fatlister Documentation

Release 1.0.0

Patrick Neumann

May 09, 2017

Contents:

CHAPTER 1

INTRODUCTION

The task was to write a python script which will analyse a FAT 16 file system and provide the list of files (with metadata) in a CSV format. The functionality is similar to parts of Sleuthkit's *fls* and *istat* commands. The format of the command should be:

```
python fatlister.py [-o offset] [-f filename] imagefile
```

The output should be formatted as:

```
id, path, name, LFN, Allocated, Size, Accessed, Modified, Created, Starting Cluster
```

where:

- id is a unique number (generate by fatlister) for each file
- path is the SFN (short file name) path to the file (root is / as in Linux!)
- name is the SFN in uppercase
- LFN is the Long File Name (if present)
- Allocated is the allocation state (allocated or deleted)
- Size is the file size in Bytes
- Accessed is the Access date
- Modified is the Modified date/time
- Created is the Creation date/time
- Starting Cluster is the first cluster of data content

Some additional notes from the discussions:

- Virtual files and the Volume Label Entry will be skipped.
- The first character of a deleted SFN will be converted to a question mark.
- If the first character of a SFN is \x05 it will be converted to a sigma sign.
- Data and time will be converted to ISO8601.
- An existing output file will not be overwritten. The user has to delete it first.

The script should be well designed and well commented (see *USAGE* and *fatlister MODULE (apidoc)*) and should handle error conditions gracefully (see *EXIT STATES*).

The autodoc feature is not really perfect but better than nothing.

For a report on the testing see *fatlister TESTS*.

CHAPTER 2

USAGE

If you are new to fatlister you may ask yourself how to use it. Here is the answer:

```
$ ./fatlister.py --help
usage: fatlister.py [-h] [-o OFFSET] [-f FILE] image

positional arguments:
  image                 raw image file (esp.: image.dd)

optional arguments:
  -h, --help            show this help message and exit
  -o OFFSET, --offset OFFSET
                        offset in sectors (default=0)
  -f FILE, --file FILE  output file (default="")
```

CHAPTER 3

DESIGN

3.1 Sketch

While breaking down the features into smaller parts (= functions) I decided early to build more a class than a module.

I decided to use python3 because strings in version 3 are unicode by default and the LFN (long file names) are unicode too.

I decided to switch from single variables or dictionaries I passed to the functions in the last assignment to class attributes.

That is the main reason for implementing some "private" functions/methods (getargs and checks) to force other developers to pass the correct arguments to my functions.

While prototyping it has come out that the code will not really become that "complex" like fatmapper. I keeped performance in mind but it was not really measurable.

Because I used simple debugging over and over I left it commented out in the source code for future use.

The development was mostly done under **Arch Linux** and **Python 3.6.1**.

3.2 Documentation

Documentation was done by Spinx-doc (http://www.sphinx-doc.org/) like the last time (fatmapper).

Pylint was to time consuming this time. But I left the output in the documentation for the sake of completeness.

The "real" documentation was generated with **Spinx 1.5.5** and **Pylint 1.7.1** under Arch Linux and Python 3.6.1.

3.3 Tests

fatlister was successfully tested on following systems:

- **ArchLinux** (64-Bit) + python **3.6.1**
- Raspbian GNU/Linux 8.0 (**32-Bit**) + python **3.4.2**
- **macOS** (10.12.4) + python **3.6.1** (from Homebrew)

- Bash on Ubuntu on **Windows 10** “1703” (64-Bit) + python **3.5.2**

fatlister was successfully tested (incl. exit states) with following images:

- raw images
- filesystem(s) in partition(s) <— TODO!
- filesystem without a partition
- no partition/no filesystem (empty file)
- invalid filesystem
- FAT16

CHAPTER 4

fatlister MODULE (apidoc)

List file and directory names in a FAT16 file system (disk image).

class fatlister.**Fatlister**(*image*, *offset*)

Bases: object

printoutput()

Print to stdout.

Prints every item of self.output to stdout.

