Carmina Bradbury
MICH CS 42
IoT Final Project Documentation

Find the Flag in Firmware

Environment & Tools
-MQTT Explorer
-Strings

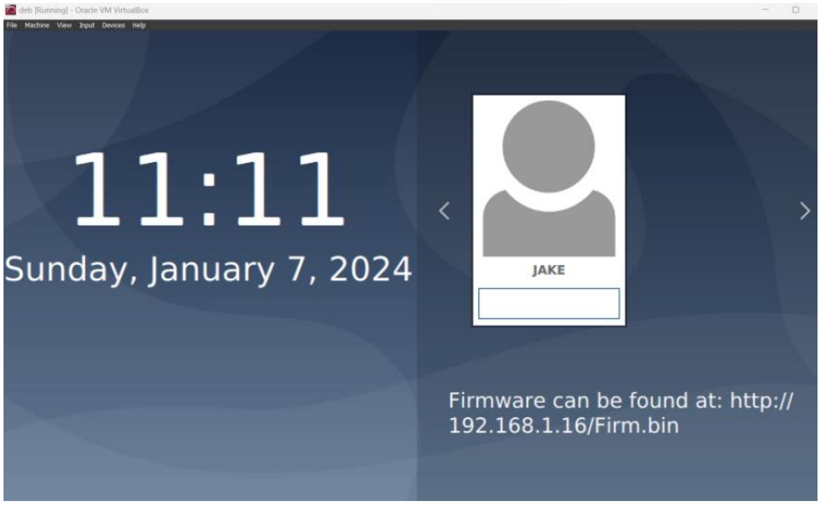
Lab Files
-IoT_Final.ova

VM's
-WIN10 (on bridge adapter)
-Ubuntu/Kali (on bridge adapter)

Project Preparation: Import OVA

Download the **IoT_Final.ova** from Canvas. **Double-click** the file to import the virtual machine into VirtualBox. **Right-click** the virtual machine in the VirtualBox interface and click **Settings**. Click **Network** then on Adapter 1 put attached to: **Bridge Adapter**

Start the virtual machine. When it is fully started, you will be prompted to reboot. Reboot the system, and continue to do so until the firmware address appears as shown below:

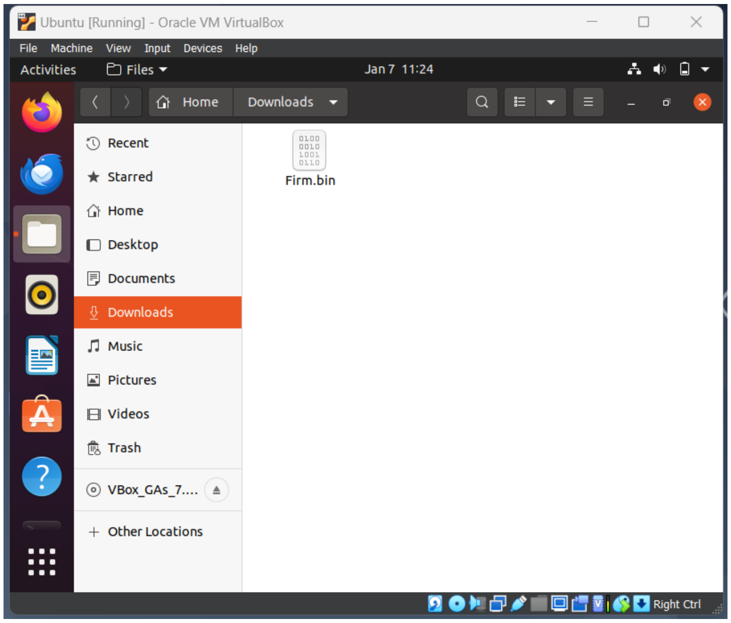

deb [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
11:11
Sunday, January 7, 2024
JAKE

Firmware can be found at: http://
192.168.1.16/Firm.bin

Carmina Bradbury
MICH CS 42
IoT Final Project Documentation

On your Kali/Ubuntu machine Go to your **Browser and search – http:// "the IP address shown below" /Firm.bin** then **Enter**, the file will be downloaded
Note that the Firmware IP address below will be different on your side

