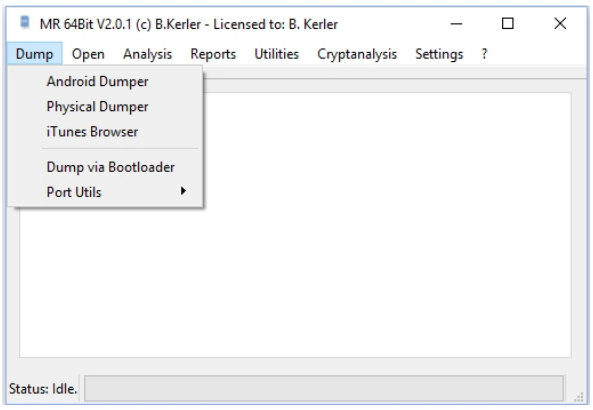
Mobile Revelator 2.2.5

Inhaltsverzeichnis

Mobile Revelator
Version 2.2.5

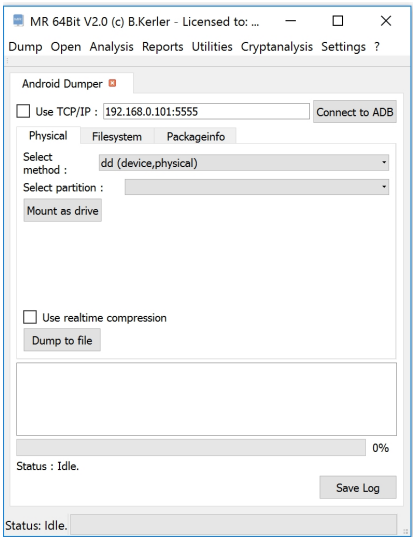
Mobile Revelator is a tool mainly developed by Bjoern Kerler. Its main aim
is to support forensic mobile researchers in conducting better forensic examinations
and in verification of existing commercial forensic solutions.

Dump



The "Dump" Menu offers several tools to Dump Android, Physical and iTunes compatible devices.

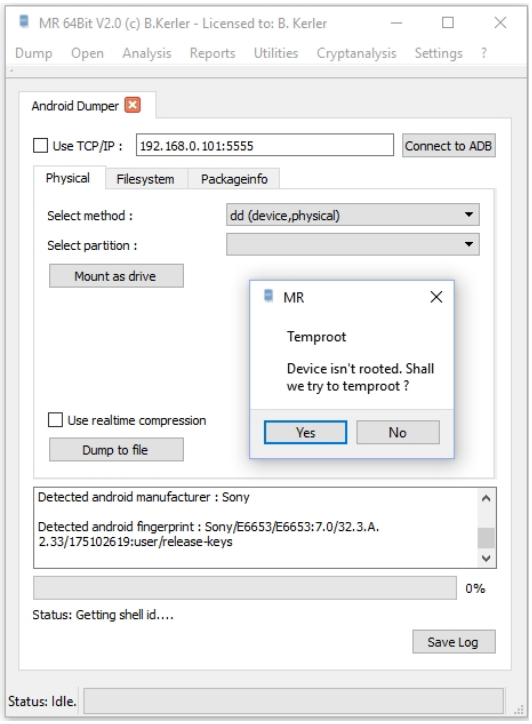
Android Dumper



The android dumper tool enables you to raw dump partitions and whole flash chips using adb connection if the device has been rooted or if it is being used with a custom recovery such as TWRP or CWM. For some devices lower android 4.4, it is also able to temproot the device.

Furthermore it enables you to do a logical backup using android backup functionality as well.

Physical

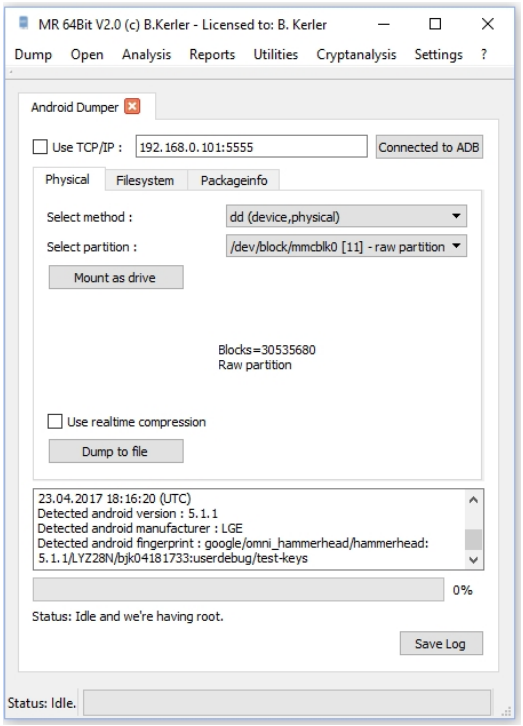


The Android Dumper provides physical dumping capabilities for unrooted Android < 6.0 stock devices and unlocked devices with custom recovery.

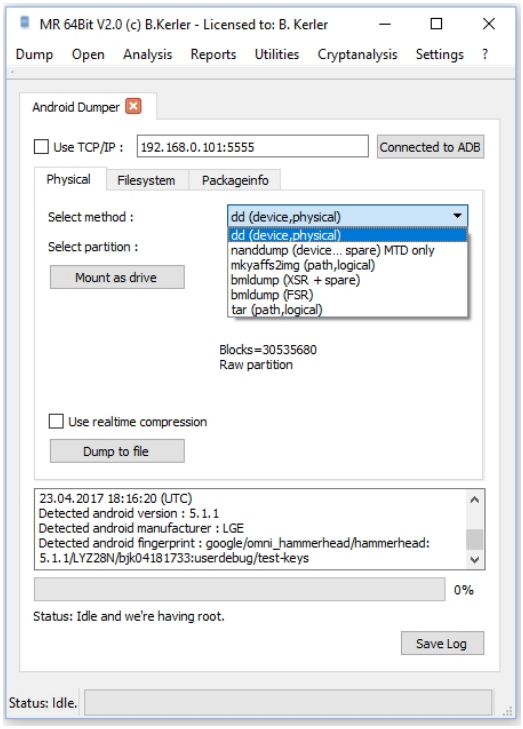
In order to physically dump, press "Connect to ADB" and make sure that USB Debugging is enabled on the device. If everything works fine, you will see that it's going to print which android version and manufacturer has been detected.

If the device isn't already rooted, it's going to ask if you want to temproot the device. Temproot does currently only work for devices with Android < 6.0.

If the device is rooted, you will then be presented the detected partition available for dumping :



MR will automatically select the full flash if available (/dev/block/mmcblk0 or /dev/block/sda).

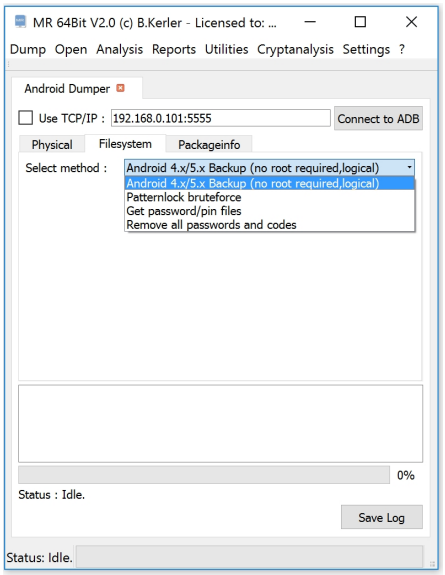


You may then choose several options for dumping. For emmc and sdcards, dd is the most appropriate option for saving. However if Nand Flash is being used, choose nanddump for MTD or bmldump for samsung devices with xsr/stl/bml wearleveling or filesystem dump methods such as mkyaffs2img and tar.

"Use realtime compression" does make sense, if you encounter a large flash (128/256 GB) with large areas of empty space.
Otherwise, selecting this option will slow down the dumping process.

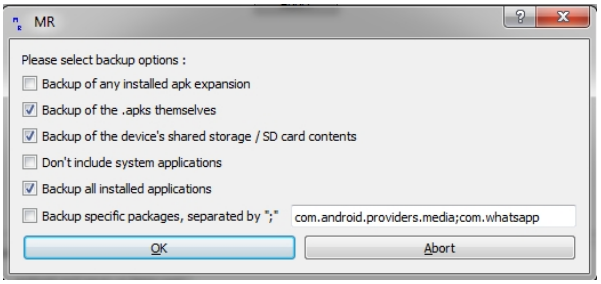
Pressing "Dump to file" will save the flash as raw image. If available, "Mount as drive" will force the usb setting of the device to enable partition access by usb driver.

Filesystem



Once you connected to ADB, you may use these Filesystem options :

- Android 4.x/5.x Backup will enable you to dump via the Android internal backup functionality. After you press "Run", you may choose what to backup :

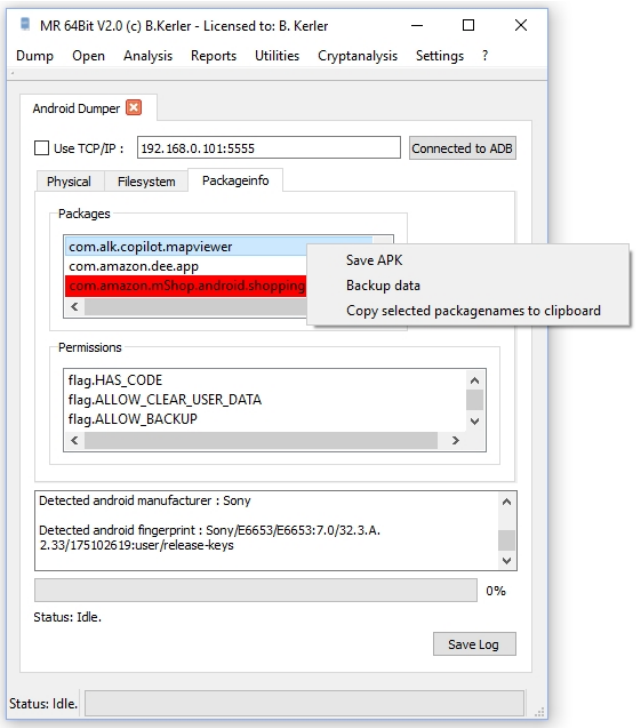


- Patternlock bruteforce will read the gesture.key file from /data/system, bruteforce the pattern using CPU and then present the pattern.

- Get password/pin files will extract the most common files used for password/pin/gesture storage from the device

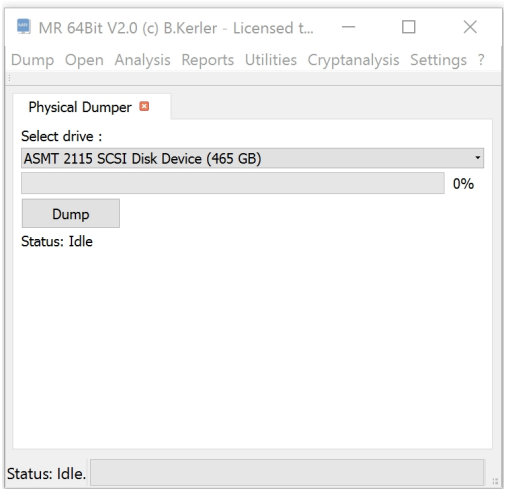
- Remove all passwords and codes will remove passwords and codes from both files and sqlite databases and should thus be choosen only if it is really needed to be done.

Packageinfo



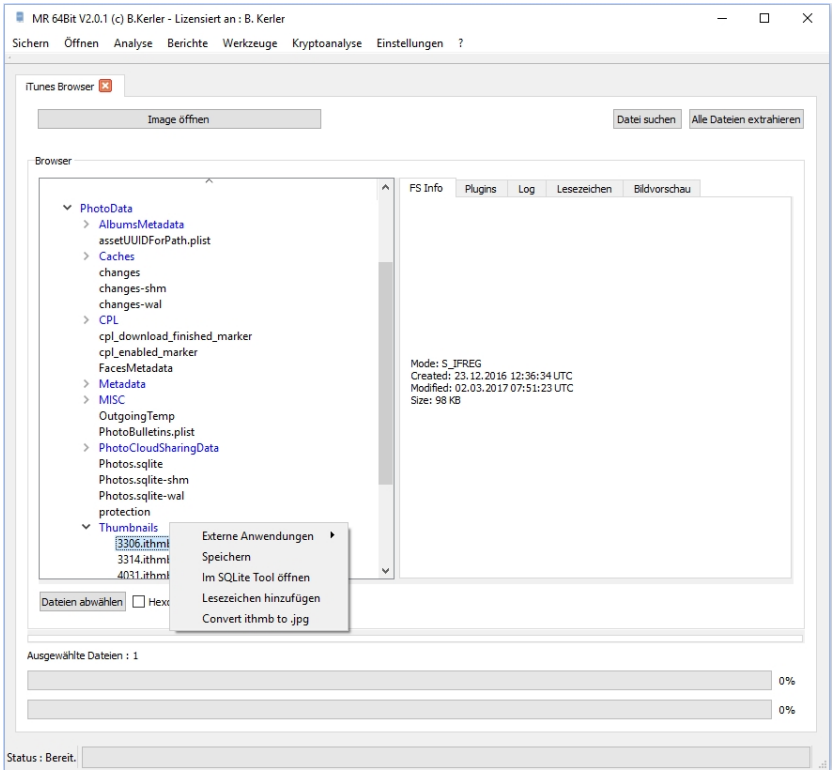
Packageinfo will read all installed and removed packages from the Android Package Manager. Clicking with the left mouse button on the entries will show specific application rights and properties. Clicking with the right mouse on the package, it will allow you to save the application apk, backup the application data and copy the packagename to the clipboard. If the entry is being highlighted in red, then the package doesn't allow application data to be backed up.

Physical Dumper



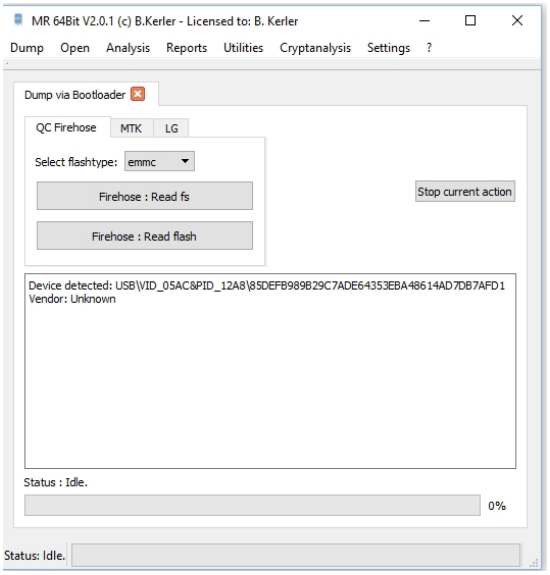
The Physical Dump Tool lets you save full physical devices connected to your PC, like harddrives or SD-Cards in SD-Cardreaders. Press "Dump" and choose where to save the dump file.
The file will be saved in RAW-Format.

iTunes Browser



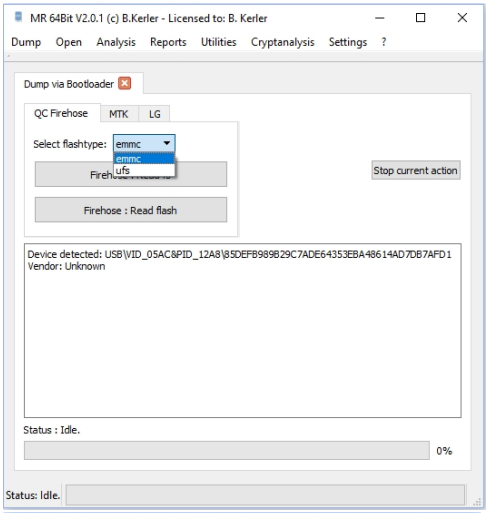
Using this tool, you may connect an iPhone/iPod/iPad. First install iTunes, connect to the device, trust on the device and trust in iTunes, it will then access the AFC-System of the device and lets you save files but also open them in the internal sqlite tool or any external viewer you wish. Furthermore, it lets you extract .ithmb databases (from PhotoData/Thumbnails) to jpg files [see more in Analysis\Apple iThmb Extract chapter in this document].

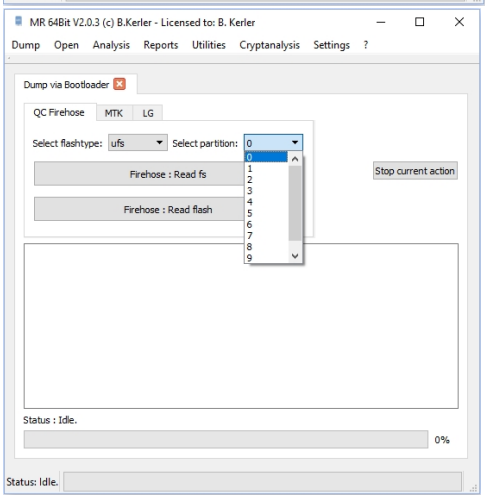
Dump via Bootloader



The "Dump via Bootloader"-Tool allows to dump several devices via bootloader, but does also show new detected or attached devices.

QC Firehose





Some devices like "Oneplus One, X, 3, 3T" and several other devices with Qualcomm CPU
newer than MSM8974 can be dumped or content written using the "QDLoader 9008" Port.

First press "Firehose: Read fs" or "Firehose: Read flash" button, and then connect a device with 9008 Mode via usb to the host pc.

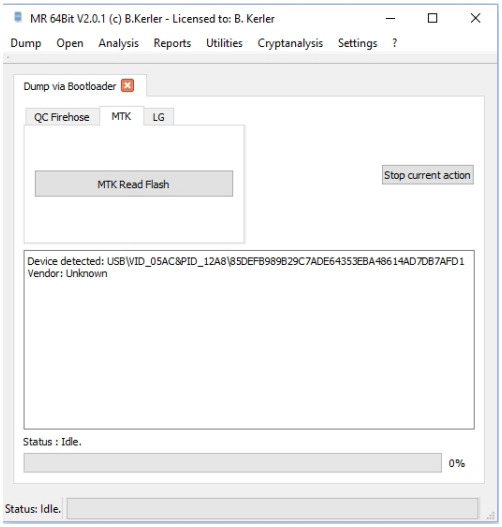
The 9008 Mode, also called "Sahara" Mode, can be enabled by either using adb and sending "adb reboot edl"
or fastboot by sending "fastboot reboot edl" or by pressing volume up and volume down while connecting the usb cable to a powered off device. Also this mode can be enabled by shorting CLK Signal of the emmc on the pcb with Ground while connecting
a powered off device and pressing power for a few seconds or by shortening d+ and gnd on usb while connecting the mobile and then
releasing the short.

For firehose, you should the right flashtype, either emmc or ufs before connecting. Be aware that a ufs flash can have multiple
partitions, so you should choose the partition number first. If unsure, let flashtype on ufs and partition number on 0.

"Firehose: Read fs" will allow you to browse and also write partitions, "Firehose: Read flash" will only dump the full flash. As a reminder, all devices coming with Android 6 out of the box are encrypted, so one option might be to flash a custom recovery like twrp or cm to the device via firehose in order to dump the unencrypted data.

You may interrupt any action pressing the "Stop current action" button.

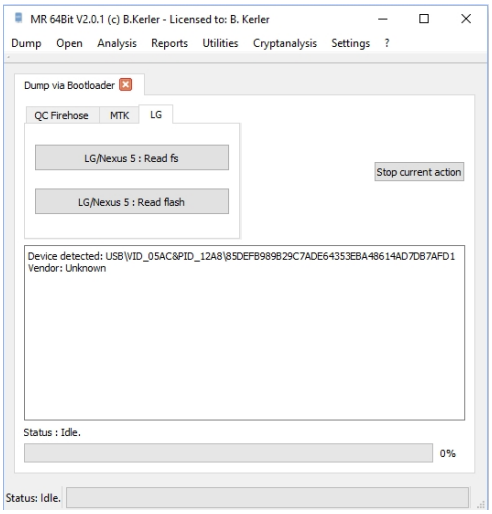
MTK



For devices using MTK chipset, power off the device, install the MTK Preloader Com port driver, press "MTK Read Flash button" and then just connect the mobile.

You may interrupt any action pressing the "Stop current action" button.

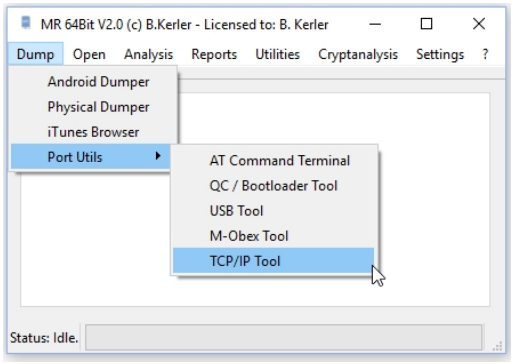
LG



For LG android devices > Android 4.x and < 5.1, you may switch to the download mode by powering the mobile off, then press and hold volume up button while connecting the usb cable to the mobile. Once you see the download mode, you may press "LG G2/Nexus 5: Read fs" button to show installed partitions or press "LG G2/Nexus 5: Read flash" button to get a physical dump of the flash chip.

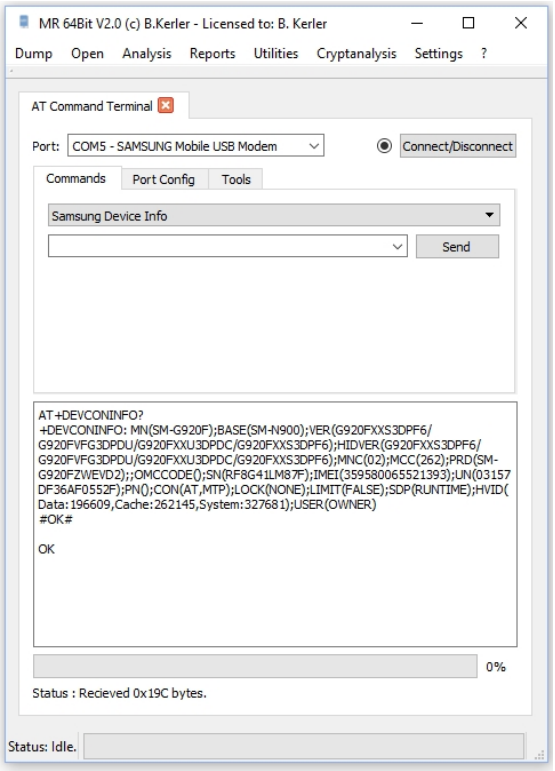
You may interrupt any action pressing the "Stop current action" button.

Port Utils



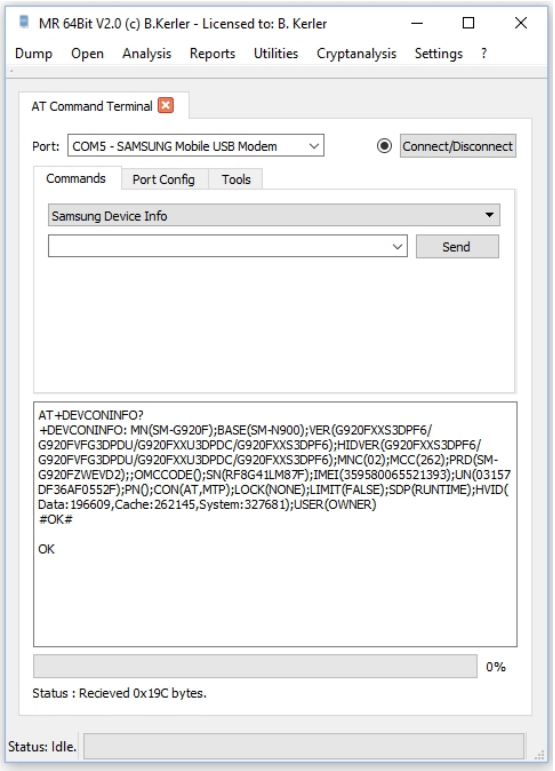
The port utilities offer functionality to access mobiles via ports such as usb, tcp/ip and com ports.

AT Command Terminal



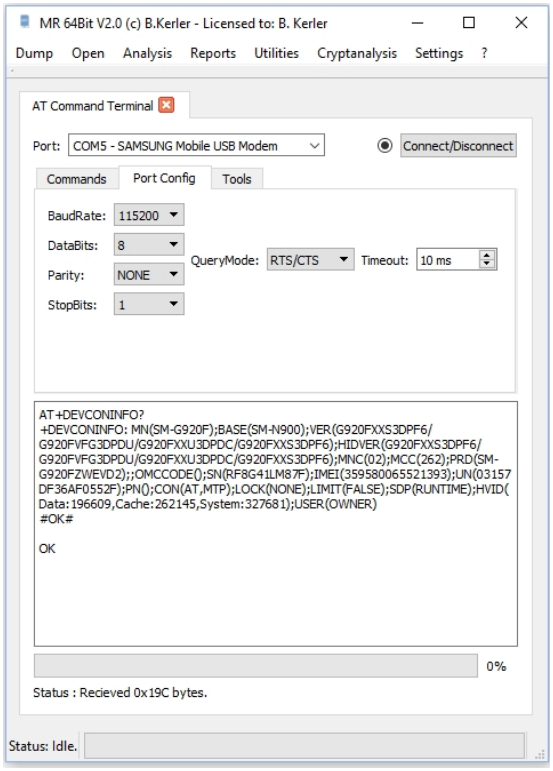
The AT Command Terminal is able to send ascii commands to a serial port device such as a modem.

Commands



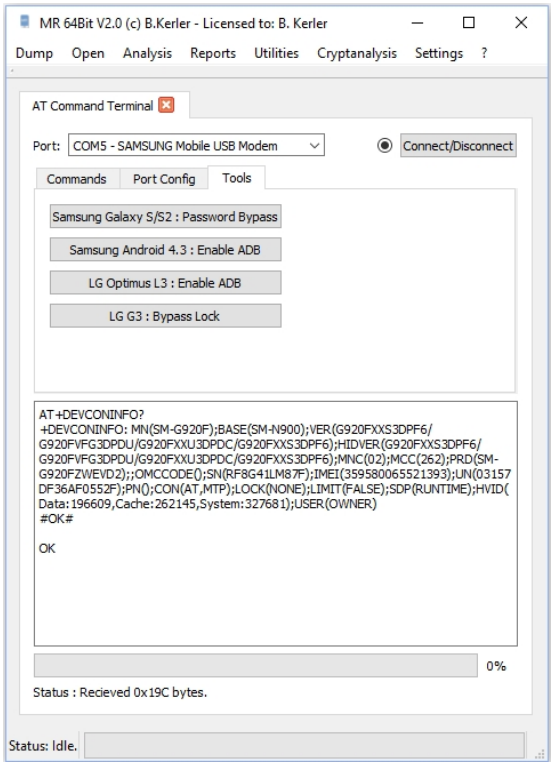
In order to send any AT commands to modem or serial ports, just select the Port and press "Connect/Disconnect" button.
If the connection has been successfully made, the circle left the the "Connect/Disconnect" button should fill.
After that you may either select a common command from the command list just above the "Send" button or enter any commands like "ATI" left to the "Send" button and then press "Send". The result will be shown in the text view below.

Port Config



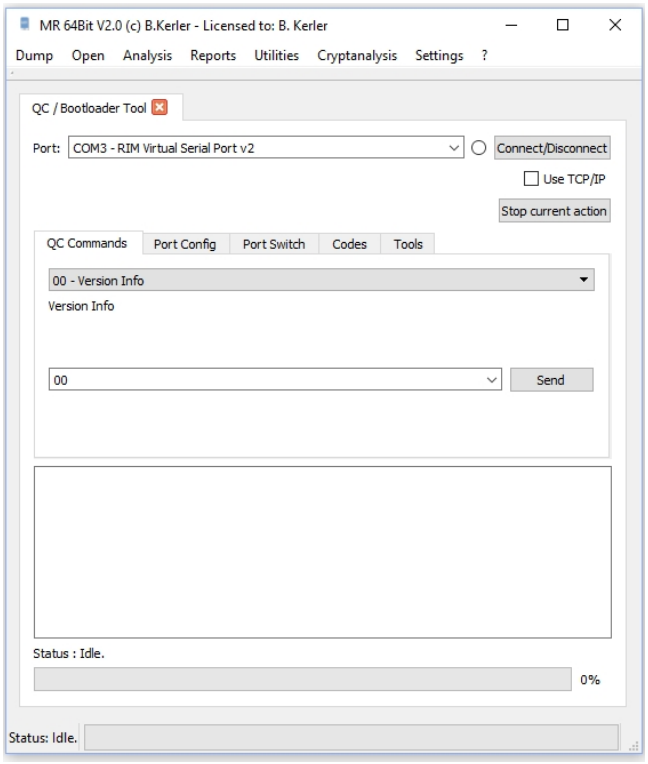
The port config tab allows you to set specific settings, such as baudrate, databits, parity, stopBits and Flow Control.

Tools



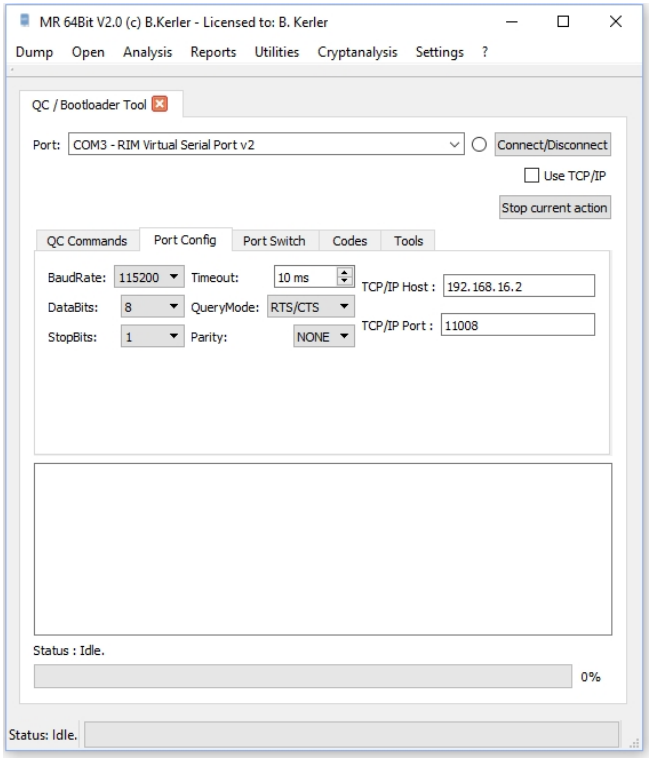
After a successful connection has been made, some functions may be available on specific devices in order to enable ADB or to bypass passwords via com port.

QC / Bootloader Tool



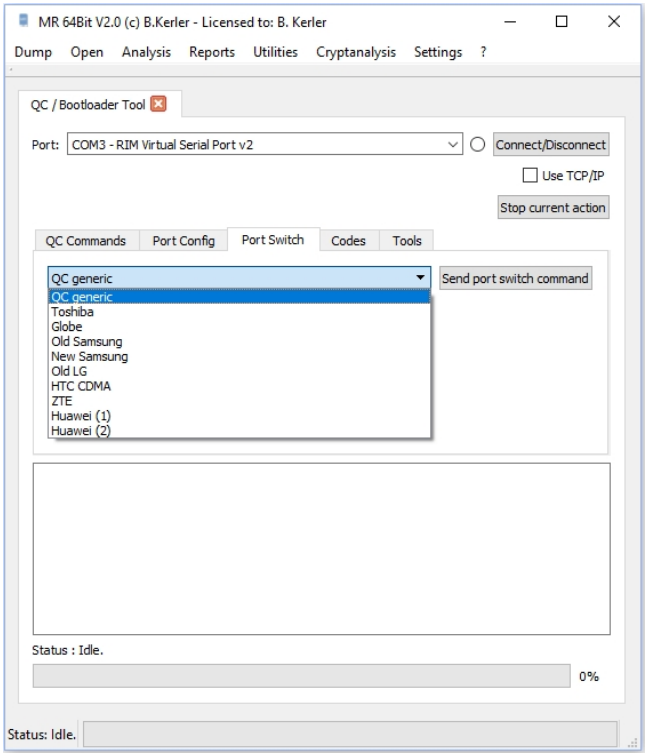
Using the Qualcomm Modem and Bootloader Tool you may send qualcomm specific commands as hex bytes to ports using qualcomm sahara and diag protocol but also has several tools for bootloaders such as LG and MTK enabled devices in order to read the flash.

Port Config



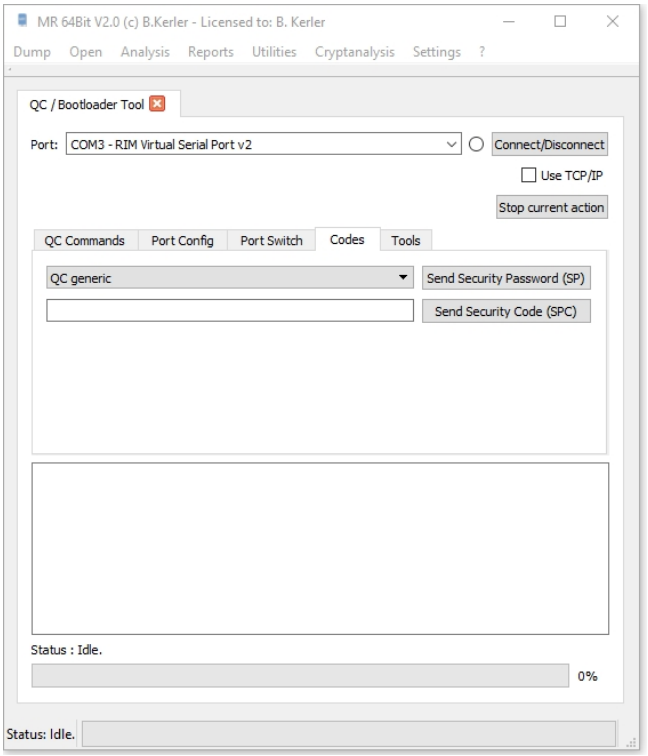
The "Port Config" tab shows possible settings for both com ports and tcp/ip connections.

Port Switch



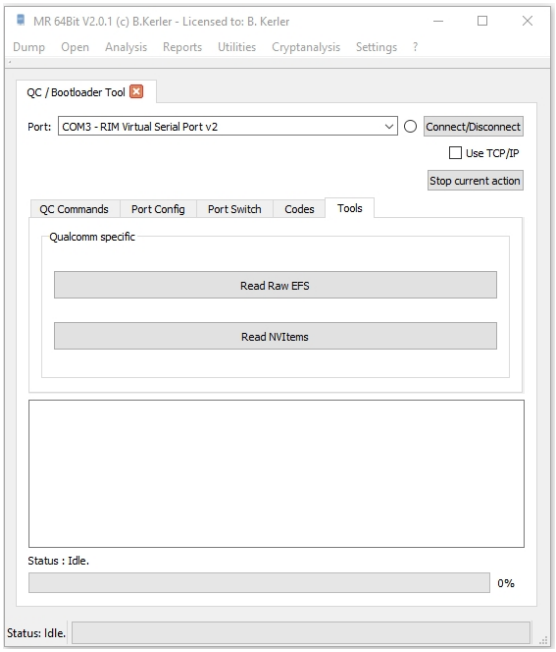
For some modem devices, you first need to switch the modem to a qualcomm interface port. Just select the type and then press "Send port switch command" button in order to switch the port.

Codes



For some qualcomm devices, reading efs and nvitems is only possible after sending the right security password (SP) or Security Code (SPC).

Tools

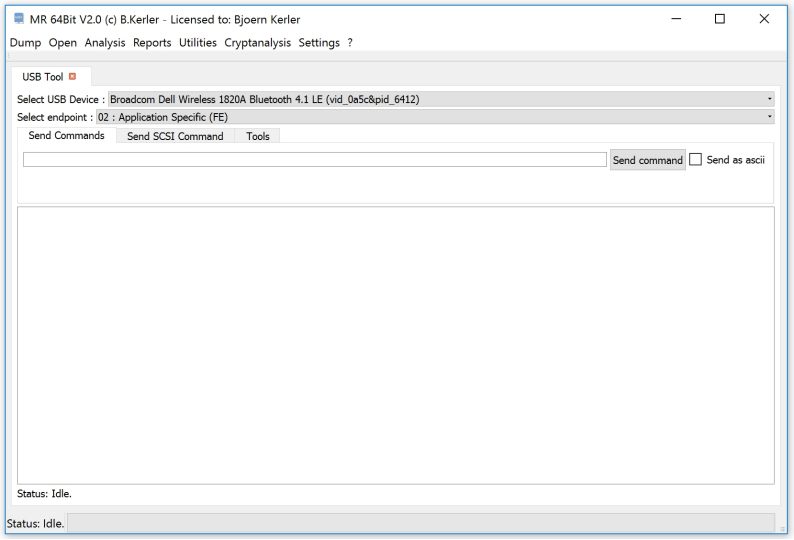


The "Tools" tab has the following functionality :

Once connected to a device with qualcomm chipset, you may read the raw efs or read the nvitems.

