



# Proxmark III User Guide

# Table of Contents

Getting Started.....	1
Pre-Flight Check .....	2
Client Software.....	2
Checking Antennas .....	3
Operating Examples.....	4
Detecting Tag Type .....	4
Reading HID Tags.....	4
Standalone Mode .....	6
Snooping on MIFARE.....	7
Flashing Firmware.....	9
Upgrading from 20090713.....	10



## Getting Started

The Proxmark III is arguably the most powerful device currently available for researching RFID and Near Field Communication systems. A powerful processor, FPGA, and custom firmware allow it to meet the demanding communications timing requirements imposed by various RFID systems. The device targets low and high frequency systems operating at 125kHz, 134kHz and 13.56Mhz.

The device was originally developed by Jonathan Westhues and then released under the GPL. It has since been enhanced and discussed by a great community of enthusiasts who can be contacted through <http://proxmark.org/>. We encourage new users to register with the site and delve into the information available on the forums. There is also a comprehensive manual maintained by the Proxmark community and made available at the link below.

**<http://code.google.com/p/proxmark3/wiki/HomePage>**

---

**⚠ WARNING** **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.

This guide has been written targeting version 20090713 of the Proxmark firmware and client software.

In addition to your Proxmark, at a minimum, you will need a mini USB cable for power and PC communications and either a high or low frequency antenna. Antennas can be made at home or purchased online from <http://proxmark3.com/>.

## Pre-Flight Check

Connect your Proxmark to a PC using the mini 5-pin USB cable pictured on the right.

All Proxmark LEDs should turn on and then quickly turn off in turn. If the LEDs stay lit, this may indicate a problem with your board or that the board has not been programmed correctly.



---

**NOTE** Every board obtained from proxmark3.com has been programmed with the latest stable firmware available at the time and rigorously tested to ensure proper functionality prior to shipping.

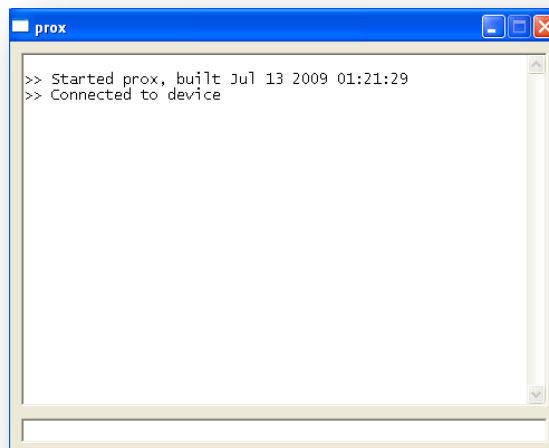
## Client Software

Download the Proxmark client software that corresponds to the version of firmware running on your board from <http://code.google.com/p/proxmark3/downloads/list>.

---

**WARNING** **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.

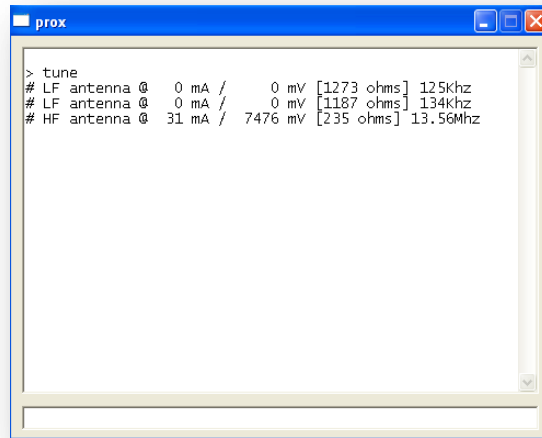
With your Proxmark connected via USB, unpack the archive and fire up a command shell (Win+R, "cmd.exe"). Switch to the winsrc folder and enter **prox gui**. This should launch the windows client and display a window like the one shown to the left.



Commands can be entered in the textbox found at the bottom of the interface. Command responses and debug messages will be printed in the larger textbox.

