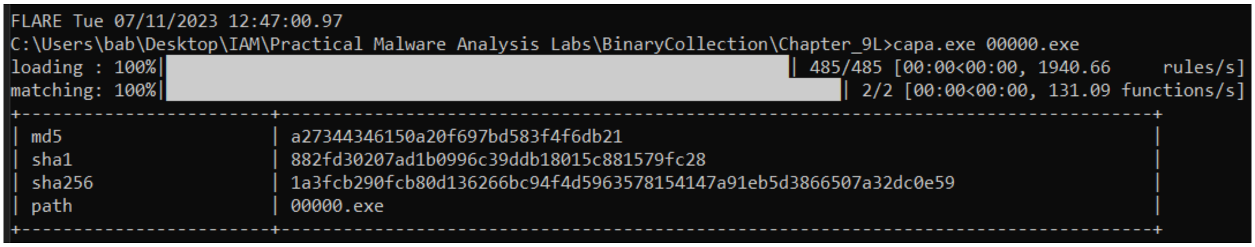
Lab 15: Patching EXEs with Ollydbg

Patching an EXE

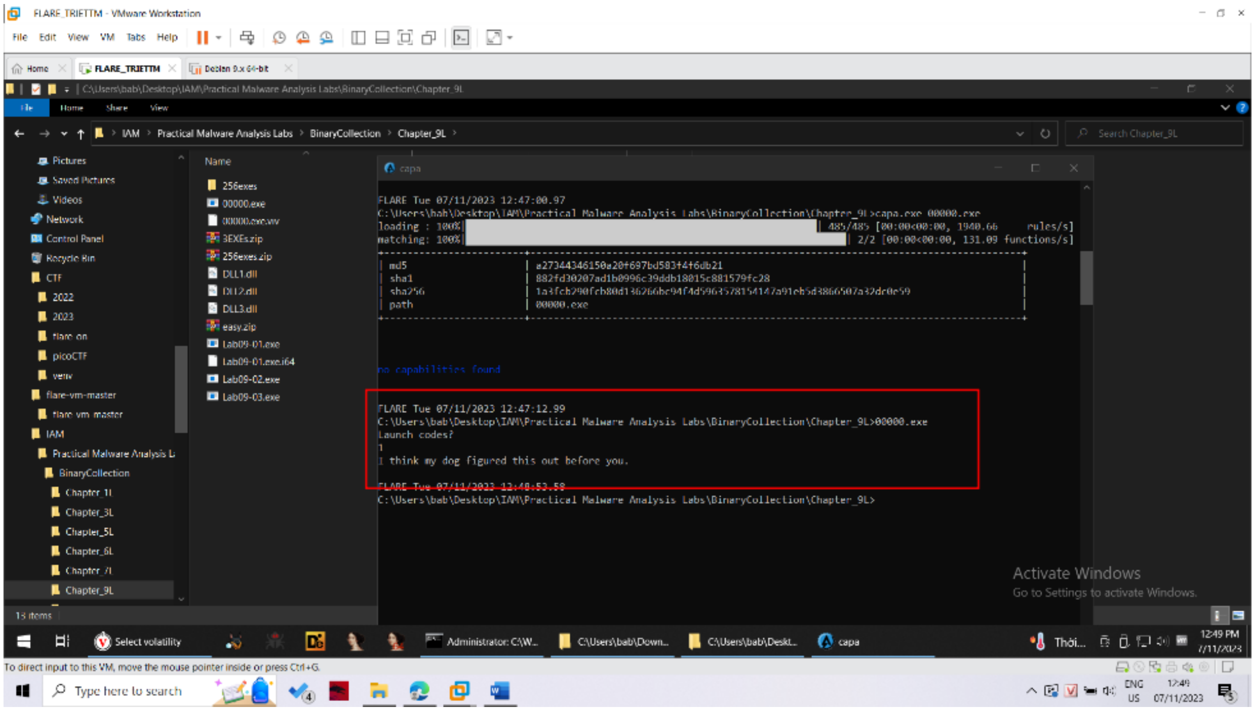
Check hash file exe



```
FLARE Tue 07/11/2023 12:47:00.97
C:\Users\bab\Desktop\IAM\Practical Malware Analysis Labs\BinaryCollection\Chapter_9L>capa.exe 00000.exe
loading : 100%|                                                              | 485/485 [00:00<00:00, 1940.66     rules/s]
matching: 100%|                                                                   | 2/2 [00:00<00:00, 131.09 functions/s]
+-------------------------+-------------------------------------------------------------------------------------+
| md5                     | a27344346150a20f697bd583f4f6db21                                                    |
| sha1                    | 882fd30207ad1b0996c39ddb18015c881579fc28                                            |
| sha256                  | 1a3fcb290fcb80d136266bc94f4d5963578154147a91eb5d3866507a32dc0e59                    |
| path                    | 00000.exe                                                                           |
+-------------------------+-------------------------------------------------------------------------------------+
```

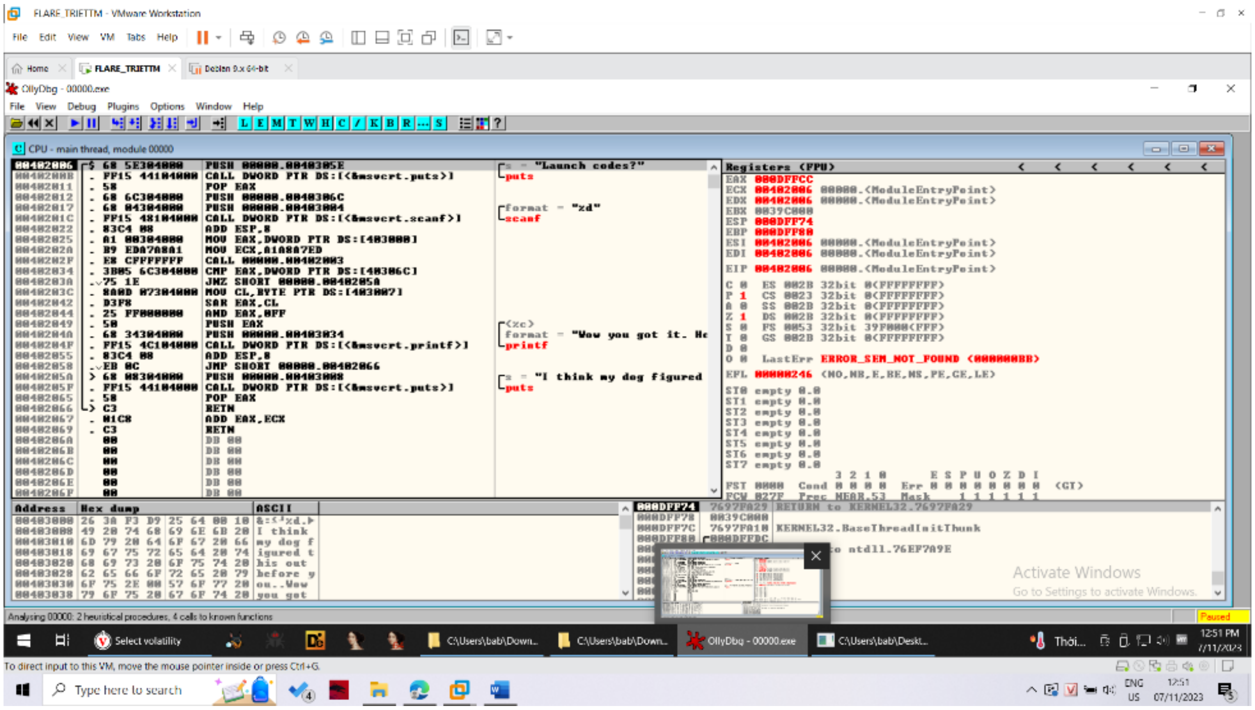
Running the EXE

Chạy thử file exe này.



```
FLARE Tue 07/11/2023 12:47:00.97
C:\Users\bab\Desktop\IAM\Practical Malware Analysis Labs\BinaryCollection\Chapter_9L>capa.exe 00000.exe
loading : 100%|                                              | 485/485 [00:00<00:00, 1940.66     rules/s]
matching: 100%|                                                   | 2/2 [00:00<00:00, 131.09 functions/s]
+-----------------------+-----------------------------------------------------------------------+
| md5                   | a27344346150a20f697bd583f4f6db21                                      |
| sha1                  | 882fd30207ad1b0996c39ddb18015c881579fc28                              |
| sha256                | 1a3fcb290fcb80d136266bc94f4d5963578154147a91eb5d3866507a32dc0e59      |
| path                  | 00000.exe                                                             |
+-----------------------+-----------------------------------------------------------------------+


no capabilities found


FLARE Tue 07/11/2023 12:47:12.99
C:\Users\bab\Desktop\IAM\Practical Malware Analysis Labs\BinaryCollection\Chapter_9L>00000.exe
Launch codes?
1
I think my dog figured this out before you.

FLARE Tue 07/11/2023 12:48:53.58
C:\Users\bab\Desktop\IAM\Practical Malware Analysis Labs\BinaryCollection\Chapter_9L>
```

Examining the EXE with Ollydbg



FLARE_TRIETTM - VMware Workstation
File Edit View VM Tabs Help
Home
FLARE_TRIETTM
Debian 9.x 64-bit
OllyDbg - 00000.exe
File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S
CPU - main thread, module 00000

```
00402006  $ 68 5E304000    PUSH 00000.0040305E               [s = "Launch codes?"
0040200B  . FF15 44104000  CALL DWORD PTR DS:[<&msvcrt.puts>] [puts
00402011  . 58             POP EAX
00402012  . 68 6C304000    PUSH 00000.0040306C
00402017  . 68 04304000    PUSH 00000.00403004               [format = "%d"
0040201C  . FF15 48104000  CALL DWORD PTR DS:[<&msvcrt.scanf>] [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  . 3B05 6C304000  CMP EAX,DWORD PTR DS:[40306C]
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                          [<%c>
0040204A  . 68 34304000    PUSH 00000.00403034               [format = "Wow you got it. He
0040204F  . FF15 4C104000  CALL DWORD PTR DS:[<&msvcrt.printf>] [printf
00402055  . 83C4 08        ADD ESP,8
00402058  .vEB 0C          JMP SHORT 00000.00402066
0040205A  > 68 08304000    PUSH 00000.00403008               [s = "I think my dog figured
0040205F  . FF15 44104000  CALL DWORD PTR DS:[<&msvcrt.puts>] [puts
00402065  . 58             POP EAX
00402066  > 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
```

