

demo

February 24, 2021

1 Demo for functional usage of CFG-explorer

Now, `cfg-explorer` can not only be used as a command line tool. We can also call it within a Python program.

1.1 Download Spec CPU Benchmark 2006

Save the suite outside our current repository:

```
$ cd ..  
$ git clone https://github.com/Multi2Sim/m2s-bench-spec2006
```

Every `.i386` file is a binary file for testing.

To demonstrate, an sample [specrand_base.i386](#) is copied to current path.

1.2 Import Libraries

If you have not installed `cfg_explorer` module, you can install it with

```
$ pip install cfg_explorer
```

Of course, If you just want to try it without installation, it's Okay:

First, to import `cfg_explore` in this subdirectory, you should include your `cfg-explorer` path into your `PATH` environment variable. You can do this by (suppose the whole `cfg-explorer` directory is located in `$HOME/cfg-explorer`):

```
$ export PATH=$HOME/cfg-explorer:$PATH
```

Or import it in this notebook by such an approach for that the target folder is actually the parent folder of this file:

```
[1]: import os  
import sys  
from pathlib import Path  
  
sys.path.insert(0, str(Path().resolve().parent))
```

1.3 Usages of `cfg_explore` Function

```
[2]: from cfgexplorer import cfg_explore
```

1.3.1 Launch an interactive web app

Now, call `cfg_explore` with the only argument `binary`, which is the path of the binary file we prepare to analysis. After running, it will host a website on `http://127.0.0.1:5050/` to show the *control flow graph* of the file. You can specify the port by `port` parameter.

```
[3]: cfg_explore(binary='./specrand_base.i386')
```

```
WARNING | 2021-02-24 17:53:21,073 | angr.analyses.cfg.cfg_fast |  
"collect_data_references" is deprecated and will be removed soon. Please  
use "data_references" instead  
WARNING | 2021-02-24 17:53:21,076 |  
angr.storage.memory_mixins.default_filler_mixin | The program is  
accessing memory or registers with an unspecified value. This could indicate  
unwanted behavior.  
WARNING | 2021-02-24 17:53:21,076 |  
angr.storage.memory_mixins.default_filler_mixin | angr will cope  
with this by generating an unconstrained symbolic variable and continuing. You  
can resolve this by:  
WARNING | 2021-02-24 17:53:21,077 |  
angr.storage.memory_mixins.default_filler_mixin | 1) setting a  
value to the initial state  
WARNING | 2021-02-24 17:53:21,079 |  
angr.storage.memory_mixins.default_filler_mixin | 2) adding the  
state option ZERO_FILL_UNCONSTRAINED_{MEMORY,REGISTERS}, to make unknown regions  
hold null  
WARNING | 2021-02-24 17:53:21,079 |  
angr.storage.memory_mixins.default_filler_mixin | 3) adding the  
state option SYMBOL_FILL_UNCONSTRAINED_{MEMORY,REGISTERS}, to suppress these  
messages.  
WARNING | 2021-02-24 17:53:21,080 |  
angr.storage.memory_mixins.default_filler_mixin | Filling register  
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded  
object)  
WARNING | 2021-02-24 17:53:21,082 |
```

```

angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:53:21,142 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:53:21,144 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
* Serving Flask app "cfgexplorer.explorer" (lazy loading)
* Environment: production
  WARNING: This is a development server. Do not use it in a production
deployment.
  Use a production WSGI server instead.
* Debug mode: on
INFO | 2021-02-24 17:53:21,235 | werkzeug | * Running on
http://127.0.0.1:5000/ (Press CTRL+C to quit)
INFO | 2021-02-24 17:53:37,765 | werkzeug | 127.0.0.1 - -
[24/Feb/2021 17:53:37] "GET / HTTP/1.1" 200 -
INFO | 2021-02-24 17:53:37,909 | werkzeug | 127.0.0.1 - -
[24/Feb/2021 17:53:37] "GET /js/svg-pan-zoom.js HTTP/1.1" 200 -
INFO | 2021-02-24 17:53:38,141 | werkzeug | 127.0.0.1 - -
[24/Feb/2021 17:53:38] "GET /api/cfg/0x80483a0 HTTP/1.1" 200 -
INFO | 2021-02-24 17:53:38,424 | werkzeug | 127.0.0.1 - -
[24/Feb/2021 17:53:38] "GET /favicon.ico HTTP/1.1" 404 -
INFO | 2021-02-24 17:53:43,886 | werkzeug | 127.0.0.1 - -
[24/Feb/2021 17:53:43] "GET / HTTP/1.1" 200 -
INFO | 2021-02-24 17:53:44,402 | werkzeug | 127.0.0.1 - -
[24/Feb/2021 17:53:44] "GET /api/cfg/0x80483a0 HTTP/1.1" 200 -

