

<b>Register No:</b>	<b>99220040570</b>
<b>Name:</b>	<b>K.Hanumaan</b>
<b>Class/Section:</b>	<b>8501 A/S06</b>
<b>Ex.No:</b>	<b>14</b>
<b>Name of the Experiment</b>	<b>Capture and Analyse DNS packet</b>
<b>Google Drive link of the packet tracer file (give view permission):</b>	<a href="https://drive.google.com/drive/folders/1GFJ2cdfYx5oDNC8sKrTu826JfcdL5KI?usp=drive_link">https://drive.google.com/drive/folders/1GFJ2cdfYx5oDNC8sKrTu826JfcdL5KI?usp=drive_link</a>

1. Use command prompt and fill the following details using ipconfig /all command. (highlight and paste screenshot for each of the output).

Parameter	Value
Your Machine IP Address.	10.2.16.28
Your Machine MAC Address	14-D4-24-17-5E-9B
Default Gateway address	10.2.0.1
DNS Server IP Address	172.16.103.254

Wireless LAN adapter Wi-Fi:

```

Connection-specific DNS Suffix . : 
Description . . . . . : MediaTek MT7921 Wi-Fi 6 802.11ax PCIe Adapter
Physical Address. . . . . : 14-D4-24-17-5E-9B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::81c6:cfc8:e5c5:292e%5(Preferred)
IPv4 Address. . . . . : 10.2.16.28(Preferred)
Subnet Mask . . . . . : 255.255.224.0
Lease Obtained. . . . . : 14 March 2025 13:40:12
Lease Expires . . . . . : 15 March 2025 01:40:12
Default Gateway . . . . . : 10.2.0.1
DHCP Server . . . . . : 10.2.0.2
DHCPv6 IAID . . . . . : 68473892
DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-F6-99-AF-E0-73-E7-CE-7D-F6
DNS Servers . . . . . : 172.16.103.254
                        4.2.2.2
                        8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled

```

2. Ping any website through command prompt and Fill the following details by applying the filter as **DNS**:  
(highlight and paste screenshot for each of the output).

### DNS Query message:

Field Name	Field Length (no of bits)	Field value
Destination MAC Address	48 bits	c8:4f:86:fc:00:10
Source MAC Address	48 bits	14:d4:24:17:5e:9b
Destination IP Address	32 bits	172.16.103.254
Source IP Address	32 bits	10.2.16.28
Destination UDP port	16 bits	53 (DNS Server)
Source UDP port	16 bits	56539 (Ephemeral Port)
DNS Tx id	16 bits	0x20f8 (Randomly generated for matching request – response)
DNS Flags	16 bits	0x0100 (Standard query)
DNS Questions	16 bits	1 (Single Query)
DNS Queries	Variable	<a href="http://www.flipkart.com">www.flipkart.com</a> : type A, class IN

The screenshot displays a Wireshark capture of network traffic on the \*Wi-Fi interface. The packet list shows four packets related to a DNS query and response. The selected packet (No. 7158) is a DNS Standard query from 10.2.16.28 to 172.16.103.254. The packet details pane shows the query structure, including the transaction ID (0x20f8), flags (0x0100), and the query for www.flipkart.com type A. The packet bytes pane shows the raw data of the query.

```

> Frame 7158: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{149AA54B-F72F-4FA9-92FD-52EABE47000A}, id 0
> Ethernet II, Src: AzureWaveTec_17:5e:9b (14:d4:24:17:5e:9b), Dst: Sophos_fc:00:10 (c8:4f:86:fc:00:10)
  > Destination: Sophos_fc:00:10 (c8:4f:86:fc:00:10)
  > Source: AzureWaveTec_17:5e:9b (14:d4:24:17:5e:9b)
    Type: IPv4 (0x0800)
    [Stream index: 72]
  > Internet Protocol Version 4, Src: 10.2.16.28, Dst: 172.16.103.254
  > User Datagram Protocol, Src Port: 56539, Dst Port: 53
  > Domain Name System (query)
    Transaction ID: 0x20f8
    > 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.flipkart.com: type A, class IN
    [Response In: 7172]
  
```

## 3. DNS Response message: (highlight and paste screenshot for each of the output).

## DNS Response message:

Field Name	Field Length (no of bits)	Field value
Destination MAC Address	48 bits	14:d4:24:17:5e:9b
Source MAC Address	48 bits	c8:4f:86:fc:00:10
Destination IP Address	32 bits	10.2.16.28
Source IP Address	32 bits	172.16.103.254
Destination UDP port	16 bits	56539
Source UDP port	16 bits	53
DNS Tx id	16 bits	0x20f8
DNS Flags	16 bits	0x8180 (Standard query response, No error)
DNS Questions	16 bits	1
DNS Queries	Variable	<a href="http://www.flipkart.com">www.flipkart.com</a> : type A, class IN

The screenshot shows a Wireshark packet capture of a DNS response. The packet list at the top shows four packets: a standard query (No. 4936), a standard query response (No. 4937), another standard query (No. 7158), and a standard query response (No. 7172). The selected packet (No. 7172) is a standard query response from 172.16.103.254 to 10.2.16.28. The packet details pane shows the following structure:

- Frame 7172: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF\_{149AA54B-F72F-4FA9-92FD-52EABE47000A}, id 0
- Ethernet II, Src: Sophos\_fc:00:10 (c8:4f:86:fc:00:10), Dst: AzureWaveTec\_17:5e:9b (14:d4:24:17:5e:9b)
- Internet Protocol Version 4, Src: 172.16.103.254, Dst: 10.2.16.28
- User Datagram Protocol, Src Port: 53, Dst Port: 56539
- Domain Name System (response)
  - Transaction ID: 0x20f8
  - 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: 2
  - Authority RRs: 0
  - Additional RRs: 0
  - Queries
  - Answers

The packet bytes pane on the right shows the raw data in hexadecimal and ASCII. The bottom status bar indicates 10432 packets displayed, 4 displayed, and 0 dropped.

Paste the Wireshark File with view permission:

Google Drive Link: [https://drive.google.com/drive/folders/1GFJ2cdfYx5oDNC8sKrTu826JfcdL5KI?usp=drive\\_link](https://drive.google.com/drive/folders/1GFJ2cdfYx5oDNC8sKrTu826JfcdL5KI?usp=drive_link)

Rubrics for Wireshark labs: (To be Filled by the Class Teacher)

Rubrics	Excellent	Fair	Poor	Marks
<b>Understanding (2)</b>	Understand the Concept very well. (2)	Understand the Concept (1)	Poor Understand the Concept (0)	
<b>Usage of filters (3)</b>	Identified and applied the filter correctly (3)	Identified the filter, but not applied correctly (2-1)	Couldn't identify and apply the filter. Just captured the packets (1)	
<b>Attach relevant Screenshots (3)</b>	clearly Highlighted the answers and attached the screenshots (3)	attached the screenshots, but not highlighted. (2-1)	Did not attach the screenshots (0)	
<b>On time Submission (2)</b>	Early or on time submission (2)	Submitted after deadline (1)	Did not Submit (0)	
Total				

Result: Thus the Capture and Analysis of DNS packet has been implemented and successfully verified.