## Checking Antennas

With your Proxmark connected to a PC and the client running, connect your LF antenna to the Proxmark. Issue the 'tune' command and check that the voltage returned is at least 13V (for 125kHz).



```
> tune
# LF antenna @ 0 mA / 0 mV [1273 ohms] 125khz
# LF antenna @ 0 mA / 0 mV [1187 ohms] 134khz
# HF antenna @ 31 mA / 7476 mV [235 ohms] 13.56Mhz
```

Next, connect your HF antenna and again issue the 'tune' command. The voltage reported should be at least 7V.

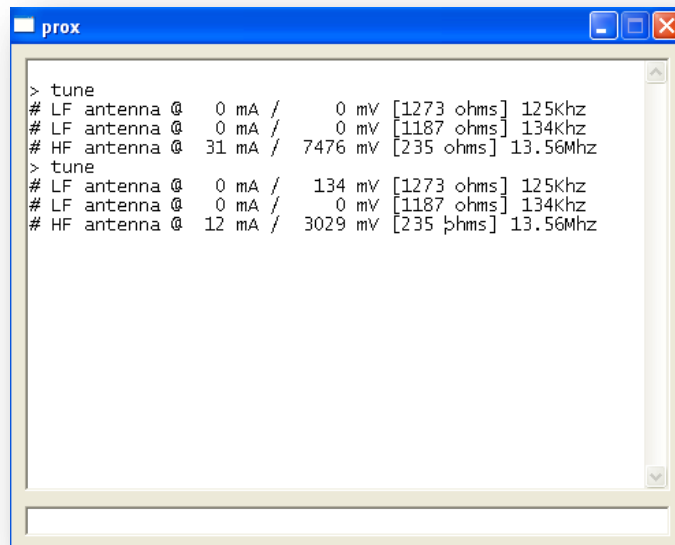
If your HF antenna reports a voltage less than 7V, try flipping the switch on your antenna to the opposite orientation.

## Operating Examples

This chapter provides reproducible demonstrations of the Proxmark in action including tag frequency detection, reading a HID Proxcard II, stand-alone mode, and snooping ISO1443-A traffic between a reader and tag.

### Detecting Tag Type

The frequency of an unknown tag can be determined by comparing antenna voltage readings when the tag is in-field vs. out of range. If the tag is high frequency, you should observe a voltage drop of 3V or more on the HF antenna when the tag is in field.



```

> tune
# LF antenna @ 0 mA / 0 mV [1273 ohms] 125khz
# LF antenna @ 0 mA / 0 mV [1187 ohms] 134khz
# HF antenna @ 31 mA / 7476 mV [235 ohms] 13.56Mhz
> tune
# LF antenna @ 0 mA / 134 mV [1273 ohms] 125khz
# LF antenna @ 0 mA / 0 mV [1187 ohms] 134khz
# HF antenna @ 12 mA / 3029 mV [235 ohms] 13.56Mhz

```

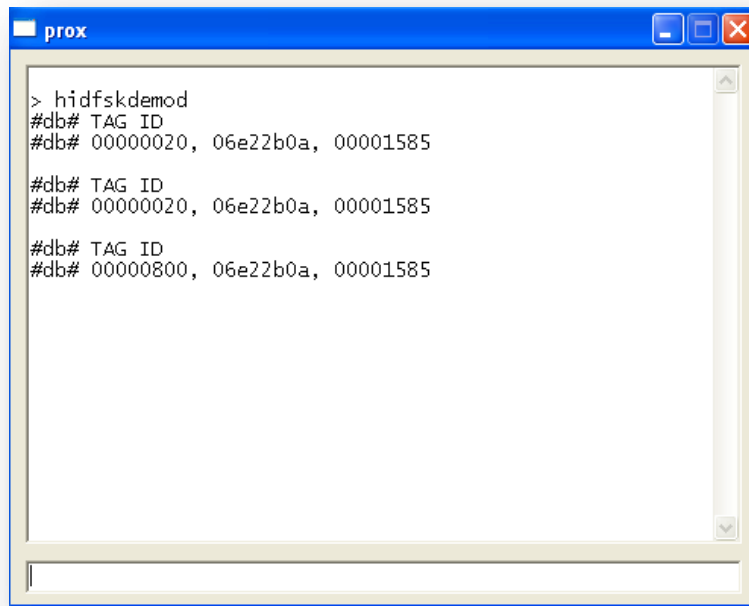
Similarly, when an LF tag is in-field, you should observe a voltage drop of 3V or more in the LF antenna.