```

Whenever you want to shut down the app, just interrupt the function. For example, in this notebook, click on interrupt the kernel button on the toolbar.

1.3.2 Generate multiple formats of outputs

Instead of launching a web app, you can also let `cfg_explore` generate output files by specifying output argument.

For instance, we can get the `svg` format CFG of `specrand_base.i386` using:

```
[4]: cfg_explore(binary='./specrand_base.i386',output='./test.svg')
```

```
WARNING | 2021-02-24 17:54:01,128 | angr.analyses.cfg.cfg_fast |  
"collect_data_references" is deprecated and will be removed soon. Please
```

```
use "data_references" instead
```

```
WARNING | 2021-02-24 17:54:01,131 |
```

```
angr.storage.memory_mixins.default_filler_mixin | Filling register
```

```
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded  
object)
```

```
WARNING | 2021-02-24 17:54:01,132 |
```

```
angr.storage.memory_mixins.default_filler_mixin | Filling register
```

```
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded  
object)
```

```
N/A% | | Elapsed Time: 0:00:00 ETA:
```

```
--:--:--WARNING | 2021-02-24 17:54:01,176 |
```

```
angr.storage.memory_mixins.default_filler_mixin | Filling register
```

```
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in  
specrand_base.i386 (0x80484fb))
```

```
WARNING | 2021-02-24 17:54:01,178 |
```

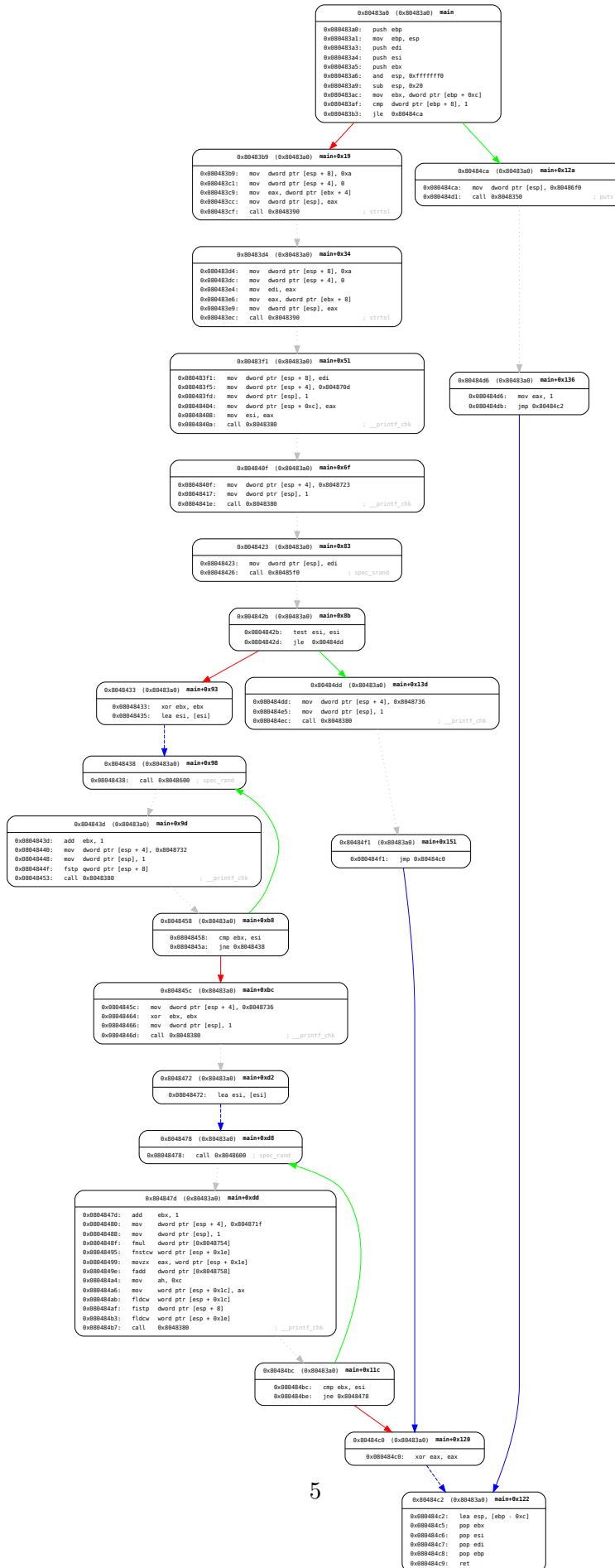
```
angr.storage.memory_mixins.default_filler_mixin | Filling register
```

```
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in  
specrand_base.i386 (0x80484fd))
```

```
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
```

