The Great Geekery

Friday, February 5, 2016

EcoPlug Wifi Switch Hacking

I opened up an ecoplug module bought from Home Depot. They are currently on clearance for $15 Canadian each (about $12 US).

The switches can only be controlled via the app (which is pretty crap) but I have captured and dissected the communication and discovered it is essentially just a UDP packet controlling the switch state. I was considering writing an openHab binding for it; but decided to open up the switch instead.

Home depot product page: http://www.homedepot.com/p/Grounded-Indoor-Wi-Fi-Adapter-2-Pack-CT-065W/206177754;jsessionid=31776537145CBE2EDAF2A319018BFF47

They are also sold under the name Wood WiOn: http://amzn.to/1R9e9Xx

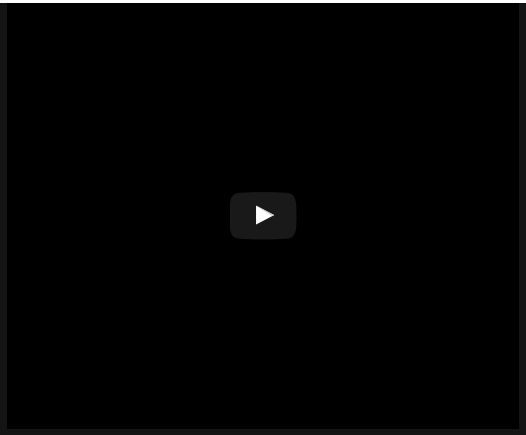
Here is the new firmware I wrote for it:
https://github.com/scottjgibson/esp8266Switch

Update: If you want to try this yourself; John has written an excellent write up filling in many of the steps omitted below; definitely worth a look.

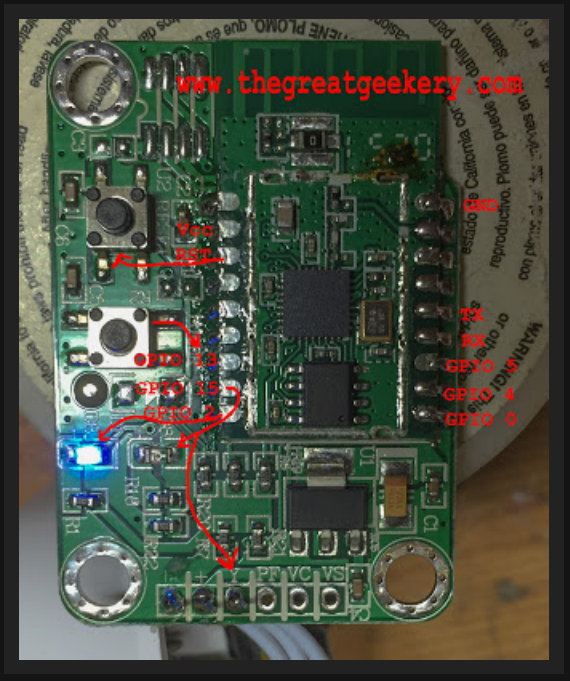
Here is my teardown and programming video:

Labels

- CNC (5)
- PixelPi (5)
- hardware (4)
- DMX (3)
- OLA (3)
- Powder Coating (3)
- RaspberryPi (3)
- High Voltage (2)
- Laser (2)
- LightingPi (2)
- Power Supply (2)
- Python (2)
- Roomba (2)
- bluetooth (2)
- roomote (2)
- Audio LM4780 (1)
- BMW (1)
- Coffee Roasting (1)



Pinout Diagram:



I confirmed the unpopulated 8 pin part was for an external adc; based on the wiring it looks like the

FTDI (1)
Macro (1)
Photography (1)
dd-wrt (1)
hacking (1)
reflow (1)

