

Exiv2 - Bug #1224

Crash when setting data in CRW

09 Sep 2016 20:20 - Robin Mills

Status:	Closed	Start date:	09 Sep 2016
Priority:	Normal	Due date:	
Assignee:	Robin Mills	% Done:	100%
Category:	tiff parser	Estimated time:	4.00 hours
Target version:	0.26		
Description			
614 rmills@rmillsmm:~/gnu/exiv2/ttt \$ cp test/data/exiv2-canon-powershot-s40.crw .			
615 rmills@rmillsmm:~/gnu/exiv2/ttt \$ exiv2 -pa --grep owner/i exiv2-canon-powershot-s40.crw			
Exif.Canon.OwnerName Ascii 15 Andreas Huggel			
616 rmills@rmillsmm:~/gnu/exiv2/ttt \$ exiv2 -M'set Exif.Canon.OwnerName robin' exiv2-canon-powershot-s40.crw			
Segmentation fault: 11			
617 rmills@rmillsmm:~/gnu/exiv2/ttt \$			

Associated revisions

Revision 4482 - 11 Sep 2016 15:47 - Robin Mills

#1224 crw-test.sh refactored to use test/functions.source, no long reference sample program crwparse and avoid crash in crwimage.cpp

History

#1 - 09 Sep 2016 20:40 - Robin Mills

- Status changed from New to Assigned
- % Done changed from 0 to 50
- Estimated time set to 4.00

Andreas: can you review this and give me feedback, please? In crwimage.cpp CiffHeader::add()#793. Change: if (!pRootDir_) pRootDir_
= new CiffDirectory;
if (pRootDir_) pRootDir_->add(crwDirs, crwTagId)->setValue(buf);

```
To:            if ( pRootDir_ ) {  
              CiffComponent* child = pRootDir_->add(crwDirs, crwTagId);  
              if ( child ) child->setValue(buf);  
              }
```

It no longer crashes, however I'm not sure about the side effects. Here's the output now:

```
625 rmills@rmillsmm:~/gnu/exiv2/trunk $ exiv2 -pa --grep owner/i exiv2-canon-powershot-s40.crw  
Exif.Canon.OwnerName                    Ascii    15   Andreas Huggel  
626 rmills@rmillsmm:~/gnu/exiv2/trunk $ exiv2 -M'set Exif.Canon.OwnerName robin' exiv2-canon-powershot-s40.crw  
627 rmills@rmillsmm:~/gnu/exiv2/trunk $ exiv2 -pa --grep owner/i exiv2-canon-powershot-s40.crw  
Exif.Canon.OwnerName                    Ascii    6   robin  
628 rmills@rmillsmm:~/gnu/exiv2/trunk $
```

I discovered this while working on crw-test.sh which seems to be severely broken. That test was never "modernised" when I refactored the test scripts to use test/functions.source several years ago. It references the program crwparse which doesn't appear to be built. In fact crwparse.cpp and crwedit.cpp are not compiled:

```
640 rmills@rmillsmm:~/gnu/exiv2/trunk $ find . -name "crw*.cpp"  
./src/crwedit.cpp  
./src/crwimage.cpp
```

```
./src/crwparsed.cpp
641 rmills@rmillsmm:~/gnu/exiv2/trunk $ find . -name "crw*.o"
./src/.libs/crwimage.o
./src/crwimage.o
642 rmills@rmillsmm:~/gnu/exiv2/trunk $
```

I'll undertake the work to fix the test harness. I will either build and run crwparsed (and crwedit) or eliminate crwparsed from the test suite. I haven't examined crwparsed.cpp and crwedit.cpp which are possibly obsolete.

#2 - 11 Sep 2016 15:49 - Robin Mills

- *Status changed from Assigned to Resolved*
- *Assignee changed from Andreas Huggel to Robin Mills*
- *% Done changed from 50 to 80*

r4482 I have committed the change discussed about as it solves the immediate issue of the crash and gets crw-test.sh working again. I have removed the dependency between the crw-test.sh and crwparsed. I'm not going to do anything about crwparsed.cpp and crwedit.cpp at this time.

#3 - 14 Sep 2016 10:45 - Robin Mills

- *Status changed from Resolved to Closed*
- *% Done changed from 80 to 100*