Exiv2 - Bug #999

Arithmetic exception in QuickTimeVideo::mediaHeaderDecoder

17 Nov 2014 23:40 - Luca Carlon

Status:	Closed	**Start date:**	17 Nov 2014
Priority:	Normal	**Due date:**	
Assignee:	Abhinav Badola	**% Done:**	100%
Category:	video	**Estimated time:**	0.00 hour
Target version:	0.25		

Description

When parsing my collection it seems that some mp4's (which were transcoded with ffmpeg) are making libexiv2 crash because of an arithmetic exception in QuickTimeVideo::mediaHeaderDecoder. In particular it seems that time_scale is found to be 0 resulting in a crash when diving. Simply

xmpData_["Xmp.video.MediaDuration"] = time_scale ? returnBufValue(buf)/time_scale : 0;

fixes the crash (same for audio). But this result of course in duration 0.
However, it seems that exiv2 returns 16000 once (no crash), and then 0 (causing the crash) for the same file. exiftool instead returns:

Time Scale: 1000
Media Time Scale: 16000

Also, don't know if this is relevant, but video is mp4, while exiv2 returns quicktime video.
So is it possible that, in addition to the check for time_scale == 0, there is also something else to fix in the determination of the time_scale?

Related issues:

Related to Exiv2 - Bug #1017: Arithmetic exception in QuickTimeVideo::mediaHe...	**Closed**	**04 Jan 2015**

History

#1 - 19 Nov 2014 22:24 - Robin Mills

- Category set to video

- Status changed from New to Assigned

- Assignee set to Abhinav Badola

- Target version set to 0.25

I've submitted a this fix you have suggested to quicktimevideo.cpp#1461 r3390

```
                if(currentStream_ == Video)
                    xmpData_["Xmp.video.MediaDuration"] = time_scale ? returnBufValue(buf)/time_scale : 0 ;
                else if (currentStream_ == Audio)
                    xmpData_["Xmp.audio.MediaDuration"] = time_scale ? returnBufValue(buf)/time_scale : 0;
                break;
```

I've assigned this issue to Abhinav as he wrote and supports our video code. Can I ask you to clarify a couple of statements in your description:

> Also, don't know if this is relevant, but video is mp4, while exiv2 returns quicktime video.

I'm not sure what you've said. Do you have an exiftool and exiv2 command (and video file) to illustrate this point.

> However, it seems that exiv2 returns 16000 once (no crash), and then 0 (causing the crash) for the same file. exiftool instead returns:
>
> Time Scale: 1000
> Media Time Scale: 16000

Do you have test files (and exiftool and exiv2 command lines) to demonstrate this?

Robin

#2 - 19 Nov 2014 23:06 - Luca Carlon

As for the first statement, I mean that, AFAIK, video/quicktime is not the same as video/mp4. I commonly refer to the first as mov container. The files for which I'm experiencing the crash are mp4 files. exiv2 returns video/quicktime. If I do not apply my patch, exiv2 crashes and no output is provided. If I do apply the patch I get:

File name : ...
File size : 37590208 Bytes
MIME type : video/quicktime
Image size : 0 x 0
...: No Exif data found in the file

But this is the output of exiftool:

ExifTool Version Number : 9.69
File Name : ...
Directory : ...
File Size : 36 MB
File Modification Date/Time : 2014:07:06 15:06:35+02:00
File Access Date/Time : 2014:11:08 13:01:34+01:00
File Inode Change Date/Time : 2014:10:05 20:32:37+02:00
File Permissions : rw-------
File Type : MP4
MIME Type : video/mp4
Major Brand : MP4 Base Media v1 [IS0 14496-12:2003]
Minor Version : 0.2.0
Compatible Brands : isom, iso2, avc1, mp41
Movie Data Size : 37543089
Movie Data Offset : 48
Movie Header Version : 0
Create Date : 0000:00:00 00:00:00
Modify Date : 0000:00:00 00:00:00
Time Scale : 1000
Duration : 0:01:59
Preferred Rate : 1
Preferred Volume : 100.00%
Preview Time : 0 s
Preview Duration : 0 s
Poster Time : 0 s
Selection Time : 0 s
Selection Duration : 0 s
Current Time : 0 s
Next Track ID : 3
Track Header Version : 0
Track Create Date : 0000:00:00 00:00:00
Track Modify Date : 0000:00:00 00:00:00
Track ID : 1
Track Duration : 0:01:58
Track Layer : 0
Track Volume : 0.00%
Image Width : 1280
Image Height : 720
Graphics Mode : srcCopy
Op Color : 0 0 0
Compressor ID : avc1
Source Image Width : 1280
Source Image Height : 720
X Resolution : 72
Y Resolution : 72
Bit Depth : 24
Video Frame Rate : 23.588
Matrix Structure : 1 0 0 0 1 0 0 0 1
Media Header Version : 0
Media Create Date : 0000:00:00 00:00:00
Media Modify Date : 0000:00:00 00:00:00
Media Time Scale : 16000
Media Duration : 0:01:59
Media Language Code : eng
Handler Description : SoundHandler
Balance : 0
Audio Channels : 2
Audio Bits Per Sample : 16
Audio Sample Rate : 16000
Handler Type : Metadata
Handler Vendor ID : Apple
Encoder : Lavf55.33.100
Avg Bitrate : 2.52 Mbps