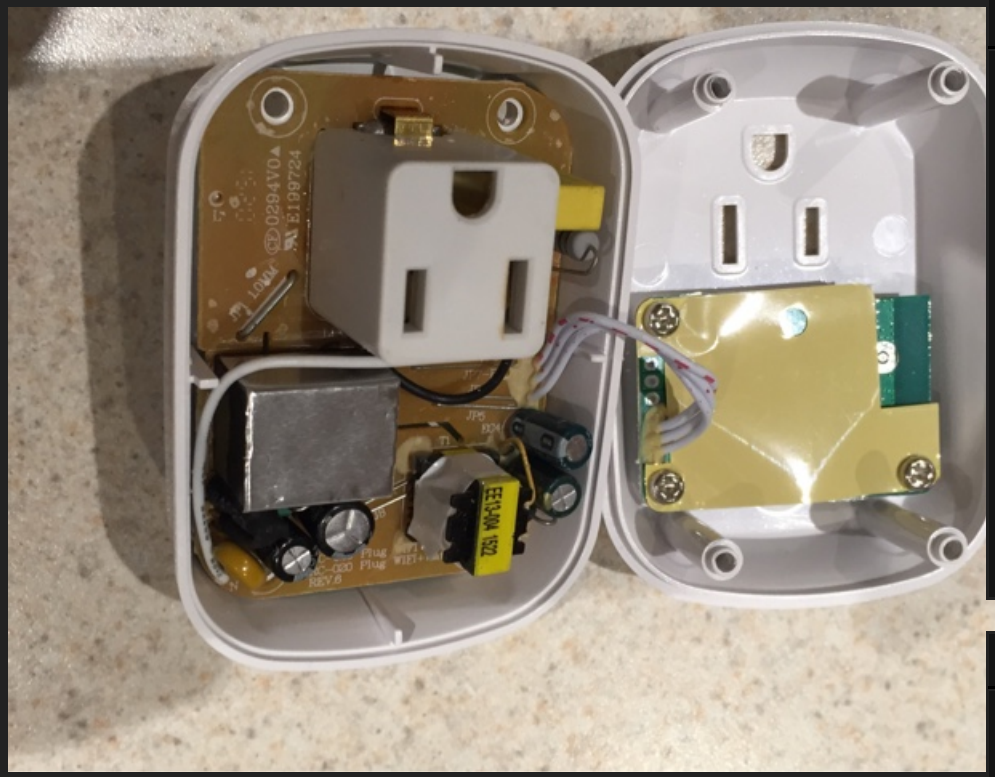
Pages

Home
DIY Macro Rail
DIY Laser CNC
Universal Temperature Controller
DIY Powder Coating
DIY Coffee Roasting
BMW e36 M50 Intake Manifold Customization
Ontario Internet
DD-WRT / Router Hacking / Shairport

Subscribe To

Posts
Comments

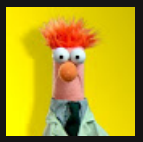
optional power meter monitors voltage; current and power factor of the load.



Blog Archive

- ▼ 2016 (2)
  - ► May (1)
  - ▼ February (1)
    - EcoPlug Wifi Switch Hacking
- ► 2014 (2)
- ► 2013 (6)
- ► 2012 (5)
- ► 2011 (18)
- ► 2010 (8)
- ► 2009 (1)
- ► 2008 (2)

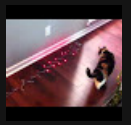
About Me



Scott Gibson

View my complete profile

Popular Posts



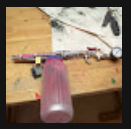
Raspberry Pi and the WS2801

Update (October 29th): Big update here:

http://thegreatgeekery.blogspot.ca /2012/10/pixelpi-update.html Update (August 19th): - Pi...

EcoPlug Wifi Switch Hacking

I opened up an ecoplug module bought from Home Depot. They are currently on clearance for $15 Canadian each (about $12 US). The switches...



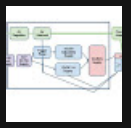
Powder Coating

Update2: Description, Schematics and boards

http://thegreatgeekery.blogspot.com /2011/10/powder-coating-system-mk-ii-progress.html Updat...

PixelPi Update

So lots has been going on with PixelPi since my last update: Rearchitecture: I've forked (https://github.com/mostley /PixelPi) github...



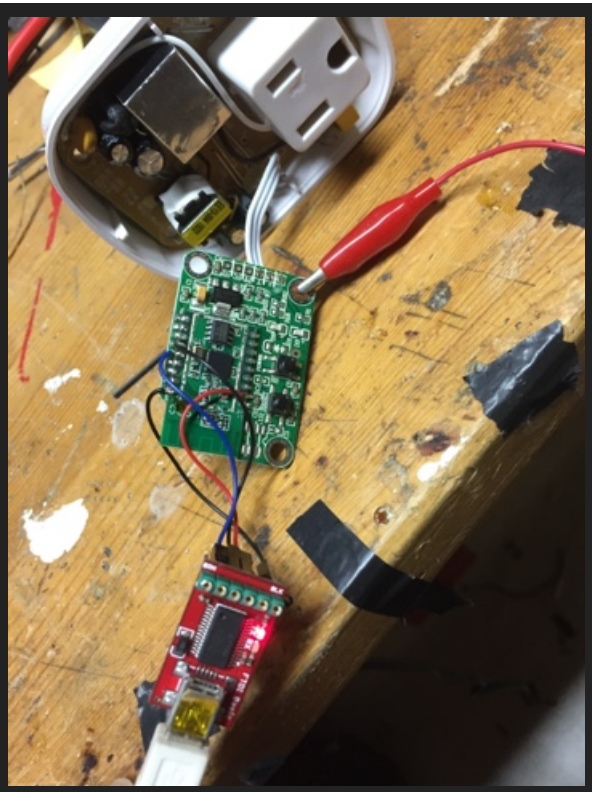
Powder Coating Build Follow Up

Update: Build Progress of the next version here; including schematics and board layouts http://thegreatgeekery.blogspot.com /2011/10/powder-...

Subscribe To

Posts

Comments



Followers

Backside of the power board; lots of depopulated parts which would be used for the optional power monitoring.

Posted by Scott Gibson at 7:04 AM

Reactions: funny (0) interesting (2) cool (2)

+4 Recommend this on Google

70 comments:

acidice333 said...