`test.svg` files can be opened by web-browser directly, it can also be displayed in this notebook:

```
[5]: from IPython.core.display import SVG  
display(SVG('test.svg'))
```



There are also a bunch of formats that `cfg_explore` can handle. The only thing you need to do is to specify proper suffix (i.e. extension name) in path which is passed as `output` argument.

Current supported formats are listed as below:

```
[6]: formats = [
    'canon', 'cmap', 'cmapx', 'cmapx_np', 'dot', 'fig', 'gd', 'gd2', 'gif',
    'imap', 'imap_np', 'ismap', 'jpe', 'jpeg', 'jpg', 'mp', 'pdf', 'plain',
    'plain-ext', 'png', 'ps', 'ps2', 'svg', 'svgz', 'vml', 'vmlz', 'vrml',
    'wbmp', 'xdot', 'raw'
]
```

Try all formats by:

```
[7]: for format in formats:
    cfg_explore(binary='./specrand_base.i386', output='./test.'+format)
```

```
0x0 (not part of a loaded object)
WARNING | 2021-02-24 17:56:31,907 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% |                               | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:31,948 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:31,950 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
WARNING | 2021-02-24 17:56:32,206 | angr.analyses.cfg.cfg_fast |
"collect_data_references" is deprecated and will be removed soon. Please
use "data_references" instead
WARNING | 2021-02-24 17:56:32,209 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:32,210 |
```

```

angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:32,252 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:32,254 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
WARNING | 2021-02-24 17:56:32,609 | angr.analyses.cfg.cfg_fast |
"collect_data_references" is deprecated and will be removed soon. Please
use "data_references" instead
WARNING | 2021-02-24 17:56:32,612 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:32,613 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:32,654 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:32,655 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
WARNING | 2021-02-24 17:56:32,890 | angr.analyses.cfg.cfg_fast |
"collect_data_references" is deprecated and will be removed soon. Please
use "data_references" instead
WARNING | 2021-02-24 17:56:32,893 |

```

```

angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:32,894 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:32,936 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:32,937 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
WARNING | 2021-02-24 17:56:33,188 | angr.analyses.cfg.cfg\_fast |
"collect\_data\_references" is deprecated and will be removed soon. Please
use "data\_references" instead
WARNING | 2021-02-24 17:56:33,191 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:33,192 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:33,236 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:33,238 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00

