# PM3 MAX

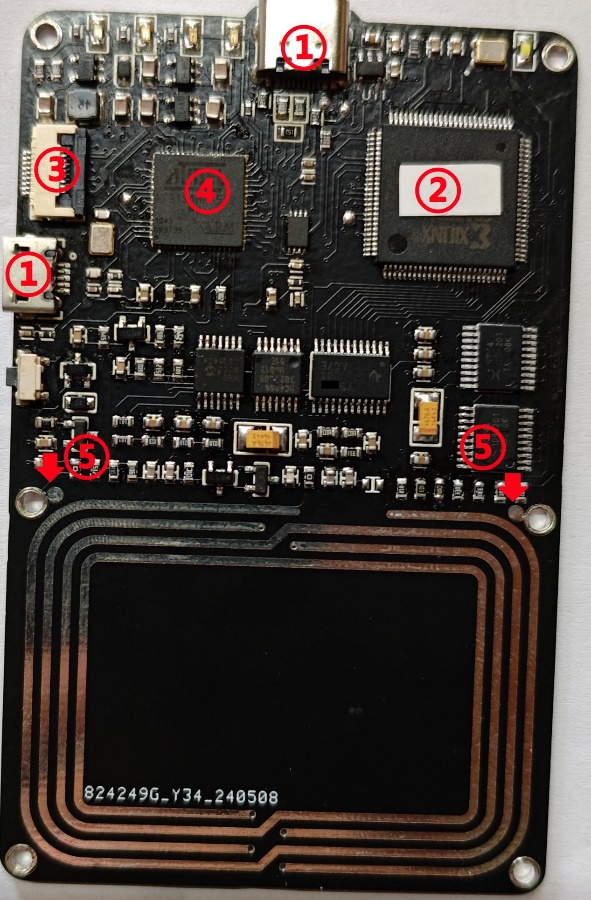
# Product features

1. Comes with two fully functional USB ports. Both the TYPE-C and MICRO ports can be connected to a computer.
2. A brand new chip model, although it cannot flash RDv4 firmware, it can flash Iceman firmware with consistent functionality.
3. FPC connector with 9-pin, supports modification of Bluetooth module, extended USB interface, SAM card module, etc.
4. 512KB memory, all functions are retained without deletion.
5. Reserve low-frequency coil solder joints for easy modification by users.
6. There are 4 solder joints on the back, which can switch between card reading mode and sniffing mode. When disconnected, it is card reading mode, stable card reading, and moderate sniffing. When short circuiting (using materials such as soldering iron, wire, conductive tape, etc.), switching the sniffing mode greatly improves the sniffing ability, and the distance is even slightly farther than RDV4.
7. The low-frequency antenna is processed with PCB hollowing out and supports multiple installation methods, making it an added advantage in some low-frequency sniffing situations. For example, hitag2 (PCF9736...)
8. Offline sniffing mode, can sniff without an app. Just power up the product and press and hold the three second button to enter the sniffing mode (green light on). At this time, card sniffing can be performed. After sniffing, the log will be stored inside the chip and can be extracted from the computer GUI. It also supports offline continuous sniffing, and the log will be added on its own. Theoretically, it can support up to 50 sniffing attempts.
9. With the offline password storage feature, frequently used passwords can be saved inside the chip via the GUI. Even after changing computers, these passwords can still be retrieved through the GUI. This offers a convenient way to store passwords without the need for an internet connection. In theory, up to1000+ passwords can be stored offline.
10. Equipped with free computer GUI software and English APP. The APP supports both OTG and Bluetooth connection.When using the computer GUI, it is necessary to flash the PC firmware，When using the APP, it is necessary to flash the APP firmware
11. Continuously updated, with features consistent with the official Iceman. If you need to flash other firmware, please add the parameter=PM3ICOPYX during compilation
12. https://github.com/rfidreadermaker/proxmark3-max

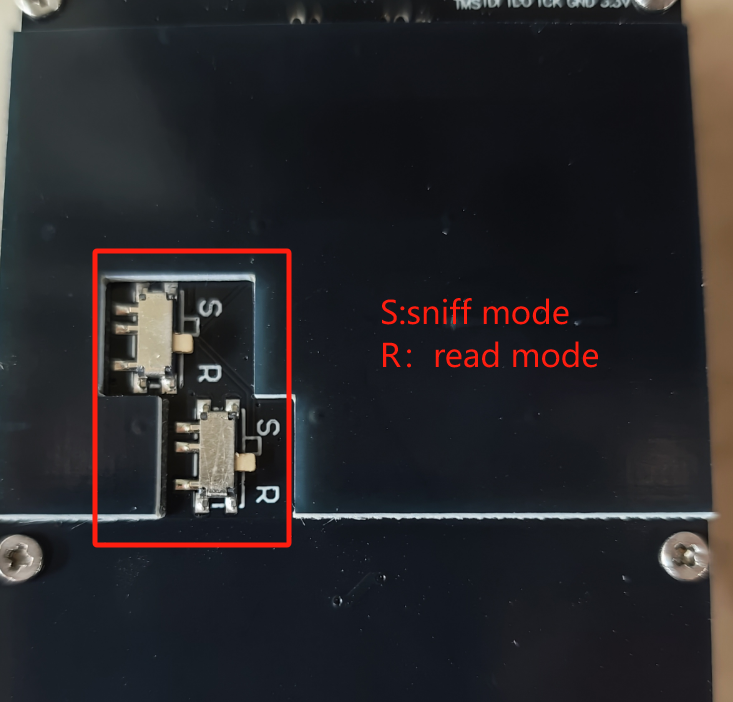
You can use PM3's advanced compilation parameters to compile the MAX firmware.