Are they listed on the Canadian home depot site? ...and where in the store did you find

yours? I'm hoping the one here in BC have some left.

February 7, 2016 at 6:19 AM

Scott Gibson said...

I got two boxes of 2 each at the Home Depot in Kanata Ontario last week.

February 7, 2016 at 7:34 AM

acidice333 said...

ended up finding a few here but sadly they were 29$ each so not quite discounted

February 7, 2016 at 4:43 PM

Anonymous said...

Nice work! I like your captive portal code but couldn't access it (lib folder) on github page?

February 7, 2016 at 10:23 PM

Anonymous said...

Home Depot Kanata has 55 of them.. But they are not at eye level... they are way up in the shelves..

February 8, 2016 at 9:57 PM

Unknown said...

$29 in manitoba

more info:
http://forums.parallax.com/discussion/162862/wifi-controlled-outlets/p2

February 8, 2016 at 10:47 PM

Rob Shearer said...

This looks interesting: Sonoff - WiFi Wireless Smart Switch For MQTT

February 8, 2016 at 10:59 PM

roger said...

Hi
Where do I find the button library

tried net an the one I found won't work
Thanks

February 9, 2016 at 6:13 AM

Scott Gibson said...

I explicitly added the libraries to the github repository; so you don't need to track them down now.

February 9, 2016 at 6:48 AM

Scott Riesebosch said...

Scott can you please call email me if you'd be interested in doing some software development work with the ESP8266? sriesebosch@gmail.com

February 10, 2016 at 11:27 AM

Kevin Groce said...

Hey Scott I created a hack.io page Detailing various pages from around the web using this module. I am going to link you back to it. Also i wanted to let you know Walmart sells them under a different name too and I do think they also sell the one with the current shunt in them.

February 12, 2016 at 12:21 PM

Garrett said...

Thanks Scott! I got a bunch of these on clearance at Home Depot last month. I'm still new to the ESP8266 and trying to learn more about it.

February 12, 2016 at 11:38 PM

Anonymous said...

was wondering if you have got your hands on one with the current sense, voltage, and power factor? and have done any work on those features

http://www.walmart.com/ip/Generic-CT-065W-WorkChoice-1-Ol-Wi-Fi-Indoor-Switch-White/46721978

February 13, 2016 at 2:11 PM

John said...

Scott, thanks so much for all of the work.

I've implemented your firmware without issue on my ecoplugs. I'm able to connect to the switch via it's IP address and can turn it on and off via /on and /off commands.

I'm now looking to integrate the switch into my OpenHAB setup via mqtt. I see that there are fields for server and port details, which I've populated, submitted and get at 'ok' response from the board.

If I then refresh the boards webpage, the fields are blank again with the exception of the port field.

It's also not clear to me how to define the mqtt topic that the switch would publish/subscribe to to be commanded by OpenHAB or push it's state to OpenHAB.

Any guidance would be appreciated as I'm just learning all of this over the past couple weekends.

Thanks again.

February 15, 2016 at 12:39 PM

Scott Gibson said...

Hwy John; glad you're using it. I'll be pushing an update tonight or tomorrow with mqtt support. I hit some issues as there are two pubsubclient libraries with different versions and slightly different API's. Keep an eye on github.

February 15, 2016 at 4:22 PM

adamrgolf said...

Scott, this is awesome! Once your custom firmware is loaded, is the device still accessible by the ios apps (ECO Plugs / WiOn)?

February 16, 2016 at 8:01 AM

Scott Gibson said...

The new softawre leaves the legacy software behind; if further analysis of the protocol is added I wouldn't be opposed to adding in support. There is some multicast discovery happening which I havn't looked into.

February 16, 2016 at 10:18 AM

Beach Geek said...

Hi all,
I've mirrored Scott's work on the EcoPlug and retrieved a dump of the serial console output with the default firmware. Posting here for anyone interested. XXXYYYZZZ is the SSID of the wifi network the EcoPlug was configured to connect to.

My unit *does* have the power monitoring hardware which is depopulated in Scott's hardware. I'm in process if trying to figure out how it is connected to the ESP8266 so power usage details can be included in Scott's firmware.

Does anyone know how to extract a hex from an ESP8266 that is able to be re-loaded later? Ie, is there a way I can save the default firmware?