```



```

WARNING | 2021-02-24 17:56:33,502 | angr.analyses.cfg.cfg_fast |
"collect_data_references" is deprecated and will be removed soon. Please
use "data_references" instead
WARNING | 2021-02-24 17:56:33,505 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:33,506 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:33,549 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:33,551 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
WARNING | 2021-02-24 17:56:33,807 | angr.analyses.cfg.cfg_fast |
"collect_data_references" is deprecated and will be removed soon. Please
use "data_references" instead
WARNING | 2021-02-24 17:56:33,810 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:33,812 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:33,853 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:33,855 |

```

```

angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
WARNING | 2021-02-24 17:56:34,213 | angr.analyses.cfg.cfg_fast |
"collect_data_references" is deprecated and will be removed soon. Please
use "data_references" instead
WARNING | 2021-02-24 17:56:34,216 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:34,217 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:34,259 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:34,261 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
WARNING | 2021-02-24 17:56:34,521 | angr.analyses.cfg.cfg_fast |
"collect_data_references" is deprecated and will be removed soon. Please
use "data_references" instead
WARNING | 2021-02-24 17:56:34,523 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:34,525 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:34,566 |

```

```

angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:34,568 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
WARNING | 2021-02-24 17:56:34,926 | angr.analyses.cfg.cfg_fast |
"collect_data_references" is deprecated and will be removed soon. Please
use "data_references" instead
WARNING | 2021-02-24 17:56:34,929 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:34,930 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:34,971 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:34,973 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
WARNING | 2021-02-24 17:56:35,249 | angr.analyses.cfg.cfg_fast |
"collect_data_references" is deprecated and will be removed soon. Please
use "data_references" instead
WARNING | 2021-02-24 17:56:35,253 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:35,254 |

```

```

angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:35,297 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:35,298 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
WARNING | 2021-02-24 17:56:35,571 | angr.analyses.cfg.cfg_fast |
"collect_data_references" is deprecated and will be removed soon. Please
use "data_references" instead
WARNING | 2021-02-24 17:56:35,575 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:35,576 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:35,618 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:35,619 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
WARNING | 2021-02-24 17:56:35,906 | angr.analyses.cfg.cfg_fast |
"collect_data_references" is deprecated and will be removed soon. Please
use "data_references" instead
WARNING | 2021-02-24 17:56:35,910 |

```

```

angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:35,911 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:35,962 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:35,964 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
WARNING | 2021-02-24 17:56:36,267 | angr.analyses.cfg.cfg\_fast |
"collect\_data\_references" is deprecated and will be removed soon. Please
use "data\_references" instead
WARNING | 2021-02-24 17:56:36,271 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:36,272 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:36,314 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:36,316 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00

```

```

WARNING | 2021-02-24 17:56:36,677 | angr.analyses.cfg.cfg_fast |
"collect_data_references" is deprecated and will be removed soon. Please
use "data_references" instead
WARNING | 2021-02-24 17:56:36,680 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:36,681 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:36,722 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:36,724 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
WARNING | 2021-02-24 17:56:37,145 | angr.analyses.cfg.cfg_fast |
"collect_data_references" is deprecated and will be removed soon. Please
use "data_references" instead
WARNING | 2021-02-24 17:56:37,147 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:37,148 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:37,188 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:37,189 |

```

```

angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
WARNING | 2021-02-24 17:56:37,487 | angr.analyses.cfg.cfg_fast |
"collect_data_references" is deprecated and will be removed soon. Please
use "data_references" instead
WARNING | 2021-02-24 17:56:37,489 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
WARNING | 2021-02-24 17:56:37,491 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)
N/A% | | Elapsed Time: 0:00:00 ETA:
--:--:--WARNING | 2021-02-24 17:56:37,531 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))
WARNING | 2021-02-24 17:56:37,533 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
View the output png:

```

1.3.3 Traversal a large folder to generate all CFGs

We still use `m2s-bench-spec2006` as an example.

