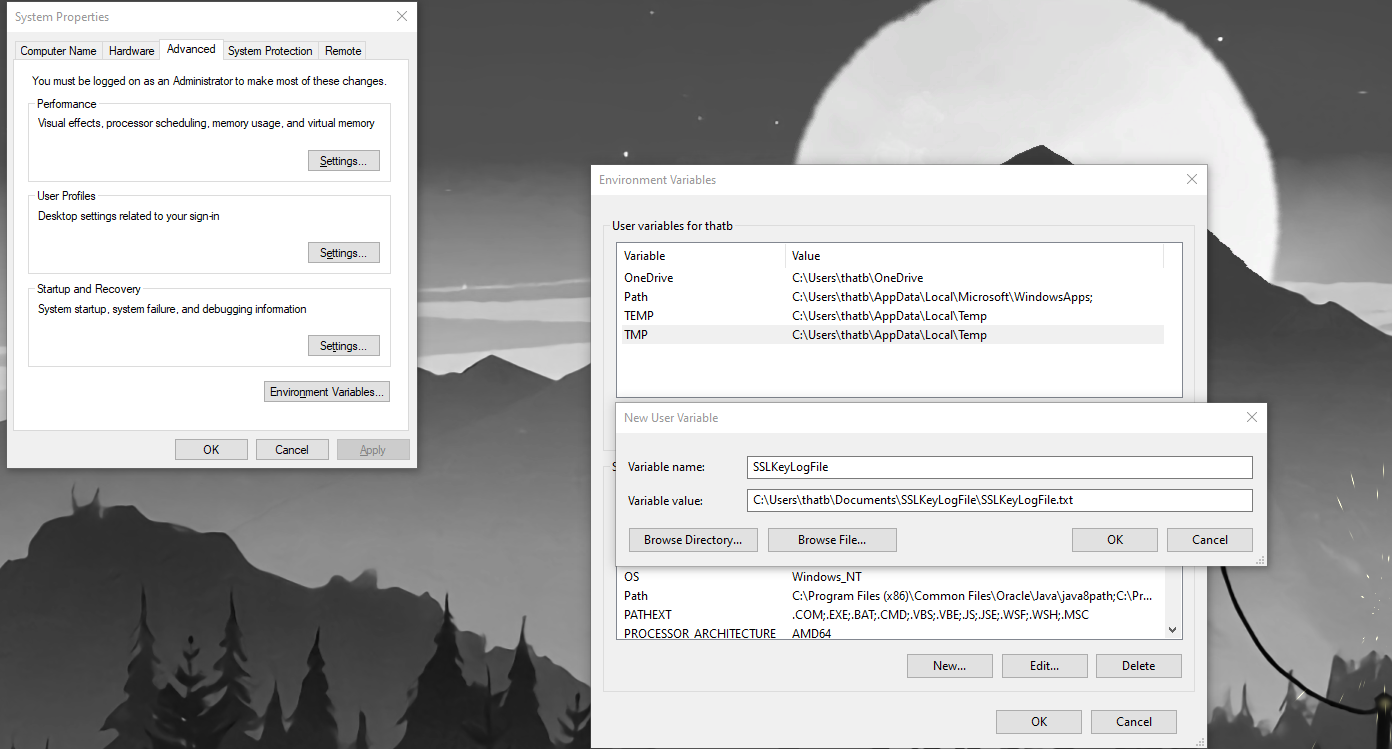
