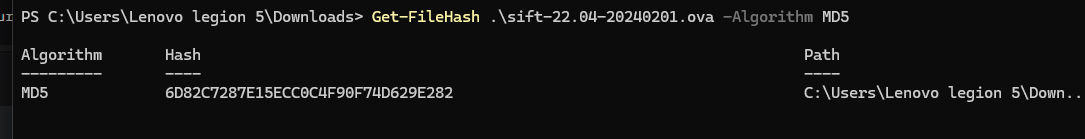
**Nguyen Nam Khanhh – HE191159 – IA1902 – IAM302**

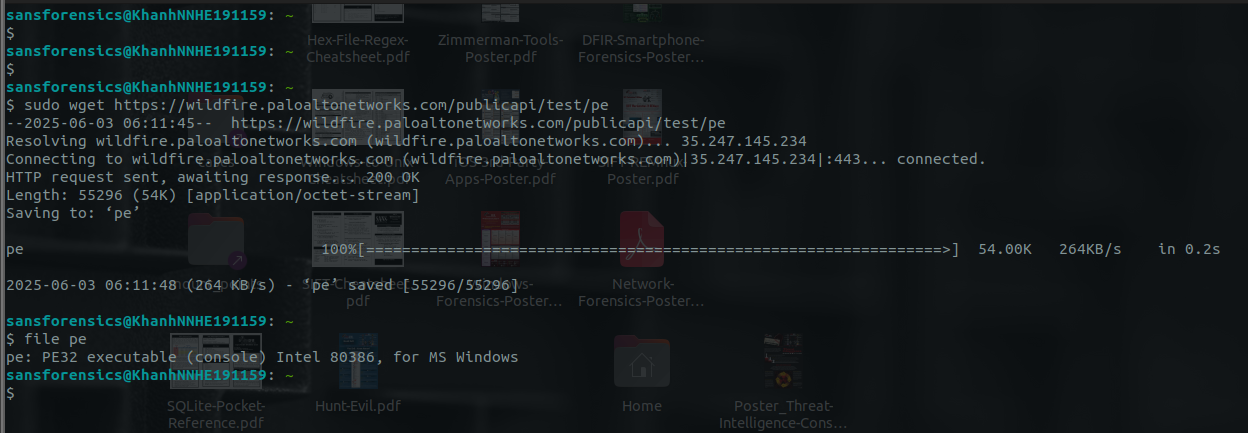
**Lab 5: Sandbox Setup and Configuration**

