# Exiv2 - Bug #513

## Sony Makernote crashes exiv2

26 Apr 2007 04:57 - Andreas Huggel

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Andreas Huggel | **% Done:** | 0% |
| **Category:** | exif | **Estimated time:** | 0.00 hour |
| **Target version:** | 0.15 | | |

**Description**

This digiKam crash happens in exiv2:

http://bugs.kde.org/show_bug.cgi?id=144574

At first glance it seems to be caused by the Makernote of the SONY MVC-CD500 images. It's not clear from the digiKam bug report whether the images come straight from the camera or were processed with other software.

**Related issues:**

| | |
|---|---|
| Related to Exiv2 - Bug #521: Image with large invalid Exif tag crashes exiv2 | **Closed** |
| Has duplicate Exiv2 - Bug #520: crash when loading certain image | **Closed** |

### Associated revisions

**Revision 1124 - 09 Jun 2007 08:18 - Andreas Huggel**

Added check for TIFF entry size (ported from trunk, untested). Fixes #513 in this branch.

### History

**#1 - 26 Apr 2007 06:42 - Aaron D Campbell**

I uploaded the three images I have that cause the problem. I have other pictures from that camera that work fine. Would it be helpful to have a couple of those? Also, I do not believe the images were processed with any other software, but I can't guarantee that (May 2004 seems like so long ago).

**#2 - 26 Apr 2007 07:50 - Andreas Huggel**

Thanks. The images which cause the problem should be sufficient. I'll try to find some time to look into this over the weekend.

**#3 - 30 Apr 2007 19:37 - Andreas Huggel**

r1106 fixes the problem in the JPEG parser.
A similar fix for the new TIFF parser is required as well.

**#4 - 09 Jun 2007 08:19 - Andreas Huggel**

r1124 fixes the problem in the new TIFF parser.

### Files

| | | | |
|---|---|---|---|
| DSC01199.JPG | 2.05 MB | 26 Apr 2007 | Redmine Admin |
| DSC01205.JPG | 2 MB | 26 Apr 2007 | Redmine Admin |
| DSC01211.JPG | 1.82 MB | 26 Apr 2007 | Redmine Admin |