Proxmark3 V3.0 DEV Easy Kits Manual

Description

The Proxmark3 is an open-source device developed by Jonathan Westhues that enables sniffing, reading and cloning of RFID (Radio Frequency Identification) tags. The Proxmark3 could be arguably regarded as the most powerful device currently available for researching RFID and Near Field Communication systems. The FPGA allows it to meet the demanding communications timing requirements imposed by various RFID systems. The device targets low and high frequency systems operating at 125 kHz, 134 kHz and 13.56 Mhz.

Watch this video Mifare Hack.

Proxmark3 V3.0 DEV Easy Kits have upgraded from Proxmark3 V2.

Compared with Proxmark3 V2, we made some improvement for V3.0 as below :

1、Built-in high frequency antenna, perfectly compatible, eliminate dead zone, read the card data smoothly without interruption.

2、Increase the speed of parse the key , compatible with all size cards.
3、Detect and read data completely and stably with low error rate.

4、Adopt low frequency antenna to improve SNR(Signal to Noise Ratio),more higher recognition rate, detachable design to meet kinds of needs.

5、Remove antenna interface to avoid plug in and out, more conveniently.

6、Remove the lithium battery interface,more simple. (Offline mode can use portable power source).

7、Optimized circuit and remove some irrelevant components, cut down cost, lightweight and portable.

Electrical Parameter

When Low frequency antenna installed on the right side :

LF antenna: 29.84 V @ 125.00 kHz
LF antenna: 32.31V @ 134.00 kHz
HF antenna: 28.43V @ 13.56 MHz

When Low frequency antenna installed on the left side :

LF antenna: 43.86 V @ 125.00 kHz
LF antenna: 24.48 V @ 134.00 kHz
HF antenna: 25.13 V @ 13.56 MHz

Operating Voltage : 3.5-5.5V
Operating Current : 50-130mA
Dimensions : 54mm * 86.6mm
Size : 6.2mm (thinnest) 9.8mm (plus screw) 15.8mm (plus LF antenna)

Supporting Cards and Tags

Tags	Recognize	Read& Write	Advanced Operation					
			Offline Decryption	Online Sniffing	Default Key Crack	Data Dump	Simulation	Copy
MIFARE CLASSIC	√	√	√	√	√	×	√	√
MAFARE CLASSIC (CHINESE Magic Card/UID)	√	√	×	√	√	√	×	√
MAFARE Ultralight	√	√	×	×	×	√	×	×
HID	√	√	×	×	×	×	√	√
HID iClass	√	√	√	√	×	√	√	√
ISO14443a	√	√	×	√	×	√	√	√
ISO14443b	√	√	×	√	×	×	√	√
ISO15693	√	√	×	√	×	√	√	√
SRI512	√	√	×	×	×	×	√	×
SRIX4K	√	√	×	×	×	×	√	×
Legic	√	√	×	×	×	√	√	×
epa	√	√	×	×	×	×	×	×
em410X	√	√	×	×	×	×	√	√
Em4x50	√	√	×	×	×	√	√	√
Ti	√	√	×	×	×	×	×	×
Hitag/Hitag2	√	√	×	√	×	×	√	×
indala	√	√	×	×	×	×	×	√
T55xx	√	√	×	×	×	×	×	√
FlexPass	√	√	×	×	×	×	×	×
VeriChip	√	√	×	×	×	×	×	×
PCF7931	√	√	×	×	×	×	×	×
Kantech ioProx	√	√	×	×	×	×	×	×

Resource

1、Basic Document

* Download Manual

* Software pm3-bin-2.0.0 (visit this page for the latest version)

2、Video instruction

* Video: how to install driver

* Video: how to upgrade firmware

* Video: how to read/write Mifare classic

* Video: how to hack/clone Mifare classic

* Video: how to clone EM410x tags

3、Official Wiki

* Proxmark3 official wiki (new)

* Proxmark3 official wiki (old)

The Proxmark has proven itself to be an invaluable tool within the research community. Here are some examples of how the Proxmark has been used to perform research:

* Proxmark3: The Swiss Army Knife of Security Research

* Exploring the NFC Attack Surface

* A Practical Attack on the MIFARE Classic

* Analysis of the MIFARE Classic used in the OV-Chipkaart project

* Potential Misuse of NFC Enabled Mobile Phones with Embedded Security Elements as Contactless Attack Platforms

* Outsmarting Smart Cards

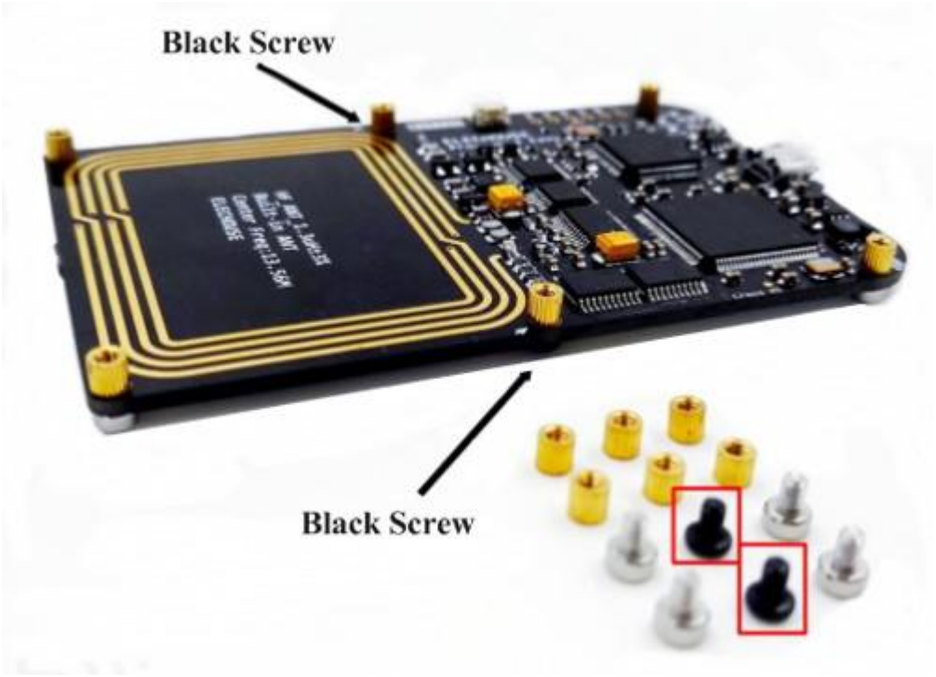
* Evaluation of the feasible attacks against RFID tags for access control systems

The Proxmark also makes a great educational tool. The entire platform (including hardware and software) is open source and can be readily analyzed and inspected. The Proxmark includes many of the major components found in a general purpose SDR but is simpler and therefore easier to understand. Faculty members should contact us about educational discounts if interested in incorporating the Proxmark into a course of study.

Warning: The Proxmark3 is a research and development tool. It has not been evaluated for compliance with regulations governing transmission and reception of radio signals. You are responsible for using this product in compliance with your local laws.

Assemble Instruction

1、Proxmark3 V3.0 DEV Easy Module



2、Assemble the protection shell

3、Assemble the LF antenna

4、Paste the protection film for back

Software

Visit this page to download the latest version:
http://proxmark.org/forum/viewtopic.php?id=1562

The Zip file contains driver for windows, firmware for Proxmark and client software for windows.

No driver installation is required on Linux based machines.

Note: Operating your Proxmark with the wrong client software version will produce unpredictable results and could lead to damage of the device. The client software does not verify that it is communicating with a compatible version of firmware. So read carefully the product page to confirm your firmware version where you purchase this product.

Windows 7 Driver Installation

(Please turn off Driver signature certification on your PC)

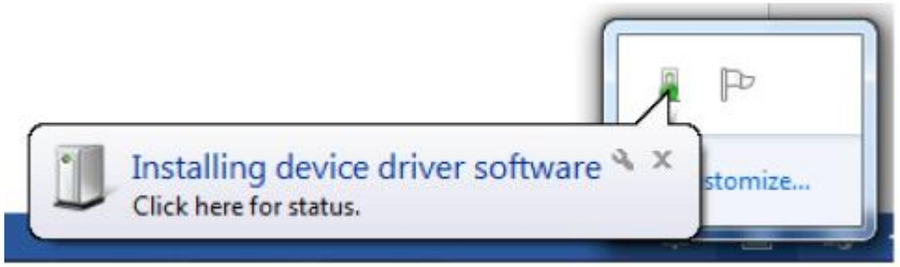
Recent versions of the Proxmark client require the use of a libusb "driver" on the Windows hosts. Please install the driver according to the steps as below:

Step 1:

Download the software: Software pm3-bin-2.0.0 (visit this page for the latest version).

