Boscloner RFID Cloner Instruction Manual

[Boscloner/Proxmark3 Board overview](#_30j0zll)

[Building the Board](#_1fob9te)

[Source code development for the Boscloner PM3 Board](#_3znysh7)

[Boscloner Shield Board Overview](#_2et92p0)

[Building the BCS](#_tyjcwt)

[Standard SMT assembly process](#_3dy6vkm)

[Off-the-shelf modules](#_1t3h5sf)

[Source code development for the Boscloner Shield](#_4d34og8)

[Maxiprox modifications](#_2s8eyo1)

[Maxiprox back Shield](#_17dp8vu)

[Maxiprox Boscloner Power Supply](#_3rdcrjn)

[Complete Assembly](#_lnxbz9)

[Boscloner App Overview.](#_35nkun2)

[App Installation instructions](#_1ksv4uv)

[App Usage Instructions](#_44sinio)

[Boscloner/PM3 Operation](#_2jxsxqh)

[Operation Features](#_z337ya)

[Instructions](#_3j2qqm3)

[Known Issues](#_1y810tw)

[Boscloner/PM3 board](#_4i7ojhp)

[Boscloner App](#_2xcytpi)

# 

# 

# Boscloner/Proxmark3 Board overview

The Boscloner/Proxmark3 (BC/PM3) board is based upon the available Proxmark3 design. The BC/PM3 has the added following features. The BC/PM3 board has added 2x 8 Pin headers which breakout the SPI bus and extra IO on the PM3 board. The extra headers are used to allow a Boscloner “shield” to be plugged into and communicate with the PM3 board. The Boscloner Shield is intended to act as a gateway to the PM3 which allows for custom commands and functionality to added to the base functionality of the PM3. The shield also allows for many types of additional functions to be added, some of which were used on the Boscloner Shield board.

See below images of the BC/PM3 and the attached Boscloner Shield.

# Files to Build Custom PM3/Boscloner Hardware

## Gerbers/PCB Order PCBs OSHPARK Links

Primary Links:

<https://oshpark.com/shared_projects/hZJ27cS3>

<https://oshpark.com/shared_projects/u9C9kyNT>

Alternate Links:

<https://goo.gl/BhkWMU>

<https://goo.gl/qOoT3d>

## BOMs

**PM3 Boscloner BOM:**

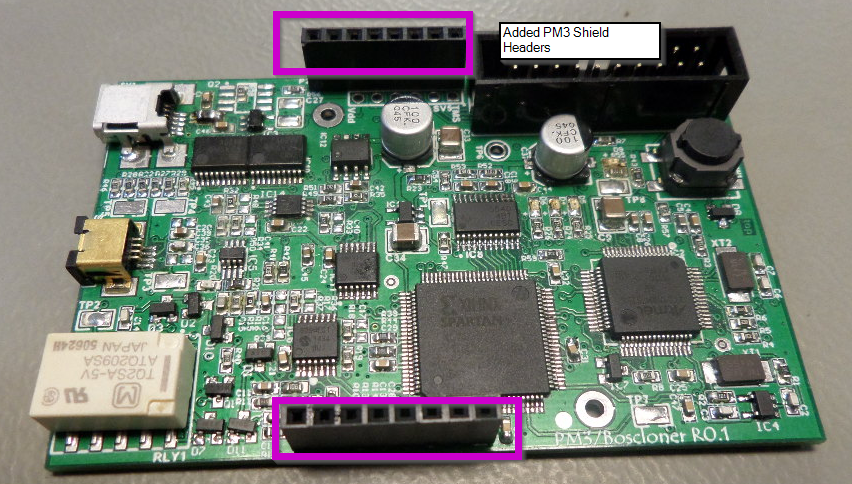
https://drive.google.com/open?id=1QqRfBo-nAWihncCsJcRonsI2mHAPkj5nPE-OU\_Jk-BA

