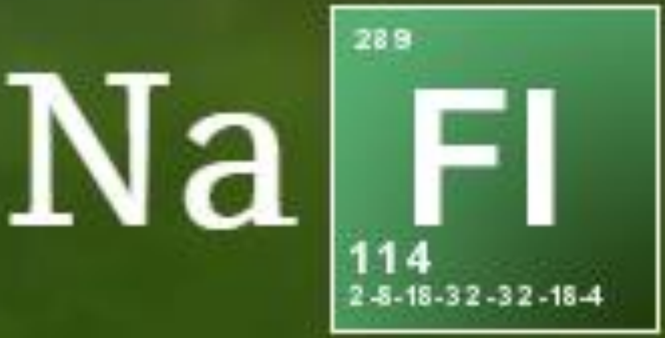


It is totally not AFL

DISCLAIMER

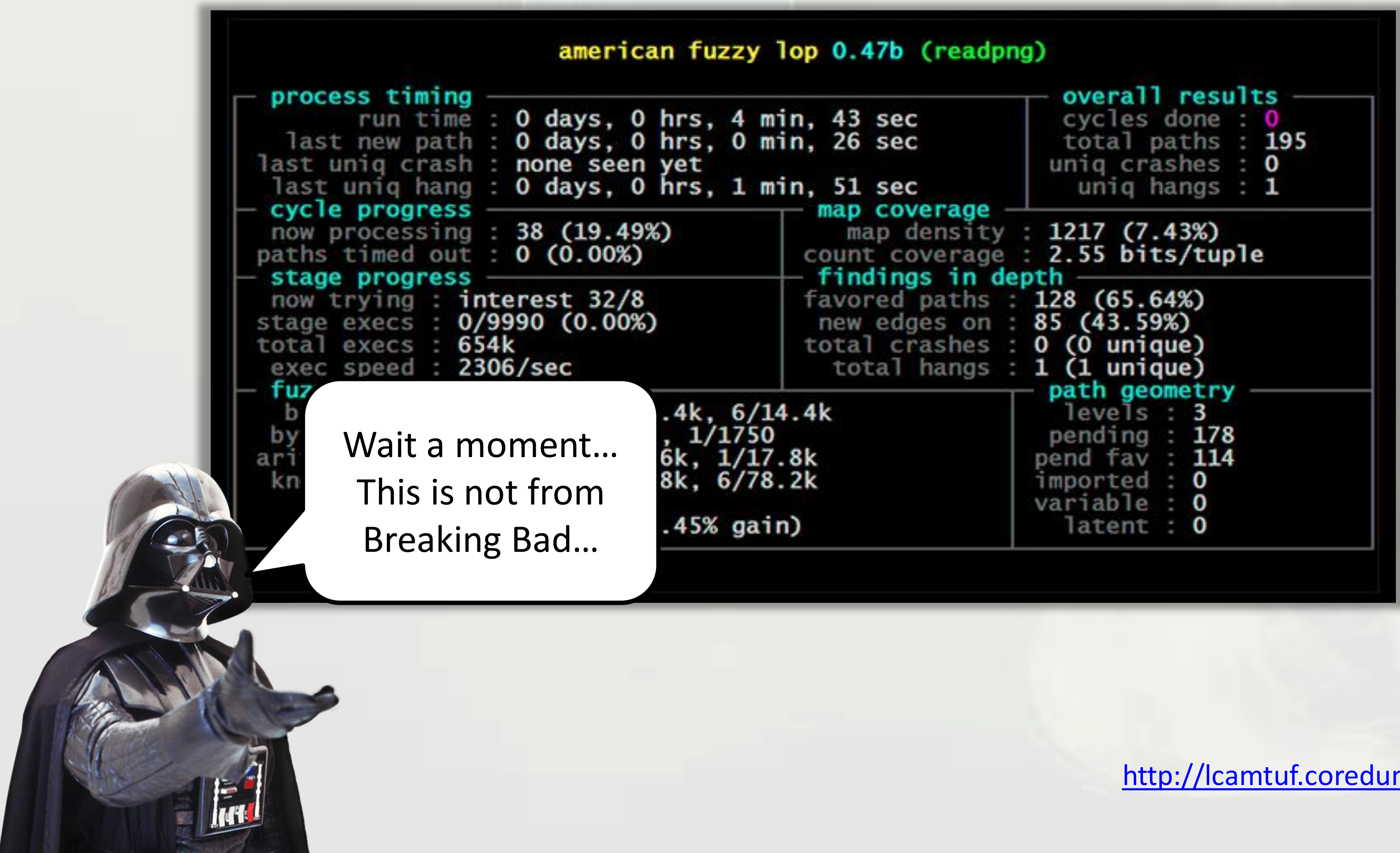
What & why?

- CSA *Vorfeld* Time (~2 weeks)
- I wanted to do something related to fuzzing
- You say fuzzing
    - I only hear AFL

- AFL is the *new cool kid on the block*

126.90447 2 8 18 18 7 53

I am your father



```
                 american fuzzy lop 0.47b (readpng)

┌─ process timing ─────────────────────────────────────┬─ overall results ─────┐
│        run time : 0 days, 0 hrs, 4 min, 43 sec        │  cycles done : 0      │
│   last new path : 0 days, 0 hrs, 0 min, 26 sec        │  total paths : 195    │
│ last uniq crash : none seen yet                       │ uniq crashes : 0      │
│  last uniq hang : 0 days, 0 hrs, 1 min, 51 sec        │   uniq hangs : 1      │
├─ cycle progress ───────────────────┬─ map coverage ─┴───────────────────────┤
│  now processing : 38 (19.49%)      │    map density : 1217 (7.43%)          │
│ paths timed out : 0 (0.00%)        │ count coverage : 2.55 bits/tuple       │
├─ stage progress ───────────────────┼─ findings in depth ────────────────────┤
│  now trying : interest 32/8        │ favored paths : 128 (65.64%)           │
│ stage execs : 0/9990 (0.00%)       │  new edges on : 85 (43.59%)            │
│ total execs : 654k                 │ total crashes : 0 (0 unique)           │
│  exec speed : 2306/sec             │   total hangs : 1 (1 unique)           │
├─ fuz                               ──────────────┬─ path geometry ───────────┤
│   b                       .4k, 6/14.4k           │    levels : 3             │
│  by                       , 1/1750               │   pending : 178           │
│ ari                       6k, 1/17.8k            │  pend fav : 114           │
│  kn                       8k, 6/78.2k            │  imported : 0             │
│                                                  │  variable : 0             │
│                           .45% gain)             │    latent : 0             │
└──────────────────────────────────────────────────┴───────────────────────────┘
```

http://lcamtuf.coredump.cx/afl/

Dbirty Binary Instrumentation

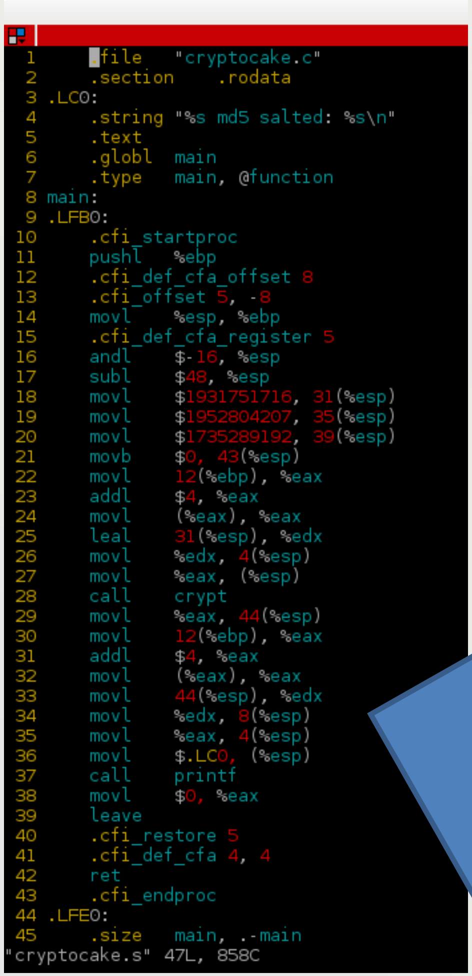
AFL: **dirty** but hey, **effective**…

From the docs:

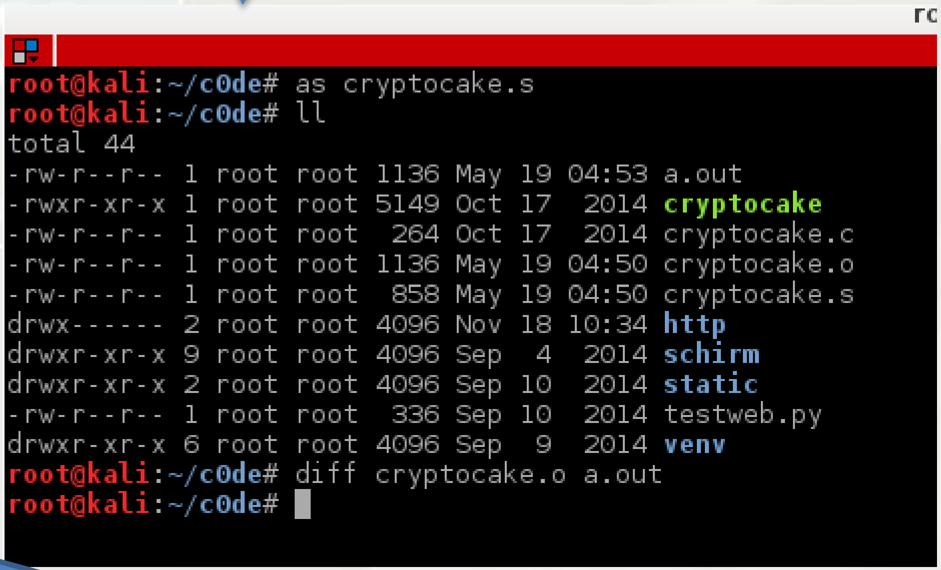
*“When source code is available, instrumentation can be injected by a companion tool that works as a **drop-in replacement for gcc or clang** in any standard build process for third-party code.”*

```
$ CC=/path/to/afl/afl-gcc ./configure
$ make clean all
```

Dbirty Binary Instrumentation



```
        .file   "cryptocake.c"
        .section        .rodata
.LC0:
        .string "%s md5 salted: %s\n"
        .text
        .globl  main
        .type   main, @function
main:
.LFB0:
        .cfi_startproc
        pushl   %ebp
        .cfi_def_cfa_offset 8
        .cfi_offset 5, -8
        movl    %esp, %ebp
        .cfi_def_cfa_register 5
        andl    $-16, %esp
        subl    $48, %esp
        movl    $1931751716, 31(%esp)
        movl    $1952804207, 35(%esp)
        movl    $1735289192, 39(%esp)
        movb    $0, 43(%esp)
        movl    12(%ebp), %eax
        addl    $4, %eax
        movl    (%eax), %eax
        leal    31(%esp), %edx
        movl    %edx, 4(%esp)
        movl    %eax, (%esp)
        call    crypt
        movl    %eax, 44(%esp)
        movl    12(%ebp), %eax
        addl    $4, %eax
        movl    (%eax), %eax
        movl    44(%esp), %edx
        movl    %edx, 8(%esp)
        movl    %eax, 4(%esp)
        movl    $.LC0, (%esp)
        call    printf
        movl    $0, %eax
        leave
        .cfi_restore 5
        .cfi_def_cfa 4, 4
        ret
        .cfi_endproc
.LFE0:
        .size   main, .-main
"cryptocake.s" 47L, 858C
```



```
root@kali:~/c0de# as cryptocake.s
root@kali:~/c0de# ll
total 44
-rw-r--r-- 1 root root 1136 May 19 04:53 a.out
-rwxr-xr-x 1 root root 5149 Oct 17  2014 cryptocake
-rw-r--r-- 1 root root  264 Oct 17  2014 cryptocake.c
-rw-r--r-- 1 root root 1136 May 19 04:50 cryptocake.o
-rw-r--r-- 1 root root  858 May 19 04:50 cryptocake.s
drwx------ 2 root root 4096 Nov 18 10:34 http
drwxr-xr-x 9 root root 4096 Sep  4  2014 schirm
drwxr-xr-x 2 root root 4096 Sep 10  2014 static
-rw-r--r-- 1 root root  336 Sep 10  2014 testweb.py
drwxr-xr-x 6 root root 4096 Sep  9  2014 venv
root@kali:~/c0de# diff cryptocake.o a.out
root@kali:~/c0de# 
```