Install SIFT

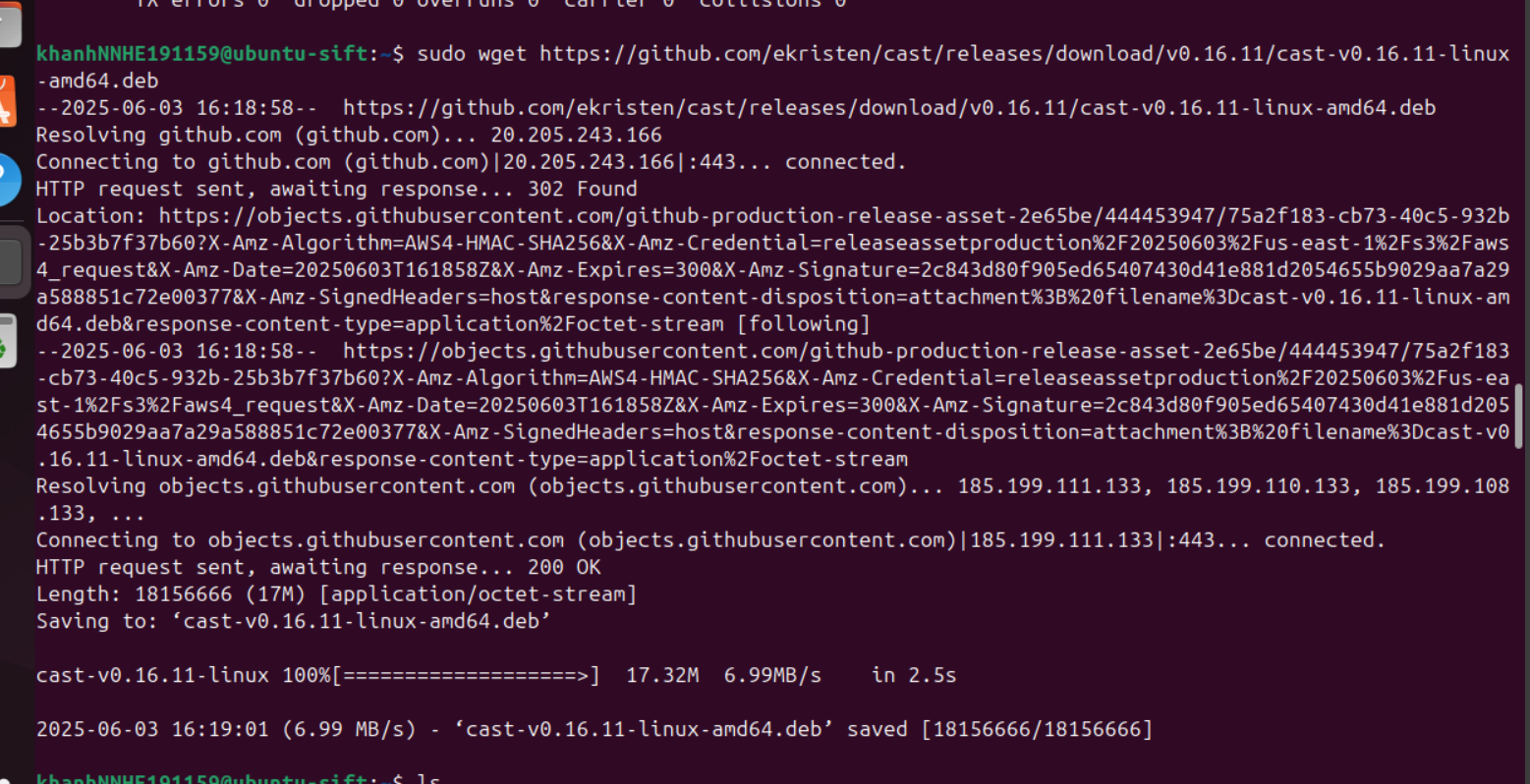
**Option 1: SIFT Workstation VM Appliance**

