

Lab #5 - Assessment Worksheet

Performing Packet Capture and Traffic Analysis

Course Name and Number:

Student Name:

Instructor Name:

Lab Due Date:

Lab Assessment Questions & Answers

1. Why would a network administrator use Wireshark and NetWitness Investigator together?
2. What was the IP address for Indy?
3. When the 172.30.0.10 IP host responded to the ICMP echo-requests, how many ICMP echo-reply packets were sent back to the vWorkstation?
4. What was the terminal password for Indy?
5. When using SSH to remotely access a Cisco router, can you see the terminal password? Why or why not?
6. Are packet capturing tools like Wireshark less dangerous on switched LANs?