CYSE425

Mahish Mahendarkar

11/10/2021

Drone Lab

Lab purpose:

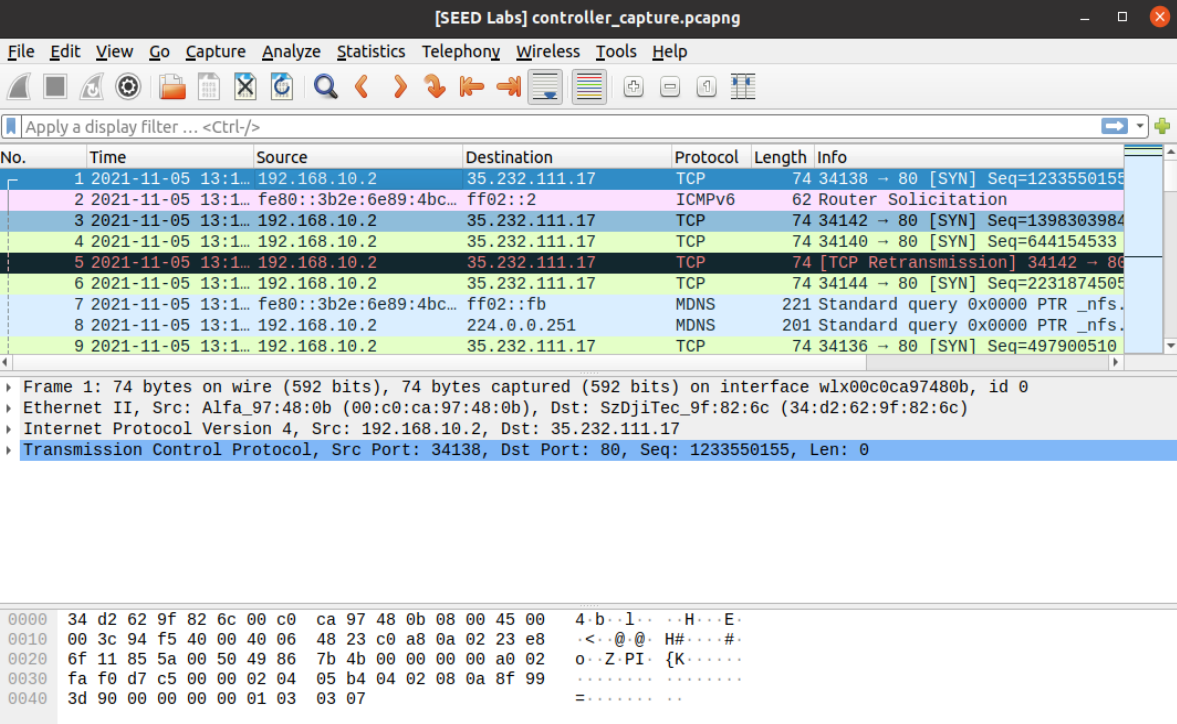
The purpose of this lab is to become familiar with drone controls, data streams and network settings.

Pre-Lab configuration settings:

* An arch linux VM was used for this lab. This lab was completed in collaboration with Zaine Wilson and Aidan Shaughnessy as Group 3 of the second session on Friday November 5th 2021.

Lab tasks:

1. Connect to the drone and capture network traffic.

****

**Q 3.1.1 [2.5 pts] What is the IP address of the drone?**

**192.168.10.1**

Text

Description automatically generated

**Q 3.1.2 [2.5 pts] What is the IP address of your connecting device?**

**192.168.10.2**

**Include a screenshot from your computer or mobile device’s network settings.**

Text

Description automatically generated

**Q 3.1.3 [5 pts] What wireless security protocol is in use?**

**UDP**

**Table

Description automatically generated**

**Q 3.1.4 [5 pts] On the controller, which port is used to send commands to the drone?**

**8889**

**Q 3.1.5 [5 pts] On the drone, which port receives commands from the controller?**

**8889**

Graphical user interface

Description automatically generated with medium confidence

**Q 3.1.1 [2.5 pts]** What is the IP address of the drone? **192.168.10.1**

**Q 3.1.2 [2.5 pts]** What is the IP address of your connecting device? **192.168.10.2**

Include a screenshot from your computer or mobile device’s network settings.