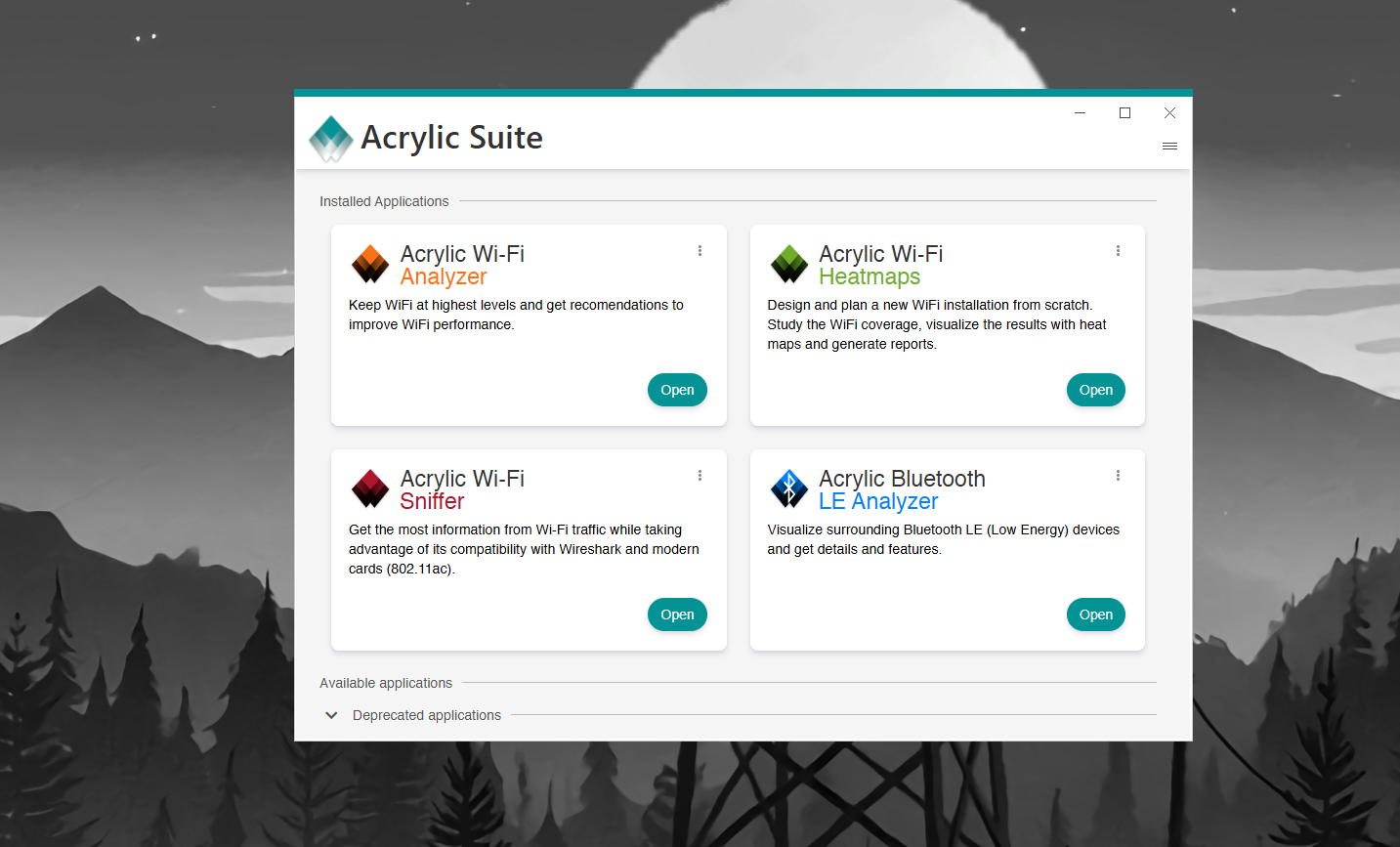
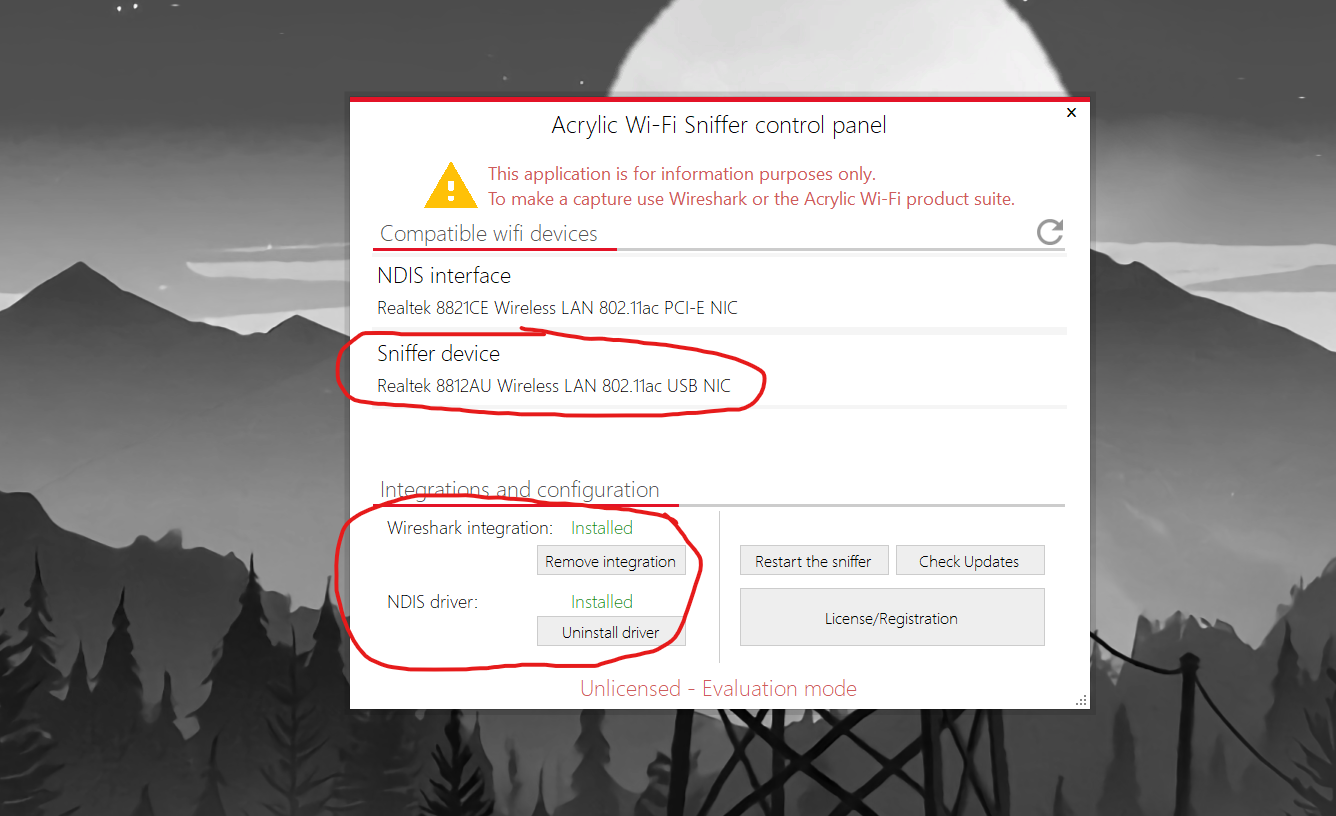
