

Họ và tên: Trần Trí Dũng

Mã số sinh viên: HE190680

Lớp: IA1901

## Lab 5:

Download SIFT Workstation VMware Appliance:

The screenshot shows the SANS Institute website's page for SIFT Workstation. The page has a navigation bar with links for Training, Learning Paths, Community Resources, and For Organizations. A search bar and a 'Talk with an expert' button are also present. The main content area features the SIFT Workstation logo and a description of the tool as a collection of free and open-source incident response and forensic tools. Below this, there is a section titled 'Option 1: SIFT Workstation VM Appliance' with a 'Download' button. This section provides instructions on how to download the virtual machine and lists the login credentials and hash values for the appliance. A 'Having trouble downloading SIFT?' section offers contact information for support.

**SIFT Workstation**

The SIFT Workstation is a collection of free and open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings. It can match any current incident response and forensic tool suite. SIFT demonstrates that advanced incident response capabilities and deep-dive digital forensic techniques can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

By Rob Lee

**Option 1: SIFT Workstation VM Appliance** [Download](#)

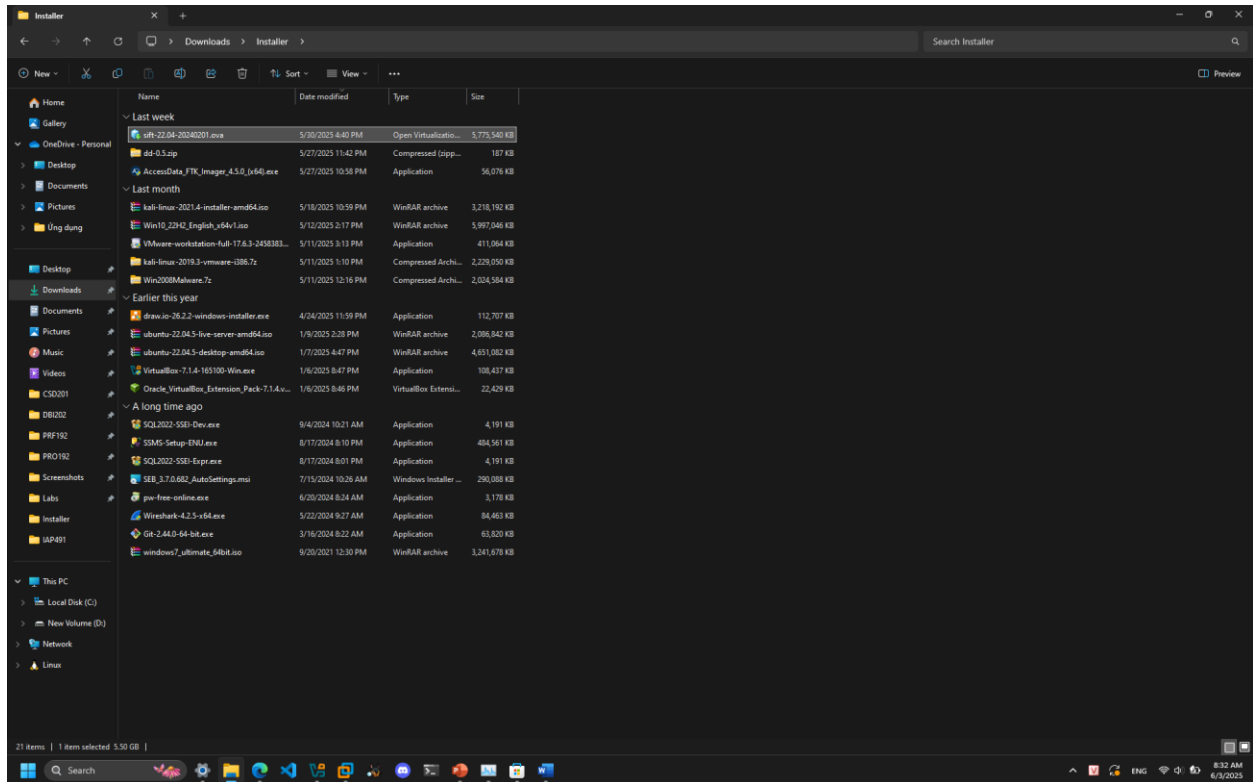
Click the 'Login to Download' button and input (or create) your SANS Portal account credentials to download the virtual machine. Once you have booted the virtual machine, use the credentials below to gain access.

