

# S2E GUI

SEE PREVIOUS RESULTS

TIMEOUT (S) :

15



Browse...

No file selected.

RUN

SAVE CONFIG

CallSiteMonitor

ModuleExecutionDetector

ProcessExecutionDetector

ExecutionTracer

InstructionCounter

StateSwitchTracer

TBCoverageTracer

TestCaseGenerator

ControlFlowGraph

SeedScheduler

CUPASearcher

MultiSearcher

SeedSearcher

TranslationBlockCoverage

BasicBlockCoverage

# Analysis Configuration

SEE PREVIOUS RESULTS

TIMEOUT (S) : 15

Browse... No file selected.

RUN

Please select a file.

SAVE CONFIG

ControlFlowGraph

CallSiteMonitor

InstructionCounter

TestCaseGenerator

StateSwitchTracer

ExecutionTracer

TBCoverageTracer

SeedSearcher

MultiSearcher

CUPASearcher

SeedScheduler

BasicBlockCoverage

TranslationBlockCoverage

ProcessExecutionDetector

ModuleExecutionDetector

## CallSiteMonitor

CallSiteMonitor S2E plugin

dumpInfoInterval:

## ProcessExecutionDetector

ProcessExecutionDetector S2E plugin

Fetch the list of modules where to report the calls

moduleNames:

## ModuleExecutionDetector

Plugin for monitoring module execution

When true, pass events about all module loads and unloads to client plugins but do not notify them about the execution. This is useful for execution tracers to record modules loads to provide debug information offline without actually recording any trace.

trackAllModules: ☒ True ☐ False

Custom plugin selection

Dynamic error checking

Currently supports following types : Integer, Boolean, String, List of string, List of integer and generic Lists

# Analysis Overview

OVERVIEW

WARNING

INFO

DEBUG

INSTRUCTION COUNTER

LINE COVERAGE

STATISTICS

GRAPH

RUN NEW ANALYSIS

Analysis finished

State	Status	Message
0	0x0	program terminated
1	0x0	program terminated
2	0x0	program terminated

Display the termination status and message of each states.

# Analysis Overview

OVERVIEW

WARNING

INFO

DEBUG

INSTRUCTION COUNTER

LINE COVERAGE

STATISTICS

GRAPH

RUN NEW ANALYSIS

## Analysis finished

State	Status	Message
0	0x0	program terminated
1	0x1	killing state with error
2	0x0	program terminated
3	0x0	program terminated
4	-1	Segfault
5	-1	Segfault

Can be used to quickly find an error.

# Analysis Logs

OVERVIEW WARNING INFO DEBUG INSTRUCTION COUNTER LINE COVERAGE STATISTICS GRAPH

RUN NEW ANALYSIS

Full log ▾

```
[Z3] Initializing
BEGIN searcher description
DFSSearcher
END searcher description
Creating plugin CorePlugin
Creating plugin HostFiles
Creating plugin Vmi
Creating plugin BaseInstructions
Creating plugin LinuxMonitor
Initializing BaseInstructions
Initializing LinuxMonitor
Initializing Vmi
Initializing HostFiles
Initializing CorePlugin
1 [State 0] Created initial state
3 [State 0] BaseInstructions: Message from guest (0x7ffeab9e1f80): Process map:
3 [State 0] BaseInstructions: Message from guest (0x7ffeab9e1f80): Base=0x400000 Limit=0x401000 Name=/home/s2e/first_program
3 [State 0] BaseInstructions: Message from guest (0x7ffeab9e1f80): Base=0x7eff6d3a1000 Limit=0x7eff6d3a4000 Name=/lib/x86_64-linux-
gnu/libdl-2.19.so
3 [State 0] BaseInstructions: Message from guest (0x7ffeab9e1f80): Base=0x7eff6d5a5000 Limit=0x7eff6d746000 Name=/lib/x86_64-linux-
gnu/libc-2.19.so
3 [State 0] BaseInstructions: Message from guest (0x7ffeab9e1f80): Base=0x7eff6d950000 Limit=0x7eff6d955000 Name=/home/s2e/s2e.so
3 [State 0] BaseInstructions: Message from guest (0x7ffeab9e1f80): Base=0x7eff6db56000 Limit=0x7eff6db76000 Name=/lib/x86_64-linux-gnu/ld-
2.19.so
3 [State 0] BaseInstructions: Message from guest (0x7ffeab9e1f80): Base=0x7ffeab9e9000 Limit=0x7ffeab9eb000 Name=[vdso]
3 [State 0] BaseInstructions: Message from guest (0x7ffeab9e1f80): Base=0xffffffff600000 Limit=0xffffffff601000 Name=[vsyscall]
3 [State 0] BaseInstructions: Inserted symbolic data @0x7ffeab9e20b0 of size 0x1: rows pc=0x4005a6
3 [State 0] Forking state 0 at pc = 0x40060a at pagedir = 0xdaa4000
state 1
state 0
3 [State 0] Forking state 0 at pc = 0x400650 at pagedir = 0xdaa4000
```

Display Log of analysis.  
Message from guest in yellow.

