Lab 15: Patching EXEs with Ollydbg

Course Name: Malware Analysis and Reverse Engineering (IAM302)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 11/3/2023

Purpose

- To practice disassembling and modifying binaries.

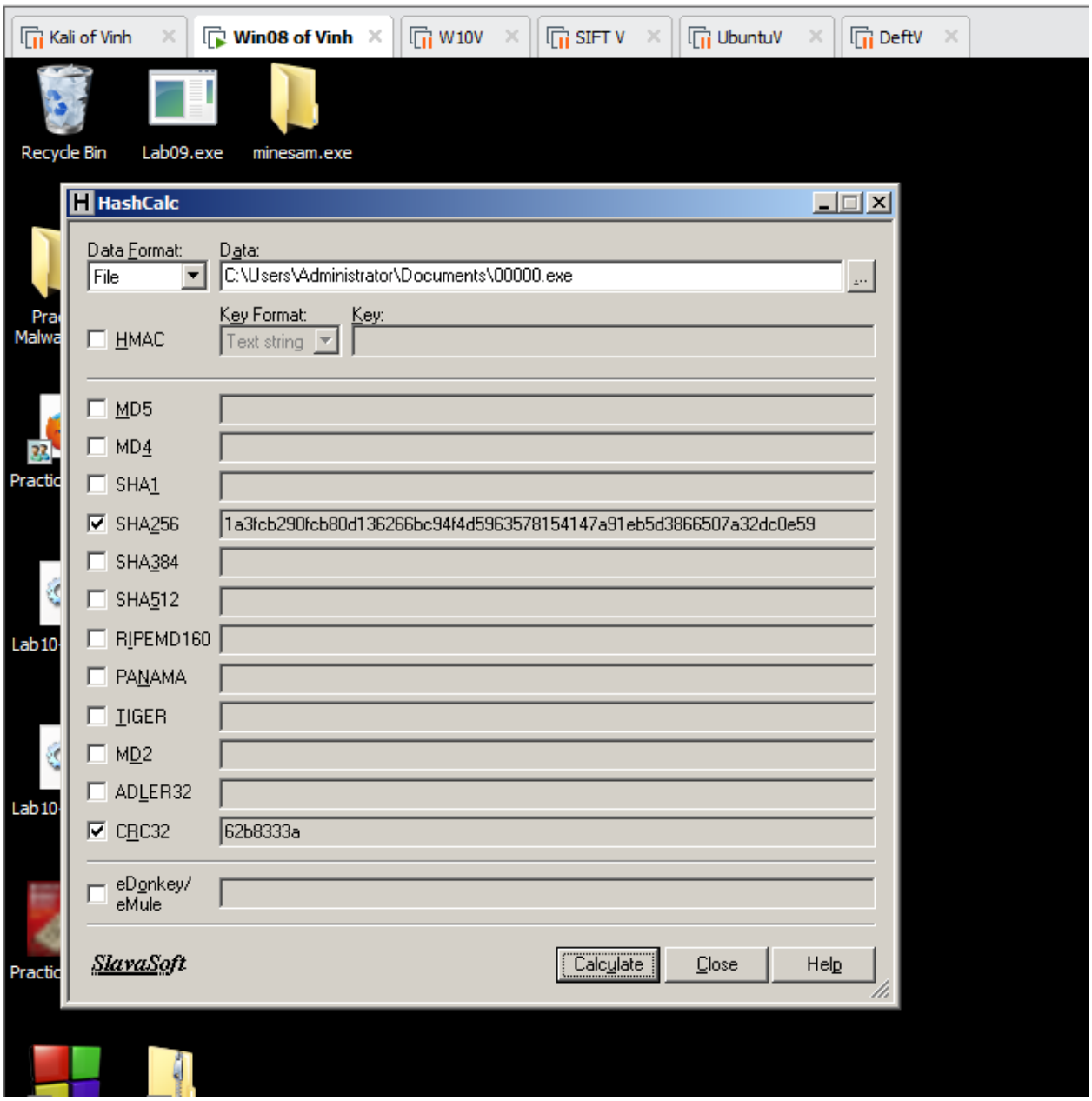
What You Need

- A Windows machine, real or virtual. I used a Windows Server 2008 virtual machine.
- You need several files to examine. They are all in the Documents folder of the VM your instructor handed out. If you don't have that, download them with these links:
  - exe
  - 3EXEs.zip
  - easy.zip
  - 256exes.zip

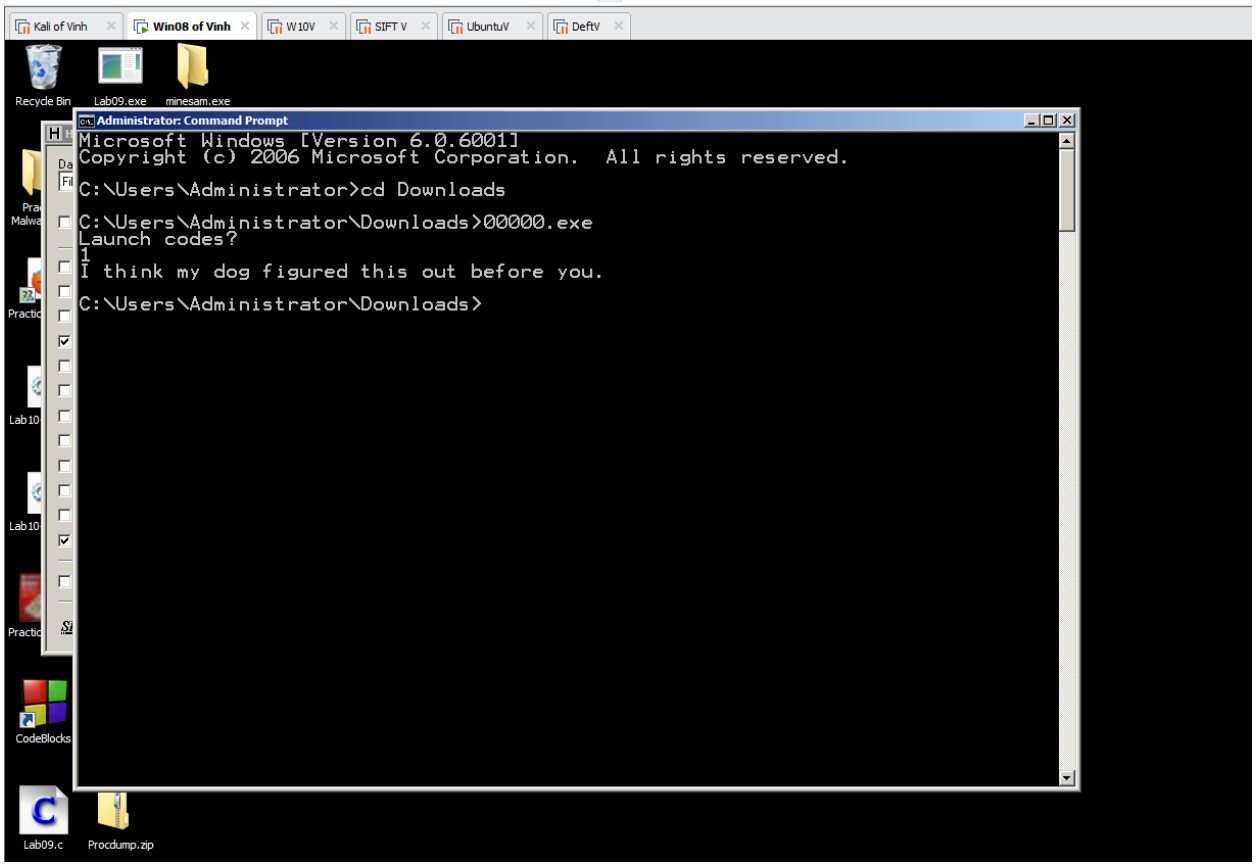
9.1: Patching an EXE (15 pts)

