

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.

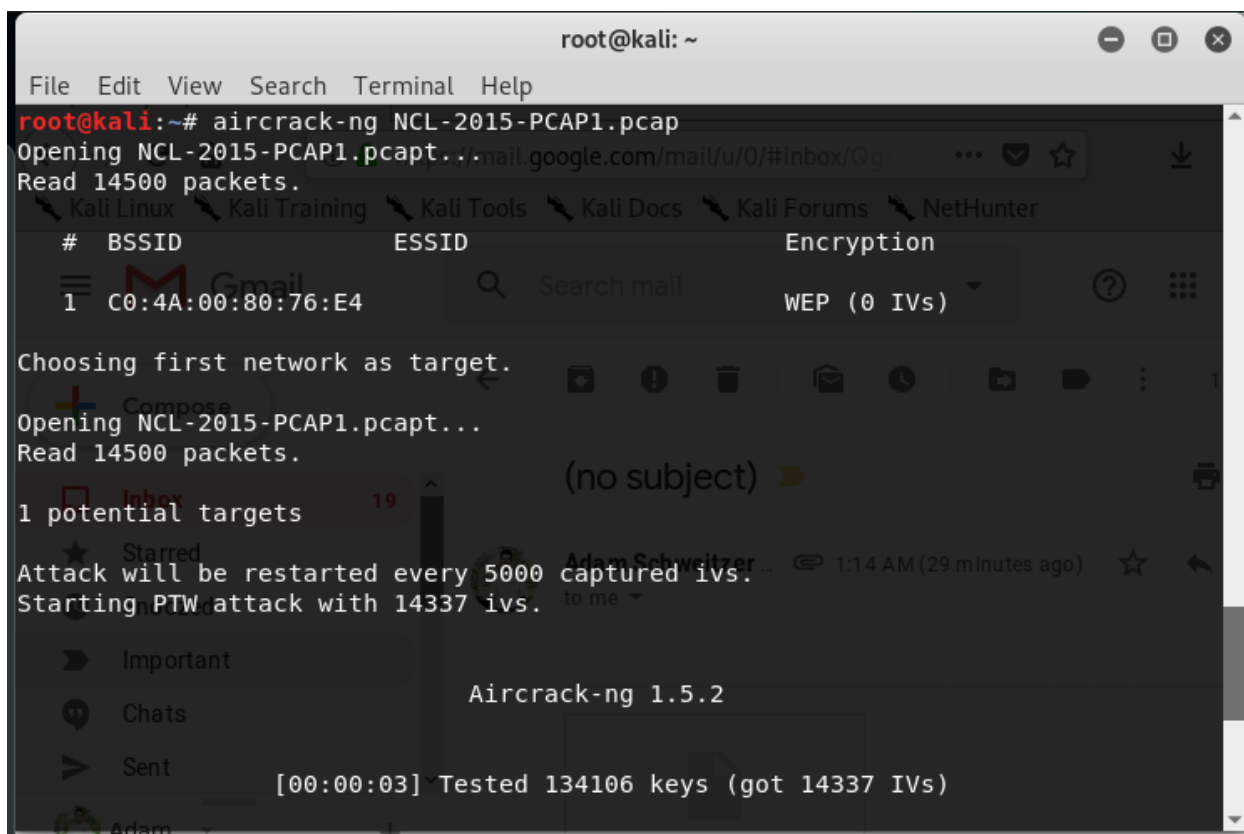
Background

- 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 IV's



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# aircrack-ng NCL-2015-PCAP1.pcap  
Opening NCL-2015-PCAP1.pcap...  
Read 14500 packets.  
# BSSID ESSID Encryption  
1 C0:4A:00:80:76:E4 WEP (0 IVs)  
Choosing first network as target.  
Opening NCL-2015-PCAP1.pcap...  
Read 14500 packets.  
1 potential targets  
Attack will be restarted every 5000 captured ivs.  
