Exiv2 - Bug #1277

Crash with Canon CR2 file

14 Feb 2017 18:31 - Ben Touchette

Status:	Closed	**Start date:**	14 Feb 2017
Priority:	Normal	**Due date:**	
Assignee:	Robin Mills	**% Done:**	100%
Category:	image format	**Estimated time:**	1.00 hour
Target version:	0.26		

Description

Have a client with a crash on a Canon CR2 file that contains unknown tags with random sizes (most likely a corrupted file) on an inner tiff structure. The camera model as a 350D (Rbel XT) according to the metadata.

Including the image and a fix for the crash. When we detect an unknown tag with value of 0 break from the foor loop for that tiff data dir.

Associated revisions

Revision 4706 - 14 Feb 2017 20:07 - Robin Mills

#1277 Fix submitted. Thank You to Ben for reporting this and providing a patch.

History

#1 - 14 Feb 2017 20:07 - Robin Mills

- File Tiff.png added

- Category set to image format

- Status changed from New to Assigned

- Assignee set to Robin Mills

- Target version set to 0.26

- % Done changed from 0 to 50

- Estimated time set to 2.00 h

Ben

Thanks for you little Valentine's Day surprise gift! The surprise is that I don't get a crash on my trunk r4705 with either command:

```
$ exiv2 -pR ~/Downloads/IMG_3770.CR2
or
$ exiv2 -pa ~/Downloads/IMG_3770.CR2
```

Type should always be in 1-13 as illustrated in this drawing below which I made about the structure of Tiff files (in exiv2/team/drawings/Tiff.graffle).

Thanks very much for reporting this and for investigating and providing a patch.

I've submitted a variant of your patch: r4706. I made a little change to check the range type being 1-13. I also write a warning to std::cerr when this is detected.

```
576 rmills@rmillsmbp:~/gnu/exiv2/trunk $ exiv2 -pR ~/Downloads/*.CR2 > /dev/null
invalid type value detected in Image::printIFDStructure:  0
577 rmills@rmillsmbp:~/gnu/exiv2/trunk $
```

There is a "loose end". I'm wondering how the TiffVisitor will handle this situation. However as the file isn't causing a crash, I believe the situation is benign.

Perhaps you could review my change. If you are happy, please close the issue. If you have other CR2 files which cause Exiv2 to crash I will investigate more.

Happy Valentines.

#2 - 14 Feb 2017 20:17 - Ben Touchette

I don't pay attention to most holidays, lol, more so if they are hyper commercialized :) sorry if i messed up any plans :)

Yes i understand that but on my end the file gets a type 0. The size for the bit of data was around 4GB.

I was testing with r4703, just looked at the latest code updates and not sure why the changes after that would help though.

Doesn't hurt to have the check anyways :)

#3 - 14 Feb 2017 20:53 - Robin Mills

- Status changed from Assigned to Closed

- % Done changed from 50 to 100

- Estimated time changed from 2.00 h to 1.00 h

We don't do anything on Valentines. Or maybe, every day is Valentines!

I totally agree that this test is necessary. This was bug waiting to appear and it hasn't revealed itself to me. If you discover files that cause this message to appear, please attach them and change the status to "Assigned" and I'll investigate. In the meanwhile, I'll close this issue.

Tiff.png

Files

IMG_3770.CR2	8.18 MB	14 Feb 2017	Ben Touchette
cr2_crash_fix.diff	639 Bytes	14 Feb 2017	Ben Touchette
Tiff.png	40.1 KB	14 Feb 2017	Robin Mills