# Exiv2 - Bug #664

## Crash when reading PNG image

28 Dec 2009 04:10 - Marcel Wiesweg

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 28 Dec 2009 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Andreas Huggel | **% Done:** | 100% |
| **Category:** | image format | **Estimated time:** | 0.00 hour |
| **Target version:** | 0.19 | | |

**Description**

Exiv2 crashes when reading this PNG image found by a digikam user:
http://bugs.kde.org/attachment.cgi?id=39398
(pay attention when clicking under KDE, may also crash konqueror which is using exiv2 through a component)

Backtrace of command line tool (sorry, didn't manage to compile with debug info):
#0  0x00007ffff7ac8259 in Exiv2::Internal::PngChunk::parseChunkContent(Exiv2::Image*, unsigned char const*, Exiv2::DataBuf) () from /usr/lib64/libexiv2.so.5
#1  0x00007ffff7ac8cea in Exiv2::Internal::PngChunk::decodeTXTChunk(Exiv2::Image*, Exiv2::DataBuf const&, Exiv2::Internal::PngChunk::TxtChunkType) () from /usr/lib64/libexiv2.so.5
#2  0x00007ffff7ac6500 in Exiv2::PngImage::readMetadata() () from /usr/lib64/libexiv2.so.5
#3  0x000000000041895c in Action::Print::printList() ()

The image can be opened with GIMP, it contains valid image data.
Related digikam bug is here:
http://bugs.kde.org/show_bug.cgi?id=220322

### Associated revisions

**Revision 1978 - 29 Dec 2009 02:45 - Andreas Huggel**

#664: Check key size before comparing it.

### History

**#1 - 28 Dec 2009 05:34 - Andreas Huggel**

> sorry, didn't manage to compile with debug info

That requires some insider-info:

1. make config; ./configure
2. edit config/config.mk and replace -O2 with -ggdb
3. make; make install

**#2 - 28 Dec 2009 18:43 - Andreas Huggel**

*- File bug664.patch added*

*- Category set to image format*

*- Status changed from New to Assigned*

*- Assignee set to Andreas Huggel*

*- Target version set to 0.19*

*- % Done changed from 0 to 90*

Attached patch fixes the problem. I'll apply the patch later today and it will be included in 0.19.

**#3 - 28 Dec 2009 20:10 - Andreas Huggel**

> pay attention when clicking under KDE, may also crash konqueror which is using exiv2 through a component

Interesting, I didn't know that. What component are you referring to?

Indeed, according to the Debian package dependencies, some core KDE packages (kdelibs5, kdebase-runtime and others) depend on the streamanalyzer library (libstreamanalyzer0) which depends on libexiv2-5.

#### #4 - 29 Dec 2009 02:46 - Andreas Huggel

*- Status changed from Assigned to Resolved*

*- % Done changed from 90 to 100*

Patch checked-in.

#### #5 - 29 Dec 2009 05:44 - Marcel Wiesweg

It's gwenview, crashing on its own as well as konqueror embedding the gwenview component.
libgwenview seems to use libexiv2 directly, not through libkexiv2.

#### #6 - 30 Dec 2009 07:50 - Andreas Huggel

*- Status changed from Resolved to Closed*

## Files

| | | | |
|---|---|---|---|
| bug664.patch | 8.98 KB | 28 Dec 2009 | Andreas Huggel |