### Reading HID Tags

The Proxmark firmware already includes comprehensive support for reading and simulating HID tags. The firmware does not include routines for writing to HID tags. Reading and simulation functions are accessed via the commands **hidfskdemod** and **hidsimtag**.

The following steps demonstrate how to read and replay a HID tag.

1. Connect the LF antenna to the Proxmark
2. Connect the Proxmark to the PC
3. Run 'prox.exe gui'
4. Enter 'hidfskdemod' and then allow a HID tag to enter the antenna's field. When the tag is in-range you should observe messages displaying the facility code and tag ID like those shown below.



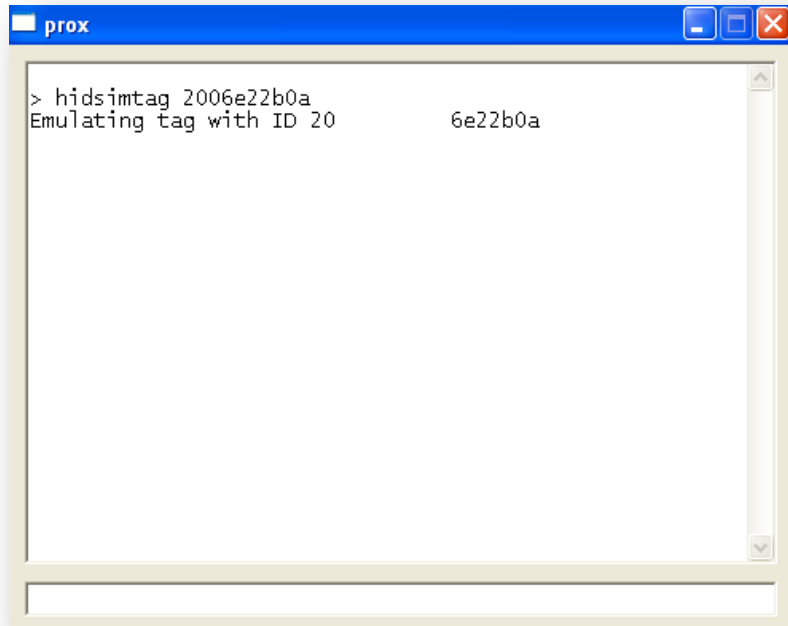
```
prox
> hidfskdemod
#db# TAG ID
#db# 00000020, 06e22b0a, 00001585

#db# TAG ID
#db# 00000020, 06e22b0a, 00001585

#db# TAG ID
#db# 00000800, 06e22b0a, 00001585
```

5. To simulate the tag previously read, concatenate the first two hexadecimal values and pass them as the first parameter to the hidsimtag command as

shown below (e.g. hidsimtag 2006e22b0a).



6. This will cause the yellow LED of the proxmark 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's button.

## Standalone Mode

Standalone mode allows for storage and replay of two different HID tags without the Proxmark being attached to a PC.

---

**NOTE** You will need a USB battery to operate the Proxmark without a PC. USB batteries are sold separately.

To enter standalone mode, hold the button down for a few seconds until the LEDs begin to dance. It is best to get comfortable with it by running attached to a PC initially as you will be able to view debug messages.