# Analysis Logs

OVERVIEW WARNING INFO **DEBUG** INSTRUCTION COUNTER LINE COVERAGE STATISTICS GRAPH

RUN NEW ANALYSIS

State 4 ▾

2 [State 4] BaselineInstructions: Message from guest (0x7ffe37d02b20): key example value : 4  
2 [State 4] LinuxMonitor: Received segfault type=0 pagedir=0xd044000 pid=0x521 name=segfault\_demo pc=0x400833 addr=0x0  
2 [State 4] Terminating state early: Segfault  
2 [State 4] Switching from state 4 to state 3

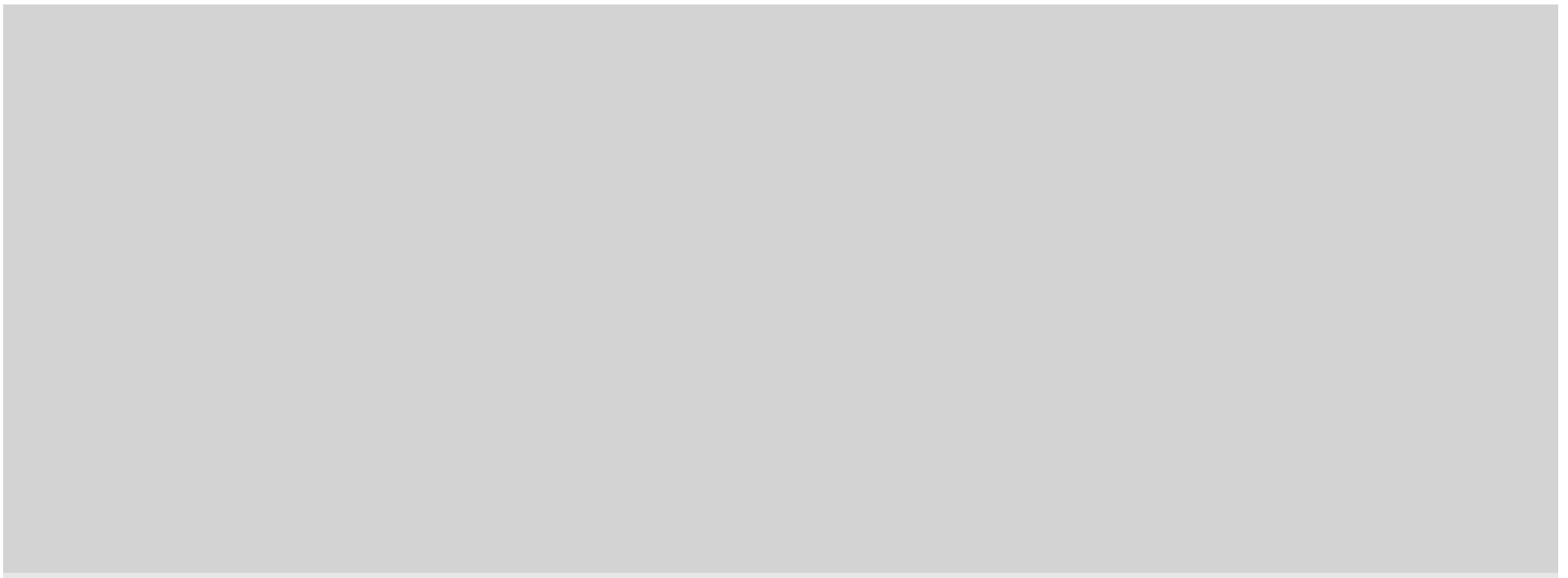
Can select the log for a specific state.  
Useful to quickly find a message related to a single state.

# Plugin specific output



**No instruction count data found :**

To have an instruction count table, make sure to enable InstructionCounter



Instruction counter and TranslationBlockCoverage custom output.  
They must be enabled to display it.