Getting the EXE

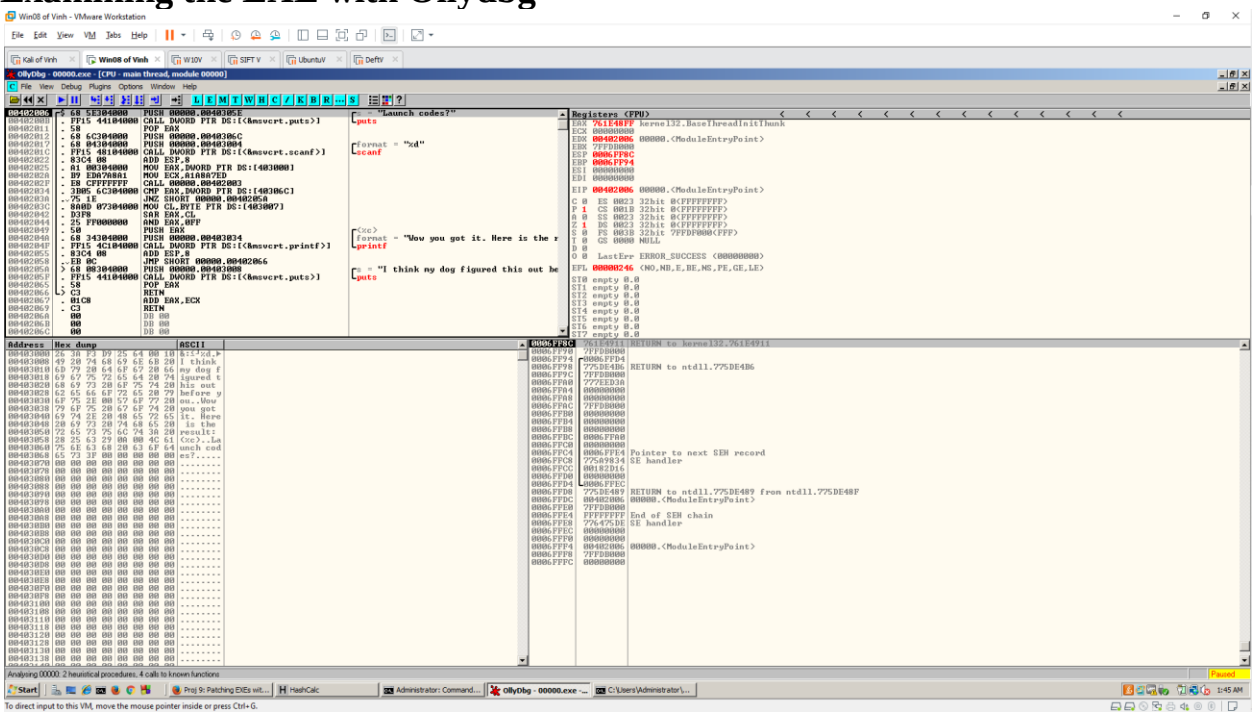
Checking the Hash



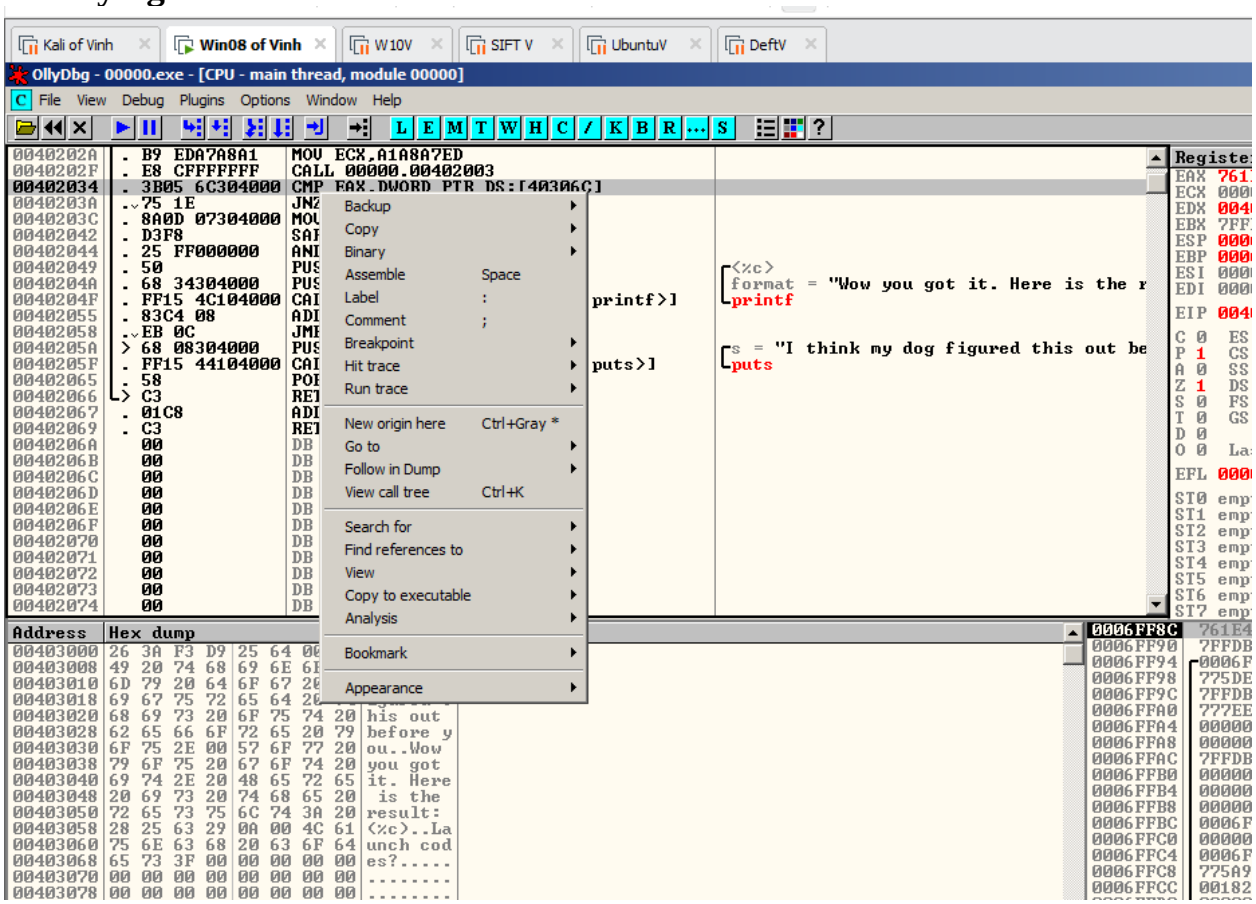
Running the EXE

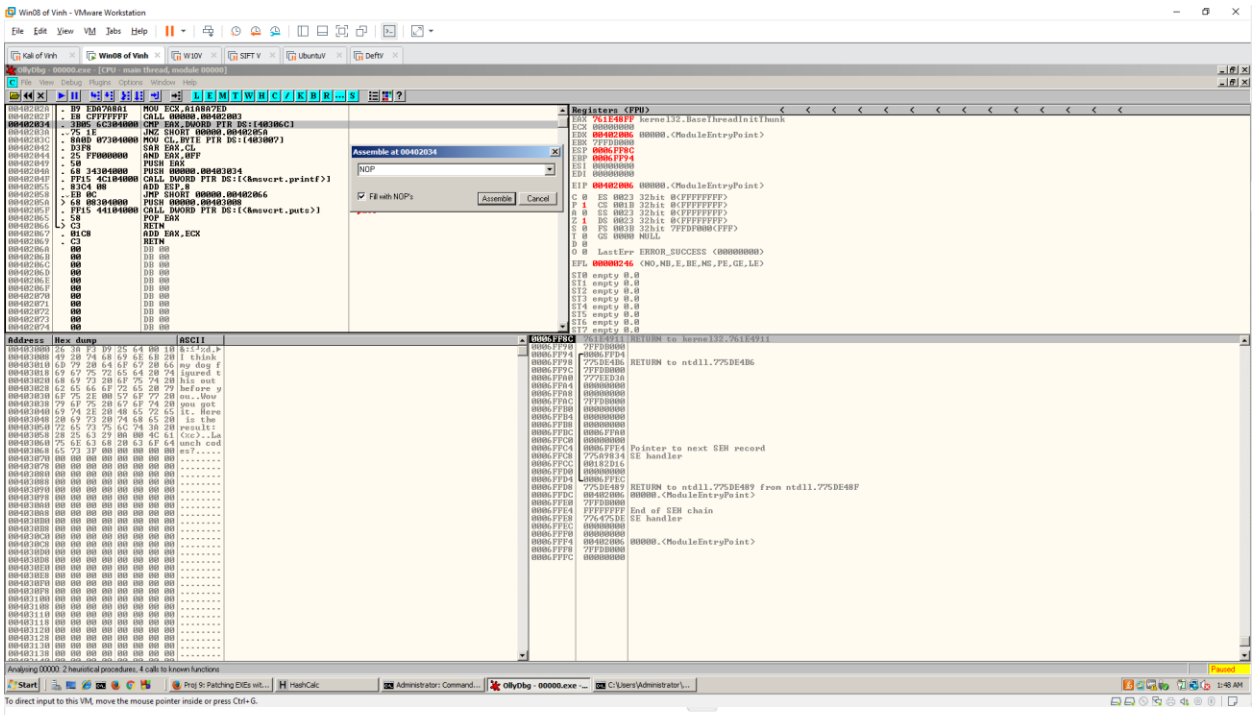


Examining the EXE with Ollydbg



Modifying the EXE





Kali of Vinh | Win08 of Vinh | W10V | SIFT V | UbuntuV | DeftV

OllyDbg - 00000.exe - [CPU - main thread, module 00000]

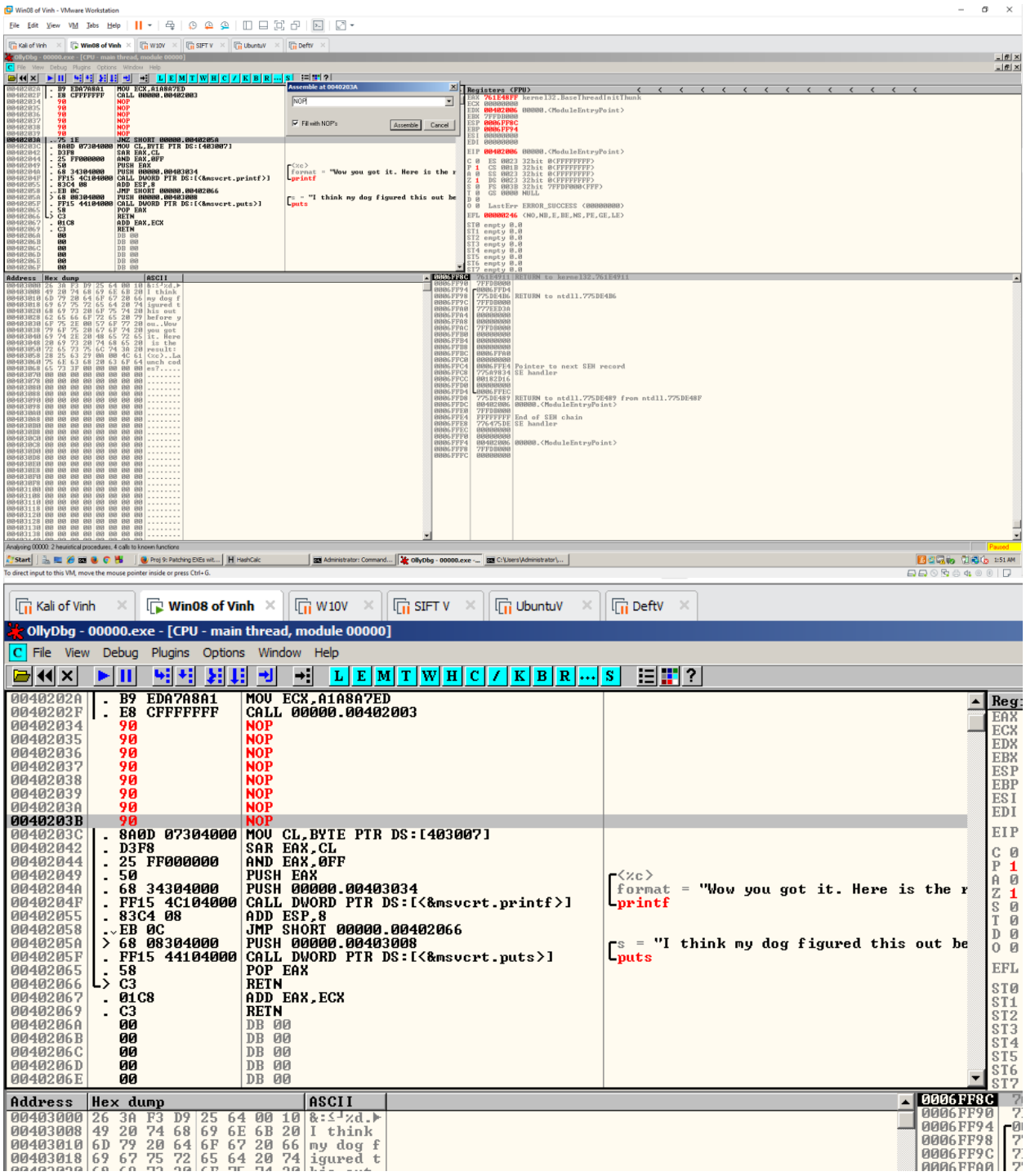
File View Debug Plugins Options Window Help

```
00402020   . B9 EDA7A8A1    MOV ECX,A1A8A7ED
0040202F   . E8 CFFFFFFF    CALL 00000.00402003
00402034     90             NOP
00402035     90             NOP
00402036     90             NOP
00402037     90             NOP
00402038     90             NOP
00402039     90             NOP
0040203A   .v75 1E          JNZ SHORT 00000.0040205A
0040203C   . 8A0D 07304000  MOV CL,BYTE PTR DS:[403007]
00402042   . D3F8            SAR EAX,CL
00402044   . 25 FF000000     AND EAX,0FF
00402049   . 50              PUSH EAX
0040204A   . 68 34304000    PUSH 00000.00403034          <%c>
0040204F   . FF15 4C104000  CALL DWORD PTR DS:[<&msvcrt.printf>]   format = "Wow you got it. Here is the r
00402055   . 83C4 08        ADD ESP,8                    printf
00402058   .vEB 0C          JMP SHORT 00000.00402066
0040205A   > 68 08304000    PUSH 00000.00403008          s = "I think my dog figured this out be
0040205F   . FF15 44104000  CALL DWORD PTR DS:[<&msvcrt.puts>]   puts
00402065   . 58              POP EAX
00402066   L> C3            RETN
00402067   . 01C8            ADD EAX,ECX
00402069   . C3              RETN
0040206A     00             DB 00
0040206B     00             DB 00
0040206C     00             DB 00
0040206D     00             DB 00
0040206E     00             DB 00
0040206F     00             DB 00
```

