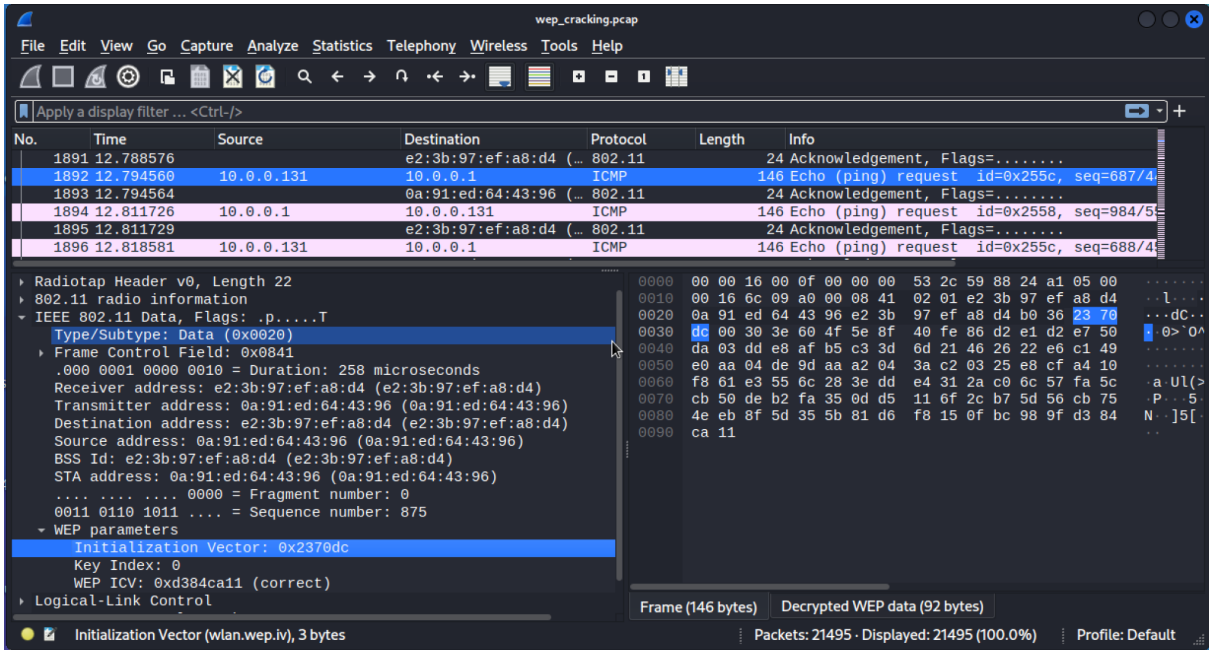
1. **Which protocols do you observe after decrypting WEP network traffic in Wireshark? (0.5 points)**
    a. ICMP
    b. ARP
    c. 802.11
2. **Using Wireshark, how can you tell a packet uses WEP encryption? Add a screenshot showing an IV. (0.5 points**)

On observing the pcap file for IEE802.11 decrypted data, it is observed that the 802.11 protocol frame has WEP parameters which implies that the packet is using WEP encryption. Please check the screenshot above. IV is highlighted as well.

3. **How many packets would one have to capture to recover the WEP encryption key? (0.5 points)**

Strength of WEP is from the randomization of IV because all the clients in the AP network share the same key. But IV is only 24 bits in the 64 bit key and that translates to 2^24 or roughly 16 million packets. But according to the birthday paradox and related key attacks, It is estimated that 20,000 IVs are enough to crack WEP in the 64 bit key and 40,000 IVs are encough to crack WEP in 128 bit key using PTW technique in air-crack ng. Please check the link below.

https://www.aircrack-ng.org/doku.php?id=faq#how_many_ivs_are_required_to_crack_wep