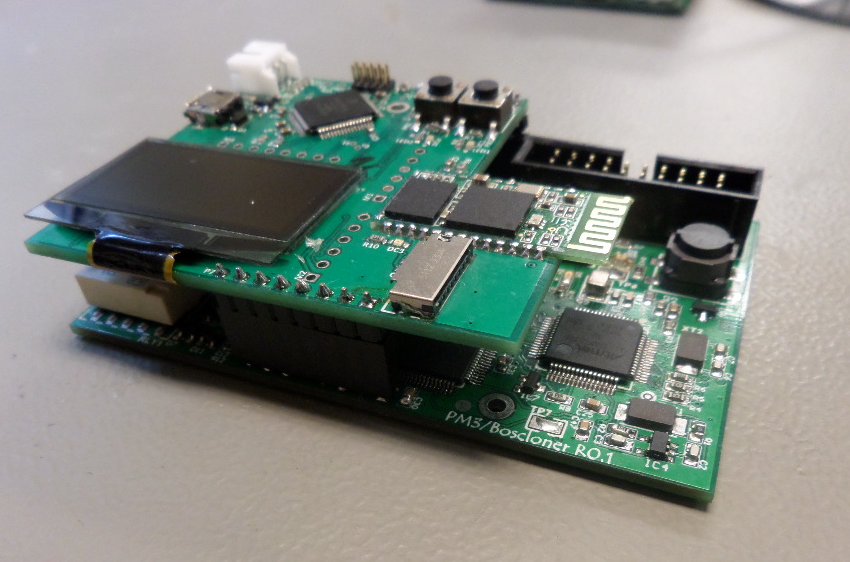
**PM3 Boscloner Shield BOM**

https://drive.google.com/open?id=1wFyfo9XqFWLF1M1fU2edb8gq\_--JXYc7XXYAJH63Omo

## Building the Board

To build the board, the user can order the parts from the supplied BOM and self build the board.

**PM3/Boscloner Board**



**PM3 with Boscloner Shield**

## Source code development for the Boscloner PM3 Board

The Boscloner PM3 functionality is based upon the stock Proxmark ProxSpace project which contains all of the stock PM3 functionality. Instructions for setting using the Proxmark3 (all apply to using the Boscloner Proxmark3) can be found on the [Proxmark3 github wiki here](https://github.com/Proxmark/proxmark3/wiki/Windows) (https://github.com/Proxmark/proxmark3/wiki/Windows). The modified source code for the Boscloner project is available from the Boscloner source package (<https://goo.gl/gdNiVp>) and can be used as a basis for further adding additional custom functionality to the Boscloner/PM3 environment.

# Boscloner Shield Board Overview

The Boscloner Shield (BCS) was designed as a shield to plug into the BC/PM3 board and add the following features.

**Features**

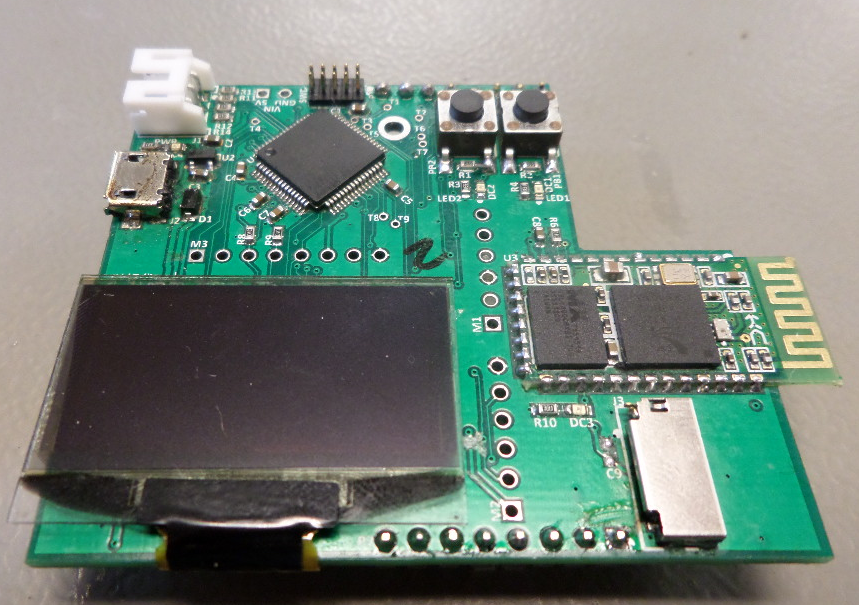
* SPI gateway to send and receive custom commands from the BC/PM3 board.
* Bluetooth communication
* OLED 128x64 LCD
* Wiegand decoding plug in interface
* Optional SD card expansion
* 2x Push buttons
* 2x User LEDs
* High performance MK22FN512LH12 MCU
  + 120Mhz performance
  + Floating point operation
  + 512KB flash
  + 128KB SRAM
* Optional USB functionality
  + Additional power
  + Optional USB communication

