

## Assignment 7 - Wireless Security

- This is an individual assignment and worth 20 points.
- This is due at 2:30 (sec01) or 5:30 (sec76) on Tuesday, November 29.
- 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. Send the attached pcap file to your email and download from Kali using Firefox. The file will be downloaded to the 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**.

14337 IVs

```
(root@kali)-[~/Downloads]
└─# aircrack-ng NCL-PCAP1.pcap
Reading packets, please wait ...
Opening NCL-PCAP1.pcap
Read 14500 packets.

# BSSID          ESSID          Encryption
1 C0:4A:00:80:76:E4  WEP (14337 IVs)

Choosing first network as target.

Reading packets, please wait ...
Opening NCL-PCAP1.pcap
Read 14500 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.

AirCrack-ng 1.6

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

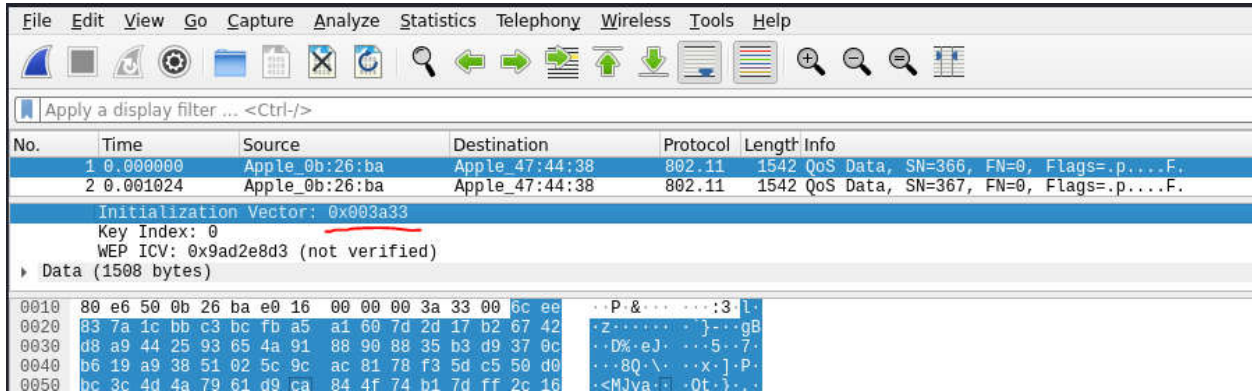
KB  depth  byte(vote)
0   1/ 3    A4(20736) 81(19968) DE(19200) 65(18944) F9(18944) 97(18688)
1   1/ 11   81(19200) 4C(19200) D0(18944) 47(18432) A6(18176) BE(18176)
2   2/ 26   53(18944) 73(18432) A0(18432) BE(18432) C6(18432) 21(18432)
3   4/ 9    B4(18944) 10(18688) 2D(18432) 4B(18432) D8(18432) 19(18176)
4  12/ 18  15(17408) 34(17152) 46(17152) 51(17152) 7D(17152) FB(17152)

KEY FOUND! [ A4:81:53:B4:CF ]
Decrypted correctly: 100%

└─(root@kali)-[~/Downloads]
```

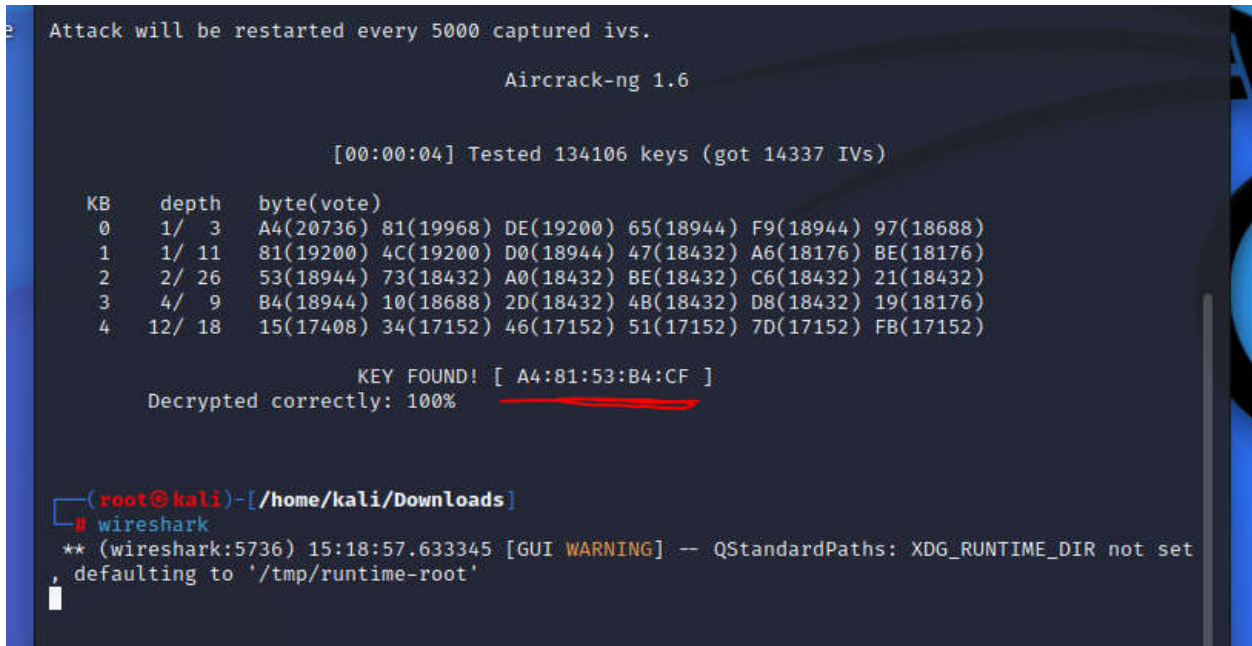
2. What is the IV in the first packet in the capture (in hex)? Provide a screenshot that supports your answer.