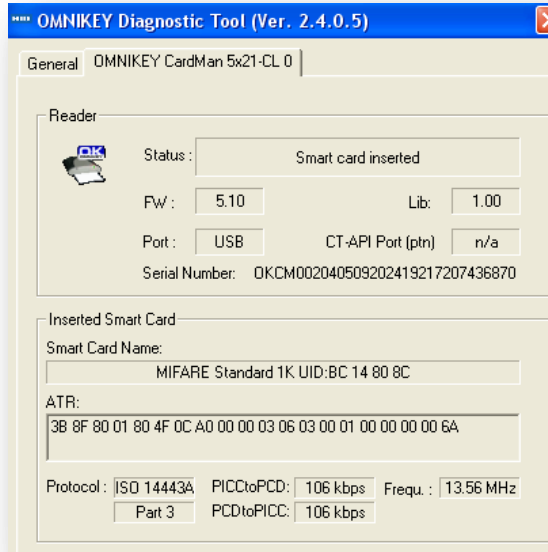
To record a tag, hold the button again while close to the tag and wait for LEDs to change. To replay, press button once more. Make a note of which LED is lit at the time of recording/replay as this indicates the active slot. There are two slots, red and orange.

Further information on standalone mode can be found at the URL below.

[http://code.google.com/p/proxmark3/wiki/RunningPM3#Standalone\\_Mode\\_-\\_HID\\_Prox\\_emulation](http://code.google.com/p/proxmark3/wiki/RunningPM3#Standalone_Mode_-_HID_Prox_emulation)

## 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 Omnikey 5321 and a Mifare 1k Classic tag.



Use the Omnikey Diagnostic Tool to obtain the tag UID.

In the sample read to the left, we see that our tag has UID **bc 14 80 8c**.

Now fire up your Proxmark and connect an HF antenna. Position your antenna between the reader and tag. Launch the Proxmark client and enter the command **hi14asnoop**.

The Proxmark LEDs should blink for a while until you see a COMMAND FINISHED message like the one shown below.

```
> hi14asnoop
#db# COMMAND FINISHED
#db# 00000022, 00000000, 00000001

#db# 00000020, 00000bb9, 00000052
#db# 00000022, 00000000, 00000001

#db# 00000020, 00000bb9, 00000052
```

Next, enter the command **hi14alist** and observe the tag UID in the resulting trace.

```
> hi14alist
recorded activity:
ETU      :rssi: who bytes
-----+-----+-----+-----
+      0:      :      50 00 57 cd
+ 20232:      :      93 20
```

+ 10768: : 93 70 bc 14 80 8c a4 cb 8b  
+ 92000: 0: TAG 04  
+ 19992: : 52  
+ 64: 0: TAG 04 00  
+ 7696: : 93 20  
+ 64: 0: TAG **bc 14 80 8c** a4

## Flashing Firmware

Proxmark firmware is comprised of three logical sections: bootrom, fpga and operating system. The bootrom is a relatively small bit of code that performs some basic hardware initialization, supports reflashing the device over USB and knows how to transfer execution to the operating system. Due to the limited number of features exposed by the bootrom, it is not frequently updated and so you should only rarely need to update it when there is a compatibility conflict.

### Bootrom

- Supports reflashing over USB
- Transfers execution to OS
- Safety in case OS is corrupted

### FPGA

- Intermediate processing of RF signals
- Makes signals available to ARM

### Operating System

- Communicates with client over USB
- Implements most of the Proxmark's functionality
- Most frequently updated

The FPGA code processes analog signals coming from the antennas and makes those signals available to the ARM. Like the bootrom code, the FPGA code is not frequently updated. Presently, the operating system is the most frequently updated portion of Proxmark code. It is responsible for receiving and executing most of the commands advertised in the client user interface.

### WARNING

**Upgrading the bootrom of your Proxmark can brick the device.** Please exercise caution when upgrading the bootloader. If the bootloader is corrupted, the only way to restore your Proxmark to working order will be through the use of a JTAG programmer.

## Upgrading from 20090713

Ensure that you have read the prior section before proceeding. In order to upgrade to the latest version of firmware, you will need to first upgrade the Proxmark's bootloader.

The steps below will upgrade a 20090713 bootloader to version 20090905 using a Windows based host PC.

