

## Assignment 7 - Wireless Security

- This is an individual assignment and worth 20 points.
- This is due on Wednesday, November 29 at midnight.
- Apply the usual naming convention.

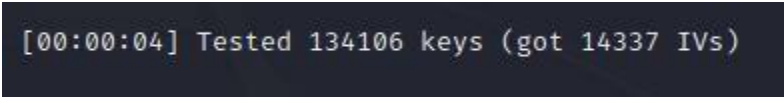
### Background

- This assignment is from National Cyber League (NCL) exercise. Use the attached “NCL-PCAP1.pcap”.
- You need to use Kali to answer the questions below. You can use your own Kali VM.
- When you use Proxmox, send the attached pcap file to the Kali on Proxmox. The file will be downloaded to the following directory: **/home/kali/Downloads**.
- Use **aircrack-ng** on Kali. Refer to the “CIS 480 Aircrack-ng.pptx” for ideas. You do not need to install aircrack-ng on Kali.
- You can find several websites that discuss “how to crack WEP with aircrack-ng.” For example, refer to: <https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-aircrack-ng-0147340/>.

### Tasks

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


**There are 14337 IVs in the packet capture.**



```
[00:00:04] Tested 134106 keys (got 14337 IVs)
```

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

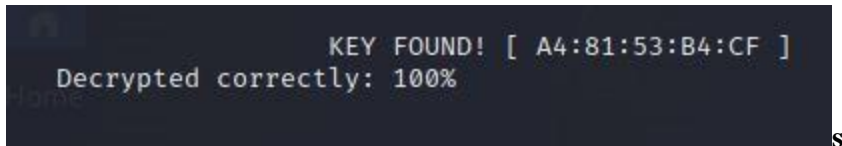
**The initialization vector of the first packet in the capture is 0x003a33**



```
0001 0000 0000 0000 - Sequence Number: 000
  Qos Control: 0x0000
  WEP parameters
    Initialization Vector: 0x003a33
    Key Index: 0
    WEP ICV: 0x9ad2e8d3 (not verified)
  Data (1508 bytes)
```

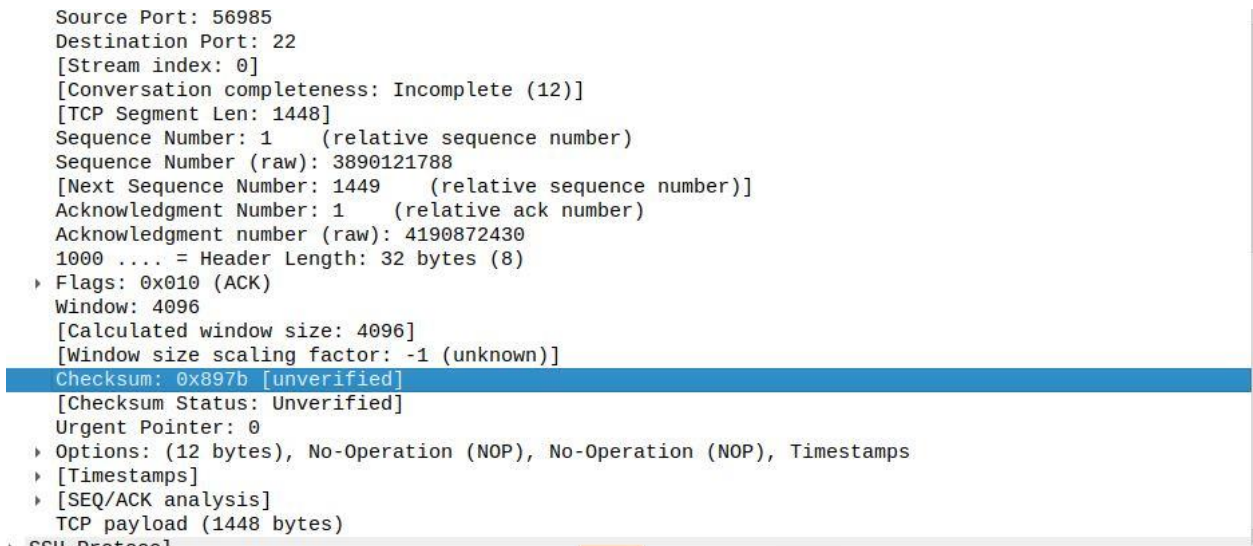
3. What is the key (i.e., password input) you obtained after running aircrack-ng? Provide a screenshot that supports your answer.

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



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

**The TCP checksum of the first packet of the capture is 0x897b.**



- How to decrypt the capture?
  - Go to Wireshark > Edit > Preferences > IEEE 802.11 > ...

