

Proxmark III User Guide



Getting Started

Overview

The Proxmark III is an open-source device developed by Jonathan Westhues that enables sniffing, reading and cloning of RFID (Radio Frequency Identification) tags. The Proxmark III 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.

ELECHOUSE Proxmark III is an improved version in hardware based on the original version. It has smaller size and could be easily integrated into other device. Antennas are also be improved to make it easier for users. The software is completely compatible.

Note: Bare PCBs are susceptible to Electrostatic Discharge or "ESD". Please keep this in mind when handling the bare Proxmark PCB. This warning can be ignored if you operate your Proxmark inside an enclosure.

With our Proxmark III board, it comes the antennas (for Low Frequency and High Frequency) and several tags. Along with the boards comes a Micro USB cable. You just need to connect it with your PC.

Feature

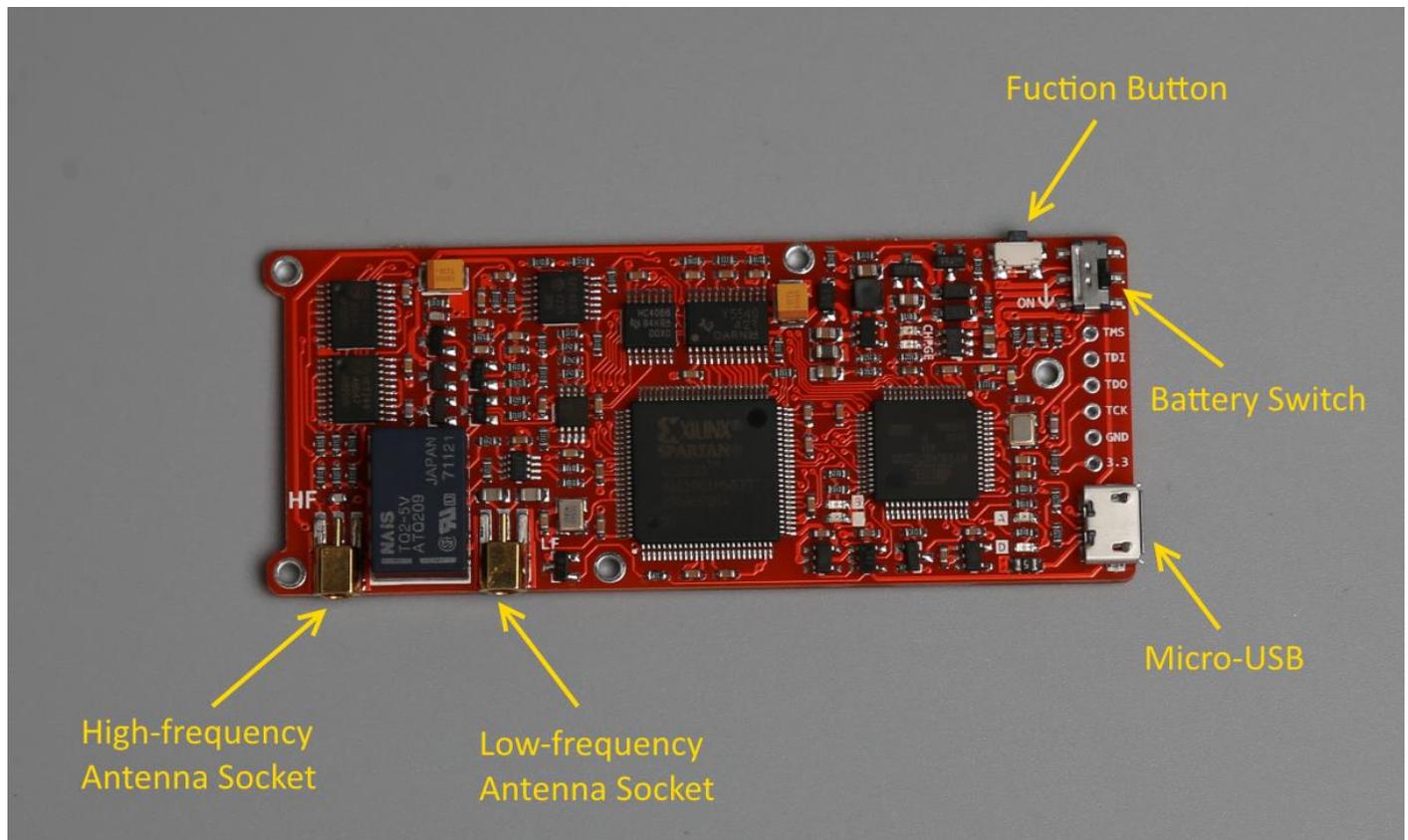
- Powerful functions: Snoop, listen and emulate everything from Low Frequency (125kHz) to High Frequency (13.56MHz) tags
- Complete open-source software: free to modify and use
- Easy to use: plug in and play, no need to obtain knowledge of hardware
- Full kits: everything you need to play

Hardware

Main Board

- CPU : ARM, 256 (AT91SAM7S256) of flash memory, 64kB of RAM
- FPGA : Xilinx Spartan-II
- Two independent RF circuits, HF and LF
- Power : through USB port or battery
- Connectivity : Micro-USB port for PC and MMCX sockets for antennas
- User interface: one button, one switch, 6 LEDs.

The FPGA does the low level modulation/demodulation (-A, -B, ASK, OOK, etc), whereas the CPU should handle the coding/decoding of the frames (Manchester, Miller, etc) as well as more advanced functions.



Function Button

It is a touch switch, not a self-lock switch. In this manual, if you are supposed to “press the button”, it means this one.

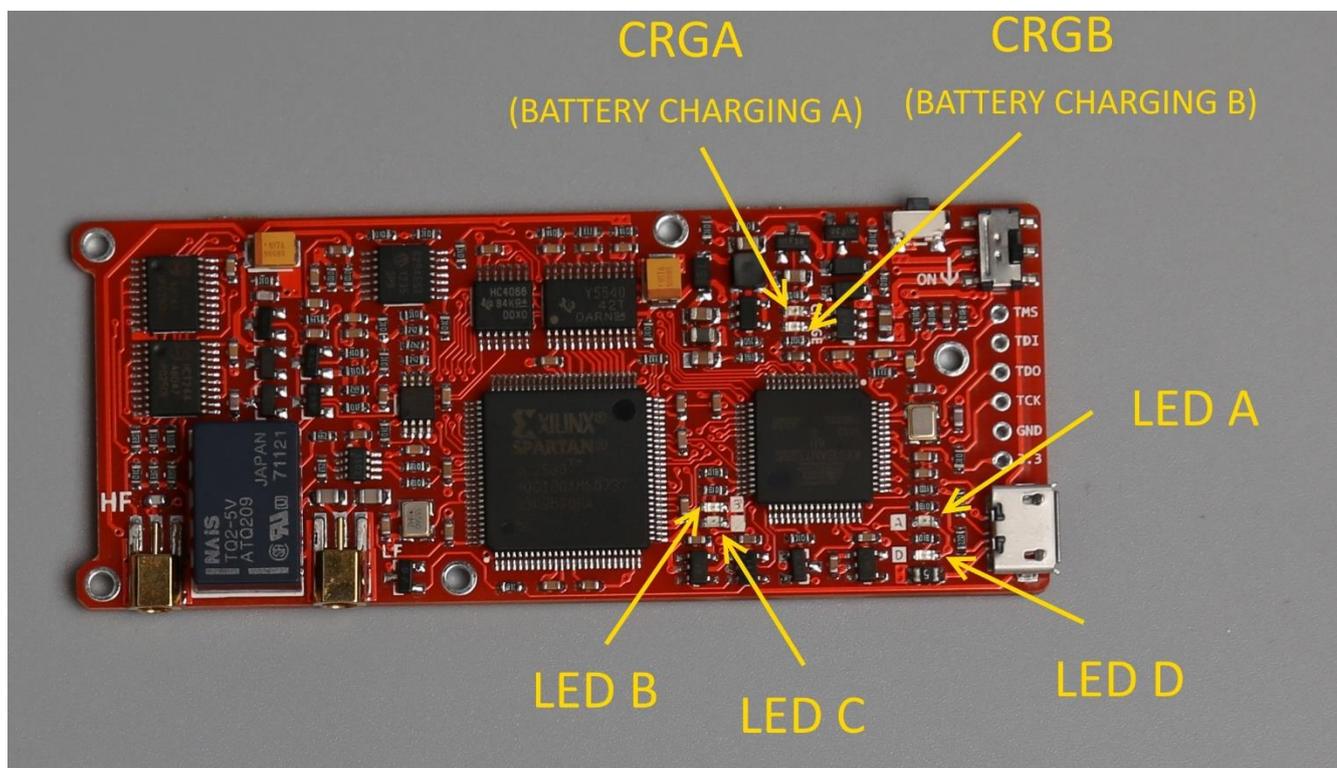
Battery switch

This switch is a slide switch. It is used as battery power switch.

Micro USB Port

Most widely used nowadays. Most phones (except iPhone) adopt this kind of USB standard.

