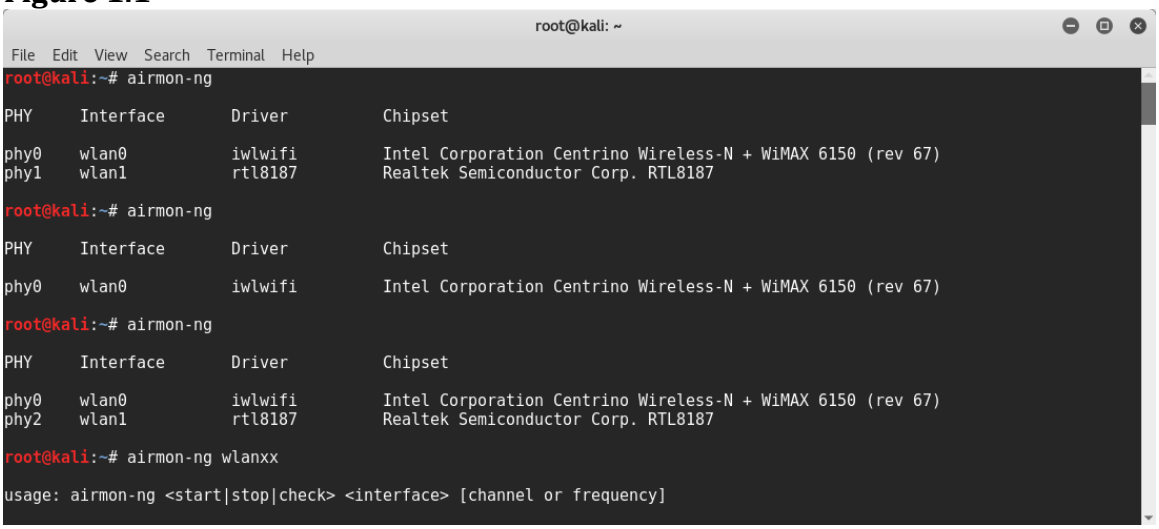
Introduction:
I began my the lab setting up a live boot Kali Linux USB drive. After setting up the USB, I booted into Kali. To capture the handshake I used an external piece of hardware, the Alfa AWUS036H 1000mW 1W 802.11b/g network adapter.

Procedure:

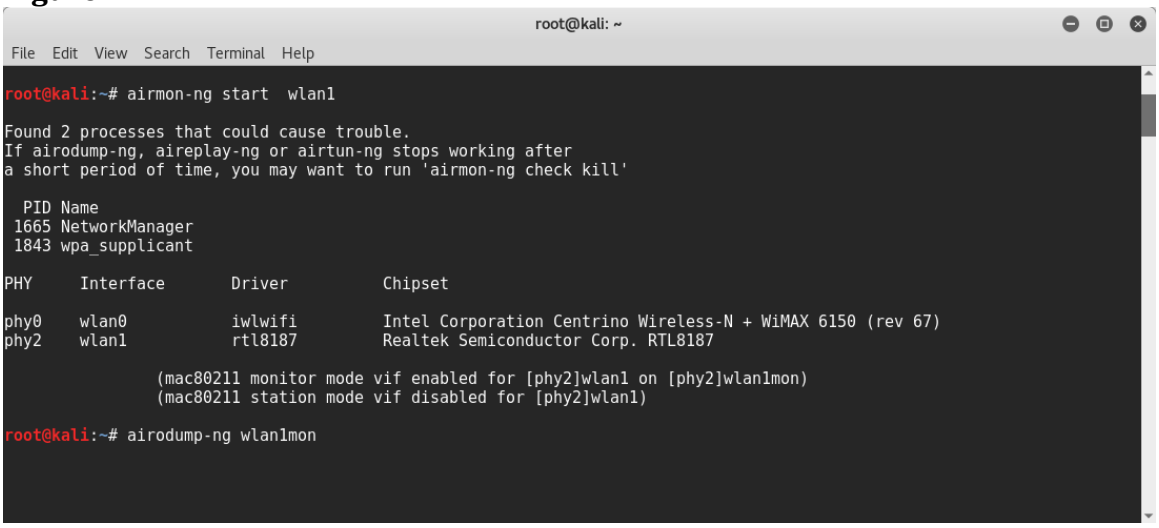
1. After booting into Kali I used the command airmon-ng to determine if the wireless adapter is connected and "seen" by Kali Linux. I took not of the interface, chipset, and driver. See **Figure 1.1**