Console output below:

```
*****************BOX INFOR**********************
^_^Hello,ESP8266!
FirmWare Ver:1.6.0
SDK Ver:1.0.0
Compile Time:May 28 2015,14:18:25
data : 0x3ffe8000 ~ 0x3ffe89e4, len: 2532
rodata: 0x3ffe89f0 ~ 0x3ffe90a0, len: 1712
bss : 0x3ffe90a0 ~ 0x3fff4228, len: 45448
heap : 0x3fff4228 ~ 0x3fffc000, len: 32216
[Memory_Infor]Heap is:31944
****************************************
[Flash]Read the Dst:1
[^_^]Get Power Detect Write_OffSet_flag:10
[Flash]SN SLqrXGZsiM Read Flash 3 Sector0+1024+512 Successful !
[Flash]Factory Infor IP: 203.66.65.34 SSID:ECO-Plugs Wifi_Main_Name:ECO- Read
Flash 3 Sector0+1024+512+128 Successful !
nRouter_Conn_Flag:1
[15SX_D]Write 2014-01-01-0-0-0 to Flash
[15SX_D] Basic SN:SLqrXGZsiM alias:dwmeco1 pwd:78024662
[15SX_D]Internet Top-Cms:61.220.255.143 M-P2P:203.66.65.34 S-P2P:203.66.65.34
Wifi_Main_Name:ECO-
[Wifi]Try to re-Connect SSID:XXXYYYZZZ PWD:
^_^Connect Front Router SSID:XXXYYYZZZ, PSW:
^_^Creat UDP BoardCast :25!
^_^Creat Comm Server Success :80 !
[Memory_Infor]Heap is:21320
^_^Creat TCP Upgrade Server :1932!
[15SX-D]SSID: SLqrXGZsiM in_ssid:SLqrXGZsiM PWD:78024662 Main_Name:ECO-
78024662 Version 1.6.0 2015-05-28
[15SX-D]P2P-Svr Create esp_udp Socket at Port: 48440 p2p_port:11620
Main_Name:ECO-78024662 TopCms:61.220.255.143 Wifi_Main_name:ECO-
[Memory_Infor]Memory is:20976
mode : sta(38:2b:78:02:46:62)
```

add if0
No Press Long Key,Exit Time!
[Flash]Write Flash DST:1
scandone
no XXXYYYZZZ found, reconnect after 1s
reconnect
[15SX_D]Send Reg to P2P Server :203.66.65.34
####WH_Data:48
####WH_Data:0
####WH_Data:0
####WH_Data:0
Hw ret_data:0
[Pow_detect]A ret_data:434531 362
W ret_data:0 1723
V ret_data:12318 [1089 ~ 6535]
#######Today_Hw_Total:0
scandone
no XXXYYYZZZ found, reconnect after 1s

February 16, 2016 at 6:53 PM

Beach Geek said...

Some more GPIO info:

On the ESP unit, the pin about GPIO13 is GPIO12. The pin about that is GPIO14. So, reading down the left side of the ESP unit in the picture, the pin order is GND, VCC, RESET, unknown, GPIO14, GPIO12, GPIO13, GPIO15, GPIO2.

In my tests, writing HIGH to GPIOs 7, 8, 9, or 11 (and possibly more) cause the unit to either sleep, crash, or reset - still investigating this.

I have not been able to determine anything about the current monitoring hardware and how it is connected to the ESP uC.

February 17, 2016 at 6:11 PM

Beach Geek said...

Oops, in last comment "about" should be "above" in first and second sentence.

February 17, 2016 at 6:12 PM

Anonymous said...

Hey scott,

15$ price that you mentioned. Do you mean 15$ for each outlet ? or 15$ for the box (which contains 2 outlets) ?.

February 19, 2016 at 10:10 PM

Vladimir Razgulin said...

What are the three wires going from the power board to the digital board?
AC or DC?

February 21, 2016 at 6:39 PM

Peter Feerick said...

@Vladimir: Looks like it would be DC. If you look at the pinout diagram, you can see that that two of the wires trace back to the regulator located at the bottom right of the board. So possibly 5v or 12v DC, regulated down to probably 3v3 for the ESP8266.

February 22, 2016 at 1:07 AM

Randy Glenn said...

I'm trying to upload the firmware from Github to my outlet, and it isn't running - no debug info on the serial port. I'm wondering if it's the flash chip - do you know what size it is? My guess right now is that SPIFFS is trying to access flash that doesn't exist, so it's dying early on. More investigation later...

February 24, 2016 at 2:59 PM

Unknown said...

I was looking into the current sense; U2 appears to have the lable 1588NAZ04 on the bottom. Haven't found anything that tells what it is. Pin 5 is connected to GPIO0 for what seems like a clock and Pin6 goes through a resister as a input into GPIO12. Almost seems like a I2C device. Anyone else have a clue?

February 27, 2016 at 1:10 PM

Dario said...

The current/voltage sensor seems to be the HLW8012 (it is visible on my unit). There is some description for the chip in this page: http://www.tlola.com/en/Industry_Knowledge /2015/0828/64.html. It doesn't look like the communication is I2C though...

February 27, 2016 at 6:49 PM

Dario said...

Found some specs for the chip here: http://www.hiliwi.com/products_detail /&productId=36.html (chinese, use google translator). Not i2c, pwm output and input it seems...

7 CF1 Digital Output
SEL = 0, CF1 output RMS current, pulse duty 50%
SEL = 1; CF1 RMS output voltage, pulse duty cycle of 50%

February 27, 2016 at 6:54 PM

David Ewing said...