Parameters **self.output** (*list*) – List with every line of output as a item.

writeoutput()

Write to file.

Writes every item of self.output to a file.

Parameters **self.output** (*list*) – List with every line of output as a item.

Raises Exits if output directory is not writable.

CHAPTER 5

PYLINT REPORT

W: 89,-1: String statement has no effect (pointless-string-statement) W: 93, 0: String statement has no effect (pointless-string-statement) C:289, 8: Invalid attribute name “StartOfFAT0” (invalid-name) C:290, 8: Invalid attribute name “StartOfFAT1” (invalid-name) C:293, 8: Invalid attribute name “firstRootDirectoryEntryLocation” (invalid-name) C:294, 8: Invalid attribute name “startOfClusterArea” (invalid-name) C:295, 8: Invalid attribute name “bytesPerCluster” (invalid-name) C:105, 0: Missing class docstring (missing-docstring) R:105, 0: Too many instance attributes (9/7) (too-many-instance-attributes) R:123, 4: Method could be a function (no-self-use) C:282,12: Invalid variable name “bytesPerSector” (invalid-name) C:283,12: Invalid variable name “sectorsPerCluster” (invalid-name) C:284,12: Invalid variable name “reservedSectors” (invalid-name) C:285,12: Invalid variable name “fatCopies” (invalid-name) C:286,12: Invalid variable name “rootDirectoryEntries” (invalid-name) C:288,12: Invalid variable name “sectorsPerFat” (invalid-name) C:299, 4: Invalid argument name “unsignedShort” (invalid-name) E:299, 4: Method should have “self” as first argument (no-self-argument) C:307, 4: Invalid argument name “unsignedShort” (invalid-name) E:307, 4: Method should have “self” as first argument (no-self-argument) R:319, 4: Too many local variables (35/15) (too-many-locals) C:326, 8: Invalid variable name “directoryOffsets” (invalid-name) C:329, 8: Invalid variable name “longFileName” (invalid-name) C:333,16: Invalid variable name “directoryOffset” (invalid-name) C:334,16: Invalid variable name “fileOffset” (invalid-name) C:340,24: Invalid variable name “fileOffset” (invalid-name) C:354,20: Invalid variable name “filenameExtension” (invalid-name) C:355,20: Invalid variable name “fileAttributes” (invalid-name) C:371,24: Invalid variable name “longFileName” (invalid-name) C:372,24: Invalid variable name “fileOffset” (invalid-name) C:375,20: Invalid variable name “filenameExtension” (invalid-name) C:381,21: Invalid variable name “createdHours” (invalid-name) C:381,35: Invalid variable name “createdMinutes” (invalid-name) C:381,51: Invalid variable name “createdSeconds” (invalid-name) C:382,21: Invalid variable name “createdYear” (invalid-name) C:382,34: Invalid variable name “createdMonth” (invalid-name) C:382,48: Invalid variable name “createdDay” (invalid-name) C:383,21: Invalid variable name “accessedYear” (invalid-name) C:383,35: Invalid variable name “accessedMonth” (invalid-name) C:383,50: Invalid variable name “accessedDay” (invalid-name) C:387,21: Invalid variable name “modifiedHours” (invalid-name) C:387,36: Invalid variable name “modifiedMinutes” (invalid-name) C:387,53: Invalid variable name “modifiedSeconds” (invalid-name) C:388,21: Invalid variable name “modifiedYear” (invalid-name) C:388,35: Invalid variable name “modifiedMonth” (invalid-name) C:388,50: Invalid variable name “modifiedDay” (invalid-name) C:389,20: Invalid variable name “startingCluster” (invalid-name) C:392,24: Invalid variable name “longFileName” (invalid-name) C:393,24: Invalid variable name “clusterOffset” (invalid-name) C:406,24: Invalid variable name “fileOffset” (invalid-name) C:408,20: Invalid variable name “fileSize” (invalid-name) C:421,24: Invalid variable name “longFileName” (invalid-name) C:423,20: Invalid variable name “fileOffset” (invalid-name) W:335,20: Unused variable ‘entry’ (unused-variable) W:360,28: Unused variable ‘step’ (unused-variable) R:319, 4: Too many branches (15/12) (too-many-branches) R:319, 4: Too many statements (67/50) (too-many-statements) W:508, 8: Attribute ‘file’ defined outside __init__ (attribute-defined-outside-init)

