**\* 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**

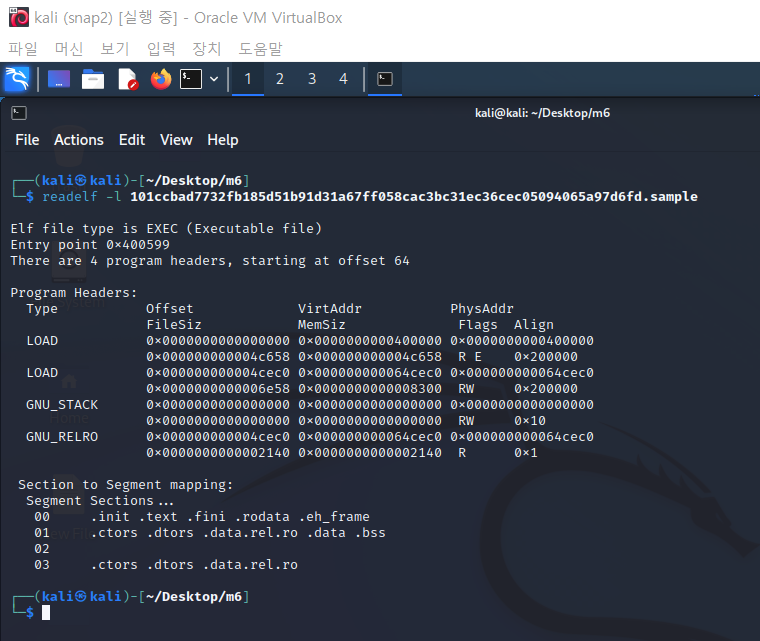
**Sample 3:**

**f808a42b10cf55603389945a549ce45edc6a04562196d14f7489af04688f12bc.sample**

**1. Is the malware sample packed? What evidence do you have for your answer?**

**Sample1: It’s packed.**

Evidence: Segment types and count. The file contains only PT\_LOAD segments (and PT\_GNU\_STACK).



**Sample2: It’s not packed.**

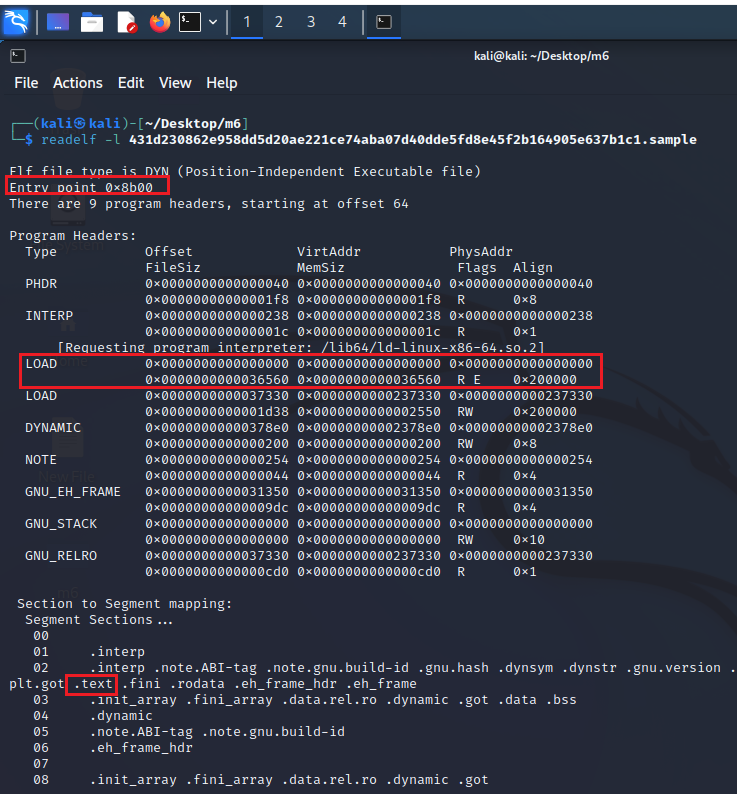
Evidence:

- readelf: Entry point resides in PT\_LOAD which is designated with RE. Also, I can see ‘.text’ in the Segment section and its location is in PT\_LOAD. Looking at segment table but I couldn’t find anything wrong.

- ELFparser: Didn't show anything about packer

- DIE(Detect it Easy): The program just died when chose a file. So I tried light version of it(the file also included in a deployment) and it showed nothing about packer.

- strings command: No signs of 'UPX' or 'LSD'



텍스트이(가) 표시된 사진

자동 생성된 설명

**Sample3: It’s not packed.**

Evidence:

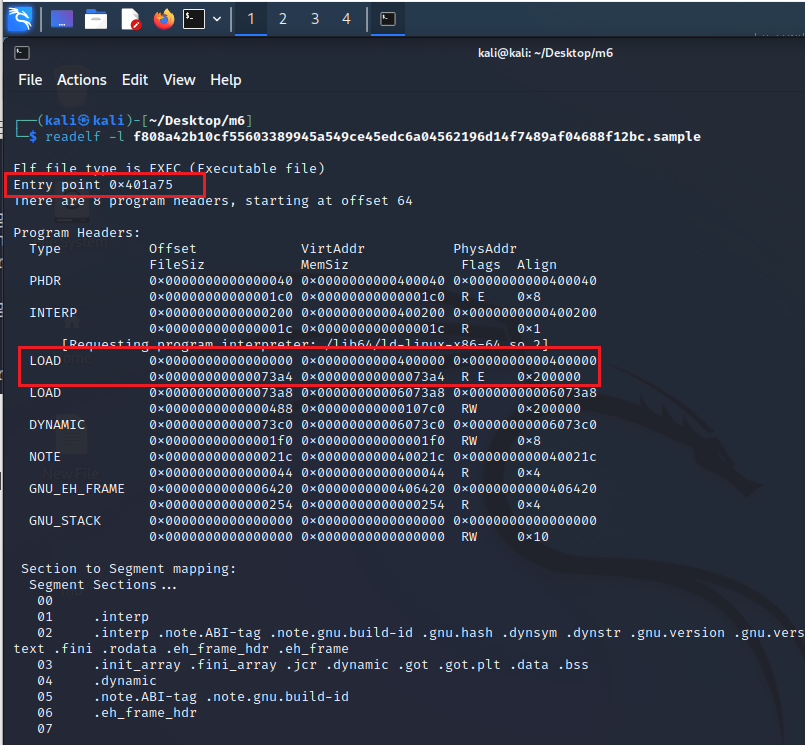
- readelf: Entry point resides in PT\_LOAD which is designated with RE. Also, I can see ‘.text’ in the Segment section and its location is in PT\_LOAD. Looking at segment table but I couldn’t find anything wrong.

- ELFparser: Didn't show anything about packer

- DIE(Detect it Easy): The program just died when chose a file. So I tried light version of it(the file also included in a deployment) and it showed nothing about packer.

- strings command: No signs of 'UPX' or 'LSD'

Entry point resides in PT\_LOAD which is designated with RE. Also, I can see ‘.text’ in the Segment section and its location is in PT\_LOAD.

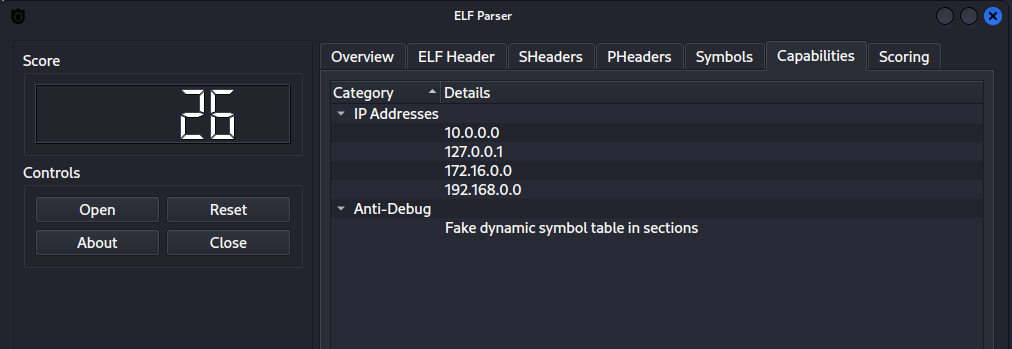


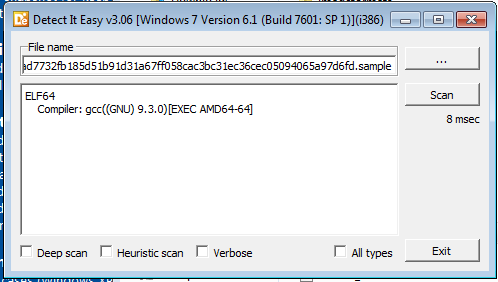
텍스트이(가) 표시된 사진

자동 생성된 설명

**2. If so, can you unpack it easily? If so, what program/command can you use to unpack it? If not, why not? Please provide evidence either way.**

Sample1: I could not get any information about packer from ELFparser and DetectItEasy. And I just tried to unpack it using UPX but it didn’t work.





Sample2: It’s not unpacked.

Sample3: It’s not unpacked.

**3. Are there any host- or network-based indicators that might help identify this malware if it were seen in the wild?**

Sample1:

There are several IP address in Sample1 and I assume that 172.16.0.0 would be a host IP address and it could be an indicator of this malware.

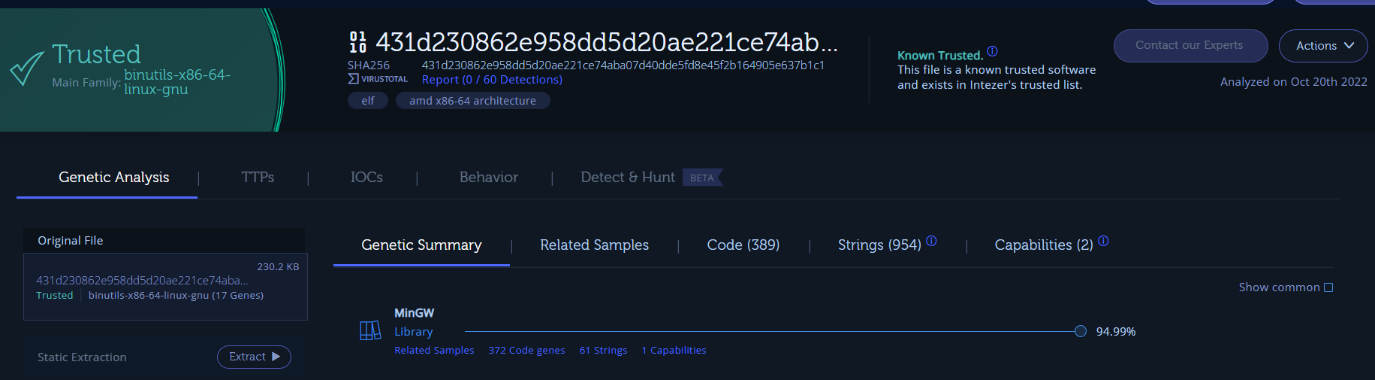
**4. Can you make an educated guess at any of the malware sample's functionality?**

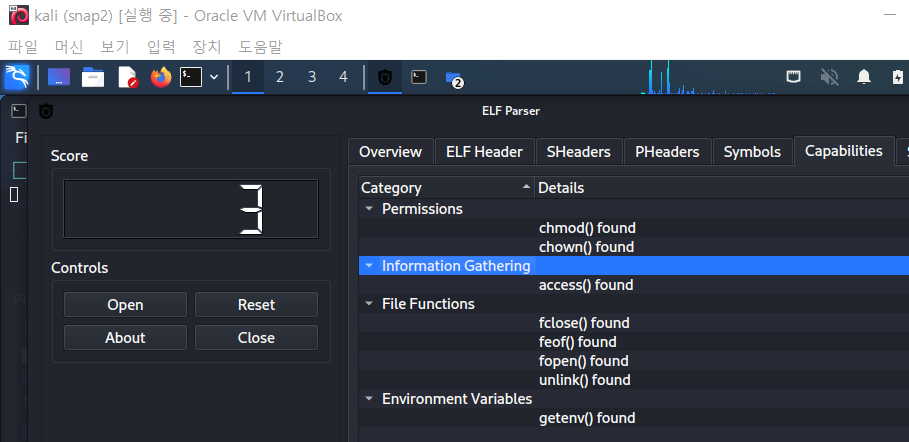
I think Sample1 and Sample3 are the malware program because when I ran the all 3 program using INTEZER ANALYZE and it showed Sample1 and 3 are malicious program.

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.



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.





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.

