Nguyen Nam Khanh – HE191159 – IA1902

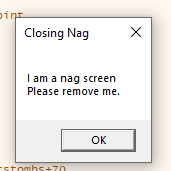
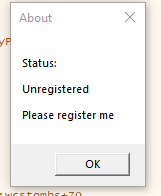
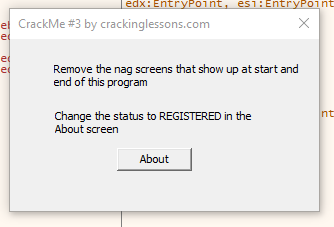
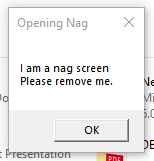
**Crack me 3:**

Objective:

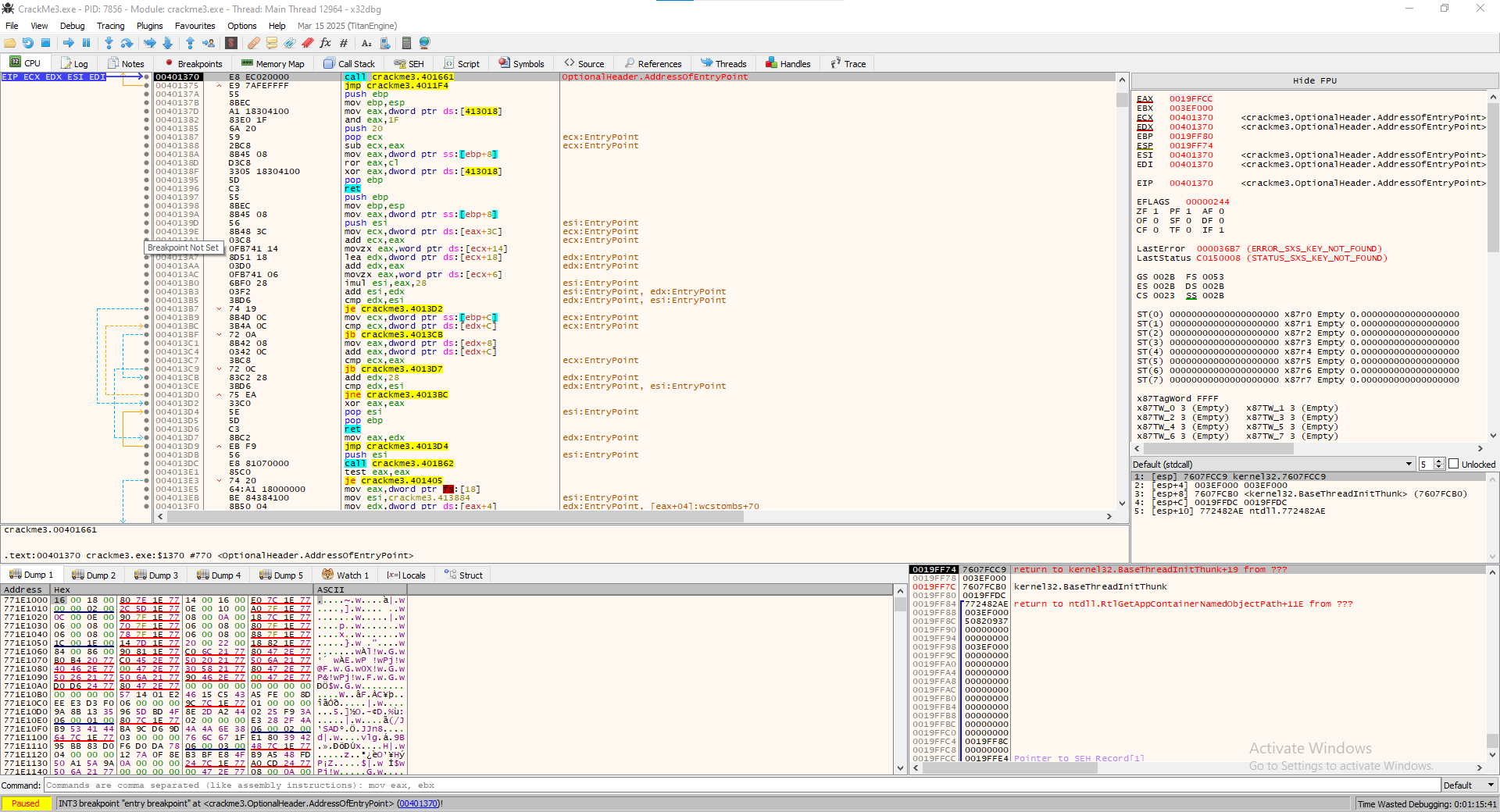
1. Remove the 2 nag screens – one at startup and one at close of program.
2. In the About screen – change status to Registered.