Image Size : 1280x720
Rotation : 0

As you can see, far more data is extracted, mime type is not video/quicktime but video/mp4 and there are two time scales: one is 16000, the other one is 1000. exiv2 correctly extracts 16000 (I see that by debugging), but extracts 0 instead of 1000. The crash seems more an effect of something else (although I'd keep the patch anyway).

If you want, I can provide this file (~36MB).

#3 - 20 Nov 2014 08:32 - Luca Carlon

Here is a link from where to download the file: https://drive.google.com/file/d/0B5VttTNsGwvKYTk1OE42azJ6Yjg/view?usp=sharing.

#4 - 20 Nov 2014 08:40 - Robin Mills

Luca:
Thanks for all this information and the test file. I'm going to leave Abhinav to respond to this.

Abhinav:
I know you're busy at college. If you don't have time to dig into this, assign the issue to me and I'll do my best.

Robin

#5 - 30 Nov 2014 20:54 - Abhinav Badola

Hi Luca, Robin,

Robin Mills wrote:

> Luca:
> Thanks for all this information and the test file. I'm going to leave Abhinav to respond to this.
>
> Abhinav:
> I know you're busy at college. If you don't have time to dig into this, assign the issue to me and I'll do my best.
>
> Robin

We have tried our best to provide as much information as exiftool. It is an awesome tool written in perl and I use it many a times to verify the results fetched by exiv2.

The **MP4** file comes under the class of Quicktime.
Thats why it shows **video/quicktime**

To quote from the official website of Exiftool -
http://www.sno.phy.queensu.ca/~phil/exiftool/TagNames/QuickTime.html

```
QuickTime Tags

The QuickTime format is used for many different types of audio, video and image files (most commonly, MOV and
MP4 videos).
```

The differentiation has been based on the types of tags they use, and not on the extension of the file format.
Internally, they all (MOV, MP4, 3GP....and many more..) have almost the same structure, and they all use the standards defined by QuickTime format specified by Apple Developers' website.

See http://developer.apple.com/mac/library/documentation/QuickTime/QTFF/QTFFChap1/qtff1.html for the official specification.

Also if you may have noticed, the tag where it specifies it as **video/quicktime** is **Xmp.video.MimeType**
When I was designing these tags, I tried to incorporate as much information as provided by exiftool.
Even most of the tags have been inspired from Exiftool.

The tags are pretty much generic, so that they can incorporate any video file that may come up in the future.
But if you have some better solution, then please do suggest it. After all, this is an ever improving project.

Robin has already fixed the bug, and that must be why the file is not crashing anymore.

The command to view all tags of the file is -
./bin/exiv2 -pa ../../VID_20140118_173927_high.mp4

The command **exiv2 <videofile>** wont fetch results as the pretty print function of exiv2 needs to be modified to retrieve all tags of video files.
Currently it has been designed to extract Exif tags only, which are found in images.