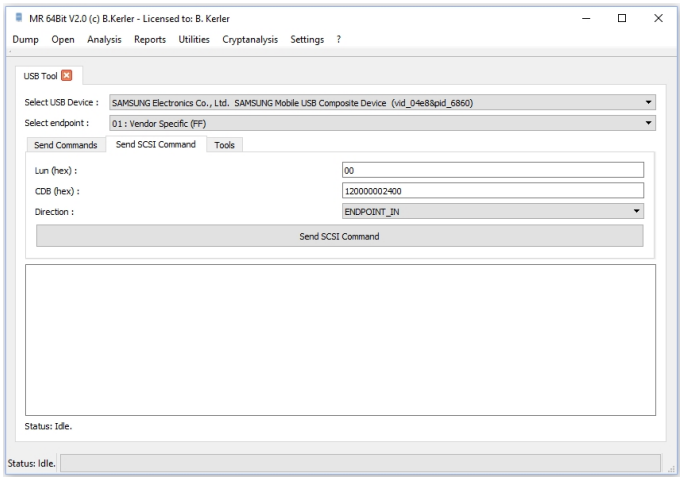
You may interrupt any action pressing the "Stop current action" button.

USB Tool



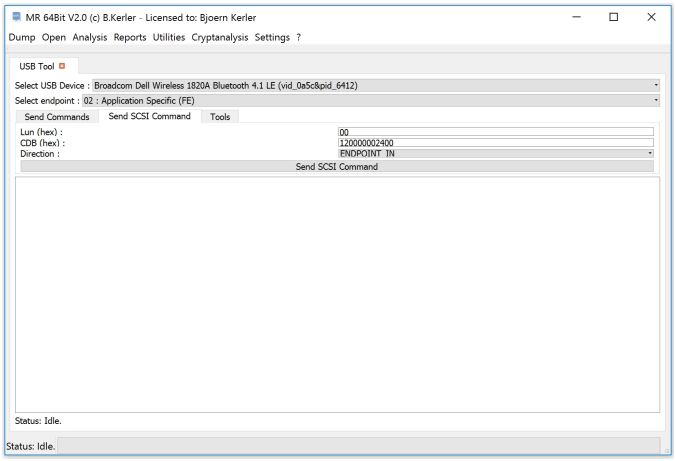
The USB tool enables you to send raw data to connected USB devices.

Send Commands



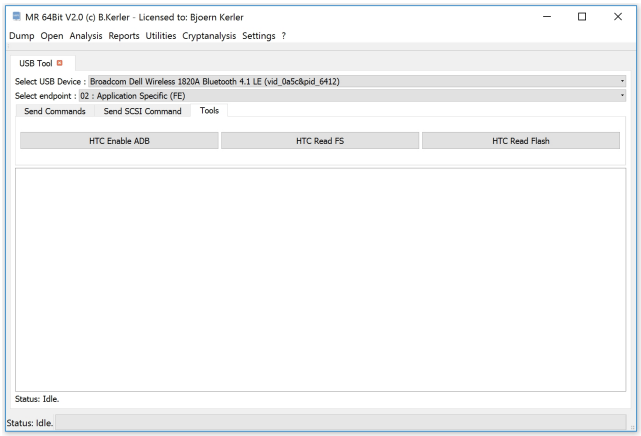
This tool is able to send raw hex bytes or ascii packets to usb devices.

Send SCSI Command



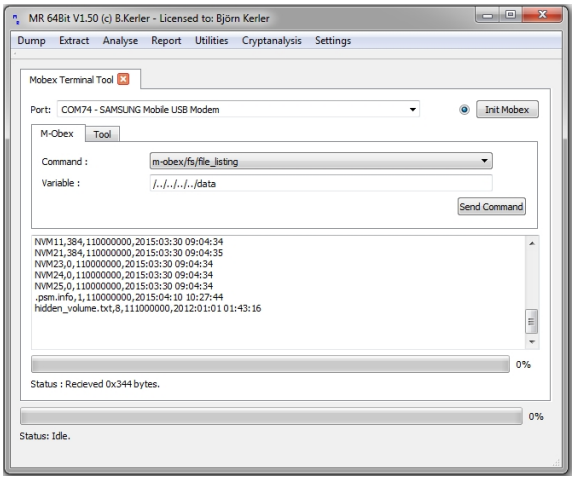
This tool is able to send SCSI commands to USB devices.

Tools

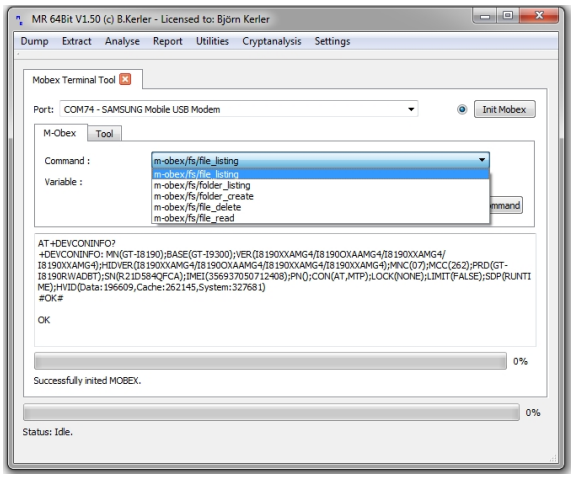


For enabling ADB for some HTC devices such as "Wildfire", select the HTC device as USB device and Mass Storage (08) as endpoint and then press "HTC enable ADB" to enable ADB. For older HTC android devices, you may as well boot the device into bootloader mode, select the HTC devices as USB device and then click "HTC Read FS" to open up the Partition Tool in order to show/read/save partition contents.

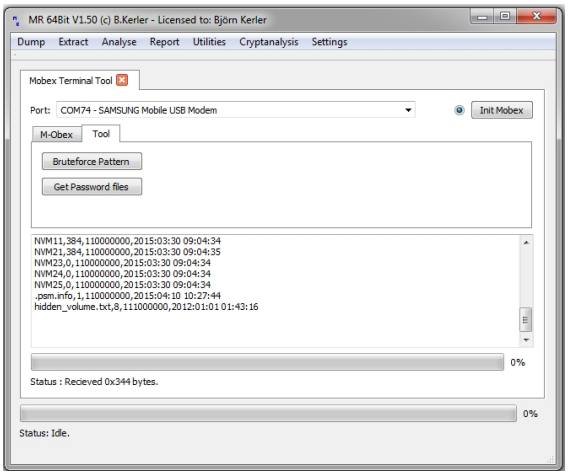
M-Obex Tool



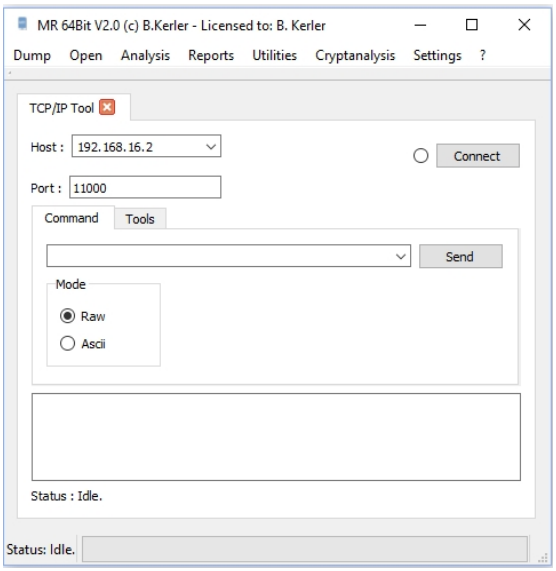
The M-Obex tool offers functionality to access the Samsung Modem Obex interface. Just select the Samsung Mobile Port and press "Init Mobex". Once it's successfully connected, the circle left of the "Init Mobex" button will be filled. You may then send any file command by entering into the text field such as "../../../../../data" and pressing the "Send command" button.



Once Mobex has been successfully connected, you may bruteforce the pattern lock or get password files for Samsung android mobiles if the firmware version is higher 4.0 and lower than 4.2.2.

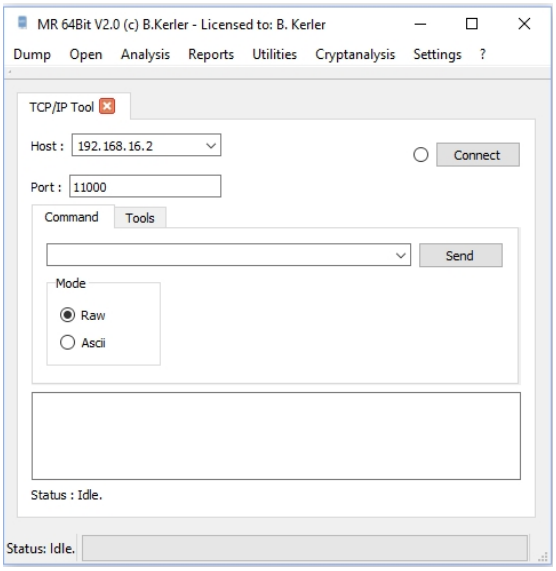


TCP/IP Tool



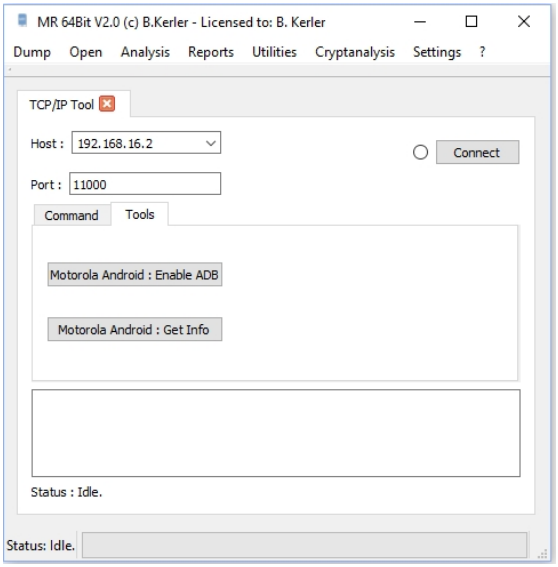
The tcp/ip tools tab offers functions for sending Hex or Ascii messages via tcp/ip such as motorola android mobiles.

Command



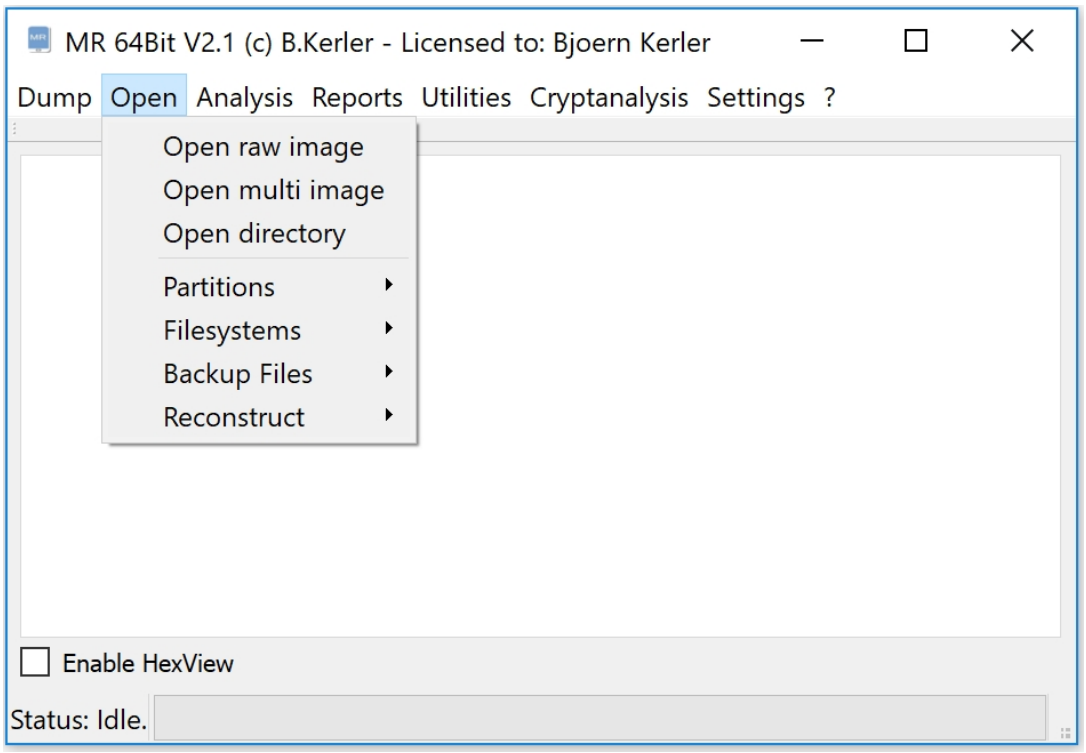
Select the right host and then press connect. Once successfully connected, the left circle at the "Connect" button will be filled. Then you are able to send either raw bytes as hex values or ascii chars being entered at the left side of the "Send" button by pressing the "Send" button.

Tools



The tcp/ip tools tab offers functions for motorola android mobiles. Select the right host and then press connect. Once successfully connected, the left circle at the "Connect" button will be filled.

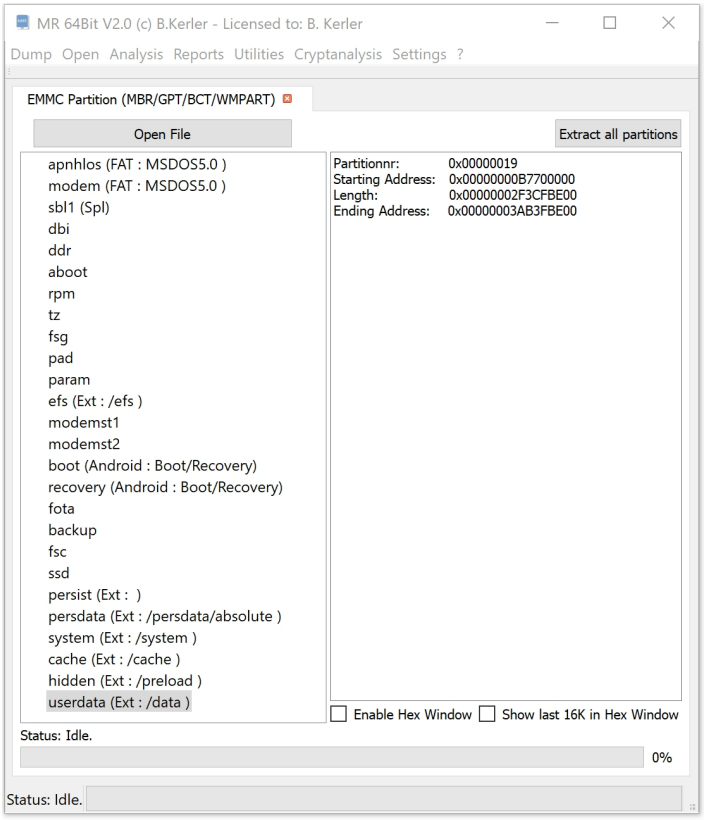
Open



The Open menu offers options to work with partition systems, filesystems, backup files,
flash wearleveling (reconstruct) and options to extract and carve files, including Apple thumbnail databases.

"Open raw image" allows to open full raw dumps of flashchips or jtag images such as emmc dumps.
"Open multi image" combines several dumps or folders into one single filesystem view.
"Open directory" uses a local directory as a filesystem view.

Open raw flash

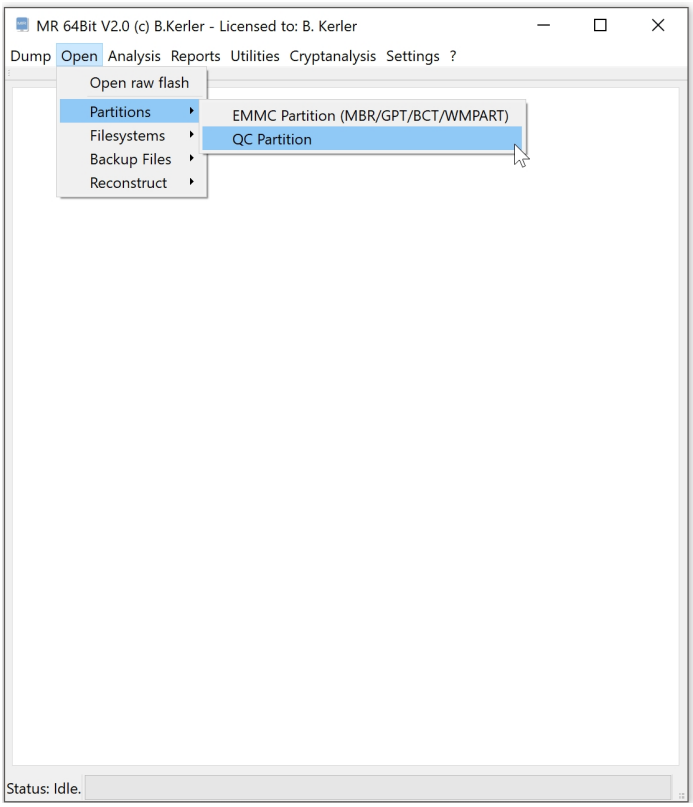


Using "Open File" you may open any raw flash binary file. If a known Partitiontype is detected, which may be MBR, GPT, BCT and WM7 it will show all including partitions.

Clicking with the left mouse button on a partition entry will reveal its attributes.
Doubleclicking with the left mouse button will open the partition.
Clicking with the right mouse button on a partition will offer to extract or to open the partition.
The menu button "Extract all partitions" will extract all partitions by their name into separate files.

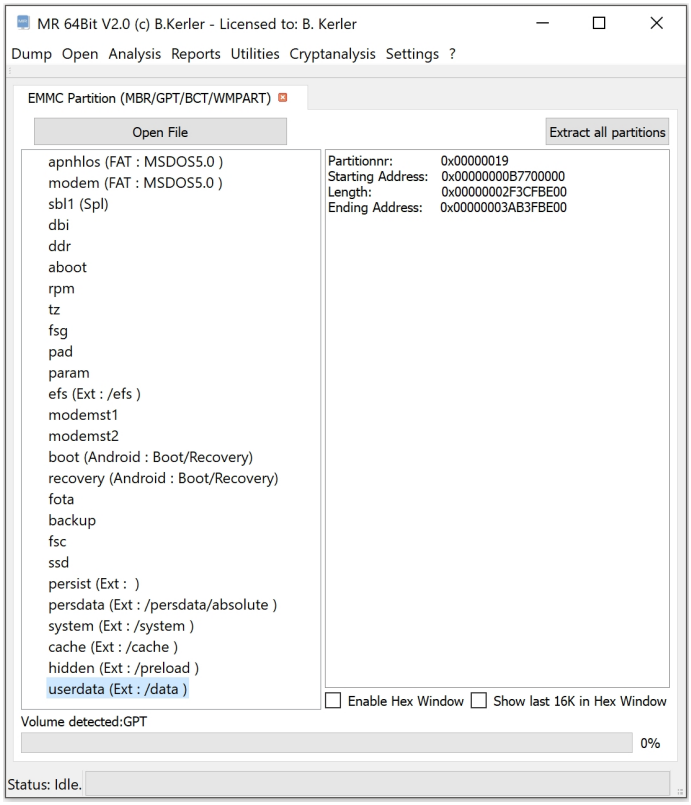
If no known Partitiontypes have been found, MR will offer an option to carve for FAT and/or EXT partitions.

Partitions



The partitions menu helps you extracting and viewing several flash dumps from modern devices using EMMC flash chips.

EMMC Partition (MBR/GPT/BCT/WMPART)

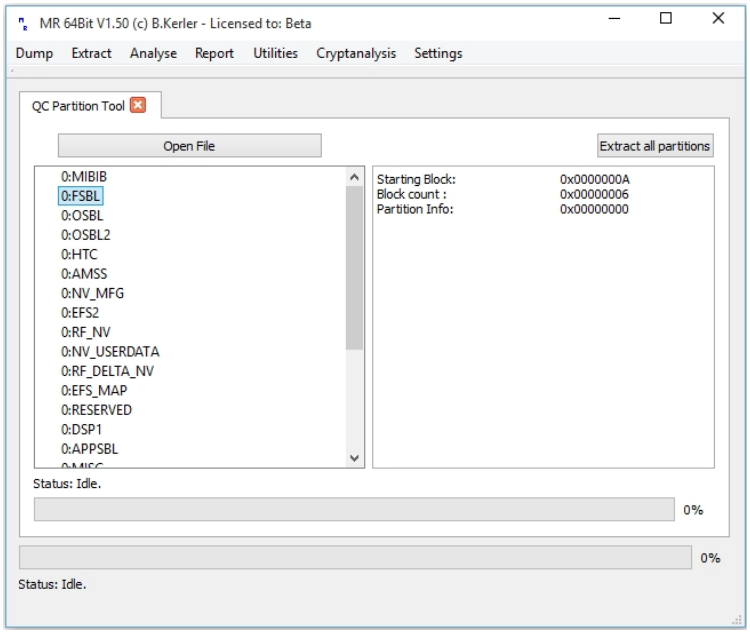


Using "Open File" you may open any raw flash binary file. If a known Partitiontype is detected, which may be MBR, GPT, BCT and WM7 it will show all including partitions.

Clicking with the left mouse button on a partition entry will reveal its attributes.
Doubleclicking with the left mouse button will open the partition.
Clicking with the right mouse button on a partition will offer to extract or to open the partition.
The menu button "Extract all partitions" will extract all partitions by their name into separate files.

If no known Partitiontypes have been found, MR will offer an option to carve for FAT and/or EXT partitions.

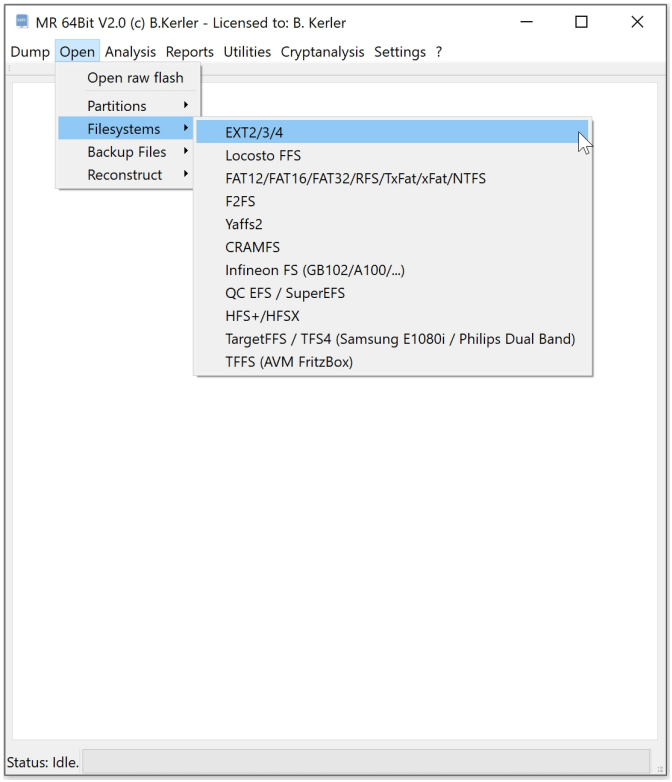
QC Partition



Using "Open File" you may open any raw flash binary file or qualcomm mbn file.

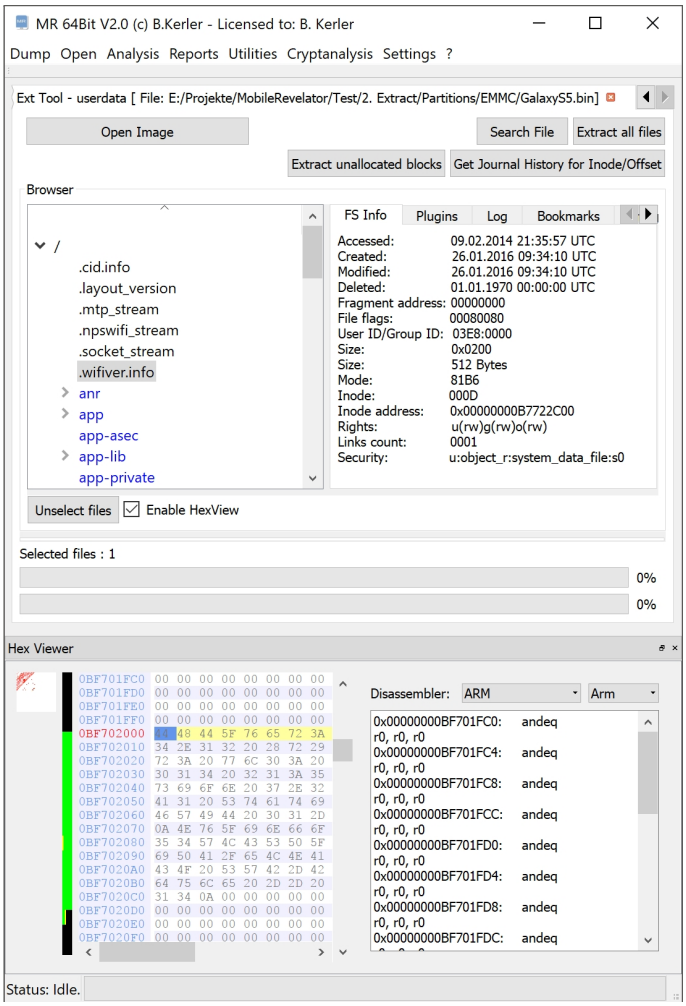
Clicking with the left mouse button on a partition entry will reveal its attributes.
The menu button "Extract all partitions" will try to extract all partitions by their name into separate files.

Filesystems



The filesystems menu offers several interpreters for many partition types.

Generic



All filesystem modules have three different tabs :
1. FS Info : Shows the current filesystem information
2. Plugins : Allows to run custom python scripts
3. Log : Logs all user actions within the filesystem tab
4. Bookmark : Press Ctrl-B with selected files to bookmark or select any entry in the bookmark list and press del key to remove the entry.
5. Image Preview: On enabling Image Preview when clicking any file, pictures will be displayed and can be rotated (alt-r, alt-l), scaled (ctrl-,ctrl+), etc. using the right-click button on the picture.

You can enable the Hex Viewer by clicking "Enable HexView" and separate/combine the Hex Viewer from main window by double-clicking the Hex Viewer Titlebar.

Doubleclicking on a file-entry will try to open up the file using associated programs.

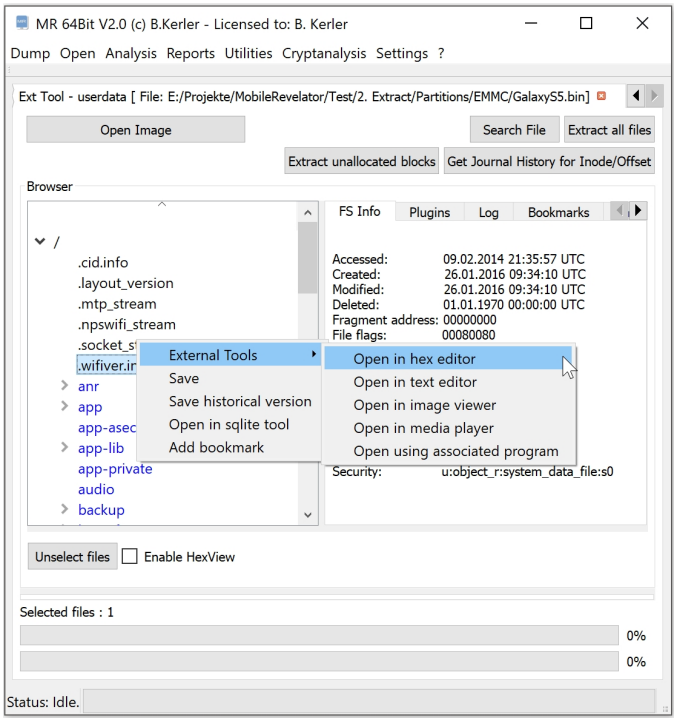
Plugins : you may select the main plugin to run all plugins and single plugins as well to just run one plugin.

Log : you may save the log at any time by pressing the "Save Log" button.

Specific

This topic takes care about all specific filesystem modules MR has.

EXT2/3/4



Using "Open Image" you may open any ext2/3/4 partition file/raw file.

Clicking with the left mouse button on a file will reveal its attributes.
Clicking with the right mouse button on a file will show a menu, which features different options :

- External Tools :
  This menu option lets you open you the selected file in a Hex Editor, Text Editor, Image Viewer, Media Player or any associated
  program in the OS. On first run, you must set the application paths in the "Settings"-Main Menu to point to executables.

- Save :
  This menu option will save all selected files. In order to select multiple files, just keep Ctrl-Key on your keyboard pressed while
  selecting files using the left mouse button.

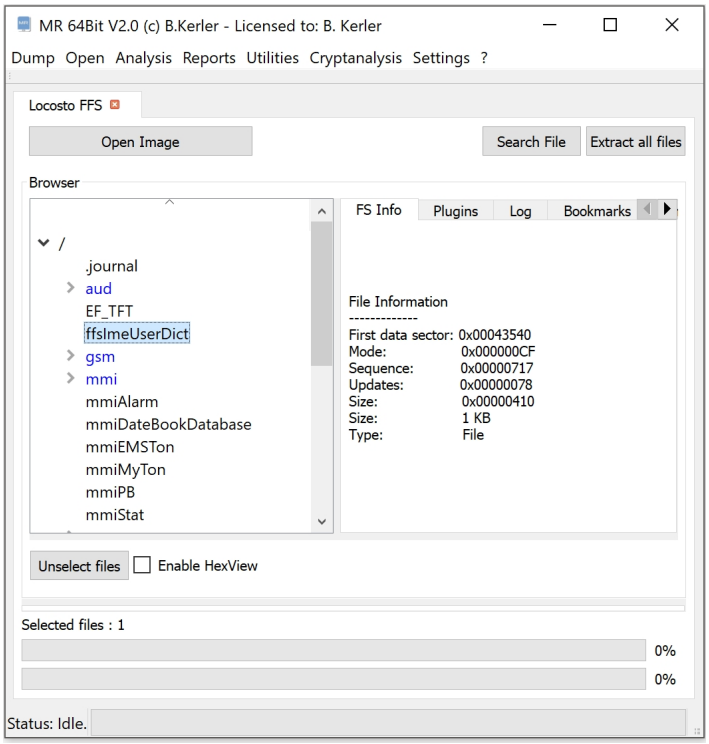
- Save historical version :
  This menu option will seek for journal entries for the selected files, and lets you choose to extract a different version by timestamp.

- Open in sqlite tool :
  This menu will open the selected file into the MR internal Sqlite Editor.

The menu button "Extract all files" will extract all files to a given directory, and will also write a log file to its parent directory.
The menu button "Extract unallocated blocks" will extract all blocks that aren't in use of the filesystem.
The menu button "Get Journal History for given Inode/Offset" will show any journal history entry for any inode or physical data offset.
The menu button "Search" lets you search for any filename and will present a table with all entries found. Clicking using the left mouse button on the entry will point directly to the entry in the filesystem.

Clicking on "Enable HexView" will show the first data sector of the selected file or directory entry/inode.

Locosto FFS



Using "Open Image" you may open any TI locosto chipset based FFS flash image.

Clicking with the left mouse button on a file will reveal its attributes.
Clicking with the right mouse button on a file will show a menu, which features different options :

- External Tools :
  This menu option lets you open you the selected file in a Hex Editor, Text Editor, Image Viewer, Media Player or any associated
  program in the OS. On first run, you must set the application paths in the "Settings"-Main Menu to point to executables

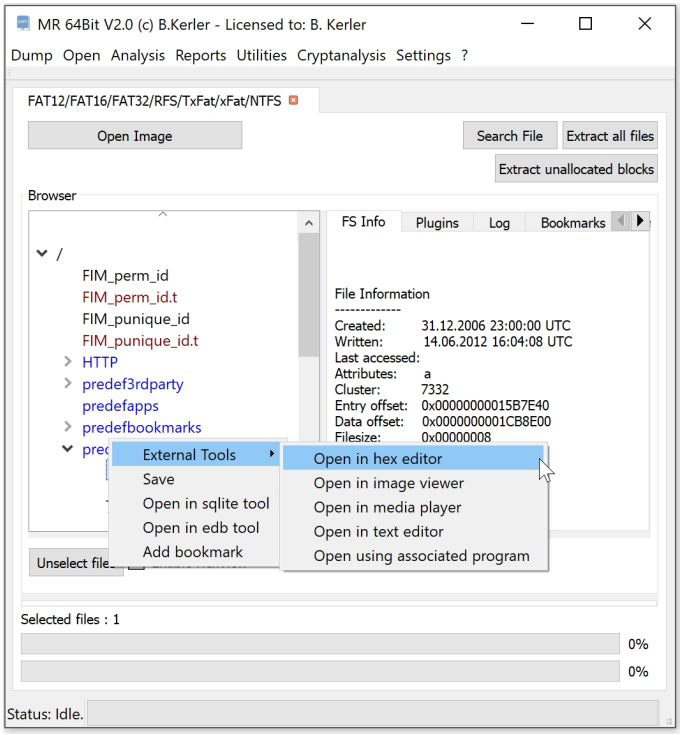
- Save :
  This menu option will save all selected files. In order to select multiple files, just keep Ctrl-Key on your keyboard pressed while
  selecting files using the left mouse button.

- Open in sqlite tool :
  This menu will open the selected file into the MR internal Sqlite Editor.

The menu button "Extract all files" will extract all files to a given directory, and will also write a log file to its parent directory.
The menu button "Search" lets you search for any filename and will present a table with all entries found. Clicking using the left mouse button on the entry will point directly to the entry in the filesystem.

Clicking on "Enable HexView" will show the first data sector of the selected file or directory entry/inode.

FAT12/FAT16/FAT32/RFS/TxFat/xFat/NTFS



Using "Open Image" you may open any Fat12/Fat16/Fat32/NTFS/RFS/ExFat/Transactioned ExFat partition file/raw file.

Clicking with the left mouse button on a file will reveal its attributes.
Clicking with the right mouse button on a file will show a menu, which features different options :

- External Tools :
  This menu option lets you open you the selected file in a Hex Editor, Text Editor, Image Viewer, Media Player or any associated
  program in the OS. On first run, you must set the application paths in the "Settings"-Main Menu to point to executables

- Save :
  This menu option will save all selected files. In order to select multiple files, just keep Ctrl-Key on your keyboard pressed while
  selecting files using the left mouse button.

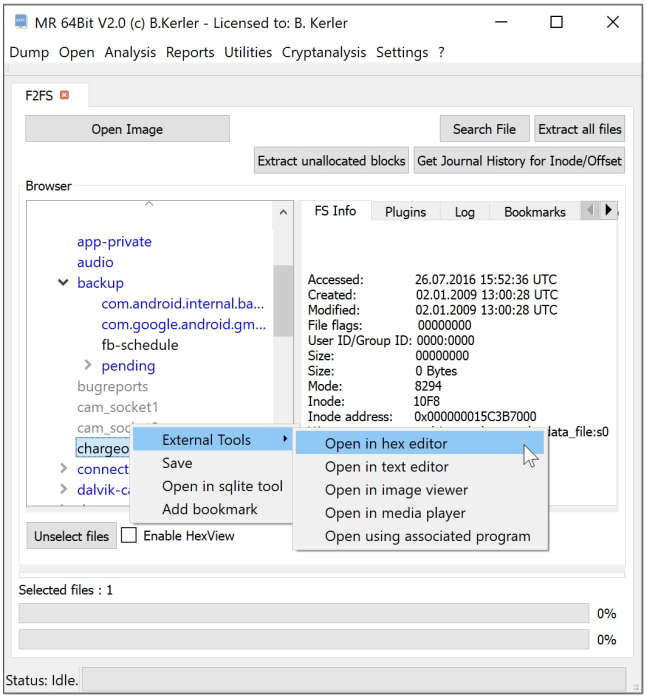
- Open in sqlite tool :
  This menu will open the selected file into the MR internal Sqlite Editor.

- Open in edb tool :
  This menu will open the selected file into the MR internal WP7 EDB Database Viewer.

The menu button "Extract all files" will extract all files to a given directory, and will also write a log file to its parent directory.
The menu button "Extract unallocated blocks" will extract all blocks that aren't in use of the filesystem.
The menu button "Search" lets you search for any filename and will present a table with all entries found. Clicking using the left mouse button on the entry will point directly to the entry in the filesystem.

Clicking on "Enable HexView" will show the first data sector of the selected file or directory entry/inode.

F2FS



Using "Open Image" you may open any f2fs partition file/raw file.

Clicking with the left mouse button on a file will reveal its attributes.
Clicking with the right mouse button on a file will show a menu, which features different options :

- External Tools :
  This menu option lets you open you the selected file in a Hex Editor, Text Editor, Image Viewer, Media Player or any associated
  program in the OS. On first run, you must set the application paths in the "Settings"-Main Menu to point to executables.

