Wireless Access Exploitation

PCAP 1 (Easy)

This challenge evaluates the contestant's ability to crack WEP encryption given a packet capture. The aircrack-ng Linux tool can be used to solve this challenge.

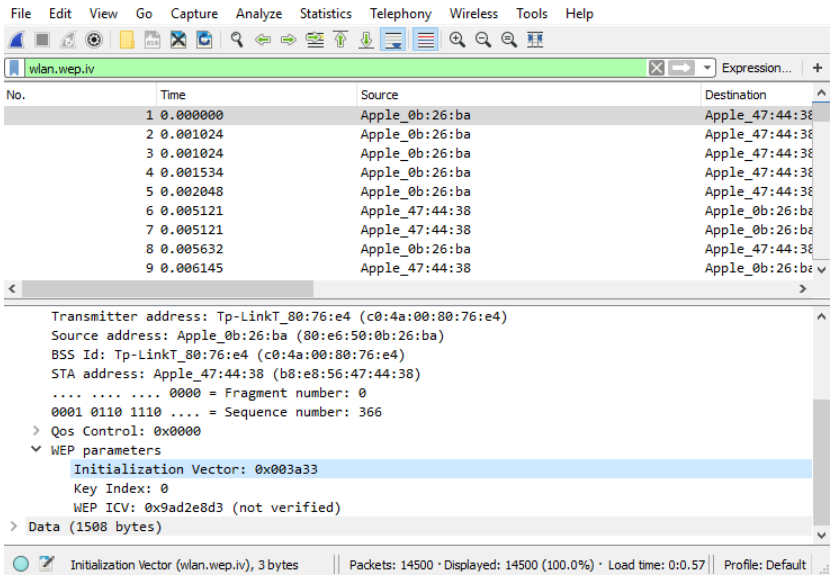
Questions 1, 2, and 4 can be solved by simply running aircrack-ng on the packet capture. The summary lists the number of IVs that were found in the packet capture along with the WEP key. The key size can be determined by counting the number of bits in the key text (5 bytes * 8 bits per byte = 40 bits) and comparing that to the possible WEP key sizes and configurations. Note: WEP keys are larger than the password input size.

```
aircrack-ng NCL-2015-WIFI1.pcap
```

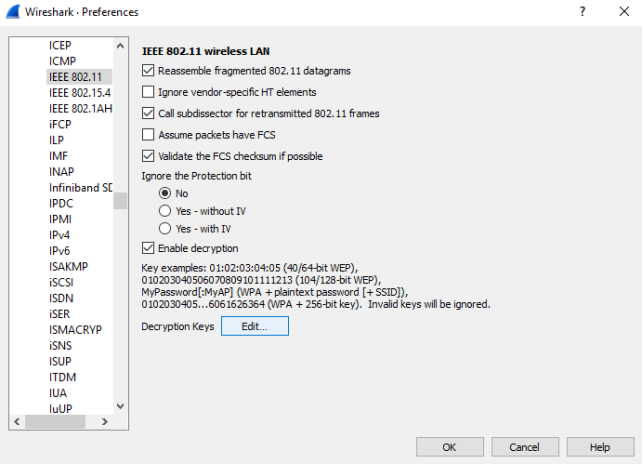
© 2017 Cyber Skyline. All Rights Reserved.
Unauthorized reproduction or distribution of this copyrighted work is illegal.

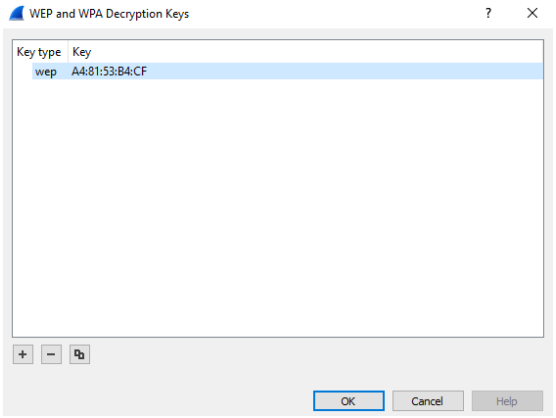
Question 3 can be solved by viewing the packet capture in Wireshark and using the following filter:

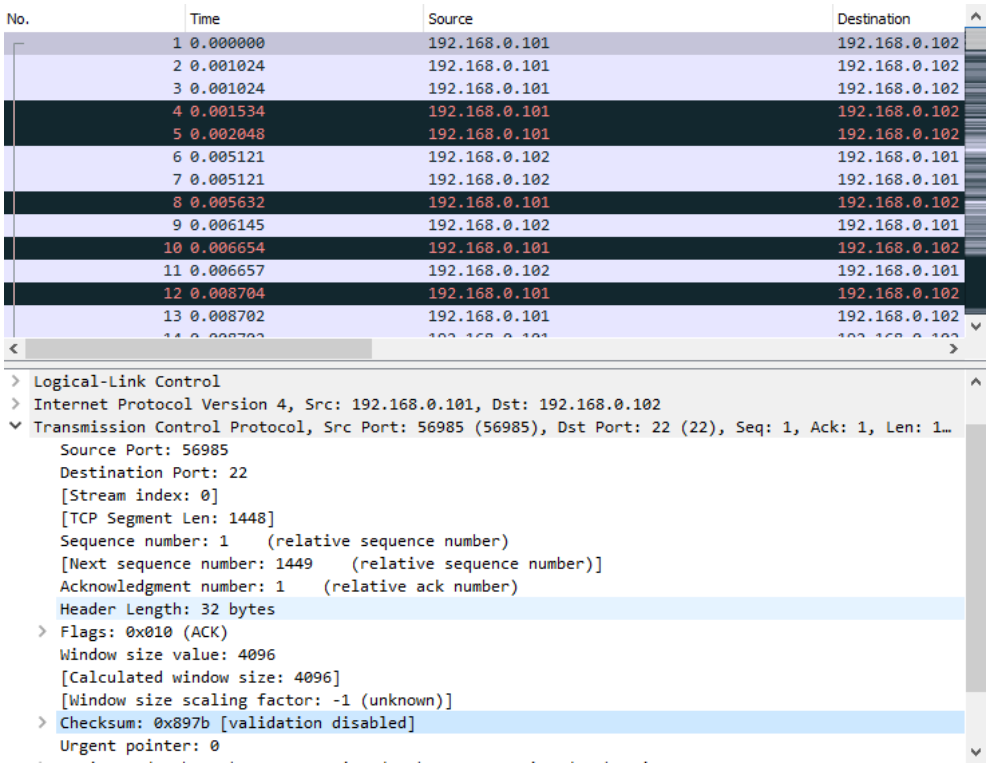
```
wlan.wep.iv
```



Question 6 can be solved by using the previously acquired WEP key to decrypt traffic in Wireshark. This can be done by selecting “Edit > Preferences > Protocols > IEEE 802.11” and then checking “Enable decryption” and adding the decryption key.







© 2017 Cyber Skyline. All Rights Reserved.
Unauthorized reproduction or distribution of this copyrighted work is illegal.

Question	Answer
How many IVs are in the packet capture?	14337
What is the key size of the wireless network in bits?	64
What is the IV for the first packet in the capture (in hex)?	0x003a33
What is the WEP key?	A4:81:53:B4:CF
What is the TCP checksum of the first packet in the capture (in hex)?	0x897b

© 2017 Cyber Skyline. All Rights Reserved.
Unauthorized reproduction or distribution of this copyrighted work is illegal.