Exiv2 - Bug #1084

Garbage in Exif.Image.Make and Exif.Image.Model in some Samsung SRW files

18 May 2015 15:03 - Pedro Côrte-Real

Status:	Closed	**Start date:**	18 May 2015
Priority:	Normal	**Due date:**	
Assignee:	Alan Pater	**% Done:**	100%
Category:	image format	**Estimated time:**	0.00 hour
Target version:	0.25		

Description

Some Samsung SRW files seem to return garbage bytes after the correct strings in Exif.Image.Make and Exif.Image.Model. For example:

```
$ exiv2 -g Exif.Image.Make RAW_SAMSUNG_NX300_PHOTO.SRW
Exif.Image.Make                              Ascii      20  SAMSUNG◆◆0
$ exiv2 -g Exif.Image.Model originals/samsung/nx2000/RAW_SAMSUNG_NX2000.SRW
Exif.Image.Model                             Ascii      20  NX2000p◆◆~y◆
```

Since these seem to be reading memory past the end of the string this is potentially a security issue.

The NX300 sample file is available at:

http://scratch.corujas.net/RAW_SAMSUNG_NX300_PHOTO.SRW

And NX2000 sample files can be found at:

http://www.photographyblog.com/reviews/samsung_nx2000_review/sample_images/

History

#1 - 18 May 2015 18:41 - Alan Pater

- Category deleted (image format)

I can't reproduce this on my system, neither with exiv2 0.24 nor with the trunk build.

```
asp@exiv2:~/image.tests/1084.Samsung.raw$ exiv2 -g Exif.Image.Make *
RAW_SAMSUNG_EX2F.SRW  Exif.Image.Make                              Ascii       8  SAMSUNG
RAW_SAMSUNG_NX300_PHOTO.SRW  Exif.Image.Make                             Ascii      20  SAMSUNG
samsung_nx2000_09.srw  Exif.Image.Make                              Ascii      20  SAMSUNG

asp@exiv2:~/image.tests/1084.Samsung.raw$ exiv2 -g Exif.Image.Model *
RAW_SAMSUNG_EX2F.SRW  Exif.Image.Model                             Ascii      24  EX2F
RAW_SAMSUNG_NX300_PHOTO.SRW  Exif.Image.Model                            Ascii      20  NX300
samsung_nx2000_09.srw  Exif.Image.Model                             Ascii      20  NX2000
```

#2 - 18 May 2015 21:41 - Pedro Côrte-Real

It's already fixed then. I am using 0.23 as shipped by Ubuntu 14.04.

#3 - 18 May 2015 21:44 - Alan Pater

- Category set to image format

- Status changed from New to Resolved

- Assignee set to Alan Pater

- Target version set to 0.25

- % Done changed from 0 to 100

#4 - 21 Jun 2015 16:39 - Andreas Huggel

- Status changed from Resolved to Closed