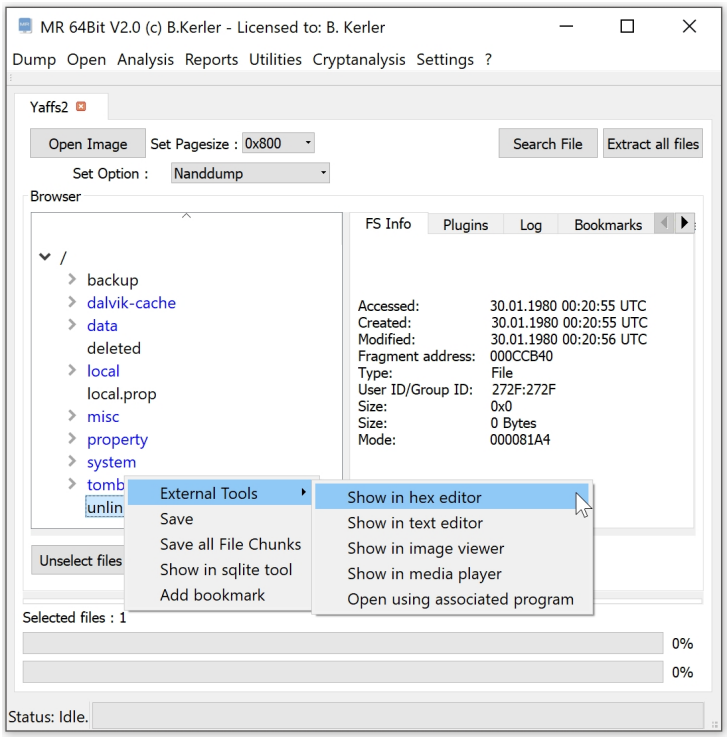
- Save :
  This menu option will save all selected files. In order to select multiple files, just keep Ctrl-Key on your keyboard pressed while
  selecting files using the left mouse button.

- Open in sqlite tool :
  This menu will open the selected file into the MR internal Sqlite Editor.

The menu button "Extract all files" will extract all files to a given directory, and will also write a log file to its parent directory.
The menu button "Extract unallocated blocks" will extract all blocks that aren't in use of the filesystem.
The menu button "Search" lets you search for any filename and will present a table with all entries found. Clicking using the left mouse button on the entry will point directly to the entry in the filesystem.

Clicking on "Enable HexView" will show the first data sector of the selected file or directory entry/inode.

Yaffs2



Using "Open Image" you may open any Yaffs2 partition file/raw file. In order to extract Yaffs2 partitions, you will need the according spare bytes from the Flash arranged by page/spare/page/spare/... Select the appropriate spare order by choosing "Generic/Mk2yaffs" or "Nanddump" and its pagesize, which may be 0x200, 0x400, 0x800 (default) and 0x1000.

Clicking with the left mouse button on a file will reveal its attributes.
Clicking with the right mouse button on a file will show a menu, which features different options :

- External Tools :
  This menu option lets you open you the selected file in a Hex Editor, Text Editor, Image Viewer, Media Player or any associated program in the OS. On first run, you must set the application paths in the "Settings"-Main Menu to point to executables

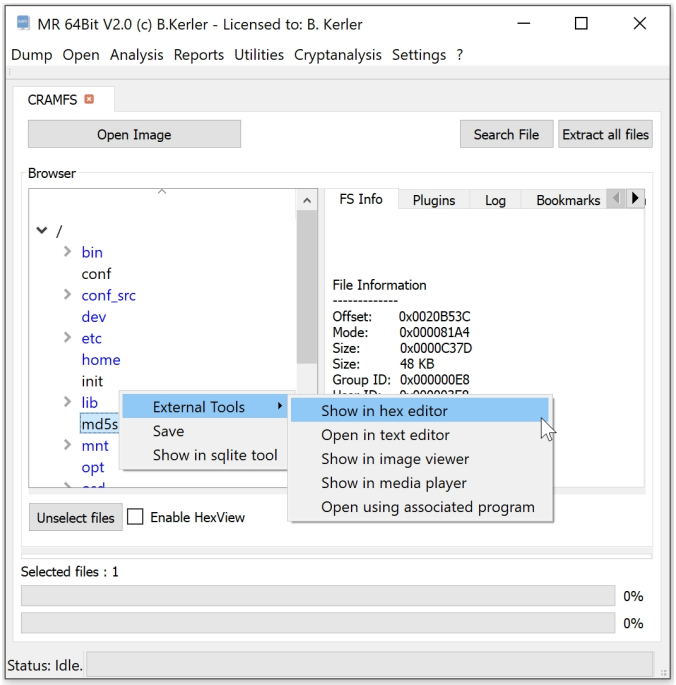
- Save :
  This menu option will save all selected files. In order to select multiple files, just keep Ctrl-Key on your keyboard pressed while selecting files using the left mouse button.

- Open in sqlite tool :
  This menu will open the selected file into the MR internal Sqlite Editor.

The menu button "Extract all files" will extract all files to a given directory, and will also write a log file to its parent directory.
The menu button "Extract unallocated blocks" will extract all blocks that aren't in use of the filesystem.
The menu button "Get Journal History for given Inode/Offset" will show any journal history entry for any inode or physical data offset.
The menu button "Search" lets you search for any filename and will present a table with all entries found. Clicking using the left mouse button on the entry will
point directly to the entry in the filesystem.

Clicking on "Enable HexView" will show the first data sector of the selected file or directory entry/inode.

CRAMFS



Using "Open Image" you may open any Compressed ROM flash image, indicated by "Compressed ROMFS" at the start of the image.

Clicking with the left mouse button on a file will reveal its attributes.
Clicking with the right mouse button on a file will show a menu, which features different options :

- External Tools :
  This menu option lets you open you the selected file in a Hex Editor, Text Editor, Image Viewer, Media Player or any associated program in the OS. On first run, you must set the application paths in the "Settings"-Main Menu to point to executables

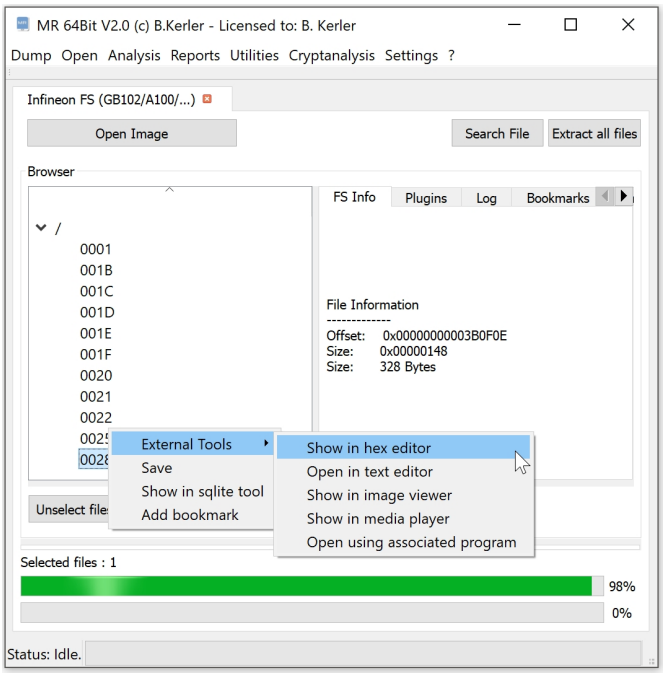
- Save :
  This menu option will save all selected files. In order to select multiple files, just keep Ctrl-Key on your keyboard pressed while selecting files using the left mouse button.

- Open in sqlite tool :
  This menu will open the selected file into the MR internal Sqlite Editor.

The menu button "Extract all files" will extract all files to a given directory, and will also write a log file to its parent directory.
The menu button "Search" lets you search for any filename and will present a table with all entries found. Clicking using the left mouse button on the entry will point directly to the entry in the filesystem.

Clicking on "Enable HexView" will show the first data sector of the selected file or directory entry/inode.

Infineon FS (GB102/A100/...)



Using "Open Image" you may open any Infineon chipset based flash image.

Clicking with the left mouse button on a file will reveal its attributes.
Clicking with the right mouse button on a file will show a menu, which features different options :

- External Tools :
  This menu option lets you open you the selected file in a Hex Editor, Text Editor, Image Viewer, Media Player or any associated
  program in the OS. On first run, you must set the application paths in the "Settings"-Main Menu to point to executables

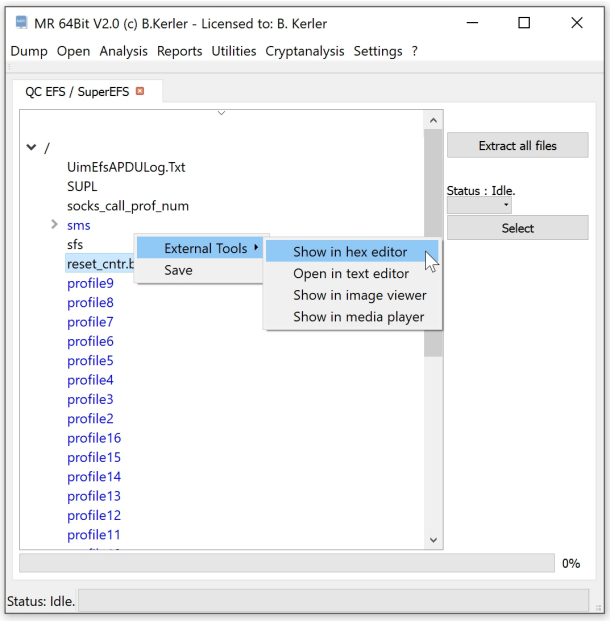
- Save :
  This menu option will save all selected files. In order to select multiple files, just keep Ctrl-Key on your keyboard pressed while selecting files using the left mouse button.

- Open in sqlite tool :
  This menu will open the selected file into the MR internal Sqlite Editor.

The menu button "Extract all files" will extract all files to a given directory, and will also write a log file to its parent directory.
The menu button "Search" lets you search for any filename and will present a table with all entries found. Clicking using the left mouse button on the entry will point directly to the entry in the filesystem.

Clicking on "Enable HexView" will show the first data sector of the selected file or directory entry/inode.

QC EFS / SuperEFS



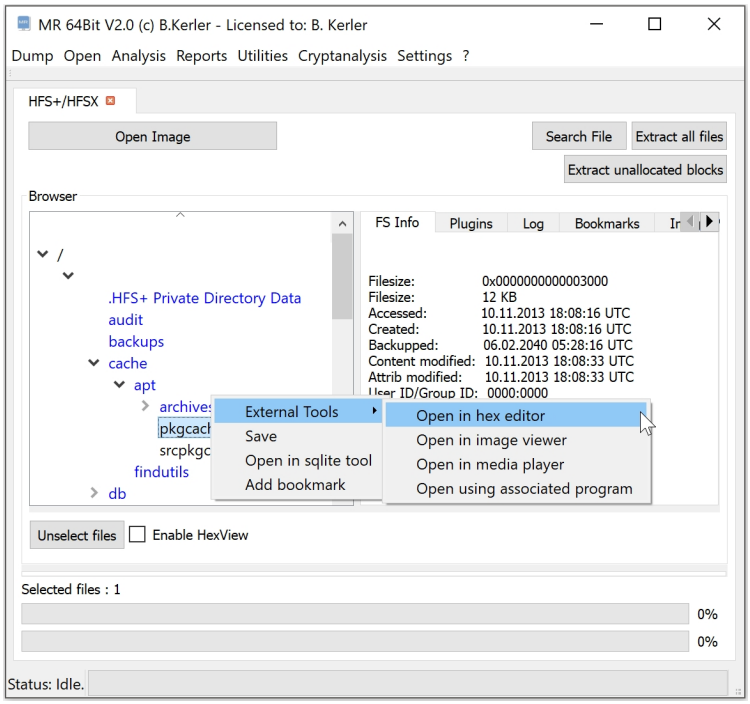
Using "Open Image" you may open any Qualcomm chipset based Embedded File System (EFS) image.
If the image contains older versions due to journaling, you may select the version just below the "Extract all files" button
.
Clicking with the left mouse button on a file will reveal its attributes.
Clicking with the right mouse button on a file will show a menu, which features different options :

- External Tools :
  This menu option lets you open you the selected file in a Hex Editor, Text Editor, Image Viewer, Media Player or any associated
  program in the OS. On first run, you must set the application paths in the "Settings"-Main Menu to point to executables

- Save :
  This menu option will save all selected files. In order to select multiple files, just keep Ctrl-Key on your keyboard pressed while selecting files using the left mouse button.

The menu button "Extract all files" will extract all files to a given directory, and will also write a log file to its parent directory.

HFS+/HFSX



Using "Open Image" you may open any HFS/HFS+/HFSX image.

Clicking with the left mouse button on a file will reveal its attributes.
Clicking with the right mouse button on a file will show a menu, which features different options :

- External Tools :
  This menu option lets you open you the selected file in a Hex Editor, Text Editor, Image Viewer, Media Player or any associated program in the OS. On first run, you must set the application paths in the "Settings"-Main Menu to point to executables

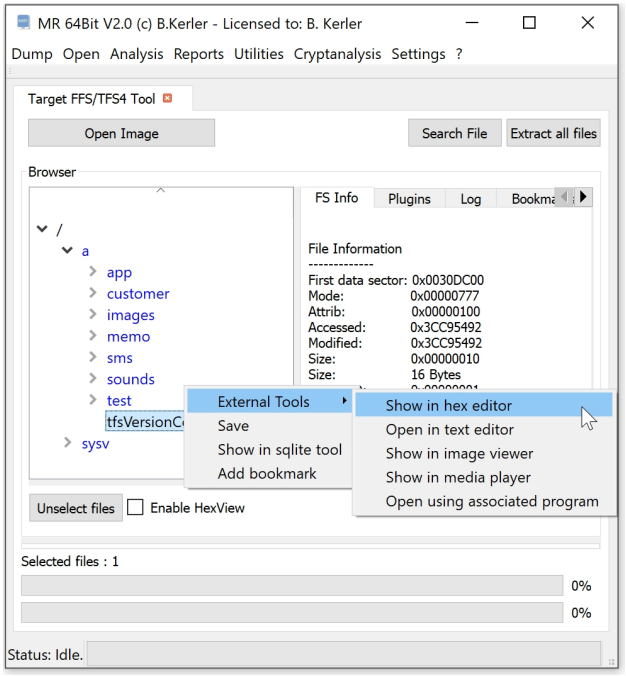
- Save :
  This menu option will save all selected files. In order to select multiple files, just keep Ctrl-Key on your keyboard pressed while
  selecting files using the left mouse button.

- Open in sqlite tool :
  This menu will open the selected file into the MR internal Sqlite Editor.

The menu button "Extract all files" will extract all files to a given directory, and will also write a log file to its parent directory.
The menu button "Search" lets you search for any filename and will present a table with all entries found. Clicking using the left mouse button on the entry will point directly to the entry in the filesystem.

Clicking on "Enable HexView" will show the first data sector of the selected file or directory entry/inode.

TargetFFS / TFS4 (Samsung E1080i / Philips Dual Band)



Using "Open Image" you may open any TargetFFS/TFS4 image.

Clicking with the left mouse button on a file will reveal its attributes.
Clicking with the right mouse button on a file will show a menu, which features different options :

- External Tools :
  This menu option lets you open you the selected file in a Hex Editor, Text Editor, Image Viewer, Media Player or any associated program in the OS. On first run, you must set the application paths in the "Settings"-Main Menu to point to executables

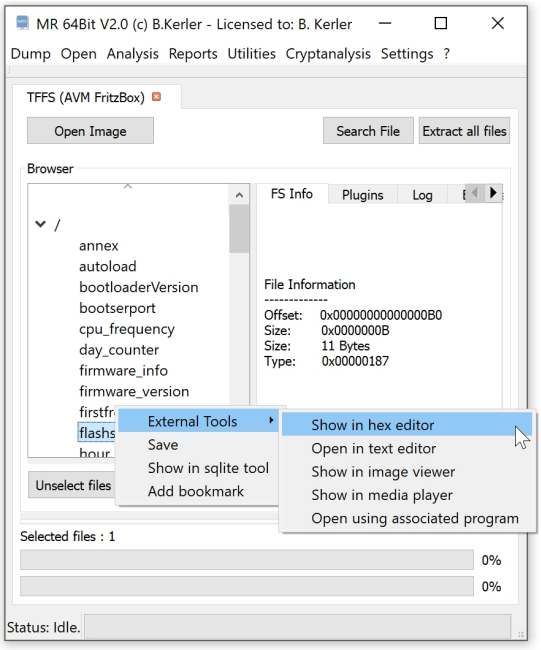
- Save :
  This menu option will save all selected files. In order to select multiple files, just keep Ctrl-Key on your keyboard pressed while selecting files using the left mouse button.

- Open in sqlite tool :
  This menu will open the selected file into the MR internal Sqlite Editor.

The menu button "Extract all files" will extract all files to a given directory, and will also write a log file to its parent directory.
The menu button "Search" lets you search for any filename and will present a table with all entries found. Clicking using the left mouse button on the entry will point directly to the entry in the filesystem.

Clicking on "Enable HexView" will show the first data sector of the selected file or directory entry/inode.

TFFS (AVM FritzBox)



Using "Open Image" you may open any TFFS AVM Fritzbox image. You cannot use RAW flash image, you need to extract the flash partitions from the RAW flash image first, starting with bytes "01 00 04 00 FF FF FE".

Clicking with the left mouse button on a file will reveal its attributes.
Clicking with the right mouse button on a file will show a menu, which features different options :

- External Tools :
  This menu option lets you open you the selected file in a Hex Editor, Text Editor, Image Viewer, Media Player or any associated program in the OS. On first run, you must set the application paths in the "Settings"-Main Menu to point to executables

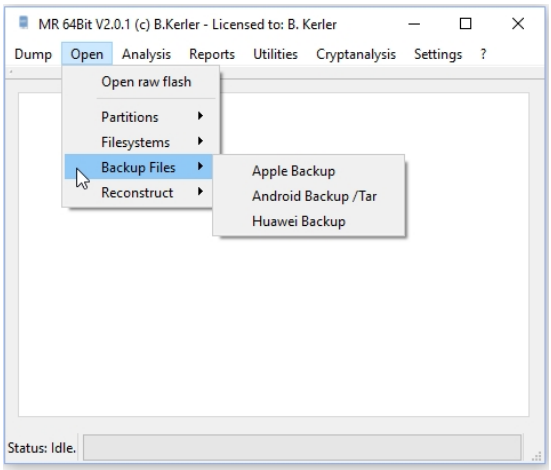
- Save :
  This menu option will save all selected files. In order to select multiple files, just keep Ctrl-Key on your keyboard pressed while selecting files using the left mouse button.

- Open in sqlite tool :
  This menu will open the selected file into the MR internal Sqlite Editor.

The menu button "Extract all files" will extract all files to a given directory, and will also write a log file to its parent directory.
The menu button "Search" lets you search for any filename and will present a table with all entries found. Clicking using the left mouse button on the entry will point directly to the entry in the filesystem.

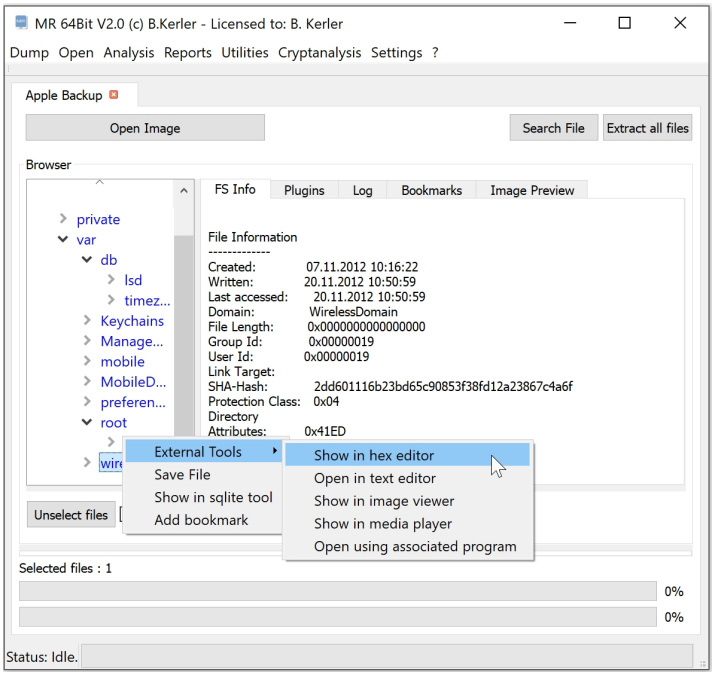
Clicking on "Enable HexView" will show the first data sector of the selected file or directory entry/inode.

Backup Files



The backup files menu offers functionality for viewing and extracting apple and android backup files.

Apple Backup



Using "Open Image" you may open any Apple iTunes backup file whether it may be encrypted or not. If the backup is encrypted,
it will ask for the password for decryption. On "Open Image", choose the appropriate "Manifest.mbdb" file.

Clicking with the left mouse button on a file will reveal its attributes.
Clicking with the right mouse button on a file will show a menu, which features different options :

- External Tools :
  This menu option lets you open you the selected file in a Hex Editor, Text Editor, Image Viewer, Media Player or any associated program in the OS. On first run, you must set the application paths in the "Settings"-Main Menu to point to executables.

- Save :
  This menu option will save all selected files. In order to select multiple files, just keep Ctrl-Key on your keyboard pressed while selecting files using the left mouse button.

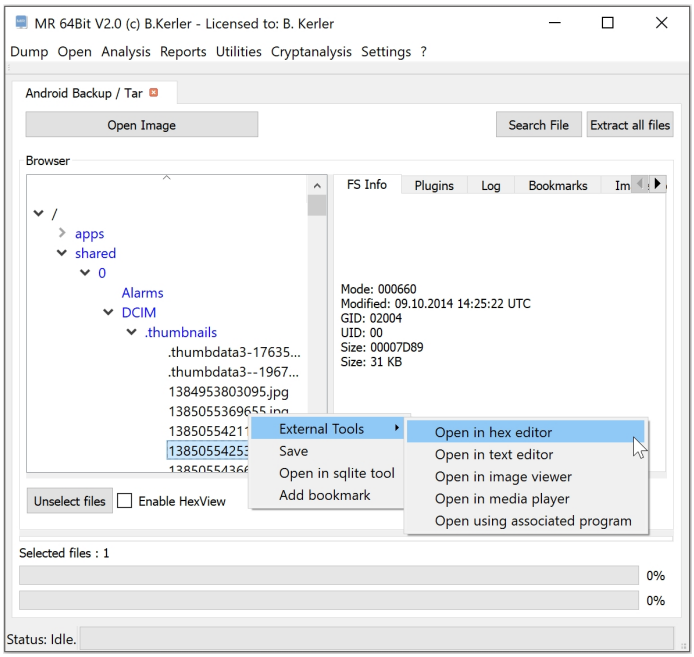
- Open in sqlite tool :
  This menu will open the selected file into the MR internal Sqlite Editor.

- Open in plist tool :
  This menu will open the selected file into the MR internal Apple PList Editor.

The menu button "Extract all files" will extract all files to a given directory, and will also write a log file to its parent directory.
The menu button "Search" lets you search for any filename and will present a table with all entries found. Clicking using the left mouse button on the entry will point directly to the entry in the filesystem.

Clicking on "Enable HexView" will show the first data sector of the selected file or directory entry/inode.

Android Backup / Tar



Using "Open Image" you may open any Android Backup "*.ab", Gzipped Tar or Tar file, whether it may be encrypted or not. If the backup is encrypted, it will ask for the password for decryption.

Clicking with the left mouse button on a file will reveal its attributes.
Clicking with the right mouse button on a file will show a menu, which features different options :

- External Tools :
  This menu option lets you open you the selected file in a Hex Editor, Text Editor, Image Viewer, Media Player or any associated program in the OS. On first run, you must set the application paths in the "Settings"-Main Menu to point to executables.

- Save :
  This menu option will save all selected files. In order to select multiple files, just keep Ctrl-Key on your keyboard pressed while selecting files using the left mouse button.

- Open in sqlite tool :
  This menu will open the selected file into the MR internal Sqlite Editor.

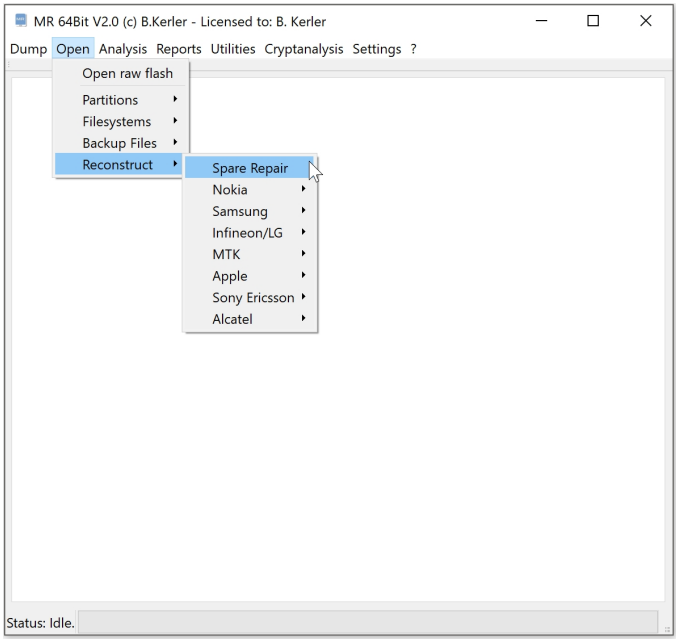
The menu button "Extract all files" will extract all files to a given directory, and will also write a log file to its parent directory.
The menu button "Search" lets you search for any filename and will present a table with all entries found. Clicking using the left mouse button on the entry will point directly to the entry in the filesystem.

Clicking on "Enable HexView" will show the first data sector of the selected file or directory entry/inode.

Huawei Backup

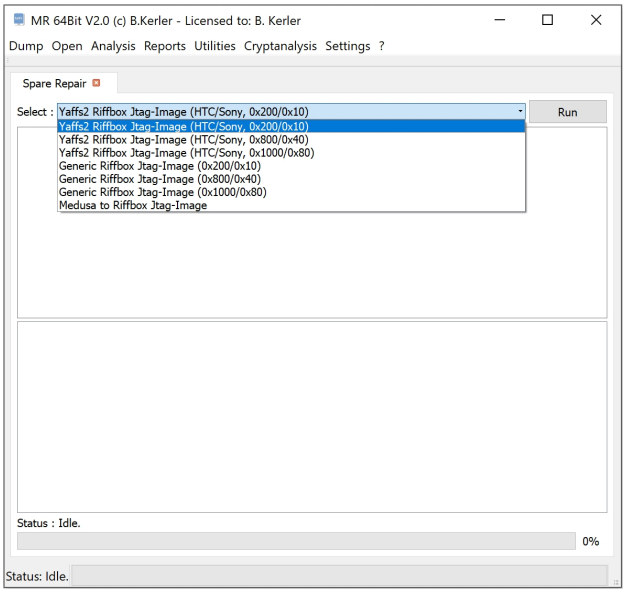
The Huawei Backup Tool offers a method to convert the sqlite database files and contents to a filesystem.
In order to do a full backup, in the smartphone go to Tools, Huawei Backup and store all data to an external sdcard or sdcard connected via otg cable.

Reconstruct



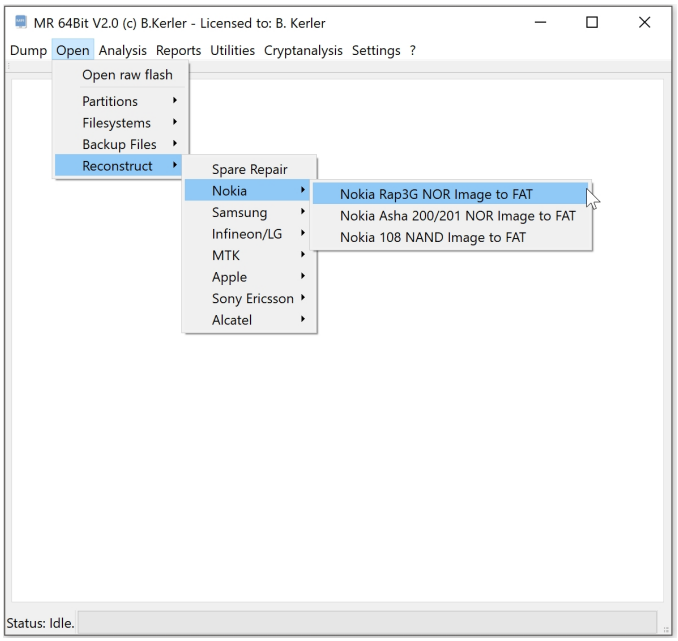
The Reconstruct menu offers functionality for reconstructing filesystems due to usage of wearleveling or flash transaction layers.

Spare Repair



The Spare Repair Tool will reorder spare areas from other Tools like RiffBox or MedusaBox to make the flash images being
used by the MR Tool correctly. It will sort the Spares from the end of the flash to the end of each page, where they should be.

Nokia



The Nokia tools offer specific functions for reconstruction wear-leveling for Nokia devices.

Nokia Rap3G NOR Image to FAT

This tool will extract the FAT partition from any Nokia Rap3G flash image.

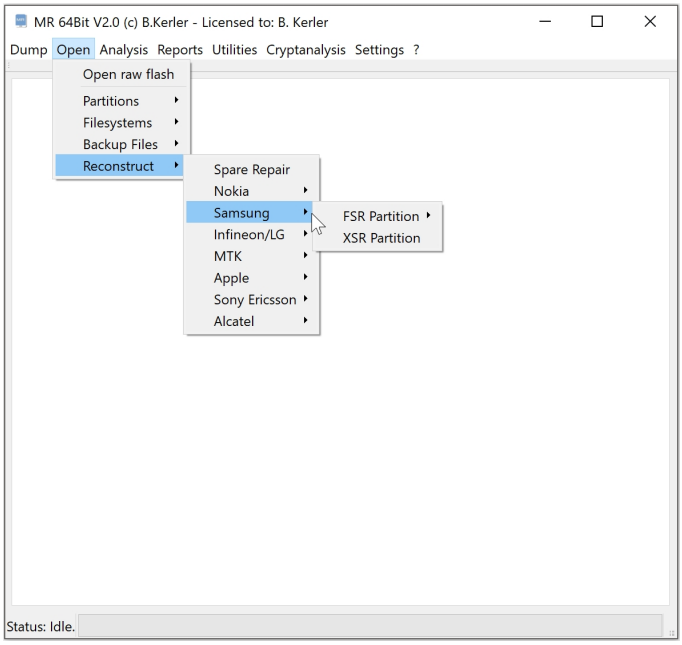
Nokia Asha 200/201 NOR Image to FAT

This tool will extract the FAT partition from any Nokia Asha 200/201 flash image.

Nokia 108 NAND Image to FAT

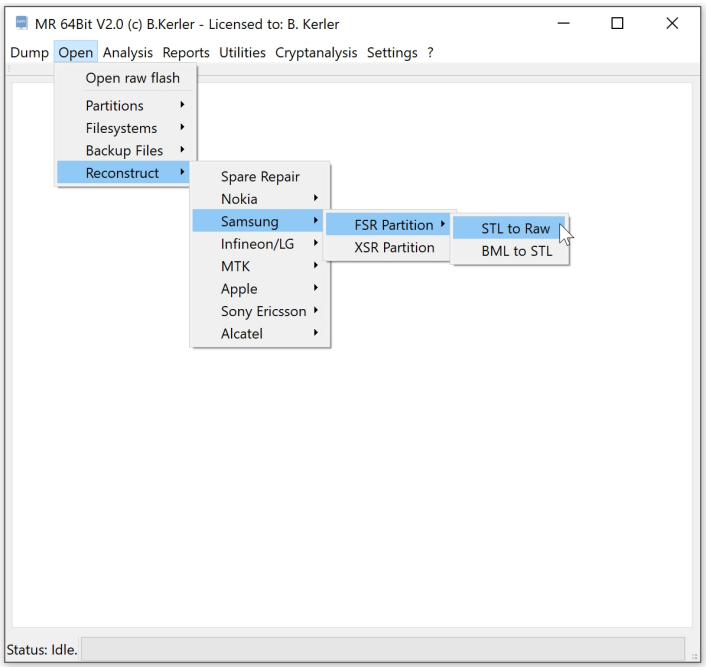
This tool will extract the FAT partition from any Nokia 108 flash image.

Samsung



The Samsung reconstruction tools will extract RAW Partitions, called BML and filesystems, called STL from Wear-Leveling as well will reconstruct any partitions from XSR1/2/3.

FSR Partition



The FSR partition is the RAW partition with Flash Transaction Layer by Samsung. BML is the main raw flash image with flash transaction layers consisting of several STL Partitions.

STL to Raw

This tool will extract any partition from wearleveling STL data flash image.

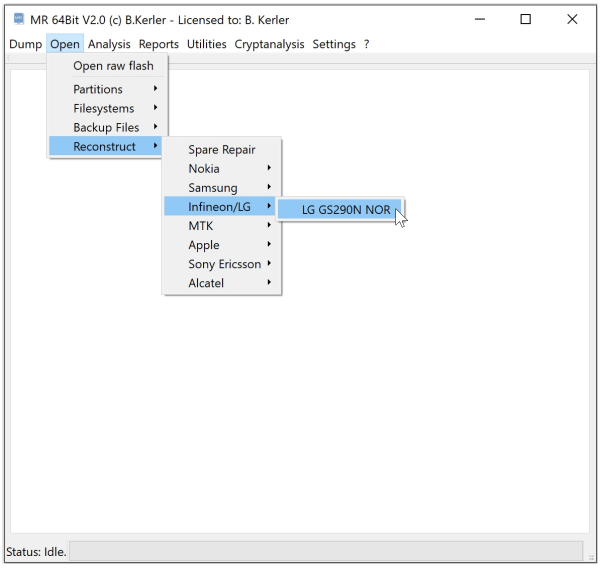
BML to STL

This tool will extract any STL partition from wearleveling BML data flash image.

XSR Partition

This tool will extract any partition from wearleveling XSR1/2/3 data flash image. It will automatically detect block and pagesize needed for extraction. In order to extract XSR partition data, spare data has to be at the end of each page.

Infineon/LG

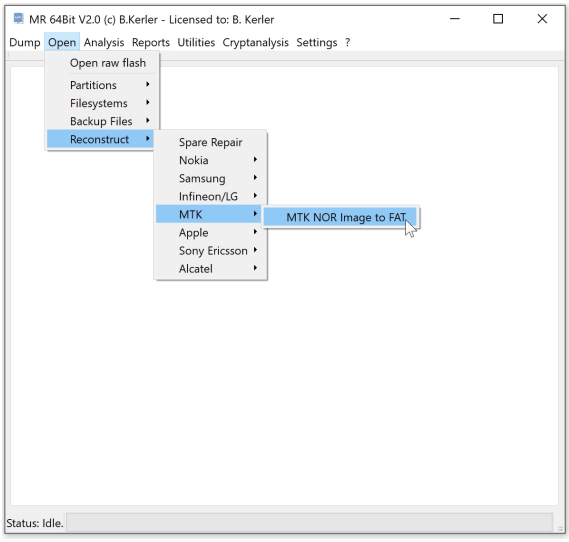


The Infineon tools offer specific functions for reconstruction wear-leveling for infineon devices.

LG GS290N NOR

This tool will extract any partition from wearleveling LG GS290N NOR data flash image.

MTK

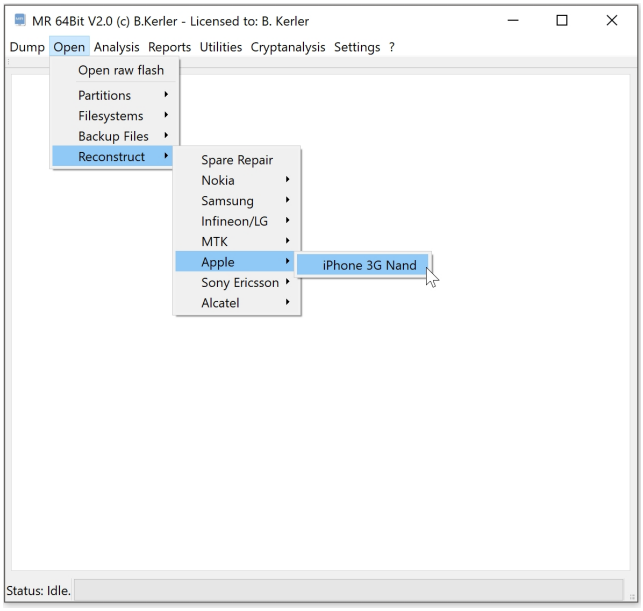


The MTK tools offer specific functions for reconstruction wear-leveling for MTK devices.

MTK NOR Image to FAT

This tool will extract any partition from wearleveling MTK NOR flash image.

Apple

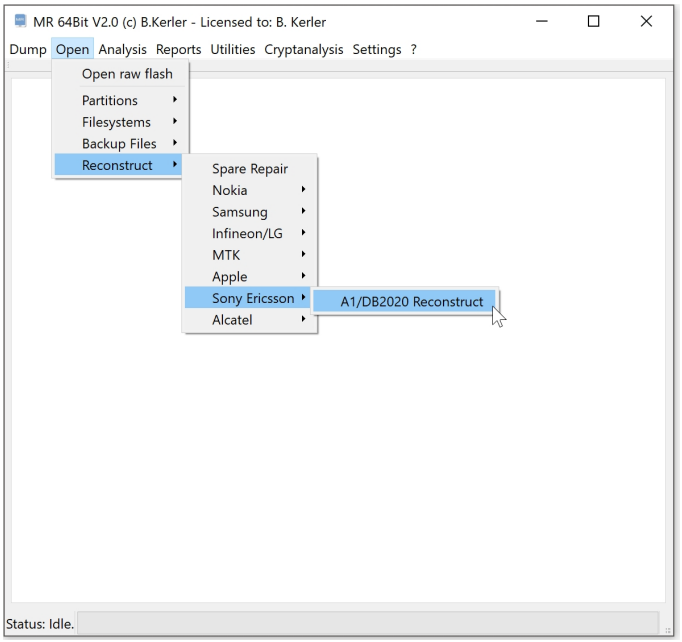


The Apple tools offer specific functions for reconstruction wear-leveling for Apple devices.

iPhone 3G Nand

This tool will extract any partition from wearleveling iPhone 3G nand data flash image. Spare data is needed for reconstruction
and should be at the end of each page.