Confirm that you can locate the Firm.bin file on Kali/ubuntu machine

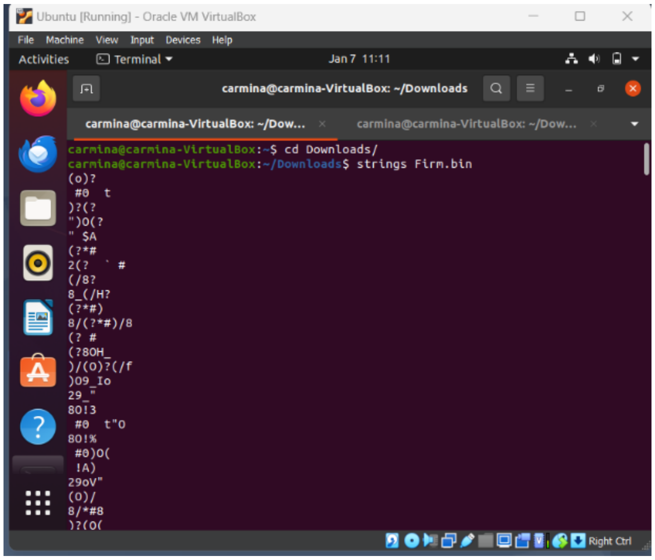


Carmina Bradbury
MICH CS 42
IoT Final Project Documentation

Access the firmware and locate Strings

On your kali terminal, navigate to the **Downloads** directory using the command **cd Downloads/**

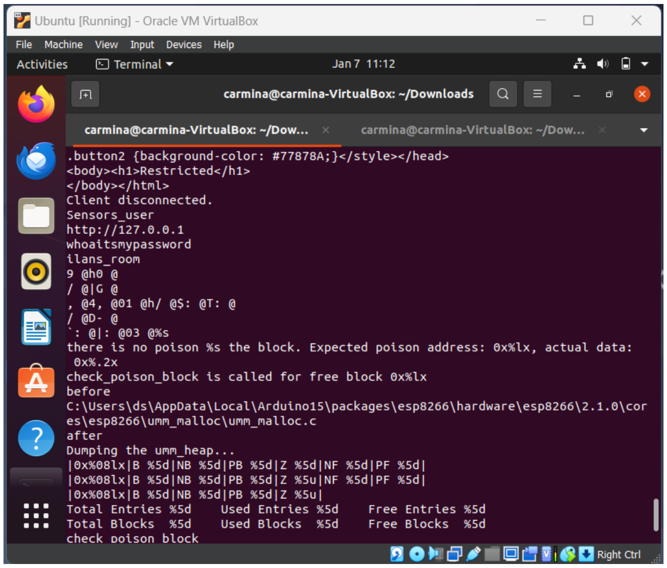
Use the command **strings Firm.bin** to print the file's strings


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Jan 7 11:11
carmina@carmina-VirtualBox: ~/Downloads
carmina@carmina-VirtualBox: ~/Dow...
carmina@carmina-VirtualBox: ~/Dow...
Right Ctrl

```
carmina@carmina-VirtualBox:~$ cd Downloads/
carmina@carmina-VirtualBox:~/Downloads$ strings Firm.bin
(o)?
 #0  t
)?(?
")O(?
" $A
(?*#
2(?  ` #
(/8?
8_(/H?
(?*#)
8/(?*#)/8
(? #
(?8OH_
)/(O)?(/f
)O9_Io
29_"
8O!3
 #0  t"O
8O!%
 #0)O(
 !A)
29oV"
(O)/
8/*#8
)?(O(
```

Scroll and find the credentials like **Ip address, username, password**

Hint: If your firmware shows a loopback IP, use the IP that was designated when you download the firmware.


