Software Security A.A. 2021-2022
Individual Project 3
Stanco Donato Francesco Pio 2027523

1 Setting up the tool and initial difficulties

1.1 Understand the tool and download ImageMagick

The first thing to do for this project was to install the AFL tool that I installed with the terminal of my pc using the command:

```
brew install afl-fuzz
```

This command works for MacOS and downloaded the latest version of American Fuzzy Loop that is 2.57b.

Initially I try to understand how the tool works using other applications, such as fuzzgoat to start making preliminary tests, before proceeding with ImageMagick. After that I downloaded the latest version of ImageMagick which is currently the 7.1.0-19 from a github repository, I made the git clone of the project on my pc and started testing it.

I tested this version of ImageMagick using images in **JPEG format** but after three hours of execution the tool had not yet found unique crashes so I decided to test a previous version, the 6.7.9-10 of ImageMagick, which dates back to 2012/10/08.

1.2 Commands for compile ImageMagick with AFL

In order for ImageMagick to be compiled with the afl tool, the following terminal commands are required:

```
export CC=PATH-TO-afl-clang
./configure  --prefix=PATH-TO-ImageMagick-6.7.9-10
make
mkdir afl_in
mkdir afl_out
sudo make install
```

For this project I didn’t use the AddressSanitizer tool (ASAN) because by implementing the following commands together with the ones above I encountered problems following the architecture of my machine. The commands that have been used are the following:

```
CFLAGS=”-fsanitize=address -g”
AFL_USE_ASAN=1
```

- `CFLAGS` is a flag for C compiler where I specify in this case the use of the address sanitizer

- `AFL_USE_ASAN` is a variable that if is set this equal to 1 we allow AFL to use the AddressSanitizer tool. This assignment must be done before the make command

In order to perform this step I used the guide provided by the ImageMagick repository called *Install-mac.txt*.
The command used for fuzz-testing is the following:

```
afl-fuzz -d -m none -i afl_in -o afl_out -- ./bin/convert @@ /dev/null
```

More specifically:

- `/dev/null` is used to not save the output
- `-d` is used to quickly achieve wider, albeit shallower, coverage