Sony Ericsson

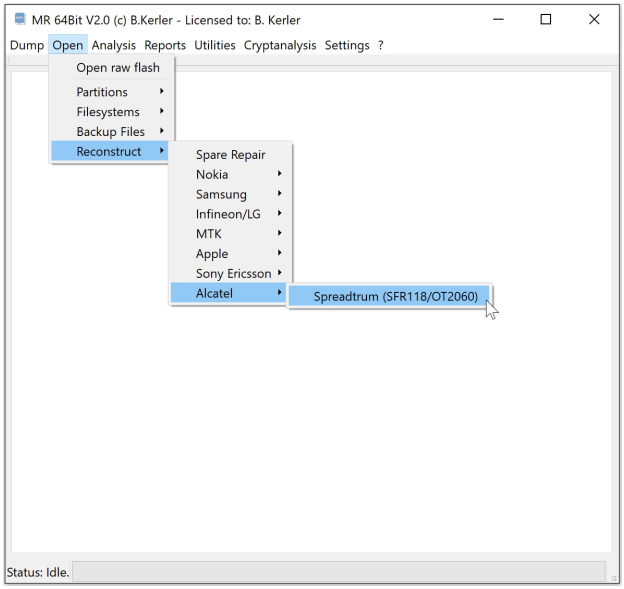


The Sony Ericsson tools offer specific functions for reconstruction wear-leveling for Sony Ericsson devices.

A1/DB2020 Reconstruct

This tool will extract any partition from wearleveling A1/DB2020 nand data flash image. Spare data is needed for reconstruction
and should be at the end of each page.

Alcatel

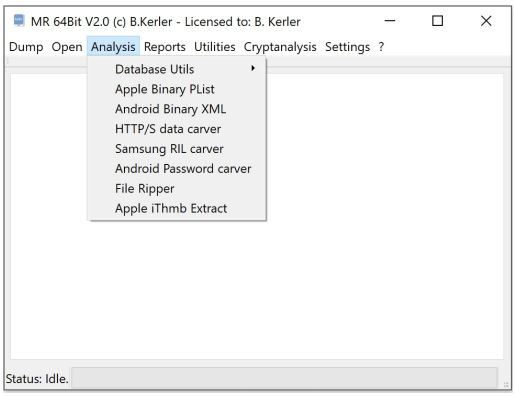


The Alcatel tools offer specific functions for reconstruction wear-leveling for Alcatel devices.

Spreadtrum (SFR118/OT2060)

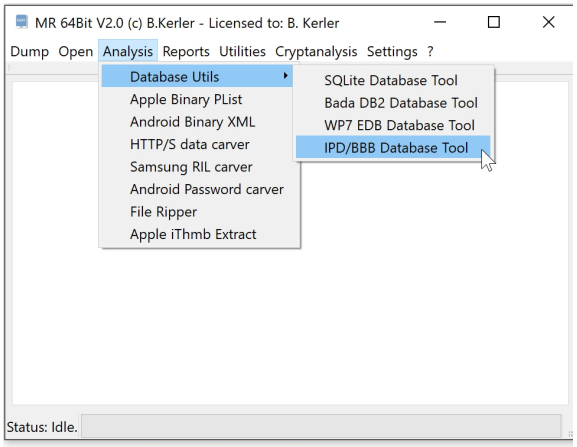
This tool will extract any partition from wearleveling Alcatel device with Spreadtrum chipset data flash image.

Analysis



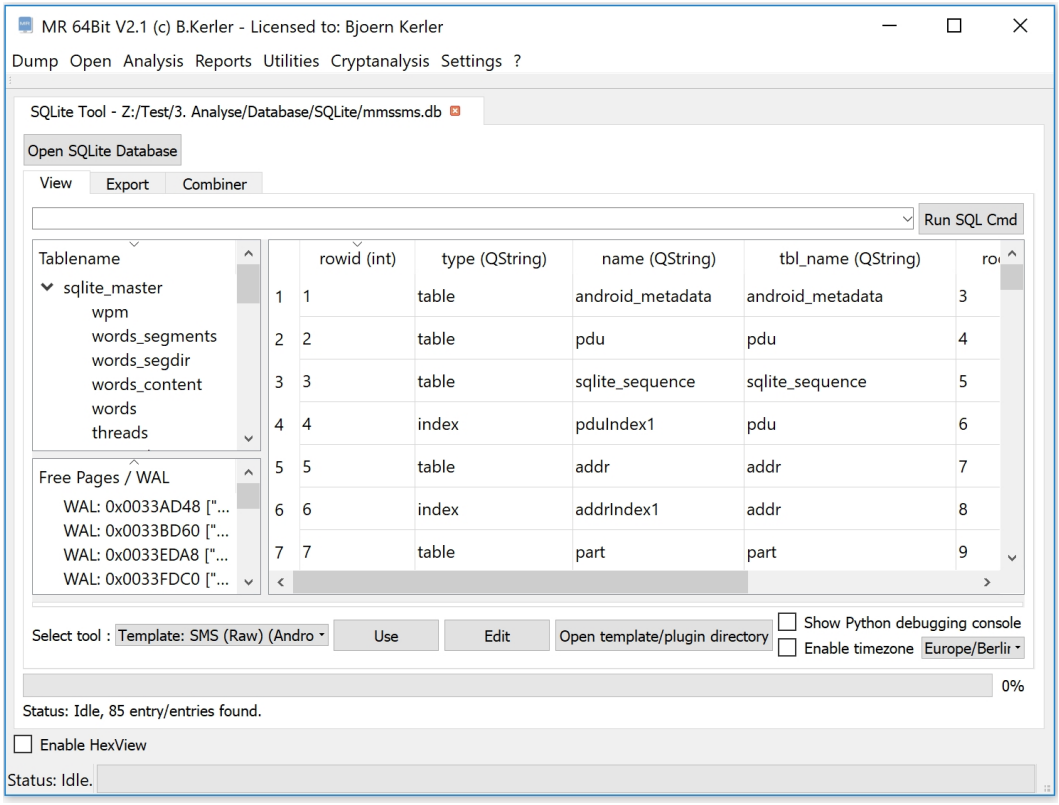
The Analyse menu contains several tools for interpretation of various data formats, such as databases, xml files but also has great tools for carving information from raw images or files.

Database Utils



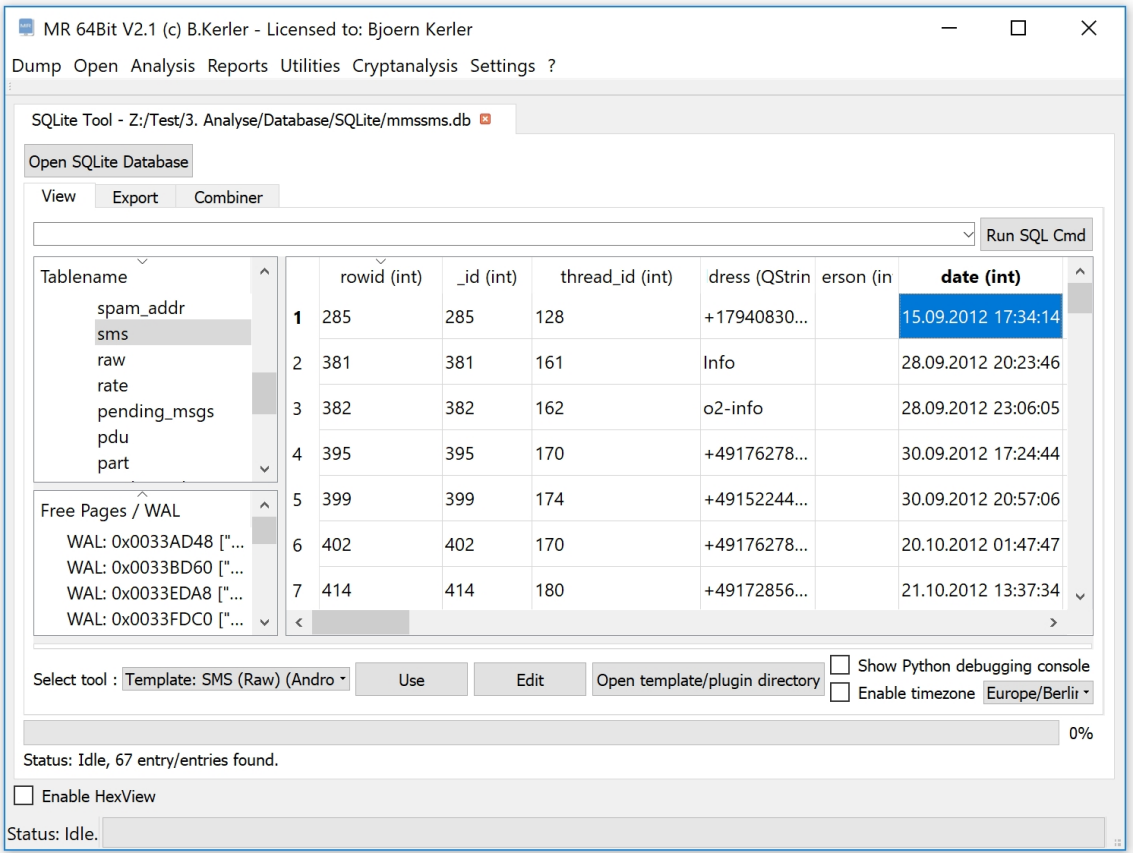
The SQLite Database Tools is able to open generic SQLite3 databases and enables to reconstruct wal (Write Ahead Logs), Journals and deleted SQLite entries from free pages.

SQLite Database Tool



The sqlite database tool lets you open sqlite database, recover deleted entries from free pages, journal and write-ahead-logs (WAL) and lets you convert timestamps in a user-friendly way. Moreover, you have the option to export the modified or current table to a xlsx, csv or xml-file.

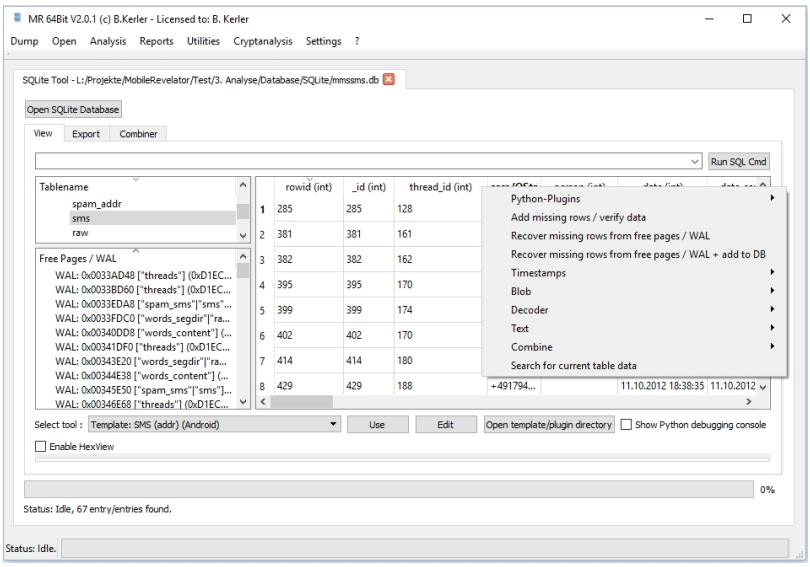
View



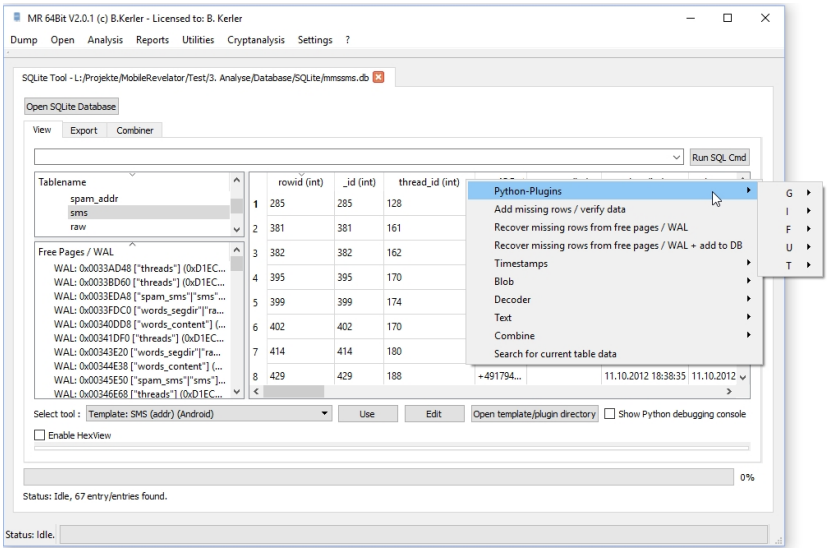
The windows is split into three different regions :
On the upper left side, you see the current tables from the database.
The lower left side, you see any deleted or active transactions according to free pages, journals or write-ahead log.
Selecting an entry from either the upper or lower left side, its content is being displayed on the right side.

Using Ctrl-F you can search for any string, clicking on an entry in the result tab will show the selected entry in the table.
Using Ctrl-T if an entry is selected will automatically try to convert the integer value to a readable date / timestamp value for the
whole column. Converted timestamps via Ctrl-T conversion can also be converted to a local time by choosing the location and by enabling the
"Enable timezone" checkbox.

Right-Click-Menu

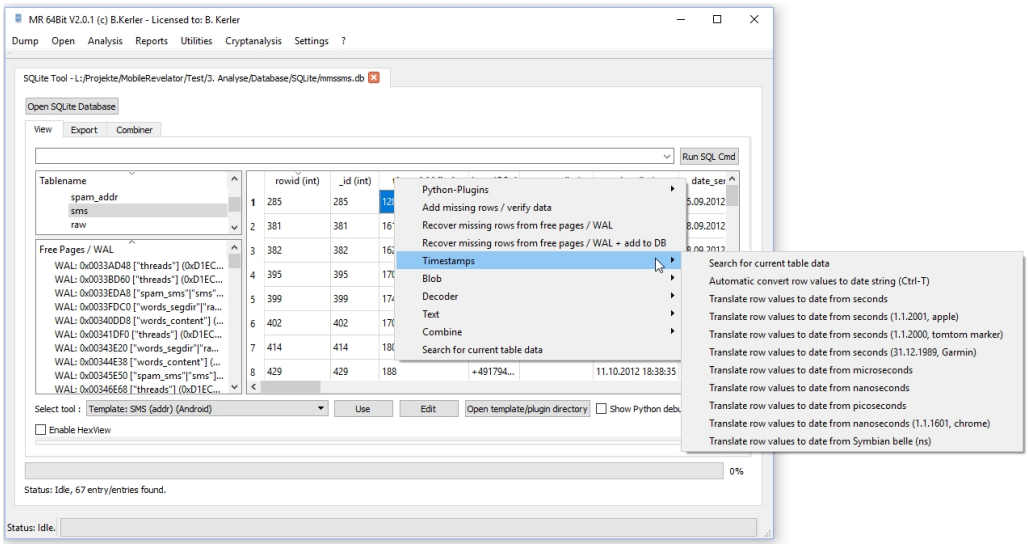


Python-Plugins



This menu lets you run custom python plugins.

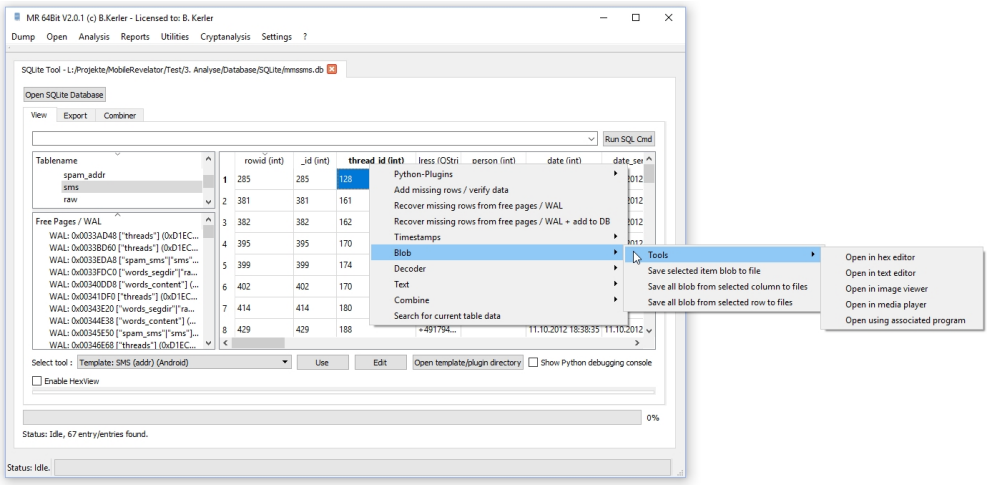
Timestamps



There are two ways to convert current column integer values to a time stamp :

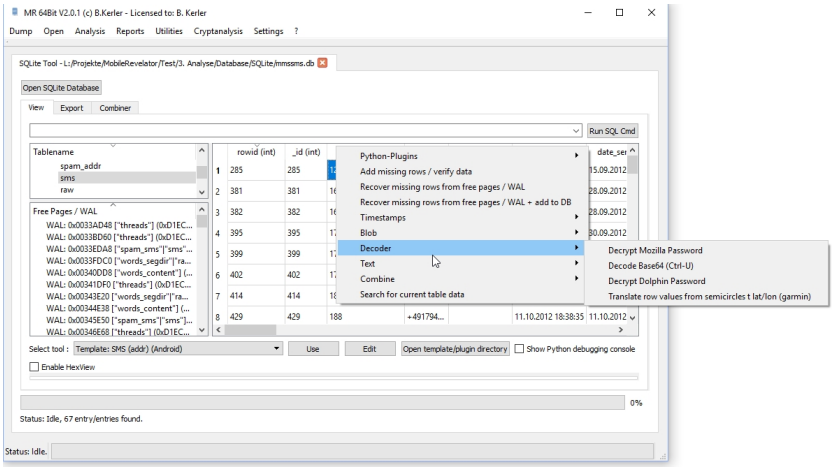
First one, try the automatic algorithm : select any column to be converted and press CTRL-T. If the conversion fails or seems to be wrong, choose the second one, by right clicking into the field, in the menu select "Timestamps" and the the appropriate timestamp. If the conversion doesn't seem to be fine, just reselect the table on the left side and the table will be reset, allowing you to reselect another timestamp method.

Blob



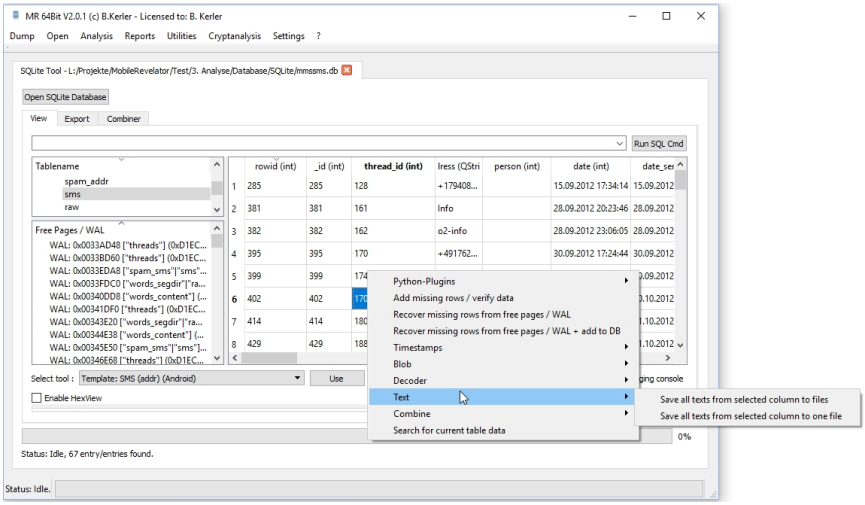
The blob menu lets you either use your favorite tool for viewing the data or save either the current data field or selected column or row data field to a file.

Decoder



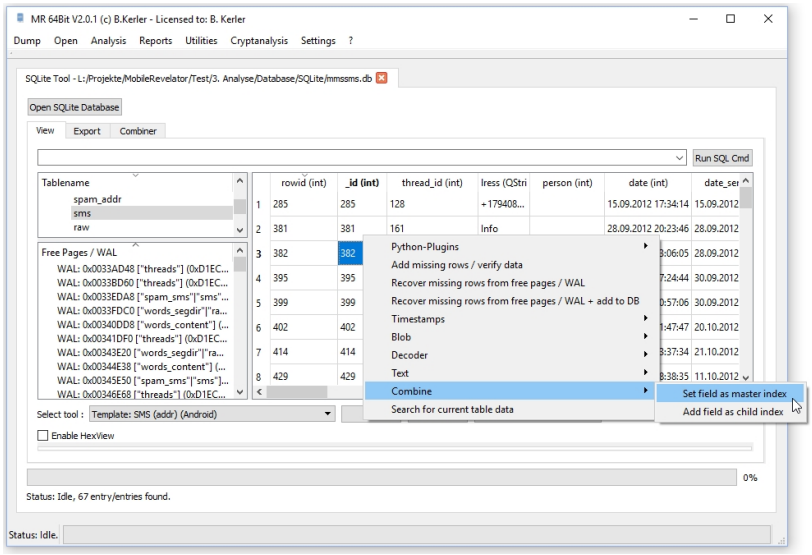
The decoder menu has functionality to convert garmin integer values to latitude/longitude, but will also allow to decrypt saved encrypted key4.db mozilla passwords.

Text



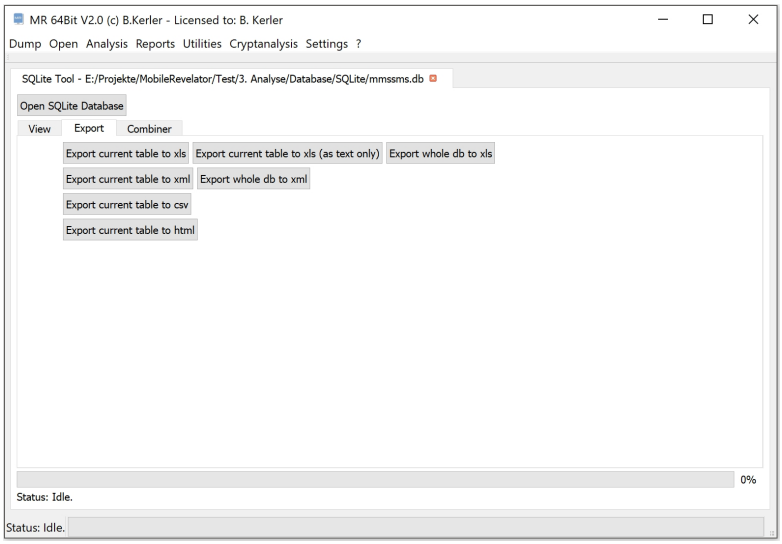
The text menu functions will extract all text within current selected column either as a file for each line or as multiple lines in one file.

Combine



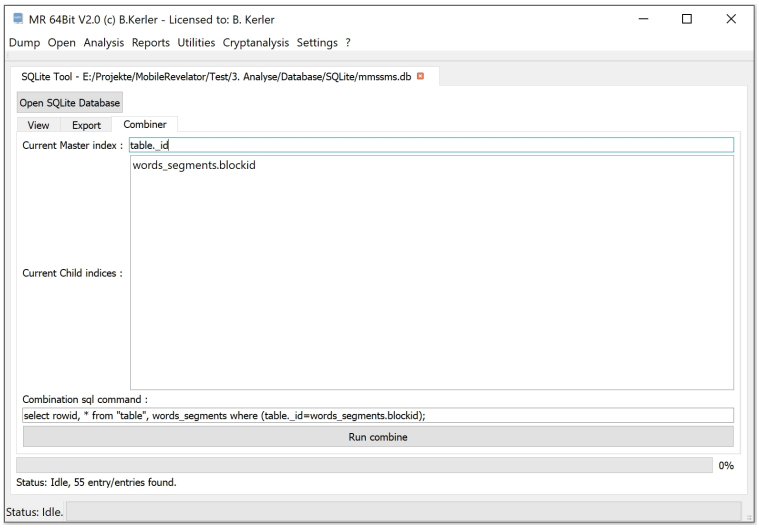
The combine menu lets you combine database entries. Just click into the column to be combined and then select the master index first, followed by child indices (columns) you want to combine from different tables.

Export



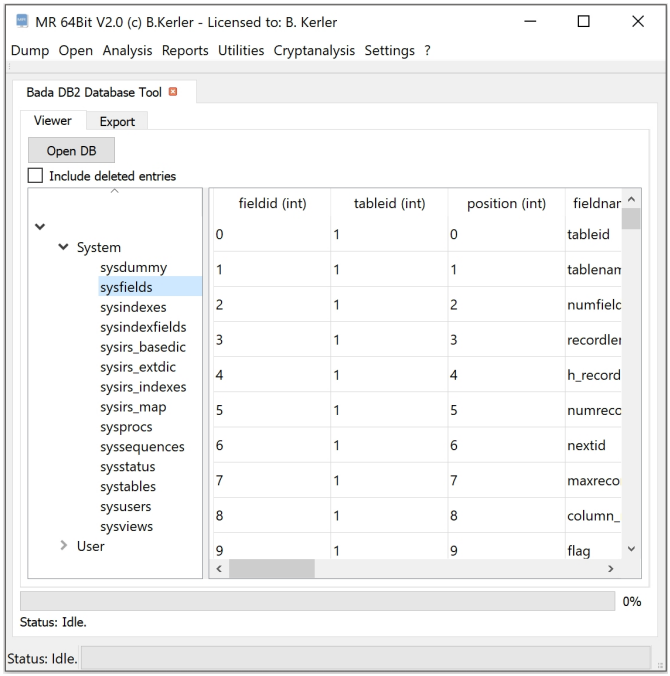
You may export the current table view either as a xlsx, xml or csv file or even the complete database (without changes being added). If any data columns may exist, the "Export current table to xls (as text only)" function will just export unicode text but will filter any data bytes.

Combine



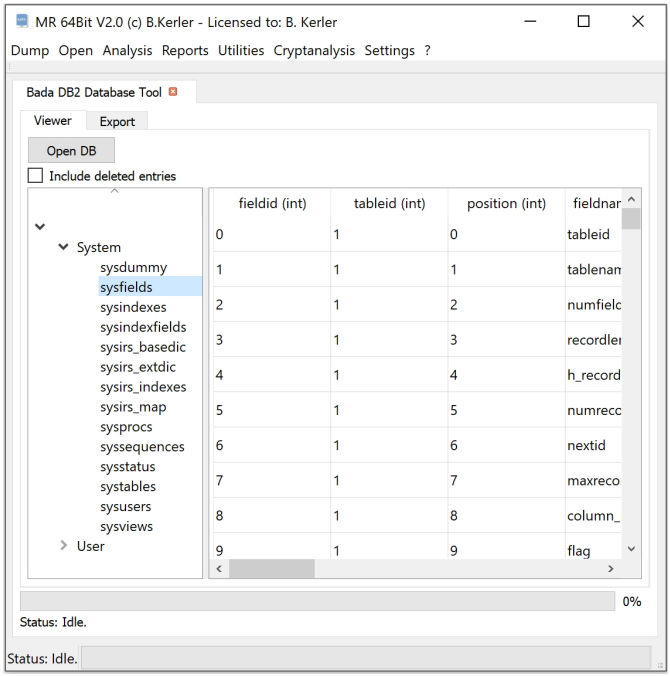
Once columns have been selected in the table view as main and child indexes, they will be displayed in the combine tab. You may delete single indices by selecting and pressing the del-key on the keyboard. Pressing the "Run combine" button will execute the sql query being displayed in the "Combination sql command" field.

Bada DB2 Database Tool



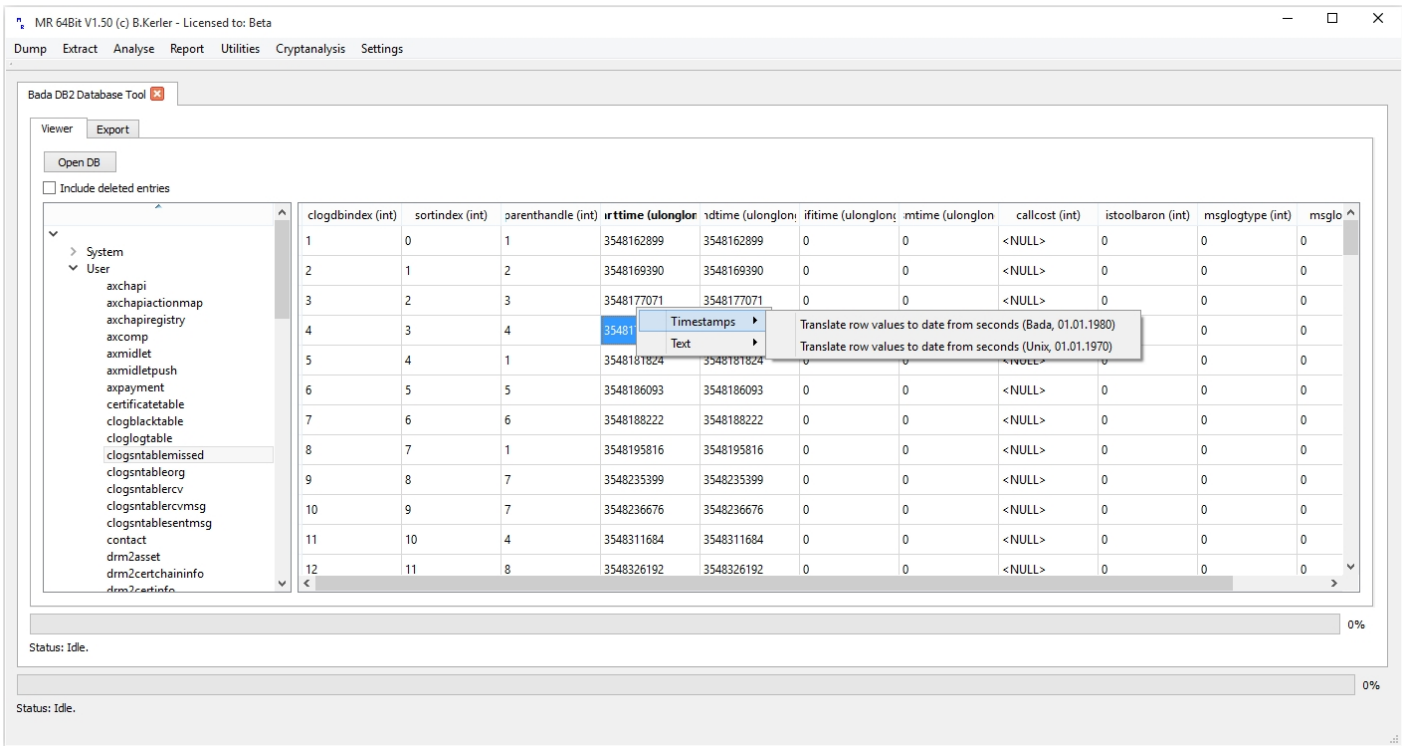
The bada DB2 database tool is able to open and read Samsung DB2 and EMware databases (mainly to be found on Samsung Bada based devices at /DB2/phonedb.00).

View

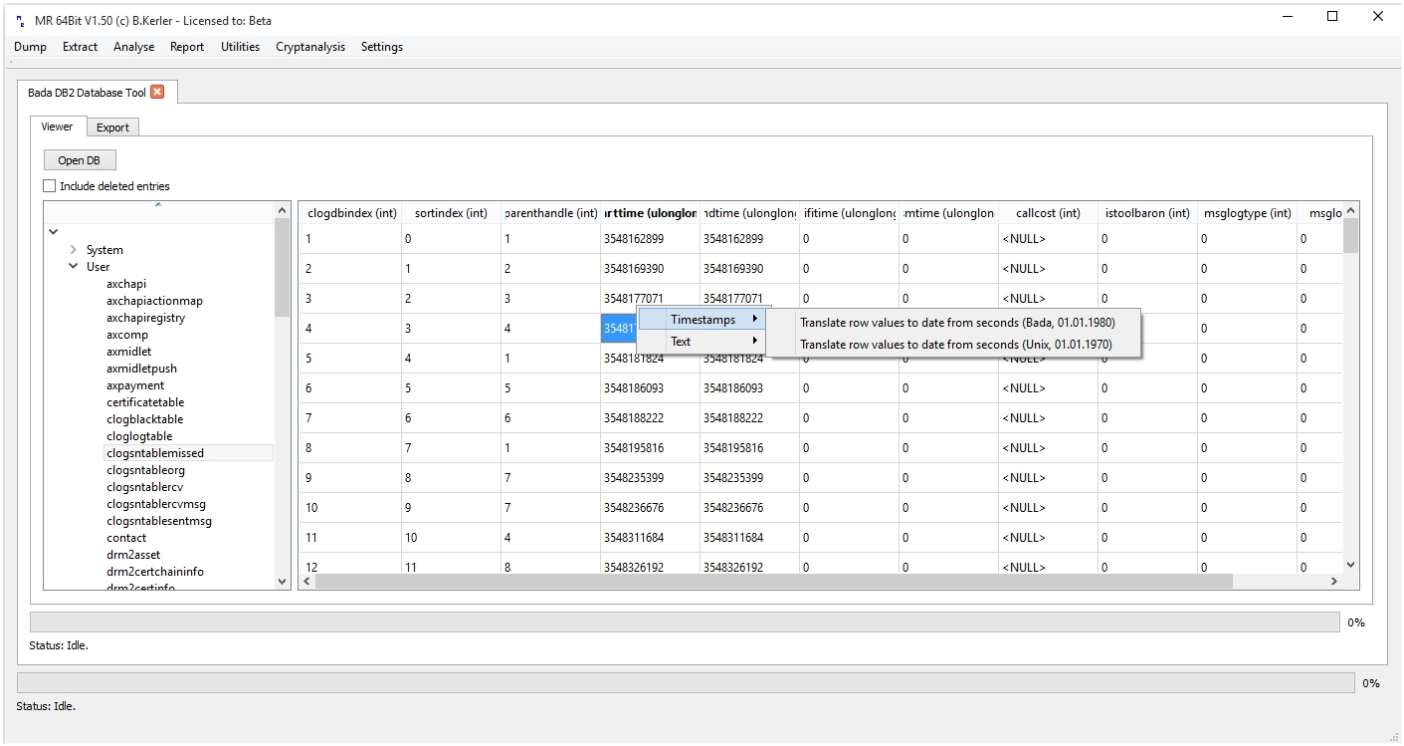


You may select "Include deleted entries" to show deleted entries while clicking at the Index at the left side.

Right-Click-Menu

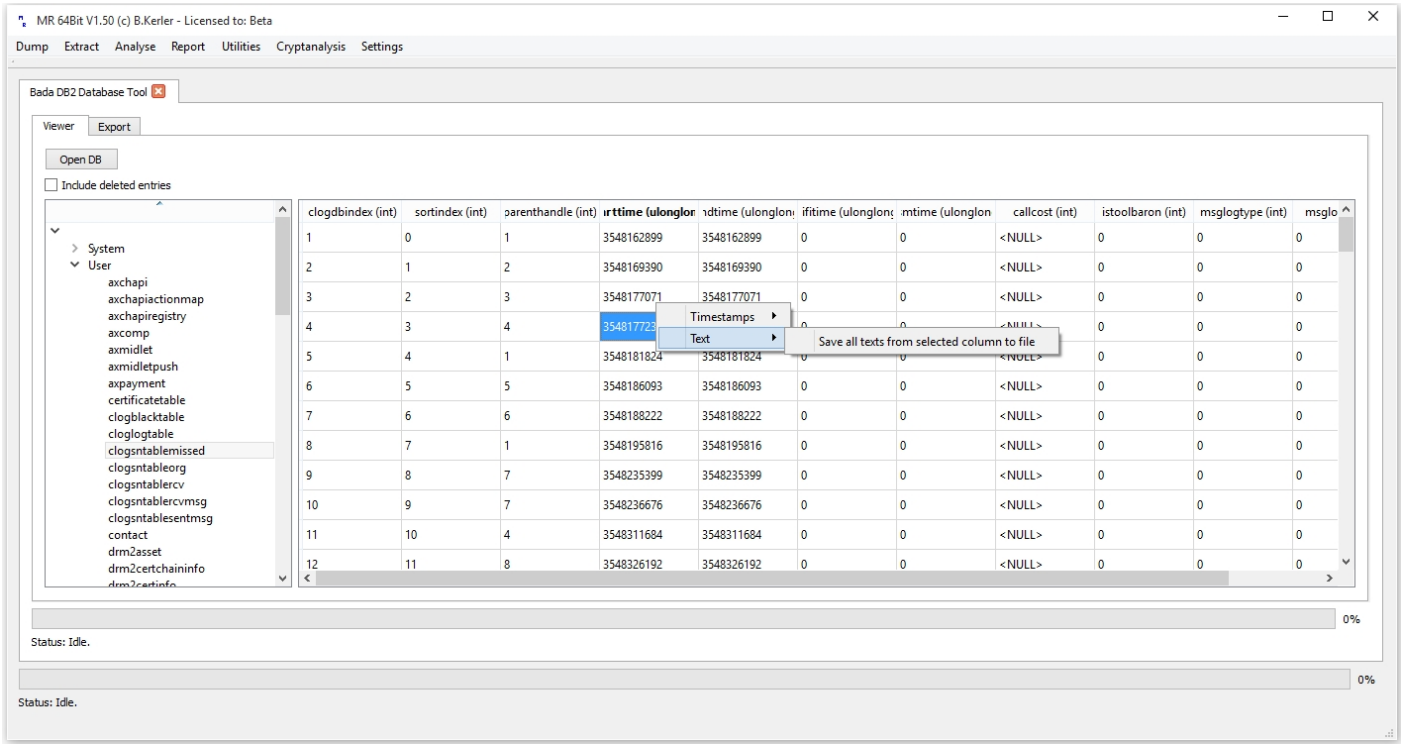


Timestamps



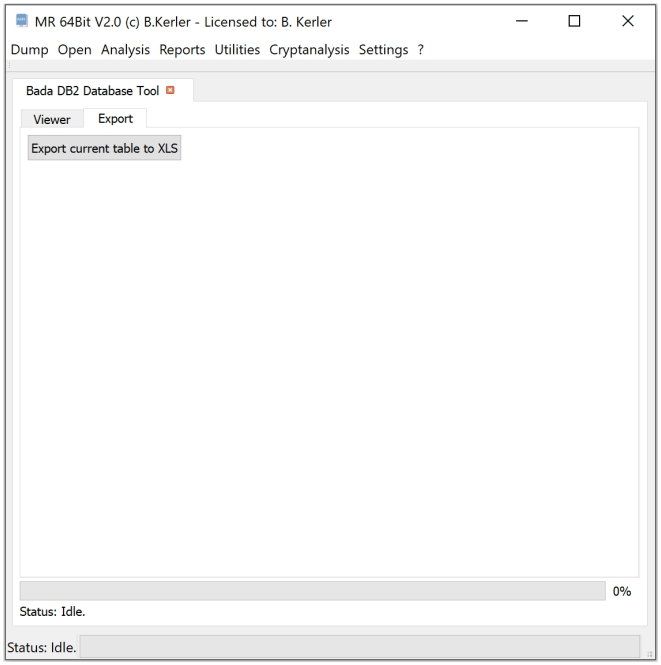
The timestamp submenu allows you to convert integer fields to timestamps.