Step 2:

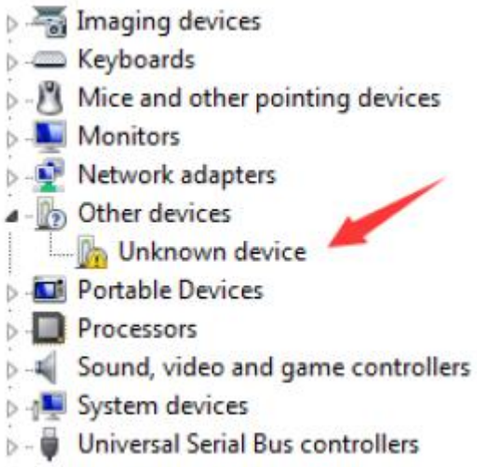
Connect your Proxmark board with PC via USB cable. Windows Update starts to search driver.



After a while, it will tell you "Fail to find the driver"

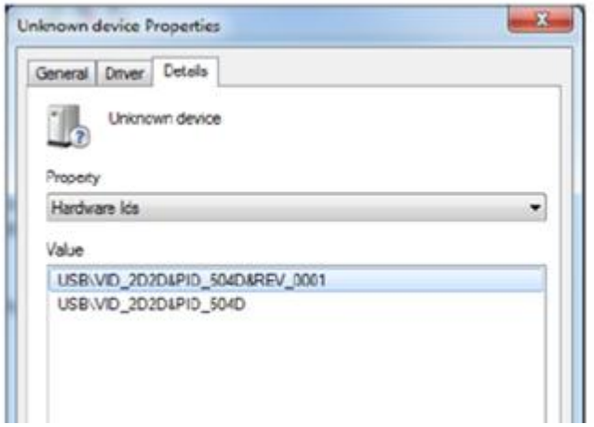
Step 3:

Open "Device Manager" and you will find an "Unkonwn device"



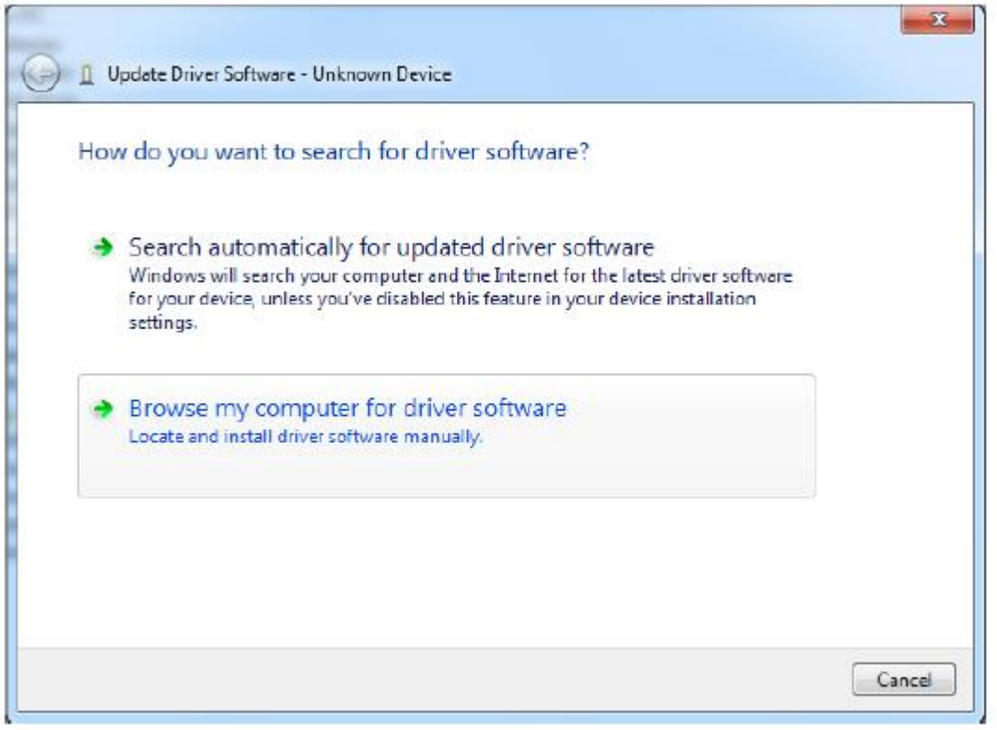
Step 4:

Right click on "Unknown Device" and then click Properties. Verify that the properties of the device match these information shown as below:

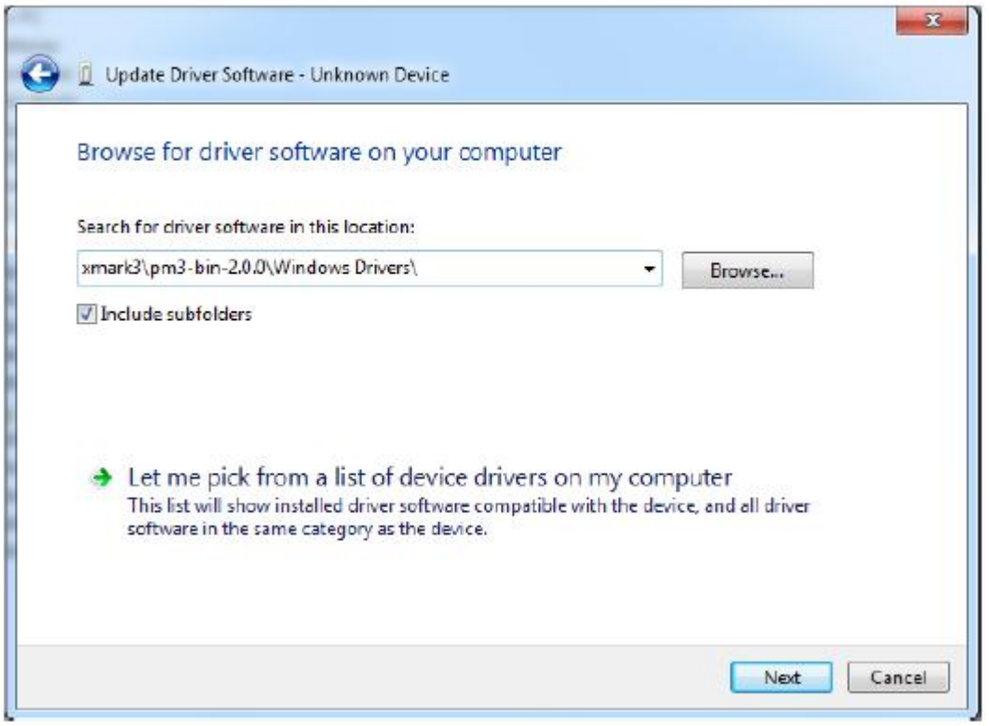


Step 5:

Exit the properties dialog and right click the device once more. This time select "Update Driver Software"



Select "Browse my computer for driver software" Select the driver folder within the Proxmark client software distribution.

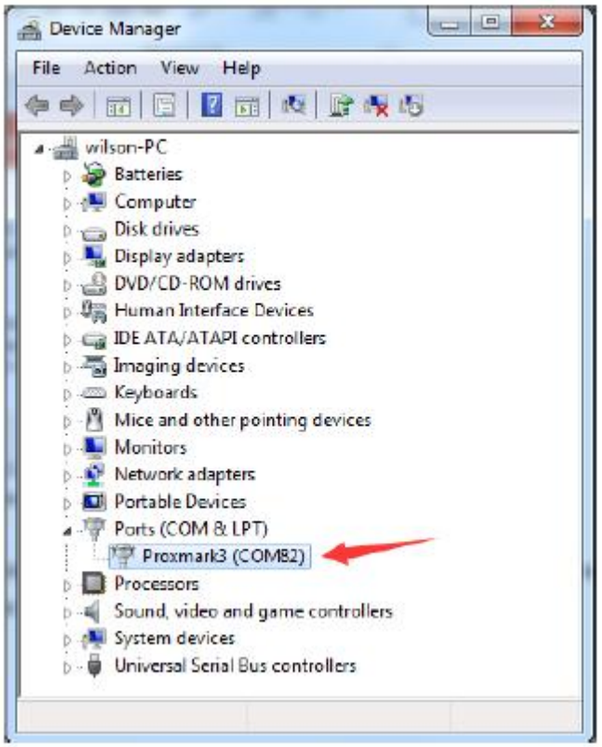


Click "Next" button. It will come out as below:

Click "Install this driver software anyway". Then it install the driverThen it installs the driver.