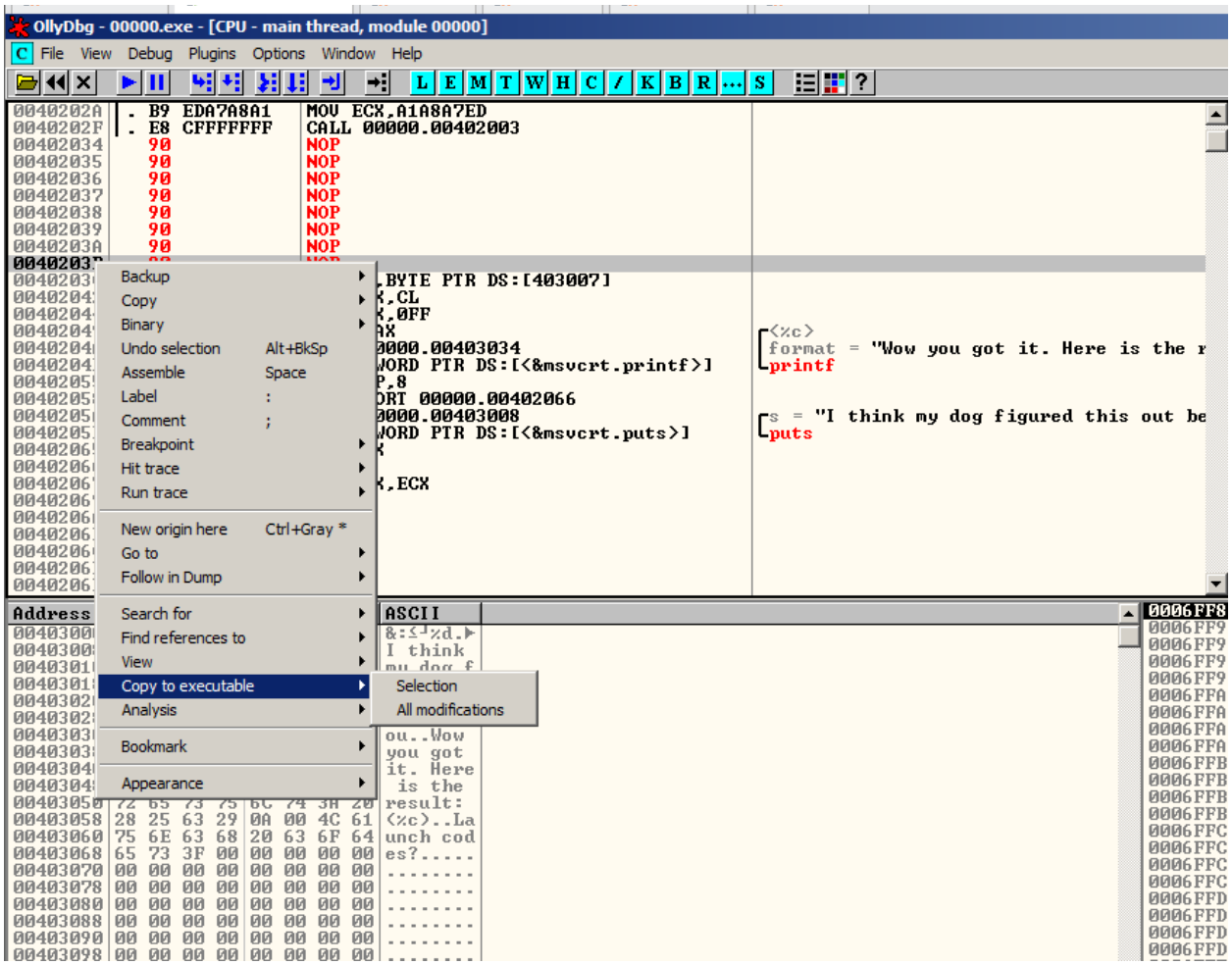
```
Registers (FPU)
EAX 761E48FF kernel32.Ba
ECX 00000000
EDX 00402006 00000.<Modu
EBX 7FFDB000
ESP 0006FF8C
EBP 0006FF94
ESI 00000000
EDI 00000000

EIP 00402006 00000.<Modu

C 0  ES 0023 32bit 0(FFF
P 1  CS 001B 32bit 0(FFF
A 0  SS 0023 32bit 0(FFF
Z 1  DS 0023 32bit 0(FFF
S 0  FS 003B 32bit 7FFD
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCE

EFL 00000246 (NO,NB,E,BE

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
```

