

Computer Network and Defense Fundamentals





Module 01



Basic Network Administration and Troubleshooting Using Windows Command Line Utilities

Windows offers several powerful command line utilities that help administrators in troubleshooting their network connections.

ICON KEY

-  Valuable Information
-  Test Your Knowledge
-  Web Exercise
-  Workbook Review

Lab Scenario

Network troubleshooting is becoming the most common task that a network admin needs to perform in large or medium organizations. As a network administrator, you are often required to troubleshoot the network problems as a part of your role and responsibilities. Administrators should have basic knowledge of network troubleshooting required to diagnose, monitor, and repair network connections. There are various basic Windows commands available to diagnose a network problem that every network admin needs to know.

Lab Objectives

This lab demonstrates the use of basic Windows command-line utilities to perform troubleshooting in the network

Lab Environment

To carry out this lab, you need:

- Windows Server 2012 and Windows 10 VMs
- Administrator privileges to run the tools

Lab Duration

Time: 25 Minutes

Overview of the Lab

Windows Command utilities such as ipconfig, Ping, tracert, nslookup, netstat, arp, etc., allows you to administer, diagnose, monitor, and repair network connections.

Note: Before starting this lab, login to Windows 10 VM (User: Admin, Password: Pa\$\$w0rd) and disable the network adapter:

- Go to Control Panel → Network and Internet → Network and Sharing Center, and click Change adapter settings

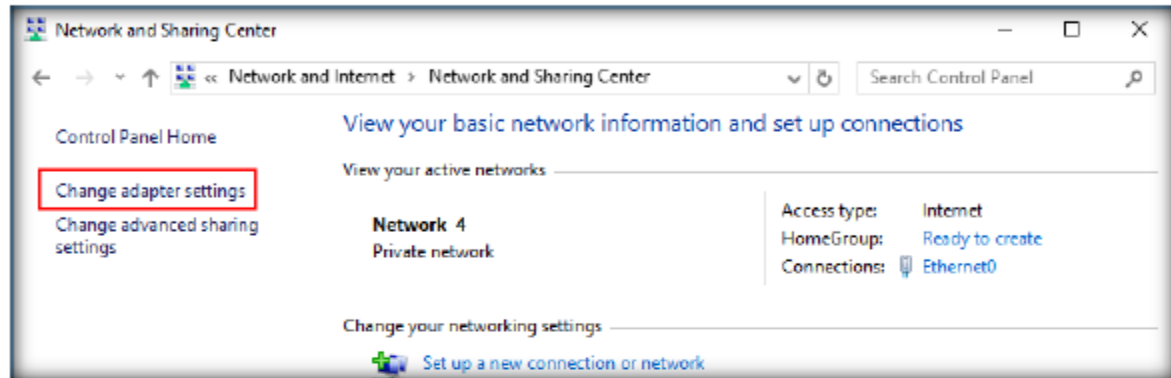


FIGURE 1.1: Change Adapter Settings

- Select and right-click the Ethernet adapter, and click Disable from the context menu.

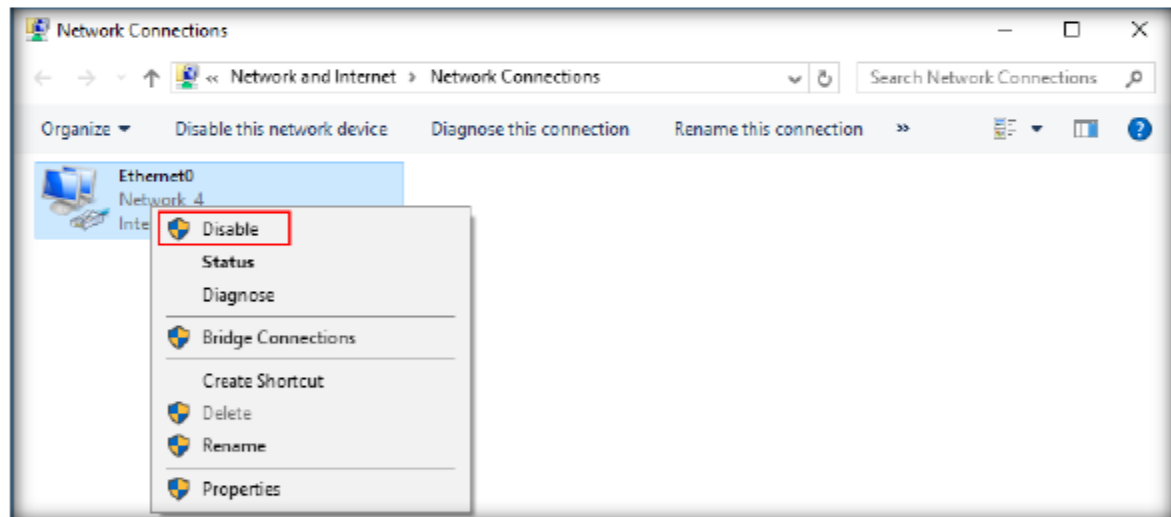


FIGURE 1.2: Disabling Network Adapter

- It will disable Ethernet adapter as shown below.

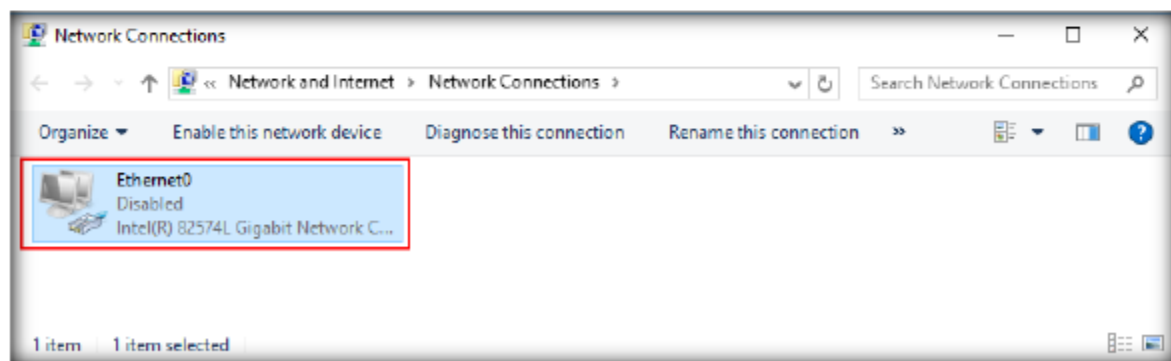


FIGURE 1.3: Network Adapter Disabled

Lab Tasks

TASK 1

Verifying IP Configuration Settings

1. Launch **Windows Server 2012** VM, and login to the local administrator account (username: **Administrator** and password: **Pa\$\$w0rd**).
2. Open a command prompt in Admin mode by right-clicking on the **Start** icon and then click on **Command Prompt (Admin)** from the context menu.

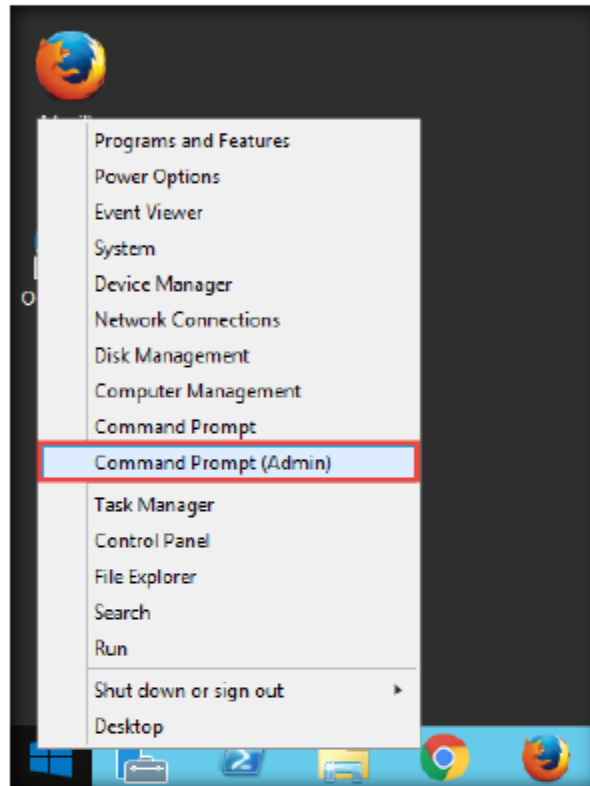


FIGURE 1.4: Launching Command Prompt

3. The command prompt appears on the screen

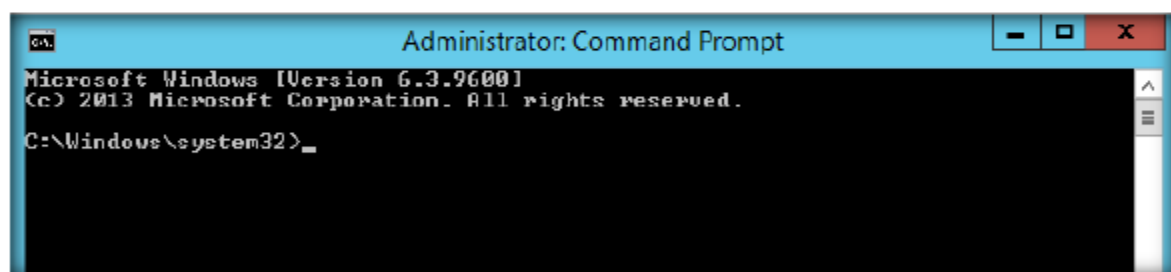


FIGURE 1.5: User Account Control

4. Type **ipconfig** in the command prompt and press **Enter** to verify the IP configuration settings of the machine.
5. The IP Configuration details of the system will be displayed. As a network admin you should know the IP configuration details of all the systems in the network.

ipconfig Syntax

```
ipconfig [/all] [/renew
[Adapter]] [/release
[Adapter]] [/flushdns]
[/displaydns] [/registerdns]
[/showclassid Adapter]
[/setclassid Adapter
[ClassID]].
```

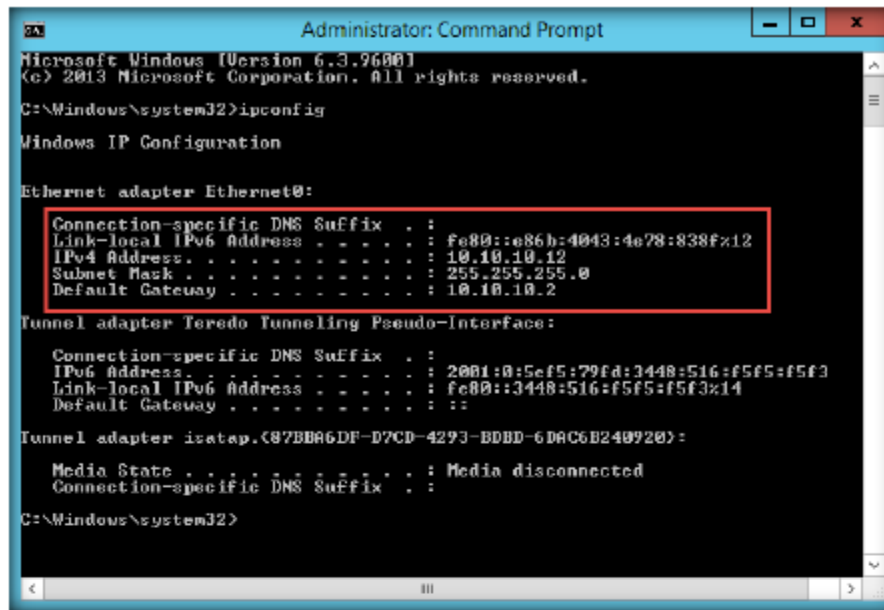


FIGURE 1.6: Checking IP Configuration

- You can use different ipconfig parameters to perform various network troubleshooting activities.

ipconfig Parameters	
/all	Displays the full TCP/IP configuration for all adapters.
/renew [Adapter]	Renews DHCP configuration for all adapters
/release [Adapter]	Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and discard the IP address configuration for either all adapters (if an adapter is not specified) or for a specific adapter
/flushdns	Flushes and resets the contents of the DNS client resolver cache.
/displaydns	Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer.
/registerdns	Initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer.
/showclassid Adapter	Displays the DHCP class ID for a specified adapter.
/setclassid Adapter [ClassID]	Configures the DHCP class ID for a specified adapter.
/?	Displays help at the command prompt.

- Now, type **ipconfig /all** and press **Enter**. This command will list out the System's IP configuration, host name, Ethernet Adapter installed and its MAC Address (Physical Address) and so on, as shown in the screenshot.