Figure 1.1



2. After seeing that Kali Linux recognized the wireless adapter. I used the command airmon-ng start wlan1 to put the adapter in monitor mode. See **Figure 2.1**

Figure 2.1



3. After putting the wireless adapter in monitor mode I used the command ariodump-ng wlan1mon to display the critical information about all the wireless networks that are "seen" by the wireless adapter. See **Figure 3.1-3.2**

Figure 3.1

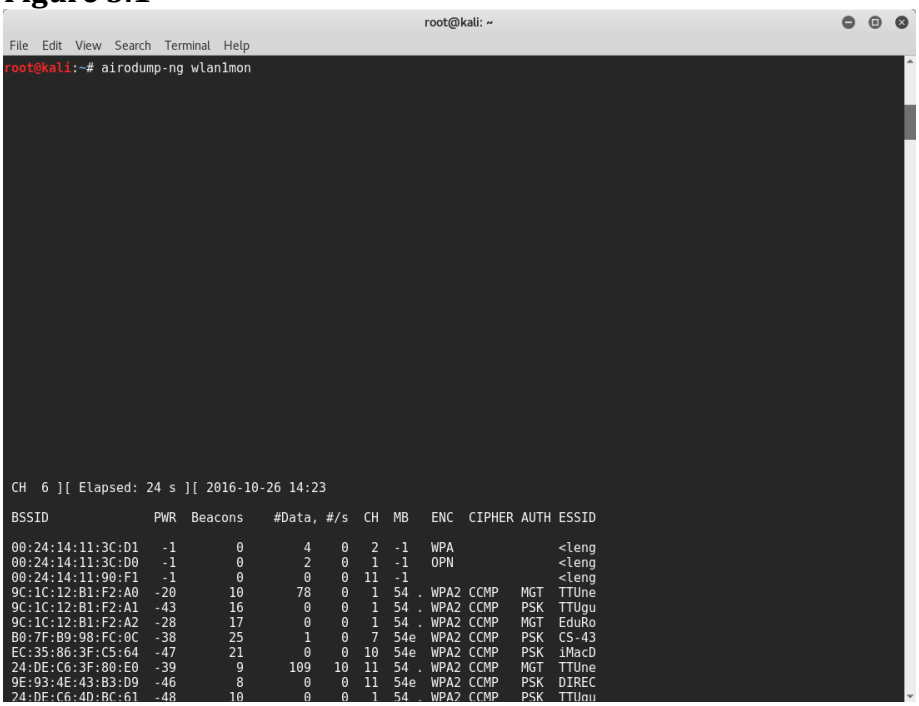
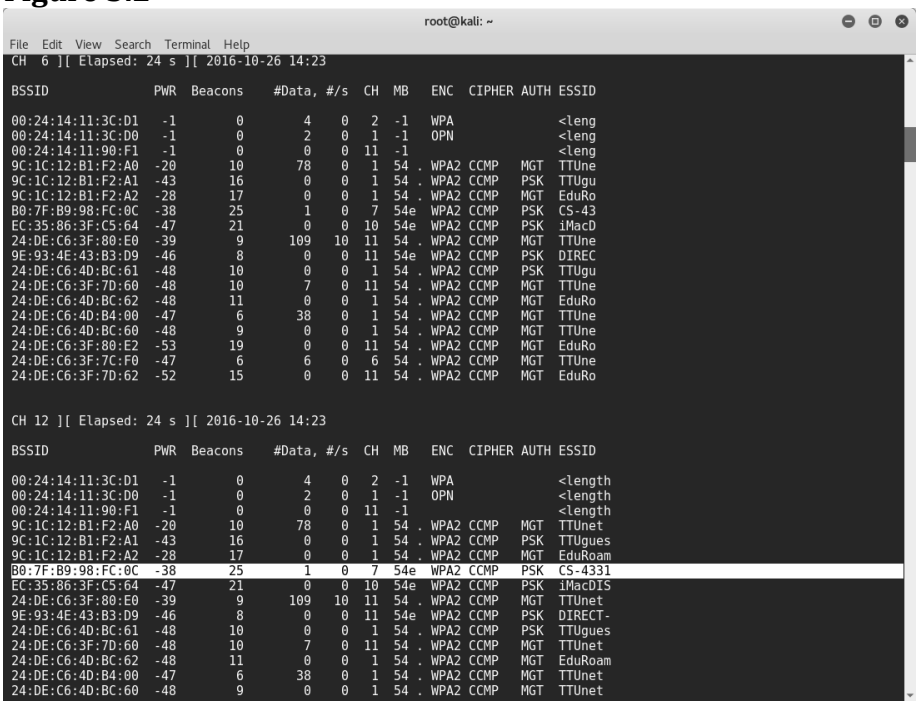
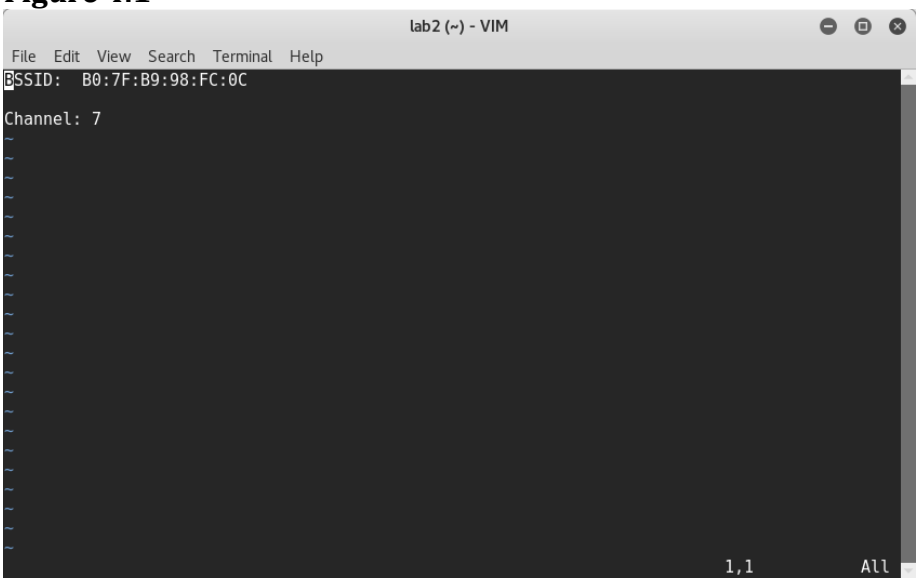


