**Basic Wireshark Lab**

By gaining an understanding of the basic protocol analyzer (Wireshark), students will be able to set up and read basic digital traffic, including:

· Gaining a foundational understanding of logging

· Identifying the source and destination IPs

· Translating IP addresses into websites

· Identifying ports and protocols

· Creating a timeline of events

View "2-3 Wireshark Lab," from the video playlist located in Class Resources. In this lab, you will explore some basic Wireshark and Linux commands.

**Part 1:**

Complete the following Wireshark tasks and capture screenshots of each task result:

· On the Kali Linux VM, start a Wireshark packet capture and show all network traffic.

· Identify the IP addresses for the Kali Linux and Windows 10 VMs from within Wireshark.

· Add an ICMP filter and ping the Windows 10 VM.

· Add an IP Address filter with the Windows 10 VM IP Address and run an Nmap service scan against the Windows 10 VM IP Address.

· Research and apply two additional filters to demonstrate their effect on the capture.

· Save the captured packets to a file using your last name as the file name.

· Close the capture session and then load the capture file that you saved.

**Part 2:**

Write a 250- to 500-word summary addressing the following:

· Your Kali IP address.

· The Windows IP Address.

· For both Windows and Linux, identify and explain the following commands:  
- Command used to change directory/folder  
- Command that moves a file  
- Command that removes a file  
- Command that creates a new directory/folder

· An explanation for why a timestamp is important on Wireshark, as well as other logging tools.

· A list of 10 well-known ports and associated protocols.

· A brief explanation of the difference between a port and a protocol.

· Describe how Wireshark can be used to identify events that indicate an attack is in progress or has happened.

Place all screenshots in a Microsoft Word document and submit it to the assignment dropbox. When submitting screenshots as part of your assignment, you must always include a full image of your desktop window, including the date and time in the lower right-hand corner of the Windows desktop or the upper-right corner of the macOS desktop.

While APA style is not required for the body of this assignment, solid academic writing is expected, and documentation of sources should be presented using APA formatting guidelines, which can be found in the APA Style Guide, located in the Student Success Center.

This assignment uses a rubric. Review the rubric prior to beginning the assignment to become familiar with the expectations for successful completion.

You are required to submit this assignment to LopesWrite. A link to the LopesWrite technical support articles is located in Class Resources if you need assistance.