Secure Coding Lab-8

S.Poojith

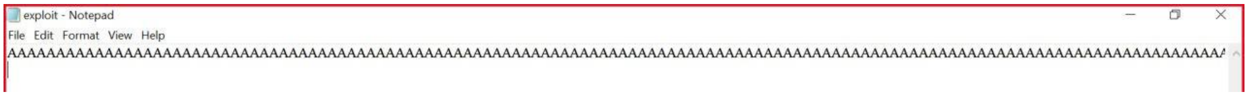
18BCN7032

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.

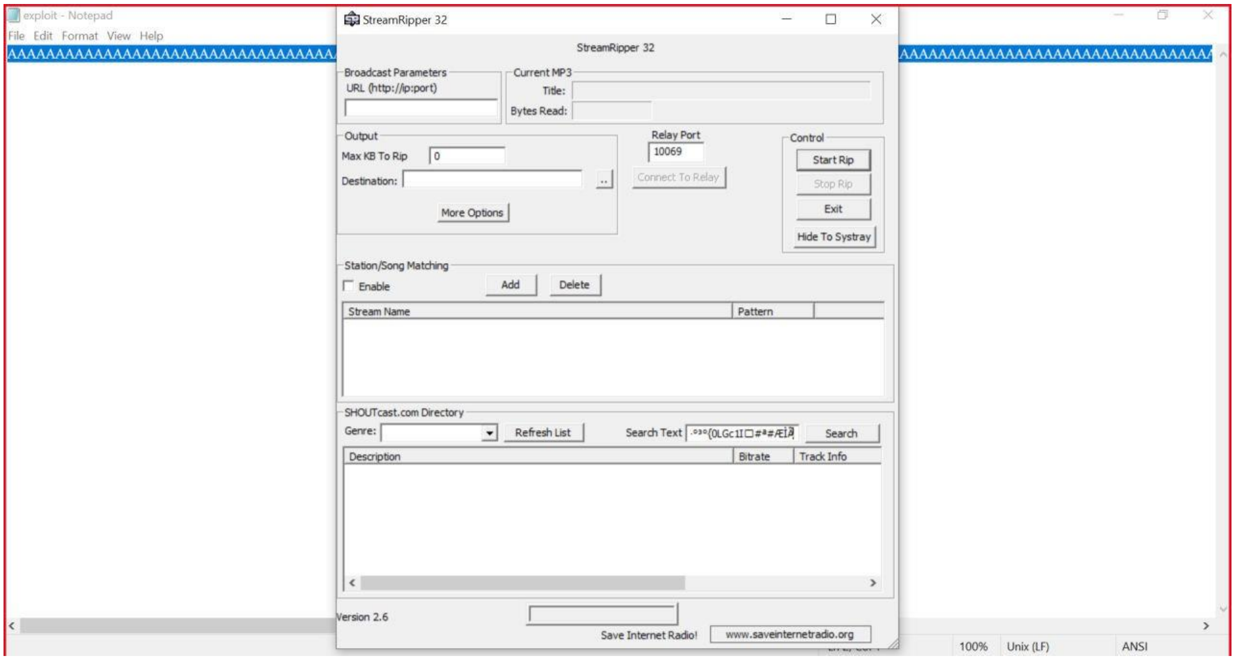
```
>notepad exploit.txt
```



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

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

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



Max KB To Rip: 0

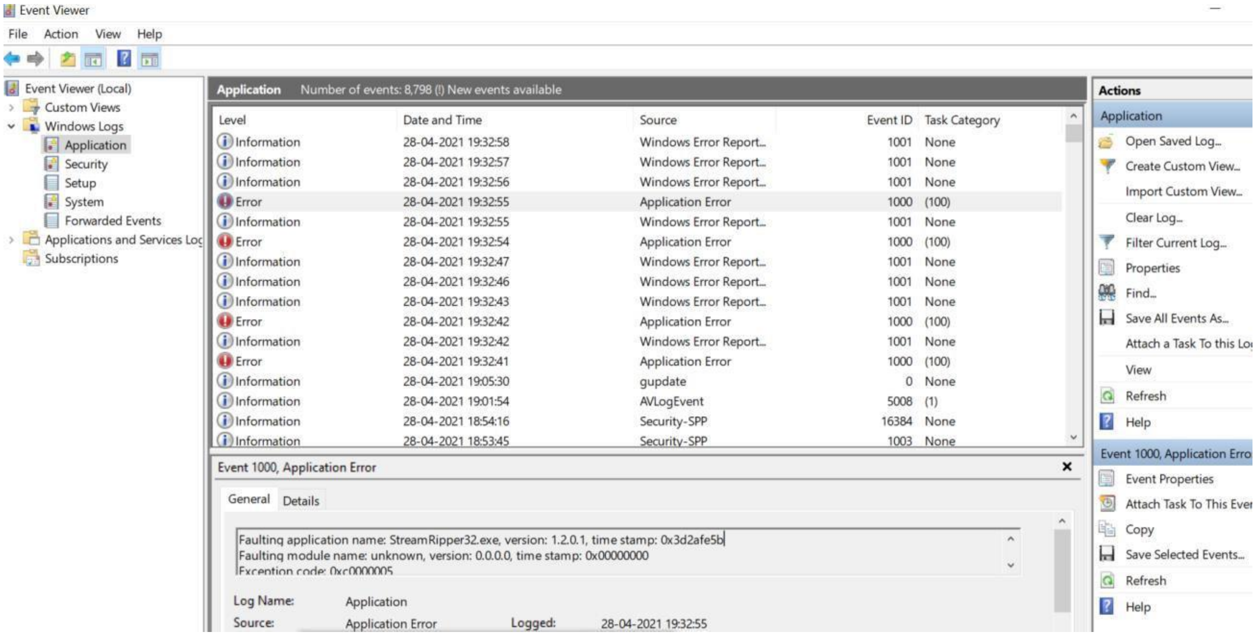
Relay Port: 10069

Search Text: ·ɔ³º{0LGc1I□≠ª≠Æ1ã

Version 2.6

By exploiting buffer overflow vulnerabilitiy we have crashed the application.