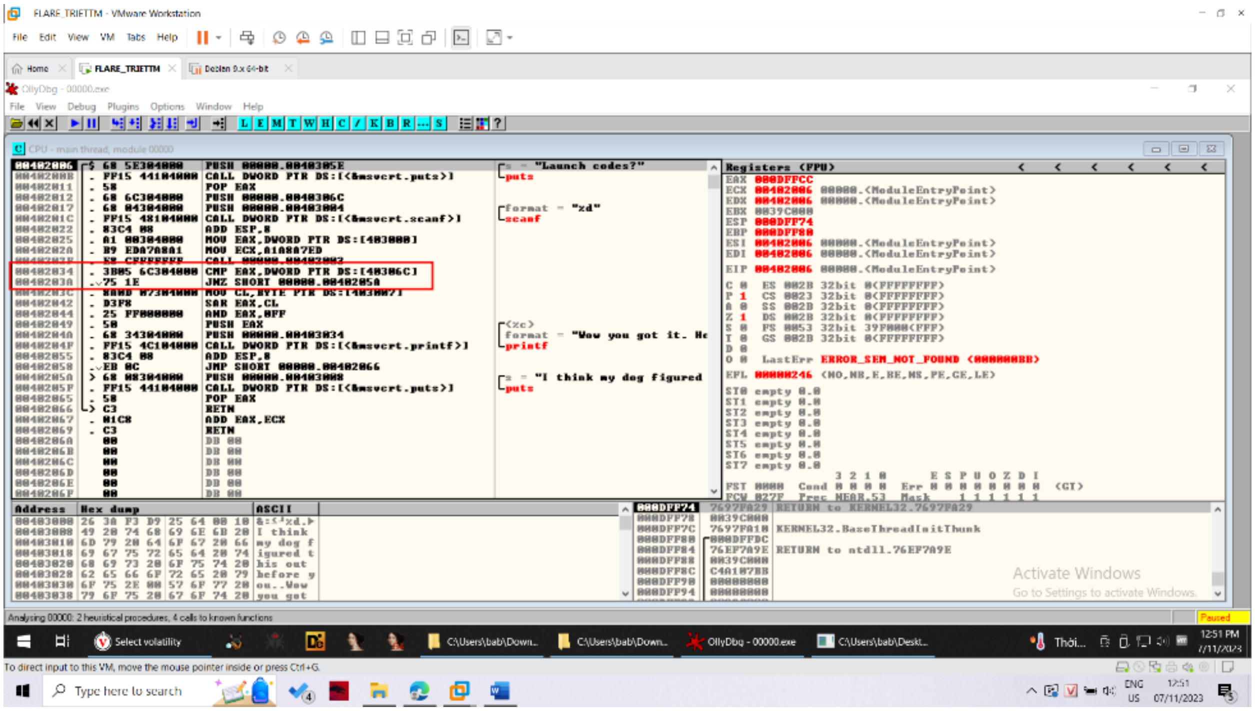
```
Registers (FPU)
EAX 000DFFCC
ECX 00402006 00000.<ModuleEntryPoint>
EDX 00402006 00000.<ModuleEntryPoint>
EBX 0039C000
ESP 000DFF74
EBP 000DFF80
ESI 00402006 00000.<ModuleEntryPoint>
EDI 00402006 00000.<ModuleEntryPoint>

EIP 00402006 00000.<ModuleEntryPoint>

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 39F000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SEM_NOT_FOUND (000000BB)

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

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

```
Address   Hex dump                 ASCII
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
```

```
000DFF74  7697FA29  RETURN to KERNEL32.7697FA29
000DFF78  0039C000
000DFF7C  7697FA10  KERNEL32.BaseThreadInitThunk
000DFF80  000DFFDC
                    to ntdll.76EF7A9E
```

Analysing 00000: 2 heuristical procedures, 4 calls to known functions

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



```
00402006  $ 68 5E304000    PUSH 00000.0040305E               [s = "Launch codes?"
0040200B  . FF15 44104000  CALL DWORD PTR DS:[<&msvcrt.puts>] [puts
00402011  . 58             POP EAX
00402012  . 68 6C304000    PUSH 00000.0040306C
00402017  . 68 04304000    PUSH 00000.00403004               [format = "%d"
0040201C  . FF15 48104000  CALL DWORD PTR DS:[<&msvcrt.scanf>] [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  . 3B05 6C304000  CMP EAX,DWORD PTR DS:[40306C]
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                          [<%c>
0040204A  . 68 34304000    PUSH 00000.00403034               [format = "Wow you got it. He
0040204F  . FF15 4C104000  CALL DWORD PTR DS:[<&msvcrt.printf>] [printf
00402055  . 83C4 08        ADD ESP,8
00402058  .vEB 0C          JMP SHORT 00000.00402066
0040205A  > 68 08304000    PUSH 00000.00403008               [s = "I think my dog figured
0040205F  . FF15 44104000  CALL DWORD PTR DS:[<&msvcrt.puts>] [puts
00402065  . 58             POP EAX
00402066  > 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
```

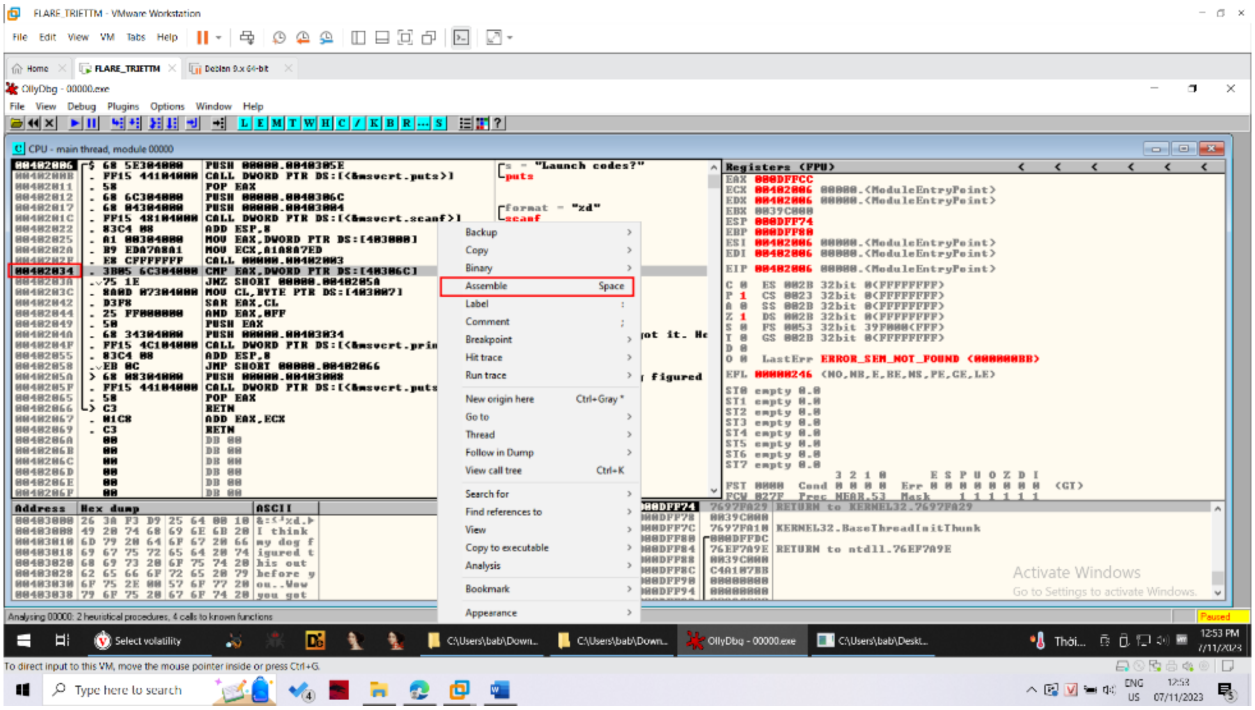
```
Registers (FPU)
EAX 000DFFCC
ECX 00402006 00000.<ModuleEntryPoint>
EDX 00402006 00000.<ModuleEntryPoint>
EBX 0039C000
ESP 000DFF74
EBP 000DFF80
ESI 00402006 00000.<ModuleEntryPoint>
EDI 00402006 00000.<ModuleEntryPoint>

EIP 00402006 00000.<ModuleEntryPoint>

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 39F000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SEM_NOT_FOUND (000000BB)

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

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

```
Address   Hex dump                 ASCII
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
```

```
000DFF74  7697FA29  RETURN to KERNEL32.7697FA29
000DFF78  0039C000
000DFF7C  7697FA10  KERNEL32.BaseThreadInitThunk
000DFF80  000DFFDC
000DFF84  76EF7A9E  RETURN to ntdll.76EF7A9E
000DFF88  0039C000
000DFF8C  C4A107BB
000DFF90  00000000
000DFF94  00000000
```

Analysing 00000: 2 heuristical procedures, 4 calls to known functions

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



```
00402006  $ 68 5E304000      PUSH 00000.0040305E                       s = "Launch codes?"
0040200B  . FF15 44104000    CALL DWORD PTR DS:[<&msvcrt.puts>]        puts
00402011  . 58               POP EAX
00402012  . 68 6C304000      PUSH 00000.0040306C
00402017  . 68 04304000      PUSH 00000.00403004                       format = "%d"
0040201C  . FF15 48104000    CALL DWORD PTR DS:[<&msvcrt.scanf>]       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  . 3B05 6C304000    CMP EAX,DWORD PTR DS:[40306C]
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                                  <%c>
0040204A  . 68 34304000      PUSH 00000.00403034                       format = "Wow you got it. He
0040204F  . FF15 4C104000    CALL DWORD PTR DS:[<&msvcrt.printf>]      printf
00402055  . 83C4 08          ADD ESP,8
00402058  .vEB 0C            JMP SHORT 00000.00402066
0040205A  > 68 08304000      PUSH 00000.00403008                       s = "I think my dog figured
0040205F  . FF15 44104000    CALL DWORD PTR DS:[<&msvcrt.puts>]        puts
00402065  . 58               POP EAX
00402066  > 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
```

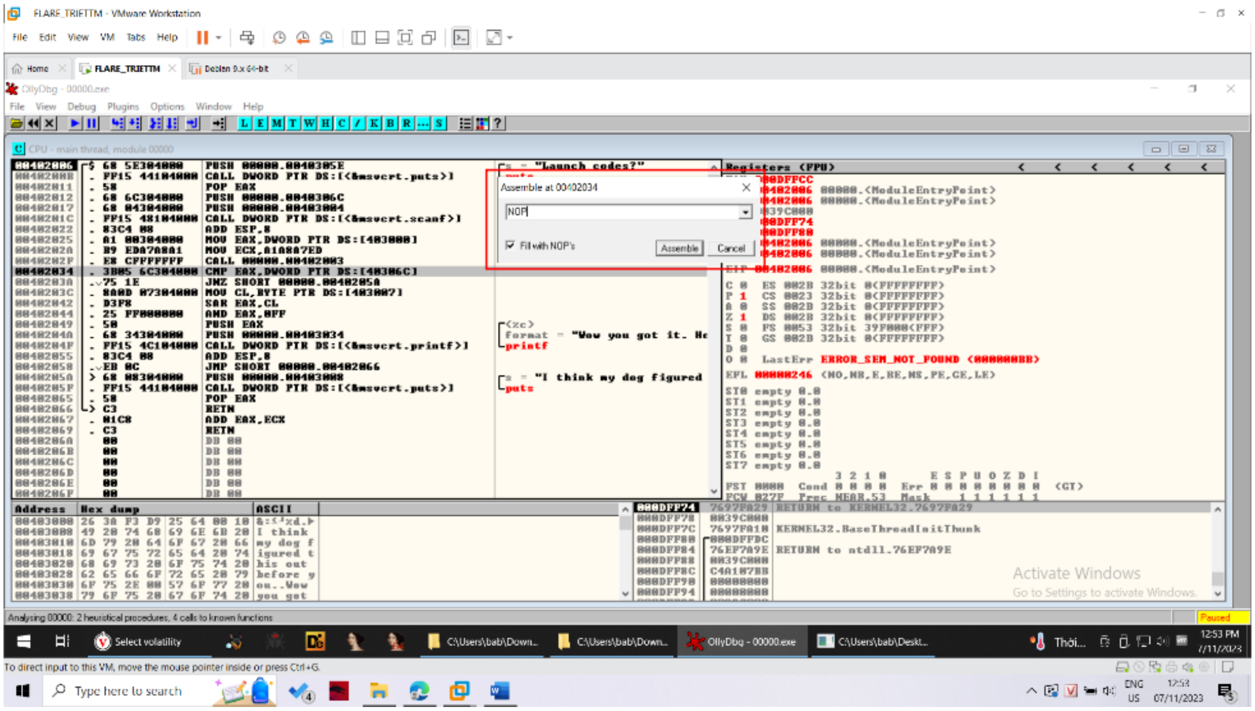
```
Registers (FPU)
EAX 000DFFCC
ECX 00402006 00000.<ModuleEntryPoint>
EDX 00402006 00000.<ModuleEntryPoint>
EBX 0039C000
ESP 000DFF74
EBP 000DFF80
ESI 00402006 00000.<ModuleEntryPoint>
EDI 00402006 00000.<ModuleEntryPoint>

EIP 00402006 00000.<ModuleEntryPoint>

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 39F000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SEM_NOT_FOUND (000000BB)

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

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

