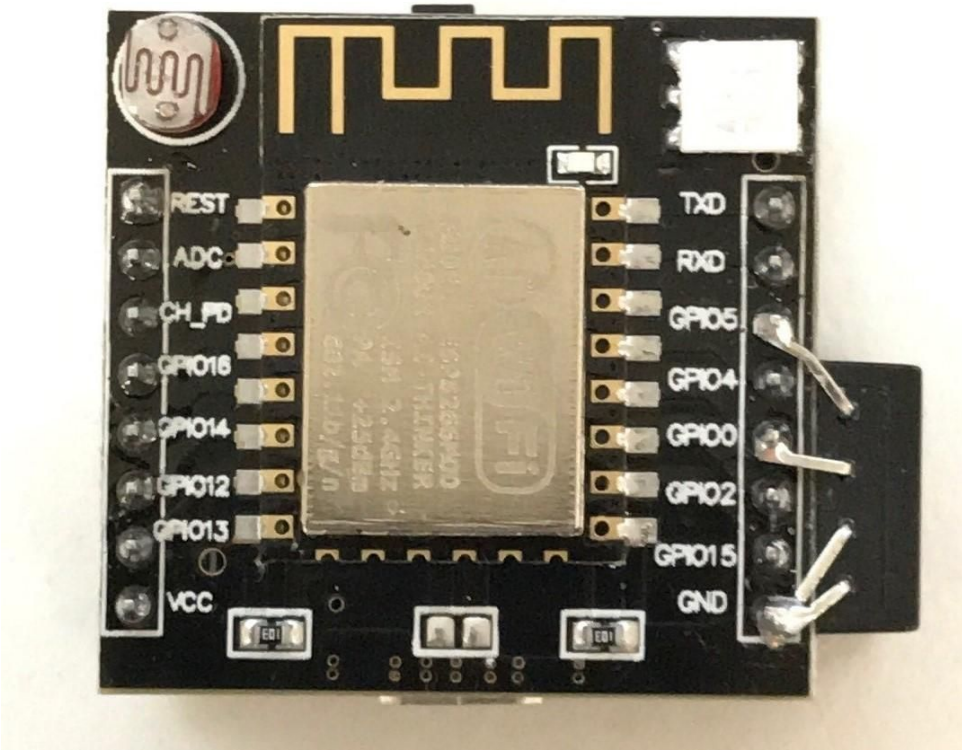
CySCA 2017 IoT Information Pack

Congratulations for being involved in the 2017 Australian Cyber Challenge. As you would be aware this year's challenge revolves around the IoT Company TICTOC - **Totally Innovative Cloud Things of Connectedness.**

Please carefully read through this document, as it will give you information regarding the IoT device you should have received. This is important as how to use the IoT Device is required for a number of challenges in this year's competition.

Pack Contents

The Contains of the pack is the players to keep, If anything is missing or broken please contact `support@cyberchallenge.com.au`



Each player will receive:

- 1x Modified ESP8266 serial WIFI Witty Cloud Development Board.
    - (AM2320 Temperature/Humidity Sensor added)
- 1x USB WiFi Adapter to connect the Witty module to your VPN.
- 1x Micro-USB Cable for console connection and power.

CySCA Challenge Requirements

For this years challenge players are *strongly encouraged* to set up a KALI 2016.2 Virtual machine as the challenges have been built and tested with KALI 2016.2.

All the IoT hardware and challenges have been built such that the IoT device require a connection to your virtual game network via the VPN. This is why you have been provided with a USB WiFi Adapter. Players will need to setup a WiFi Hotspot from a machine connected to the VPN. VPN Connectivity Instructions are detailed in VPN connectivity document provided with your VPN Keys.

Players who can't setup a virtual machine can also use a Live Boot Kali with Persistence however due to the number of USB interfaces needed you may require your own USB hub to connect all the devices at once.

For a Virtual machine setup

Both VMware and Virtualbox have been tested and confirmed working. Players should follow the kali hard disk install process to install kali into a virtual machine http://docs.kali.org/installation/kali-linux-hard-disk-install (You will not need to copy the ISO to a USB key or a dvd as you can mount the ISO directly to the virtual machine)

For a Live Boot Kali with Persistence

The Kali website has a set of instructions for creating a persistent live kali USB setup. Players who want to use this option should follow the instructions http://docs.kali.org/downloading/kali-linux-live-usb-persistence