After the application crashes, go to event viewer.



Application Number of events: 8,798 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	28-04-2021 19:32:58	Windows Error Report...	1001	None
Information	28-04-2021 19:32:57	Windows Error Report...	1001	None
Information	28-04-2021 19:32:56	Windows Error Report...	1001	None
Error	28-04-2021 19:32:55	Application Error	1000	(100)
Information	28-04-2021 19:32:55	Windows Error Report...	1001	None
Error	28-04-2021 19:32:54	Application Error	1000	(100)
Information	28-04-2021 19:32:47	Windows Error Report...	1001	None
Information	28-04-2021 19:32:46	Windows Error Report...	1001	None
Information	28-04-2021 19:32:43	Windows Error Report...	1001	None
Error	28-04-2021 19:32:42	Application Error	1000	(100)
Information	28-04-2021 19:32:42	Windows Error Report...	1001	None
Error	28-04-2021 19:32:41	Application Error	1000	(100)
Information	28-04-2021 19:05:30	gupdate	0	None
Information	28-04-2021 19:01:54	AVLogEvent	5008	(1)
Information	28-04-2021 18:54:16	Security-SPP	16384	None
Information	28-04-2021 18:53:45	Security-SPP	1003	None

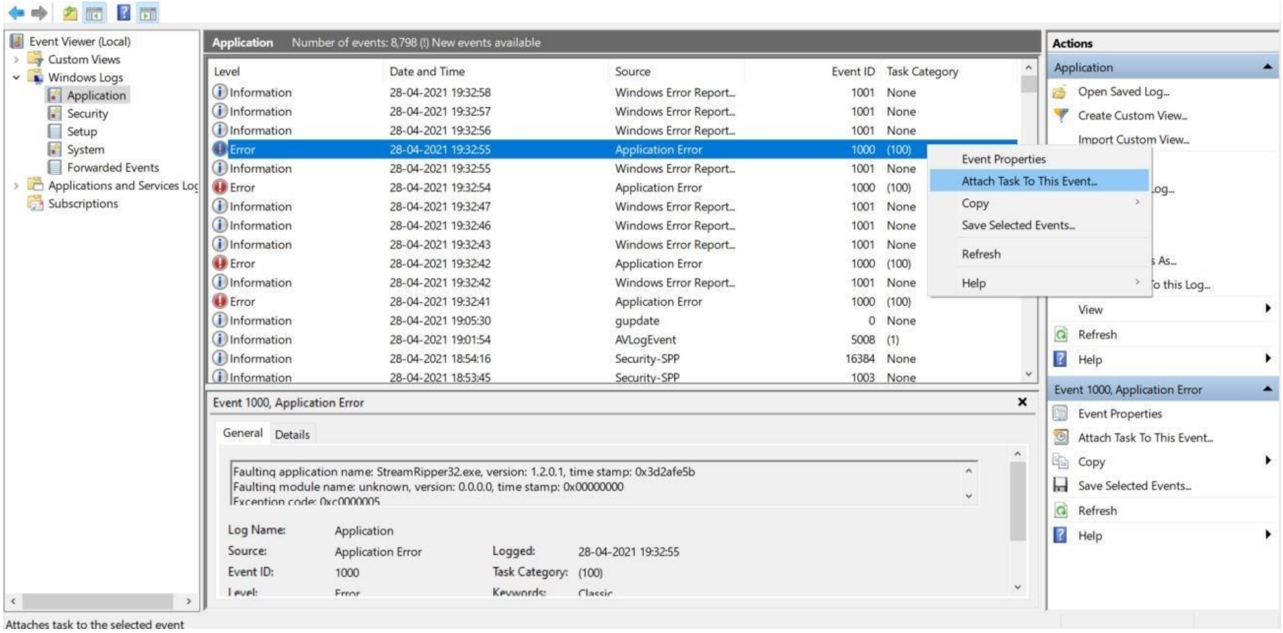
Event 1000, Application Error

General Details

```
Faulting application name: StreamRipper32.exe, version: 1.2.0.1, time stamp: 0x3d2afe5b
Faulting module name: unknown, version: 0.0.0.0, time stamp: 0x00000000
Exception code: 0xc0000005
```