CHAPTER 6

EXIT STATES

6.1 Usage (2)

If too few:

```
$ ./fatlister.py
usage: fatlister.py [-h] [-o OFFSET] [-f FILE] image
fatlister.py: error: the following arguments are required: image
```

or too many arguments are supplied:

```
$ ./fatlister.py --offset 0 --too many image.dd
usage: fatlister.py [-h] [-o OFFSET] [-f FILE] image
fatlister.py: error: unrecognized arguments: --too image.dd
```

or if OFFSET is not an integer:

```
$ ./fatlister.py --offset string fat16.dd
usage: fatlister.py [-h] [-o OFFSET] [-f FILE] image
fatlister.py: error: argument -o/--offset: invalid int value: 'string'
```

The exit state of 2 is set by the argparse module.

6.2 Python version (1)

Too old:

```
$ ./fatlister.py
Sorry, your Python version was not tested but may work?
```

Phyton version 2:

```
$ ./fatlister.py
Error: Python 2.x is not supported!
```

6.3 Image file (3/4)

Check if IMAGE exists:

```
$ ./fatlister.py thisimagedoesnotexist.dd
Error: image file does not exist!
```

and is readable:

```
$ ./fatlister.py permission_denied.dd
Error: image file is not readable!
```

6.4 Offset (5)

Check if the offset is positive integer:

```
$ ./fatlister.py --offset -1 fat16.dd
Error: offset is not equal or greater zero!
```

6.5 File (6/7)

Exits if (output) FILE already exists:

```
$ ./fatlister.py --file output_is_already_there.txt fat16.dd
Error: output file already exist!
```

(The user has to delete it first.)

Or the (output) FILE can not be created because of missing write permissions in the target directory:

```
$ ./fatlister.py --file permission_denied/output.csv fat16.dd
Error: output directory is not writable!
```

6.6 Size vs. Offset (8/9)

There is no place for a filesystem in an empty file:

```
$ ./fatlister.py empty.dd
Error: the image file is an empty file!
```

If the offset is too big there will not be enough place for a filesystem:

```
$ ./fatlister.py --offset 65536 fat16.dd
Error: size of the image file is smaller than offset (+ 512 byte)!
```

6.7 Filesystems (10)

fatlister does only support FAT12/FAT16 filesystems:

```
$ ./fatlister.py invalid.dd
Error: no valid FAT12/FAT16 VBR found!
```

CHAPTER 7

fatlister TESTS

7.1 32MB Test image

For the 1st test I created a test image under **Arch Linux** with the folowing bash script:

```
#!/usr/bin/env bash

fallocate -l 32M fat16.dd
mkfs.vfat -F 16 -s 2 -n "IMG_4_A2" fat16.dd

mkdir fat16.loop
mount -o loop fat16.dd fat16.loop

cd fat16.loop

echo "Short file name." > SFN.TXT
echo "Short file name with a leading sigma." > X_SIGMA.TXT
echo "Short file name that will be deleted soon." > DELSFN.TXT

echo "Long file name." > Long_file_name.txt
echo "Long file name with spaces." > "LFN with spaces.txt"
echo "Long file name that will be deleted soon." > Del_long_file_name.txt

dd if=/dev/urandom of=BIGFILE.BIN bs=1024 count=1024

mkdir SDN
cd SDN

mkdir SSUBDN
cd SSUBDN

echo "Another short file name." > SFN2.TXT

cd ../..

mkdir Long_directory_name
cd Long_directory_name

mkdir Long_subdirectory_name
```

```
cd Long_subdirectory_name

echo "Another long file name." > Long_file_name2.txt

cd ../..

mkdir BIGDIR
cd BIGDIR

for id in {01..30} ; do
  echo "I am in the first cluster of the directory." > FILE${id}.TXT
done
echo "I am in the second cluster of the directory." > FILE31.TXT

cd ..

rm DELSFN.TXT
rm Del_long_file_name.txt

cd ..

umount fat16.loop
rmdir fat16.loop

chmod 444 fat16.dd

echo
echo "Do not forget to change the X in X_SIGMA.TXT to \x05 with a hex editor!"
echo

exit 0
```

