*** Before start, below are sample file we're going to analyze and I will refer those file by Sample 1, 2 and 3.**

Sample 1:

101ccbad7732fb185d51b91d31a67ff058cac3bc31ec36cec05094065a97d6fd.sample

Sample 2:

431d230862e958dd5d20ae221ce74aba07d40dde5fd8e45f2b164905e637b1c1.sample

Sample 3:

f808a42b10cf55603389945a549ce45edc6a04562196d14f7489af04688f12bc.sample

1. What do you expect to see based on the static analysis?

Sample1: I couldn't unpack the Sample1 so there's not many thing to analyze. But from the 'strings' command I can see several IP addresses and it will try to connect a host when run this program. **In short, it uses internet connection and doing something.**

Sample2: It's not a malicious program. Anyway, it is related with file operation from the information of ELFparser. And there are also chmod and chwon string found, so it is also trying to change the permission of the file. **In short, it will change permission of the file and run some program.**

Sample3: From the information from ELFparser, it will kill some process and will create another process. It also look up and set environment variable, I think it is trying to change process with another process. **In short, it will try to run a process while killing normal process.**

2. What sorts of system calls does the program make when it runs?

Sample1:

```
open("/tmp/.X11-unix/22", O_RDWR|O_CREAT, 0600) = 0
flock(0, LOCK_EX|LOCK_NB)              = 0
rt_sigprocmask(SIG_BLOCK, ~[], [], 8)   = 0
rt_sigprocmask(SIG_SETMASK, [], NULL, 8) = 0
```

Sample2:

```
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
```

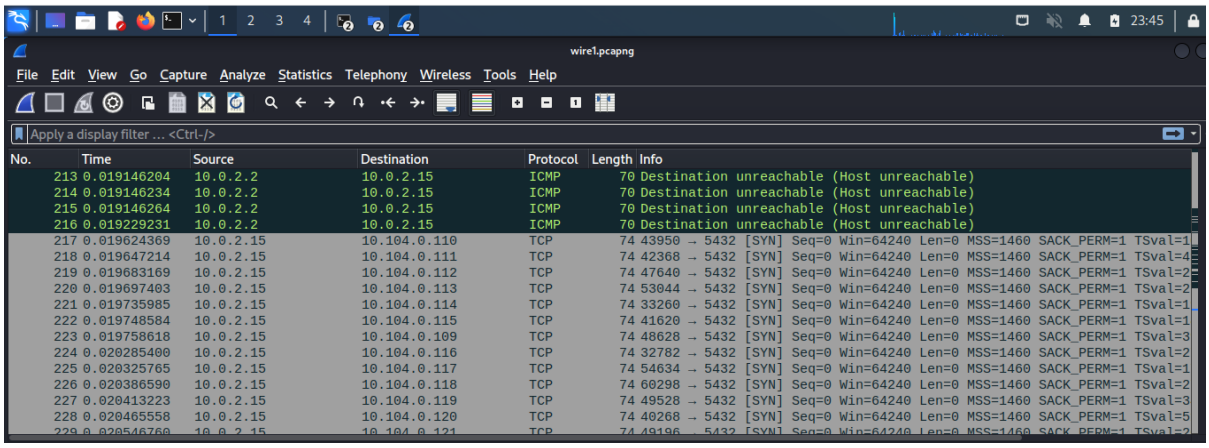
```
newfstatat(3, "", {st_mode=S_IFREG|0644, st_size=75123, ...}, AT_EMPTY_PATH)
= 0

mmap(NULL, 75123, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f6dbf120000

close(3)

openat(AT_FDCWD,      "/lib/x86_64-linux-gnu/glibc-hwcaps/x86-64-v2/libbfd-
2.30-system.so", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No such file or directory)

newfstatat(AT_FDCWD,        "/lib/x86_64-linux-gnu/glibc-hwcaps/x86-64-v2",
0x7ffee98fe3d0, 0) = -1 ENOENT (No such file or directory)
```

Sample3:

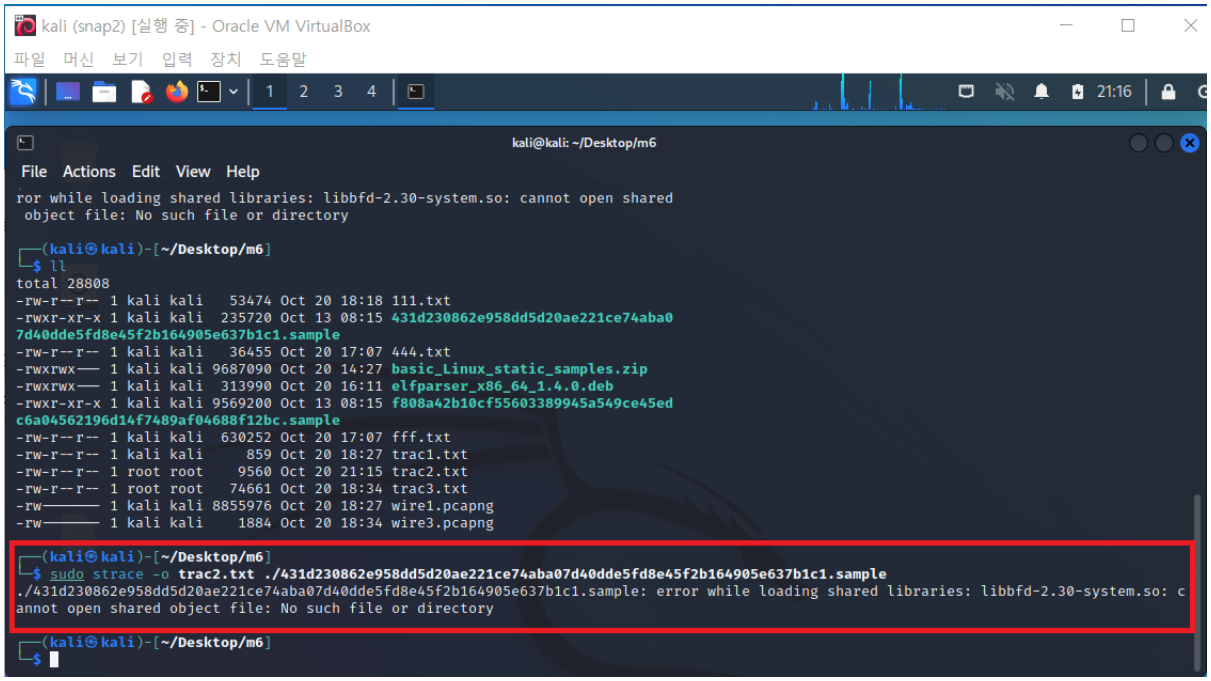
```
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libdl.so.2", O_RDONLY|O_CLOEXEC) =
3

read(3,
"\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\0\0\0\0\0\0\0\0"..., 832) =
832

newfstatat(3, "", {st_mode=S_IFREG|0644, st_size=18744, ...}, AT_EMPTY_PATH)
= 0

mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x7f0dc0da7000

pread64(3,
"\6\0\0\0\4\0\0\0@\0\0\0\0\0\0\0@\0\0\0\0\0\0\0@\0\0\0\0\0\0\0"..., 784, 64)
= 784

mprotect(0x7f0dc0d75000, 16384, PROT_READ) = 0

lseek(3, 9568256, SEEK_SET)            = 9568256

mkdir("/tmp/_MEId1VZff", 0700)         = 0

write(3,                                                                "\320\315
\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\266\17\0\0\0\0\0\0"..., 3048) =
3048

fchmod(3, 0700)                        = 0
```

3. Does the program initiate any network activity? If so, what does the network traffic look like, and can you gain any info from it?

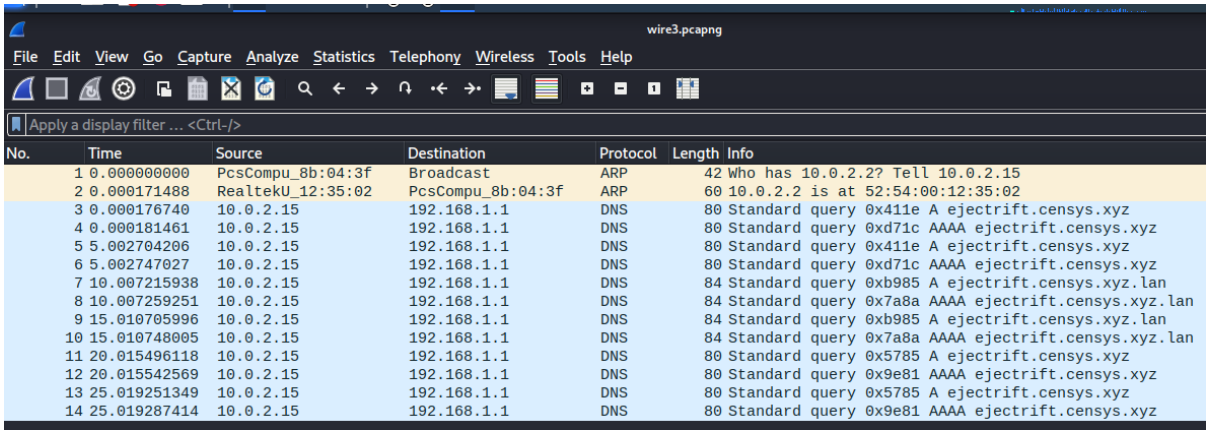
Sample1: It is trying to connect to a host using 10.104.0.XXX using TCP. But I turn off internet connection, so it keeps trying to connect. If I allowed the internet connection, it reached to a host and trying to do something.