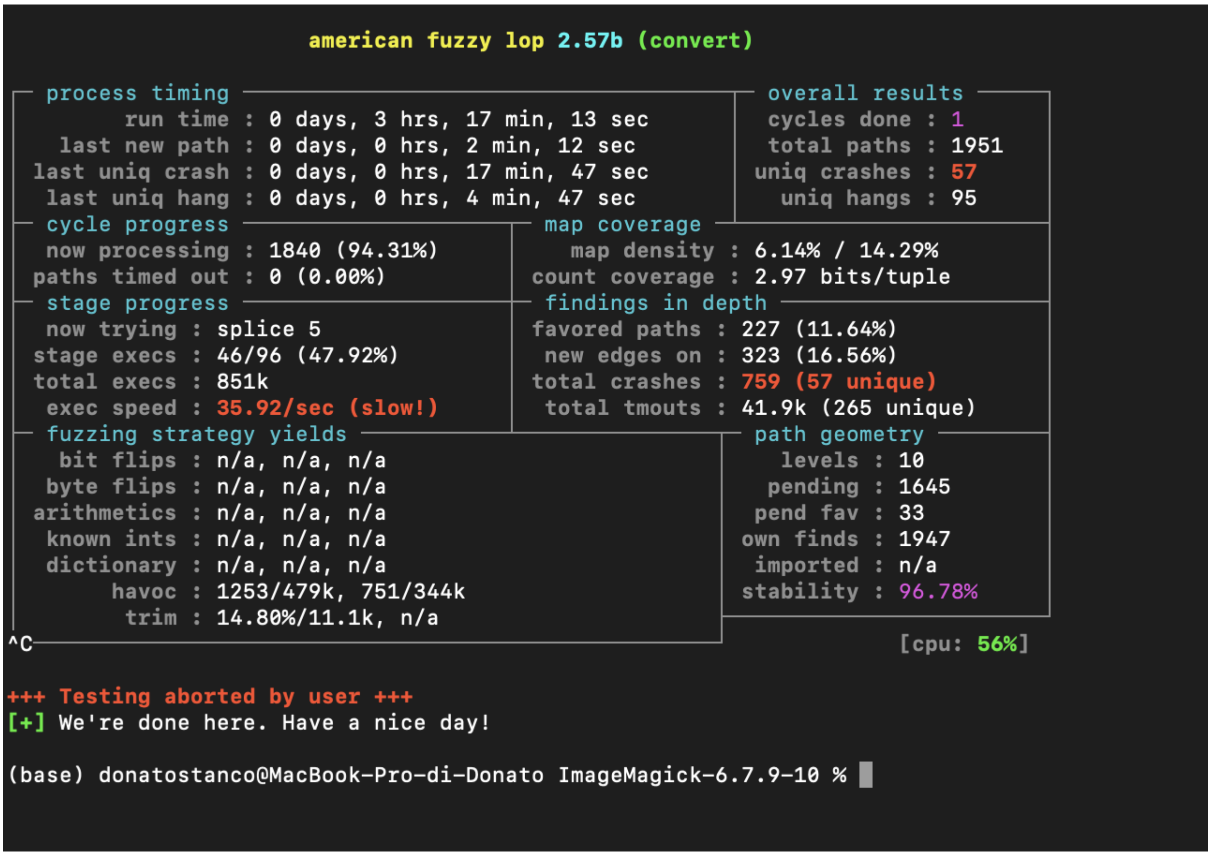
2. AFL and ASAN

American fuzzy lop (**AFL**) is a free software fuzzer that employs genetic algorithms in order to efficiently increase code coverage of the test cases. So far it helped in detection of significant software bugs in dozens of major free software projects. The fuzzing engine of American fuzzy lop uses several algorithms whose goal is to trigger unexpected behavior, including bit flips or replacing bytes of input file with various integers that can trigger edge cases.
AddressSanitizer (**ASAN**), originally introduced by Google, is a powerful alternative to both runtime error checking and (static analysis). Provides runtime bug-finding technologies that directly use existing build systems and existing test assets.

3. Results of the experiments

In this section I report the results of the experiments for which I used the test cases present in the afl repository and for completeness I also used those of the afl site.

