ProxmarkPro User Guide

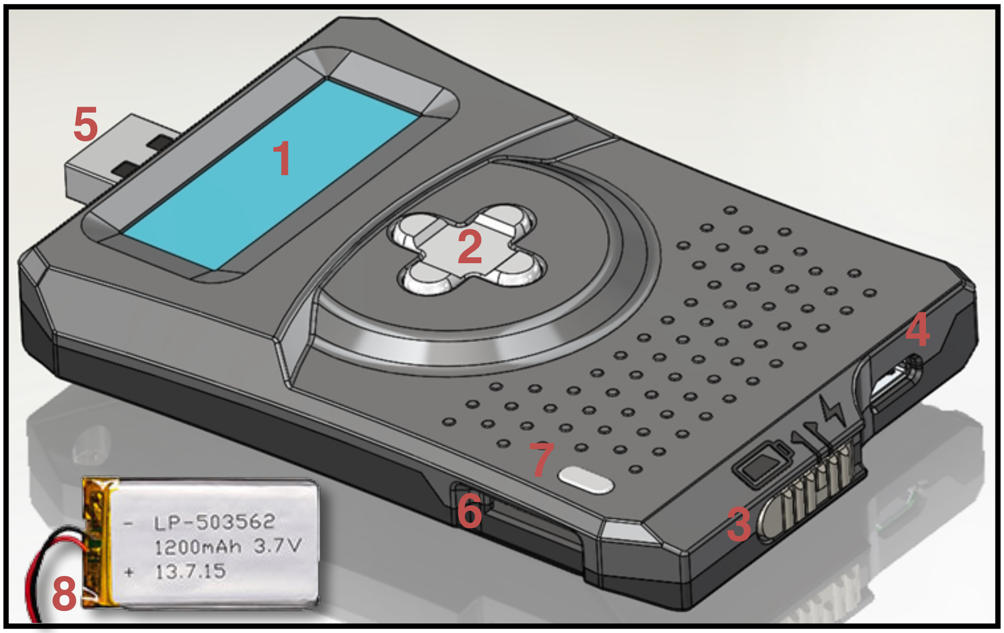
Firmware Version pro-1

January, 2019

Table of Contents

Introduction

The ProxmarkPro is a portable RFID test instrument designed for use in the field.



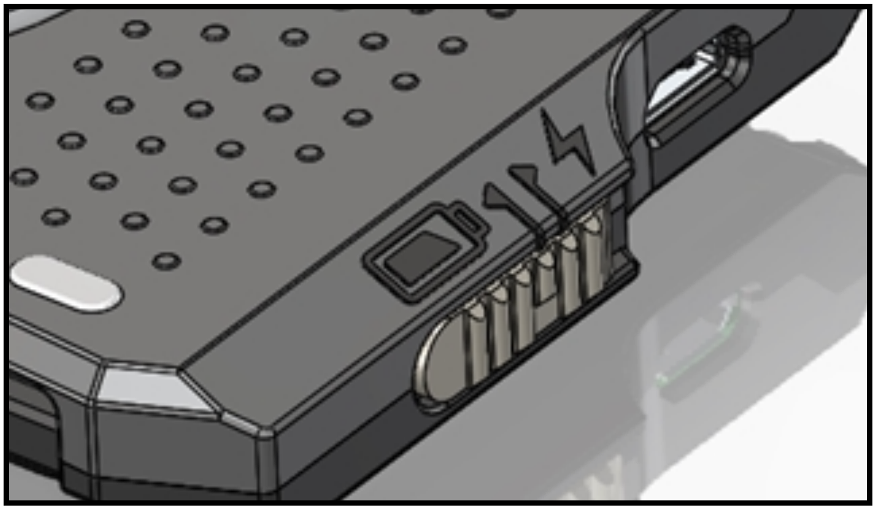
Key components include:

1. **LCD**: 2x16 backlit display, readable in sunlight.
2. **Navigation Switch**: Four button switch allows Navigation in four directions. ↑ ↓ ← →
3. **Power Switch**: Allows device to select between battery and USB power/charge mode.
4. **Power Port**: Micro USB that allows for charge and communication between ProxmarkPro and Computer.
5. **Antenna Port**: USB Type A port where user can connect either an LF or HF Antenna.
6. **Micro SD Card Slot**: Storage for saving and loading tags. Supports cards up to 64 GBs.
7. **LED Charge Indicator**: Tells the user if the battery is being charged.
8. **Rechargeable Battery**: A 1200mAh Li-Po battery gives up to 6 hours of unchained use.