Step 6:

Back in Device Manager, the Unknown Device will now show up as a Proxmark3. Take note of the COM port associated with the device (COM82 in the picture below). Later we will use this COM number.(COM82 can be any useful COM Port)



Application Test

Fully compatible with all new official firmware, brush any versions according to your need.

Here we recommand 2.0.0 and more new version firmware, and this module come with 2.0.0 version by default.

Please use the official "Command Line" or "Proxmark Tool.exe" to operate this module.

1、Command Line

1) Client Running on Linux

The Proxmark exposes a USB CDC interface to the host machine. On linux, the Proxmark will show up as the device /dev/ttyACM\<N>. To launch the client, run./proxmark3 /dev/ttyACM\<N>.

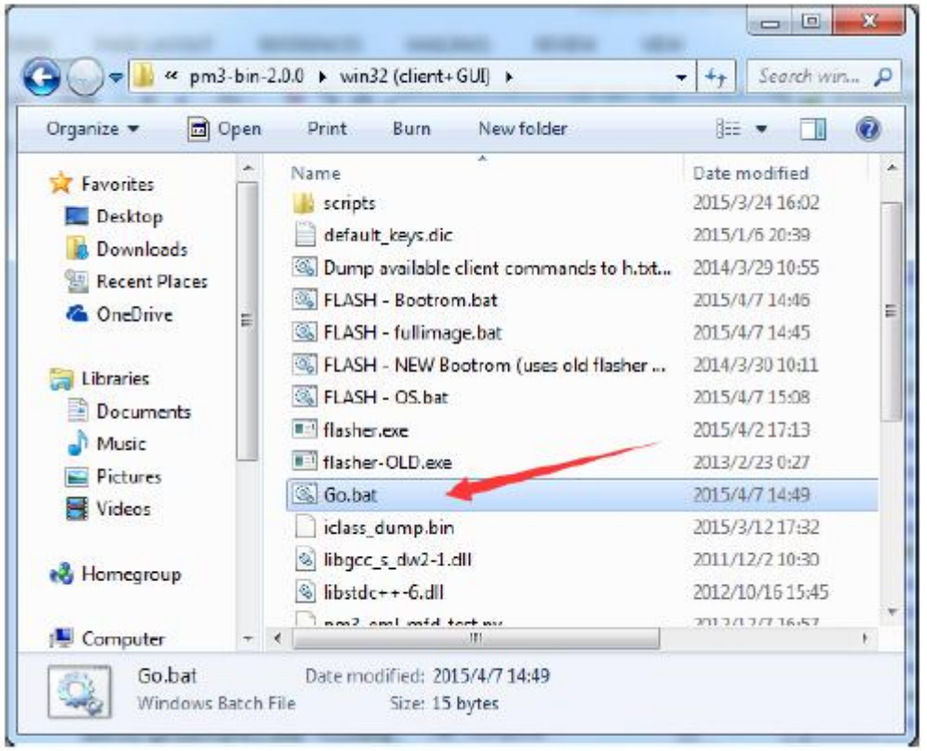
You can inspect the output of the dmesg command to figure out the specific device name.

```
[1142387.760068] usb 2-1.1: new full-speed USB device number 71 using ehci_hcd
[1142387.853698] cdc_acm 2-1.1:1.0: This device cannot do calls on its own. It is not a modem.
[1142387.853742] cdc_acm 2-1.1:1.0: ttyACM0: USB ACM device
```

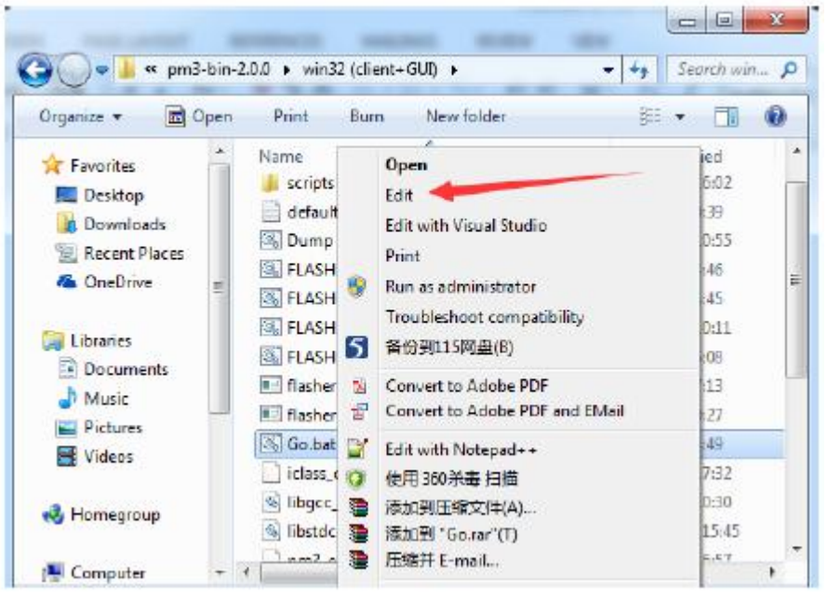
2) Client Running on Windows

You could find the folder "win32(client+GUI)"

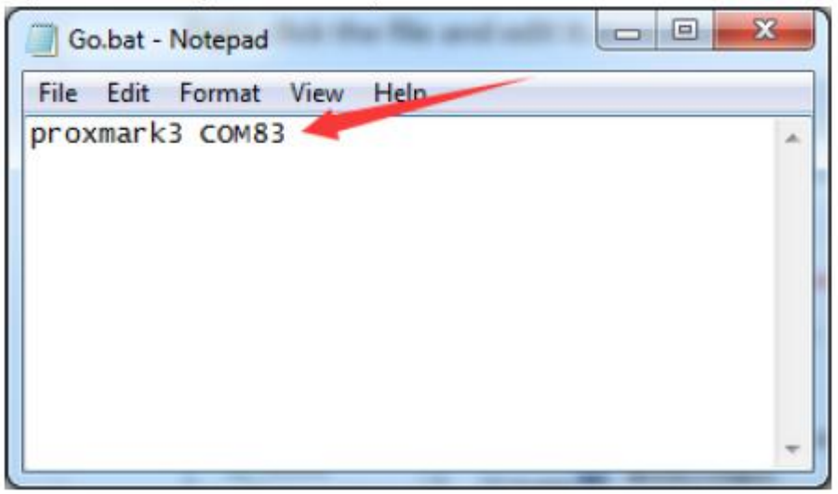
Open the folder and the find the following file "Go.bat" (On your computer it might be Go):



Right click the file and edit it.



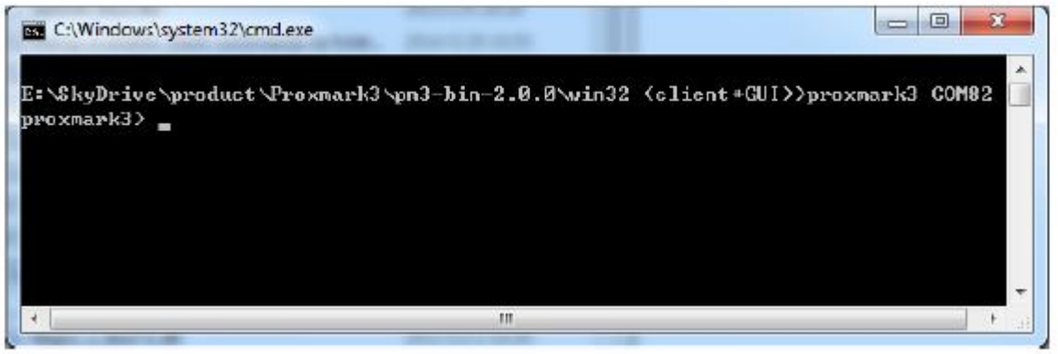
By default it is opened in Notepad.