Assume that we need to analyze all binary files in this folder. Wrapping `cfg-explorer` as a function makes the task more flexible inside a Python script.

First, get all potential binary files for analysis:

```

[8]: from glob import glob
progs = sorted(glob('../m2s-bench-spec2006/*/*.i386'))
progs

```

```
[8]: ['.../m2s-bench-spec2006/401.bzip2/bzip2_base.i386',
      '.../m2s-bench-spec2006/403.gcc/gcc_base.i386',
      '.../m2s-bench-spec2006/410.bwaves/bwaves_base.i386',
      '.../m2s-bench-spec2006/416.gamess/gamess_base.i386',
      '.../m2s-bench-spec2006/429.mcf/mcf_base.i386',
      '.../m2s-bench-spec2006/433.milc/milc_base.i386',
      '.../m2s-bench-spec2006/434.zeusmp/zeusmp_base.i386',
      '.../m2s-bench-spec2006/435.gromacs/gromacs_base.i386',
      '.../m2s-bench-spec2006/436.cactusADM/cactusADM_base.i386',
      '.../m2s-bench-spec2006/437.leslie3d/leslie3d_base.i386',
      '.../m2s-bench-spec2006/444.namd/namd_base.i386',
      '.../m2s-bench-spec2006/445.gobmk/gobmk_base.i386',
      '.../m2s-bench-spec2006/447.dealII/dealII_base.i386',
      '.../m2s-bench-spec2006/450.soplex/soplex_base.i386',
      '.../m2s-bench-spec2006/453.povray/povray_base.i386',
      '.../m2s-bench-spec2006/454.calculix/calculix_base.i386',
      '.../m2s-bench-spec2006/456.hmmmer/hmmmer_base.i386',
      '.../m2s-bench-spec2006/458.sjeng/sjeng_base.i386',
      '.../m2s-bench-spec2006/459.GemsFDTD/GemsFDTD_base.i386',
      '.../m2s-bench-spec2006/462.libquantum/libquantum_base.i386',
      '.../m2s-bench-spec2006/464.h264ref/h264ref_base.i386',
      '.../m2s-bench-spec2006/465.tonto/tonto_base.i386',
      '.../m2s-bench-spec2006/470.lbm/lbm_base.i386',
      '.../m2s-bench-spec2006/471.omnetpp/omnetpp_base.i386',
      '.../m2s-bench-spec2006/473.astar/astar_base.i386',
      '.../m2s-bench-spec2006/481.wrf/wrf_base.i386',
      '.../m2s-bench-spec2006/482.sphinx3/sphinx3_base.i386',
      '.../m2s-bench-spec2006/483.xalancbmk/xalancbmk_base.i386',
      '.../m2s-bench-spec2006/998.specrand/specrand_base.i386',
      '.../m2s-bench-spec2006/999.specrand/specrand_base.i386']
```

```
[9]: # create a directory to store the outputs
out_dir = './output'
if not os.path.exists(out_dir):
    os.mkdir(out_dir)
```

Then, we can simply call `cfg_explore` function inside loops. Keep it alone, we just need to wait for generating all 'svg' files.

Note: it might take a extremely long time. Be patient.

```
[10]: for p in progs:
        name = p.split('/')[3]
        print('start analysis of:', name)
        output_file = os.path.join(out_dir, name + '.svg')
        if not os.path.exists(output_file):
            cfg_explore(binary=p, output=output_file)
```



```

start analysis of: 401.bzip2
start analysis of: 403.gcc
start analysis of: 410.bwaves
start analysis of: 416.gamess
start analysis of: 429.mcf
start analysis of: 433.milc
start analysis of: 434.zeusmp
start analysis of: 435.gromacs
start analysis of: 436.cactusADM
start analysis of: 437.leslie3d
start analysis of: 444.namd
start analysis of: 445.gobmk
start analysis of: 447.dealII
start analysis of: 450.soplex
start analysis of: 453.povray
start analysis of: 454.calculix
start analysis of: 456.hmmmer
start analysis of: 458.sjeng
start analysis of: 459.GemsFDTD
start analysis of: 462.libquantum
start analysis of: 464.h264ref
start analysis of: 465.tonto
start analysis of: 470.lbm
start analysis of: 471.omnetpp
start analysis of: 473.astar
start analysis of: 481.wrf
start analysis of: 482.sphinx3
start analysis of: 483.xalancbmk
start analysis of: 998.specrand
start analysis of: 999.specrand

```

Now, you can view all outputs in `out_dir`.