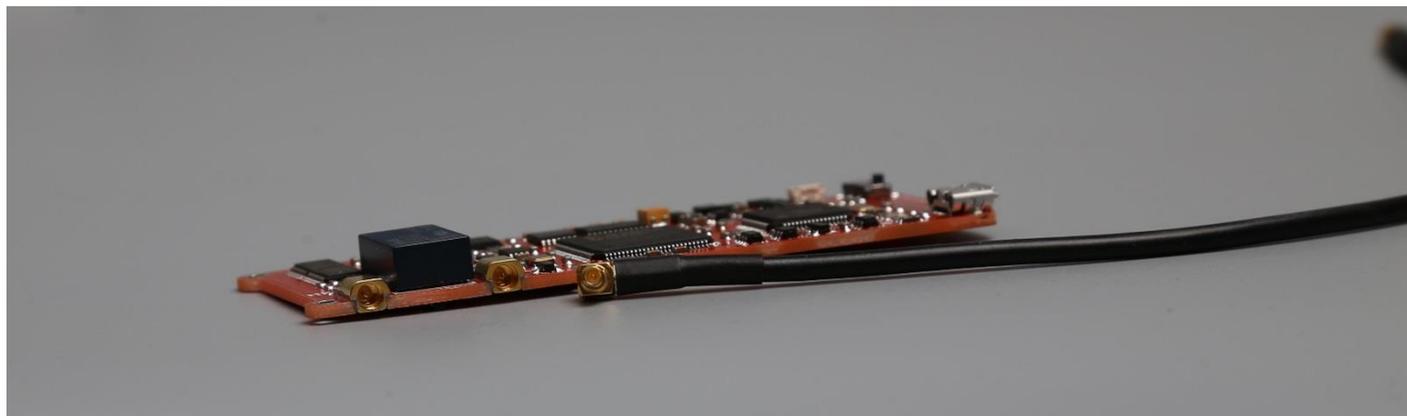
LEDs



Cases	CRGA	CRGB
USB CONNECTED, NO BATTERY	ON	FLASHING
USB AND BATTERY CONNECTED, CHARGED FULL	ON	OFF
USB AND BATTERY CONNECTED, CHARGING	OFF	ON
NO USB, BATTERY CONNECTED	OFF	OFF
NO USB, NO BATTERY	OFF	OFF

LED A~D are function indicators. Please refer to function detail for more information.

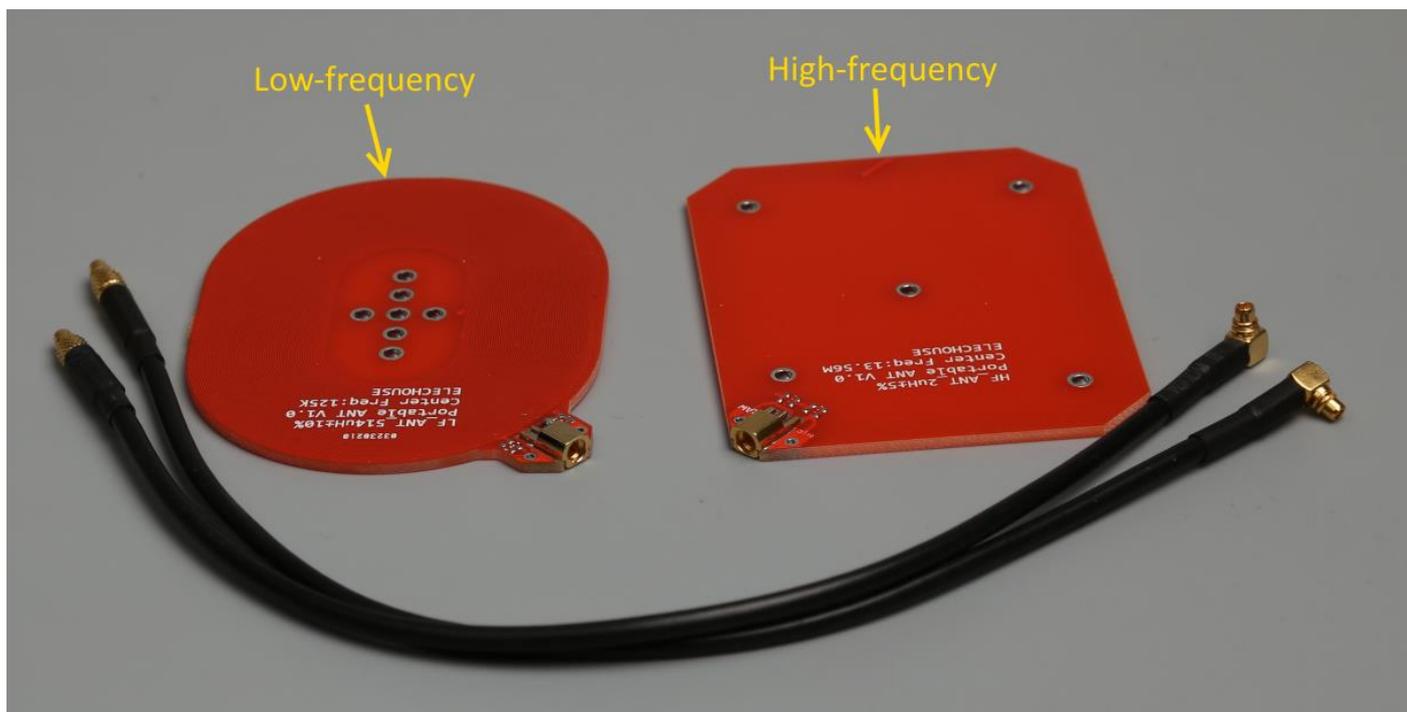
High-frequency/Low-frequency Antenna Socket



