PICOVEND
MDB SNIFFER

v1.0 – 15.02.2019

Table of Contents

I. Hardware description

The device was designed for in-field MDB communication testing and diagnostic. It is powered directly from the MDB bus and has the following functions:
- receiving 9bit MDB communication messages and converting them to 8bit messages;
- joins VMC and peripheral messages in a single message and adds the message length on the first byte, to make messages parsing very easy;
- sends all captured and translated messages over the Bluetooth, using Serial Port Profile.

The device can be easily connected with a computer or a phone that will receive the data. First byte of the received batch is the length of the first message.
The device comes with a full “Y” MDB data cable (male/female). No other cables or adapters are needed for this.

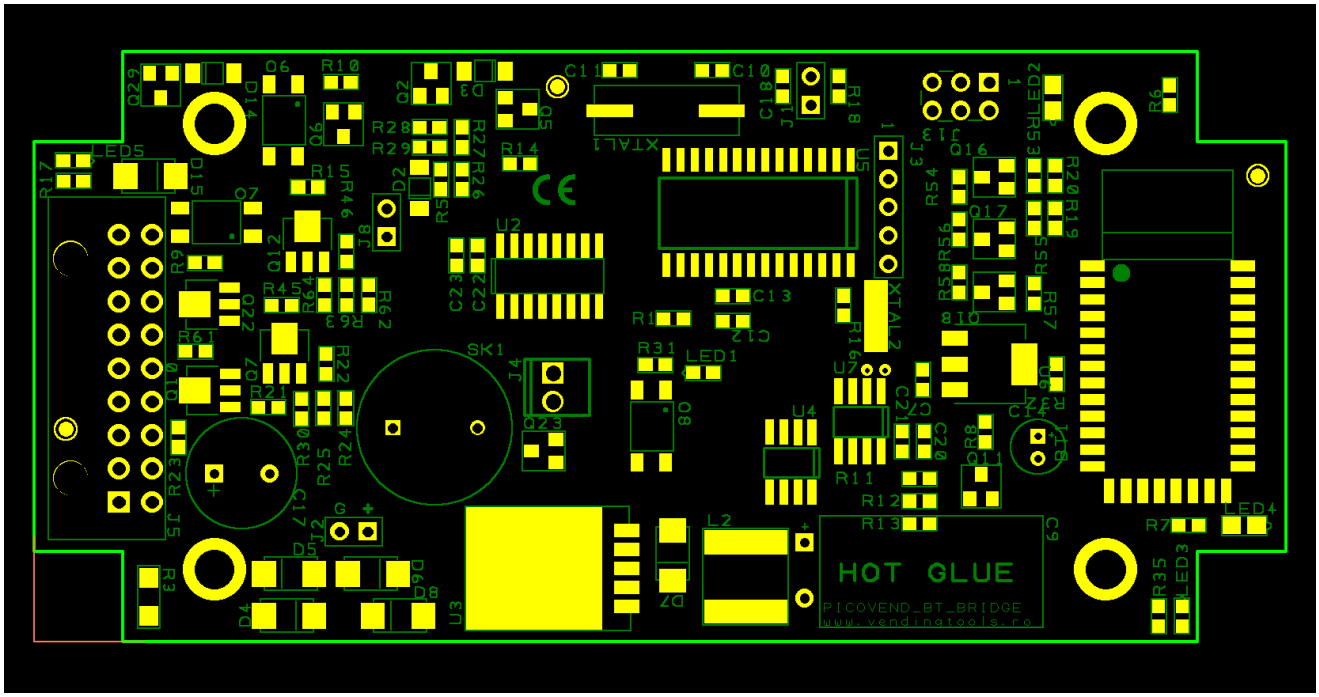


Image 1: Board overview

II. Functionality

1. Received data structure

Received data is binary and the first byte is the first message length.
For example:
- MDB bill validator poll – 0x03 0x33 0x33 0x00, first byte is the message length (including VMC and peripheral answer), second byte is VMC command (0x33 – bill validator poll), the third byte is MDB CRC and the fourth byte is peripheral's answer (0x00 – ACK).
- MDB bill validator poll with no answer from peripheral – 0x02 0x33 0x33, first byte is message length second byte is VMC command (0x33 – bill validator poll) and the third byte is MDB CRC. Since there is no answer from the bill validator, the device returns a message length of 2.

