《AFL模糊测试》实验报告

姓名：汤清云 学号：2013536 班级： 1075

**实验名称：**

AFL模糊测试实验

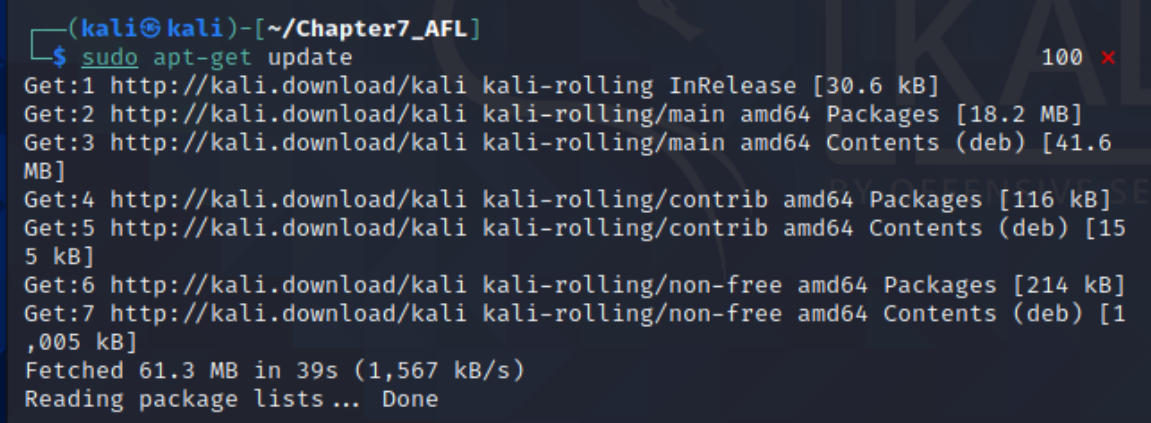
**实验要求：**

复现AFL在KALI下的安装、应用；理解覆盖引导和文件变异的概念和含义

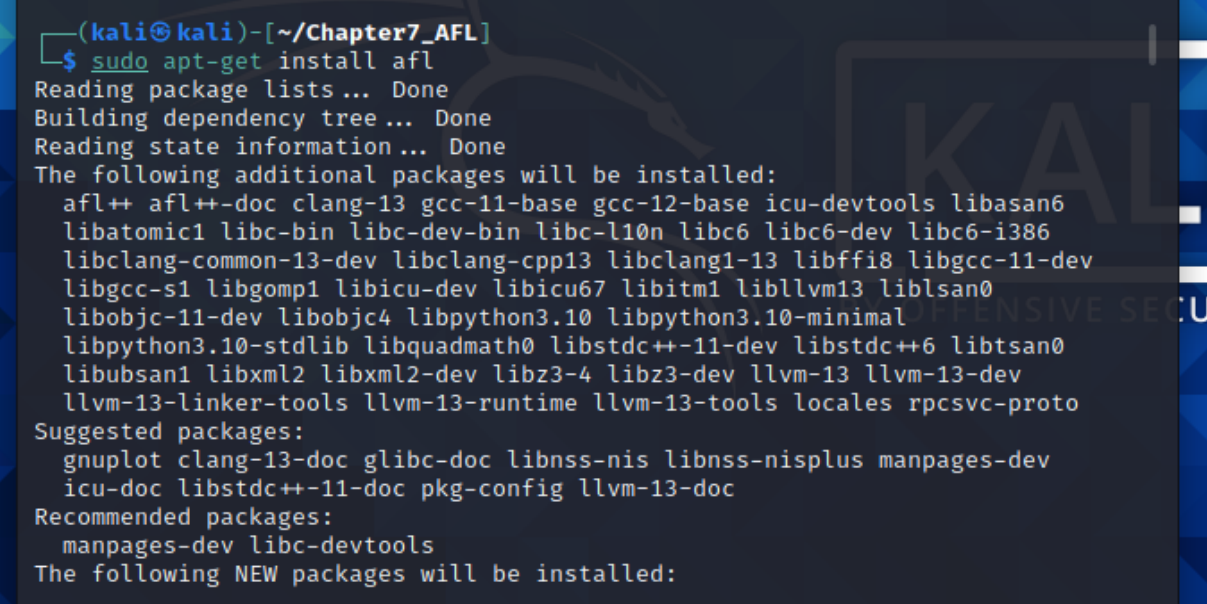
