Exiv2 - Bug #752
Crash when writing Exif.Image.Software

21 Jan 2011 15:02 - Jim Nelson

Status:	Closed	**Start date:**	21 Jan 2011
Priority:	Normal	**Due date:**	
Assignee:	Andreas Huggel	**% Done:**	100%
Category:	exif	**Estimated time:**	0.00 hour
Target version:	0.21.1		

Description

Using the attached photo, Exiv2 0.20 and 0.21 (and r2429) will crash when writing anything to the Exif.Image.Software field:

$ exiv2 -M"set Exif.Image.Software MyApp" img_1330.jpg
exiv2: tiffcomposite.cpp:1152: virtual uint32_t Exiv2::Internal::TiffDirectory::doWrite(Exiv2::Internal::IoWrapper&, Exiv2::ByteOrder, int32_t, uint32_t, uint32_t, uint32_t&): Assertion `sv == d' failed.
Aborted

Associated revisions

Revision 2435 - 30 Jan 2011 04:28 - Andreas Huggel

#752: Do not decode duplicate binary array tags.

Revision 2441 - 31 Jan 2011 23:11 - Andreas Huggel

[0.21.1] Merged fix for #752 from the trunk (c2435).

History

#1 - 23 Jan 2011 05:38 - Andreas Huggel

This is an interesting case. The image has a corrupted Canon makernote with 2 CanonCs composite tags. Exiv2 decodes both (although the data in the second one doesn't make any sense) but when it comes to writing, it tries to pack all CanonCs components back into only one composite tag and somehow gets confused in the process.

#2 - 30 Jan 2011 04:30 - Andreas Huggel

- Status changed from New to Resolved
- Assignee set to Andreas Huggel
- Target version set to 0.22
- % Done changed from 0 to 100

The second binary array is no longer decoded now.

#3 - 30 Jan 2011 04:33 - Andreas Huggel

$ exiv2 -M"set Exif.Image.Software MyApp" img_1330.jpg
Warning: Not decoding duplicate binary array tag 0x0001, group Canon, idx 28
Warning: Not decoding duplicate binary array tag 0x0001, group Canon, idx 28

```
$ exiv2 -g Exif.Image.Software -pa img_1330.jpg
Warning: Not decoding duplicate binary array tag 0x0001, group Canon, idx 28
Exif.Image.Software                  Ascii       6  MyApp
```

#4 - 31 Jan 2011 19:32 - Andreas Huggel

- File bug752-exiv2-0.20.patch added

The patch for 0.21 can be downloaded from the repository. The resulting library remains binary compatible with 0.21.

A binary compatible patch for 0.20 is attached too.

#5 - 08 Feb 2011 06:59 - Andreas Huggel

- Target version changed from 0.22 to 0.21.1

#6 - 03 May 2012 17:15 - Andreas Huggel

- Status changed from Resolved to Closed

Files

img_1330.jpg	4.8 MB	21 Jan 2011	Jim Nelson
bug752-exiv2-0.20.patch	6.16 KB	31 Jan 2011	Andreas Huggel