and executed fatlister:

```
$ ./fatlister.py fat16.dd
# This RFC4180 compliant file was created with fatlister.py at 2017-05-09T00:27:04.
"id", "path", "name", "LFN", "Allocated", "Size", "Accessed", "Modified", "Created
↪", "Starting Cluster"
"0", "/", "SFN.TXT", "", "allocated", "17", "2017-05-08", "2017-05-08T18:10:26",
↪"2017-05-08T18:10:26", "3"
"1", "/", "σ_SIGMA.TXT", "", "allocated", "38", "2017-05-08", "2017-05-08T18:10:26
↪", "2017-05-08T18:10:26", "4"
"2", "/", "?ELSFN.TXT", "", "deleted", "0", "2017-05-08", "2017-05-08T18:10:26",
↪"2017-05-08T18:10:26", "0"
"3", "/", "LONG_F~1.TXT", "Long_file_name.txt", "allocated", "16", "2017-05-08",
↪"2017-05-08T18:10:26", "2017-05-08T18:10:26", "6"
"4", "/", "LFNWIT~1.TXT", "LFN with spaces.txt", "allocated", "28", "2017-05-08",
↪"2017-05-08T18:10:26", "2017-05-08T18:10:26", "7"
"5", "/", "?EL_LO~1.TXT", "Del_long_file_name.txt", "deleted", "0", "2017-05-08",
↪"2017-05-08T18:10:26", "2017-05-08T18:10:26", "0"
"6", "/", "BIGFILE.BIN", "", "allocated", "1048576", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "9"
"7", "/BIGDIR/", "FILE01.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1040"
"8", "/BIGDIR/", "FILE02.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1041"
"9", "/BIGDIR/", "FILE03.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1042"
"10", "/BIGDIR/", "FILE04.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1043"
"11", "/BIGDIR/", "FILE05.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1044"
"12", "/BIGDIR/", "FILE06.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1045"
```

```
"13", "/BIGDIR/", "FILE07.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1046"
"14", "/BIGDIR/", "FILE08.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1047"
"15", "/BIGDIR/", "FILE09.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1048"
"16", "/BIGDIR/", "FILE10.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1049"
"17", "/BIGDIR/", "FILE11.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1050"
"18", "/BIGDIR/", "FILE12.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1051"
"19", "/BIGDIR/", "FILE13.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1052"
"20", "/BIGDIR/", "FILE14.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1053"
"21", "/BIGDIR/", "FILE15.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1054"
"22", "/BIGDIR/", "FILE16.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1055"
"23", "/BIGDIR/", "FILE17.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1056"
"24", "/BIGDIR/", "FILE18.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1057"
"25", "/BIGDIR/", "FILE19.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1058"
"26", "/BIGDIR/", "FILE20.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1059"
"27", "/BIGDIR/", "FILE21.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1060"
"28", "/BIGDIR/", "FILE22.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1061"
"29", "/BIGDIR/", "FILE23.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1062"
"30", "/BIGDIR/", "FILE24.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1063"
"31", "/BIGDIR/", "FILE25.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1064"
"32", "/BIGDIR/", "FILE26.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1065"
"33", "/BIGDIR/", "FILE27.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1066"
"34", "/BIGDIR/", "FILE28.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1067"
"35", "/BIGDIR/", "FILE29.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1068"
"36", "/BIGDIR/", "FILE30.TXT", "", "allocated", "44", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1069"
"37", "/SDN/SSUBDN/", "SFN2.TXT", "", "allocated", "25", "2017-05-08", "2017-05-
↪08T18:10:26", "2017-05-08T18:10:26", "1035"
"38", "/LONG_D~1/LONG_S~1/", "LONG_F~1.TXT", "Long_file_name2.txt", "allocated",
↪"24", "2017-05-08", "2017-05-08T18:10:26", "2017-05-08T18:10:26", "1038"
```