Log Name: Application
Source: Application Error Logged: 28-04-2021 19:32:55

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



Application Number of events: 8,798 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	28-04-2021 19:32:58	Windows Error Report...	1001	None
Information	28-04-2021 19:32:57	Windows Error Report...	1001	None
Information	28-04-2021 19:32:56	Windows Error Report...	1001	None
Error	28-04-2021 19:32:55	Application Error	1000	(100)
Information	28-04-2021 19:32:55	Windows Error Report...	1001	None
Error	28-04-2021 19:32:54	Application Error	1000	(100)
Information	28-04-2021 19:32:47	Windows Error Report...	1001	None
Information	28-04-2021 19:32:46	Windows Error Report...	1001	None
Information	28-04-2021 19:32:43	Windows Error Report...	1001	None
Error	28-04-2021 19:32:42	Application Error	1000	(100)
Information	28-04-2021 19:32:42	Windows Error Report...	1001	None
Error	28-04-2021 19:32:41	Application Error	1000	(100)
Information	28-04-2021 19:05:30	gupdate	0	None
Information	28-04-2021 19:01:54	AVLogEvent	5008	(1)
Information	28-04-2021 18:54:16	Security-SPP	16384	None
Information	28-04-2021 18:53:45	Security-SPP	1003	None

Event 1000, Application Error

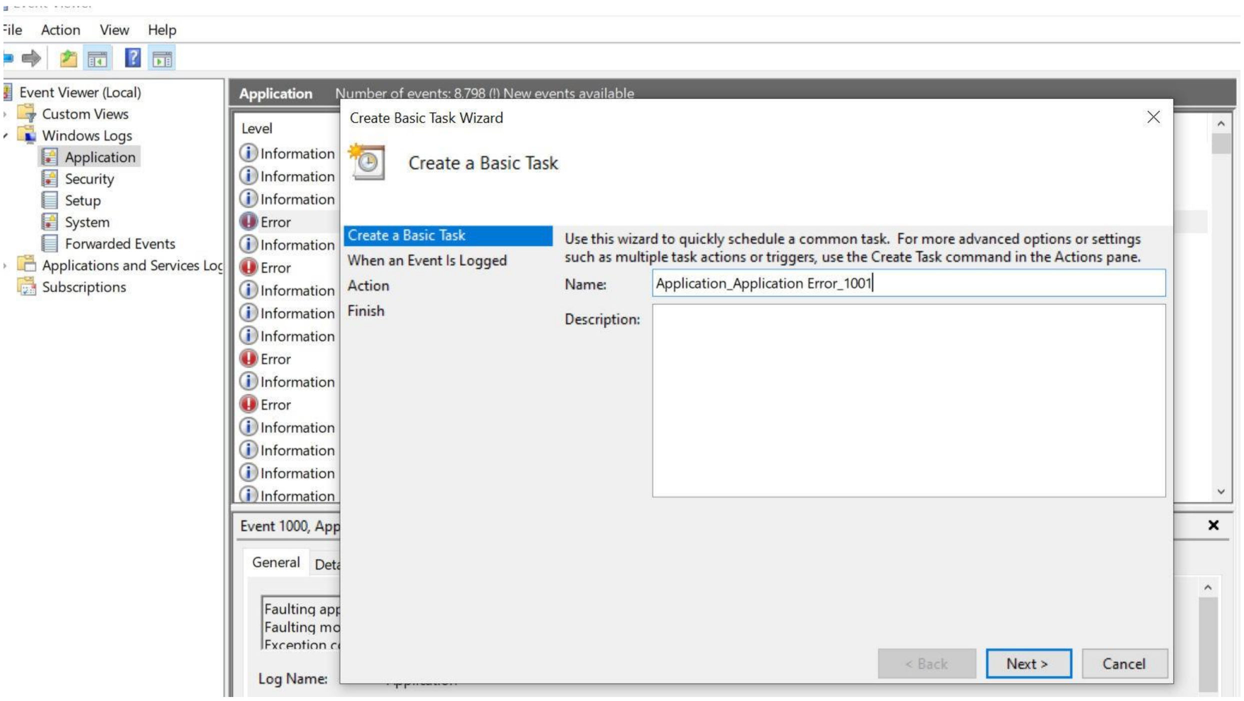
General Details

```
Faulting application name: StreamRipper32.exe, version: 1.2.0.1, time stamp: 0x3d2afe5b
Faulting module name: unknown, version: 0.0.0.0, time stamp: 0x00000000
Exception code: 0xc0000005
```

Log Name: Application
Source: Application Error Logged: 28-04-2021 19:32:55
Event ID: 1000 Task Category: (100)
Level: Error Keywords: Classic

