Biskus APFS Capture - Manual

Version 1.0

The program offers basically two functions:

1. Copy files off of APFS volumes to a local file system in order to investigate the file *contents*.
2. Create *report* files that contain all *metadata* of the files and directories on APFS volumes.

It can read the data from connected disks and from disk image files.

Preparations & Program Launch

The program is currently delivered without an installer. The program can be launched from any location. On Windows, make sure to keep the included folders besides the .exe file.

Windows

if you want to access attached disks the program needs to run with Administrator rights. You do not need this if you plan to open disk image files taken previous from an APFS disk.

To open the program, right-click on the .exe icon and choose "Run as Administrator".

Mac

In order to read attached disks, two things needs to be prepared:

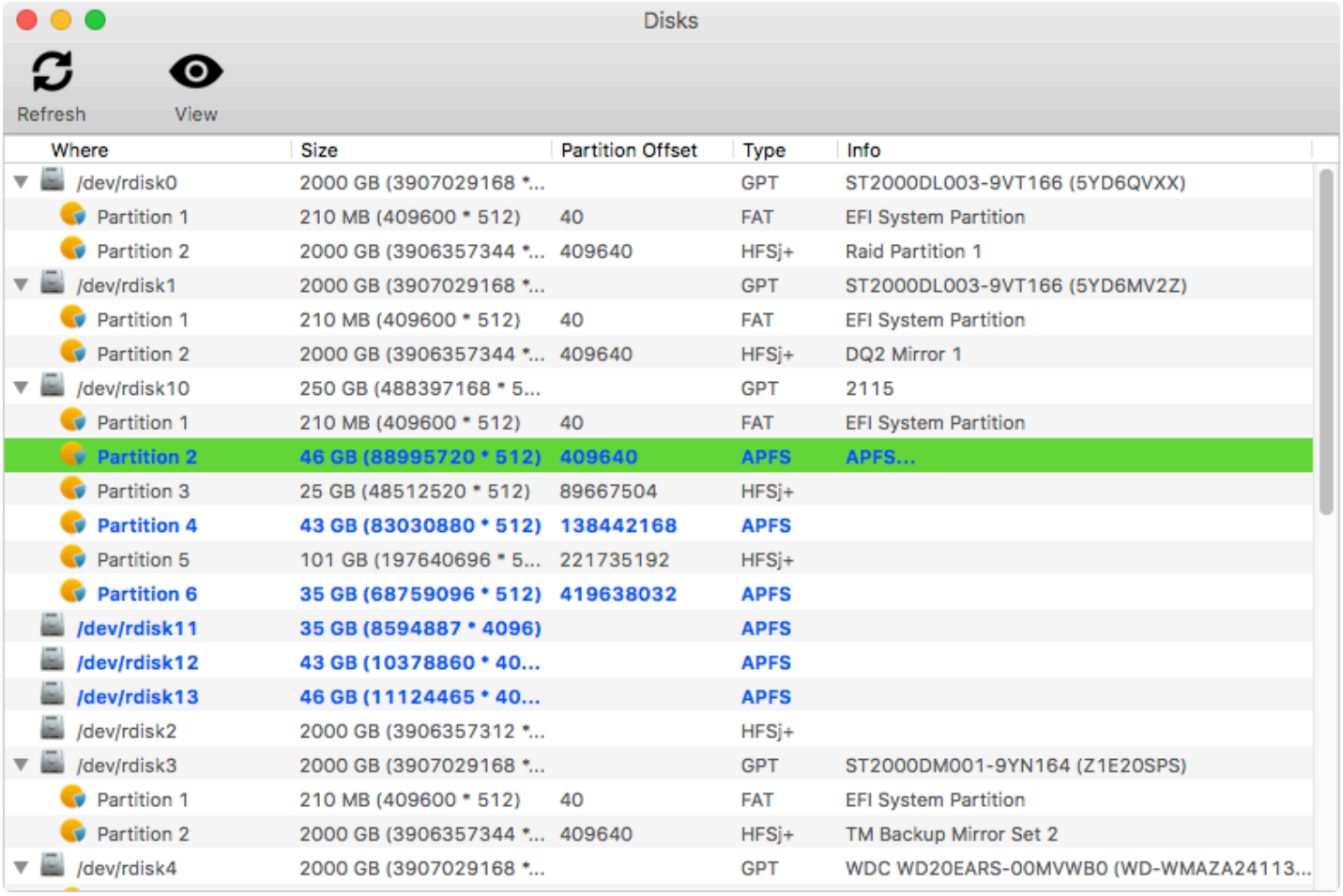
1. If you're running macOS 10.11 or later, SIP needs to be disabled on the computer.
2. The disk device(s) need to be made readable by the current user, e.g. by issuing this command in Terminal.app:

   ```
   sudo chown +r /dev/rdisk*
   ```

If you plan to just open disk image files that have been taken previous from APFS disks, you do not need to take the above steps, though.