Solution:

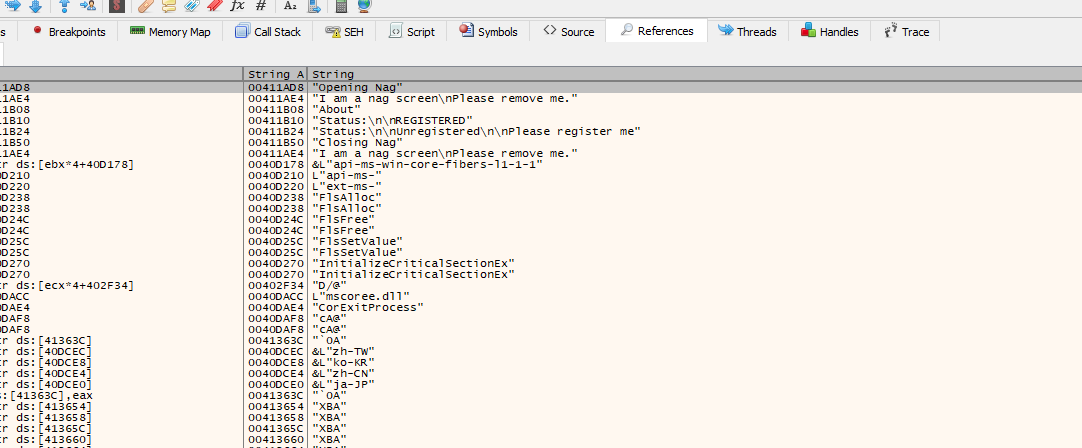
Run crackme3.exe to notice strings in box of nag screens and About screen.



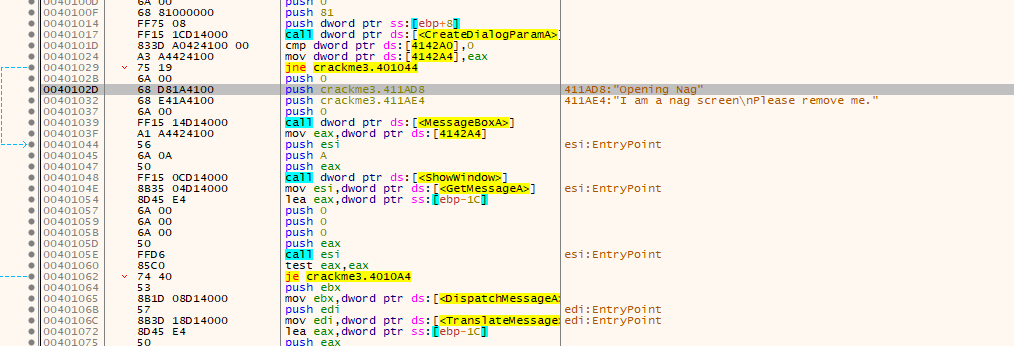
Open crackme3.exe in x32dbg tool.

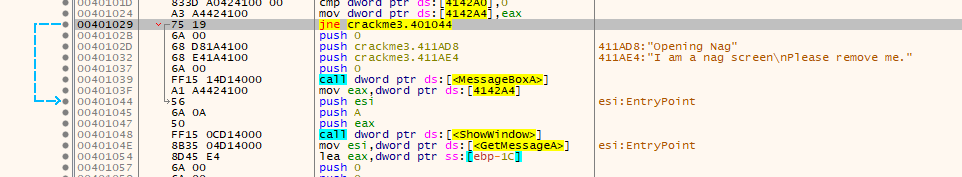
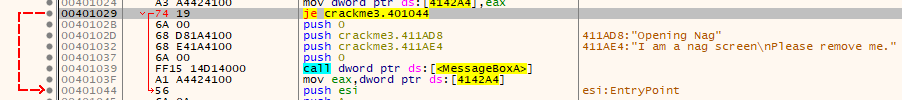