Attaches task to the selected event

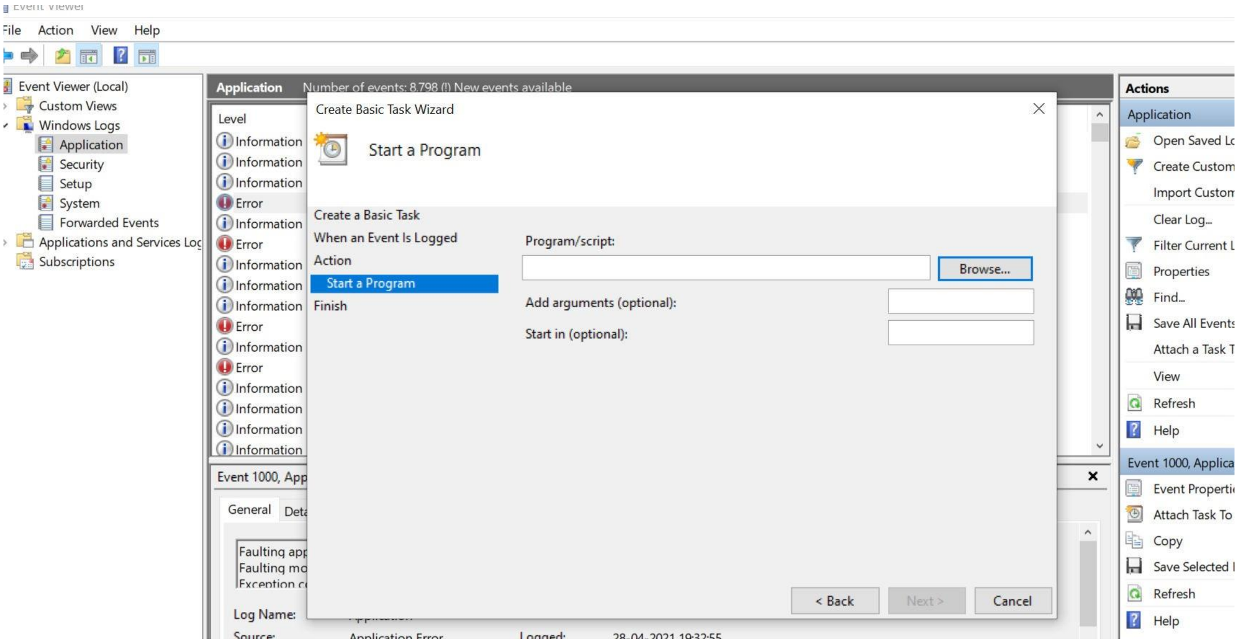
Now, create the task.



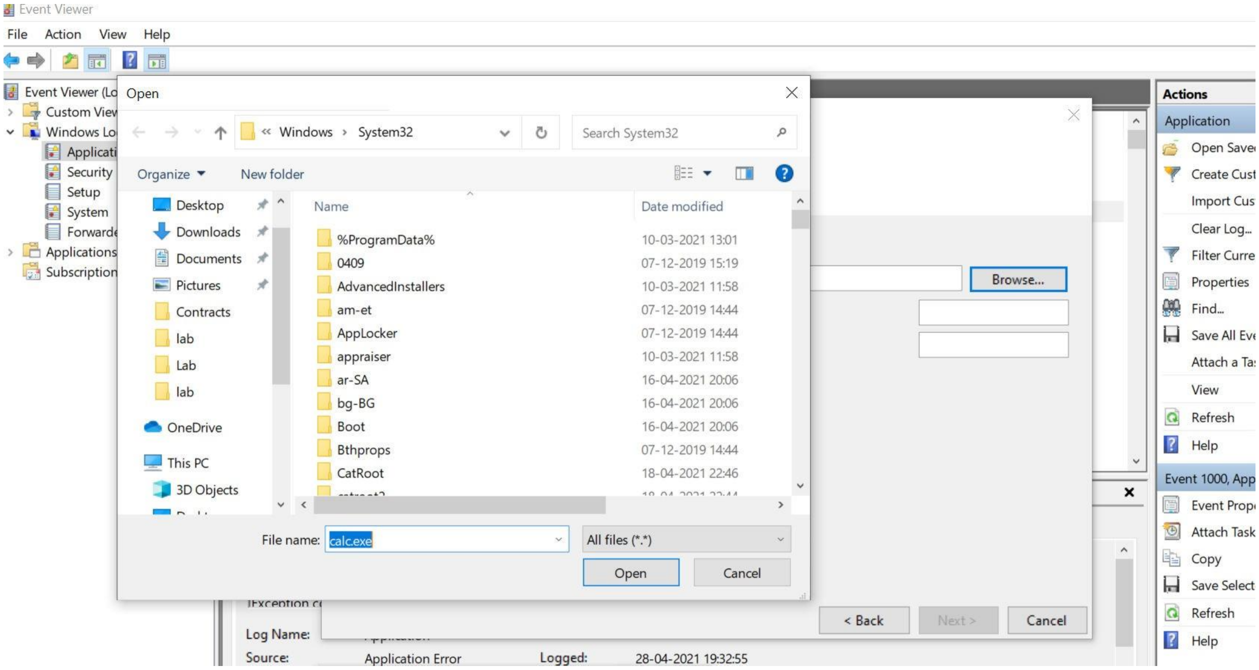
Use this wizard to quickly schedule a common task. For more advanced options or settings such as multiple task actions or triggers, use the Create Task command in the Actions pane.

Name: Application_Application Error_1001

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.