AFL writes its own ASM code here o.O

```
$ gcc -S cryptocake.c
```

meaSuring Code coVerage

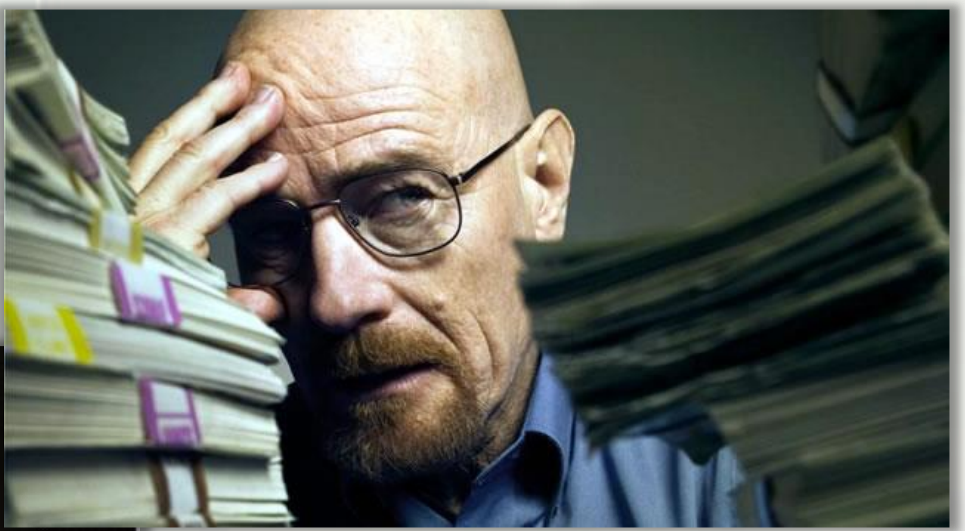
- Information about ***branches taken*** is encoded in a ***bitmap***

```
        bitmap[(current_id ^ last_id) % BITMAP_SIZE]++;
        last_id = current_id >> 1;
```

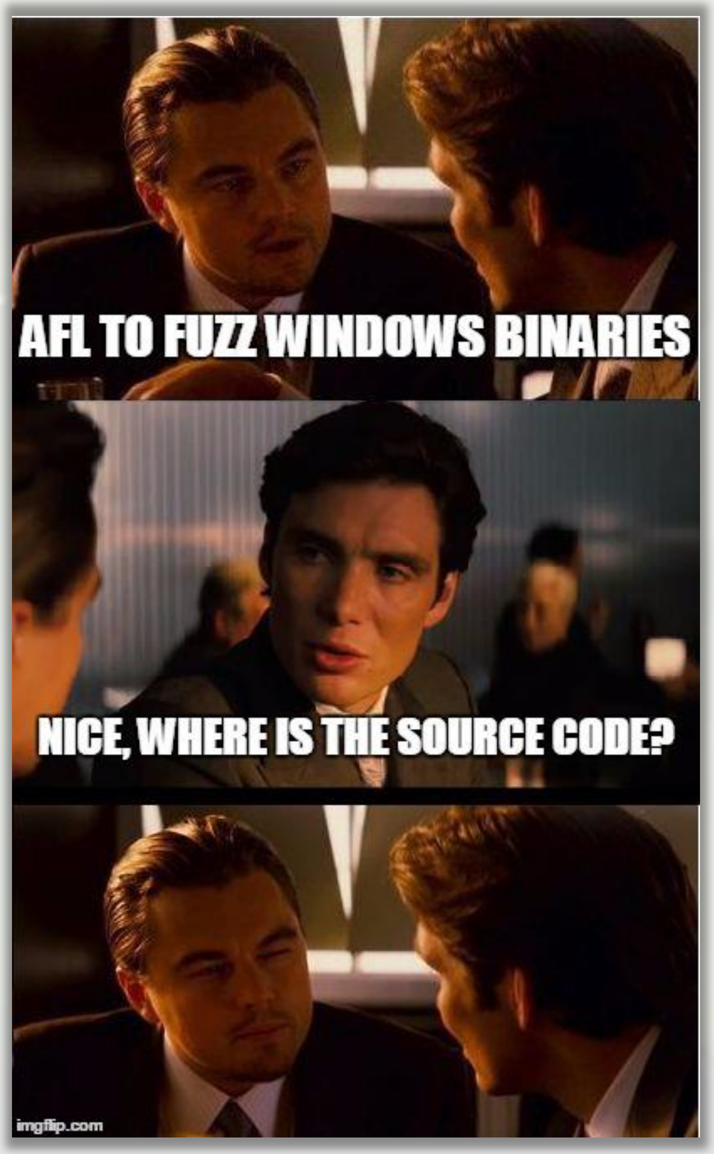
- ***Shared memory*** with the mutation engine
- ***Feedback***: this has ***exercised new code paths***

Euverything Linix Centric

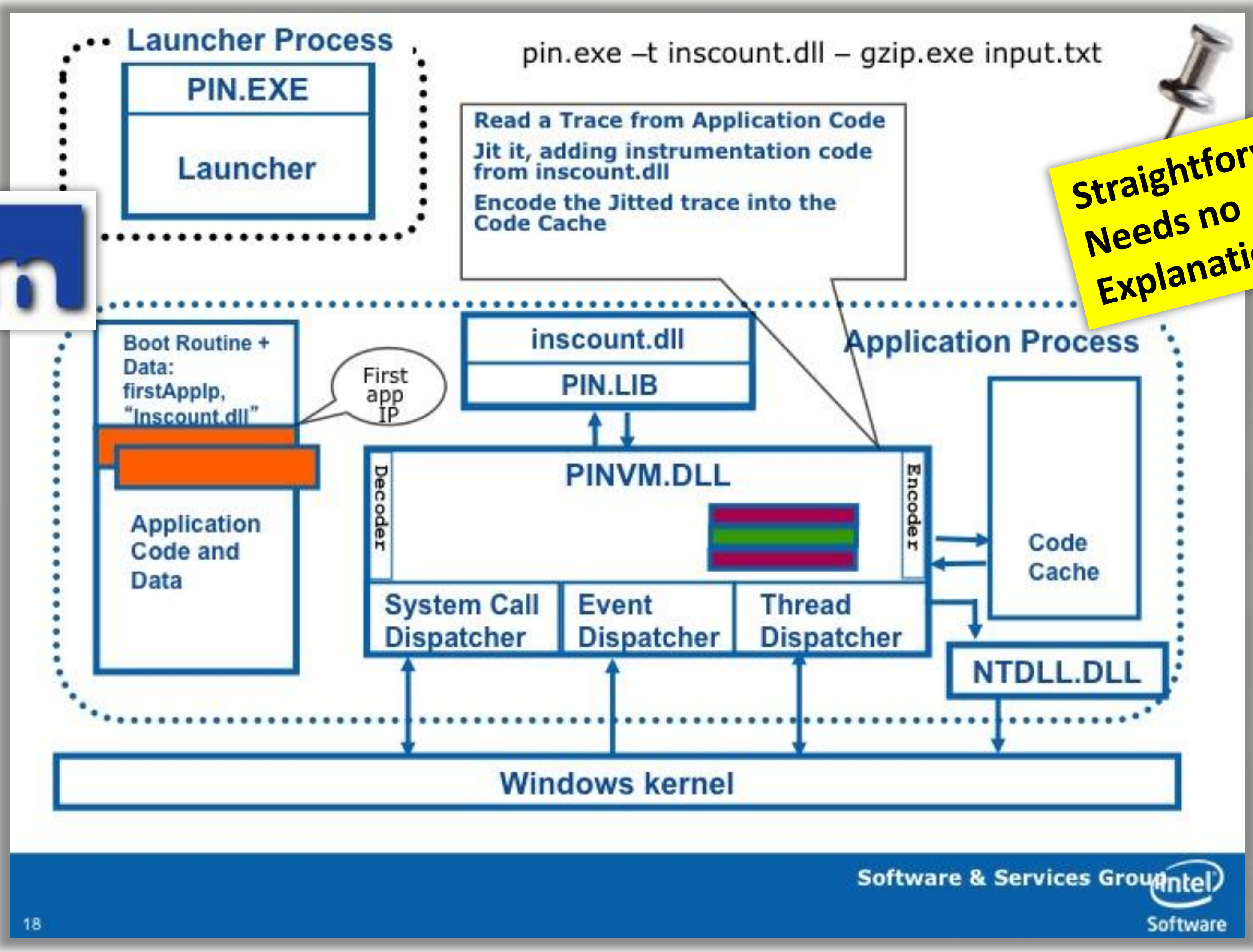
But the money is on Windows!!!1!



letS use on Windows tHen



Dbynamic Binary Instrumentation



pin.exe –t inscount.dll – gzip.exe input.txt

Launcher Process

PIN.EXE

Launcher

Read a Trace from Application Code

Jit it, adding instrumentation code from inscount.dll

Encode the Jitted trace into the Code Cache

Application Process

Boot Routine + Data: firstAppIp, "Inscount.dll"

First app IP

Application Code and Data

inscount.dll

PIN.LIB

PINVM.DLL

Decoder

Encoder

Code Cache

System Call Dispatcher

Event Dispatcher

Thread Dispatcher

NTDLL.DLL

Windows kernel

Software & Services Group

intel Software

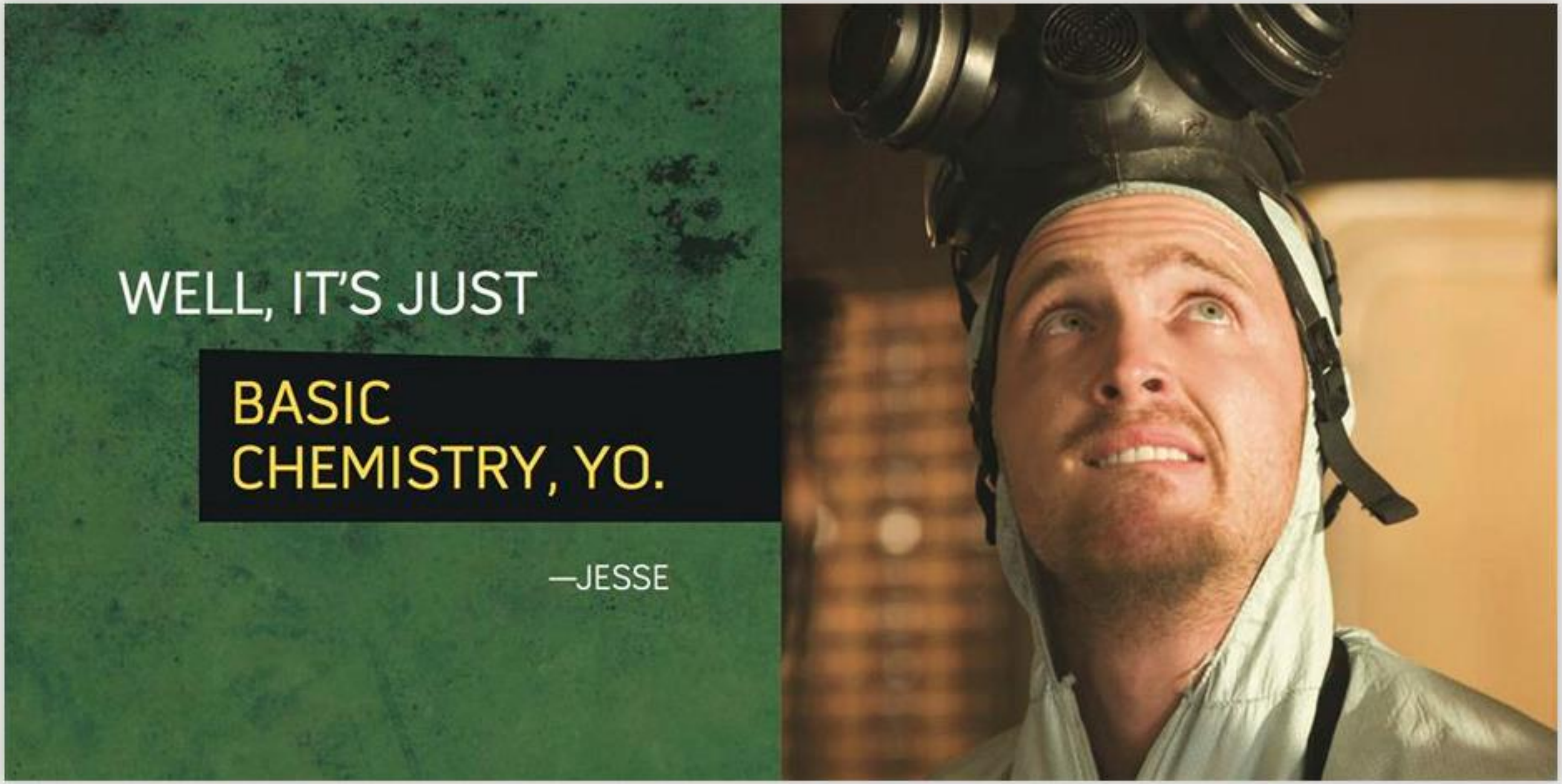
18

Straightforward
Needs no
Explanation :)

