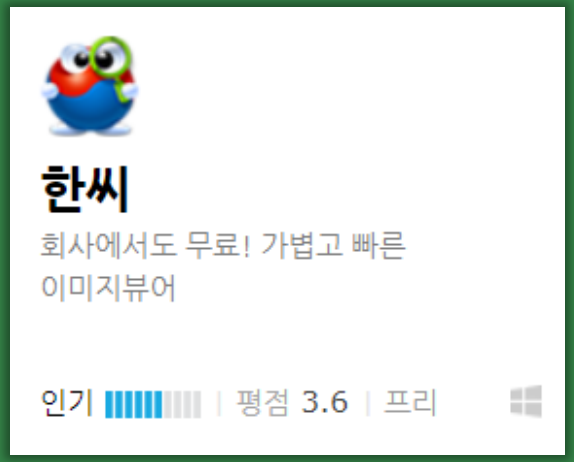
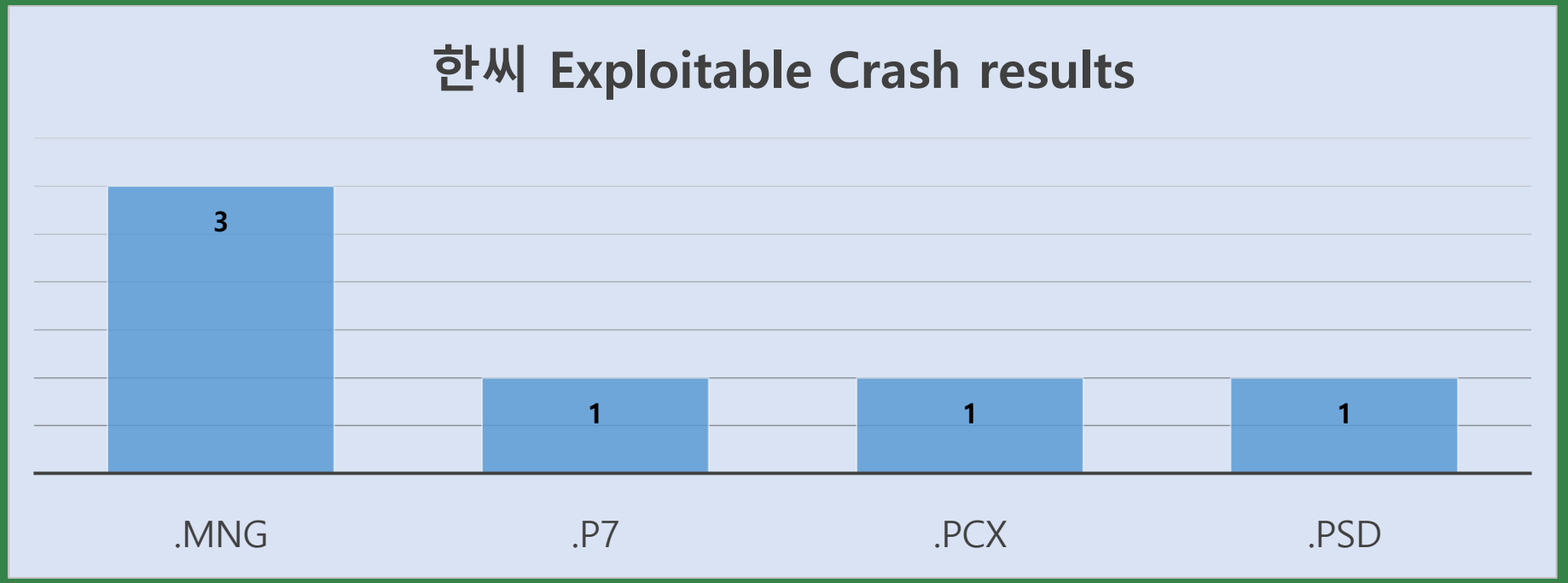
윈도우 소프트웨어 Zero-Day Hunting 2주차

