Name:M.Jai Sai Venkatesh Reddy

Regno.:18BCN7109

Slot:L39+40

Running the exploit.py file to generate payload
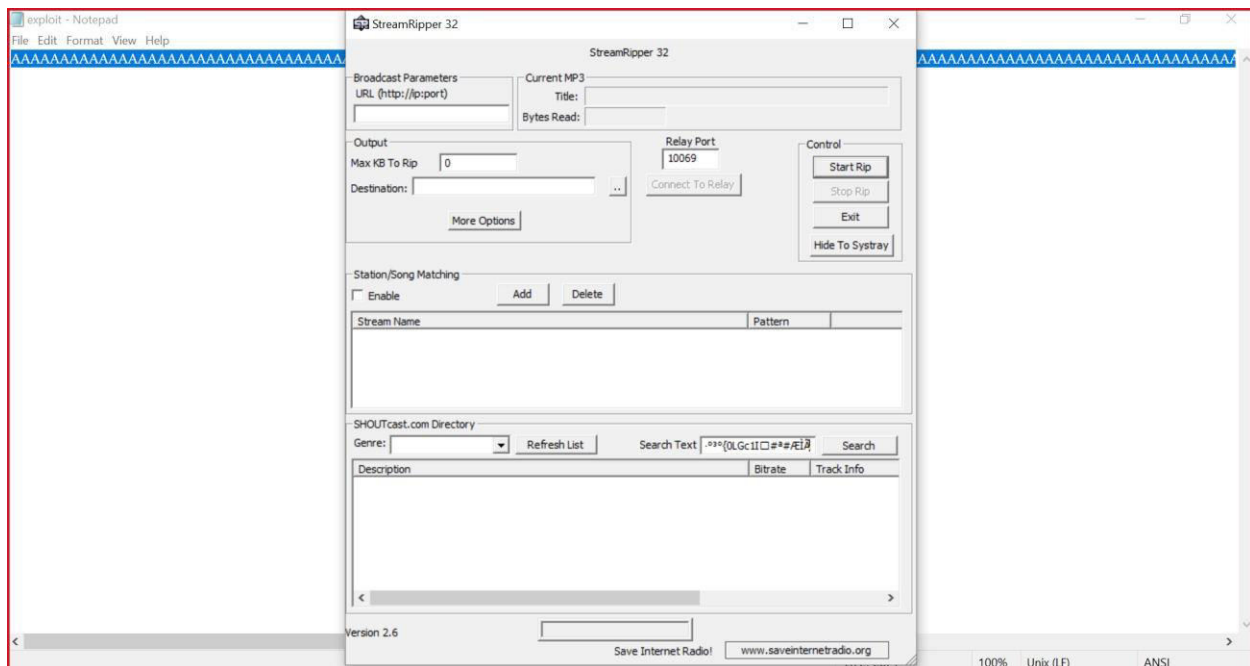
>python2exploit.py

After successfully running the python file it will generate a.txt file along with the payload.