- Login - **sansforensics**
- Password - **forensics**
- **\$ sudo su -**
  - Use to elevate privileges to root while mounting disk images.
- Hash Values
  - MD5: 6d82c7387e15ecc0c4f90f74d629e282
  - SHA256: fb7c343e65c21d0ff5919577fa1890b1eaf76acd20f31de619ea6c5c7e4dc72

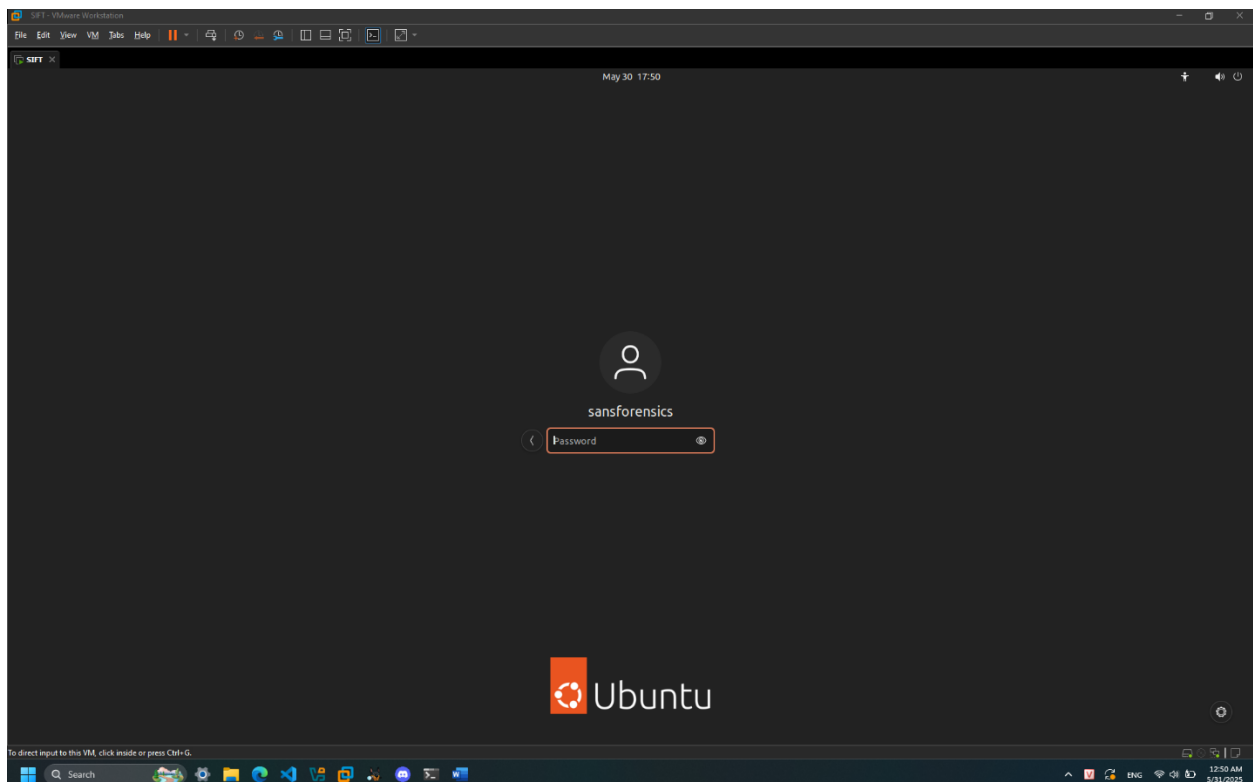
**Having trouble downloading SIFT?**

If you are having trouble downloading the SIFT Workstation VM, please contact [sift-support@sans.org](mailto:sift-support@sans.org) and include the URL you were given, your public IP address, browser type, and if you are using a proxy of any kind.