Also make sure the APFS volumes you want to inspect are not mounted, or you'll get errors (i.e. you cannot simply try this program out on your boot volume - you need to use an separate volume that you can unmount first!).

The Disks window



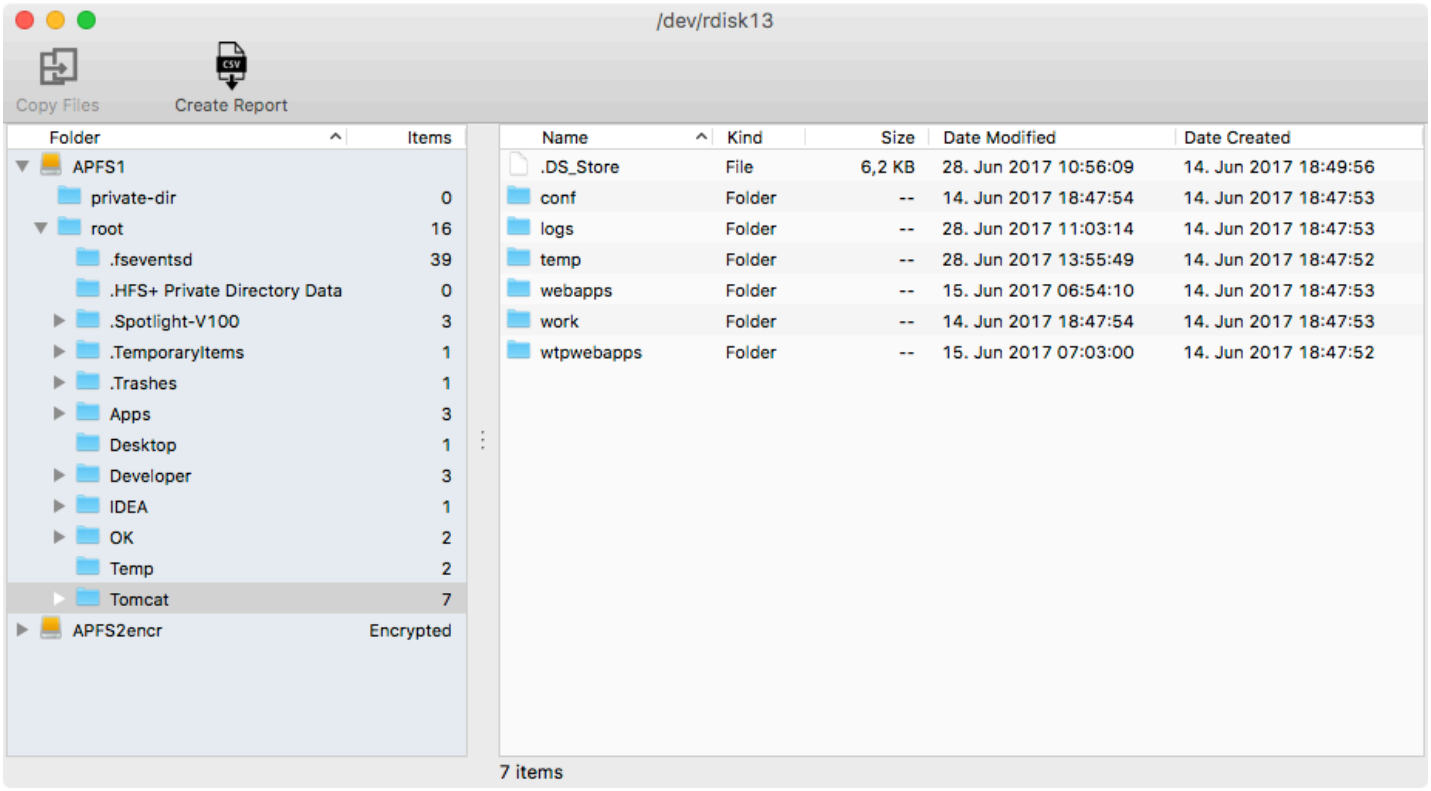
Upon launch of the program, the Disks window appear. It lists all external and internal disks attached to the computer.