**Opening nag:**

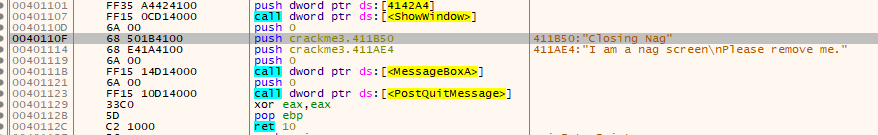
Find Opening Nag in String references

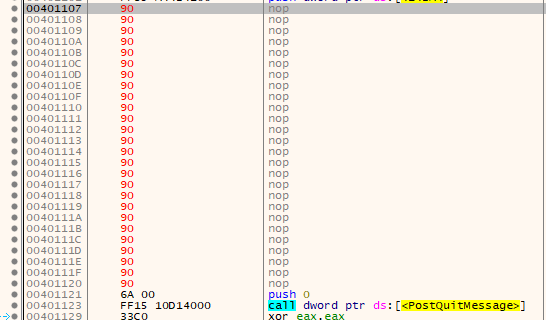
Double click to see code in CPU:



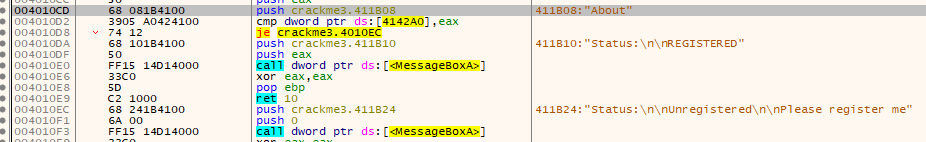
Trace code above and below, pay attention on this line ‘jne crackme3.401044’, this code is jump not equal through MessageBoxA of string “Opening Nag, I am a nag…” to address 00401044.  Need to change this one to je – jump equal to 00401044 ignoring these opening nag.

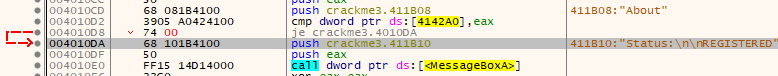
**Closing nag:**

Do it again with Closing nag

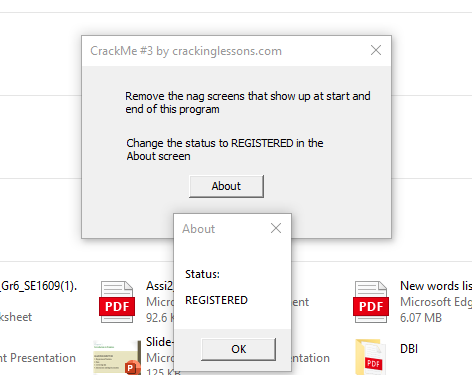
Trace code above and below to find the line jump, but no line has comparison to jump so we need to highlight 00401107 to 0040111BB (content of MessageBoxA of Closing nag) and fill with NOPs (no operation) to ignore Closing nag. 

**About screen:**

Then trace to About screen: 

Notice line “je crackme3.4010EC”, this mean jump equal to push string “Unregistered…” and call MessageBoxA, while we find out address 004010DA has string “Registered”. We need to change “je crackme3.4010EC” to “je crackme3.4010DA” to display Registered status. 

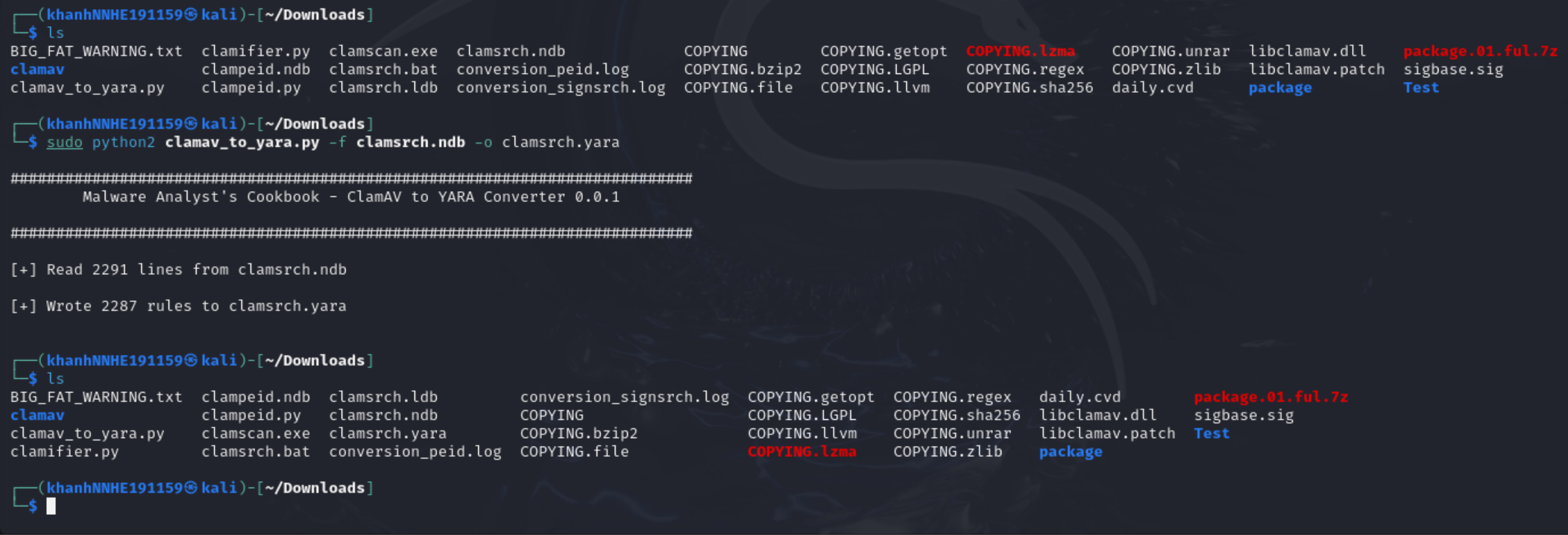
After change 3 objective, we patch file and run again to check the consequence.