MMCX (micro-miniature coaxial) sockets

- High-frequency: 13.56Mhz
- Low-frequency: 125Khz/134Khz

Antenna



Micro-USB Cable



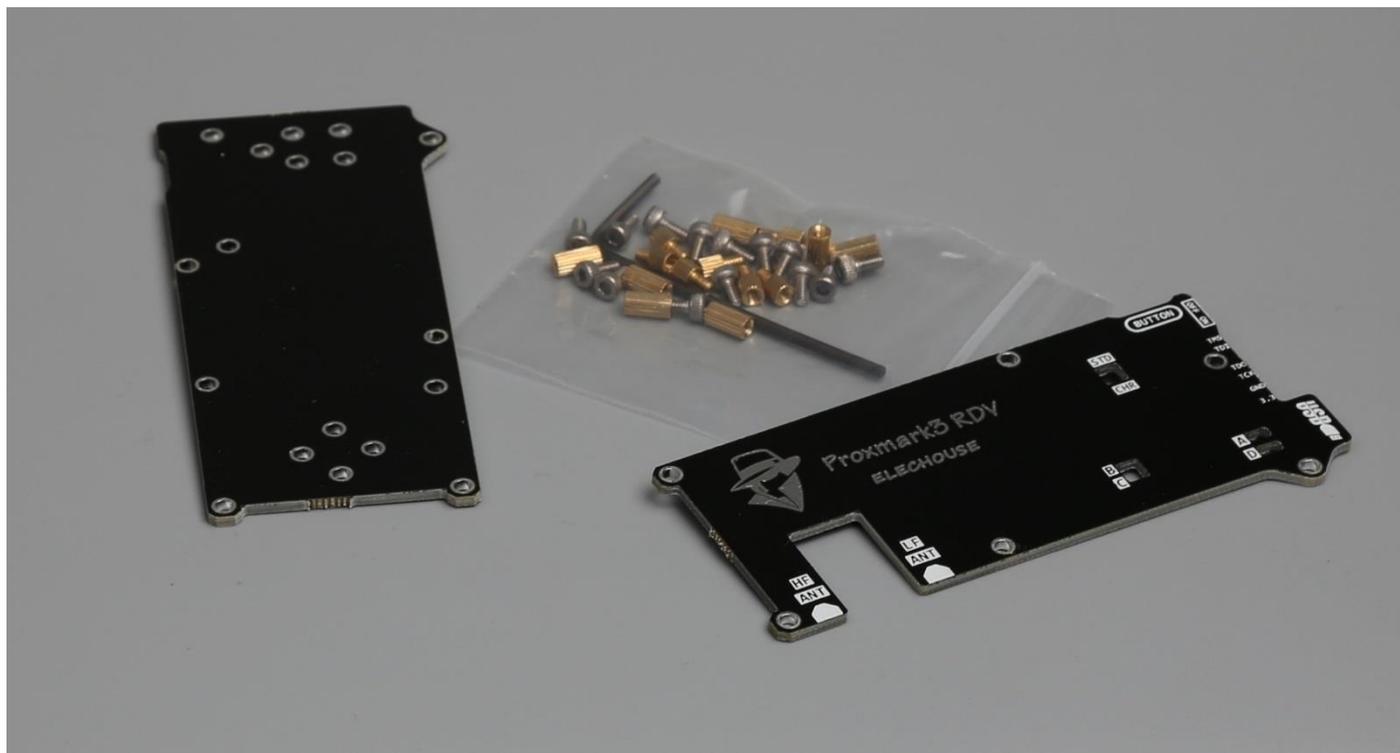
Noodle style, soft and flexible

Tags

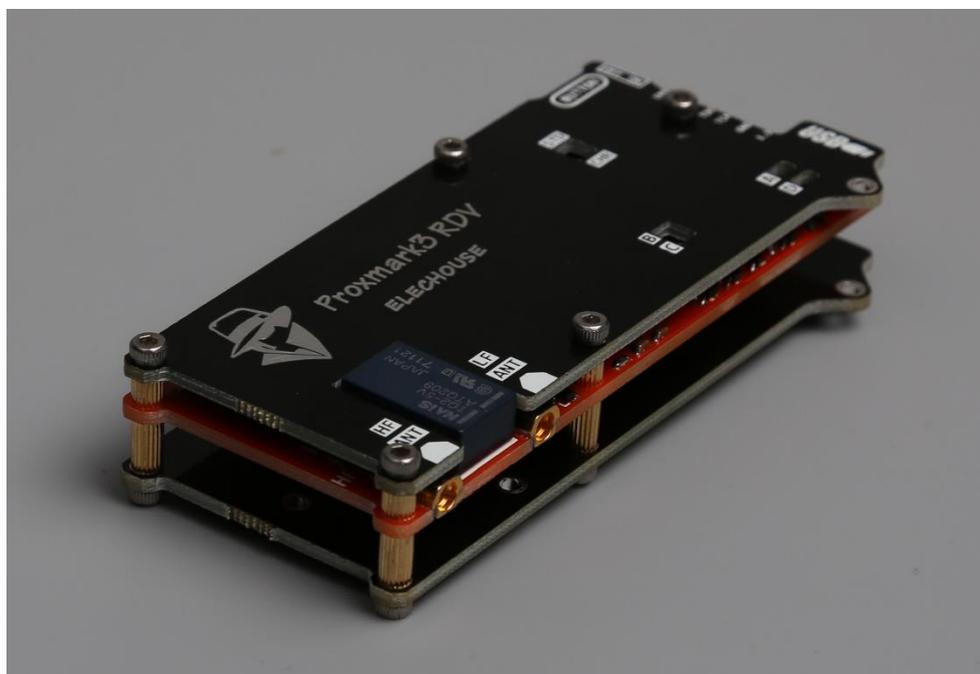


Tags	Frequency	Description
Mifare S50 (M1)	HIGH	Fixed UID, read/write user data
Mifare Ultralight (M0)	HIGH	Fixed UID, read/write user data
Mifare UID (Chinese Magic Card)	HIGH	Modify UID, used to lone, read/write user data
EM4XX (ID tag)	LOW	Fixed ID
T5577	LOW	Modify ID, used to clone
HID Prox II	LOW	Widely used in USA, read/write user data

Board Enclosure



This protector is made of RF4, which is the same material as the main board. This protector mainly prevent the Proxmark main board from being touched during working. Touching the board might cause interference to it while it is working.



Pre-Flight Check

Connect your Proxmark to a PC using Micro-USB cable. The Micro-USB cable comes with the package. While turning on the module, LEDs should be in the following state

LED	State
-----	-------

CRGA (BATTERY CHARGING A)	Light on if there is no battery or the battery is charged full
CRGB (BATTERY CHARGING B)	Flash quickly if there is no battery connected
LED A	Flash once
LED B	Flash once
LED C	Flash once
LED D	Flash twice

If the LEDs stay lit, this may indicate a problem with your board or that the board has not been programmed correctly. Every board obtained from ELECHOUSE has been programmed with the latest stable firmware available at the time and rigorously tested to ensure proper functionality prior to shipping.

Client 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

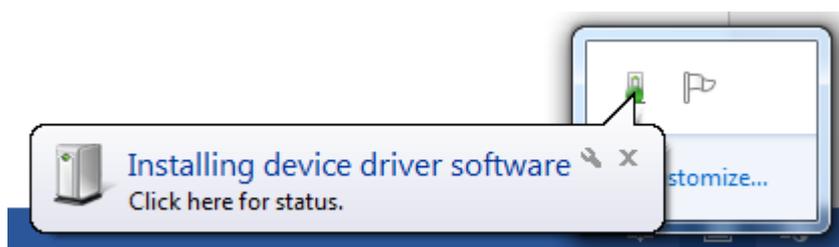
Recent versions of the Proxmark client require the use of a libusb “driver” on Windows hosts. Perform the following steps to install the driver.

Step 1:

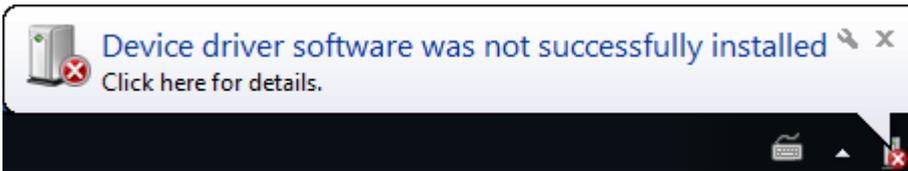
Download the software:

Step 2

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

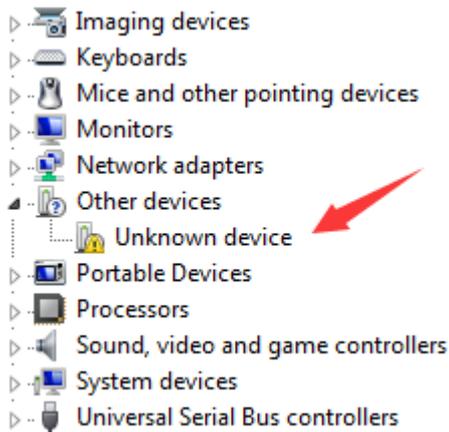


After a while, it will tell you “Fail to find drive”.



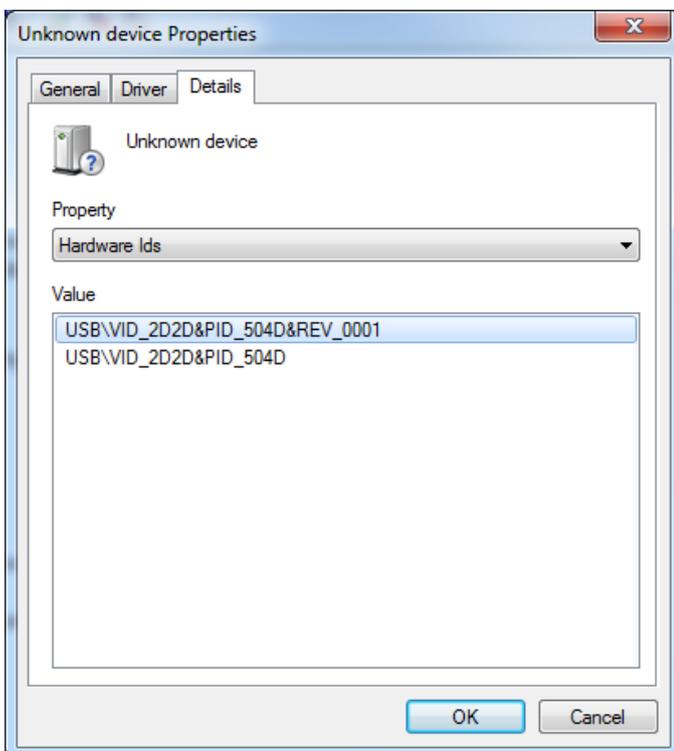
Step 3

Open "Device Manager" and you will find an Unknown Device



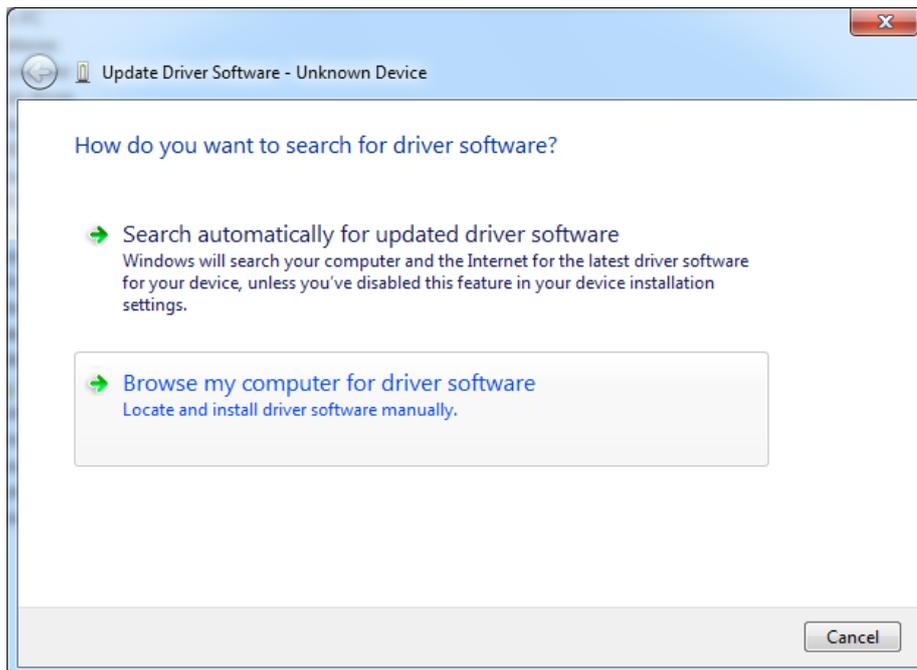
Step 4

Right click on "Unknown Device" and then click Properties. Verify that the properties of the device match those shown below.