2020-01-20

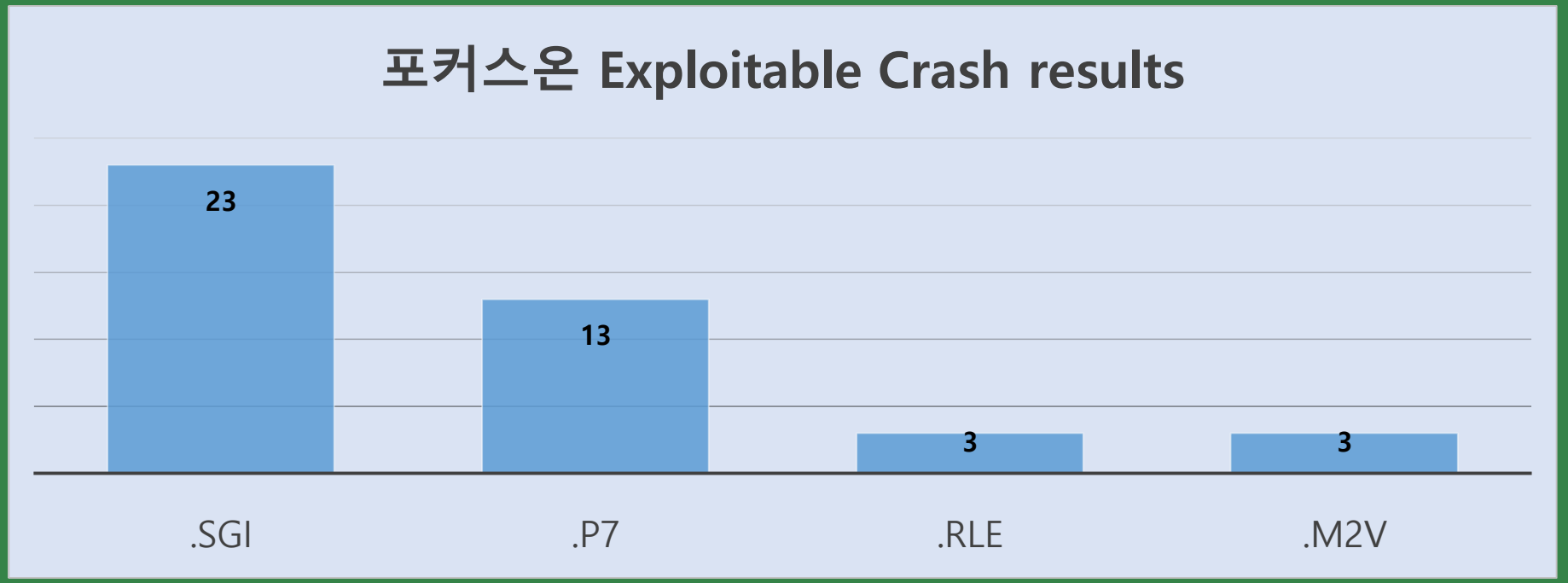
목 차

Crash results

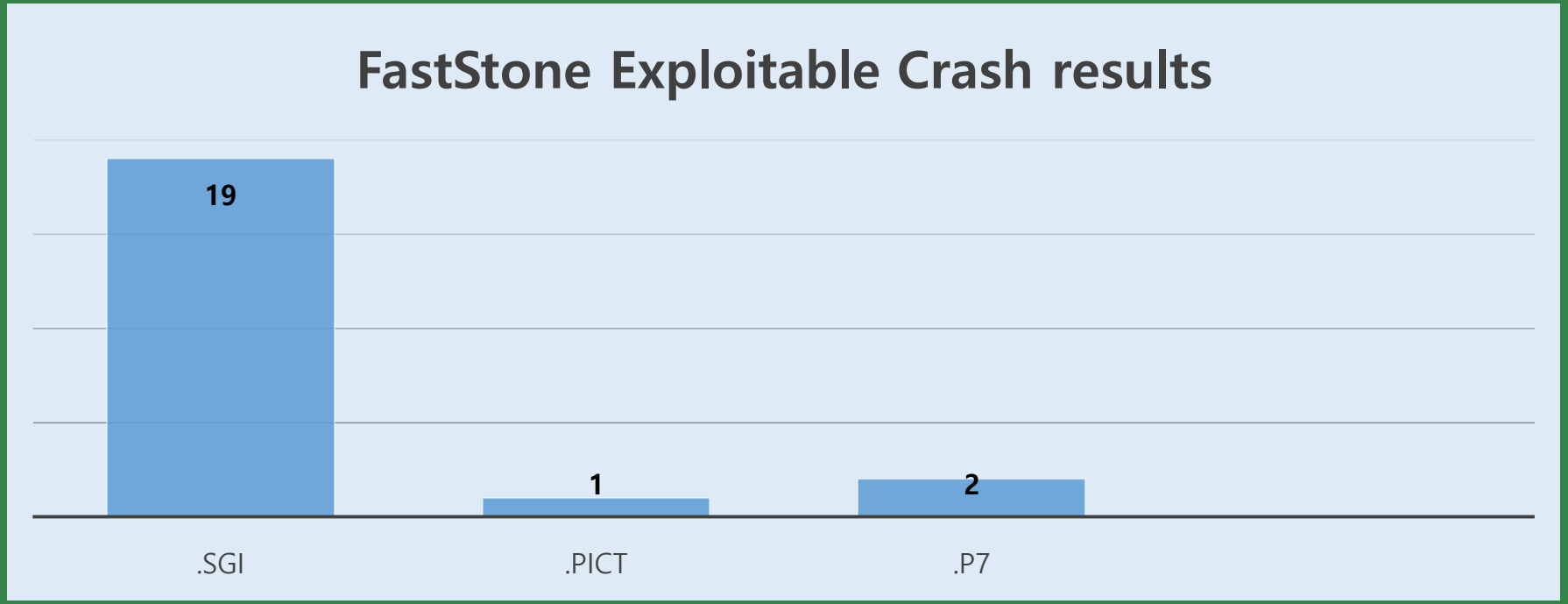




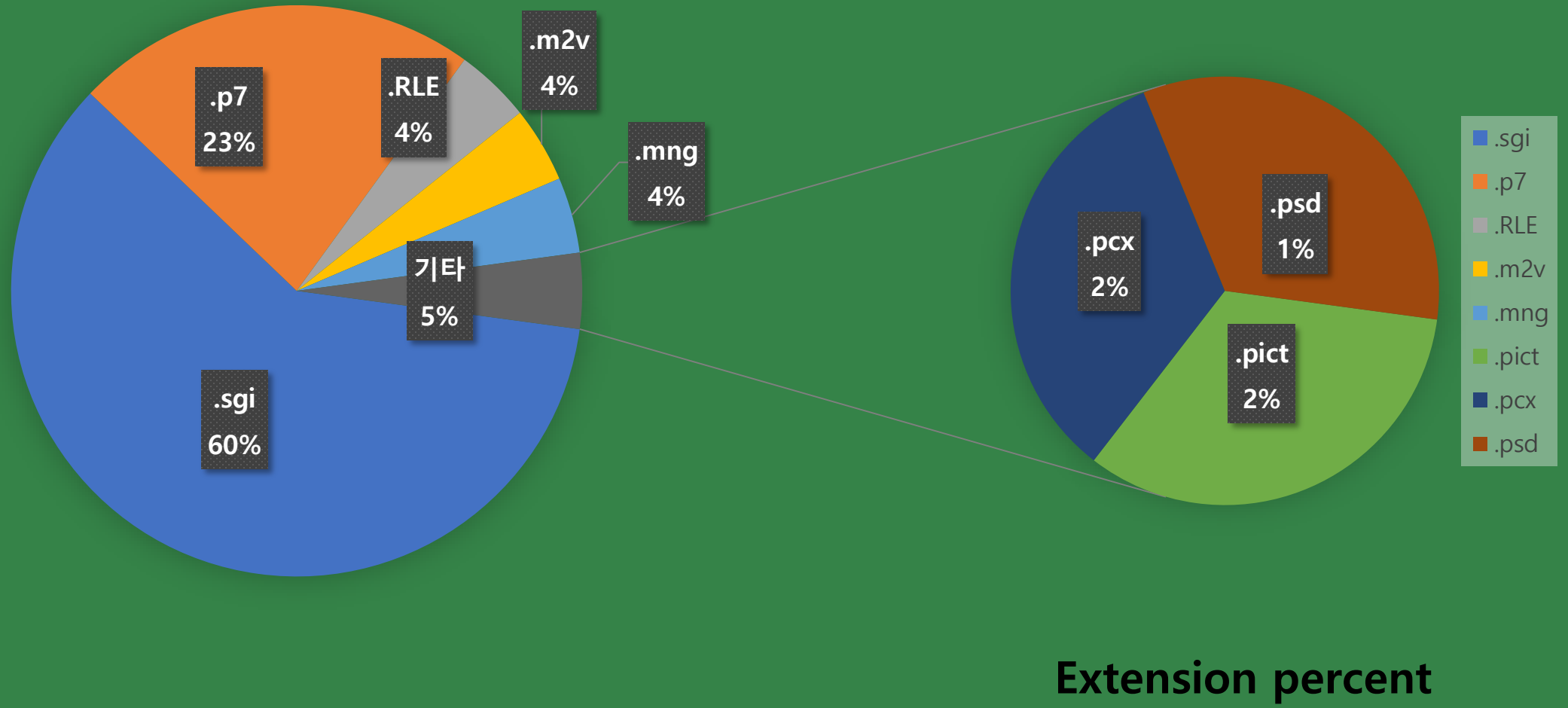
