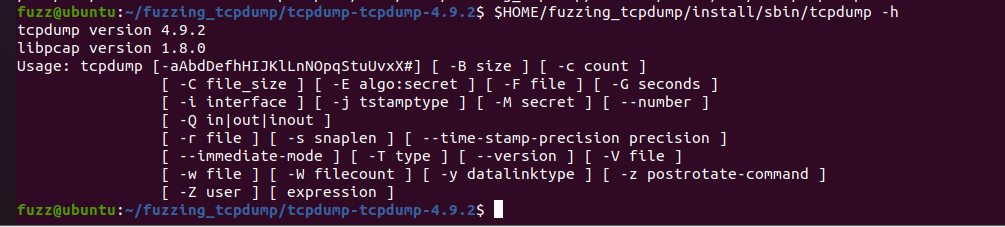
下载和构建

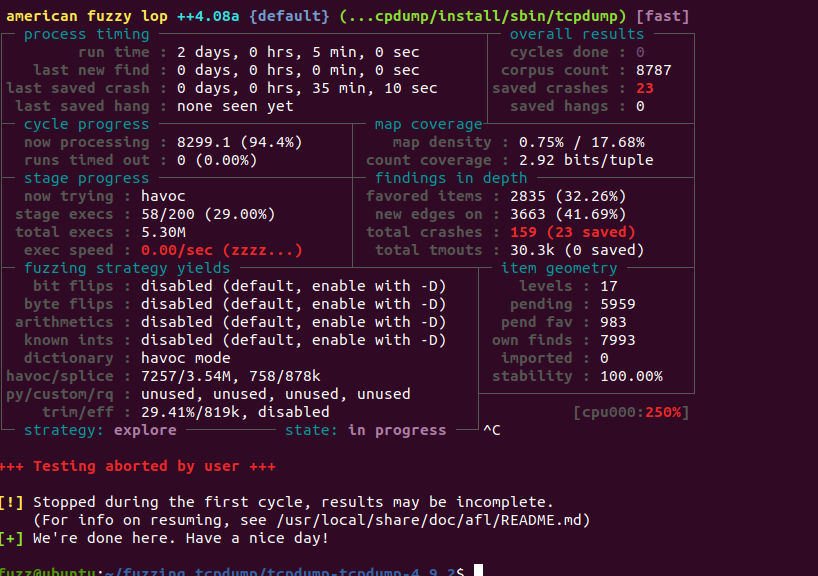
|  |  |
| --- | --- |
| 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 | cd $HOME mkdir fuzzing\_tcpdump && cd fuzzing\_tcpdump/ //下载 tcpdump-4.9.2.tar.gz wget https://github.com/the-tcpdump-group/tcpdump/archive/refs/tags/tcpdump-4.9.2.tar.gz tar -xzvf tcpdump-4.9.2.tar.gz  //下载libpcap，这是TCPdump需要的跨平台库。 wget https://github.com/the-tcpdump-group/libpcap/archive/refs/tags/libpcap-1.8.0.tar.gz tar -xzvf libpcap-1.8.0.tar.gz  //需要重命名，否则tcpdump 找不到本地路径 mv libpcap-libpcap-1.8.0/ libpcap-1.8.0  //构建并安装 libpcap cd libpcap-1.8.0/ ./configure --enable-shared=no make  //构建并安装tcpdump cd tcpdump-tcpdump-4.9.2/ ./configure --prefix="$HOME/fuzzing101/fuzzing\_tcpdump/install/" make make install  //测试是否正常 $HOME/fuzzing101/fuzzing\_tcpdump/install/sbin/tcpdump -h |