# Product images

## 1. Front view



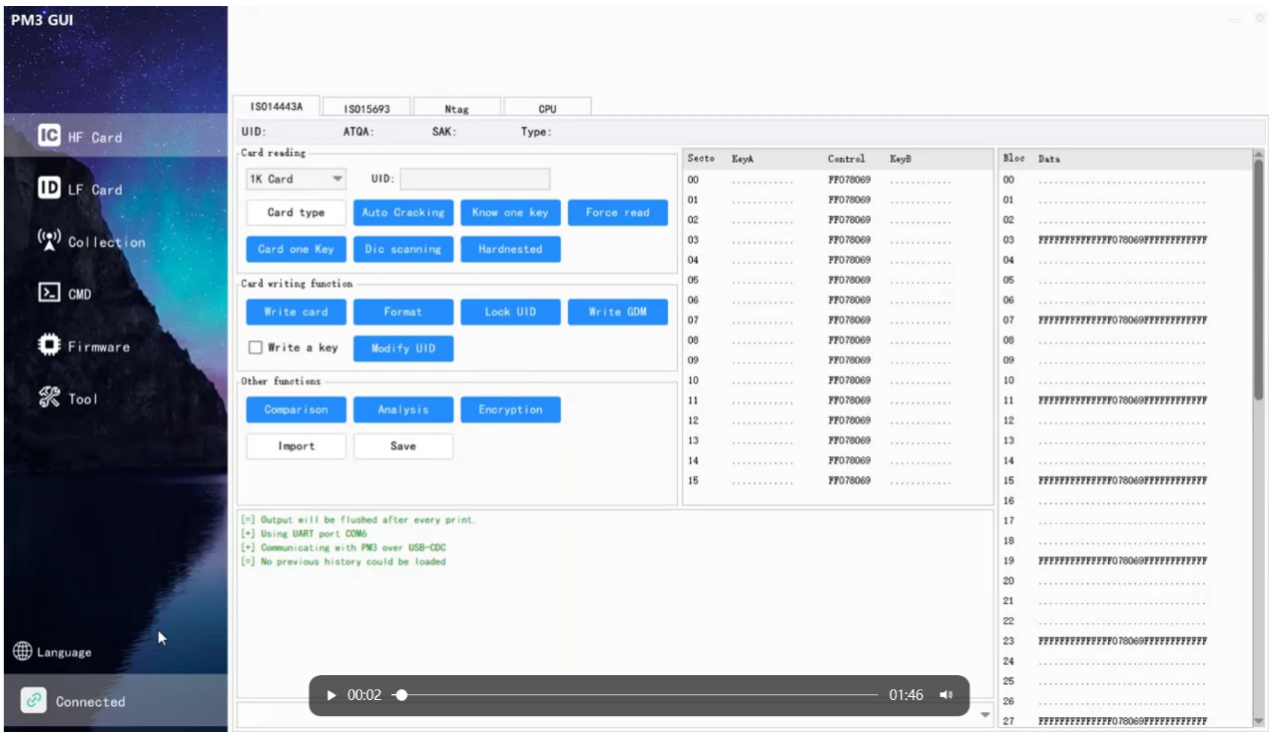
## 2. Back view



## Low frequency antenna hollowing treatment and various installation methods

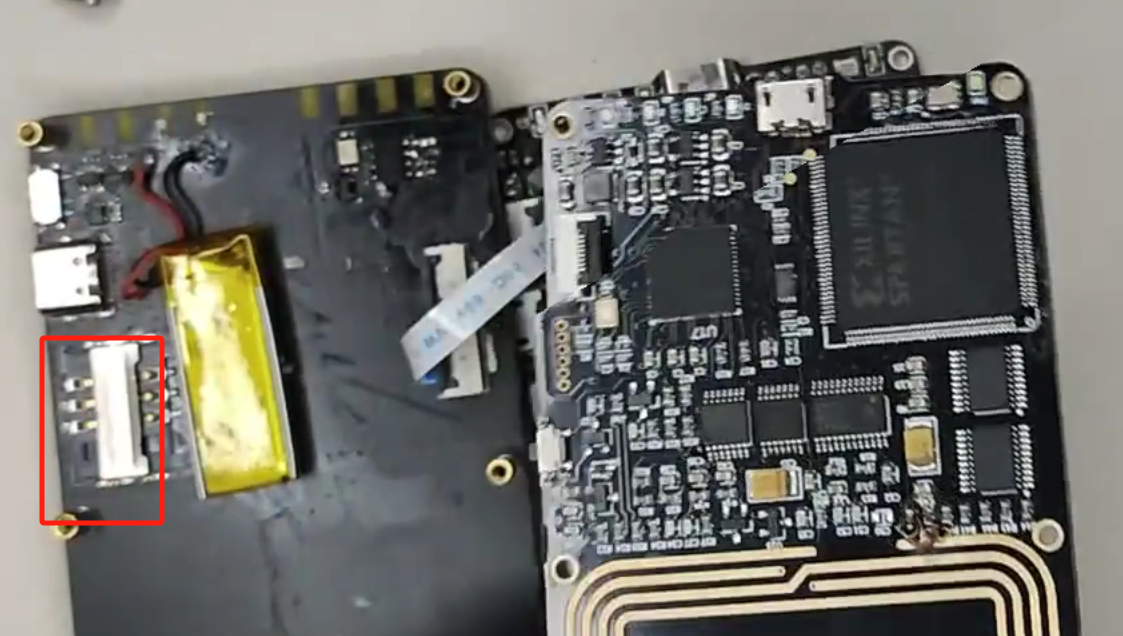


3.Free computer GUI and APP

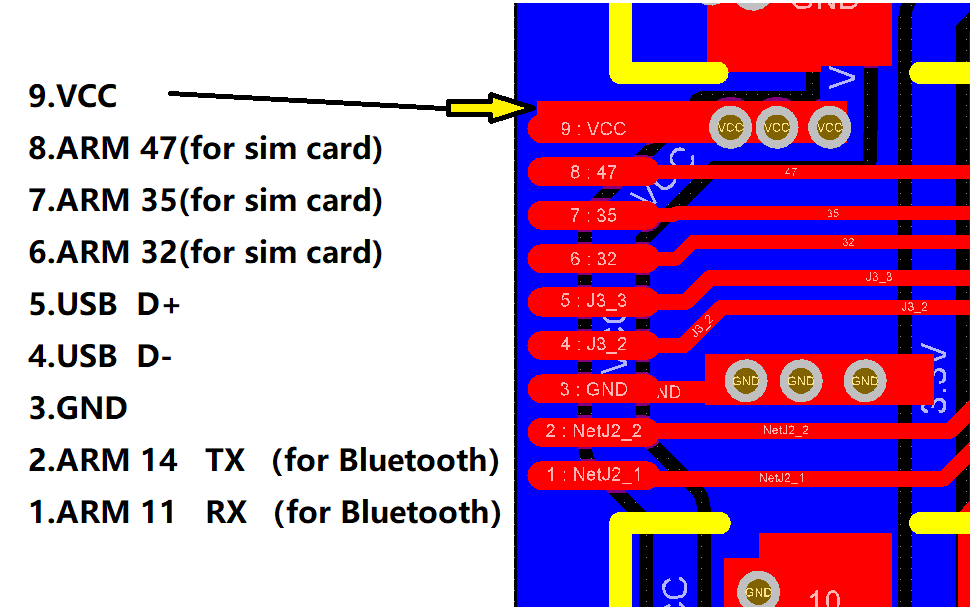




## 4. Bluetooth module modification

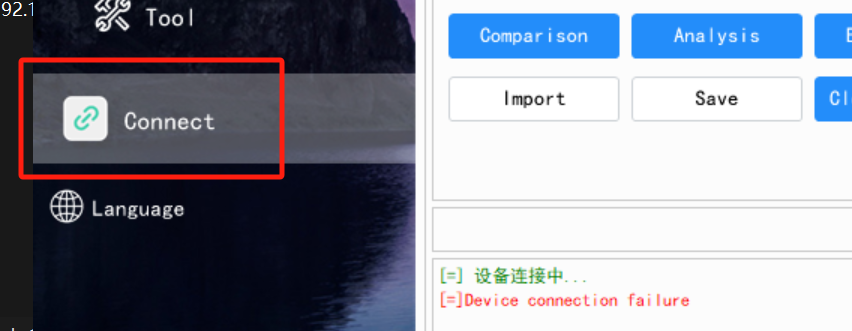


## 5. FPC connector -9PIN



1. Introduction to Computer Software

When you open the GUI, the software will automatically connect to the device.

If the device fails to connect, please check the following possible causes:

① ​​Check if the computer detects the PM3 port​​:

​​Windows 10/11​​: No driver required—the PM3 port should appear as ​​"USB Serial Device"​​.

​​Windows 7​​: Requires manual installation of the PM3 driver (installation method is the same as other PM3 devices and is omitted here).

