Register No:	**99220040570**
Name:	**K.Hanumaan**
Class/Section:	**8501 A/S06**
Ex.No:	**14**
Name of the Experiment	**Capture and Analyse DNS packet**
Google Drive link of the packet tracer file **(give view permission):**	https://drive.google.com/drive/folders/1GFJ2cdfYx5oDNC8sKrTu826JfcdrL5Kl?usp=drive_link

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

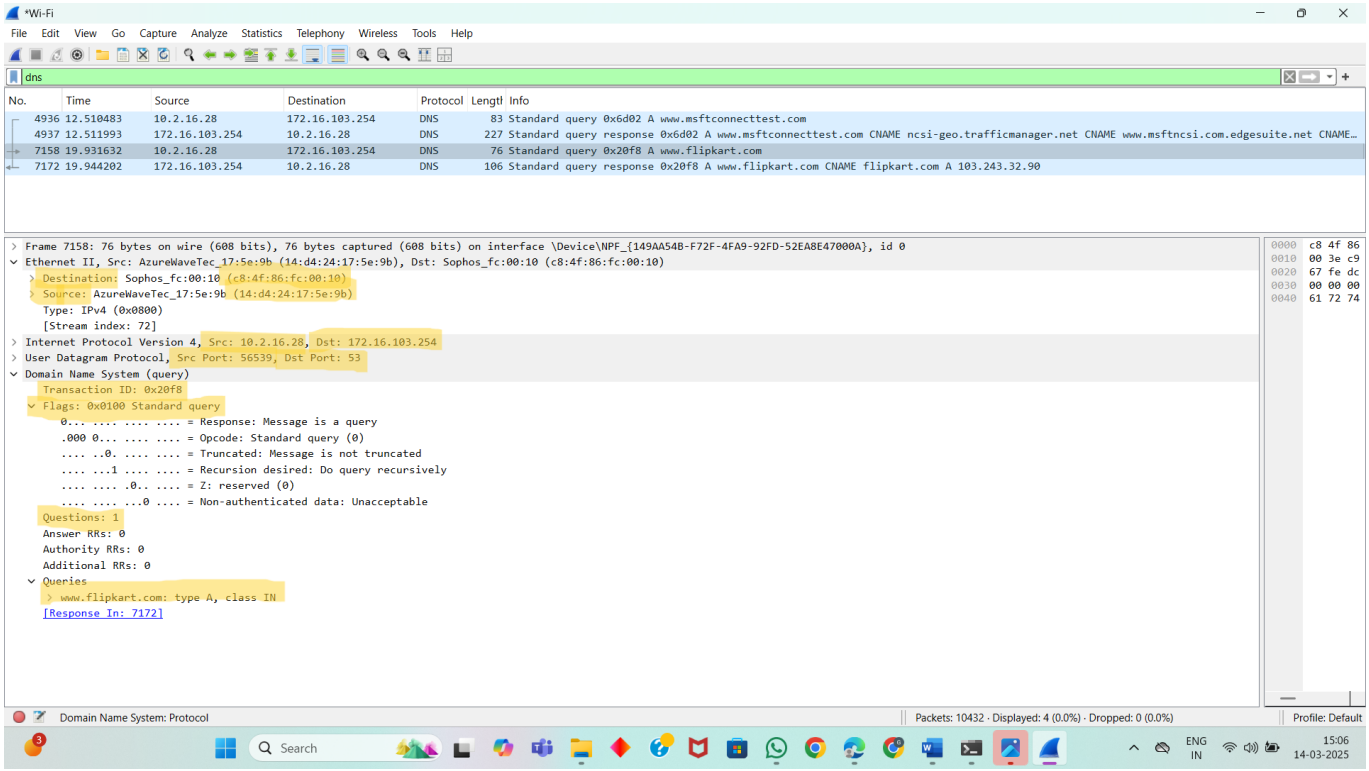
```
Wireless LAN adapter Wi-Fi:

   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:

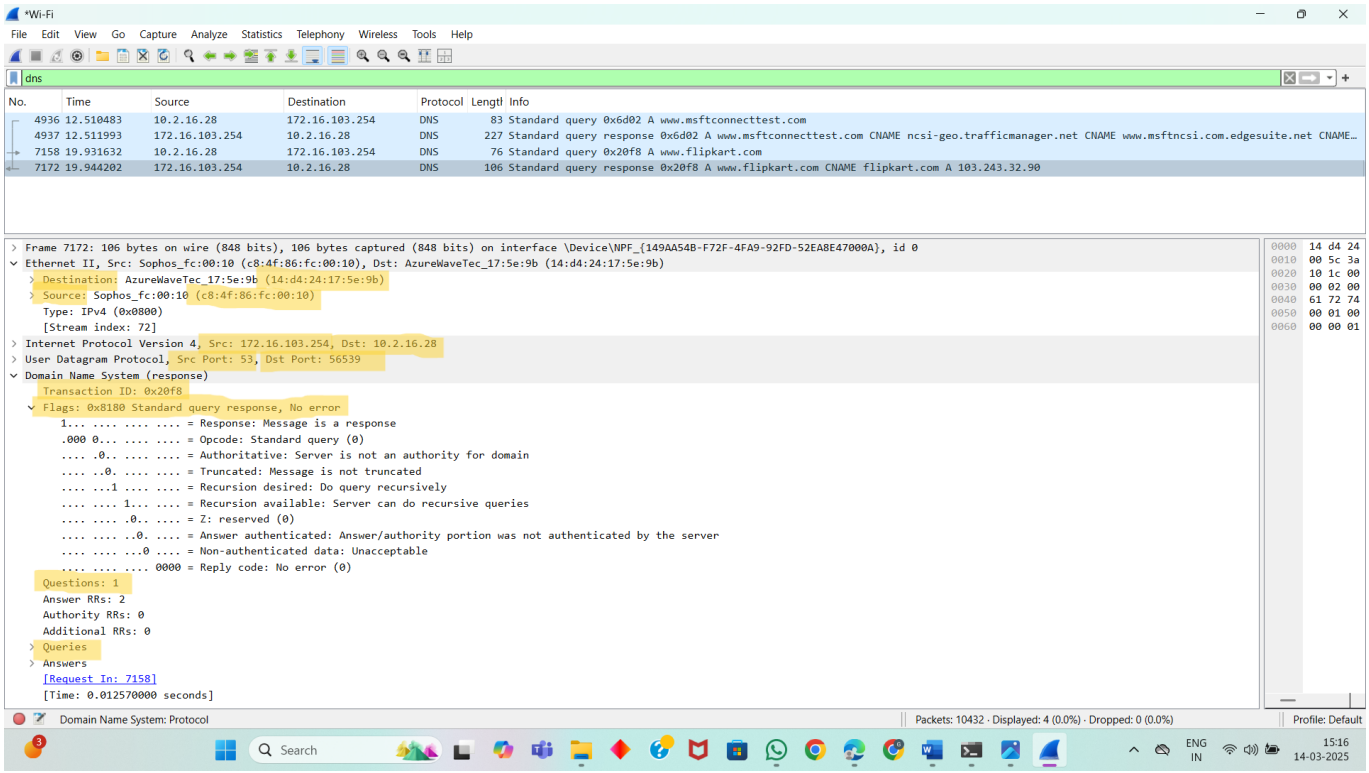
Field Name	**Field Length (no of bits)**	**Field value**
Destination MAC Address	48 bits	c8:4f:86:fc:00:10
Source MAC Address	48 bits	14:d4:24:17:5e:9b
Destination IP Address	32 bits	172.16.103.254
Source IP Address	32 bits	10.2.16.28
Destination UDP port	16 bits	53 (DNS Server)
Source UDP port	16 bits	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	www.flipkart.com: type A, class IN



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	www.flipkart.com: type A, class IN



Paste the Wireshark File with view permission:

Google Drive Link:https://drive.google.com/drive/folders/1GFJ2cdfYx5oDNC8sKrTu826JfcdrL5Kl?usp=drive_link

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

Rubrics	**Excellent**	**Fair**	**Poor**	**Marks**
Understanding (2)	Understand the Concept very well. (2)	Understand the Concept (1)	Poor Understand the Concept (0)	
Usage of filters (3)	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)	
Attach relevant Screenshots (3)	clearly Highlighted the answers and attached the screenshots (3)	attached the screenshots, but not highlighted. (2-1)	Did not attach the screenshots (0)	
On time Submission (2)	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.