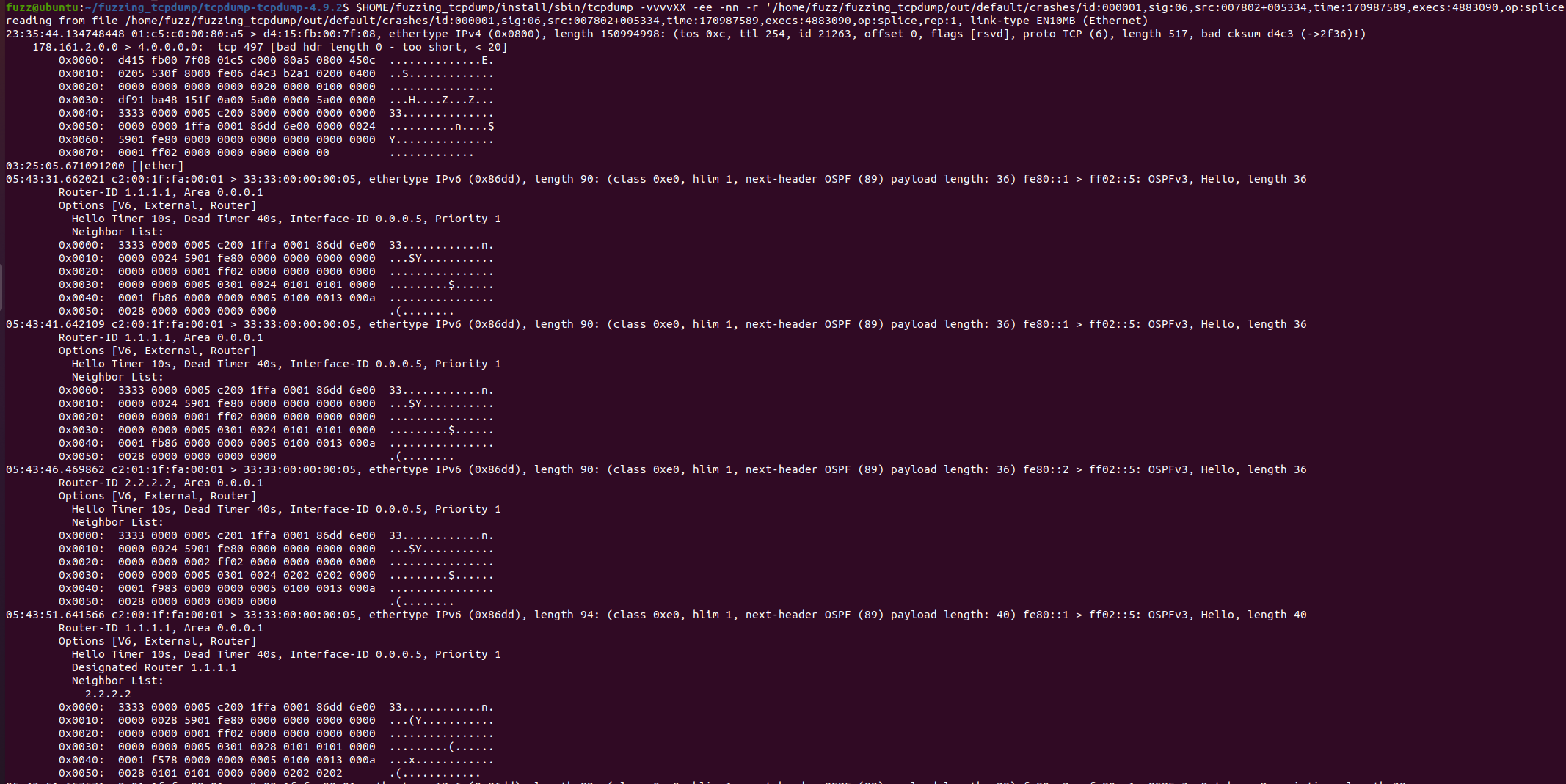


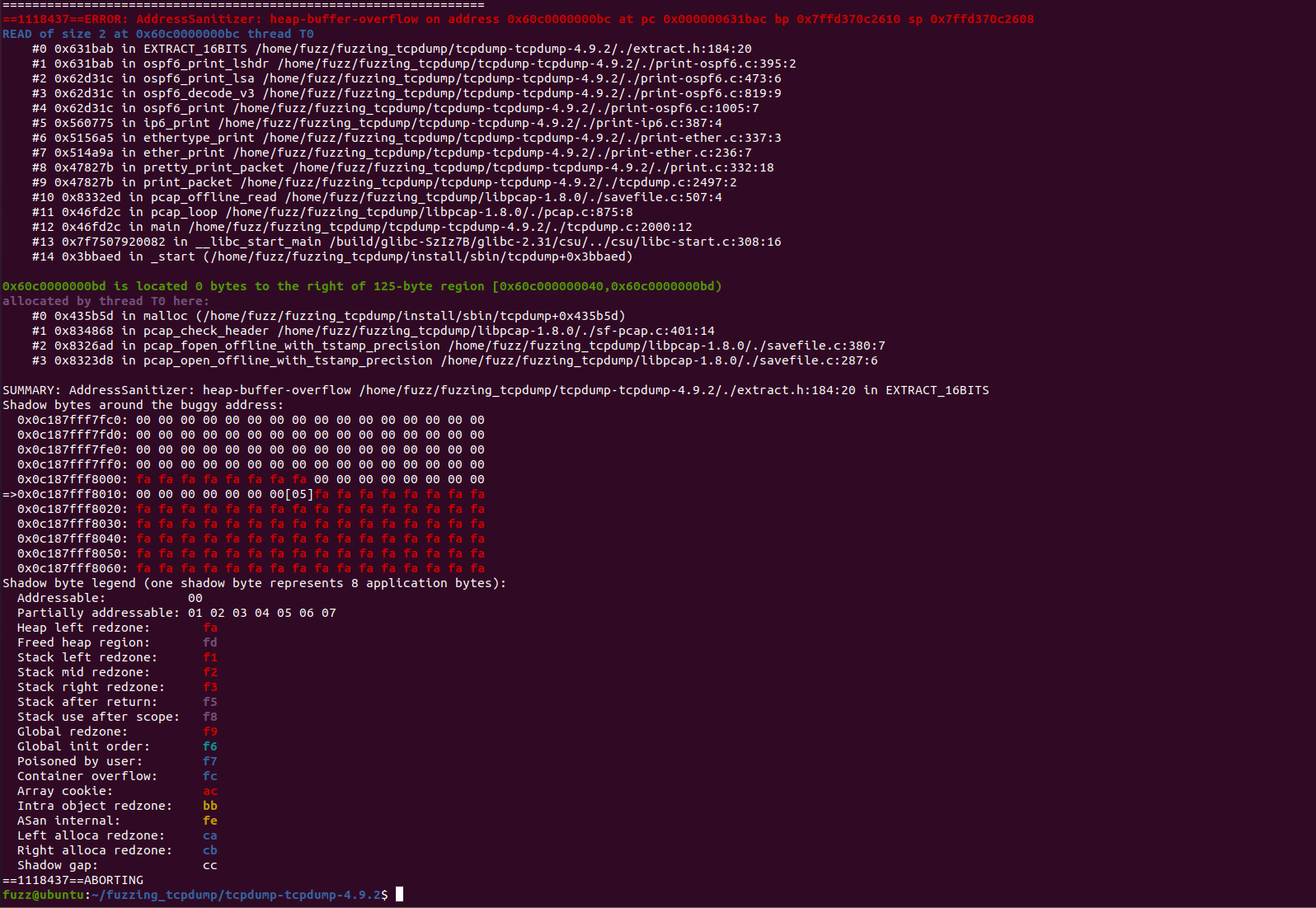
先清理所有先前编译的目标文件和可执行文件：

|  |  |
| --- | --- |
| 1 2 3 4 5 6 | rm -r $HOME/fuzzing101/fuzzing\_tcpdump/install cd $HOME/fuzzing101/fuzzing\_tcpdump/libpcap-1.8.0/ make clean  cd $HOME/fuzzing101/fuzzing\_tcpdump/tcpdump-tcpdump-4.9.2/ make clean |

|  |  |
| --- | --- |
| 1 2 3 4 5 6 7 8 9 | cd $HOME/fuzzing101/fuzzing\_tcpdump/libpcap-1.8.0/ export LLVM\_CONFIG="llvm-config-11" CC=afl-clang-lto ./configure --enable-shared=no --prefix="$HOME/fuzzing101/fuzzing\_tcpdump/install/" AFL\_USE\_ASAN=1 make  cd $HOME/fuzzing101/fuzzing\_tcpdump/tcpdump-tcpdump-4.9.2/ AFL\_USE\_ASAN=1 CC=afl-clang-lto ./configure --prefix="$HOME/fuzzing101/fuzzing\_tcpdump/install/" AFL\_USE\_ASAN=1 make AFL\_USE\_ASAN=1 make install |





直接运行crash，ASAN会给出较为详细的报错和调用栈

跑了2天才出的结果，结果显示是堆溢出。