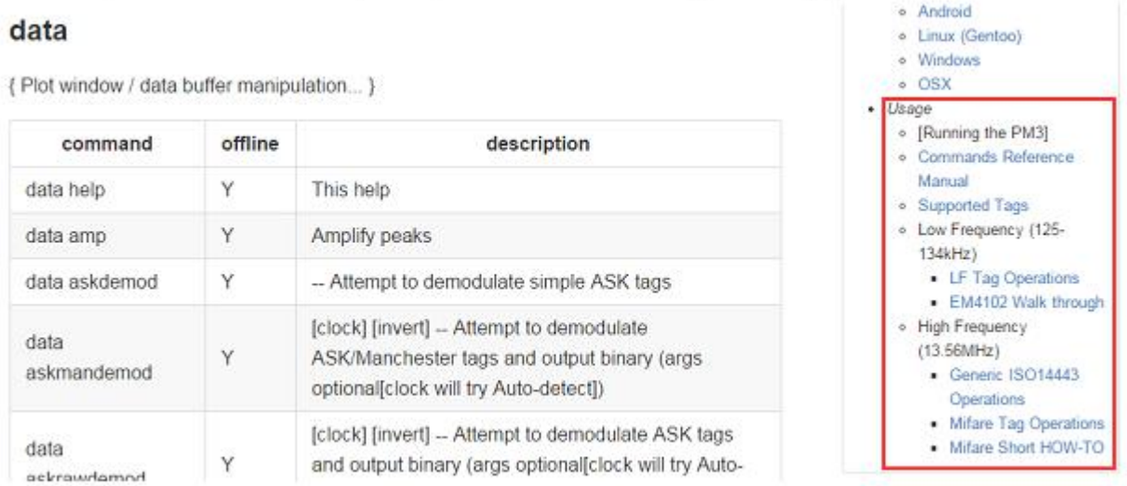
Change the COM to your COMX. Here mine is COM82.

Save and close the window.

Now double click the "Go.bat"



Now you can refer to the Commands Reference Manual:
https://github.com/Proxmark/proxmark3/wiki/commands
You could get more information by clicking the index box on the right of the page above:



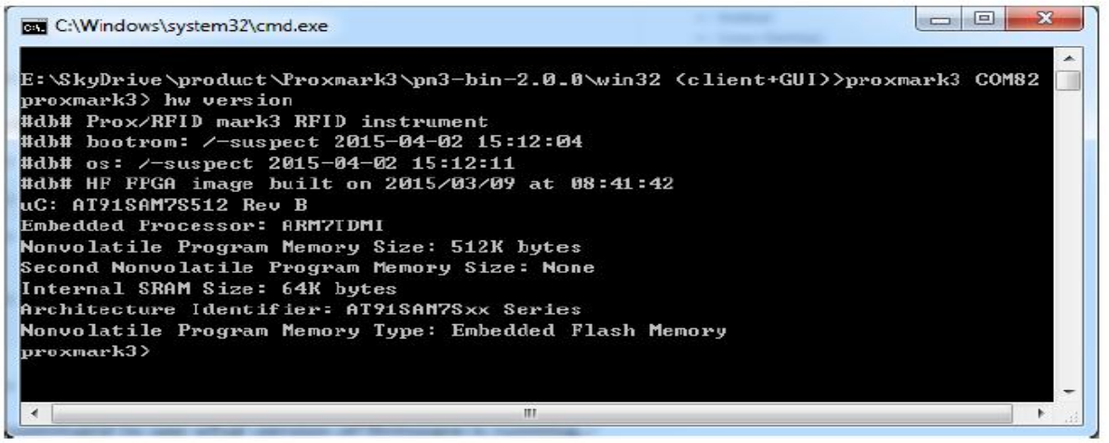
data

{ Plot window / data buffer manipulation... }

command	offline	description
data help	Y	This help
data amp	Y	Amplify peaks
data askdemod	Y	-- Attempt to demodulate simple ASK tags
data askmandemod	Y	[clock] [invert] -- Attempt to demodulate ASK/Manchester tags and output binary (args optional[clock will try Auto-detect])
data askrawdemod	Y	[clock] [invert] -- Attempt to demodulate ASK tags and output binary (args optional[clock will try Auto-

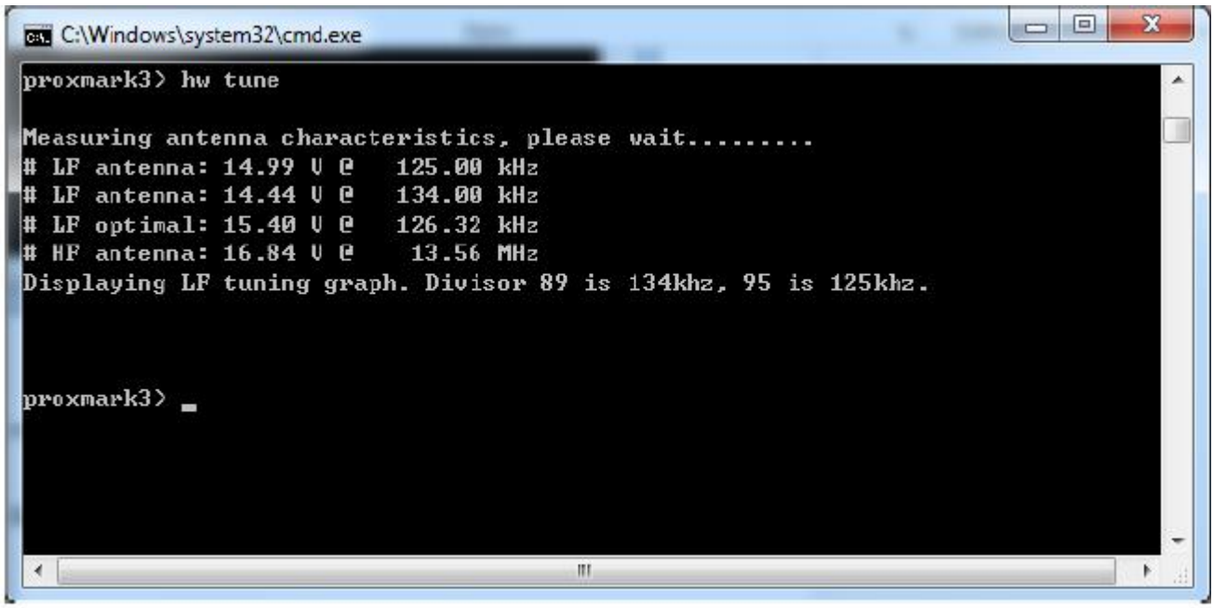
Check firmware version

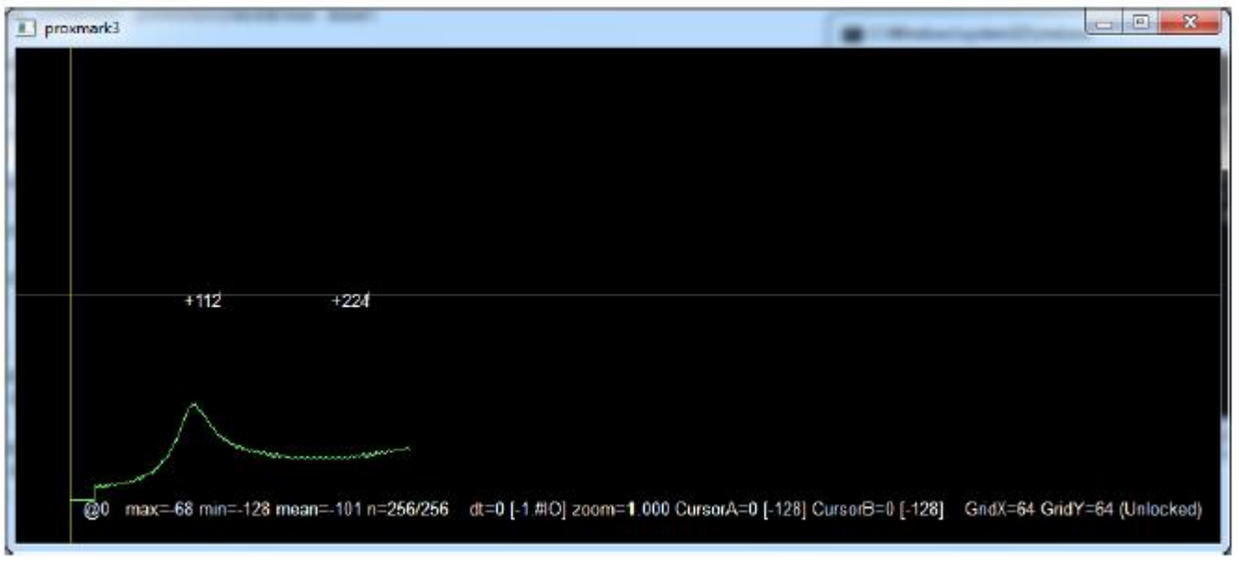
Enter the "hw version" command to see what version of firmware is running.