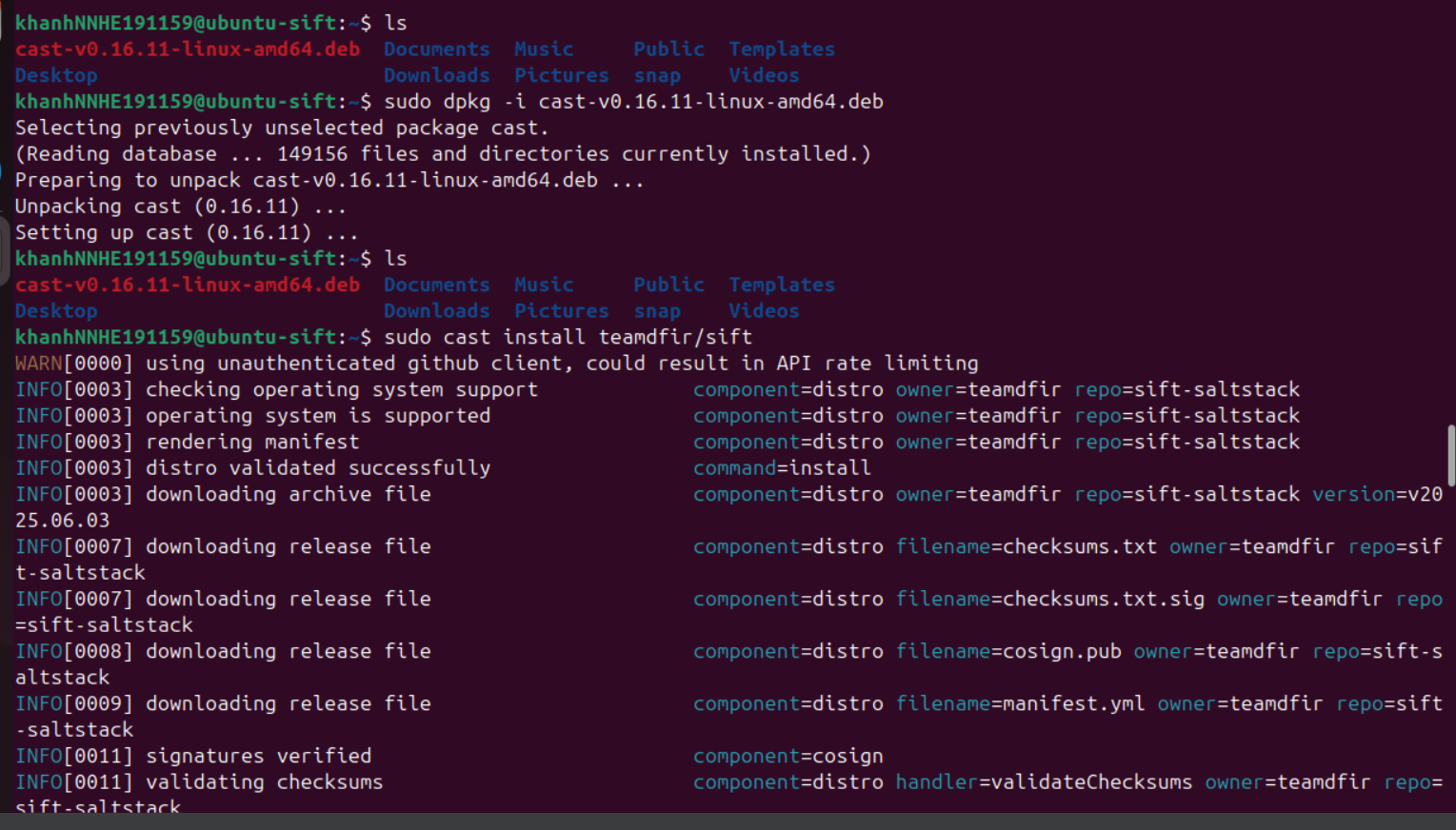
Check Hash Values of SIFT

Set up SIFT workstation WM appliance successfullyDownload the following sample to test. Using the file to check, we can see that this is a

32bit executable file, using Intel 80386, used to execute on the Windows operating system. 