## Building the BCS

The BCS can be built in two different ways to allow it to be easily assembled using off-the-shelf modules or to be professional built using standard SMT assembly processes.

## Standard SMT assembly process

The BCS uses standard SMT components to allow to be be easily assembled by any SMT assembly house. Or optionally, a user can hand-build the board using standard SMT parts from the supplied BOM.

**Complete SMT build**

## Off-the-shelf Modules

The BCS was designed to optional allow for a number of off-the-shelf modules to be directly plugged in and soldered to additional headers on the board.

Available Modules

**Adafruit 1.3” or .96” 128x64 OLED display**

<https://www.adafruit.com/product/938>

<https://www.adafruit.com/product/326>

**HC-06 Bluetooth module\***

<http://www.amazon.com/JBtek-Bluetooth-Converter-Serial-Communication/dp/B00L08GA4Q>

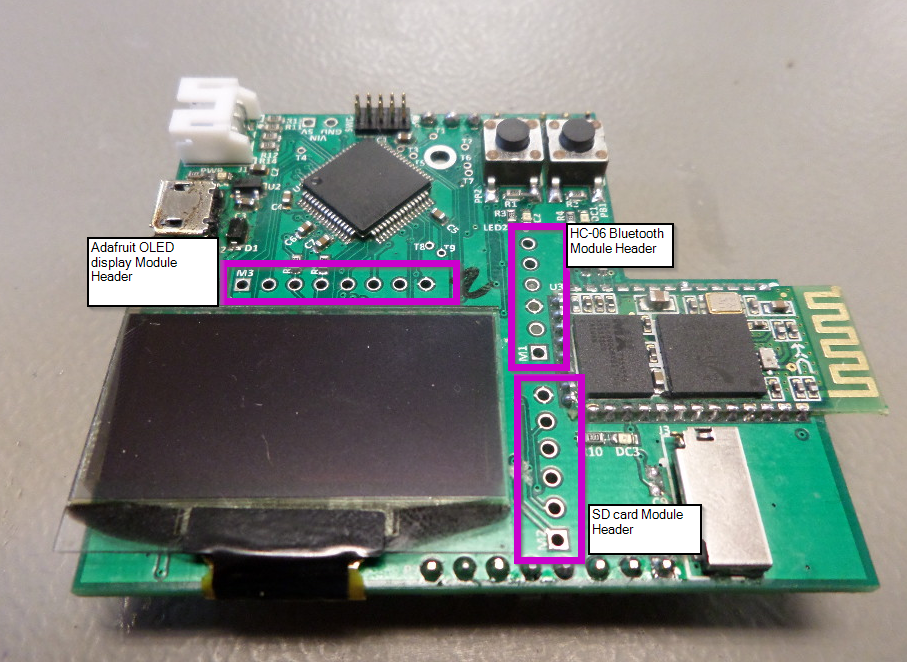
*\*Optionally, any Bluetooth module with the same pinout can be used.*

**SD Card Module**

Ebay SD Card Module: “TF Micro SD Card ModuleMini SD Card Module Memory Module For Arduino ARM”

<http://www.ebay.com/itm/like/221906031160?ul_noapp=true&chn=ps&lpid=82>

Optionally, any SD module with the same pinout can be used.