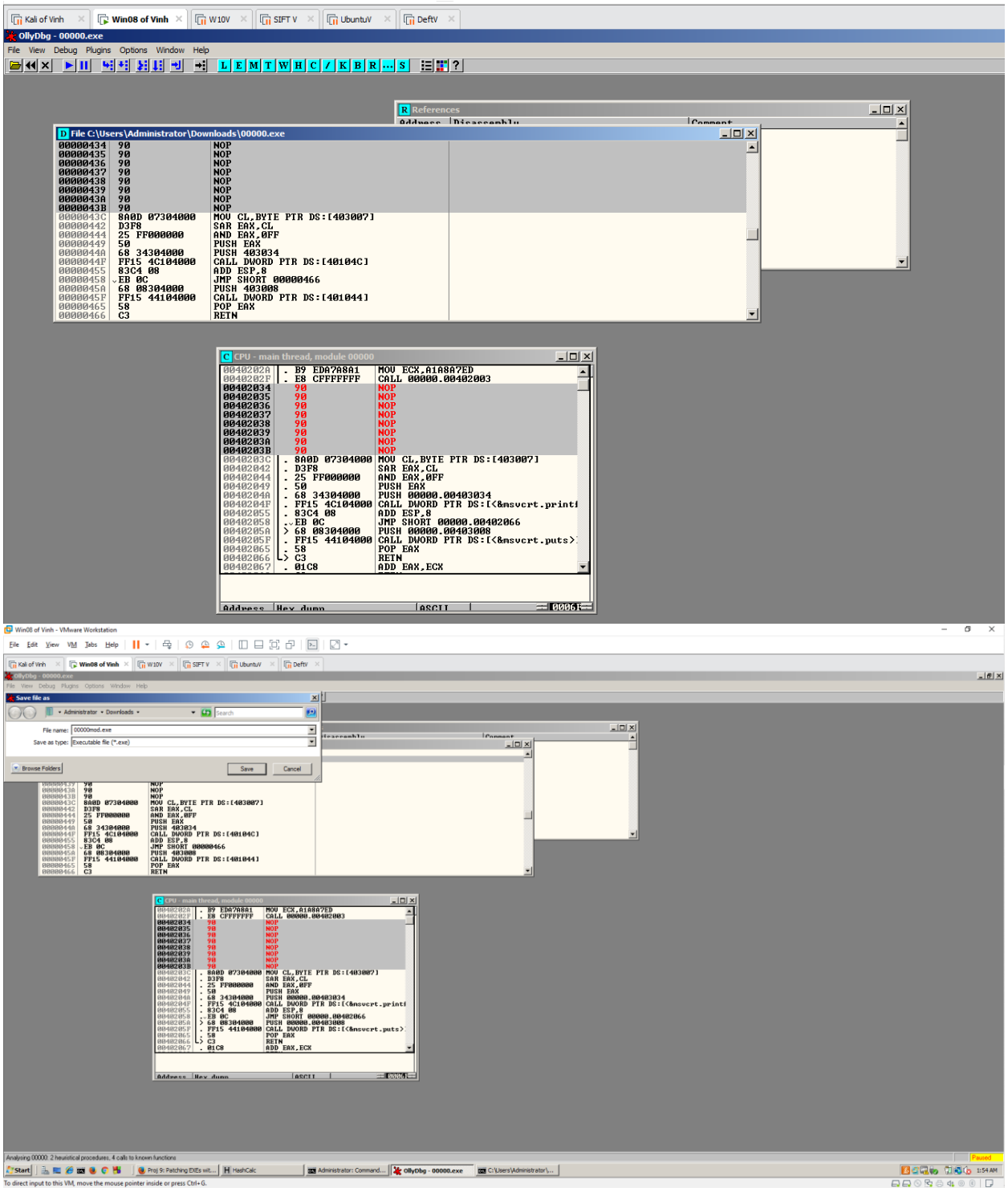
Address	Hex dump	ASCII
00403000	26 3A F3 D9 25 64 00 10	&:ó┘%d.►
00403008	49 20 74 68 69 6E 6B 20	I think
00403010	6D 79 20 64 6F 67 20 66	my dog f
00403018	69 67 75 72 65 64 20 74	igured t
00403020	68 69 73 20 6F 75 74 20	his out
00403028	62 65 66 6F 72 65 20 79	before y
00403030	6F 75 2E 00 57 6F 77 20	ou..Wow
00403038	79 6F 75 20 67 6F 74 20	you got
00403040	69 74 2E 20 48 65 72 65	it. Here
00403048	20 69 73 20 74 68 65 20	is the
00403050	72 65 73 75 6C 74 3A 20	result:
00403058	28 25 63 29 0A 00 4C 61	(%c)..La
00403060	75 6E 63 68 20 63 6F 64	unch cod
00403068	65 73 3F 00 00 00 00 00	es?.....
00403070	00 00 00 00 00 00 00 00	....
00403078	00 00 00 00 00 00 00 00	....
00403080	00 00 00 00 00 00 00 00	....
00403088	00 00 00 00 00 00 00 00	....
00403090	00 00 00 00 00 00 00 00	....
00403098	00 00 00 00 00 00 00 00	....
004030A0	00 00 00 00 00 00 00 00	....
004030A8	00 00 00 00 00 00 00 00	....
004030B0	00 00 00 00 00 00 00 00	....
004030B8	00 00 00 00 00 00 00 00	....
004030C0	00 00 00 00 00 00 00 00	....
004030C8	00 00 00 00 00 00 00 00	....
004030D0	00 00 00 00 00 00 00 00	....
004030D8	00 00 00 00 00 00 00 00	....
004030E0	00 00 00 00 00 00 00 00	....
004030E8	00 00 00 00 00 00 00 00	....
004030F0	00 00 00 00 00 00 00 00	....
004030F8	00 00 00 00 00 00 00 00	....

```
0006FF8C  761E4911  RETURN to ke
0006FF90  7FFDB000
0006FF94  0006FFD4
0006FF98  775DE4B6  RETURN to nt
0006FF9C  7FFDB000
0006FFA0  777EED3A
0006FFA4  00000000
0006FFA8  00000000
0006FFAC  7FFDB000
0006FFB0  00000000
0006FFB4  00000000
0006FFB8  00000000
0006FFBC  0006FFA0
0006FFC0  00000000
0006FFC4  0006FFE4  Pointer to n
0006FFC8  775A9834  SE handler
0006FFCC  00182D16
0006FFD0  00000000
0006FFD4  0006FFEC
0006FFD8  775DE489  RETURN to nt
0006FFDC  00402006  00000.<Modul
0006FFE0  7FFDB000
0006FFE4  FFFFFFFF  End of SEH c
0006FFE8  776475DE  SE handler
0006FFEC  00000000
0006FFF0  00000000
0006FFF4  00402006  00000.<Modul
0006FFF8  7FFDB000
0006FFFC  00000000
```

