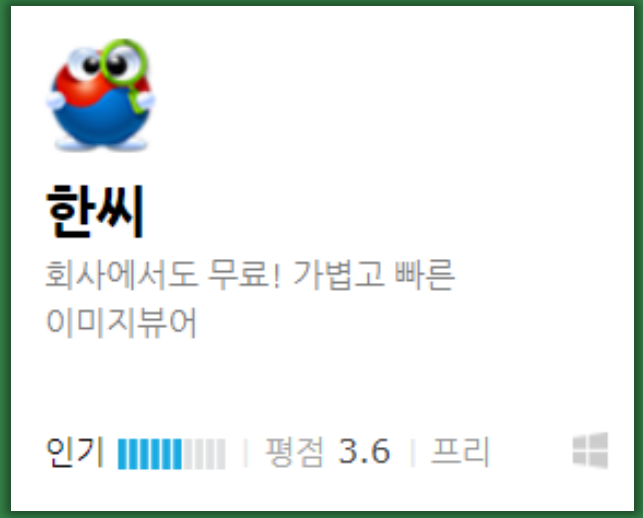
윈도우 소프트웨어 Zero-Day Hunting 3주차

2020-01-28

목 차

Crash Analysis (Hansee)

Crash Analysis



Crash Analysis

```
00000A70   64 50 34 21 CF 00 00 00 0D 49 48 44 52 00 00 00   dP4!Ï....IHDR...
00000A80   30 00 00 33 30 08 02 00 00 00 D8 60 6E D0 00 00   0..30.....Ø`nÐ..
```

Length = 00 00 00 0D

Chunk type = 49 48 44 52

Width = 00 00 00 30

Height = 00 00 33 30

Bit depth = 08

Color Type = 02

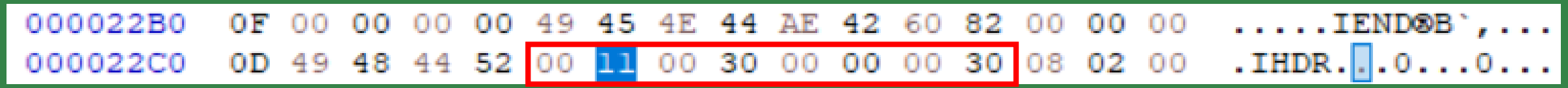
Compression method = 00

Filter method = 00

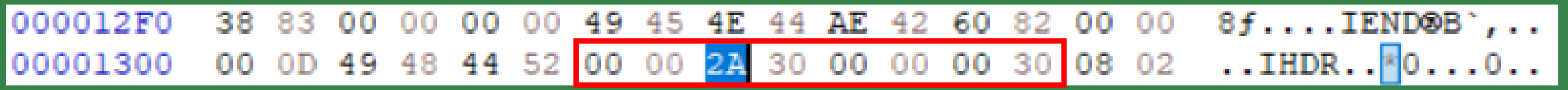
Interlace method = 00

Length(13)
Chunk type(4)
Width(4)
Height(4)
Bit depth(1)
Color Type(1)
Compression method(1)
Filter method(1)
Interlace method(1)

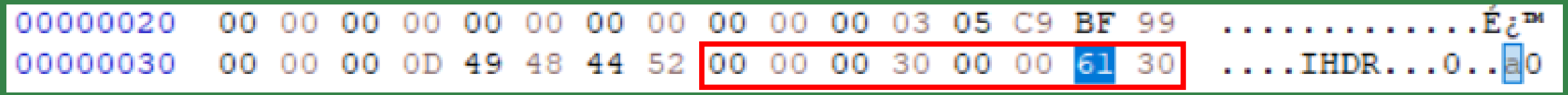
Crash Analysis



```
000022B0   0F 00 00 00 00 49 45 4E 44 AE 42 60 82 00 00 00   .....IEND®B`,...
000022C0   0D 49 48 44 52 00 11 00 30 00 00 00 30 08 02 00   .IHDR...0...0...
```



```
000012F0   38 83 00 00 00 00 49 45 4E 44 AE 42 60 82 00 00   8ƒ....IEND®B`,..
00001300   00 0D 49 48 44 52 00 00 2A 30 00 00 00 30 08 02   ..IHDR..*0...0..
```



```
00000020   00 00 00 00 00 00 00 00 00 00 00 03 05 C9 BF 99   .............É¿™
00000030   00 00 00 0D 49 48 44 52 00 00 00 30 00 00 61 30   ....IHDR...0..a0
```

