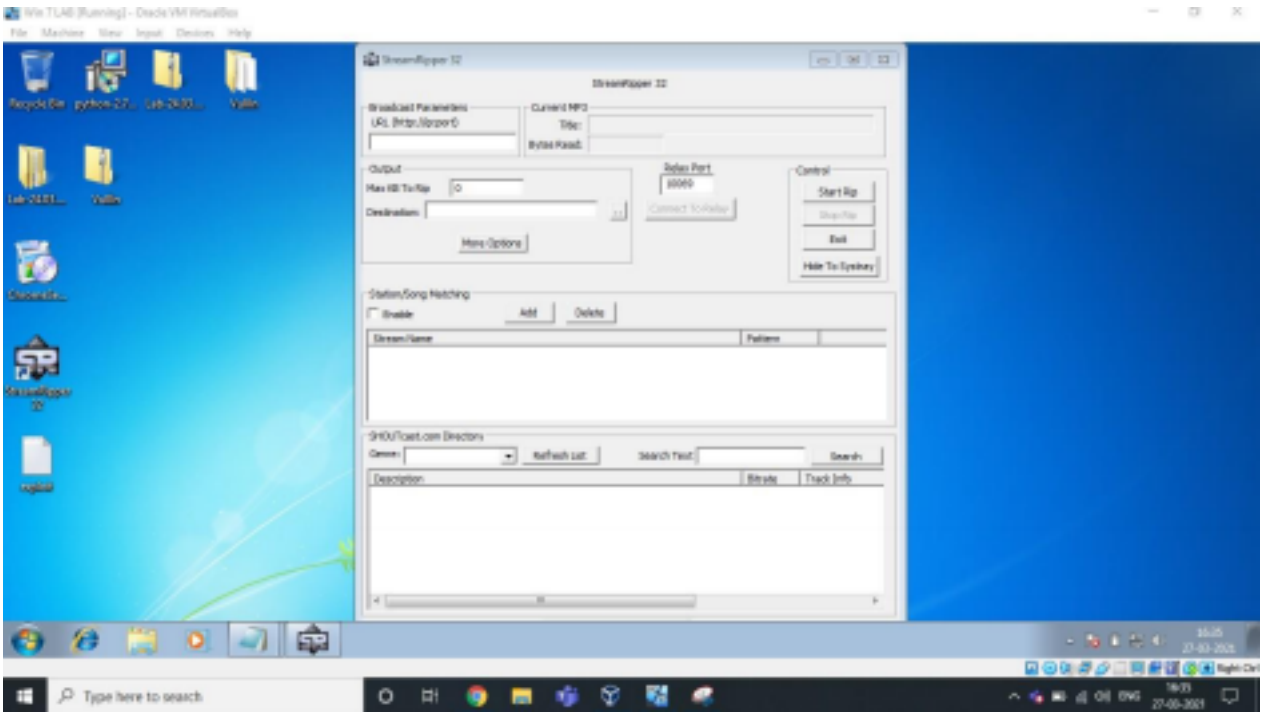
Name:K.Jai Shankar
Reg No:18bcd7075

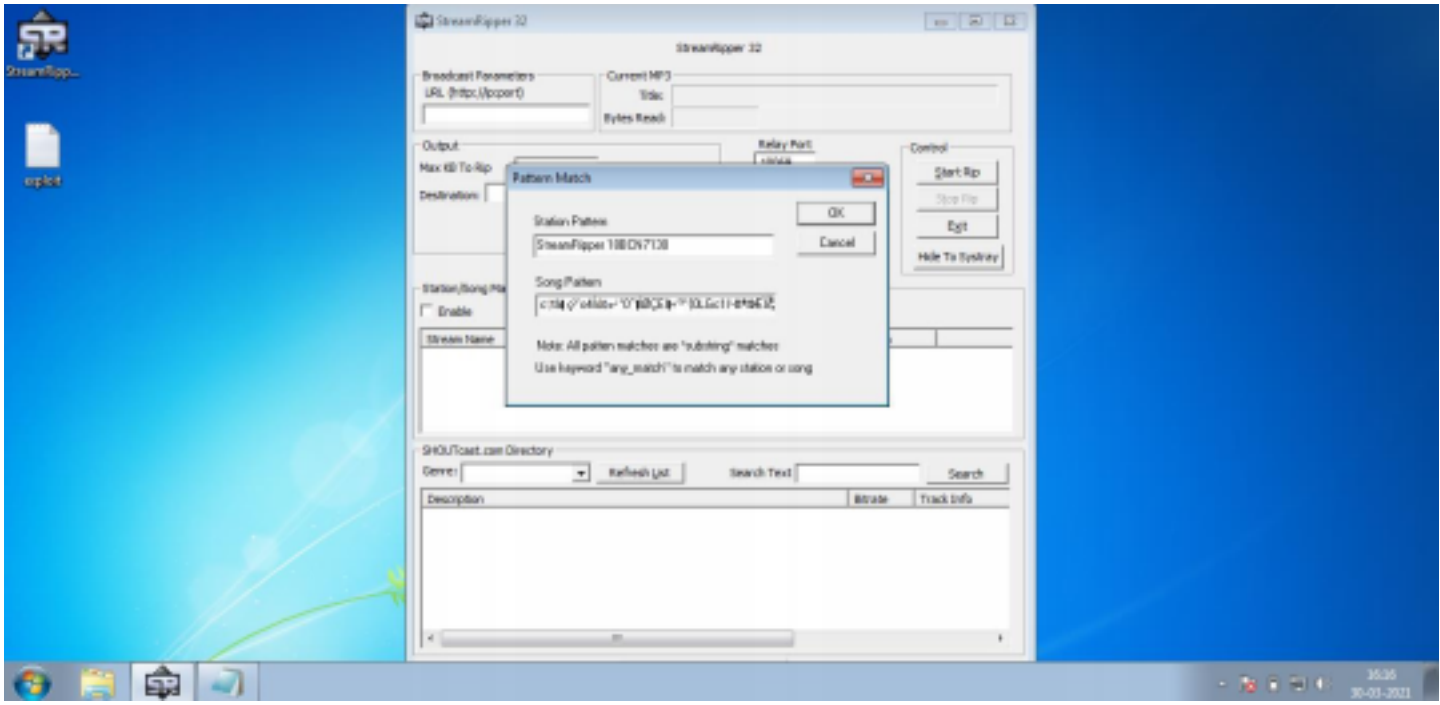
Working with the memory vulnerabilities

1) Crashing the StreamRipper32



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