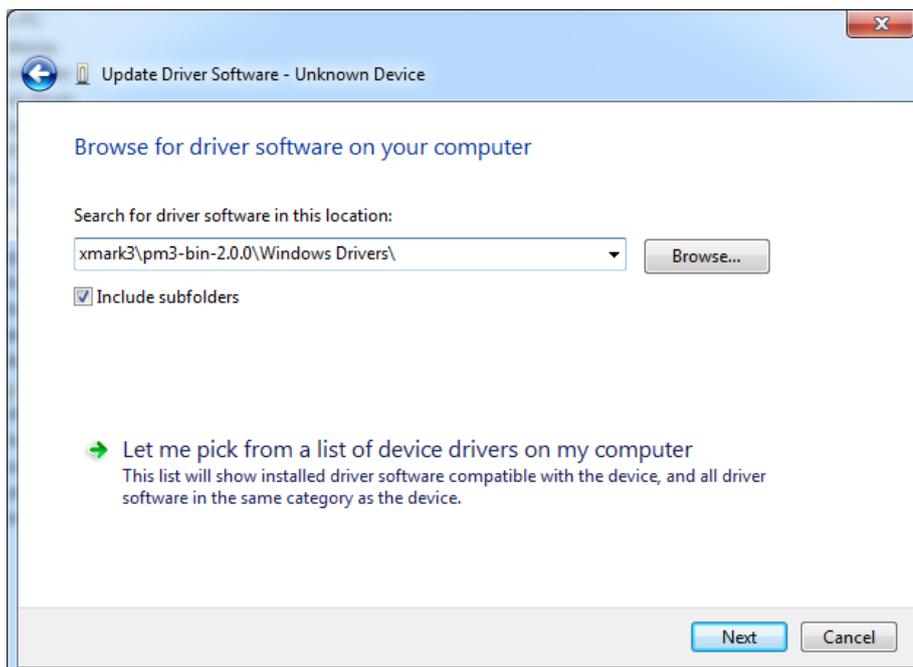


Step 5

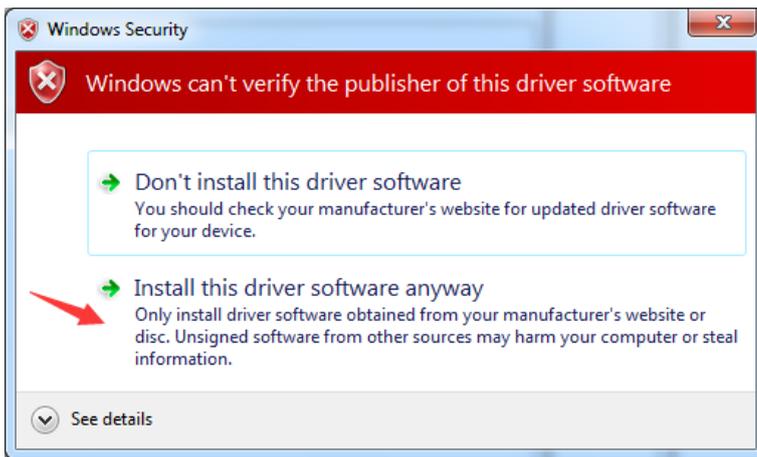
Exit the properties dialog and right click the device once more. This time select Update Driver Software.



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



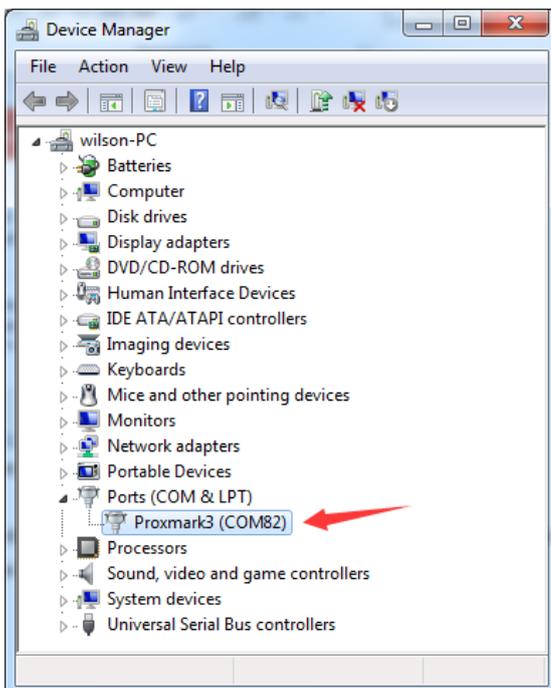
Click "Next" button. It pops up:



Click "Install this driver software anyway". Then 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 the COM number.



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>`.

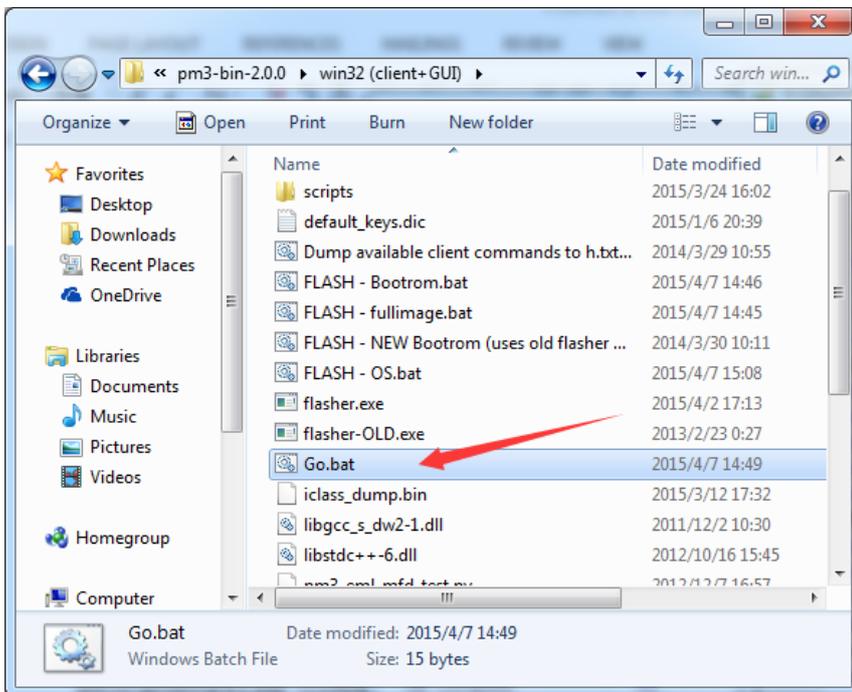
You can inspect the output of the `dmesg` command to figure out the specific device name.

```
[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
```

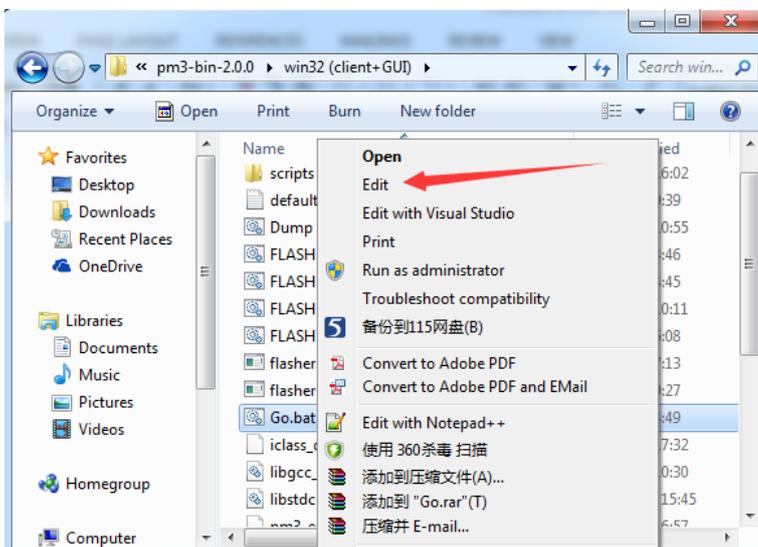
Client Running on Windows

You could find the folder “**win32 (client+GUI)**” in the software downloaded above.