​​If the port does not appear despite proper connection​​, verify:

Device connection status

USB cable integrity

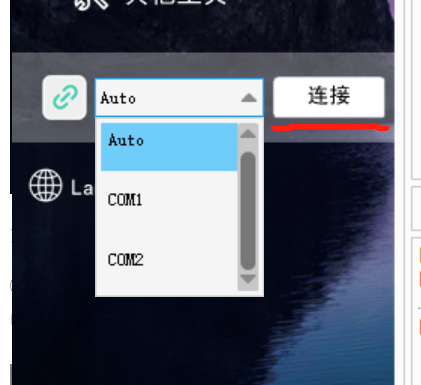
Computer USB port functionality

Device interface condition



② ​​Check if the system supports automatic port selection​​:

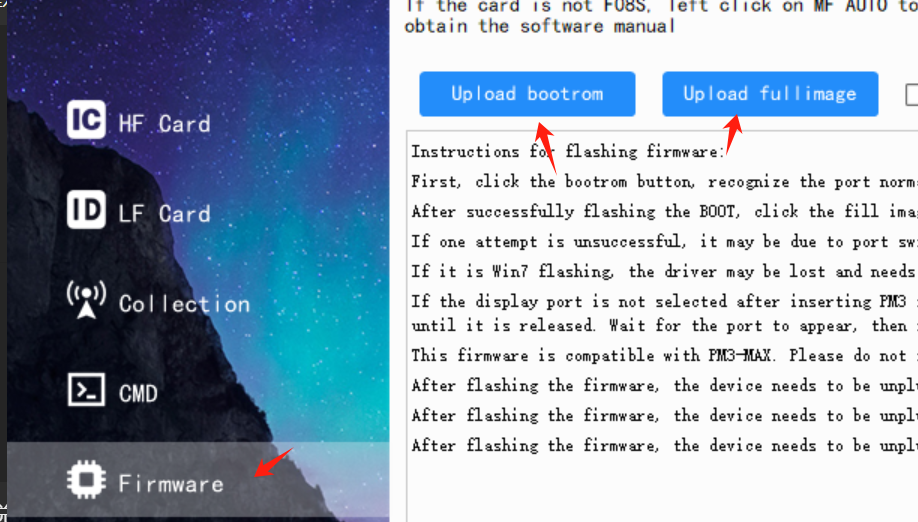
Some systems (e.g., Windows 11) may not support automatic connection.

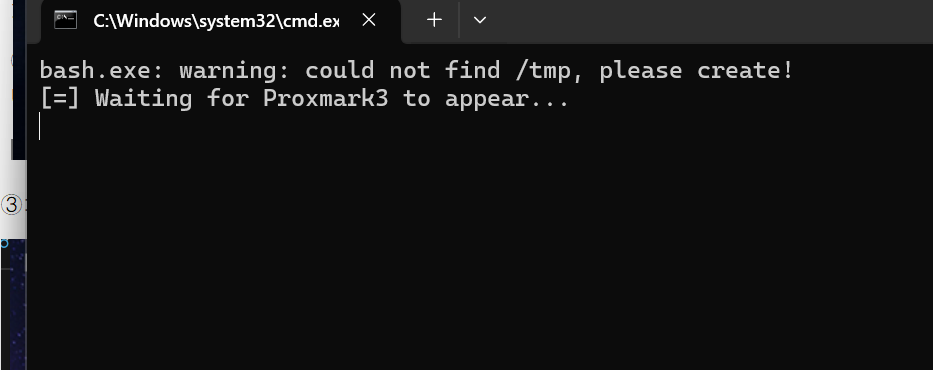
Solution​​: Click the ​​"Connect Device"​​ area and manually select the corresponding port.

③ ​​Verify firmware compatibility​​:

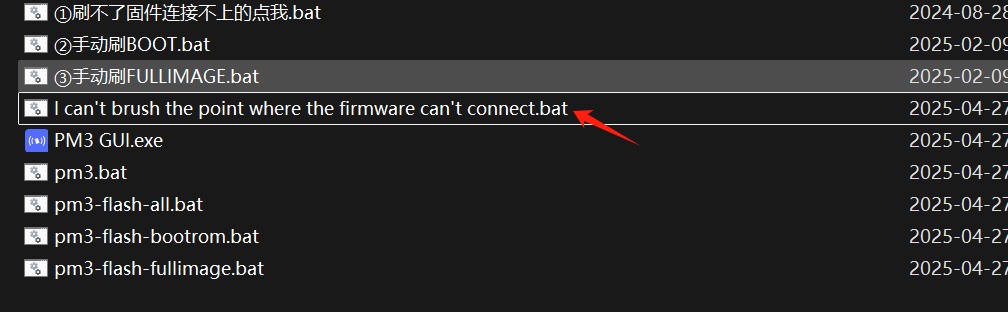
If the firmware is incompatible, flashing new firmware is required.

Important: Only PM3-MAX devices are compatible with this software's firmware.



Click ​​"Firmware"​​, then select ​​"Flash Bootrom"​​. If the following screen appears, your computer system does not support automatic port selection.

If the above situation occurs, please close the software and run the batch file ​​"①I can't brush the point where the firmware can't connect.bat"​​ located in the root directory. This batch process will copy the necessary installation environment.



After running the batch file, you may attempt to flash the firmware using ​​"pm3-flash-all.bat"​​. If the connection still fails:

Close all open windows

Manually execute the following batch files:

​​②Manual\_Bootrom\_Flash.bat​​

​​③Manual\_Fullimage\_Flash.bat​​

When prompted:

Enter the correct COM port number (visible in Device Manager)

Press ​​Enter​​ to begin flashing

​​Important Notes:​​

The COM port may change during flashing - monitor Device Manager

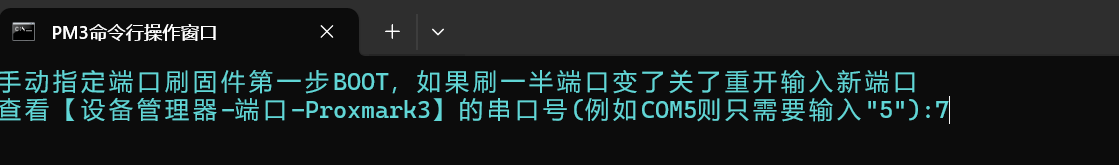
If the port changes:

Close current window

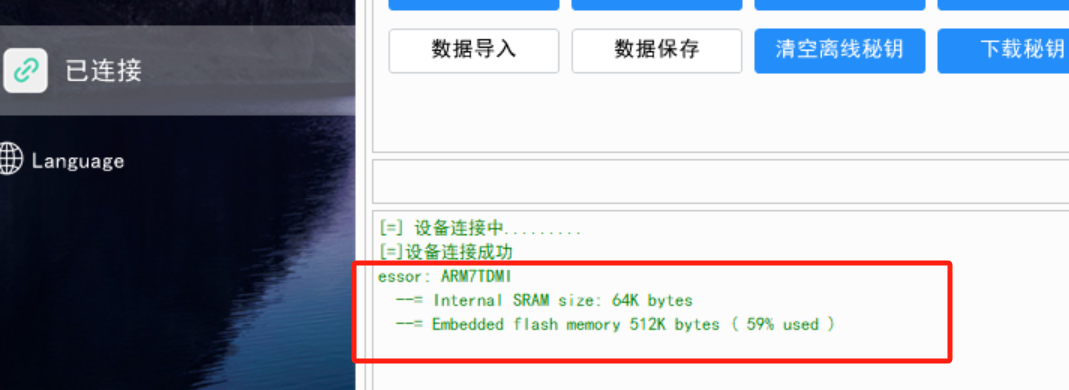
Restart the process with the new port number

