Module 5 Mastery Assessment

Equipment/Supplies Needed

- Computer with internet access
- VMware Workstation Virtualization Software
- Wireshark
- Ftp2.pcapng file

Procedure

Perform the steps in this lab in the order they are presented to you. Answer all questions and record the requested information. Use the Linux Virtual Machine to perform lab activities as directed. Unless otherwise stated, all tasks done as a non-root user. If root access is needed use the sudo command.

Assignment

1. Load the ftp2.pcapng file into WireShark.

2. Examine the file and become aware of the following aspects:

    a. What are the source and destination addresses?

    b. The FTP server type?

    c. The FTP server state when the transfer began?

3. Using your preliminary review what can you say about:

    a. FTP server type:

    b. The login and password:

    c. The transfer protocol used:

4. Provided that --

a. Given the following table https://en.wikipedia.org/wiki/Data-rate_units#Examples_of_bit_rates of various data transfer rates.

b. Given the time that *WireShark* indicates it took to transfer the *10MB.zip* file.

c. Assuming that stream encountered NO interruptions in transfer.

d. From a forensic analysis viewpoint what is the minimum internet transport method that would qualify? (e.g. 56kbps modem, T1, 802.11g, etc.)

e. Explain how you reached this conclusion.

Lab Submissions Proof: Provide screenshots as indicated in the lab; upload your proof to Moodle for grading.

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Answer to source and destination IP (10 points)	
	Criteria #2: Answer to FTP Server Type (10 points)	
	Criteria #3: Answer to FTP Server state when transfer begun (10 points)	
	Criteria #4: Answer to FTP Server type analysis (10 points)	
	Criteria #5: Answer to FTP Server login and password analysis (10 points)	
	Criteria #6: Answer to FTP Server transfer protocol analysis (10 points)	
	Criteria #7: Answer to minimum internet transport method (20 points)	

	Criteria #8: Answer to minimum internet transport method explanation (20 points)	