

**Name: Devi Jagannadh Kotha**

**Reg no.: 18BCN7079**

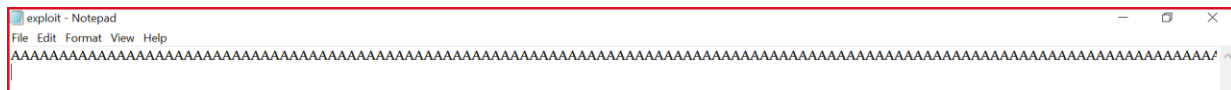
---

### Running the exploit2.py file to generate payload

>python2 exploit2.py

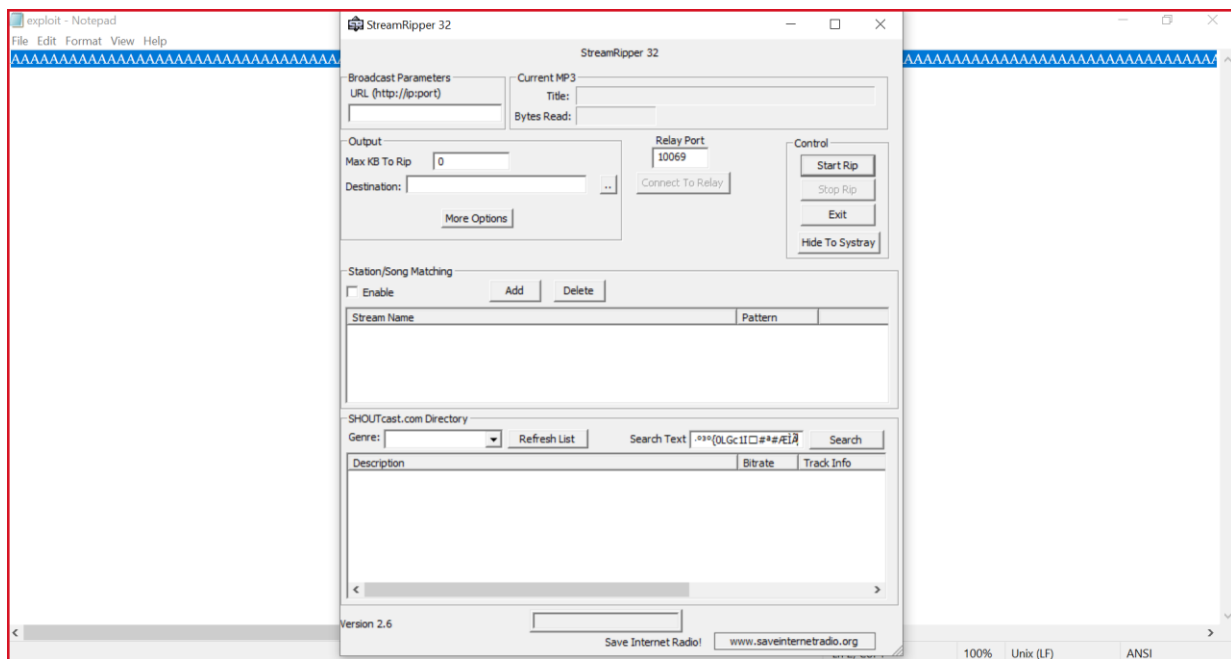
After successfully running the python file it will generate a .txt file along with the payload.

