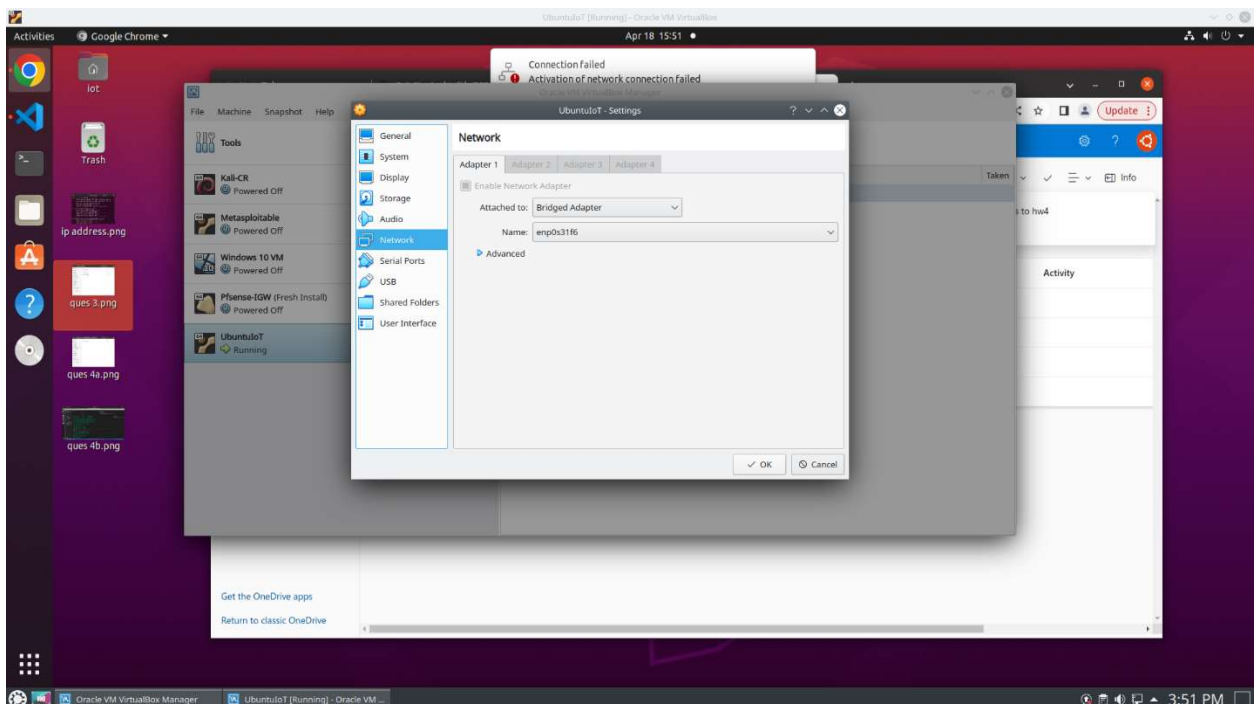**IoT Security and Privacy**

Assignment 4 – Secure ESP32 OTA through HTTPS
(10 points)

Partners: Ishan Patel, Ernest

Questions

Students are asked to repeat the work in the tutorial Secure ESP32 OTA through HTTPS.

1. Ensure your Ubuntu VM uses the bridged adapter. Include below a screenshot of the networking setting of your Ubuntu VM. (1 point)


1

2. What is the IP address of your Ubuntu VM? (1 point)

```
iot@iot-VirtualBox: ~

iot@iot-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.225  netmask 255.255.248.0  broadcast 192.168.7.255
        inet6 fe80::7708:c791:98f6:f636  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:bd:f6:76  txqueuelen 1000  (Ethernet)
        RX packets 294104  bytes 183274984 (183.2 MB)
        RX errors 0  dropped 11  overruns 0  frame 0
        TX packets 13125  bytes 3088124 (3.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 850  bytes 287518 (287.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 850  bytes 287518 (287.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlx502b73cc002f: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 50:2b:73:cc:00:2f  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
```