**Option 2A: SIFT Easy Installation on Native Ubuntu System**

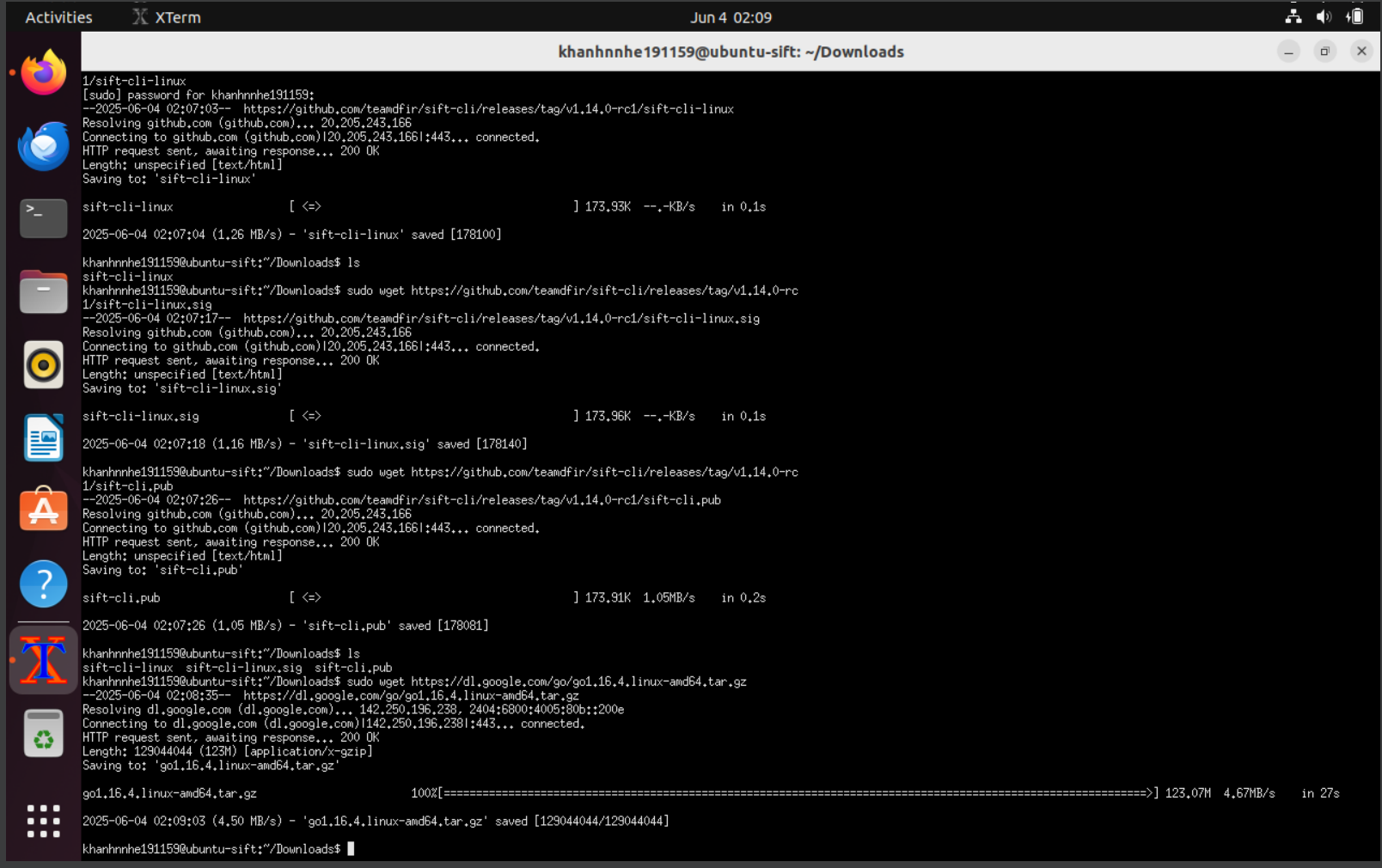
Download Cast into ubuntu****

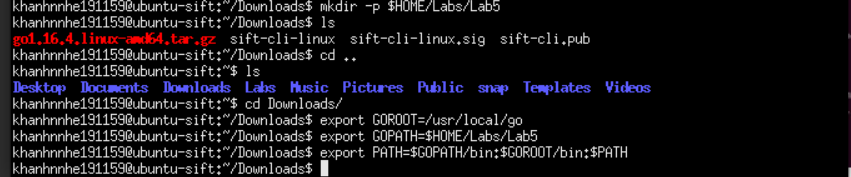
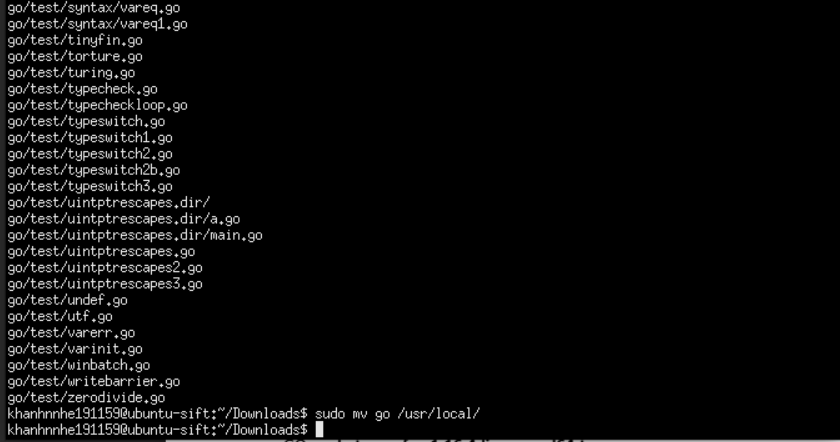
Execute Cast tools to automatically install latest version of SIFT on Github. Congrats -- you now have a SIFT workstation! 

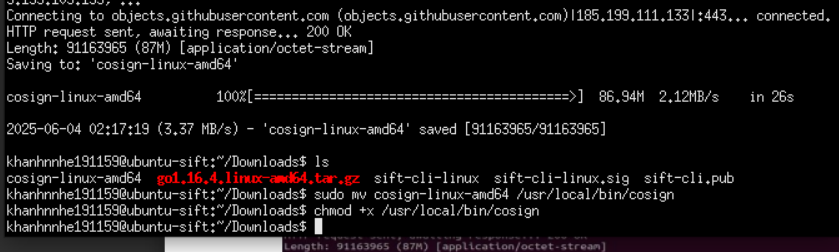
**Install for yourself(**[**https://github.com/sans-dfir/sift-cli#instructions**](https://github.com/sans-dfir/sift-cli#instructions)**)**