The device is capable of interacting with a variety of tags with operating frequencies at 125kHz, 134kHz and 13.56MHz. While inspired by the Proxmark3 and sharing some of its firmware, the ProxmarkPro hardware is a complete redesign and is not compatible with the Proxmark3.

Power Modes

The ProxmarkPro has two power modes: Battery and USB. These modes are controlled through the use of the power switch pictured below.



Placing the switch in the leftmost position will power the device from the built-in battery. Placing the switch in the rightmost position will power the device over USB when connected to a host and charge the battery simultaneously.

How to charge your ProxmarkPro

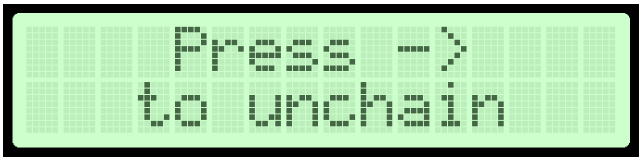
- Connect your ProxmarkPro via USB and the LED should come on. Put switch in USB position.
- When the LED goes off the Pro is fully charged.
- You can also check the status of your charge by going to the device menu and then click battery. Please note this is only an estimate.

***** Warning: Antenna Port is not power, please make sure you plug in your ProxmarkPro via the Micro USB Port. *****

Unchaining

When the ProxmarkPro first boots it will try to enumerate as a CDC modem over USB allowing the user to issue commands through the client software. The ProxmarkPro is primarily designed for use in the field without a PC.

To unchain your ProxmarkPro, place the Power Switch in Battery mode and follow the instructions on-screen.



```
  Press ->
to unchain
```

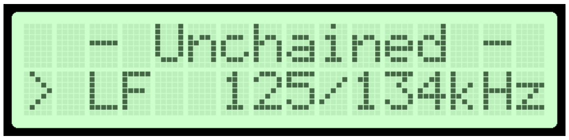
Once unchained, use the friendly on-screen menu to perform various tag operations.

The menu is hierarchical and can be navigated using the up (↑), down (↓), left (←) and right (→) buttons.

Note: *When you enter Unchained mode USB communication will not be permitted and the device will not longer show up as connected to your computer. To get USB communication back all you need to do is exit Unchained mode by pressing the* left (←) until you get back to the boot menu.

Unchained Mode

Use the ↑ and ↓ buttons to navigate to the desired menu function, then use → to select that function. Use the ← button to quickly return to the parent menu (“go back”).

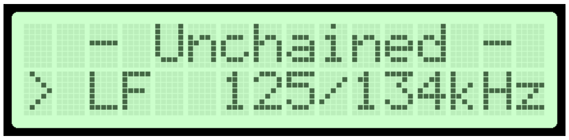
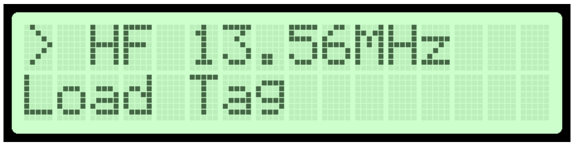
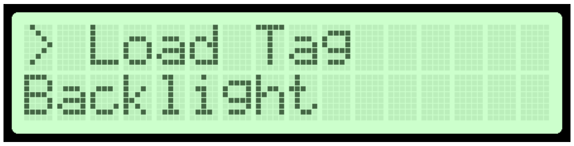
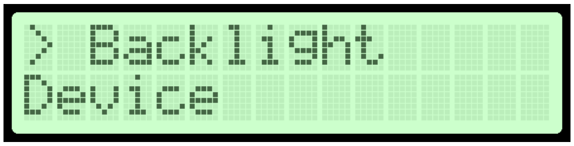
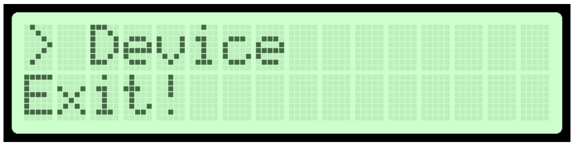


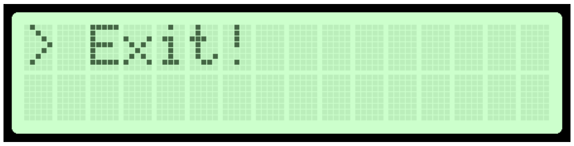
```
 - Unchained -
> LF  125/134kHz
```

The currently selected menu function is prefixed with a ‘ > ’ symbol.