Sample2: I couldn’t catch any network connection because Sample2 program didn’t run.



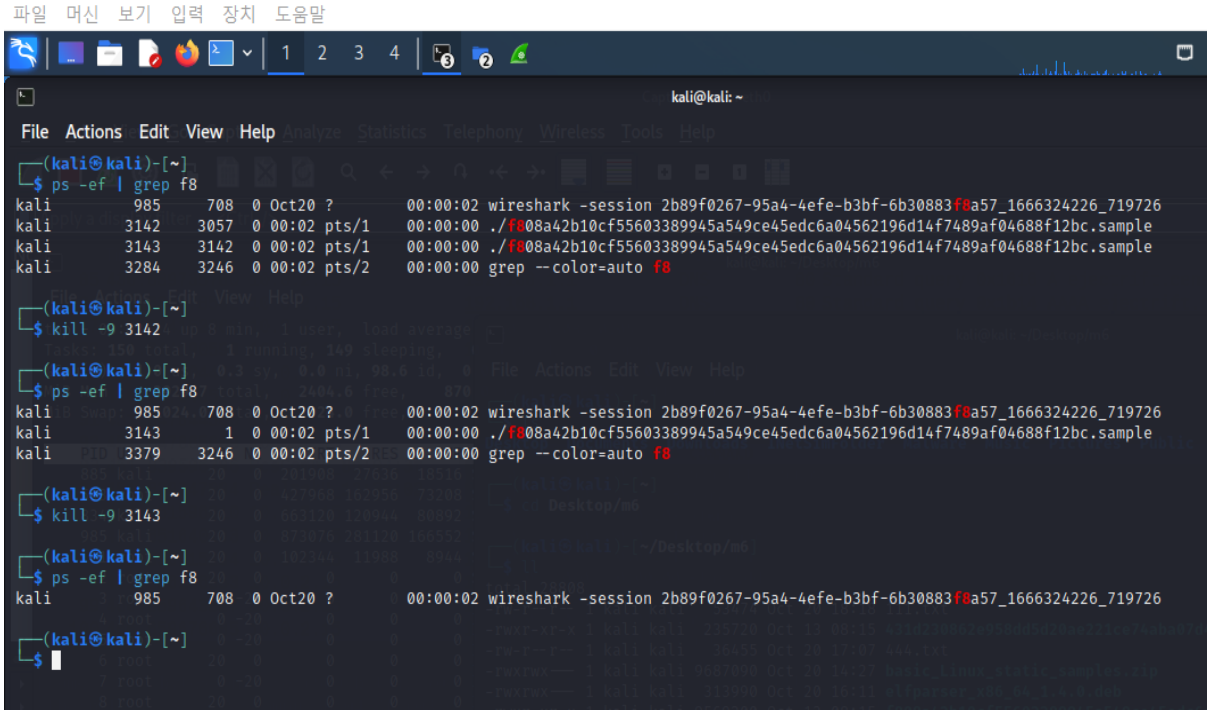
Sample3: It is trying to reach out to a host by questioning about ‘ejectrift.censys.xyz’. Also I disconnect from internet, it keeps trying to sending DNS packet to find the IP address.



4. Does the program create, communicate with, or terminate other processes? If so, what can you learn about this interaction?

Sample1: After completing the execution, I can catch the network traffic through the Wireshark. I can assume that the Sample1 created another process connecting to a host.

Sample3: It creates 2 processes by one execution. I executed the Sample3 one time but there were 2 processes and I kill them all to terminate.



5. Can you observe or infer any other effects of the program before or after it runs?

Sample1: After running the program, the file has immediately disappeared on the folder. Sample1 seems to want to hide. And maybe it sneaked into a system and waiting for a wake up, I guess.

Sample2, Sample3: I didn’t catch any effects.