**Module Header Locations**

## Source code development for the Boscloner Shield

The Boscloner shield uses a freescale kinetis MCU, which is a high performance and low cost processor very capable of handling any job that the user may want to do when working with the proxmark3 board. The source code was developed in [Kinetis Design Studio](http://www.nxp.com/products/software-and-tools/run-time-software/kinetis-software-and-tools/ides-for-kinetis-mcus/kinetis-design-studio-integrated-development-environment-ide:KDS_IDE) (KDS) (<http://www.nxp.com/products/software-and-tools/run-time-software/kinetis-software-and-tools/ides-for-kinetis-mcus/kinetis-design-studio-integrated-development-environment-ide:KDS_IDE>) which is a free unlimited eclipse based IDE that users can use to modify the existing source to create their own custom functionality. The IDE runs on Linux or Windows OS. There are many types of additional functionality that could potentially be added to the Boscloner shield and new pieces of functionality can be easily added using this environment and the available source code.

# Maxiprox 5375 modifications

The HID Maxiprox 5375 Long Range Reader can be purchased from a variety of sources, including eBay and Amazon. Expected average price is anywhere between $230 - $400:

<http://lmgtfy.com/?q=Maxiprox+5375>

Custom Wiegand Cable with [PHR-3 3pin connector:](http://www.digikey.com/product-search/en/connectors-interconnects/rectangular-connectors-housings/1442556?k=phr-3) (<http://www.digikey.com/product-search/en/connectors-interconnects/rectangular-connectors-housings/1442556?k=phr-3>)

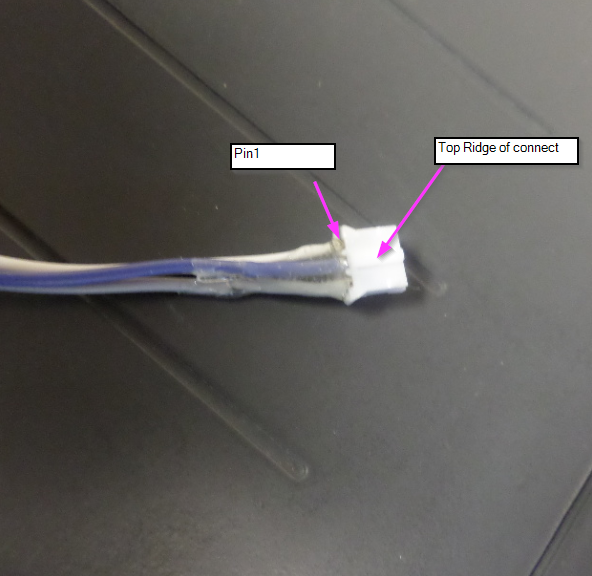
OR [assembled PH JST cable from amazon](http://www.amazon.com/3-Pin-Female-PH-Style-Distance-Sensors/dp/B00CHTNGJ4/ref=sr_1_2?ie=UTF8&qid=1456416610&sr=8-2&keywords=ph-3++cable): (<http://www.amazon.com/3-Pin-Female-PH-Style-Distance-Sensors/dp/B00CHTNGJ4/ref=sr_1_2?ie=UTF8&qid=1456416610&sr=8-2&keywords=ph-3++cable>).