2. Connecting to the device using Microsoft Windows 10 operating system

To connect the device on a computer using Microsoft Windows 10 operating system, you need to follow the procedure:

a. Pairing the device over Bluetooth

- Power up the device, applying a voltage between 10 and 34VDC, eventually by connecting to an MDB bus.
- Go to "Bluetooth and other devices setting"
- Choose "Add Bluetooth or other device"
- Choose "Bluetooth (mice, keyboard, pens, or audio and other kinds of Bluetooth device)"
- Wait for the the operating system to detect and identify the device. Sniffers Bluetooth IDs are respecting the following format: PVBTAAXXXX, where AA is the device family and XXXX is the device ID (both can be letters and numbers).
- Select the device, type the password on the device's label and wait for the operating system to install needed file (detection and installation are automatically performed, no software installation needed).
- After the finish message installation, check if the device is correctly installed (right click on "This PC" → click on "Manage" → click on "Device manager" → expand "Ports (COM & LPT) and search for one or more records "Standard Serial over Bluetooth link (COMx or COMxx).

b. Using the device over Bluetooth

You can connect and capture binary data, using RealTerm (Run as Administrator) or other terminal application. Please make sure you configure the serial port with 115200bps, 8 data bits, 1 stop bit, no parity and no hardware or software flow control. Also, please make sure you are selecting HEX data view.
Open the port, capture data while performing some MDB tasks, close the port and you finally have the corresponding MDB log.

3. Connecting to the device using Ubuntu or Raspbian (for Raspberry Pi)

- Power up the device, applying a voltage between 10 and 34VDC, eventually by connecting to an MDB bus.
- Open a terminal window and change user to root.

- Using your favorite editor, modify the file /etc/systemd/system/dbus-org.bluez.service as follows:
    - You need to have a line containing - ExecStart=/usr/lib/bluetooth/bluetoothd -C
    - You need to have a line containing - ExecStartPost=/usr/bin/sdptool add SP
- Save and reboot
- Open a terminal window and change user to root.
- Run the command bluetoothctl
- In bluetoothctl console, type the following command succession:
    - scan on
    - devices
    - agent on
    - pair XX:XX:XX:XX:XX:XX (where XX:XX:XX:XX:XX:XX is the hardware address of your device)
    - type the password you can find on device's label when asked to.
    - trust XX:XX:XX:XX:XX:XX
    - quit

In the console, type: rfcomm bind /dev/rfcomm0 XX:XX:XX:XX:XX 1
After that, you can use any serial terminal application to connect on /dev/rfcomm0
Please make sure you configure the serial port with 115200bps, 8 data bits, 1 stop bit, no parity and no hardware or software flow control. Also, please make sure you are selecting HEX data view.
Open the port, capture data while performing some MDB tasks, close the port and you finally have the corresponding MDB log.

III. The Android application

We are also providing an Android application that can be downloaded from our site (you need to enable installation from unknown sources in your phone/tablet settings) or from the Play Store.
In order to use the application in online mode (to connect to the machine) you need to power-up the device and pair it in your phone/tablet Bluetooth menu. The password is printed on the device's label.

After pairing successfully, you can start the application.

1. Barcode scan screen (start screen)

This screen has 2 functions, either scan the QR code on the device's box, or, by pressing "Skip scan" button, to switch using application in offline mode to reanalyze or send by e-mail older records.
If your VMC start-up/self-check time is very short (usually on some snack/universal vending machines without cooling device or with disabled cooling device), the best procedure is as follows:
- turn off the machine;
- star the application and scan the barcode;
- when the application shows a progress dialog about connecting to the device, turn on the machine.