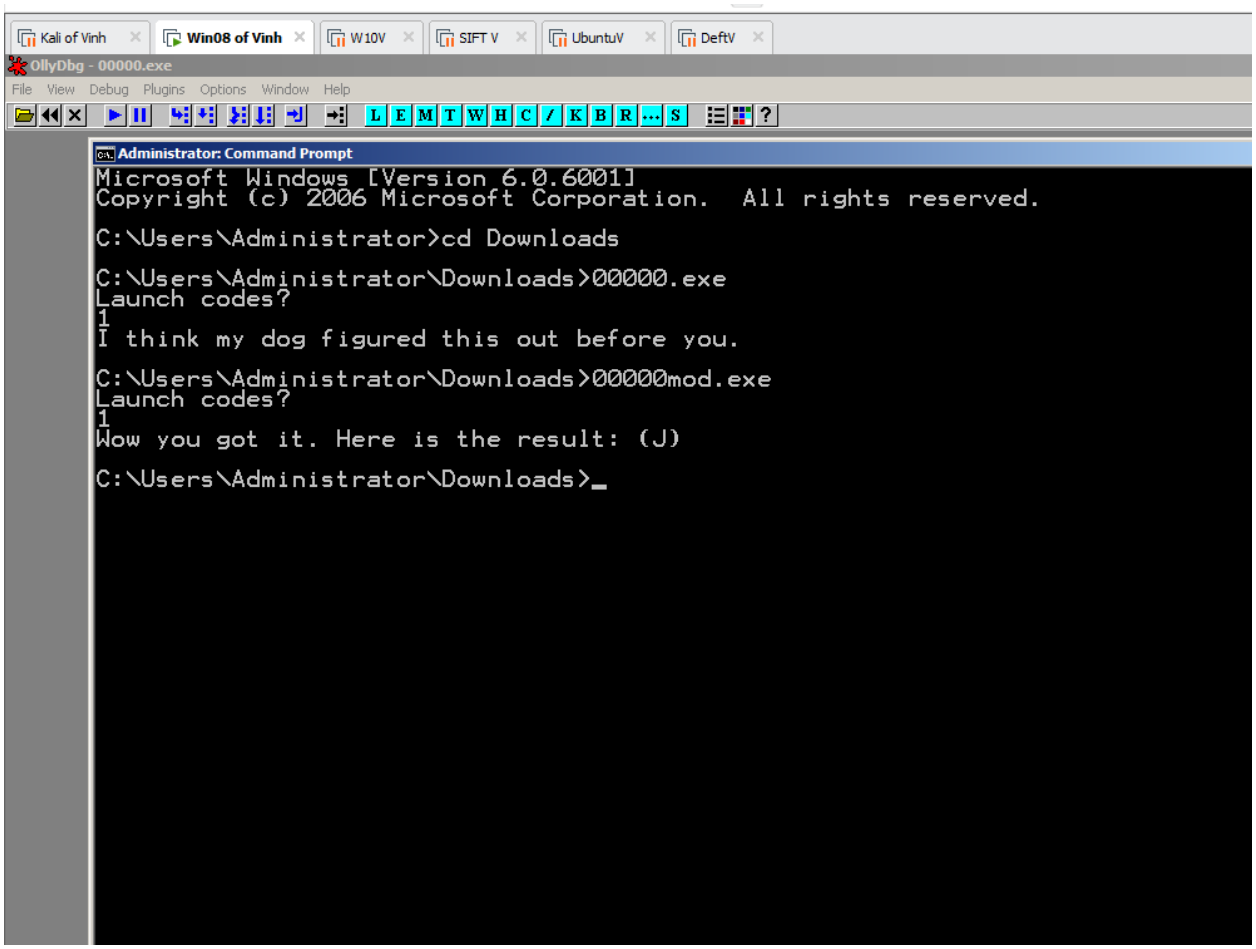


Saving the Modified File

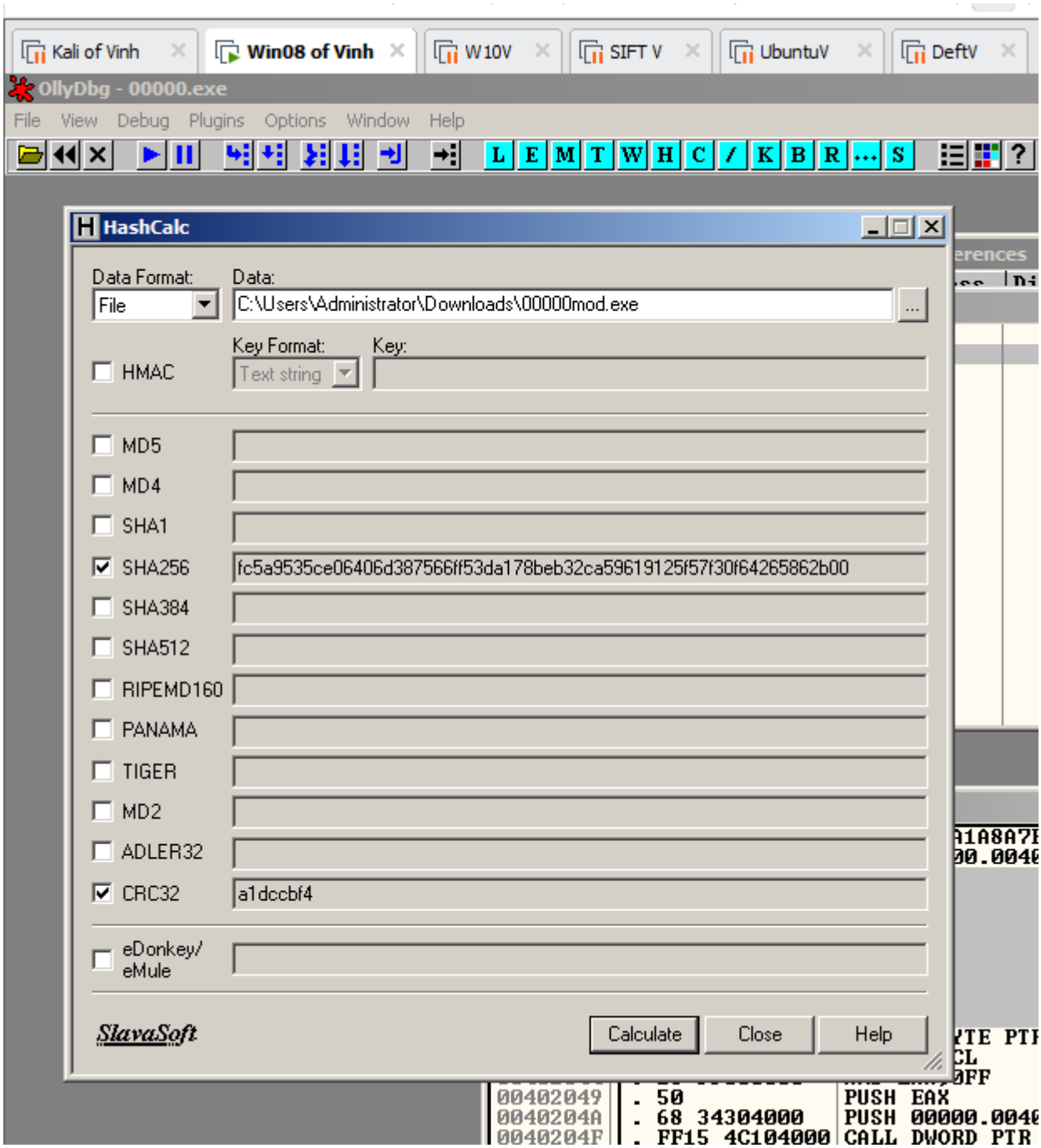

OllyDbg - 00000.exe - [CPU - main thread, module 00000]
File View Debug Plugins Options Window Help
0040202A . B9 EDA7A8A1 MOV ECX,A1A8A7ED
0040202F . E8 CFFFFFFF CALL 00000.00402003
00402034 90 NOP
00402035 90 NOP
00402036 90 NOP
00402037 90 NOP
00402038 90 NOP
00402039 90 NOP
0040203A 90 NOP
Backup
Copy
Binary
Undo selection Alt+BkSp
Assemble Space
Label :
Comment ;
Breakpoint
Hit trace
Run trace
New origin here Ctrl+Gray *
Go to
Follow in Dump
Search for
Find references to
View
Copy to executable
Analysis
Bookmark
Appearance
Selection
All modifications
Address
ASCII
I think
ou..Wow
you got
it. Here
is the
result:
(%c)..La
unch cod
es?.....



