Exiv2 - Bug #1139

LibExiv2 0.25 crashes with digiKam version 4.14.0

18 Dec 2015 07:15 - valerie venet

Status:	Closed	**Start date:**	18 Dec 2015
Priority:	Normal	**Due date:**	
Assignee:	Robin Mills	**% Done:**	100%
Category:	video	**Estimated time:**	2.00 hours
Target version:	0.26		

Description

Hi,

I've posted the following bug to this forum: https://bugs.kde.org/show_bug.cgi?id=356704

The guy said "If problem still here with 0.25, report the problem to Exiv2 team"

Here are the logs :

digiKam version 4.14.0
Composant graphique Marble: 0.21.80 (0.22 Beta 1)
Dématriçage parallélisé: Inconnu
Exiv2 peut écrire dans un fichier JP2: Oui
Exiv2 peut écrire dans un fichier JPEG: Oui
Exiv2 peut écrire dans un fichier PGF: Oui
Exiv2 peut écrire dans un fichier PNG: Oui
Exiv2 peut écrire dans un fichier TIFF: Oui
Exiv2 prend en charge les métadonnées XMP: Oui
LibCImg: 130
LibEigen: 3.2.7
LibExiv2: 0.25
LibJPEG: 80
LibJasper: 1.900.1
LibKDE: 4.14.14
LibKExiv2: 2.4.0
LibKGeoMap: 3.1.0
LibKdcraw: 2.4.2
LibLCMS: 2070
LibLensFun: 0.3.1-0
LibPGF: 6.14.12
LibPNG: 1.6.19
LibQt: 4.8.7
LibRaw: 0.17.0
LibTIFF: LIBTIFF, Version 4.0.6 Copyright (c) 1988-1996 Sam Leffler Copyright (c) 1991-1996 Silicon Graphics, Inc.
Prise en charge de LibLqr: oui
Prise en charge du codec RawSpeed: Inconnu
Prise en charge du pack Demosaic GPL2: Inconnu
Prise en charge du pack Demosaic GPL3: Inconnu
cœurs de processeur: 8
LibGphoto2: 2.5.8
LibKface: 3.5.0
LibKipi: 2.2.0
LibOpenCV: 2.4.12.2
Modules externes KIPI: 4.14.0
Moteur de base de données: QSQLITE
Prise en charge de Baloo: Oui
Prise en charge de SQLite2: non
Prise en charge des KDEPIMlibs: non