Check Antennas

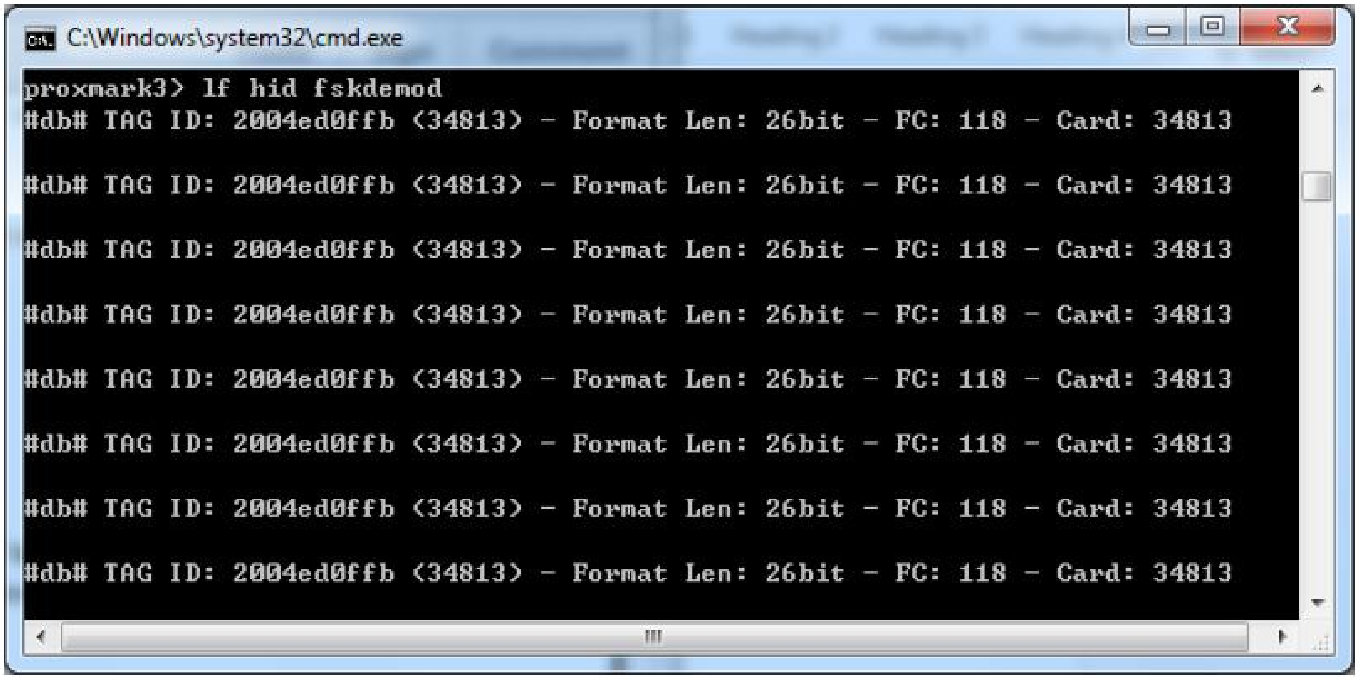
Now connect both the antennas to your Proxmark board.
Enter the "hw tune" command to run it.





Reading HID Tags

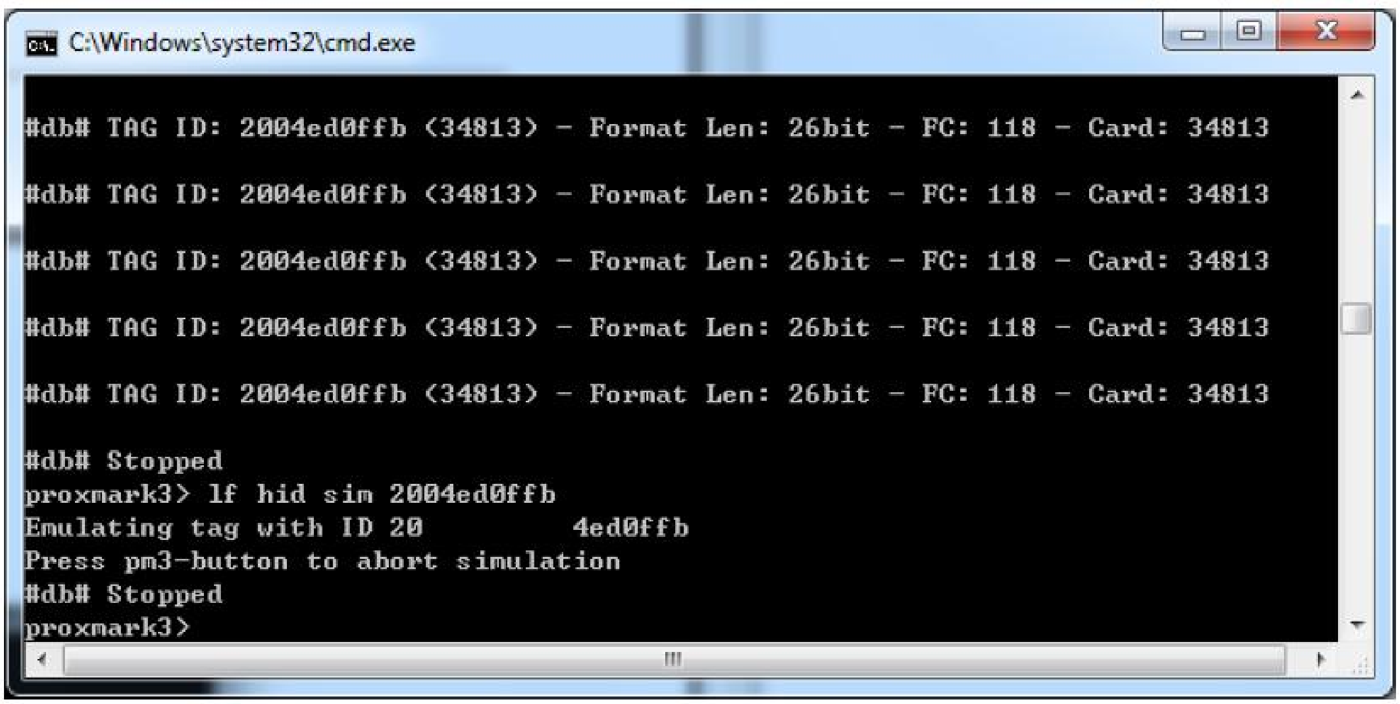
Make sure the LF antenna is connected with your Proxmark board.
Enter the "lf hid fskdemod" command to run it. Then put the HID tags within the antenna filed.



Press the button when you would like to stop reading tags. The LED D would turn off.

