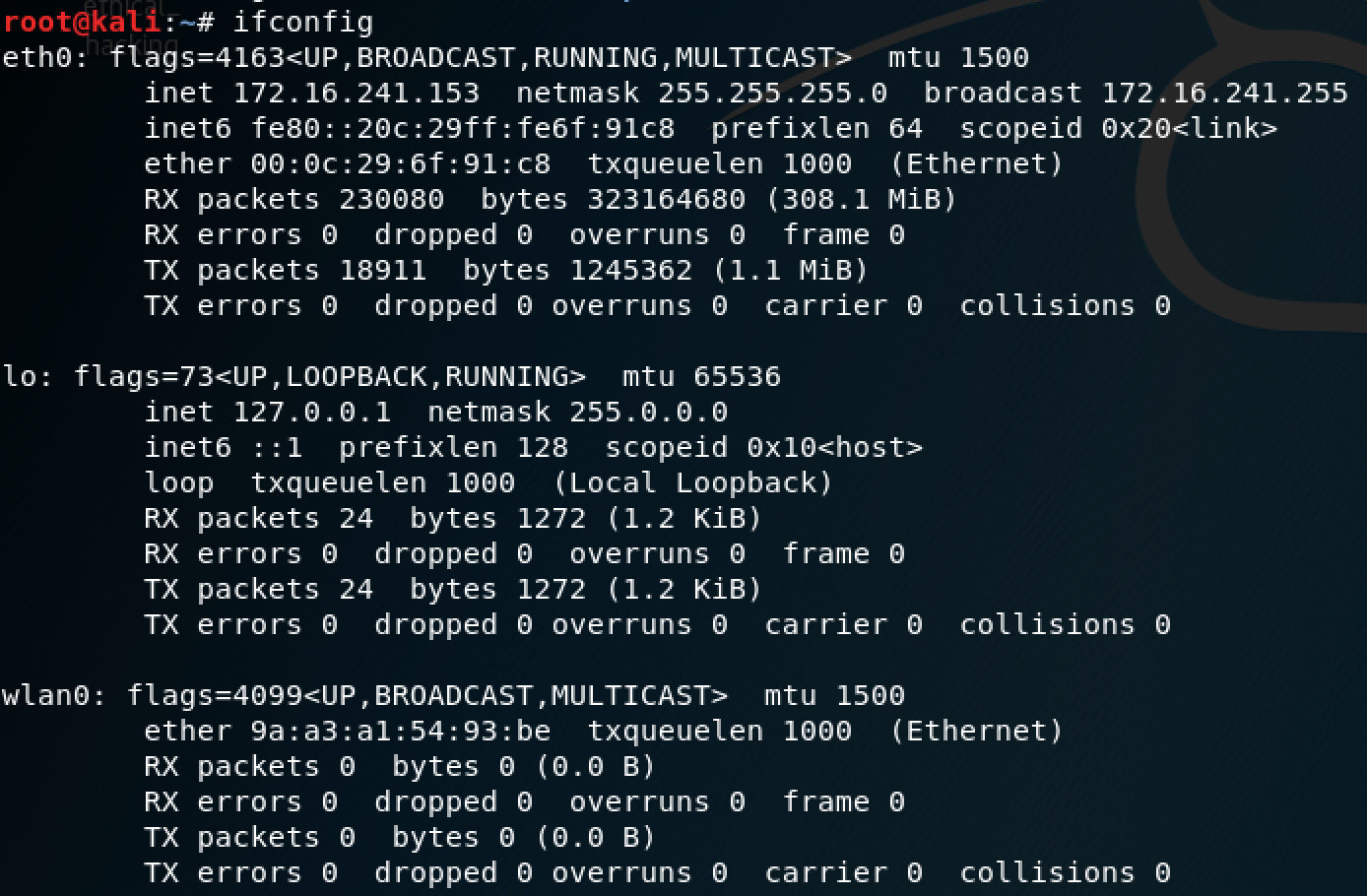
Jay Chow, Nihal Shah, Wu Guan Long, Shivani Deshpande, Abdullah Alghofaili