The below is the output of tags that I achieved through exiv2.
Please feel free to ask any doubts, or suggest any recommendation. :)

```
[badola@XPS:~/exiv2/trunk/build]$./bin/exiv2 -pa ../../VID_20140118_173927_high.mp4
Xmp.video.FileSize                          XmpText     7  35.8488
Xmp.video.FileName                          XmpText    34  ../../VID_20140118_173927_high.mp4
Xmp.video.MimeType                          XmpText    15  video/quicktime
Xmp.video.MajorBrand                        XmpText    37  MP4 Base Media v1 [IS0 14496-12:2003]
Xmp.video.MinorVersion                      XmpText     3  512
Xmp.video.CompatibleBrands                  XmpSeq      4  MP4 Base Media v1 [IS0 14496-12:2003], MP4 Base Me
dia v2 [ISO 14496-12:2005], MP4 Base w/ AVC ext [ISO 14496-12:2005], MP4 v1 [ISO 14496-1:ch13]
Xmp.video.MovieHeaderVersion                XmpText     1  0
Xmp.video.DateUTC                           XmpText     1  0
Xmp.video.ModificationDate                  XmpText     1  0
Xmp.video.TimeScale                         XmpText     4  1000
Xmp.video.Duration                          XmpText     6  119232
Xmp.video.PreferredRate                     XmpText     1  1
Xmp.video.PreferredVolume                   XmpText     3  100
Xmp.video.PreviewTime                       XmpText     1  0
Xmp.video.PreviewDuration                   XmpText     1  0
Xmp.video.PosterTime                        XmpText     1  0
Xmp.video.SelectionTime                     XmpText     1  0
Xmp.video.SelectionDuration                 XmpText     1  0
Xmp.video.CurrentTime                       XmpText     1  0
Xmp.video.NextTrackID                       XmpText     1  3
Xmp.video.TrackHeaderVersion                XmpText     1  0
Xmp.video.TrackCreateDate                   XmpText     1  0
Xmp.video.TrackModifyDate                   XmpText     1  0
Xmp.video.TrackID                           XmpText     1  1
Xmp.video.TrackDuration                     XmpText     3  118
Xmp.video.TrackLayer                        XmpText     1  0
Xmp.video.TrackVolume                       XmpText     3  100
Xmp.video.Width                             XmpText     4  1280
Xmp.video.Height                            XmpText     3  720
Xmp.video.MediaHeaderVersion                XmpText     1  1
Xmp.video.MediaCreateDate                   XmpText     1  0
Xmp.video.MediaModifyDate                   XmpText     1  0
Xmp.video.MediaTimeScale                    XmpText     1  0
Xmp.video.MediaDuration                     XmpText     1  0
Xmp.video.MediaLangCode                     XmpText     3  426
Xmp.video.HandlerType                       XmpText    11  Video Track
Xmp.video.GraphicsMode                      XmpText     7  srcCopy
Xmp.video.OpColor                           XmpText     1  0
Xmp.video.URL                               XmpText     0
Xmp.video.Codec                             XmpText    39  MP4 Base w/ AVC ext [ISO 14496-12:2005]
Xmp.video.SourceImageWidth                  XmpText     4  1280
Xmp.video.SourceImageHeight                 XmpText     3  720
Xmp.video.XResolution                       XmpText     2  72
Xmp.video.YResolution                       XmpText     2  72
Xmp.video.Compressor                        XmpText     0
Xmp.video.BitDepth                          XmpText     2  24
Xmp.video.FrameRate                         XmpText    10  0.00084302
Xmp.audio.TrackHeaderVersion                XmpText     1  0
Xmp.audio.TrackCreateDate                   XmpText     1  0
Xmp.audio.TrackModifyDate                   XmpText     1  0
Xmp.audio.TrackID                           XmpText     1  2
Xmp.audio.TrackDuration                     XmpText     3  119
Xmp.audio.TrackLayer                        XmpText     1  0
Xmp.audio.MediaHeaderVersion                XmpText     1  0
Xmp.audio.MediaCreateDate                   XmpText     1  0
Xmp.audio.MediaModifyDate                   XmpText     1  0
Xmp.audio.MediaTimeScale                    XmpText     5  16000
Xmp.audio.MediaDuration                     XmpText     3  119
Xmp.audio.MediaLangCode                     XmpText     4  5575
Xmp.audio.HandlerType                       XmpText    11  Audio Track
Xmp.audio.Balance                           XmpText     1  0
Xmp.audio.URL                               XmpText     0
Xmp.audio.Compressor                        XmpText     4  ac-3
Xmp.audio.ChannelType                       XmpText     1  2
Xmp.audio.BitsPerSample                     XmpText     2  16
Xmp.audio.SampleRate                        XmpText     5  16000
Xmp.video.AspectRatio                       XmpText     4  16:9
```

#6 - 03 Dec 2014 22:12 - Luca Carlon

I checked the output using the -pa param and yes, it seems everything is working correctly. Sorry, I didn't know that was necessary to get all the data.

I suppose the report can be closed now.