The 1588NAZ04 U2 (ESP8266 board) is connected to U1 (HLW8012 on the power board). It seems to take the 3 pulse signals from the HLW8012 and turns them into some kind of Manchester encoded data stream (clock + data) that the ESP8266 reads on GPIO12.

This makes the design more complex since it would have been just as easy to use the ESP8266 to count pulses rather than involving another IC.

My investigation continues - will work on some code to capture the data coming to the ESP8266 and see if it makes any sense.

February 28, 2016 at 1:03 AM

David Ewing said...

Just an update; does not appear to be Manchester encoded data, but clocked out via GPIO0 to GPIO12. The factory software clocks this data out at an inconsistent rate that made it look like Manchester encoding. Still might be I2C, but not quite sure. If only someone could find a manual for that chip or attach a bus pirate.

February 28, 2016 at 6:15 PM

Steve said...

I picked up 3 boxes of these on clearance at Home Depot in Halifax for $25.98 apiece. Each box has two units in giving a unit price of $13 (I think this may be where some of the pricing confusion is coming from). Home Depot appear to be dumping them as they are no longer listed on their web site and other stores in the area don't have them.

One other gotcha that may help people - to flash the rom tack solder gpio0 to ground and power cycle, there will be no response from the unit (not even a LED flash) but it is ready to receive a flash at 115200.

March 2, 2016 at 9:10 AM

Anonymous said...

well, finally to figure out on HLW8012

HLW8012 is a dummy power meter.

CF1 and CF output is dyanmic frequency with 50% duty cycle.

this means, you need to check the freq on CF1 and CF2 to know V and I consumption.

the chinese datasheet shown on how to do "freq" calcuation..

FCF is active power calcuation in freq
FCFI is RMS current calculation in feq
FCFV os RMS voltage calculation in freq

you need to detect freq on CF and CF1. the range should be 0-1KHz that depends on crystal Freq and Vref.

March 2, 2016 at 12:21 PM

Paul said...

Very interested in this project.

Can you comment; how is the stock firmware/app working through firewalls? I assume it must be doing some sort of long polling to the eco plugs server? What is the mechanism?

I would be interested in having a copy of the stock firmware so that I could revert if needed.

March 9, 2016 at 1:03 PM

Anonymous said...

I am also interested in figuring out how the units read the power load. I was able to get my logic analyzer connected to one. I see what looks like a clock on GPIO0 and data on GPIO 12. From the clock I see four 8 bit cycles followed by three 32 bit cycles. The eight bit cycles seem to be a header in that they are the same. The three 32 bit numbers are changing. I would assume they correspond to the voltage and current numbers output on the serial interface.

March 20, 2016 at 6:42 PM

Anonymous said...

I wrote a script to monitor the output on pins GPIO0 and GPIO12. I get a 128bit output in 5 second intervals but I have not been able to find anything that relates to voltage, current, and wattage. Here is my code. I used pins 4 and 5 from a second arduino board.

```
int clock_high = 0;
int clock_low = 0;
int last_clock = 1;
int current_clock = 1;
int i;
int tmp_poition = 0;
unsigned long tmp = 0;
unsigned long loopTime;

byte byte_array[16];

void setup() {


pinMode(4,INPUT);
pinMode(5,INPUT);

Serial.begin(115200);
delay(100);

Serial.println("\n\nData Monitor. SCL: D4 and DATA: D5");
}


void printBits(byte myByte){
for(byte mask = 0x80; mask; mask >>= 1){
if(mask & myByte)
Serial.print('1');
else
Serial.print('0');
}
}

void loop()
{
loopTime = millis();
i = 0;
tmp_poition = 0;
while((millis() - loopTime) < 1000)
{
current_clock = digitalRead(4);

if( (current_clock != last_clock) && current_clock == 0)
{
```

```
clock_low++;
last_clock = current_clock;
}

if( (current_clock != last_clock) && current_clock == 1)
{
clock_high++;
last_clock = current_clock;

byte_array[i] = byte_array[i] << 1;
byte_array[i] |= digitalRead(5);
tmp_poition++;

if(tmp_poition++ > 7)
{
tmp_poition = 0;

if(i < 15)
i++;
}
}
}

if(clock_low > 1)
{
//Serial.print("D4: ");
//Serial.println(digitalRead(4));
//Serial.print("D45: ");
//Serial.println(digitalRead(5));

//Serial.print("High Count: ");
//Serial.println(clock_high);
//Serial.print("Low Count: ");
//Serial.println(clock_low);

//Serial.print("\nBytes 9,10,11: ");
//Serial.print(byte_array[9]);
//Serial.print(" ");
//Serial.print(byte_array[10]);
//Serial.print(" ");
//Serial.println(byte_array[11]);


//Serial.print("32 - 32 - 32: ");
```

```
tmp = ((unsigned long)byte_array[3] << 8) + byte_array[5];
tmp = (tmp << 8) + byte_array[6];
tmp = (tmp << 8) + byte_array[7];
//Serial.print(tmp);

//Serial.print(" ");
tmp = ((unsigned long)byte_array[8] << 8) + byte_array[9];
tmp = (tmp << 8) + byte_array[10];
tmp = (tmp << 8) + byte_array[11];
//Serial.print(tmp);

//Serial.print(" ");
tmp = ((unsigned long)byte_array[12] << 8) + byte_array[13];
tmp = (tmp << 8) + byte_array[14];
tmp = (tmp << 8) + byte_array[15];
//Serial.println(tmp);


// Display output in Hex
for (i = 0; i < 16; i++)
{
Serial.print("0x");
Serial.print(byte_array[i], HEX);
Serial.print(" ");

//byte_array[i] = 0;
}
Serial.println("");


for (i = 0; i < 16; i++)
{
//Serial.print(byte_array[i], BIN);
printBits(byte_array[i]);
Serial.print(" ");

byte_array[i] = 0;
}
Serial.println("");
Serial.println("");
}
else
{
for (i = 0; i < 15; i++)
```

```
byte_array[i] = 0;
}

clock_high = 0;
clock_low = 0;

while(digitalRead(4) == 1)
clock_low = 0;
}
```