3.1 Repository Test Cases

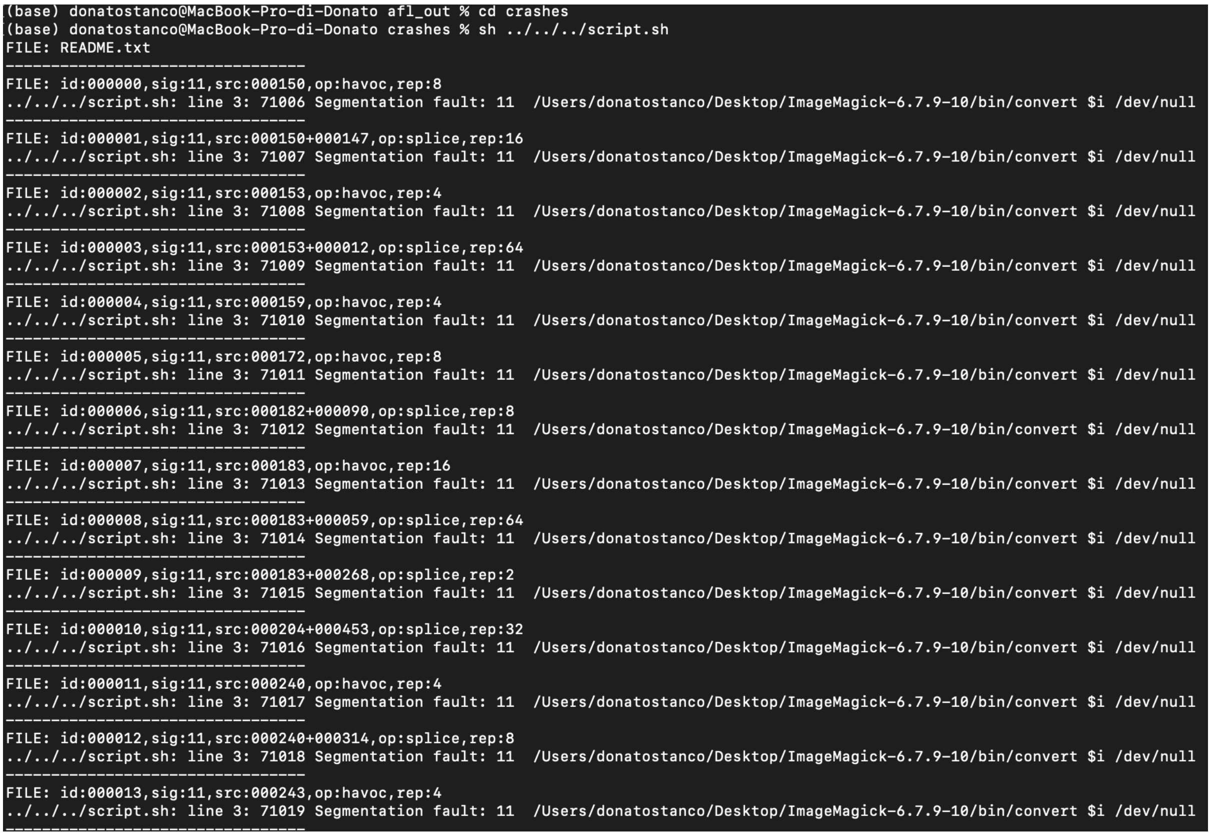


```
                       american fuzzy lop 2.57b (convert)

┌─ process timing ─────────────────────────────────────┬─ overall results ─────┐
│        run time : 0 days, 3 hrs, 17 min, 13 sec      │  cycles done : 1      │
│   last new path : 0 days, 0 hrs, 2 min, 12 sec       │  total paths : 1951   │
│ last uniq crash : 0 days, 0 hrs, 17 min, 47 sec      │ uniq crashes : 57     │
│  last uniq hang : 0 days, 0 hrs, 4 min, 47 sec       │   uniq hangs : 95     │
├─ cycle progress ────────────────────┬─ map coverage ─┴───────────────────────┤
│  now processing : 1840 (94.31%)     │    map density : 6.14% / 14.29%        │
│ paths timed out : 0 (0.00%)         │ count coverage : 2.97 bits/tuple       │
├─ stage progress ────────────────────┼─ findings in depth ────────────────────┤
│  now trying : splice 5              │ favored paths : 227 (11.64%)           │
│ stage execs : 46/96 (47.92%)        │  new edges on : 323 (16.56%)           │
│ total execs : 851k                  │ total crashes : 759 (57 unique)        │
│  exec speed : 35.92/sec (slow!)     │  total tmouts : 41.9k (265 unique)     │
├─ fuzzing strategy yields ───────────┴───────────────┬─ path geometry ────────┤
│   bit flips : n/a, n/a, n/a                         │    levels : 10         │
│  byte flips : n/a, n/a, n/a                         │   pending : 1645       │
│ arithmetics : n/a, n/a, n/a                         │  pend fav : 33         │
│  known ints : n/a, n/a, n/a                         │ own finds : 1947       │
│  dictionary : n/a, n/a, n/a                         │  imported : n/a        │
│       havoc : 1253/479k, 751/344k                   │ stability : 96.78%     │
│        trim : 14.80%/11.1k, n/a                     ├────────────────────────┘
^C────────────────────────────────────────────────────┘             [cpu: 56%]

+++ Testing aborted by user +++
[+] We're done here. Have a nice day!

(base) donatostanco@MacBook-Pro-di-Donato ImageMagick-6.7.9-10 %
```

The image format I choose is **PNG** and the number of images used for the test is 4 because as specified in the afl guide (`perf_tips.txt`) is preferable to use a small set of test cases.