#7 - 04 Dec 2014 04:32 - Abhinav Badola

- Status changed from Assigned to Resolved

- % Done changed from 0 to 100

Thanks Luca, for helping us fix this bug. :)

#8 - 04 Jan 2015 09:15 - Mathieu Clabaut

I've stumbled upon almost the same problem with exiv2 0.24 on Arch Linux for x86_64.
But two variables are concerned by a division by zero : time_scale and timeScale_.
You can download (for a limited period of time) the problematic file on http://dl.free.fr/rrfsuOUdn

The backtrace was:
The backtrace is :
#0 0x00007ffff7a396d5 in Exiv2::QuickTimeVideo::movieHeaderDecoder (this=this@entry=0x62c930, size=0x60, size@entry=0x70) at /tmp_dsk/makepkg/exiv2/src/exiv2-0.24/src/quicktimevideo.cpp:1576
#1 0x00007ffff7a3e49b in Exiv2::QuickTimeVideo::tagDecoder (this=this@entry=0x62c930, buf=..., size=size@entry=0x70) at /tmp_dsk/makepkg/exiv2/src/exiv2-0.24/src/quicktimevideo.cpp:690
#2 0x00007ffff7a3e8d0 in Exiv2::QuickTimeVideo::decodeBlock (this=this@entry=0x62c930) at /tmp_dsk/makepkg/exiv2/src/exiv2-0.24/src/quicktimevideo.cpp:672
#3 0x00007ffff7a3e438 in Exiv2::QuickTimeVideo::tagDecoder (this=this@entry=0x62c930, buf=..., size=size@entry=0x56fd) at /tmp_dsk/makepkg/exiv2/src/exiv2-0.24/src/quicktimevideo.cpp:681
#4 0x00007ffff7a3e8d0 in Exiv2::QuickTimeVideo::decodeBlock (this=0x62c930) at /tmp_dsk/makepkg/exiv2/src/exiv2-0.24/src/quicktimevideo.cpp:672
#5 0x00007ffff7a3eb45 in Exiv2::QuickTimeVideo::readMetadata (this=0x62c930) at /tmp_dsk/makepkg/exiv2/src/exiv2-0.24/src/quicktimevideo.cpp:645
#6 0x0000000000418f62 in Action::Print::printSummary (this=this@entry=0x62c570) at /tmp_dsk/makepkg/exiv2/src/exiv2-0.24/src/actions.cpp:258
#7 0x000000000041b71c in Action::Print::run (this=0x62c570, path="/home/clabaut/Pictures/2014/téléphone_Cécile/VID_20120911_182743.mp4") at /tmp_dsk/makepkg/exiv2/src/exiv2-0.24/src/actions.cpp:236
#8 0x00000000004088c6 in main (argc=<optimized out>, argv=<optimized out>) at /tmp_dsk/makepkg/exiv2/src/exiv2-0.24/src/exiv2.cpp:171

And a possible correcting patch is:

```
diff --git a/src/quicktimevideo.cpp.orig b/src/quicktimevideo.cpp
index 15d4482..5d4835a 100644
--- a/src/quicktimevideo.cpp.orig
++ b/src/quicktimevideo.cpp
@ -1456,6 +1456,7 @ namespace Exiv2 {
else if (currentStream_ == Audio)
xmpData_["Xmp.audio.MediaTimeScale"] = returnBufValue(buf);
time_scale = returnBufValue(buf);
if (time_scale == 0) {time_scale = 1;}
break;
case MediaDuration:
if(currentStream_ == Video)
@ -1571,7 +1572,9 @ namespace Exiv2 {
xmpData_["Xmp.video.ModificationDate"] = returnUnsignedBufValue(buf); break;
case TimeScale:
xmpData_["Xmp.video.TimeScale"] = returnBufValue(buf);
-               timeScale_ = returnBufValue(buf); break;
+               timeScale_ = returnBufValue(buf);
+       if (timeScale_ == 0) { timeScale_ = 1;}
+       break;
case Duration:
xmpData_["Xmp.video.Duration"] = returnBufValue(buf) * 1000 / timeScale_; break;
case PreferredRate:
```

#9 - 04 Jan 2015 10:09 - Mathieu Clabaut

Attached is a patch against last HEAD with the same spirit as the first correction.