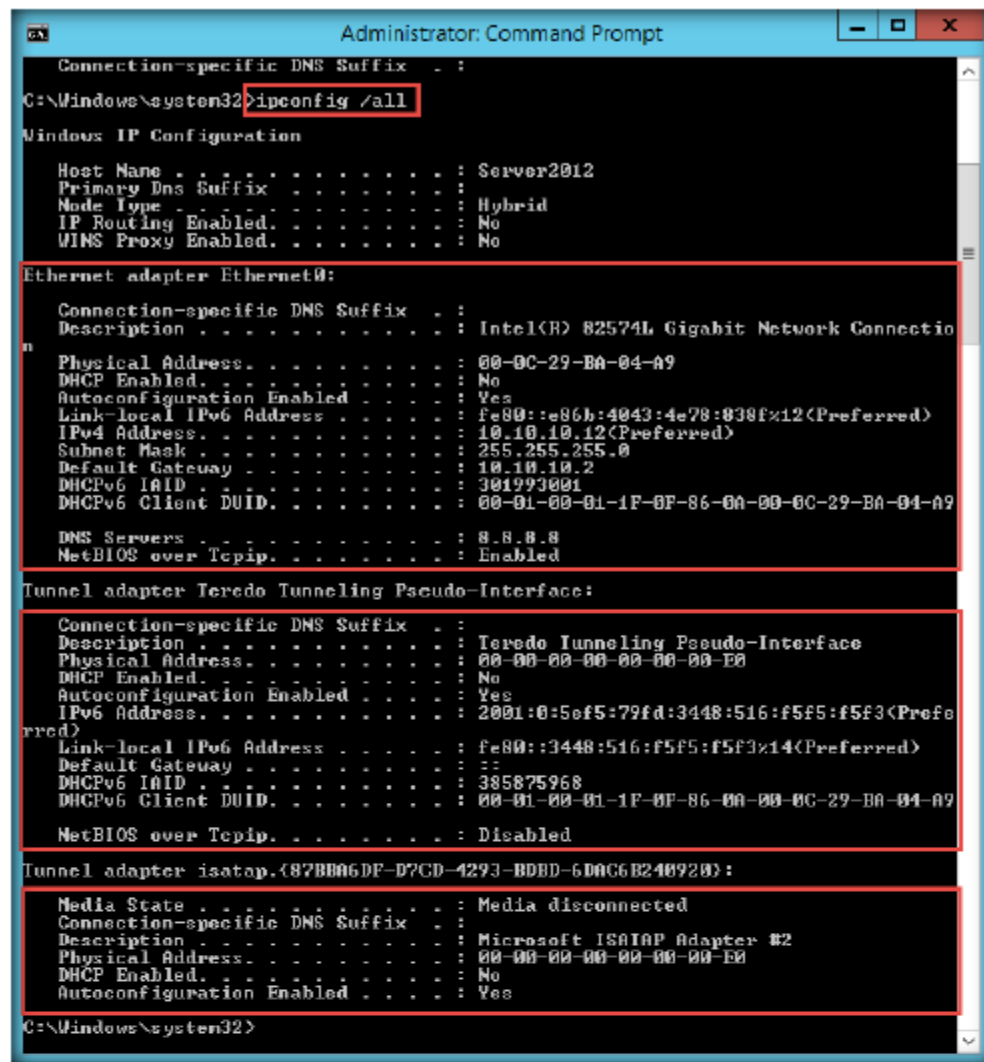


FIGURE 1.7: Complete IP Configuration

8. You can use the information obtained from the above steps to create an Inventory List of all the computing devices in the network. In later modules we will look at better and more sophisticated techniques to create a Network Inventory but this could be an ideal starting point.

S. No.	Host Name	MAC Address	DHCP State	IP Address	Subnet Mast	Gateway
1						
2						
3						

9. Close the command prompt after noting down all the information.
10. Now, we will explore the usage of the **Ping** command. Network administrators always encounter IP level Connectivity errors in the network such as **Request timed out**, **Destination host unreachable**, etc. With the help of the Ping command, they can ensure the reachability of a host to other hosts connected in the network
11. Open a command prompt in the Admin mode by right-clicking on the **Start** icon and then clicking on **Command Prompt (Admin)** from the context menu. Type **ping** followed by the IP address of the Windows 10 machine (it is 10.10.10.10 for this lab setup)

TASK 2
Checking IP level Connectivity Using Ping command

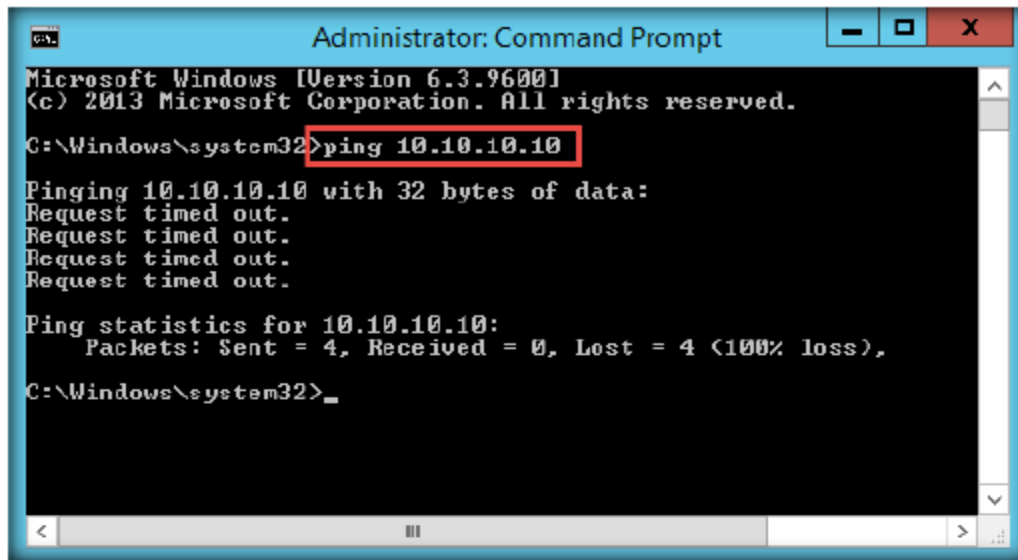


FIGURE 1.8: Demonstration of the Ping command

12. You can see that the “**Request timed out**” error. It means that the target system did not reply within the stipulated time frame. It implies that the target device is out of reach. The cause of this is either due to the target machine is turned off or the Network adapter is disabled on the target machine.

Option	Use
-n <i>Count</i>	Determines the number of echo requests to send. The default is 4 requests.
-w <i>Timeout</i>	Enables you to adjust the time-out (in milliseconds). The default is 1,000 (a 1-second time-out).
-l <i>Size</i>	Enables you to adjust the size of the ping packet. The default size is 32 bytes.
-f	Sets the Do Not Fragment bit on the ping packet. By default, the ping packet allows fragmentation.

13. Now, switch to the Windows 10 machine to troubleshoot the issue.
14. Go to **Control Panel -> Network and Internet -> Network and Sharing Center**. Check for the Network adapter status
15. Now you can see that Ethernet 2 adapter is showing up “No internet access”. Click on **Change adapter settings** in the left pane

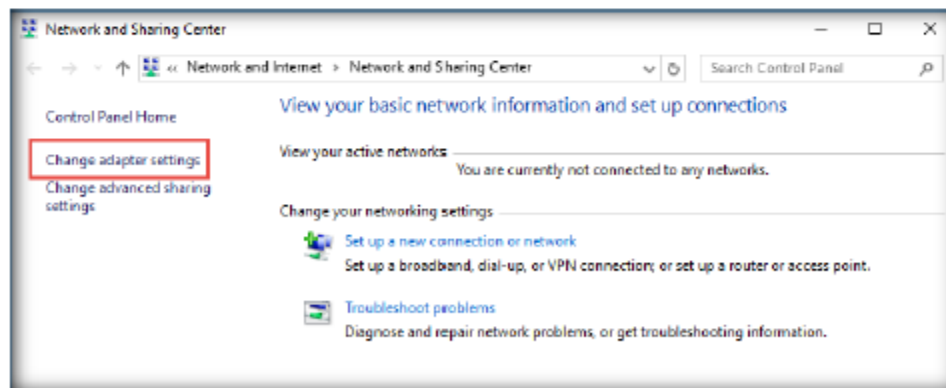


FIGURE 1.9: Ethernet 2 Network adapter error

16. Now you can see that the **Ethernet 2** adapter is disabled.

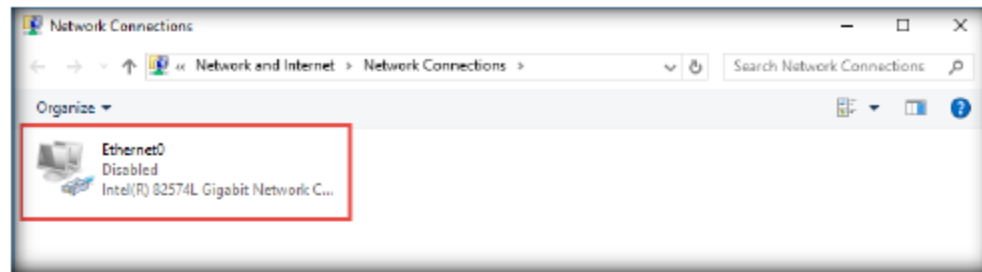


FIGURE 1.10: Disabled Ethernet adapter

17. Right click on it and select **Enable** from the context menu.

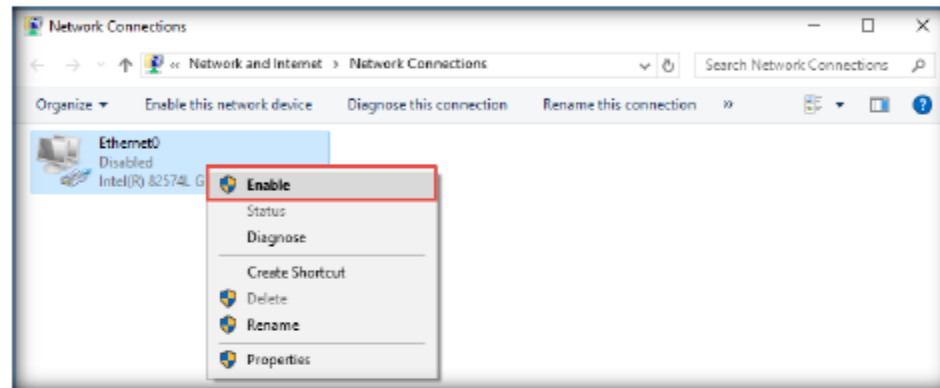


FIGURE 1.11: Enabling the disabled adapter

18. Now, switch back to **Windows Server 2012** machine and ping the target machine again

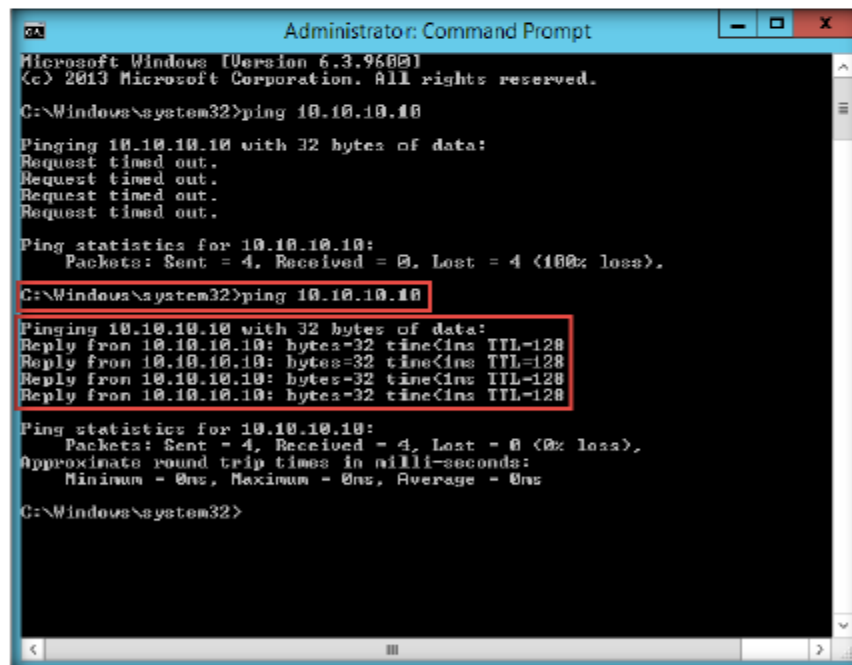


FIGURE 1.12: Ping request successfully executed

19. This time, you will be able to ping Window 10 machine successfully.

Note: Sometimes even after enabling the adapter, the ping request might not be successful due to firewall restrictions. In such cases, you need to temporarily disable the firewall on the target machine to check its reachability

TASK 3

Tracing the route of packets using tracert command

20. Now, we will see the usage of the **tracert** command to know the number of hops between a source and a destination node in a network. **tracert** is useful for troubleshooting large networks where several paths can lead to the same point or where many intermediate components (routers or bridges) are involved.