```
Address   Hex dump                 ASCII
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
```

```
000DFF74  7697FA29  RETURN to KERNEL32.7697FA29
000DFF78  0039C000
000DFF7C  7697FA10  KERNEL32.BaseThreadInitThunk
000DFF80  000DFFDC
000DFF84  76EF7A9E  RETURN to ntdll.76EF7A9E
000DFF88  0039C000
000DFF8C  C4A107BB
000DFF90  00000000
000DFF94  00000000
```

Analysing 00000: 2 heuristical procedures, 4 calls to known functions

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Assemble at 00402034

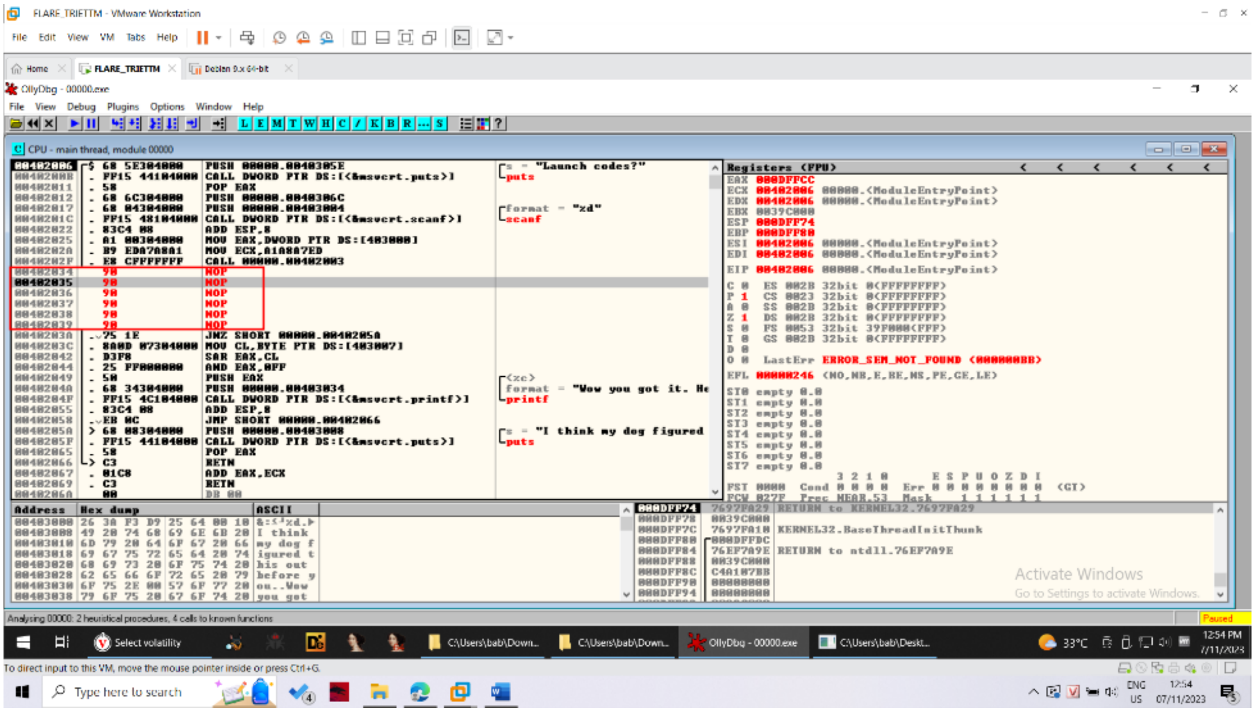
NOP

☑ Fill with NOP's

Assemble Cancel

Analysing 00000: 2 heuristical procedures, 4 calls to known functions

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



FLARE_TRIETTM - VMware Workstation
File Edit View VM Tabs Help
Home
FLARE_TRIETTM
Debian 9.x 64-bit
OllyDbg - 00000.exe
File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S
CPU - main thread, module 00000

```
00402006  ┌$ 68 5E304000    PUSH 00000.0040305E                      ┌s = "Launch codes?"
0040200B  │. FF15 44104000  CALL DWORD PTR DS:[<&msvcrt.puts>]        └puts
00402011  │. 58             POP EAX
00402012  │. 68 6C304000    PUSH 00000.0040306C
00402017  │. 68 04304000    PUSH 00000.00403004                      ┌format = "%d"
0040201C  │. FF15 48104000  CALL DWORD PTR DS:[<&msvcrt.scanf>]       └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  │.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                                 ┌<%c>
0040204A  │. 68 34304000    PUSH 00000.00403034                      │format = "Wow you got it. He
0040204F  │. FF15 4C104000  CALL DWORD PTR DS:[<&msvcrt.printf>]      └printf
00402055  │. 83C4 08        ADD ESP,8
00402058  │.vEB 0C          JMP SHORT 00000.00402066
0040205A  │> 68 08304000    PUSH 00000.00403008                      ┌s = "I think my dog figured
0040205F  │. FF15 44104000  CALL DWORD PTR DS:[<&msvcrt.puts>]        └puts
00402065  │. 58             POP EAX
00402066  └> C3             RETN
00402067   . 01C8           ADD EAX,ECX
00402069   . C3             RETN
0040206A     00             DB 00
```

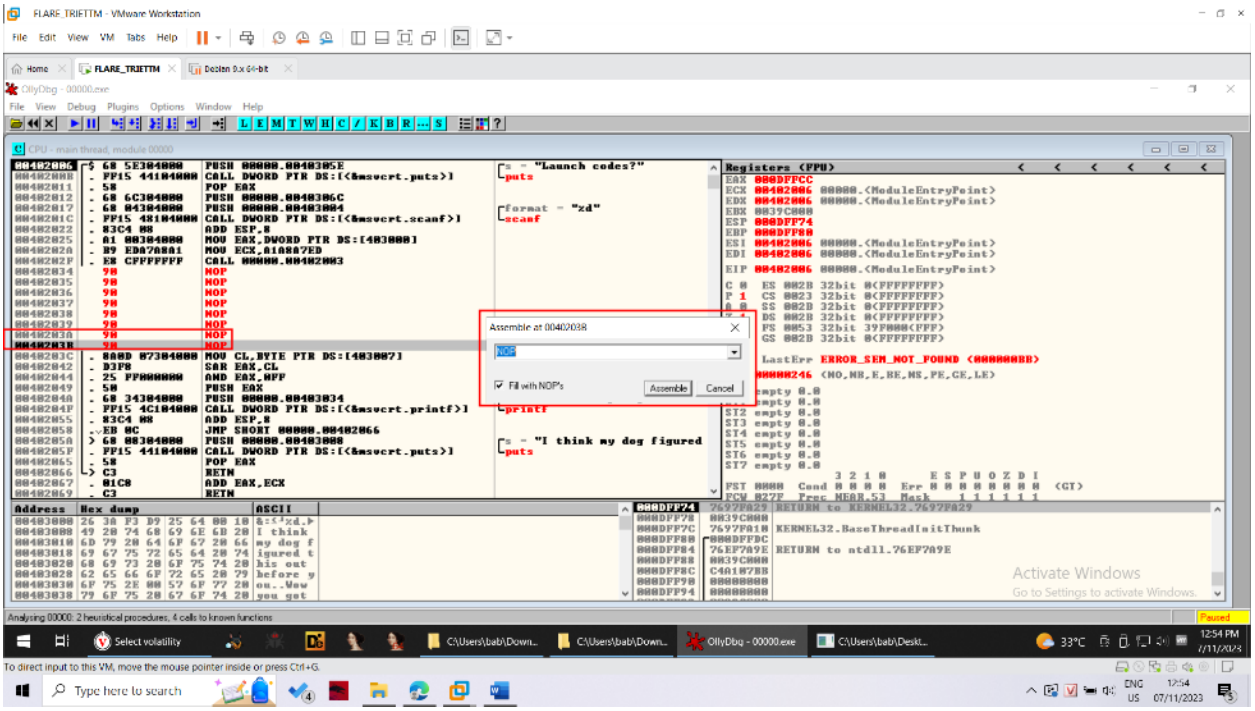
```
Registers (FPU)
EAX 000DFFCC
ECX 00402006 00000.<ModuleEntryPoint>
EDX 00402006 00000.<ModuleEntryPoint>
EBX 0039C000
ESP 000DFF74
EBP 000DFF80
ESI 00402006 00000.<ModuleEntryPoint>
EDI 00402006 00000.<ModuleEntryPoint>

EIP 00402006 00000.<ModuleEntryPoint>

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 39F000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SEM_NOT_FOUND (000000BB)

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

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

```
Address   Hex dump                 ASCII
00403000  26 3A F3 D9 25 64 00 10  &:≤┘%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
```

```
000DFF74  7697FA29  RETURN to KERNEL32.7697FA29
000DFF78  0039C000
000DFF7C  7697FA10  KERNEL32.BaseThreadInitThunk
000DFF80 ┌000DFFDC
000DFF84 │76EF7A9E  RETURN to ntdll.76EF7A9E
000DFF88 │0039C000
000DFF8C │C4A107BB
000DFF90 │00000000
000DFF94 │00000000
```

Analysing 00000: 2 heuristical procedures, 4 calls to known functions

Paused
Activate Windows
Go to Settings to activate Windows.
Select volatility
C:\Users\bab\Down...
C:\Users\bab\Down...
OllyDbg - 00000.exe
C:\Users\bab\Deskt...
33°C
12:54 PM
7/11/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
US
12:54
07/11/2023



FLARE_TRIETTM - VMware Workstation
File Edit View VM Tabs Help
Home
FLARE_TRIETTM
Debian 9.x 64-bit
OllyDbg - 00000.exe
File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S
CPU - main thread, module 00000

```
00402006  ┌$ 68 5E304000    PUSH 00000.0040305E                      ┌s = "Launch codes?"
0040200B  │. FF15 44104000  CALL DWORD PTR DS:[<&msvcrt.puts>]        └puts
00402011  │. 58             POP EAX
00402012  │. 68 6C304000    PUSH 00000.0040306C
00402017  │. 68 04304000    PUSH 00000.00403004                      ┌format = "%d"
0040201C  │. FF15 48104000  CALL DWORD PTR DS:[<&msvcrt.scanf>]       └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  . D3F8            SAR EAX,CL
00402044  . 25 FF000000     AND EAX,0FF
00402049  . 50              PUSH EAX
0040204A  . 68 34304000     PUSH 00000.00403034
0040204F  . FF15 4C104000   CALL DWORD PTR DS:[<&msvcrt.printf>]      └printf
00402055  . 83C4 08         ADD ESP,8
00402058  .vEB 0C           JMP SHORT 00000.00402066
0040205A  > 68 08304000     PUSH 00000.00403008                      ┌s = "I think my dog figured
0040205F  . FF15 44104000   CALL DWORD PTR DS:[<&msvcrt.puts>]        └puts
00402065  . 58              POP EAX
00402066  └> C3             RETN
00402067  . 01C8            ADD EAX,ECX
00402069  . C3              RETN
```