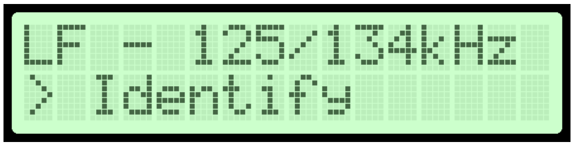
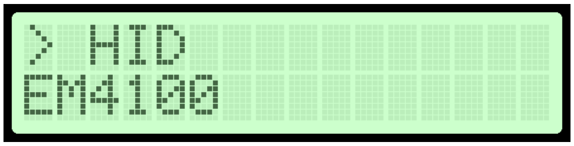
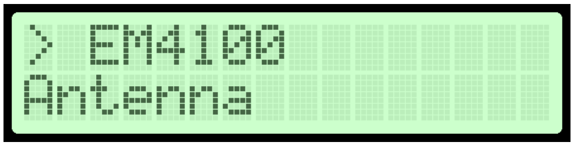
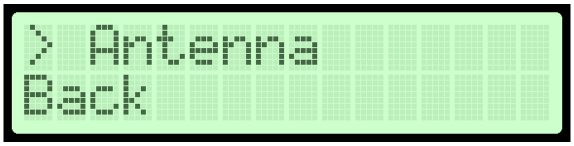
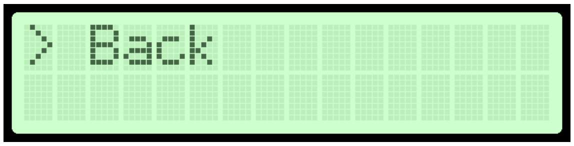
Menu Structure

Main Menu

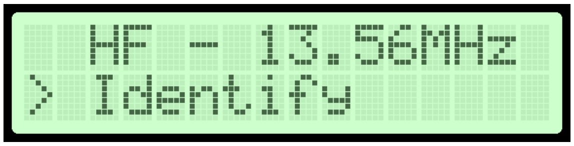
Menu Option	Description
 - Unchained - > LF 125/134kHz	Commands for tags in the Low Frequency (125/134kHz) spectrum. These would be HID 1326, EM4100, and T5577 tags.
 > HF 13.56MHz Load Tag	Commands for tags in the High Frequency (13.56MHz) spectrum. These would be Mifare Ultralight, 1K, and 4K tags.
 > Load Tag Backlight	Allows you to select from tags you have previously saved. Saved tags can be cloned or emulated. You must load tags first before doing either.
 > Backlight Device	The Backlight option allows you to turn on/off the backlight.
 > Device Exit!	Device give you further information about your device and does some functionality tests.

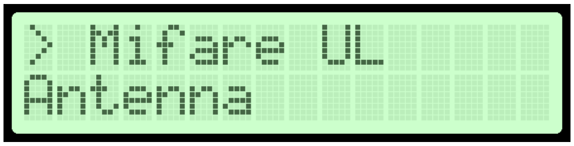
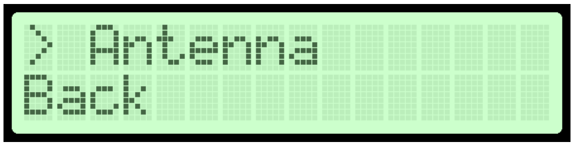
 > Exit!	Exit will leave unchained mode. This option allows communication with the USB port to be restored.

