若不知道该使用afl-clang-lto 或 afl-clang-fast，可以查看从 [AFLplusplus](https://github.com/AFLplusplus/AFLplusplus#1-instrumenting-that-target) 中提取的下图： 检测该目标

+--------------------------------+

| clang/clang++ 11+ is available | --> use LTO mode (afl-clang-lto/afl-clang-lto++)

+--------------------------------+ see [instrumentation/README.lto.md](instrumentation/README.lto.md)

|

| if not, or if the target fails with LTO afl-clang-lto/++

|

v

+---------------------------------+

| clang/clang++ 6.0+ is available | --> use LLVM mode (afl-clang-fast/afl-clang-fast++)

+---------------------------------+ see [instrumentation/README.llvm.md](instrumentation/README.llvm.md)

|

| if not, or if the target fails with LLVM afl-clang-fast/++

|

v

+--------------------------------+

| gcc 5+ is available | -> use GCC\_PLUGIN mode (afl-gcc-fast/afl-g++-fast)

+--------------------------------+ see [instrumentation/README.gcc\_plugin.md](instrumentation/README.gcc\_plugin.md) and

[instrumentation/README.instrument\_list.md](instrumentation/README.instrument\_list.md)

|

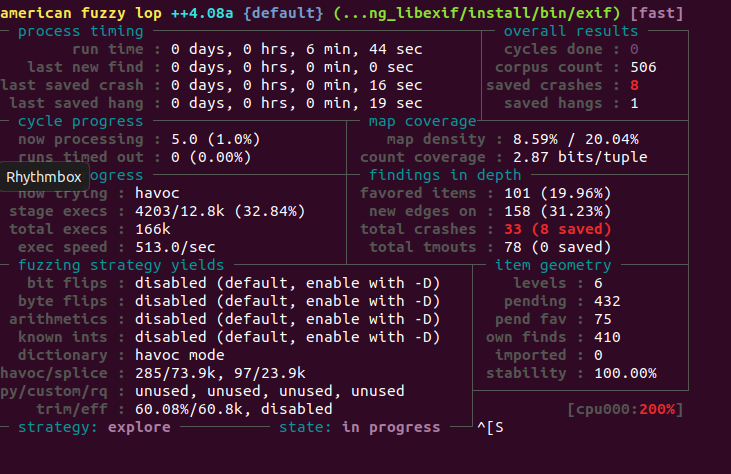
| if not, or if you do not have a gcc with plugin support

|

v

use GCC mode (afl-gcc/afl-g++) (or afl-clang/afl-clang++ for clang)

afl-fuzz -i $HOME/fuzzing\_libexif/exif-samples-master/jpg/ -o $HOME/fuzzing\_libexif/out/ -s 123 -- $HOME/fuzzing\_libexif/install/bin/exif @@



运行gdb,找出报错位置