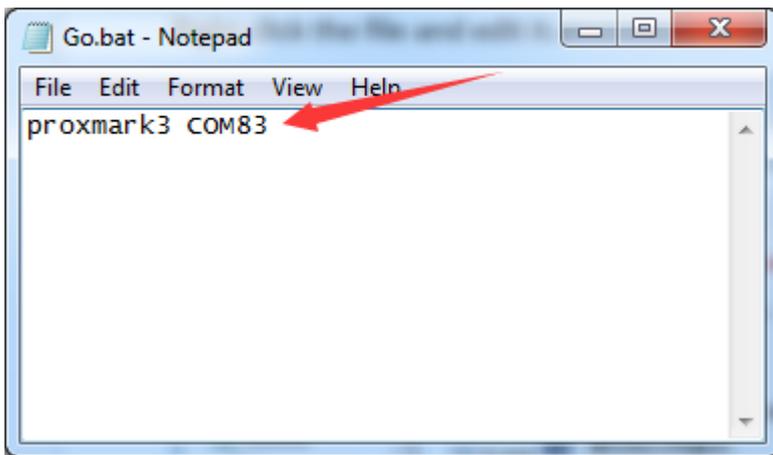
Open the folder and the find the following file **Go.bat** (On your computer it might be **Go**):



Right click the file and edit it.



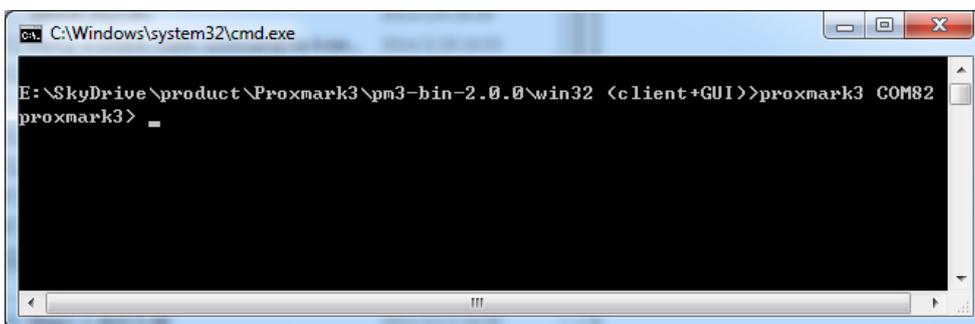
By default it is opened in Notepad.



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

Save and close the window.

Now double-click the "Go.bat".



Now you could 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-

- Android
- Linux (Gentoo)
- Windows
- OSX
- Usage
 - [Running the PM3]
 - Commands Reference Manual
 - Supported Tags
 - Low Frequency (125-134kHz)
 - LF Tag Operations
 - EM4102 Walk through
 - High Frequency (13.56MHz)
 - Generic ISO14443 Operations
 - Mifare Tag Operations
 - Mifare Short HOW-TO

Check firmware version

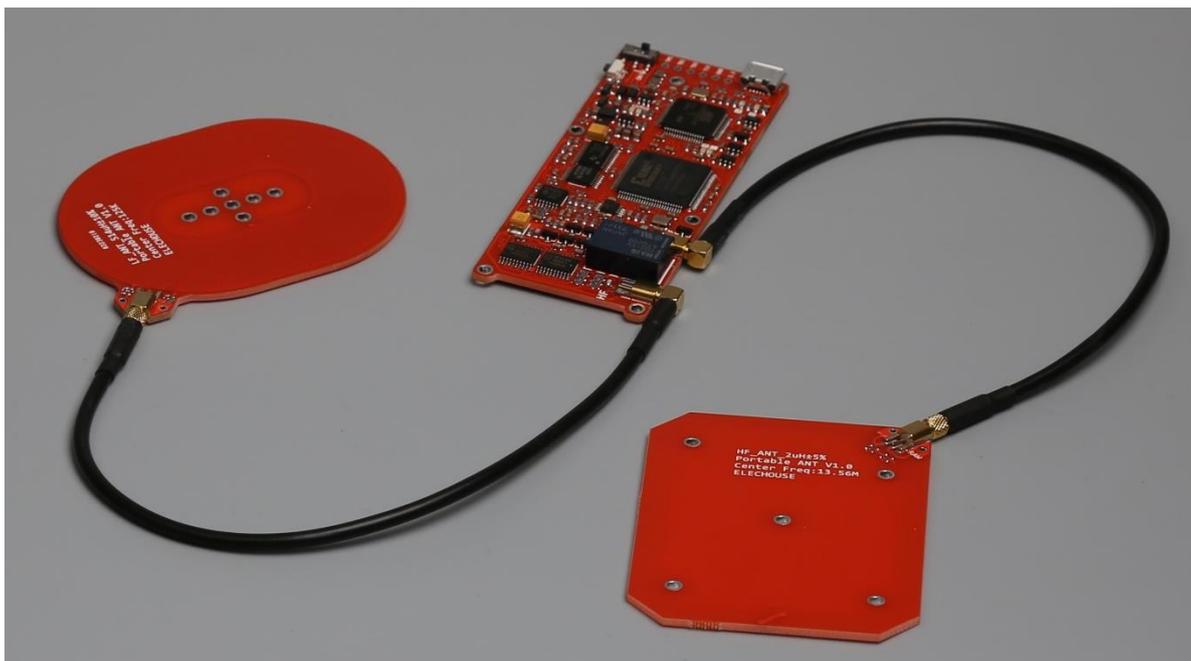
Enter the **hw version** command to see what version of firmware is running.

```
C:\Windows\system32\cmd.exe

E:\SkyDrive\product\Proxmark3\pm3-bin-2.0.0\win32 <client+GUI>>proxmark3 COM82
proxmark3> hw version
#db# Prox/RFID mark3 RFID instrument
#db# bootrom: /-suspect 2015-04-02 15:12:04
#db# os: /-suspect 2015-04-02 15:12:11
#db# HF FPGA image built on 2015/03/09 at 08:41:42
uC: AT91SAM7S512 Rev B
Embedded Processor: ARM7TDMI
Nonvolatile Program Memory Size: 512K bytes
Second Nonvolatile Program Memory Size: None
Internal SRAM Size: 64K bytes
Architecture Identifier: AT91SAM7Sxx Series
Nonvolatile Program Memory Type: Embedded Flash Memory
proxmark3>
```

Check Antennas

Now connect both the antennas to your Proxmark board.

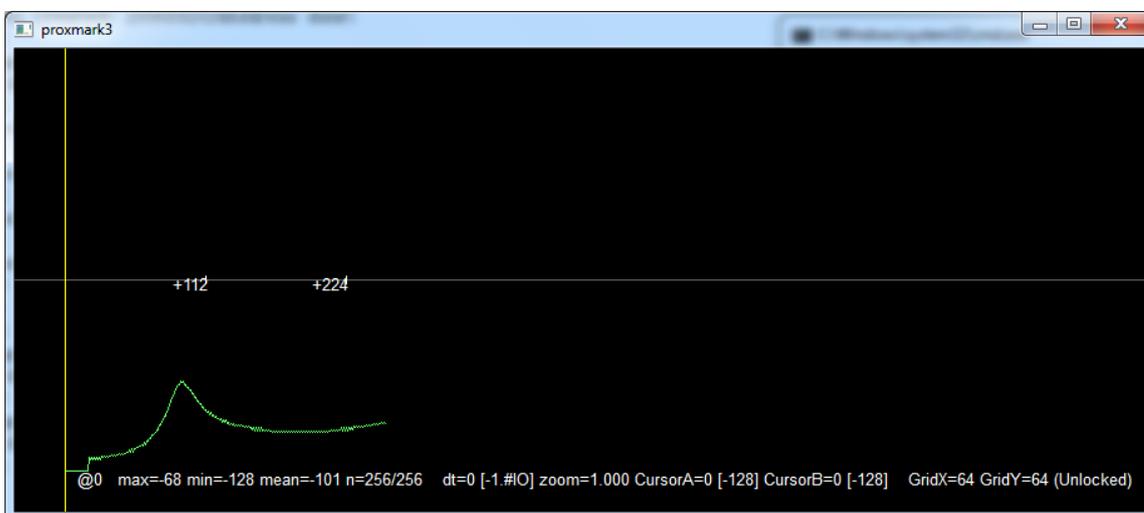


Enter the **hw tune** command to run it.

```
ca: C:\Windows\system32\cmd.exe
proxmark3> hw tune

Measuring antenna characteristics, please wait.....
# LF antenna: 14.99 V @ 125.00 kHz
# LF antenna: 14.44 V @ 134.00 kHz
# LF optimal: 15.40 V @ 126.32 kHz
# HF antenna: 16.84 V @ 13.56 MHz
Displaying LF tuning graph. Divisor 89 is 134khz, 95 is 125khz.

proxmark3> _
```



Reading HID Tags

Make sure the LF antenna is connected with your Proxmark board.