About tracert:

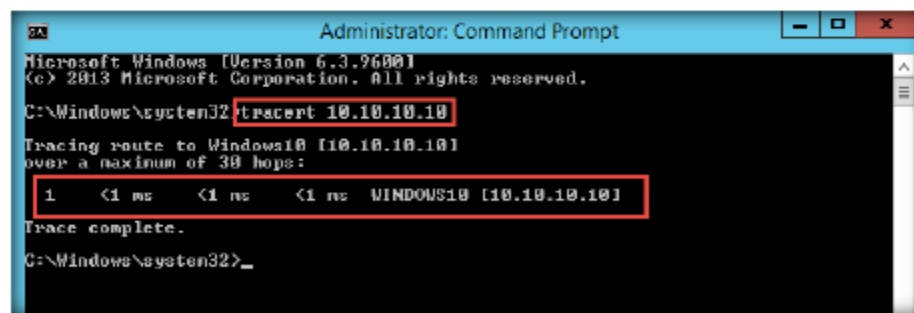
Source: <https://support.microsoft.com>

The **tracert** diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. In these packets, **tracert** uses varying IP Time-To-Live (TTL) values. Because each router along the path is required to decrement the packet's TTL by at least 1 before forwarding the packet, the TTL is effectively a hop counter. When the TTL on a packet reaches zero (0), the router sends an ICMP "Time Exceeded" message back to the source computer.

tracert sends the first echo packet with a TTL of 1 and increments the TTL by 1 on each subsequent transmission, until the destination responds or until the maximum TTL is reached. The ICMP "Time Exceeded" messages that intermediate routers send back show the route. Note however that some routers silently drop packets that have expired TTLs, and these packets are invisible to **tracert**.

tracert prints out an ordered list of the intermediate routers that return ICMP "Time Exceeded" messages. Using the **-d** option with the **tracert** command instructs **tracert** not to perform a DNS lookup on each IP address, so that **tracert** reports the IP address of the near-side interface of the routers.

21. On the Windows Server 2012 machine. Open a command prompt in the Admin mode by right-clicking on **Start** icon and then clicking **Command Prompt (Admin)** from the context menu. Type **tracert** followed by the target system IP address the command prompt and press Enter.



```

Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\system32>tracert 10.10.10.10
Tracing route to Windows10 [10.10.10.10]
over a maximum of 30 hops:
  0  <1 ms  <1 ms  <1 ms  WINDOWS10 [10.10.10.10]
Trace complete.
C:\Windows\system32>_

```

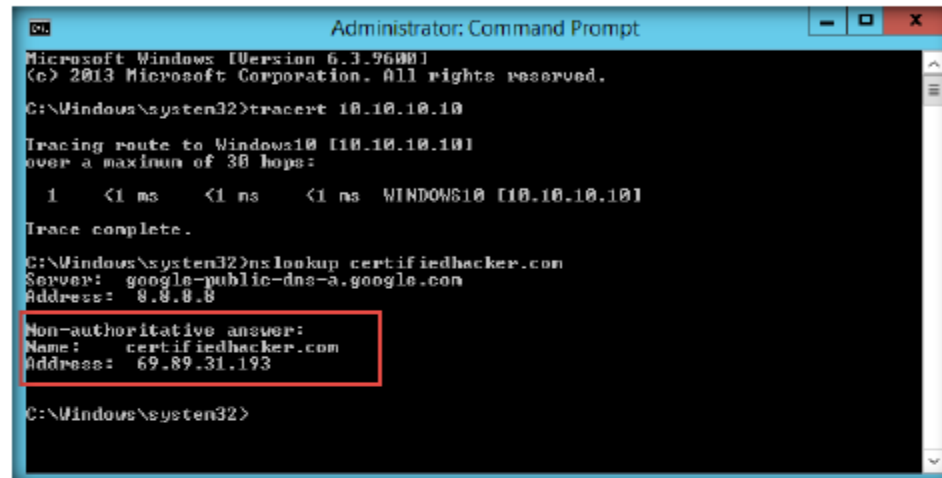
FIGURE 1.13: Demonstration of Tracert command

22. From the above screenshot, we can see that the destination was reached in the first hop itself.

TASK 4

Resolving Domain names with Using nslookup command

23. Now we will demonstrate the use of **nslookup** command. Nslookup stands for name server lookup. It is used to query a DNS server to obtain its domain name and associated IP address. It can be used with the domain name as an argument or independently
24. On the Windows Server 2012 machine, type **nslookup** followed by the domain name which you want to resolve (here, certifiedhacker.com) in the command prompt and press Enter.



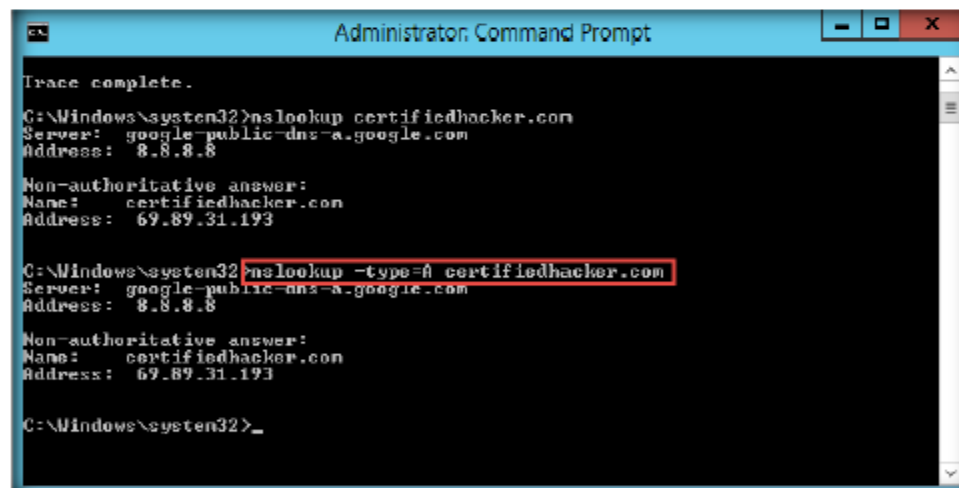
```

Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\system32>tracert 10.10.10.10
Tracing route to Windows10 [10.10.10.10]
over a maximum of 30 hops:
  0  <1 ms  <1 ns  <1 ns  WINDOWS10 [10.10.10.10]
Trace complete.
C:\Windows\system32>nslookup certifiedhacker.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8
Non-authoritative answer:
Name:   certifiedhacker.com
Address: 69.89.31.193
C:\Windows\system32>

```

FIGURE 1.14: Demonstration of nslookup command

25. From the above screenshot, you will see that the domain name (certifiedhacker.com) resolves to its corresponding IP address (69.89.31.193)
26. You can also use the nslookup command with type parameters to get non-authoritative name server (NS) information as shown in the screenshot below:




```

Administrator: Command Prompt
Trace complete.
C:\Windows\system32>nslookup certifiedhacker.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8
Non-authoritative answer:
Name:   certifiedhacker.com
Address: 69.89.31.193
C:\Windows\system32>nslookup -type=A certifiedhacker.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8
Non-authoritative answer:
Name:   certifiedhacker.com
Address: 69.89.31.193
C:\Windows\system32>_

```

FIGURE 1.15: nslookup command with type parameter

27. To get an authoritative NS information, you can use **-type=soa** parameter with nslookup.

 An Authoritative or Primary Nameserver is a nameserver (DNS Server) that holds the actual DNS records (A, CNAME, PTR, etc) for a particular domain/ address.

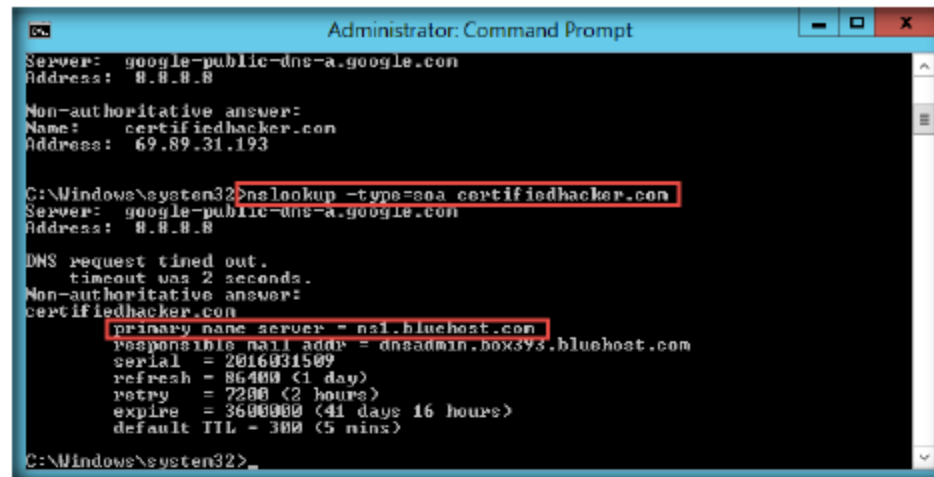


FIGURE 1.16: nslookup command with type parameter

TASK 5
Checking your network configuration and statistics netstat command

28. The address labelled as primary name server in the above screenshot is the DNS authority for the domain.
29. Now we will see the use of the **netstat** command. Netstat stands for Network statistics. Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, netstat displays active TCP connections.
30. Type the **netstat** command to check your network statistics as shown in following screenshot

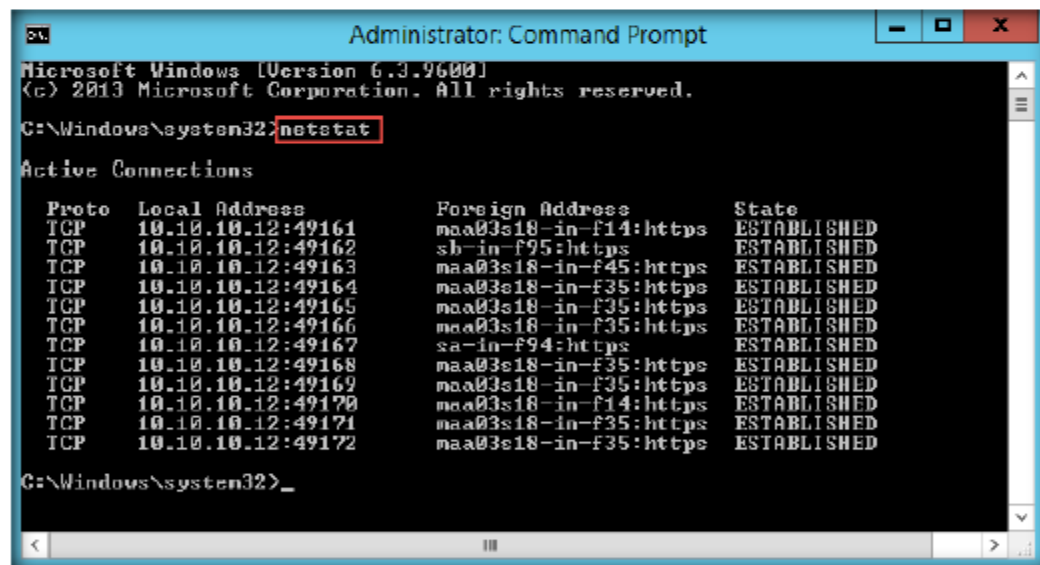


FIGURE 1.17: Demonstration of netstat command

31. You can use different **netstat** parameters to obtain important connection information

Parameters	Use
-a	Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
-e	Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s

-n	Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.
-o	Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.
-p <i>Protocol</i>	Shows connections for the protocol specified by <i>Protocol</i> . In this case, the <i>Protocol</i> can be tcp, udp, tcpv6, or udpv6. If this parameter is used with -s to display statistics by protocol, <i>Protocol</i> can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.
-s	Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The -p parameter can be used to specify a set of protocols.
-r	Displays the contents of the IP routing table. This is equivalent to the route print command.
<i>Interval</i>	Redisplays the selected information every <i>Interval</i> seconds. Press CTRL+C to stop the redisplay. If this parameter is omitted, netstat prints the selected information only once.
/?	Displays help at the command prompt.

TASK 6
**Displaying
 Address
 Resolution
 Protocol (ARP)
 cache using arp
 command**

32. The **arp -a** command displays ARP cache. The cache has a mapping of IP addresses with their respective MAC addresses. It has many options and if you use ARP without any option it displays the available options
33. Type **arp -a** command and press Enter to display the ARP cache entries.