# Instruction Counter

OVERVIEW WARNING INFO DEBUG INSTRUCTION COUNTER LINE COVERAGE STATISTICS GRAPH

RUN NEW ANALYSIS

State ID	Instruction count
0	813335
1	812622
2	812708
3	812908
4	813141
5	812554

Count the number of instruction per state.



# Line Coverage

OVERVIEW WARNING INFO DEBUG INSTRUCTION COUNTER **LINE COVERAGE** STATISTICS GRAPH

RUN NEW ANALYSIS

## LCOV - code coverage report

Current view: [top level](#) - [Downloads](#) - [segfault\\_demo.c](#) (source / [functions](#))

Test: [coverage.info](#)

Date: 2017-06-28 21:02:48

	Hit	Total	Coverage
Lines:	45	49	91.8 %
Functions:	0	0	-

Line data Source code

```
1 : #include <stdio.h>
2 : #include "include/s2e/s2e.h"
3 :
4 : int main()
5 : {
6 :     int key[11];
7 :     int i, j;
8 :     char buf[128];
9 :
10 :    s2e_make_symbolic(key, sizeof(int), "key");
11 :
12 :    if(key[0] == 5){
13 :        s2e_get_example(key, sizeof(int));
14 :        snprintf(buf, 128, "key example value : %d", key[0]);
15 :        s2e_message(buf);
16 :
17 :        s2e_kill_state(1, "killing state with error");
18 :    }
19 :
20 :    if(key[0] > 10 && key[0] < 12){
21 :        s2e_get_example(key, sizeof(int));
22 :        snprintf(buf, 128, "key example value : %d", key[0]);
23 :        s2e_message(buf);
24 :
25 :        *(int*)0 = 0;
26 :    }
27 :
28 :
29 :    if(key[0] < 5 && key[0] > 2){
30 :        s2e_get_example(key, sizeof(int));
31 :        snprintf(buf, 128, "key example value : %d", key[0]);
32 :        s2e_message(buf);
33 :
34 :        *(int*)0 = 0;
35 :    }
36 :
37 :    s2e_get_example(key, sizeof(int));
38 :    snprintf(buf, 128, "key example value : %d", key[0]);
39 :    s2e_message(buf);
40 :
41 :    s2e_kill_state(0, "program terminated");
42 :
43 :    return 0;
44 : }
```

Generated by: [LCOV version 1.12](#)

Display the line coverage of the code.

# Function Graph



Display the program flow with assembly instruction.

Green arrow for branch if true.

Red arrow for branch if false.

Blue arrow for unconditional jump.

# Statistics

OVERVIEWWARNINGINFODEBUGINSTRUCTION COUNTERLINE COVERAGESTATISTICSGRAPH

RUN NEW ANALYSIS

NumStates	CompletedPaths	CoveredBasicBlocks	TotalBasicBlocks	Bugs	NumQueries	NumQueryConstructs	NumObjects	ObjectsSize	TranslationBlocks	TranslationBlocksCo
0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	67752	277509459	0	0
0	3	0	0	0	5	57	67752	277509459	0	0

Display the statistics provided by s2e.

# Analysis Database

RUN NEW ANALYSIS

Project name: first_program		
Analysis ID	Binary Checksum	
8	d210a1592b649598725a3eb8c3e290ceb31918d23b896ffef94d80841edab90b	✗
9	d210a1592b649598725a3eb8c3e290ceb31918d23b896ffef94d80841edab90b	✗

Project name: segfault_demo		
Analysis ID	Binary Checksum	
10	a958c5f17fe28ede209c15429ad80694a7d5f72dd354b5ae67acf451fbb2466a	✗
11	a958c5f17fe28ede209c15429ad80694a7d5f72dd354b5ae67acf451fbb2466a	✗
12	a958c5f17fe28ede209c15429ad80694a7d5f72dd354b5ae67acf451fbb2466a	✗
13	a958c5f17fe28ede209c15429ad80694a7d5f72dd354b5ae67acf451fbb2466a	✗
14	a958c5f17fe28ede209c15429ad80694a7d5f72dd354b5ae67acf451fbb2466a	✗
15	a958c5f17fe28ede209c15429ad80694a7d5f72dd354b5ae67acf451fbb2466a	✗

Display every analysis the user has run.  
Analysis can be displayed by clicking them or deleted with the red x.  
Database is linked to the server.