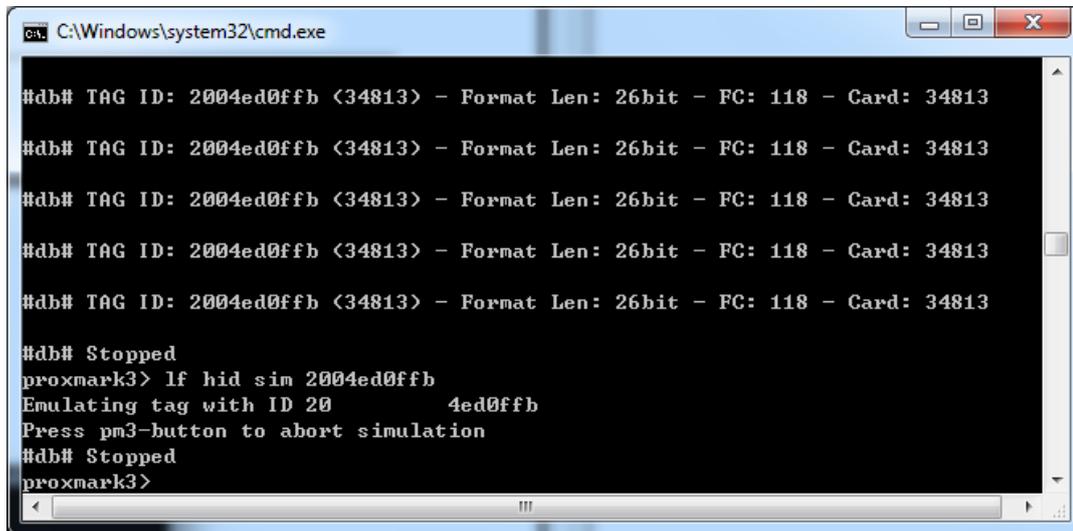
Enter the **lf hid fskdemod** command to run it. Then put the HID tags within the antenna filed.

```
ca: C:\Windows\system32\cmd.exe
proxmark3> lf hid fskdemod
#db# TAG ID: 2004ed0ffb (34813) - Format Len: 26bit - FC: 118 - Card: 34813
#db# TAG ID: 2004ed0ffb (34813) - Format Len: 26bit - FC: 118 - Card: 34813
#db# TAG ID: 2004ed0ffb (34813) - Format Len: 26bit - FC: 118 - Card: 34813
#db# TAG ID: 2004ed0ffb (34813) - Format Len: 26bit - FC: 118 - Card: 34813
#db# TAG ID: 2004ed0ffb (34813) - Format Len: 26bit - FC: 118 - Card: 34813
#db# TAG ID: 2004ed0ffb (34813) - Format Len: 26bit - FC: 118 - Card: 34813
#db# TAG ID: 2004ed0ffb (34813) - Format Len: 26bit - FC: 118 - Card: 34813
#db# TAG ID: 2004ed0ffb (34813) - Format Len: 26bit - FC: 118 - Card: 34813
```

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 "If hid sim" command as shown below



```
C:\Windows\system32\cmd.exe

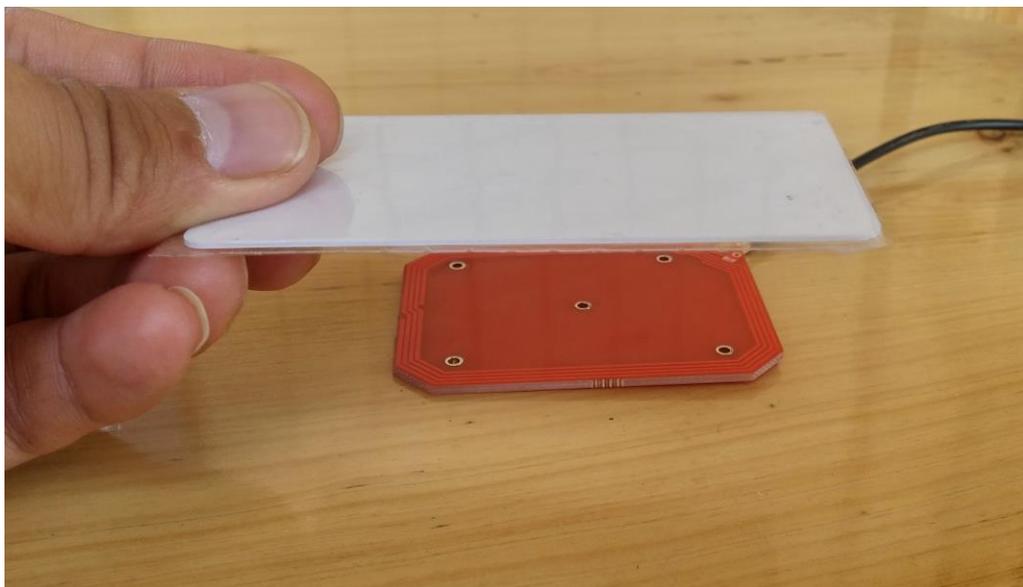
#db# TAG ID: 2004ed0ffb (34813) - Format Len: 26bit - FC: 118 - Card: 34813
#db# TAG ID: 2004ed0ffb (34813) - Format Len: 26bit - FC: 118 - Card: 34813
#db# TAG ID: 2004ed0ffb (34813) - Format Len: 26bit - FC: 118 - Card: 34813
#db# TAG ID: 2004ed0ffb (34813) - Format Len: 26bit - FC: 118 - Card: 34813
#db# TAG ID: 2004ed0ffb (34813) - Format Len: 26bit - FC: 118 - Card: 34813

#db# Stopped
proxmark3> If hid sim 2004ed0ffb
Emulating tag with ID 20      4ed0ffb
Press pm3-button to abort simulation
#db# Stopped
proxmark3>
```

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.

```

C:\Windows\system32\cmd.exe
proxmark3> hf 14a reader
ATQA : 00 04
UID : 94 8b e6 54
SAK : 08 [2]
TYPE : NXP MIFARE CLASSIC 1k ! Plus 2k SL1
proprietary non iso14443-4 card found, RATS not supported
Answers to chinese magic backdoor commands: NO
proxmark3>
  
```

I Crack 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.

```

C:\Windows\system32\cmd.exe
proxmark3> hf 14a reader
ATQA : 00 04
UID : 94 8b e6 54
SAK : 08 [2]
TYPE : NXP MIFARE CLASSIC 1k ! Plus 2k SL1
proprietary non iso14443-4 card found, RATS not supported
Answers to chinese magic backdoor commands: NO
proxmark3> hf mf mifare
-----
Executing command. Expected execution time: 25sec on average :->
Press the key on the proxmark3 device to abort both proxmark3 and client.
-----
.#db# Mifare: Can't select card
#db# Mifare: Can't select card
#db# Mifare: Can't select card
.....
  
```

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

II Crack 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, ffffffff is the default key.

Keep the S50 tag in the antenna field.

Enter the **hf mf chk 0 A ffffffff** command to run it.

```

C:\Windows\system32\cmd.exe
proxmark3> hf mf chk 0 A ffffffff
chk key[ 0] ffffffff
--sector: 0, block: 0, key type:A, key count: 1
Found valid key:[ffffffff]

proxmark3>
    
```