#10 - 04 Jan 2015 10:16 - Mathieu Clabaut

Below the output of the corrected exiv2 :

```
Xmp.video.FileSize                              XmpText      7  54.7469
Xmp.video.FileName                              XmpText     60  /home/photo/2014/téléphone_Cécile/VID_20120911_182
743.mp4
Xmp.video.MimeType                              XmpText     15  video/quicktime
Xmp.video.MajorBrand                            XmpText     37  MP4 Base Media v1 [IS0 14496-12:2003]
```

```
Xmp.video.MinorVersion                          XmpText     1  0
Xmp.video.CompatibleBrands                      XmpSeq      2  MP4 Base Media v1 [IS0 14496-12:2003], 3GPP Media
(.3GP) Release 4
Xmp.video.MovieHeaderVersion                    XmpText     1  1
Xmp.video.DateUTC                               XmpText     1  0
Xmp.video.ModificationDate                      XmpText    10  3430225701
Xmp.video.TimeScale                             XmpText     1  0
Xmp.video.PreferredRate                         XmpText     2  10
Xmp.video.PreferredVolume                       XmpText     1  0
Xmp.video.PreviewTime                           XmpText     1  0
Xmp.video.PreviewDuration                       XmpText     1  0
Xmp.video.PosterTime                            XmpText    10  1073741824
Xmp.video.SelectionTime                         XmpText     1  0
Xmp.video.SelectionDuration                     XmpText     1  0
Xmp.video.CurrentTime                           XmpText     1  0
Xmp.video.NextTrackID                           XmpText     1  0
Xmp.video.TrackHeaderVersion                    XmpText     1  1
Xmp.video.TrackCreateDate                       XmpText     1  0
Xmp.video.TrackModifyDate                       XmpText    10  3430225701
Xmp.video.TrackID                               XmpText     1  0
Xmp.video.TrackDuration                         XmpText     1  0
Xmp.video.TrackLayer                            XmpText     1  0
Xmp.video.TrackVolume                           XmpText     1  0
Xmp.video.Width                                 XmpText     1  0
Xmp.video.Height                                XmpText     1  0
Xmp.video.MediaHeaderVersion                    XmpText     1  1
Xmp.video.MediaCreateDate                       XmpText     1  0
Xmp.video.MediaModifyDate                       XmpText    10  3430225701
Xmp.video.MediaTimeScale                        XmpText     1  0
Xmp.video.MediaDuration                         XmpText     1  0
Xmp.video.MediaLangCode                         XmpText     1  1
Xmp.video.HandlerType                           XmpText    11  Video Track
Xmp.video.GraphicsMode                          XmpText     7  srcCopy
Xmp.video.OpColor                               XmpText     1  0
Xmp.video.URL                                   XmpText     0
Xmp.video.Codec                                 XmpText    39  MP4 Base w/ AVC ext [ISO 14496-12:2005]
Xmp.video.SourceImageWidth                      XmpText     4  1280
Xmp.video.SourceImageHeight                     XmpText     3  720
Xmp.video.XResolution                           XmpText     2  72
Xmp.video.YResolution                           XmpText     2  72
Xmp.video.Compressor                            XmpText    31
Xmp.video.BitDepth                              XmpText     2  24
Xmp.video.FrameRate                             XmpText     1  0
Xmp.audio.TrackHeaderVersion                    XmpText     1  1
Xmp.audio.TrackCreateDate                       XmpText     1  0
Xmp.audio.TrackModifyDate                       XmpText    10  3430225701
Xmp.audio.TrackID                               XmpText     1  0
Xmp.audio.TrackDuration                         XmpText     1  0
Xmp.audio.TrackLayer                            XmpText     1  0
Xmp.audio.MediaHeaderVersion                    XmpText     1  1
Xmp.audio.MediaCreateDate                       XmpText     1  0
Xmp.audio.MediaModifyDate                       XmpText    10  3430225701
Xmp.audio.MediaTimeScale                        XmpText     1  0
Xmp.audio.MediaDuration                         XmpText     1  0
Xmp.audio.MediaLangCode                         XmpText     1  0
Xmp.audio.HandlerType                           XmpText    11  Audio Track
Xmp.audio.Balance                               XmpText     1  0
Xmp.audio.URL                                   XmpText     0
Xmp.audio.Compressor                            XmpText     4  mp4a
Xmp.audio.ChannelType                           XmpText     1  1
Xmp.audio.BitsPerSample                         XmpText     2  16
Xmp.audio.SampleRate                            XmpText     5  48000
Xmp.video.AspectRatio                           XmpText     4  -nan
```

#11 - 21 Jun 2015 16:41 - Andreas Huggel

- Status changed from Resolved to Closed