Crash Analysis

```
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=0367fffe ebx=00000000 ecx=0367fffe edx=00000001 esi=00000000 edi=02dbc9a0
eip=006daae9 esp=0019f788 ebp=0019f790 iopl=0         nv up ei pl nz na po nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00210202
HanSee+0x2daae9:
006daae9 0fb67102        movzx   esi,byte ptr [ecx+2]       ds:002b:03680000=??
```

```
(189c.3bfc): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=9a5d039c ebx=009cb0e4 ecx=fffffff8 edx=035d27b0 esi=0019a570 edi=00000004
eip=00403611 esp=0019a54c ebp=0019c804 iopl=0         nv up ei pl nz na po nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00210202
HanSee+0x3611:
00403611 2348fc          and     ecx,dword ptr [eax-4] ds:002b:9a5d0398=????????
```

```
(189c.3bfc): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=0260125d ebx=009cb0c4 ecx=fffffff8 edx=035cb480 esi=0019ce90 edi=00000004
eip=00403611 esp=0019ce6c ebp=0019f124 iopl=0         nv up ei pl nz na po nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00210202
HanSee+0x3611:
00403611 2348fc          and     ecx,dword ptr [eax-4] ds:002b:02601259=????????
```

```
(189c.3bfc): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=035a16e0 ebx=00704a30 ecx=2770f1a0 edx=f1a00000 esi=0359fab0 edi=0019f79c
eip=004031bb esp=00199aa0 ebp=0019f860 iopl=0         nv up ei pl nz na pe cy
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00210207
HanSee+0x31bb:
004031bb 8911            mov     dword ptr [ecx],edx  ds:002b:2770f1a0=????????
```

```
(189c.3bfc): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=9a5d0398 ebx=00000000 ecx=00199ab8 edx=00000001 esi=00000000 edi=00000000
eip=00405f7a esp=0019902c ebp=00199b08 iopl=0         nv up ei ng nz na po nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00210282
HanSee+0x5f7a:
00405f7a 8b08            mov     ecx,dword ptr [eax]  ds:002b:9a5d0398=????????
```

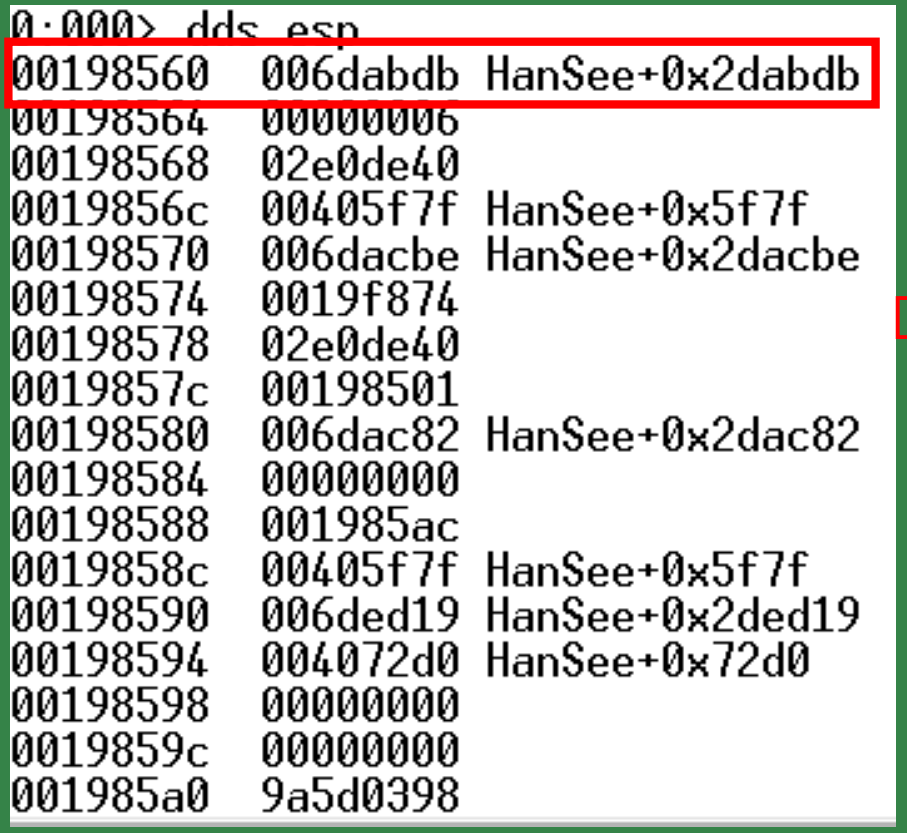
```
(189c.3bfc): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=035d0fc0 ebx=00198501 ecx=7244005c edx=02db9901 esi=034051b0 edi=00000000
eip=00405f7c esp=00198560 ebp=0019f894 iopl=0         nv up ei pl nz na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00210206
HanSee+0x5f7c:
00405f7c ff51fc          call    dword ptr [ecx-4]    ds:002b:72440058=????????
```

