Lab 2 - Assessment Worksheet

Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic

Course Name and Number:

_____

Student Name:

_____

Instructor Name:

_____

Lab Due Date:

_____

Lab Assessment Questions

1. Which tool, Wireshark or NetWitness, provides information about the wireless antenna strength during a captured transmission?

2. Which tool displays the MAC address and IP address information and enables them to be correlated for a given capture transmission?

3. What is the manufacturer-specific ID for the GemTek radio transmitter/receiver?

4. The receiver and/or transmitter address is hard-coded in hardware and cannot be changed; it can always be counted on to correctly identify the device transmitting. True or False?

5. What is the actual web host name to which www.polito.it is resolved?

6. How can one determine that the website www.polito.it is in Italy?

7. Which IP address is for www.polito.it?

8. Which destination organization is the owner of record of www.polito.it?