Old Dominion University

CYSE 301 Cybersecurity Techniques and Operations

Assignment #1.2 Basic Wireshark Practice

Alysia Beckles

01127384

**Below is the snippet of a sample lab report.**

Task A

1. Use Wireshark to capture and save ALL related packets when you ping the URL "www.odu.edu". a. Locate the DNS queries and responses in the traffic. b. What is the IP address of the DNS server? c. What information is answered from the DNS server? d. Apply the proper display filter in Wireshark to show ICMP requests. e. Apply the proper display filter in Wireshark to show ICMP responses. f. Show the Protocol Hierarchy Statistics of the traffic.

A screenshot of a computer

Description automatically generated

**Your explanation goes here. For example:**  
I pinged the website [www.odu.edu](http://www.odu.edu) in the command prompt. Then I type DNS in the Wireshark filter and obtained DNS queries and responses in the traffic.

Graphical user interface, application

Description automatically generated



**Your explanation goes here. For example:**  
While I was in Wireshark, I was able to obtain the IP address of the DNS server by looking under the Domain Number System (query), which was 128.82.95.20.



Graphical user interface, application

Description automatically generated

**Your explanation goes here. For example:**  
The DNS server provides certain information on anything linked to the internet. It will provide me the IP address of any website that I am either pinging or searching for. The DNS servers’ main function is to convert domain names to IP addresses that are numerical. The DNS server is 128.82.112.29.

Graphical user interface, text, application

Description automatically generated

**Your explanation goes here. For example:**  
To get the ICMP requests to only be displayed on Wireshark, I had to type ip.dst = = 10.254.56.39 && ICMP. The numbers were the IP address to the website I pinged earlier in this lab, which was www.odu.edu.

Graphical user interface, text, application

Description automatically generated

**Your explanation goes here. For example:**  
In order to get the ICMP responses to only be displayed on Wireshark, I had to type ip.src = = 10.254.56.39 && ICMP.

Graphical user interface, application

Description automatically generated

**Your explanation goes here. For example:**  
In order to obtain the Protocol Hierarchy Statistics of traffic I clicked the statistics tab and clicked the Protocol Hierarchy. Which shows the statistics of several protocols such as ICMP, IPv4, and etc.

1. Use Wireshark to capture and save ALL related packets when you visit the URL www.odu.edu in a new Incognito window. Stop capturing after the ODU website is fully loaded. a. Locate all DNS queries and responses after you open the website and highlight the DNS query for the ODU website. b. How many other DNS queries have been captured after the ODU website is loaded? Can you explain why this happens? c. Combine what you have observed in the previous questions. Can you identify the widgets (external links) loaded on the ODU website? d. Show the Protocol Hierarchy Statistics of the traffic.

Graphical user interface, text, application, email

Description automatically generated

**Your explanation goes here. For example:**  
I typed DNS in the Wireshark filter to see a display of queries and responses, and then I highlighted the DNS query by clicking on the word query.

A screenshot of a computer

Description automatically generated

**Your explanation goes here. For example:**  
There have been several DNS queries because those are the websites that I have visited earlier which were cached. When I was browsing a website while Wireshark was running, it showed some of the sites that I was on previous to running Wireshark.

Graphical user interface, application, table

Description automatically generated

**Your explanation goes here. For example:**  
There are several widgets that I see loaded on the ODU website such as Google API and Google manager.

Graphical user interface, text, application

Description automatically generated

**Your explanation goes here. For example:**  
In order to obtain the Protocol Hierarchy Statistics of traffic I clicked the statistics tab and clicked the Protocol Hierarchy. Which shows the statistics of several protocols such as UDP, IPv4, and etc.

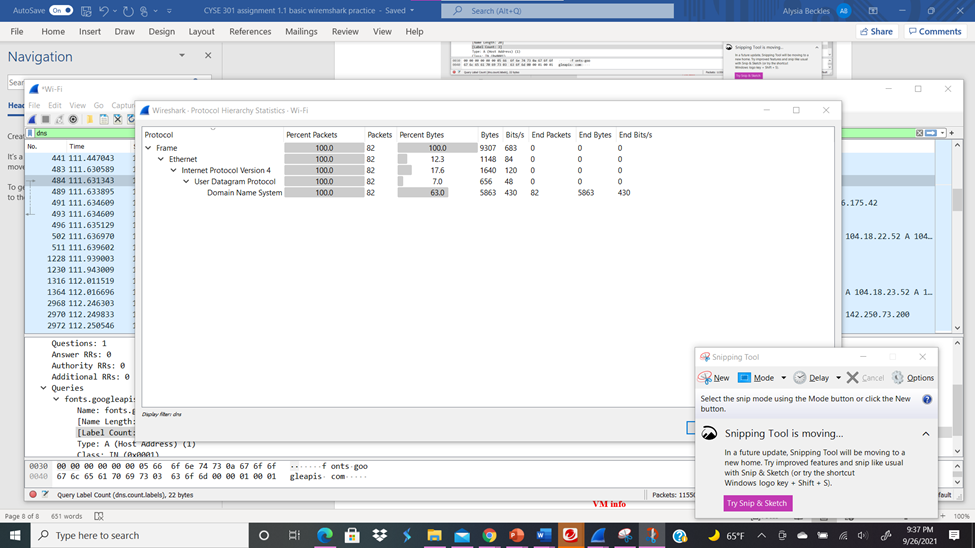
1. Study two Protocol Hierarchy Statistics in Task 1. f and Task 2.d, respectively. Explain the main differences between the two types of traffic.

1.

Graphical user interface, application

Description automatically generated

2.d



**Your explanation goes here. For example:**  
Regarding 1f I had to ping the URL [www.odu.edu](http://www.odu.edu) and then I had to search [www.odu.edu](http://www.odu.edu) in the incognito window. There are several differences when comparing the Protocol Hierarchy Statistics between the two. For instance, pinging the website had significantly less packets than searching for it on the internet; 2d had 82 packets while 1f had 4 packets. Also, both end bytes and packets are more in 2d than 1f. Some of the protocols shown above are different too.