COMP435 Written Assignment 5 Name: _____

Question 1: Packet Sniffing and Spoofing Reflection Complete these questions using your capture, code, and observations from the in-class packet sniffing and spoofing activity. Brief answers are sufficient.

1.1. What did your initial live capture show? Why was there no reply?

1.2. In your Wireshark capture, how could you identify the forged reply? What source IP address did the forged packet claim to have?

Claimed source IP: _____

1.3. What happened after you changed the ICMP ID? Why?

1.4. What does this activity show about using a source IP address as authentication?