Figure 3.2



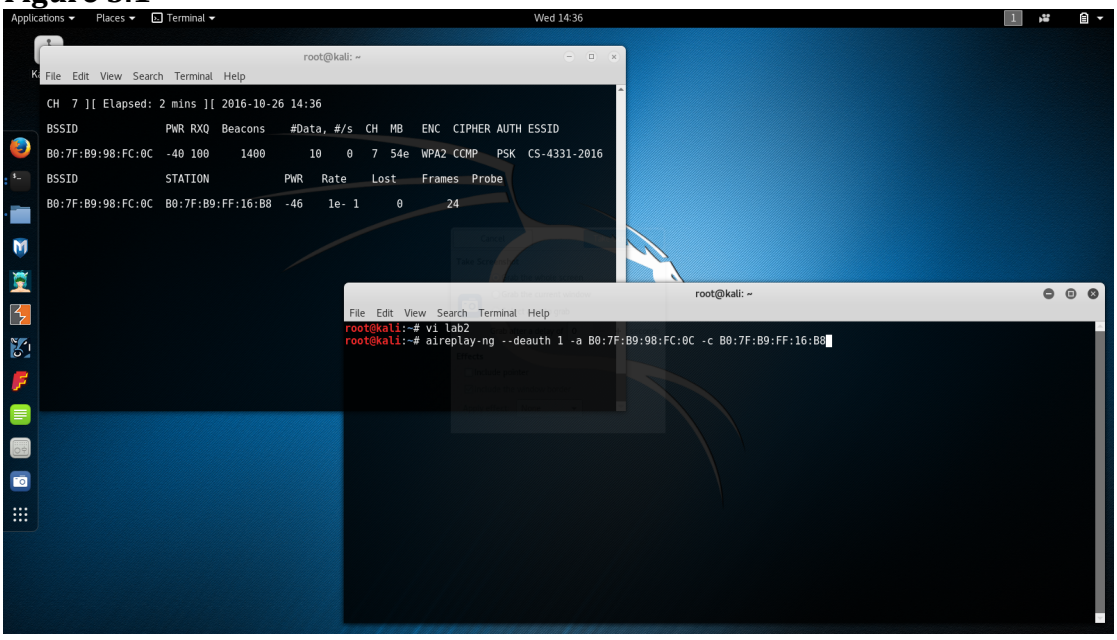
4. After displaying the critical information about the available networks. I then look for the record corresponding to CS-4331-2016 network. After finding the record, I saved the BSSID and the channel of the adapter in lab2.txt. See **Figure 4.1**

Figure 4.1



5. Now I am able to capture the traffic associated with the channel and BSSID saved from the previous step. I used the command airodump-ng --bssid B0:7F:B9:98:FC:0C –c 7 --write step5file wlan1mon. The critical information began to display and I set up a new terminal to prepare for the next step. **See Figure 5.1**

Figure 5.1



6. In this step I attempted to capture the handshake by forcing one or more clients currently associated with the AP to disassociate. To do this I used the command aireplay-ng --deauth 1 –a B0:7F:B9:98:FC:0C –c B0:7F:B9:FF:16:B8. I repeated this command until the handshake was captured. See **Figure 6.1-6.2**