Ensure stable USB connection throughout the process



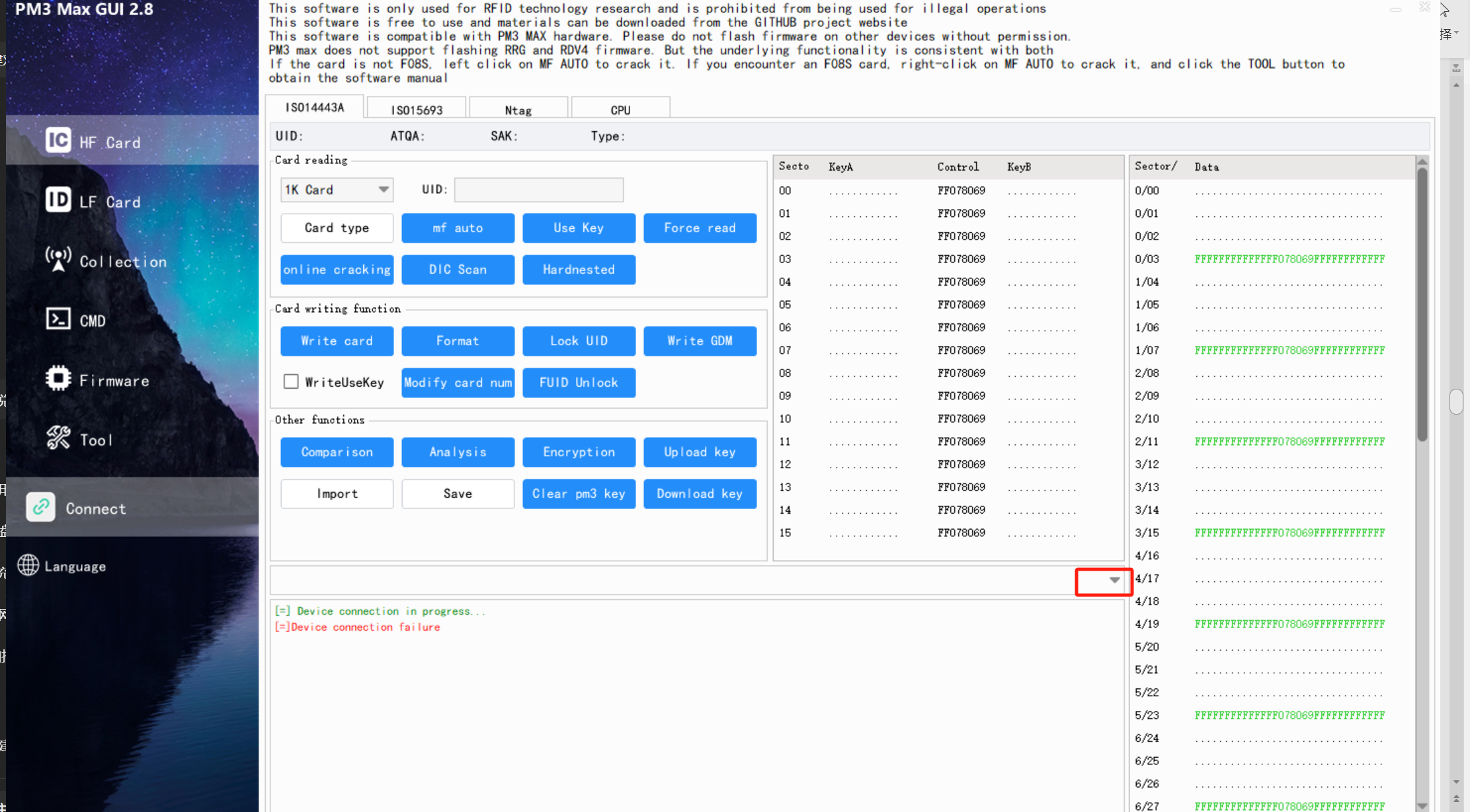




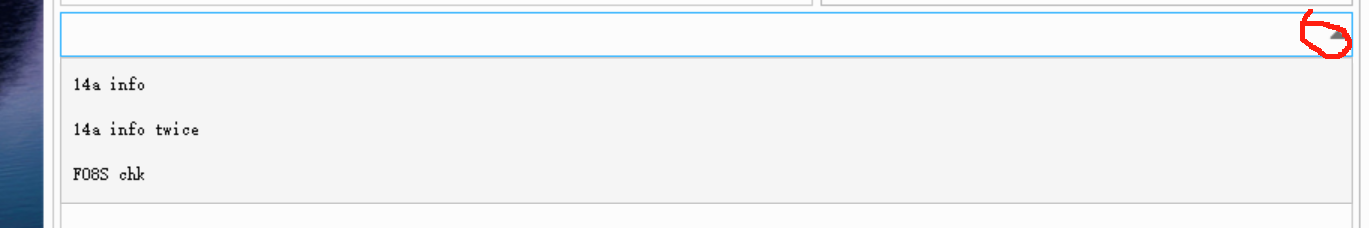
For any special issues, please discuss in the community forums. **After successful flashing, reconnect the device by unplugging and replugging it.**

The interface shown above indicates successful firmware matching and connection. If you see messages like ​​"ASM"​​, this means the firmware is incompatible and needs to be reflashed.

Interface Guide​​



Click the ​​Quick Command Arrow​​ to expand custom shortcuts. These shortcuts can be added/modified based on your operational needs.





1) PC Software Usage​​

1.1 High-Frequency Cards (1443A)​​

① Read Card Type​​

Function​​: Automatically detects and displays:Card Number (UID)\SAK (Select Acknowledge)\Card Type​​

Additional Info (if applicable)​​:

Special tags like ​​CUID/UID/GDM/CPU/QL88​​ will be flagged.

​​Workflow​​:

Place the card near the PM3-MAX antenna.

Click ​​"Read Card Type"​​ in the GUI.

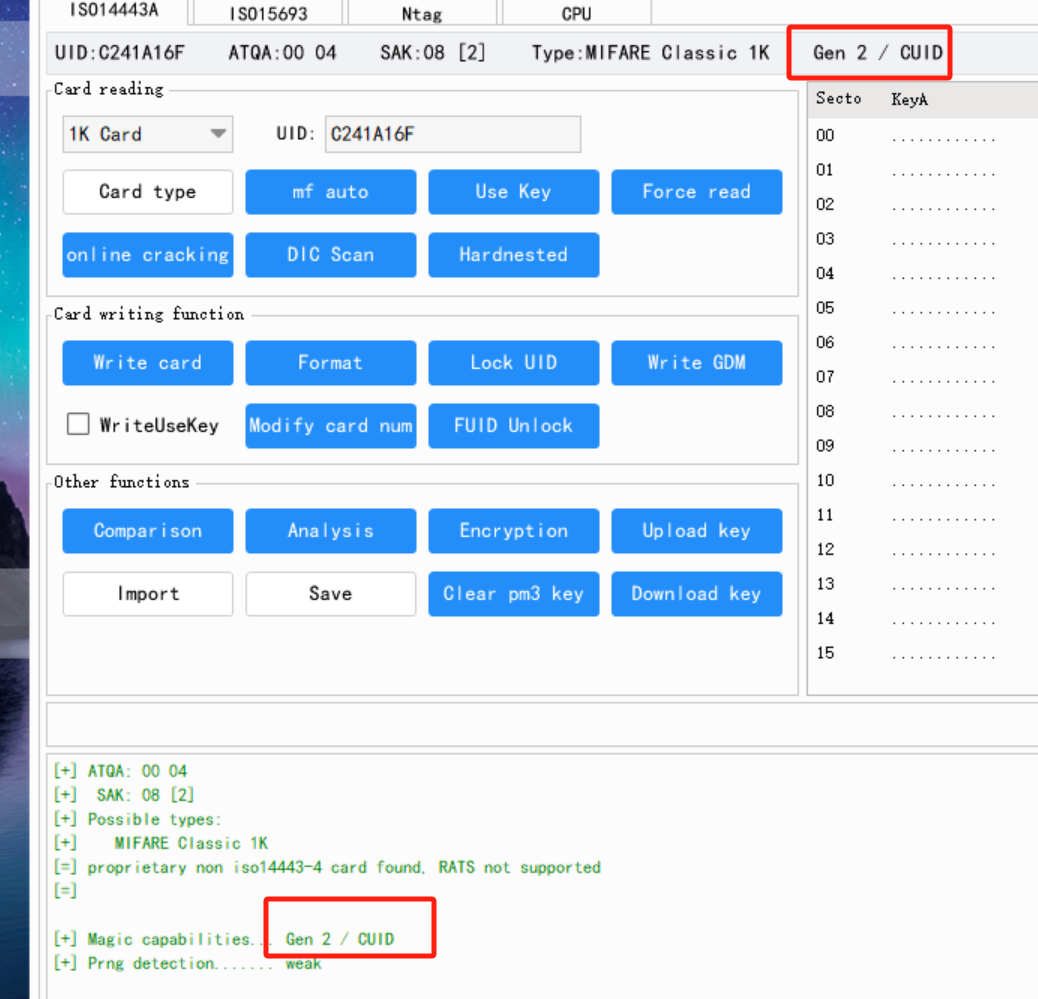
Review the displayed data for further operations.

