FROM: tom@tomthepi.com
TO: <redacted>
DATE: February 26, 2025
RE: Proxmark 3 In Lab

I've found a "Proxmark3 Easy". This version has 512 kB of flash memory, so I would suggest using the "iceman" repository:

https://github.com/RfidResearchGroup/proxmark3

On Windows, you can download a prebuilt version from the following URL: https://www.proxmarkbuilds.org/latest/rrg_other . It will be in 7z archive mode – you might want a .zip instead, so I've uploaded a copy to our shared space as well (see my email attachment zone).

As a quick guide, here is what *I* was told to do to get started:

The reader is attached to the desk in the shared lab, with enough room now to place the card on it (see photos below). If you want to get your own Proxmark3 you could use other modes (emulation mode), this shared one can only be used for reading or writing cards.

The USB cable is the one on the "end", because the connector can be fragile I've screwed the cable down. Ignore the other USB connector:
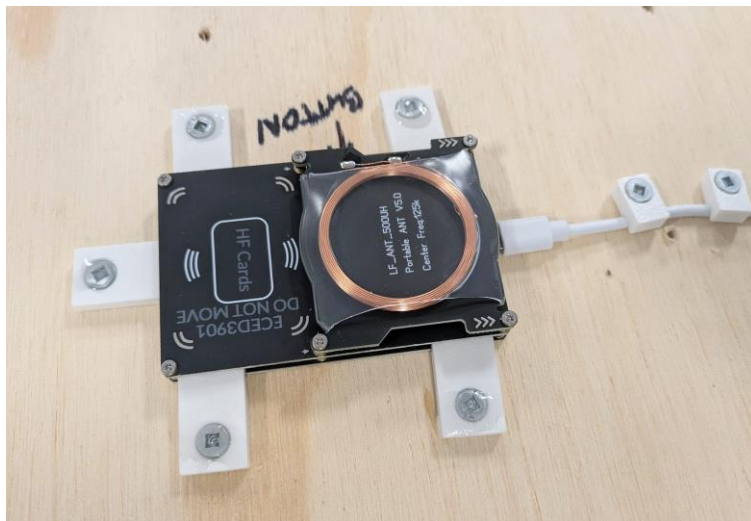

After plugging in, you should see a serial port, for example on Windows in the device manager:
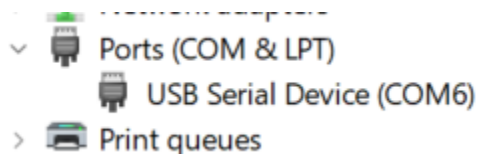
If you unplug it, the serial port should disappear. If this happens it is good news for you! If you don't have a driver, you may need to install the driver from the Windows installer.

To run proxmark3 on Windows, extract the .zip file (do NOT just "open" the zipfile). Then run the pm3.bat script by double-clicking on it:
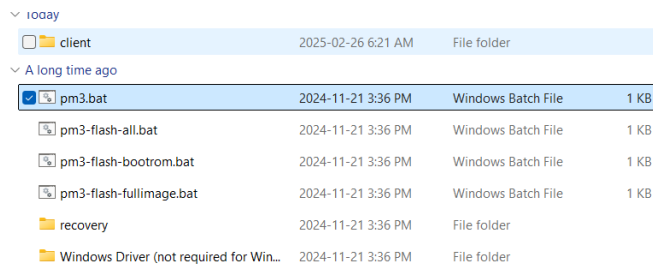
From there – you should see the promark3 detected. You'll see a similar result running the utility on Windows, Mac, or Linux if you run the 'pm3' command. On the other platforms you may need to build it from source:

```
  [ Proxmark3 RFID instrument ]

    MCU....... AT91SAM7S512 Rev A
    Memory.... 512 KB ( 65% used )

    Client.... Iceman/master/v4.18994-552-g325376d7e 2024-11-21 20:36:26
    Bootrom... Iceman/master/v4.18994-552-g325376d7e-suspect 2024-11-21 20:35:52
    OS........ Iceman/master/v4.18994-552-g325376d7e-suspect 2024-11-21 20:36:00
    Target.... PM3 GENERIC


[usb] pm3 --> |
```

