Exiv2 - Bug #1347

Segfault in Digikam when saving/loading certain TIFF images

29 Apr 2018 10:09 - V Engmark

Status:	Closed	**Start date:**	29 Apr 2018
Priority:	Normal	**Due date:**	
Assignee:	Robin Mills	**% Done:**	100%
Category:	insufficient information	**Estimated time:**	2.00 hours
Target version:	0.27		

Description

Already reported at <https://bugs.kde.org/show_bug.cgi?id=393635&gt;, I was told to report it here as well.

History

#1 - 29 Apr 2018 10:11 - V Engmark

That would be https://bugs.kde.org/show_bug.cgi?id=393635

#2 - 29 Apr 2018 10:19 - Robin Mills

- Category set to tiff parser

- Status changed from New to Assigned

- Assignee set to Robin Mills

- Priority changed from High to Normal

- Target version set to 0.27

Can you attach the test image, please?

#3 - 29 Apr 2018 10:21 - V Engmark

Here you go: https://transfernow.net/612xx2l6shgd

#4 - 10 May 2018 13:18 - Robin Mills

Apologies for the delay in dealing with this. I hosted the Exiv2 Developer's Meeting at my home last weekend and been very busy with other Exiv2 matters.

I don't have an account with transfernow.net Can you attach the files to this issue, please?

#5 - 18 Sep 2018 12:33 - Robin Mills

- Category changed from tiff parser to insufficient information

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

- Estimated time set to 1.00 h

#6 - 22 Sep 2018 09:41 - V Engmark

- File _MG_5144_v1.TIFF added

#7 - 22 Sep 2018 16:47 - Robin Mills

- Category changed from insufficient information to tiff parser

- Status changed from Closed to Assigned

- % Done changed from 100 to 20

- Estimated time changed from 1.00 h to 2.00 h

Thanks for the file. I've reopened the case.

#8 - 22 Sep 2018 19:22 - Robin Mills

- Category changed from tiff parser to insufficient information

- Status changed from Assigned to Closed

Regrettably, your file doesn't give me anything to investigate. Neither Exiv2 v0.26 nor the current 'master' (which will release as v0.27 later in 2018) exhibit problems with your file.

```
539 rmills@rmillsmbp:~/gnu/exiv2/v0.26 $ exiv2 -pa ~/Downloads/_MG_5144_v1.TIFF | wc
Warning: Directory Image3, entry 0x0111: Strip 0 is outside of the data area; ignored.
     238   30271  296580
540 rmills@rmillsmbp:~/gnu/exiv2/v0.26 $ cd ../../github/exiv2/exiv2/build
541 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ bin/exiv2 -pa ~/Downloads/_MG_5144_v1.TIFF | wc
Warning: Directory Image3, entry 0x0111: Strip 0 is outside of the data area; ignored.
     238   30271  296580
542 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ 
```

I'm happy to work to resolve your issue when we have a definition that can be reproduced with the command-line program exiv2. I'm unable to investigate any issue which can only be produced using digiKam.

#9 - 22 Sep 2018 20:12 - Robin Mills

- % Done changed from 20 to 100

#10 - 22 Sep 2018 20:53 - V Engmark

The Digikam people insist it's an Exiv2 problem - please see https://bugs.kde.org/show_bug.cgi?id=393635#c16

#11 - 22 Sep 2018 21:13 - Robin Mills

Please ask the DigiKam Engineers to reproduce your issue with the eviv2 command-line program and your issue will be investigated.

#12 - 23 Sep 2018 07:57 - Robin Mills

I've read digicam's bug report and I see it's in printStructure(). A great deal of work has been done for v0.27 concerning printStructure() and I'm confident that this issue has been resolved. I'm on vacation this week, however I'm hoping to releasee Exiv2 v0.27 RC1 when I return home in early October. I recommend that dikiKam build with Exiv2 v0.27 RC1 and verify that this issue has been resolved.

#13 - 23 Sep 2018 09:00 - Gilles Caulier

If the Exiv2 code from git/master is enough stable, i can start to embed this Exiv2 0.27 pre-version in the digiKam bundles (AppImage for Linux, PKG for MacOS, and MXE for windows).

To clarify your ideas and viewpoints about the Exiv2 use-case in DK : Exiv2 API are used in a Qt wrapper which is used multi-threaded everywhere. This point is very important, as trying to reproduce a bug in Exiv2 CLI tool cannot be enough to validate a report as a bug.

All the Exiv2 API must be re-entrant and must support multi-core (we dont not use mutex in this wrapper for the moment). Multi-threading is the way to use this king of library to process metadata in the background without to block the GUI. This permit also to speed-up process using all computer core, and not only one.