>notepad exploit.txt

Now, install **Vulnerable application (StreamRipper 32).**

After installing the application copy paste the payload in the search box and click on Search button.
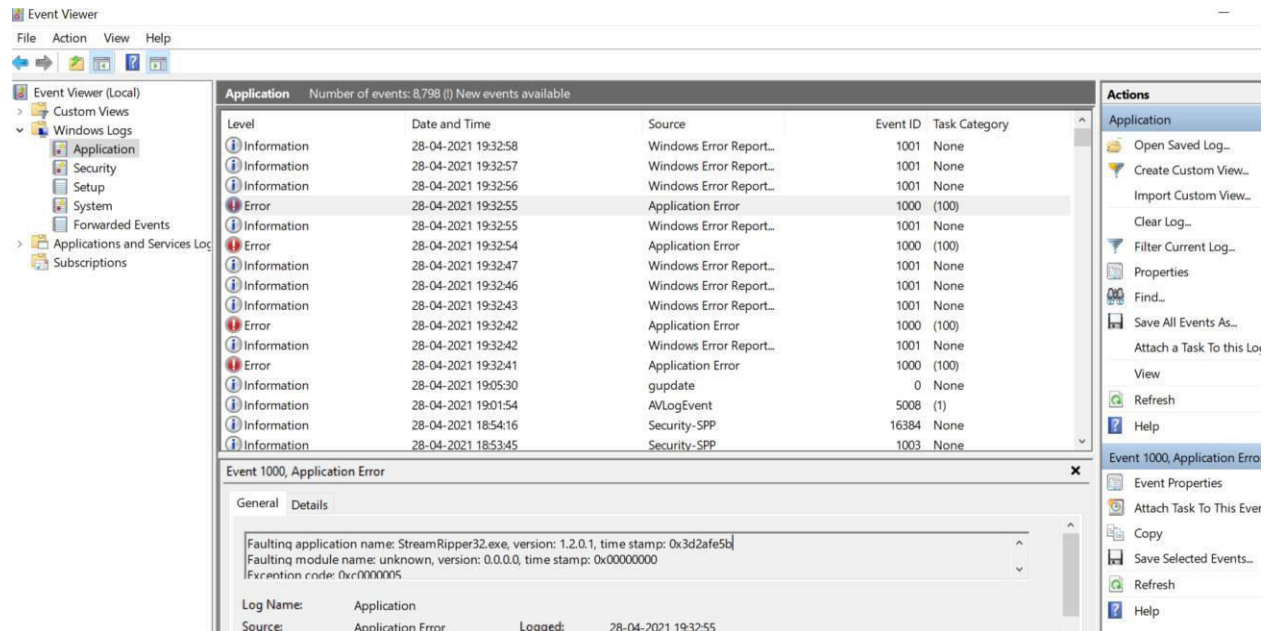

By exploiting buffer overflow vulnerabilitiy we have crashed the application.
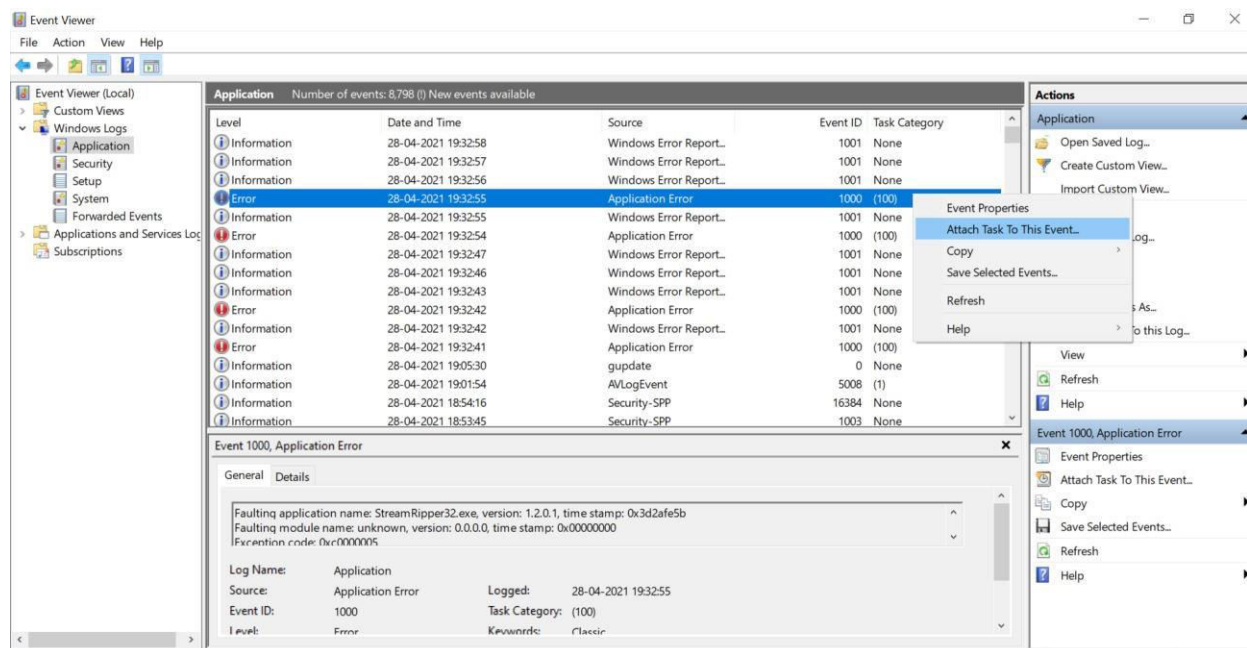
Name:M.Jai Sai Venkatesh Reddy

Regno.:18BCN7109

Slot:L39+40

Aftertheapplicationcrashes,gotoeventviewer.