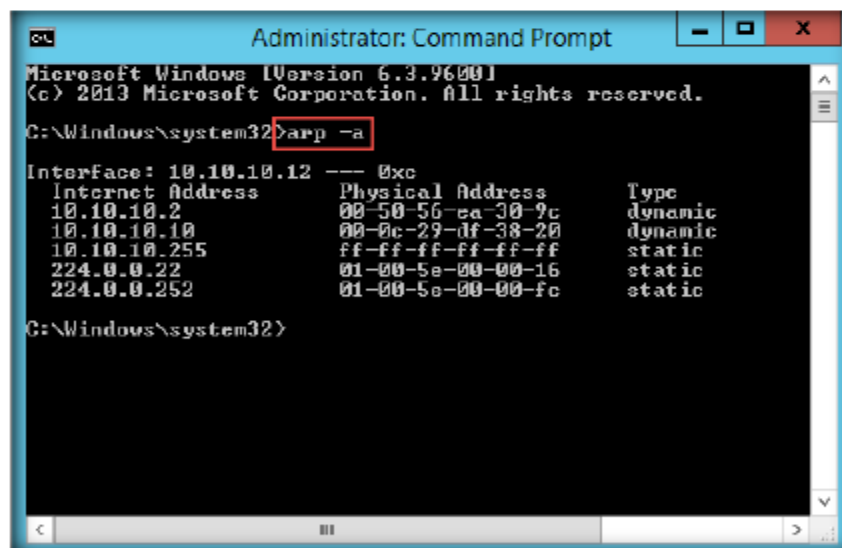


FIGURE 1.18: Using arp -a command

Note: If you want to view the MAC address of only a particular IP address, type the IP address after **arp -a** command and press Enter.

Similarly, you can use the following useful commands for network administration and troubleshooting

Commands	Objectives
Gpresult	Starts the Operating System Group Policy Result tool
ipconfig /flushdns	Flushes the DNS resolver cache. Helpful when troubleshooting DNS name resolution problems
nbtstat -a <MachineName>	Obtains info from WINS or LMHOST (discovers who is logged on)
nbtstst -A <IP>	Gets info from WINS or LMHOST (discovers who is logged on)
nbtstat -R	Purges and reloads the remote cache name table
nbtstat -n	Lists local NetBIOS names.
nbtstat -r	Useful for detecting errors when browsing WINS or NetBIOS
netstat -ab	The b switch links each used port with its application
netstat -an	Shows open ports
netstat -an 1 find "15868"	Locates only lines with the number 15868 and redisplay every one second
netstat -an find "LISTENING"	Shows open ports with LISTENING status
net use	Retrieves a list of network connections
net user	Shows user account for the computer
net user /domain	Displays user accounts for the domain
net user /domain <UserName>	Shows account details for specific user
net group /domain	Shows group accounts for the domain
net view	Displays domains in the network
net view /domain	Specifies computers available in a specific domain
net view /domain: <DomainName> more	Shows user accounts from specific domain
net view /cache	Shows workstation names
ping -a <IP>	Resolves IP to Hostname
ping -t <IP>	Pings host until stopped
Pathping	Displays the route and ping information when performing queries such as -n and -h options representing hostnames and maximum hops respectively.
set U	Shows which user is logged on
set L	Shows the logon server
telnet <IP> <port>	Confirms whether the port is open

Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.





Internet Connection Required	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



Analyzing and Examining Various Network Packet Headers

We shall analyze various packets like TCP, HTTP, ICMP, DNS with Wireshark

ICON KEY

-  Valuable information
-  Test your knowledge
-  Web exercise
-  Workbook review

Lab Scenario

Each packet in a network contains control information and user data, which is also known as the payload. The control information contains data for delivering the payload, which includes source and destination IP and MAC addresses, sequencing information, etc. The header part of the packet stores this control information. So, being a network admin, you need to know how to examine the packet headers while examining the data packets.


Lab Objectives


The objective of this lab is to help students learn how to inspect TCP/IP packet header fields of different network packets.

Lab Environment

In this lab, you need:

- Wireshark, located at **Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis\Packet Sniffing Tools\Wireshark**
- You can also download the latest version of Wireshark from the link <https://www.wireshark.org/download.html>
- If you decide to download the latest version, the screenshots shown in the lab may differ
- A virtual machine running Windows Server 2012
- A Web browser with Internet connection
- **Administrative** privileges to run tools

 **Tools demonstrated in this lab are available in Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis**

 You can download Wireshark from <http://www.wireshark.org>.


Lab Duration

Time: 30 Minutes

Overview of Wireshark Packet Capture

Packet capture is the intercepting of data packets traversing over a network using packet capture tools like Wireshark. These captured packets are analyzed in order to determine whether proper network security policies are being followed.

Lab Tasks

 **TASK 1**

**Installing and
Launching
Wireshark**

1. Log on to **Windows Server 2012** virtual machine in Hyper-V Manager
2. Before beginning this lab, ensure that WinPcap is installed.
3. Navigate to **Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis\Packet Sniffing Tools\Wireshark** and double-click **Wireshark-win64-2.0.2.exe**
4. If **Open File - Security Warning** pop-up appears, click **Run**.
5. Follow the wizard-driven installation steps to install Wireshark

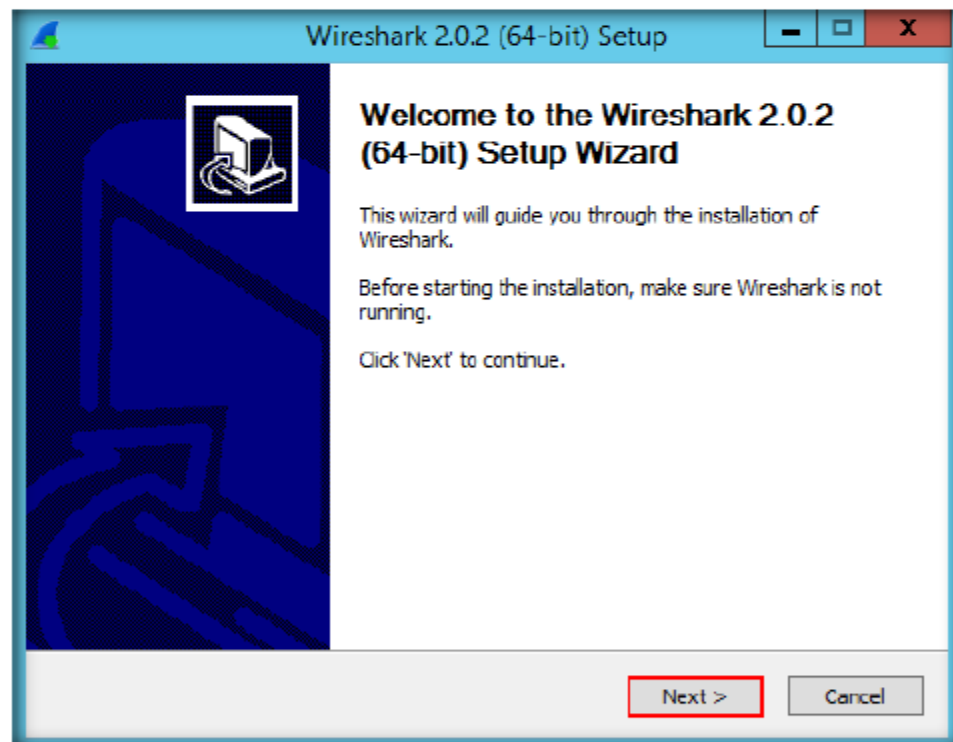


FIGURE 2.1: Wireshark installation wizard

6. During the installation, a window appears asking you to install WinPcap. If you have already installed the application, click **Cancel**; else, click **Next** if you have not installed WinPcap.

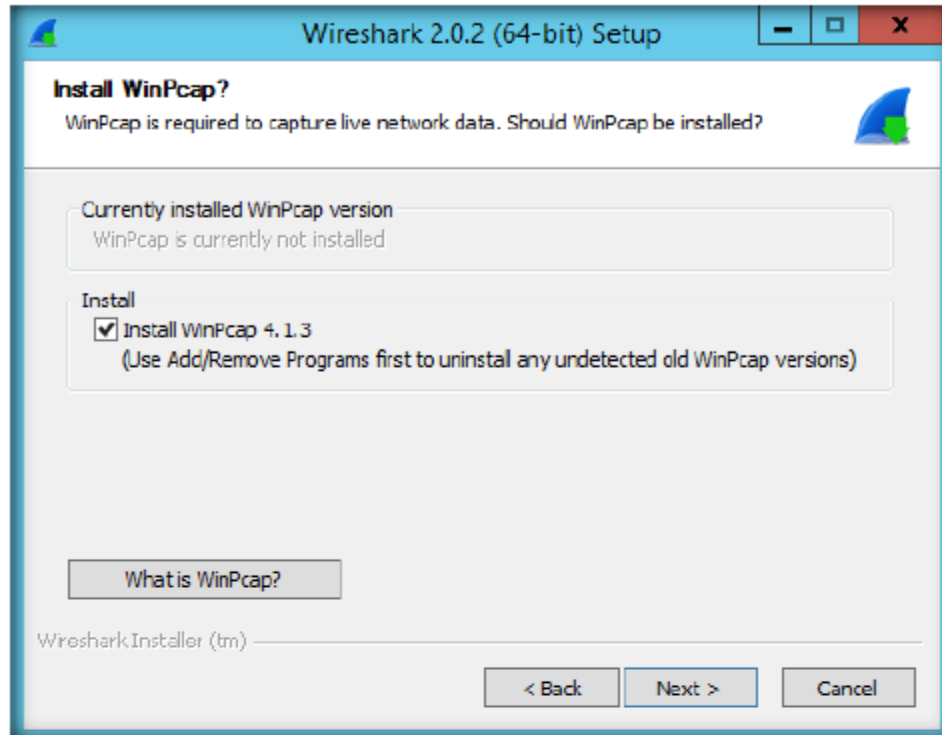


FIGURE 2.2: WinPcap installation wizard

7. On completing the installation, launch **Wireshark** from the **Apps** screen

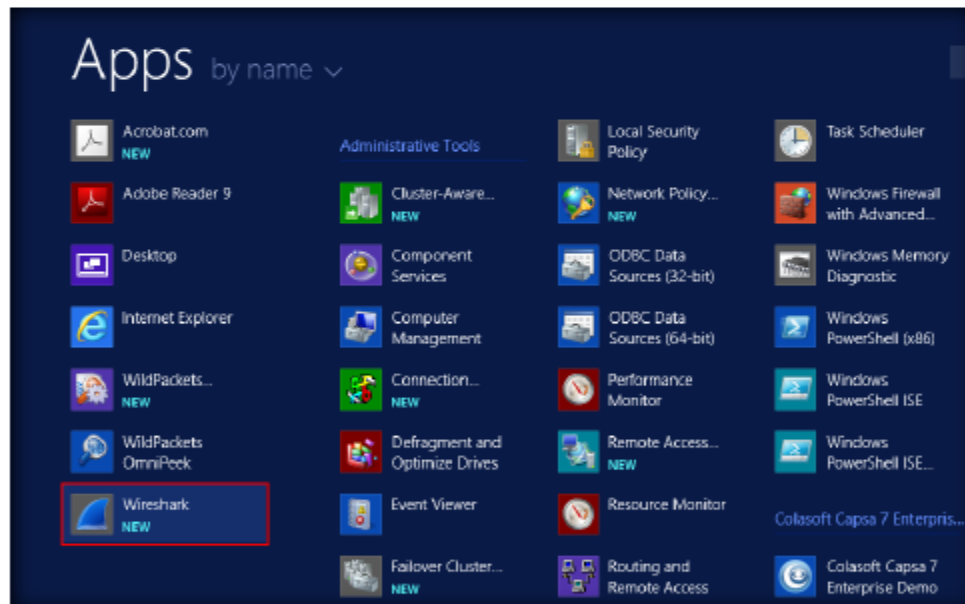


FIGURE 2.3: Windows Server 2012 Apps Screen

- The main window of Wireshark appears as shown in following screenshot:

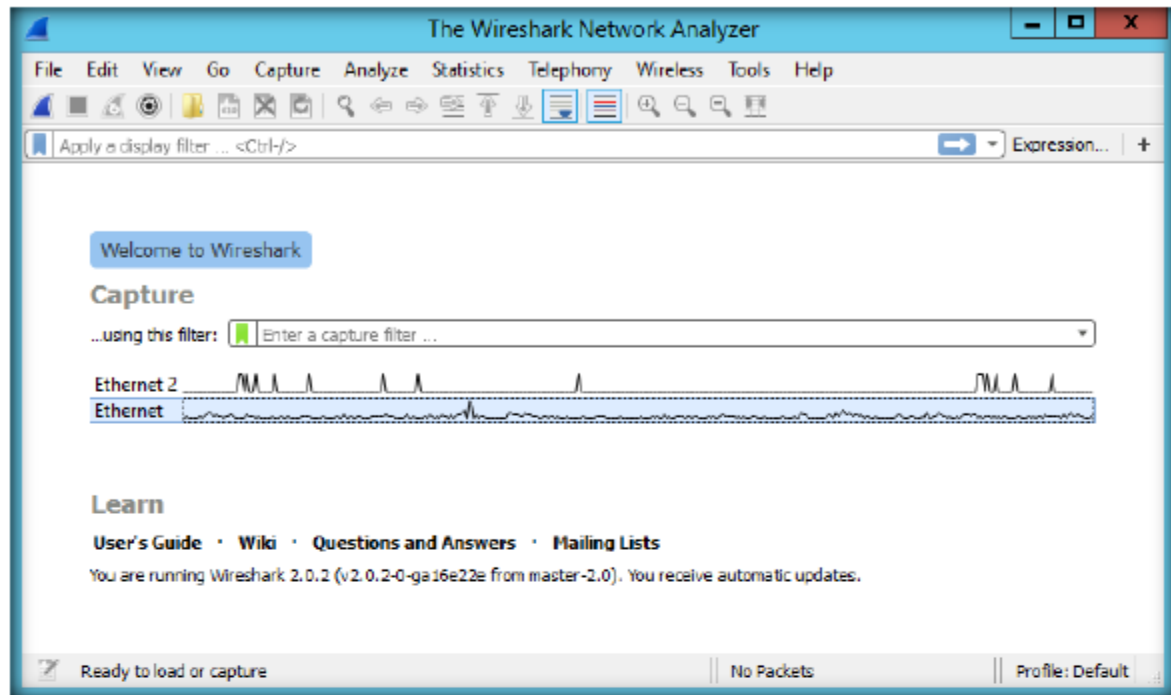


FIGURE 2.4: Wireshark Window

- Go to the **File** menu and click **Open**, to open a packet capture file

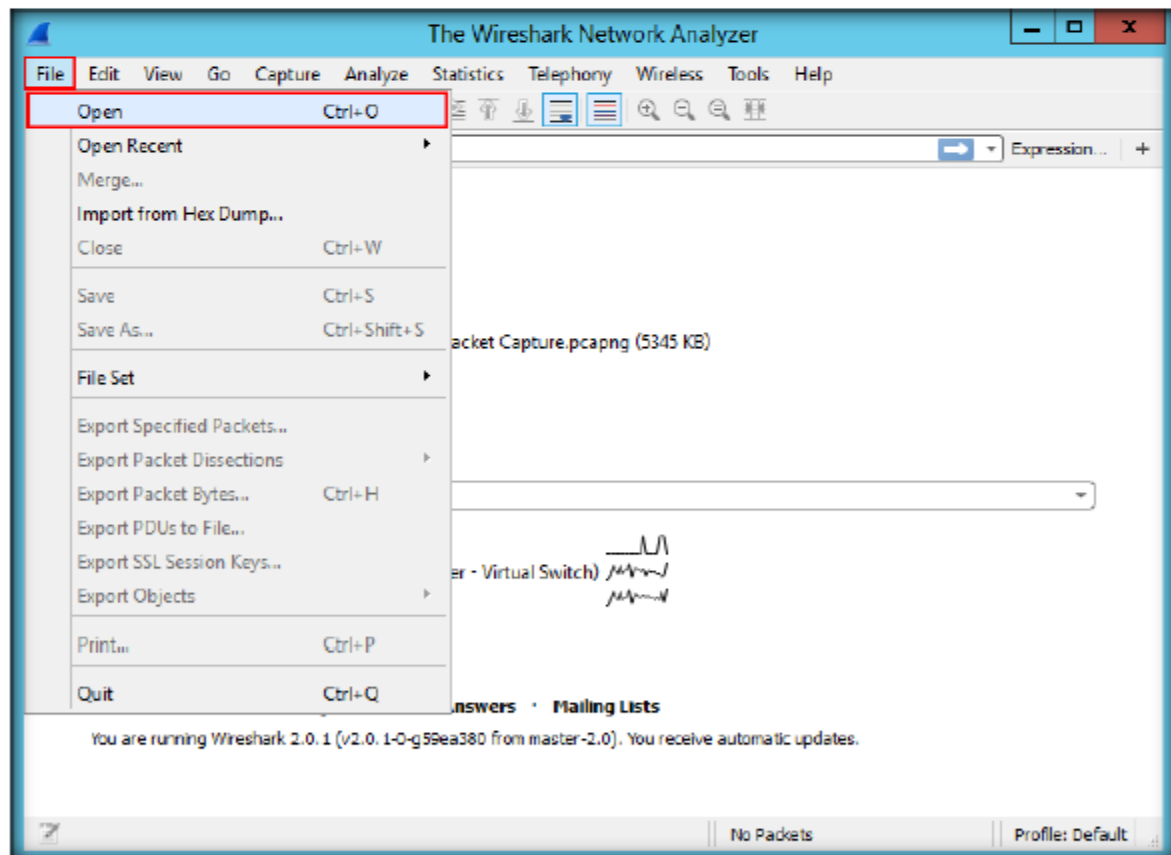


FIGURE 2.5: Opening a captured file

- Wireshark: The Open Capture File window appears, navigate to **Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis\Packet Sniffing Tools\Wireshark**, select **Packet Capture.pcapng** and click **Open**

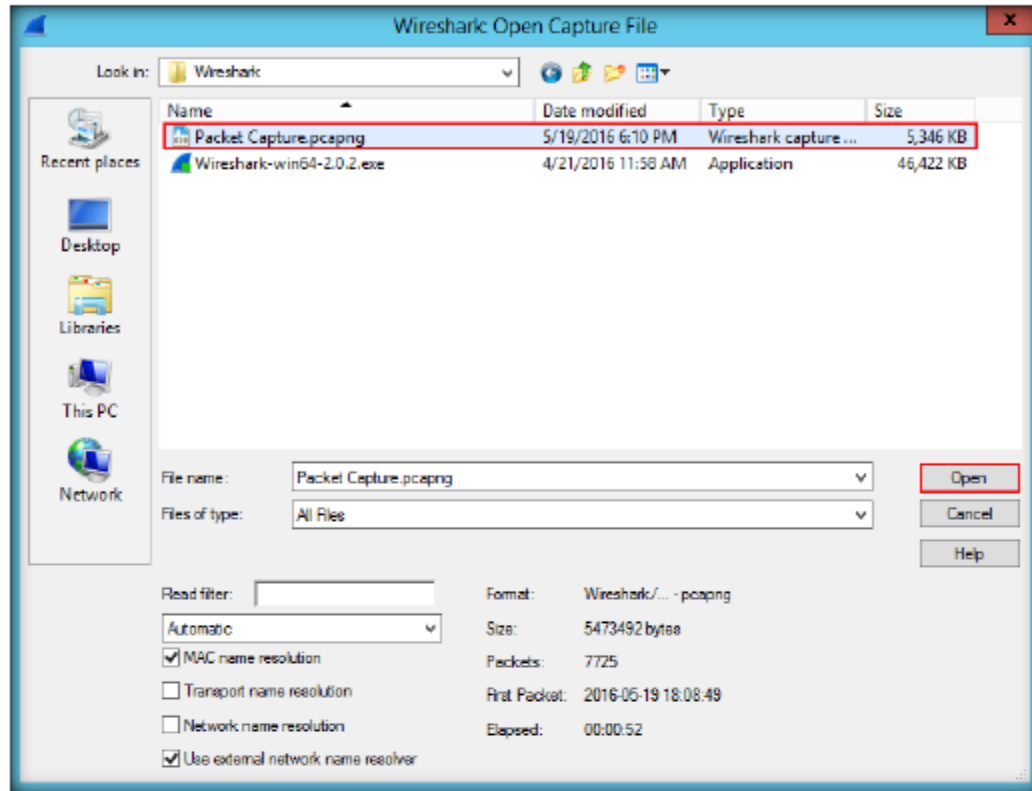


FIGURE 2.6: Selecting the captured file

TASK 2

Opening a Packet Capture File

- Wireshark displays the captured packets associated with the file as shown in the following screenshot

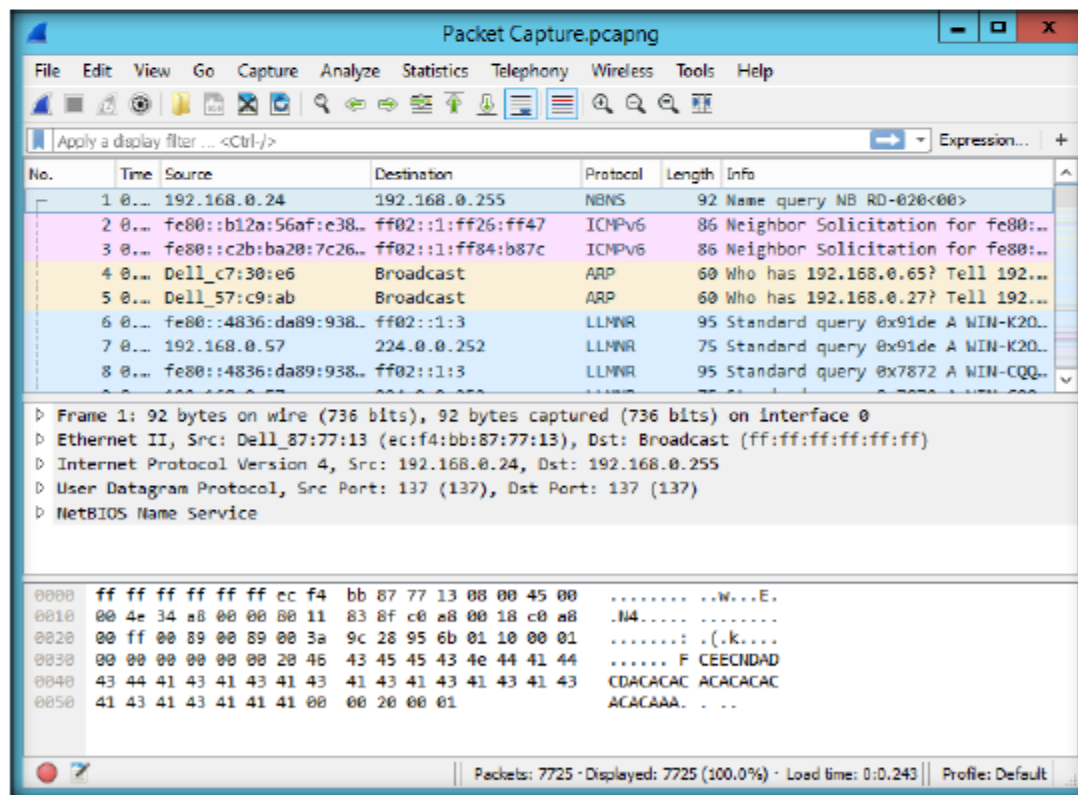


FIGURE 2.7: Wireshark GUI with Stop Button Highlighted

TASK 3

Inspecting ARP
Packet Header

12. Typical format of an ARP packet header is as shown in following figure

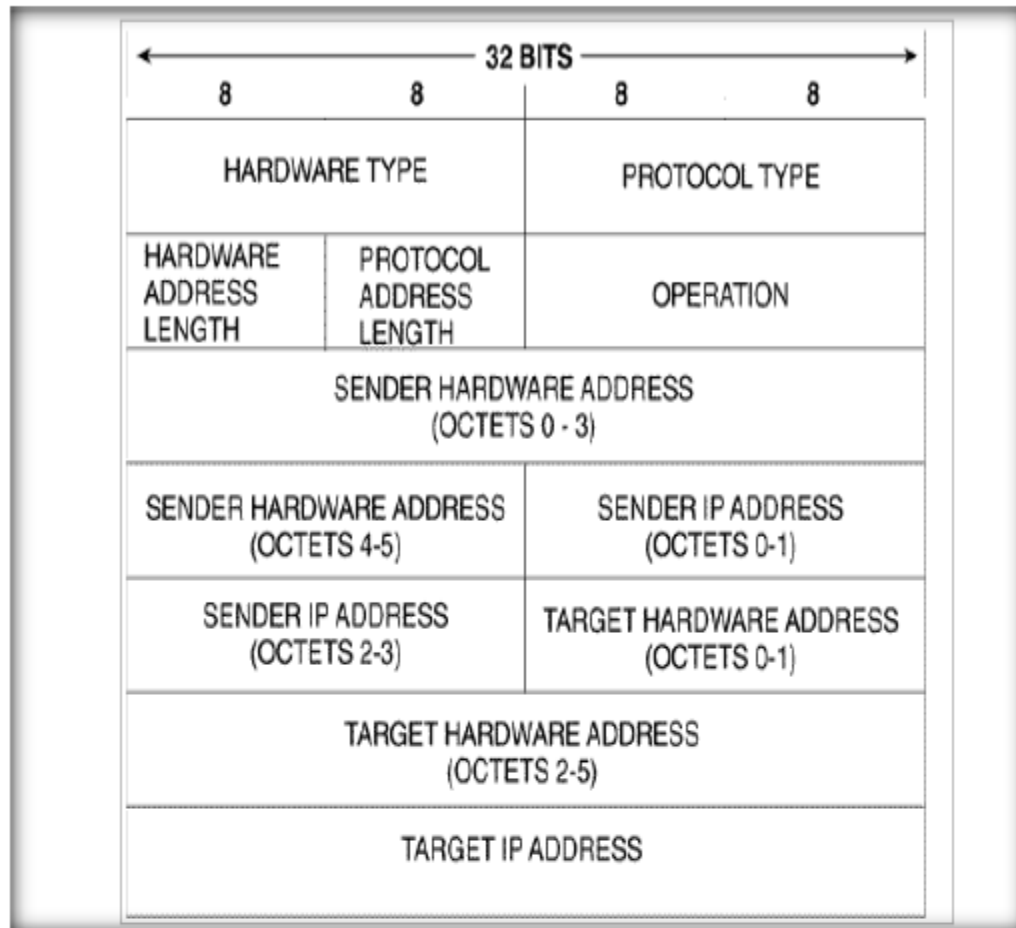


FIGURE 2.8: Typical Structure of an ARP Packet

The various fields are explained below

- I. **Hardware Type (HTYPE):** Describes the Network adapter used, which is Ethernet.
- II. **Protocol Type(PTYPE):** Describes the inter network protocol, for which the ARP packet was sent
- III. **Hardware size (HLEN):** Describes the hardware address length
- IV. **Protocol size (PSIZE):** Describes the protocol address length
- V. **Opcode:** The operational code of an ARP packet, which describes if it is a request or a reply packet
- VI. **Sender MAC address:** Source system's MAC address
- VII. **Sender IP address:** Source system's IP address.
- VIII. **Target MAC address:** Destination system's MAC address
- IX. **Target IP address:** Destination system's IP address.