March 23, 2016 at 10:45 PM

Stive Peterson said...

This comment has been removed by a blog administrator.

April 22, 2016 at 6:57 AM

David Ewing said...

Had some time to investigate the power monitoring. Here is the quick and dirty:

There is some unknown IC connected to the power monitoring chip that appears to convert the pulses from the power monitor chip everyone has already idenfied into I2C device on Pin 12 for data and Pin 0 for clock. You can then read 16 bytes from it on a regular basis. The first 4 bytes (unsigned long low byte first) appear to count the current or power not sure which. Everytime you read from that chip, the count is reset, so the speed the data is read from it is important part of the calculation used.

I setup mine to read every 10 seconds and use a formula that I came up with by testing with several loads. Different timings require adjusting the formula. I have noticed that occationally, the count doesn't get reset. It may be necessary for your application to keep a running average and/or ignore data that represents a sudden change for several readings.

Here's just a quick code fragment to demo this below. This code is partially extracted from a much larger custom home automation system that I've built. Data structures have been simplified here.

```
//Initialize stuff
#include

byte d[16],count;
unsigned long value;
int watts;
```

```
pinMode(12, INPUT_PULLUP);
Wire.begin(12, 0);

while(true)
{
count=0;

// Request 16 bytes
Wire.requestFrom(0, 16);

while(count<16)
if (Wire.available())
d[count++]=Wire.read();
else
yield();
value=d[3];
value=(value<<8)+d[2];
value=(value<<8)+d[1];
value=(value<<8)+d[0];
watts=(value/(400-(value/1800)));
Serial.print("Watts: ");
Serial.println(watts);
delay(10000);
}
```

Hope you guys find this useful. With further testing, it should be possible to identify the other 3 long values. There should be current, voltage, and power at least given what my test probes of the connections between the mystery chip and the HLW8012.

April 26, 2016 at 6:32 PM

David Ewing said...

Correction: It is High byte first.

The code would change like this:

```
value=d[0];
value=(value<<8)+d[1];
value=(value<<8)+d[2];
value=(value<<8)+d[3];
```

April 26, 2016 at 6:48 PM

Scott Riesebosch said...

Apparently the mystery chip is a micro-controller but I don't know which one. I also have a copy of what I believe is the original firmware but not sure.

April 26, 2016 at 8:56 PM

David Ewing said...

Scott, I can't imagine that the original firmware is of much use unless someone wants to return the thing to factory default. I think we can agree is not that desirable as I believe people have already identified that your SSID and password are sent in clear text to some server in China. I also think disassembling the ESP8266 code would be a nightmare.

With all the efforts everyone has put in, we can flash the ESP8266, control the relay, and read the button. Now with the I2C code, we can at least get a estimated watts being used. Just a matter of more experimentation to map the other values to current and voltage readings. Someone with a better electronics workbench and gear than I have might be able to do that - since I was just using a fan, some lights, and a toaster as load sources and a meter to measure current.

I suppose it might be interesting to integrate this into the github code to make it all plug and play.

April 26, 2016 at 10:31 PM

Steve Pierce said...

Walmart.com has them for $14.88 each as of Apr 28, 2016

April 28, 2016 at 1:08 PM

Anonymous said...

There was an exploit to get root access to the stock firmware on a similar module described at https://labs.bitdefender.com/2016/08/hackers-can-use-smart-sockets-to-shut-down-critical-systems/

Might be a route for getting fresh firmware on the devices without cracking them open, and all the more reason to write open source firmware for these.

August 19, 2016 at 2:27 AM

Anonymous said...

Does anyone know any power switch with esp8266 for the european market?

September 15, 2016 at 11:09 AM

Anonymous said...

A hearty thanks. I originally found the instructable for this project and migrated over here for more help. After originally trying with an arduino uno, voltage divider etc I finally caved and found a ttl adapter locally yesterday. Got the original firmware out and stock esp firmware in last night and played around with AT commands for a while before quitting. After dealing with some library issues, and remembering which button to hold and which to release got your firmware installed. FYI Home depot's web page is listing these again, possibly for the holidays. Watch for them again after Christmas. Now to try to figure out openhab and getting this connected there.