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

```

C:\Windows\system32\cmd.exe
proxmark3> hf mf nested 1 0 A ffffffff
Testing known keys. Sector count=16
nested...
Time in nested: 4.393 (inf sec per key)

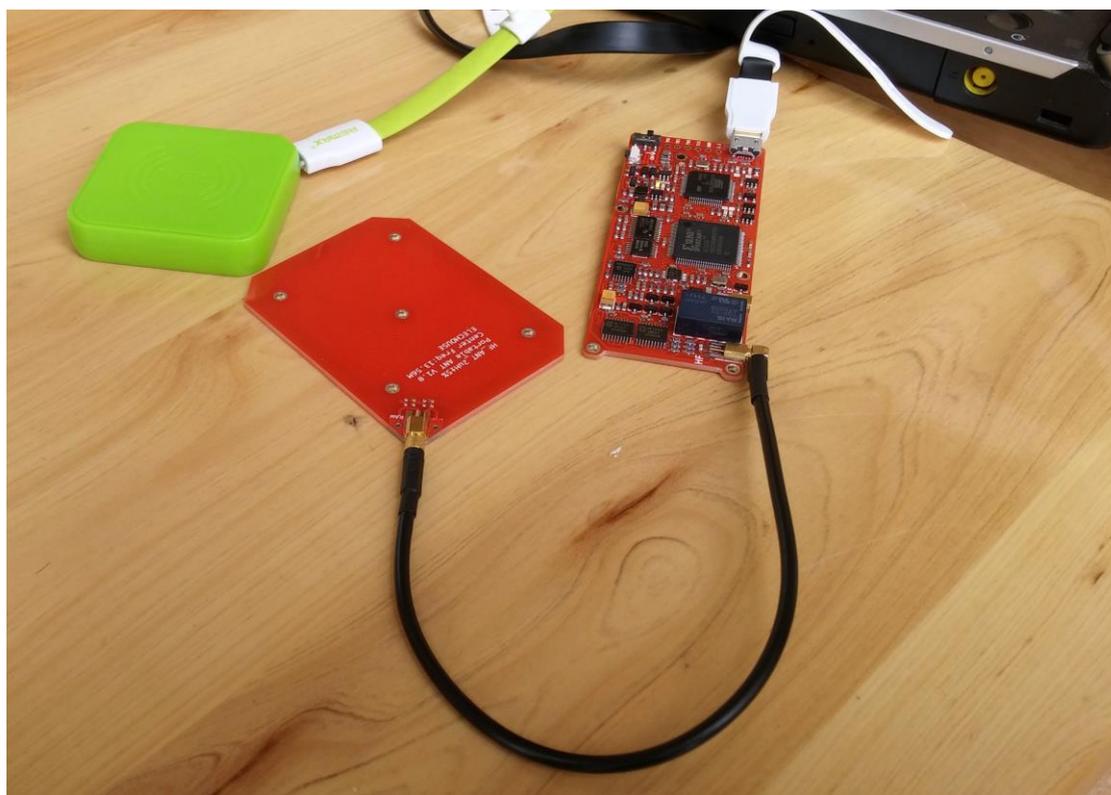
-----
Iterations count: 0

|---|-----|---|-----|---|
|sec|key A          |res|key B          |res|
|---|-----|---|-----|---|
|000| ffffffff       | 1 | ffffffff       | 1 |
|001| ffffffff       | 1 | ffffffff       | 1 |
|002| ffffffff       | 1 | ffffffff       | 1 |
|003| ffffffff       | 1 | ffffffff       | 1 |
|004| ffffffff       | 1 | ffffffff       | 1 |
|005| ffffffff       | 1 | ffffffff       | 1 |
|006| ffffffff       | 1 | ffffffff       | 1 |
|007| ffffffff       | 1 | ffffffff       | 1 |
|008| ffffffff       | 1 | ffffffff       | 1 |
|009| ffffffff       | 1 | ffffffff       | 1 |
|010| ffffffff       | 1 | ffffffff       | 1 |
|011| ffffffff       | 1 | ffffffff       | 1 |
|012| ffffffff       | 1 | ffffffff       | 1 |
|013| ffffffff       | 1 | ffffffff       | 1 |
|014| ffffffff       | 1 | ffffffff       | 1 |
|015| ffffffff       | 1 | ffffffff       | 1 |
|---|-----|---|-----|---|

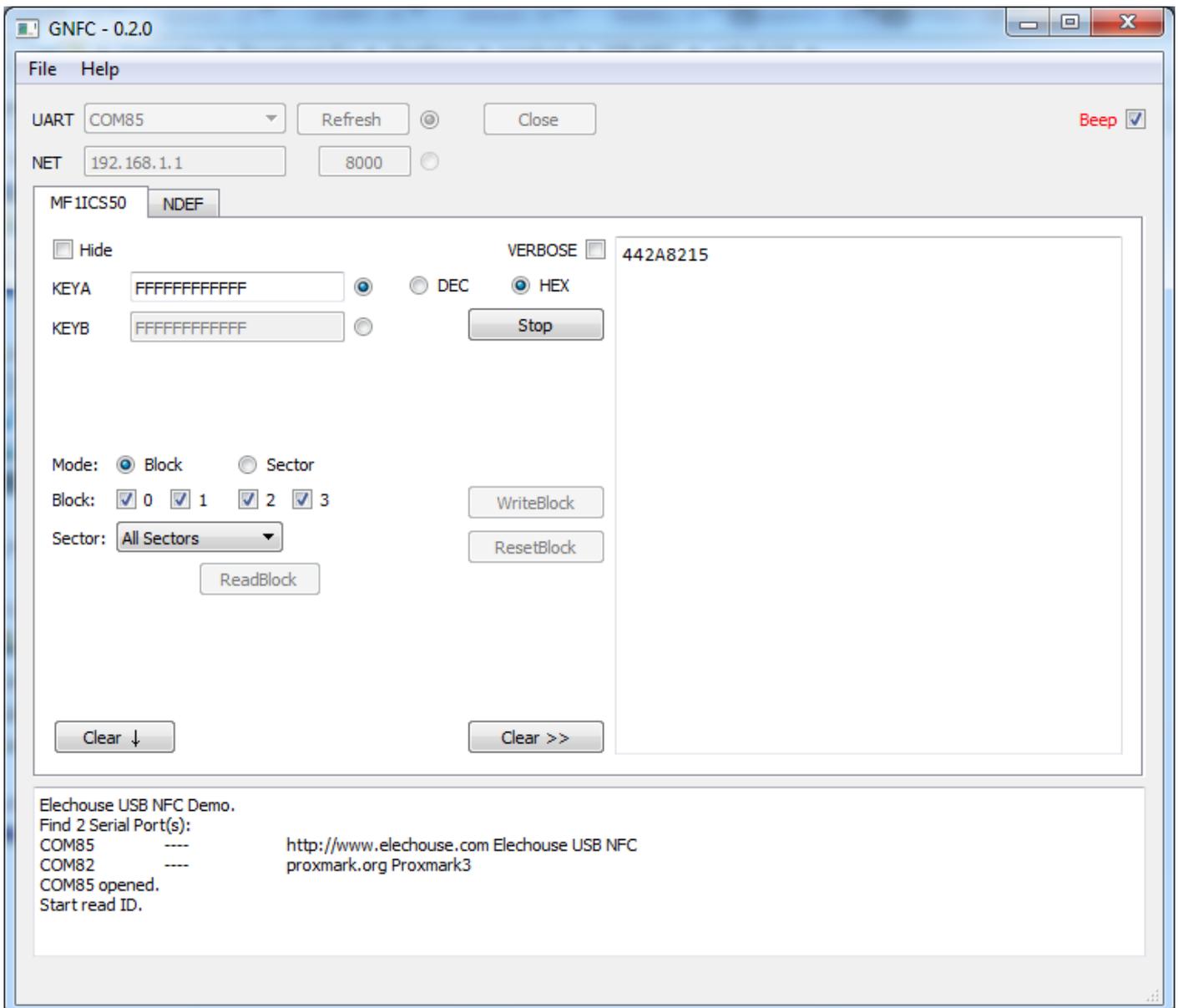
proxmark3>
    
```

Snooping on MIFARE

In order to follow along with the steps in this section you will need an ISO14443-A contactless reader such as the [ELECHOUSE GO2NFC141U NFC Reader](#) and a Mifare 1k Classic tag.

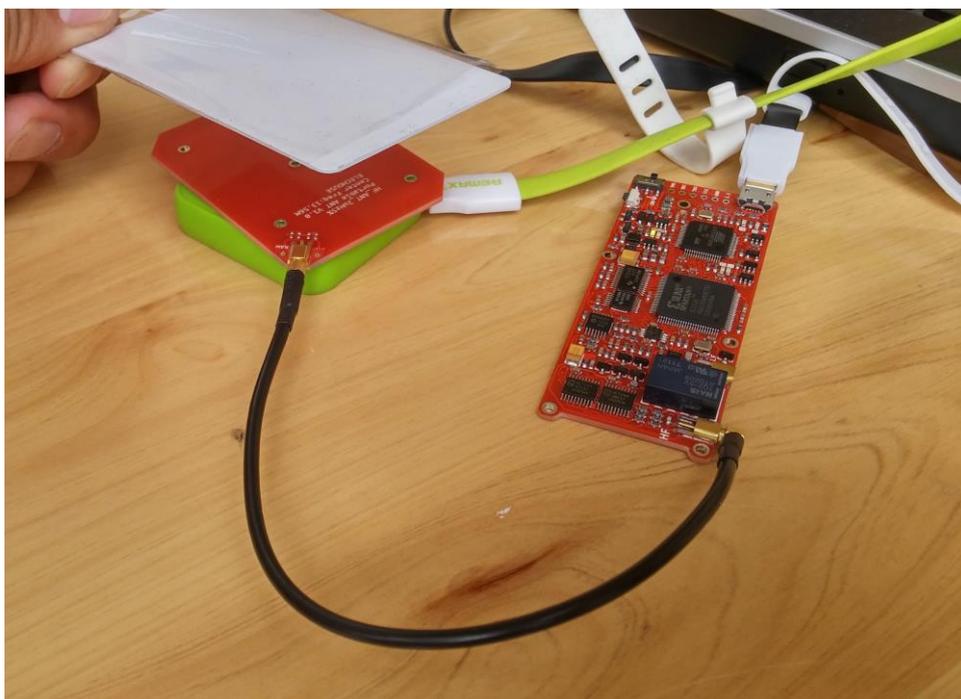


Use the Gonfc Tool to obtain the tag UID.