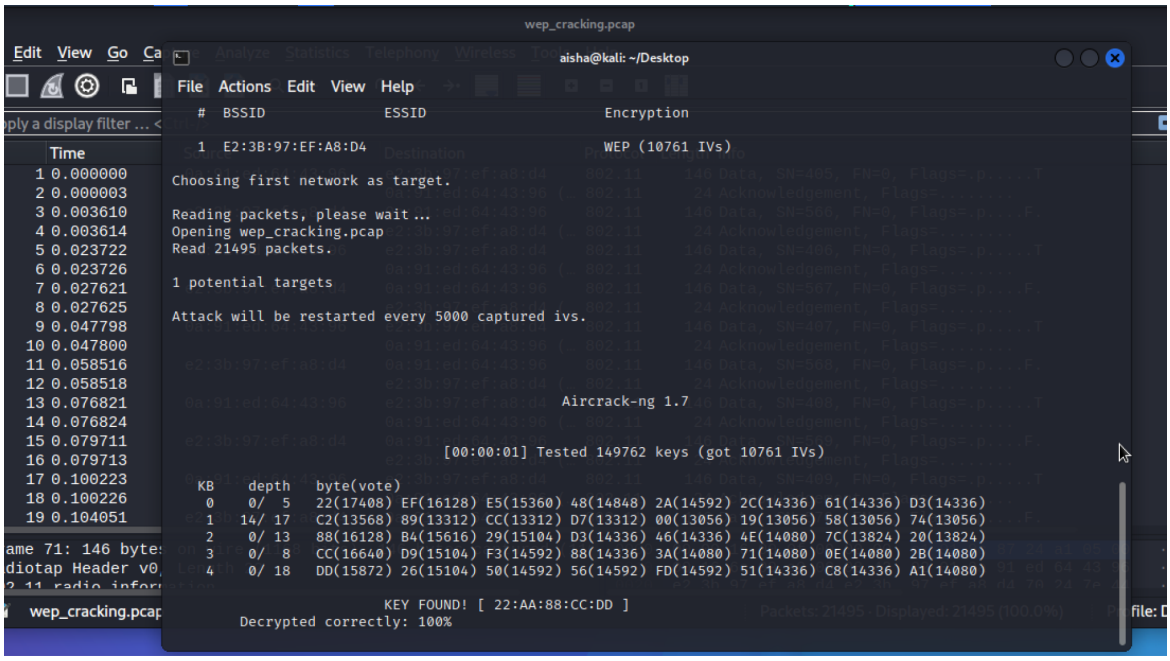
4. **For WEP attack, what could you do to reduce the time needed to capture a sufficient number of IVs? (0.5 points)**

1. **Increasing the number of new IVs generated**: ARP request-replay attacks available in Aircrack-ng can be used to generate new IVs and thereby reduce the

time needed to capture sufficient number of IVs. Cafe Latte attack also works in a very similar way, modifying the ARP packets to generate new IVs and thereby reducing the time needed to crack WEPs.
https://www.aircrack-ng.org/~~v:/doku.php?id=arp-request_reinjection
https://www.aircrack-ng.org/~~v:/doku.php?id=cafe-latte

2. **Using powerful wireless adapter** to capture signals from a greater distance that will allow us to capture more IVs in a shorter period of time.
3. **Targeting specific clients or access points**: By targeting specific clients or access points that are active on the network, the likelihood of capturing packets with unique IVs can be increased as each client or access point generates its own sequence of IVs, which can increase the chances of capturing a sufficient number of unique IVs in a shorter amount of time.

5. **What is the WEP password that you recovered? (0.25 points)**
   Key : 22:AA:88:CC:DD



6. **What is a limitation of the WEP based attack? (0.5 points)**

WEP is an outdated protocol and not many devices use it anymore and most devices have switched to WPA2 or 3. WEP attack doesnt work on WPA2 or WPA3 devices.

7. How many 4-way handshakes do you need to capture to crack WPA-2 and why? (0.5 points)
Cracking WPA-2 involves brute-forcing the PSK and not capturing any specific number of handshakes or IVs like WEP. We are only limited by the computational power and strength of the password and not a number of handshakes.

8. How would you relate the security (or entropy, or unguessability) of a password with regards to a list of passwords? (0.5 points)
In techniques such as cracking WPA/WPA2, the adversary is only limited by the computational power and strength of the password. Since we can't control the computational power of the attacker, it is very important to have a strong password that has characteristics such as long length, using special characters and not using common words and terminologies.
Using good wordlists(password files) can improve the chances of breaking WPA2 greatly.

Aircrack-ng says 63 character password with special characters is effectively impossible to brute force. But thats only in 2010.

Please find the source below. https://www.aircrack-ng.org/doku.php?id=cracking_wpa
9. What is the WPA-2 password that you recovered? (0.25 points)

treasure

10. Demonstrate deauthentication attack to any of the TAs. (0.5 points)

Demonstrated after much difficulty 🙃

11. How does the official patch mitigate the demonstrated deauthentication attack 14? (0.5 point)

Updating to wpa_supplicant/hostapd v2.10 or newer.
A better source address validation check has to be added to prevent the de-auth attack demonstrated in the class. Typically checking for incorrect source addresses such as broadcast addresses have to be filtered out to prevent such attacks.

The link for the patch given in the assignment addresses the potential denial of service cases that can occur when an unprotected frame causes an AP to send a response to another device, which then processes the unexpected response. It modifies the code to silently ignore management frames from unexpected source addresses so that the software does not add any state for unexpected STA addresses or send out frames to unexpected destinations. The patch checks the source address of the received management frame and ignores the frame if it has an unexpected or invalid source address, such as a multicast address, a zero address, or an address that matches the AP's address. By doing this, the patch prevents a potential denial of service attack where the unexpected response frame from the AP might result in a connected station dropping its association. The link specifying the patch: https://w1.fi/security/2019-7/0001-AP-Silently-ignore-management-frame-from-unexpected-.patch