Using the above procedure, you can easily capture the MDB initialization phase.

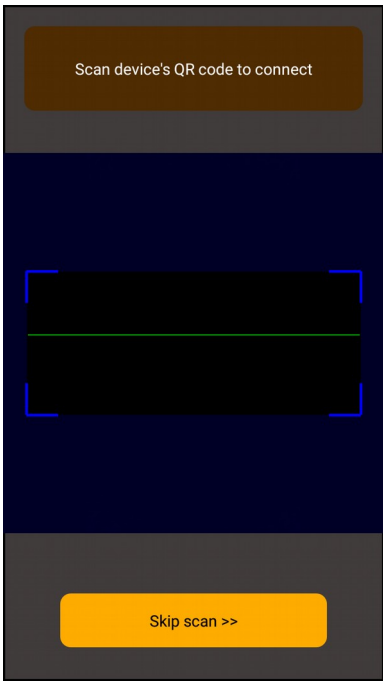


Image 2: Barcode scanner

After scanning the barcode, if the connection to the Bluetooth device is ready, the application will switch to the main screen.

2. Main screen

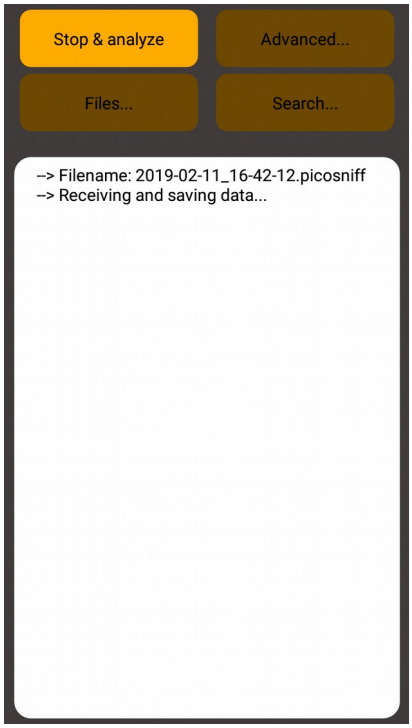


Image 4: Main screen - online mode - after device connection

The main screen has two layouts (one for online mode – connected with the device over the Bluetooth and one for offline mode).In online mode, after scanning the device and connecting, the main screen is automatically started in receiving mode.
When you want to finish the reception, simply touch the “Stop & analyze” button. The application will analyze all received data and will display the interpreted activity log.
You may scroll the log area to check the data.
In offline mode, the application will show a blank log area. You should select an existing file for reanalyze. Using device’s “Back” button in main screen will terminate then application (if you press “Back” button another time within 5 seconds.

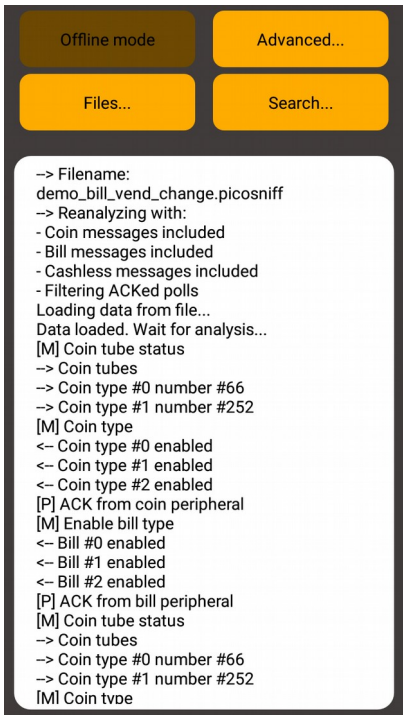


Image 3: Main screen - offline mode

The main screen has 4 buttons, each with specific function:
a. Stop & analyze button will stop the current reception and will automatically trigger the analyzing procedure. After the analyze, the log area will show the interpreted data. Also, the button’s caption will change to “Receive” and all other buttons will be activated.
b. Advanced button will show the advanced analyze options
c. Files button will show the files list and options
d. Search button will show the search bar onto of the log area