ESP8266 WiFi Witty Board Information

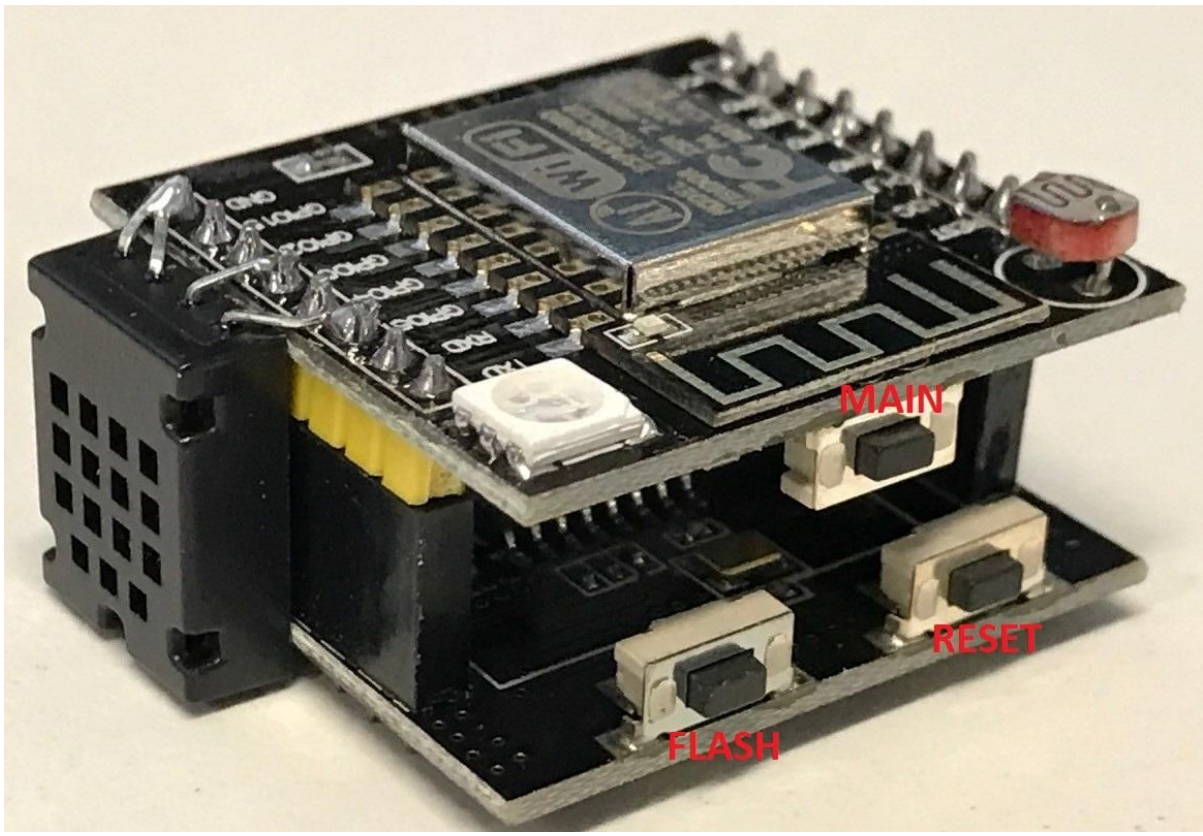
This cloud development board is based on the ESP8266 wifi microcontroller. The ESP8266 is a SOC(System-On-Chip) created by Espressif that has a full TCP/IP stack and 802.11b/g/n capabilities. It has a 4MB flash for storage. For full details on the chip see https://en.wikipedia.org/wiki/ESP8266

The ESP8266 can be programmed using their SDK and multiple languages. For the challenge, we are using micropython. Players will NOT be required to compile their own firmware however you will be required to flash the board.

The Witty board provides a Serial interface to flash the device and to view the device console when plugged into the bottom micro-USB port. The board comes with a LDR(Light Dependent Resistors) and a 3 colour RGB LED. We have attached a AM2320 Temperature/Humidity Sensor to the board to align with one of the challenges.
There is 1 button on the top board, we call this the MAIN button.
There are 2 other buttons on the bottom board:

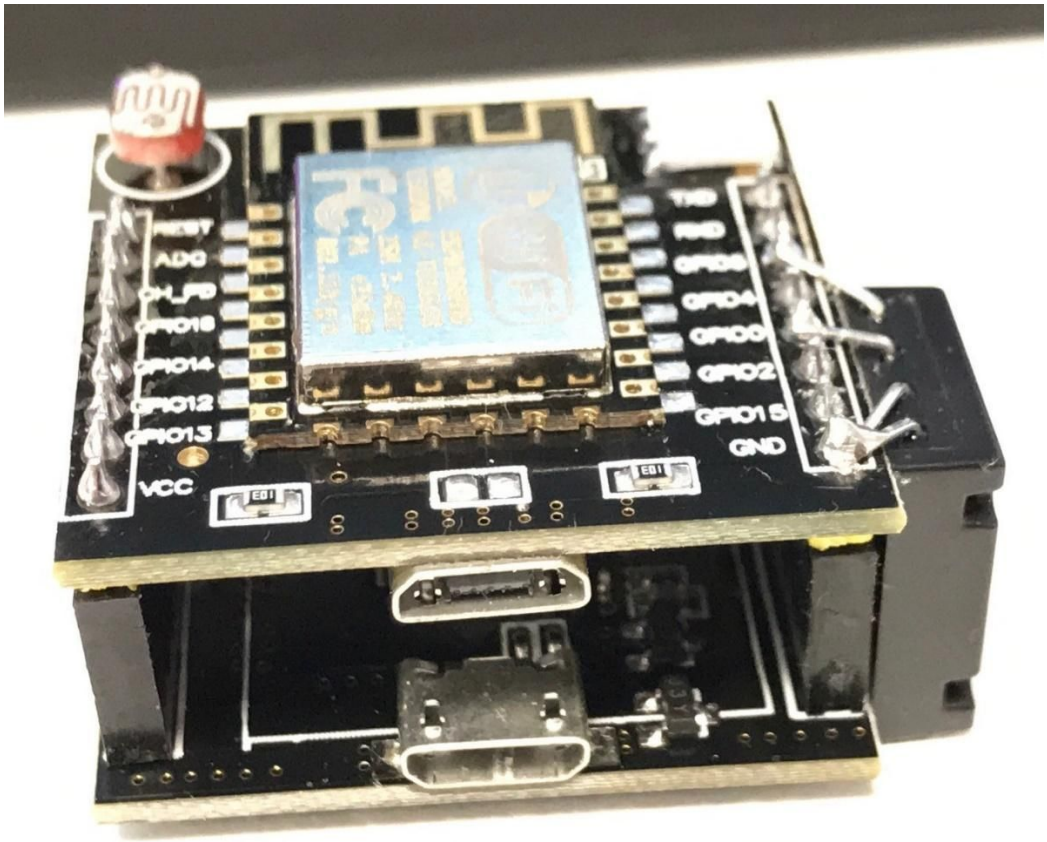
- 1 to flash the board .
- 1 to reset the board.

These are both labelled on the bottom of the board. **Players should only need to use the MAIN and RESET buttons.**



The Witty board can be separated into 2 halves, the bottom part is the Serial interface board and the top half is the actual ESP8266 part of the board.

We suggest you leave them together as you will need access to the device console which can only be done when the 2 boards are together. The bottom micro-USB port allows console access. The top micro-USB port will just power the ESP8266 and will not allow console access. You only need to connect 1 of these at a time, **DO NOT PLUG BOTH IN AT THE SAME TIME.**



Players have also been provided with a USB WiFI adapter. This adapter is provided so you can create a hotspot on the VPN machine, the Witty device will connect to this hotspot.

Players will need to create a hotspot on a machine connected to their team VPN so the IoT device can communicate with the IoT Server in their game Environment. The device/challenges will not work if it cannot connect to your team's game environment via a hotspot.

Details for setting up a hotspot are outlined in the VPN connectivity document provided with your VPN keys that your institution representative will provide to you.

Connecting to the Witty Board Serial Console

The serial baud rate for the device is `115200`

To connect to the Witty board first connect to the bottom micro-USB port. The device should show up as a CH340 USB-Serial Device.

Drivers for this device are built into Windows 10, Linux and MAC. On Windows, you will need to go into device manager to find the com port number. HOWEVER, we highly recommend you use Kali Linux. You can bridge the device with or without a driver into a virtual machine and may show up as a "QinHeng USB2.0-Serial device".

Once bridged it can be accessed from the VM as `/dev/ttyUSB0`.
note: this number will increase as more devices bridged to the same VM.

Once physically connected you will need a serial/terminal application. On Linux/MAC we recommend using `screen` or `minicom`, On windows you can use `putty`.
Just connect to the serial port Eg. `/dev/ttyUSB0` or `COM8` at the `115200` baud rate.

Press the reset button on the device and you will see the serial console messages.

Flashing/Accessing the Witty Board

The best tool to use to flash the Witty Board is **ESPTOOL**, this is the default and has been used when building and testing the challenges.
Players should familiarise themselves with the commands available to ESPTOOL https://github.com/espressif/esptool/blob/master/README.md.