October 6, 2016 at 1:27 PM

Anonymous said...

Sorry forgot to post Home depot link.
http://www.homedepot.com/p/15-Amp-Wi-Fi-Adapter-Single-Outlet-White-CT-065W/206948864
web page says they are in seasonal in our store

October 7, 2016 at 1:49 AM

Chuck said...

Excellent project! I found one of these switch at Wal Mart called the Eco WiFi switch and quickly came across your code here. Had some issue with the Arduino IDE with esp8266 board - using Generic ESP8266 Module and the default flash size of 512k kept getting a fatal error (28) - then stumbled on setting that to 1M (512k SPIFFS) and then it all works - also had to change ON = 1 and OFF = 0 to work right, but it's talking thru my mqtt server now.

Thanks again!

October 8, 2016 at 11:55 PM

Chuck said...

Also - had to put a server.send(200, "text/plain", "ok");
in handle_on() and handle_off() otherwise the browser or wget would just spin waiting for a reply (and the browser would keep requesting the page which would override anything injected via mqtt!).

October 9, 2016 at 10:50 AM

Peter Fales said...

Has anyone tried the current measurement code? I'm having a few issues. It seems to "sort of" work. I get values out of it, those values are close to zero when no current is being drawn, and nonzero when something is plugged in. But other than that, the values

don't seem to reflect any consistent measurements. I'm measuring every 10 seconds (like the sample code) so I would expect to get values around 100. Typical values I see are around 54, or around 475. Values in those ranges are typical, but I've seen other values too.

October 15, 2016 at 5:50 PM

Unknown said...

search for "workchoice indoor switch" on walmart.com, 18$ each, and have the voltage reading chips in them.

October 27, 2016 at 3:10 AM

Unknown said...

Super excited by this! Found a ton at a REStore: habitat for humanity near me, cheap.

I was trying to use a 3.3v micro controller (spark core, also a particle photon, the more recent version) as a serial bridge between the ESP and my laptop. (The Spark Core has a hardware UART) and everytime I hooked up the serial pins the ESP would turn off its lights - same behaviour as if the serial pins were shorted to each other on the ESP. Removing the serial connection (also unshorting the TX/RX) and the ESP would apparently reboot. Any thoughts?

I'm also going to try to make a jig so I can do this without soldering (although I'm not sure how I'd ensure contact).

October 28, 2016 at 11:49 AM

Unknown said...

Went back to my Spark Core after reading the difference between .write and .print and it worked first try. Now on to the fun stuff, thanks for this.

(First cut at the jig wasn't stiff enough to maintain pin contact)

November 4, 2016 at 1:56 PM

Anonymous said...

Home Depot in the states (well in PA and OH at least) has the single outlet for $7.77 USD. It is the Ct-065w and the bar code is 82721 406057.
Eco # 1001 763 273.

Can someone point me to a description of how to dump the existing code?

December 30, 2016 at 1:51 AM

sognovero said...

I'm running a bunch of these and concerned about the hackability. But all of this is Greek to me. Is there any easy way for me to make these more secure without opening up the device? Thanks!

January 16, 2017 at 12:42 PM

Chris said...

I'm using an FTD1232 and I can connect to the Eco plug using Putty but all I get is the following data in the terminal window, over and over and over. How do I get this thing to accept AT commands?

reconnect
[15SX_D]Send Reg to P2P Server :210.61.12.186
scandone
state: 0 -> 2 (b0)
state: 2 -> 3 (0)
state: 3 -> 0 (19)
reconnect
scandone
state: 0 -> 2 (b0)
state: 2 -> 3 (0)
state: 3 -> 0 (19)
[15SX_D]Send Reg to P2P Server :210.61.12.186
reconnect
esp8266 scandone
state: 0 -> 2 (b0)
state: 2 -> 3 (0)
state: 3 -> 0 (19)

January 19, 2017 at 8:59 PM

David Ewing said...

The stock firmware is designed to talk with some server in China and the phone application talks to the same server and provides your Wifi password information so it can get onto your network. I believe many people have looked at this communication and found it was pretty insecure, plus some unknown entity now has a copy of your WIFI SSID and password. Stock firmware doesn't really have any interface (network or serial) that lets you do anything useful with it. It won't accept AT commands.

To be able to not only get a much more secure product, you have to replace the firmware. The only way to do that is to open it up, connect up serial lines, reset, and GIPO0 and flash it just like any other ESP8266. Basically following this article as a guide. No real shortcuts here I'm afraid. Takes about 30 minutes per module once you do it a few times.

January 19, 2017 at 9:17 PM

Michael Maeda said...

Has anyone gotten MQTT and remote control of the switch working with the homie firmware? I was able to set it up with homie and it is connecting to my WiFi but I can't seem to control the switch. Should I be seeing MQTT updates when I press the button?