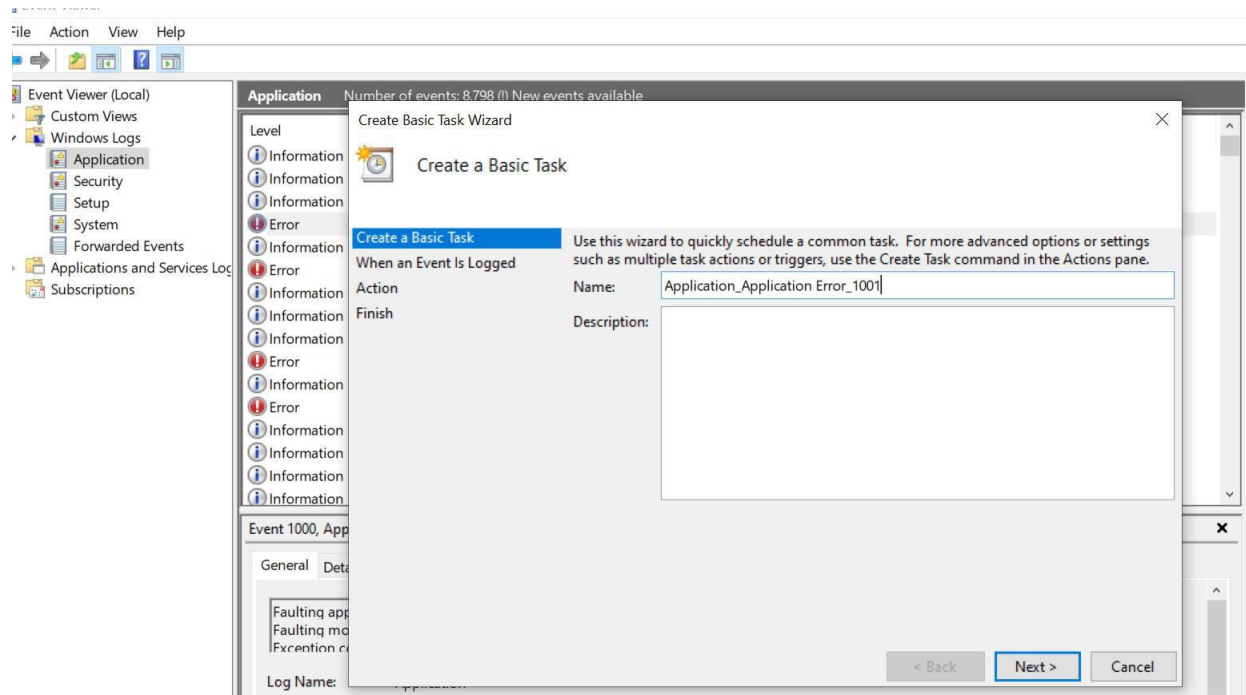

Rightclickontheerrorandselectattachtasktothisevent.