Crash Analysis

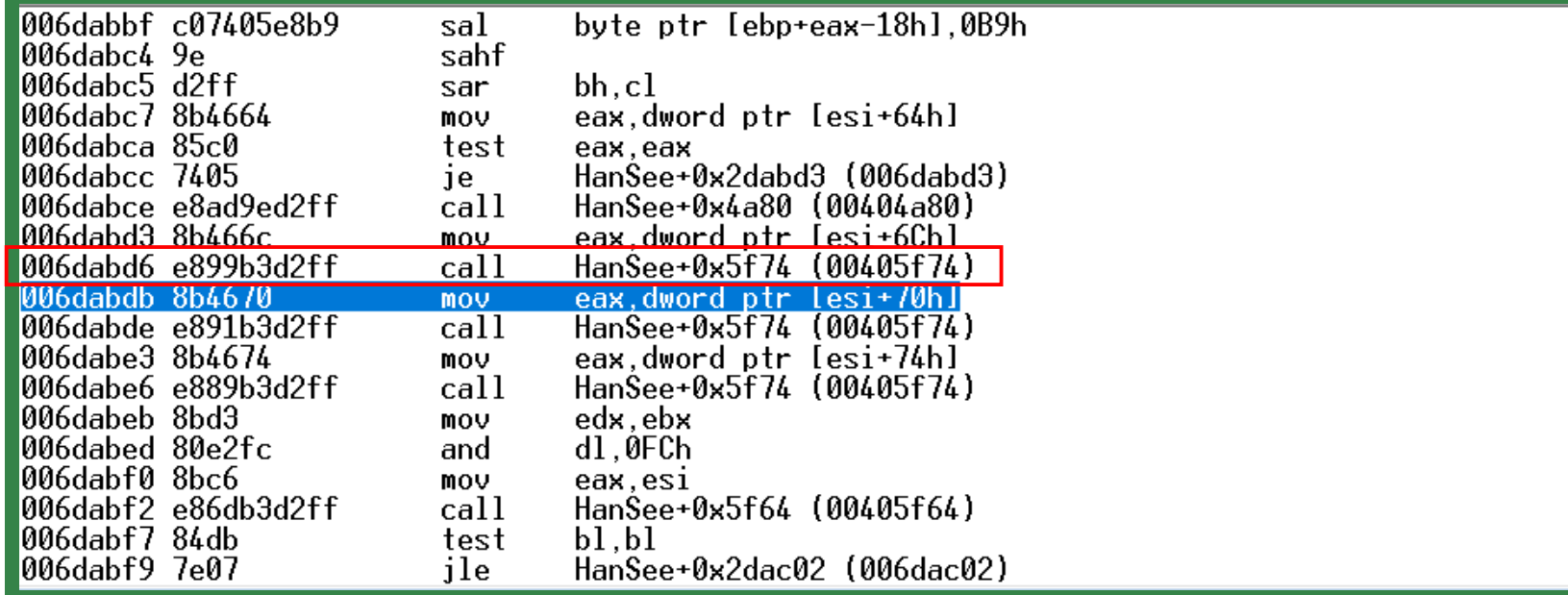
```
(189c.3bfc): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=035d0fc0 ebx=00198501 ecx=7244005c edx=02db9901 esi=034051b0 edi=00000000
eip=00405f7c esp=00198560 ebp=0019f894 iopl=0         nv up ei pl nz na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00210206
HanSee+0x5f7c:
00405f7c ff51fc          call    dword ptr [ecx-4]    ds:002b:72440058=????????
0:000> !load msec
0:000> !exploitable
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - Read Access Violation on Control Flow starting at HanSee+0x5f7c (Hash=0x736e040d.0x44254801)

Access violations not near null in control flow instructions are considered exploitable.
```