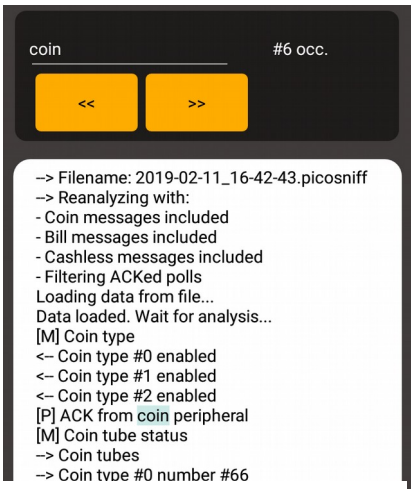
Image 5: Advanced options screeen

3. Advanced screen

This screen is showing the analysis options. By default, on start, the analysis includes all informations about coin mechanism, bill validator and the cashless #1 device and, also, the machine's polls to peripherals.
Using this screen, you can select only the device/devices you need to analyze. Also, you can exclude all machine's polls where the peripheral answer was simple ACK, to reduce the log data amount making it easier to view.
For the same reason, on the same screen there is an option to remove from analysis, all machine's messages where the peripheral did not answered.
There is a reserved space for future analysis options, that will be subject of future application updates.
The two buttons on this screen have the following functions:
a. Reanalyze button – will show the main screen and will trigger a new analysis with the existing data and with selected options.
b. Reanalyze & send button – will show the main screen and will trigger a new analysis with the existing data and with the selected data. After the analysis is finished, the application will generate and try to send an e-mail, attaching the interpreted log data file. For this option, you will be redirected to select an existing e-mail application. You need to have installed and configured an e-mail application and you need to select the correct e-mailing application when required.
Use device's "Back" button to return to the main screen.

4. Main screen with search bar

By pressing "Search" button on the main screen, the search bar will be displayed on top of the log data area.
Type your search term and click on ">>" button to search. Near the text field, the application shows the current selected occurrence number.
You may, also, use "<<" button to search backward.
The search function is case insensitive and may help you to jump to the desired log data.
Use device's "Back" button to hide the search bar.



5. Files screen

This screen show a list with saved/captured files. On capture, the application automatically saves data in a file with the name

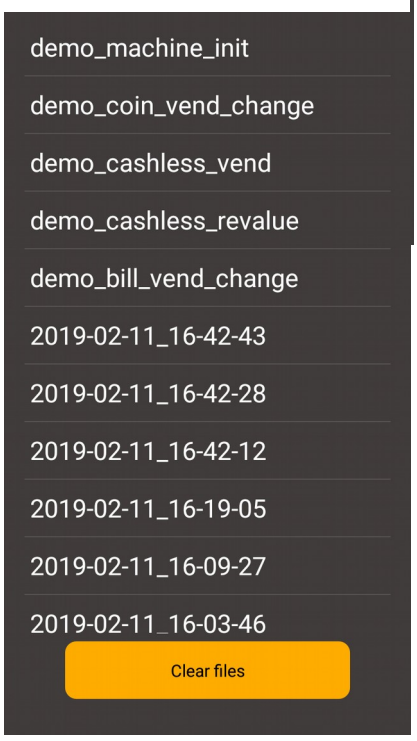
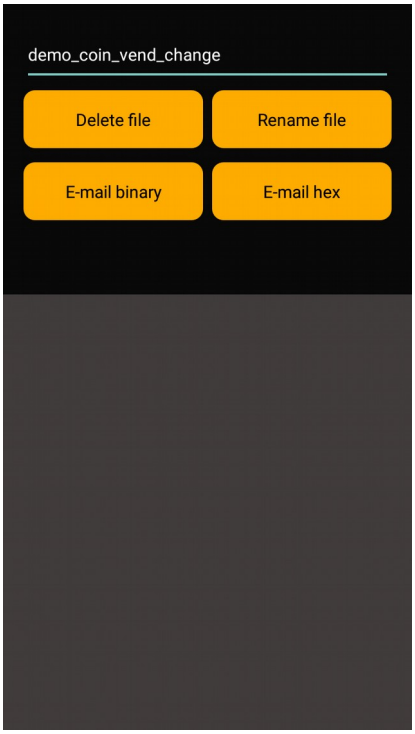