>notepad exploit.txt



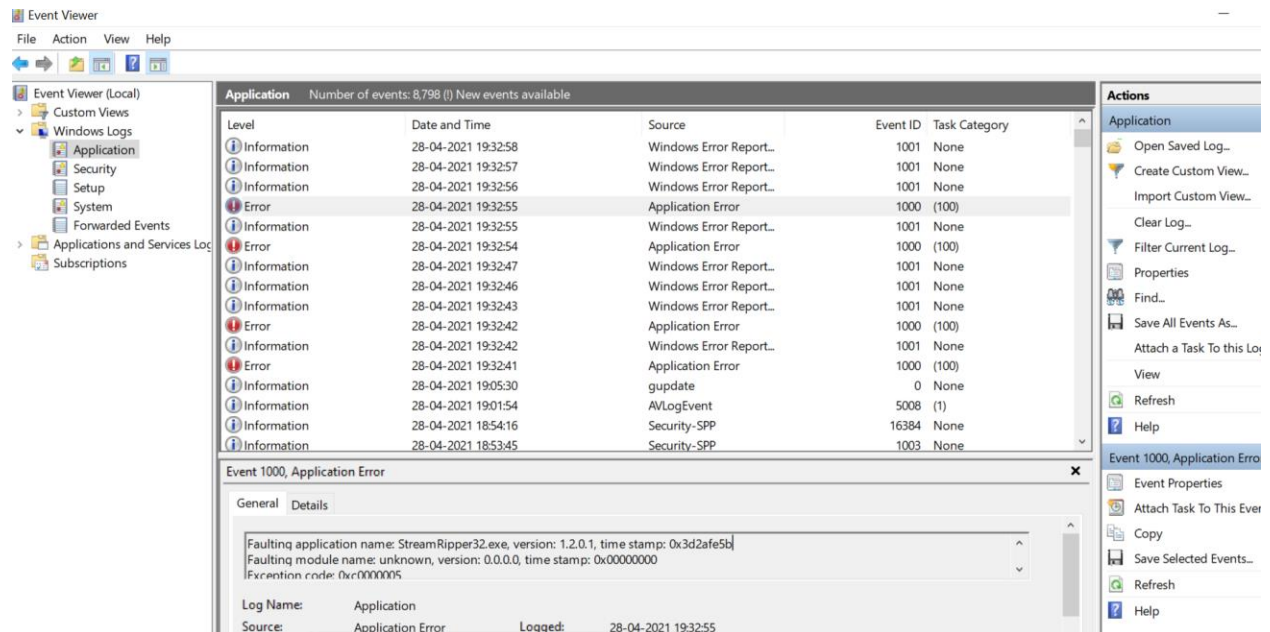
Now, install **Vulnerable application (StreamRipper32)**.