Crash results



Crash results

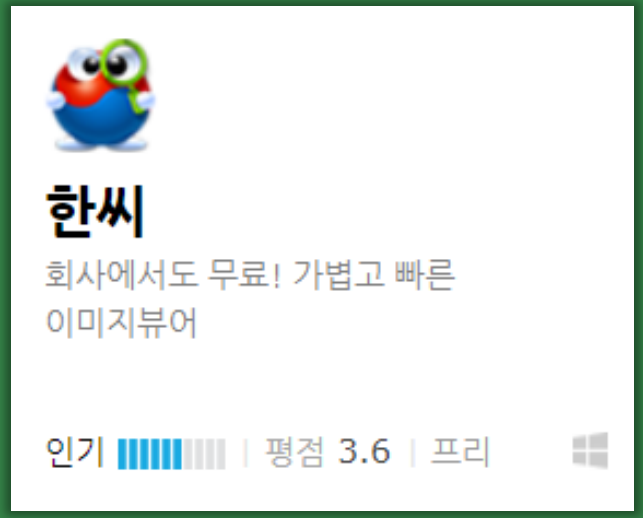


Crash results



Extension percent

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 00 30 08 02 00 00 00 D8 60 6E D0 00 00   0...0.....Ø`nÐ..
```

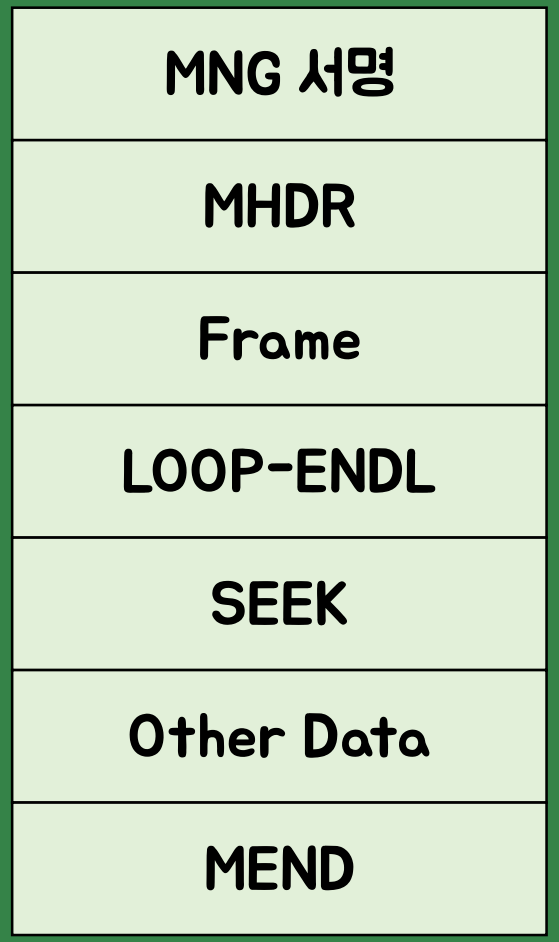
원본 파일

