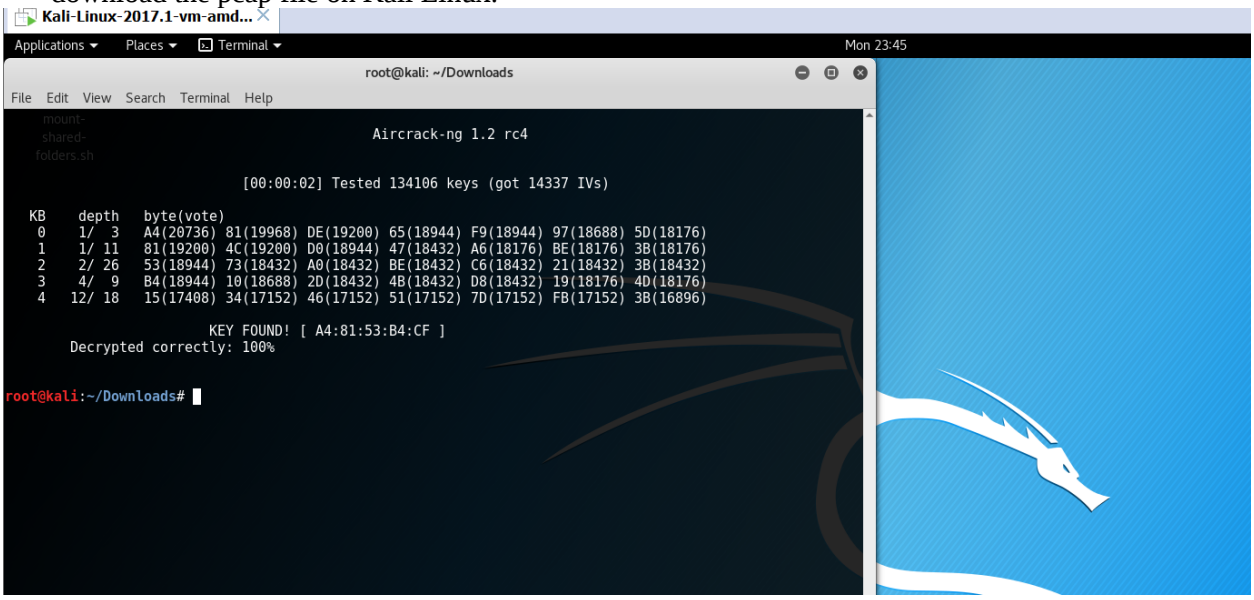
Lab - 6 NCL Wireless Access Exploitation

- This is an individual assignment, and is worth 20 points.
- The due date and time is Friday, October 20 Midnight.
- Change the file name following the naming convention suggested below. Naming convention is as follows: homework, underscore, last name, first initial, and extension (e.g., Crypto-Assignment-ImG.docx). If you do not follow the convention, I will deduct 0.5.

- Log in to the following site: https://ncl.cyberskyline.com
- Go to Dashboard > NCL Fall 2017 Gymnasium > Wireless Access Exploitation
- You will find five questions. Answer each question and provide necessary screenshots and explanation to justify your answer. Take advantage of the hints provided on the page.

1. How many IVs are in the packet capture? Provide a screenshot that supports your answer.

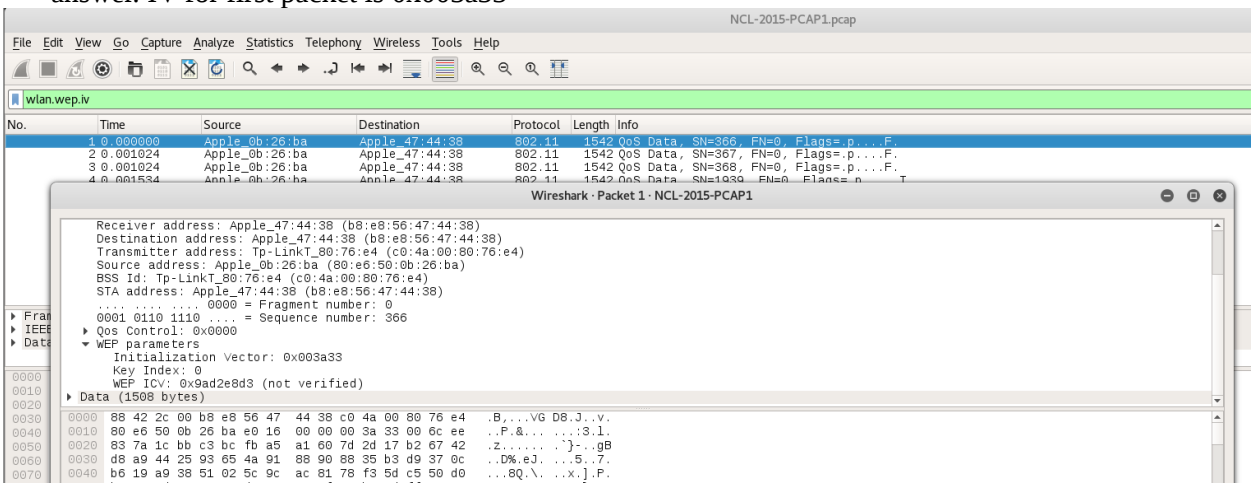
- Hints: For this, go to Kali Linux and launch Firefox. And login to ncl.cyberskyline.com, and download the pcap file on Kali Linux.