Crash Analysis



```
0:000> dds esp
00198560  006dabdb HanSee+0x2dabdb
00198564  00000006
00198568  02e0de40
0019856c  00405f7f HanSee+0x5f7f
00198570  006dacbe HanSee+0x2dacbe
00198574  0019f874
00198578  02e0de40
0019857c  00198501
00198580  006dac82 HanSee+0x2dac82
00198584  00000000
00198588  001985ac
0019858c  00405f7f HanSee+0x5f7f
00198590  006ded19 HanSee+0x2ded19
00198594  004072d0 HanSee+0x72d0
00198598  00000000
0019859c  00000000
001985a0  9a5d0398
```



```
006dabbf c07405e8b9      sal     byte ptr [ebp+eax-18h],0B9h
006dabc4 9e              sahf
006dabc5 d2ff            sar     bh,cl
006dabc7 8b4664          mov     eax,dword ptr [esi+64h]
006dabca 85c0            test    eax,eax
006dabcc 7405            je      HanSee+0x2dabd3 (006dabd3)
006dabce e8ad9ed2ff      call    HanSee+0x4a80 (00404a80)
006dabd3 8b466c          mov     eax,dword ptr [esi+6Ch]
006dabd6 e899b3d2ff      call    HanSee+0x5f74 (00405f74)
006dabdb 8b4670          mov     eax,dword ptr [esi+70h]
006dabde e891b3d2ff      call    HanSee+0x5f74 (00405f74)
006dabe3 8b4674          mov     eax,dword ptr [esi+74h]
006dabe6 e889b3d2ff      call    HanSee+0x5f74 (00405f74)
006dabeb 8bd3            mov     edx,ebx
006dabed 80e2fc          and     dl,0FCh
006dabf0 8bc6            mov     eax,esi
006dabf2 e86db3d2ff      call    HanSee+0x5f64 (00405f64)
006dabf7 84db            test    bl,bl
006dabf9 7e07            jle     HanSee+0x2dac02 (006dac02)
```

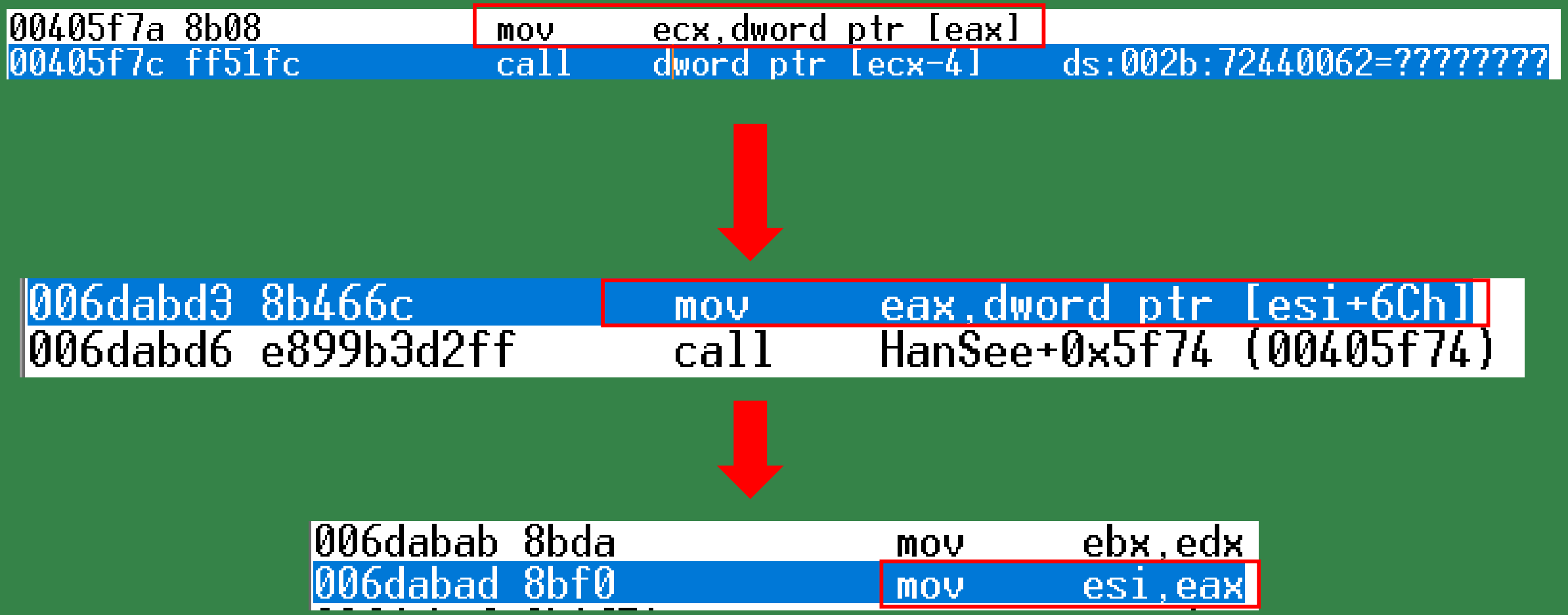
Crash Analysis

```
text:006DED14          call    sub_405F74
text:00405F7C          call    dword ptr [ecx-4]
text:006dac72          call    sub_00406628
text:00406631          call    dword ptr [edx-18h]
text:006DAC7D          call    sub_6DAC9C
text:006DACA4          call    sub_40A40C
text:006DACB9          call    sub_405F74
text:00405F7C          call    dword ptr [ecx-4]
text:006DABA6          call    sub_406628
text:00406631          call    dword ptr [edx-18h]
text:00404a84          call    dword ptr [HanSee+0x5cb768 (009cb768)]
text:006DABD6          call    sub_405F74
text:00405f7c          call    dword ptr [ecx-4]    ds:002b:72440063=????????
```