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

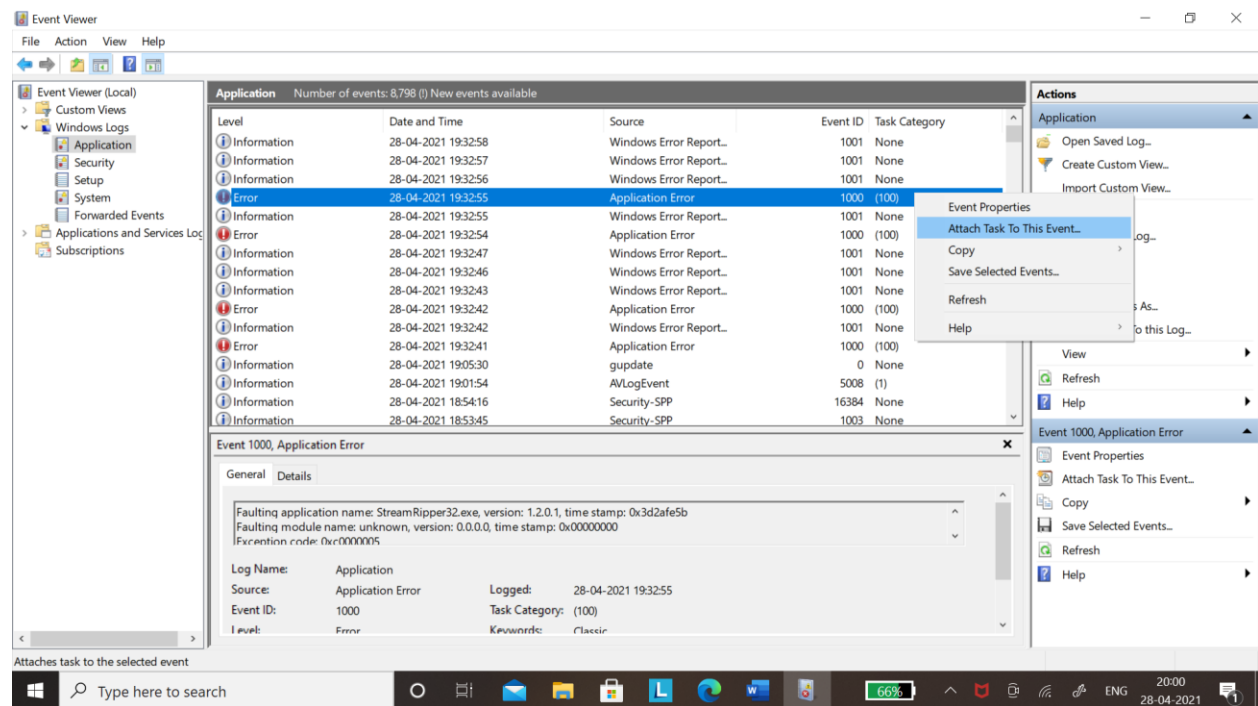


**By exploiting buffer overflow vulnerability we have crashed the application.**

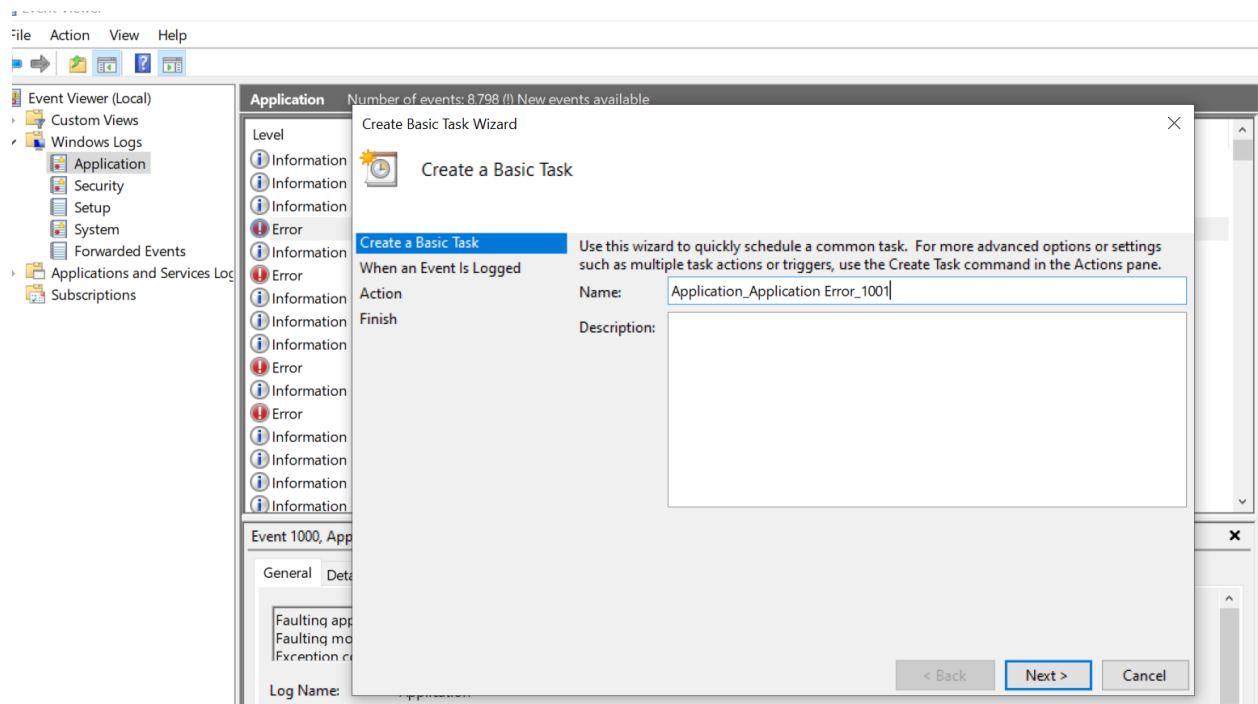
After the application crashes, go to event viewer.