2. What is the key size of the wireless network in bits? Explain how you arrived at your answer.

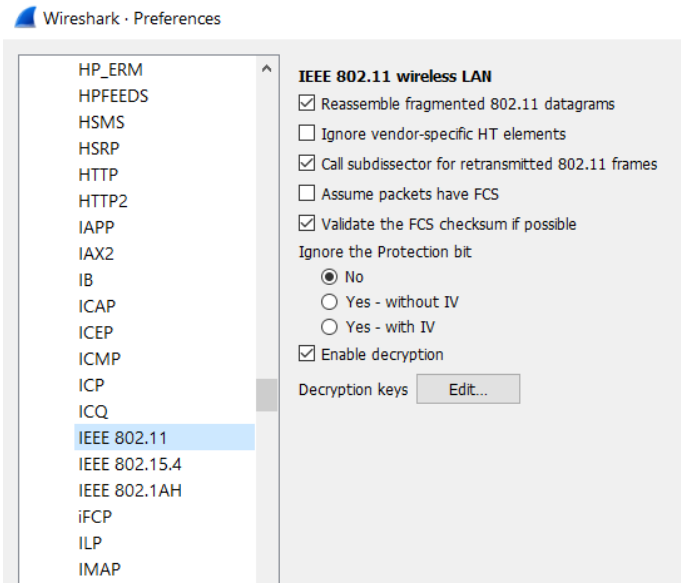
The key size is 64 bits long. I arrived at this answer by running aircrack-ng on the PCAP file and examining the key in hex. By counting how many pairs of hex values there were, I was able to determine that 40 bits of data were needed to access the WEP network, and 24 bits of data were set by the factory since the passcode users would enter was only 40 bits long. This is standard in WEP configurations with small key sizes.

3. What is the IV for the first packet in the capture (in hex)? Provide a screenshot that supports your answer. IV for first packet is 0x003a33

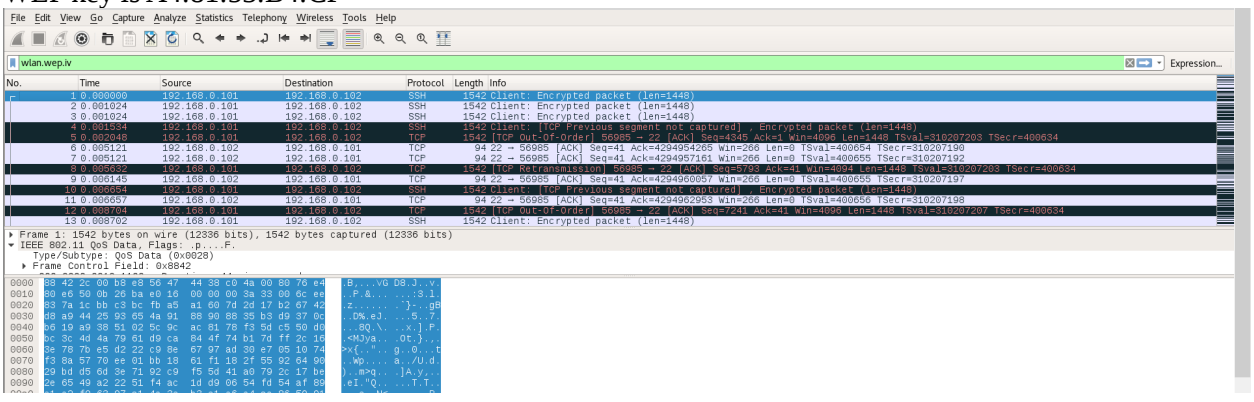


4. What is the WEP key? Provide a screenshot that supports your answer.

- Hints: Go to Wireshark > Edit > Preferences > IEEE 802.11



WEP key is A4:81:53:B4:CF



5. What is the TCP checksum of the first packet in the capture (in hex)? Provide a screenshot that supports your answer.

   TCP checksum of the first packet is 0x897b