The time required for the execution was about 3 hours, in which I obtained **1951 mutations** generated by afl, finding **57 uniq crashes** and **95 uniq hangs** and **1 complete cycle**. I stopped the execution after this time because a cycle was done and my device's memory ran out (ImageMagick creates large temp files).

After that I used a simple bash script to apply the convert to all the files that caused the crash and these were all caused by segmentation fault (error related to memory management).



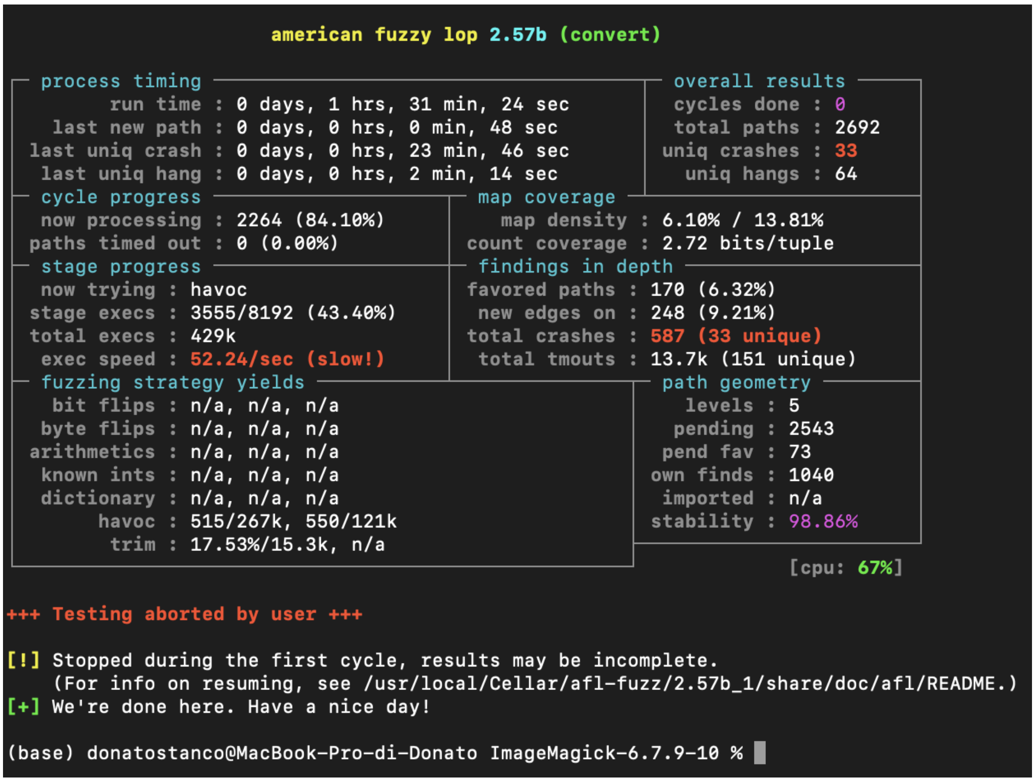
```
(base) donatostanco@MacBook-Pro-di-Donato afl_out % cd crashes
(base) donatostanco@MacBook-Pro-di-Donato crashes % sh ../../../script.sh
FILE: README.txt
---------------------------------
FILE: id:000000,sig:11,src:000150,op:havoc,rep:8
../../../script.sh: line 3: 71006 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000001,sig:11,src:000150+000147,op:splice,rep:16
../../../script.sh: line 3: 71007 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000002,sig:11,src:000153,op:havoc,rep:4
../../../script.sh: line 3: 71008 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000003,sig:11,src:000153+000012,op:splice,rep:64
../../../script.sh: line 3: 71009 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000004,sig:11,src:000159,op:havoc,rep:4
../../../script.sh: line 3: 71010 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000005,sig:11,src:000172,op:havoc,rep:8
../../../script.sh: line 3: 71011 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000006,sig:11,src:000182+000090,op:splice,rep:8
../../../script.sh: line 3: 71012 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000007,sig:11,src:000183,op:havoc,rep:16
../../../script.sh: line 3: 71013 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000008,sig:11,src:000183+000059,op:splice,rep:64
../../../script.sh: line 3: 71014 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000009,sig:11,src:000183+000268,op:splice,rep:2
../../../script.sh: line 3: 71015 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000010,sig:11,src:000204+000453,op:splice,rep:32
../../../script.sh: line 3: 71016 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000011,sig:11,src:000240,op:havoc,rep:4
../../../script.sh: line 3: 71017 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000012,sig:11,src:000240+000314,op:splice,rep:8
../../../script.sh: line 3: 71018 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000013,sig:11,src:000243,op:havoc,rep:4
../../../script.sh: line 3: 71019 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
```