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Jan 7 11:12
carmina@carmina-VirtualBox: ~/Downloads
carmina@carmina-VirtualBox: ~/Dow...
carmina@carmina-VirtualBox: ~/Dow...
Right Ctrl

```
.button2 {background-color: #77878A;}</style></head>
<body><h1>Restricted</h1>
</body></html>
Client disconnected.
Sensors_user
http://127.0.0.1
whoaitsmypassword
ilans_room
9 @h0 @
/ @|G @
, @4, @01 @h/ @$: @T: @
/ @D- @
`: @|: @03 @%s
there is no poison %s the block. Expected poison address: 0x%lx, actual data:
 0x%.2x
check_poison_block is called for free block 0x%lx
before
C:\Users\ds\AppData\Local\Arduino15\packages\esp8266\hardware\esp8266\2.1.0\cor
es\esp8266\umm_malloc\umm_malloc.c
after
Dumping the umm_heap...
|0x%08lx|B %5d|NB %5d|PB %5d|Z %5d|NF %5d|PF %5d|
|0x%08lx|B %5d|NB %5d|PB %5d|Z %5u|NF %5d|PF %5d|
|0x%08lx|B %5d|NB %5d|PB %5d|Z %5u|
Total Entries %5d    Used Entries %5d    Free Entries %5d
Total Blocks  %5d    Used Blocks  %5d    Free Blocks  %5d
check poison block
```

Carmina Bradbury
MICH CS 42
IoT Final Project Documentation

Run the command

sudo apt update

sudo apt install mosquitto -y to install the mosquito server

sudo apt install mosquito-clients -y

use the command **sudo nano /etc/mosquitto/mosquitto.conf** to open Mosquitto's configuration file

At the bottom of the configuration file, add the following lines:

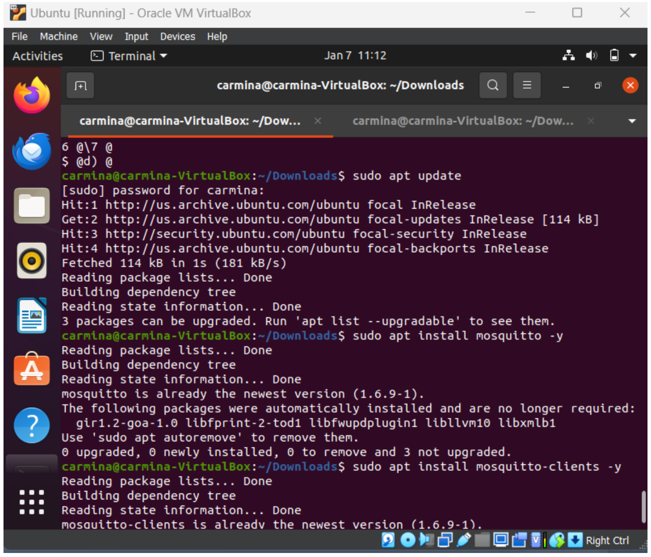
Allow_anonymous false

Password_file /etc/mosquito/pwfile

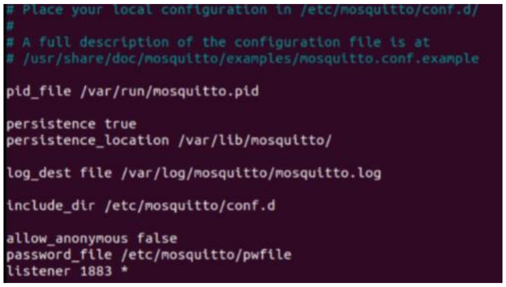
Listener 1883 *

Then save the file by using **Ctrl+S** then exit by **Ctrl+X**

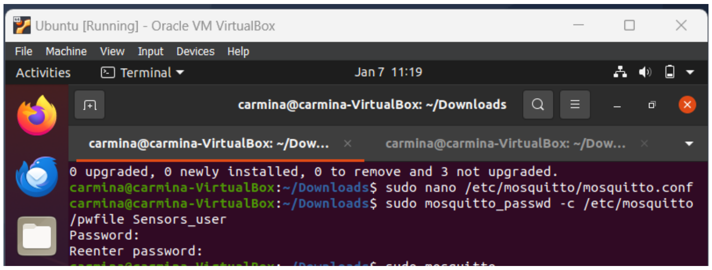
Use the command **sudo mosquito_passwd -c /etc/mosquito/pwfile Sensors_user** to create a new user named for the Mosquitto server, then provide a password (**whoaitsmypassword**) when prompted