EN.650.431 Ethical Hacking Home Work #4

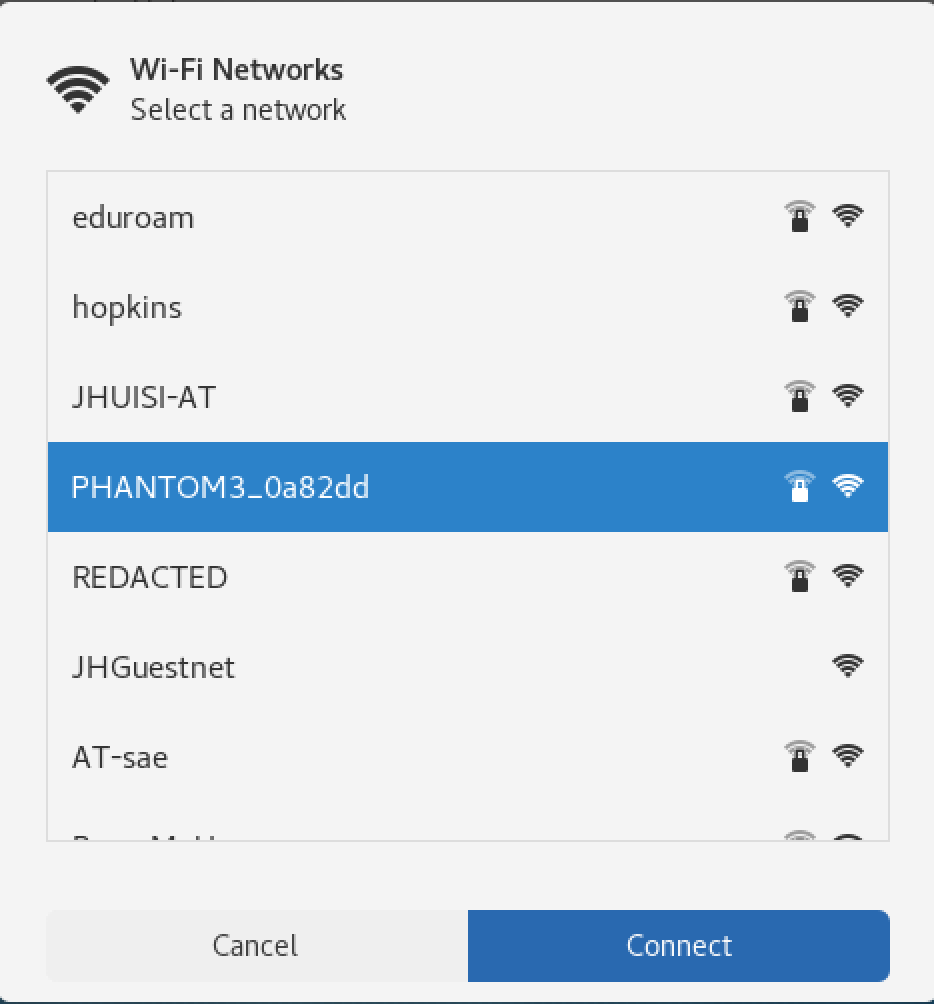
2nd April 2019

1. Focusing on the wireless connection between the DJI Phantom 3 and its controller(smartphone running the DJI Go Application), use Wireshark to analyze this interaction and technically document it:

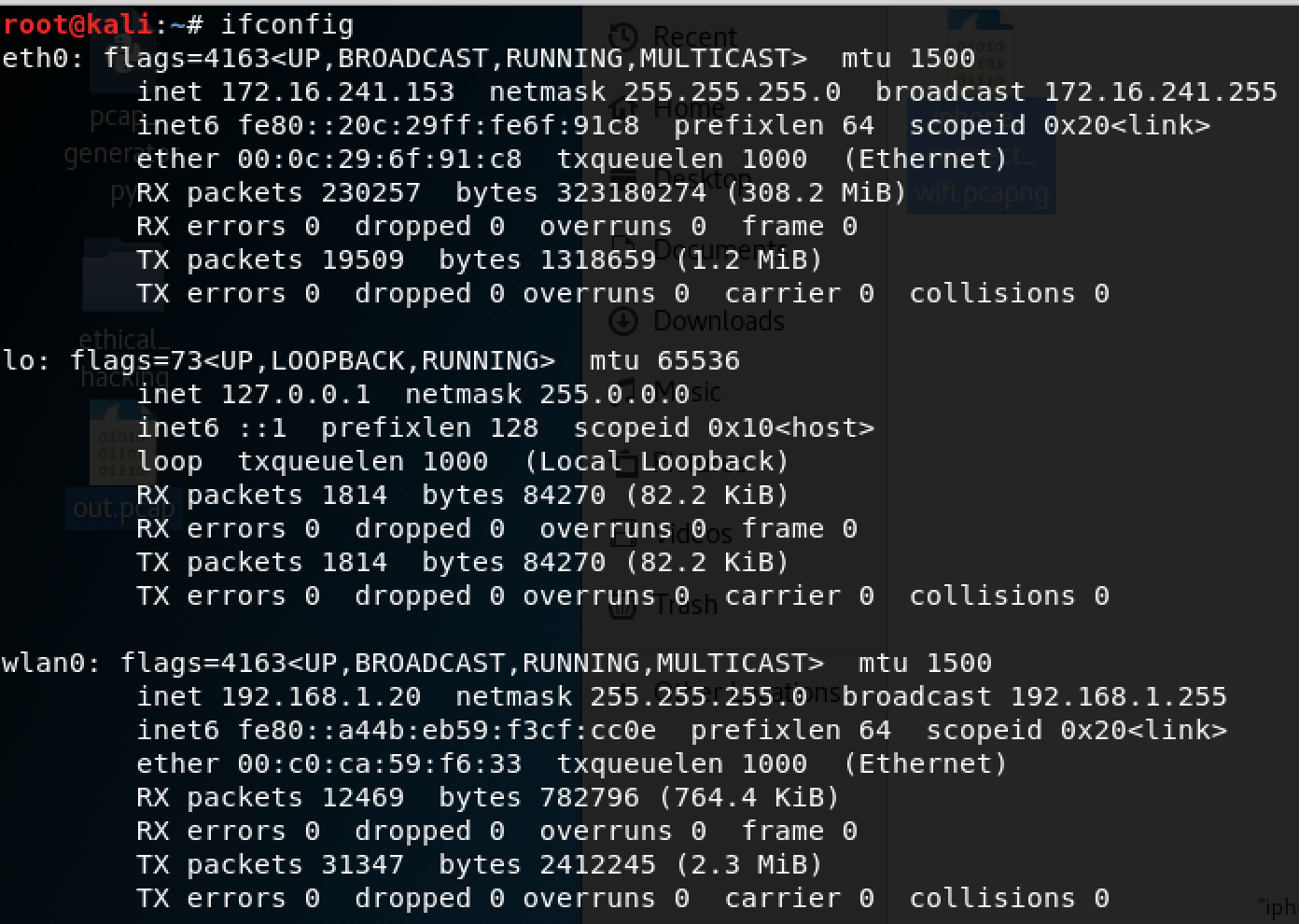
Before connecting to the white controller’s AP:



Now, on the next page, my Kali will connect to the AP in the white controller using the password 12341234(in the user manual). If the password is changed, we need to crack the WPA2 password by using airodump-ng. Note that the controller creates a wireless network, not on the physical drone itself:



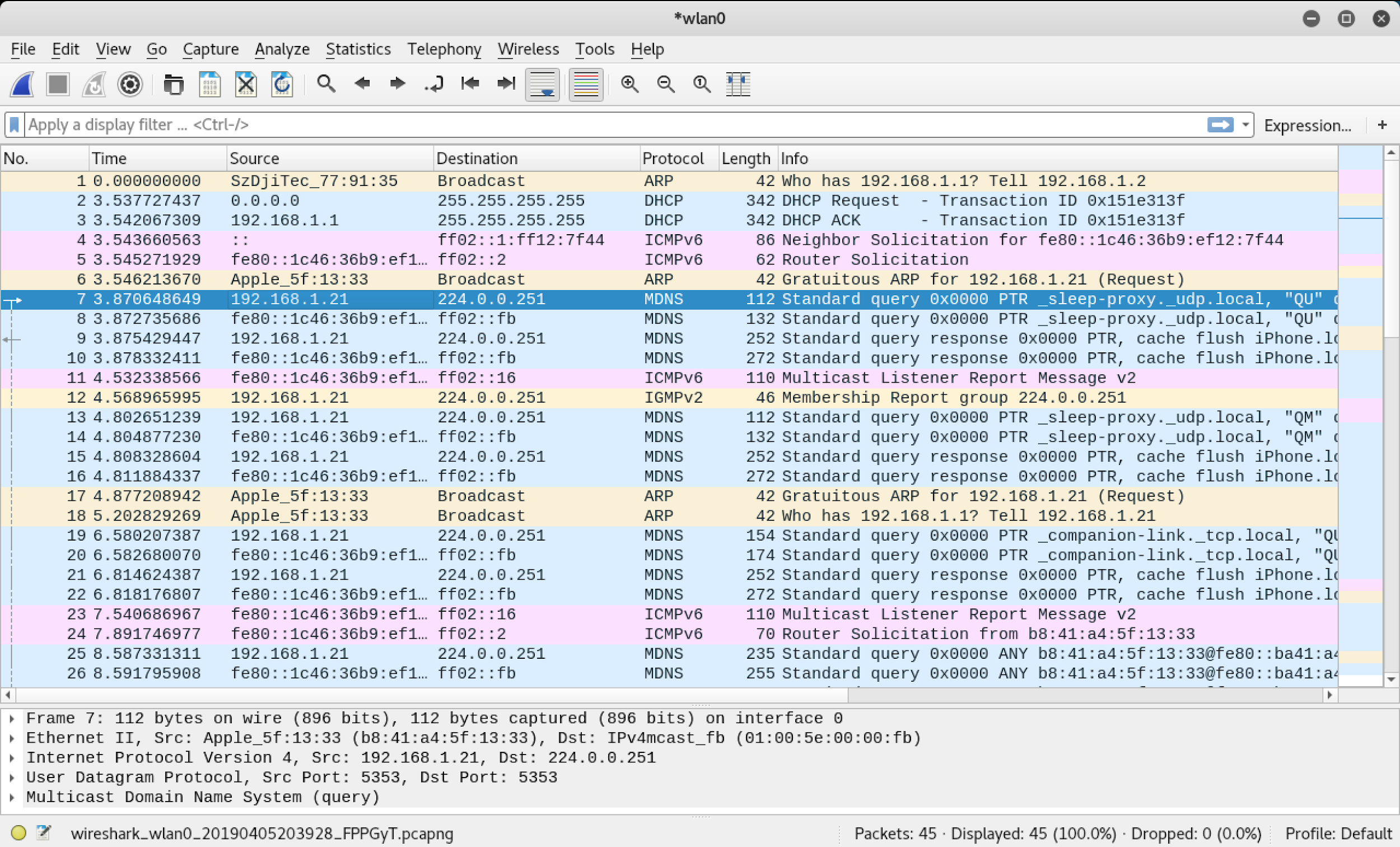




Now that the Kali Linux also has an IP after connecting to the white controller’s AP, which is 192.168.1.20.

So now, we will run wireshark on wlan0 on the Kali to capture the handshake between the phone and the white controller. Now, we will connect the iphone phone to the WLAN created by the white controller.

This was captured on wireshark when my iPhone connected to the drone via the DJI Go app:



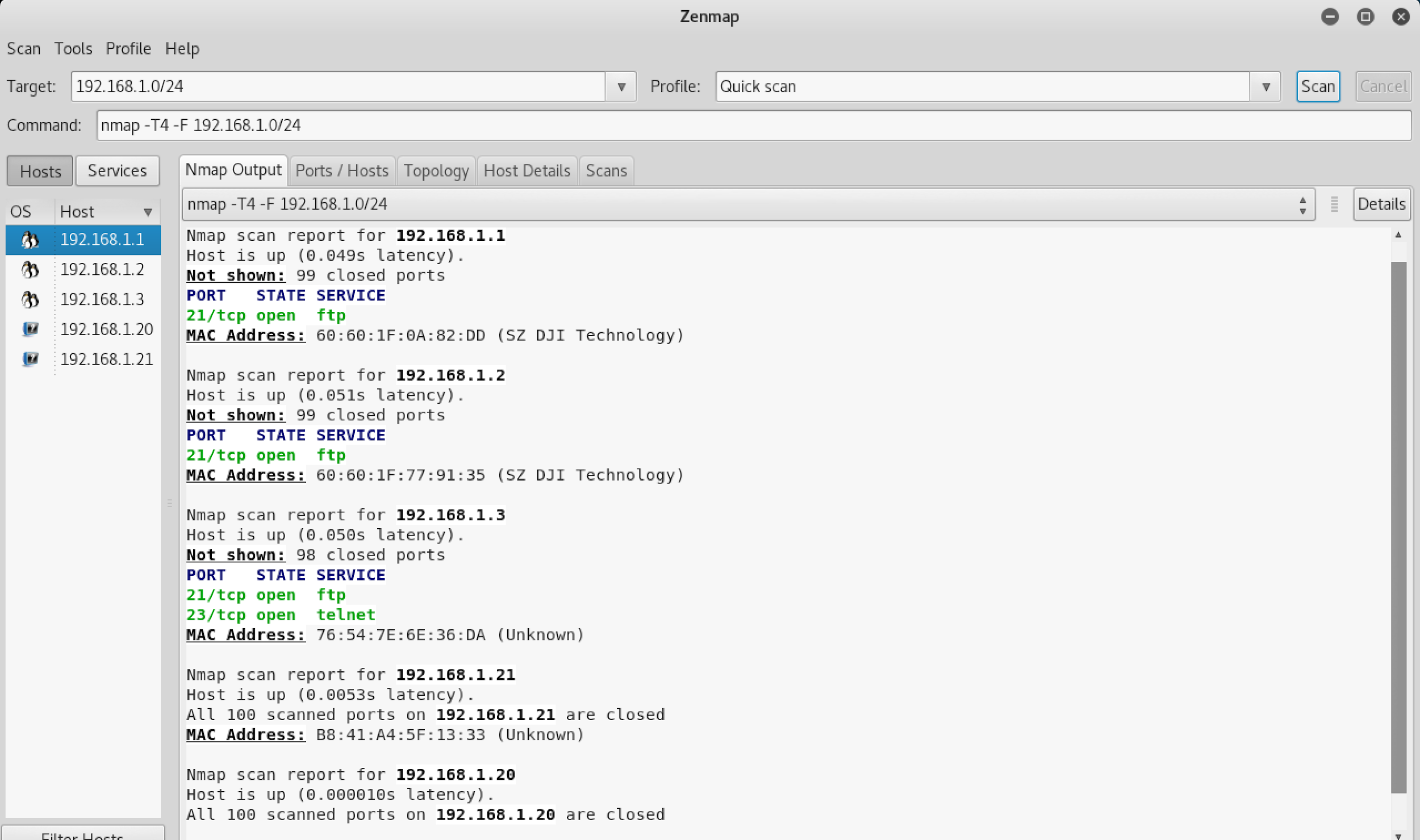
On my iPhone after connecting the PHANTOM3\_0A82dd wifi network and going into the DJI GO app:



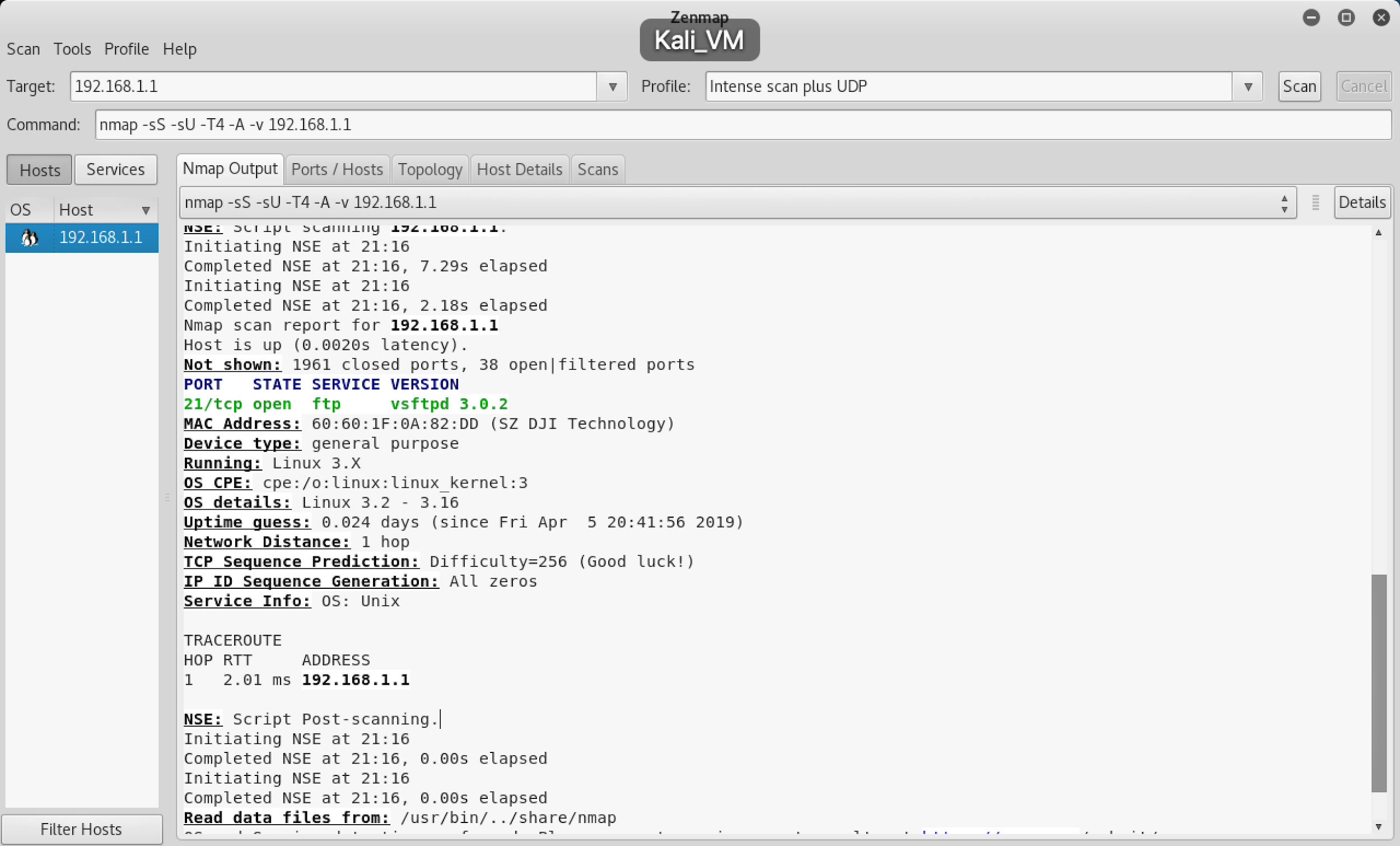
Note that my iPhone’s private IP is 192.168.1.21