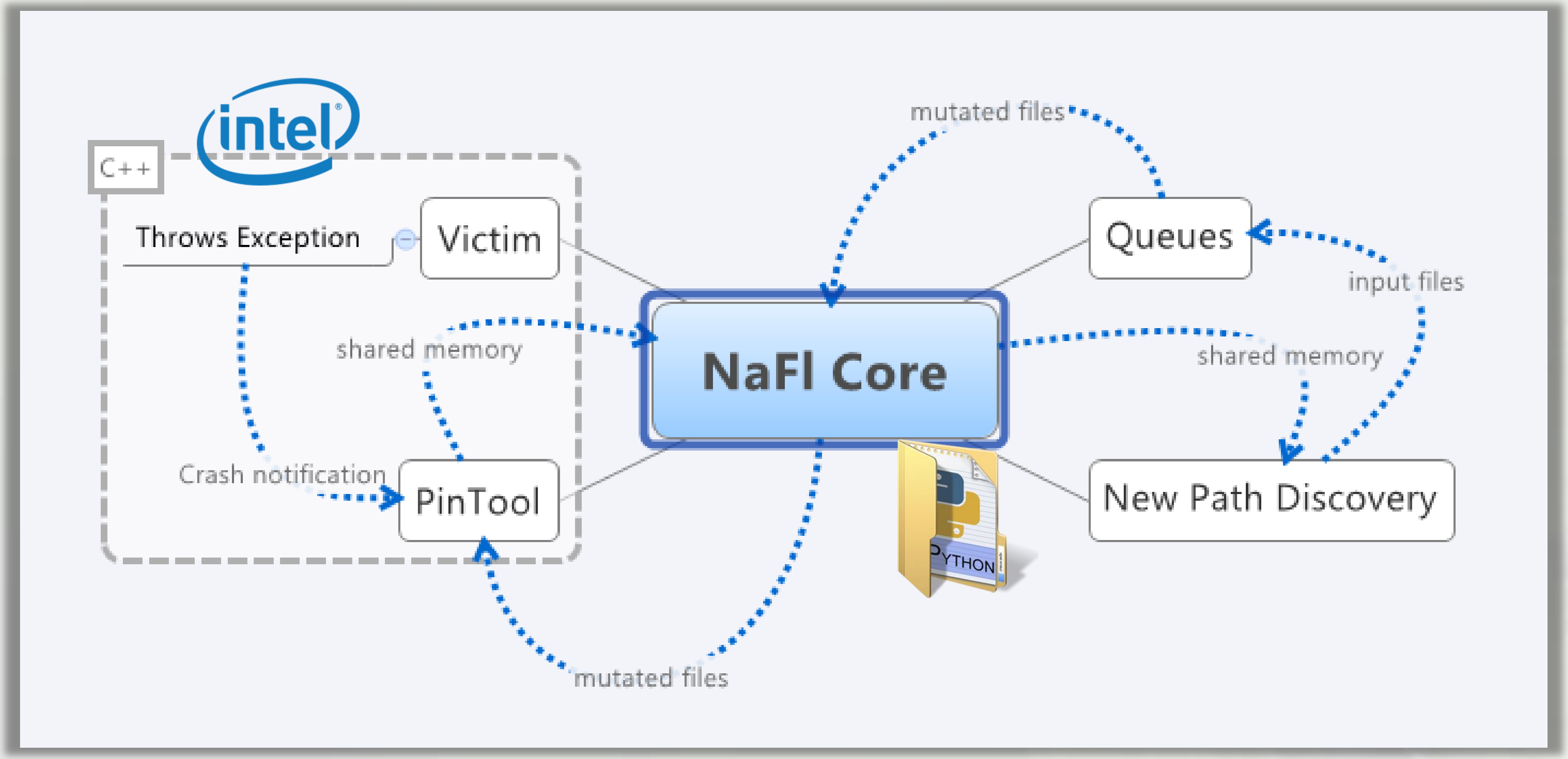
Dbynamic Binary Instrumentation

```
void Trace(TRACE trace, void *v)
{
  // Iterate through basic blocks
  for (BBL bbl = TRACE_BblHead(trace); BBL_Valid(bbl); bbl = BBL_Next(bbl))
  {
    // Code to instrument the events at the end of a BBL (execution transfer)
    // Checking for jnz, jle, ja, etc.
    // NOTE: This is not a BB like shown in IDA but following the definition :)
    INS tail = BBL_InsTail(bbl);

    // Instrument only the interesting code
    if (withinInterestingExecutable(INS_Address(tail)))
    {
      if (INS_IsBranch(tail))
      {
        if (INS_HasFallThrough(tail) || INS_IsCall(tail))
        {
          // From the documentation:
          // So HasFallThrough is TRUE for
          // * instructions which don't change the control flow(most instructions)
          // * or conditional branches (which might change the control flow, but might not),
          // and FALSE for:
          // * unconditional branches and calls (the next instruction to be executed is always explicitly specified).
          INS_InsertPredicatedCall(
            tail,
            IPOINT_BEFORE,
            AFUNPTR(LogConditionalJmp),  // Analysis function
            IARG_INST_PTR,        // [R|E]IP of instruction
            IARG_END          // No more args
            );
        }
```

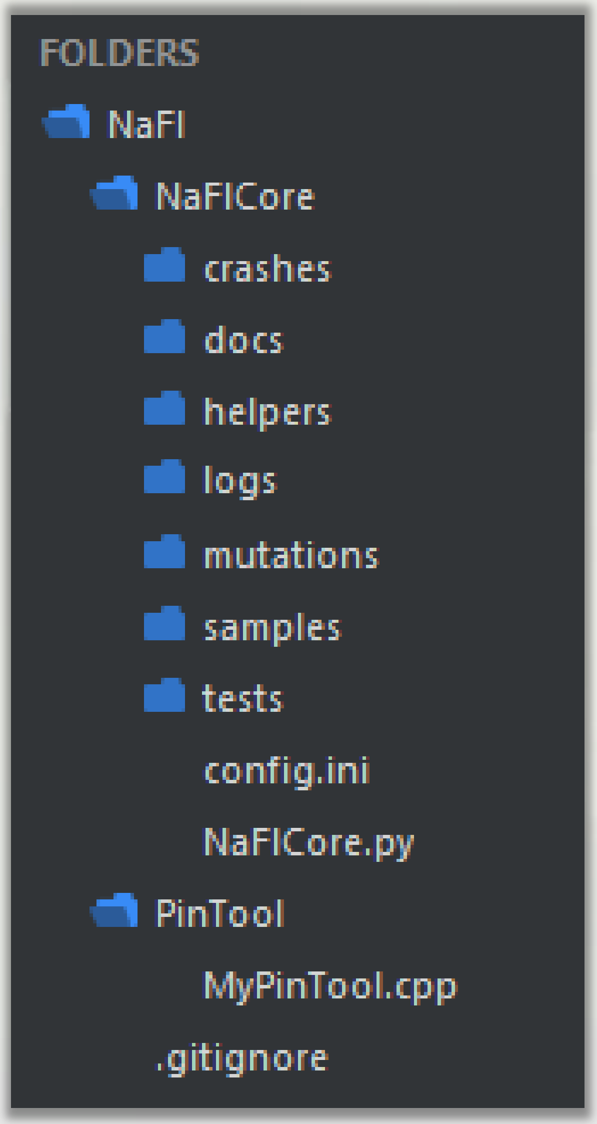
Dbynamic Binary Instrumentation



OvervIew

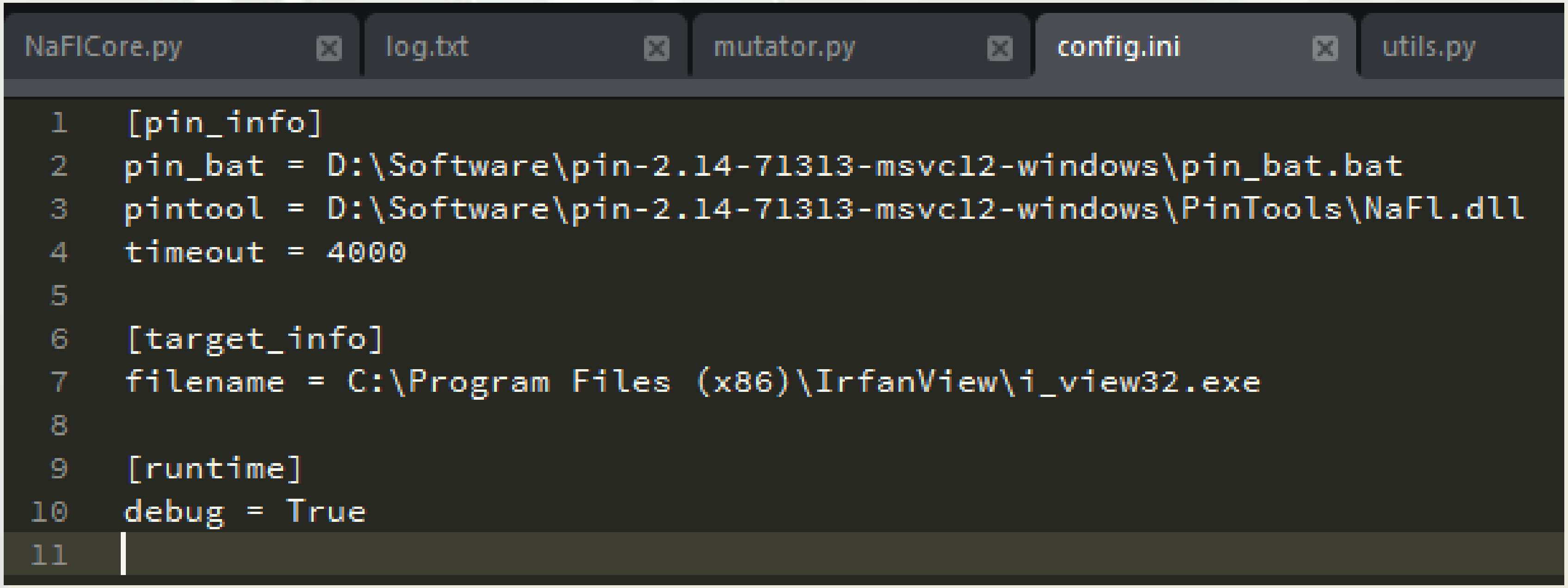

intel
C++
Throws Exception
Victim
shared memory
Crash notification
PinTool
mutated files
NaFl Core
PYTHON
mutated files
Queues
input files
shared memory
New Path Discovery