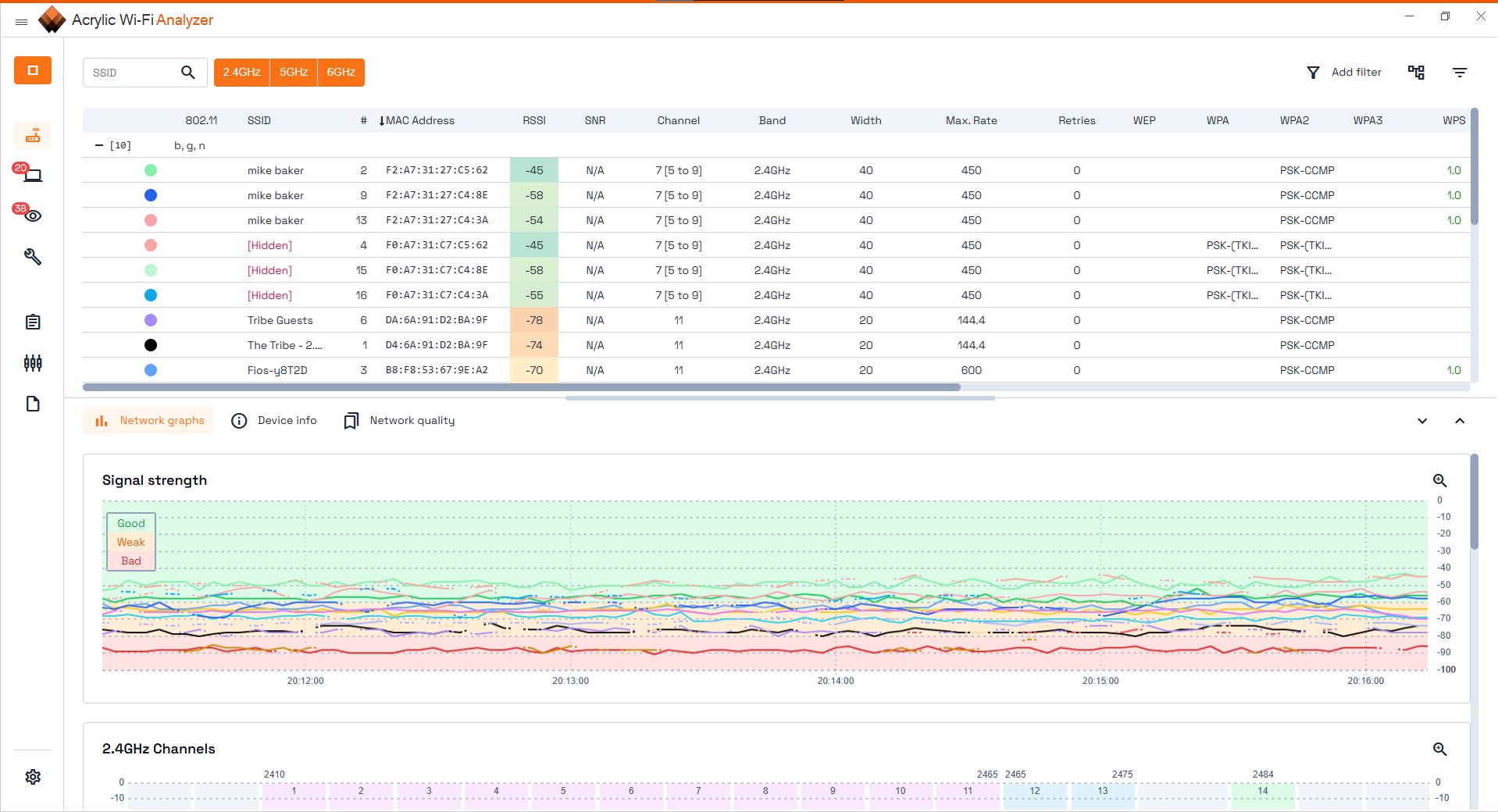