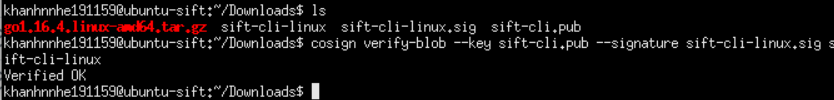
**(Download SIFT manually)**

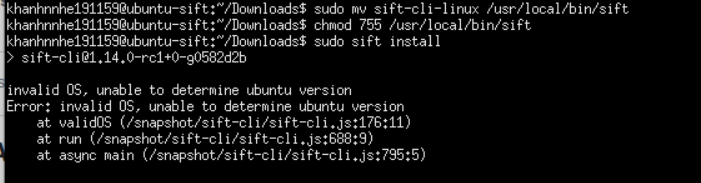
Install 3 package • sift-cli-linux • sift-cli-linux.sig • sift-cli.pubm of SIFT

****

Download Golang and setup Go environment for supported tools such as Cosign, SIFT****

Install and setup Cosign to check public key (sift-cli.pub) and verify signature (sift-cli-linux.sig) of SIFT****

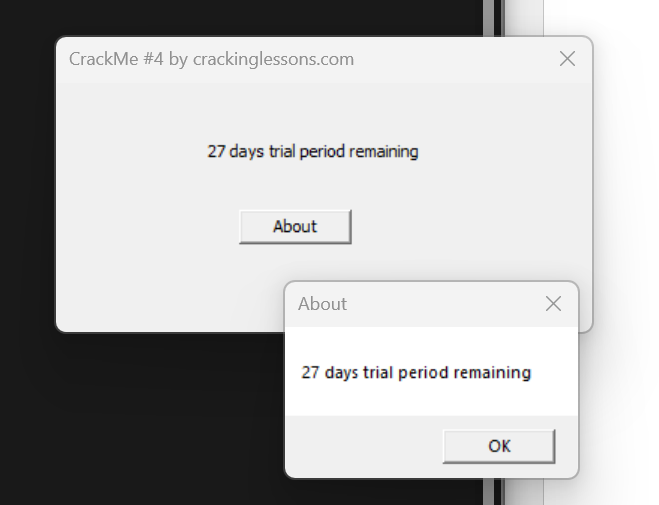
Verified successfully!****

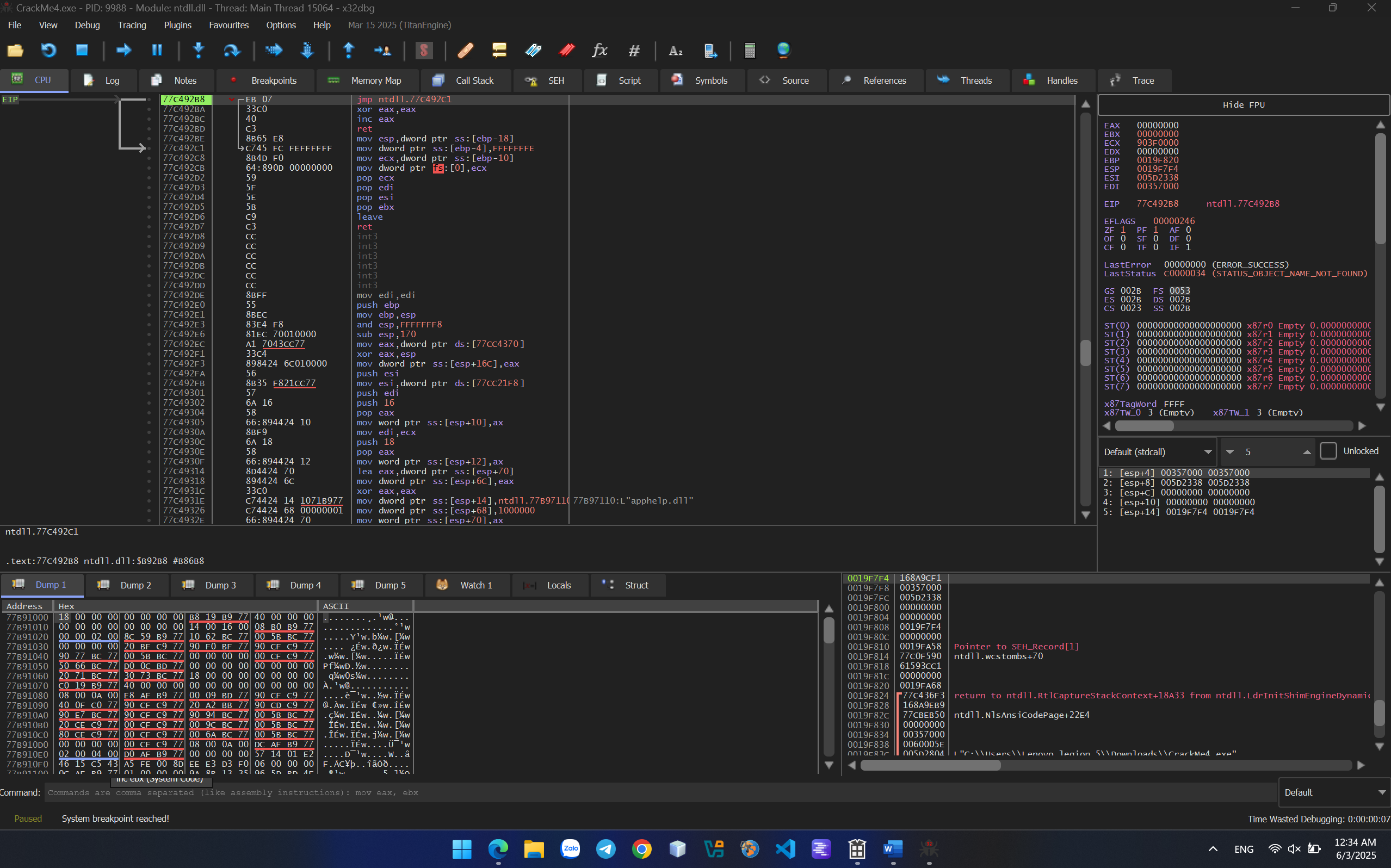
Afer verifying, transfer SIFT file to Go environment, and setup permission to install.