0x003a33



3. 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



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.

0x897b

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.101	192.168.0.102	SSH	1542	Client: Encrypted packet (len=1448)
2	0.001024	192.168.0.101	192.168.0.102	SSH	1542	Client: Encrypted packet (len=1448)
3	0.001024	192.168.0.101	192.168.0.102	SSH	1542	Client: Encrypted packet (len=1448)
4	0.001534	192.168.0.101	192.168.0.102	SSH	1542	Client: [TCP Previous segment not captured]
5	0.002048	192.168.0.101	192.168.0.102	TCP	1542	[TCP Out-Of-Order] 56985 → 22 [ACK] Seq=
6	0.005121	192.168.0.102	192.168.0.101	TCP	94	22 → 56985 [ACK] Seq=41 Ack=4294954265 W
7	0.005121	192.168.0.102	192.168.0.101	TCP	94	22 → 56985 [ACK] Seq=41 Ack=4294957161 W
8	0.005632	192.168.0.101	192.168.0.102	TCP	1542	[TCP Retransmission] 56985 → 22 [ACK] Seq=
9	0.006145	192.168.0.102	192.168.0.101	TCP	94	22 → 56985 [ACK] Seq=41 Ack=4294960057 W
10	0.006654	192.168.0.101	192.168.0.102	SSH	1542	Client: [TCP Previous segment not captured]
11	0.006657	192.168.0.102	192.168.0.101	TCP	94	22 → 56985 [ACK] Seq=41 Ack=4294962953 W
12	0.008704	192.168.0.101	192.168.0.102	TCP	1542	[TCP Out-Of-Order] 56985 → 22 [ACK] Seq=
13	0.008702	192.168.0.101	192.168.0.102	SSH	1542	Client: Encrypted packet (len=1448)
14	0.008702	192.168.0.101	192.168.0.102	SSH	1542	Client: Encrypted packet (len=1448)
15	0.008702	192.168.0.101	192.168.0.102	SSH	1542	Client: Encrypted packet (len=1448)
16	0.008704	192.168.0.101	192.168.0.102	TCP	1542	[TCP Out-Of-Order] 56985 → 22 [ACK] Seq=
17	0.009213	192.168.0.101	192.168.0.102	SSH	1542	Client: Encrypted packet (len=1448)
18	0.009725	192.168.0.101	192.168.0.102	SSH	1542	Client: Encrypted packet (len=1448)
19	0.010751	192.168.0.102	192.168.0.101	TCP	94	22 → 56985 [ACK] Seq=41 Ack=4294948473 W
20	0.010753	192.168.0.102	192.168.0.101	SSH	134	Server: Encrypted packet (len=40)

Transmission Control Protocol, Src Port: 56985, Dst Port: 22, Seq: 1, Ack: 1, Len: 1448

Source Port: 56985  
Destination Port: 22  
[Stream index: 0]  
[Conversation completeness: Incomplete (12)]  
[TCP Segment Len: 1448]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 3890121788  
[Next Sequence Number: 1449 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 4190872430  
1000 ... = Header Length: 32 bytes (8)  
Flags: 0x010 (ACK)  
Window: 4096  
[Calculated window size: 4096]  
[Window size scaling factor: -1 (unknown)]  
Checksum: 0x897b [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps  
[Timestamps]

```

0020 e7 de 8c 3c f9 cb a3 6e 80 10 10 00 89 7b 00 00  ...<...n ...{...
0030 01 01 08 0a 12 7d 62 e1 00 06 1c f9 06 92 7b d2  ....}b .....{.

```

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