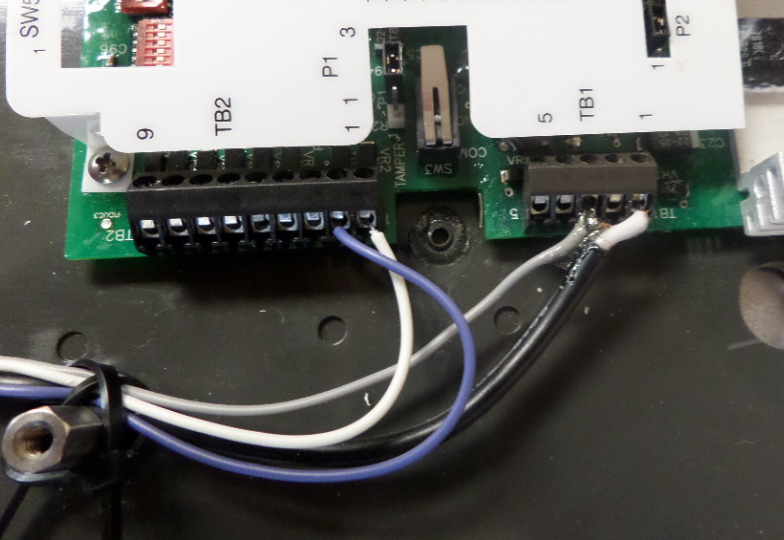
The cable should be roughly 12” in length. The wiring should be as shown in the image:

Pin1: D0 connect to TB3-1

Pin2: D1 connect to TB3-2

Pin3: Ground connect to TB1-3 (with the power supply ground)





Custom Power Cable : See section “Maxiprox Boscloner Power Supply” for instructions

# Maxiprox Boscloner Power Supply

Lenmar Powerport 19V/5V Power Supply - PPU916RS

<http://www.amazon.com/gp/product/B008EG64PC?psc=1&redirect=true&ref_=oh_aui_detailpage_o00_s00>

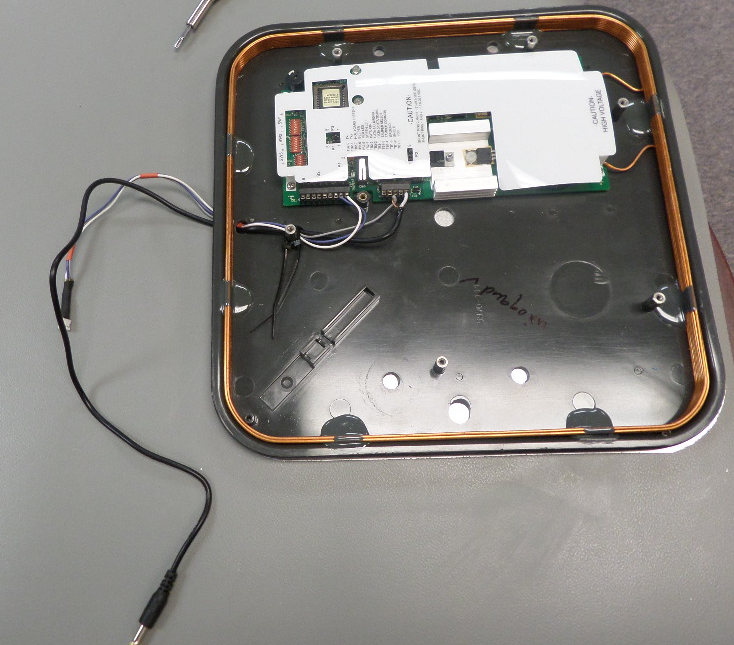
<http://www.amazon.com/Lenmar-PPU916RS-Ppu916rs-Powerport-Notebook/dp/B00E4TJYDM/ref=sr_1_6?s=pc&ie=UTF8&qid=1456360181&sr=1-6&keywords=Lenmar+PowerPort>