Assemble at 0040203B

NOP

☑ Fill with NOP's

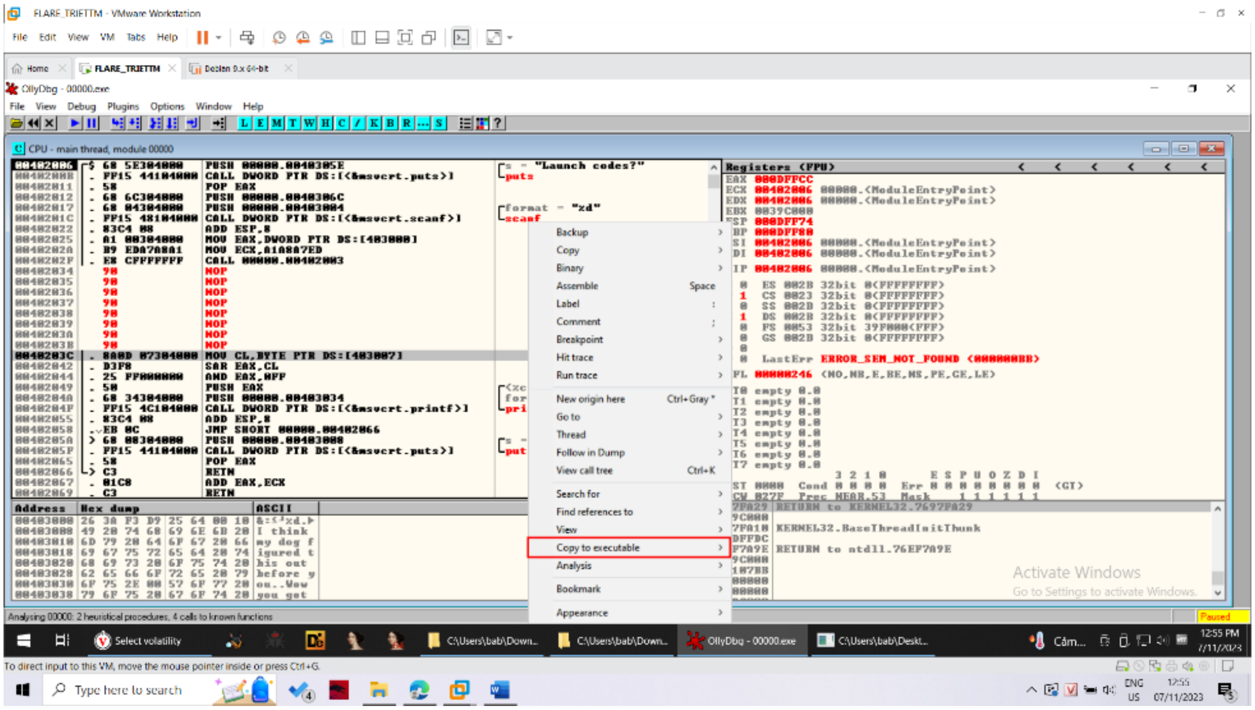
Assemble   Cancel

```
Registers (FPU)
EAX 000DFFCC
ECX 00402006 00000.<ModuleEntryPoint>
EDX 00402006 00000.<ModuleEntryPoint>
EBX 0039C000
ESP 000DFF74
EBP 000DFF80
ESI 00402006 00000.<ModuleEntryPoint>
EDI 00402006 00000.<ModuleEntryPoint>

EIP 00402006 00000.<ModuleEntryPoint>

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
     DS 002B 32bit 0(FFFFFFFF)
     FS 0053 32bit 39F000(FFF)
     GS 002B 32bit 0(FFFFFFFF)

     LastErr ERROR_SEM_NOT_FOUND (000000BB)
00000246 (NO,NB,E,BE,NS,PE,GE,LE)
empty 0.0
empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address   Hex dump                 ASCII
00403000  26 3A F3 D9 25 64 00 10  &:≤┘%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
```

```
000DFF74  7697FA29  RETURN to KERNEL32.7697FA29
000DFF78  0039C000
000DFF7C  7697FA10  KERNEL32.BaseThreadInitThunk
000DFF80 ┌000DFFDC
000DFF84 │76EF7A9E  RETURN to ntdll.76EF7A9E
000DFF88 │0039C000
000DFF8C │C4A107BB
000DFF90 │00000000
000DFF94 │00000000
```

Analysing 00000: 2 heuristical procedures, 4 calls to known functions



```
00402006 ┌$ 68 5E304000   PUSH 00000.0040305E                       ┌s = "Launch codes?"
0040200B │. FF15 44104000 CALL DWORD PTR DS:[<&msvcrt.puts>]        └puts
00402011 │. 58            POP EAX
00402012 │. 68 6C304000   PUSH 00000.0040306C
00402017 │. 68 04304000   PUSH 00000.00403004                       ┌format = "%d"
0040201C │. FF15 48104000 CALL DWORD PTR DS:[<&msvcrt.scanf>]       └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 │. D3F8          SAR EAX,CL
00402044 │. 25 FF000000   AND EAX,0FF
00402049 │. 50            PUSH EAX                                  ┌<%c
0040204A │. 68 34304000   PUSH 00000.00403034                       │for
0040204F │. FF15 4C104000 CALL DWORD PTR DS:[<&msvcrt.printf>]      └pri
00402055 │. 83C4 08       ADD ESP,8
00402058 │.vEB 0C         JMP SHORT 00000.00402066
0040205A │> 68 08304000   PUSH 00000.00403008                       ┌s -
0040205F │. FF15 44104000 CALL DWORD PTR DS:[<&msvcrt.puts>]        └put
00402065 │. 58            POP EAX
00402066 └> C3            RETN
00402067  . 01C8          ADD EAX,ECX
00402069  . C3            RETN
```

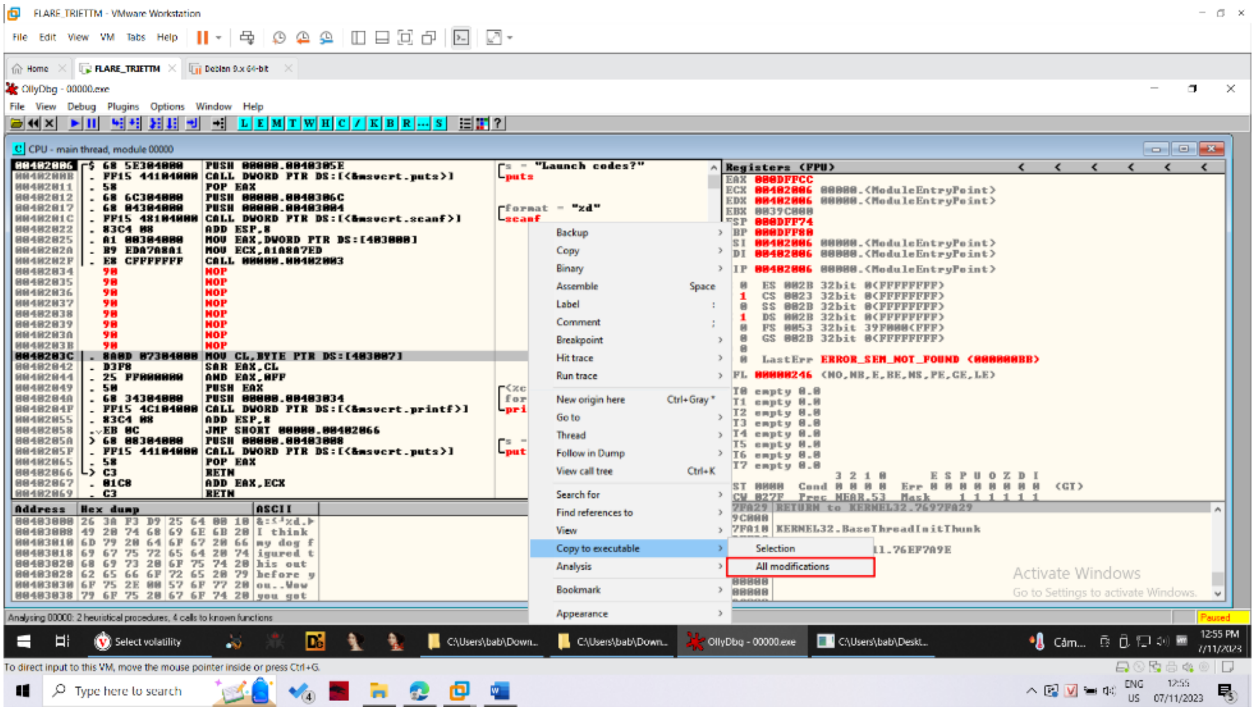
```
Address  Hex dump                 ASCII
00403000 26 3A F3 D9|25 64 00 10 &:≤┘%d.►
00403008 49 20 74 68|69 6E 6B 20 I think
00403010 6D 79 20 64|6F 67 20 66 my dog f
00403018 69 67 75 72|65 64 20 74 igured t
00403020 68 69 73 20|6F 75 74 20 his out
00403028 62 65 66 6F|72 65 20 79 before y
00403030 6F 75 2E 00|57 6F 77 20 ou..Wow
00403038 79 6F 75 20|67 6F 74 20 you got
```

```
Registers (FPU)
EAX 000DFFCC
ECX 00402006 00000.<ModuleEntryPoint>
EDX 00402006 00000.<ModuleEntryPoint>
EBX 0039C000
ESP 000DFF74
EBP 000DFF80
ESI 00402006 00000.<ModuleEntryPoint>
EDI 00402006 00000.<ModuleEntryPoint>

EIP 00402006 00000.<ModuleEntryPoint>
 0  ES 002B 32bit 0(FFFFFFFF)
 1  CS 0023 32bit 0(FFFFFFFF)
 0  SS 002B 32bit 0(FFFFFFFF)
 1  DS 002B 32bit 0(FFFFFFFF)
 0  FS 0053 32bit 39F000(FFF)
 0  GS 002B 32bit 0(FFFFFFFF)
 0
 0  LastErr ERROR_SEM_NOT_FOUND (000000BB)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
7FA29 RETURN to KERNEL32.7697FA29
9C000
7FA10 KERNEL32.BaseThreadInitThunk
DFFDC
F7A9E RETURN to ntdll.76EF7A9E
9C000
107BB
00000
00000
```

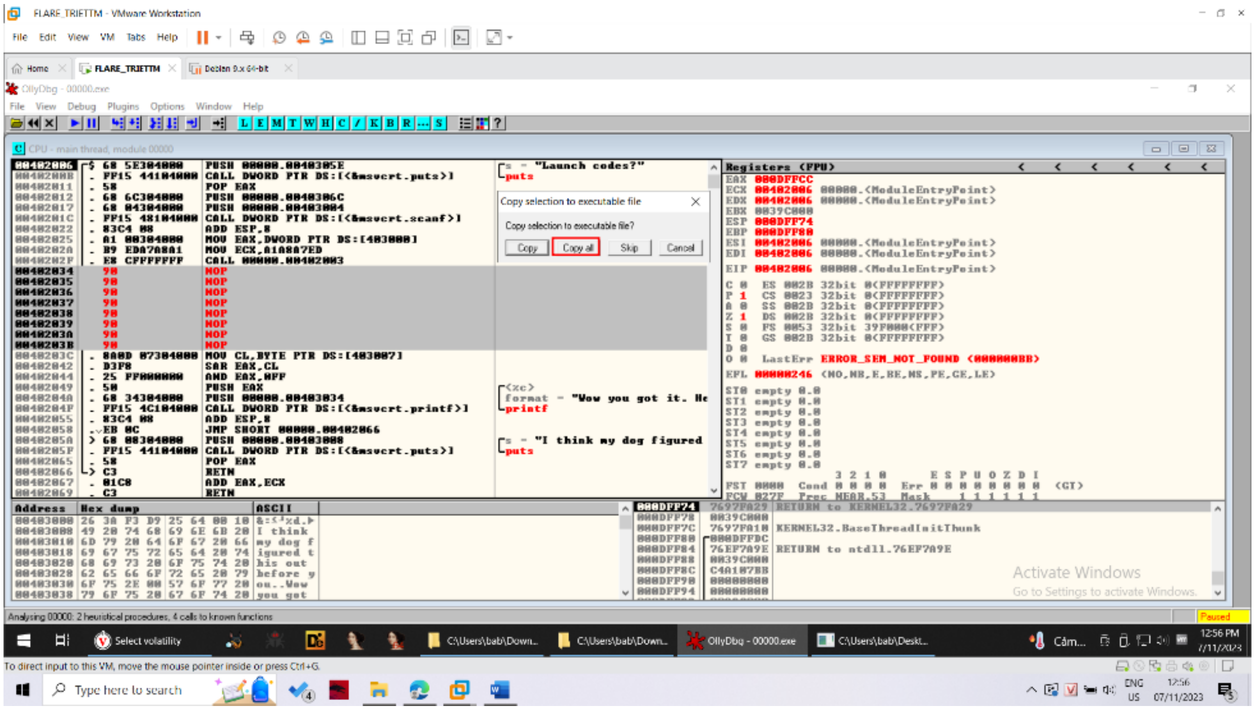
Analysing 00000: 2 heuristical procedures, 4 calls to known functions