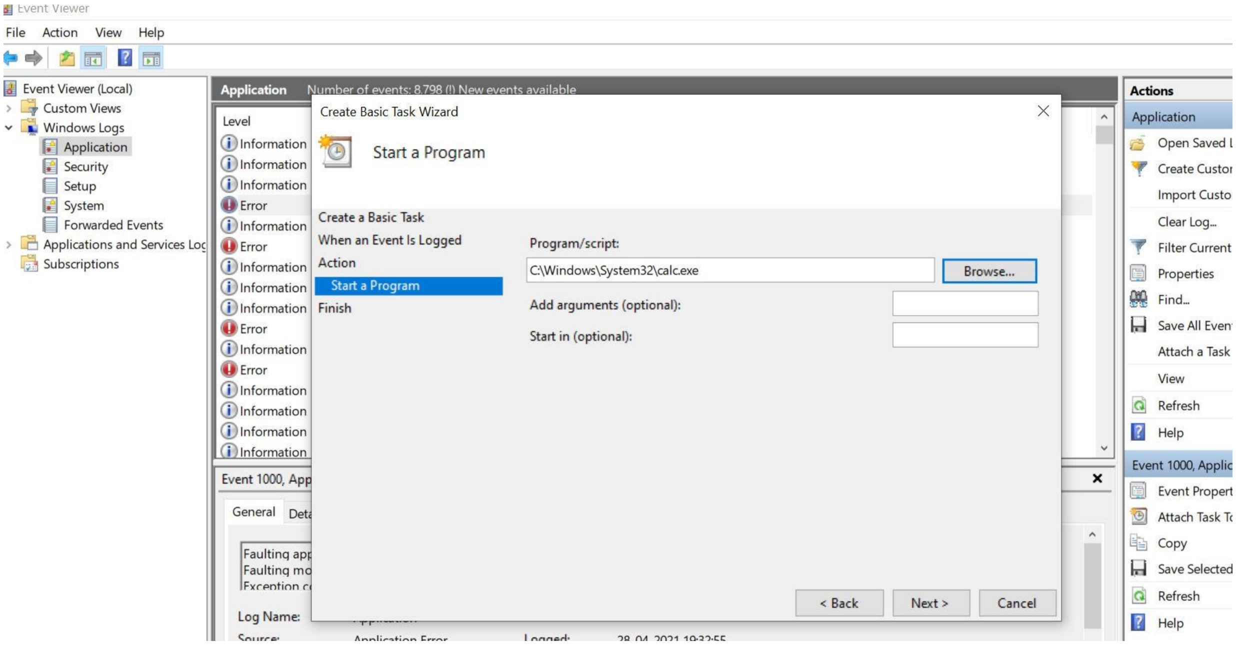
Name	Date modified
%ProgramData%	10-03-2021 13:01
0409	07-12-2019 15:19
AdvancedInstallers	10-03-2021 11:58
am-et	07-12-2019 14:44
AppLocker	07-12-2019 14:44
appraiser	10-03-2021 11:58
ar-SA	16-04-2021 20:06
bg-BG	16-04-2021 20:06
Boot	16-04-2021 20:06
Bthprops	07-12-2019 14:44
CatRoot	18-04-2021 22:46

File name: calc.exe

All files (*.*)

Log Name:

Source: Application Error Logged: 28-04-2021 19:32:55



Number of events: 8,798 (!) New events available

Create Basic Task Wizard

Start a Program

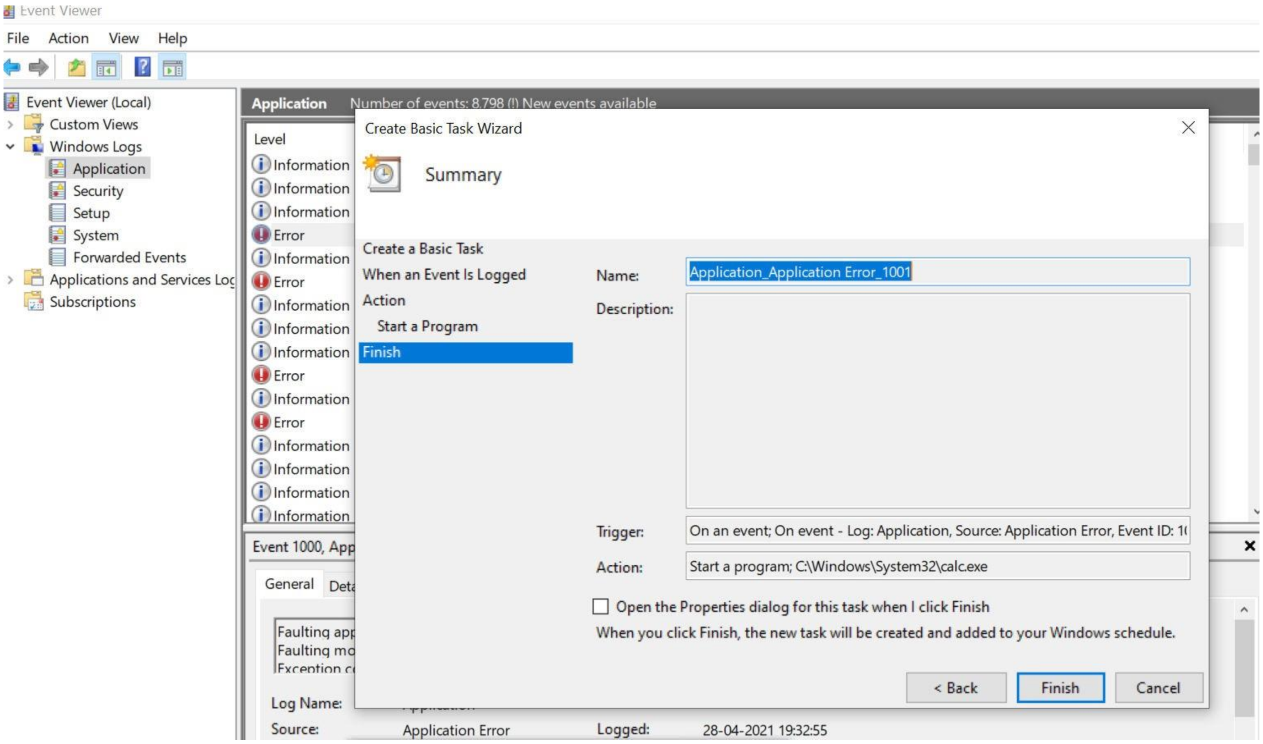
Program/script: C:\Windows\System32\calc.exe