Notice: when install SIFT manually, i got stuck in invalid OS version error and trying change many version 22.04, 24.04 and having same error. So i inspected to source code of SIFT on Github and found that the code only checks 3 versions of Ubuntu: bionic (18.04), focal (20.04), and hirsute (21.04 not support). Other versions (such as jammy - 22.04, or noble - 24.04) are not tested, resulting in an invalid OS error, unable to determine ubuntu version if the user runs on these versions. Hence, if i change version to exact 2 of them, i may have install SIFT manual successfully. But at this time, It’s not a big matter, I reached to the last step of lab with 3 option of setup SIFT. Thanks for read this report.****

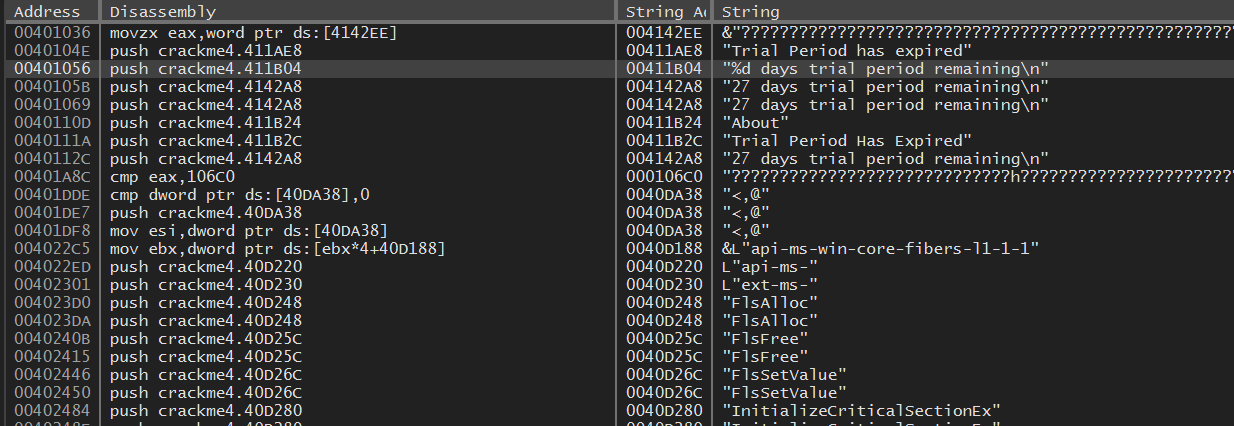
CRACK ME 4

1. Crack it to extend beyond 30 days
2. In the About screen – also extend it to beyond 30 days

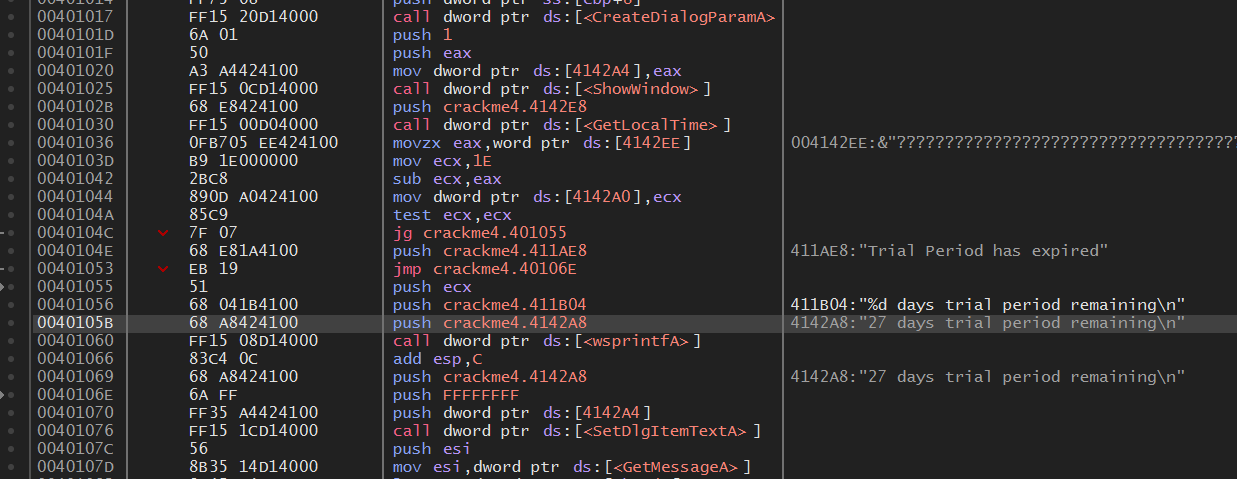


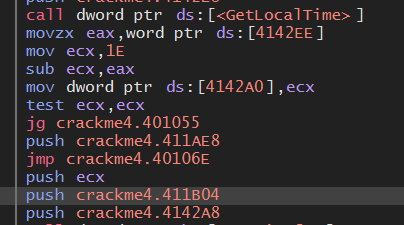
Open CrackMe4.exe in x32dbg to analyze.