1. What are ALL the IPs associated with DJI P3?

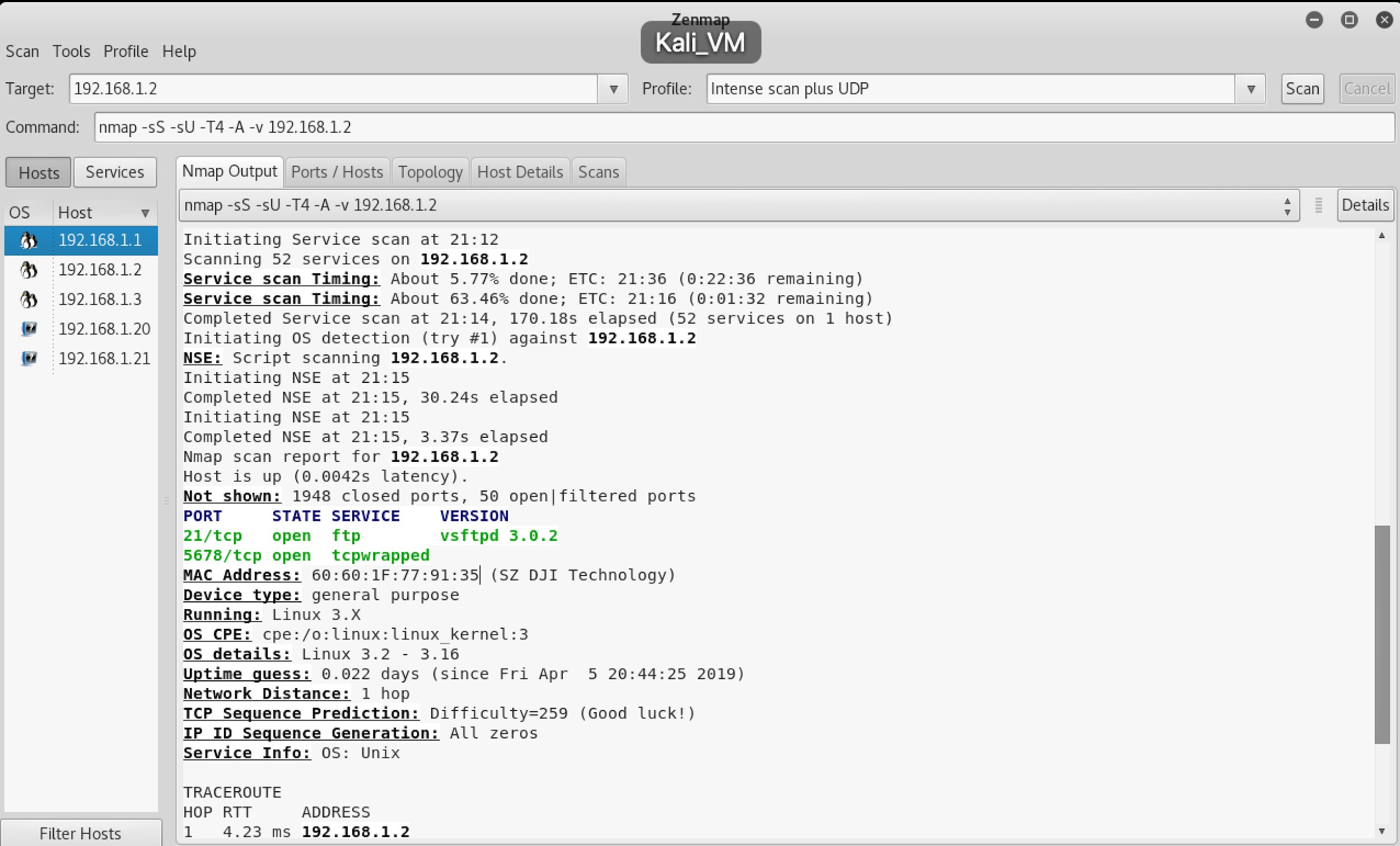
Now, we find ALL devices on the wireless network using zenmap:



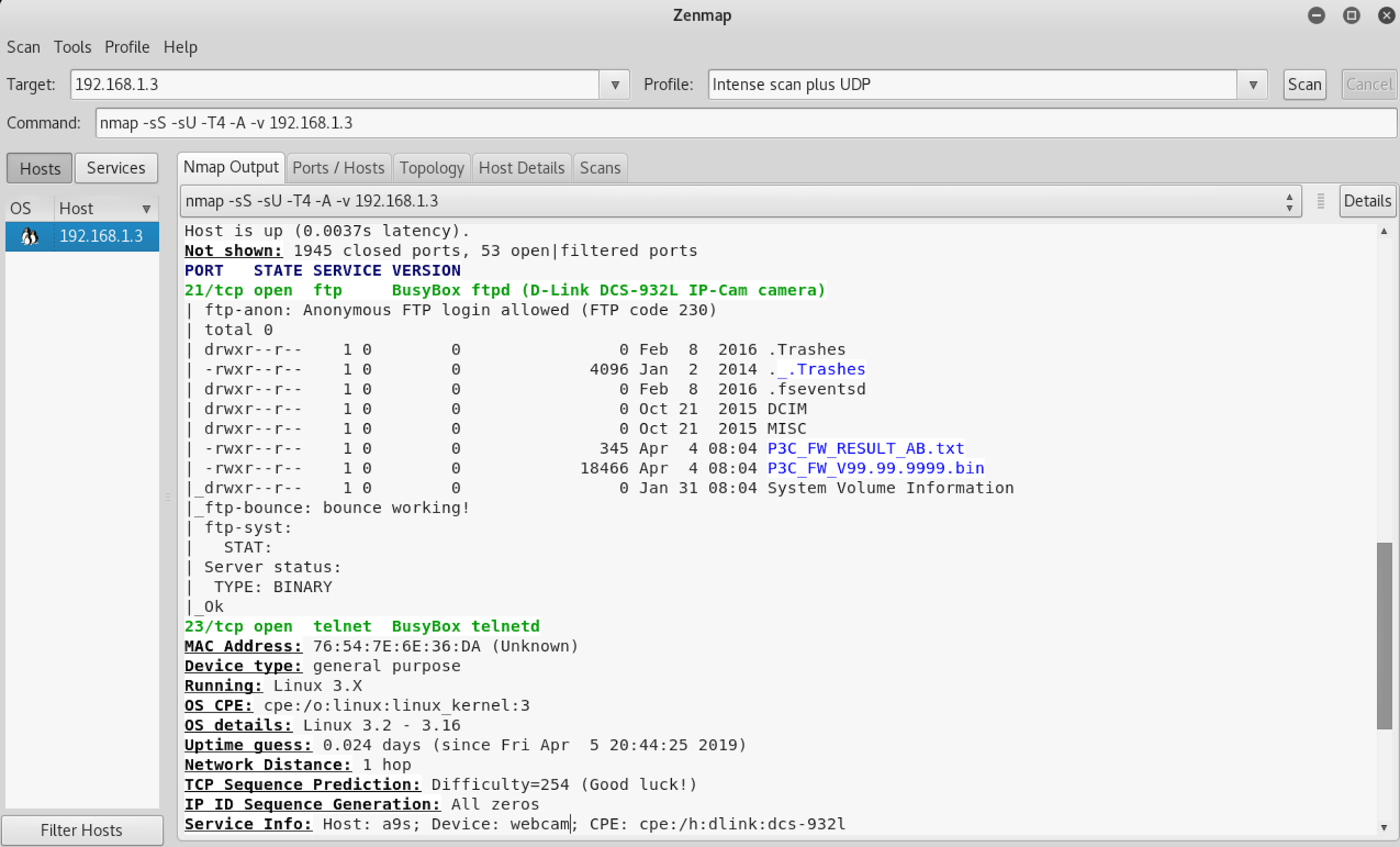
We found a total of 5 IPs in the wireless network, as shown above. Recall that .20 is my Kali box and .21 is my iPhone. As such, I will do an intense scan on .1, .2, .3:



As shown on my previous page, we know that this belong to the white controller as we matched the MAC address from zenmap to the MAC address that was pasted on the controller.