Figure 6.1

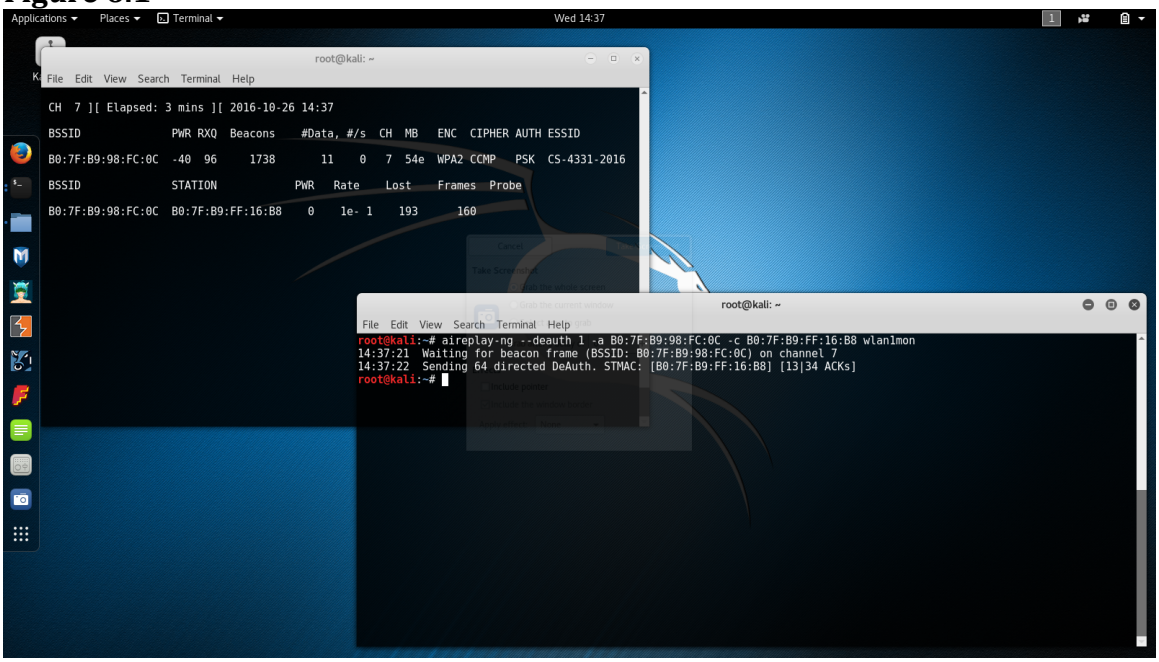
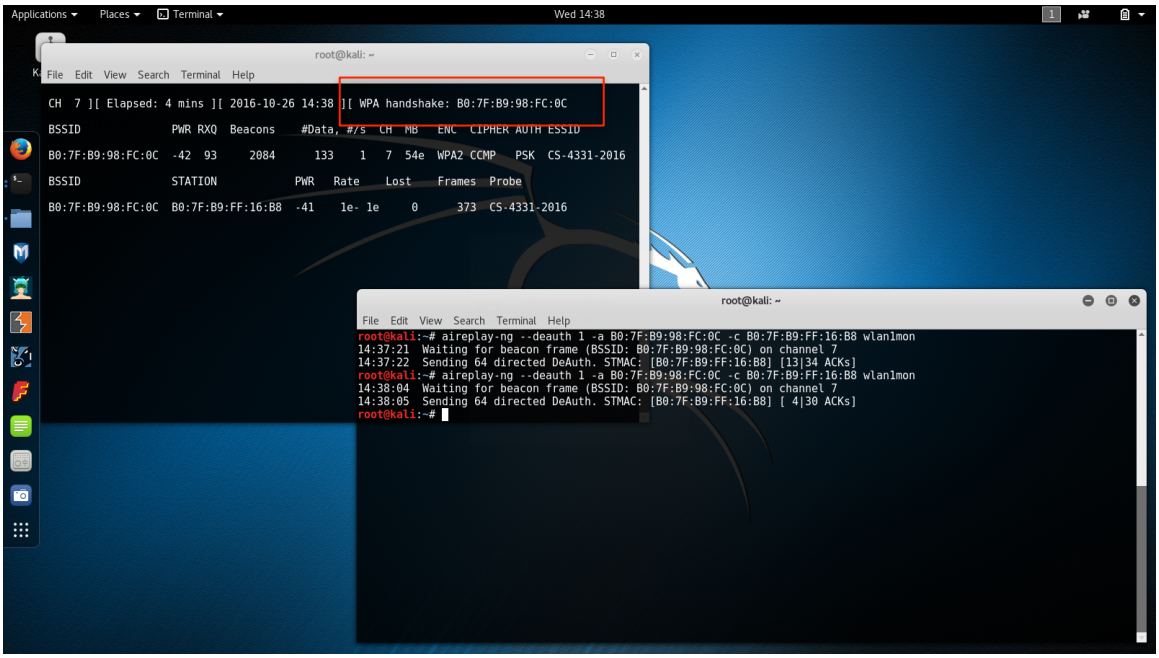


Figure 6.2



7.

a. After capturing the handshake I then attempted to crack the password using the command aircrack-ng step5file-01.cap –w rockyou.txt. The step5file-01.cap contains the critical information about the network. The rockyou.txt contains the password file or dictionary. See **Figure 7.1-7.2**