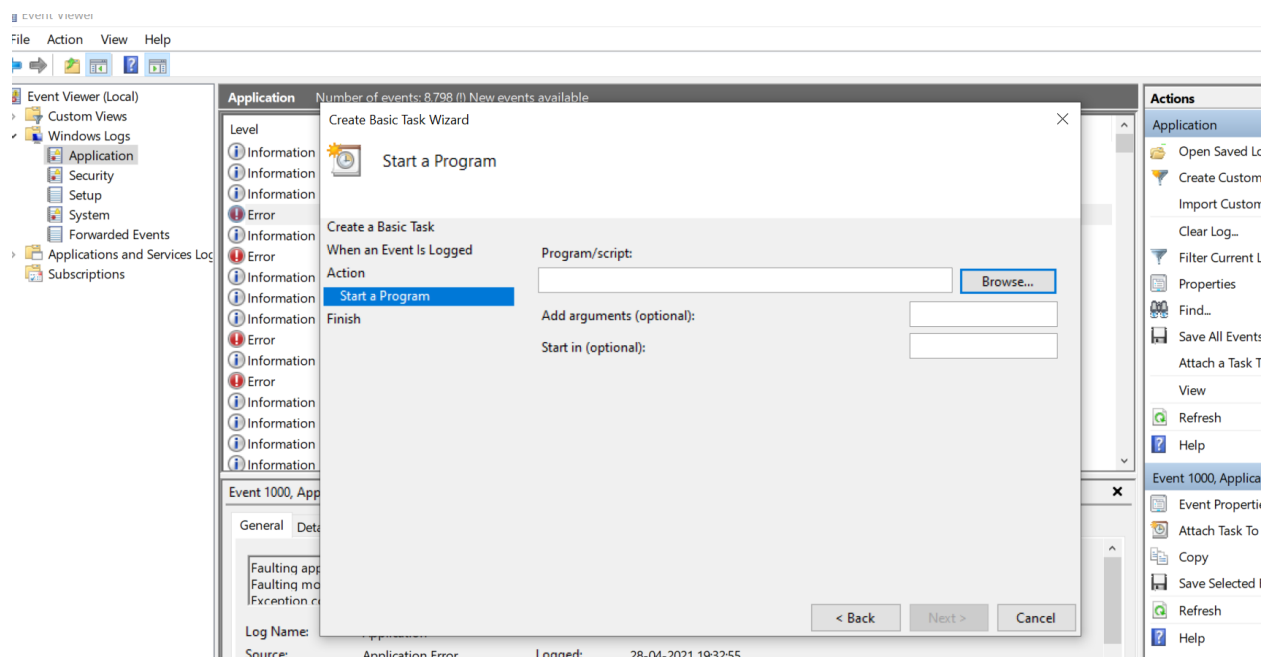
Right click on the error and select attach task to this event.