We matched this MAC address to the MAC address pasted on the drone. This IP was the drone’s IP.



Since we see the word “webcam” under Service Info, this was the IP of the camera on the drone.

1. What are ALL the open ports on ALL the IP addresses on the DJI P3?

If we are only looking at the DJI P3 Drone itself(192.168.1.2), the open ports from part (a) indicate 21(ftp) and 5678(tcpwrapped). If we look at the camera on the drone(192.168.1.3), the open ports from part(a) are 21(ftp) and 23(telnet). If we look at the controller(192.168.1.1), the open port from part (a) is 21(ftp)

1. What operating systems does the DJI P3 use?

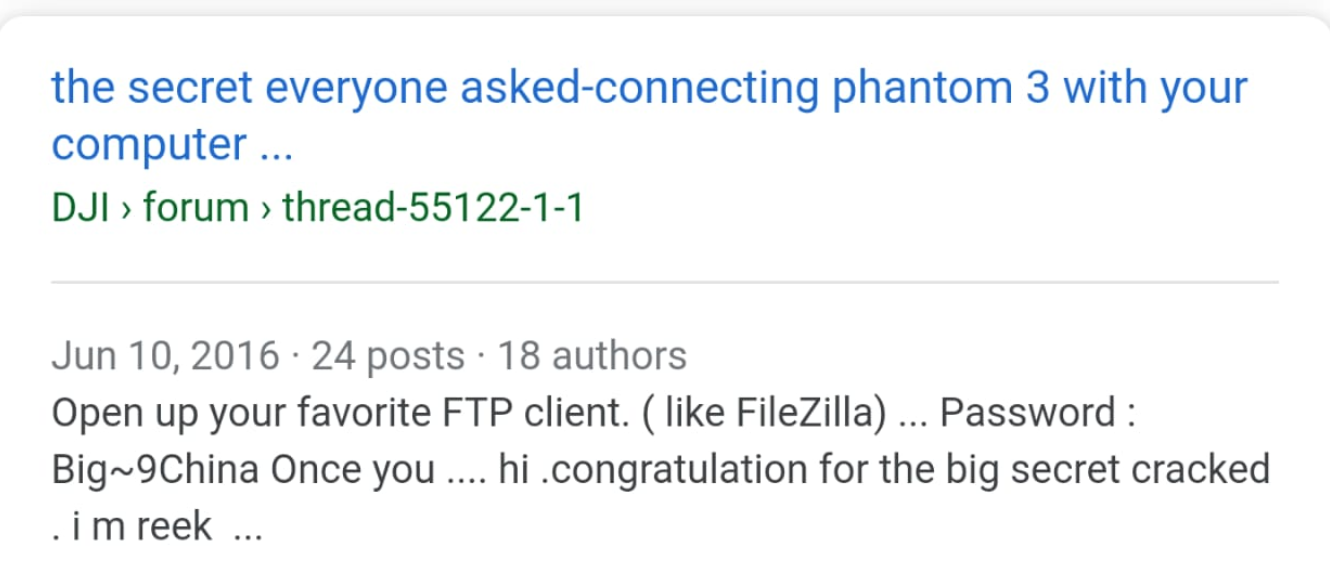
If we are only looking at the DJI P3 Drone itself(192.168.1.2), the OS from part (a) indicate Linux 3.2 - 3.16. If we look at the camera on the drone(192.168.1.3), the OS is Linux 3.2 - 3.16. If we look at the controller(192.168.1.1), the OS is also Linux 3.2 - 3.16

1. What services are running on ALL the IP addresses?

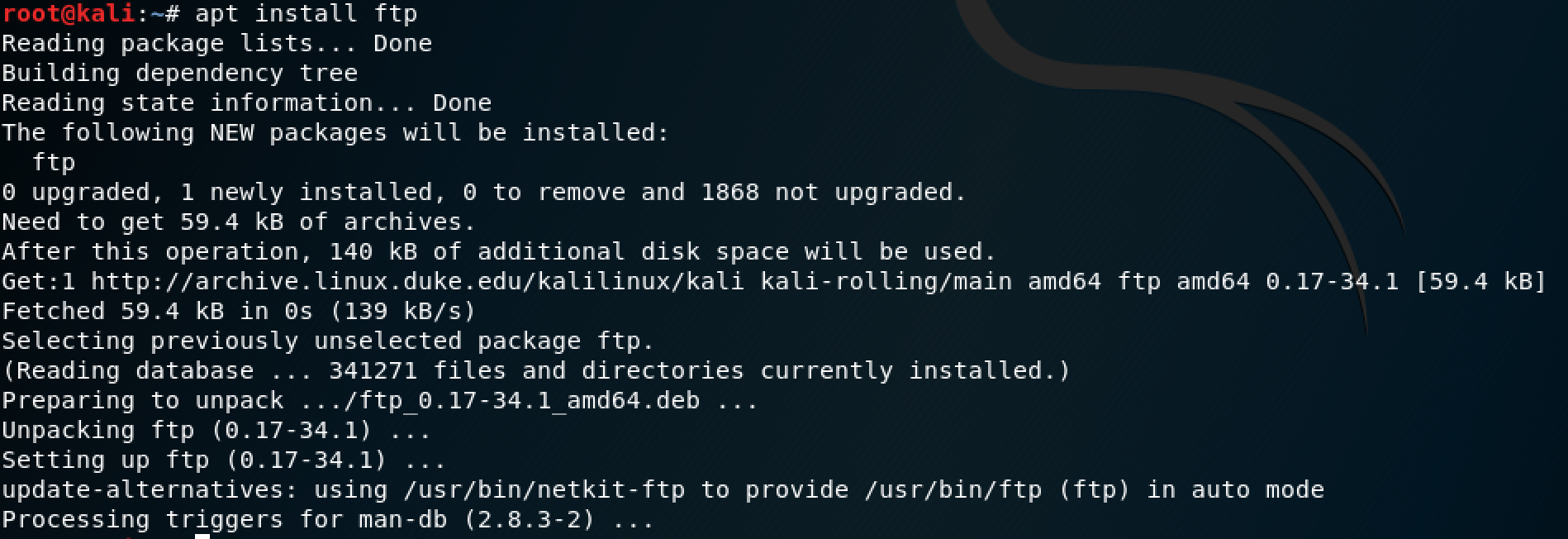
On the controller, ftp is running. For the camera on the drone, ftp and telnet are running. On the drone, ftp and tcpwrapped are running. For the controller, ftp is running on it.