Add arguments (optional):

Start in (optional):

Log Name:

Source: Application Error Logged: 28-04-2021 19:32:55



Name: Application_Application Error_1001

Description:

Trigger: On an event; On event - Log: Application, Source: Application Error, Event ID: 1(

Action: Start a program; C:\Windows\System32\calc.exe

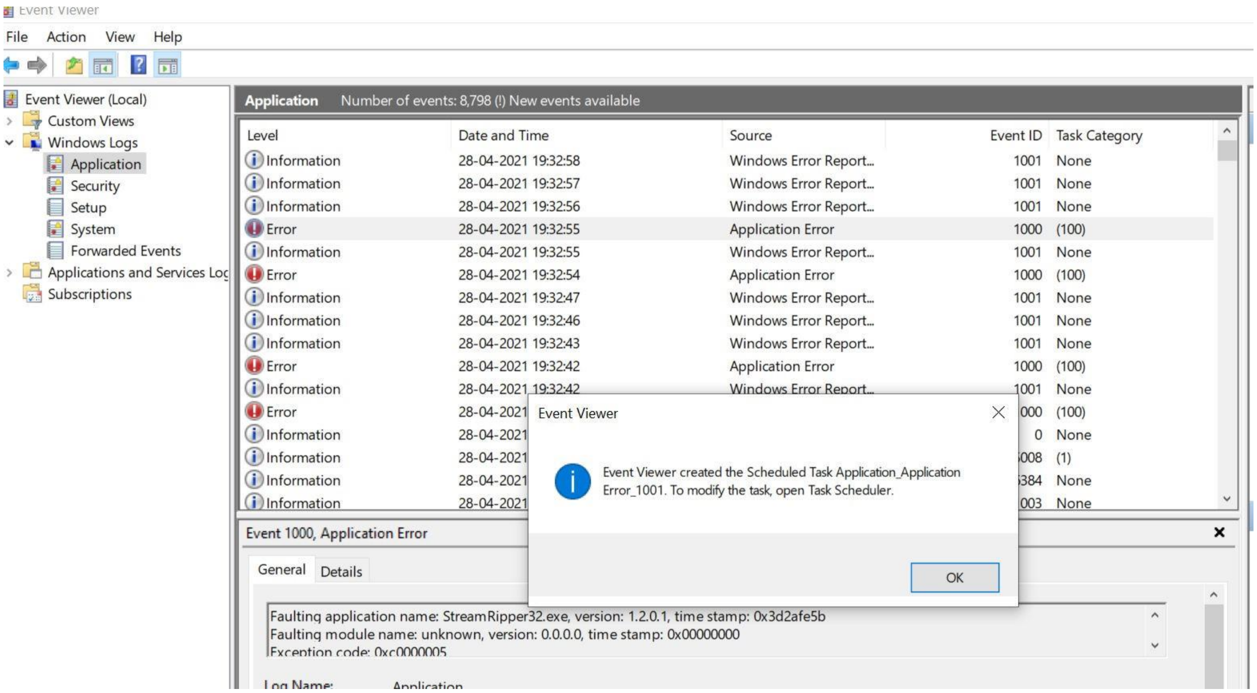
☐ Open the Properties dialog for this task when I click Finish

When you click Finish, the new task will be created and added to your Windows schedule.

```
Faulting app
Faulting mo
Exception c
```

Log Name:

Source: Application Error   Logged: 28-04-2021 19:32:55



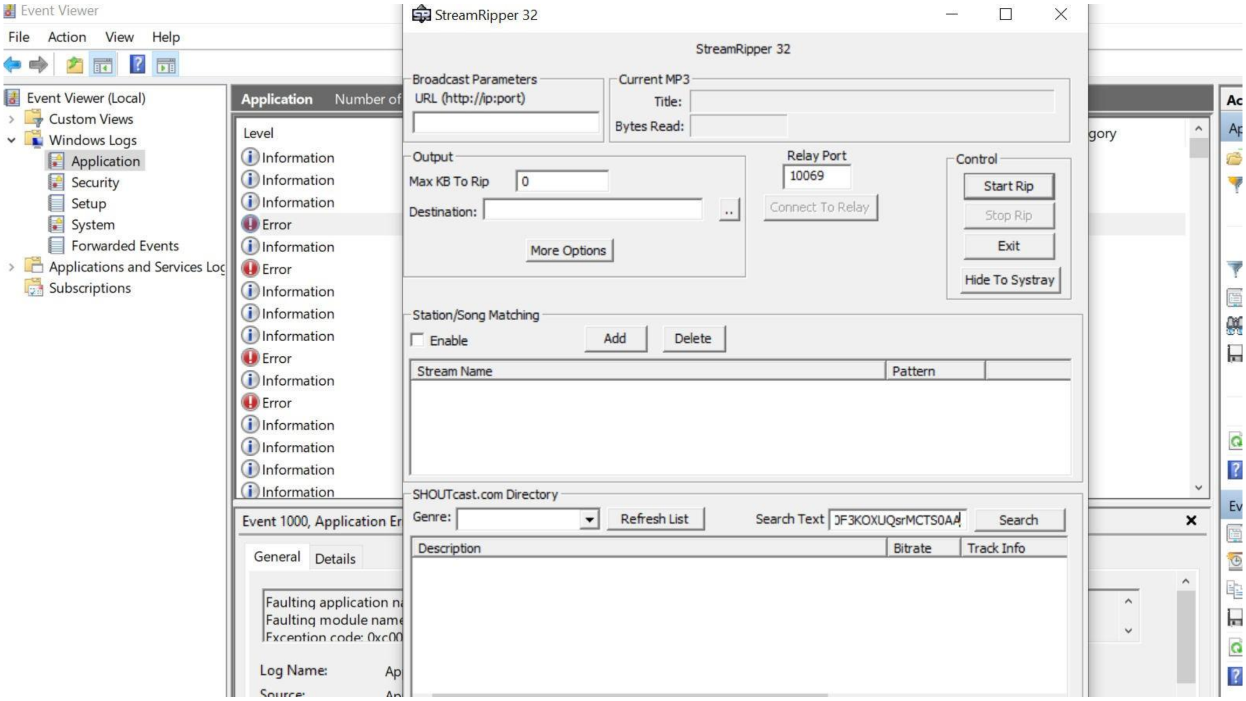
Level	Date and Time	Source	Event ID	Task Category
Information	28-04-2021 19:32:58	Windows Error Report...	1001	None
Information	28-04-2021 19:32:57	Windows Error Report...	1001	None
Information	28-04-2021 19:32:56	Windows Error Report...	1001	None
Error	28-04-2021 19:32:55	Application Error	1000	(100)
Information	28-04-2021 19:32:55	Windows Error Report...	1001	None
Error	28-04-2021 19:32:54	Application Error	1000	(100)
Information	28-04-2021 19:32:47	Windows Error Report...	1001	None
Information	28-04-2021 19:32:46	Windows Error Report...	1001	None
Information	28-04-2021 19:32:43	Windows Error Report...	1001	None
Error	28-04-2021 19:32:42	Application Error	1000	(100)
Information	28-04-2021 19:32:42	Windows Error Report...	1001	None
Error	28-04-2021		000	(100)
Information	28-04-2021		0	None
Information	28-04-2021		008	(1)
Information	28-04-2021		384	None
Information	28-04-2021		003	None

Event Viewer created the Scheduled Task Application_Application Error_1001. To modify the task, open Task Scheduler.

```
Faulting application name: StreamRipper32.exe, version: 1.2.0.1, time stamp: 0x3d2afe5b
Faulting module name: unknown, version: 0.0.0.0, time stamp: 0x00000000
Exception code: 0xc0000005
```

Log Name: Application

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



Level
Information
Information
Information
Error
Information
Error
Information
Information
Information
Error
Information
Error
Information
Information
Information
Information