In DK, we use multi-core everywhere : database queries, image processing, file management, and of course metadata. DK play with metadata only through Exiv2. This can be around the file from disk, but also in memory though byte-array, for exemple to prepare the registration of photo informations in database.

And of course, there is a famous point of XMP SDK from Adobe. We have a copy inside DK core to build the DNG SDK from Adobe in goal to convert RAW file to DNG. All source code from Adobe are bad quality, as i can see through the reports from static analyzer. So, i'm sure that re-entrancy is not respected everywhere with XMP SDK (it's easy to see, with source code and the way to implement some classes).

So you must considerate the XMP SDK as a critical section in Exiv2. You must take a care.

This is imply to have few test units in Exiv2 which test the re-entrancy of all API with a complete collection of images. Re-using the exist test to run in separated thread can be a solution.

The DK users base is very important, especially since the Windows version become better and better (thanks to MXE cross-compilation). We can provide an alpha version of Exiv2 in the pre-release bundles published weekly. We will receive quickly a feedback about the code stability.

Gilles Caulier

#14 - 23 Sep 2018 09:08 - Gilles Caulier

Another point very import : in digiKam bundle, e disable few option that don't use or considerate as very instable :

https://cgit.kde.org/digikam.git/tree/project/bundles/3rdparty/ext_exiv2/CMakeLists.txt

For exemple, the video support in Exiv2 crash digiKam in few seconds. We use ffmpeg metadata parser instead in digiKam.

Gilles Caulier

#15 - 23 Sep 2018 09:24 - Gilles Caulier

- File exiv2-0.27-clang-scan-build-report.tar.lzma added

Exiv2 0.27 git code parsed with clang scan-build static analyzer.

Enjoy the XMP SDK source code...

Gilles Caulier

#16 - 23 Sep 2018 09:27 - Gilles Caulier

Note about clang scan-build report : it compile files and parse at the same time. So, only compiled files are checked.

I use this script to configure Exiv2 :

https://cgit.kde.org/digikam.git/tree/project/scripts/bootstrap-exiv2.sh

So take a care, not all Exiv2 code are compiled in this report, as it's the configuration used for digiKam...

Gilles Caulier

#17 - 23 Sep 2018 09:35 - Gilles Caulier

- File exiv2-0.27-cppcheck-report.tar.lzma added

Exiv2 0.27 git code parsed with cppcheck static analyzer.

Note : no code are compiled here and all source code are parsed as well...

Gilles Caulier

#18 - 23 Sep 2018 18:58 - Robin Mills

- Status changed from Closed to Assigned

Thank You, Gilles, for all this valuable feedback. I hope you're good and recovered from your accident.

Your observations about multi-threading are valid. Perhaps we should be give multi-threading more consideration in v0.28. I'm glad to let you know that I have a couple of very good engineers working with me on Exiv2 and they have undertaken most of the work for v0.27. I've been hoping to retire from Exiv2 and perhaps I really will retire in another year or two!

The primary goal of v0.27 has been to fix lots of security flaws which have been reported during the last 12 months. I hope to publish RC1 in early October and aiming for GM in December. Exiv2 v0.27 will have "long term support" and "dot releases" (exiv2 v0.27.1 , v0.27.2 etc) will have security features added in parallel to the development of v0.28.

I believe one of your DK colleagues discussed printStructure() with me last year. Here's my reply.
http://dev.exiv2.org/boards/3/topics/3080?r=3081#message-3081

I'm on vacation at the moment. I'll have to find time to review your various contributions and decide how to proceed. If you have specific changes you want in Exiv2 v0.27 RC1, I recommend that your report an issue (preferably as a PR) to http://github.com/exiv2/exiv2 and Dan or Luis (my wonderful team mates) may accept and integrate your suggestions.

I am very pleased that you are interested in integrating Exiv2 v0.27 RC1 into digiKam. During the 6 month review period for Exiv2 v0.26, I don't recall anybody reporting anything concerning any release candidate. No matter how much testing Team Exiv2 performs, there are execution paths which are unique to applications such as digiKam. Your feedback is valuable and appreciated.

#19 - 08 Nov 2018 09:43 - Robin Mills

- Status changed from Assigned to Closed

I'm going to close this issue. The files attached to this issue are not exhibiting issues.

I know that Gilles means well by giving my vast amounts of information about threading and all manner of concerns. This needs to be distilled into specific issues and reported on https://github.com/exiv2/exiv2 in 2019. The team is totally focused on achieving Exiv2 v0.27 GM by the end of 2018.

Files

_MG_5144_v1.TIFF	13.4 MB	22 Sep 2018	V Engmark
exiv2-0.27-clang-scan-build-report.tar.lzma	168 KB	23 Sep 2018	Gilles Caulier
exiv2-0.27-cppcheck-report.tar.lzma	430 KB	23 Sep 2018	Gilles Caulier