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Analysing 00000: 2 heuristical procedures, 4 calls to known functions

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


FLARE_TRIETTM - VMware Workstation
File Edit View VM Tabs Help
Home
FLARE_TRIETTM
Debian 9.x 64-bit
OllyDbg - 00000.exe
File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S
CPU - main thread, module 00000

```
00402006 ┌$ 68 5E304000    PUSH 00000.0040305E          ┌s = "Launch codes?"
0040200B │. FF15 44104000  CALL DWORD PTR DS:[<&msvcrt.puts>]  └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 │. D3F8           SAR EAX,CL
00402044 │. 25 FF000000    AND EAX,0FF
00402049 │. 50             PUSH EAX                     ┌<%c>
0040204A │. 68 34304000    PUSH 00000.00403034          │format = "Wow you got it. He
0040204F │. FF15 4C104000  CALL DWORD PTR DS:[<&msvcrt.printf>] └printf
00402055 │. 83C4 08        ADD ESP,8
00402058 │.vEB 0C          JMP SHORT 00000.00402066
0040205A │> 68 08304000    PUSH 00000.00403008          ┌s = "I think my dog figured
0040205F │. FF15 44104000  CALL DWORD PTR DS:[<&msvcrt.puts>]  └puts
00402065 │. 58             POP EAX
00402066 └> C3             RETN
00402067  . 01C8           ADD EAX,ECX
00402069  . C3             RETN
```

Copy selection to executable file

Copy selection to executable file?

Copy | Copy all | Skip | Cancel

```
Registers (FPU)
EAX 000DFFCC
ECX 00402006 00000.<ModuleEntryPoint>
EDX 00402006 00000.<ModuleEntryPoint>
EBX 0039C000
ESP 000DFF74
EBP 000DFF80
ESI 00402006 00000.<ModuleEntryPoint>
EDI 00402006 00000.<ModuleEntryPoint>

EIP 00402006 00000.<ModuleEntryPoint>

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 39F000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SEM_NOT_FOUND (000000BB)

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

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

```
Address   Hex dump                 ASCII
00403000  26 3A F3 D9 25 64 00 10  &:≤┘%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
```

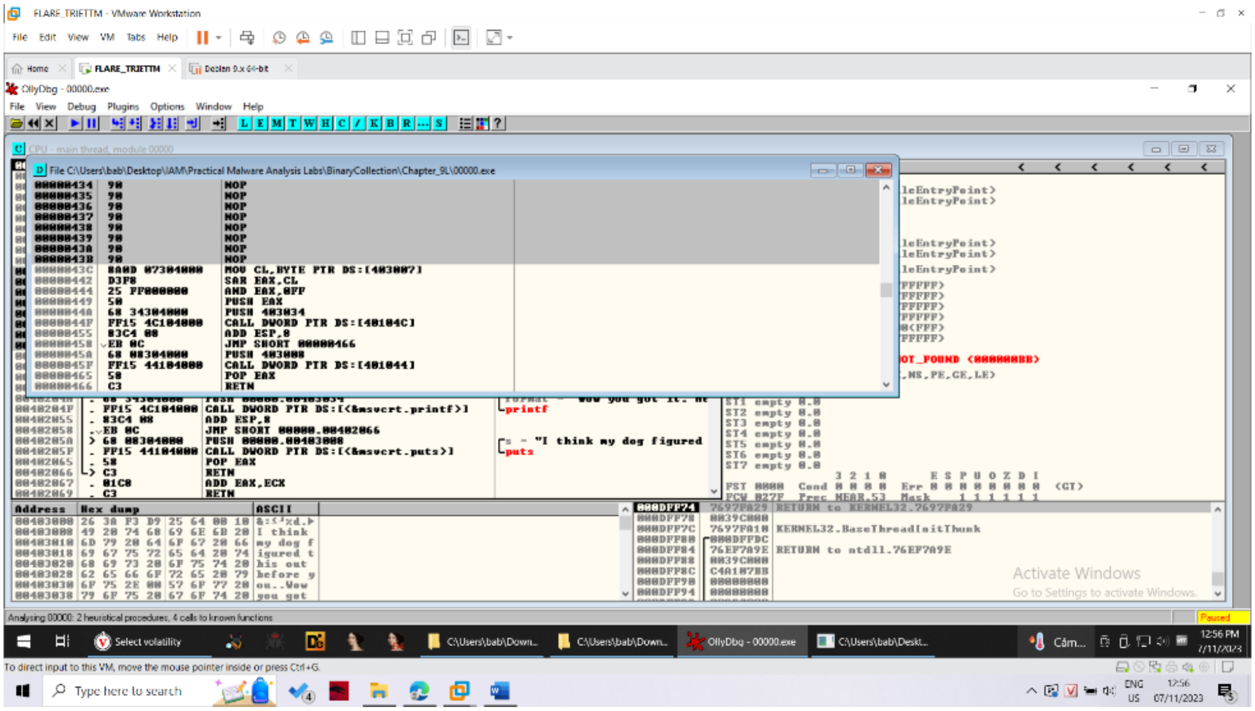
```
000DFF74   7697FA29  RETURN to KERNEL32.7697FA29
000DFF78   0039C000
000DFF7C   7697FA10  KERNEL32.BaseThreadInitThunk
000DFF80  ┌000DFFDC
000DFF84  │76EF7A9E  RETURN to ntdll.76EF7A9E
000DFF88  │0039C000
000DFF8C  │C4A107BB
000DFF90  │00000000
000DFF94  │00000000
```

Activate Windows
Go to Settings to activate Windows.

Analysing 00000: 2 heuristical procedures, 4 calls to known functions

Paused

Select volatility
C:\Users\bab\Down...
C:\Users\bab\Down...
OllyDbg - 00000.exe
C:\Users\bab\Deskt...
Cám...
12:56 PM
7/11/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
US
12:56
07/11/2023


FLARE_TRIETTM - VMware Workstation
File Edit View VM Tabs Help
Home
FLARE_TRIETTM
Debian 9.x 64-bit
OllyDbg - 00000.exe
File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S
CPU - main thread, module 00000

File C:\Users\bab\Desktop\IAM\Practical Malware Analysis Labs\BinaryCollection\Chapter_9L\00000.exe

```
00000434   90             NOP
00000435   90             NOP
00000436   90             NOP
00000437   90             NOP
00000438   90             NOP
00000439   90             NOP
0000043A   90             NOP
0000043B   90             NOP
0000043C   8A0D 07304000  MOV CL,BYTE PTR DS:[403007]
00000442   D3F8           SAR EAX,CL
00000444   25 FF000000    AND EAX,0FF
00000449   50             PUSH EAX
0000044A   68 34304000    PUSH 403034
0000044F   FF15 4C104000  CALL DWORD PTR DS:[40104C]
00000455   83C4 08        ADD ESP,8
00000458  vEB 0C          JMP SHORT 00000466
0000045A   68 08304000    PUSH 403008
0000045F   FF15 44104000  CALL DWORD PTR DS:[401044]
00000465   58             POP EAX
00000466   C3             RETN
```

```
0040204F │. FF15 4C104000  CALL DWORD PTR DS:[<&msvcrt.printf>] └printf
00402055 │. 83C4 08        ADD ESP,8
00402058 │.vEB 0C          JMP SHORT 00000.00402066
0040205A │> 68 08304000    PUSH 00000.00403008          ┌s = "I think my dog figured
0040205F │. FF15 44104000  CALL DWORD PTR DS:[<&msvcrt.puts>]  └puts
00402065 │. 58             POP EAX
00402066 └> C3             RETN
00402067  . 01C8           ADD EAX,ECX
00402069  . C3             RETN
```

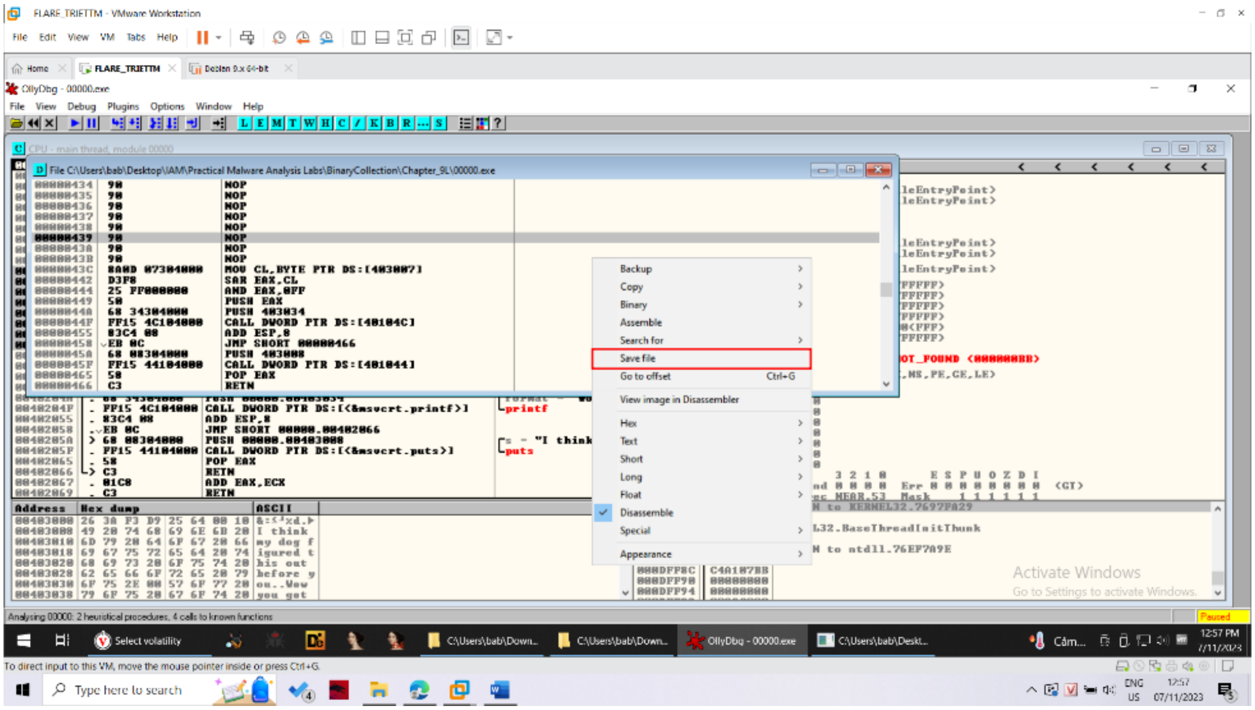
```
Address   Hex dump                 ASCII
00403000  26 3A F3 D9 25 64 00 10  &:≤┘%d.►
00403008  49 20 74 68 69 6E 6B 20  I think
00403010  6D 79 20 64 6F 67 20 66  my dog f
00403018  69 67 75 72 65 64 20 74  igured t
00403020  68 69 73 20 6F 75 74 20  his out
00403028  62 65 66 6F 72 65 20 79  before y
00403030  6F 75 2E 00 57 6F 77 20  ou..Wow
00403038  79 6F 75 20 67 6F 74 20  you got
```