3. Please read the section of *Prepare the OTA Firmware Image*. Include below a screenshot or photo of the contents of /home/iot/server. (1 point)
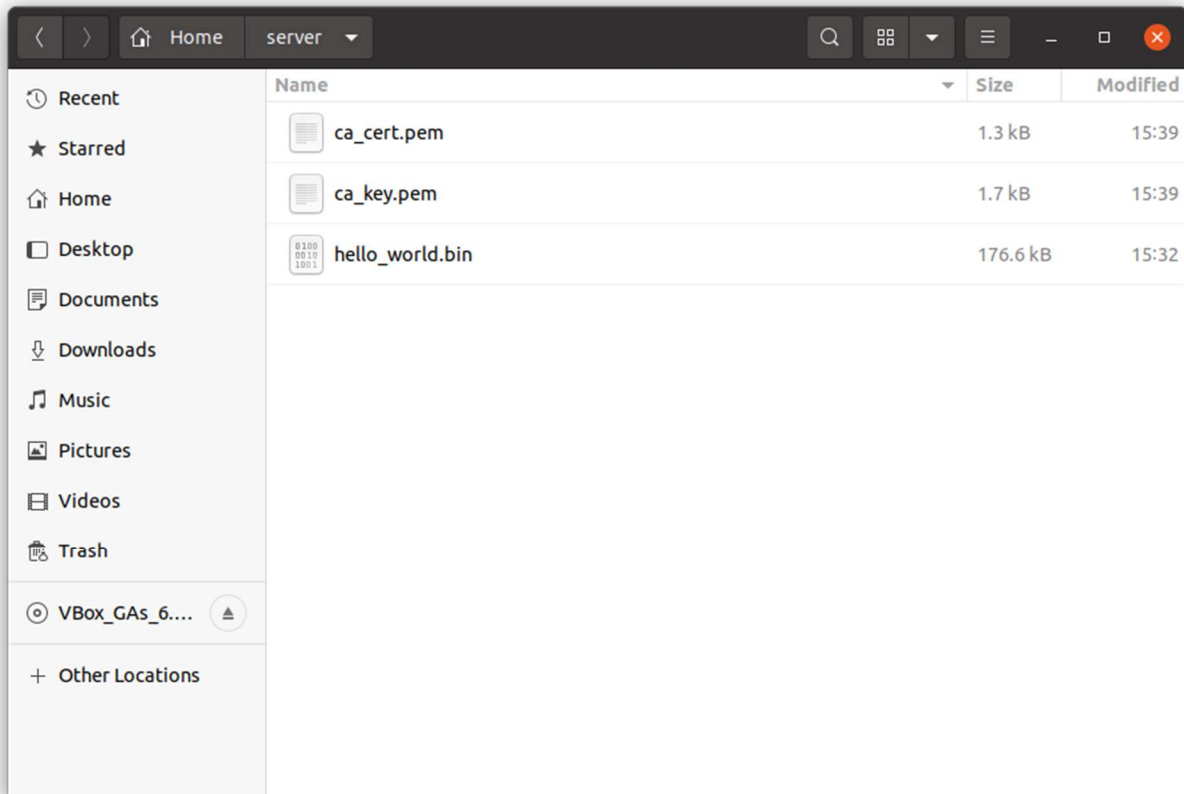
4. Please read the section of *Run the simple_ota_example Project*.
    a. Provide a screenshot or photo of the folder of *server_certs* and *ca_cert.pem* in *server_certs*. (1 point)
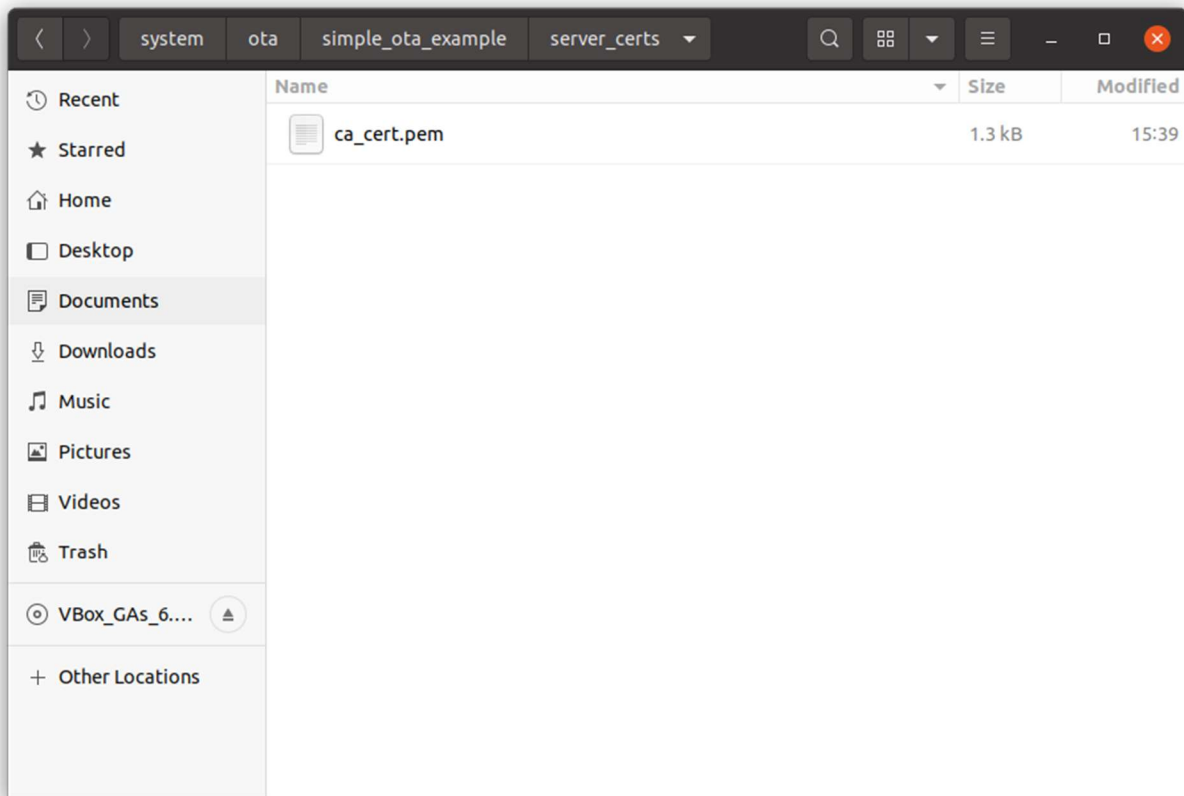
    b. Provide a screenshot or photo of serial monitor after the firmware upgrading operation. (4 points)