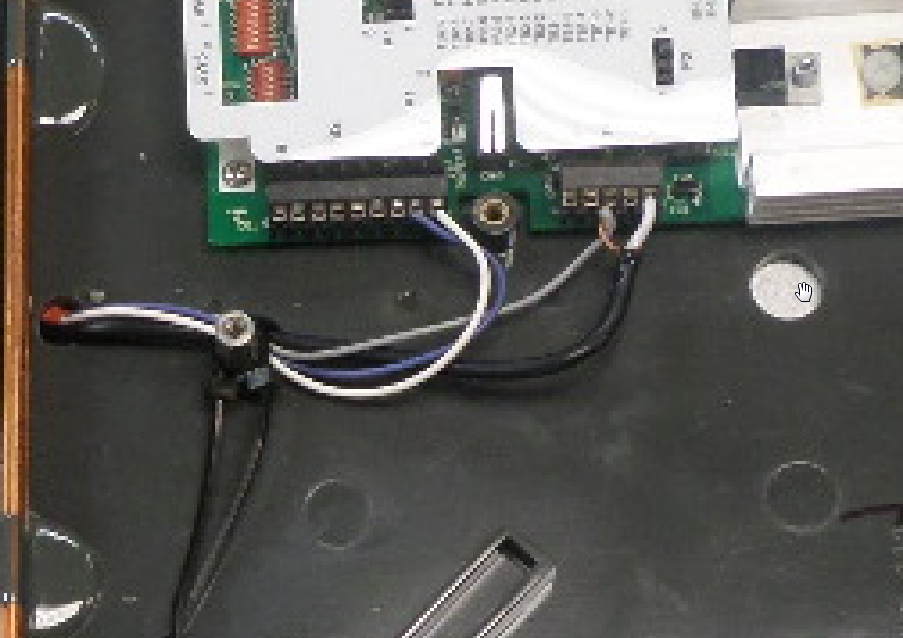
The supplied output power cable for the Lenmar will need to be cut and connected as shown below in order to power the Maxiprox from the Lenmar power supply.

**Lenmar Power cable wiring**

White = 19V Power - connect to TB1 pin1 as shown of the Maxiprox

Copper = Ground - Solder to Wiegand ground and connect to TB1 Pin3 of the Maxiprox header as shown.





# Complete Assembly

* Use double sided Velcro attached to backside of the Boscloner/PM3 and the LF antenna
* Connect power mini USB power cable to the Boscloner/PM3
* Connect Hirose USB connector to Boscloner/PM3 and LF antenna
* Connect Wiegand cable from the Maxiprox to the Boscloner/PM3
* Connect the Maxiprox power cable to the Lenmar power supply

# 

# Boscloner App Overview

**Features:**

* View cloned and scanned cards history
* Enable/disable autoclone functionality of Boscloner/pm3
* Clone any of the cards stored in history

## App Installation Instructions

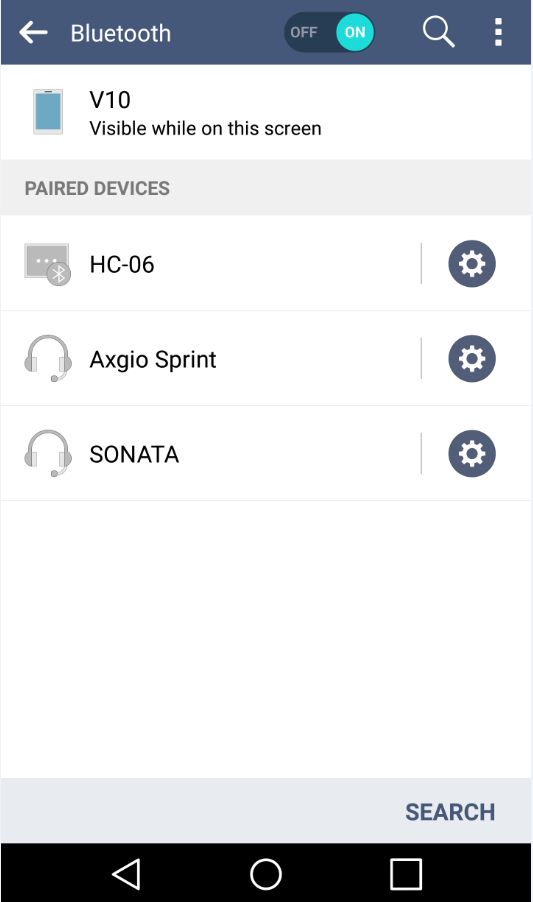
The user can directly download the Boscloner APK application package from the download link (<https://goo.gl/lgySLj>). There may be some warnings about installing an application from outside of the Google Play Store. Click OK on these warnings and install the Boscloner App.