Text

Description automatically generated

Initially we got a [Exception: Did not receive a state packet from the Tello] error this was fixed by allowing UDP traffic across the ports(11111,8899,8890) that tello uses to communicate by turning off the firewall completely.

Graphical user interface

Description automatically generated

Observations: This task had one issue. Initially we got a [Exception: Did not receive a state packet from the Tello] error this was fixed by allowing UDP traffic across the ports that tello uses to communicate by turning off the firewall completely.

1. Important Ports

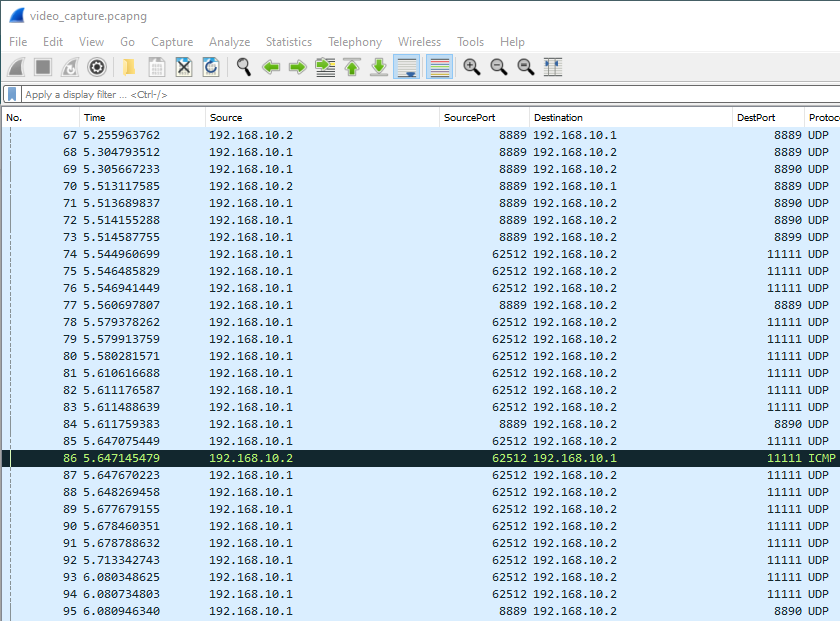
This task describes the ports associated with the sending and receiving of drone data such as video, state and command&receive.

* **Q 3.2.1a [5 pts]** On the controller, which port is used to send commands to the drone?
  + **8889**
* **Q 3.2.1b [5 pts]** On the drone, which port receives commands from the controller?
  + **8889**

Graphical user interface, text, application, email

Description automatically generated

* **Q 3.2.2a [5 pts]** On the drone, which port is used to send video feed to the controller?
  + **62512**
* **Q 3.2.2b [5 pts]** On the controller, which port receives video feed?
  + **11111**



* **Q 3.2.3a [5 pts]** On the drone, which port sends directional status messages to the controller?
  + **8889**
* **Q 3.2.3b [5 pts]** On the controller, which port receives the status updates from the drone?
  + **8890**

Table

Description automatically generated

Observations: This task had no issues or errors.

1. Drone Photography

This task details the relevant ports and process of a drone photo capture.

**Q 4.1 [5 pts] Was the photo that was taken stored on the drone or only on the VM? which port is used to send that photo to the controller?**

The photo was stored only on the VM. The port used to transmit the photo to the controller was 62512.

**Graphical user interface, application

Description automatically generated**

Observations: This task had no issues or errors.

1. Drone Videography

This task involves the conversion of network packets with video data to a actual video.

**Q 4.2.1 [10 pts] What file format are videos saved in and what is the video codec of the stream?**

The file format is [.raw] and the video codec of the stream is h264.

**Convert the video stream to a format that your device can easily view. (Please do this with a command line tool rather than sketchy online services). Include a screenshot of the command used.**

* Wireshark capture as drone takes video
* Find drone (192.168.10.1) to controller (192.168.10.2) transmissions on the ports used for video streaming (found in earlier sections)
* Follow one packet by UDP stream
* Show data as ASCII should be changed to raw
* Save this file as capture\_2.raw
* Ffmpeg command for conversion
* Lastly screenshots from the video

Graphical user interface, application

Description automatically generated

Table

Description automatically generated

Graphical user interface, text

Description automatically generated

**A picture containing text

Description automatically generatedA picture containing person, indoor

Description automatically generated**

**A picture containing person

Description automatically generated**

**Q 4.2.2 [10 pts] Attach a segment of this video (no longer than 15 seconds please) from the drone in your submission on Blackboard.**

Observations: This task had no issues or errors.