Running the Modified File



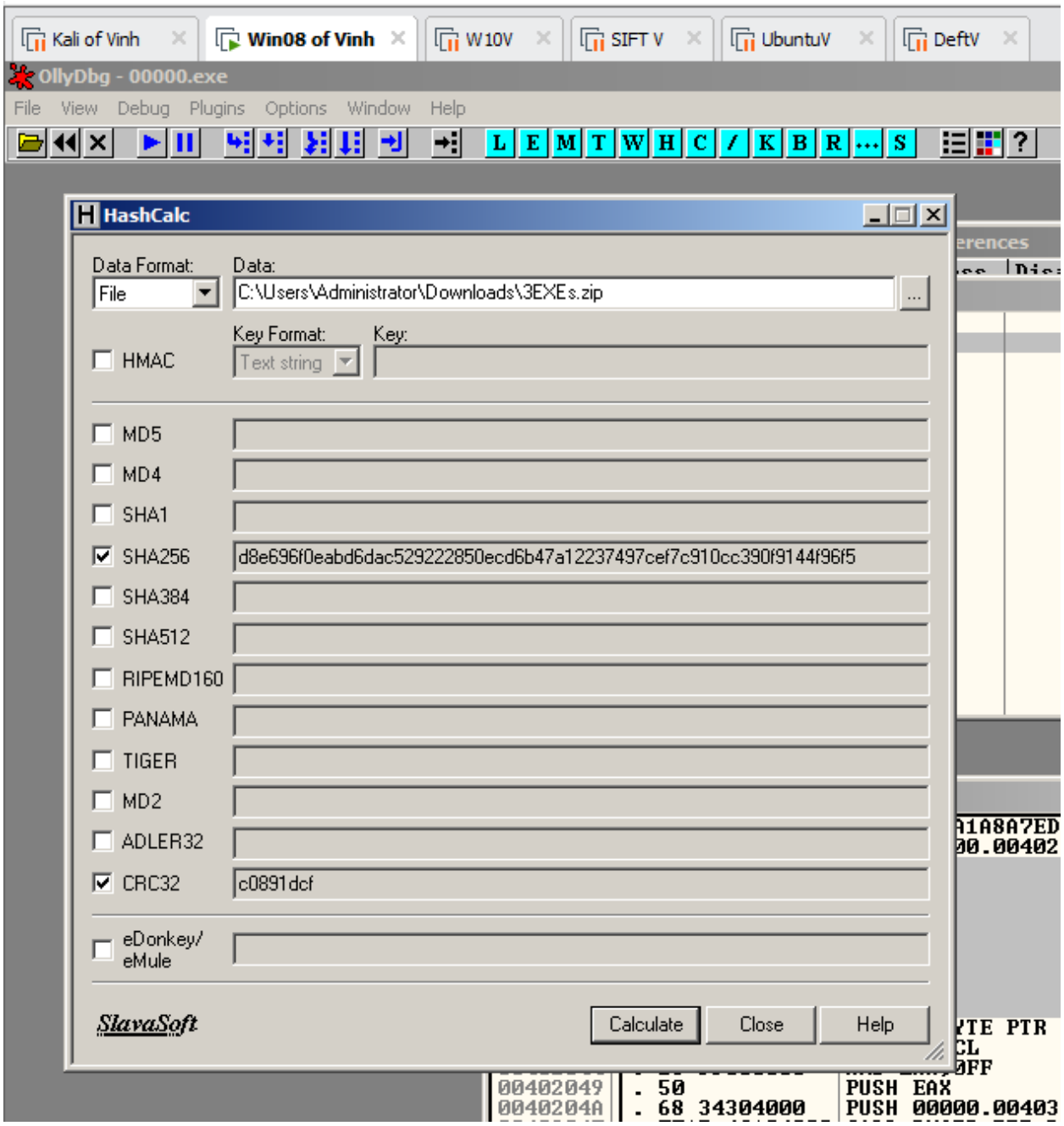
Checking the Hash



9.2: Patching Three EXEs

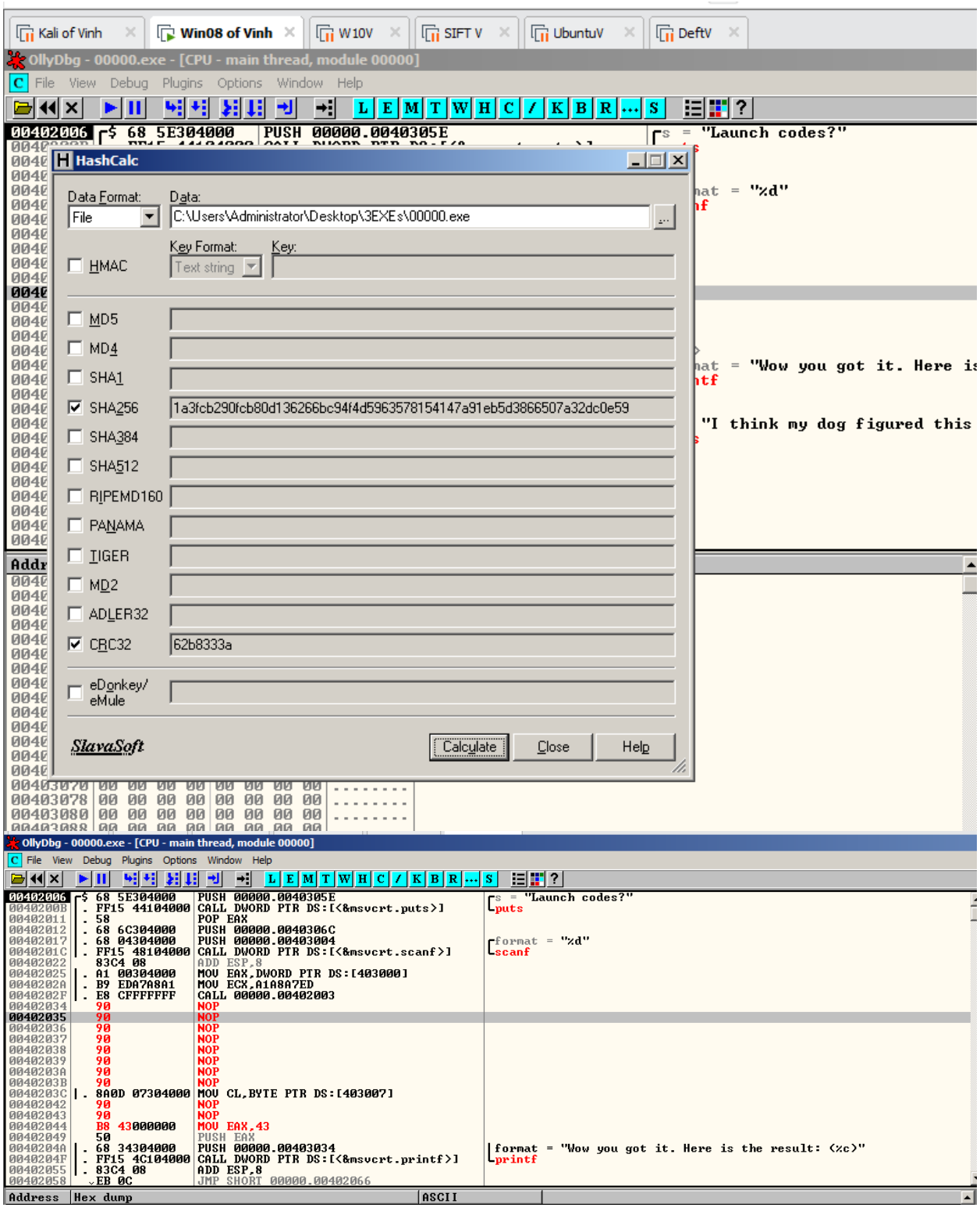
Getting the EXEs

Checking the Hash

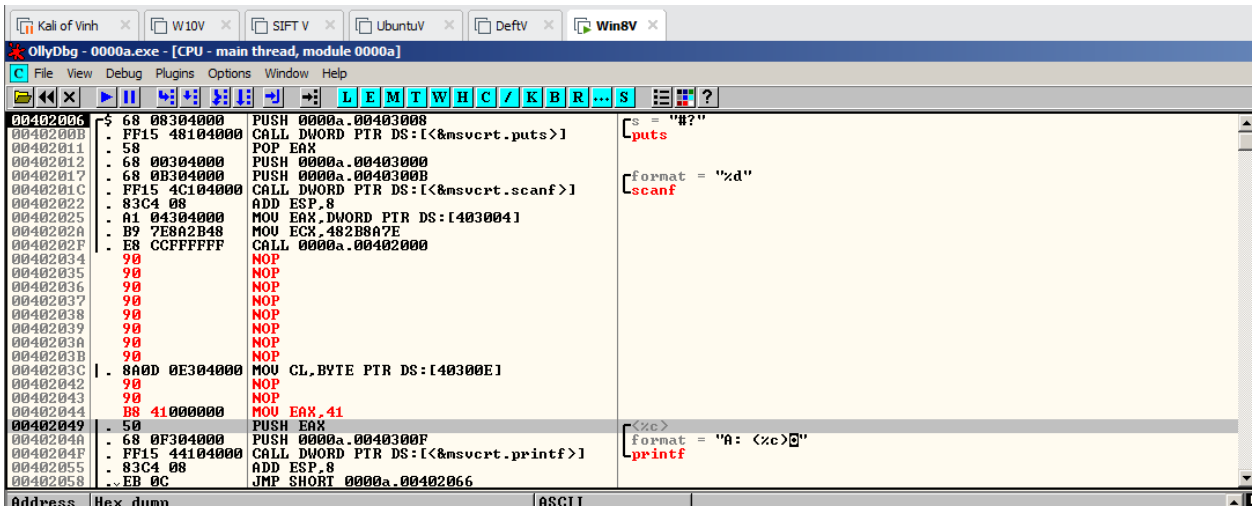


Patch the Files

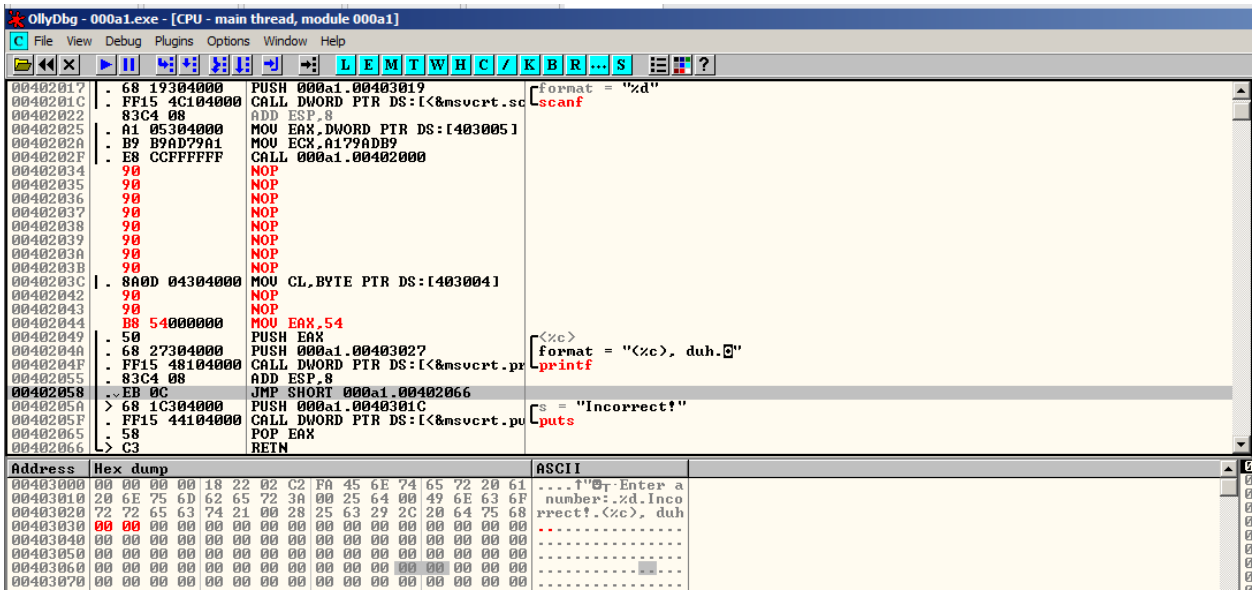
00000.exe


Kali of Vinh
Win08 of Vinh
W10V
SIFT V
UbuntuV
DeftV
OllyDbg - 00000.exe - [CPU - main thread, module 00000]
File View Debug Plugins Options Window Help
HashCalc
Data Format:
File
Data:
C:\Users\Administrator\Desktop\3EXEs\00000.exe
Key Format:
Text string
Key:
HMAC
MD5
MD4
SHA1
SHA256
1a3fcb290fcb80d136266bc94f4d5963578154147a91eb5d3866507a32dc0e59
SHA384
SHA512
RIPEMD160
PANAMA
TIGER
MD2
ADLER32
CRC32
62b8333a
eDonkey/ eMule
SlavaSoft
Calculate
Close
Help
00402006 $ 68 5E304000 PUSH 00000.0040305E
s = "Launch codes?"
nat = "%d"
nf
nat = "Wow you got it. Here is
ntf
"I think my dog figured this
Addr
00403070 00 00 00 00 00 00 00 00
00403078 00 00 00 00 00 00 00 00
00403080 00 00 00 00 00 00 00 00
OllyDbg - 00000.exe - [CPU - main thread, module 00000]
File View Debug Plugins Options Window Help
00402006 $ 68 5E304000 PUSH 00000.0040305E
0040200B . FF15 44104000 CALL DWORD PTR DS:[<&msvcrt.puts>]
00402011 . 58 POP EAX
00402012 . 68 6C304000 PUSH 00000.0040306C
00402017 . 68 04304000 PUSH 00000.00403004
0040201C . FF15 48104000 CALL DWORD PTR DS:[<&msvcrt.scanf>]
00402022 83C4 08 ADD ESP,8
00402025 . A1 00304000 MOV EAX,DWORD PTR DS:[403000]
0040202A . B9 EDA7A8A1 MOV ECX,A1A8A7ED
0040202F . E8 CFFFFFFF CALL 00000.00402003
00402034 90 NOP
00402035 90 NOP
00402036 90 NOP
00402037 90 NOP
00402038 90 NOP
00402039 90 NOP
0040203A 90 NOP
0040203B 90 NOP
0040203C . 8A0D 07304000 MOV CL,BYTE PTR DS:[403007]
00402042 90 NOP
00402043 90 NOP
00402044 B8 43000000 MOV EAX,43
00402049 50 PUSH EAX
0040204A . 68 34304000 PUSH 00000.00403034
0040204F . FF15 4C104000 CALL DWORD PTR DS:[<&msvcrt.printf>]
00402055 . 83C4 08 ADD ESP,8
00402058 EB 0C JMP SHORT 00000.00402066
s = "Launch codes?"
puts
format = "%d"
scanf
format = "Wow you got it. Here is the result: (%c)"
printf
Address Hex dump ASCII