January 23, 2017 at 12:08 AM

Scott Gibson said...

I have it working; look at this example (https://github.com/marvinroger/homie-esp8266/tree/develop/examples/IteadSonoffButton) it will work once you modify the pin definitions.

January 23, 2017 at 7:41 AM

Randy Glenn said...

Michael, I have a fork of Scott's code with the button updating MQTT as well:

https://github.com/rglenn/esp8266Switch

Scott, I plan to clean this up a bit and submit a pull request When Time Permits.

January 23, 2017 at 3:40 PM

Michael Maeda said...

Thank you. I updated the pin assignments for the button, LED, and relay this morning using Scott's code and I began getting MQTT updates. I wasn't able to get the state to change in response to a publish though. Should that functionality be working? I'll give your fork a try once I get home this evening.

January 23, 2017 at 3:44 PM

Randy Glenn said...

Michael, keep in mind that to control a Homie device from MQTT, you need to write to a different topic than the one that reflects the state. So if you have an ecoplug set up as:

homie/an-ecoplug/switch

then the current state is in the topic

homie/an-ecoplug/switch/on

and to change the state, you publish to

homie/an-ecoplug/switch/on/set

Hope this helps!

January 23, 2017 at 3:49 PM

Michael Maeda said...

Thanks Randy! When I published to /set the plug responded. I appreciate your help.

Is there a topic I can publish to that will return the current switch status?

January 31, 2017 at 8:42 PM

Randy Glenn said...

Michael: to the best of my knowledge, you can only check the status by subscribing. I believe that Homie defaults to using retained messages by default, so the current state will be sent when you subscribe (without retained messages, you only receive messages when the state changes).

February 1, 2017 at 11:53 AM

David Lang said...

has there been any further progress on decoding the power data?

I'm working on modifying https://github.com/arendst/Sonoff-Tasmota to support these devices. I have it modified to support the switch, and I have it gathering something that looks like data, but it doesn't result in anything that seems sane

February 27, 2017 at 5:32 AM

David Lang said...

for what it's worth, I'm using http://www.homedepot.com/p/Woods-WiOn-Indoor-Wi-Fi-Current-Tap-with-2-USB-Charging-Ports-Wireless-Switch-and-Programmable-Timer-50055/206758644 also available on Amazon https://www.amazon.com/WiOn-50055-Indoor-Monitor-Wireless/dp/B00ZYLUBJU/ref=sr_1_4?s=hi&ie=UTF8&qid=1487485998&sr=1-4&keywords=wion

There was a question earlier about european plugs, there are these for <13 euro https://www.itead.cc/smart-home/smart-socket.html

February 27, 2017 at 5:52 AM

Beach Geek said...

@David Lang:

Check https://bitbucket.org/xoseperez/espurna. There is support for this device (called ecoPlug in the firmware) and support for some power monitoring chips in the Sonoff devices - so if your WiON / ecoPlug device has the power monitoring chip, you might be able to add in the code from this firmware to support it.

February 27, 2017 at 11:15 AM

David Lang said...

These devices are not supported by the firmware at https://github.com/arendst/Sonoff-Tasmota

the power monitoring chip in the itead sonoff pow is the same chip as in these devices, but it's connected up directly to the esp8266 where I understand that on these systems there is some other intermediate chip.

I'll poke around and check if it's really setup that way or if it's directly connected on ports 0 and 12

February 28, 2017 at 6:00 PM

David Lang said...

@Beach Geek, the espurna firmware doesn't have support for the power sensing

February 28, 2017 at 6:27 PM

Marcus said...

Did two of these and run with home assistant-works great.

Does anyone know if the outdoor version (black with plug) https://www.google.ca/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwiX6PjHlffSAhUs64MKHSpWCO8QjRwIBw&url=http%3A%2F%2Fwww.kab-cable.com%2Fproduct_description.php%3FPNo%3D470&psig=AFQjCNE1MuLU-b6trZVL0fTA-4tSBa73hg&ust=1490720713001085

is the same hardware inside?

Marcus

March 27, 2017 at 1:05 PM

Peter Fales said...

Has anyone tried to flash these devices with software that supports OTA (Over The Air) updates with ArduinoOTA? OTA is very cool, and I use it with most of my esp8266 based devices. Once the initial software is installed, you can send updates directly to the device

without having to remove it from it's installed location and carry it to a computer for programming. I've used it with a number of different devices, including re-flashed devices with embedded esp8266's like the Sonoff switches. But for some reason, I can't get it to work on these ecoplug/workchoice devices.

May 7, 2017 at 8:24 AM

Beach Geek said...

OTA working on ecoPlug for me using the espurna firmware.

May 7, 2017 at 11:21 AM

Unknown said...

the tasmota firmeware supports ota upgrades. I don't think it uses the ArduinoOTA library, when the subject came up IIRC the discussion as that that particular library would add significantly to the image size, pushing it over the limit to be able to be upgraded.

David Lang

May 18, 2017 at 7:02 AM

Post a Comment

Links to this post

Create a Link

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)