​​Notes​​:

For ​​cloneable cards (CUID/UID)​​, proceed to "Write" functions.

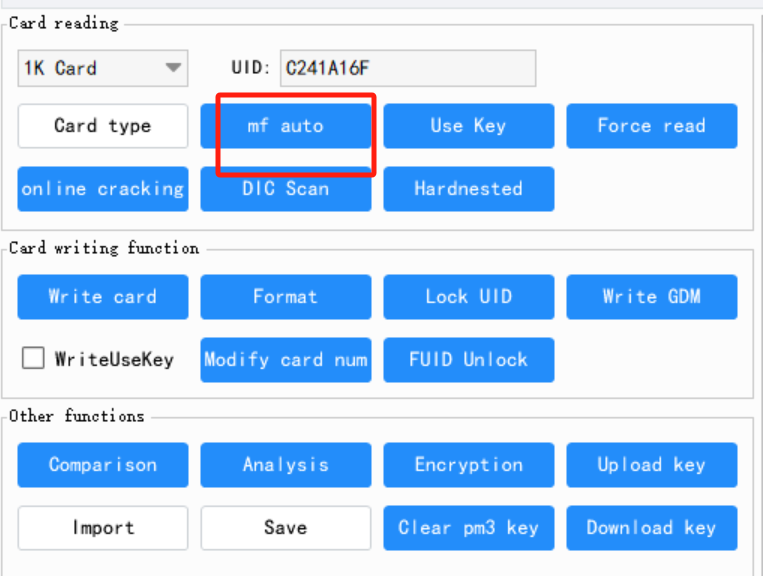
​​GDM/CPU cards​​ may require advanced cracking (see Auto-Crack section).

​​QL88​​ indicates a specific Chinese magic card variant.



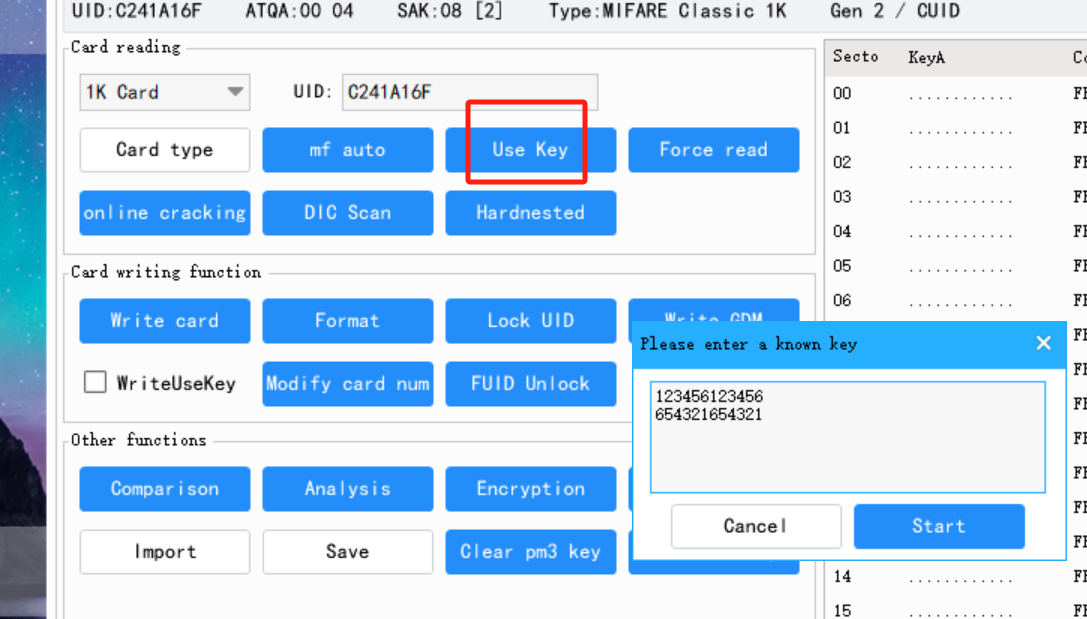
​​② High-Frequency Card Data Cracking​​

Left-click the ​​"Auto Crack"​​ button, and the device will automatically crack the data. Upon successful cracking, both the password field and data field will be populated. The cracking process may take anywhere from a few seconds to several dozen minutes (for ​​Hard​​-type cards, cracking speed depends on your computer's performance).



If cracking is interrupted, the following issues may occur:

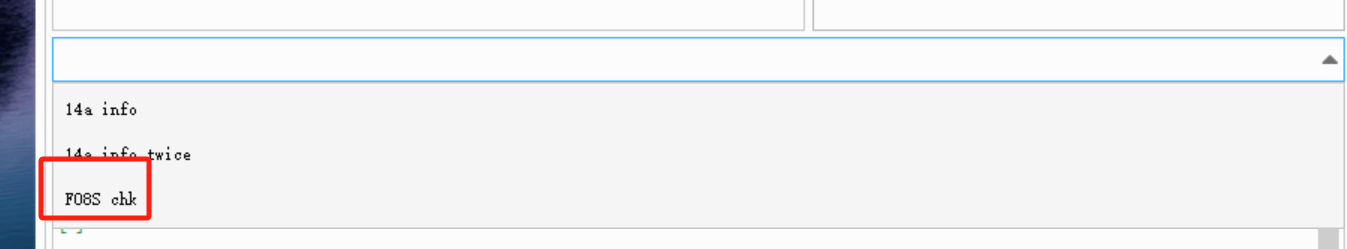
Fully encrypted non-vulnerable Gen1/Gen2 cards: You can use the "online craching" button to try cracking. If cracking fails, sniff the password first and then use the "USE key" function by entering the password to crack. If there are multiple passwords, separate them with the Enter key.



For third-generation non-vulnerable card types:

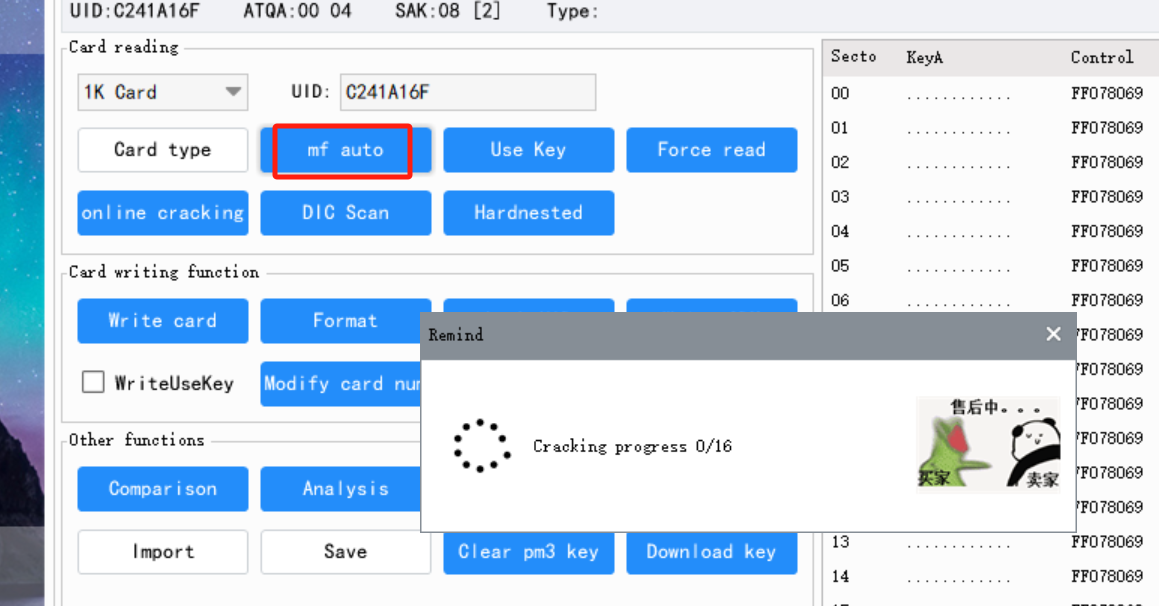
This type of card requires right-clicking the "mf Auto " button to crack.