```
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..
```

Crash 파일

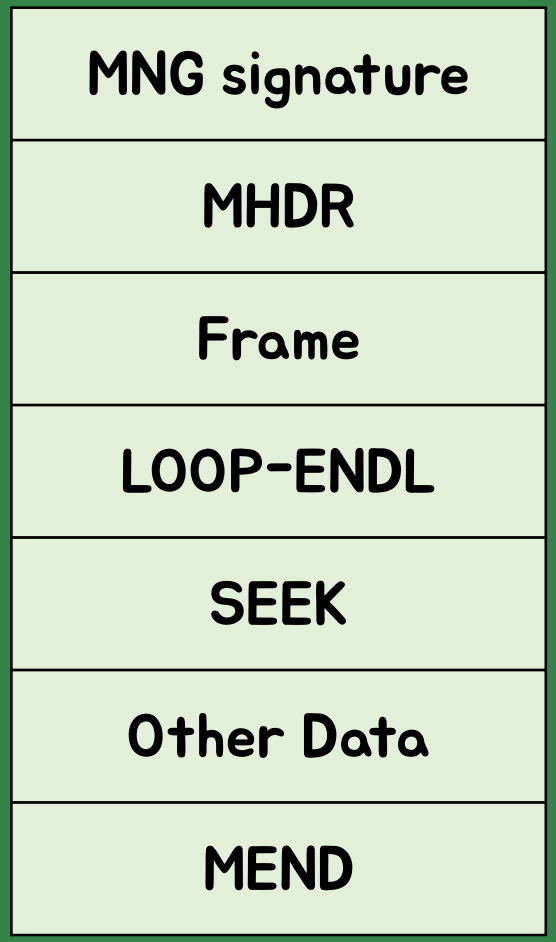
Crash Analysis

MNG = (Multiple-image Network Graphics)



MNG datastream

Crash Analysis



MNG datastream

MNG signature (8-byte)

MNG datastream 최상위 data

하나 이상의 Layer

동일한 청크 반복 방지

datastream point 표시

이미지 및 기타 객체 생성

MNG datastream의 끝

Crash Analysis

Frame 하나 이상의 Layer

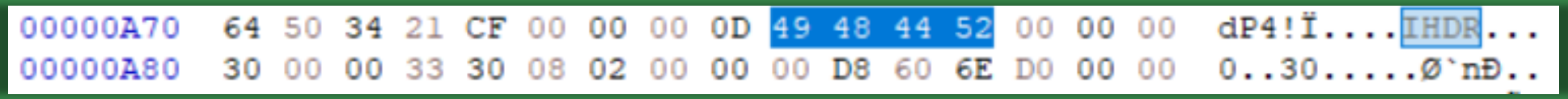
Layer : PNG or JNG datastream or MNG BASI chunk

Crash Analysis

PNG = (Portable Network Graphics)

IHDR

IDAT

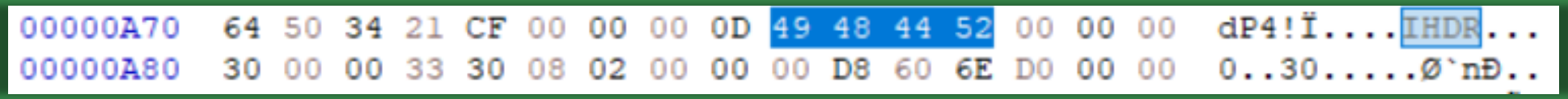


IEND

Crash Analysis

PNG = (Portable Network Graphics)

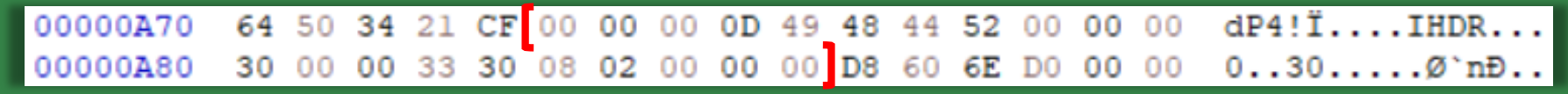
IHDR



Crash Analysis

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



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

```
This exception may be expected and handled.
eax=03f58fff ebx=0000001e ecx=03f58fff edx=00000010 esi=0000001e edi=02e4c9a0
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:03f59001=??
```

```
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=03620000 ebx=0000004d ecx=03620000 edx=0000001f esi=00000090 edi=02cfca10
eip=006daaf0 esp=0019f788 ebp=0019f790 iopl=0         nv up ei pl nz ac po nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00210212
HanSee+0x2daaf0:
006daaf0 885902          mov     byte ptr [ecx+2],bl        ds:002b:03620002=90
```

감사합니다