# Assignment 6 NCL Wireless Access Exploitation

|  |
| --- |
| * This is an individual assignment, and is worth 20 points. * The due date and time is Tuesday, 1:00 pm (sec01) / 5:30 pm (sec76), October 22. * Apply the usual naming convention. |

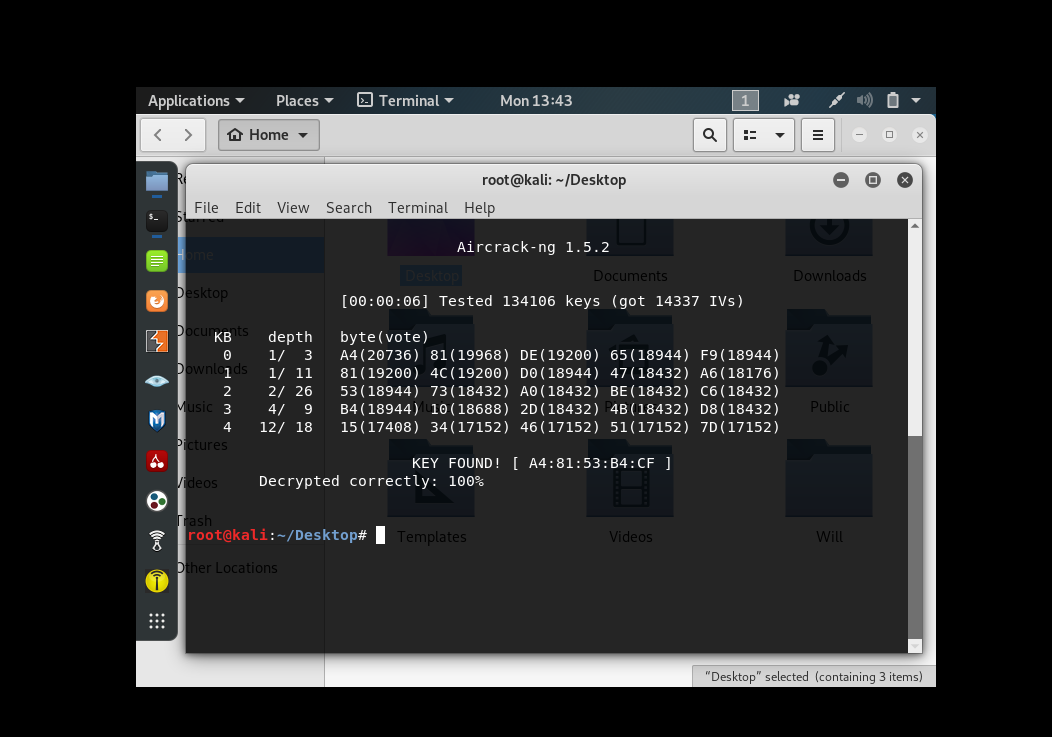
# Background

* This assignment is from National Cyber League (NCL) exercise.
* Use the attached “NCL-2015-PCAP1.pcap”.
* You need to use Kali to answer the questions below. Send the attached pcap file to your email and download from Kali using Firefox. Move the capture file to **Desktop** on Kali.
* Use **aircrack-ng** on Kali. Refer to the “CIS 480 Aircrack-ng.pptx” for hints.

# Tasks

1. How many IVs are in the packet capture? Provide a screenshot that supports your answer. Run the following command: **aircrack-ng NCL-2015-PCAP1.pcap**.

There are 14337 IVs.