Simulate HID

To simulate the tag previously read, concatenate the first two hexadecimal values and pass them as the first parameter to the "lf hid sim" command as shown below

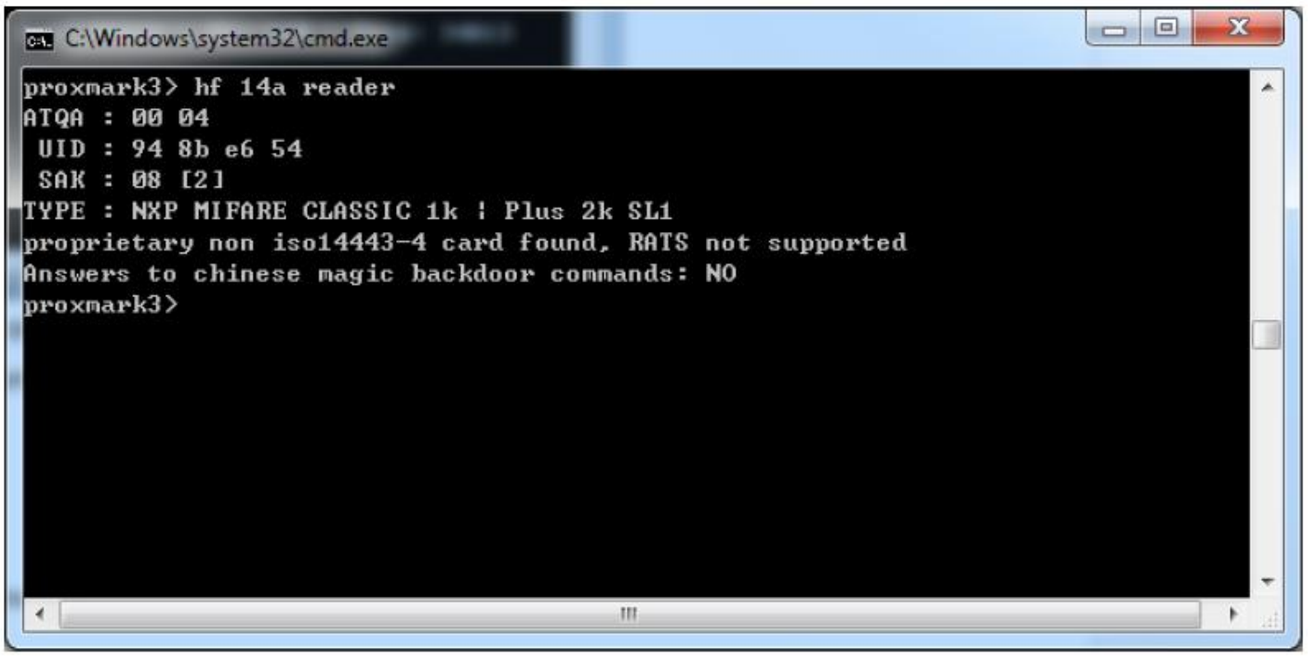


This will cause the yellow LED A to stay lit until the button is pressed. During this time the waveform representing the tag ID specified will be replayed continuously. When you are ready to stop replaying the tag, press the Proxmark button.

Read Mifare Classic tags

Make sure the HF antenna is connected with your Proxmark board.
Put the S50 tag in the antenna field.

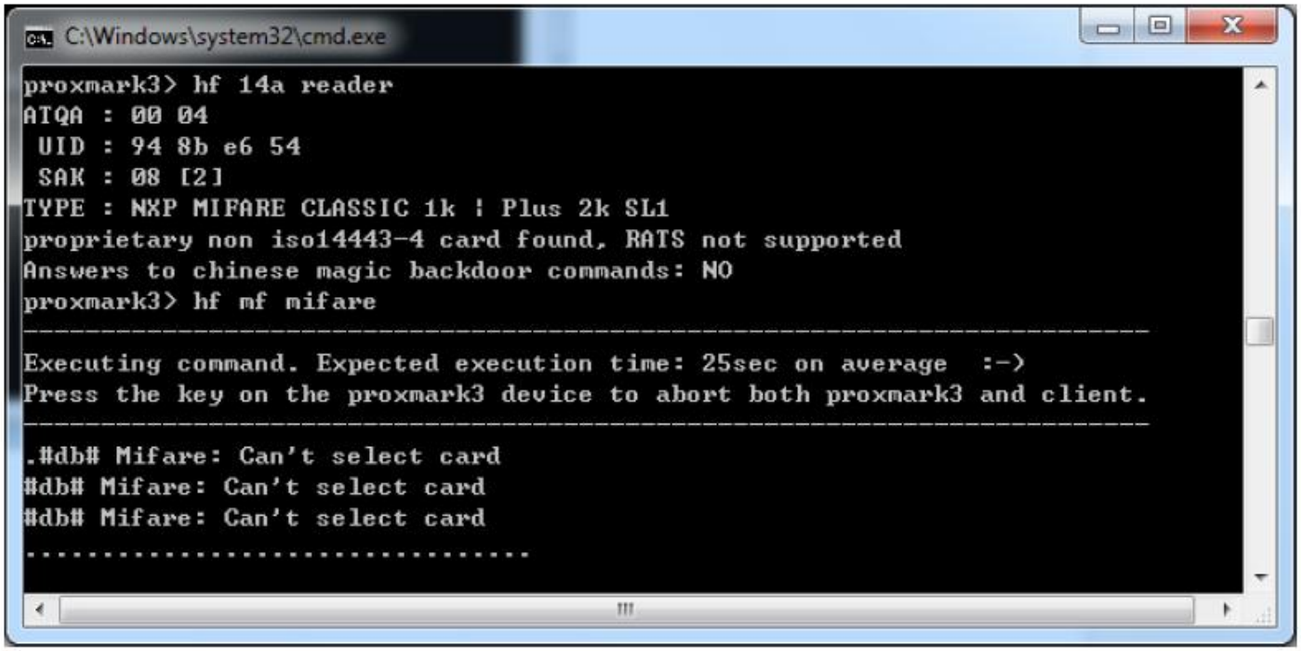
Enter the "hf 14a" reader command to run it.



1) Mifare S50/S70 Keep the S50 tag in the antenna field.

Enter the "hf mf mifare" command to run it.

Note: Crack PRNG vulnerability, Success rate is low. Usually it causes the USB connection line off the PC. Common error: "Can't select card". According to our testing, firmware 816 is the best version for this command. If you want to try to crack in this way, we recommend you to degrade the firmware to 816 version. Anyway, remember that the success rate is low, but possible.

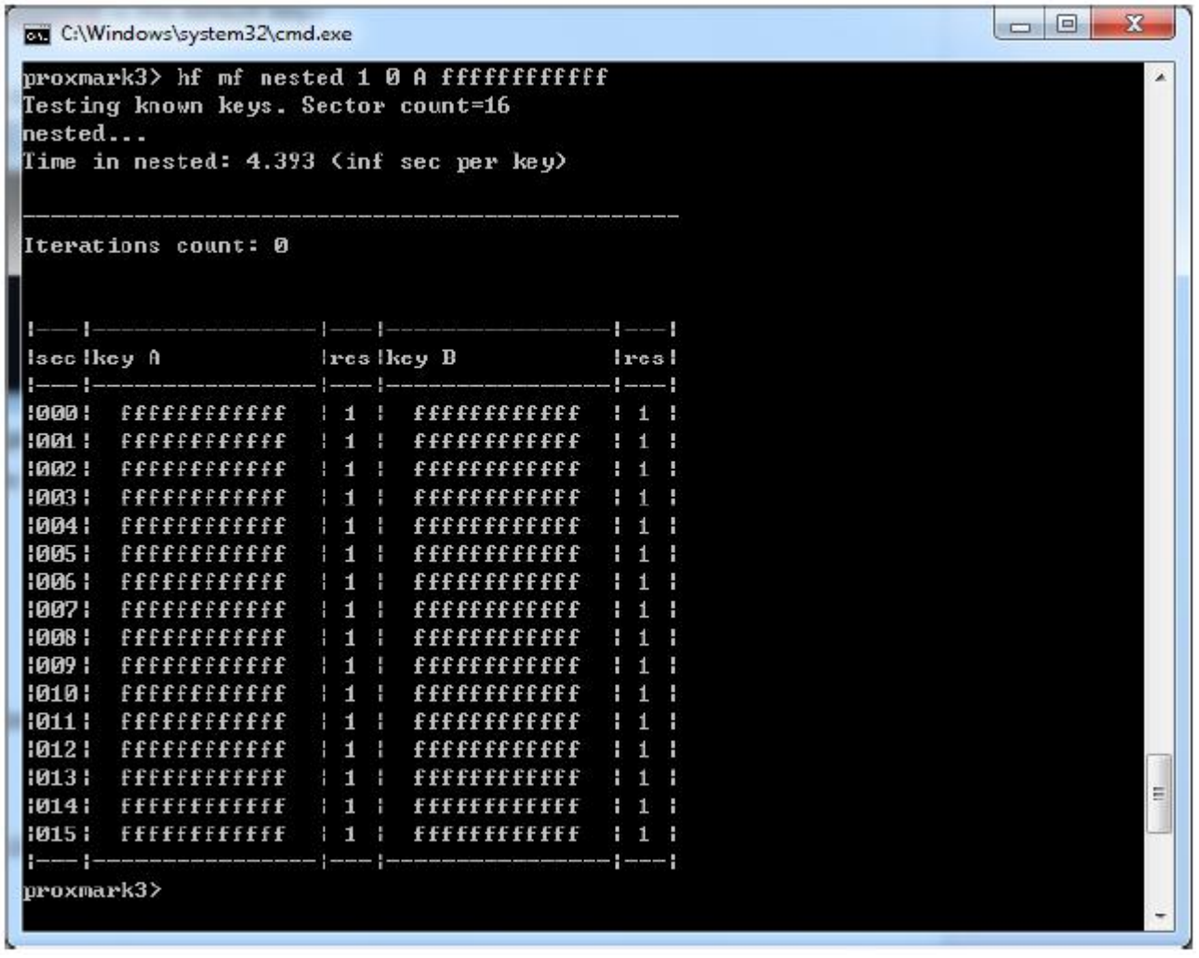


Press the button when you would like to stop the execution.