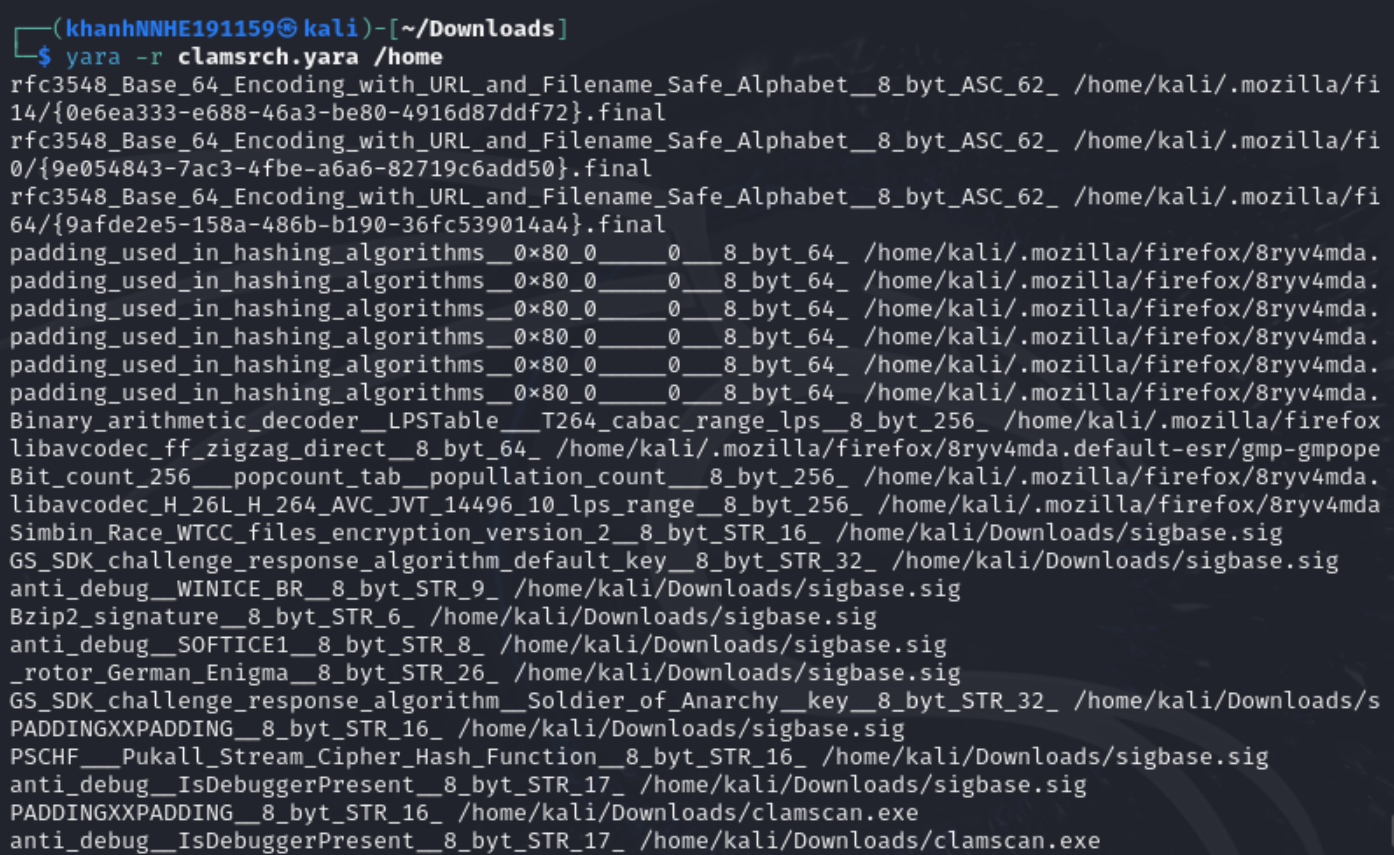


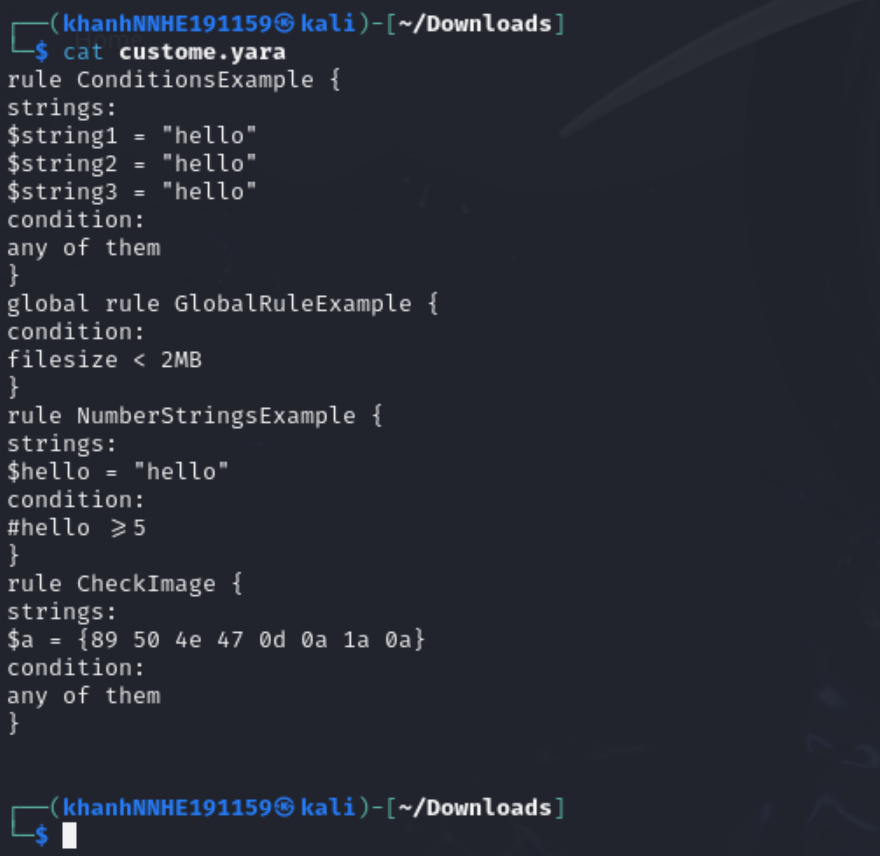
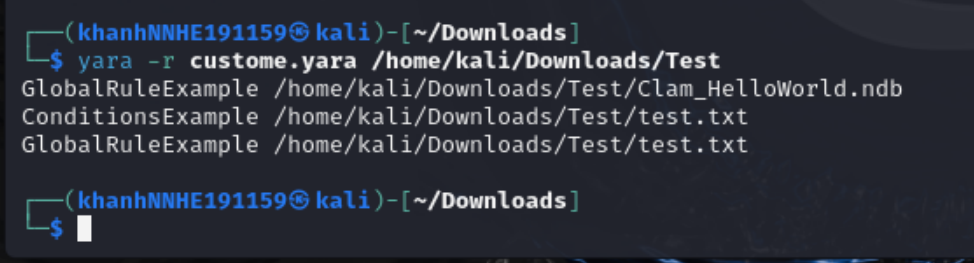
Done!

**LAB 4:Detect Malware Capabilities with YARA**

Convert file clamav to yara with the command:

sudo python2 clamav\_to\_yara.py -f clamsrch.ndb -o clamsrch.yara 

Start scanning with the yara:

Create a new rule file called custome.yara and cat to see: Test yara rules: Here we see yara's report for the rule we created as follows: ConditionExample means that yara has detected that the test.txt file matches the rule we provided and contains the string “hello” in there. In addition, other files will match yara's GlobalRuleExample.