The Verification was (not really) **successful**:

```
$ fls -F -r fat16.dd | grep -v 'v/v' | grep -F -v 'Volume Label Entry'
r/r 4:        SFN.TXT
r/r 5:        ^_SIGMA.TXT
r/r * 6:        _ELSFN.TXT
r/r 9:        Long_file_name.txt
r/r 12:        LFN with spaces.txt
r/r * 15:        Del_long_file_name.txt
r/r 16:        BIGFILE.BIN
```

```
r/r 33541:        SDN/SSUBDN/SFN2.TXT
r/r 33639:        Long_directory_name/Long_subdirectory_name/Long_file_name2.txt
r/r 33701:        BIGDIR/FILE01.TXT
r/r 33702:        BIGDIR/FILE02.TXT
r/r 33703:        BIGDIR/FILE03.TXT
r/r 33704:        BIGDIR/FILE04.TXT
r/r 33705:        BIGDIR/FILE05.TXT
r/r 33706:        BIGDIR/FILE06.TXT
r/r 33707:        BIGDIR/FILE07.TXT
r/r 33708:        BIGDIR/FILE08.TXT
r/r 33709:        BIGDIR/FILE09.TXT
r/r 33710:        BIGDIR/FILE10.TXT
r/r 33711:        BIGDIR/FILE11.TXT
r/r 33712:        BIGDIR/FILE12.TXT
r/r 33713:        BIGDIR/FILE13.TXT
r/r 33714:        BIGDIR/FILE14.TXT
r/r 33715:        BIGDIR/FILE15.TXT
r/r 33716:        BIGDIR/FILE16.TXT
r/r 33717:        BIGDIR/FILE17.TXT
r/r 33718:        BIGDIR/FILE18.TXT
r/r 33719:        BIGDIR/FILE19.TXT
r/r 33720:        BIGDIR/FILE20.TXT
r/r 33721:        BIGDIR/FILE21.TXT
r/r 33722:        BIGDIR/FILE22.TXT
r/r 33723:        BIGDIR/FILE23.TXT
r/r 33724:        BIGDIR/FILE24.TXT
r/r 33725:        BIGDIR/FILE25.TXT
r/r 33726:        BIGDIR/FILE26.TXT
r/r 33727:        BIGDIR/FILE27.TXT
r/r 33728:        BIGDIR/FILE28.TXT
r/r 33729:        BIGDIR/FILE29.TXT
r/r 33730:        BIGDIR/FILE30.TXT
r/r 34691:        BIGDIR/FILE31.TXT
```

7.2 More Test images

There was not enough time for more testing... SORRY!

7.3 Summary

The result of the test was that fatlister should work as expected! (not really)

CHAPTER 8

CHANGES in fatlister

8.1 Release 1.0 (in development)

8.1.1 (Incompatible) changes

- none

8.1.2 Features added

- none

8.1.3 Bugs fixed

- none

CHAPTER 9

TODOs for fatlister

As time of writing this documentation there was left a missing feature:

If a directory has more entries than a single cluster is able to store, the next clusters are ignored.

CHAPTER 10

fatlister AUTHORS

fatlister is written and maintained by Patrick Neumann <patrick@neumannsland.de>.

CHAPTER 11

LICENSE

11.1 Comments and Documentation

You are free to:

Share — copy and redistribute the material in any medium or format Adapt — remix, transform, and build upon the material

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

NonCommercial — You may not use the material for commercial purposes.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Notices:

You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation. No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material.

Source: https://creativecommons.org/licenses/by-nc/4.0/legalcode

11.2 Software

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

See the LICENSE file for more details.

CHAPTER 12

Indices and tables

- genindex
- modindex
- search

Python Module Index

f

Index