Name:M.Jai Sai Venkatesh Reddy

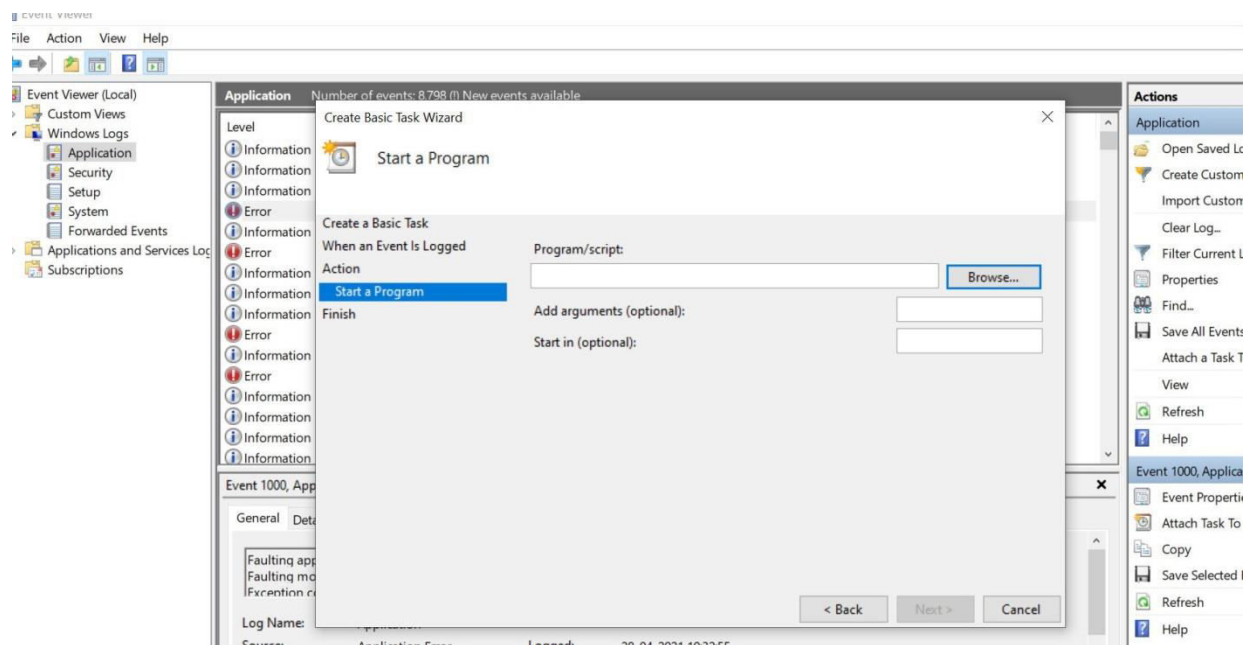**Regno.:18BCN7109**

Slot:L39+40

Now,createthetask.