CVE

The flaws I found were not registered as CVE, the following are the useful links where I checked these things for version 6.7.9-10 of ImageMagick:

- ImageMagick security vulnerabilities
- ImageMagick CVE

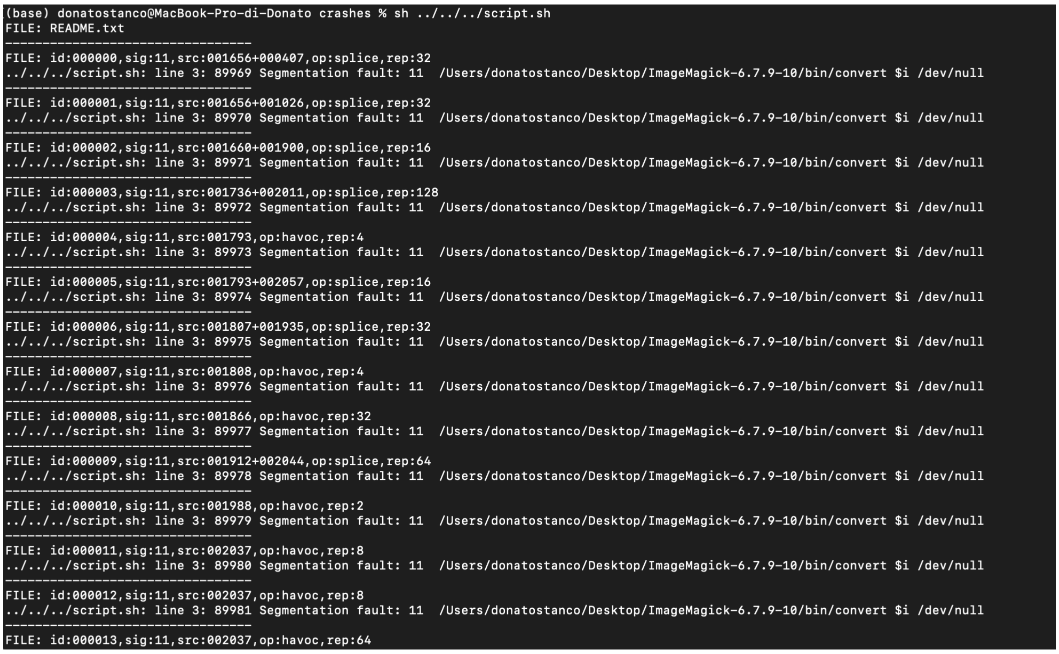
3.2 Site Test Cases



```
                       american fuzzy lop 2.57b (convert)

┌─ process timing ─────────────────────────────────────┬─ overall results ─────┐
│        run time : 0 days, 1 hrs, 31 min, 24 sec      │  cycles done : 0      │
│   last new path : 0 days, 0 hrs, 0 min, 48 sec       │  total paths : 2692   │
│ last uniq crash : 0 days, 0 hrs, 23 min, 46 sec      │ uniq crashes : 33     │
│  last uniq hang : 0 days, 0 hrs, 2 min, 14 sec       │   uniq hangs : 64     │
├─ cycle progress ───────────────────┬─ map coverage ─┴───────────────────────┤
│  now processing : 2264 (84.10%)    │    map density : 6.10% / 13.81%        │
│ paths timed out : 0 (0.00%)        │ count coverage : 2.72 bits/tuple       │
├─ stage progress ───────────────────┼─ findings in depth ────────────────────┤
│  now trying : havoc                │ favored paths : 170 (6.32%)            │
│ stage execs : 3555/8192 (43.40%)   │  new edges on : 248 (9.21%)            │
│ total execs : 429k                 │ total crashes : 587 (33 unique)        │
│  exec speed : 52.24/sec (slow!)    │  total tmouts : 13.7k (151 unique)     │
├─ fuzzing strategy yields ──────────┴───────────────┬─ path geometry ────────┤
│   bit flips : n/a, n/a, n/a                        │    levels : 5          │
│  byte flips : n/a, n/a, n/a                        │   pending : 2543       │
│ arithmetics : n/a, n/a, n/a                        │  pend fav : 73         │
│  known ints : n/a, n/a, n/a                        │ own finds : 1040       │
│  dictionary : n/a, n/a, n/a                        │  imported : n/a        │
│       havoc : 515/267k, 550/121k                   │ stability : 98.86%     │
│        trim : 17.53%/15.3k, n/a                    ├────────────────────────┘
└────────────────────────────────────────────────────┘          [cpu: 67%]

+++ Testing aborted by user +++

[!] Stopped during the first cycle, results may be incomplete.
    (For info on resuming, see /usr/local/Cellar/afl-fuzz/2.57b_1/share/doc/afl/README.)
[+] We're done here. Have a nice day!

(base) donatostanco@MacBook-Pro-di-Donato ImageMagick-6.7.9-10 %
```