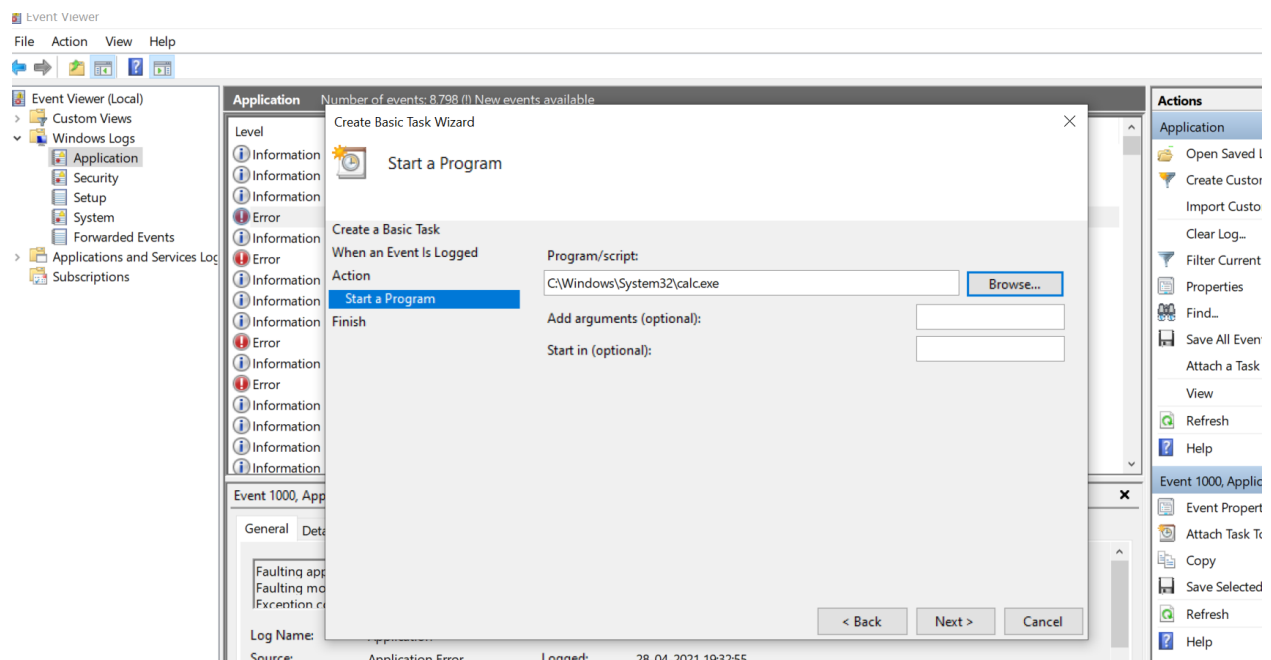
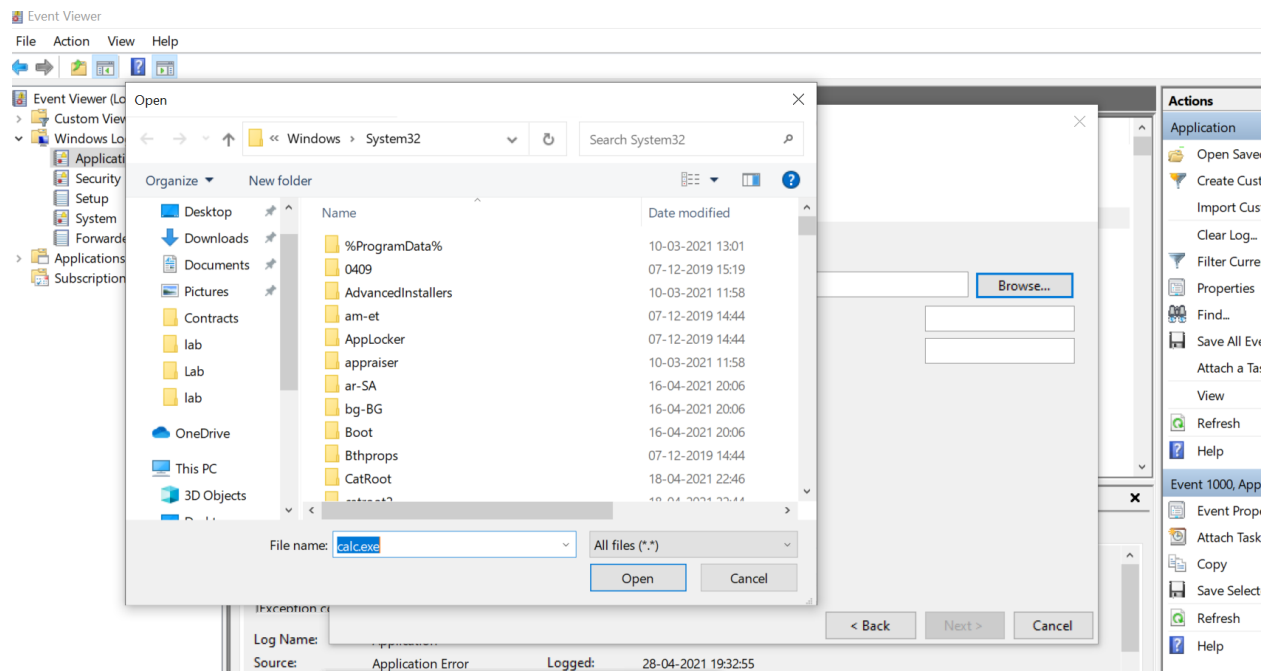
Now, create the task.