Browsetheresultantprogrami.ecalc.exe.
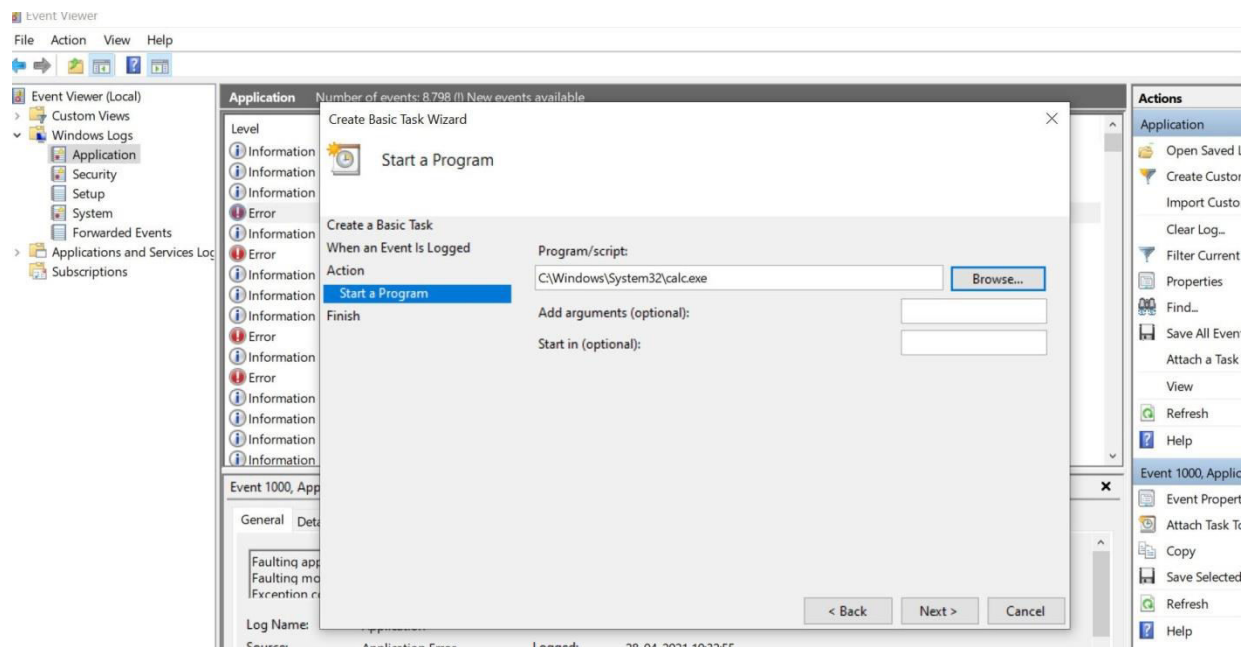