```
000DFF74   7697FA29  RETURN to KERNEL32.7697FA29
000DFF78   0039C000
000DFF7C   7697FA10  KERNEL32.BaseThreadInitThunk
000DFF80  ┌000DFFDC
000DFF84  │76EF7A9E  RETURN to ntdll.76EF7A9E
000DFF88  │0039C000
000DFF8C  │C4A107BB
000DFF90  │00000000
000DFF94  │00000000
```

Activate Windows
Go to Settings to activate Windows.

Analysing 00000: 2 heuristical procedures, 4 calls to known functions

Paused


FLARE_TRIETTM - VMware Workstation
OllyDbg - 00000.exe
CPU - main thread, module 00000
File C:\Users\bab\Desktop\IAM\Practical Malware Analysis Labs\BinaryCollection\Chapter_9L\00000.exe
Backup
Copy
Binary
Assemble
Search for
Save file
Go to offset Ctrl+G
View image in Disassembler
Hex
Text
Short
Long
Float
Disassemble
Special
Appearance
Activate Windows
Go to Settings to activate Windows.

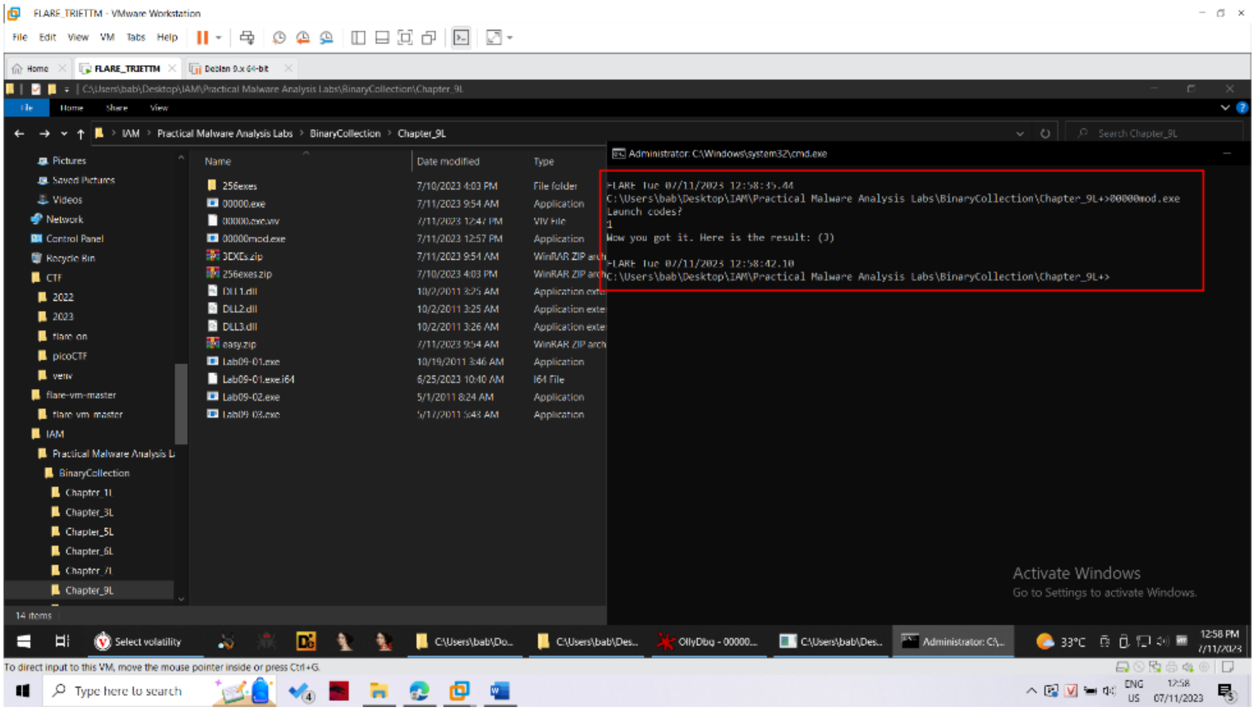
```
00000434   90              NOP
00000435   90              NOP
00000436   90              NOP
00000437   90              NOP
00000438   90              NOP
00000439   90              NOP
0000043A   90              NOP
0000043B   90              NOP
0000043C   8A0D 07304000   MOV CL,BYTE PTR DS:[403007]
00000442   D3F8            SAR EAX,CL
00000444   25 FF000000     AND EAX,0FF
00000449   50              PUSH EAX
0000044A   68 34304000     PUSH 403034
0000044F   FF15 4C104000   CALL DWORD PTR DS:[40104C]
00000455   83C4 08         ADD ESP,8
00000458  vEB 0C           JMP SHORT 00000466
0000045A   68 08304000     PUSH 403008
0000045F   FF15 44104000   CALL DWORD PTR DS:[401044]
00000465   58              POP EAX
00000466   C3              RETN
```

```
0040204F  . FF15 4C104000  CALL DWORD PTR DS:[<&msvcrt.printf>]   printf
00402055  . 83C4 08        ADD ESP,8
00402058  .vEB 0C          JMP SHORT 00000.00402066
0040205A  > 68 08304000    PUSH 00000.00403008                    s = "I think
0040205F  . FF15 44104000  CALL DWORD PTR DS:[<&msvcrt.puts>]     puts
00402065  . 58             POP EAX
00402066  > C3             RETN
00402067  . 01C8           ADD EAX,ECX
00402069  . C3             RETN
```

```
Address   Hex dump                 ASCII
00403000  26 3A F3 D9 25 64 00 10  &:≤┘%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
```

Analysing 00000: 2 heuristical procedures, 4 calls to known functions

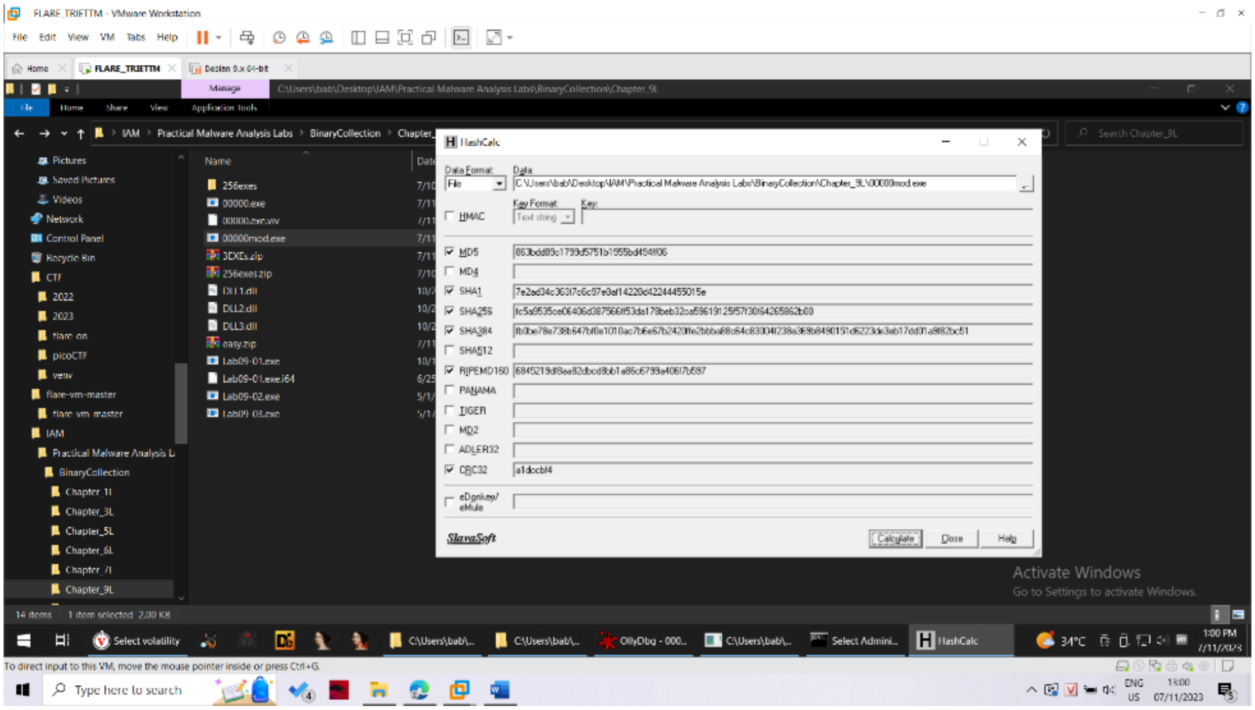
Paused


FLARE_TRIETTM - VMware Workstation
C:\Users\bab\Desktop\IAM\Practical Malware Analysis Labs\BinaryCollection\Chapter_9L
IAM > Practical Malware Analysis Labs > BinaryCollection > Chapter_9L
Search Chapter_9L
Administrator: C:\Windows\system32\cmd.exe
14 items
Activate Windows
Go to Settings to activate Windows.

Name	Date modified	Type
256exes	7/10/2023 4:03 PM	File folder
00000.exe	7/11/2023 9:54 AM	Application
00000.exe.viv	7/11/2023 12:47 PM	VIV File
00000mod.exe	7/11/2023 12:57 PM	Application
3CXEs.zip	7/11/2023 9:54 AM	WinRAR ZIP arch
256exes.zip	7/10/2023 4:03 PM	WinRAR ZIP arch
DLL1.dll	10/2/2011 3:25 AM	Application exte
DLL2.dll	10/2/2011 3:25 AM	Application exte
DLL3.dll	10/2/2011 3:26 AM	Application exte
easy.zip	7/11/2023 9:54 AM	WinRAR ZIP arch
Lab09-01.exe	10/19/2011 3:46 AM	Application
Lab09-01.exe.i64	6/25/2023 10:40 AM	I64 File
Lab09-02.exe	5/1/2011 8:24 AM	Application
Lab09-03.exe	5/17/2011 5:43 AM	Application

```
FLARE Tue 07/11/2023 12:58:35.44
C:\Users\bab\Desktop\IAM\Practical Malware Analysis Labs\BinaryCollection\Chapter_9L+>00000mod.exe
Launch codes?
1
Wow you got it. Here is the result: (J)