13. Now, click on an **ARP packet** to analyze its various header fields

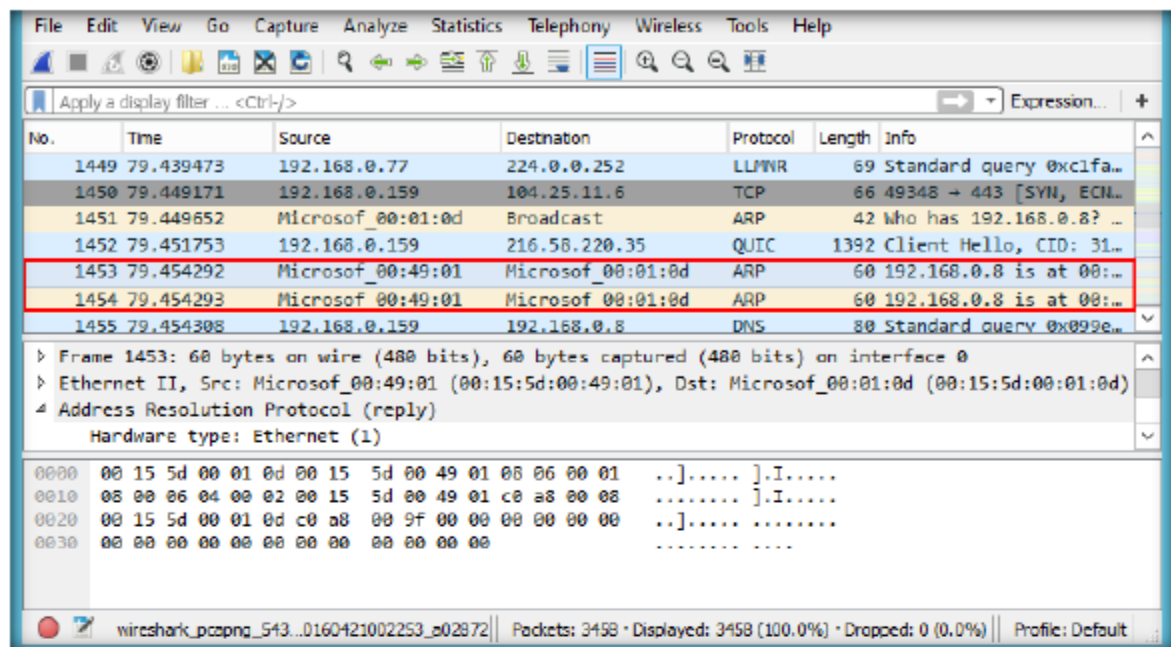


FIGURE 2.9: Wireshark Captured Packets

14. Expand the **Address Resolution Protocol** node (here, **ARP Reply** node) under the **Packet details** Pane

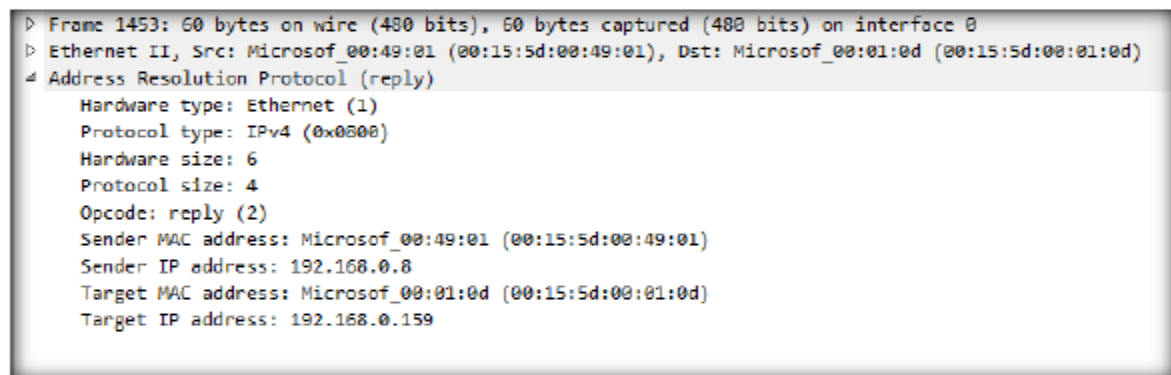


FIGURE 2.10 Captured ARP Packet

15. Compare and analyze the various fields in an ARP packet with the ARP packet header format

TASK 4

Inspecting TCP
Packet Header

16. Typical TCP packet header format is as shown in following figure

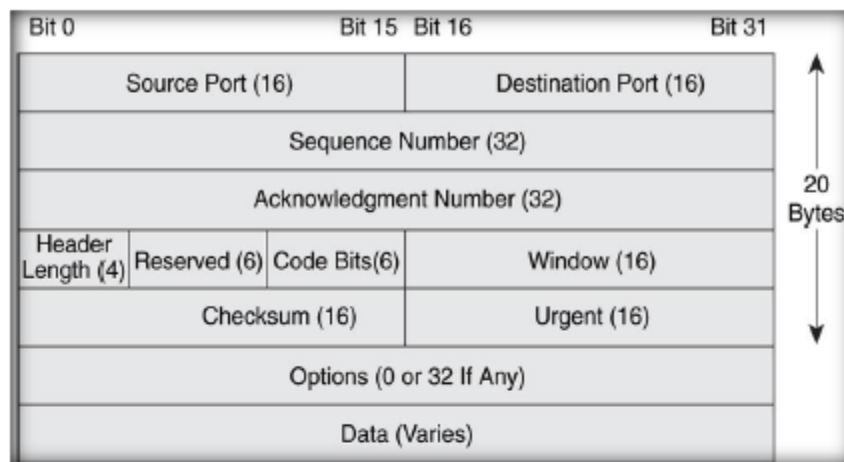


FIGURE 2.11: Typical Structure of a TCP Packet

The various fields are explained below

- I. **Source port:** Port number of the source machine.
- II. **Destination port:** Port number of the destination
- III. **Sequence number:** The sequence number of the segment
- IV. **Acknowledgement number:** The acknowledgement number of the segment
- V. **Header length:** Specifies segment's total header length
- VI. **Reserved:** Reserved bits for future use
- VII. **Code bits (flags):** Specifies which flags are set based on nature of segment.
- VIII. **Window size:** Maximum length of segment which the sender can receive as a reply to this segment and starts from acknowledgement number
- IX. **Checksum:** Specifies the error detection data
- X. **Urgent:** If set, implies that urgent reply needed from recipient.
- XI. **Options:** Can be from 0-32 bits in multiples of eight, used optionally in checksum calculation.
- XII. **Segment data:** total data length of the segment

17. Now, **click on a TCP packet** to analyze its various header fields.

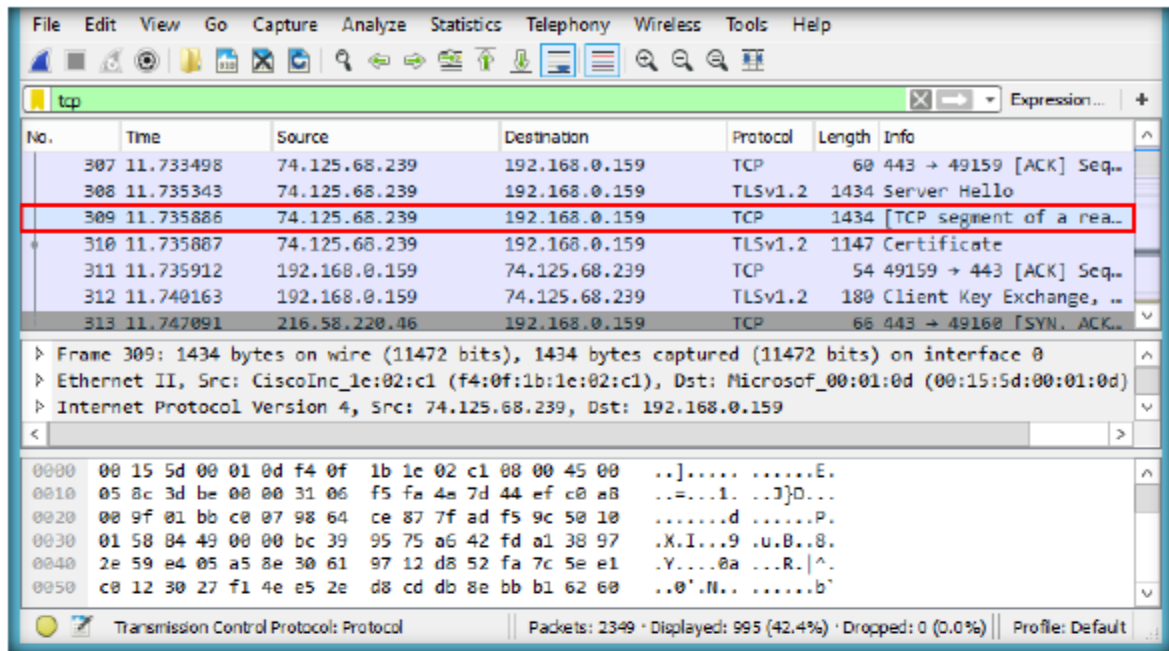


FIGURE 2.12: TCP Packets in Wireshark

18. Expand the **Transmission Control Protocol** node in the **Packet Details Pane**

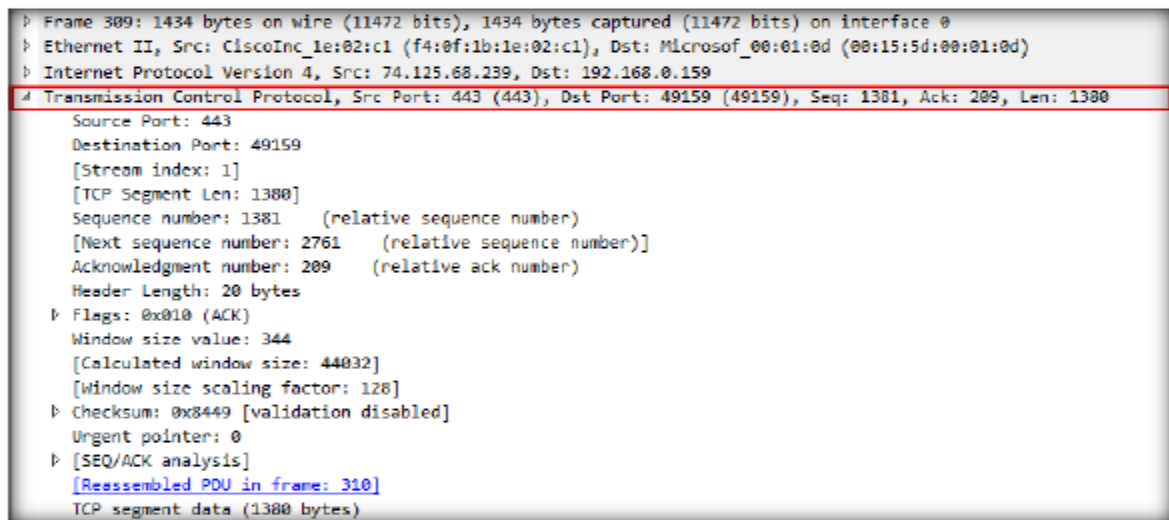


FIGURE 2.13: TCP Packet

19. Compare and analyze the various fields in a TCP packet with the TCP packet header format

TASK 5

Inspecting HTTP
Packet Header

20. Typical structure of a HTTP request header is shown in the following figure:

Key	Value
Request	GET /Protocols/rfc2616/rfc2616-sec14.html HTTP/1.1
Accept	text/html, application/xhtml+xml, */*
Referer	http://www.google.com/url?sa=t&source=web&cd=3&ved=0CC4QFjAC8
Accept-Language	en-US
User-Agent	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5
Accept-Encoding	gzip, deflate
Host	www.w3.org
If-Modified-Since	Wed, 01 Sep 2004 13:24:52 GMT
If-None-Match	"1edec-3e3073913b100"
Connection	Keep-Alive