This test was made for completeness and the number of PNG files used for the tests is the same as that provided by the AFL archive i.e. 1652 images. In this case I finished testing after an hour and a half, in which I obtained **2692 mutations** generated by afl, finding **33 uniq crashes** and **64 uniq hangs** were found, because given the greater number of files, my device's memory ran out earlier.

Also in this case I applied the convert to all files that caused the crash and I got the same results, all the crashes are segmentation fault.



```
(base) donatostanco@MacBook-Pro-di-Donato crashes % sh ../../../script.sh
FILE: README.txt
---------------------------------
FILE: id:000000,sig:11,src:001656+000407,op:splice,rep:32
../../../script.sh: line 3: 89969 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000001,sig:11,src:001656+001026,op:splice,rep:32
../../../script.sh: line 3: 89970 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000002,sig:11,src:001660+001900,op:splice,rep:16
../../../script.sh: line 3: 89971 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000003,sig:11,src:001736+002011,op:splice,rep:128
../../../script.sh: line 3: 89972 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000004,sig:11,src:001793,op:havoc,rep:4
../../../script.sh: line 3: 89973 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000005,sig:11,src:001793+002057,op:splice,rep:16
../../../script.sh: line 3: 89974 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000006,sig:11,src:001807+001935,op:splice,rep:32
../../../script.sh: line 3: 89975 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000007,sig:11,src:001808,op:havoc,rep:4
../../../script.sh: line 3: 89976 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000008,sig:11,src:001866,op:havoc,rep:32
../../../script.sh: line 3: 89977 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000009,sig:11,src:001912+002044,op:splice,rep:64
../../../script.sh: line 3: 89978 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000010,sig:11,src:001988,op:havoc,rep:2
../../../script.sh: line 3: 89979 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000011,sig:11,src:002037,op:havoc,rep:8
../../../script.sh: line 3: 89980 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000012,sig:11,src:002037,op:havoc,rep:8
../../../script.sh: line 3: 89981 Segmentation fault: 11  /Users/donatostanco/Desktop/ImageMagick-6.7.9-10/bin/convert $i /dev/null
---------------------------------
FILE: id:000013,sig:11,src:002037,op:havoc,rep:64
```