1. Capture the flag

This task involved getting a video extracted from a pcap file containing a video.

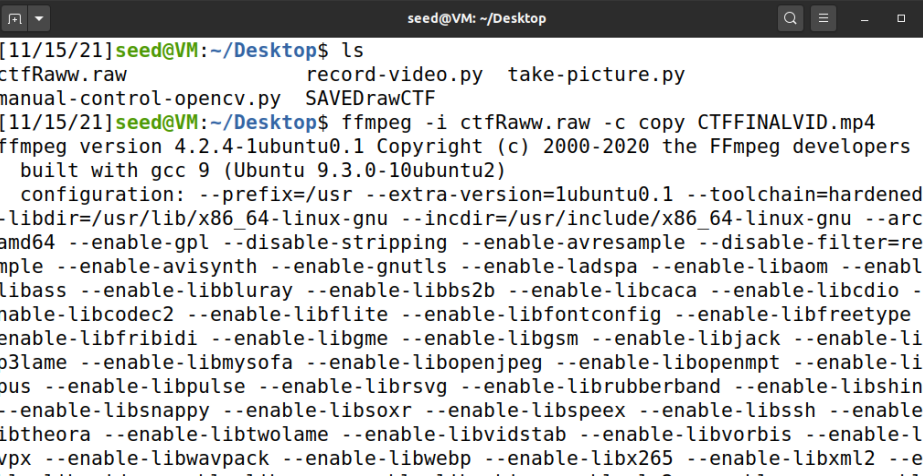
**Q 4.3 [20 pts] What is the flag shown in the video? Show screenshots and explain your steps.**