**实验过程：**

1. AFL在KALI下的安装

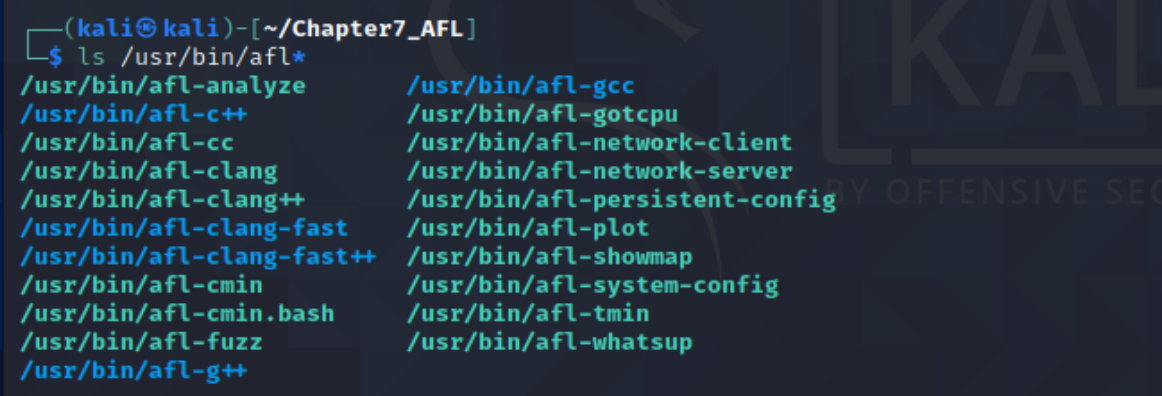
使用语句sudo apt-get update更新系统：



使用语句sudo apt-get install afl安装AFL：



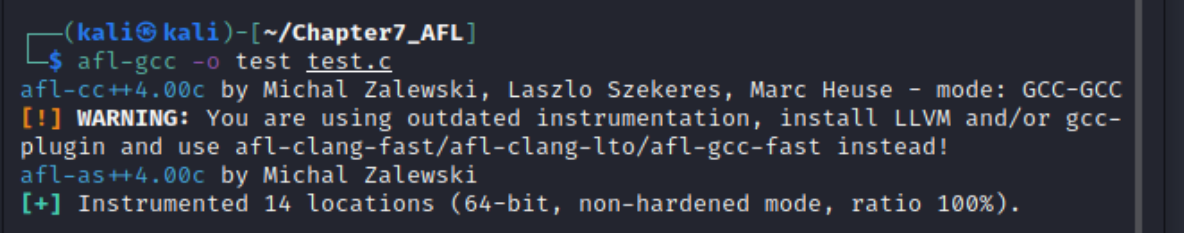
使用语句ls /usr/bin/afl\*打开查看afl目录下文件。



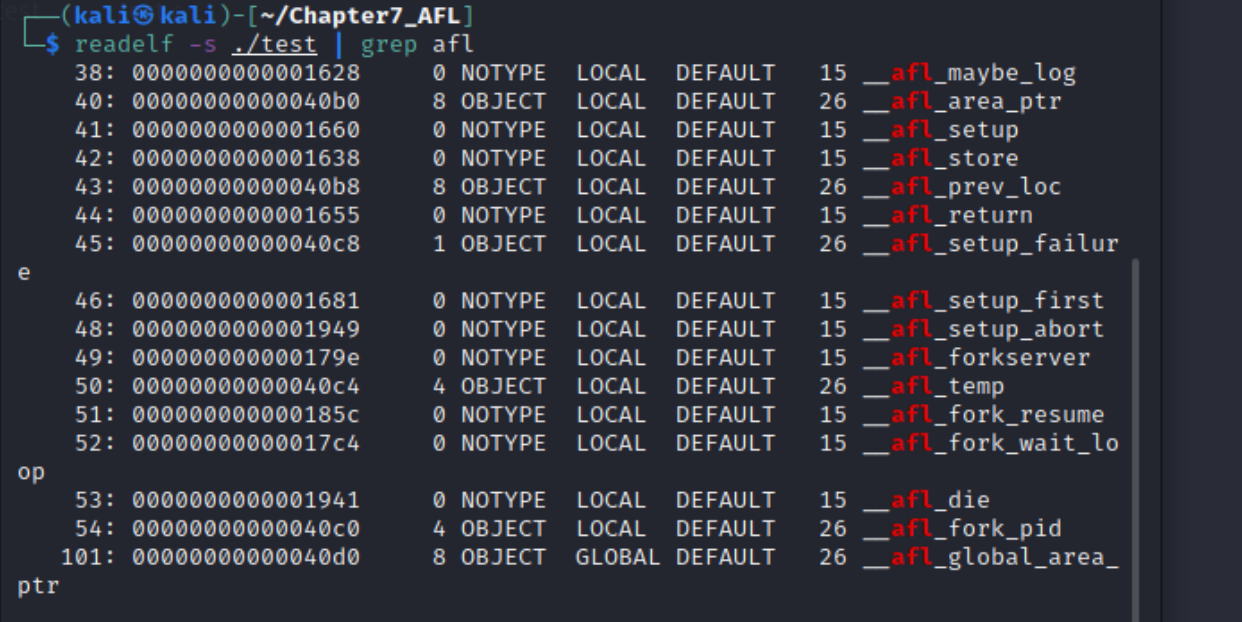
1. AFL在KALI下的应用

添加空白c语言文件命名为test.c，复制所给代码并保存，

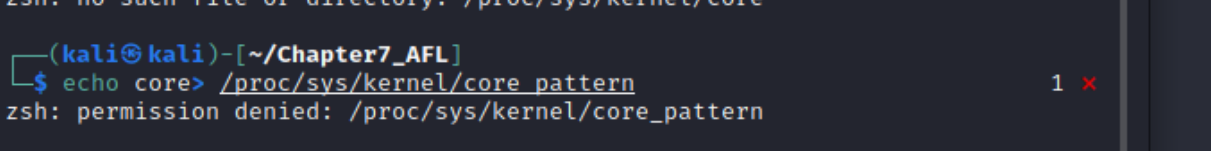
使用语句afl-gcc -o test test.c编译



使用语句readelf -s ./test | grep afl查看插桩符号

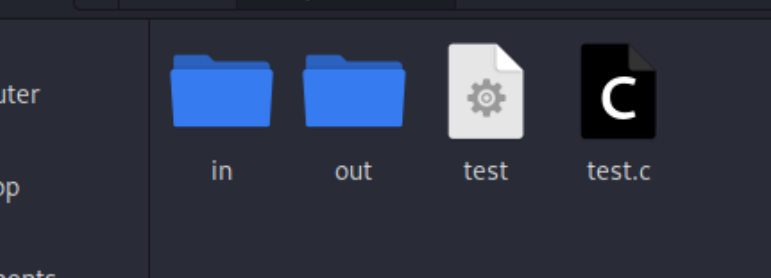


使用语句echo core > /proc/sys/kernel/ore\_pattern，将信息输出到core\_pattern位置

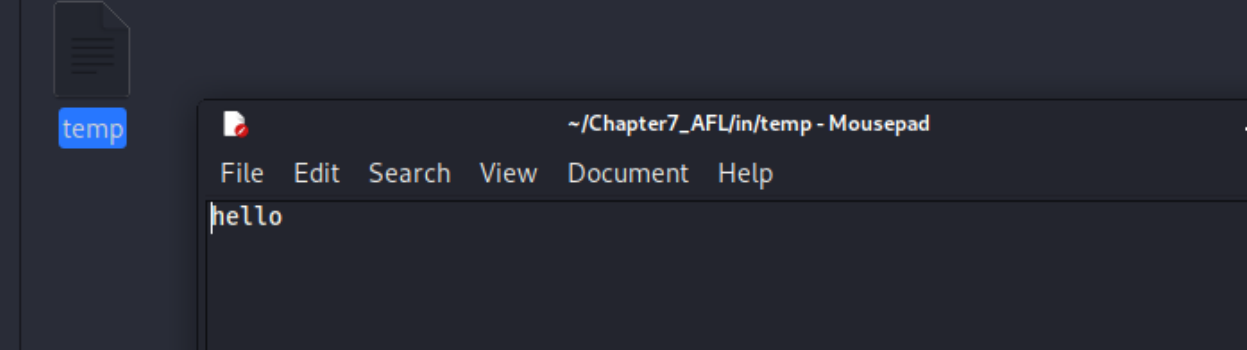


