HUMBER

CPAN 226

Lab 03: Using Wireshark to Examine the DNS and FTP protocols.

Introduction

This lab has two sections: examining DNS and examining FTP. DNS is a distributed network of servers that translates user-friendly domain names like www.google.com to an IP address. When you type a website URL into your browser, your PC performs a DNS query using the **User Datagram Protocol (UDP)** as the transport layer protocol. UDP is connectionless and does not require a session setup like TCP.

The File Transfer Protocol (FTP) is used to transfer files between network devices. FTP is frequently used for files that are too large for email attachments. When using FTP, one computer acts as the server and the other as the client, typically requiring a username and password.

Objectives:

- Communicate with a DNS server using UDP.
- Use Wireshark to examine DNS query and response exchanges.
- Use anonymous FTP from the Windows command line and a browser.

Required Resources:

- PC with command prompt and Internet access.
- Wireshark installed.

Section A: DNS

Part 1: Record a PC's IP Configuration Information

Use the ipconfig /all command to find and record the following information.

Table 1: Local PC Configuration

Item	Details	Source
IP Address		
MAC Address		
Default Gateway IP Address		
DNS Server IP Address		

Q1: Record this information in Table 1 above. This information will be used in the following parts of this lab.

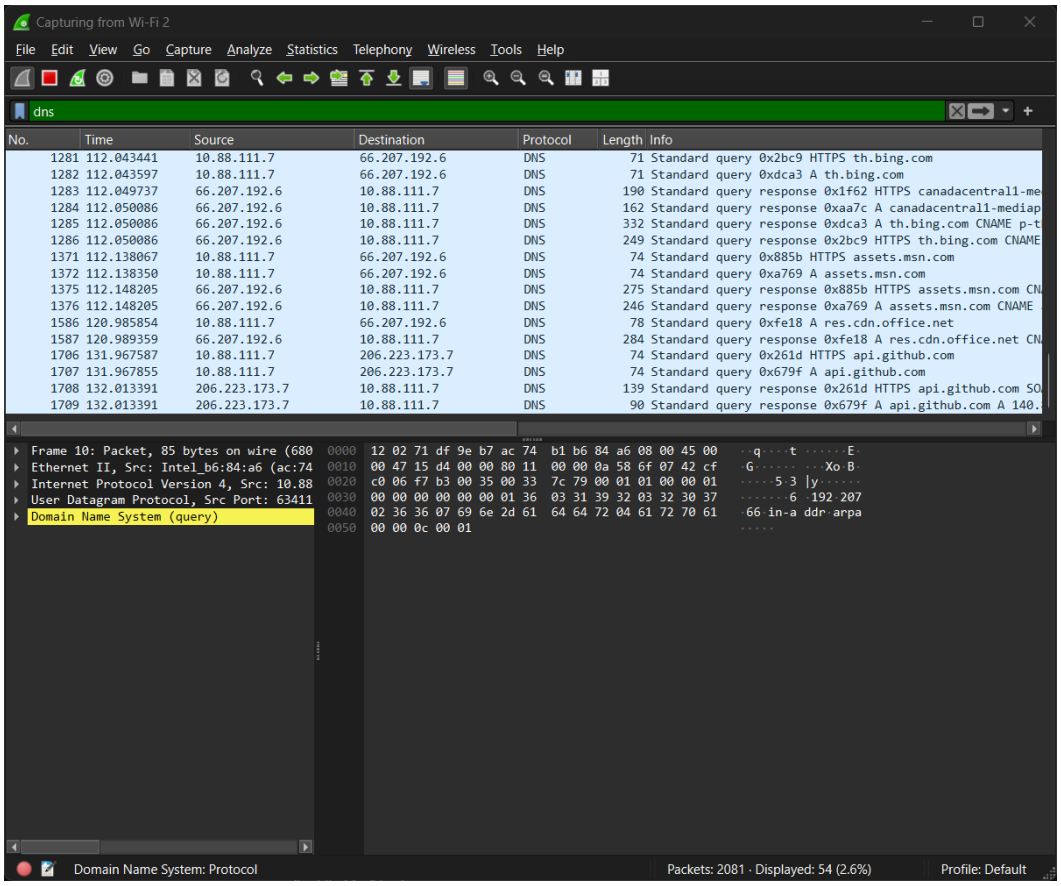
Part 2: Use Wireshark to Capture DNS Queries and Responses

1. Start Wireshark and select the interface associated with your recorded IP/MAC addresses.
2. Click **Start** to capture packets.
3. Open a browser, type www.google.com, and press Enter.
4. Click **Stop** once the page loads.

Part 3: Analyze Captured DNS or UDP Packets

1. Filter results by typing dns in the Filter toolbar.
2. Locate the "standard query" for www.google.com (Example: Frame 4).

Note: If you do not see any results after the DNS filter was applied, close the web browser and in the command prompt window, type **ipconfig /flushdns** to remove all previous DNS results. Restart the Wireshark capture and repeat the instructions in **Part 2**. If this does not resolve the issue, in the command prompt window, you can type **nslookup www.google.com** as an alternative to the web browser.



Q2: What is the source MAC address? Is it the same as recorded from Part 1 in Table 1 for the local PC?

Q3: Can you pair up the IP and MAC addresses for the source and destination devices?