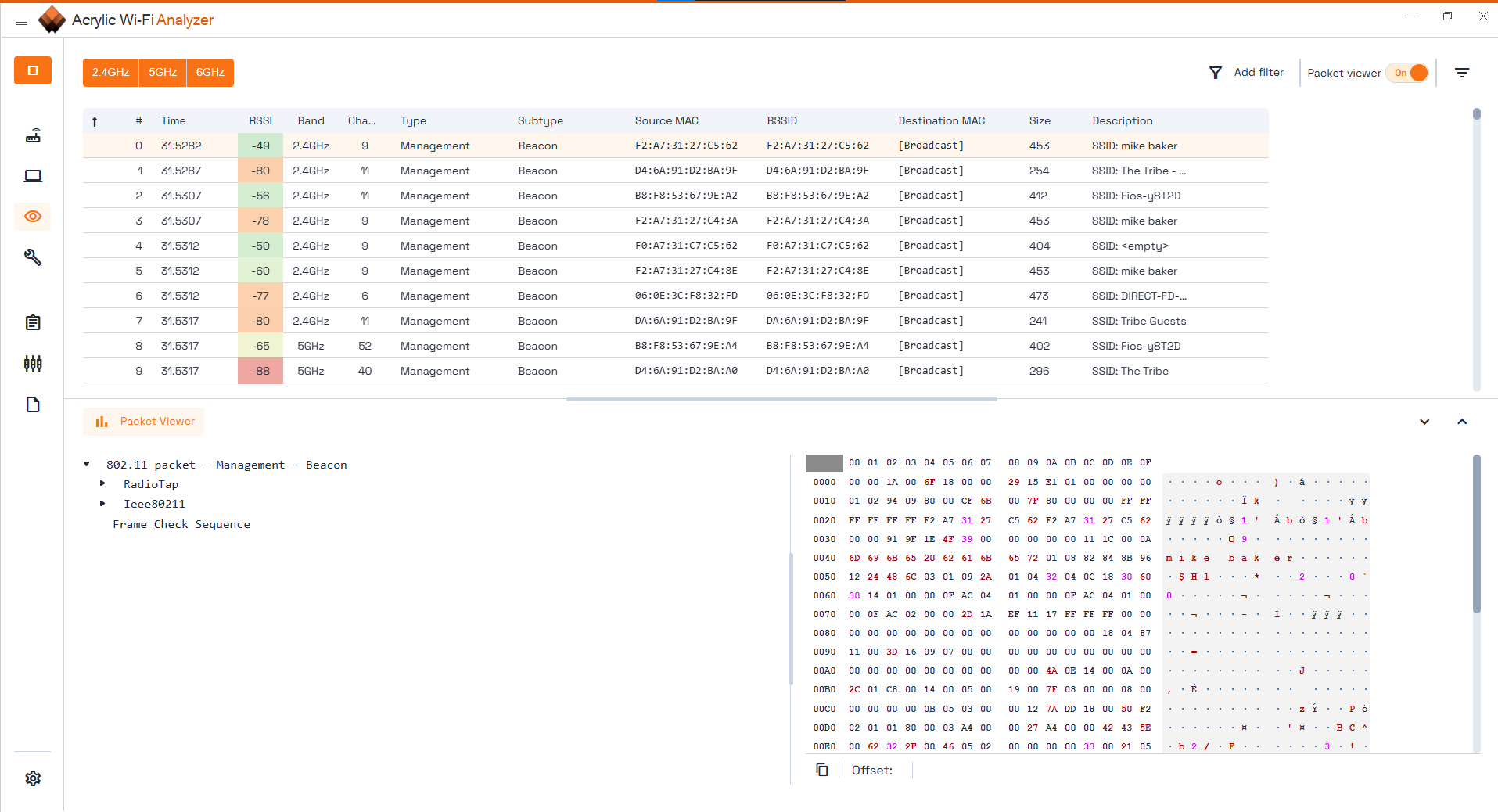
Dominic Baker