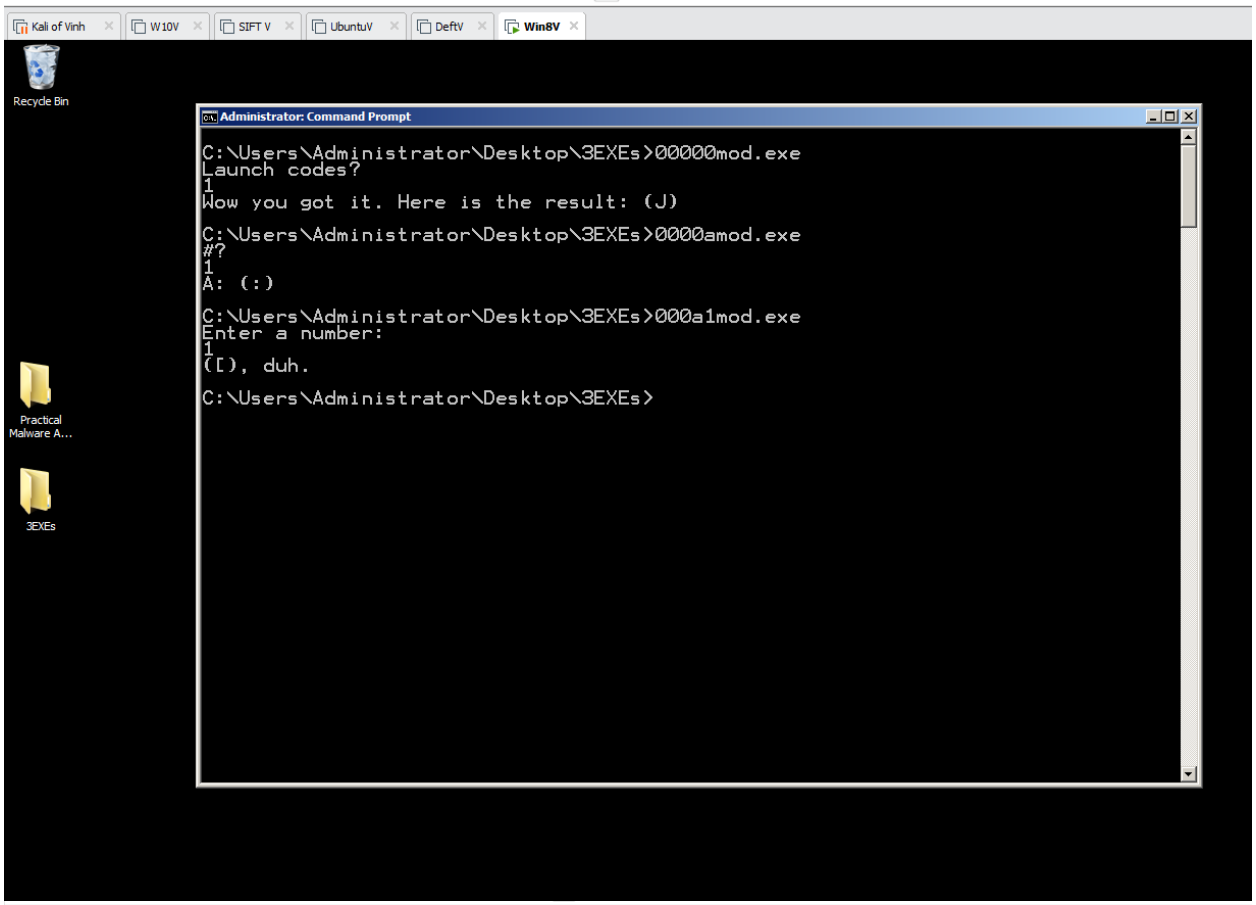
0000a.exe

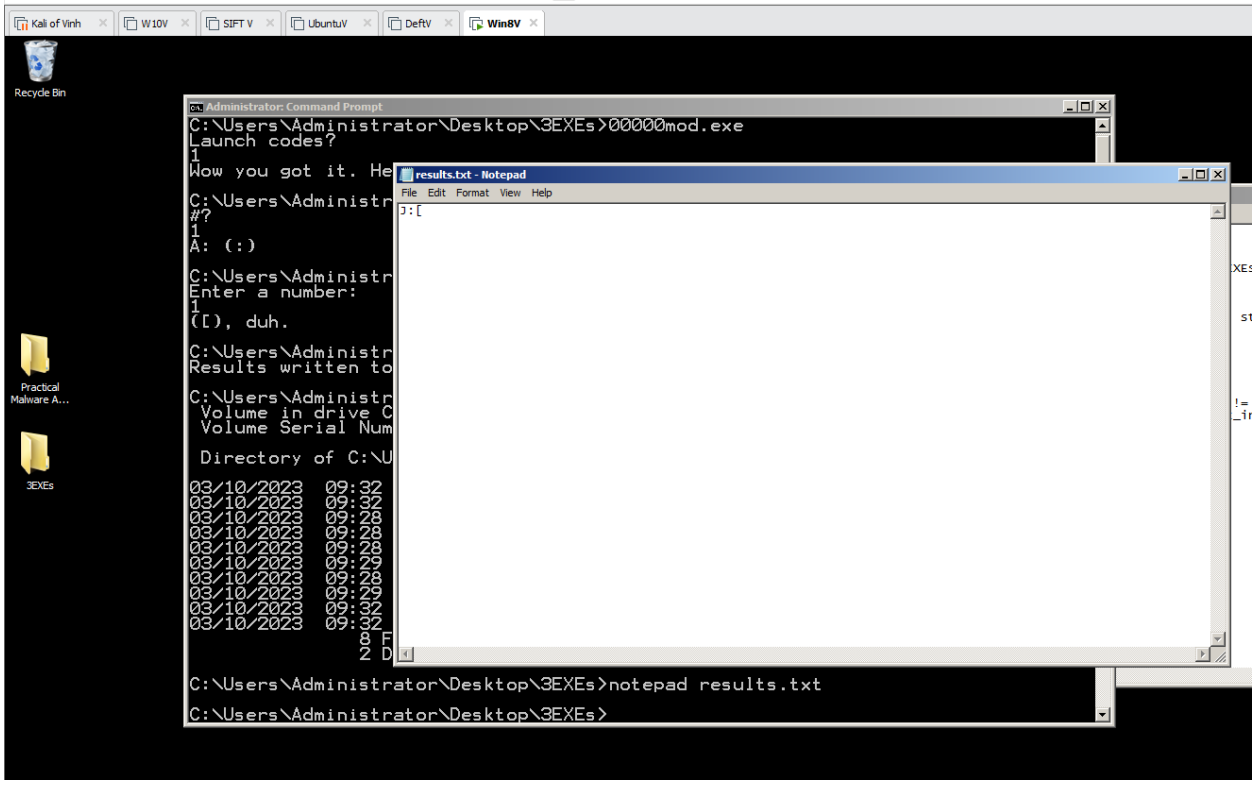


000a1.exe

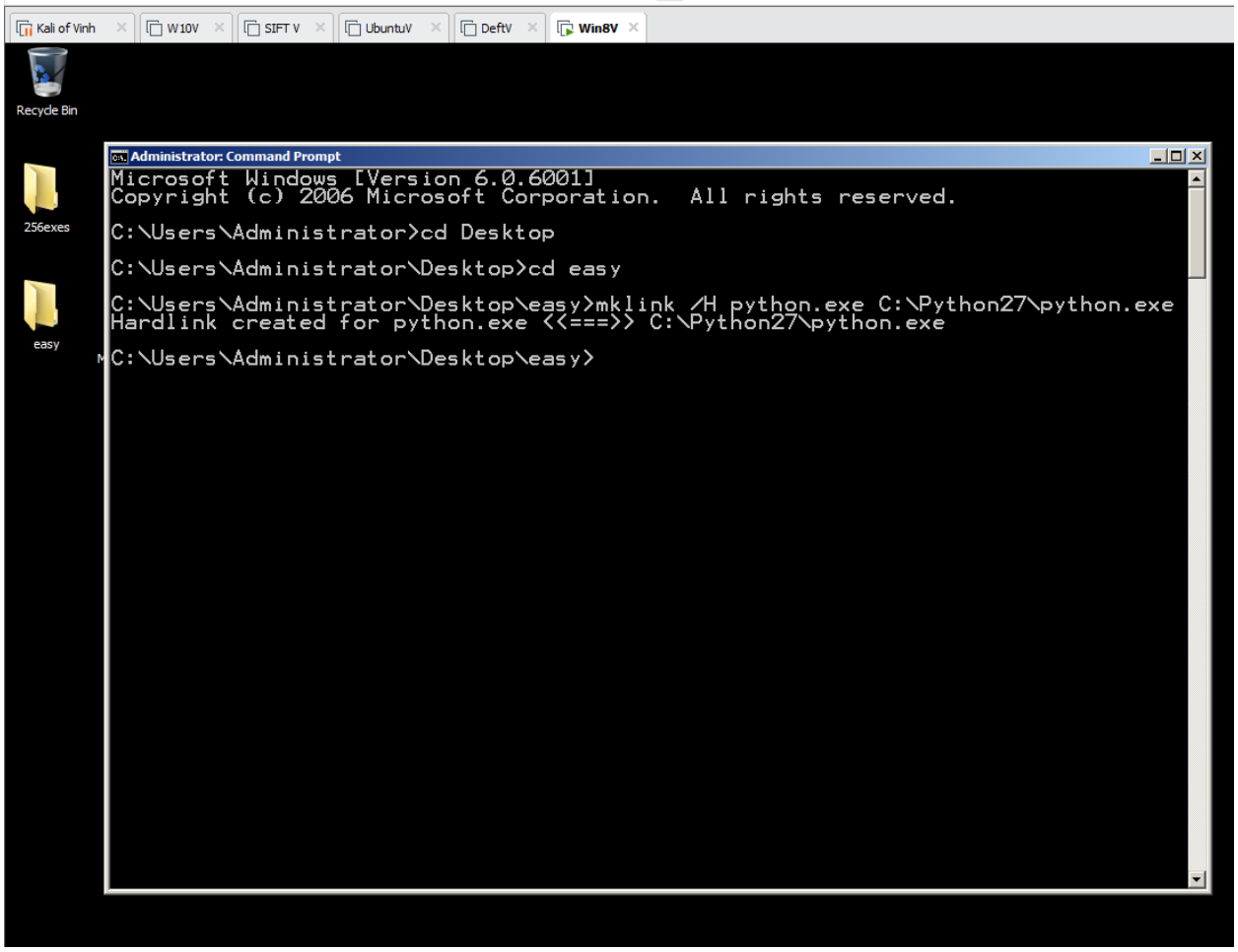


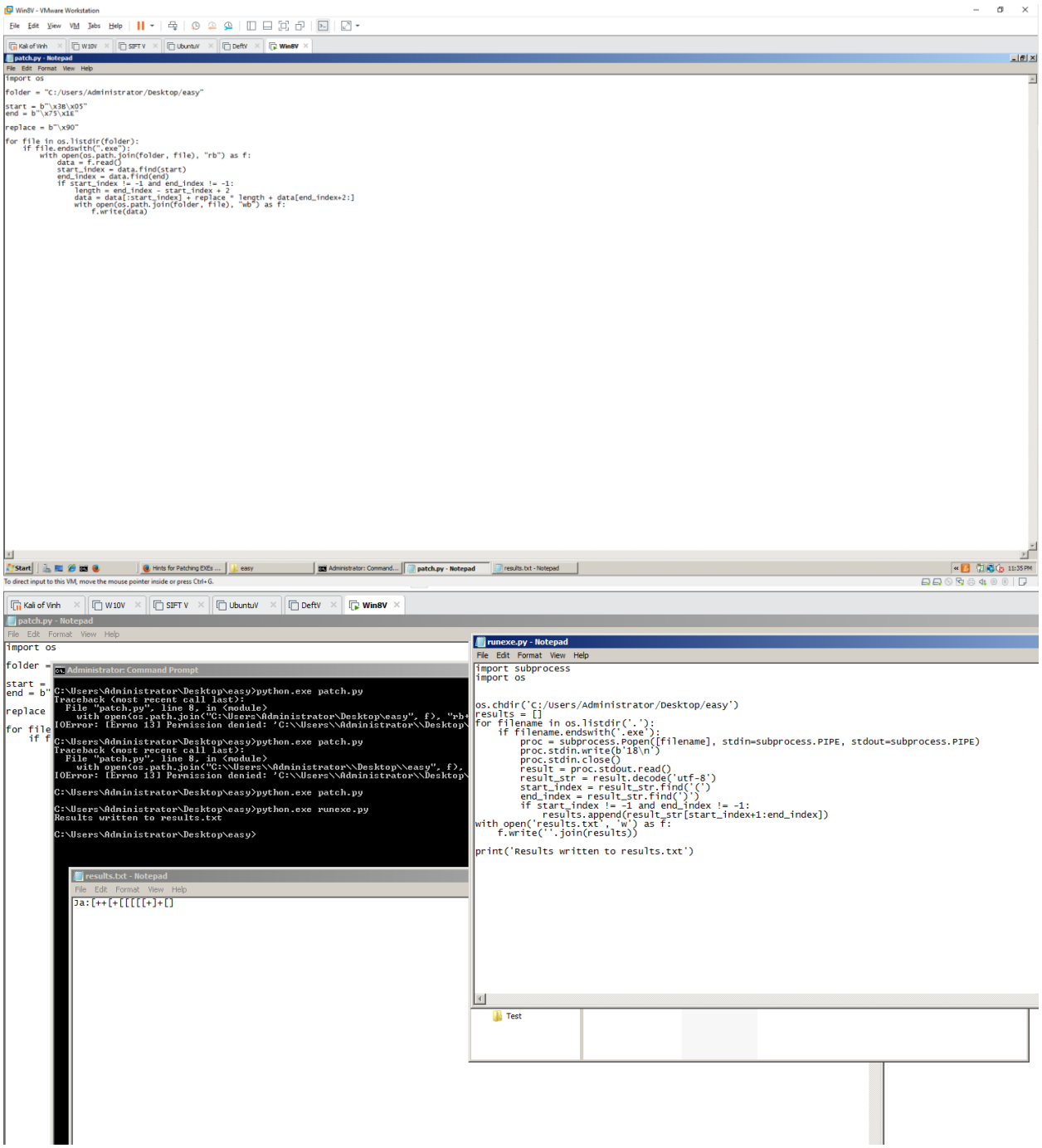
Run file


Kali of Vinh
W10V
SIFT V
UbuntuV
DeftV
Win8V
Recycle Bin
Practical Malware A...
3EXEs
Administrator: Command Prompt
C:\Users\Administrator\Desktop\3EXEs>00000mod.exe
Launch codes?
1
Wow you got it. Here is the result: (J)
C:\Users\Administrator\Desktop\3EXEs>0000amod.exe
#?
1
A: (:)
C:\Users\Administrator\Desktop\3EXEs>000a1mod.exe
Enter a number:
1
([), duh.
C:\Users\Administrator\Desktop\3EXEs>

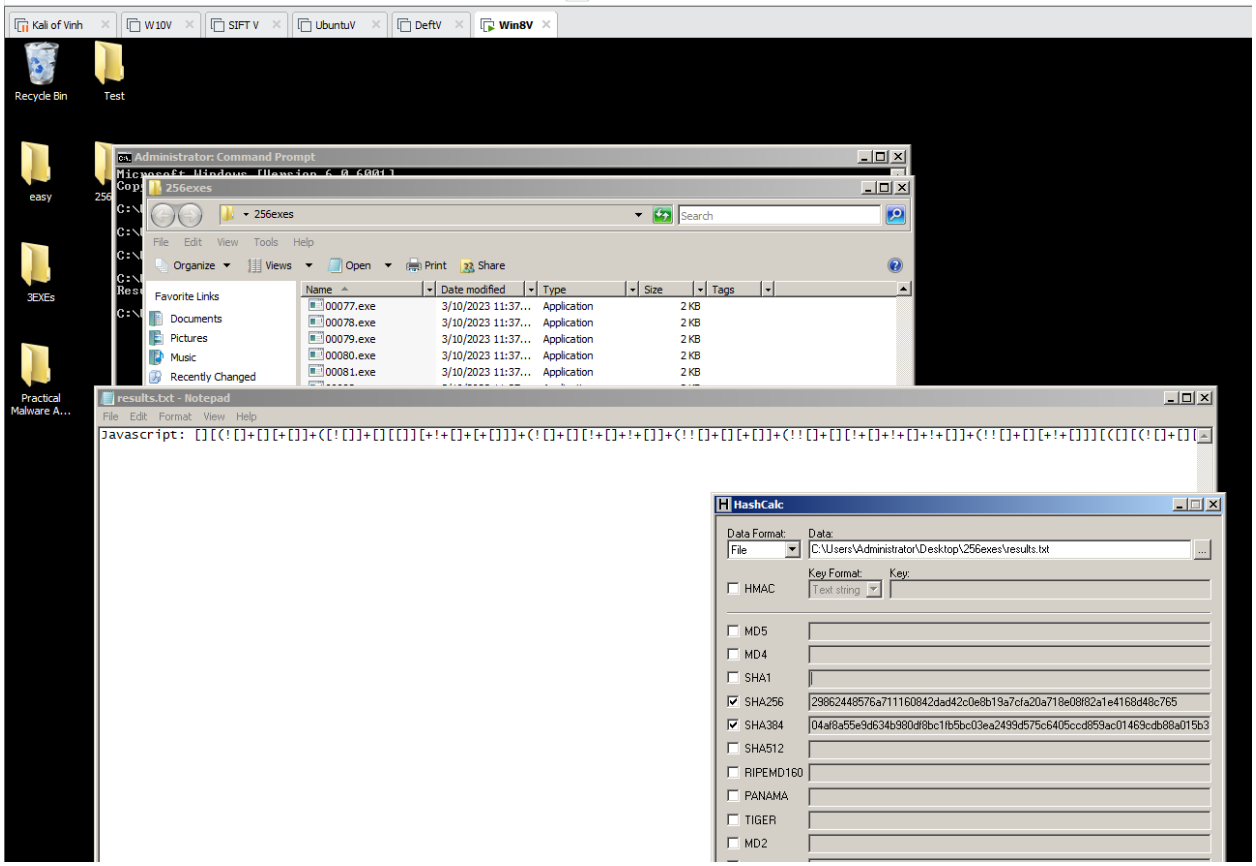

Kali of Vinh
W10V
SIFT V
UbuntuV
DeftV
Win8V
Recycle Bin
Practical Malware A...
3EXEs
Administrator: Command Prompt
C:\Users\Administrator\Desktop\3EXEs>00000mod.exe
Launch codes?
1
Wow you got it. He
C:\Users\Administr
#?
1
A: (:)
C:\Users\Administr
Enter a number:
1
([), duh.
C:\Users\Administr
Results written to
C:\Users\Administr
Volume in drive C
Volume Serial Num
Directory of C:\U
03/10/2023 09:32
03/10/2023 09:32
03/10/2023 09:28
03/10/2023 09:28
03/10/2023 09:28
03/10/2023 09:29
03/10/2023 09:28
03/10/2023 09:29
03/10/2023 09:32
03/10/2023 09:32
8 F
2 D
C:\Users\Administrator\Desktop\3EXEs>notepad results.txt
C:\Users\Administrator\Desktop\3EXEs>
results.txt - Notepad
File Edit Format View Help
J:[

9.3: Patching 19 EXEs
Making Python Run on Windows




patch.py - Notepad
import os
folder = "C:/Users/Administrator/Desktop/easy"
start = b"\x38\x05"
end = b"\x75\x1E"
replace = b"\x90"
for file in os.listdir(folder):
if file.endswith(".exe"):
with open(os.path.join(folder, file), "rb") as f:
data = f.read()
start_index = data.find(start)
end_index = data.find(end)
if start_index != -1 and end_index != -1:
length = end_index - start_index + 2
data = data[:start_index] + replace * length + data[end_index+2:]
with open(os.path.join(folder, file), "wb") as f:
f.write(data)
Administrator: Command Prompt
C:\Users\Administrator\Desktop\easy>python.exe patch.py
Traceback (most recent call last):
File "patch.py", line 8, in <module>
with open(os.path.join("C:\\Users\\Administrator\\Desktop\\easy", f),
IOError: [Errno 13] Permission denied: 'C:\\Users\\Administrator\\Desktop\
