Netw360 week 7 lab

When we expanded frame 4 the signal strength was -60dbm, the data rate was 1mbps, and the SSID in the beacon frame was Amory. In frame 5, looking at the Hex Details, the BSSID for this access point was 00 15 E9 D1 48. The authentication status in frame 14 was successful. In frame 15, the Association Response status was in a successful state. When we tried to the Microsoft Network Monitor we were unable to pick up any management packets during our capture. SNMP management We were able to successfully ping 10. 7. 8. 80 to verify we had access to the " managed" device. The batch file was set up with the 10. 27. 8. 80 addresses and had commanded to get information from that address. The name of the device was NPIF9460B and the status of it was " ready to print". After we downloaded the MIB Browser and entered 10. 27. 8. 80 into the address field, we were able to get the sysUpTime which was 830 hours 13 min and 2 sec. Finding rogue access points When using the command " netsh WLAN show networks mode= bssid" in the command prompt we were able to identify 17 access points. Out of the 17 access points, 11 were not part of the DeVry wireless network.

1. Is Wireshark open source or propriety? (7 points) Wireshark is an Open-source program.
2. What is seen in each of the three panes that display the packets seen on a local area network? The top pane is the packet list pane that shows each packet on a separate line and has five columns with the following information: the time that the packet came in, source, the destination of each packet, the protocol being used with the packet, and information about each packet. The second pane is the tree view pane and it displays the headers of the various protocols captured in

the packet and this is displayed in a hierarchal view from the physical layer to the application layer. The third pane is the byte view pane that shows the raw data in a hexadecimal format.

3. What does a display filter do? (7 points) The display filter enables you to filter what you want to view when capturing your packets. So if you wanted to just view the packets that were using the protocol TCP you could filter those out. You can also use expression filters that let you be more specific in what you want to filter.
4. What does the protocol column show? (7 points) The protocol column shows the highest layer protocol in the frame.
5. How do you expand the details in a layer of the packet in the middle frame? 7 points) To expand the details you must click on the plus sign.
6. In frame 1 what channel is being used? (7 points) Frame 1 is using channel 6.
7. In frame 1 what frequency is being used? (7 points) The frequency being used is 2437MHz.
8. In frame 1 what is the signal level? (7 points) The signal level in frame 1 is 11.
9. What type of frame is frame 1? (7 points) Frame 1 is a broadcast initiation frame to the access point
10. In frame 1 what is the beacon interval in milliseconds? (7 points) The beacon interval is 102. 4ms.