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



Pattern Match

OK

Station Pattern

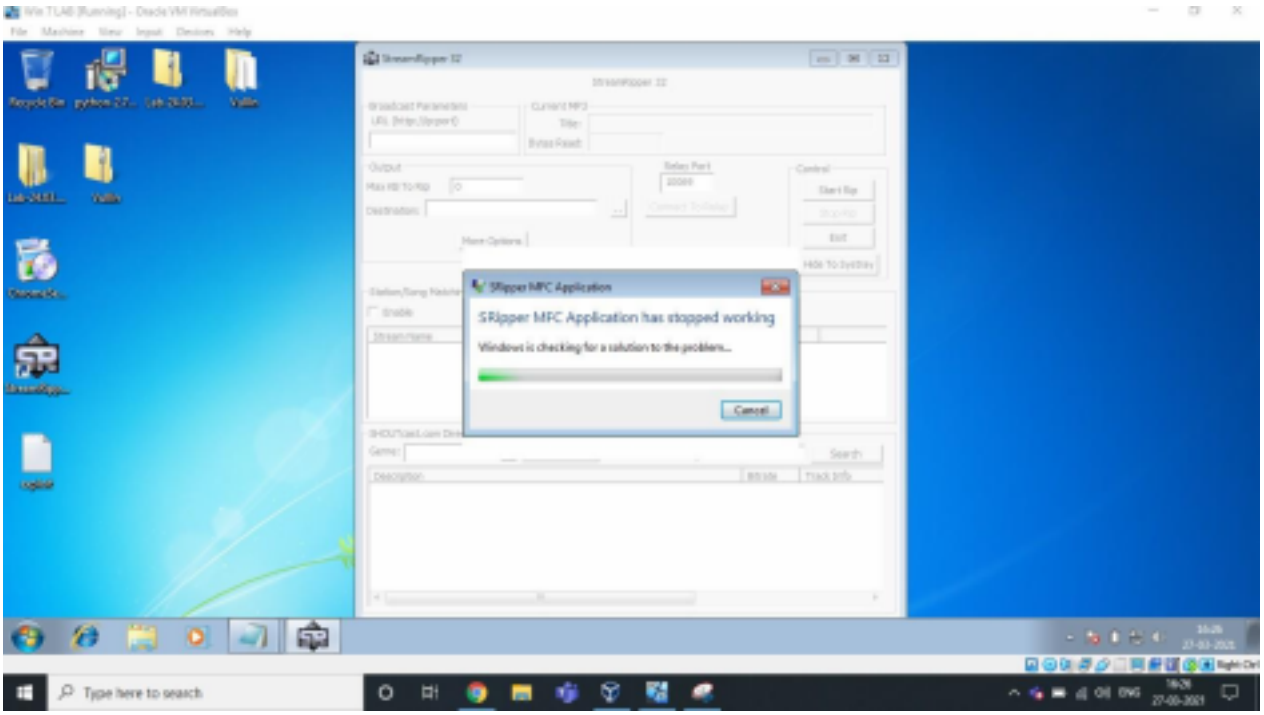
18BCD7075 Cancel

Song Pattern

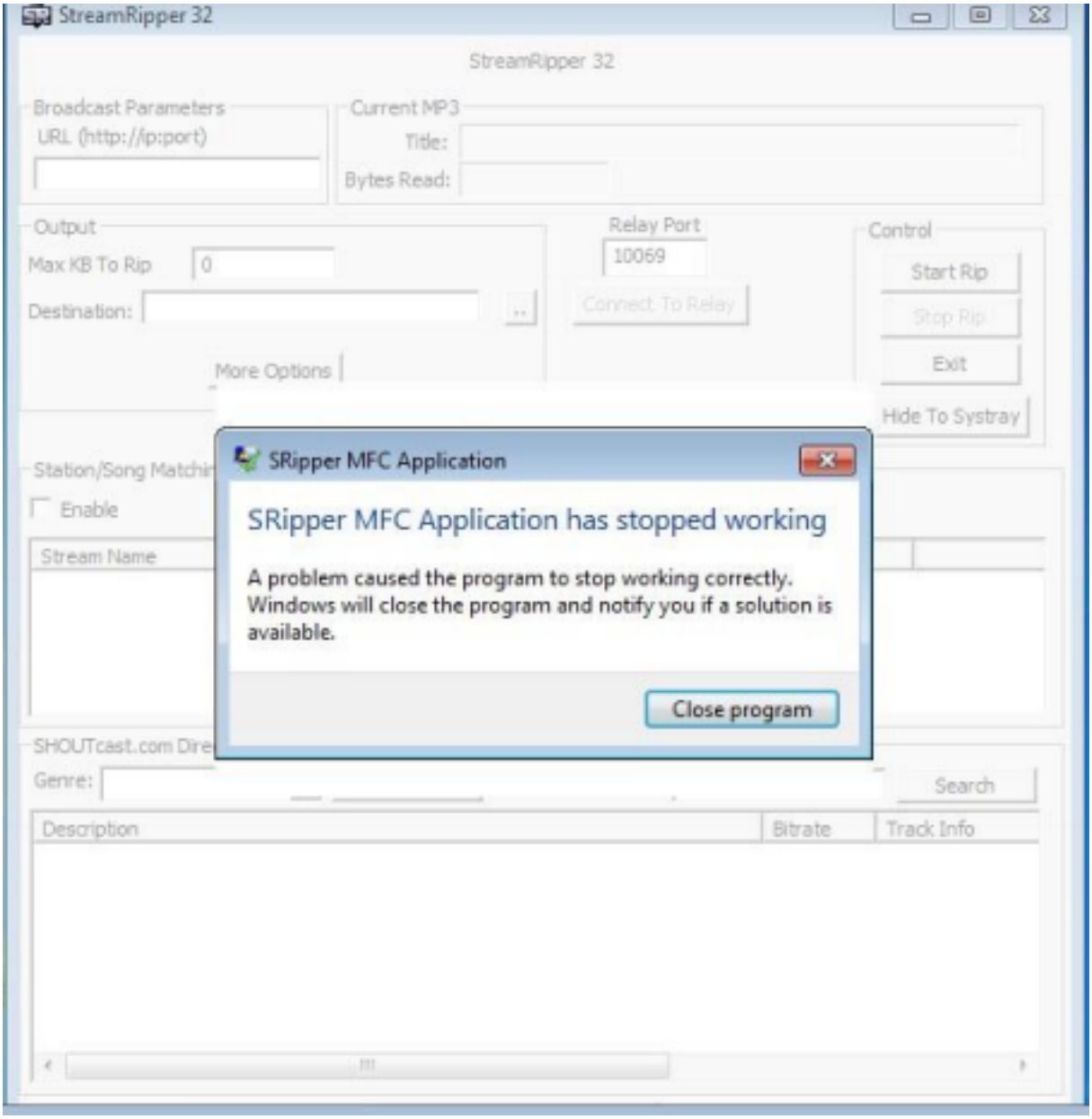
canal o4l e ”0°l l<SEll-”” (0LGc1l-tt°Wlb

Note: All patten matches are "substring" matches

Usekeyword"any_match" tomatchany stationor song



Here is the Exploit used above.



As we can see, it's crashed.

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 is crashed.