2. How would you pull down the shadow file from the DJI P3?

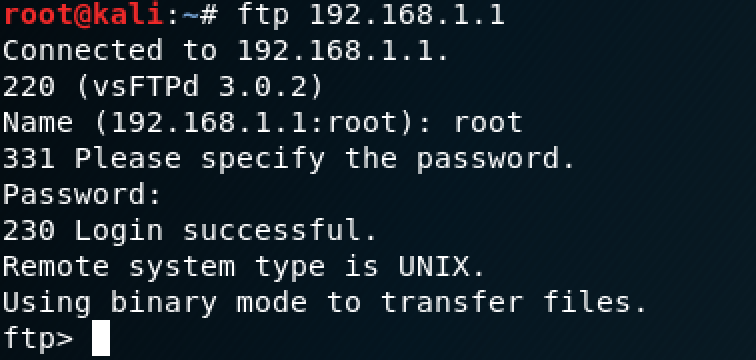
After some googling, we managed to find the ftp password online for the controller(192.168.1.1). As such, we attacked the ftp port 21 on the controller. We will connect to the ftp server on the controller. Note that we could ftp connect the drone as well.



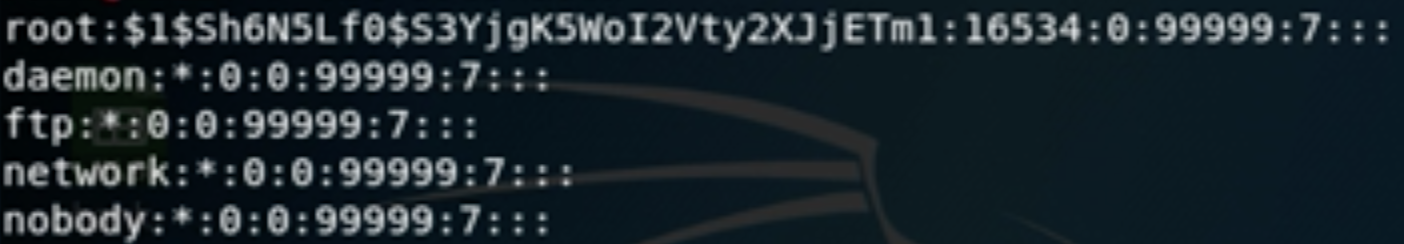
Now, we first had to install ftp on our kali:



Next, we managed to log into the control using ftp:

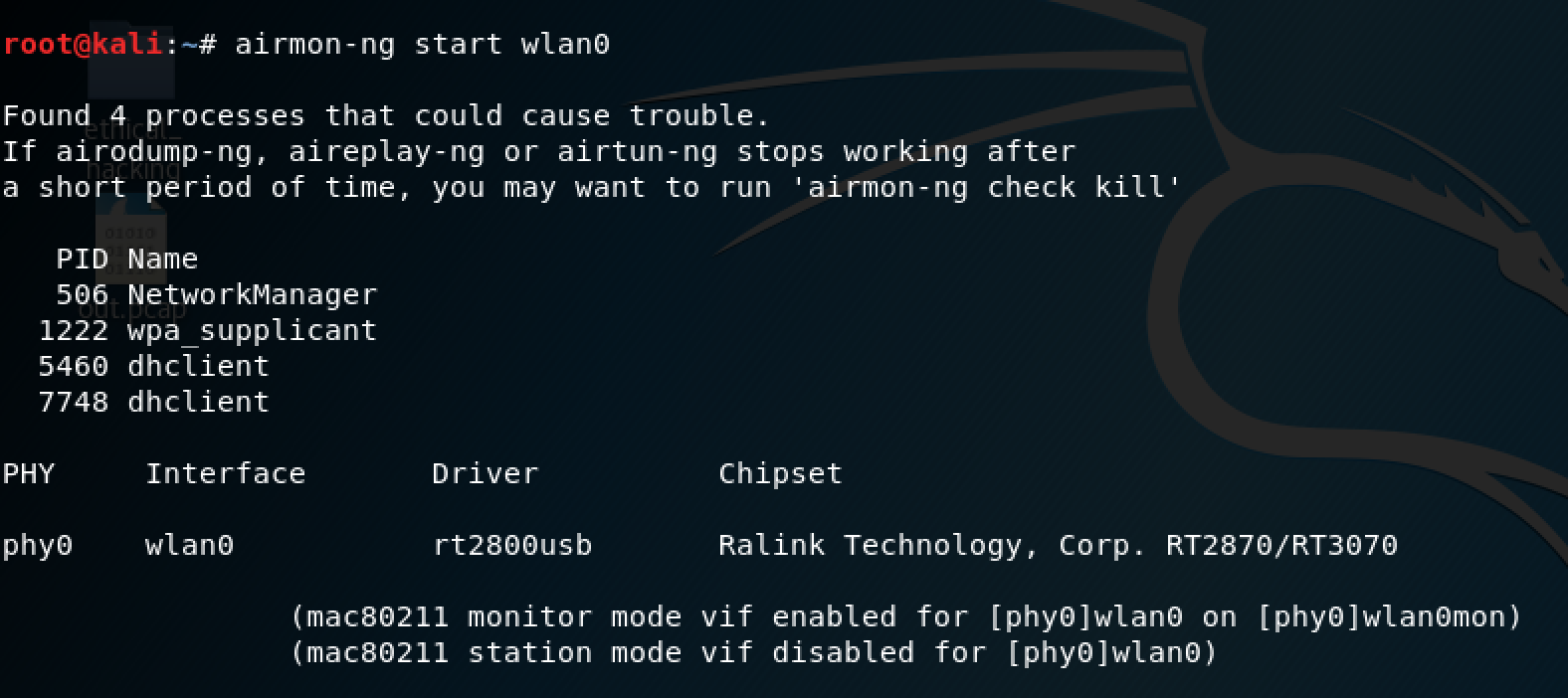


Now, we ran this command inside ftp: get ../etc/shadow ./shadow

When we exited out of ftp, and cat the file shadow on my local Kali, we can see the contents:

1. Find a weakness in the DJI P3 connection. Since we did a TCP replay using a MDNS packet within the same wireless network in the previous homework to attack the bebop drone, we will use an attack outside of the wireless network.