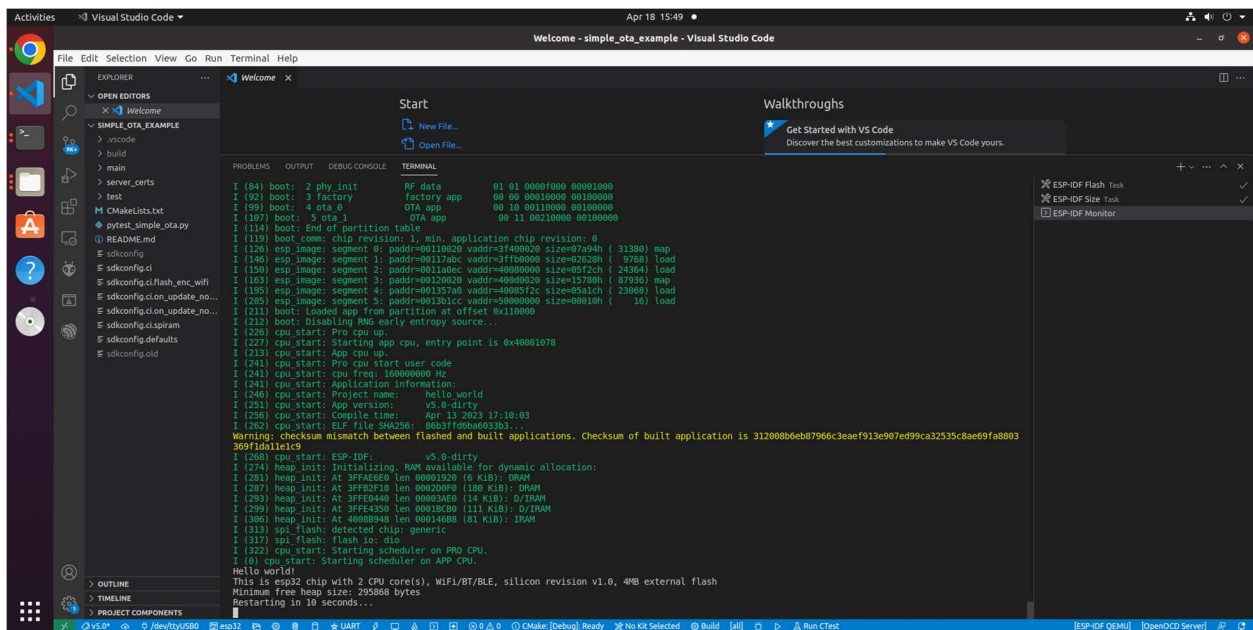
5. Please discuss the OTA used in this assignment. Is the OTA secure? (2 points)

    The OTA used in this assignment updates the firmware without physically accessing the the esp32 device. It uses the ArduinOTA library to update it over the air. The OTA isn't secure because the update process isn't encrypted and an attacker can intercept the firmware while its updating.