You may get a warning about "firmware mismatch" if building your own version of Proxmark like this:
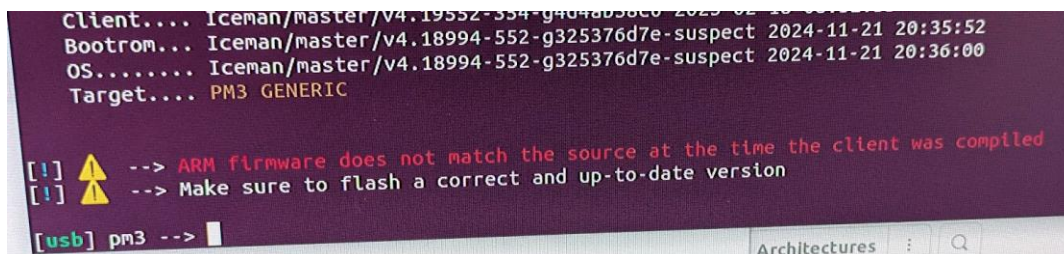
Try using it as it would be *better not to reflash (this can brick it)*. Building a <u>new</u> version of Proxmark3 from the "iceman" repo (https://github.com/RfidResearchGroup/proxmark3) seems to work for the commands we need. Using older prebuilt Proxmark3 utilities might not work.

If someone else has reflashed it, you can run the "`pm3-flash-all`" command – on the Windows installer there is a `pm3-flash-all.bat` that should work. This command reloads the firmware so it exactly matches the utility version.

From here you are on your own – I don't know much about using this thing! But I did test that you can find a high frequency tag by putting it on the "lower" side like this:

And running:

hf search

inside the pm3 utility should yield a hit like:


```
[usb] pm3 --> hf search
[-] Searching for ISO14443-A tag...
[=] ---------- ISO14443-A Information ----------
[+]  UID: 8D 6D 30 03   ( ONUID, re-used )
[+] ATQA: 00 04
[+]  SAK: 08 [2]
[+] Possible types:
[+]    MIFARE Classic 1K
[=] proprietary non iso14443-4 card found, RATS not supported
[=]

[+] Magic capabilities... Gen 1a
[#] Static nonce......... 009080a2
[+] Static nonce......... yes

[?] Hint: use `hf mf c*` magic commands
[?] Hint: try `hf mf` commands


[+] Valid ISO 14443-A tag found
```

And a low-frequency tag OR card on the "upper" side like this:
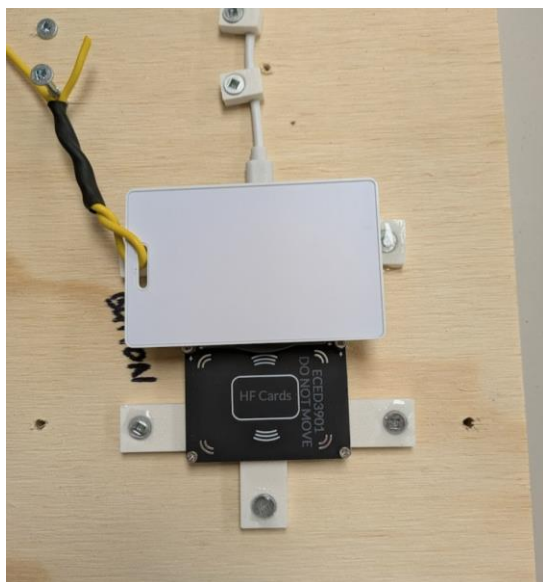
And running:

lf search

Should also yield some information.

Be aware that cards & tags can both be HF or LF! That "clone" card I left for you before might yield some information about what you need to clone it – after all that "clone" card I left you was one someone programmed, maybe you can find the chip & order it?

You may need to hold things at angles as well – especially with the HF antenna, there is some metal (screws) around it. Most tap credit cards are HF cards for example, but I needed to hold one at a slight angle like this:

Best of luck – I can't provide much more help, but hopefully you can find the resources you need. Don't do anything I wouldn't do with the reader!

--

Tom Mumford
Private Eye for Hire (Not licensed in Quebec)

ATTACHMENT 1 / 1 [proxmark3_rrg_other_fromtom.zip]: Uploaded to Brightspace