Image 7: Files screen

generated by the following algorithm:<year>-<month>-<day>_<hour>-<min>-<second>.picosniff
You can rename a file at any time, by using files action bar described in another section below.

The “Clear files” button will delete all not renamed files, starting with number “2”. Files may be also delete individually by using files action bar. The application comes with 5 demo files that cannot be removed nor renamed:
- **demo_machine_init** – is a file containing data for a machine initialization, with a bill validator, a coin changer and a cashless device connected on the bus.
- **demo_coin_vend_change –** is a file containing data for some cash sales, based on coins, with also some change returned to the customer.
- **demo_cashless_vend** – is a file containing data for some cashless sales.
- **demo_cashless_revalue** – is a file containing data for cashless revalue transaction, based on bill acceptance.
- **demo_bill_vend_change** – is a file containing data for some cash sales, based on bill acceptance, with coins change.
Those files are installed by default to let you evaluate the application in offline mode, before buying the sniffing device.
Use device’s “Back” button to return to the main screen.

6. Files action bar



By a long touch over a file name in files screen, the files action bar will be displayed on the screen.
This contains 4 buttons:
- “**Delete file**” - will erase the selected file (excepting the demo files, that cennot be deleted).
- “**Rename file**” - will rename the selected file with a name you have typed in the text box above.
- “**E-mail binary**” - will send the raw file data on the e-mail. For this option, you will be redirected to select an existing e-mail application. You need to have installed and configured an e-mail application and you need to select the correct e-mailing application when required.
- “**E-mail hex**” - will parse the binary file and generate a hex text, with each command/answer on o single line and send on the e-mail. For this option, you will be redirected to select an existing e-mail application. You need to have installed and configured an e-mail application and you need to select the correct e-mailing application when required.
The format is the same as in binary, with the first byte representing the message length, but as a text file that you can open and read with any text editor.
For example:
[0x03 0x08 0x08 0x00] - **this means cashless #1 poll and ACK**
[0x03 0x0B 0x0B 0x00] - **this means a coin acceptor poll and ACK**
[0x1A 0x09 0x09 0x03 0x16 0x42 0x0A 0x02 0x00 0x03 0x01 0x05 0x0F 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x7F] - **this means ca coin acceptor setup info request and answer**
[0x03 0x0B 0x0B 0x00]
[0x25 0x0F 0x00 0x0F 0x4D 0x45 0x49 0x34 0x32 0x36 0x38 0x47 0x39 0x30 0x32 0x39 0x30 0x33 0x20 0x43 0x46 0x37 0x39 0x30 0x30 0x4D 0x44 0x42 0x20 0x20 0x20 0x01 0x16 0x00 0x00 0x00 0x07 0xF7]
[0x03 0x0B 0x0B 0x00]

[0x15 0x0A 0x0A 0x00 0x00 0x42 0xFC 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x3E]
[0x03 0x0B 0x0B 0x00]
[0x07 0x0C 0x00 0x00 0xFF 0xFF 0x0A 0x00]
[0x03 0x0B 0x0B 0x00]

IV. Further options (for next application versions):

- add cashless 32bit values (for the moment only 16bits data are interpreted for cashless devices);
- add 0x37 bill functions from 0x03 and up;
- add bill recycler functions;
- add second cashless device detection;
- add communication gateway;
- add universal satellite device;
- add age verification device;