FLARE Tue 07/11/2023 12:58:42.10
C:\Users\bab\Desktop\IAM\Practical Malware Analysis Labs\BinaryCollection\Chapter_9L+>
```

Checking the Hash


HashCalc

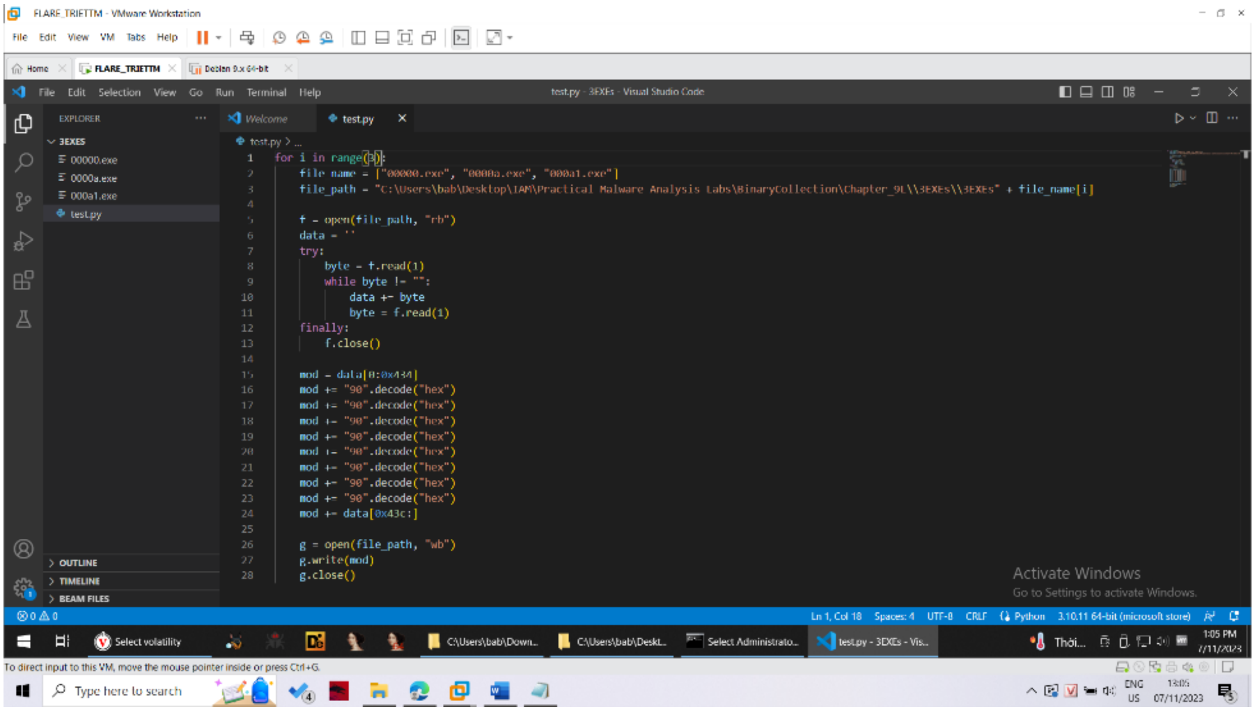
Data Format: File

Data: C:\Users\bab\Desktop\IAM\Practical Malware Analysis Labs\BinaryCollection\Chapter_9L\00000mod.exe

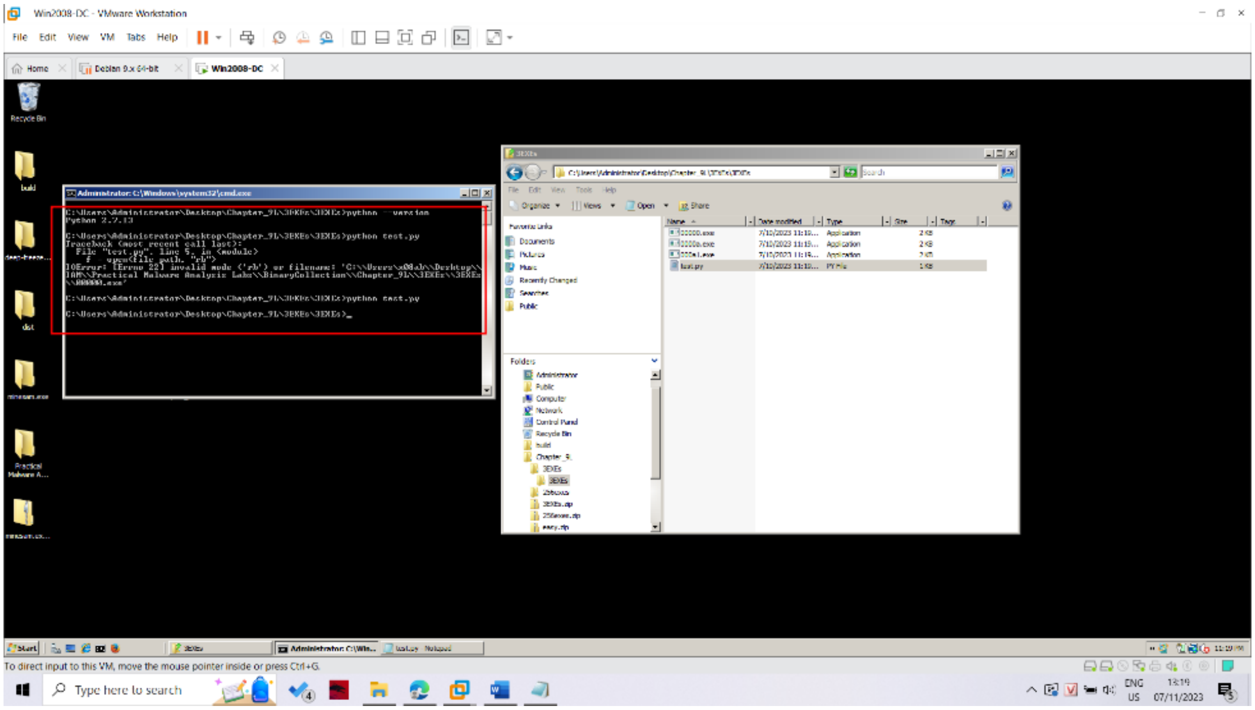
☐ HMAC Key Format: Text string Key:

☑ MD5 863bdd89c1799d5751b1955bd494ff06
☐ MD4
☑ SHA1 7e2ad34c363f7c6c97e9af14220d42244455015e
☑ SHA256 fc5a9535ce06406d387566ff53da178beb32ca59619125f57f30f64265862b00
☑ SHA384 fb0be78e738b647bf0e1010ac7b6e67b2420ffe2bbba88c64c83004f238a369b8490151d6223de3eb17dd01a9f82bc51
☐ SHA512
☑ RIPEMD160 6845219df8ea82dbcd8bb1a86c6799a406f7b597
☐ PANAMA
☐ TIGER
☐ MD2
☐ ADLER32
☑ CRC32 a1dccbf4
☐ eDonkey/eMule

Patching Three EXEs


test.py - 3EXEs - Visual Studio Code

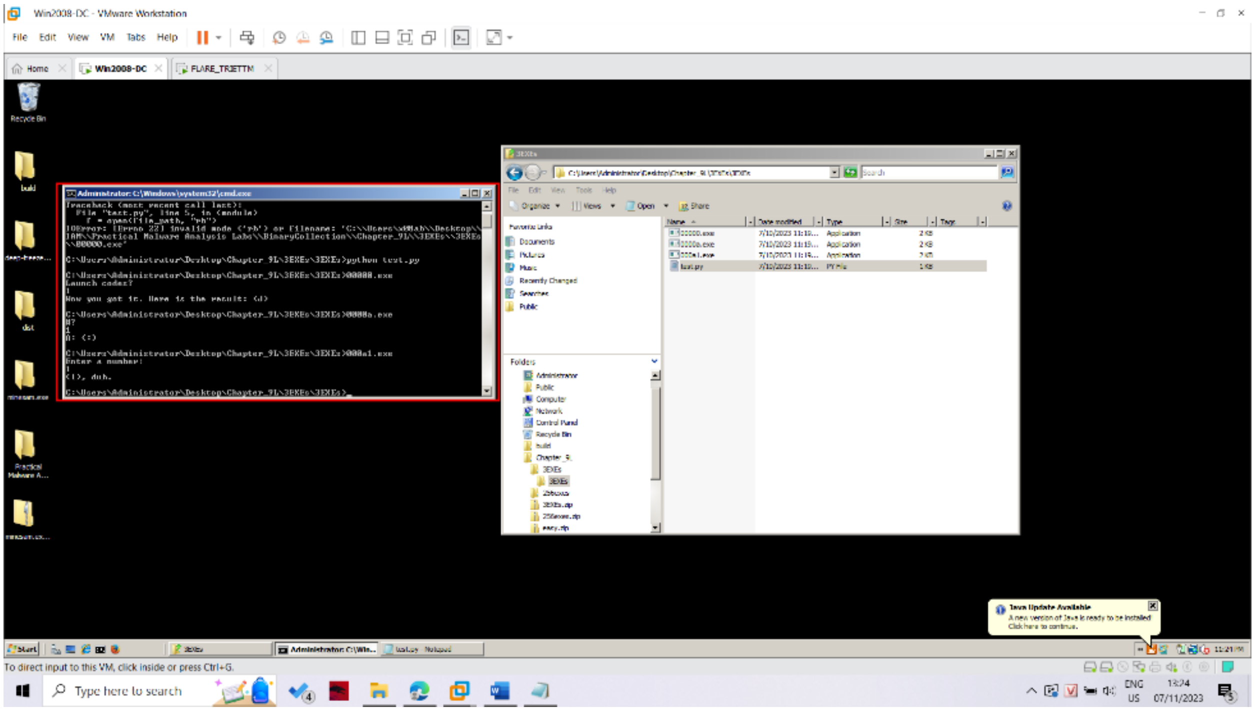
```python
for i in range(3):
    file_name = ["00000.exe", "0000a.exe", "000a1.exe"]
    file_path = "C:\Users\bab\Desktop\IAM\Practical Malware Analysis Labs\BinaryCollection\Chapter_9L\\3EXEs\\3EXEs" + file_name[i]

    f = open(file_path, "rb")
    data = ''
    try:
        byte = f.read(1)
        while byte != "":
            data += byte
            byte = f.read(1)
    finally:
        f.close()

    mod = data[0:0x434]
    mod += "90".decode("hex")
    mod += "90".decode("hex")
    mod += "90".decode("hex")
    mod += "90".decode("hex")
    mod += "90".decode("hex")
    mod += "90".decode("hex")
    mod += "90".decode("hex")
    mod += "90".decode("hex")
    mod += data[0x43c:]

    g = open(file_path, "wb")
    g.write(mod)
    g.close()
```



Win2008-DC - VMware Workstation
File Edit View VM Tabs Help
Home
Debian 9.x 64-bit
Win2008-DC
Administrator: C:\Windows\system32\cmd.exe
3EXEs
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG US
13:19
07/11/2023

```
C:\Users\Administrator\Desktop\Chapter_9L\3EXEs\3EXEs>python --version
Python 2.7.13

C:\Users\Administrator\Desktop\Chapter_9L\3EXEs\3EXEs>python test.py
Traceback (most recent call last):
  File "test.py", line 5, in <module>
    f = open(file_path, "rb")
IOError: [Errno 22] invalid mode ('rb') or filename: 'C:\\Users\\x08ab\\Desktop\\
IAM\\Practical Malware Analysis Labs\\BinaryCollection\\Chapter_9L\\3EXEs\\3EXEs
\\00000.exe'