Text



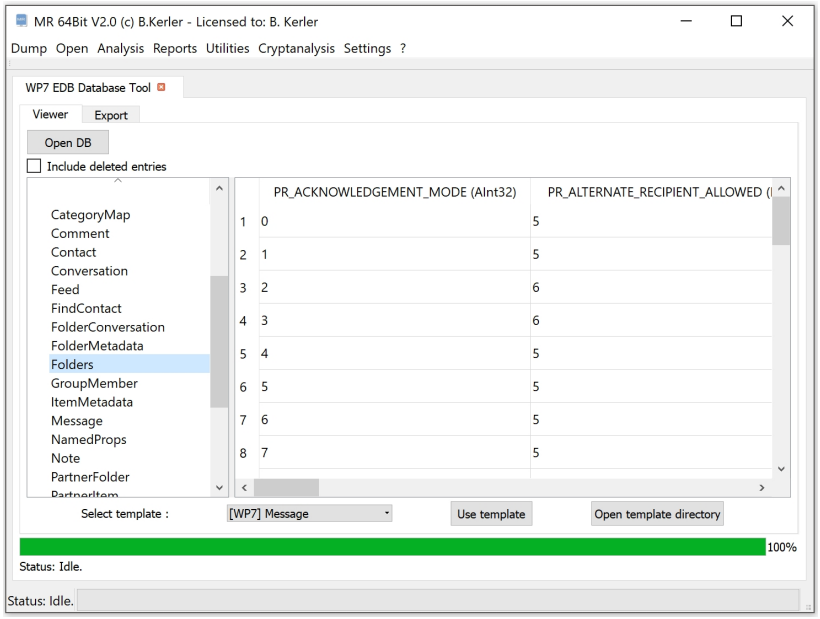
The text submenu allows you to save all texts from selected column in the current table to a file.

Export



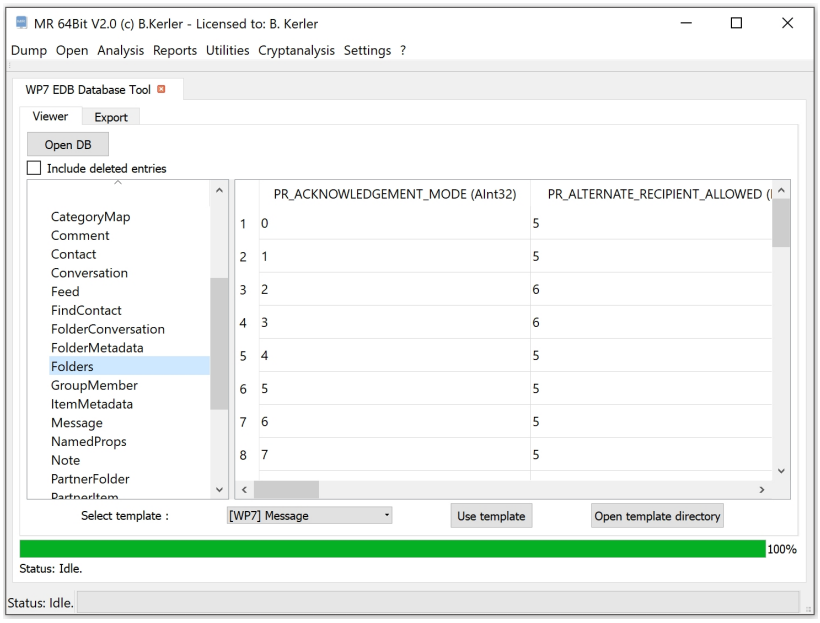
The export tab will allow you to save the current table to a xlsx file.

WP7 EDB Database Tool



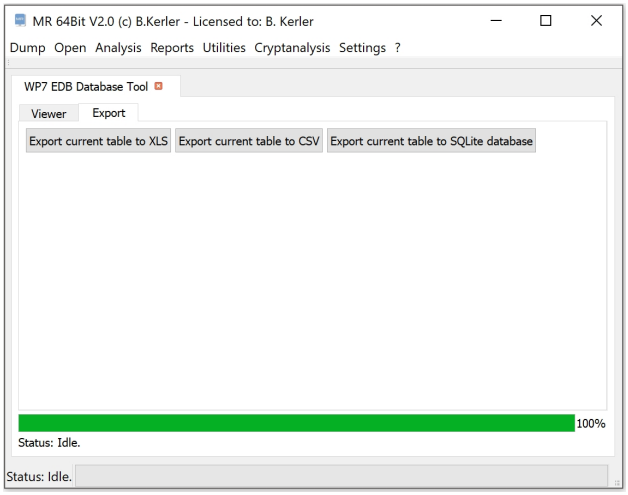
The WP7 EDB Database Tool lets you open WP7 and WM6 EDB databases like "store.vol".

View



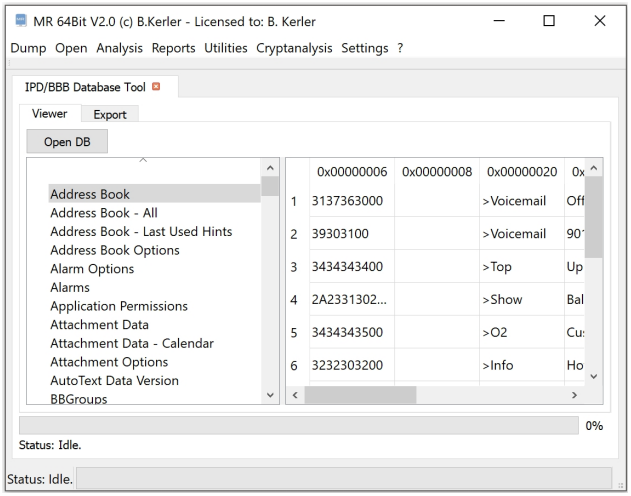
Press "Open DB" to open a database and select "Include deleted entries" to show deleted entries when clicking at the left index.

Export



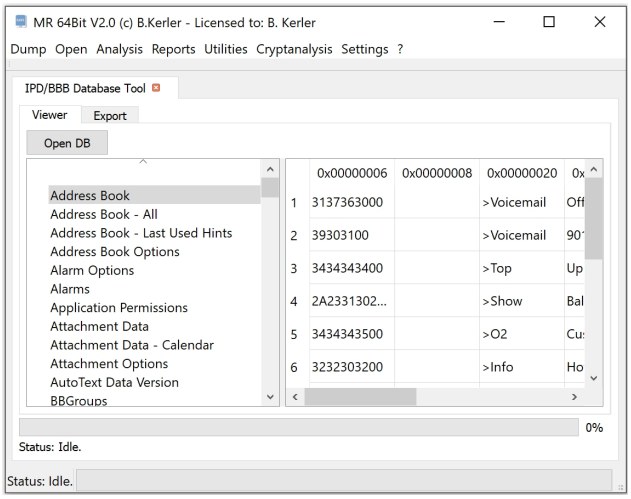
The export tab will allow you to extract the current table to either xls, csv or sqlite database file.

IPD/BBB Database Tool



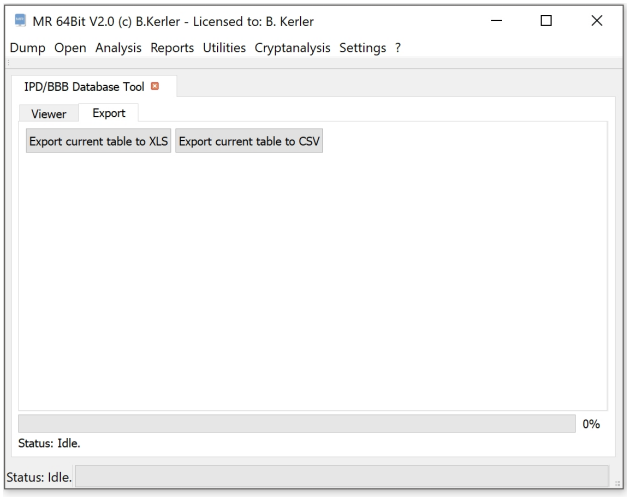
The Blackberry IPD Database Tool lets you examine .bbb or .ipd database files.

View



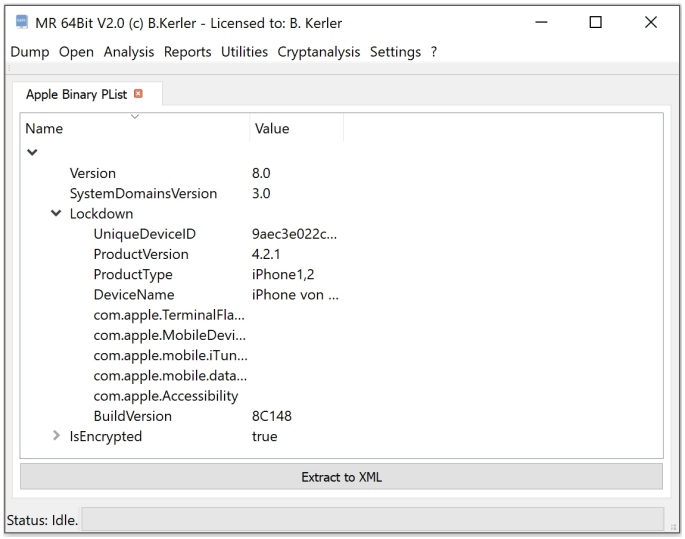
Click "Open DB" to open any Blackberry Messenger .bbb or .ipd Backup File. Values not being interpreted are being shown as Hex Values.

Export



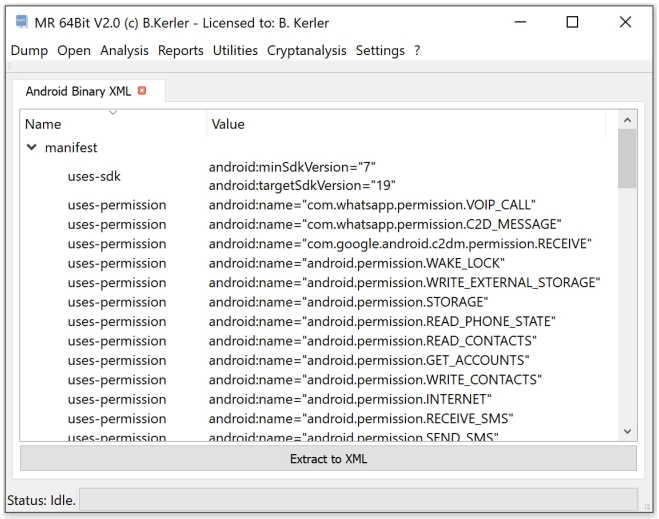
The export function lets you export the current field to a xls or csv file.

Apple Binary PList



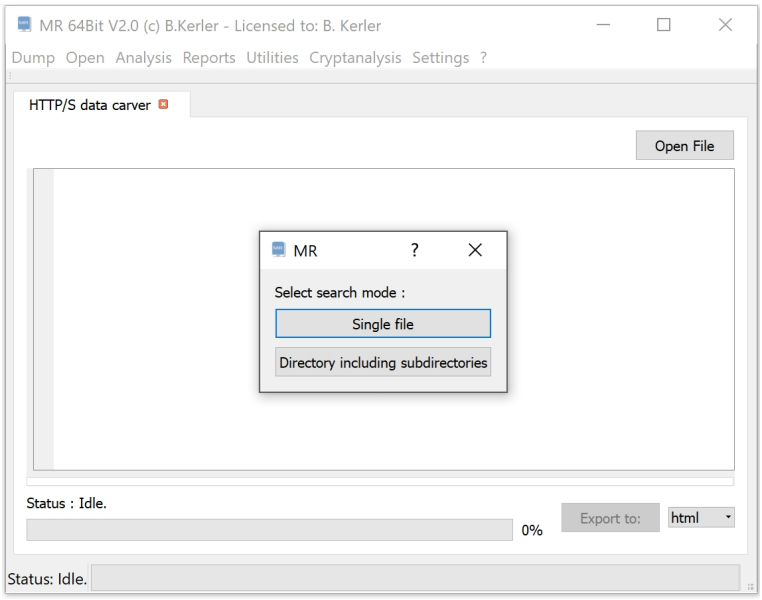
This tool will present all data from both Apple Binary and Raw XML Format and lets you either copy the data to the clipboard if selected using Ctrl-C or lets you extract all data to a XML-formatted file using the "Extract to XML" button.

Android Binary XML

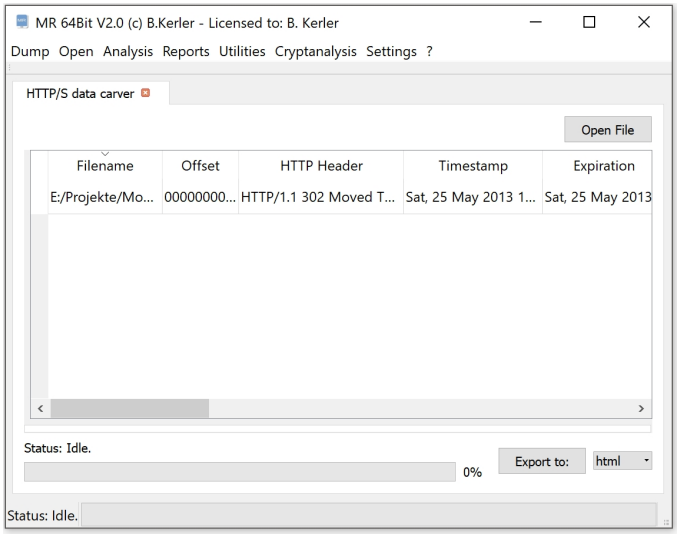


This tool will present all data from Android Binary XML Format and lets you either copy the data to the clipboard if selected using Ctrl-C or lets you extract all data to a XML-formatted file using the "Extract to XML" button.

HTTP/S data carver

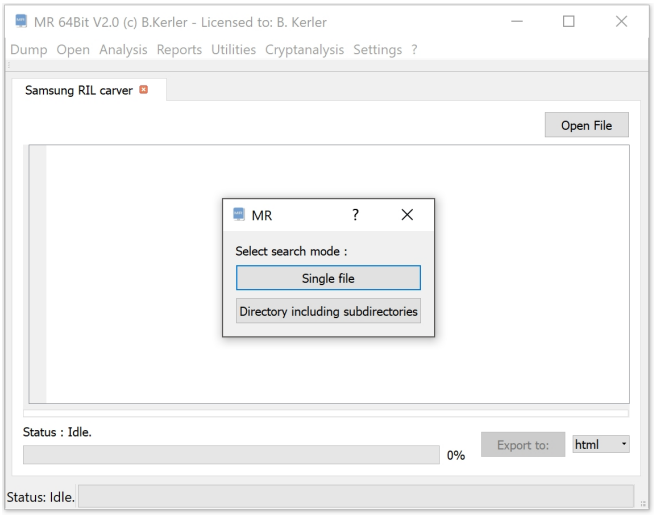


This tool will search for any HTTP header that might have been cached in the raw flash images or single cache files. Either choose
"Single file" to search within a single file or "Directory including subdirectories" to search within any folder and its subfolders being selected.

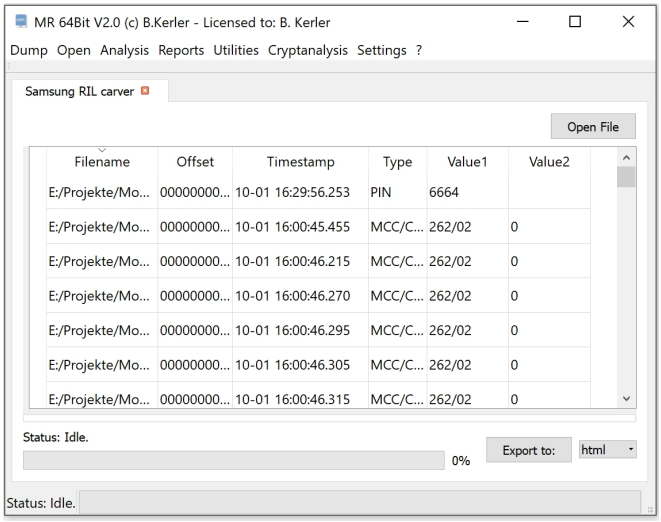


In order to sort any data, just click on the header. You may export the data to text-formatted CSV-Format, Office XLSX-Format and SQLite database.

Samsung RIL carver

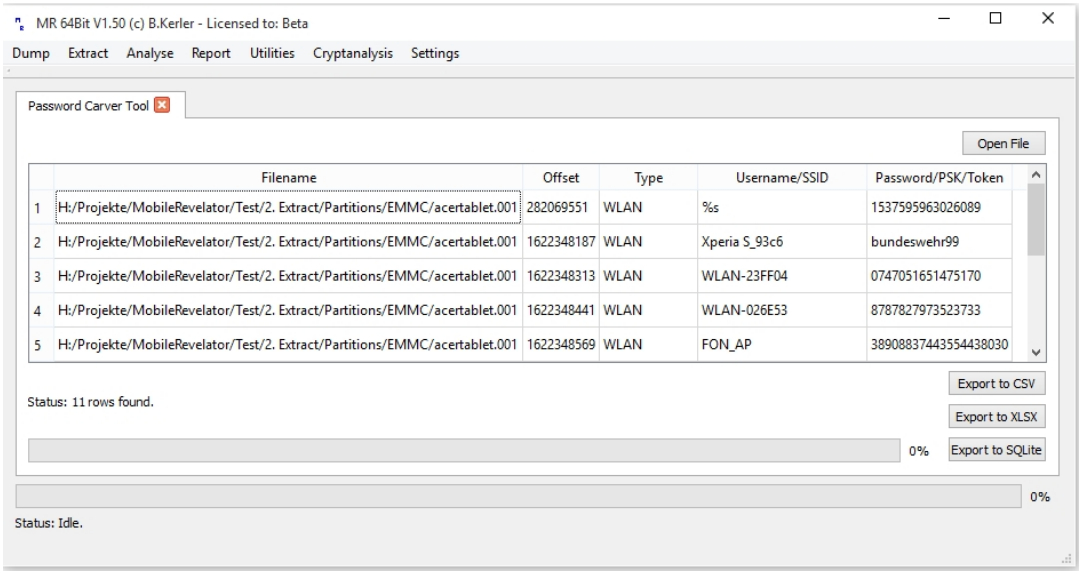


This tool will extract all Cell-Information, SIM-PIN, SIM-Provider-Information and much more from Samsung Radio Information Layer (RIL) like on the Samsung Galaxy S3 Mini. Either choose "Single file" to search within a single file or "Directory including subdirectories" to search within any folder and its subfolders being selected.



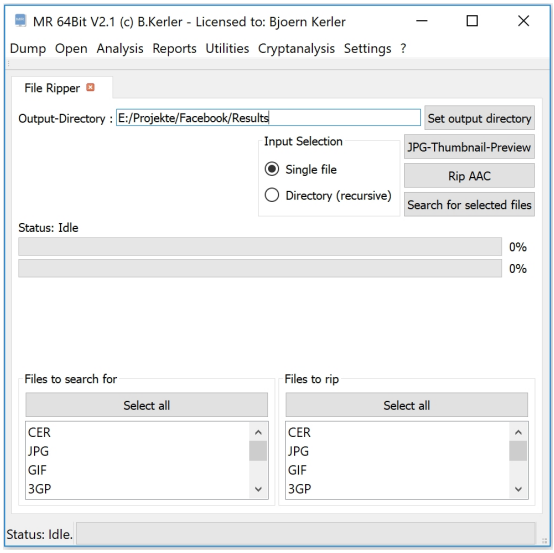
In order to sort any data, just click on the header. You may export the data to text-formatted CSV-Format, Office XLSX-Format and SQLite database.

Android Password carver



This tool will extract any WLAN or HTTP Plaintext password. In order to sort any data, just click on the header. You may export the data to text-formatted CSV-Format, Office XLSX-Format and SQLite database.

File Ripper



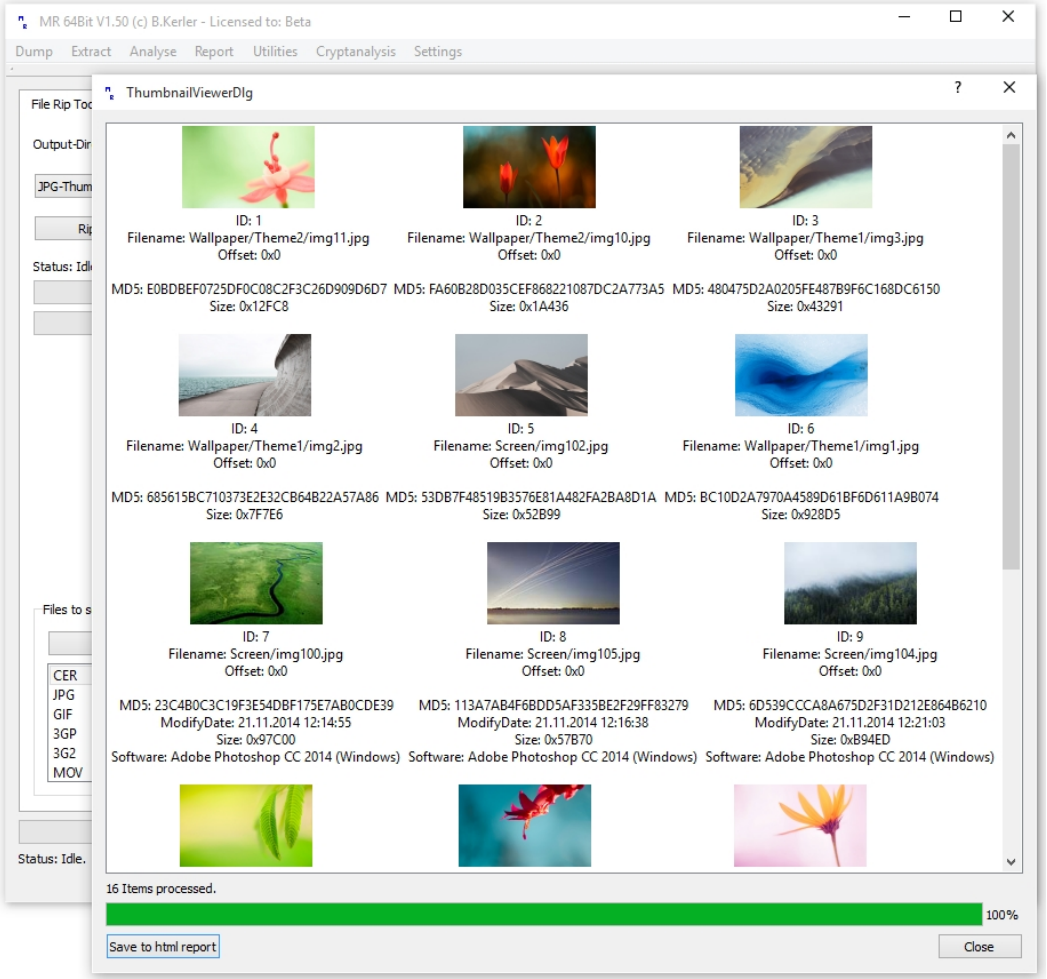
The File Ripper utility lets you search and rip known filetypes. Before running any option, you should select a directory where the reports and files should be written to using "1. Set Outputdirectory". Then choose if you want to search in one single file or in a directory using the "Input selection" field.

You may then choose the following functions :

- "Run search" will rip (search full file content) / search (look at file start) any selected file. You may select multiple file types
  using Ctrl-Key as well.

- "Rip AAC" will rip any AAC MP4-Fragments it may find.

- "JPG-Thumbnail-Preview" extracts and carves jpgs and thumbnails, pressing "Save to html report" will save the found files
  and thumbails to the output-directory. You may doubleclick on the pictures to see the full image size, if available :


MR 64Bit V1.50 (c) B.Kerler - Licensed to: Beta
Dump Extract Analyse Report Utilities Cryptanalysis Settings
ThumbnailViewerDlg
ID: 1
Filename: Wallpaper/Theme2/img11.jpg
Offset: 0x0
MD5: E0BDBEF0725DF0C08C2F3C26D909D6D7
Size: 0x12FC8
ID: 2
Filename: Wallpaper/Theme2/img10.jpg
Offset: 0x0
MD5: FA60B28D035CEF868221087DC2A773A5
Size: 0x1A436
ID: 3
Filename: Wallpaper/Theme1/img3.jpg
Offset: 0x0
MD5: 480475D2A0205FE487B9F6C168DC6150
Size: 0x43291
ID: 4
Filename: Wallpaper/Theme1/img2.jpg
Offset: 0x0
MD5: 685615BC710373E2E32CB64B22A57A86
Size: 0x7F7E6
ID: 5
Filename: Screen/img102.jpg
Offset: 0x0
MD5: 53DB7F48519B3576E81A482FA2BA8D1A
Size: 0x52B99
ID: 6
Filename: Wallpaper/Theme1/img1.jpg
Offset: 0x0
MD5: BC10D2A7970A4589D61BF6D611A9B074
Size: 0x928D5
ID: 7
Filename: Screen/img100.jpg
Offset: 0x0
MD5: 23C4B0C3C19F3E54DBF175E7AB0CDE39
ModifyDate: 21.11.2014 12:14:55
Size: 0x97C00
Software: Adobe Photoshop CC 2014 (Windows)
ID: 8
Filename: Screen/img105.jpg
Offset: 0x0
MD5: 113A7AB4F6BDD5AF335BE2F29FF83279
ModifyDate: 21.11.2014 12:16:38
Size: 0x57B70
Software: Adobe Photoshop CC 2014 (Windows)
ID: 9
Filename: Screen/img104.jpg
Offset: 0x0
MD5: 6D539CCCA8A675D2F31D212E864B6210
ModifyDate: 21.11.2014 12:21:03
Size: 0xB94ED
Software: Adobe Photoshop CC 2014 (Windows)
16 Items processed.
100%
Save to html report
Close
Status: Idle.

Apple iThmb Extract

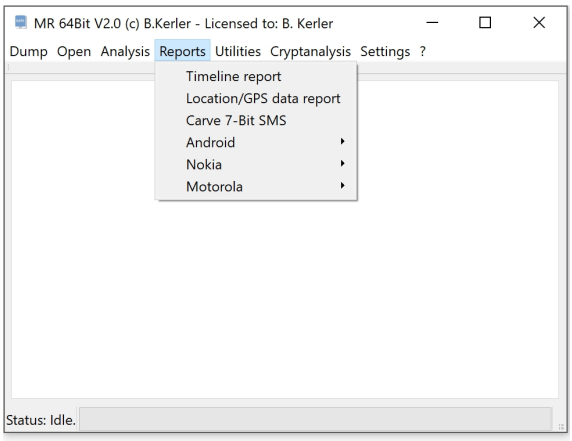
This tool lets you extract JPG Pictures from .ithmb thumbnail databases being found in Apple devices under PhotoData/Thumbnails directory. The Filename contains the index which is being used in the /PhotoData/Photos.sqlite database as well.

For getting information about deleted images, run

"SELECT * FROM ZGENERICASSET as asset, ZADDITIONALASSETATTRIBUTES as attrib WHERE attrib.ZASSET == asset.Z_PK AND asset.ZTHUMBNAILINDEX == 1234;" as sqlite command

whereas the thumbnail index to be retrieved would be 1234 in this example.

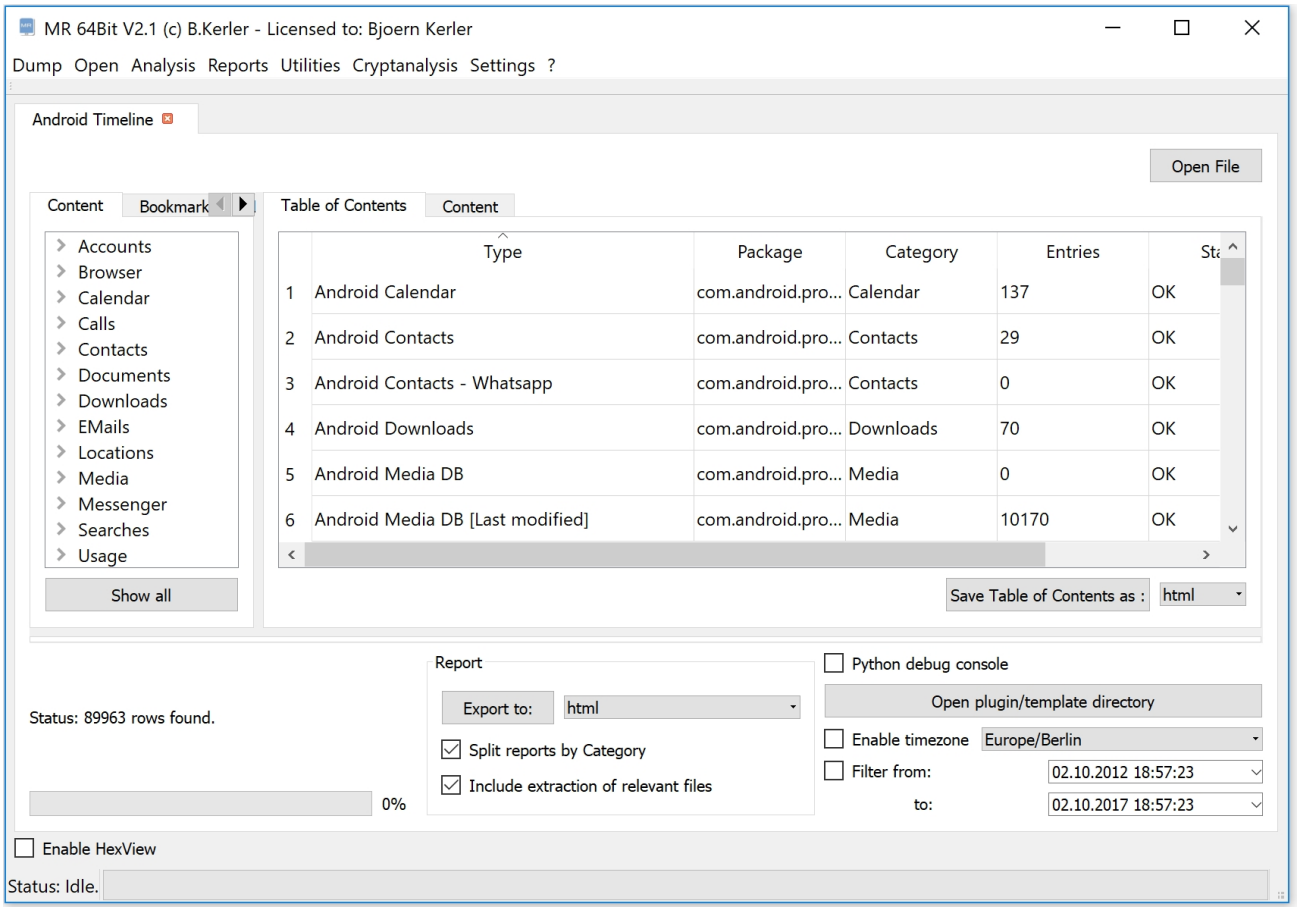
Report

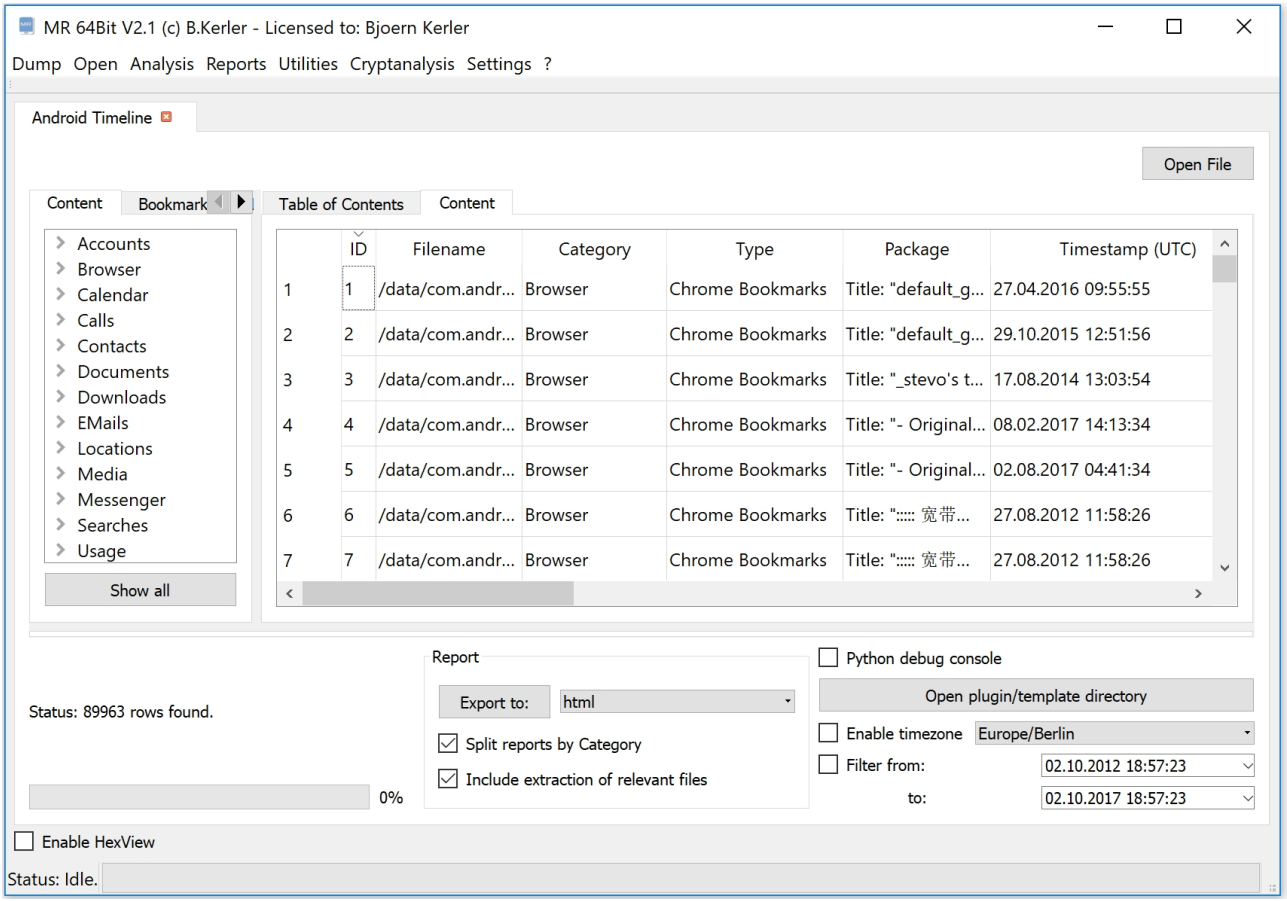


The report menu offers several tools for generating reports.

Timeline report

The Android timeline module will search for time relevant information within raw files and/or extracted database files. Choosing a huawei backup or android backup
as raw file is also possible. You may add custom databases at any time by creating a new xml file in the "C:\Users\xxx\Documents\Mobile Revelator\Template\[OS]" path. Please see Templates Documentation on how to create and use Python and Timeline modues. If the additional cell database has been installed, detected cell information from herrevad databases will be converted to place names automatically.