You can use the quick command "F08S chk" function - "F08S" indicates a third-generation non-vulnerable card.

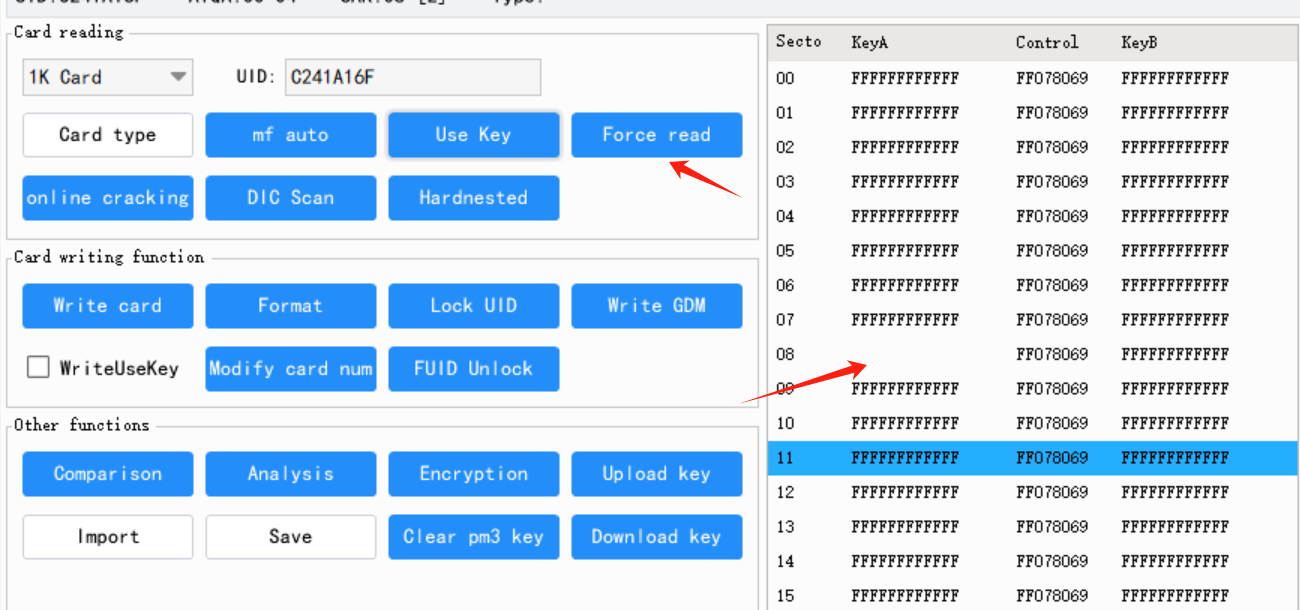


③F08S：

Right-click the ​​"MF Auto"​​ button, and the device will execute the ​​third-generation non-vulnerable card cracking​​.。



Right-click ​​"Force Read"​​, and the software will exploit vulnerabilities to read data from third-generation non-vulnerable cards ​​without requiring passwords​​.



Right-click the blank password field and select ​​"Single Sector Crack"​​ to decrypt the password of a specified sector on F08S cards.



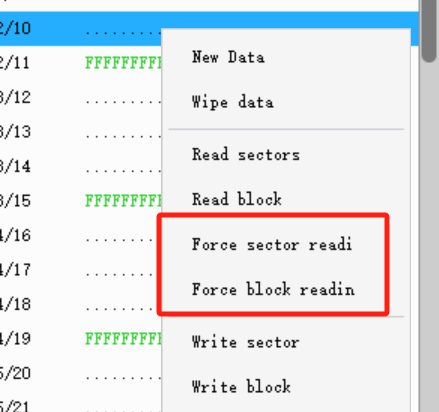
Left-click​​ any data block to highlight it (the block will change color), then ​​right-click​​ to select:

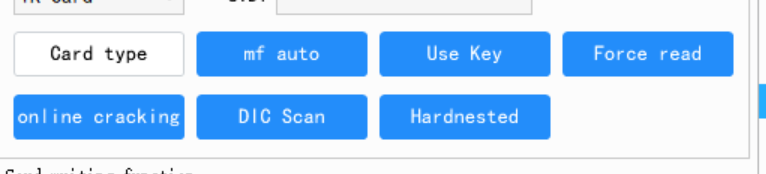
​​"Force Read Sector Data"​​ (for third-generation non-vulnerable cards)

​​"Force Read Block Data"​​

​​Purpose​​:

This function is primarily used to ​​recover missing data​​ when the card signal is weak or unstable.





USE KEY: Know certain passwords and use them to crack the card. Separate multiple passwords with Enter.

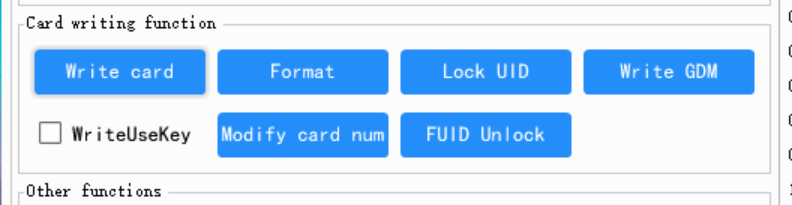
Force read: When left-clicked, forcibly read card data using the password in the password field. When right-clicked, forcibly read card data (excluding passwords) using the backdoor of third-generation non-vulnerable cards.

Online cracking: Use the card to calculate passwords and attempt to crack cards encrypted by some Chinese suppliers with these passwords.

Dic scan: Scan the specified .dic dictionary.

Hardnested: Manually input information to crack Hard-type cards.

WRITE CARD



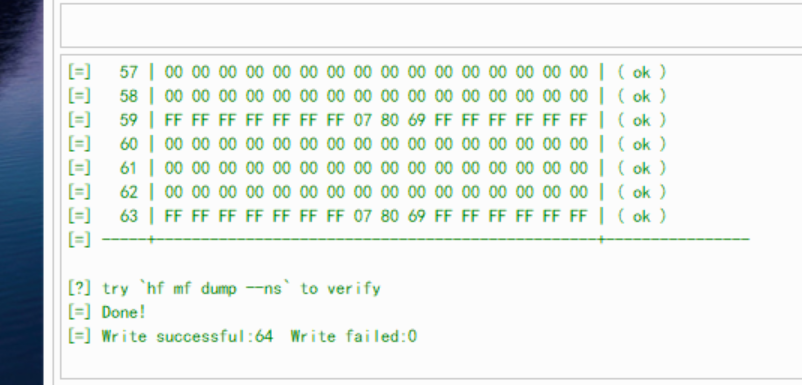
WRITE CARD:​​ When the data field contains correct data, click this button and the device will automatically determine the card type (UID/CUID) and write to the card (if using CUID or authorized cards, the card must be blank). After writing, the success/failure count will be displayed.

Note:​​

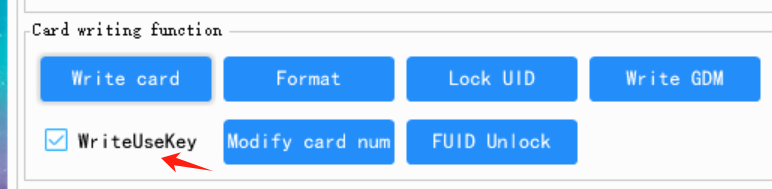
If writing with an ​​authorized card​​, the error count will always be ​​at least 1​​.

For ​​non-blank cards​​, enable the "Write use key" option – the software will use passwords from the password field to write data.

Drag and drop password files into the password field to import keys.