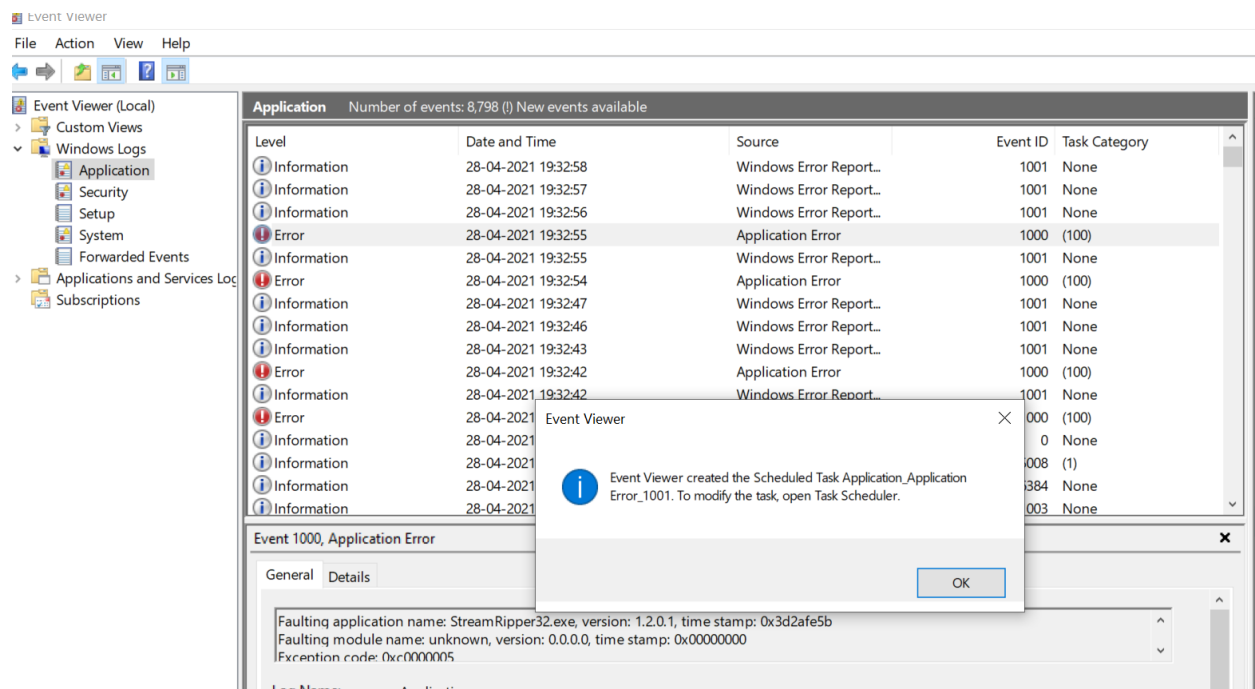
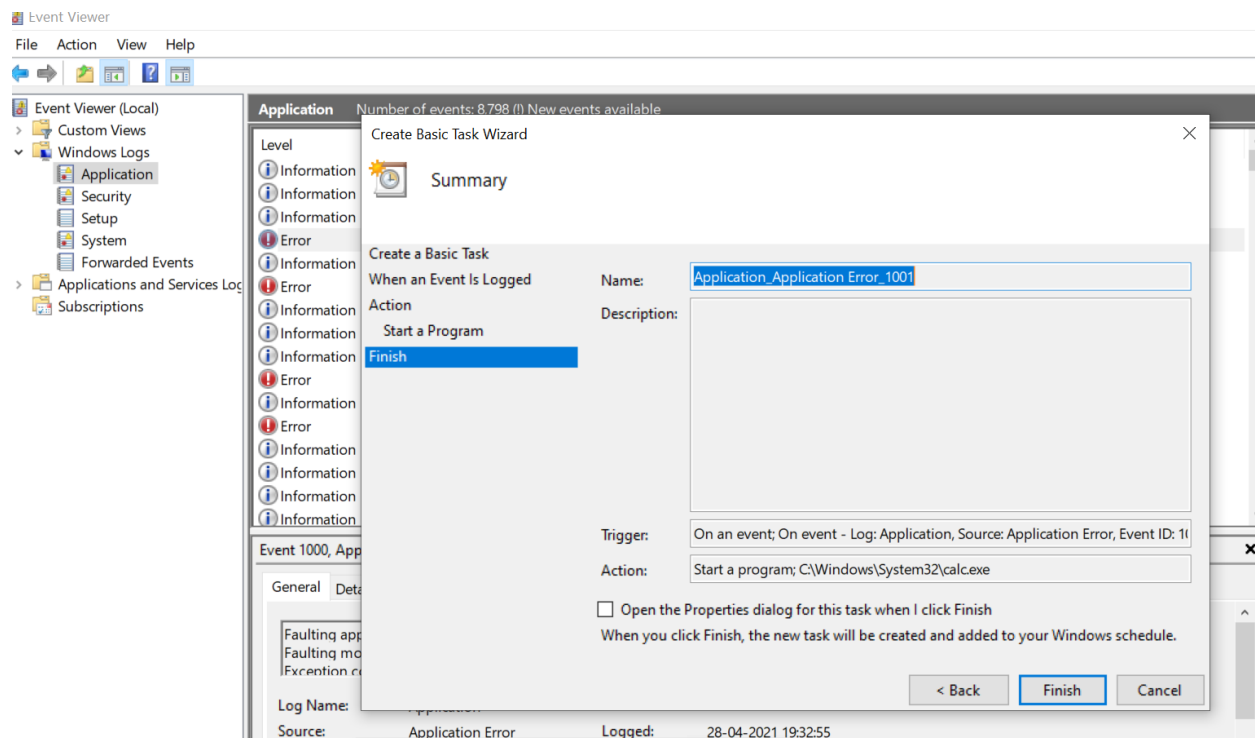