Starting PTW attack with 14337 ivs.  
Aircrack-ng 1.5.2  
[00:00:03] Tested 134106 keys (got 14337 IVs)
```

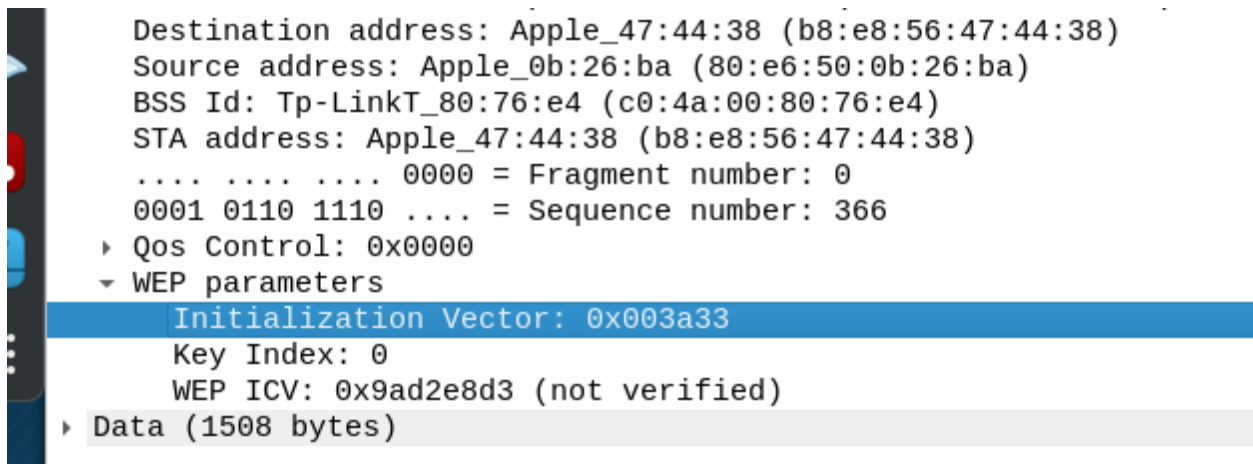
2. What is the WEP key size of the wireless network in bits? WEP keys are larger than the size of your password input (the key obtained via aircrack-ng). Explain how you arrived at your answer.

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.

5 bytes * 8 (bits/byte) = 40 bits + 24 factory set bits = 64 bit WEP

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

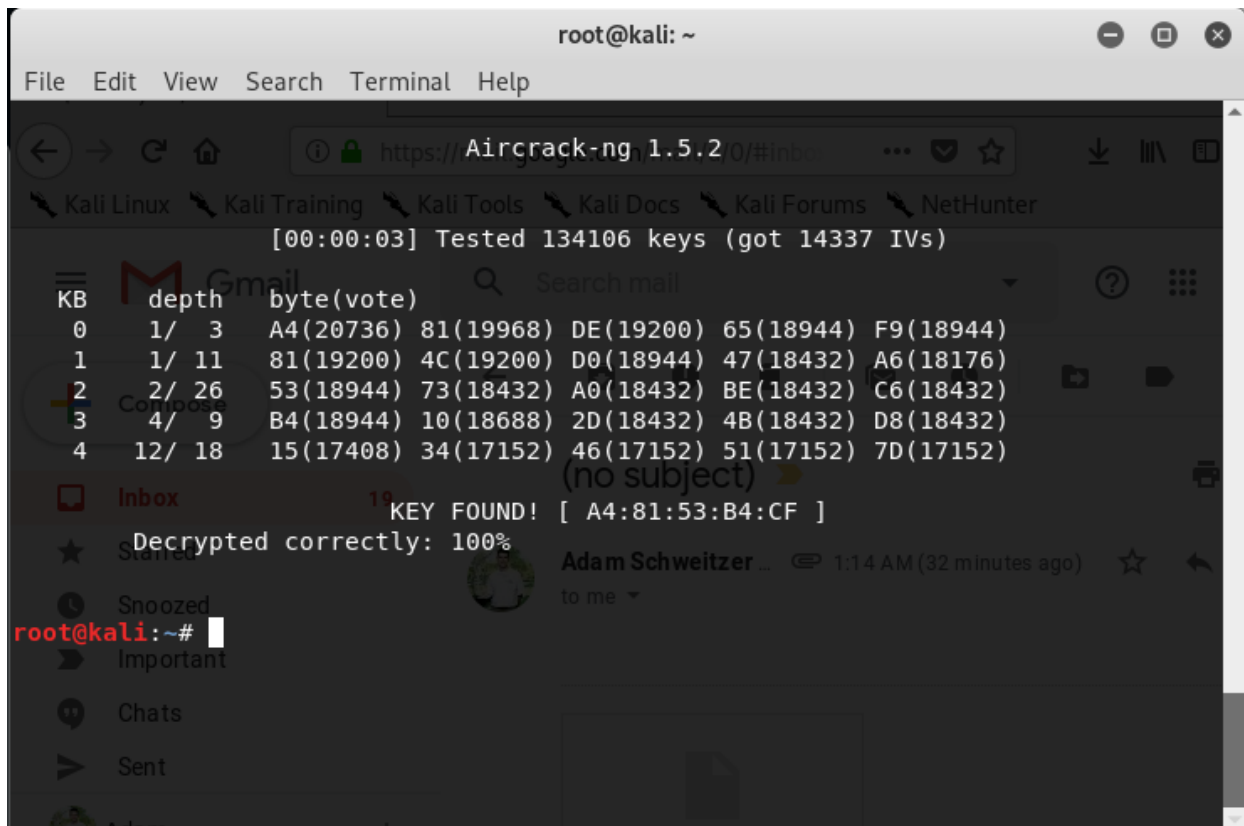
0c003a33



