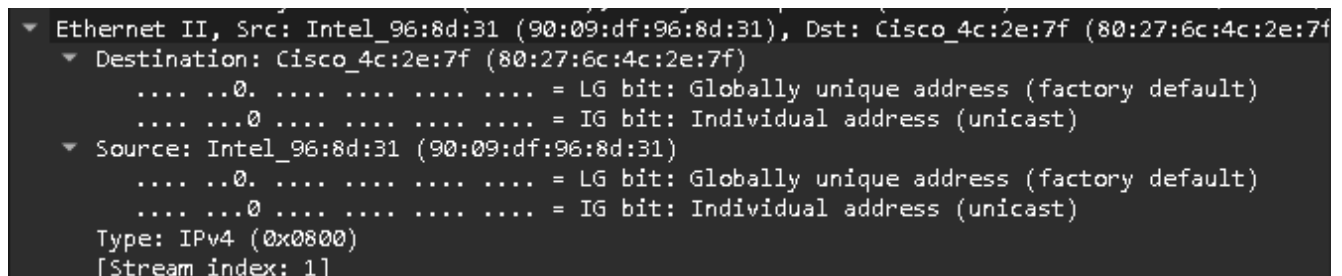
- a. Observe the traffic captured in the Wireshark Packet List pane. Enter `udp.port == 53` in the filter box and click the arrow (or press enter) to display only DNS packets.



- b. Select the DNS packet labeled **Standard query 0x0002 A www.cisco.com**. In the Packet Details pane, notice this packet has Ethernet II, Internet Protocol Version 4, User Datagram Protocol and Domain Name System (query).



- c. Expand Ethernet II to view the details. Observe the source and destination fields.



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

Ans: The source MAC address is associated with the NIC on the PC and the destination MAC address is associated with the default gateway. If there is a local DNS server, the destination MAC address would be the MAC address of the local DNS server.

- d. Expand Internet Protocol Version 4. Observe the source and destination IPv4 addresses.

```

▼ Internet Protocol Version 4, Src: 192.168.60.120, Dst: 192.168.255.227
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 71
  Identification: 0xcbb4 (52180)
  ▼ 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.60.120
  Destination Address: 192.168.255.227
  [Stream index: 55]

```

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

Ans: The source IP address is associated with the NIC on the PC and the destination IP address is associated with the DNS server.

- 1) Expand the User Datagram Protocol. Observe the source and destination ports.

```

▼ User Datagram Protocol, Src Port: 62802, Dst Port: 53
  Source Port: 62802
  Destination Port: 53
  Length: 51
  Checksum: 0xbdf1 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 189]
  [Stream Packet Number: 1]
  ▼ [Timestamps]
    [Time since first frame: 0.000000000 seconds]
    [Time since previous frame: 0.000000000 seconds]
  UDP payload (43 bytes)

```

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

Ans: The source port number is 62802 and the destination port is 53, which is the default DNS port number.

- 2) Open a Command Prompt and enter `arp -a` and `ipconfig /all` to record the MAC and IP addresses of the PC.

```
C:\Users\DELL>arp -a
```

```
Interface: 192.168.60.120 --- 0x7
```

Internet Address	Physical Address	Type
192.168.60.1	80-27-6c-4c-2e-7f	dynamic
192.168.60.138	f8-54-f6-ef-de-2f	dynamic
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

```
Interface: 192.168.128.1 --- 0xd
```

Internet Address	Physical Address	Type
192.168.128.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static

```
C:\Users\DELL>
```



```

C:\Users\DELL>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : DESKTOP-CTB9450
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Mixed
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : jnec.edu.bt

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix . :
    Description . . . . . : VirtualBox Host-Only Ethernet Adapter
    Physical Address. . . . . : 0A-00-27-00-00-0D
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::7106:5771:1dfe:8f8f%13(Preferred)
    IPv4 Address. . . . . : 192.168.128.1(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
    DHCPv6 IAID . . . . . : 906625063
    DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-0D-54-2F-4C-D7-17-79-7F-AA
    NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Local Area Connection* 9:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
    Physical Address. . . . . : 90-09-DF-96-8D-32
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

```

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

Ans: The IP and MAC addresses captured in the Wireshark results are the same as the addresses listed in arp - a and ipconfig /all command.

05240133

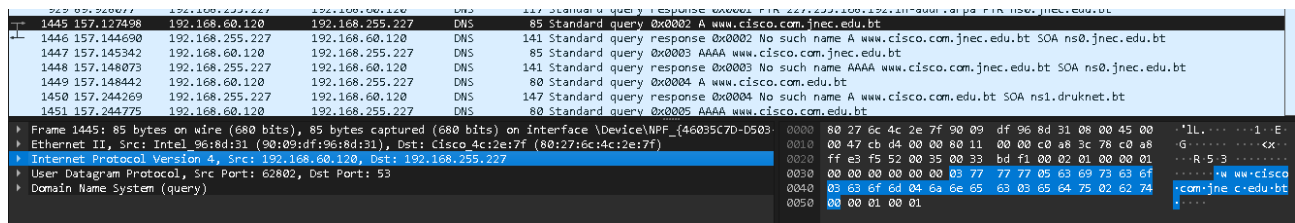
- 3) Expand Domain Name System (query) in the Packet Details pane. Then expand the Flags and Queries.

```
Domain Name System (query)
  Transaction ID: 0x0002
  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.jnec.edu.bt: type A, class IN
    [Response In: 1446]
```

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

Part 3: Explore DNS Response Traffic

- a. Select the corresponding response DNS packet labeled Standard query response 0x0002 A www.cisco.com.



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?

Ans: The source IP, MAC address, and port number in the query packet are now destination addresses. The destination IP, MAC address, and port number in the query packet are now source addresses.

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

```

Domain Name System (query)
  Transaction ID: 0x0002
  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.jnec.edu.bt: type A, class IN
    [Response In: 1446]

```

Observe the results.

Can the DNS server do recursive queries?

Ans: Yes, the DNS can handle recursive queries.

- c. Observe the CNAME and A records in the answers details.

How do the results compare to nslookup results?

Ans: The results in the Wireshark should be the same as the results from nslookup in the Command Prompt.

Reflection Question

1. From the Wireshark results, what else can you learn about the network when you remove the filter?

Ans: Without the filters, the results display other packets, such as DHCP and ARP. From these packets and the information contained within these packets, you can learn about other devices and their functions within the LAN.

2. How can an attacker use Wireshark to compromise your network security?

Ans: An attacker on the LAN can use Wireshark to observe the network traffic and can get sensitive information in the packet details if the traffic is not encrypted.