LF - 125/134kHz Menu

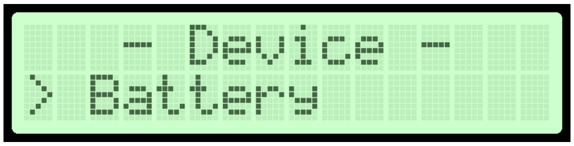
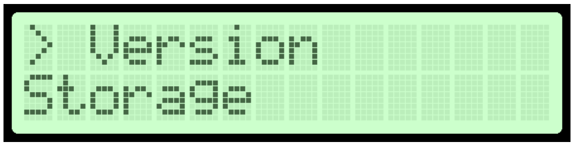
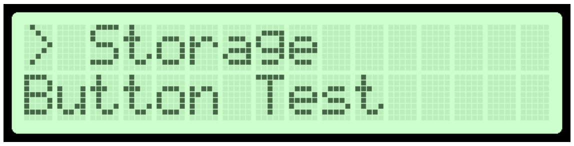
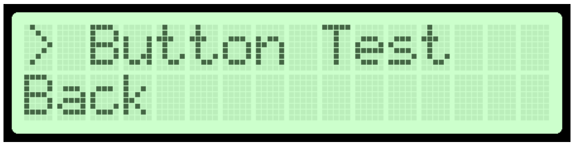
Menu Option	Description
 LF - 125/134kHz > Identify	The Identify command is used to determine an unknown LF tag.
 > HID EM4100	HID specific commands, such as Read, Save, Replay, Clone and Brute.
 > EM4100 Antenna	EM4100 specific commands, such as Read, Save, Replay, and Clone.
 > Antenna Back	Displays Antenna voltage at 125KHz and 134KHz in mV.
 > Back	Returns to previous menu. You will find this at the bottom of every menu structure.

HF - 13.56MHz

Menu Option	Description
 HF - 13.56MHz > Identify	The Identify command is used to determine an unknown LF tag.

 > Mifare UL Antenna	Mifare Ultralight specific commands, such as Read, Save, Replay, and Clone.
 > Antenna Back	Displays Antenna voltage at 13.56MHz in mV.

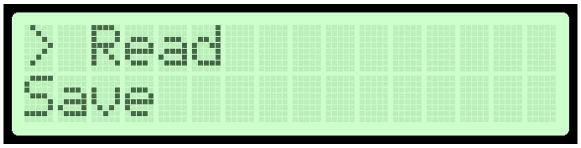
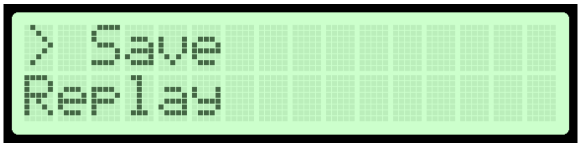
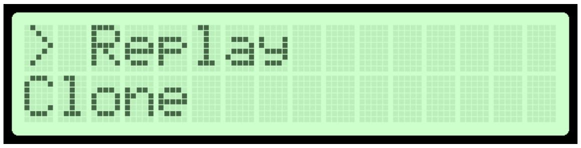
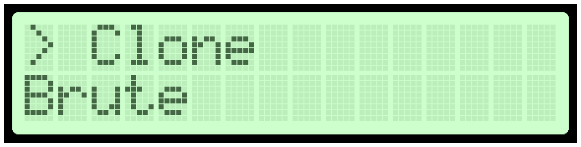
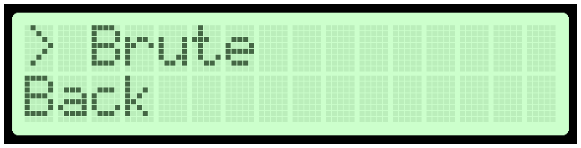
Device

Menu Option	Description
 - Device - > Battery	Displays battery charge percentage.
 > Version Storage	Displays firmware version information.
 > Storage Button Test	Displays SD Card available and total space.
 > Button Test Back	Test the buttons for functionality.

General Tag Operations

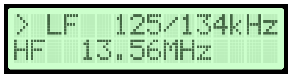
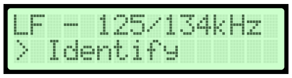
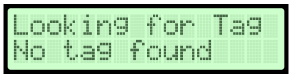
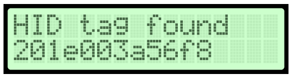
Each supported tag has a submenu located under the LF or HF menus. These menus will typically include **Read**, **Replay** and **Save** operations. Once a tag is read, it is saved in memory as the *current tag***.** At any time, the current tag can be replayed or saved using the menu. A saved tag can also be loaded from storage (SD Card) as the current tag.

General Tag Operations

Menu Option	Description
	Read a tag into memory and make it the *current tag*.
	Save the *current tag* onto the SD card. If there is no current tag, attempt to read the tag and save it. Saved tags will be stored under a directory bearing the name of the tag type (e.g. HID, EM4100). Filenames are automatically generated.
	Simulate the *current tag* for an external reader.
	Make a physical clone of the *current tag*. Before invoking, bring the physical target tag in-field of the antenna. For example, this function can be used to clone the *current tag* onto a T55x7 tag.
	Attempt to guess a valid tag by simulating some portion of the search space. This is only implemented for HID Tags.