Players can follow the Easy Installation instructions for KALI Linux. ESPTOOL can be installed on other platforms however this has not been tested. The Witty Board comes with the CySCA testing firmware for connectivity testing. At the start of the event players will need to flash their device with the Game firmware. Information on this will be provided on the scoring system under the IoT Challenges section.

NOTE: Before flashing new firmware, players should first erase the flash on the device. This can be done using the command:

```
>esptool.py --port /dev/ttyUSB0 erase_flash
```

This will reset the board to a clean state before you flash the actual game firmware.

Setting WiFi Hotspot Details on the IoT Device

Players will need to set the WiFi details of their hotspot using the Witty Board serial console. When the device first starts up, it will prompt for Wireless details such as `SSID`, `Password`. Enter details as appropriate for your Hotspot. IP Address options are `STATIC` or `DHCP`, `DHCP` is recommended.

If you specify the static option, the device will prompt for the all IP information of your Hotspot. It will also allow you to overwrite the DNS server address, we recommend you only do this if necessary. The device is flashed and pre-configured with the correct DNS server for your game environment.

Resetting WiFi Detail

At any point players can reset the WiFi details on your device without performing an erase/flash.

To do this press and hold the `MAIN` button and then press and release the reset button.

The console will ask you if you wish to reset for a new challenge, Enter '`NO`' here.
It will then ask if you wish to reset the WiFi details.
Type '`YES`' here and the WiFi details will be reset and the device will reboot and ask for new details.

Pre-Game Testing

The device comes with a testing firmware written for the CySCA challenge. This testing firmware tests connectivity to your team's game environment and if the Temperature/Humidity Sensor is functional.

Before the event players will be able to connect to their VPN and set up their playing environment. During this time players can also test if their IoT devices can connect to the IoT control server by connecting the device console then setting up the WiFi details and verifying the connectivity message that shows up when the device is connected.

If you manage to break your device firmware during this testing time you can re-download the testing firmware from https://extras.cyberchallenge.com.au/iot/testing/ Players should also validate this downloaded file using the sha1sum checksum file.

CySCA 2017 IoT Challenges

There is a total of five dedicated IoT challenges that focus on this device, with a sixth challenge where this device is optional.
Before you start any of these challenges you will need to flash the Game Firmware. This firmware will be provided on the scoring system in the IOT challenge section once the challenge starts.
Before flashing your device make sure you read the **ESPTOOL** commands and the flashing section of this document.

The first step is to download the game firmware file and its sha1sum file. Players should validate the download using the sha1sum file. This firmware file is a fully combined firmware so you do not need any extra flashing parameters.

When flashing 1st erase the current flash

```
>esptool.py --port /dev/ttyUSB0 erase_flash
```

Then flash the new firmware

```
>esptool.py --baud 115200 --port /dev/ttyUSB0 write_flash 0x0 gamefw.bin
```

The game firmware is just a WiFi setup and loader system. Because this one device is used for multiple challenges setup is done via the Serial console. A normal device that only does one task would have this setup as a webpage.
When you have connected to your WiFi Hotspot and the device can successfully connect to your

game environment you will be prompted for a Challenge ID. This will be provided either via the scoring system or a link from the scoring system.
When you enter this ID the related challenge code will be downloaded and installed on the device. It will then automatically reboot and boot with the challenge code.
This code may just display information or it will ask for some additional configuration depending on the challenge.
Note:Flags for some challenges will be delivered back to the serial console.

loading a new challenge

During the game, you will need to reset the device to load the code for other challenges. Because we built a challenge loader into the base firmware you will not need to reflash the device.

To load a new challenge, press and hold the `MAIN` button then press and release the `reset` button. On the console the device will ask if you wish to reset the device to load a new firmware.
Type `YES` here and the device will wipe the current game code and reset itself read for a new `challenge ID`.
Note: Doing this will not remove the WiFi or IP address configuration from the device.

Post-Game

After CySCA 2017 is over you will not be able to connect the device to your game environment. We plan to release the code for the device sometime after the event. We aim to provide the IoT server VM as well as source code. Players however can look at other uses for the device including some of the many esp8266 micropython or nodeMCU tutorials for the device.

However the device is now yours to keep.
Some useful information if you are going to write your own apps:

```
#button
mainbtn_pin = 4

#LED
blue_pin = 13
green_pin = 12
red_pin = 15

#LDR
ADC(0)

#Temp/Humidity sensor. Use DHT22 library. Pull power pin high to enable sensor.
data_pin = 0
power_pin = 5
```