1. Download the 20090713 software distribution if you have not done so already
2. Download the 20090905 software distribution from <http://proxmark3.googlecode.com/files/pm3-20090905-r216.zip>
3. While holding the Proxmark button down, connect it to the PC. The yellow and red LEDs should stay lit.
4. From the 20090713 folder, execute the command below. Note that the target bootrom image is in the 20090905 software distribution folder.

```
> prox bootrom ..\pm3-20090905-r216\bootrom\obj\bootrom.s19
```

```
expected = 000017e4 flush, c.ext1 = 00001700
done.
```

---

**NOTE** At this point the bootrom has been updated and the Proxmark is now in a position to have its OS upgraded. You can still interact with the Proxmark using the 20090713 client at this stage.

The following steps will upgrade the Proxmark Operating System and FPGA code to version 20090905.

1. Ensure that the Proxmark is not connected to the PC.
2. Hold down the Proxmark's button and connect it to the PC. After the yellow and red LEDs are lit, execute the command below from within the 20090905 software distribution folder

```
> prox fpga ..\armsrc\obj\fpimage.s19
```

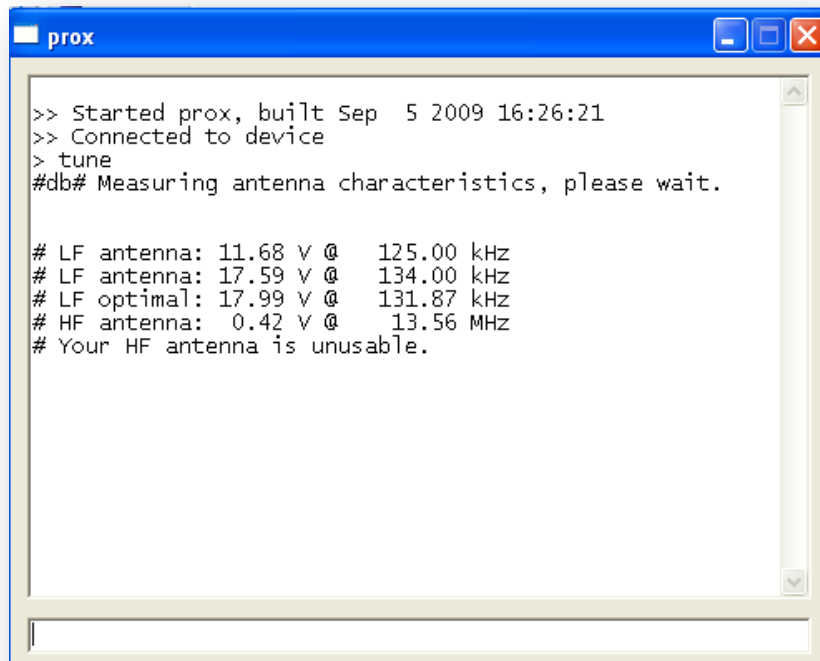
```
..no device connected, polling for it now
Flashing fpga from ..\armsrc\obj\fpimage.s19
Flashing address: 0010c400
done.
```

3. If the previous step is successful, disconnect the Proxmark.
4. While holding the button, connect the Proxmark to the PC and wait for the yellow and red LEDs to stay lit. Execute the command below from within the 20090905 software distribution folder

```
> prox os ..\armsrc\obj\osimage.s19
```

```
Flashing os from ..\armsrc\obj\osimage.s19  
Flashing address: 00120400  
done.
```

5. Disconnect the Proxmark from the PC and then reconnect it.
6. Launch the client software by executing “prox gui” from a command shell. The client should display a build date of “Sep 5 2009” as shown below.



```
prox  
>> Started prox, built Sep  5 2009 16:26:21  
>> Connected to device  
> tune  
#db# Measuring antenna characteristics, please wait.  
  
# LF antenna: 11.68 V @ 125.00 kHz  
# LF antenna: 17.59 V @ 134.00 kHz  
# LF optimal: 17.99 V @ 131.87 kHz  
# HF antenna:  0.42 V @ 13.56 MHz  
# Your HF antenna is unusable.
```

---

**NOTE** The Proxmark is now running firmware version 20090905 and can be controlled using the client included with the software distribution.