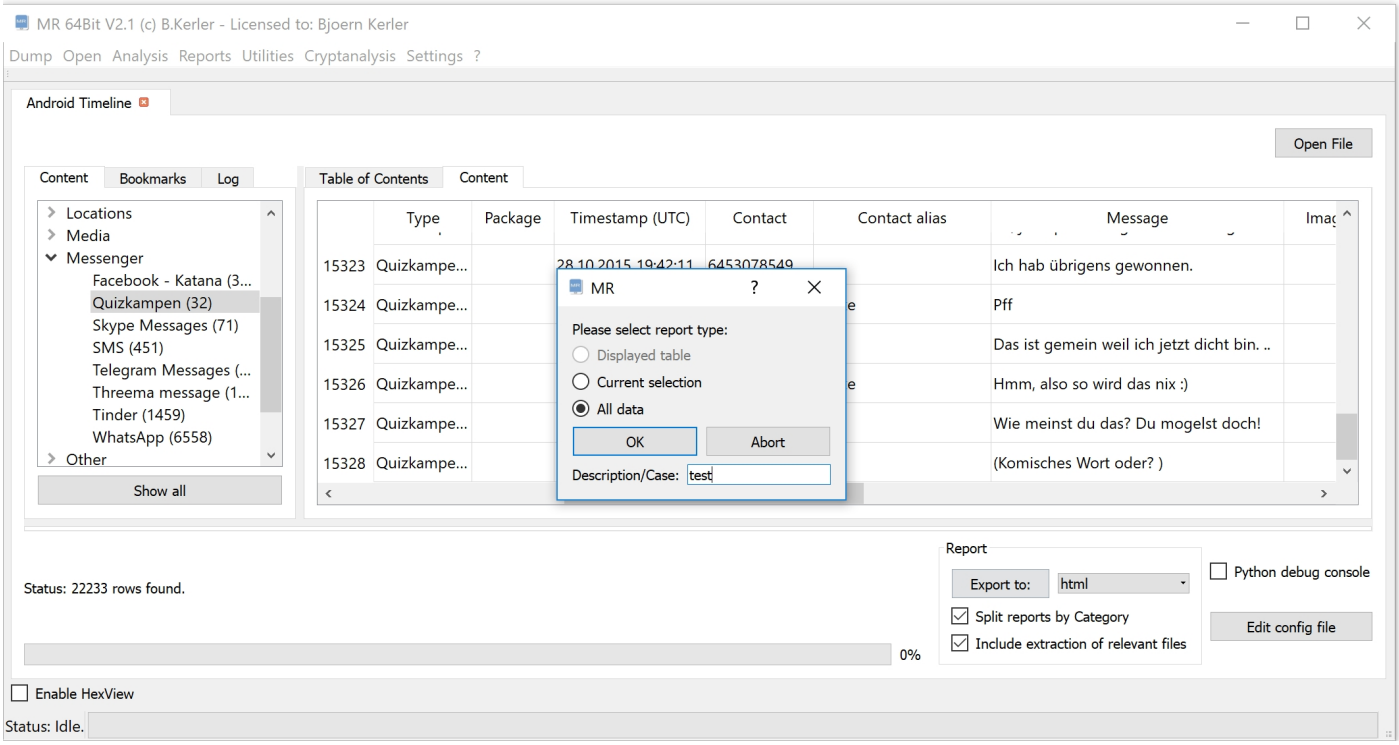


Using Ctrl-F you can search for any string, clicking on an entry in the result tab will show the selected entry in the table. Double-left-clicking a category with the mouse on the tree will only show the current selected entry. Using CTRL-Key on the keyboard and left-click with the mouse you can select multiple categories, pressing right-click on the mouse will offer you a menu to only show selected items or to hide selected items from the current table display.

Using Ctrl-B you can bookmark selected lines. on the bookmarks tab, you can select entries to show which also allows you to bookmark any results and generate reports based on bookmarked items.

Clicking on the table header, you may sort items as required. Enabling timezones will display the selected timezone in both view and report.
You can also filter between two dates, which will then show only the entries with timestamps in between.

Reports



You may select any report type by clicking on the list right hand of the "Export to:" button. Pressing the "Export to: " button, you may choose whether the currently displayed table, the current selection (in the tree and/or in the content tab) or all data will
be extracted to reports.

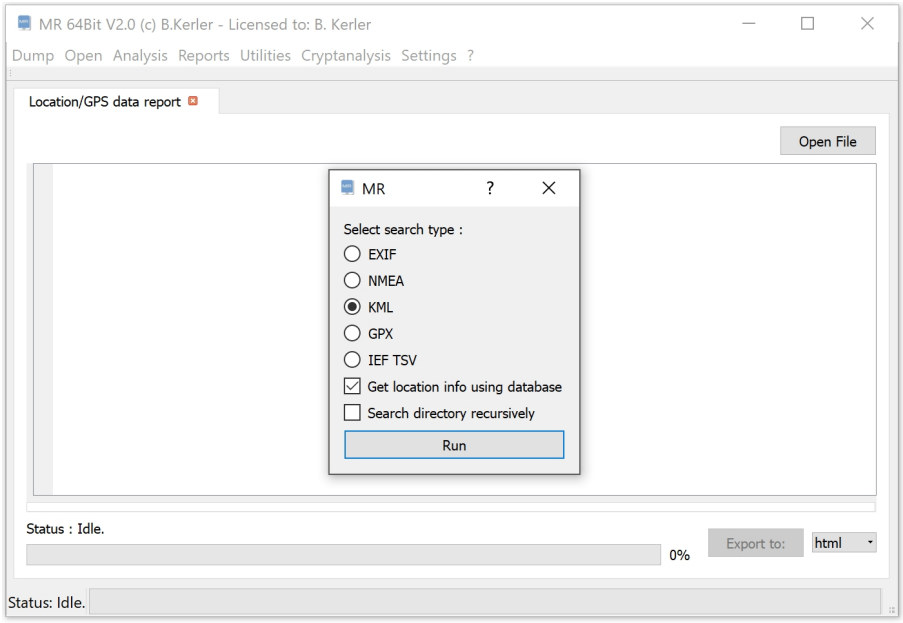
For PDF and HTML reports, you may sort items and report will be sorted as well. Just click on the header of the table to sort items.

Right clicking on a content filename, you can select "Jump to filename" in order to open up a filesystem view, pointing to the selected file in the report.

Using "Split reports by Category", you can automatically generate separate report files for each category.

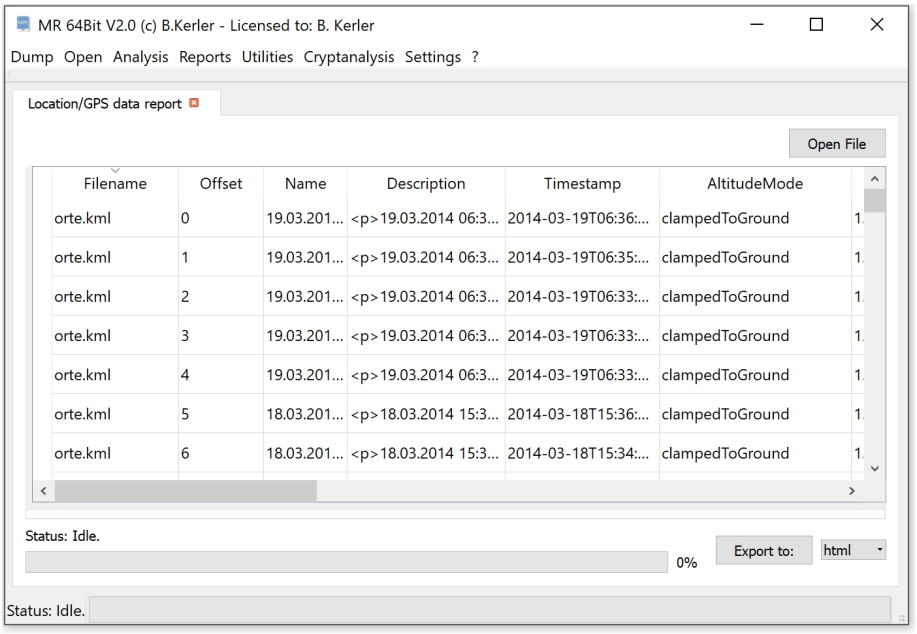
If "Include extraction of relevant files" has been selected, all files including necessary files will be extracted to the "files" subdirectory in the report folder
and contents will be clickable in both pdf and html reports.

Location/GPS data report



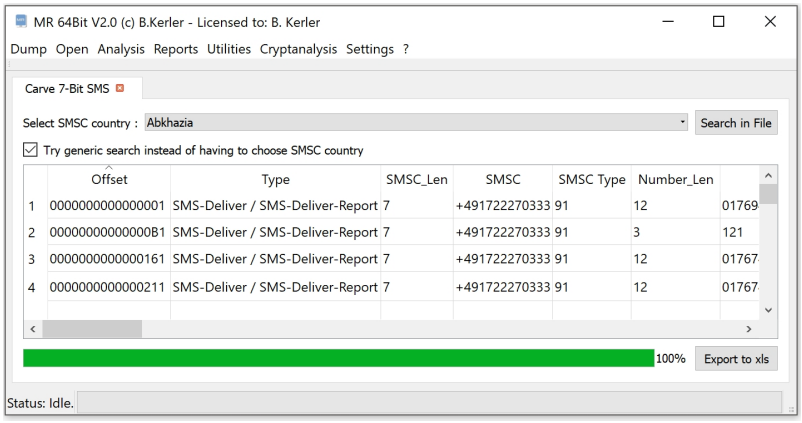
This tool will carve any gps data from either EXIF-information being using in JPG-Files, from GPS-Ascii-Standard NMEA, from Google KML-based data structures, from any Garming GPX dataset and from Internet Evidence Finder report files as well.

If you choose to "Get location info using database", MR will retrieve its town and country information without online connection.
Selecting "Select directory recursively" will seek within any file that has been selected, recursively for each subdirectory.
Pressing "run" you will either be able to select the directory or file to search for.



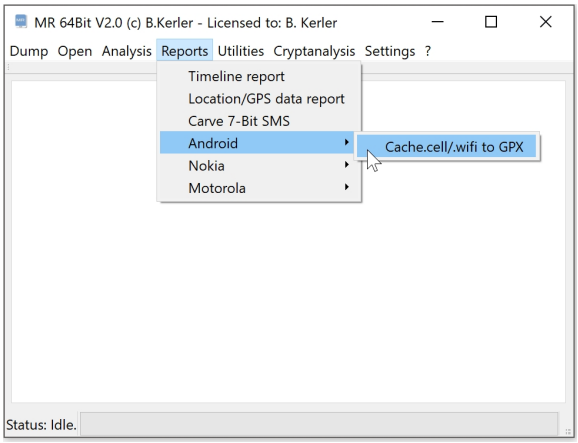
In order to sort any data, just click on the header. The data fields "Country Code", "Postal Code", "Town" and "Distance to town" are generated by MR to get a quicker overview about the coordinates. You may export the data to text-formatted CSV-Format, Office XLSX-Format and SQLite database.

Carve 7-Bit SMS



This tool will extract any 7-Bit formatted sms that matches the 3GPP standard. Either use the generic method by selecting "Try generic search instead of having to choose SMS country" or, if more precision and less wrongly carved sms data is needed, uncheck the option and select the appropriate SMSC Country. Export of the data to the Office XLSX-Format is possible using the button "Export to xls". In order to sort any data, just click on the header.

Android

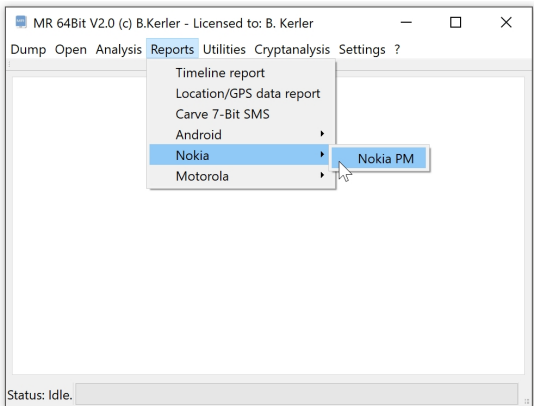


This menu will convert cache.cell and cache.wifi files to Google .gpx Files.

Cache.cell/.wifi to GPX

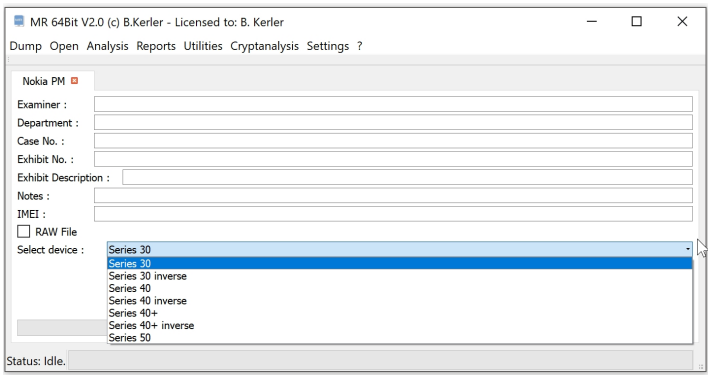
This function allows to convert cache.cell and cache.wifi files to google gpx files.

Nokia



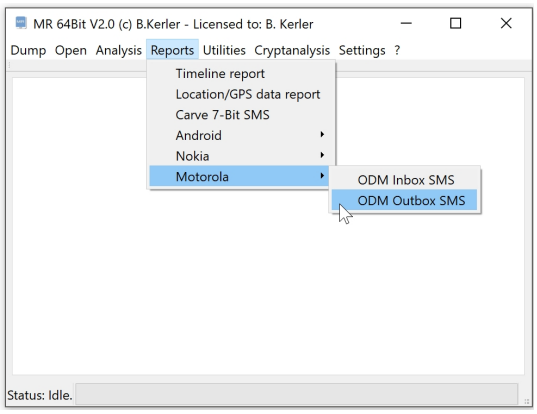
The Nokia PM report tool is able to extract call logs, sms and much more from Nokia .pm files.

Nokia PM



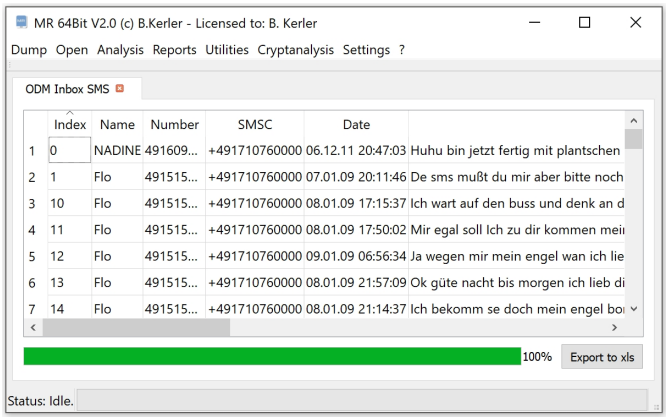
The Nokia PM report tool allows you to extract numbers, calllogs, SMS, etc. from PM files. In order to ensure proper decryption of userlock codes, make sure you enter the right IMEI before. The resulting report will be written as an HTML file.

Motorola



The Motorola ODM Tool converts raw inbox and outbox sms files to a readable format.

ODM Inbox SMS

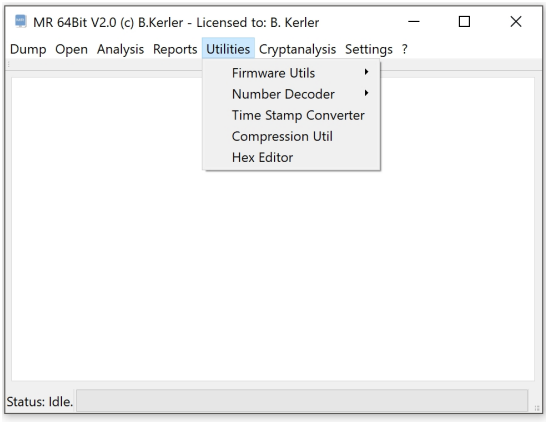


The Motorola ODM SMS Inbox tool lets you decode the "smsIBMsg" file. Pressing on "Export to xls", the decoded data in the table will be written into a XLSX file.

ODM Outbox SMS

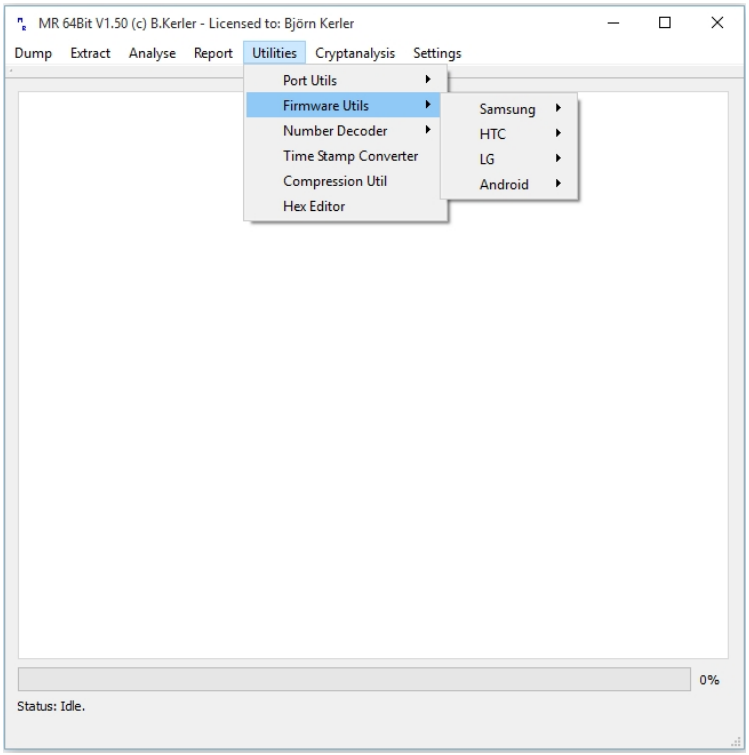
The Motorola ODM SMS Inbox tool lets you decode the "smsOBInfo" file. Pressing on "Export to xls", the decoded data in the table will be written into a XLSX file.

Utilities



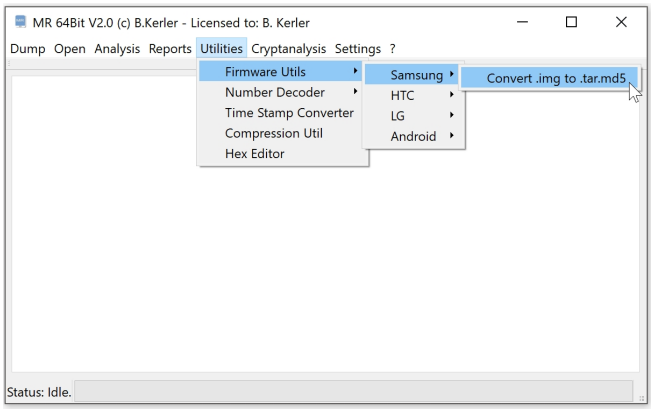
The utilities menu contains several tools which are hardware based or offer additional information.

Firmware Utils



The firmware utils offer many tools for conversion between proprietary firmware formats and regular file formats.

Samsung

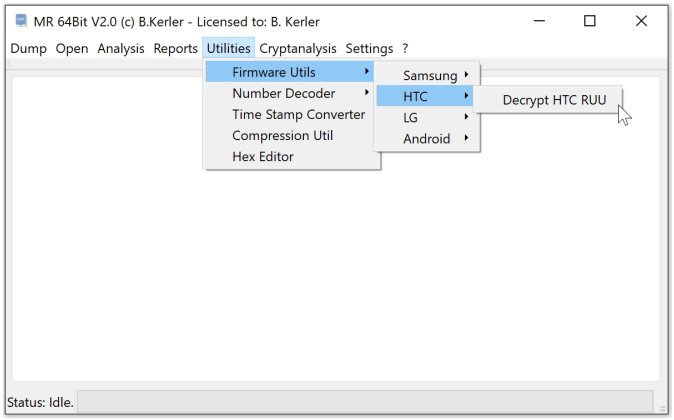


This util offers functionality to convert Samsung firmware.

Convert .img to .tar.md5

This tool is able to convert Samsung raw image files to .tar.md5 files for usage in Samsung's Odin tool.

HTC

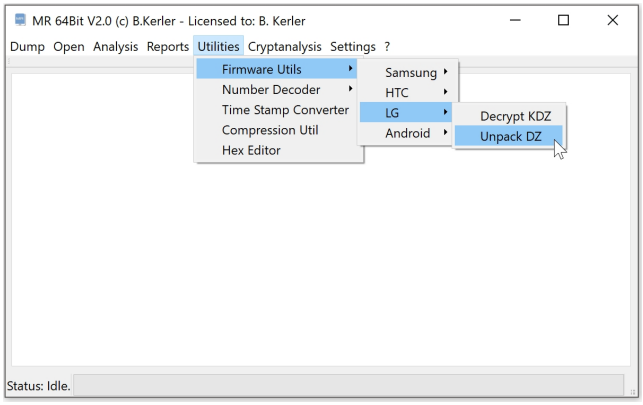


This util offers functionality to convert HTC firmware.

Decrypt HTC RUU

This tool is able to decrypt encrypted HTC RUU .ZIP firmware containers.

LG



This util offers functionality to convert LG firmware.

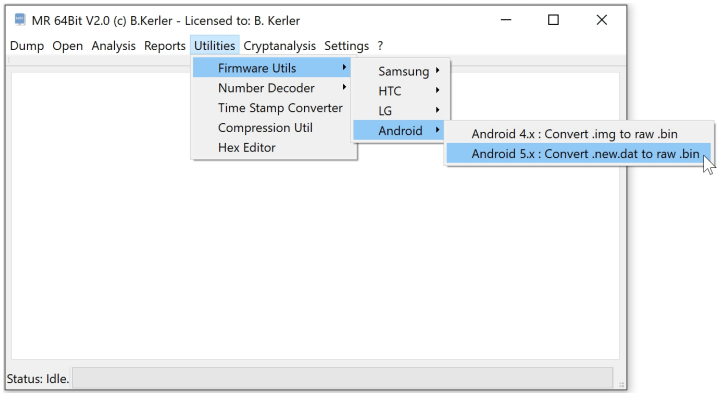
Decrypt KDZ

This tool is able to convert encrypted LG KDZ containers to LG .DZ containers.

Unpack DZ

This tool is able to convert encrypted LG DZ containers to .cab files.

Android



This util offers functionality to convert Android generic firmware.

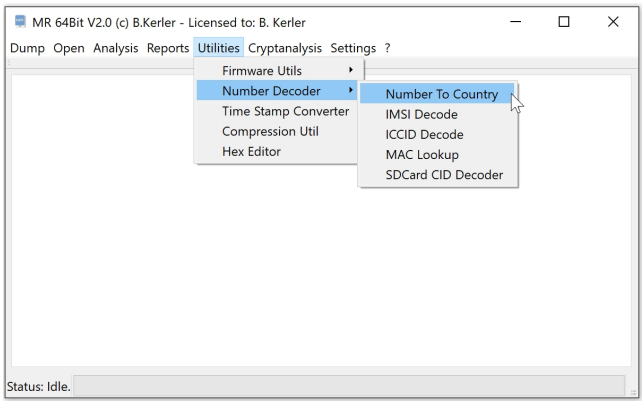
Android 4.x : Convert .img to raw .bin

This tool is able to convert android 4.x firmware in ".img" format to raw .bin files.

Android 5.x : Convert .new.dat to raw .bin

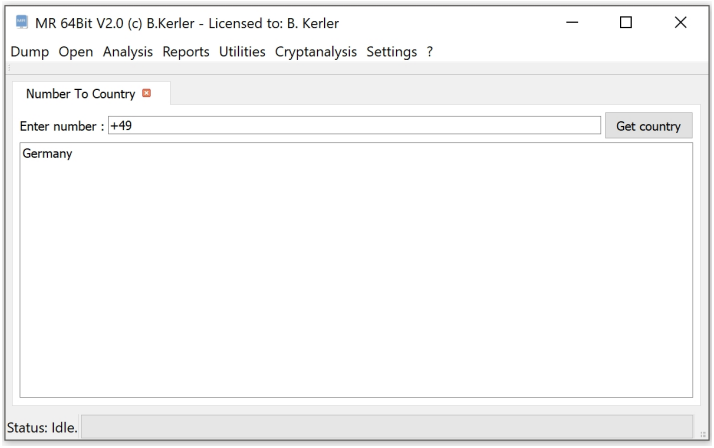
This tool is able to convert android 5.x firmware in ".new.dat" format to raw .bin files.

Number Decoder



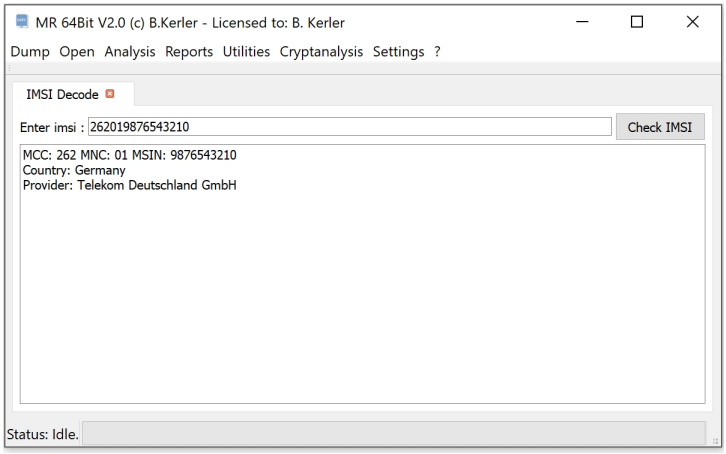
The number decoder tools offer tools for identification and generating more information about unique serial numbers and standardized items.

Number To Country



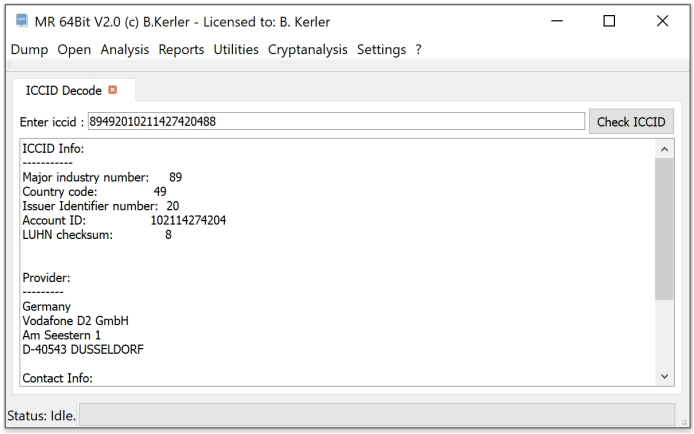
The number decoder will convert international telephony codes into country names.

IMSI Decode



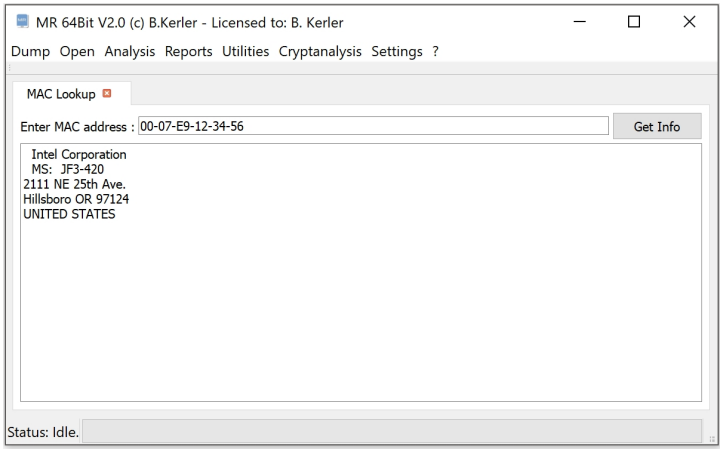
The IMSI decoder is able to decode IMSI data to provider information.

ICCID Decode



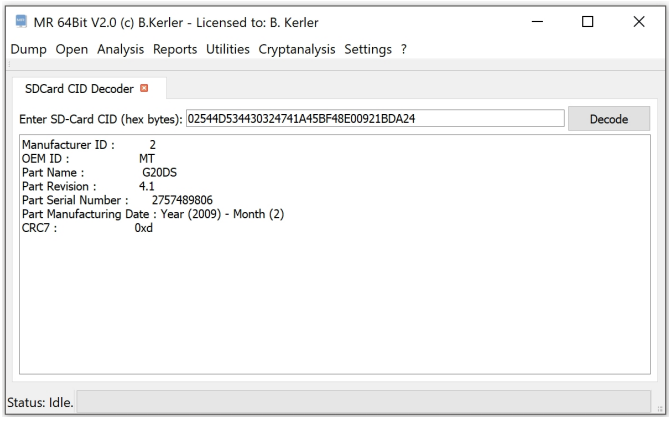
This tool converts SIM card ICCID numbers to provider Information according to the ITU E.118 standard.

MAC Lookup



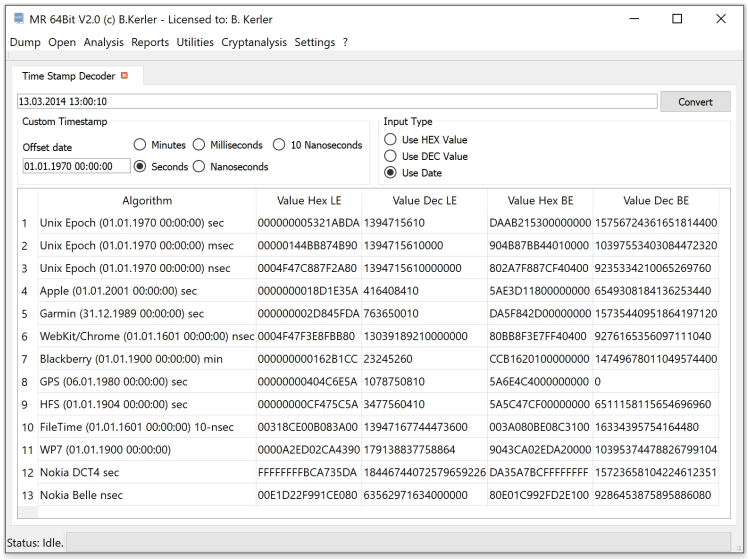
The mac lookup is able to show vendor information for mac addresses.

SDCard CID Decoder



The SDCard CID decoder tool is able to convert hex values into the appropriate JEDEC description.

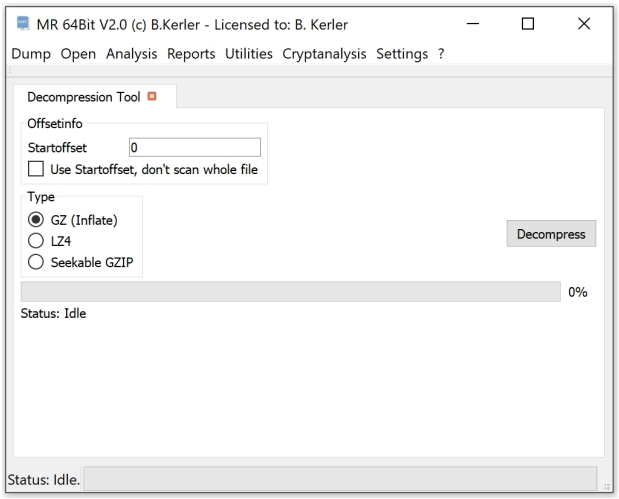
Time Stamp Decoder



	Algorithm	Value Hex LE	Value Dec LE	Value Hex BE	Value Dec BE
1	Unix Epoch (01.01.1970 00:00:00) sec	0000000005321ABDA	1394715610	DAAB215300000000	15756724361651814400
2	Unix Epoch (01.01.1970 00:00:00) msec	00000144BB874B90	1394715610000	904B87BB44010000	10397553403084472320
3	Unix Epoch (01.01.1970 00:00:00) nsec	0004F47C887F2A80	1394715610000000	802A7F887CF40400	9235334210065269760
4	Apple (01.01.2001 00:00:00) sec	0000000018D1E35A	416408410	5AE3D11800000000	6549308184136253440
5	Garmin (31.12.1989 00:00:00) sec	000000002D845FDA	763650010	DA5F842D00000000	15735440951864197120
6	WebKit/Chrome (01.01.1601 00:00:00) nsec	0004F47F3E8FBB80	13039189210000000	80BB8F3E7FF40400	9276165356097111040
7	Blackberry (01.01.1900 00:00:00) min	000000000162B1CC	23245260	CCB1620100000000	14749678011049574400
8	GPS (06.01.1980 00:00:00) sec	00000000404C6E5A	1078750810	5A6E4C4000000000	0
9	HFS (01.01.1904 00:00:00) sec	00000000CF475C5A	3477560410	5A5C47CF00000000	6511158115654696960
10	FileTime (01.01.1601 00:00:00) 10-nsec	00318CE00B083A00	13947167744473600	003A080BE08C3100	16334395754164480
11	WP7 (01.01.1900 00:00:00)	0000A2ED02CA4390	179138837758864	9043CA02EDA20000	10395374478826799104
12	Nokia DCT4 sec	FFFFFFFFBCA735DA	1844674407257965922 6	DA35A7BCFFFFFFFF	15723658104224612351
13	Nokia Belle nsec	00E1D22F991CE080	63562971634000000	80E01C992FD2E100	9286453875895886080

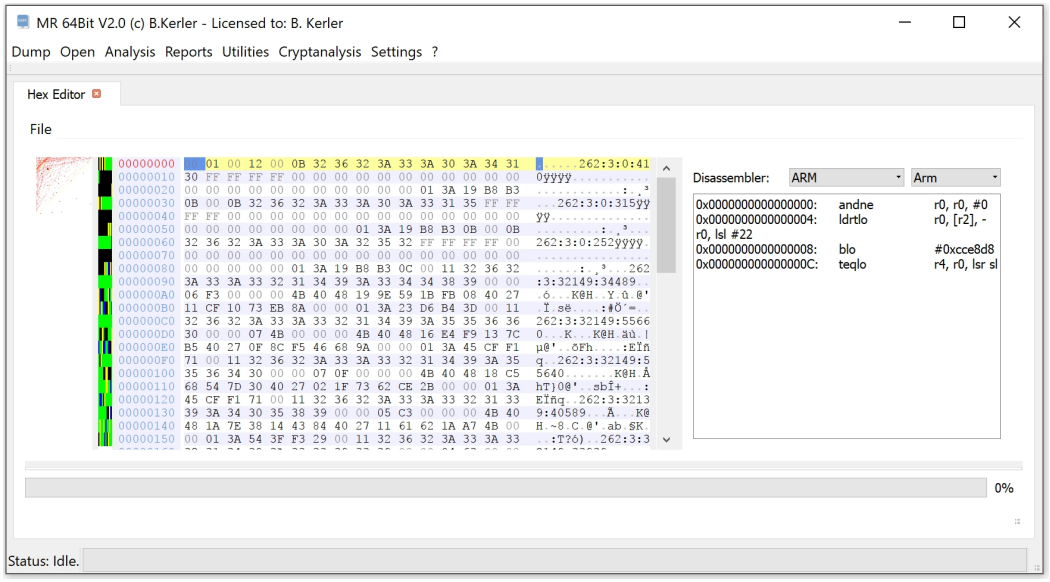
The timestamp converter is able to both convert from dates to values as well from values to dates.

Compression Util

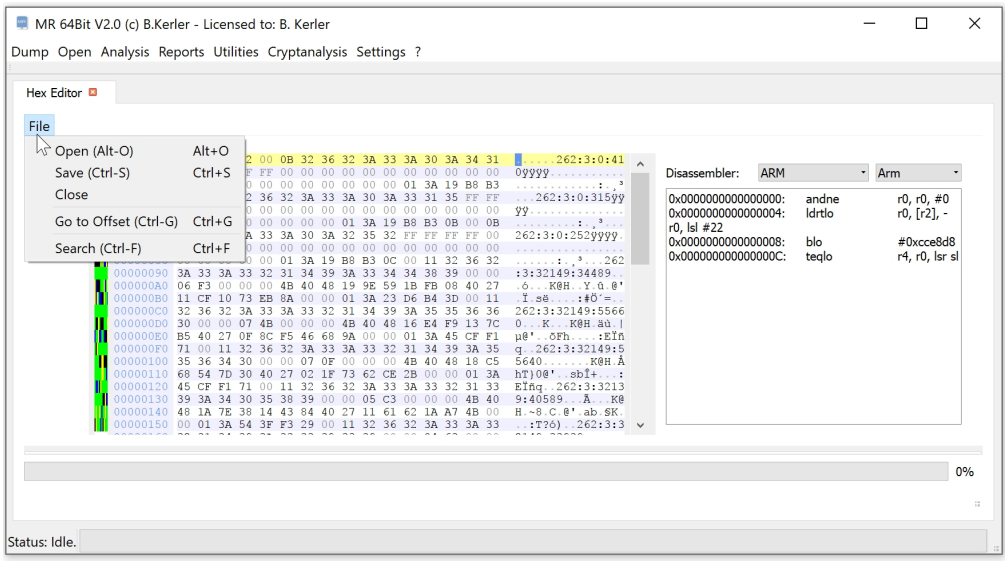


The decompression tool is able to uncompress any gzipped or lz4 zipped data, which is likely common in kernels and router firmwares.If you leave the settings as they are, the tool will try to find and automatically extract each segment as a different file. If the autodetection fails you may as well check the "Use startoffset" checkbox, which will allow you to enter a specific offset as a hex value as the startoffset for decompression.