FIGURE 2.14: Typical Structure of a HTTP Request Header

The various fields are explained below

- I. **HTTP type:** There are two types of HTTP messages. Request and response. All HTTP packets belong to one of the above two formats.
- II. **Request type:** Specifies the type of request. GET, POST, HEAD and so on
- III. **Accept:** Uses wild cards to specify the acceptable media
- IV. **Referer:** Points to the site which requested a resource on behalf of the client
- V. **Accept language:** Language in which the requested response is preferred
- VI. **User agent:** Client software which requested the resource on the client's behalf
- VII. **Accept encoding:** Specifies the content coding acceptable in the response packet
- VIII. **Host:** The URL at which the actual resource requested or part of resource is available.
- IX. **If-modified-since:** Used to impose a condition. If the requested response is not modified after the time period specified then the resource is not returned. A *304- not modified* message is returned
- X. **If-none-match:** Used to impose a condition. Client specifies a set of resources it already has, in this field. If requested information is same as the information in this field server does not need to send the same information again. It sends a *304 message*.
- XI. **Connection:** Defines the type of connection to be established.

21. Now, click on a HTTP packet to analyze various fields

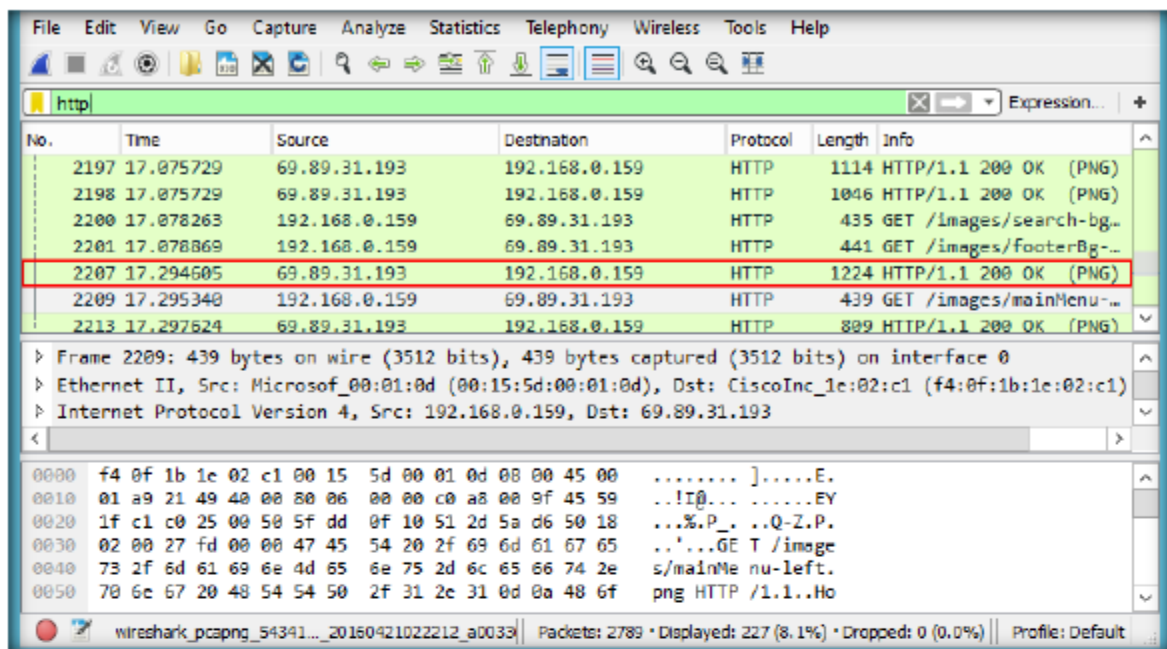


FIGURE 2.15: HTTP Packets in Wireshark

22. Expand the **Hypertext Transfer Protocol** node in the Packet Details Pane

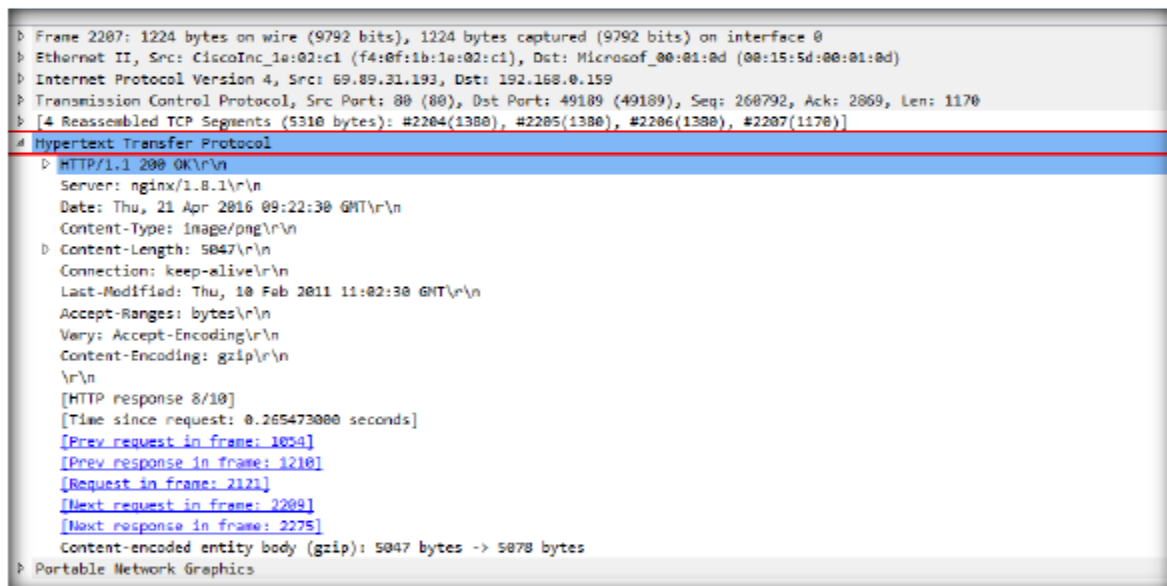


FIGURE 2.16: HTTP Packet

23. Compare and analyze the various fields in the HTTP packet with the HTTP request header format

TASK 6

Inspecting ICMP Packet Header

24. Typical structure of an ICMP packet is as shown in following figure

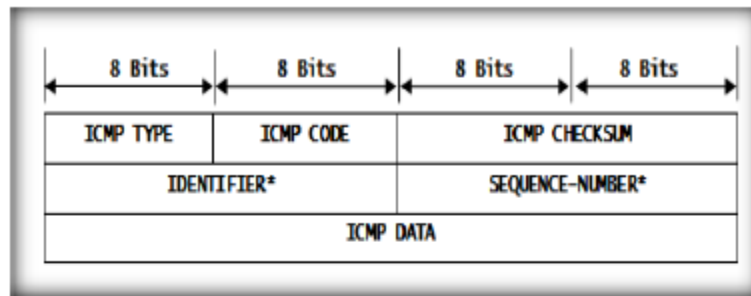


FIGURE 2.17: Typical structure of an ICMP packet

The various fields are explained below

- I. **Type:** It defines the ICMP message type. It has two values. 0 or 8. 0 implies that it is an echo reply ICMP packet and 8 implies that it is an echo request packet.
- II. **Code:** Code is zero for both ICMP request and reply packets. Its value varies in other types of ICMP packets.
- III. **Checksum:** Checksum data is used for error detection.
- IV. **Identifier:** It is set to the process ID of the sender
- V. **Sequence Number:** It begins with zero and increments by one, with every ICMP echo request packet being sent.
- VI. **Data:** Contains ICMP data

25. Now click on the ICMP packet to analyze its various fields

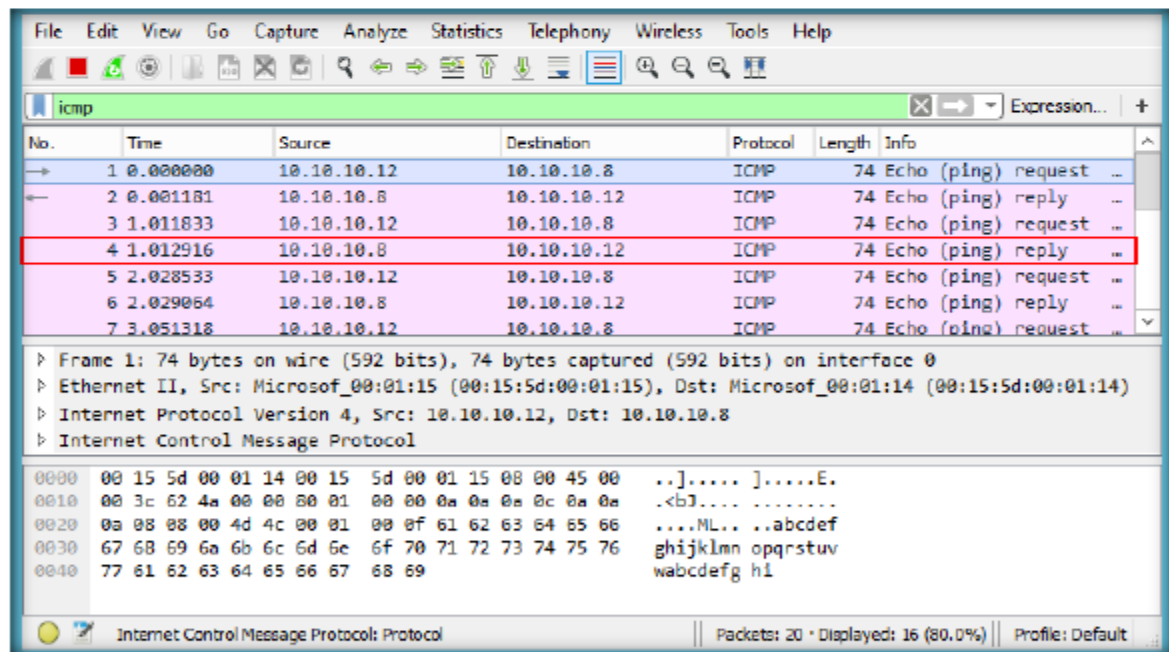


FIGURE 2.18: ICMP Packets in Wireshark

26. Expand the **Internet Control Message Protocol** node in the **Packet Details Pane**

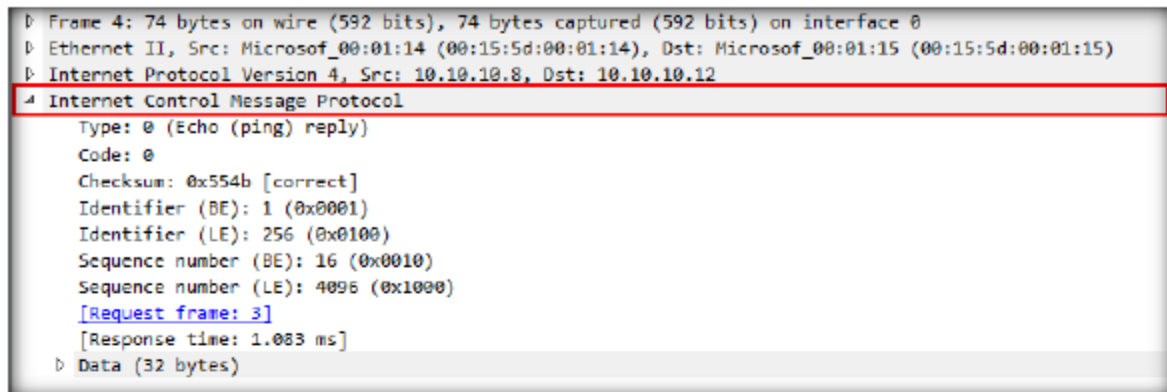


FIGURE 2.19: Captured ICMP packet

27. Compare and analyze the various fields in an ICMP packet with the ICMP header format

TASK 7
Inspecting DNS Packet Header

28. Typical structure of a DNS packet header is as shown in following figure

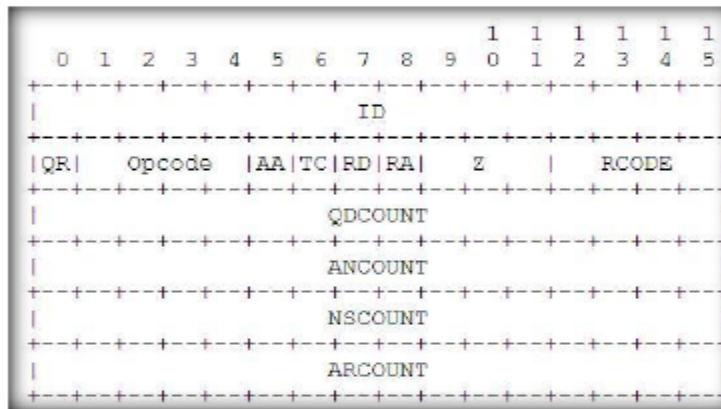


FIGURE 2.20: Typical structure of a DNS Packet Header

The various fields are explained as follows:

- I. **Identifier:** A 2-byte ID created by the system that created the DNS query.
- II. **Query/response flag:** Defines the type of DNS packet, if it is a Query type or response type flag.
- III. **Operational code:** Specifies the type of query present in the message. It is created by the sender and is the same in the response message as well
- IV. **Authoritative answer flag (AA):** Applies to response messages. A non-authoritative response is indicated by zero and a 1 implies that the server is responsive
- V. **Truncation flag (TC):** If set to 1 implies the message was truncated as it was long, and a zero indicates no truncation.
- VI. **Recursion Desired (RD):** Applies to request type packets. If set to 1, implies that server needs to recursively reply to the client.
- VII. **Recursion available (RA):** Applies to response queries. If set to 1, implies that server supports recursive reply.
- VIII. **Zero(Z):** Three bits are reserved and are always set to zero

- IX. **Response code (Rcode):** Set to zero in a request query. Server does not alter the query if response was successful. (zero). Any other value returned by server implies an error in response
- X. **Question count (QD count):** Specifies the number of questions in question segment
- XI. **Answer record count (AN count):** Specifies number of resource records in answer section.
- XII. **Authority record count(NS count):** Specifies number of records in authority section
- XIII. **Additional record count (AR count):** Specifies number of resource records in the additional section

29. Now, click on any DNS packet capture to analyze it various fields

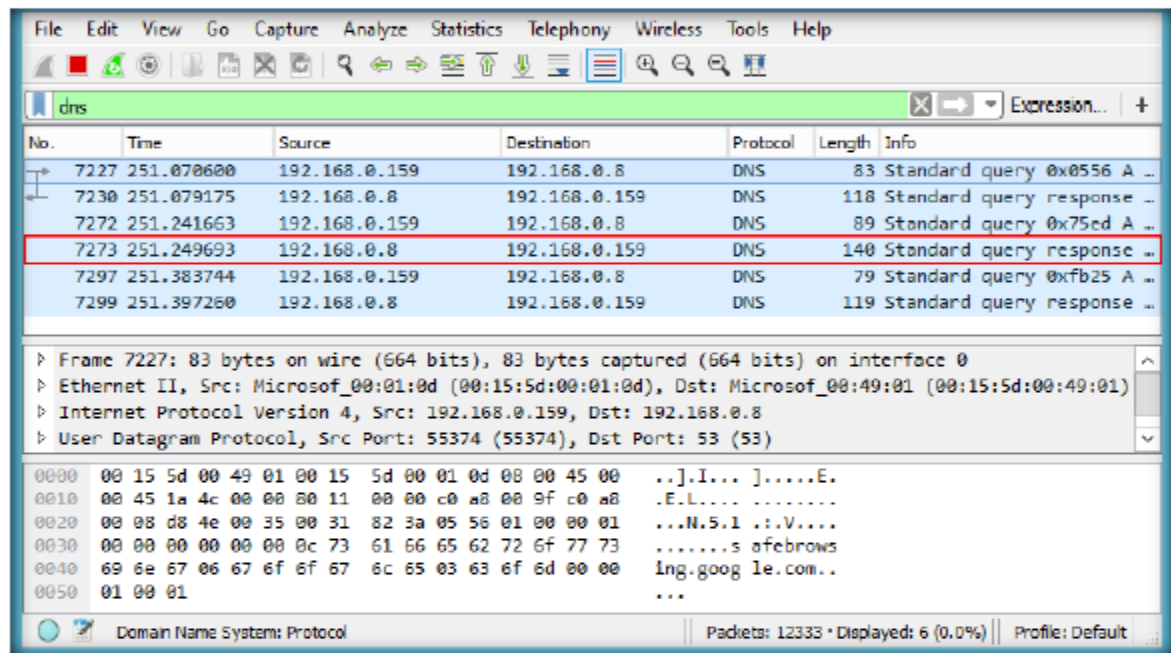


FIGURE 2.21: DNS Packets in Wireshark

30. Expand the **Domain Name System(Query)** node in the Packet details Pane

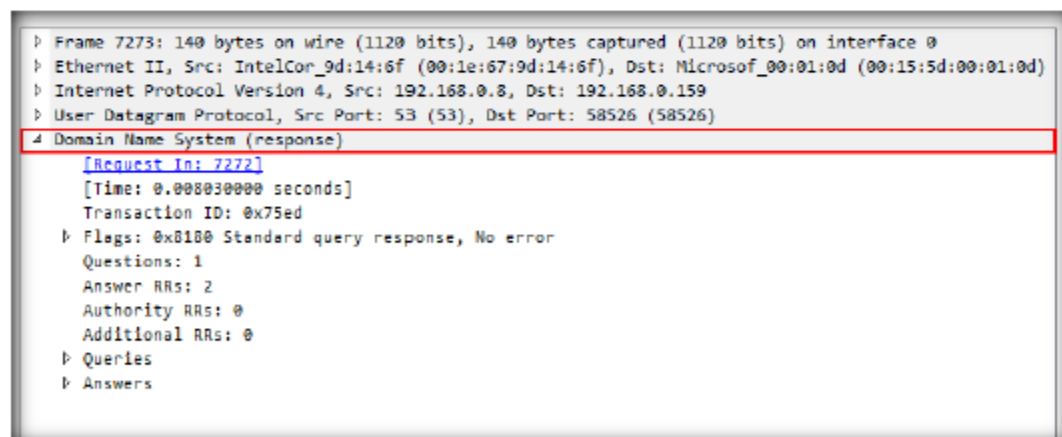


FIGURE 2.22: Captured DNS Packet

31. Compare and analyze the various fields in the DNS packet with the DNS header format

TASK 8

Inspecting UDP Packet Header

32. Typical structure of a UDP packet is as shown in following figure

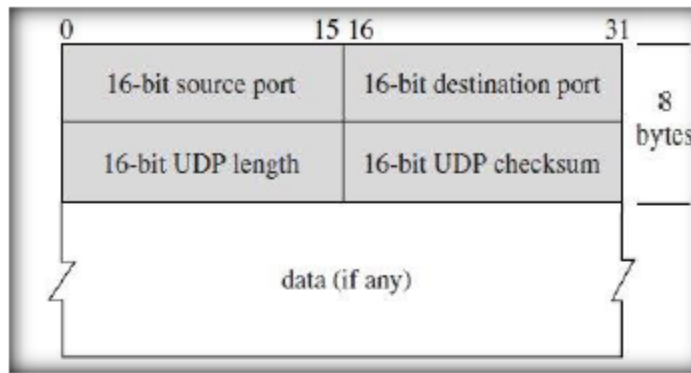


FIGURE 2.23: Typical Structure of a UDP Packet

The various fields are described as follows:

- I. **Source port:** Contains the port number of the process that originated the UDP datagram
- II. **Destination port:** Port number of the process towards which the datagram is destined.
- III. **UDP length:** Length of the datagram, which includes header size and data size
- IV. **UDP Checksum:** An optional field used in error detection
- V. **Data:** An optional field, contains higher layer message in encapsulated format

33. Since UDP works in conjunction with higher level protocols to help manage data transmission services. Common application-layer protocols that are built atop UDP are Domain Name System (DNS), Trivial File Transfer Protocol (TFTP), Real Time Streaming Protocol (RTSP), Simple Network Protocol (SNP), etc.

34. Now, click on a DNS packet capture to analyze various fields of an UDP header

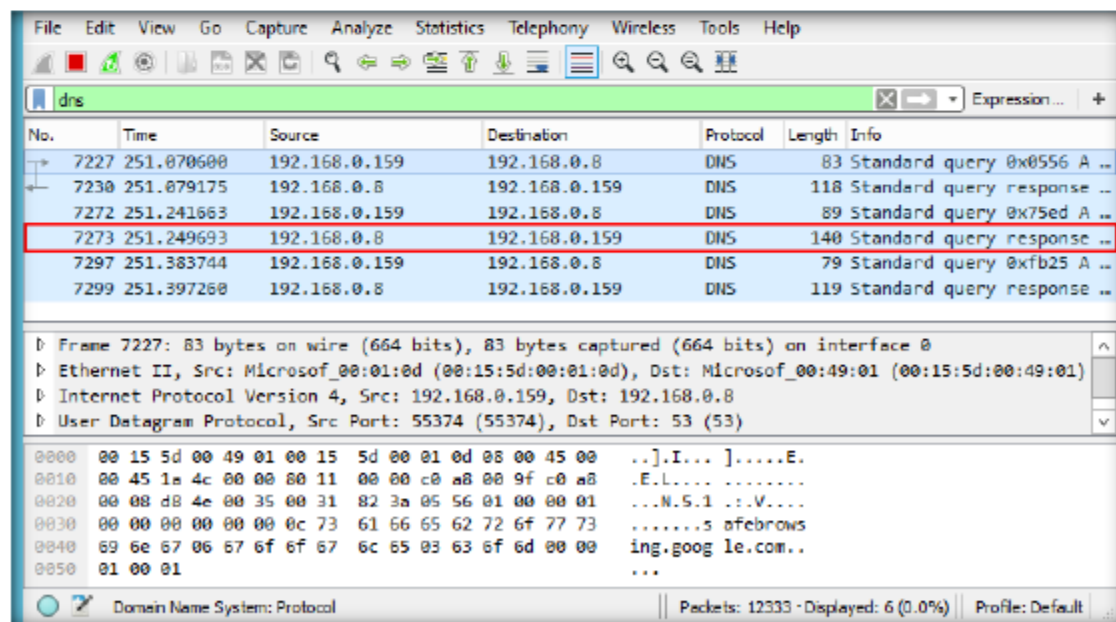


FIGURE 2.24: DNS Packets in Wireshark

35. Expand the **User Datagram Protocol** node in the **Packet Details Pane**

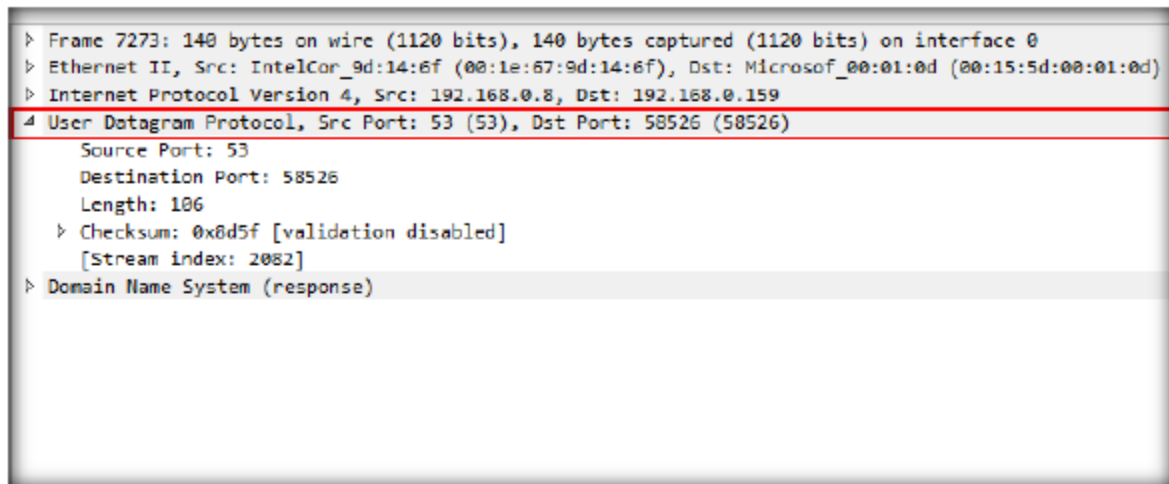


FIGURE 2.25: Captured UDP Packet

36. Compare and analyze the various fields in an UDP packet with the UDP header format

Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs