

* 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
```


Wireshark packet capture showing network traffic. The display filter is 'Apply a display filter ... <Ctrl-/>'. The packet list shows several ICMP Destination unreachable (Host unreachable) packets and TCP SYN packets.

No.	Time	Source	Destination	Protocol	Length	Info
213	0.019146204	10.0.2.2	10.0.2.15	ICMP	70	Destination unreachable (Host unreachable)
214	0.019146234	10.0.2.2	10.0.2.15	ICMP	70	Destination unreachable (Host unreachable)
215	0.019146264	10.0.2.2	10.0.2.15	ICMP	70	Destination unreachable (Host unreachable)
216	0.019229231	10.0.2.2	10.0.2.15	ICMP	70	Destination unreachable (Host unreachable)
217	0.019624369	10.0.2.15	10.104.0.110	TCP	74	43950 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1
218	0.019647214	10.0.2.15	10.104.0.111	TCP	74	42368 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4
219	0.019683169	10.0.2.15	10.104.0.112	TCP	74	47640 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2
220	0.019697403	10.0.2.15	10.104.0.113	TCP	74	53044 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2
221	0.019735985	10.0.2.15	10.104.0.114	TCP	74	33260 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1
222	0.019748584	10.0.2.15	10.104.0.115	TCP	74	41620 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2
223	0.019758618	10.0.2.15	10.104.0.109	TCP	74	48628 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3
224	0.020285400	10.0.2.15	10.104.0.116	TCP	74	32782 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2
225	0.020325765	10.0.2.15	10.104.0.117	TCP	74	54634 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1
226	0.020386590	10.0.2.15	10.104.0.118	TCP	74	60298 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2
227	0.020413223	10.0.2.15	10.104.0.119	TCP	74	49528 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3
228	0.020465558	10.0.2.15	10.104.0.120	TCP	74	40268 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=5
229	0.020546760	10.0.2.15	10.104.0.121	TCP	74	49196 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2

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

Terminal window showing file permissions and a red box highlighting an error message.

```

kali (snap2) [실행 중] - Oracle VM VirtualBox
파일  머신  보기  입력  장치  도움말

kali@kali: ~/Desktop/m6
File Actions Edit View Help
error while loading shared libraries: libbfd-2.30-system.so: cannot open shared
object file: No such file or directory

(kali@kali)~/Desktop/m6]
$ ll
total 28808
-rw-r--r-- 1 kali kali 53474 Oct 20 18:18 111.txt
-rwxr-xr-x 1 kali kali 235720 Oct 13 08:15 431d230862e958dd5d20ae221ce74aba0
7d40dde5fd8e45f2b164905e637b1c1.sample
-rw-r--r-- 1 kali kali 36455 Oct 20 17:07 444.txt
-rwxrwx-- 1 kali kali 9687090 Oct 20 14:27 basic_linux_static_samples.zip
-rwxrwx-- 1 kali kali 313990 Oct 20 16:11 elfparser_x86_64_1.4.0.deb
-rwxr-xr-x 1 kali kali 9569200 Oct 13 08:15 f808a42b10cf55603389945a549ce45ed
c6a04562196d14f7489af04688f12bc.sample
-rw-r--r-- 1 kali kali 630252 Oct 20 17:07 fff.txt
-rw-r--r-- 1 kali kali 859 Oct 20 18:27 trac1.txt
-rw-r--r-- 1 root root 9560 Oct 20 21:15 trac2.txt
-rw-r--r-- 1 root root 74661 Oct 20 18:34 trac3.txt
-rw----- 1 kali kali 8855976 Oct 20 18:27 wire1.pcapng
-rw----- 1 kali kali 1884 Oct 20 18:34 wire3.pcapng

(kali@kali)~/Desktop/m6]
$ sudo strace -o trac2.txt ./431d230862e958dd5d20ae221ce74aba07d40dde5fd8e45f2b164905e637b1c1.sample
./431d230862e958dd5d20ae221ce74aba07d40dde5fd8e45f2b164905e637b1c1.sample: error while loading shared libraries: libbfd-2.30-system.so: c
annot open shared object file: No such file or directory

(kali@kali)~/Desktop/m6]
$

```

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.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_8b:04:3f	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
2	0.000171488	RealtekU_12:35:02	PcsCompu_8b:04:3f	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
3	0.000176740	10.0.2.15	192.168.1.1	DNS	80	Standard query 0x411e A ejectrift.censys.xyz
4	0.000181461	10.0.2.15	192.168.1.1	DNS	80	Standard query 0xd71c AAAA ejectrift.censys.xyz
5	5.002704296	10.0.2.15	192.168.1.1	DNS	80	Standard query 0x411e A ejectrift.censys.xyz
6	5.002747027	10.0.2.15	192.168.1.1	DNS	80	Standard query 0xd71c AAAA ejectrift.censys.xyz
7	10.007215938	10.0.2.15	192.168.1.1	DNS	84	Standard query 0xb985 A ejectrift.censys.xyz.lan
8	10.007259251	10.0.2.15	192.168.1.1	DNS	84	Standard query 0x7a8a AAAA ejectrift.censys.xyz.lan
9	15.010705996	10.0.2.15	192.168.1.1	DNS	84	Standard query 0xb985 A ejectrift.censys.xyz.lan
10	15.010748005	10.0.2.15	192.168.1.1	DNS	84	Standard query 0x7a8a AAAA ejectrift.censys.xyz.lan
11	20.015496118	10.0.2.15	192.168.1.1	DNS	80	Standard query 0x5785 A ejectrift.censys.xyz
12	20.015542569	10.0.2.15	192.168.1.1	DNS	80	Standard query 0x9e81 AAAA ejectrift.censys.xyz
13	25.019251349	10.0.2.15	192.168.1.1	DNS	80	Standard query 0x5785 A ejectrift.censys.xyz
14	25.019287414	10.0.2.15	192.168.1.1	DNS	80	Standard query 0x9e81 AAAA ejectrift.censys.xyz

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.

```

파일  머신  보기  입력  장치  도움말

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ps -ef | grep f8
kali    985      708  0 Oct20 ?        00:00:02 wireshark -session 2b89f0267-95a4-4efe-b3bf-6b30883f8a57_1666324226_719726
kali    3142    3057  0 00:02 pts/1    00:00:00 ./f808a42b10cf55603389945a549ce45edc6a04562196d14f7489af04688f12bc.sample
kali    3143    3142  0 00:02 pts/1    00:00:00 ./f808a42b10cf55603389945a549ce45edc6a04562196d14f7489af04688f12bc.sample
kali    3284    3246  0 00:02 pts/2    00:00:00 grep --color=auto f8

(kali@kali)-[~]
$ kill -9 3142
$ ps -ef | grep f8
kali    985      708  0 Oct20 ?        00:00:02 wireshark -session 2b89f0267-95a4-4efe-b3bf-6b30883f8a57_1666324226_719726
kali    3143      1  0 00:02 pts/1    00:00:00 ./f808a42b10cf55603389945a549ce45edc6a04562196d14f7489af04688f12bc.sample
kali    3379    3246  0 00:02 pts/2    00:00:00 grep --color=auto f8

(kali@kali)-[~]
$ kill -9 3143
$ ps -ef | grep f8
kali    985      708  0 Oct20 ?        00:00:02 wireshark -session 2b89f0267-95a4-4efe-b3bf-6b30883f8a57_1666324226_719726

```

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.