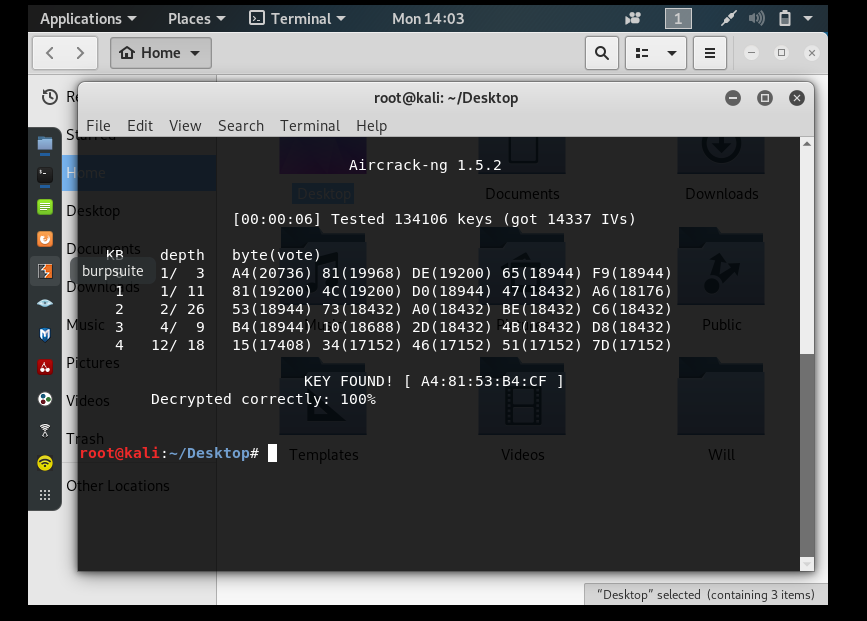
1. What is the WEP key size of the wireless network in bits? WEP keys are larger than the size of your password input (the key obtained via aircrack-ng). Explain how you arrived at your answer.

For this, we need to count the number of bits in the input password text (x bytes \* 8 bits per byte = x bits). Then, we compare that to the possible WEP key sizes and configurations. Refer to the attached file: WEP Shared Key Authentication.pdf.

The key size is 64-bit. This is because the length of the password is only 5 ASCII characters. This indicates the PW is 64-bit.

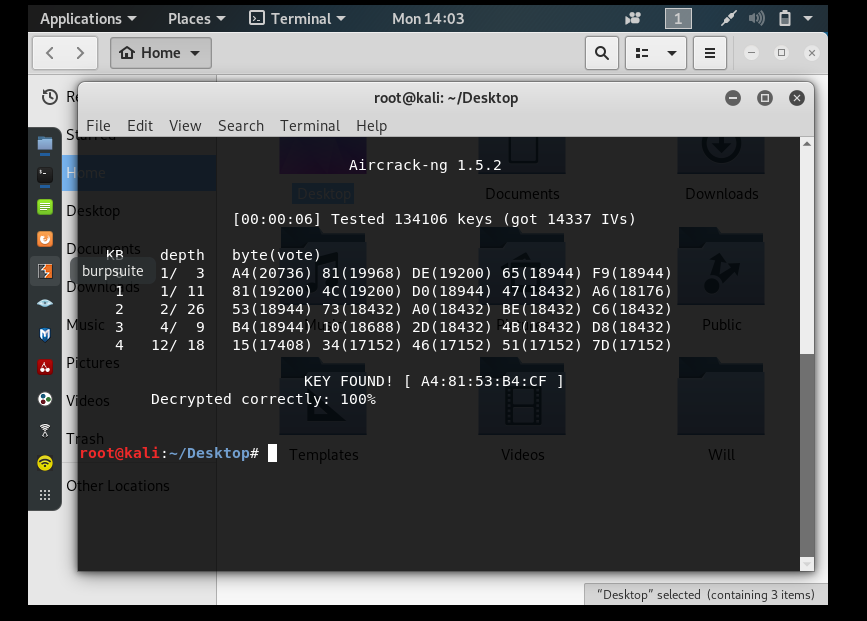
1. What is the IV for the first packet in the capture (in hex)? Provide a screenshot that supports your answer.

The first byte in hex is A4.



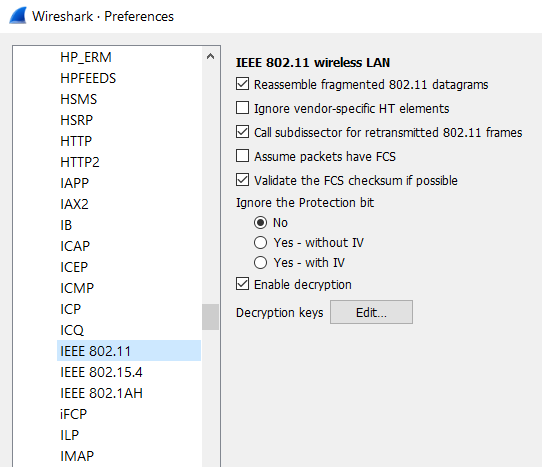
1. What is the key (i.e., password input) you obtained after running aircrack-ng? Provide a screenshot that supports your answer.

The key is A4:81:53:B4:CF.



1. What is the TCP checksum of the first packet in the capture (in hex)? Provide a screenshot that supports your answer. You should decrypt the capture with the key you obtained.

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



The checksum is 0x897b.