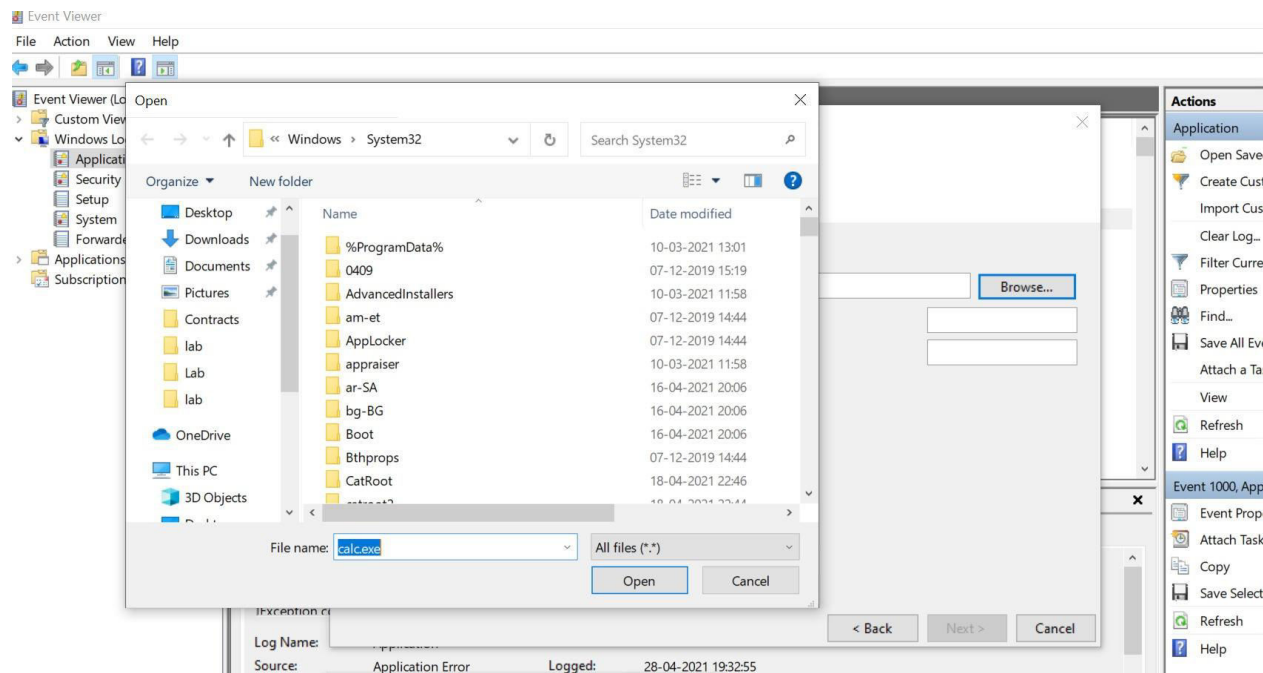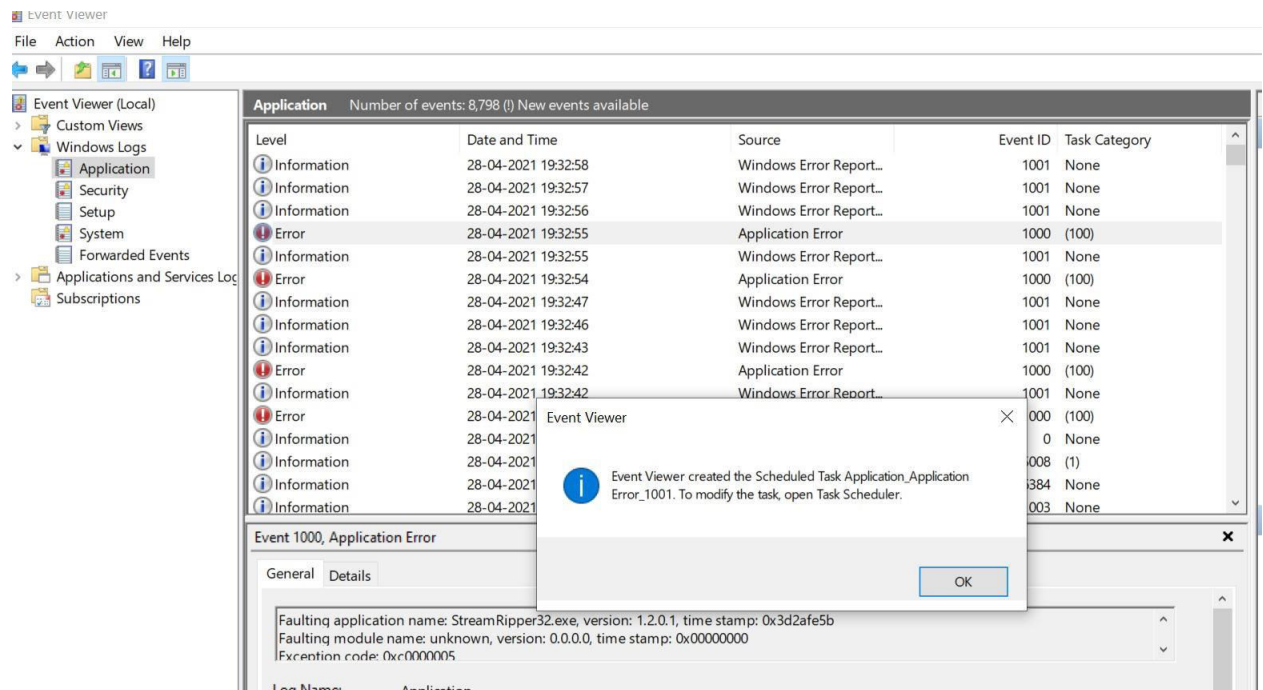
Name:M.Jai Sai Venkatesh Reddy