Press F9 to run until the box of “27 days trial period remaining” displays.

Choose Search for > Current Module > typing “27 days trial period remaining” and find related strings. 

Notice the string "%d days trial period remaining\n" and inspect to the assembly code of these string.

Analyze above and below code of this string.

Notice these some line of code. 

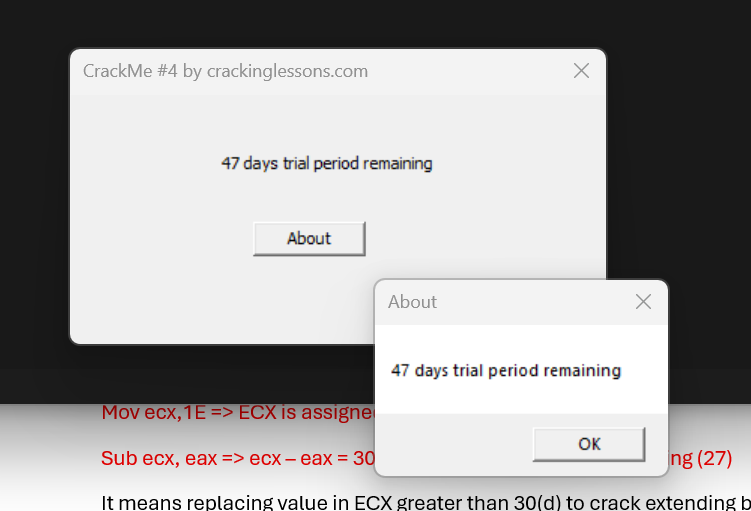
Function GetLocalTime get time of system and move to EAX.

Mov ecx,1E => ECX is assigned 1E (equal decimal 30).

Sub ecx, eax => ecx – eax = 30 – system time(3) = time remaining (27)

It means replacing value in ECX greater than 30(d) to crack extending beyond 30 days.

Decison change it to another value greater than 1E, such 32 (50 in decimal). Patch it and run to check the result.



Explain: because the time of doing this lesson is 3rd of June, 2025. Hence, when changing ECX to 50 decimal, we could receive 47 days trial period remaining.

Done!