Application: digiKam (digikam), signal: Aborted
Using host libthread_db library "/usr/lib/libthread_db.so.1".
[Current thread is 1 (Thread 0x7fabbec0ea40 (LWP 3788))]

```
Thread 4 (Thread 0x7fab99663700 (LWP 3789)):
#0  0x00007fabb79ab18d in poll () from /usr/lib/libc.so.6
#1  0x00007faba0370cbc in ?? () from /usr/lib/libusb-1.0.so.0
#2  0x00007fabb58f94a4 in start_thread () from /usr/lib/libpthread.so.0
#3  0x00007fabb79b413d in clone () from /usr/lib/libc.so.6

Thread 3 (Thread 0x7fab92fc5700 (LWP 3790)):
[KCrash Handler]
#6  0x00007fabb78fe5f8 in raise () from /usr/lib/libc.so.6
#7  0x00007fabb78ffa7a in abort () from /usr/lib/libc.so.6
#8  0x00007fabb793d05a in __libc_message () from /usr/lib/libc.so.6
#9  0x00007fabb79429a6 in malloc_printerr () from /usr/lib/libc.so.6
#10 0x00007fabb794318e in _int_free () from /usr/lib/libc.so.6
#11 0x00007fabb6f0f7d1 in Exiv2::RiffVideo::infoTagsHandler() () from /usr/lib/libexiv2.so.14
#12 0x00007fabb6f149a5 in Exiv2::RiffVideo::decodeBlock() () from /usr/lib/libexiv2.so.14
#13 0x00007fabb6f145c8 in Exiv2::RiffVideo::tagDecoder(Exiv2::DataBuf&, unsigned long) () from /usr/lib/libexiv2.so.14
#14 0x00007fabb6f149a5 in Exiv2::RiffVideo::decodeBlock() () from /usr/lib/libexiv2.so.14
#15 0x00007fabb6f14dd8 in Exiv2::RiffVideo::readMetadata() () from /usr/lib/libexiv2.so.14
#16 0x00007fabbe3eee45 in KExiv2Iface::KExiv2::load(QString const&) const () from /usr/lib/libkexiv2.so.11
#17 0x00007fabbca28286 in Digikam::DMetadata::load(QString const&) const () from /usr/lib/libdigikamcore.so.4.14.0
#18 0x00007fabbd011bc7 in Digikam::ImageScanner::loadFromDisk() () from /usr/lib/libdigikamdatabase.so.4.14.0
#19 0x00007fabbd011e00 in Digikam::ImageScanner::newFile(int) () from /usr/lib/libdigikamdatabase.so.4.14.0
#20 0x00007fabbcfa1d6b in Digikam::CollectionScanner::scanNewFile(QFileInfo const&, int) () from
/usr/lib/libdigikamdatabase.so.4.14.0
#21 0x00007fabbcfa6807 in Digikam::CollectionScanner::scanAlbum(Digikam::CollectionLocation const&, QString const&) () from
/usr/lib/libdigikamdatabase.so.4.14.0
#22 0x00007fabbcfa66f8 in Digikam::CollectionScanner::scanAlbum(Digikam::CollectionLocation const&, QString const&) () from
/usr/lib/libdigikamdatabase.so.4.14.0
#23 0x00007fabbcfa72c3 in Digikam::CollectionScanner::scanAlbumRoot(Digikam::CollectionLocation const&) () from
/usr/lib/libdigikamdatabase.so.4.14.0
#24 0x00007fabbcfa836b in Digikam::CollectionScanner::completeScan() () from /usr/lib/libdigikamdatabase.so.4.14.0
#25 0x00000000007206df in Digikam::ScanController::run() ()
#26 0x00007fabb851914c in ?? () from /usr/lib/libQtCore.so.4
#27 0x00007fabb58f94a4 in start_thread () from /usr/lib/libpthread.so.0
#28 0x00007fabb79b413d in clone () from /usr/lib/libc.so.6

Thread 2 (Thread 0x7fab927c4700 (LWP 3791)):
#0  0x00007fabb0c45614 in g_mutex_unlock () from /usr/lib/libglib-2.0.so.0
#1  0x00007fabb0c00fb1 in ?? () from /usr/lib/libglib-2.0.so.0
#2  0x00007fabb0c010cc in g_main_context_iteration () from /usr/lib/libglib-2.0.so.0
#3  0x00007fabb8659856 in QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from
/usr/lib/libQtCore.so.4
#4  0x00007fabb8627dc1 in QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/libQtCore.so.4
#5  0x00007fabb8628135 in QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/libQtCore.so.4
#6  0x00007fabb8516859 in QThread::exec() () from /usr/lib/libQtCore.so.4
#7  0x00007fabb8607f13 in ?? () from /usr/lib/libQtCore.so.4
#8  0x00007fabb851914c in ?? () from /usr/lib/libQtCore.so.4
#9  0x00007fabb58f94a4 in start_thread () from /usr/lib/libpthread.so.0
#10 0x00007fabb79b413d in clone () from /usr/lib/libc.so.6

Thread 1 (Thread 0x7fabbec0ea40 (LWP 3788)):
#0  0x00007fabb58ff07f in pthread_cond_wait@@GLIBC_2.3.2 () from /usr/lib/libpthread.so.0
#1  0x00007fabb85196b6 in QWaitCondition::wait(QMutex*, unsigned long) () from /usr/lib/libQtCore.so.4
#2  0x00007fabb8518cde in QThread::wait(unsigned long) () from /usr/lib/libQtCore.so.4
#3  0x000000000071e1bb in Digikam::ScanController::~ScanController() ()
#4  0x000000000071e387 in ?? ()
#5  0x00007fabb7900f88 in __run_exit_handlers () from /usr/lib/libc.so.6
#6  0x00007fabb7900fd5 in exit () from /usr/lib/libc.so.6
#7  0x00007fabb90fa468 in ?? () from /usr/lib/libQtGui.so.4
#8  0x00007fabba05b1f0 in KApplication::xioErrhandler(_XDisplay*) () from /usr/lib/libkdeui.so.5
#9  0x00007fabb435891e in _XIOError () from /usr/lib/libX11.so.6
#10 0x00007fabb435625d in _XEventsQueued () from /usr/lib/libX11.so.6
#11 0x00007fabb4347b10 in XEventsQueued () from /usr/lib/libX11.so.6
#12 0x00007fabb9133e3c in ?? () from /usr/lib/libQtGui.so.4
#13 0x00007fabb0c009f1 in g_main_context_check () from /usr/lib/libglib-2.0.so.0
#14 0x00007fabb0c00f60 in ?? () from /usr/lib/libglib-2.0.so.0
#15 0x00007fabb0c010cc in g_main_context_iteration () from /usr/lib/libglib-2.0.so.0
```

```
#16 0x00007fabb8659834 in QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from
/usr/lib/libQtCore.so.4
#17 0x00007fabb91343f6 in ?? () from /usr/lib/libQtGui.so.4
#18 0x00007fabb8627dc1 in QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/libQtCore.so.4
#19 0x00007fabb8628135 in QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/libQtCore.so.4
#20 0x000000000071bd21 in Digikam::ScanController::completeCollectionScanCore(bool, bool) ()
#21 0x000000000064eeef in Digikam::NewItemsFinder::slotStart() ()
#22 0x00007fabb86433b1 in QObject::event(QEvent*) () from /usr/lib/libQtCore.so.4
#23 0x00007fabb908b39c in QApplicationPrivate::notify_helper(QObject*, QEvent*) () from /usr/lib/libQtGui.so.4
#24 0x00007fabb90921f6 in QApplication::notify(QObject*, QEvent*) () from /usr/lib/libQtGui.so.4
#25 0x00007fabba05c8aa in KApplication::notify(QObject*, QEvent*) () from /usr/lib/libkdeui.so.5
#26 0x00007fabb862954d in QCoreApplication::notifyInternal(QObject*, QEvent*) () from /usr/lib/libQtCore.so.4
#27 0x00007fabb862c9d6 in QCoreApplicationPrivate::sendPostedEvents(QObject*, int, QThreadData*) () from
/usr/lib/libQtCore.so.4
#28 0x00007fabb86596e3 in ?? () from /usr/lib/libQtCore.so.4
#29 0x00007fabb0c00dc7 in g_main_context_dispatch () from /usr/lib/libglib-2.0.so.0
#30 0x00007fabb0c01020 in ?? () from /usr/lib/libglib-2.0.so.0
#31 0x00007fabb0c010cc in g_main_context_iteration () from /usr/lib/libglib-2.0.so.0
#32 0x00007fabb8659834 in QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from
/usr/lib/libQtCore.so.4
#33 0x00007fabb91343f6 in ?? () from /usr/lib/libQtGui.so.4
#34 0x00007fabb8627dc1 in QEventLoop::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/libQtCore.so.4
#35 0x00007fabb8628135 in QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib/libQtCore.so.4
#36 0x00007fabb862dad9 in QCoreApplication::exec() () from /usr/lib/libQtCore.so.4
#37 0x00000000005b1c54 in main ()
```