Dbirectory Structure



```
FOLDERS
NaFI
    NaFICore
        crashes
        docs
        helpers
        logs
        mutations
        samples
        tests
        config.ini
        NaFICore.py
    PinTool
        MyPinTool.cpp
    .gitignore
```

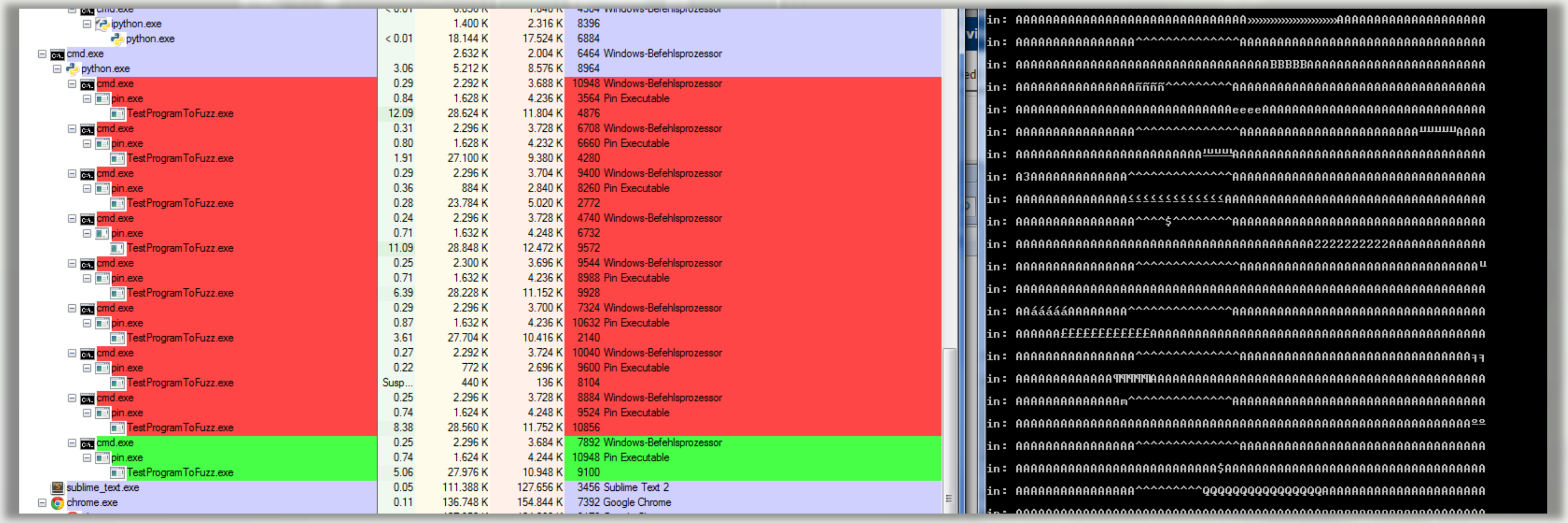
Config file



```
[pin_info]
pin_bat = D:\Software\pin-2.14-71313-msvc12-windows\pin_bat.bat
pintool = D:\Software\pin-2.14-71313-msvc12-windows\PinTools\NaFl.dll
timeout = 4000

[target_info]
filename = C:\Program Files (x86)\IrfanView\i_view32.exe

[runtime]
debug = True

```

at Work

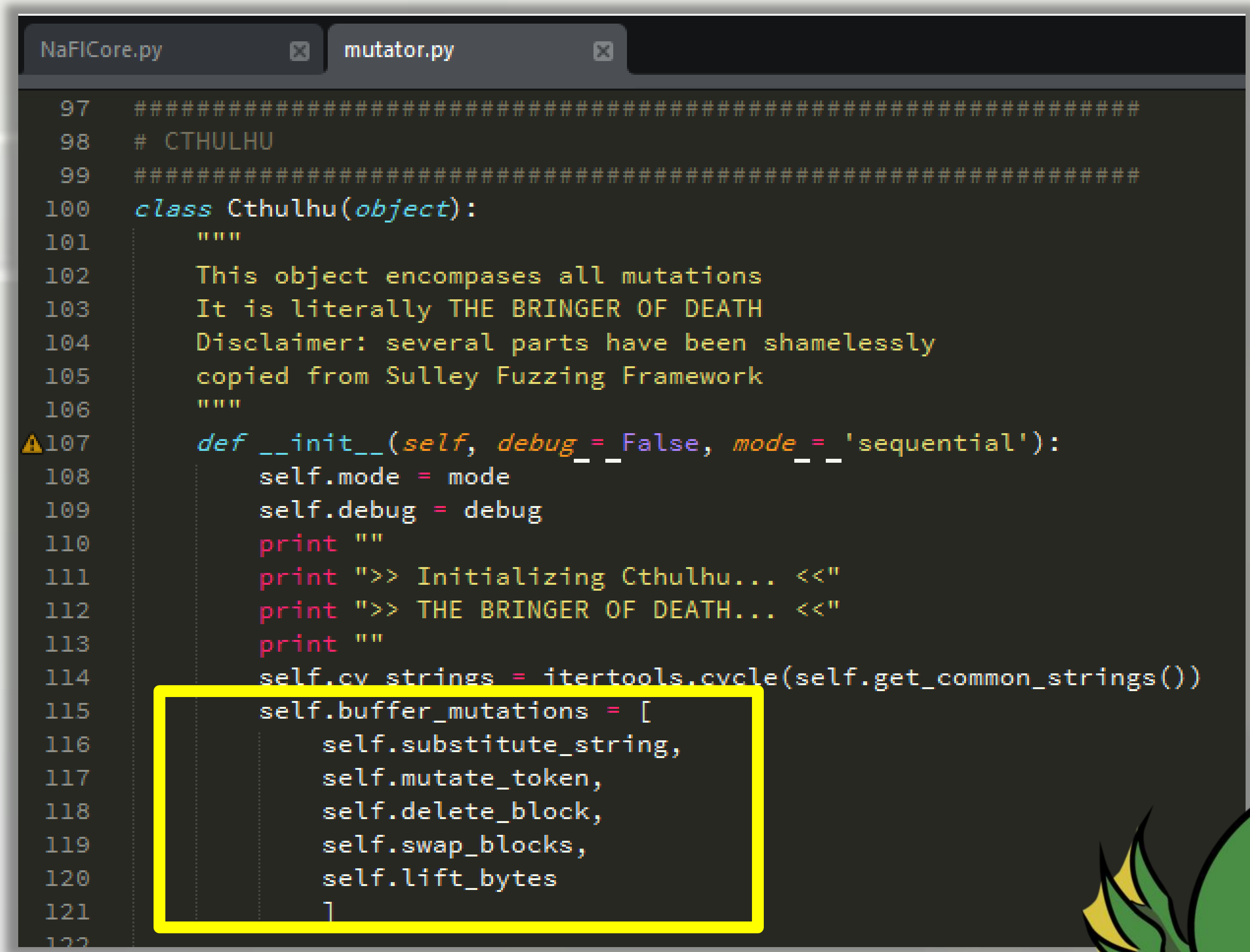
183.84 74 2 8 18 32 12 2



ipython.exe		1.400 K	2.316 K	8396	
python.exe	< 0.01	18.144 K	17.524 K	6884	
cmd.exe		2.632 K	2.004 K	6464	Windows-Befehlsprozessor
python.exe	3.06	5.212 K	8.576 K	8964	
cmd.exe	0.29	2.292 K	3.688 K	10948	Windows-Befehlsprozessor
pin.exe	0.84	1.628 K	4.236 K	3564	Pin Executable
TestProgramToFuzz.exe	12.09	28.624 K	11.804 K	4876	
cmd.exe	0.31	2.296 K	3.728 K	6708	Windows-Befehlsprozessor
pin.exe	0.80	1.628 K	4.232 K	6660	Pin Executable
TestProgramToFuzz.exe	1.91	27.100 K	9.380 K	4280	
cmd.exe	0.29	2.296 K	3.704 K	9400	Windows-Befehlsprozessor
pin.exe	0.36	884 K	2.840 K	8260	Pin Executable
TestProgramToFuzz.exe	0.28	23.784 K	5.020 K	2772	
cmd.exe	0.24	2.296 K	3.728 K	4740	Windows-Befehlsprozessor
pin.exe	0.71	1.632 K	4.248 K	6732	
TestProgramToFuzz.exe	11.09	28.848 K	12.472 K	9572	
cmd.exe	0.25	2.300 K	3.696 K	9544	Windows-Befehlsprozessor
pin.exe	0.71	1.632 K	4.236 K	8988	Pin Executable
TestProgramToFuzz.exe	6.39	28.228 K	11.152 K	9928	
cmd.exe	0.29	2.296 K	3.700 K	7324	Windows-Befehlsprozessor
pin.exe	0.87	1.632 K	4.236 K	10632	Pin Executable
TestProgramToFuzz.exe	3.61	27.704 K	10.416 K	2140	
cmd.exe	0.27	2.292 K	3.724 K	10040	Windows-Befehlsprozessor
pin.exe	0.22	772 K	2.696 K	9600	Pin Executable
TestProgramToFuzz.exe	Susp...	440 K	136 K	8104	
cmd.exe	0.25	2.296 K	3.728 K	8884	Windows-Befehlsprozessor
pin.exe	0.74	1.624 K	4.248 K	9524	Pin Executable
TestProgramToFuzz.exe	8.38	28.560 K	11.752 K	10856	
cmd.exe	0.25	2.296 K	3.684 K	7892	Windows-Befehlsprozessor
pin.exe	0.74	1.624 K	4.244 K	10948	Pin Executable
TestProgramToFuzz.exe	5.06	27.976 K	10.948 K	9100	
sublime_text.exe	0.05	111.388 K	127.656 K	3456	Sublime Text 2
chrome.exe	0.11	136.748 K	154.844 K	7392	Google Chrome