使用语句mkdir in out创建文件夹 in 和 out

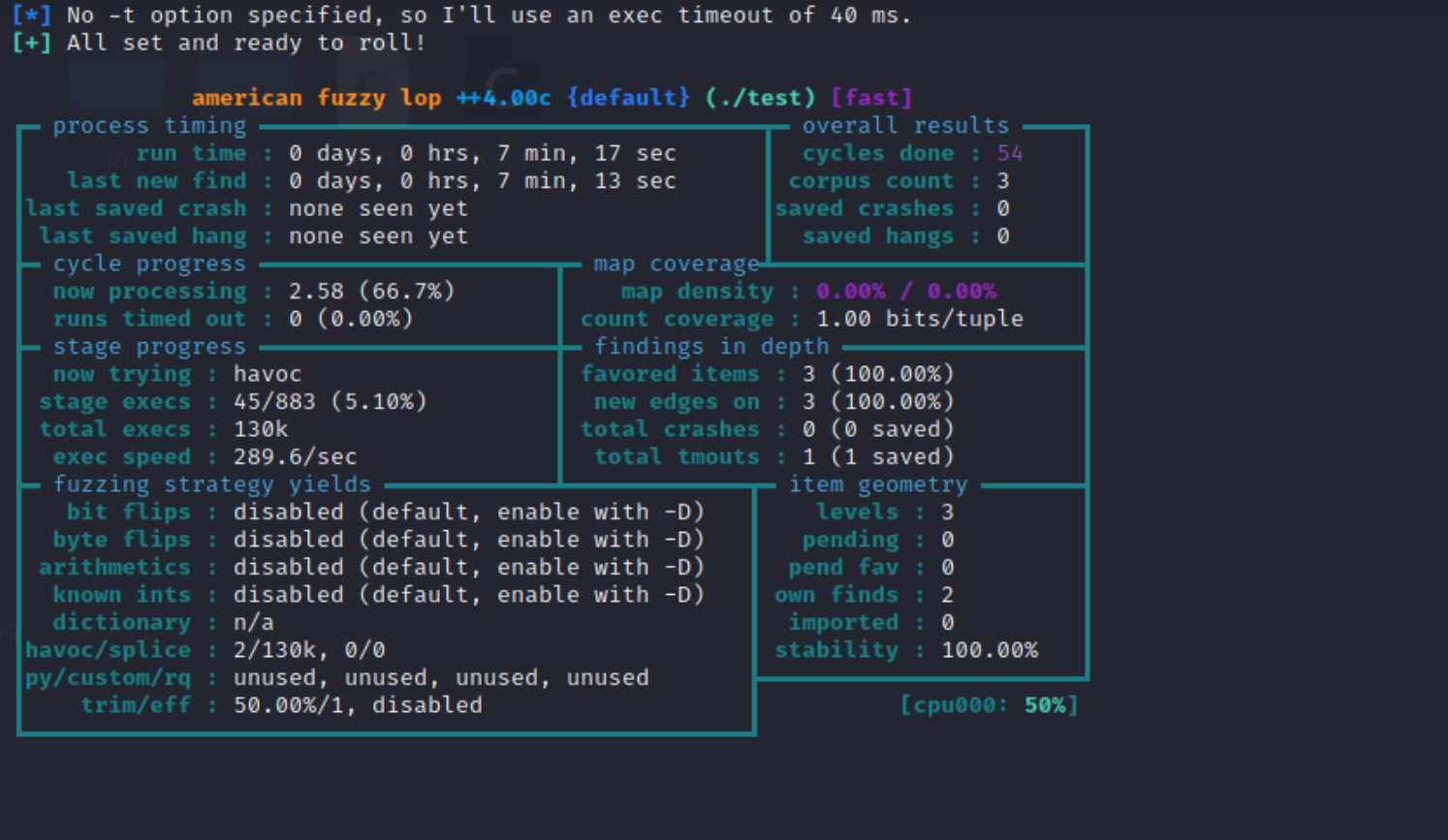




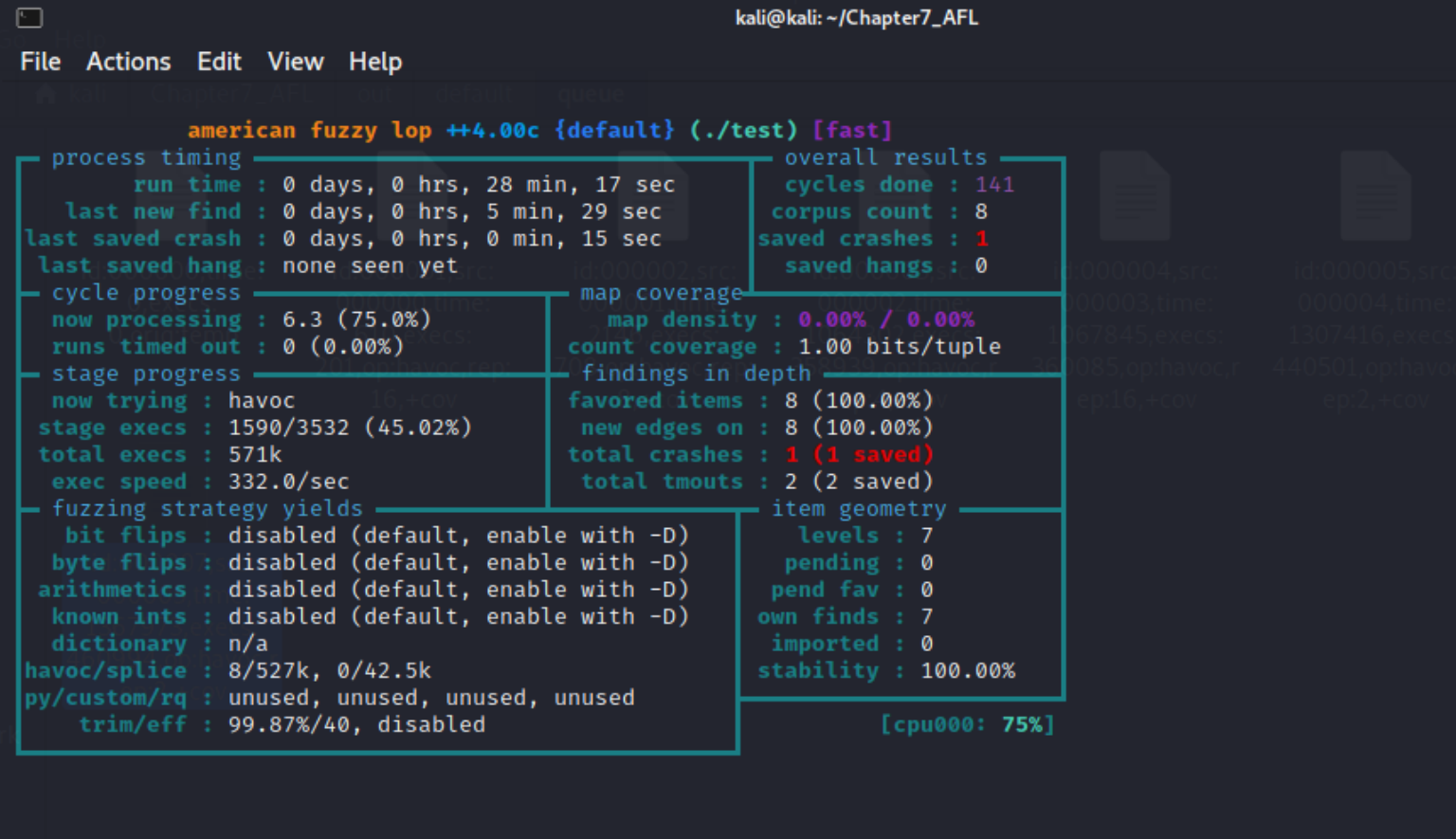
使用语句echo hello> in/temp在in文件夹中添加文件temp，并输入hello到temp文件中：