If some sectors fail to write, you can left-click any block in the failed sector in the data area, then right-click and choose to write the sector or block. Please use the "Write use key" option flexibly (do not check it if the sector password failed to write, but check it if the password was written successfully while the data failed).



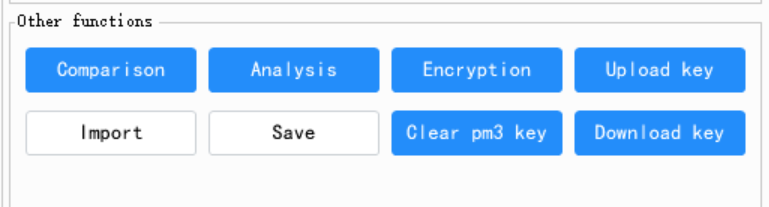
Format:​​ Formats the card data to a blank state. Requires the password in the password field to match the card's current password.

​​Lock UID:​​ After writing to a UFUID card, click this function to permanently lock the UFUID card number.

​​Write GDM:​​ When writing data, use this option if writing to a GDM card.

​​UID Modify:​​ Only modifies the card's UID. Can also repair certain firewall-damaged cards during modification.

​​FUID Unlock:​​ Unlocks an FUID card. Requires the FUID to be of an unlockable type (currently, there are two types—one can be unlocked and reused).



​​Data Comparison:​​ Import two sets of data to compare differences.

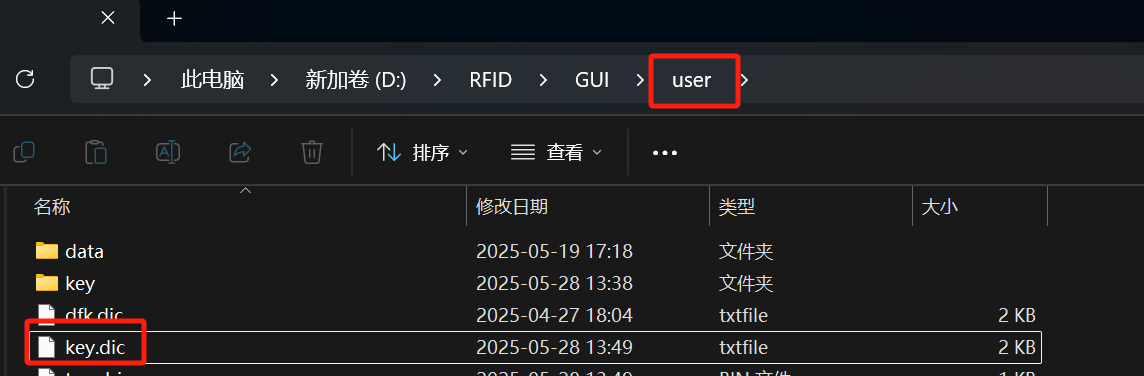
​​Data Analysis:​​ Analyze data systems, timestamps, etc. For certain systems, double-click the timestamp to modify it. After modification, writing the data can achieve timestamp extension. If the timestamp cannot be modified, the software does not support extension for that system.

​​One-Click Encryption:​​ Fully encrypts the data in the data area.

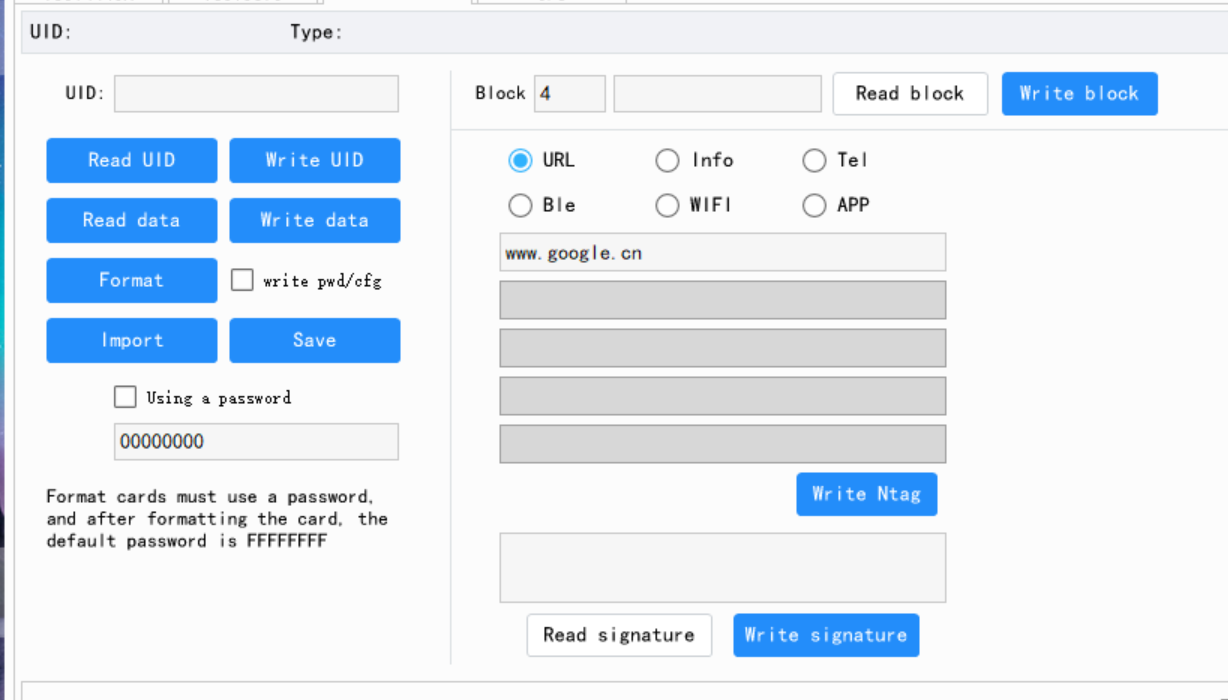
​​Upload Keys / Download Keys:​​

​​Upload:​​ Saves .DIC files to the device's internal storage for password backup.

​​Download:​​ Enables dictionary scan functionality. Downloaded keys are saved in the ​​key.dic​​ file.



NTAG-CARD



① Click ​​"Read Data"​​, and the software will read all data from the card. If the card is password-protected, first check ​​"Use Password"​​ and enter the correct password before reading.

When writing to a card, click ​​"Write Data"​​. If ​​"Write Password Configuration"​​ is checked, the software will write the password to the new card as well.

​​Note:​​ When writing to a password-protected card, check ​​"Use Password"​​ and enter the correct password.

② ​​Tag Writing Function​​

The software supports writing URLs, business cards, phone numbers, and other information.