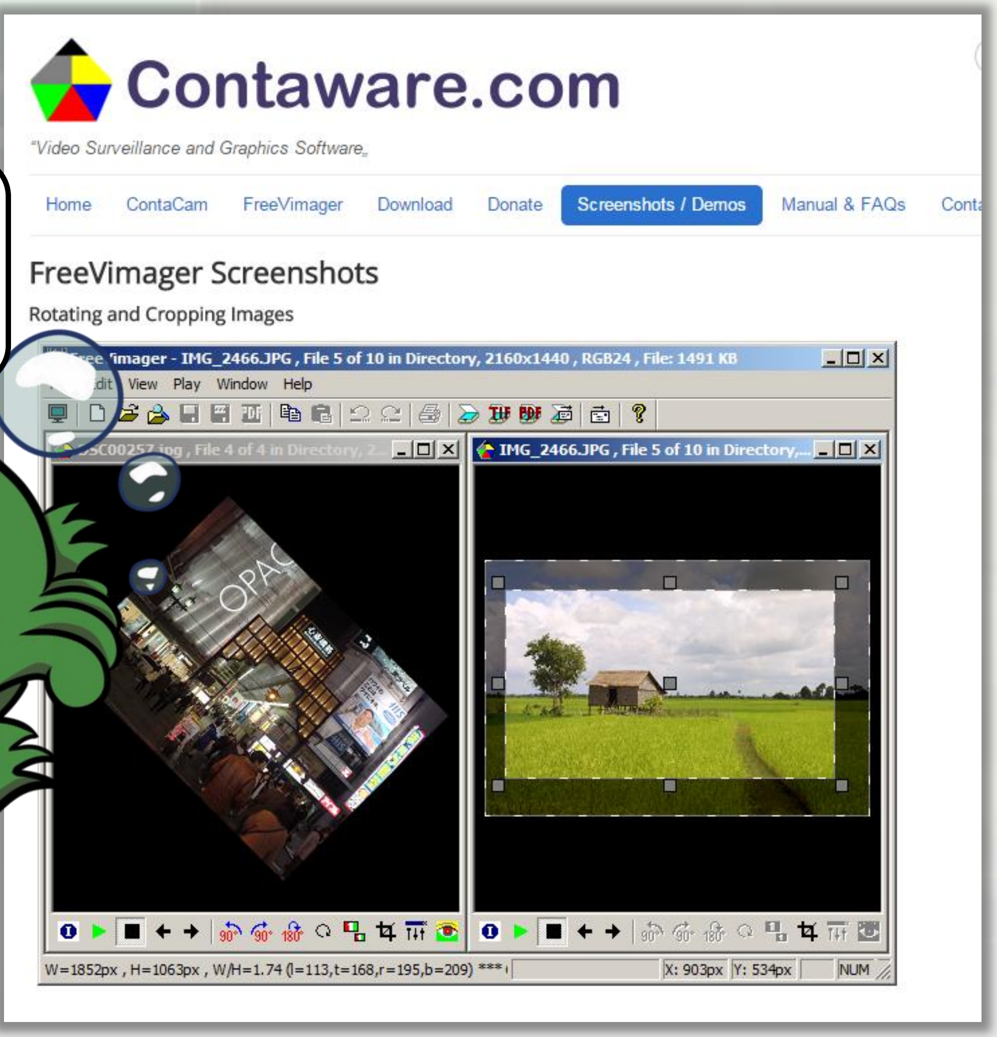
```
in: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA»»»»»»»»»»»»AAAAAAAAAAAAAAAAAAAA
in: AAAAAAAAAAAAAAAA^^^^^^^^^^^^^^AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
in: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBBBAAAAAAAAAAAAAAAAAAAAAAAA
in: AAAAAAAAAAAAAAAAññññ^^^^^^^^^AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
in: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAeeeeAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
in: AAAAAAAAAAAAAAAA^^^^^^^^^^^^^^AAAAAAAAAAAAAAAAAAAAAAAAA⊔⊔⊔⊔⊔AAAA
in: AAAAAAAAAAAAAAAAAAAAAAAAA╨╨╨╨AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
in: A3AAAAAAAAAAAAA^^^^^^^^^^^^^^AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
in: AAAAAAAAAAAAAAA≤≤≤≤≤≤≤≤≤≤≤≤≤AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
in: AAAAAAAAAAAAAAAA^^^^$^^^^^^^^AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
in: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA2222222222AAAAAAAAAAAAA
in: AAAAAAAAAAAAAAAA^^^^^^^^^^^^^^AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA⊔
in: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
in: AAáááááAAAAAAAA^^^^^^^^^^^^^^AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
in: AAAAAA££££££££££££AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
in: AAAAAAAAAAAAAAAA^^^^^^^^^^^^^^AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA╕╕
in: AAAAAAAAAAAAA¶¶¶¶¶AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
in: AAAAAAAAAAAAAAm^^^^^^^^^^^^^^AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
in: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAºº
in: AAAAAAAAAAAAAAAA^^^^^^^^^^^^^^AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
in: AAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
in: AAAAAAAAAAAAAAAA^^^^^^^^^QQQQQQQQQQQQQQQQAAAAAAAAAAAAAAAAAAAAAAA
```

Cthulhu



```
###################################################################
# CTHULHU
###################################################################
class Cthulhu(object):
    """
    This object encompases all mutations
    It is literally THE BRINGER OF DEATH
    Disclaimer: several parts have been shamelessly
    copied from Sulley Fuzzing Framework
    """
    def __init__(self, debug = False, mode = 'sequential'):
        self.mode = mode
        self.debug = debug
        print ""
        print ">> Initializing Cthulhu... <<"
        print ">> THE BRINGER OF DEATH... <<"
        print ""
        self.cy_strings = itertools.cycle(self.get_common_strings())
        self.buffer_mutations = [
            self.substitute_string,
            self.mutate_token,
            self.delete_block,
            self.swap_blocks,
            self.lift_bytes
            ]
```

Picking an easY target



Contaware.com

"Video Surveillance and Graphics Software"

FreeVimager Screenshots

Rotating and Cropping Images

ree Vimager - IMG_2466.JPG , File 5 of 10 in Directory, 2160x1440 , RGB24 , File: 1491 KB

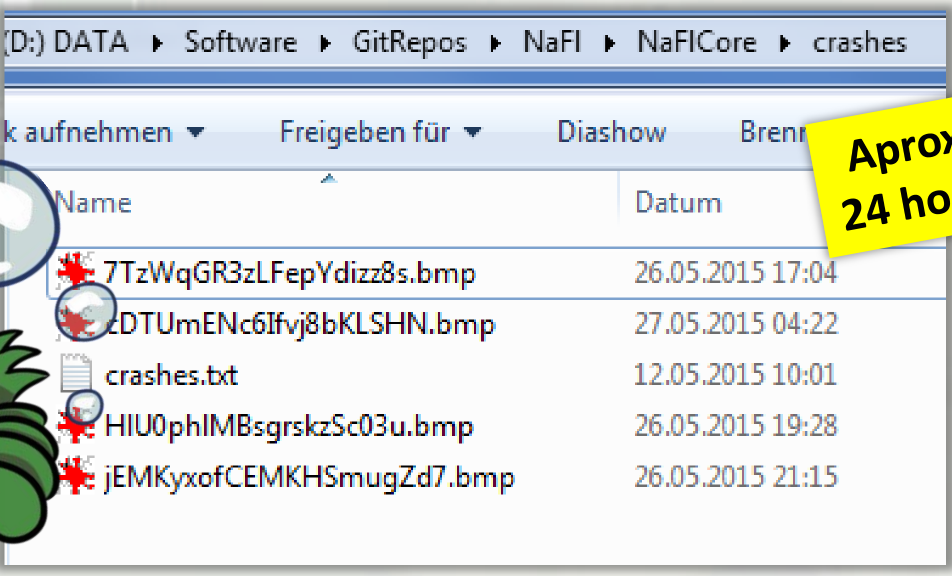
SC00257.jpg , File 4 of 4 in Directory, 2...

IMG_2466.JPG , File 5 of 10 in Directory,...

W=1852px , H=1063px , W/H=1.74 (l=113,t=168,r=195,b=209) *** X: 903px Y: 534px NUM

http://www.contaware.com/freevimager.html

Picking an easY target


(D:) DATA ▸ Software ▸ GitRepos ▸ NaFl ▸ NaFlCore ▸ crashes

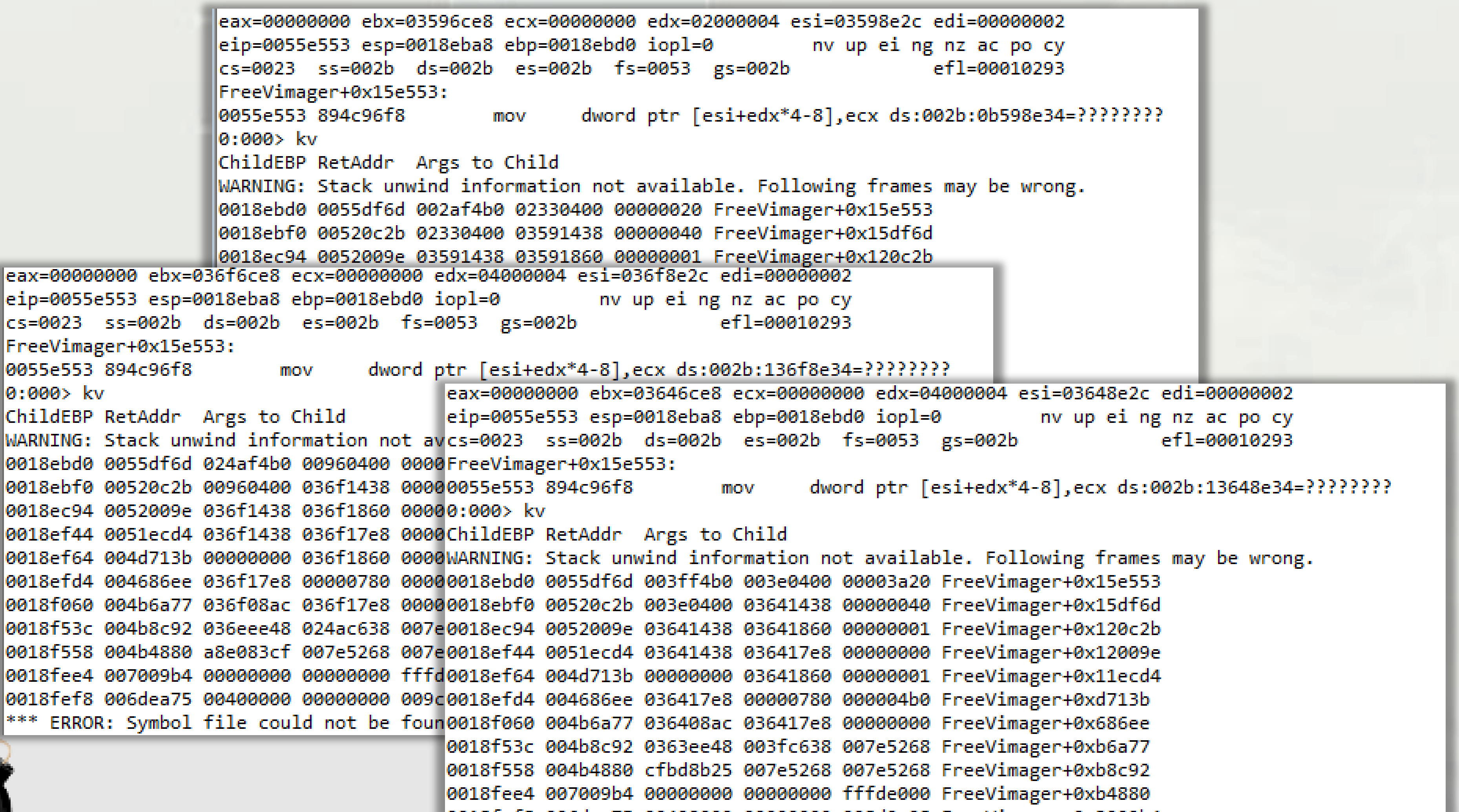
Name	Datum
7TzWqGR3zLFepYdizz8s.bmp	26.05.2015 17:04
zDTUmENc6Ifvj8bKLSHN.bmp	27.05.2015 04:22
crashes.txt	12.05.2015 10:01
HIU0phIMBsgrskzSc03u.bmp	26.05.2015 19:28
jEMKyxofCEMKHSmugZd7.bmp	26.05.2015 21:15