2 Get output files for more than one functions at once

If `output` is specified as a non-empty and valid filename, you can analyze CFG with multiple start addresses by passing an address list to `starts`. Addresses can also be specified as symbol names (e.g. function name) used in source codes in the binary.

For example, now, we are going to get all function names in `specrand_base.i386`:

```

[8]: import angr

[11]: proj = angr.Project('./specrand_base.i386', load_options={'auto_load_libs':
    ↪False})
    idfer = proj.analyses.Identifier()
    names = [funcInfo.name for funcInfo in idfer.func_info]

```

```
print(names)
```

CRITICAL | 2021-02-24 18:07:13,165 | angr.analyses.identifier.identify
| The identifier currently works only on CGC binaries. Results may be
completely unexpected.

WARNING | 2021-02-24 18:07:13,168 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)

WARNING | 2021-02-24 18:07:13,169 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded
object)

WARNING | 2021-02-24 18:07:13,211 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
eax with 4 unconstrained bytes referenced from 0x80484fb (_start+0x8 in
specrand_base.i386 (0x80484fb))

WARNING | 2021-02-24 18:07:13,212 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
edx with 4 unconstrained bytes referenced from 0x80484fd (_start+0xa in
specrand_base.i386 (0x80484fd))

WARNING | 2021-02-24 18:07:13,822 |
angr.storage.memory_mixins.default_filler_mixin | Filling register
mm0 with 8 unconstrained bytes referenced from 0x804844f (main+0xaf in
specrand_base.i386 (0x804844f))

['_init', 'puts', 'sub_8048356', '__gmon_start__', '__libc_start_main',
 '__printf_chk', 'strtoul', 'main', 'deregister_tm_clones', 'register_tm_clones',
 '__do_global_ctors_aux', 'frame_dummy', '__libc_csu_init']

The CFG of those functions should be exported to a folder called spec_func

```
[12]: dir = './spec_func/'  
      if not os.path.exists(dir):  
          os.mkdir(dir)
```

Then, analyze all those functions above:

```
[14]: cfg_explore(binary='./specrand_base.i386', output=os.path.join(dir, './test.  
      ↪svg'), starts=names)
```

WARNING | 2021-02-24 18:12:54,615 | axt.cfgexplorer | Starting
address unrecognized sub_8048356

```
WARNING | 2021-02-24 18:12:54,618 | angr.analyses.cfg.cfg_fast |  
"collect_data_references" is deprecated and will be removed soon. Please  
use "data_references" instead
```

```
WARNING | 2021-02-24 18:12:54,620 |  
angr.storage.memory_mixins.default_filler_mixin | Filling register  
es with 4 unconstrained bytes referenced from 0x0 (not part of a loaded  
object)
```

```
WARNING | 2021-02-24 18:12:54,622 |  
angr.storage.memory_mixins.default_filler_mixin | Filling register  
gs with 4 unconstrained bytes referenced from 0x0 (not part of a loaded  
object)
```

```
100% |#####| Elapsed Time: 0:00:00 Time: 0:00:00
```

Some of them may not have a plotable CFG to export, thus all CFGs derived from the binary are:

```
[15]: !ls {dir}
```

```
test-deregister_tm_clones.svg  test-__libc_csu_init.svg  
test-__do_global_dtors_aux.svg test-main.svg  
test-frame_dummy.svg         test-register_tm_clones.svg  
test-_init.svg               test.svg
```

```
[ ]:
```