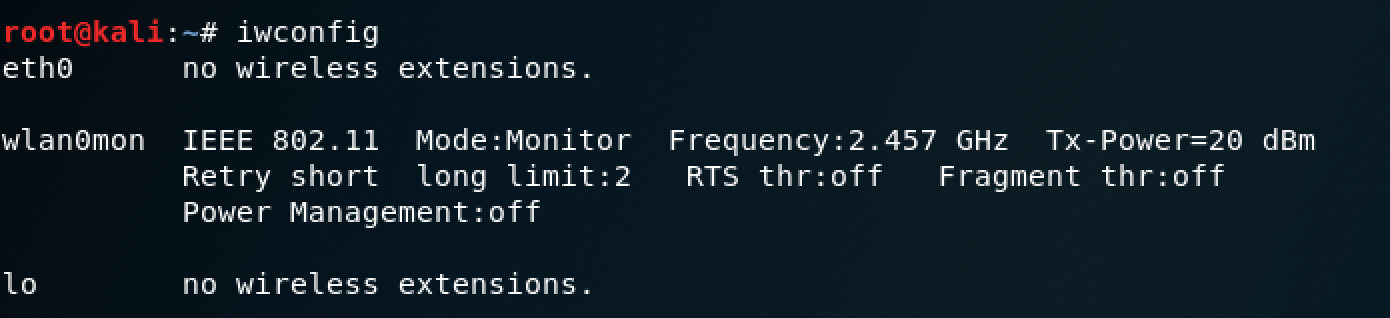
We first had to set up monitor mode on Kali using the command below:



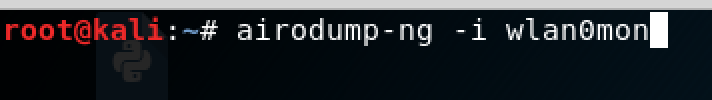
After we turned on monitor mode, we can see ALL access points within our radius. As shown below, wlan0mon is created, as a result:

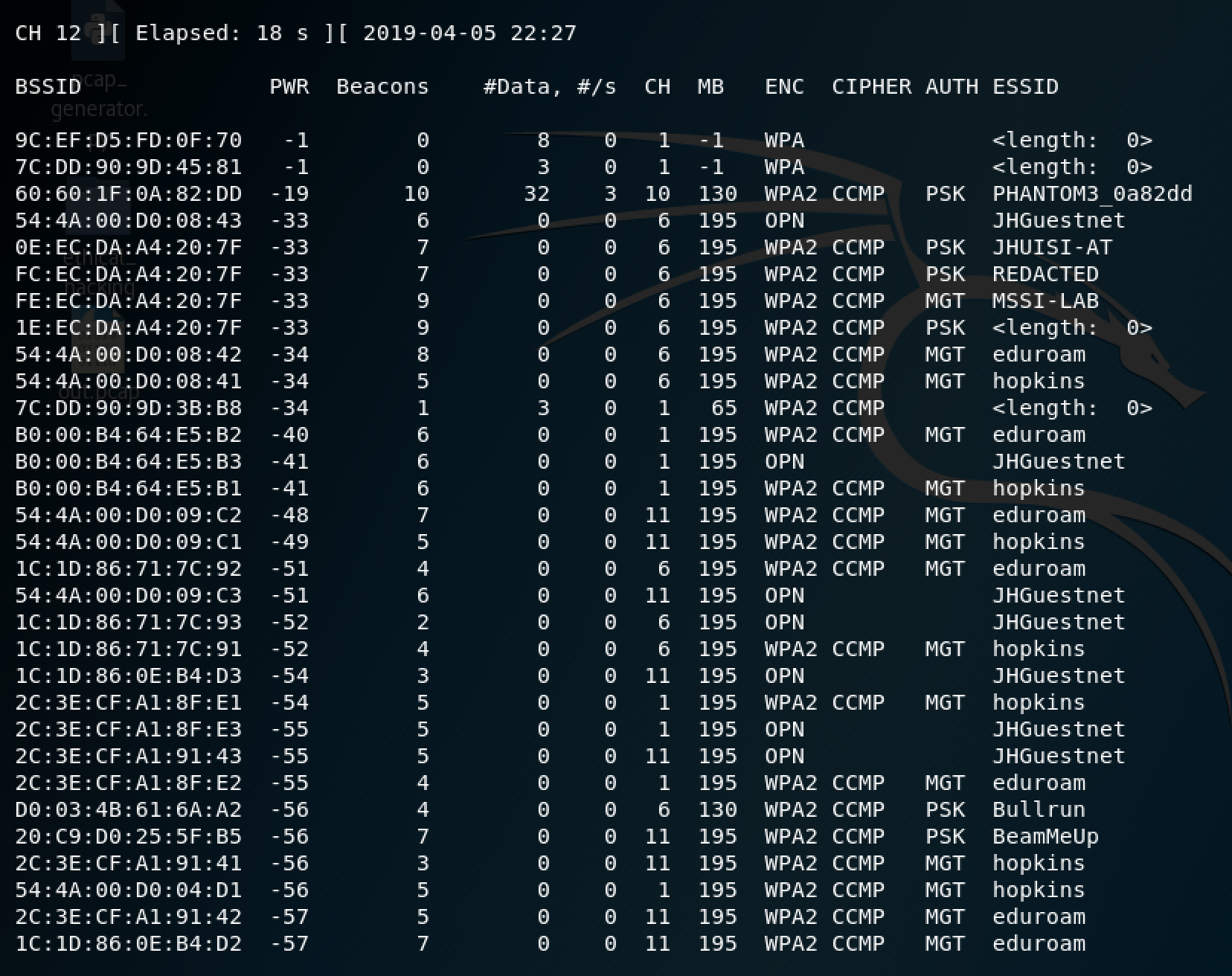


Also, we ran iwconfig:



Now, we had to find the MAC address of the access point and the associated channel to launch a final aireplay-ng de-authentication attack. First we ran airodump-ng on the monitor mode interface:



  
As shown from above, on the third line, the MAC address of PHANTOM3\_0a82dd is 60:60:1F:0A:82:DD, the channel is 10 and the encryption type is WPA2.

Now, we can conduct the aireplay-ng attack. The final attack will be demonstrated in the video attached with the homework assignment. Note that -a is the MAC address of the access point and -c is the MAC address of the drone. The drone still works but only the video streaming is not working.