Browse the resultant program i.e calc.exe.

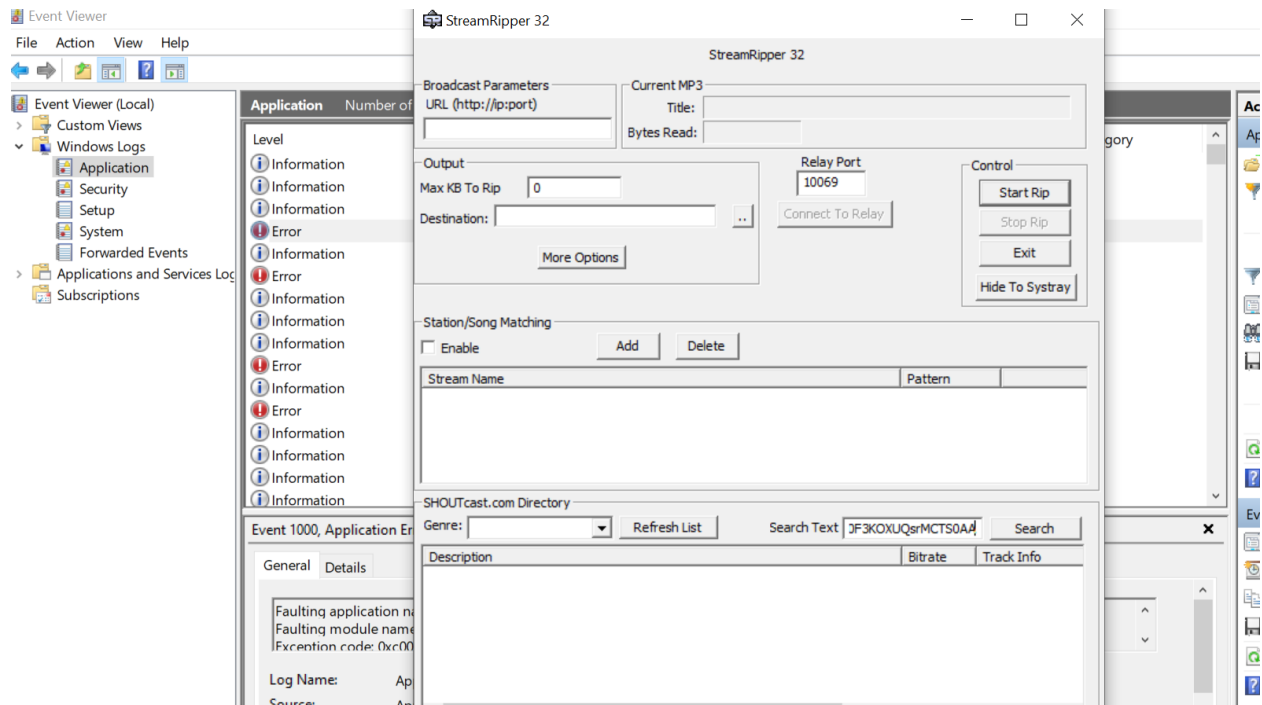


Next, we put in calc.exe as default trigger on crash and it opens up, as programmed.





**Succesfully task has been created. Now again put the payload in StreamRipper Application. Then Calculator is opened.**



Presently, to trigger an occasion of our decision when something occurs, we can do as such by examining a portion of the occasion logs

Each occasion has its own fixed properties and controllers. At the point when Stream App is slammed, an Application mistake is produced and it gets put away in the log with all its data.