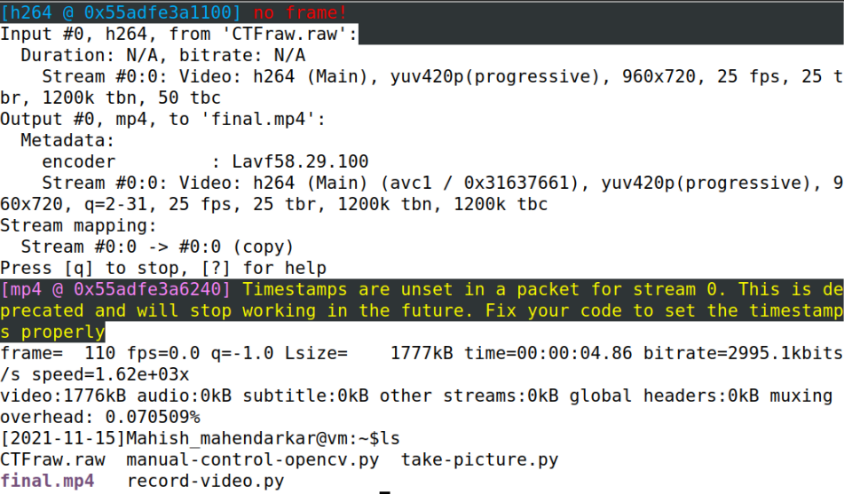
Flag: spymaster

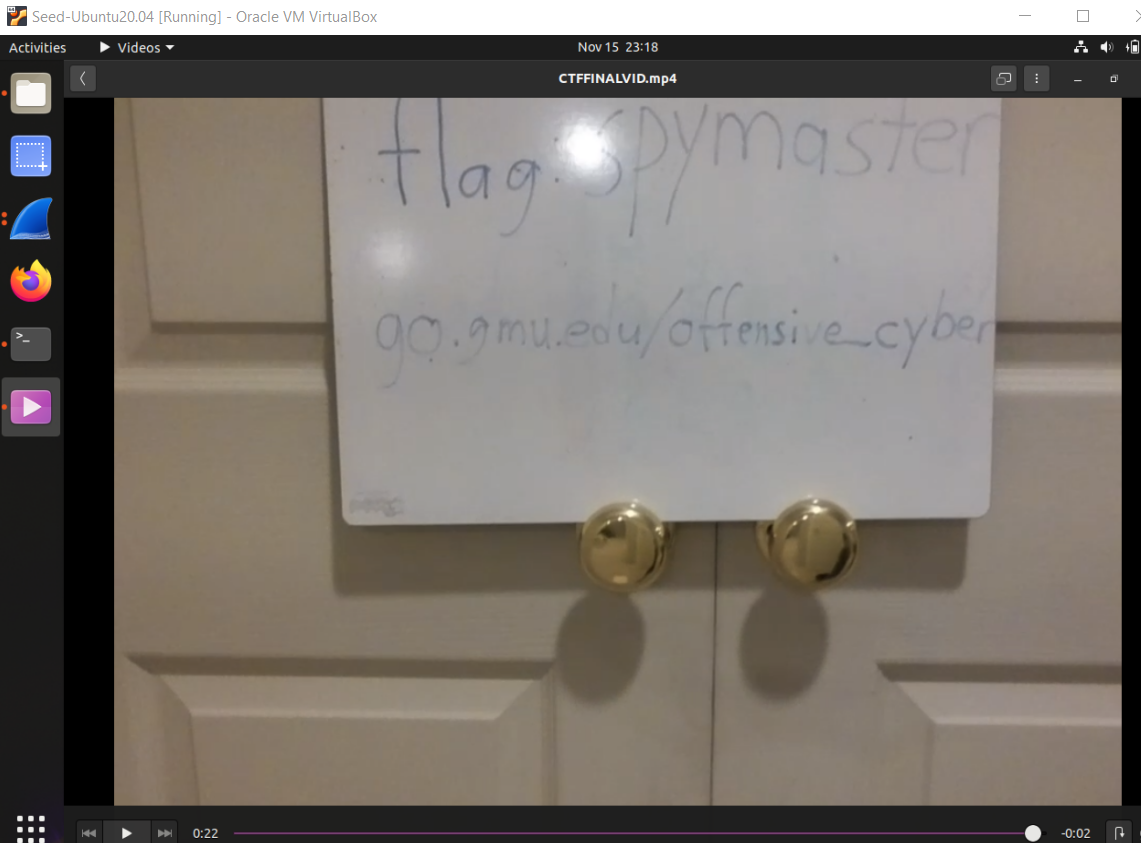
* Open CTF pcap
* Follow UDP stream from a packet exiting port 62512 from the drone
* Change data from packet to raw instead of ASCII
* Ffmpeg command with the raw data file that was saved [ffmpeg -i ctfRaww.raw -c copy CTFFINALVID.mp4]
* Show video - FAIL
* Install h264 ubuntu package [sudo apt-get install ubuntu-restricted-extras]
* Show video

Text

Description automatically generated



****

****

Observations: This task had no issues or errors.

1. Drone commands

This task shows the network capture of command-and-control transmissions.

**Q 5.1 [5 pts] What keyword initiates the control mode?**

**Include a screenshot of command and control traffic.**

Command

Table

Description automatically generated

**Q 5.2 [5 pts] What two possible responses can the drone reply with when receiving a command?**

Ok or error

Observations: This task had no issues or errors.

References:

Understanding tello controls

<https://www.youtube.com/watch?v=kcXN7CYgQ0g>

Understanding networking configuration of drone

<https://dlcdn.ryzerobotics.com/downloads/Tello/20180212/Tello+User+Manual+v1.0_EN_2.12.pdf>

Understanding available drone data (acceleration, velocity, barometric pressure etc.)

<https://dl-cdn.ryzerobotics.com/downloads/Tello/Tello%20SDK%202.0%20User%20Guide.pdf>

Troubleshooting initial connection issues

<https://github.com/damiafuentes/DJITelloPy/issues/79>

<https://githubmemory.com/repo/damiafuentes/DJITelloPy/issues/91>

<https://tellopilots.com/threads/tello-drone-firmware-v1-3-2-not-getting-expected-responses.4766/>

Capture the flag extraction

<https://knowledgebase-iframe.polycom.com/kb/viewContent.do;jsessionid=25E28062482EC97508C5FB72EBDDEDA3?externalId=34917>