AVIStreamWrite exception.. need help !!

Posted by miamia - 14 Oct 2010 - 04:25

I got one excpetion when trying to create AVI file using AVIstreamWrite API. Normally it works fine but i have one another thread sometimes working in parallel to this thread and at that time some exception occurs. it is properly handled but i could not figure out the reason. I tried to use WindDBG . Sorry i am very new to WINDDBG and infact this is the first case i am trying !!! any help will be really appreciated.

Exception in WinDBG

```
ModLoad: 73b50000 73b67000   C:WINDOWSsystem32AVIFIL32.dll
ModLoad: 75a70000 75a91000   C:WINDOWSsystem32MSVFW32.dll
ModLoad: 73c00000 73c17000   C:WINDOWSsystem32iccvid.dll
(13c4.155c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=fffffbff ebx=00000200 ecx=00235264 edx=00000080 esi=09200048 edi=02c5b790
eip=73c02792 esp=02c5b70c ebp=02c5bf0c iopl=0         nv up ei ng nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010286
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for
C:WINDOWSsystem32iccvid.dll -
iccvid+0x2792:
73c02792 66a5            movs    word ptr es:,word ptr  es:0023:02c5b790=0000 ds:0023:09200048=????
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for
C:WINDOWSsystem32AVIFIL32.dll -
```

I think the pointer 09200048 is inaccessible and hence the error. Hope my understanding is correct.

```
0:007> dd 09200048
09200048  ???????? ???????? ???????? ????????
09200058  ???????? ???????? ???????? ????????
09200068  ???????? ???????? ???????? ????????
09200078  ???????? ???????? ???????? ????????
09200088  ???????? ???????? ???????? ????????
09200098  ???????? ???????? ???????? ????????
092000a8  ???????? ???????? ???????? ????????
092000b8  ???????? ???????? ???????? ????????
```

Stack Trace

```
0:007> k
ChildEBP RetAddr
WARNING: Stack unwind information not available. Following frames may be wrong.
02c5bf0c 73c03cb7 iccvid+0x2792
02c5bf20 73c03d47 iccvid+0x3cb7
02c5bf3c 73c01aa8 iccvid+0x3d47
02c5bf64 73c01fb5 iccvid+0x1aa8
02c5bfac 73c0ca27 iccvid+0x1fb5
02c5bfdc 73c065d1 iccvid!DllInstanceInit+0x6104
```

```
02c5bffc 75a718a8 iccvid!DriverProc+0x11f
02c5c020 75a74c09 MSVFW32!ICSendMessage+0x2b
02c5c068 73b5aecf MSVFW32!ICCompress+0x63
02c5c0d8 73b5b47c AVIFIL32!DllCanUnloadNow+0x4145
02c5c0f0 73b5609f AVIFIL32!DllCanUnloadNow+0x46f2
02c5c118 08cd3a5c AVIFIL32!AVIStreamWrite+0x23
.....
.....

0:007> u iccvid+0x2792
iccvid+0x2792:
73c02792 66a5            movs    word ptr es:,word ptr
73c02794 a4              movs    byte ptr es:,byte ptr
73c02795 0f8498feffff    je      iccvid+0x2633 (73c02633)
73c0279b ff8578f8ffff    inc     dword ptr
73c027a1 e98dfeffff      jmp     iccvid+0x2633 (73c02633)
73c027a6 8bb578f8ffff    mov     esi,dword ptr
73c027ac 8a4601          mov     al,byte ptr
73c027af 8ad0            mov     dl,al
```

Can anyone help me on how to proceed with this analysis . Thank you for your help

==========