Source code files for the Boscloner app for the purpose of revising the source code, adding features, etc.. can be found below:

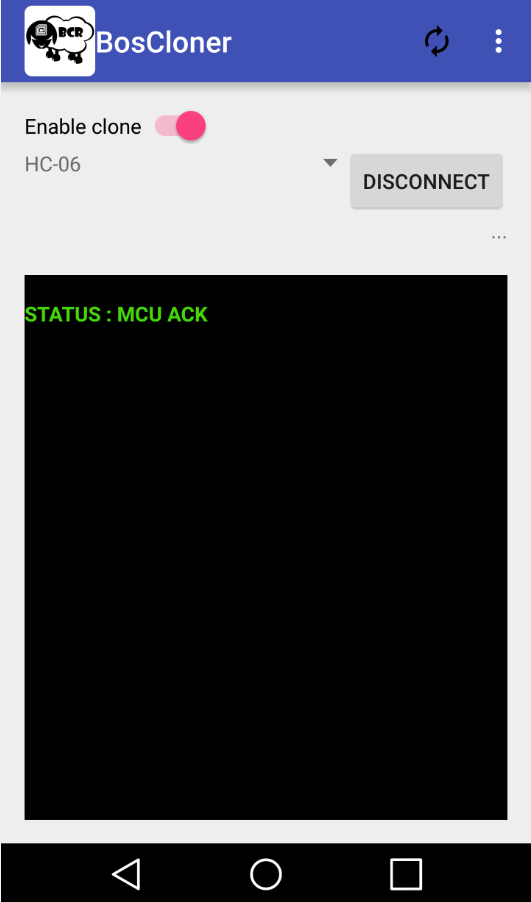
<https://goo.gl/4n48H2>

## App Usage Instructions

1. You must first “pair” with the HC-06 device from the Bluetooth settings in the Android app. Be sure the Boscloner/PM3 is powered on and the Bluetooth LED is blinking. Go to Bluetooth settings from the Android settings, search, then pair with the found HC-06 device.



2) Once the HC-06 has been paired, you can open the Boscloner app and connect to the HC06. Select the HC06 from the drop down menu and press the Connect button. The pink “clone” button will light up and the terminal window will show “MCU ACK” (acknowledge).

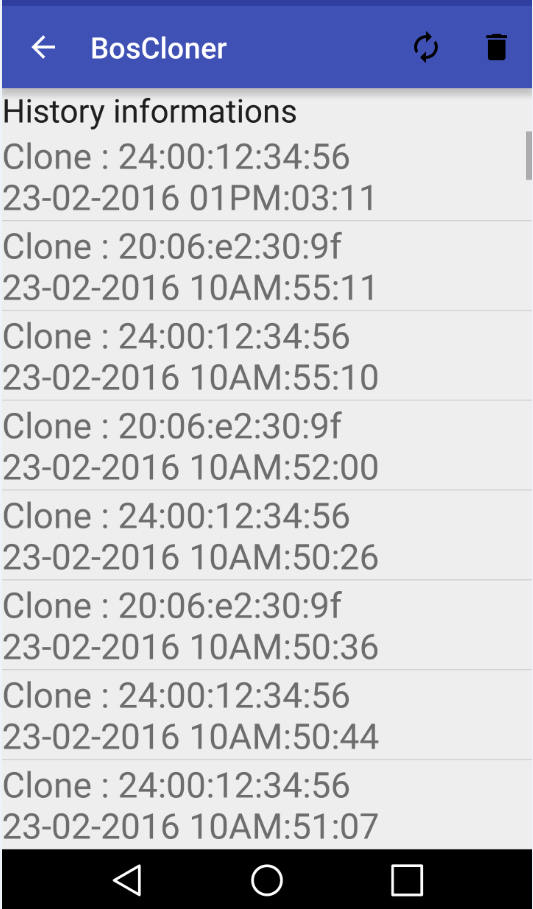


3) The “Clone” button is enabled by default and will cause the Boscloner/PM3 to autoclone cards when the Maxiprox scans card data.