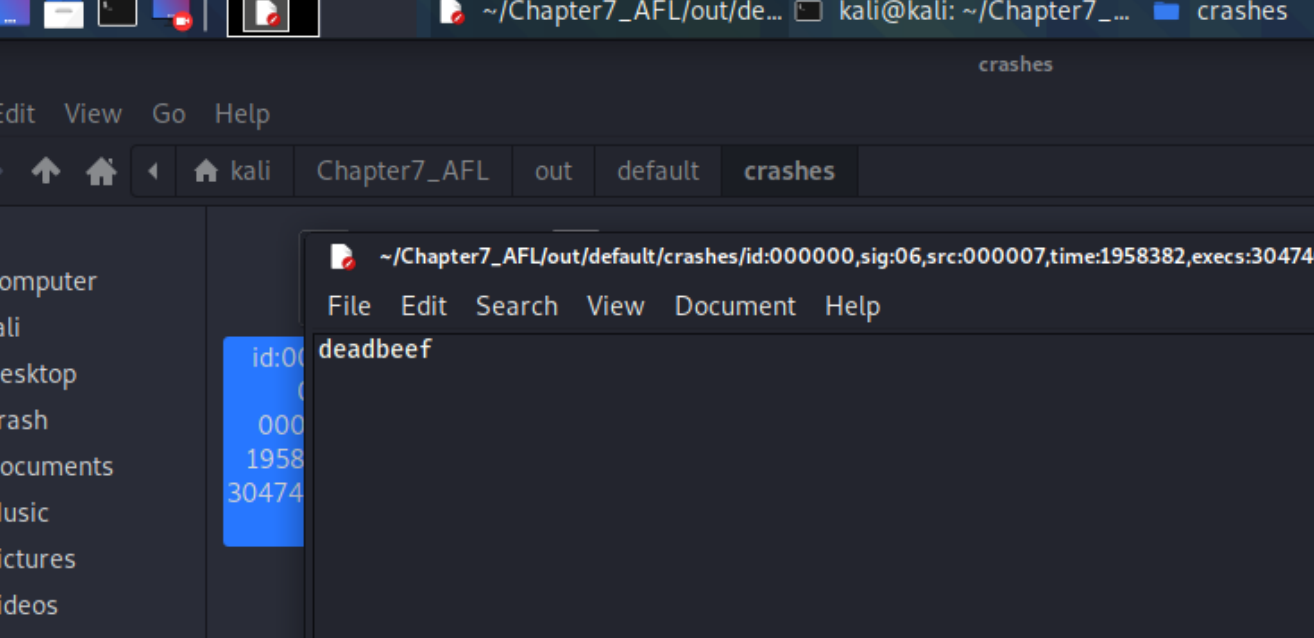
使用语句afl-fuzz -i in -o out -- ./test @@查看系统运行