C:\Users\Administrator\Desktop\Chapter_9L\3EXEs\3EXEs>python test.py

C:\Users\Administrator\Desktop\Chapter_9L\3EXEs\3EXEs>_
```

Name	Date modified	Type	Size
00000.exe	7/10/2023 11:19...	Application	2 KB
0000a.exe	7/10/2023 11:19...	Application	2 KB
000a1.exe	7/10/2023 11:19...	Application	2 KB
test.py	7/10/2023 11:18...	PY File	1 KB

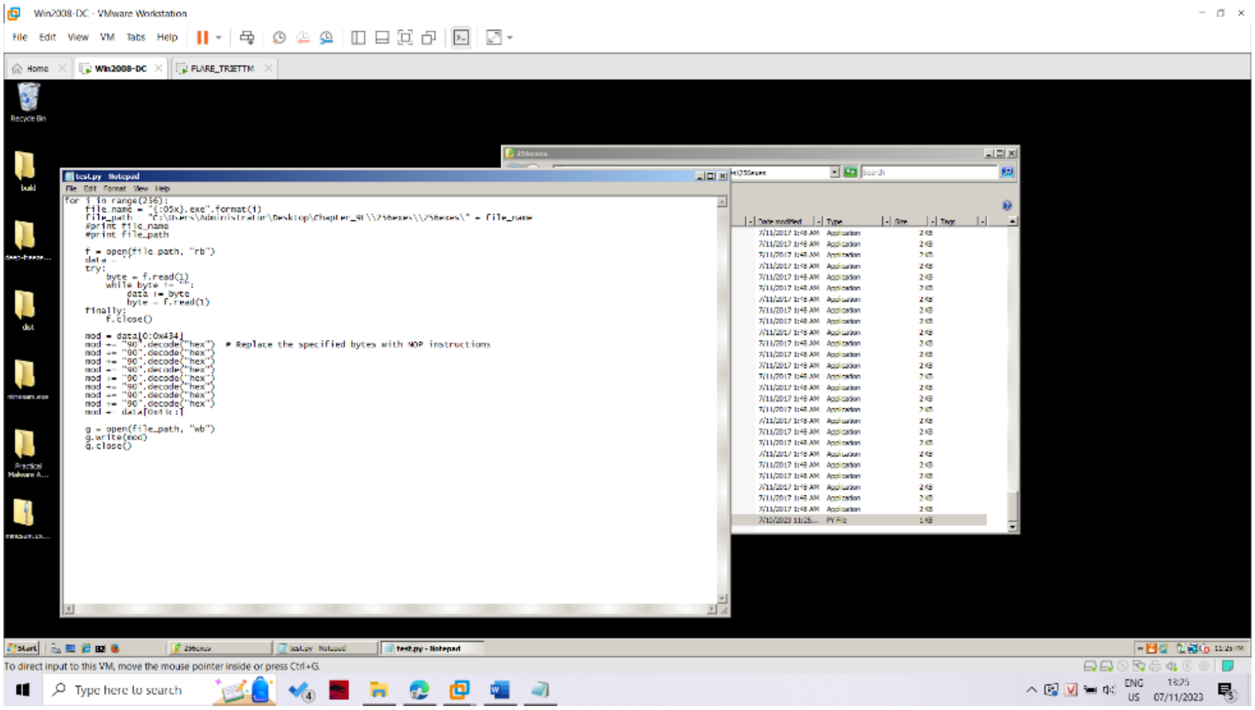


Win2008-DC - VMware Workstation
File Edit View VM Tabs Help
Home
Win2008-DC
FLARE_TRIETTM
Administrator: C:\Windows\system32\cmd.exe
3EXEs
Java Update Available
A new version of Java is ready to be installed
Click here to continue.
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
ENG US
13:24
07/11/2023

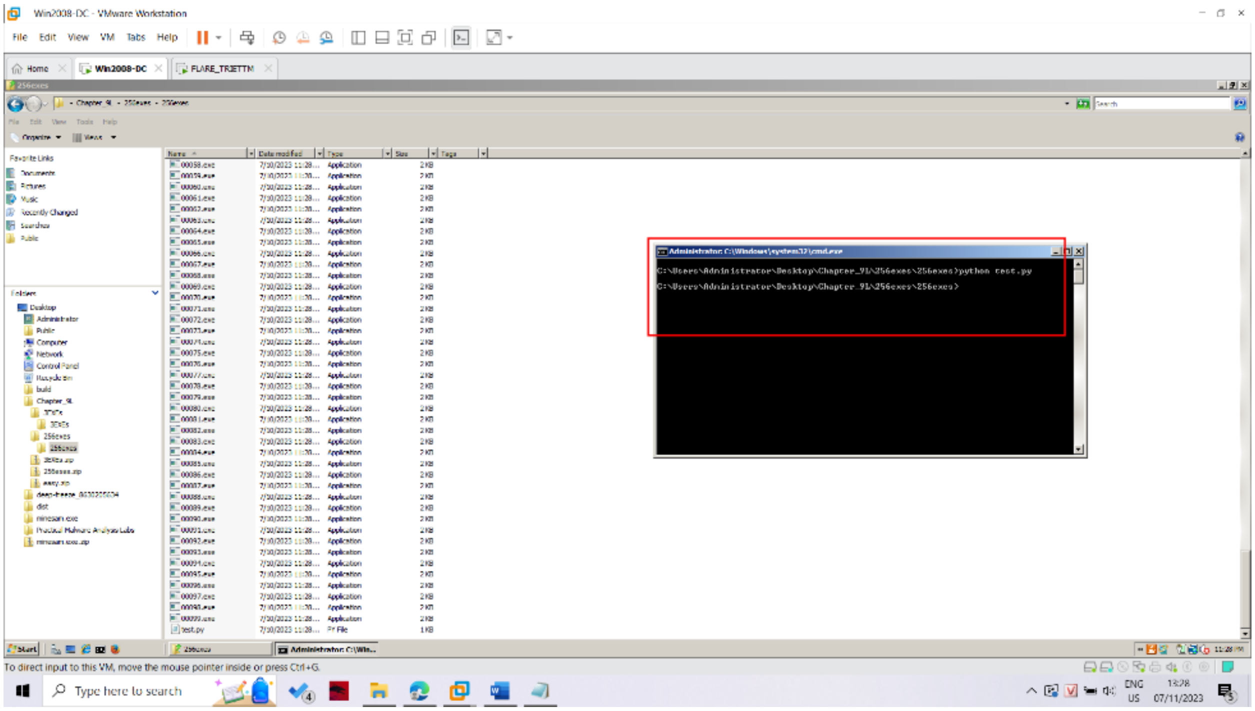
```
Traceback (most recent call last):
  File "test.py", line 5, in <module>
    f = open(file_path, "rb")
IOError: [Errno 22] invalid mode ('rb') or filename: 'C:\\Users\\x08ab\\Desktop\\
IAM\\Practical Malware Analysis Labs\\BinaryCollection\\Chapter_9L\\3EXEs\\3EXEs
\\00000.exe'

C:\Users\Administrator\Desktop\Chapter_9L\3EXEs\3EXEs>python test.py

C:\Users\Administrator\Desktop\Chapter_9L\3EXEs\3EXEs>00000.exe
Launch codes?
1
Now you got it. Here is the result: (d)

C:\Users\Administrator\Desktop\Chapter_9L\3EXEs\3EXEs>0000a.exe
H?
1
A: (:)

C:\Users\Administrator\Desktop\Chapter_9L\3EXEs\3EXEs>000a1.exe
Enter a number!
1
(1), duh.

C:\Users\Administrator\Desktop\Chapter_9L\3EXEs\3EXEs>_
```

Name	Date modified	Type	Size
00000.exe	7/10/2023 11:19...	Application	2 KB
0000a.exe	7/10/2023 11:19...	Application	2 KB
000a1.exe	7/10/2023 11:19...	Application	2 KB
test.py	7/10/2023 11:18...	PY File	1 KB

Patching 256 EXEs



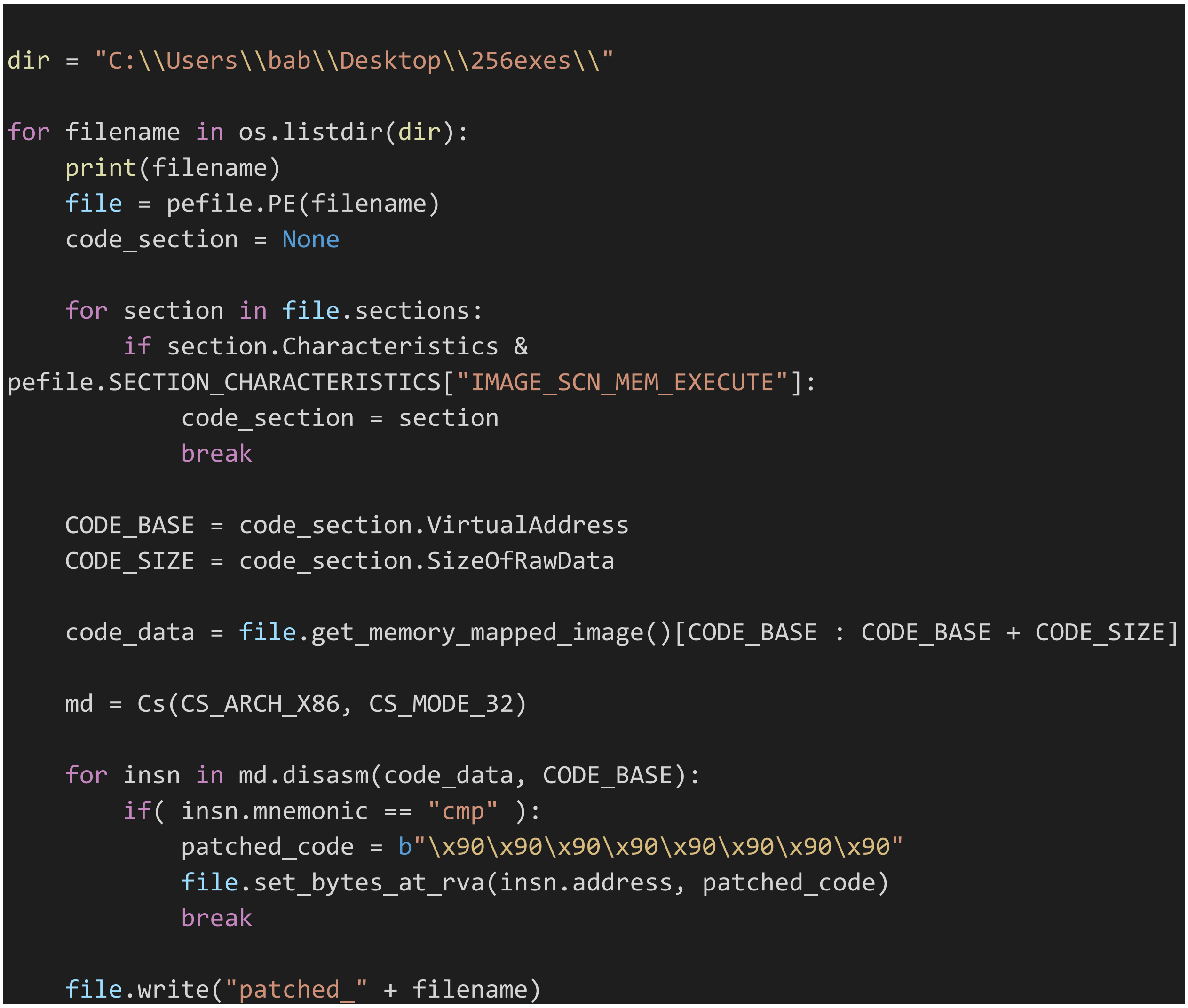
```
for i in range(256):
    file_name = "{:05x}.exe".format(i)
    file_path = "C:\Users\Administrator\Desktop\Chapter_9L\\256exes\\256exes\" + file_name
    #print file_name
    #print file_path

    f = open(file_path, "rb")
    data = ''
    try:
        byte = f.read(1)
        while byte != "":
            data += byte
            byte = f.read(1)
    finally:
        f.close()

    mod = data[0:0x434]
    mod += "90".decode("hex")  # Replace the specified bytes with NOP instructions
    mod += "90".decode("hex")
    mod += "90".decode("hex")
    mod += "90".decode("hex")
    mod += "90".decode("hex")
    mod += "90".decode("hex")
    mod += "90".decode("hex")
    mod += "90".decode("hex")
    mod += data[0x43c:]

    g = open(file_path, "wb")
    g.write(mod)
    g.close()
```


Win2008-DC - VMware Workstation
256exes
Administrator: C:\Windows\system32\cmd.exe

```
C:\Users\Administrator\Desktop\Chapter_9L\256exes\256exes>python test.py

C:\Users\Administrator\Desktop\Chapter_9L\256exes\256exes>
```

Because 256 file have the different offset, so we have to scripting a bit difficult to patch. I use following script

```
import os
import pefile
from capstone import *
from capstone.x86 import *
```



```
dir = "C:\\Users\\bab\\Desktop\\256exes\\"

for filename in os.listdir(dir):
    print(filename)
    file = pefile.PE(filename)
    code_section = None

    for section in file.sections:
        if section.Characteristics &
pefile.SECTION_CHARACTERISTICS["IMAGE_SCN_MEM_EXECUTE"]:
            code_section = section
            break

    CODE_BASE = code_section.VirtualAddress
    CODE_SIZE = code_section.SizeOfRawData

    code_data = file.get_memory_mapped_image()[CODE_BASE : CODE_BASE + CODE_SIZE]

    md = Cs(CS_ARCH_X86, CS_MODE_32)

    for insn in md.disasm(code_data, CODE_BASE):
        if( insn.mnemonic == "cmp" ):
            patched_code = b"\x90\x90\x90\x90\x90\x90\x90\x90"
            file.set_bytes_at_rva(insn.address, patched_code)
            break

    file.write("patched_" + filename)
```

Using above script then all file will corectly patched.