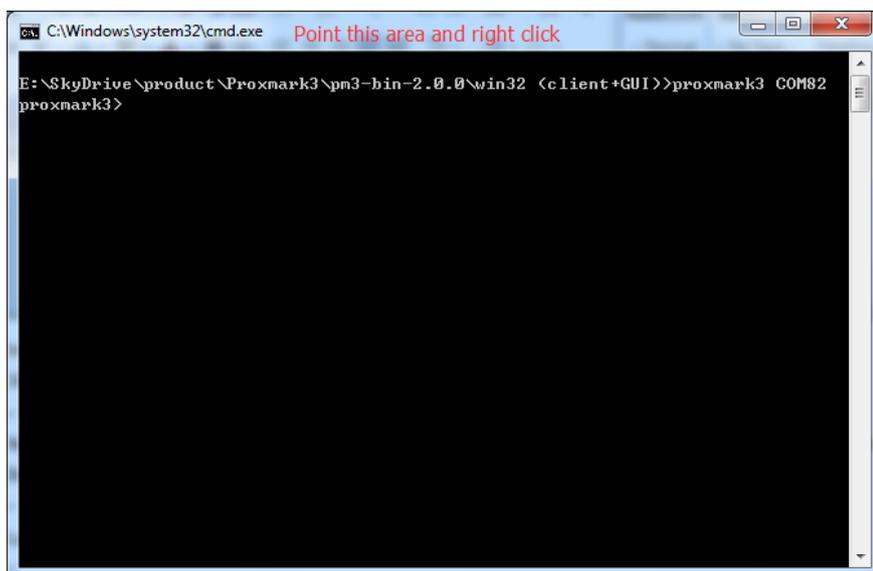


In this example, the tag has UID 44 2A 82 15.

Now fire up your Proxmark and connect an HF antenna. Position your antenna between the reader and tag.

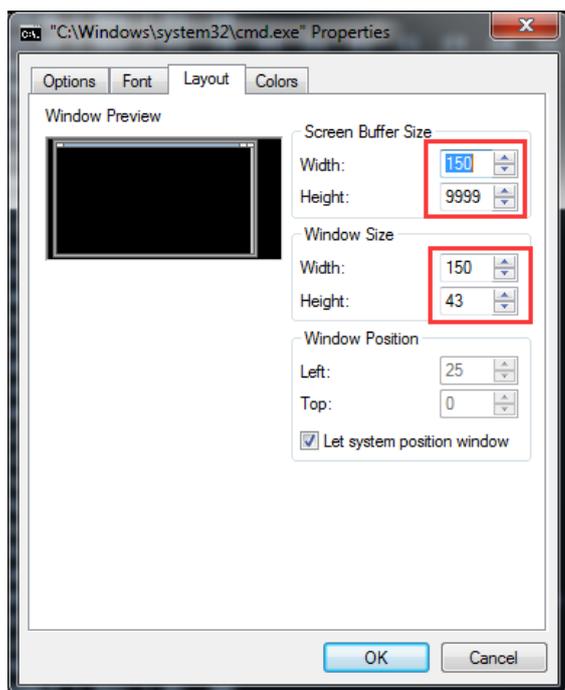


Before sending command to your Proxmark, let's change the property of Command Windows:



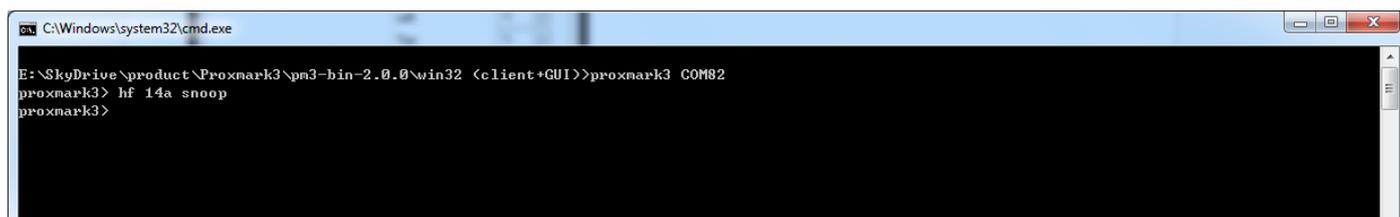
Note that move your mouse to the head of the window.

Right click and chose "**Properties**":

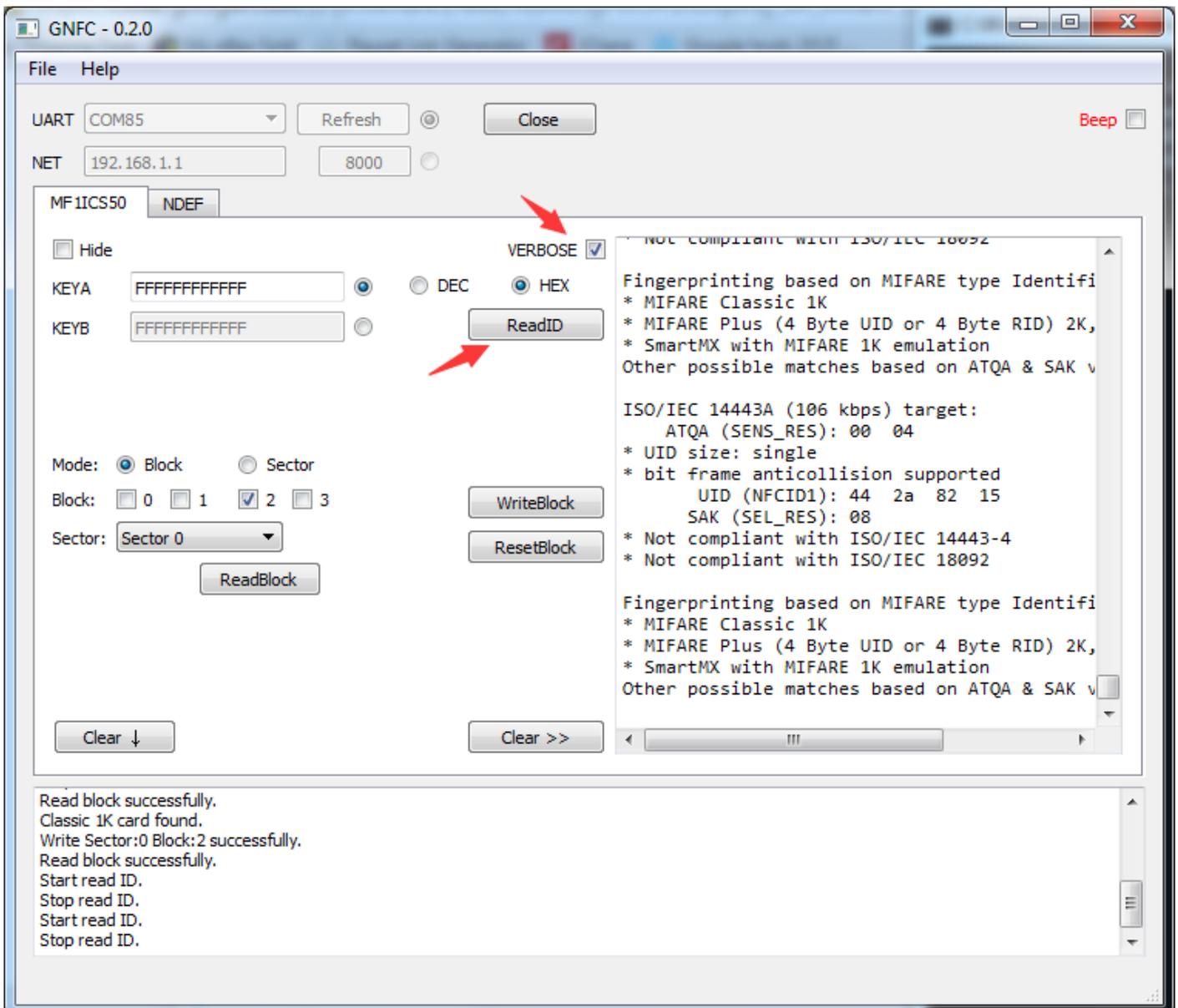


Click OK and the window becomes large.

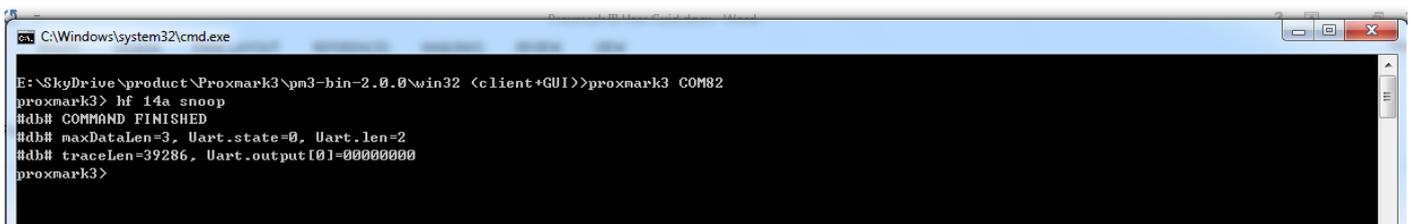
Enter the command **hf 14a snoop**.



Now click the **ReadID** button of Gonfc tool to keep reading the card.



The Proxmark LEDs should blink for a while. Once the buffer of your Proxmark is full, you could see a COMMAND FINISHED message like the one shown below.



Enter the **hf list 14a** command to run it.

Revision History

Rev.	Date	Author	Description
A	May. 1st, 2015	Wilson	Initial version