```
Destination address: Apple_47:44:38 (b8:e8:56:47:44:38)
Source address: Apple_0b:26:ba (80:e6:50:0b:26:ba)
BSS Id: Tp-LinkT_80:76:e4 (c0:4a:00:80:76:e4)
STA address: Apple_47:44:38 (b8:e8:56:47:44:38)
.... .... 0000 = Fragment number: 0
0001 0110 1110 .... = Sequence number: 366
▶ Qos Control: 0x0000
▼ WEP parameters
  Initialization Vector: 0x003a33
  Key Index: 0
  WEP ICV: 0x9ad2e8d3 (not verified)
▶ Data (1508 bytes)
```

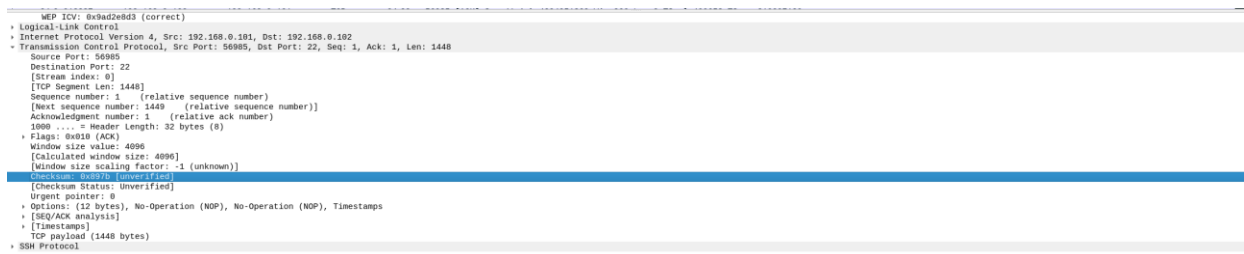
4. What is the key (i.e., password input) you obtained after running aircrack-ng? Provide a screenshot that supports your answer.

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. You should decrypt the capture with the key you obtained.

0x897b



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

The image shows the 'Wireshark · Preferences' dialog box. On the left is a list of protocol categories, with 'IEEE 802.11' selected and highlighted in blue. The right pane is titled 'IEEE 802.11 wireless LAN' and contains the following settings:

- Reassemble fragmented 802.11 datagrams
- Ignore vendor-specific HT elements
- Call subdissector for retransmitted 802.11 frames
- Assume packets have FCS
- Validate the FCS checksum if possible
- Ignore the Protection bit
 - No
 - Yes - without IV
 - Yes - with IV
- Enable decryption

At the bottom, there is a 'Decryption keys' label and an 'Edit...' button.