Proxmark III V2 User Guid

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
**Hardware**

**Main Board**

- CPU : ARM, 512K (AT91SAM7S512) 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**

Battery is not included in the product list, due to battery shipping restriction. [Find more information here.](#)

The board has battery managing and charging circuit. With USB connected, the board automatically draws power from USB and meanwhile charges the battery. With 300mA charging current, the 600mAh battery could be charged full in around 3 hours. It could work for around 4 hours.
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**

<table>
<thead>
<tr>
<th>Cases</th>
<th>LED STD</th>
<th>LED CHR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Indicator</td>
<td>LEB B</td>
<td>LED D</td>
</tr>
<tr>
<td></td>
<td>LED C</td>
<td>LED A</td>
</tr>
<tr>
<td></td>
<td>STD</td>
<td>CHR</td>
</tr>
<tr>
<td></td>
<td>Jlink</td>
<td></td>
</tr>
<tr>
<td>USB CONNECTED, NO BATTERY</td>
<td>ON</td>
<td>FLAShING</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----</td>
<td>---------</td>
</tr>
<tr>
<td>USB AND BATTERY CONNECTED, CHARGED FULL</td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>USB AND BATTERY CONNECTED, CHARGING</td>
<td>OFF</td>
<td>ON</td>
</tr>
<tr>
<td>NO USB, BATTERY CONNECTED</td>
<td>OFF</td>
<td>OFF</td>
</tr>
<tr>
<td>NO USB, NO BATTERY</td>
<td>OFF</td>
<td>OFF</td>
</tr>
</tbody>
</table>

LED **Power Indicator** lights if the board is powered on.

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

<table>
<thead>
<tr>
<th>Tags</th>
<th>Frequency</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mifare S50 (M1)</td>
<td>HIGH</td>
<td>Fixed UID, read/write user data</td>
</tr>
<tr>
<td>Mifare Ultralight (M0)</td>
<td>HIGH</td>
<td>Fixed UID, read/write user data</td>
</tr>
<tr>
<td>Mifare UID (Chinese Magic Card)</td>
<td>HIGH</td>
<td>Modify UID, used to clone, read/write user data</td>
</tr>
<tr>
<td>EM4XX (ID tag)</td>
<td>LOW</td>
<td>Fixed ID</td>
</tr>
<tr>
<td>T5577</td>
<td>LOW</td>
<td>Modify ID, used to clone</td>
</tr>
<tr>
<td>HID Prox II</td>
<td>LOW</td>
<td>Widely used in USA, read/write user data</td>
</tr>
</tbody>
</table>
Board Shell

This shell is made of RF4, which is the same material as the main board. This shell mainly prevents 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:

<table>
<thead>
<tr>
<th>LED</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>STD</td>
<td>Light on if there is no battery or the battery is charged full</td>
</tr>
<tr>
<td>CHR</td>
<td>Flash quickly if there is no battery connected</td>
</tr>
<tr>
<td>LED A</td>
<td>Flash once</td>
</tr>
<tr>
<td>LED B</td>
<td>Flash once</td>
</tr>
<tr>
<td>LED C</td>
<td>Flash once</td>
</tr>
<tr>
<td>LED D</td>
<td>Flash twice</td>
</tr>
</tbody>
</table>

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...
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.

![Unknown device Properties](image)

Step 5

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

![Update Driver Software - Unknown Device](image)

Select “Browse my computer for driver software”. Select the driver folder within the Proxmark 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 2-1:1.1: new full-speed USB device number 71 using ehci_hcd
[1142387.853698] cdc_acm 2-1:1:0: This device cannot do calls on its own. It is not a modem.
[1142387.853742] cdc_acm 2-1:1:0: ttyACMD: 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:

**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.

```
$ proxmark3 hw tune

Measuring antenna characteristics, please wait........
- LF antenna: 14.99 u & 125.00 kHz
- LF antenna: 14.44 u & 134.00 kHz
- LF optimal: 15.40 u & 126.32 kHz
- HF antenna: 16.94 u & 13.56 MHz

Displaying LF tuning graph. Divide 89 is 134kHz, 95 is 125kHz.
```

![Image of proxmark3 output]

![Image of tuning graph]
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.

![Command Output](image)

**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.*
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.

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.
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.
Next, enter the command hf 14a list and observe the tag UID in the resulting trace.

With to those data you could also do crack things. For more information, please refer to this page:

https://code.google.com/p/proxmark3/wiki/RunningPM3#Snooping_on_Mifare_communications

More reference:

https://github.com/Proxmark/proxmark3/wiki/
https://code.google.com/p/proxmark3/wiki/RunningPM3#Running_the_PM3

Disclaimer

I. This document is for ELECHOUSE Proxmark3 board. This product is provided ‘as is’ without any representation or endorsement made and without warranty of any kind whether express or implied, including but not limited to the implied warranties of satisfactory quality, fitness for a particular purpose, non-infringement, compatibility, security and accuracy. We do not warrant that the functions of this module will be uninterrupted or error free, or that defects will be corrected. This product is not designed for medical, life saving, or life sustaining application. In no event will we be liable for any loss or damage including, without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from use or loss of use of, data, or profits, arising out of or in connection with the use of Proxmark3 board.

II. This board should be used at your own risk. We do not afford any loss or illegal consequence caused by misuse of this product.

III. We have the right to refuse offering any technique service in certain cases as this product could do beyond law. All the software and code is free to modify and use.

IV. This document might be modified in the future without any notification.
## Revision History

<table>
<thead>
<tr>
<th>Rev.</th>
<th>Date</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>May. 1st, 2015</td>
<td>Wilson</td>
<td>Initial version</td>
</tr>
<tr>
<td>B</td>
<td>Jun. 30th, 2015</td>
<td>Wilson</td>
<td>For V2</td>
</tr>
</tbody>
</table>