Faulting application na
Faulting module name
Exception code: 0xc00

Log Name: Ap
Source: Ap

Max KB To Rip: 0

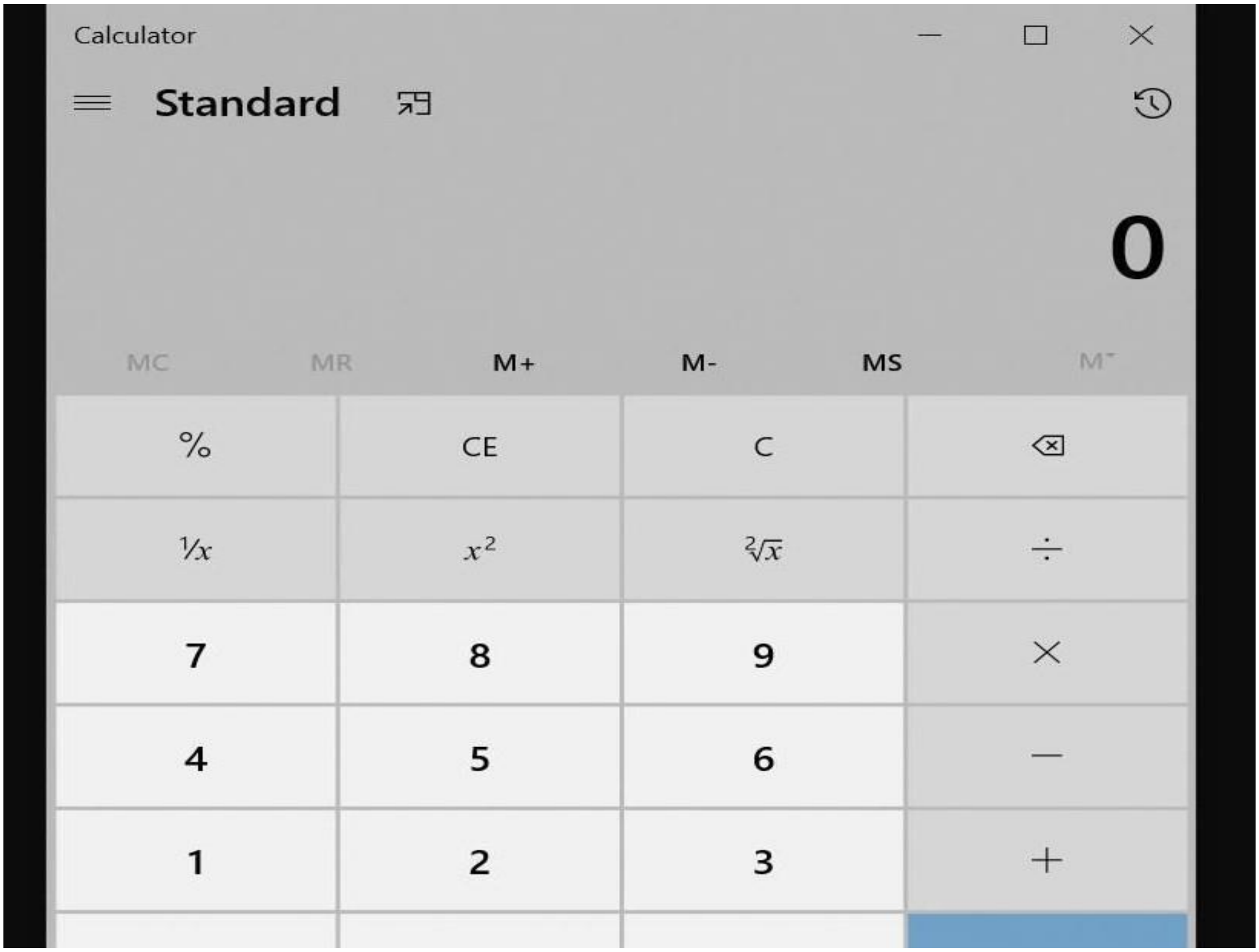
Relay Port: 10069

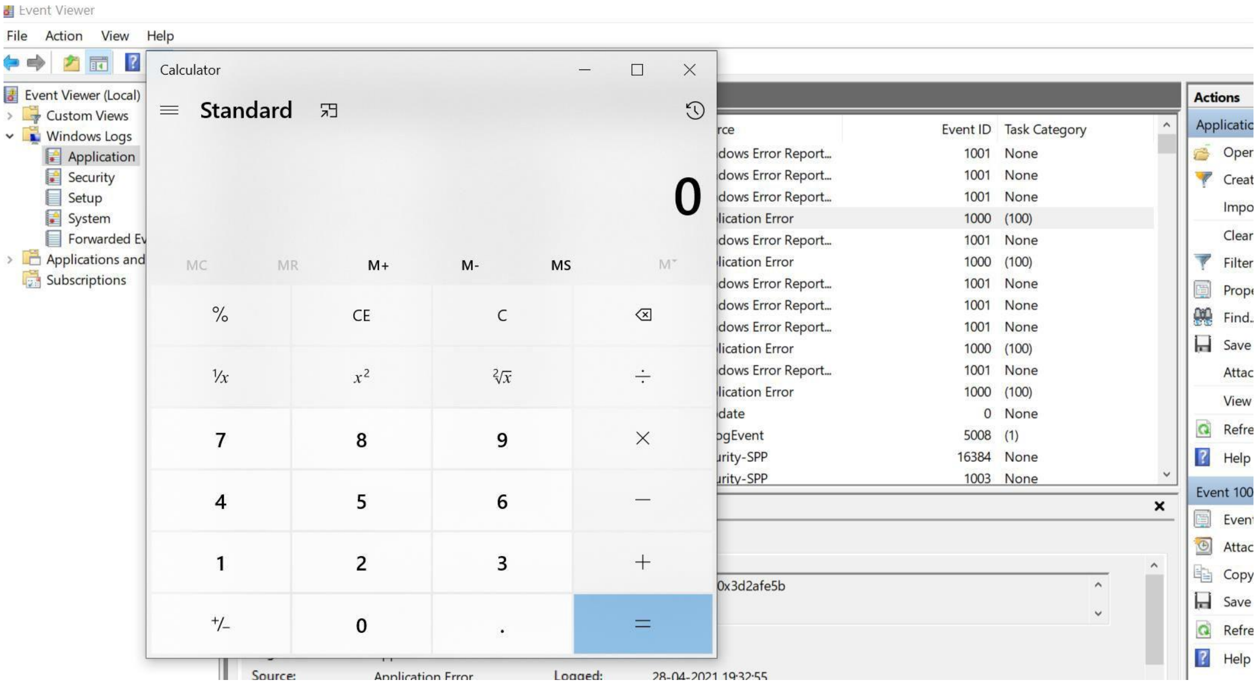
☐ Enable

Search Text: JF3KOXUQsrMCTS0AA

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.


Calculator
Standard
0
MC
MR
M+
M-
MS
M˅
%
CE
C
⌫
⅟x
x^2
$\sqrt[2]{x}$
÷
7
8
9
×
4
5
6
−
1
2
3
+



rce	Event ID	Task Category
dows Error Report...	1001	None
dows Error Report...	1001	None
dows Error Report...	1001	None
lication Error	1000	(100)
dows Error Report...	1001	None
lication Error	1000	(100)
dows Error Report...	1001	None
dows Error Report...	1001	None
dows Error Report...	1001	None
lication Error	1000	(100)
dows Error Report...	1001	None
lication Error	1000	(100)
date	0	None
ogEvent	5008	(1)
urity-SPP	16384	None
urity-SPP	1003	None

0x3d2afe5b

Source: Application Error Logged: 28-04-2021 19:32:55