Aprox.
24 hours

log.txt

http://www.contaware.com/freevimager.html

What Happened

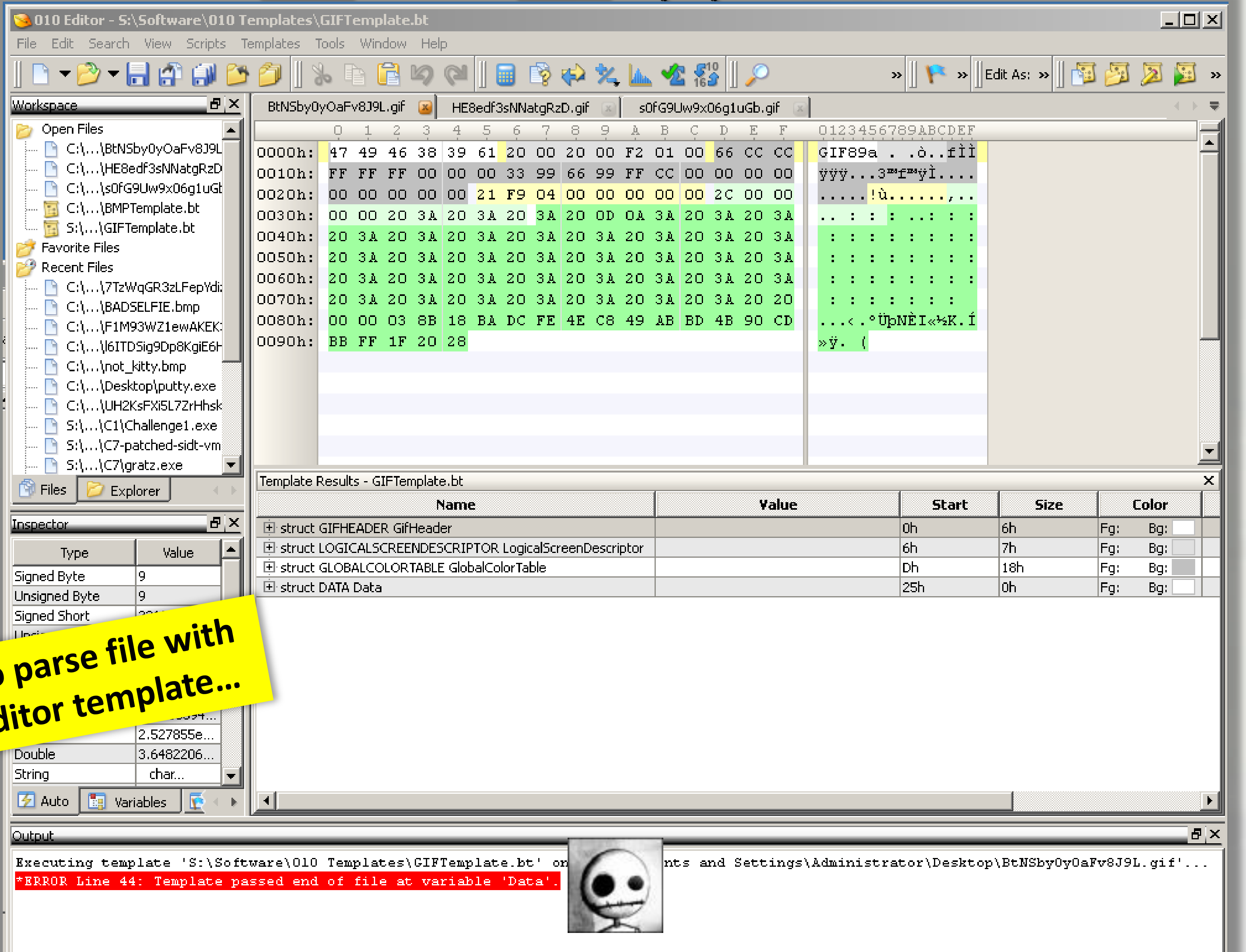


```
eax=00000000 ebx=03596ce8 ecx=00000000 edx=02000004 esi=03598e2c edi=00000002
eip=0055e553 esp=0018eba8 ebp=0018ebd0 iopl=0         nv up ei ng nz ac po cy
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010293
FreeVimager+0x15e553:
0055e553 894c96f8        mov     dword ptr [esi+edx*4-8],ecx ds:002b:0b598e34=????????
0:000> kv
ChildEBP RetAddr  Args to Child
WARNING: Stack unwind information not available. Following frames may be wrong.
0018ebd0 0055df6d 002af4b0 02330400 00000020 FreeVimager+0x15e553
0018ebf0 00520c2b 02330400 03591438 00000040 FreeVimager+0x15df6d
0018ec94 0052009e 03591438 03591860 00000001 FreeVimager+0x120c2b
```

```
eax=00000000 ebx=036f6ce8 ecx=00000000 edx=04000004 esi=036f8e2c edi=00000002
eip=0055e553 esp=0018eba8 ebp=0018ebd0 iopl=0         nv up ei ng nz ac po cy
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010293
FreeVimager+0x15e553:
0055e553 894c96f8        mov     dword ptr [esi+edx*4-8],ecx ds:002b:136f8e34=????????
0:000> kv
ChildEBP RetAddr  Args to Child
WARNING: Stack unwind information not av
0018ebd0 0055df6d 024af4b0 00960400 0000
0018ebf0 00520c2b 00960400 036f1438 0000
0018ec94 0052009e 036f1438 036f1860 0000
0018ef44 0051ecd4 036f1438 036f17e8 0000
0018ef64 004d713b 00000000 036f1860 0000
0018efd4 004686ee 036f17e8 00000780 0000
0018f060 004b6a77 036f08ac 036f17e8 0000
0018f53c 004b8c92 036eee48 024ac638 007e
0018f558 004b4880 a8e083cf 007e5268 007e
0018fee4 007009b4 00000000 00000000 fffd
0018fef8 006dea75 00400000 00000000 009c
*** ERROR: Symbol file could not be foun
```

```
eax=00000000 ebx=03646ce8 ecx=00000000 edx=04000004 esi=03648e2c edi=00000002
eip=0055e553 esp=0018eba8 ebp=0018ebd0 iopl=0         nv up ei ng nz ac po cy
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010293
FreeVimager+0x15e553:
0055e553 894c96f8        mov     dword ptr [esi+edx*4-8],ecx ds:002b:13648e34=????????
0:000> kv
ChildEBP RetAddr  Args to Child
WARNING: Stack unwind information not available. Following frames may be wrong.
0018ebd0 0055df6d 003ff4b0 003e0400 00003a20 FreeVimager+0x15e553
0018ebf0 00520c2b 003e0400 03641438 00000040 FreeVimager+0x15df6d
0018ec94 0052009e 03641438 03641860 00000001 FreeVimager+0x120c2b
0018ef44 0051ecd4 03641438 036417e8 00000000 FreeVimager+0x12009e
0018ef64 004d713b 00000000 03641860 00000001 FreeVimager+0x11ecd4
0018efd4 004686ee 036417e8 00000780 000004b0 FreeVimager+0xd713b
0018f060 004b6a77 036408ac 036417e8 00000000 FreeVimager+0x686ee
0018f53c 004b8c92 0363ee48 003fc638 007e5268 FreeVimager+0xb6a77
0018f558 004b4880 cfbd8b25 007e5268 007e5268 FreeVimager+0xb8c92
0018fee4 007009b4 00000000 00000000 fffde000 FreeVimager+0xb4880
```

W hat H appened



010 Editor - S:\Software\010 Templates\GIFTemplate.bt

```
         0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h:  47 49 46 38 39 61 20 00 20 00 F2 01 00 66 CC CC   GIF89a . .ò..fÌÌ
0010h:  FF FF FF 00 00 00 33 99 66 99 FF CC 00 00 00 00   ÿÿÿ...3™f™ÿÌ....
0020h:  00 00 00 00 00 21 F9 04 00 00 00 00 00 2C 00 00   .....!ù.......,..
0030h:  00 00 20 3A 20 3A 20 3A 20 0D 0A 3A 20 3A 20 3A   .. : : : ..: : :
0040h:  20 3A 20 3A 20 3A 20 3A 20 3A 20 3A 20 3A 20 3A    : : : : : : : :
0050h:  20 3A 20 3A 20 3A 20 3A 20 3A 20 3A 20 3A 20 3A    : : : : : : : :
0060h:  20 3A 20 3A 20 3A 20 3A 20 3A 20 3A 20 3A 20 3A    : : : : : : : :
0070h:  20 3A 20 3A 20 3A 20 3A 20 3A 20 3A 20 3A 20 20    : : : : : : :
0080h:  00 00 03 8B 18 BA DC FE 4E C8 49 AB BD 4B 90 CD   ...‹.°ÜþNÈI«½K.Í
0090h:  BB FF 1F 20 28                                    »ÿ. (
```

Template Results - GIFTemplate.bt

Name	Value	Start	Size	Color
struct GIFHEADER GifHeader		0h	6h	Fg: Bg:
struct LOGICALSCREENDESCRIPTOR LogicalScreenDescriptor		6h	7h	Fg: Bg:
struct GLOBALCOLORTABLE GlobalColorTable		Dh	18h	Fg: Bg:
struct DATA Data		25h	0h	Fg: Bg:

Inspector

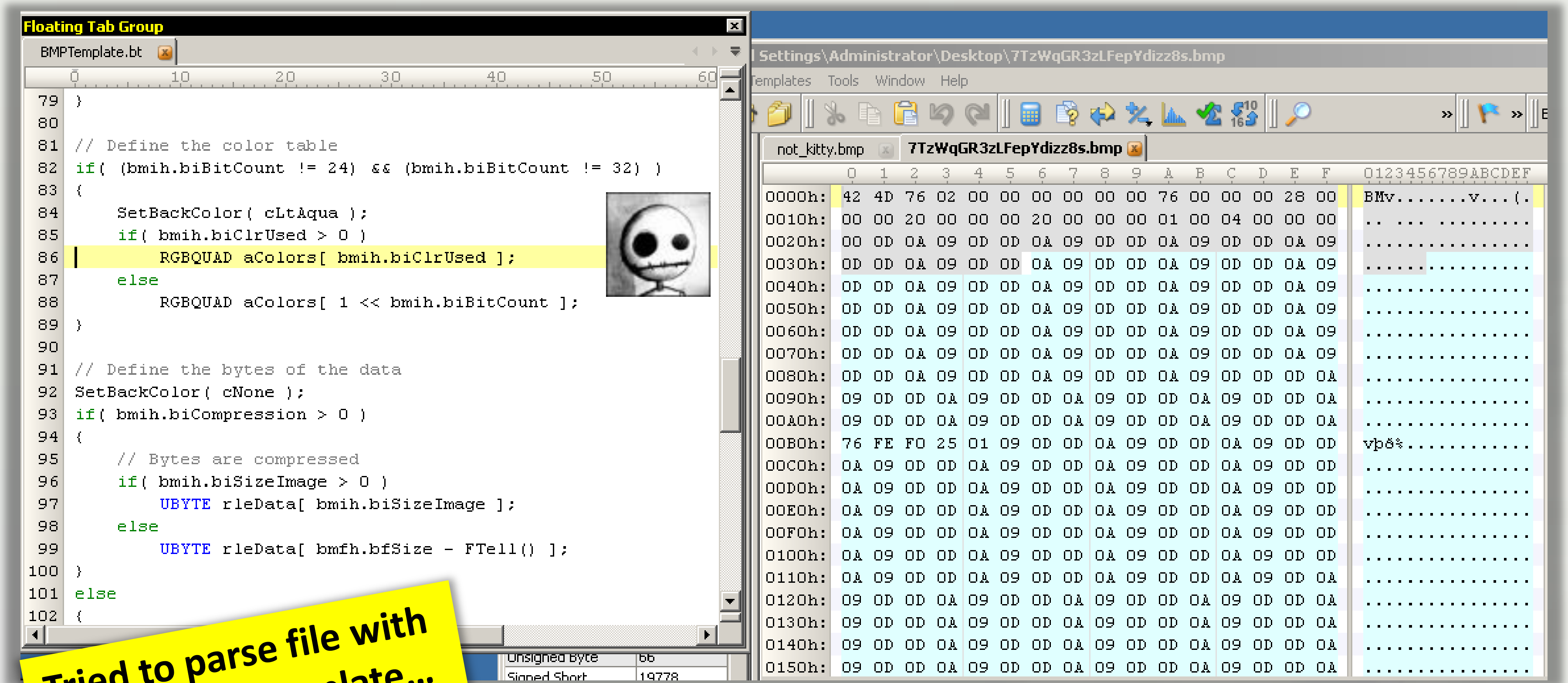
Type	Value
Signed Byte	9
Unsigned Byte	9
Signed Short	
	2.527855e...
Double	3.6482206...
String	char...