Crash Analysis

```
(189c.3bfc): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=035d0fc0 ebx=00198501 ecx=7244005c edx=02db9901 esi=034051b0 edi=00000000
eip=00405f7c esp=00198560 ebp=0019f894 iopl=0         nv up ei pl nz na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00210206
HanSee+0x5f7c:
00405f7c ff51fc          call    dword ptr [ecx-4]   ds:002b:72440058=????????
```

Crash Analysis



Crash Analysis

```
004035f5        lea     ebx,HanSee+0x5cb084 (009cb084)[eax*8]
004035fe        mov     edx,dword ptr [ebx+8]
00403601        mov     eax,dword ptr [edx+10h]
006DEBDE        mov     [ebp-8], eax
006ded11        mov     eax,dword ptr [ebp-8]
006dac79        mov     esi,eax
006dac7b        mov     eax,esi
006dac9f        mov     ebx,eax
006dacb3        mov     eax,dword ptr [ebx+0Ch]
006dacb6        mov     eax,dword ptr [eax+edi*4] (edi = 0)
006DABAD        mov     esi, eax
006DABD3        mov     eax, [esi+6Ch]
00405F7A        mov     ecx, [eax]
00405F7C        call    dword ptr [ecx-4]
```

Crash Analysis

```
0:000> s -a 0x00000000 L?0xffffffff IHDR
006d9927  49 48 44 52 0d 00 00 00-00 00 00 00 00 07 00 00  IHDR............
006d9de3  49 48 44 52 02 00 02 a0-9a 6d 00 1e 00 00 00 04  IHDR.....m......
006da488  49 48 44 52 02 00 08 40-74 44 00 0c 00 0a 49 44  IHDR...@tD....ID
006da7d7  49 48 44 52 02 00 00 e4-10 40 00 02 00 04 42 69  IHDR.....@....Bi
008d64e2  49 48 44 52 00 00 ec 64-8d 00 07 0f 45 50 6e 67  IHDR...d....EPng
008d64f9  49 48 44 52 c8 64 8d 00-bc c7 41 00 00 00 14 56  IHDR.d....A....V
008d687f  49 48 44 52 4e 6f 74 46-69 72 73 74 00 90 68 8d  IHDRNotFirst..h.
008d6896  49 48 44 52 4e 6f 74 46-69 72 73 74 6c 68 8d 00  IHDRNotFirstlh..
008d87a7  49 48 44 52 44 61 74 61-0d 00 00 00 00 00 00 00  IHDRData........
008d898d  49 48 44 52 44 61 74 61-02 00 01 9c 10 40 00 68  IHDRData.....@.h
008d8a8b  49 48 44 52 5f 00 18 b7-8d 00 0e 4c 6f 61 64 46  IHDR_.......LoadF
008d8bc8  49 48 44 52 b4 88 8d 00-c8 85 8d 00 00 00 14 56  IHDR...........V
009d9d5e  49 48 44 52 49 45 4e 44-4d 48 44 52 4d 45 4e 44  IHDRIENDMHDRMEND
009da66b  49 48 44 52 20 4d 61 72-6b 65 72 0a 00 45 72 72  IHDR Marker..Err
009da683  49 48 44 52 20 42 6f 78-0a 00 45 78 70 65 63 74  IHDR Box..Expect
00a027cb  49 48 44 52 49 44 41 54-49 45 4e 44 50 4c 54 45  IHDRIDATIENDPLTE
```

감사합니다