History

#1 - 18 Dec 2015 11:51 - Robin Mills

- File libexiv2.so.14.0.0 added

- Category set to video

- Assignee set to Robin Mills

- Target version set to 0.26

- % Done changed from 0 to 50

- Estimated time set to 2.00 h

You are crashing in RiffVideo which should not be compiled into v0.25. I attach my linux build of v0.25 which does not have that code compiled into it.

To discover where on your system to put this file, please run this command ***(it might run for several minutes)***:

```
$ sudo find / -name libexiv2.so.14.0.0 2>/dev/null
```

I don't know why DigiKam would want to inspect the metadata of a video file on start up. So replacing the library with a version without video code may lead to a different event. Anyway, please try my version of the library.

If you are still crashing, can you think about the puzzle of why DigiKam wants to read the metadata from a video file. Does DigiKam always start up in your ~/Pictures directory which contains a video file? Try logging on as a different user (preferably a brand new user) and starting DigiKam.

Robin Mills
Exiv2Logo.png

#2 - 18 Dec 2015 12:03 - Gilles Caulier

> I don't know why DigiKam would want to inspect the metadata of a video file on >start up.

==> To register files lead metadata in digiKam database, in goal to speed-up searches, sorts, etc...

#3 - 18 Dec 2015 12:09 - Robin Mills

I've just installed DigiKam 4.12.0 on kubuntu ($ sudo apt-get install digikam) and ran it. Yup it's searching in ~/Pictures. It's using /usr/local/lib/libexiv2.so.14.0.0

```
rmills@rmillsmbp-k1504:~/gnu/exiv2/exiv2-0.25$ lsof | grep libexiv2
digikam   18258                rmills  mem       REG               8,1  3137376    3019447 /usr/local/lib/li
bexiv2.so.14.0.0
```

```
digikam   18258 18259           rmills  mem       REG                8,1  3137376    3019447 /usr/local/lib/li
bexiv2.so.14.0.0
Digikam:: 18258 18321           rmills  mem       REG                8,1  3137376    3019447 /usr/local/lib/li
bexiv2.so.14.0.0
QInotifyF 18258 18322           rmills  mem       REG                8,1  3137376    3019447 /usr/local/lib/li
bexiv2.so.14.0.0
QThread   18258 18331           rmills  mem       REG                8,1  3137376    3019447 /usr/local/lib/li
bexiv2.so.14.0.0
QProcessM 18258 18334           rmills  mem       REG                8,1  3137376    3019447 /usr/local/lib/li
bexiv2.so.14.0.0
baloo_fil 18356                 rmills  mem       REG                8,1  3137376    3019447 /usr/local/lib/li
bexiv2.so.14.0.0
QXcbEvent 18356 18357           rmills  mem       REG                8,1  3137376    3019447 /usr/local/lib/li
bexiv2.so.14.0.0
rmills@rmillsmbp-k1504:~/gnu/exiv2/exiv2-0.25$
```

Good to hear from you Gilles. I hope you and your family are well. I've been working hard on CMake/Visual Studio with Daniel for v0.26. I'm hoping our CMake support will be perfect in the spring. Daniel's dealing with nmake files.

Robin

#4 - 18 Dec 2015 12:30 - valerie venet

I have replaced my libexiv2.so.14.0.0 with yours. Thanks! It now works perfectly!

#5 - 18 Dec 2015 12:48 - Robin Mills

- Status changed from New to Closed

- % Done changed from 50 to 100

Good News. Thanks for letting me know.

Files

libexiv2.so.14.0.0	2.97 MB	18 Dec 2015	Robin Mills