Output

```
Executing template 'S:\Software\010 Templates\GIFTemplate.bt' on nts and Settings\Administrator\Desktop\BtNSby0yOaFv8J9L.gif'...
*ERROR Line 44: Template passed end of file at variable 'Data'.
```

Tried to parse file with 010 editor template…

What Happened


Floating Tab Group
BMPTemplate.bt
Settings\Administrator\Desktop\7TzWqGR3zLFepYdizz8s.bmp
Templates Tools Window Help
not_kitty.bmp
7TzWqGR3zLFepYdizz8s.bmp

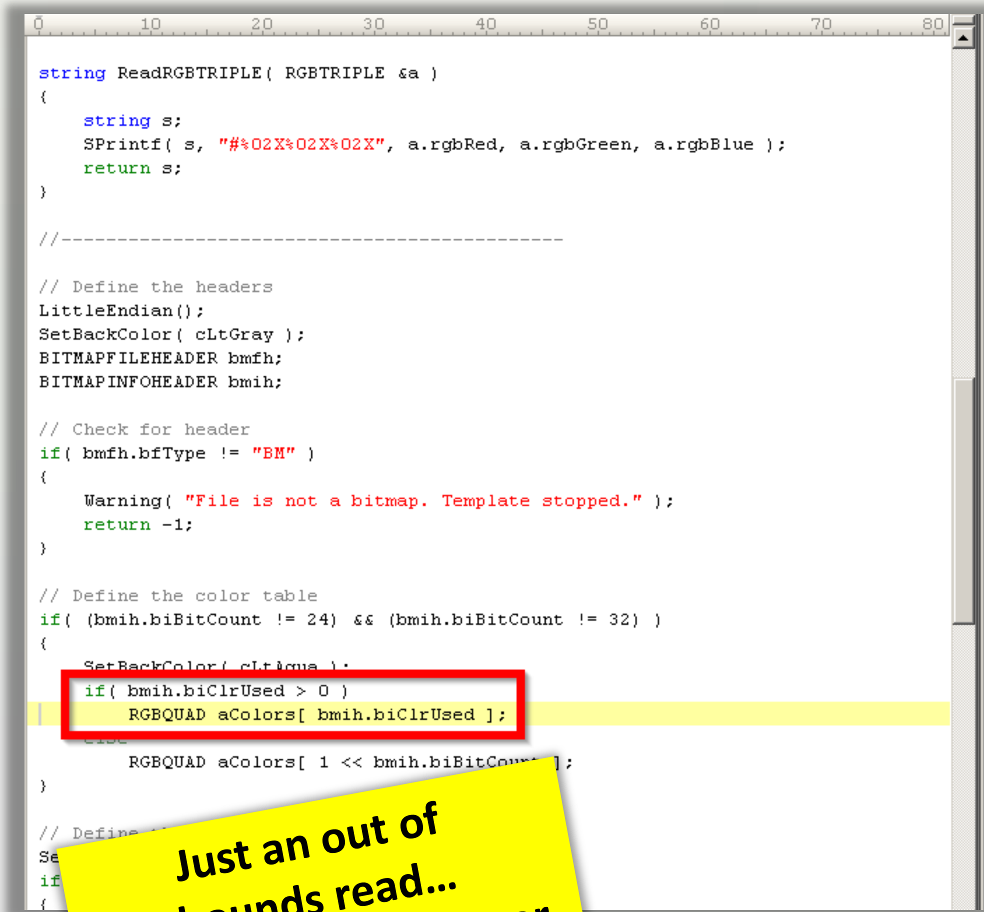
```
}

// Define the color table
if( (bmih.biBitCount != 24) && (bmih.biBitCount != 32) )
{
    SetBackColor( cLtAqua );
    if( bmih.biClrUsed > 0 )
        RGBQUAD aColors[ bmih.biClrUsed ];
    else
        RGBQUAD aColors[ 1 << bmih.biBitCount ];
}

// Define the bytes of the data
SetBackColor( cNone );
if( bmih.biCompression > 0 )
{
    // Bytes are compressed
    if( bmih.biSizeImage > 0 )
        UBYTE rleData[ bmih.biSizeImage ];
    else
        UBYTE rleData[ bmfh.bfSize - FTell() ];
}
else
{
```

```
Unsigned Byte   66
Signed Short    19778
```

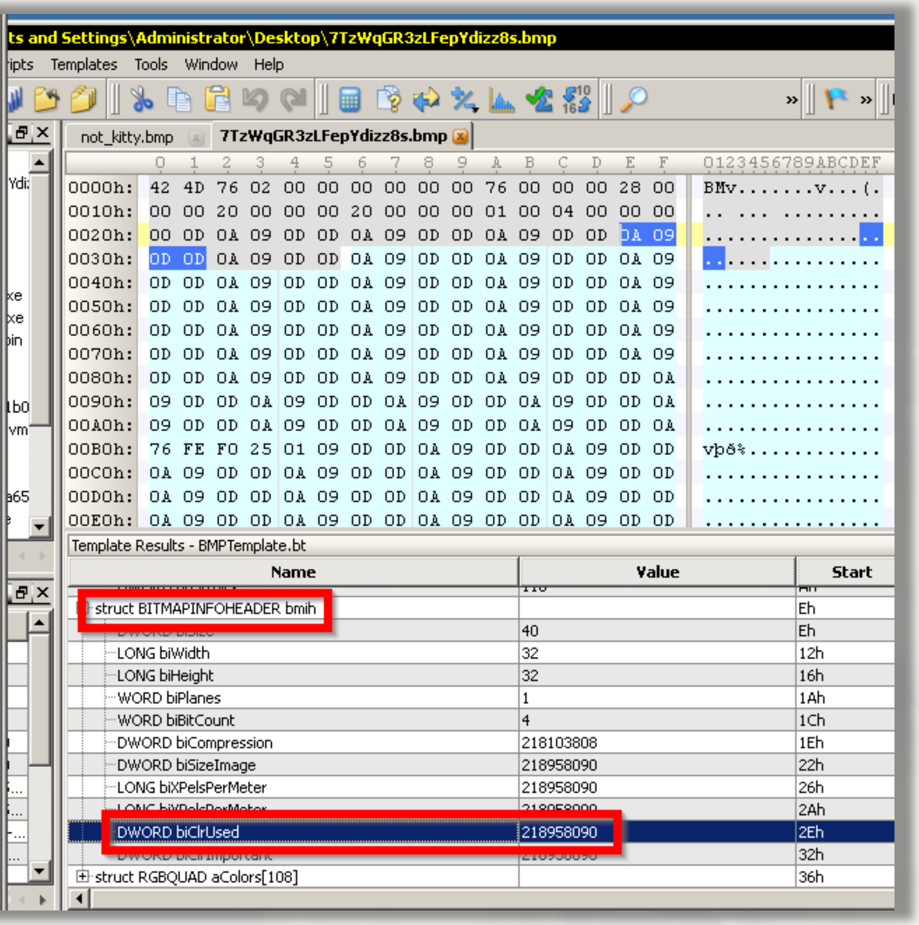
```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 42 4D 76 02 00 00 00 00 00 00 76 00 00 00 28 00   BMv.......v...(.
0010h: 00 00 20 00 00 00 20 00 00 00 01 00 04 00 00 00   .. ... .........
0020h: 00 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09   ................
0030h: 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09   ................
0040h: 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09   ................
0050h: 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09   ................
0060h: 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09   ................
0070h: 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09   ................
0080h: 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0D 0A   ................
0090h: 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A   ................
00A0h: 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A   ................
00B0h: 76 FE F0 25 01 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D   vþð%............
00C0h: 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D   ................
00D0h: 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D   ................
00E0h: 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D   ................
00F0h: 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D   ................
0100h: 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D   ................
0110h: 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0A   ................
0120h: 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A   ................
0130h: 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A   ................
0140h: 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A   ................
0150h: 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A   ................
```

Tried to parse file with 010 editor template...

What Happened



```
string ReadRGBTRIPLE( RGBTRIPLE &a )
{
    string s;
    SPrintf( s, "#%02X%02X%02X", a.rgbRed, a.rgbGreen, a.rgbBlue );
    return s;
}

//-----------------------------------------------

// Define the headers
LittleEndian();
SetBackColor( cLtGray );
BITMAPFILEHEADER bmfh;
BITMAPINFOHEADER bmih;

// Check for header
if( bmfh.bfType != "BM" )
{
    Warning( "File is not a bitmap. Template stopped." );
    return -1;
}

// Define the color table
if( (bmih.biBitCount != 24) && (bmih.biBitCount != 32) )
{
    SetBackColor( cLtAqua );
    if( bmih.biClrUsed > 0 )
        RGBQUAD aColors[ bmih.biClrUsed ];
    else
        RGBQUAD aColors[ 1 << bmih.biBitCount ];
}

// Define
Se
if
{
```



ts and Settings\Administrator\Desktop\7TzWqGR3zLFepYdizz8s.bmp

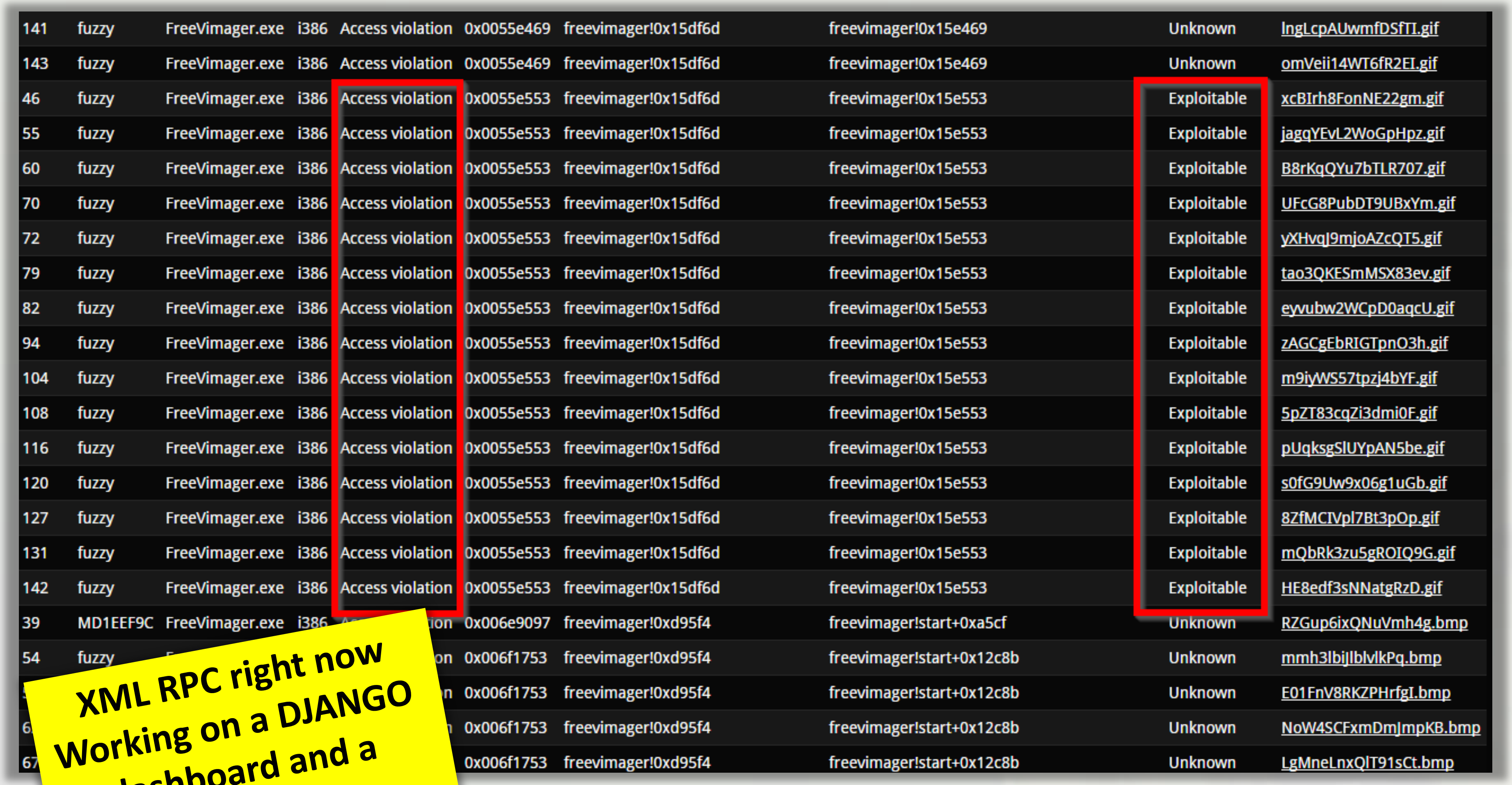
```
       0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 42 4D 76 02 00 00 00 00 00 00 76 00 00 00 28 00  BMv.......v...(.
0010h: 00 00 20 00 00 00 20 00 00 00 01 00 04 00 00 00  .. ... .........
0020h: 00 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09  ................
0030h: 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09  ................
0040h: 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09  ................
0050h: 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09  ................
0060h: 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09  ................
0070h: 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09  ................
0080h: 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0D 0A  ................
0090h: 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A  ................
00A0h: 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A  ................
00B0h: 76 FE F0 25 01 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D  vþð%............
00C0h: 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D  ................
00D0h: 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D  ................
00E0h: 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D 0A 09 0D 0D  ................
```