The terminal window will show the data that is “cloned” or “scanned” (only read and not cloned) in the terminal window. When a card is “cloned” the card ID will be stored in the “History” window of the App.

The user can view and clone card IDs directly from the “History” window from the Boscloner App.

4) To clone a stored history value. Click the “...” icon from the main window in the Boscloner App. This will bring up all stored ID values. Scroll to the ID you want to clone and Long Press the ID. A pop-up will ask you if you really want to clone this ID value. Click “OK” and the ID will be sent to the Boscloner/PM3 to be cloned. The result will be displayed on the OLED display of the Boscloner/PM3.



# Boscloner/PM3 Operation

## Operation Features

The Boscloner PM3 has the features outlined in the Overview section. The below image shows the given functions applicable to using the Boscloner to clone and scan cards.

* The Boscloner/PM3 connects to the Boscloner app through the Bluetooth adapter.
* Update data is displayed on the OLED Display.
* Pushbutton enables and disables Auto Clone feature
* The right Pushbutton resets the Shield board.
* The Wiegand connect is used to connect the Maxiprox Wiegand signals to the Boscloner Shield.
* Optional USB power is available through the micro USB connector
* An optional microSD footprint is on the PCB for alternative storage functions



## Instructions

* Power the Boscloner/PM3 using the Mini USB connector on the PM3 Board
* Connect the Wiegand cable from the Maxiprox to the Wiegand Connector shown in the image
* Connect a LF antenna to the PM3 board using the Hirose USB connector

Once the board is powered it will be “Auto-Clone” mode and once a card ID is received from the Wiegand Cable a clone will be run on the PM3 Board and LF Antenna. The display will update with events that are occurring. The Auto-Clone feature can be enabled or disabled using the left push button. Connect to the board using the Boscloner App to utilize more features.

Desired Future Features

* To add the ability to simply type in the ID values that the user wishes to write to a blank card, rather than relying solely on scanning new badges or using the history file.
* Bug fixes
* iOS App
* App and Boscloner shield diversification to support other Wiegand cards, other than HID.

# Known Issues

## Boscloner/PM3 board

* When the PM3 board is connected to a PC and a terminal connection has not been opened, the board will periodically lock up and reset. Tests have done with the original PM3 and the same problem occurs, therefore it is believed that the issue is within the USB driver code of the official Proxspace source code.
* The issue does not occur when the Boscloner/PM3 board is connected to a power supply, which is how the board is expected to be used during real-world applications.

## Boscloner App

* Periodically the “Ring” stops working when a clone or scan is received. The problem is fixed by restarting the App.
* With some Android phones, if the Boscloner app is running and the phone’s display turns off and returns to the lock screen, the App will occasionally become unresponsive and will need to be completely closed and re-opened to restore intended functionality.
* A seemingly rare glitch occurs at times whereby the “history” of cloned badges is replaced with values of all 0’s. Sometimes closing the App and reopening it restores the original values, and other times, the values stored within the history file are lost entirely.

Boscloner Real-World Use

* The Maxiprox “read” antenna is very strong, and can cause interference with the smaller “write” antenna that is used for cloning/writing to new badges. To remedy this, the write antenna and corresponding badge needs to be isolated from possible interference. This is achieved by using a faraday cage based approach. A simple paper cup (large enough to fit the “write” antenna, that is surround with tinfoil, is enough to prevent disruptive interference (See figure of simple faraday cage below). The Boscloner is designed to be used within a laptop messenger bag, but is flexible so as long as the “read” antenna does not interfere with the “write” antenna
* The “write” antenna is weak, and the blank HID badge to be written must be very close and almost directly centered. To remedy this, one may simply attach a one-side sticky piece of velcro to both the HID badge itself, and the “write” antenna. This ensures it is easy enough to place the badge where it needs to be to be properly written to while the user moves around their environment.



**Simple Faraday Cage**

Created with a paper cup, wrapped with tin foil and duct tape on the outside of the cup.