Regno.:18BCN7109

Slot:L39+40

Next,weputincalc.exe asdefaulttriggeroncrashanditopensup,asprogrammed.

Name:M.Jai Sai Venkatesh Reddy
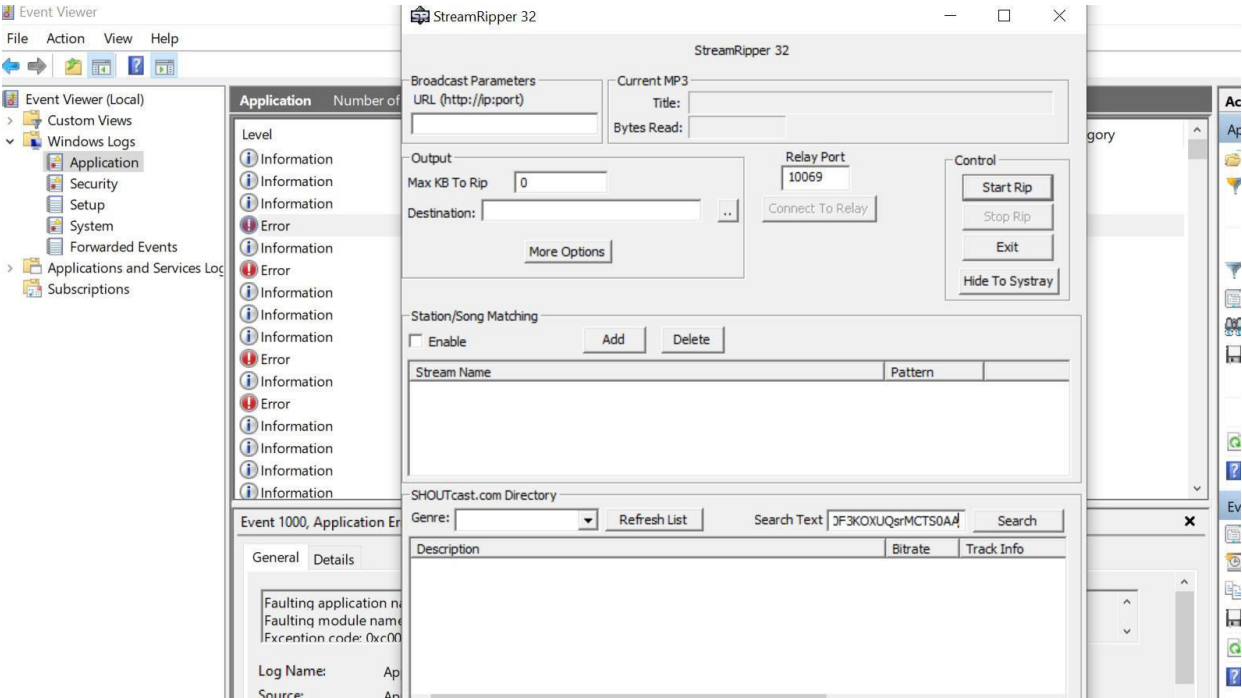
Regno.:18BCN7109

 Slot:L39+40

Succefullytaskhasbeencreated.NowagainputthepayloadinStreamRipperApplication.The nCalculatorisopened.
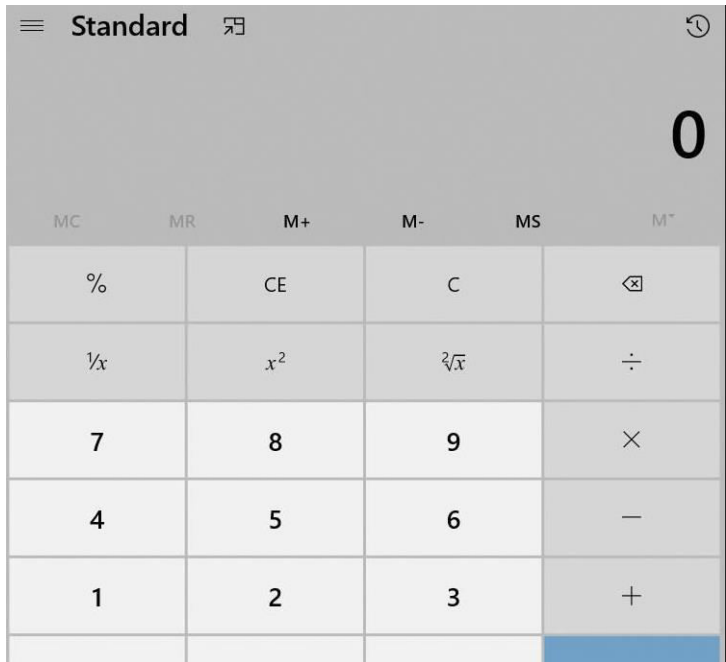
Name:M.Jai Sai Venkatesh Reddy

Regno.:18BCN7109

Slot:L39+40

Presently,totriggeranoccasionofourdecisionwhensomethingoccurs,wecando
assuchbyexaminingaportionoftheoccasionlogs

Eachoccasionhasitsownfixedpropertiesandcontrollers.AtthepointwhenStreamAppisslam
med,anApplication mistakeisproducedand itgetsputawayinthelogwithallitsdata.

Name:M.Jai Sai Venkatesh Reddy

Regno.:18BCN7109

Slot:L39+40