2) Mifare S50/S70

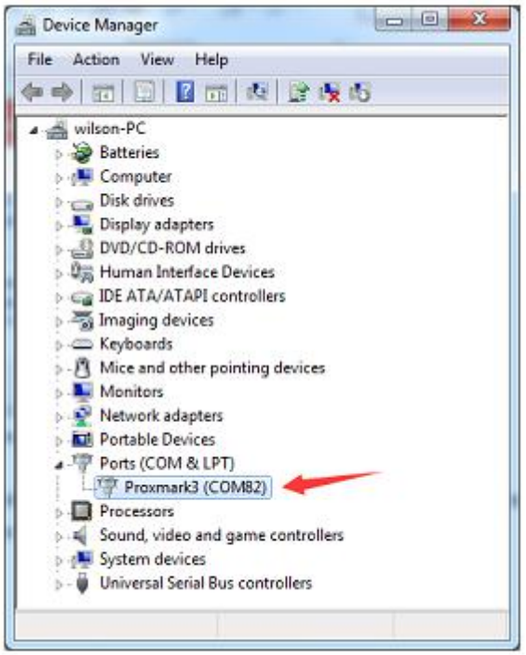
Crack the tag key based on one known key of any sector.
First to check one key for certain sector. You know, ffffffffffff is the default key.
Keep the S50 tag in the antenna field.
Enter the " hf mf chk 0 A ffffffffffff " command to run it.

Once we get one key, we could crack the card and get all the keys.
Enter the " hf mf nested 1 0 A ffffffffffff " command to run it.



2、Proxmark Tool.exe

Back in Device Manager, the Unknown Device will now show up as a Proxmark3. Take note of the COM port associated with the device (COM82 in the picture below). Later we will use this COM number (COM82 can be any useful COM Port).



Client Running on Windows

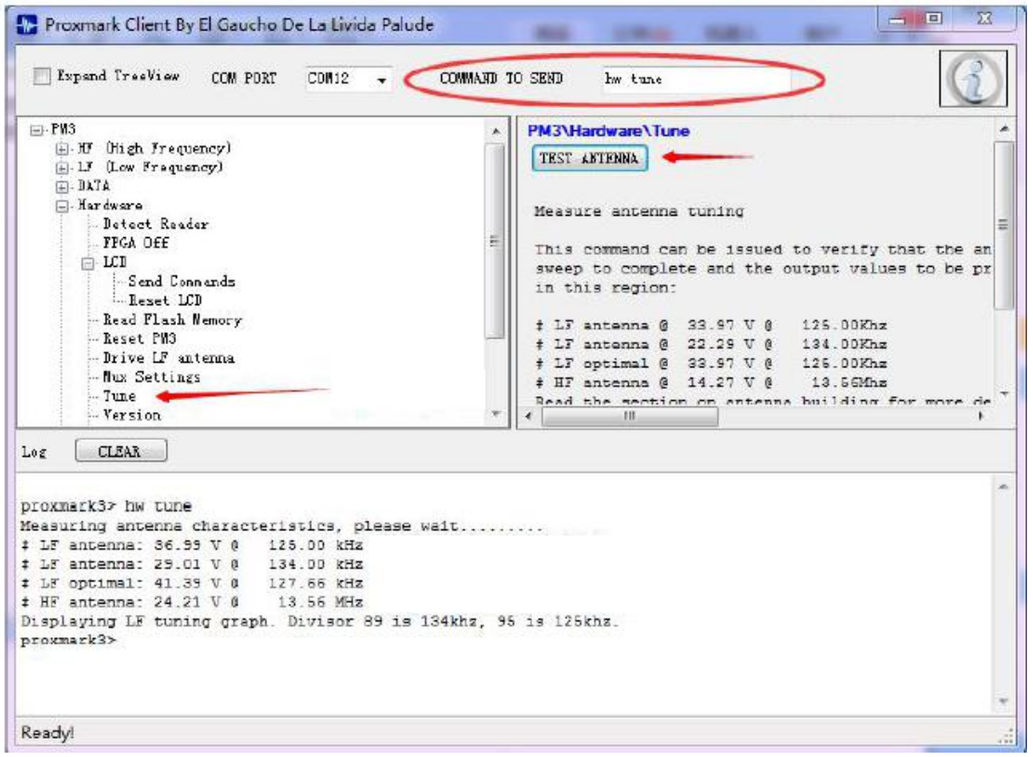
You could find the folder "win32(client+GUI)".
Now double click the "Proxmark Tool.exe" and choose the COM82 port.

If the below is blank, then connection is normal； If it shows "ERROR: invalid serial port", then means it is not normal, please try to pull out the USB, choose another COM port, and plug in USB, after "ding-dong" sound, choose the COM82 port again.

Check Antennas

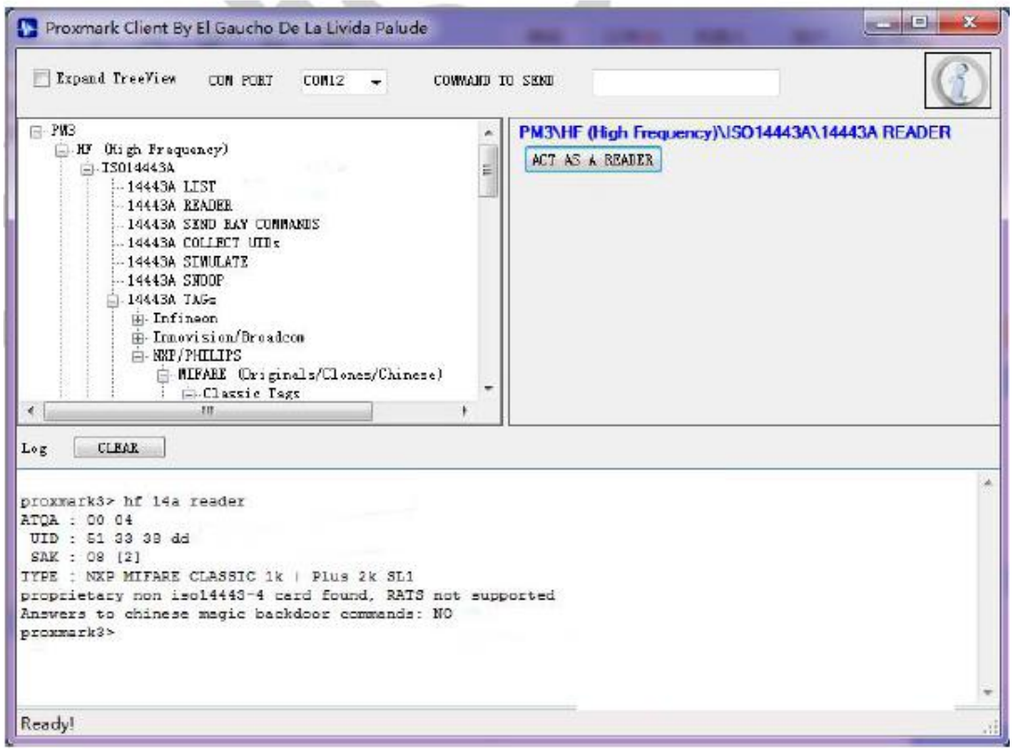
Now connect both the antennas to your Proxmark board.

Enter the "hw tune" command to run it.