运行结果为：

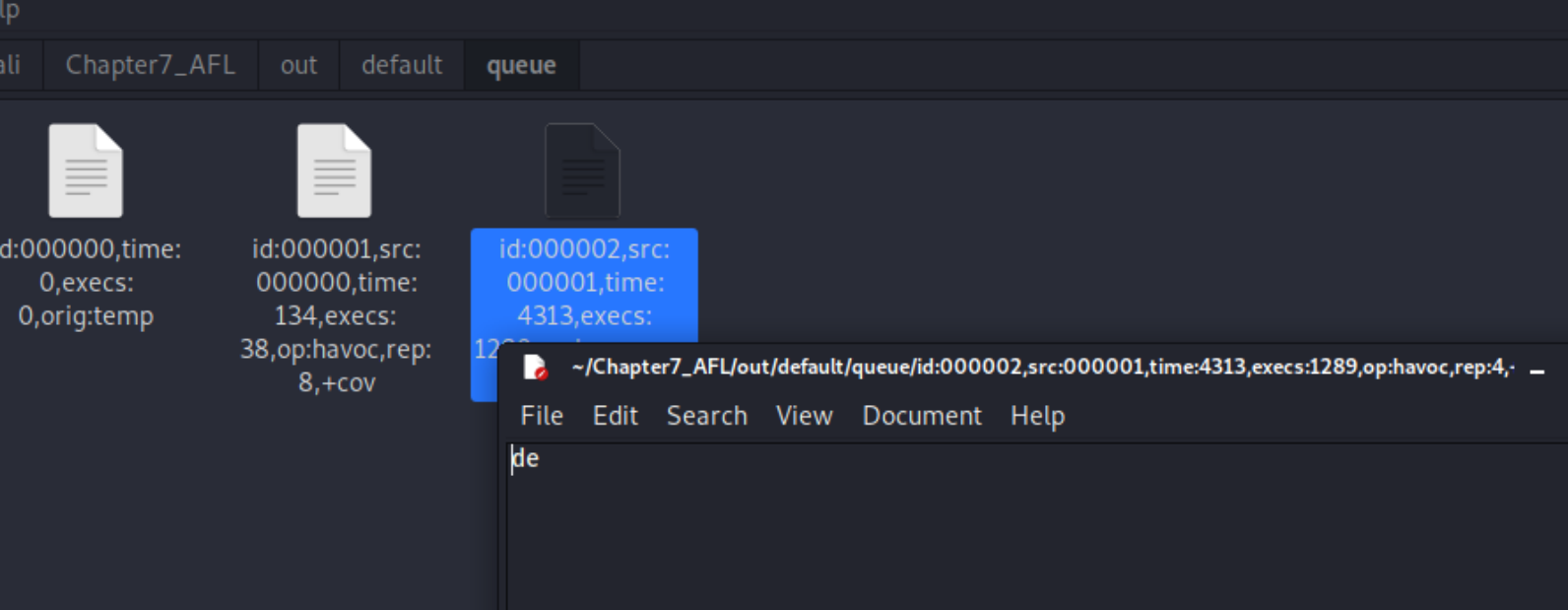


打开crashes得：



1. 覆盖引导和文件变异的概念以及含义

变异字符存放在/out/default/queue文件夹下的文档中。



覆盖引导：将文件按照一定策略进行“突变”，如果这些突变了的文件能够更新覆盖范围，则保留在队列中。

文件变异：1.按位翻转；2.从8bit级别开始进行加减操作；3。使用1过程中产生的重要的额外重要数据信息替换文件内容；4.使用token替换要进行变异的文件内容；5.对源文件进行大量变异：随机选择bit翻转；随机选择byte构成随机的重要信息；6.拼接两个文件，如果两个文件差别不大则重新选择，否则就随机选取位置将两个文件切割，将当前文件的头与随机文件的尾拼接得到新文件；7.下一轮继续变异。

**心得体会：**

对kali系统下的AFL模糊测试进行初步了解；

在老师的引导下复现了文件变异实验；

查阅资料了解了更多AFL在kali下的应用；

了解了覆盖引导和文件变异的概念以及含义。