To inspect an image file, either drag the file into the Disks window or use the Open command from the File menu.

Note: **Disk images need to be uncompressed**, i.e. plain sector images, and may be either taken from an APFS container partition or from an entire disk. Exception: Compressed disk images taken with iBored can be opened.

If any disks are shown, those that contain APFS partitions will appear in bold blue color. To view their volume contents, double click them.

The File Browser window



The left panel shows the volumes and all directories, whereas the right panel shows the defails of the directly that's been selected in the left panel.

Encrypted volumes are tagged as such and cannot be read, currently.

Copy files

Select a folder or entire volume on the left, then click the **Copy Files** button. This will prompt you to select a local folder to which you want to save the selected folder structure.

While in Trial mode, i.e. if you have not purchase a license and activated it, you can only copy a single file each time you run the program.

Currently, the copy process has the following behaviors:

- Aborts if there is a write error. This is probably always desired.
- Aborts if there is a read error from the APFS container. This may not be desirable if it's a "soft" error, and thus will be improved soon, so that such errors will be collected and listed at the end.
- Does not write symlinks. While this can be implemented easily on macOS, it is a bit difficult to handle on Windows - maybe a shortcut file should be written. Please provide feedback if you care about this.
- Does not write resource forks nor extended attributes. The reason is similar to that for symlinks: It's difficult to apply on Windows.
- Sets only some attributes, such as:
    - Creation date
    - Modification date

- Other attributes, especially those that would limit access (permission, user and group id, invisible state) are not set on purpose. Please give feedback when you need a different behavior.

Please note that all the aforementioned skipped attributes are still accessible through the Report's SQLite database file.

Create Report

When clicking this button, it'll always create a report for the entire APFS container, including all volumes in it (it'll not report any encrypted volumes, though). You will be prompted to choose the location for a .sqlite file.

While in Trial mode, the report will randomly leave out about 30% of inode records.

The Report will generate two files:

1. An sqlite database file
2. A CSV spreadsheet file

The CSV file can be opened in Microsoft Excel, for instance. It will list every file and folder, along with most of its attributes, such as path, name, dates, file size.

The database file can be viewed with various GUI and command line tools.

The database consists of the following tables, which directly imitate the directory records used by APFS (with the exception of the *path* table, which is created from the other tables for your convenience):

Table	Description
disk	The source of the APFS container
volume	Every volume inside the APFS container
named	Every directory entry by its name.inode
extent	An extent used by a file.path
xattr	Extended attributes (resource forks, FinderInfo etc.)

Most records in the tables are linked by their *cnid* (Catalog Node ID) fields, others are linked by their rowid. The columns are accordingly named (such as *inode_cnid* to indicate that it's a reference to a *cnid* in the *inode* table).

The relationships and most important properties are as follows:

- named
  - file name (*named.name*)
  - metadata in inodes (*named.inode_cnid* = *inode.cnid*)

    - parent directory (*named.cnid*)
    - path (*named.cnid* = *path.cnid*)

- inode
    - file content extents (*inode.extent_cnid* = *extent.cnid*)
    - attr records (*inode.cnid* = *xattr.cnid*)

- xattr
    - fork content extents (*xattr.extent_cnid* = *extent.cnid*)

For instance, to list all paths of files that have a resource fork, the following SQL statement would be used:

```
SELECT path, named.name FROM xattr
JOIN inode ON (inode.cnid = xattr.cnid)
JOIN named ON (named.inode_cnid = inode.cnid)
JOIN path ON (path.cnid = named.cnid)
WHERE xattr.name = 'com.apple.ResourceFork'
```

Note how the above relationships are used to get from the xattr table to the path table.

Program updates

The program is still evolving heavily. As long as the program does not check for updates on its own, you will be notified of new versions through the email address you've purchased a license with. You may also send an email to support@biskus.com to request being notified of updates.

Support, Bug Reports, Feature Requests

Write to: Thomas Tempelmann, support@biskus.com