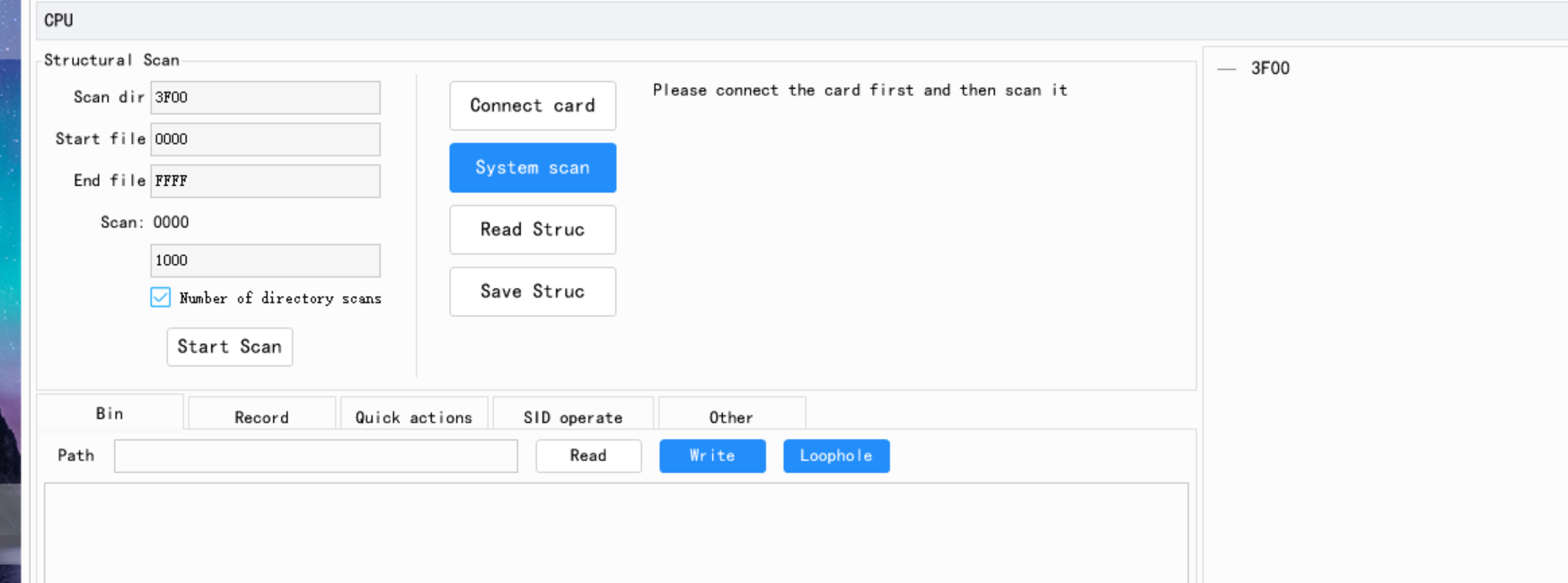
③ ​​Modify Signature​​

Use the ​​"Read Signature"​​ and ​​"Write Signature"​​ buttons to modify the ​​SIG signature​​ of cloned cards.

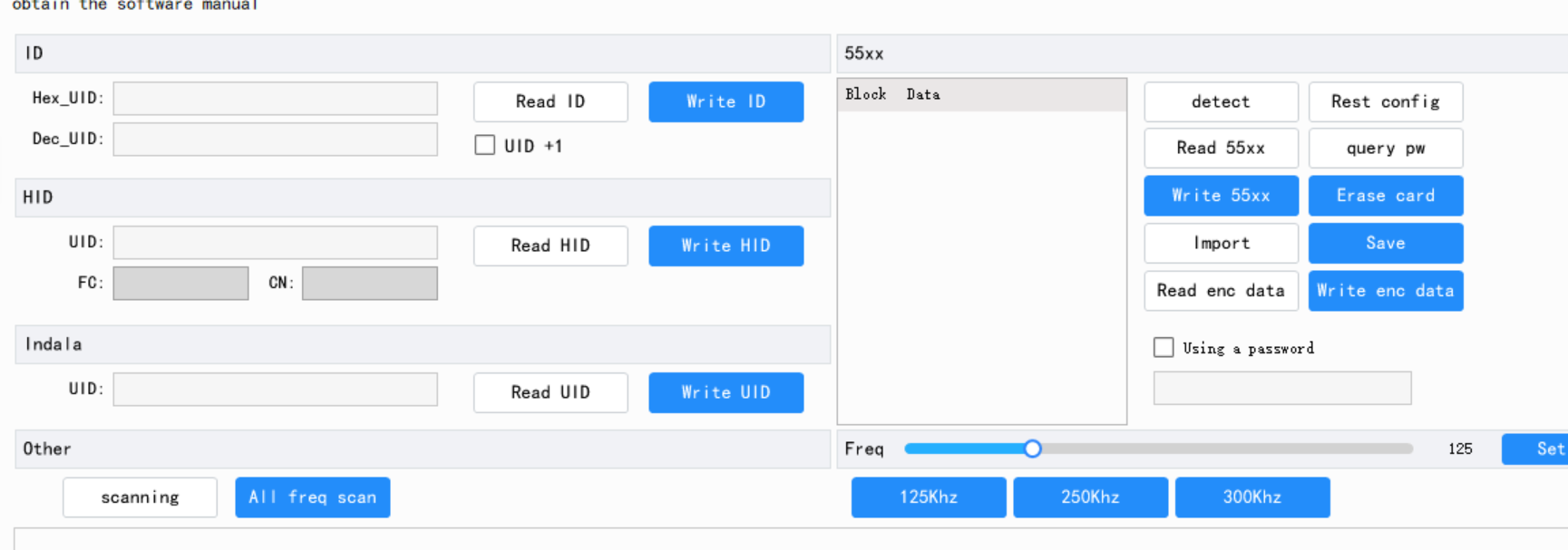
​​CPU Cards​​

The software supports reading, writing, and cloning ​​1208-09/1208-10 chip cards​​, and allows custom directory/file creation for ​​1208, TID, BOMB, and SID cards​​.

Note: This feature is complex—please refer to community tutorial videos for guidance.



LF-CARD



①: ​​UID+1​​ means the card number automatically increments by 1 during writing.

②: ​​ID card writing​​ supports ​​5200/5577/8268/8310/8211​​. For cards starting with ​​8​​, you may need to adjust the card placement to successfully write.

③: ​​Frequency adjustment​​ allows tuning the low-frequency coil frequency.

④: ​​55xx functions​​

​​Password query​​: Attempts to crack ​​5577​​ using dictionary passwords.

​​Card erase​​: Formats ​​5577​​.

​​Read encrypted card data​​: Reads ​​5577​​ data (excluding passwords). After reading, click ​​"Write encrypted card data"​​ to clone the card.

Note: This function ​​does not use or write 5577 passwords​​, commonly used for cloning encrypted ​​5577​​ cards.

COLLECTION



​​Card Sniffing:​​

After enabling, the device's green light turns on. First, place the device (orange light turns on), then swipe the card (blue light flashes), indicating successful sniffing. If the blue or orange light doesn't turn on, switch to sniffing mode using the toggle switch on the back and retry. After sniffing, press the side button to turn off the green light.

​​Sniffing Results:​​

After sniffing (green light off), click this button to display the sniffing results.

​​Cardless Sniffing:​​

Enter the UID and click Cardless Sniffing (green light on). Place the device near the reader to sniff passwords. For NTAG cards, input the card number and check "NTAG" before starting. Use the back toggle switch to switch to sniffing mode for better results.

​​Offline Sniffing Results:​​

When the device is disconnected from the computer (standalone power), press the side button for 2 seconds until all lights flash. Release immediately (green light on; if not, release faster and retry). The device enters offline card sniffing mode. After sniffing, press the side button—green light flashes 3 times and turns off. Reconnect to the computer to extract results. Multiple offline sniffing results accumulate. Clear results afterward to free storage space.

​​Sniffing Analysis:​​

Analyzes log data, extracting key info to the top of the log.

(Technical notes preserved: light indicators, UID input, NTAG option, toggle switch function, and offline mode workflow.)

。

APP

​​Notice:​​

The APP is provided for free by the community, and our company is not responsible for it.

​​Before using the APP:​​

You must first flash the ​​APP firmware​​ via the computer software.

If your system does ​​not support automatic port selection​​ for firmware flashing:

Copy the ​​two firmware files​​ from the APP folder into the ​​"client" directory​​.

Then manually flash the firmware.

​​Current Limitations:​​

The APP ​​does not support third-generation non-vulnerable (F08S) cracking​​, so its use is ​​not recommended​​.

To install the APP, click the ​​"Other Tools"​​ button and locate ​​"ENPM3MAX.APK"​​ in the pop-up window.

(Key details preserved: firmware flashing steps, manual workaround, F08S incompatibility warning, and APK location.)

​​Alternative concise version:​​

"Community-provided APP (unsupported by us). Requires manual firmware flash if auto-port fails. Not recommended—lacks F08S cracking. Find ENPM3MAX.APK under 'Other Tools'."