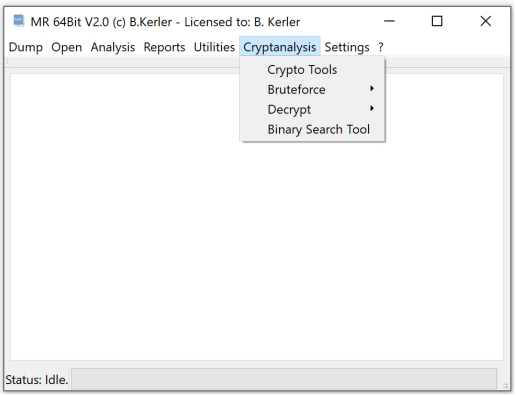
Hex Editor



The hex editor is able to show binary files with different types of interpretation. You may choose a disassembler at the right for disassembling code patterns in the current hex editor data. On the left side, you may see that ascii bytes are colored green, 00's and FF's are colored black, and lower bytes in between are colored blue as well as higher bytes in between are colored yellow. On the left most side, you can see a statistical interpretation of each triple-bytes including entropy, which may help you identify different file types without having a file header.

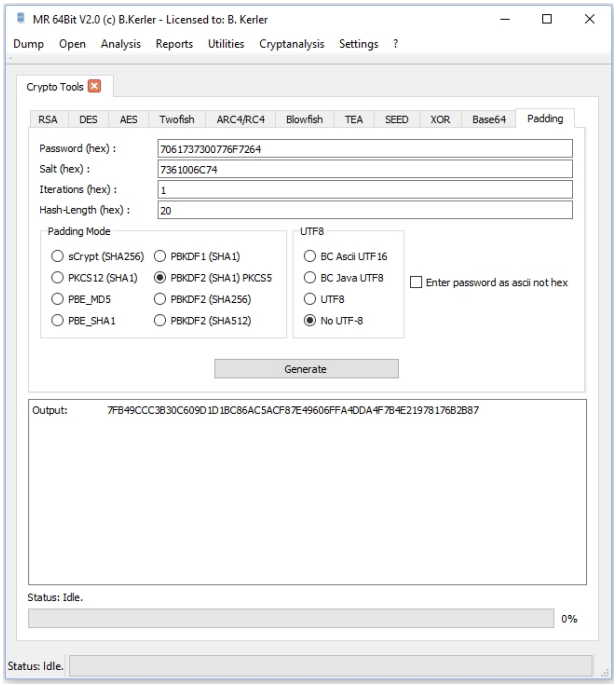


Cryptanalysis



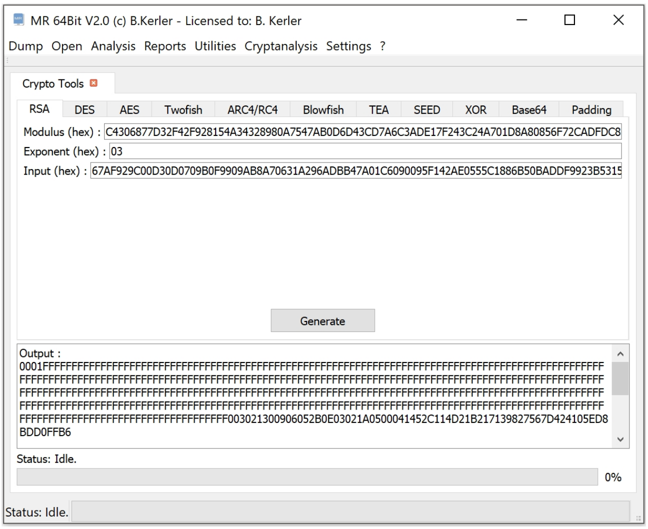
The cryptanalysis menu offers several tools for decrypting information from different apps or vendors and contains "Crypto Tools" for experimentations with several crypto standards and techniques.

Crypto Tools

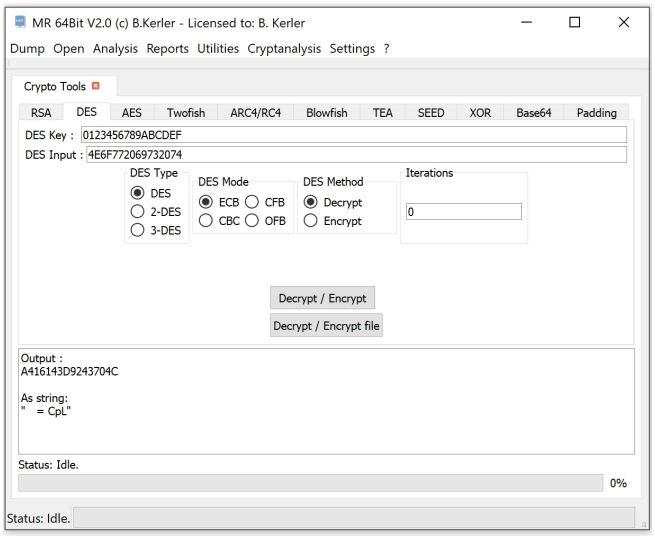


The crypto tools allows you to play with several cryptographical functions.

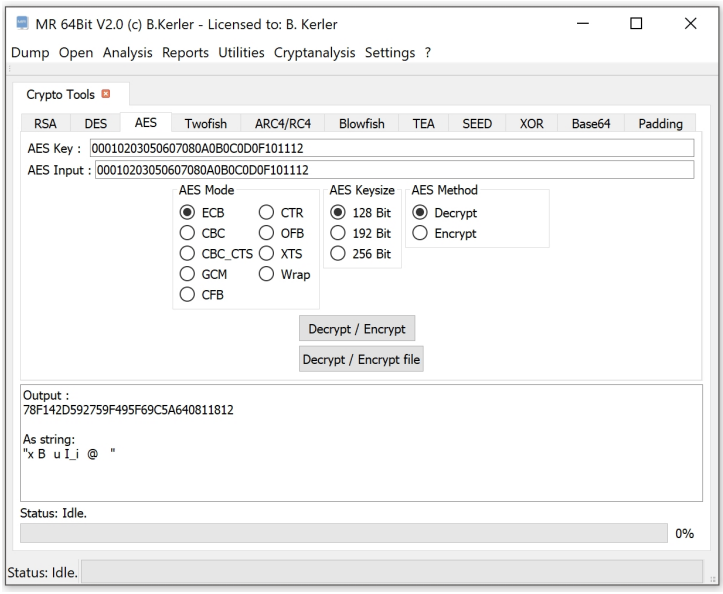
RSA


MR 64Bit V2.0 (c) B.Kerler - Licensed to: B. Kerler
Dump Open Analysis Reports Utilities Cryptanalysis Settings ?
Crypto Tools
RSA DES AES Twofish ARC4/RC4 Blowfish TEA SEED XOR Base64 Padding
Modulus (hex) :
Exponent (hex) : 03
Input (hex) :
Generate
Output :
Status: Idle.
0%
Status: Idle.

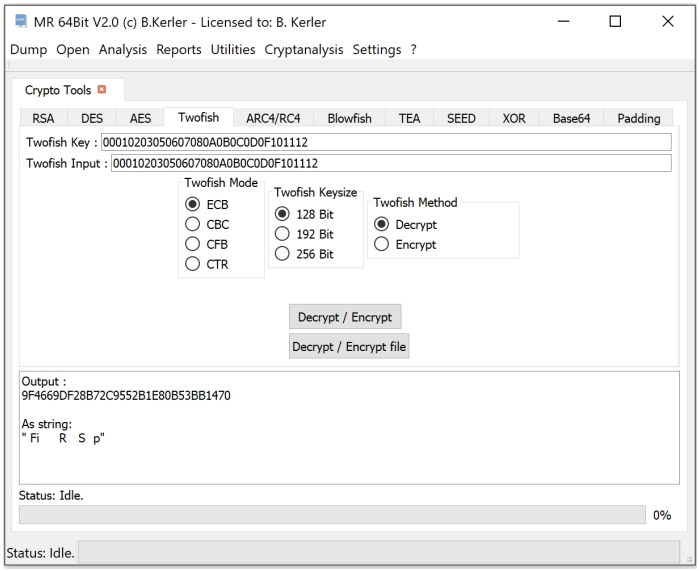
DES


MR 64Bit V2.0 (c) B.Kerler - Licensed to: B. Kerler
Dump Open Analysis Reports Utilities Cryptanalysis Settings ?
Crypto Tools
RSA DES AES Twofish ARC4/RC4 Blowfish TEA SEED XOR Base64 Padding
DES Key : 0123456789ABCDEF
DES Input : 4E6F772069732074
DES Type
DES
2-DES
3-DES
DES Mode
ECB CFB
CBC OFB
DES Method
Decrypt
Encrypt
Iterations
0
Decrypt / Encrypt
Decrypt / Encrypt file
Output :
A416143D9243704C
As string:
" = CpL"
Status: Idle.
0%
Status: Idle.

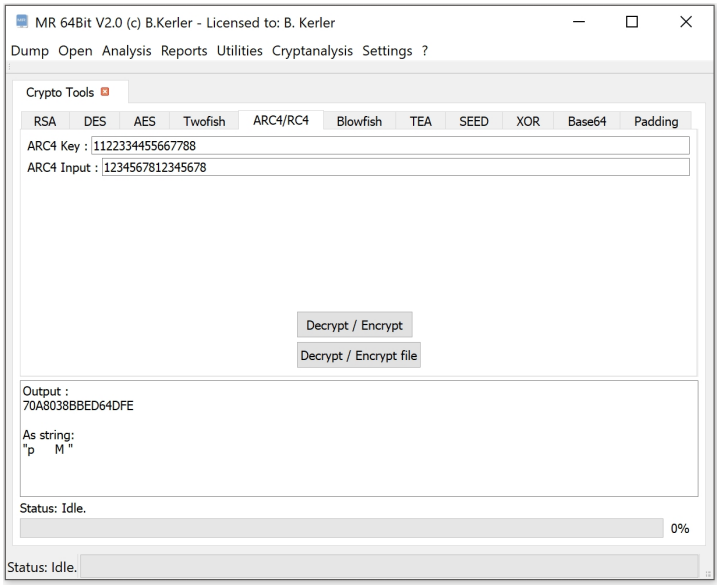
AES


MR 64Bit V2.0 (c) B.Kerler - Licensed to: B. Kerler
Dump Open Analysis Reports Utilities Cryptanalysis Settings ?
Crypto Tools
RSA DES AES Twofish ARC4/RC4 Blowfish TEA SEED XOR Base64 Padding
AES Key : 000102030506070 80A0B0C0D0F101112
AES Input : 000102030506070 80A0B0C0D0F101112
AES Mode
ECB CTR
CBC OFB
CBC_CTS XTS
GCM Wrap
CFB
AES Keysize
128 Bit
192 Bit
256 Bit
AES Method
Decrypt
Encrypt
Decrypt / Encrypt
Decrypt / Encrypt file
Output :
78F142D592759F495F69C5A640811812
As string:
"x B u I_i @ "
Status: Idle.
0%
Status: Idle.

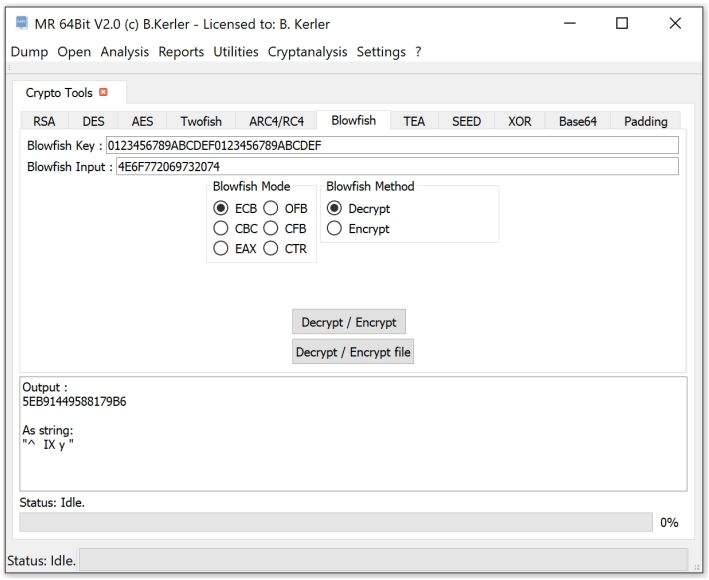
Twofish


MR 64Bit V2.0 (c) B.Kerler - Licensed to: B. Kerler
Dump Open Analysis Reports Utilities Cryptanalysis Settings ?
Crypto Tools
RSA DES AES Twofish ARC4/RC4 Blowfish TEA SEED XOR Base64 Padding
Twofish Key : 000102030506070 80A0B0C0D0F101112
Twofish Input : 000102030506070 80A0B0C0D0F101112
Twofish Mode
ECB
CBC
CFB
CTR
Twofish Keysize
128 Bit
192 Bit
256 Bit
Twofish Method
Decrypt
Encrypt
Decrypt / Encrypt
Decrypt / Encrypt file
Output :
9F4669DF28B72C9552B1E80B53BB1470
As string:
" Fi R S p"
Status: Idle.
0%
Status: Idle.

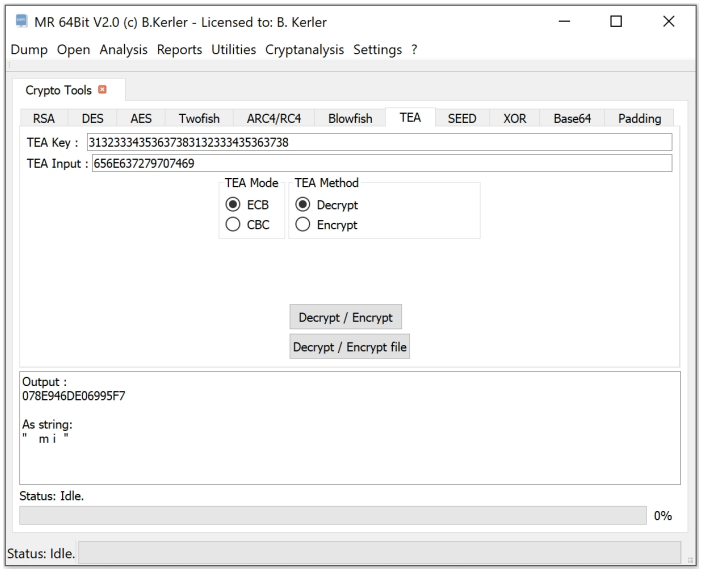
ARC4/RC4


MR 64Bit V2.0 (c) B.Kerler - Licensed to: B. Kerler
Dump Open Analysis Reports Utilities Cryptanalysis Settings ?
Crypto Tools
RSA DES AES Twofish ARC4/RC4 Blowfish TEA SEED XOR Base64 Padding
ARC4 Key : 1122334455667788
ARC4 Input : 1234567812345678
Decrypt / Encrypt
Decrypt / Encrypt file
Output :
70A8038BBED64DFE
As string:
"p M "
Status: Idle.
0%
Status: Idle.

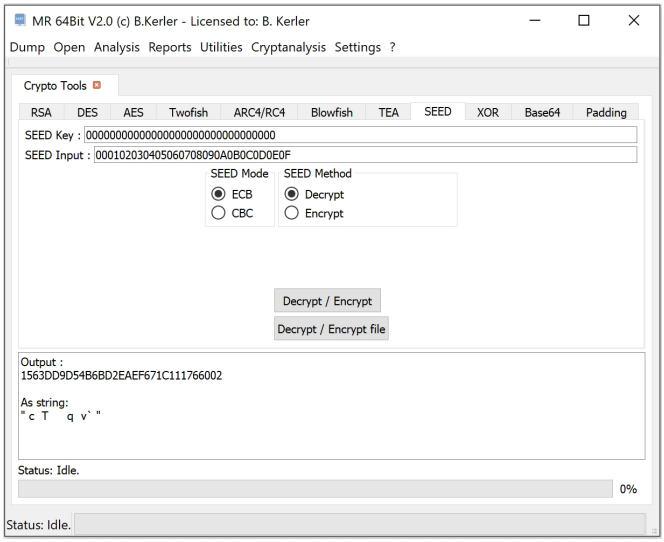
Blowfish


MR 64Bit V2.0 (c) B.Kerler - Licensed to: B. Kerler
Dump Open Analysis Reports Utilities Cryptanalysis Settings ?
Crypto Tools
RSA DES AES Twofish ARC4/RC4 Blowfish TEA SEED XOR Base64 Padding
Blowfish Key : 0123456789ABCDEF0123456789ABCDEF
Blowfish Input : 4E6F772069732074
Blowfish Mode
ECB OFB
CBC CFB
EAX CTR
Blowfish Method
Decrypt
Encrypt
Decrypt / Encrypt
Decrypt / Encrypt file
Output :
5EB91449588179B6
As string:
"^ IX y "
Status: Idle.
0%
Status: Idle.

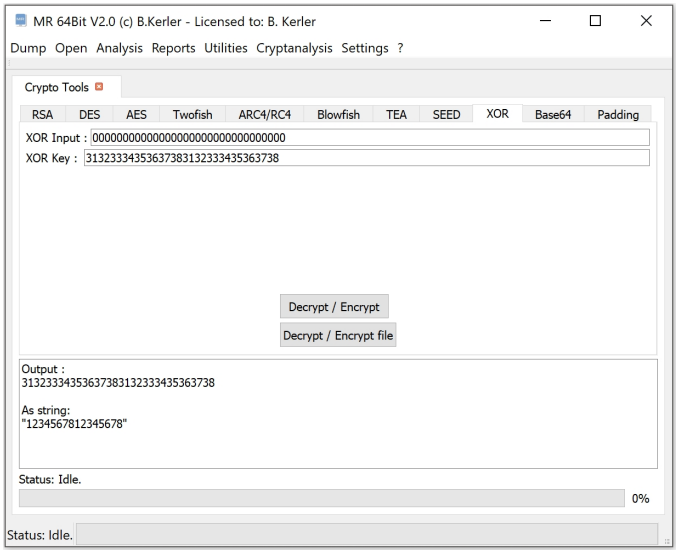
TEA


MR 64Bit V2.0 (c) B.Kerler - Licensed to: B. Kerler
Dump Open Analysis Reports Utilities Cryptanalysis Settings ?
Crypto Tools
RSA DES AES Twofish ARC4/RC4 Blowfish TEA SEED XOR Base64 Padding
TEA Key : 31323334353637383132333435363738
TEA Input : 656E637279707469
TEA Mode
ECB
CBC
TEA Method
Decrypt
Encrypt
Decrypt / Encrypt
Decrypt / Encrypt file
Output :
078E946DE06995F7
As string:
" m i "
Status: Idle.
0%
Status: Idle.

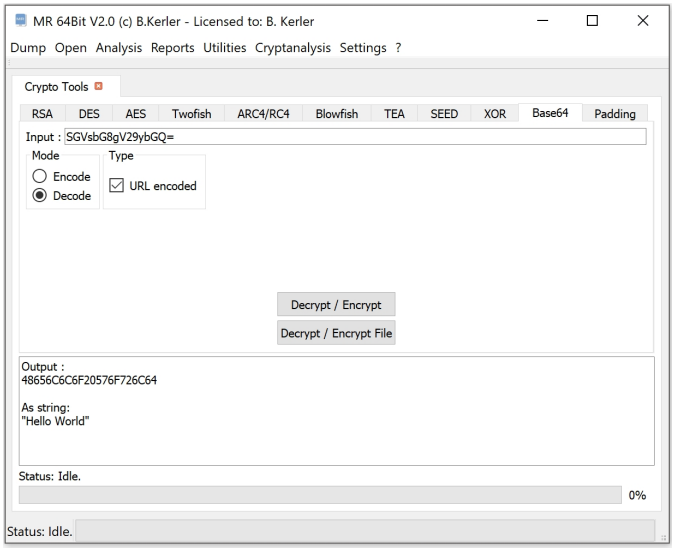
SEED


MR 64Bit V2.0 (c) B.Kerler - Licensed to: B. Kerler
Dump Open Analysis Reports Utilities Cryptanalysis Settings ?
Crypto Tools
RSA DES AES Twofish ARC4/RC4 Blowfish TEA SEED XOR Base64 Padding
SEED Key : 00000000000000000000000000000000
SEED Input : 000102030405060708090A0B0C0D0E0F
SEED Mode
ECB
CBC
SEED Method
Decrypt
Encrypt
Decrypt / Encrypt
Decrypt / Encrypt file
Output :
1563DD9D54B6BD2EAEF671C111766002
As string:
" c T q v` "
Status: Idle.
0%
Status: Idle.

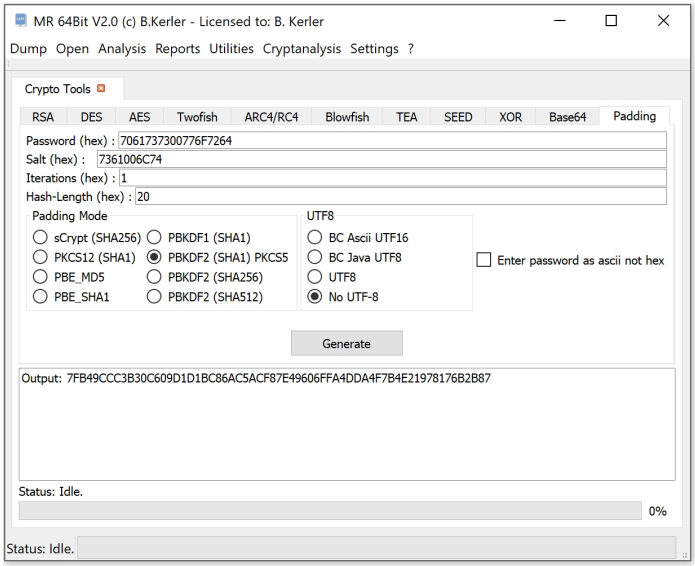
XOR


MR 64Bit V2.0 (c) B.Kerler - Licensed to: B. Kerler
Dump Open Analysis Reports Utilities Cryptanalysis Settings ?
Crypto Tools
RSA DES AES Twofish ARC4/RC4 Blowfish TEA SEED XOR Base64 Padding
XOR Input : 00000000000000000000000000000000
XOR Key : 31323334353637383132333435363738
Decrypt / Encrypt
Decrypt / Encrypt file
Output :
31323334353637383132333435363738
As string:
"1234567812345678"
Status: Idle.
0%
Status: Idle.

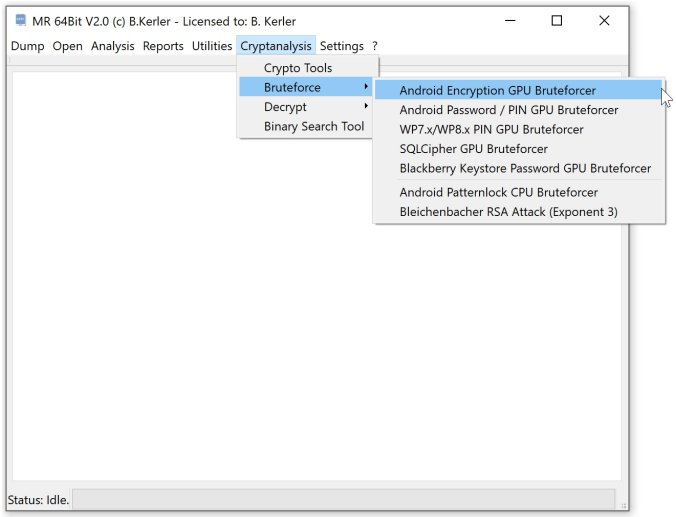
Base64


MR 64Bit V2.0 (c) B.Kerler - Licensed to: B. Kerler
Dump Open Analysis Reports Utilities Cryptanalysis Settings ?
Crypto Tools
RSA DES AES Twofish ARC4/RC4 Blowfish TEA SEED XOR Base64 Padding
Input : SGVsbG8gV29ybGQ=
Mode
Encode
Decode
Type
URL encoded
Decrypt / Encrypt
Decrypt / Encrypt File
Output :
48656C6C6F20576F726C64
As string:
"Hello World"
Status: Idle.
0%
Status: Idle.

Padding

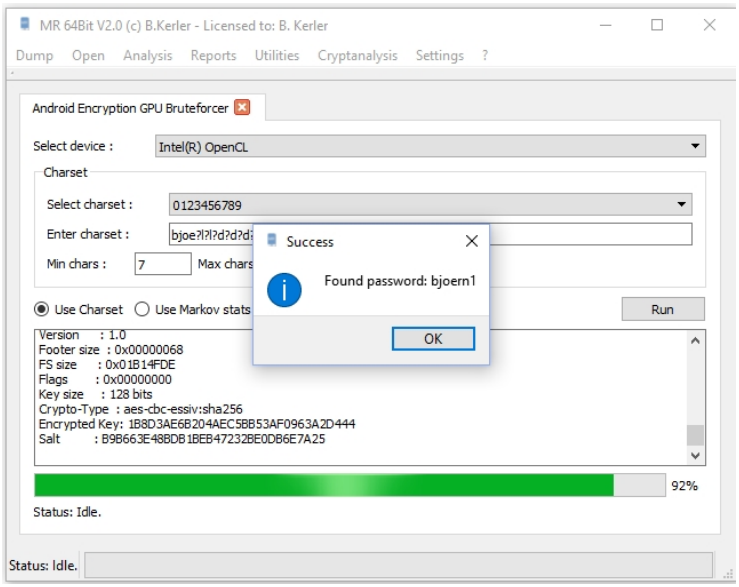

MR 64Bit V2.0 (c) B.Kerler - Licensed to: B. Kerler
Dump Open Analysis Reports Utilities Cryptanalysis Settings ?
Crypto Tools
RSA DES AES Twofish ARC4/RC4 Blowfish TEA SEED XOR Base64 Padding
Password (hex) : 7061737300776F7264
Salt (hex) : 7361006C74
Iterations (hex) : 1
Hash-Length (hex) : 20
Padding Mode
sCrypt (SHA256) PBKDF1 (SHA1)
PKCS12 (SHA1) PBKDF2 (SHA1) PKCS5
PBE_MD5 PBKDF2 (SHA256)
PBE_SHA1 PBKDF2 (SHA512)
UTF8
BC Ascii UTF16
BC Java UTF8
UTF8
No UTF-8
Enter password as ascii not hex
Generate
Output: 7FB49CCC3B30C609D1D1BC86AC5ACF87E49606FFA4DDA4F7B4E21978176B2B87
Status: Idle.
0%
Status: Idle.

Bruteforce



The bruteforce menu offers several functionality in order to bruteforce passwords and pin codes either via GPU or CPU. If no GPU has been installed, it is recommended to install the Intel OpenCL SDK, otherwise the program may crash when trying to use GPU functions. Also we strongly recommend AMD graphic cards, as NVIDIA cards are comparable slower and error prone.

Android Encryption GPU Bruteforcer



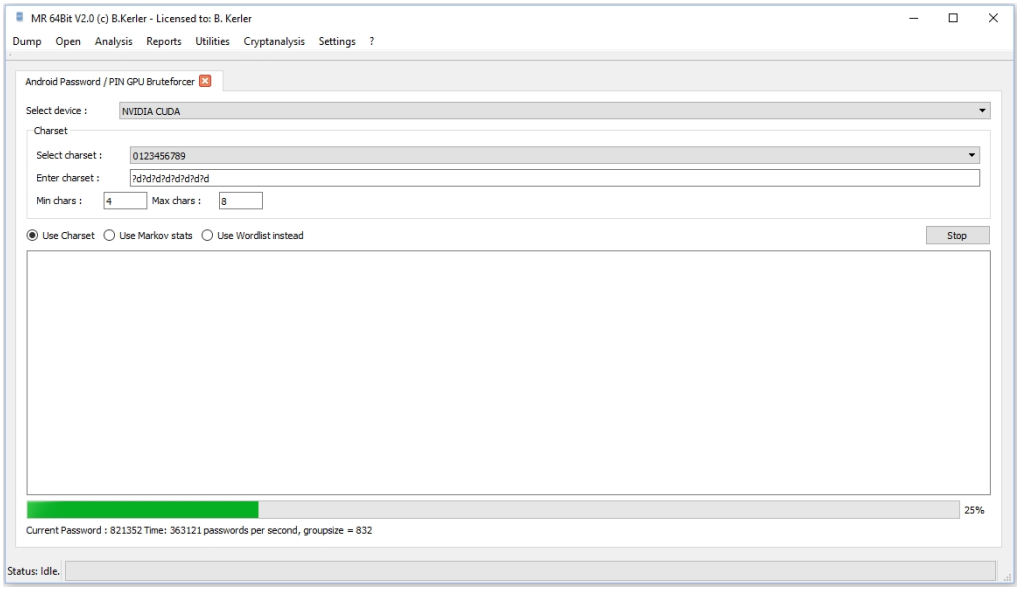
The android GPU encryption bruteforcer is able to bruteforce the PIN/passwords for android devices without hardware encryption using keymaster. Choosing "Markov stats" might speed up password guesses but may not find all passwords and is slower than the "Charset" attack. If you select "Wordlist", you may use a wordlist for bruteforcing instead.

The charset may be any of the known hashcat charsets, which are :

?a = all chars
?d = digit
?u = uppercase letters
?l = lowercase letters
?1 = digits, lower and uppercase letters and some special chars
?2 = 0-9 and A-Z
?3 = a-z and A-Z

For bruteforcing password/PINs, you will need the footer which is either at the end of the userdata partition (last 16K, hex bytes starting with "C5B1B5"
and at least 0xA00 bytes long) or within the metadata partition. The header contains the first 0x1000 bytes from the encrypted userdata partition.

Android Password / PIN GPU Bruteforcer



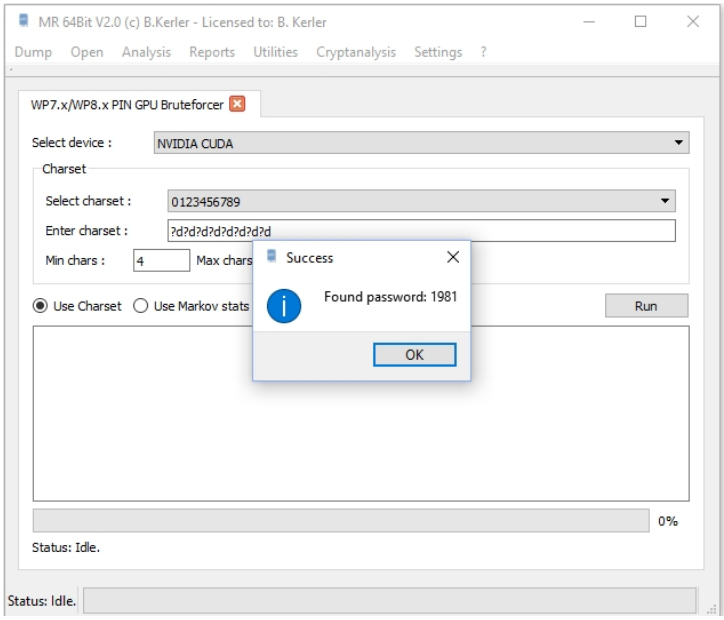
The android password/PIN GPU bruteforcer is able to bruteforce the PIN/passwords for android devices without hardware encryption using keymaster. Choosing "Markov stats" might speed up password guesses but may not find all passwords and is slower than the "Charset" attack. If you select "Wordlist", you may use a wordlist for bruteforcing instead.

The charset may be any of the known hashcat charsets, which are :

?a = all chars
?d = digit
?u = uppercase letters
?l = lowercase letters
?1 = digits, lower and uppercase letters and some special chars
?2 = 0-9 and A-Z
?3 = a-z and A-Z

For bruteforcing password/PINs, you will need the password.key or sparepassword.key file from /data/system as well as either /data/com.android.provider.settings/databases/settings.db for android < 4 or /data/system/locksettings.db including its
-wal and -shm files.

WP7.x/WP8.x PIN GPU Bruteforcer

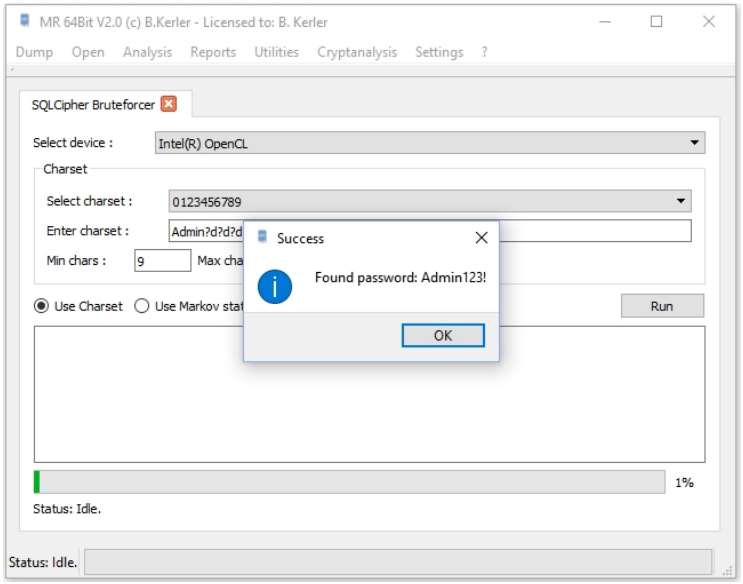


The WP7.x/WP8.x PIN GPU bruteforcer is able to bruteforce the PIN for Windows Phone 7 and 8 devices. The charset may be any of the known
hashcat charsets, which are :

?a = all chars
?d = digit
?u = uppercase letters
?l = lowercase letters
?1 = digits, lower and uppercase letters and some special chars
?2 = 0-9 and A-Z
?3 = a-z and A-Z

For bruteforcing WP PINs, you will need the Registry Files, such as "system.hv" or "SOFTWARE" from MainOS/UserFS partition.
Choosing "Markov stats" might speed up password guesses but may not find all passwords and is slower than the "Charset" attack.
If you select "Wordlist", you may use a wordlist for bruteforcing instead.

SQLCipher Bruteforcer

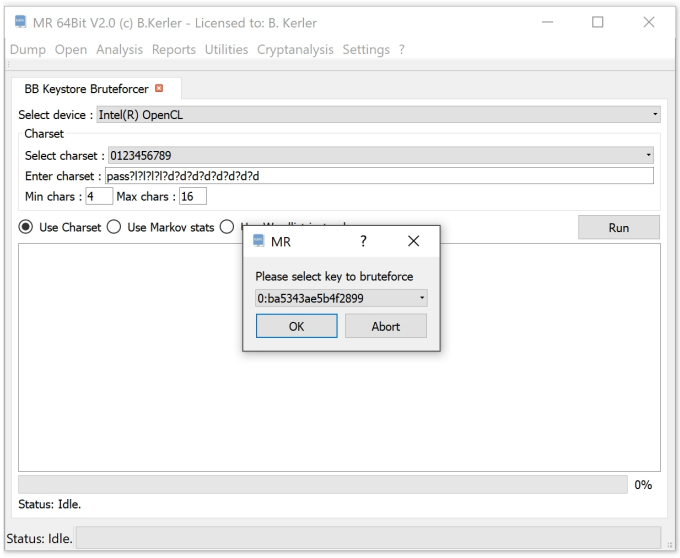


The Sqlcipher GPU bruteforcer is able to bruteforce passwords for encrypted sqlite databases using sqlcipher v2 and v3. The charset may be any of the known hashcat charsets, which are :

?a = all chars
?d = digit
?u = uppercase letters
?l = lowercase letters
?1 = digits, lower and uppercase letters and some special chars
?2 = 0-9 and A-Z
?3 = a-z and A-Z

Choosing "Markov stats" might speed up password guesses but may not find all passwords and is slower than the "Charset" attack.
If you select "Wordlist", you may use a wordlist for bruteforcing instead.

BB Keystore Bruteforcer

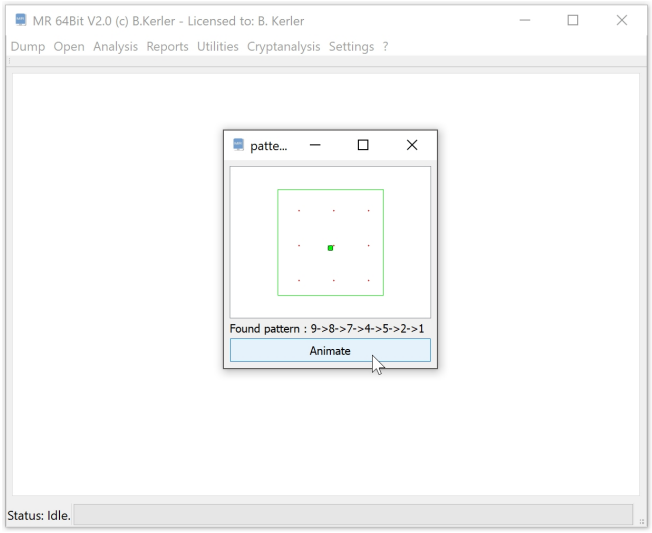


The Blackberry Keystore Password GPU bruteforcer is able to bruteforce keystore passwords for either raw images or .ipd/.bbb backup files. The charset may be any of the known hashcat charsets, which are :

?a = all chars
?d = digit
?u = uppercase letters
?l = lowercase letters
?1 = digits, lower and uppercase letters and some special chars
?2 = 0-9 and A-Z
?3 = a-z and A-Z

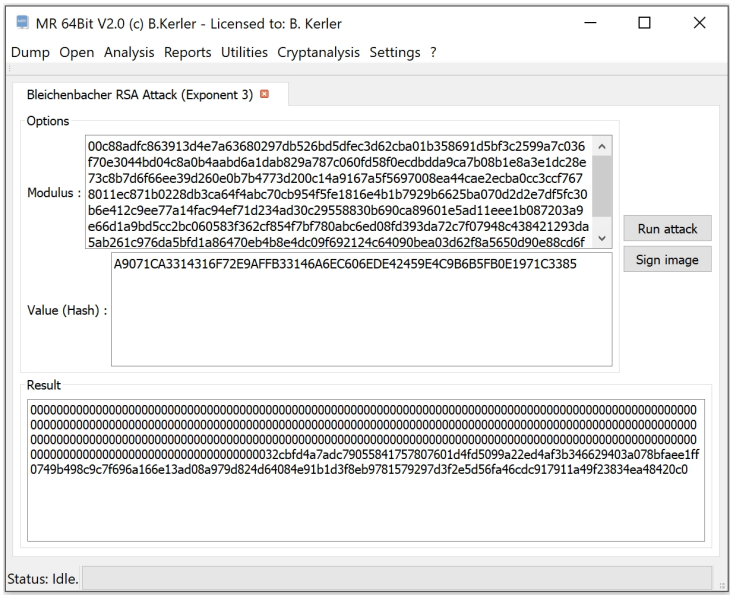
Choosing "Markov stats" might speed up password guesses but may not find all passwords and is slower than the "Charset" attack.
If you select "Wordlist", you may use a wordlist for bruteforcing instead.