Ubuntu [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Activities
Terminal
Jan 7 11:12
carmina@carmina-VirtualBox: ~/Downloads
carmina@carmina-VirtualBox: ~/Dow...
carmina@carmina-VirtualBox: ~/Dow...
Right Ctrl

```
6 @\7 @
$ @d) @
carmina@carmina-VirtualBox:~/Downloads$ sudo apt update
[sudo] password for carmina:
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Hit:3 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Fetched 114 kB in 1s (181 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
3 packages can be upgraded. Run 'apt list --upgradable' to see them.
carmina@carmina-VirtualBox:~/Downloads$ sudo apt install mosquitto -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
mosquitto is already the newest version (1.6.9-1).
The following packages were automatically installed and are no longer required:
  gir1.2-goa-1.0 libfprint-2-tod1 libfwupdplugin1 libllvm10 libxmlb1
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
carmina@carmina-VirtualBox:~/Downloads$ sudo apt install mosquitto-clients -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
mosquitto-clients is already the newest version (1.6.9-1).
```



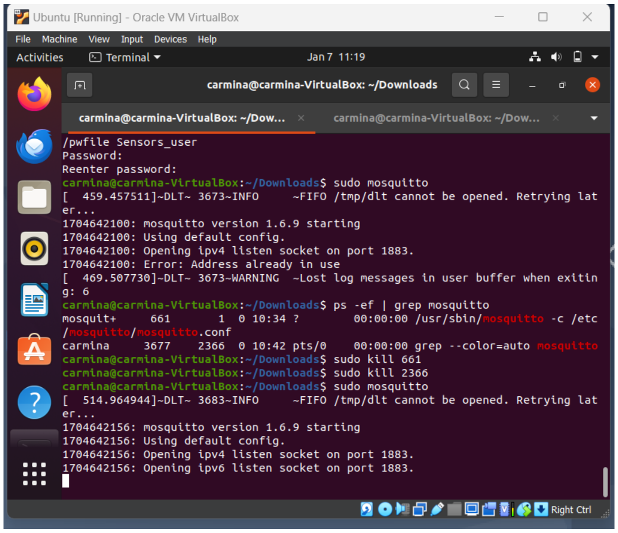
```
# Place your local configuration in /etc/mosquitto/conf.d/
#
# A full description of the configuration file is at
# /usr/share/doc/mosquitto/examples/mosquitto.conf.example

pid_file /var/run/mosquitto.pid

persistence true
persistence_location /var/lib/mosquitto/

log_dest file /var/log/mosquitto/mosquitto.log

include_dir /etc/mosquitto/conf.d

allow_anonymous false
password_file /etc/mosquitto/pwfile
listener 1883 *
```


Ubuntu [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Activities
Terminal
Jan 7 11:19
carmina@carmina-VirtualBox: ~/Downloads
carmina@carmina-VirtualBox: ~/Dow...
carmina@carmina-VirtualBox: ~/Dow...

```
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
carmina@carmina-VirtualBox:~/Downloads$ sudo nano /etc/mosquitto/mosquitto.conf
carmina@carmina-VirtualBox:~/Downloads$ sudo mosquitto_passwd -c /etc/mosquitto
/pwfile Sensors_user
Password:
Reenter password:
carmina@carmina-VirtualBox:~/Downloads$ sudo mosquitto
```

Carmina Bradbury
MICH CS 42
IoT Final Project Documentation

Use the command **sudo mosquitto** to start the server. If you get the error massage “Address already in use,” use **ps -ef | grep mosquitto** to find the process, and then run **sudo kill [PID]**


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Jan 7 11:19
carmina@carmina-VirtualBox: ~/Downloads
carmina@carmina-VirtualBox: ~/Dow...
carmina@carmina-VirtualBox: ~/Dow...
Right Ctrl

```
/pwfile Sensors_user
Password:
Reenter password:
carmina@carmina-VirtualBox:~/Downloads$ sudo mosquitto
[  459.457511]~DLT~ 3673~INFO     ~FIFO /tmp/dlt cannot be opened. Retrying lat
er...
1704642100: mosquitto version 1.6.9 starting
1704642100: Using default config.
1704642100: Opening ipv4 listen socket on port 1883.
1704642100: Error: Address already in use
[  469.507730]~DLT~ 3673~WARNING  ~Lost log messages in user buffer when exitin
g: 6
carmina@carmina-VirtualBox:~/Downloads$ ps -ef | grep mosquitto
mosquit+     661       1  0 10:34 ?        00:00:00 /usr/sbin/mosquitto -c /etc
/mosquitto/mosquitto.conf
carmina     3677    2366  0 10:42 pts/0    00:00:00 grep --color=auto mosquitto
carmina@carmina-VirtualBox:~/Downloads$ sudo kill 661
carmina@carmina-VirtualBox:~/Downloads$ sudo kill 2366
carmina@carmina-VirtualBox:~/Downloads$ sudo mosquitto
[  514.964944]~DLT~ 3683~INFO     ~FIFO /tmp/dlt cannot be opened. Retrying lat
er...
1704642156: mosquitto version 1.6.9 starting
1704642156: Using default config.
1704642156: Opening ipv4 listen socket on port 1883.
1704642156: Opening ipv6 listen socket on port 1883.
```