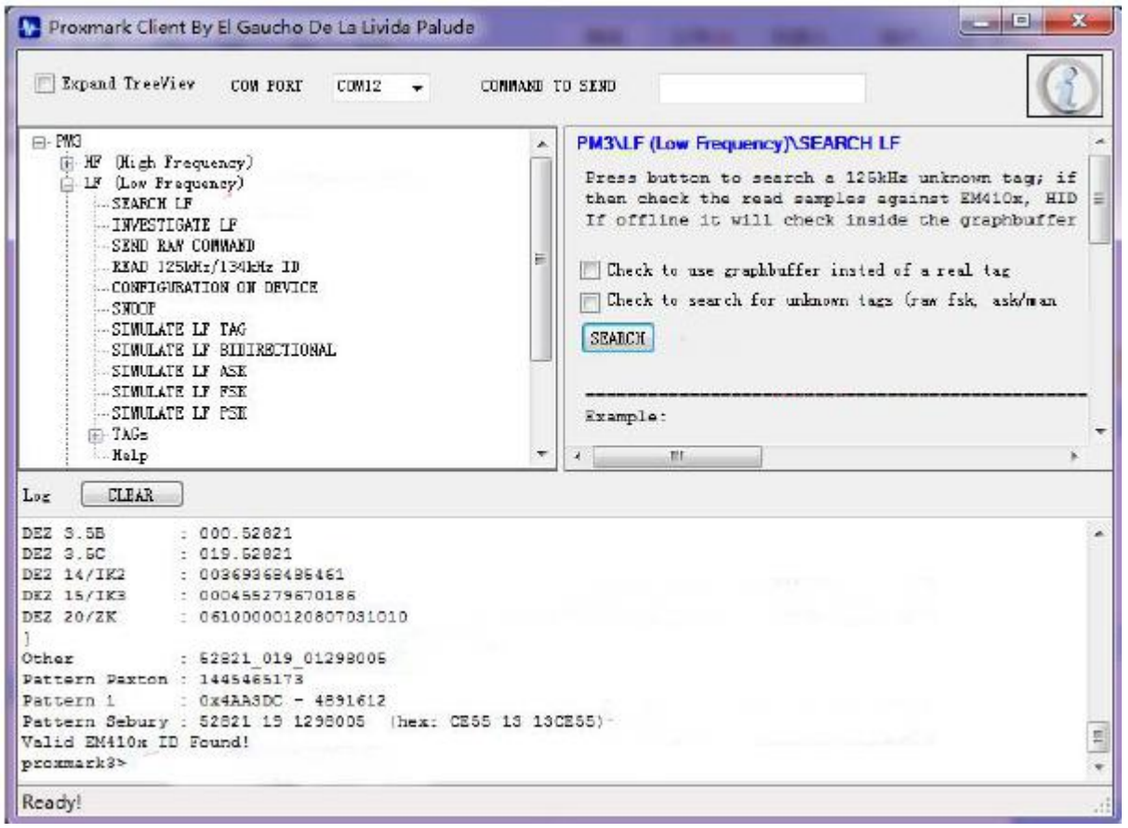
Antenna cannot be placed around the card or metal, or measurement results will be low.

Test Reading HF Cards



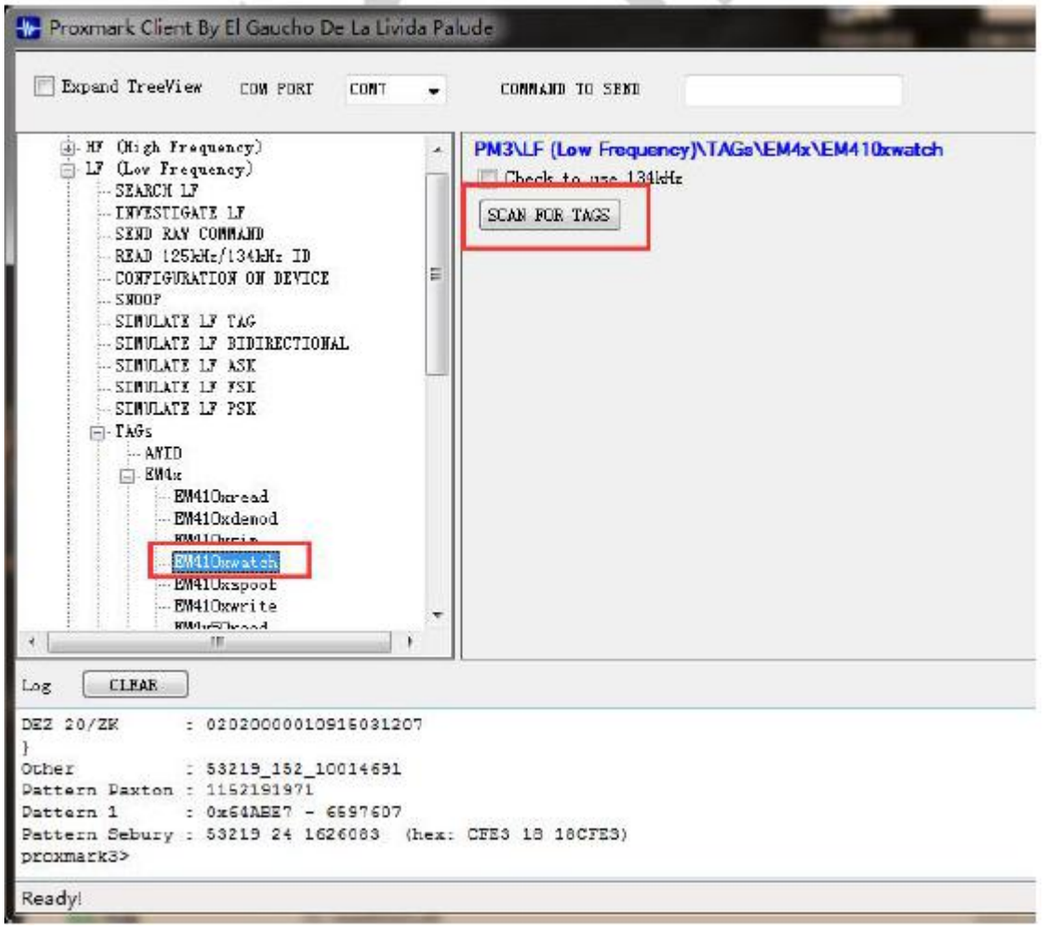
Try to put M1 S50 "M1" UID "etc different cards on the antenna

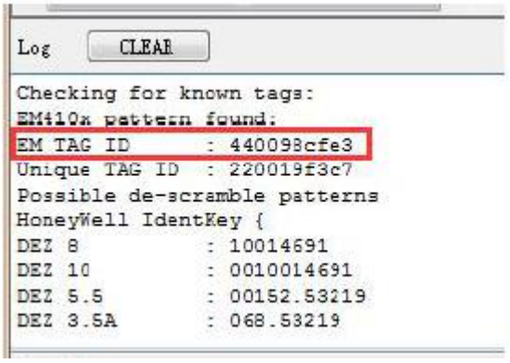
Test Reading LF Cards



Try to put "HID" "T5577 etc different cards on antenna to test card types.

The sensitivity is not perfect through this reading command, so when some cards can not be read smoothly, please try another command as below:


Proxmark Client By El Gaucho De La Livida Palude
Expand TreeView
COM PORT
CONT
COMMAND TO SEND
HF (High Frequency)
LF (Low Frequency)
SEARCH LF
INVESTIGATE LF
SEND RAW COMMAND
READ 125kHz/134kHz ID
CONFIGURATION ON DEVICE
SNOOP
SIMULATE LF TAG
SIMULATE LF BIDIRECTIONAL
SIMULATE LF ASK
SIMULATE LF FSK
SIMULATE LF PSK
TAGs
AWID
EM4x
EM410xread
EM410xdemod
EM410xwatch
EM410xspoof
EM410xwrite
PM3\LF (Low Frequency)\TAGs\EM4x\EM410xwatch
SCAN FOR TAGS
Log
CLEAR
DEZ 20/ZK : 02020000010916031207
}
Other : 53219_152_10014691
Pattern Paxton : 1152191971
Pattern 1 : 0x64ABE7 - 6597607
Pattern Sebury : 53219 24 1626083 (hex: CFE3 18 18CFE3)
proxmark3>
Ready!


Log
CLEAR
Checking for known tags:
EM410x pattern found:
EM TAG ID : 440098cfe3
Unique TAG ID : 220019f3c7
Possible de-scramble patterns
HoneyWell IdentKey {
DEZ 8 : 10014691
DEZ 10 : 0010014691
DEZ 5.5 : 00152.53219
DEZ 3.5A : 068.53219