Wireshark and Acrylic Setup & Vulnerability Scan

  
***Figure 1 shows the SSL Log file being added in the environment variables.  
  
  
Figure 2 shows Acrylic installed on the computer and the accompanying programs in Acrylic.  
  
  
Figure 3 shows the Acrylic Wi-Fi sniffer. Circled in red are the recognized Realtek Wi-Fi sniffer device, Wireshark integrated, and the NDIS drivers installed.  
  
***

***Figure 4 shows the Acrylic Wi-Fi Analyzer capturing packets.***

***  
Figure 5 shows the Acrylic Wi-Fi Analyzer’s built-in packet viewer function working.***

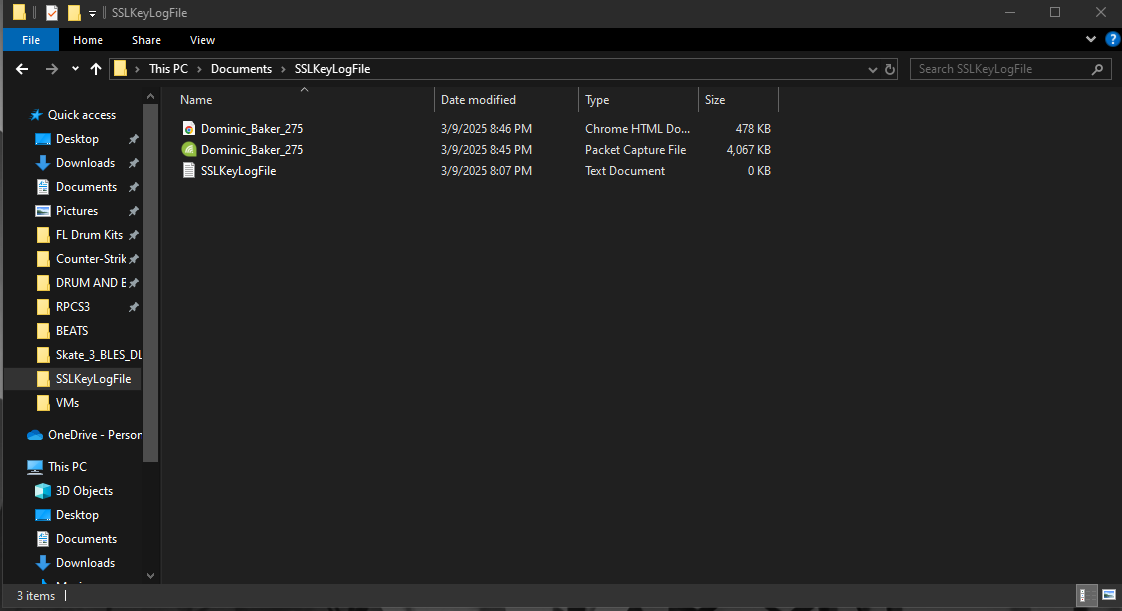
**Questions:**

**3. Expand and study both the RadioTap and 802.11   
 a. Do you see Frame Control and Management? What is the subtype?** Yes, I see Frame Control and Management, the subtype is 8. **b. Are there any fragments?** No, as under “Flags,” sent/recieved with fragmentation is set to false (0), meaning there are no fragments. **c. Does it allow re-transmit? Why?**

No, it does not allow re-transmission because the packet did not use TCP. **d. What is the header length of the record you selected?** The header length was 26. **e. Select the Timestamp under Present Flags. What does that number mean in actual time?** The number in actual time represents the number of seconds that have passed since Jan. 1st, 2001. **f. Select the Channel antenna and identify the Channel number.** The channel number is 2452 MHz.

**g. Select PCAP Options and export a PCAP and save it as FirstName\_LastName\_275.PCAP.**

**h. Click reports → Generate reports and send screenshot.**

**  
*Figure 6 shows saved PCAP file and HTML report.***