Identifying a Tag

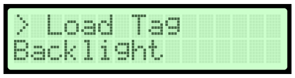
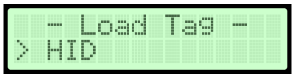
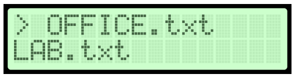
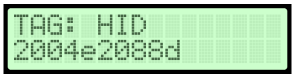
The ProxmarkPro is handy for quickly identifying an unknown tag. Before proceeding, ensure the appropriate antenna is connected.

 > LF 125/134kHz HF 13.56MHz	 LF - 125/134kHz > Identify	 Looking for Tag No tag found	 HID tag found 201e003a56f8
Scroll through the main menu and select LF or HF by pressing →	Press → to select **Identify**	The device is now searching for tags. Bring the tag toward the antenna and let the ProxmarkPro attempt to identify it.	If successful, you will see confirmation on-screen that a tag has been recognized.

Once a tag has been recognized, press → to jump to the corresponding submenu where various tag-specific operations can be performed.

Saving & Loading Tags

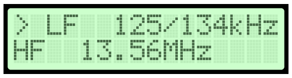
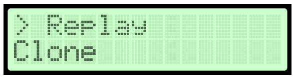
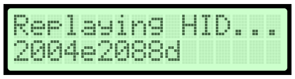
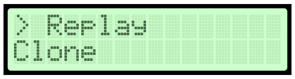
The SD card used to store tags must be formatted with the FAT file system. Note that long file names are not supported. The ProxmarkPro will store tags under directories corresponding to the type of tag (e.g. HID, EM4100). When a tag is saved it is automatically named according to the format TAG*N*.txt. Where *N* is a serial number.

 > Load Tag Backlight	 - Load Tag - > HID	 > OFFICE.txt LAB.txt	 TAG: HID 2004e2088d
Select Load Tag by pressing →	Navigate to the tag type and press →	Select the desired tag by pressing →	Note the on-screen confirmation that the tag has loaded successfully. This is now the current tag. Press → to access the corresponding tag menu.

Stored tags can be renamed by ejecting the SD card, inserting it into a PC, browsing the card and renaming the target file to something more memorable.

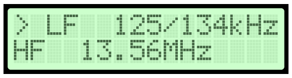
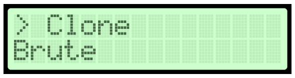
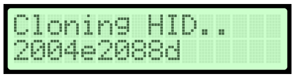
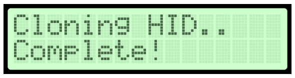
Replaying a Tag

With a tag loaded you can now simulate the *current tag* for an external reader.

 > LF 125/134kHz HF 13.56MHz	 > Replay Clone	 Replaying HID... 2004e2088d	 > Replay Clone
Scroll through the main menu and select LF or HF by pressing →	Press → to select **Replay**	Your Tag will now replay until stopped.	Press the ← to stop replaying. This will take you back to the previous menu.

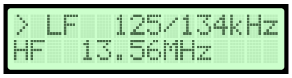
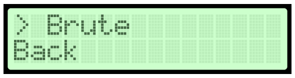
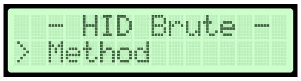
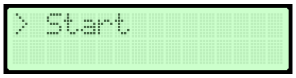
Cloning a Tag

With a tag loaded you can now make a physical clone of the *current tag to a T55x7*.

 > LF 125/134kHz HF 13.56MHz	 > Clone Brute	 Cloning HID.. 2004e2088d	 Cloning HID.. Complete!
Scroll through the main menu and select LF or HF by pressing →	Press → to select **Clone.** Make sure your T55x7 tag is in field.	Cloning will start, if you are given a "Failed!" try again with the T55x7 tag more in field.	Your cloning should now be complete. Check your tag copied correctly by trying to read it.

Brute

Attempt to guess a valid HID tag by simulating some portion of the search space.

 > LF 125/134kHz HF 13.56MHz	 > Brute Back	 - HID Brute - > Method	 > Start
Scroll through the main menu and select LF by pressing →	Press → to select **Brute.**	Configure your Brute by changing the Method, Format, Facility Code, Card Number, Duration, and Delay.	When done configuring click **Start**.