Figure 7.1

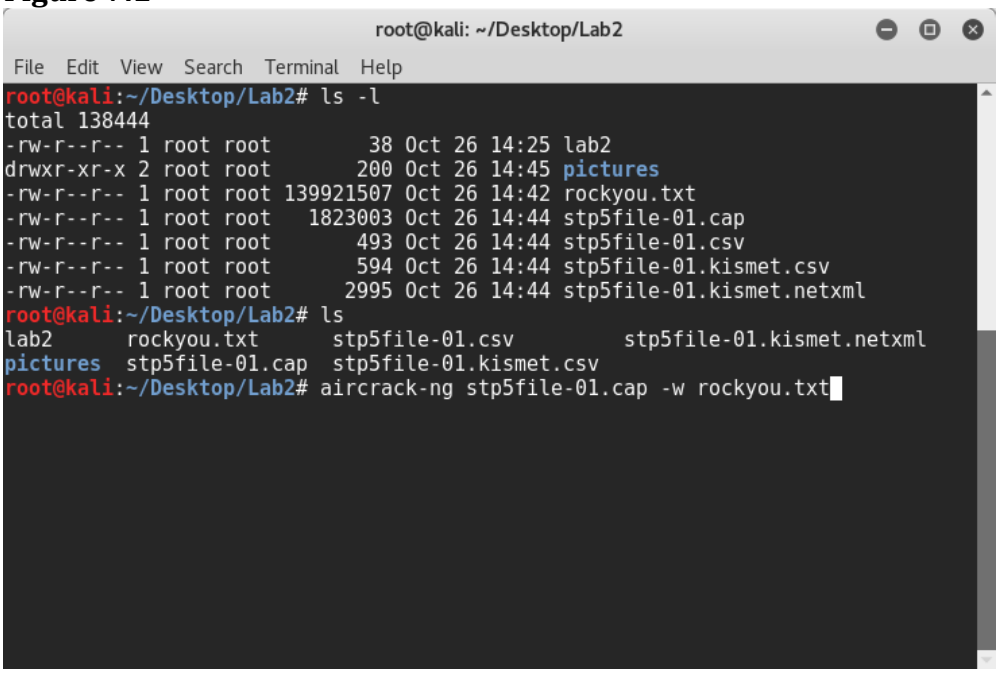
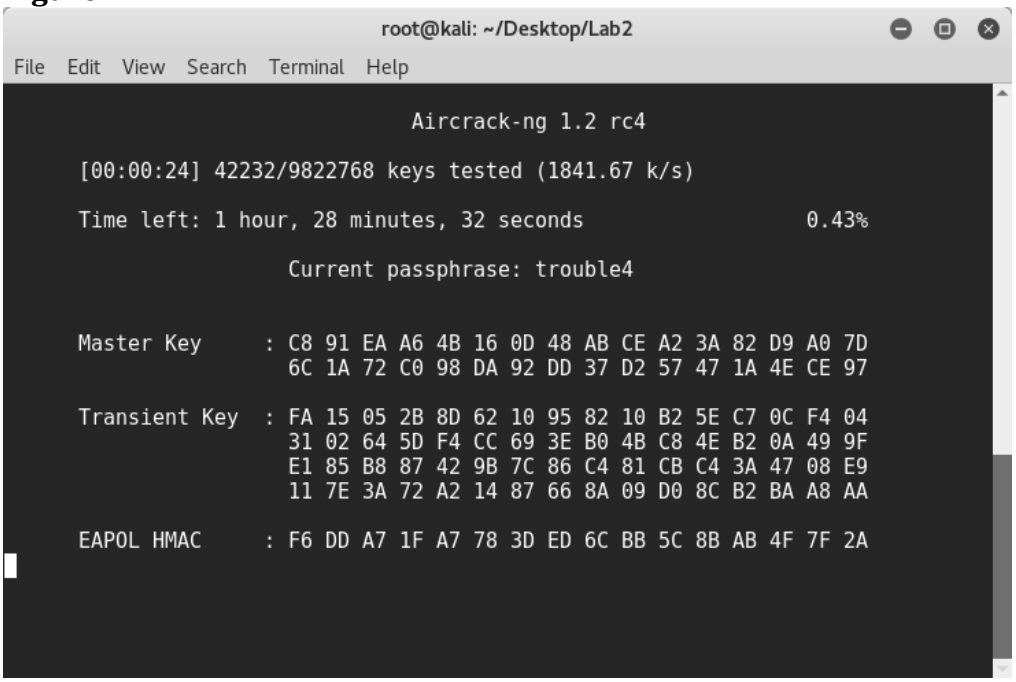
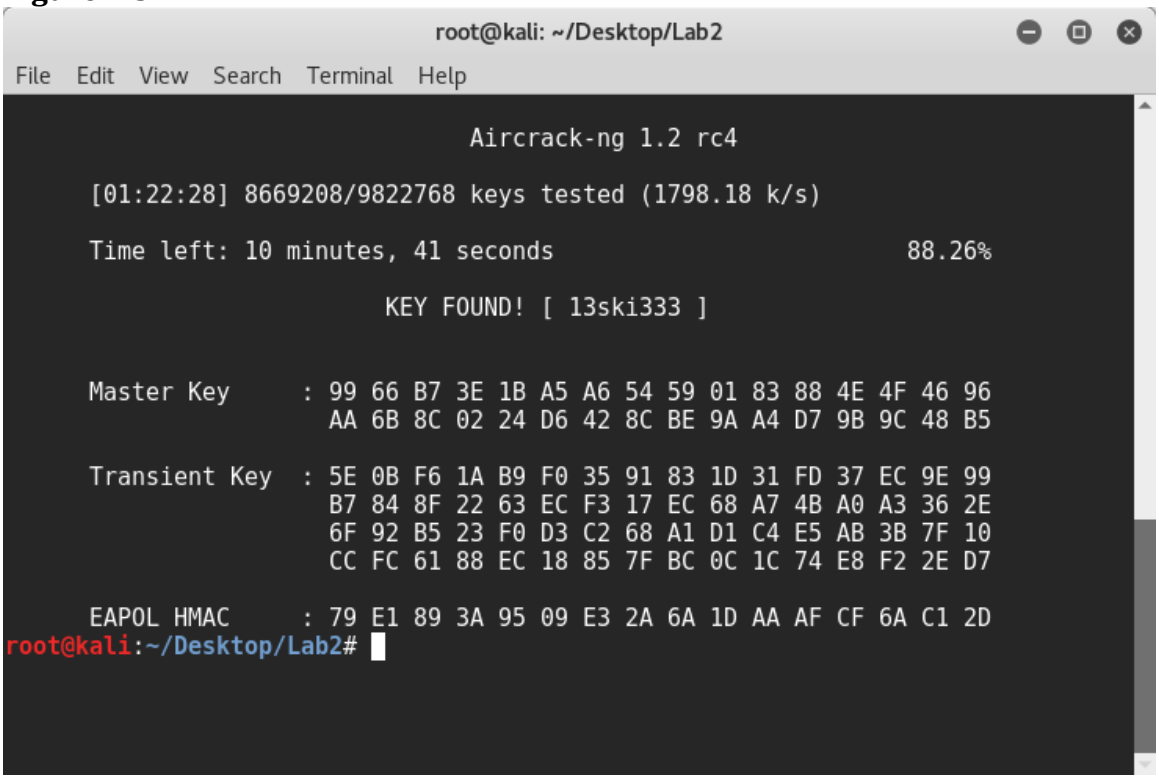


Figure 7.2



b. It took my HP Pavilion 1 hour and 22 minutes to complete the dictionary attack. See **Figure 7.3**

Figure 7.3



Conclusion:

In conclusion there are some key steps in the lab that are important to understand. By my understanding, the term monitor mode in step 2 means to put the wireless adapter in a state were it is collecting all the information about active wireless networks in its maximum proximity.

In step 7 we take the information from capturing the handshake specifically the MIC and try and guess the PMK through brute force. Once we see the PMK is correct, we can verify it against the MIC to obtain the correct password for the network.

I don't believe MAC whitelisting would prevent this attack because then anyone listing to the network can gain access to your network.