C:\Users\Administrator\Desktop\easy>python.exe patch.py
Traceback (most recent call last):
File "patch.py", line 8, in <module>
with open(os.path.join("C:\\Users\\Administrator\\Desktop\\easy", f),
IOError: [Errno 13] Permission denied: 'C:\\Users\\Administrator\\Desktop\
C:\Users\Administrator\Desktop\easy>python.exe patch.py
C:\Users\Administrator\Desktop\easy>python.exe runexe.py
Results written to results.txt
C:\Users\Administrator\Desktop\easy>
results.txt - Notepad
Ja:[++[+[[[[[+]+[]
runexe.py - Notepad
import subprocess
import os
os.chdir('C:/Users/Administrator/Desktop/easy')
results = []
for filename in os.listdir('.'):
if filename.endswith('.exe'):
proc = subprocess.Popen([filename], stdin=subprocess.PIPE, stdout=subprocess.PIPE)
proc.stdin.write(b'18\n')
proc.stdin.close()
result = proc.stdout.read()
result_str = result.decode('utf-8')
start_index = result_str.find('(')
end_index = result_str.find(')')
if start_index != -1 and end_index != -1:
results.append(result_str[start_index+1:end_index])
with open('results.txt', 'w') as f:
f.write(''.join(results))
print('Results written to results.txt')
Test

256exes


Kali of Vinh
W 10V
SIFT V
UbuntuV
DeftV
Win8V
Recycle Bin
Test
easy
3EXEs
Practical Malware A...
Administrator: Command Prompt
256exes
Search
File Edit View Tools Help
Organize Views Open Print Share
Favorite Links
Documents
Pictures
Music
Recently Changed
Name Date modified Type Size Tags
00077.exe 3/10/2023 11:37... Application 2 KB
00078.exe 3/10/2023 11:37... Application 2 KB
00079.exe 3/10/2023 11:37... Application 2 KB
00080.exe 3/10/2023 11:37... Application 2 KB
00081.exe 3/10/2023 11:37... Application 2 KB
results.txt - Notepad
File Edit Format View Help
Javascript: [][(![]+[][+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[][!+[]+!+[]]+(!![]+[][+[]]+(!![]+[][!+[]+!+[]+!+[]]+(!![]+[][+!+[]]][([][(![]+[]
HashCalc
Data Format: File
Data: C:\Users\Administrator\Desktop\256exes\results.txt
HMAC
Key Format: Text string
Key:
MD5
MD4
SHA1
SHA256 29862448576a711160842dad42c0e8b19a7cfa20a718e08f82a1e4168d48c765
SHA384 04af8a55e9d634b980df8bc1fb5bc03ea2499d575c6405ccd859ac01469cdb88a015b3
SHA512
RIPEMD160
PANAMA
TIGER
MD2