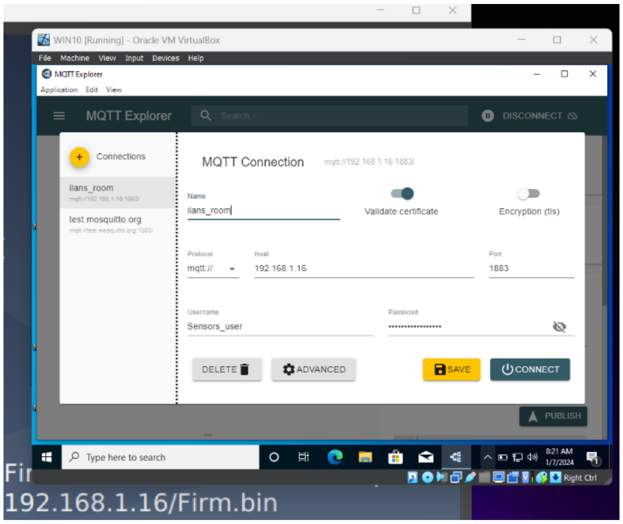
Start your WIN10 machine, double-click **MQTT Explorer** to start it

Name the connection **ilans_room**

In the Host field, provide the IP address of the MQTT server (deb ova, firmware Ip addr) and make sure the port is **1883**

Enter the username that was created for Mosquitto and its password. Click **ADVANCE** use the wildcard **#** on the topic, note: delete the existing topics

Click **Back,** and then **SAVE** and **CONNECT**

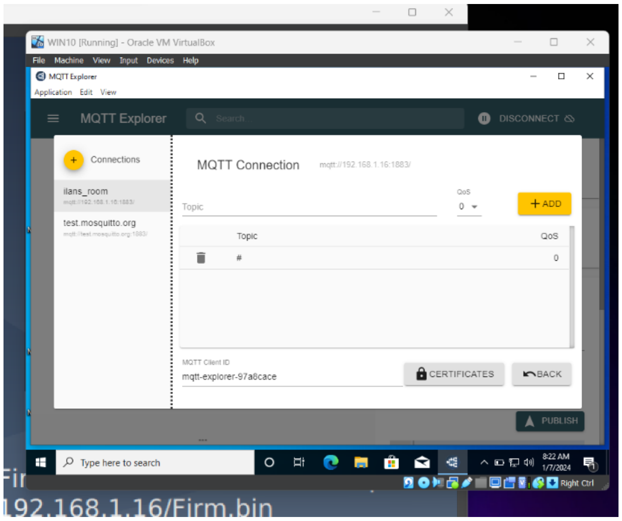


MQTT Connection mqtt://192.168.1.16:1883/

Name: ilans_room

Protocol: mqtt://
Host: 192.168.1.16
Port: 1883

Username: Sensors_user
Password: ••••••••••••••••••



MQTT Connection mqtt://192.168.1.16:1883/

QoS: 0

Topic	QoS
#	0

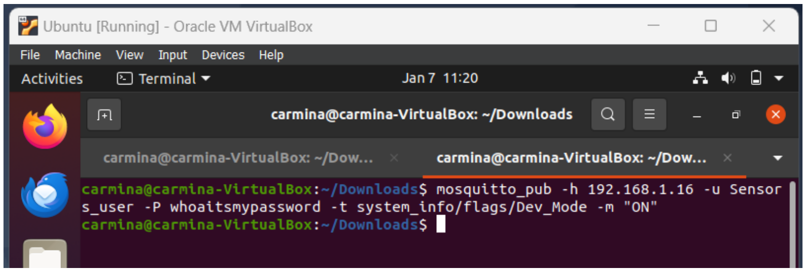
MQTT Client ID: mqtt-explorer-97a8cace

Carmina Bradbury
MICH CS 42
IoT Final Project Documentation

In the Kali/Ubuntu machine, run **mosquitto_pub -h “IP addr from your ova” -u Sensors_user -P whoaitsmypassword -t system_info/flags/Dev_Mode -m “ON”**