Table 2: Device Mapping

Device	IP Address	MAC Address
Source (Local PC)		
Destination (Default Gateway)		

Q4: Record your Wireshark results in Table 3 below:

Table 3: UDP Segment Analysis

Field	Captured Value	Source
Source IP Address		
Destination IP Address		
Source Port		
Destination Port		
UDP Payload Length		
UDP Header Length		

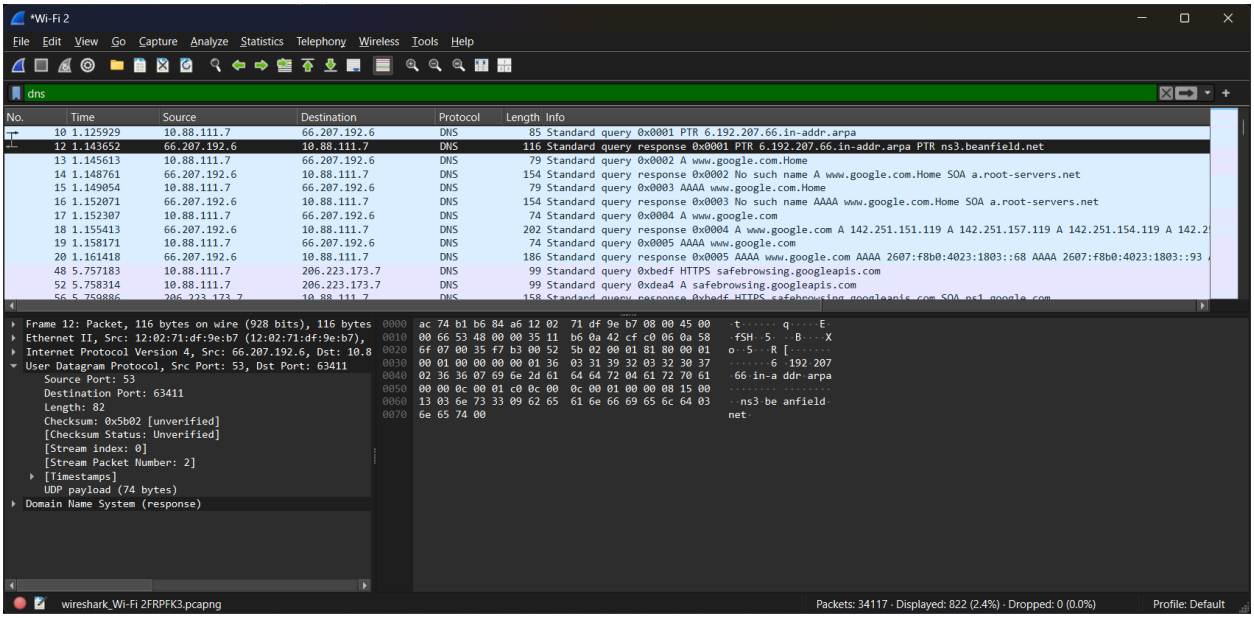
Q5: Is the source IP address the same as the local PC's IP address recorded in Part 1?

Q6: Is the destination IP address the same as the default gateway/DNS server noted in Part 1?

Step 3: Examine UDP using DNS response

Examine UDP by using a DNS query for www.google.com as captured by Wireshark. In this example, Wireshare captured frame 12 in the packet list pane is selected for analysis. The protocols in this query are displayed in the packet details pane (bottom left side) of the

Wireshark window. The protocol layers are show in reverse order (lower layers on top, higher layers on the bottom). Frame 12 had 116 bytes of data on wire as displayed in the first line. This is the number of bytes to send a DNS query to a name server requesting the IP address of www.google.com.



Q7: In the Ethernet II frame for the DNS response, from what device is the source MAC address and what device is the destination MAC address?

Q8: What are the source and destination IP addresses in the IP packet?

Q9: What are the resolved IP addresses for www.google.com?

Section B: FTP

Part 1: Use FTP from a Command Prompt

1. Open a command window (cmd) and start Wireshark with the filter FTP.
2. Type ftp ftp.cdc.gov. Use anonymous as the username and leave the password blank.
3. Type quit to exit.
4. In Wireshark, select the Quit request packet (Figure 9).

Q10: Record your Wireshark results in Table 4 below:

Table 4: FTP Transport Analysis

Field	Captured Value	Source

Transport Protocol		
Source Port		
Destination Port		
Sequence Number		
Acknowledgement Number		
TCP Payload Size		

Q11: What is the Acknowledgement Number and how is this number generated/calculated?

Reflection

1. What are the benefits of using UDP instead of TCP as a transport protocol for DNS?
2. Briefly explain the differences between the UDP and TCP protocols of the transport layer.
3. What is the difference between connection-oriented and connectionless protocols?

General Requirements

- Ensure the screenshots show the local system's time and date
- Use a unique identification for any filename you submit (name, student#, etc).
- The file format can be DOCX or PDF. If you choose to use this document and complete it, highlight your additions with a different color. You can also copy the questions and tables to a clean document and treat it as an answer sheet if you prefer. In this case make sure you identify the questions/tables appropriately.

Grading

Tables – 40 points (10 points each)

Table 1 (Local PC Config): 10 points. Correct identification of IP, MAC, Gateway, and DNS server.

Table 2 (Device Mapping): 10 points. Correct pairing of the Source IP/MAC and Destination IP/MAC.

Table 3 (DNS Analysis): 10 points. Accuracy in recording UDP ports and lengths.

Table 4 (FTP Analysis): 10 points. Accuracy in recording TCP sequence and acknowledgement numbers

Analysis Questions (20 Points)

Each question (Q2 through Q11) is worth 2 points.

Screenshot Verification (20 Points)

DNS Capture: 10 points. Must show the filter dns and the specific query/response frames for www.google.com. The image must show the local system time/date.

FTP Capture: 10 points. Must show the filter ftp and the successful login/quit sequence with ftp.cdc.gov. The image must show the local system time/date.

Reflection Questions (20 Points)

R1 (7 points)

R2 (7 points)

R3 (6 points)