Android Patternlock CPU Bruteforcer



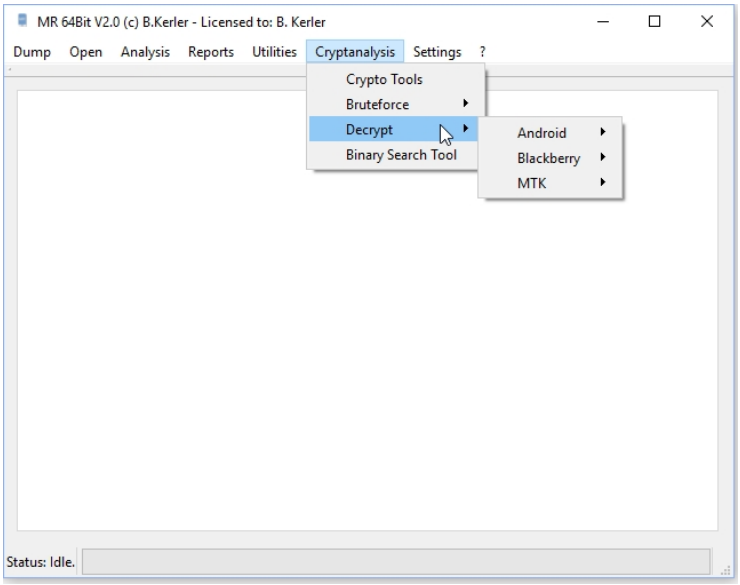
Opening the "gesture.key" file from /data/system directory, this tool will bruteforce and show you the pattern lock. Just press "Animate" to show an emulation of the pattern.

Bleichenbacher RSA Attack (Exponent 3)



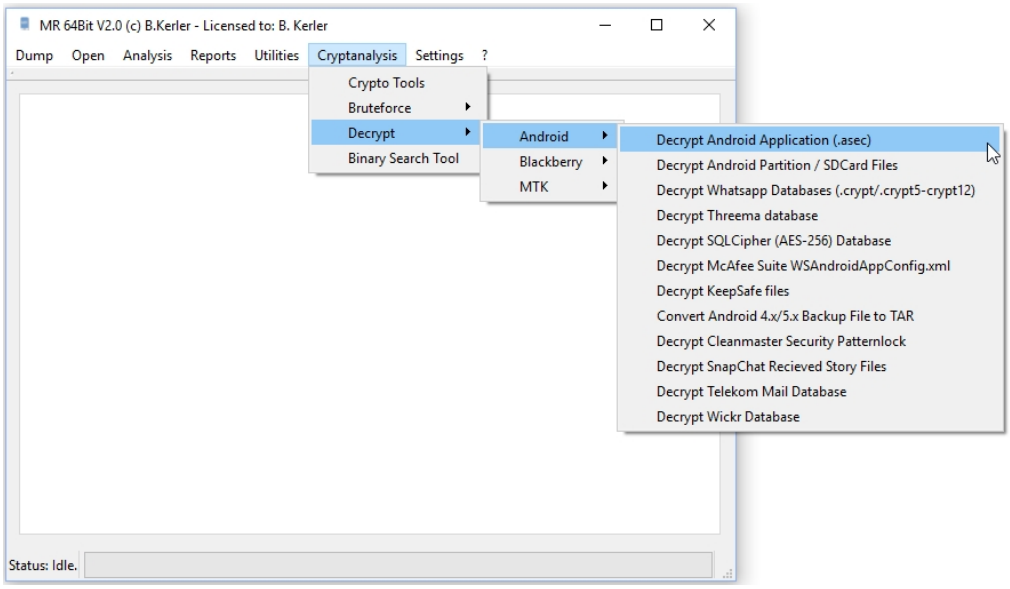
The Bleichenbacher Attack is able to create a fake and valid signature if a rsa certificate with exponent 3 is being used. Using "Sign image" you are able to sign android images. "Run attack" lets you try fake signatures, just set the correct modulus (public key) and the hash value to sign for.

Decrypt



The decrypt menu offers several tools to decrypt vendor specific and app specific encryption.

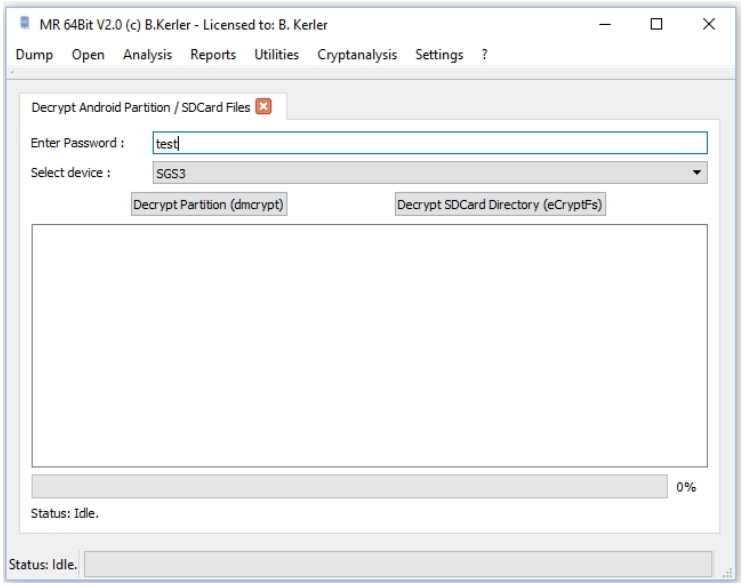
Android


MR 64Bit V2.0 (c) B.Kerler - Licensed to: B. Kerler
Dump
Open
Analysis
Reports
Utilities
Cryptanalysis
Settings
?
Crypto Tools
Bruteforce
Decrypt
Binary Search Tool
Android
Blackberry
MTK
Decrypt Android Application (.asec)
Decrypt Android Partition / SDCard Files
Decrypt Whatsapp Databases (.crypt/.crypt5-crypt12)
Decrypt Threema database
Decrypt SQLCipher (AES-256) Database
Decrypt McAfee Suite WSAndroidAppConfig.xml
Decrypt KeepSafe files
Convert Android 4.x/5.x Backup File to TAR
Decrypt Cleanmaster Security Patternlock
Decrypt SnapChat Recieved Story Files
Decrypt Telekom Mail Database
Decrypt Wickr Database
Status: Idle.

Decrypt Android Application (.asec)

Paid Android Applications may use encrypted Containers with the extension .asec to store the application itself and application data. Those asec files are normally stored into the directory /data/app-asec. For decryption you will need the AppsOnSD.sks file from /data/misc/systemkeys.

Decrypt Android Partition / SDCard Files



This menu lets you decrypt any Android partition via "Decrypt Partition (dmcrypt)" or sdcard raw image via "Decrypt SDCard Directory (eCryptFs)" button. Enter the password before pressing any decrypt button. For SDCard decryption you will need the edk_p_sd file and for partition decryption, you will need the correct footer, starting with hex bytes "C5B1B5" with a size of at least 0x1000 bytes.

Decrypt Whatsapp Databases (.crypt/.crypt5-12)

This function will decrypt all encrypted whatsapp databases (.crypt/.crypt5/.crypt6/.crypt7/.crypt8/.crypt9/.crypt10/.crypt11/.crypt12) in one directory using the "key" file from "/data/data/com.whatsapp/files".

Decrypt Threema database

This function will decrypt any Threema application databases.

Decrypt SQLCipher (AES-256) Database

This function will decrypt any sqlcipher version 2 or 3 encrypted application databases.

Decrypt McAfee Suite WSAndroidAppConfig.xml

This function will decrypt McAfee Suite WSAndroidAppConfig.xml file.

Decrypt KeepSafe files

This function will decrypt any keepsafe files without the need of the PIN.

Convert Android 4.x/5.x Backup File to TAR

This function will decrypt android .ab backup files with the given password to a .tar file.

Decrypt Cleanmaster Security Patternlock

This function will deobfuscate the Patternlock stored in the cleanmaster security config xml "com.cleanmaster.mguard_preferences.xml".

Decrypt SnapChat Received Story Files

This function will try to decrypt all snapchat received story files with known or available aes keys.

Decrypt Telekom Mail Database

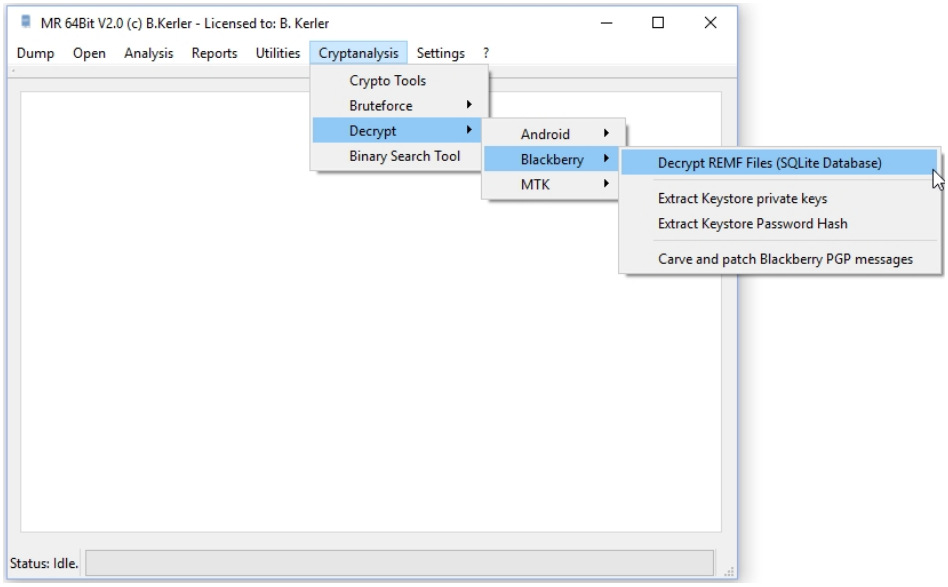
This tool is able to decrypt the Telekom Mail App database.

Decrypt Wickr Database

This tool is able to decrypt wickr databases for both PC (using given password and user SID) and Android (using given password and android_id).

In order to get the user SID for Windows based wickr databases, just run the following command under windows console : "whoami /user". For android databases, the android_id is stored in the database "com.android.providers.settings/databases/settings.db" in the table secure.

Blackberry



The blackberry menu offers tools to bruteforce/extract passwords, but also extract pgp keys from blackberry backups (*.bbb / *.ipd) or raw images.

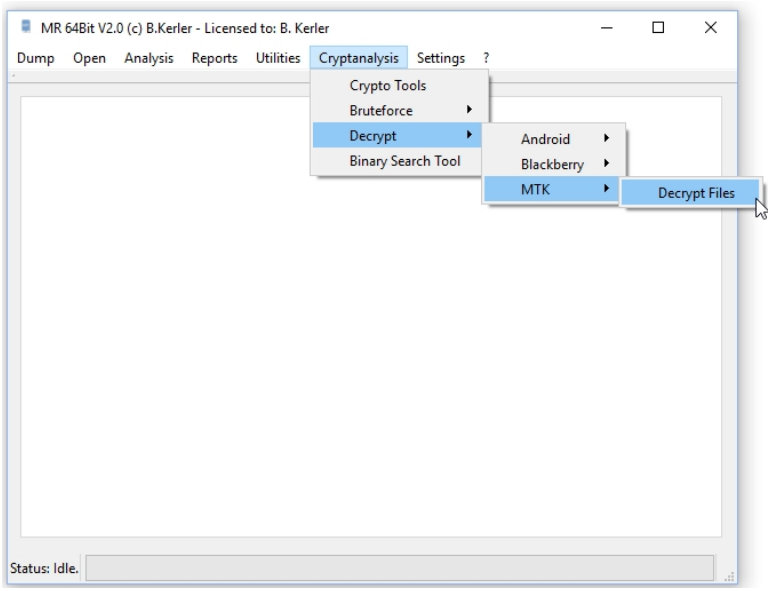
Decrypt Blackberry REMF SQLite Database

This function decrypts any Blackberry SQLite Database encrypted by "REMF" Container using a given Backup .ipd or .bbb file.

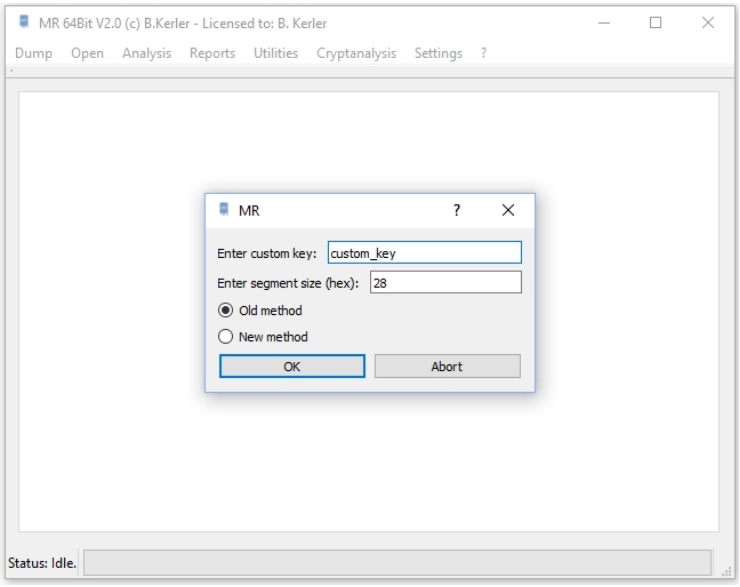
Retrieve Blackberry PGP Private Key

This function will extract any PGP Private key given a password from either Backberry Backup file .ipd/.bbb or any raw flash image after wear leveling has been reconstructed.

MTK

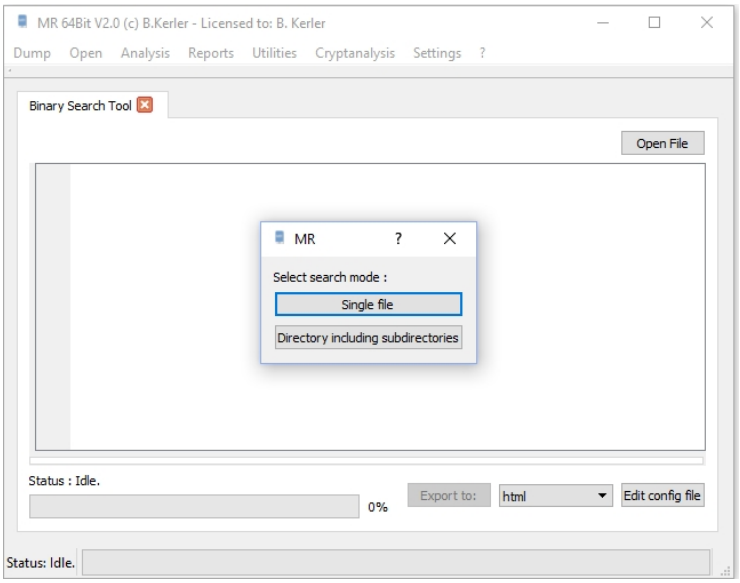

MR 64Bit V2.0 (c) B.Kerler - Licensed to: B. Kerler
Dump
Open
Analysis
Reports
Utilities
Cryptanalysis
Settings
?
Crypto Tools
Bruteforce
Decrypt
Binary Search Tool
Android
Blackberry
MTK
Decrypt Files
Status: Idle.

MTK Decrypt Files



You can decrypt MTK files using this menu. Normally, for correct decryption, segment size has to be modified fitting to the content. If a non-generic MTK key has been used, enter the customkey as ascii, otherwise leave this field empty. Depending on the age of the device, you may need to select new or old method for proper decryption.

Binary Search Tool



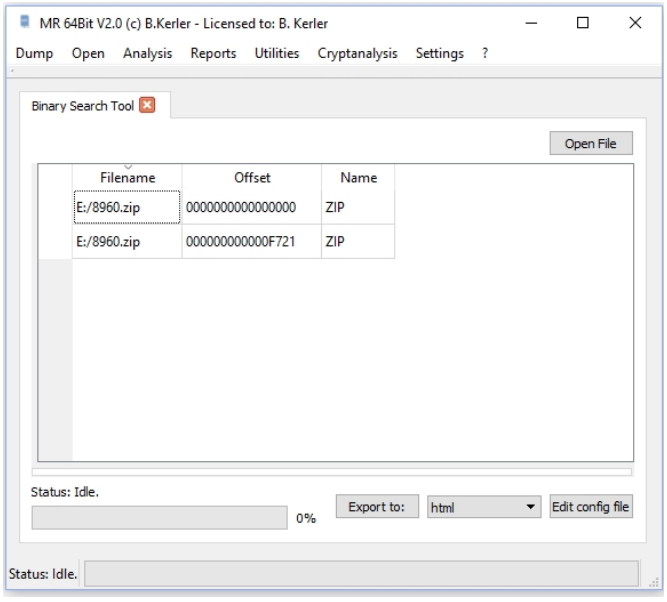
The Binary Search Tool searches for most common file type headers and crypto variables. Using the "Edit config file" button, you may edit the config file that will be used for searching within files.

The structure within the binarysearch.xml file is :

<crypto signature="EB??904D5357494E" name="FAT MSWIN "/>

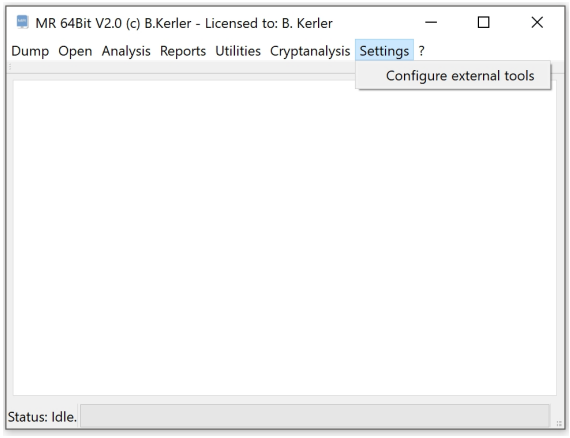
- "signature" specifies the signature in hex bytes to search for. "??" is a wildcard for one byte being unknown.
- "name" specifies the displayed name in the report table.

Pressing "Open File", you may specify to search in one single file or in a directory including the subdirectories.



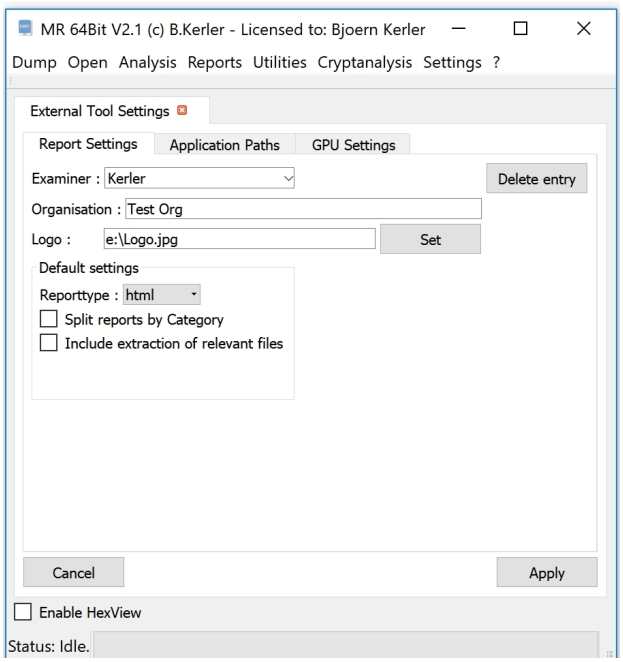
Once it's finished, it's going to show you the corresponding filenames, offsets and the identified name.

Settings

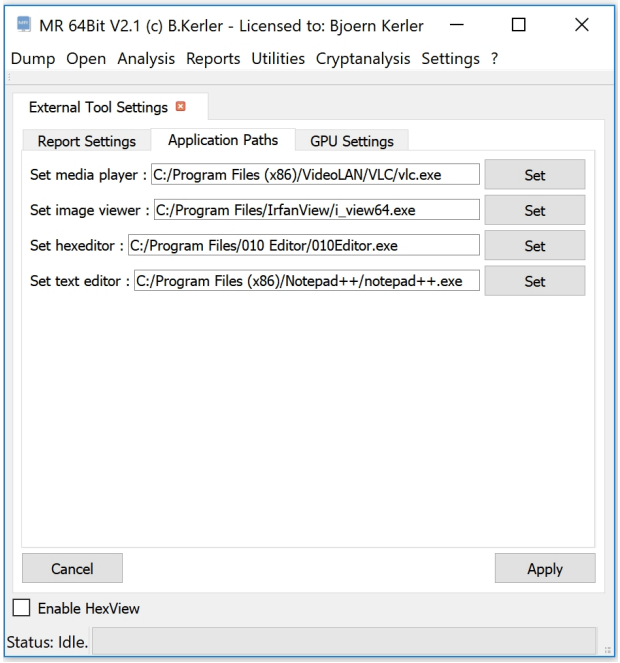


The setting menu uses predefined options for the whole MR program.

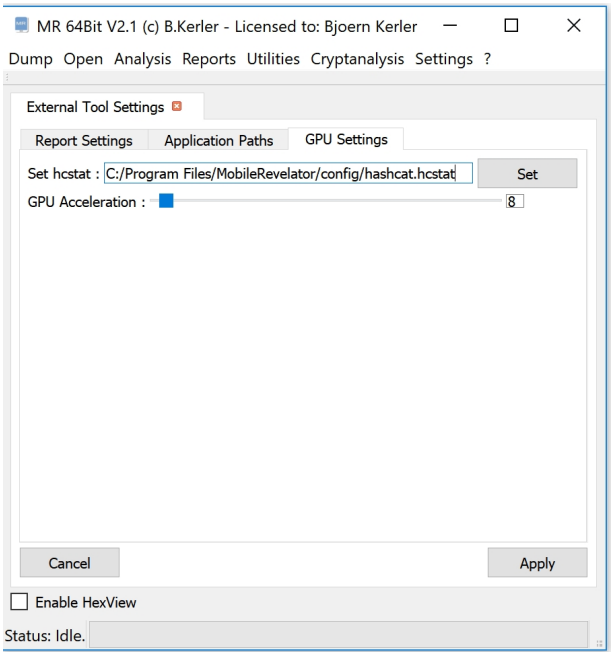
Configure



On the Report Settings screen, you can set default settings for reports, including Examiner and Organisation name and Logo to be displayed on the report.



On the Application Paths screen you can set the application paths for the filesystem tools.



On the GPU Settings tab, you can modify GPU Acceleration and own hcstat files used for GPU Bruteforcing. Higher GPU Accleration can increase speed, but can also crash your graphic card driver or slow down your pc to be unusable.

Press "Set" in order to choose the application executable that should be used. Once you're finished setting up the options, just press "Apply" and the settings will be stored.

Templates Documentation

SQLite Template and Timeline xml Files :

Templates help you to automatically interpret known fields using self-written xml-templates. Pressing "Open template/plugin directory" will open up the directory containing the template directory. Alternatively, you may open up the path "c:\Users\[Username]\Documents\MobileRevelator\templates\" on windows. Templates are being written as package name unter its Operating System Directory name such as "Android" or "iOS".

Timeline XML Documentation

Example :

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<Items>
<Template table="messages" name="Tinder tinder.db" path="tinder.db">
    <column id="user_id (QString)" type="sqlcmd">
      <r cmd="SELECT matches.user_name FROM matches WHERE matches.user_id=='[%1]';"/>
    </column>
    <column id="match_id (QString)" type="sqlcmd">
      <r cmd="SELECT matches.user_name FROM matches WHERE matches.id=='[%1]';"/>
    </column>
</Template>
<Timeline path="com.tinder/databases/tinder.db" type="database">
     <sql cmd="select messages.rowid, messages.created, matches.user_name, messages.text from messages
INNER JOIN matches ON matches.id = messages.match_id;">
        <type text="Tinder" category="Messenger"/>
        <package/>
        <timestamp field="{%1}" format="yyyy-MM-ddThh:mm:ss.zzzZ"/>
        <foregroundtime/>
        <desc/>
        <contact/>
        <contact_alias>
          <field addfields="{%2}"/>
        </contact_alias>
        <message>
          <field addfields="{%3}"/>
        </message>
     </sql>
</Timeline>
</Items>
```

The timeline module has a fixed amount of table columns and are specified as :

type : Title of the extracted content
package : Package information, such as namespace or application
timestamp : Timestamp
foregroundtime : Total commulated foreground time or total call time
desc : Additional data or description
contact : Raw contact id as used by the application
contact_alias : Alias given for a raw contact id
message : Message or Email content only
image : Images as ByteArray to display

All timeline applications can be defined in separate xml files under the os directory name such as "Android" or "Windows". Timeline entries always have to start with "<Timeline" entry. Be aware that you may need to replace special chars as defined at the beginning of the xml file, otherwise the xml file cannot be interpreted correctly.

1. Timeline items

<Timeline path="com.android.providers.media/databases/external.db" type="database">
<Timeline path="databases/analytics_db2" type="database">
<Timeline path="kuaiya.play/databases*emmsg.db" type="database">

Every timeline item is unique for each database being extracted. You can define the path, which points directly to the application database. You may use * as a wildcard, if filename changes or path is unknown. The type defines whether it is an sqlite database as "database" or a raw file with type "raw". For raw files, you need to provide python scripts for decoding.

2. Analysis of Timeline items

<attach database="com.sgiggle.mango/files/profilecache.db" alias="profile"/>

Each item can have different databases being attached using an alias, which can then be used by any sqlite command for

requests. One sqlite request for example with an attached database would be : "select * from profile.table;"

<python run="Zapya (Android)">
<sql cmd="SELECT rowid, name, direction, createtime, url, path, category, totalbytes from transfer;">

You can either run sql commands or run python plugins. Python plugins use the defined plugin name in the python itself. Sql Commands can be any valid sqlite command.

<python run="Zapya (Android)" arguments="user=False">

Using the arguments field, you can send custom small python scripts to the given python script as initial argument being run before running the script. Given arguments can then be used within the script.

3. Categories

For each result of the sql or python result table, you can define where the table cell entry should be used for.

Type:

<type text="Tango Messages" category="Messenger">

The Type field has the description text of the module, called "text" and a describing category which will be listed when the report is done, called "category".

Timestamps and Foregroundtime:

<timestamp field="{%3}" int="/1000"/>
<timestamp field="{%6}" format="yyyy-MM-dd hh:mm:ss"/>
<foregroundtime field="{%5}" int="*1000"/>

In the examples, {%3} and {%6] define the 4th and 7th result entry. The timestamp field additionally contains the function "int", which can be used for calculations of the returned value and the function "format" in case the result value is a formatted time string.

Description, Contact, Contact_Alias, Message, Image:

```
<desc>
   <field addfields="Media_Id: {%4};"/>
   <field addfields="Del_Status: {%12}" replace="0=False;1=True"/>
   <field addfields="Status: &amp;quot;{%5}&amp;quot;" unbase64="0"/>
   <field addfields="Memo:&amp;quot;{%3}&amp;quot;;" unhtml="1"/>
   <field latitude="{%1}" longitude="{%2}"/>
</desc>
```

The field addfields function can be used to combine Text together with result entries. Each field addfields line only is able to hold one result entry. Additionally, you can replace result entries using the "replace" function, whereas each value to be replaced is separated by semicolon. Furthermore result entries with Base64 content can be regulary decoded using the function "unbase64" and the value 0, and url decoded using the value 1. The function "unhtml" with the value 1 can be used to unescape html based text. If a field contains latitude and longitude instead of addfields, it will return a location string based on the given latitude and longitude.

Template XML Documentation

Example :

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<Items>
<Template table="messages" name="Tinder tinder.db" path="tinder.db">
    <column id="user_id (QString)" type="sqlcmd">
      <r cmd="SELECT matches.user_name FROM matches WHERE matches.user_id=='[%1]';"/>
    </column>
    <column id="match_id (QString)" type="sqlcmd">
      <r cmd="SELECT matches.user_name FROM matches WHERE matches.id=='[%1]';"/>
    </column>
</Template>
<Timeline path="com.tinder/databases/tinder.db" type="database">
      <sql cmd="select messages.rowid, messages.created, matches.user_name, messages.text from messages INNER
JOIN matches ON matches.id = messages.match_id;">
         <type text="Tinder" category="Messenger"/>
         <package/>
         <timestamp field="{%1}" format="yyyy-MM-ddThh:mm:ss.zzzZ"/>
         <foregroundtime/>
         <desc/>
         <contact/>
         <contact_alias>
            <field addfields="{%2}"/>
         </contact_alias>
         <message>
            <field addfields="{%3}"/>
         </message>
      </sql>
</Timeline>
</Items>
```

The name-Field is the name being displayed in the Template List. Path should be the name of the database in order to autodetect the database when opening up.
Each template for each table starts with either the "table", in this case "btopp" or a sql database query which starts with "database". If you only want to see
the columns being listed in the template, add the option "deletemissingfields="true". Then, for each column, you may start the following actions :
1. Replace an integer range with text : r from="xxx" to="xxx" with=text"
2. Replace an integer or text with text : r replace="xxx" with="xxx"
3. Run any sqlcmd with the current value in the column [%1] with : r cmd="sqlquery"

Python API Documentation

1. Generic information :

For SQLite or Timeline plugins :

Each python plugin has to have a first line which indicates the name of the plugin, example :
#Pluginname="Telegram Messages (Android)"

For FS plugins :

Each python plugin has to have two first lines which indicate the name and the category of the plugin, example :
#FSPluginname="Telegram Messages (Android)"
#Category="Reports"

Errors on runs can be shown by using the python console display.

The plugin class is **ctx**.

2. Python functions :

Main functions which interact with MR GUI:

void gui_setMainMessage (int type, QString text, QString title) Display a messagebox with title and text, type 0 is Information, type 1 is Warning.
void gui_setMainProgressBar (int pos) Set the main progressbar to a position between 0 and 100
void gui_setMainLabel (QString text) Set the main label
QString gui_getpythonpath() Return the path to the installed python executable
QString gui_getpythonscriptpath() Returns the path where the python scripts reside
QString gui_askSaveDir (QString label) Asks for a directory to save to and returns the directory name, otherwise "" if user aborted.
QString gui_askSaveFile (QString label, QString filename="", QString filter="") Asks for a file name to save and returns the file name. otherwise "" if user aborted.
QString gui_askFile (QString label, QString filename="", QString filter="") Asks for a file name to read and returns the file name. otherwise "" if user aborted.
QString gui_askDir (QString label) Asks for a directory and returns the directory name, otherwise "" if user aborted.
bool gui_askYesNo (QString label) Will display label, asking the user to press yes or no. Result is true for yes and false for no.
void gui_log_addText (QString text, bool clear=false) Add a text to the log window. Set clear if log window shall be cleared first
QString gui_getscriptpath() Returns the current script path.
QString gui_getDate (unsigned int query) Convert unix timestamp to time string.
QString gui_add_report_relevant_file (QString filename) Add report relevant file paths for timeline module to extract.

QVariantList gui_data_size() Return the row and column count from the current table view as List.
QVariant gui_get_data (int row, int col) Get data from current table view
bool gui_set_data (int row, int col, QVariant entry) Set any data in current table view
bool gui_set_data_bytearray (int row, int col, QVariant entry) Set any data as bytearray in current table view
void gui_update() Refresh gui in order to show table results
void gui_update (int connection) Refresh gui in order to show table results for a given sqlite connection index.
bool gui_remove_rows (int row, int col, int count) Remove rows from the current table view.
bool gui_remove_columns (int row, int col, int count) Remove columns from the current table view.
bool gui_add_column (QString text) Add Columns to the current table view.
bool gui_set_data_color (int row, int col, int r, int g, int b, int a=0) Set the background color of a specific cell of the current table view.
QStringList gui_get_headers() Get the headers from the current table view.
bool gui_set_headers (QStringList headers) Set the headers from the current table view.
void gui_clear_data() Clear all table data.
QStringList gui_get_currentcell() Returns current active selected cell (row,column) as an

array.
QStringList pluginfilenames() Returns filenames to be parsed by the timeline module.

FS Browser specific functions:

int fs_file_extract (QString filetoextract, QString outpath) Extract file from file tree, return -1 if it fails.
Example:
fs_file_extract("/data/local/tmp/file.db","C:/extracttohere")
void fs_hide (QString filename) Hide a file from file tree
int fs_isDir (QString filename) Returns 1 if given filename is a directory
int fs_isFile (QString filename) Returns 1 if given filename is a file
int fs_dir_extract (QString dirtoextract, QString outdir) Extract directory from file tree, return -1 if it fails.
Example:
fstree_dir_extract("/data/local/tmp","C:/extracttohere")
QStringList fs_filelist() Returns a list of all files and directories from the file tree
QStringList fs_getselected() Returns a list of all currently selected files
QStringList fs_getDir (QString filename) Returns a list of all files from a given file tree directory
bool fs_sqlcipher_decrypt (QString inputfile, QString outputfile, QString passwd) Decrypt a sqlciphered database using a given password.
QStringList fs_gettime (QString filename) Returns created, lastRead and modified timestamp for a given file as a string list

SQLite functions for accessing databases:

int sqlite_open (QString filename, bool external) Open a file as sqlite database, set external to true for external files, false for files from file tree.
Returns -1 if it fails, otherwise db connection index.
If the filename specific is "gui", the current open database in the program context is being used.
QString sqlite_last_error (int dbconnection) Return the last Sqlite error using a given connection index.
bool sqlite_close (int dbconnection) Close the given db connection index.
int sqlite_run_cmd (int dbconnection, QString query) Runs a given query string using a given db connection index, returns -1 if it fails, otherwise connection index.
Example: "sqlite_run_cmd(dbindex,"SELECT * from table;")",

bool sqlite_cmd_close (int connection) Close the given connection index.
int sqlite_get_deletedrecords (int dbconnection, QString tablename) Returns all reconstructable deleted records and stores them into the sqlite table using given database
connection index.
Returns -1 if it fails, otherwise connection index.

QStringList sqlite_get_headers (int connection) Returns a list with all field names from given connection index.
bool sqlite_set_headers (int connection, QStringList headers) Sets all field names from given connection index and field names as string list.
QVariantList sqlite_get_data_size (int connection) Returns a list with current rows and column count.
QVariant sqlite_get_data (int connection, int row, int col) Return sqlite table entry using given row, column and connection index.
bool sqlite_set_data (int connection, int row, int col, QVariant entry) Set sqlite table entry using given connection index.
Example: "sqlite_set_data(cmdindex,0,0,"Hello World")".
bool sqlite_set_data_bytearray (int connection, int row, int col, QVariant entry) Set sqlite table entry as bytearray using given connection index.
Example: "sqlite_set_data(cmdindex,0,0,"Hello World")".
bool sqlite_remove_rows (int connection, int row, int count) Remove rows at row index with row count using given connection index.
bool sqlite_remove_columns (int connection, int col, int count) Remove columns at column index with column count using given connection index.
bool sqlite_add_column (int connection, QString text) Add column to the sqlite table data with given field name to given connection index.
bool sqlite_set_data_color (int connection, int row, int col, int r, int g, int b, int a) Set sqlite table entry color using given row and column, connection index, and color (rgb) as well as
alpha(transparency) value.
void sqlite_clear_data (int connection) Clear the current sqlite table with given connection index.
bool sqlite_save_as_xlsx (int connection, QString fileName, QString name) Save the current sqlite table as xlsx-file with given connection index, filename to save to and name.

QString sqlite_get_filename (int connection) Return the current sqlite database filename from a given connection index.
QString sqlite_get_filename() Return the current sqlite database filename.

Generic functions:

QByteArray base64todata (QString text, int type) Convert Base64 Data to QByteArray.
QString htmltotext (QString html) Convert HTML to plaintext.
QString getlocationcell (QString mcc, QString mnc, QString lac, QString cid) Convert cell data to location string.
QString getlocation (double lat, double lon) Convert latitude and longitude to string.