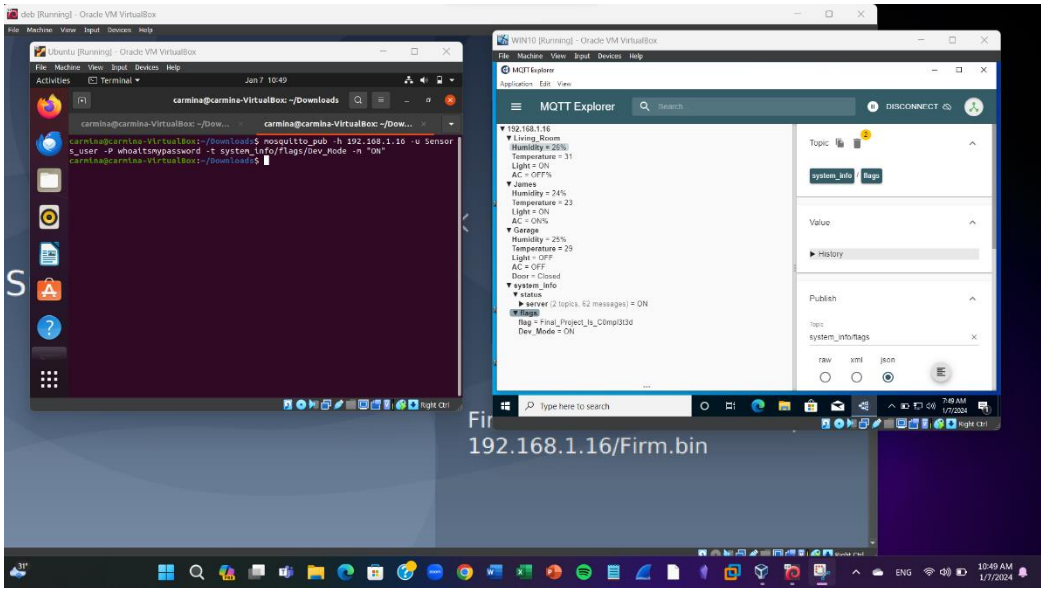
Note: Make sure your modification is in all caps (ON vs. on)

And then CTF is Done!



Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Jan 7 11:20
carmina@carmina-VirtualBox: ~/Downloads
carmina@carmina-VirtualBox: ~/Dow...
carmina@carmina-VirtualBox: ~/Dow...

```
carmina@carmina-VirtualBox:~/Downloads$ mosquitto_pub -h 192.168.1.16 -u Sensor
s_user -P whoaitsmypassword -t system_info/flags/Dev_Mode -m "ON"
carmina@carmina-VirtualBox:~/Downloads$
```



deb [Running] - Oracle VM VirtualBox
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Jan 7 10:49
carmina@carmina-VirtualBox: ~/Downloads
WIN10 [Running] - Oracle VM VirtualBox
MQTT Explorer
Application Edit View
Search
DISCONNECT
Topic
system_info
flags
Value
History
Publish
Topic
raw
xml
json
Type here to search
Fir
192.168.1.16/Firm.bin

```
carmina@carmina-VirtualBox:~/Downloads$ mosquitto_pub -h 192.168.1.16 -u Sensor
s_user -P whoaitsmypassword -t system_info/flags/Dev_Mode -m "ON"
carmina@carmina-VirtualBox:~/Downloads$
```

```
▼ 192.168.1.16
  ▼ Living_Room
    Humidity = 26%
    Temperature = 31
    Light = ON
    AC = OFF%
  ▼ James
    Humidity = 24%
    Temperature = 23
    Light = ON
    AC = ON%
  ▼ Garage
    Humidity = 25%
    Temperature = 29
    Light = OFF
    AC = OFF
    Door = Closed
  ▼ system_info
    ▼ status
      ▶ server (2 topics, 62 messages) = ON
    ▼ flags
      flag = Final_Project_Is_C0mpl3t3d
      Dev_Mode = ON
```

Publish topic: system_info/flags