Template Results - BMPTemplate.bt

Name	Value	Start
struct BITMAPINFOHEADER bmih		Eh
DWORD biSize	40	Eh
LONG biWidth	32	12h
LONG biHeight	32	16h
WORD biPlanes	1	1Ah
WORD biBitCount	4	1Ch
DWORD biCompression	218103808	1Eh
DWORD biSizeImage	218958090	22h
LONG biXPelsPerMeter	218958090	26h
LONG biYPelsPerMeter	218958090	2Ah
DWORD biClrUsed	218958090	2Eh
DWORD biClrImportant	218958090	32h
struct RGBQUAD aColors[108]		36h

Just an out of bounds read… Nothing a *dumb* fuzzer would not find :-(

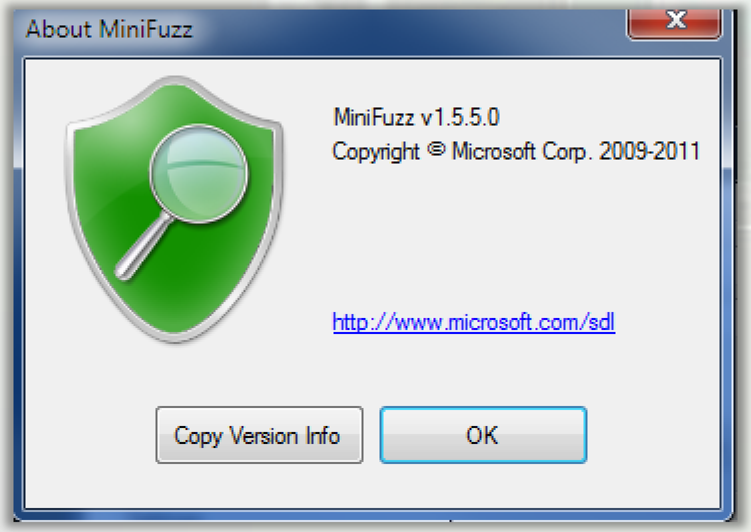
Central point



141	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e469	freevimager!0x15df6d	freevimager!0x15e469	Unknown	lngLcpAUwmfDSfTI.gif
143	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e469	freevimager!0x15df6d	freevimager!0x15e469	Unknown	omVeii14WT6fR2EI.gif
46	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e553	freevimager!0x15df6d	freevimager!0x15e553	Exploitable	xcBIrh8FonNE22gm.gif
55	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e553	freevimager!0x15df6d	freevimager!0x15e553	Exploitable	jagqYEvL2WoGpHpz.gif
60	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e553	freevimager!0x15df6d	freevimager!0x15e553	Exploitable	B8rKqQYu7bTLR707.gif
70	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e553	freevimager!0x15df6d	freevimager!0x15e553	Exploitable	UFcG8PubDT9UBxYm.gif
72	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e553	freevimager!0x15df6d	freevimager!0x15e553	Exploitable	yXHvqJ9mjoAZcQT5.gif
79	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e553	freevimager!0x15df6d	freevimager!0x15e553	Exploitable	tao3QKESmMSX83ev.gif
82	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e553	freevimager!0x15df6d	freevimager!0x15e553	Exploitable	eyvubw2WCpD0aqcU.gif
94	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e553	freevimager!0x15df6d	freevimager!0x15e553	Exploitable	zAGCgEbRIGTpnO3h.gif
104	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e553	freevimager!0x15df6d	freevimager!0x15e553	Exploitable	m9iyWS57tpzj4bYF.gif
108	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e553	freevimager!0x15df6d	freevimager!0x15e553	Exploitable	5pZT83cqZi3dmi0F.gif
116	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e553	freevimager!0x15df6d	freevimager!0x15e553	Exploitable	pUqksgSlUYpAN5be.gif
120	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e553	freevimager!0x15df6d	freevimager!0x15e553	Exploitable	s0fG9Uw9x06g1uGb.gif
127	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e553	freevimager!0x15df6d	freevimager!0x15e553	Exploitable	8ZfMCIVpl7Bt3pOp.gif
131	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e553	freevimager!0x15df6d	freevimager!0x15e553	Exploitable	mQbRk3zu5gROIQ9G.gif
142	fuzzy	FreeVimager.exe	i386	Access violation	0x0055e553	freevimager!0x15df6d	freevimager!0x15e553	Exploitable	HE8edf3sNNatgRzD.gif
39	MD1EEF9C	FreeVimager.exe	i386	Access violation	0x006e9097	freevimager!0xd95f4	freevimager!start+0xa5cf	Unknown	RZGup6ixQNuVmh4g.bmp
54	fuzzy	[illegible]	[illegible]	[illegible]	0x006f1753	freevimager!0xd95f4	freevimager!start+0x12c8b	Unknown	mmh3lbiJlblvlkPq.bmp
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	0x006f1753	freevimager!0xd95f4	freevimager!start+0x12c8b	Unknown	E01FnV8RKZPHrfgI.bmp
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	0x006f1753	freevimager!0xd95f4	freevimager!start+0x12c8b	Unknown	NoW4SCFxmDmJmpKB.bmp
67	[illegible]	[illegible]	[illegible]	[illegible]	0x006f1753	freevimager!0xd95f4	freevimager!start+0x12c8b	Unknown	LgMneLnxQlT91sCt.bmp

XML RPC right now
Working on a DJANGO dashboard and a REST API

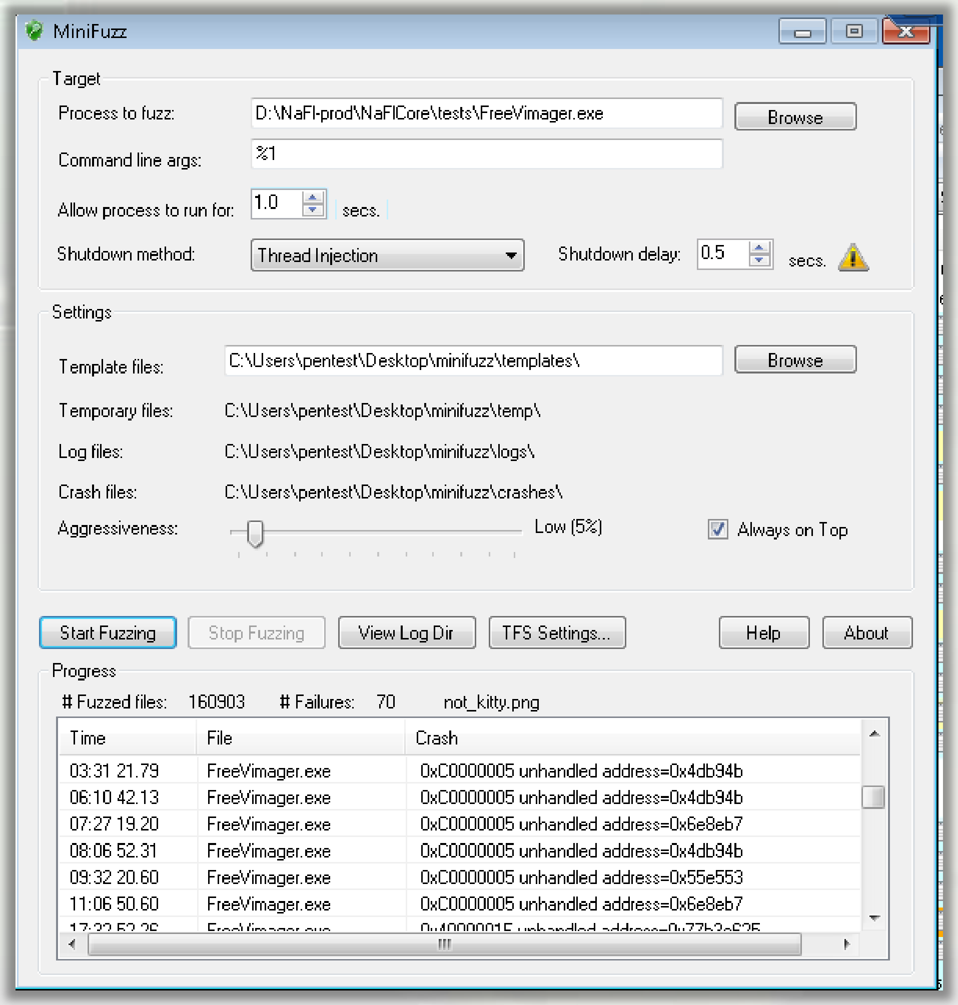
Other small Fuzzers



About MiniFuzz

MiniFuzz v1.5.5.0
Copyright © Microsoft Corp. 2009-2011

http://www.microsoft.com/sdl



MiniFuzz

Target

Process to fuzz: D:\NaFl-prod\NaFlCore\tests\FreeVimager.exe

Command line args: %1

Allow process to run for: 1.0 secs.

Shutdown method: Thread Injection

Shutdown delay: 0.5 secs.

Settings

Template files: C:\Users\pentest\Desktop\minifuzz\templates\

Temporary files: C:\Users\pentest\Desktop\minifuzz\temp\

Log files: C:\Users\pentest\Desktop\minifuzz\logs\

Crash files: C:\Users\pentest\Desktop\minifuzz\crashes\

Aggressiveness: Low (5%)

☑ Always on Top

Progress

Fuzzed files: 160903 # Failures: 70 not_kitty.png

Time	File	Crash
03:31 21.79	FreeVimager.exe	0xC0000005 unhandled address=0x4db94b
06:10 42.13	FreeVimager.exe	0xC0000005 unhandled address=0x4db94b
07:27 19.20	FreeVimager.exe	0xC0000005 unhandled address=0x6e8eb7
08:06 52.31	FreeVimager.exe	0xC0000005 unhandled address=0x4db94b
09:32 20.60	FreeVimager.exe	0xC0000005 unhandled address=0x55e553
11:06 50.60	FreeVimager.exe	0xC0000005 unhandled address=0x6e8eb7

Future enHancements

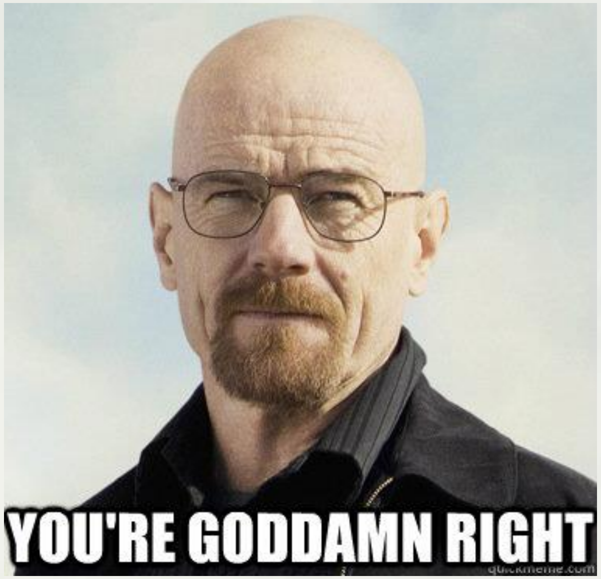
- **SO MANY…**

- Static **analysis** of the **victim** binary itself
  - Cannibalize strings
  - Check proximity to str(n)cmp and alike…
    - Maybe implement in JARVIS?

- **Analysis** of the **samples**
  - Find high entropy regions (uninteresting)
  - Find ASCII regions
  - Compare samples to find fixed tokens (*PNG*, etc.)

- Regularly evaluate the quality of mutations in the queue
  - Remove ones not yielding anything interesting in a long time?
  - Trim mutations?

Future enHancements



In a Nutshell