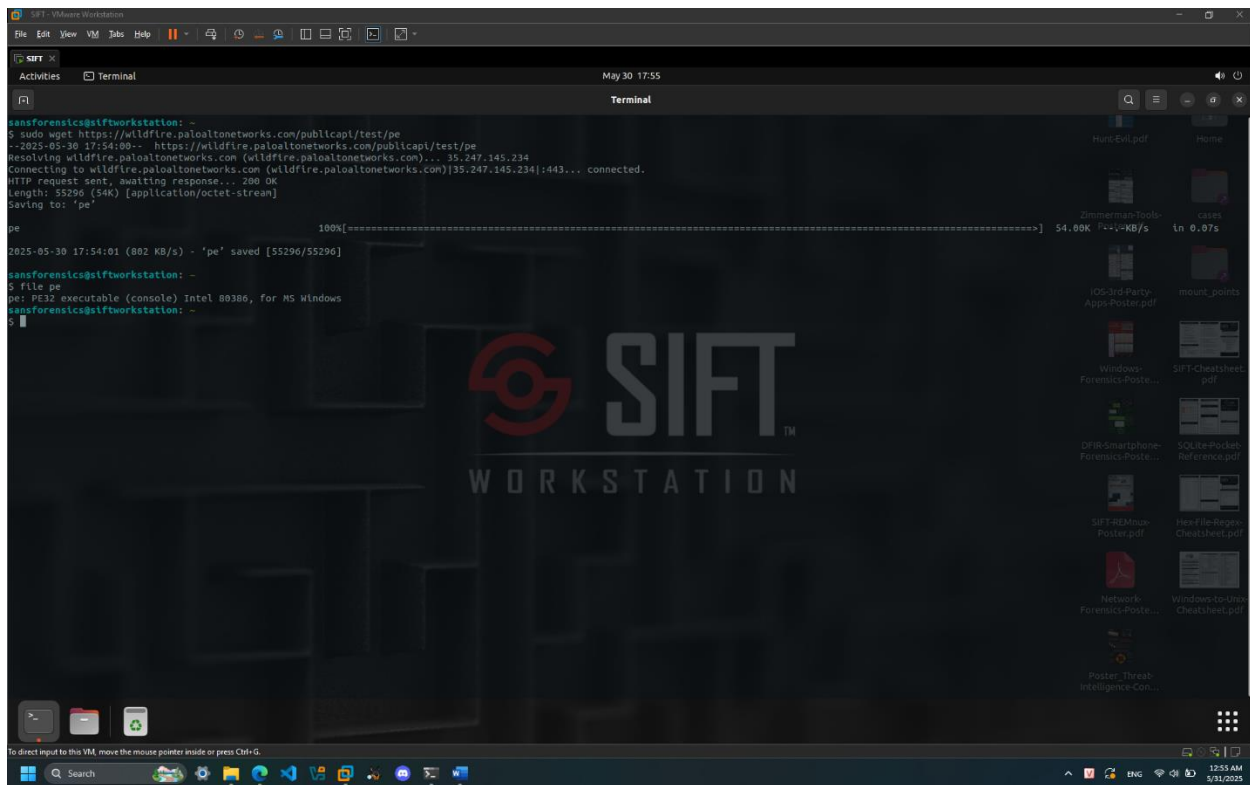
## Run Sans Sift in VMware:



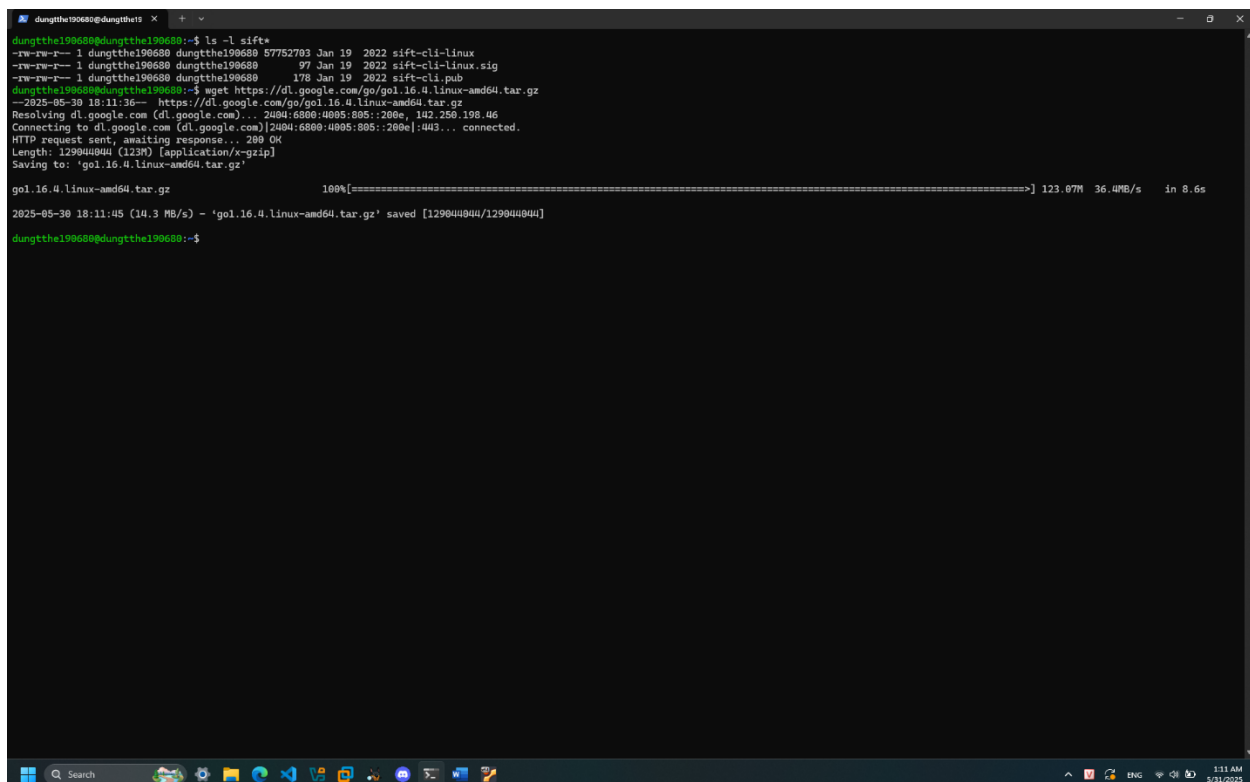
## Log in Sans Sift:



Download sample to test -> Use file to check:



Download related files -> Download GO's zip file:



```

dunqthel19068@ubuntu:~$ go test/typeswitch.go
go test/typeswitch1.go
go test/typeswitch2.go
go test/typeswitch3.go
go test/typeswitch4.go
go test/uintptrscapes_dir/
go test/uintptrscapes_dir/main.go
go test/uintptrscapes_dir/main.go
go test/uintptrscapes2.go
go test/uintptrscapes3.go
go test/undef.go
go test/utf.go
go test/varerr.go
go test/wadint.go
go test/windbatch.go
go test/writebarrier.go
go test/zerodivide.go
dunqthel19068@dunqthel19068:~$ sudo mv go /usr/local
dunqthel19068@dunqthel19068:~$ export GOPATH=/usr/local/go
dunqthel19068@dunqthel19068:~$ export GOPATH=$HOME/Labs/Lab5
dunqthel19068@dunqthel19068:~$ export PATH=$GOPATH/bin:$GOPATH/bin:$PATH
dunqthel19068@dunqthel19068:~$ wget https://github.com/sigstore/cosign/releases/download/v1.6.0/cosign-linux-amd64
--2025-06-03 08:05:56-- https://github.com/sigstore/cosign/releases/download/v1.6.0/cosign-linux-amd64
Resolving github.com (github.com)... 20.205.243.166
Connecting to github.com (github.com):20.205.243.166:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/339592417/0fff5c167-650d-45f1-8671-9ec4b7178a237X-Amz-Algorithm=AWS4-HMAC-SHA256X-Amz-Credential=releaseassetproduction%2F20250603%2Fus-east-1%2Fs3%2Faws4_requestX-Amz-Date=20250603T010556Zx-Amz-Expires=3086X-Amz-Signature=c9458efee9b5b062cb44c3175bc59c7d7d1d5098ef4f8e22d9cc59b2f6X-Amz-SignedHeaders=host&response-content-disposition=attachment%3Bfilename%3Dcosign-linux-amd64response-content-type=application/octet-stream [following]
--2025-06-03 08:05:57-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/339592417/0fff5c167-650d-45f1-8671-9ec4b7178a237X-Amz-Algorithm=AWS4-HMAC-SHA256X-Amz-Credential=releaseassetproduction%2F20250603%2Fus-east-1%2Fs3%2Faws4_requestX-Amz-Date=20250603T010556Zx-Amz-Expires=3086X-Amz-Signature=c9458efee9b5b062cb44c3175bc59c7d7d1d5098ef4f8e22d9cc59b2f6X-Amz-SignedHeaders=host&response-content-disposition=attachment%3Bfilename%3Dcosign-linux-amd64response-content-type=application/octet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.110.133, 185.199.108.133, 185.199.109.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com):185.199.110.133:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 91163965 (87M) [application/octet-stream]
Saving to: 'cosign-linux-amd64'

cosign-linux-amd64 100%[=====] 86,94M 1,59MB/s in 76s

2025-06-03 08:07:15 (1.14 MB/s) - 'cosign-linux-amd64' saved [91163965/91163965]

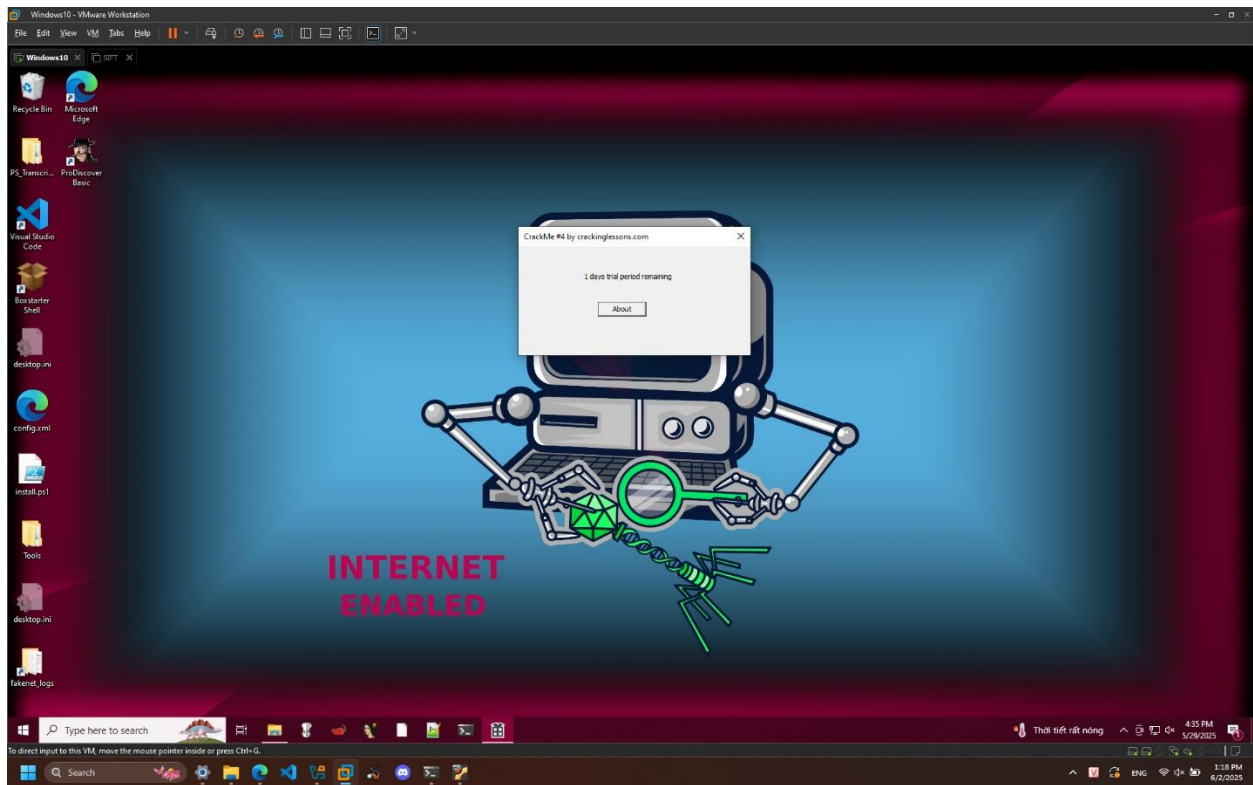
dunqthel19068@dunqthel19068:~$ sudo mv cosign-linux-amd64 /usr/local/bin/cosign
[sudo] password for dunqthel19068:
dunqthel19068@dunqthel19068:~$ chmod +x /usr/local/bin/cosign
dunqthel19068@dunqthel19068:~$

```

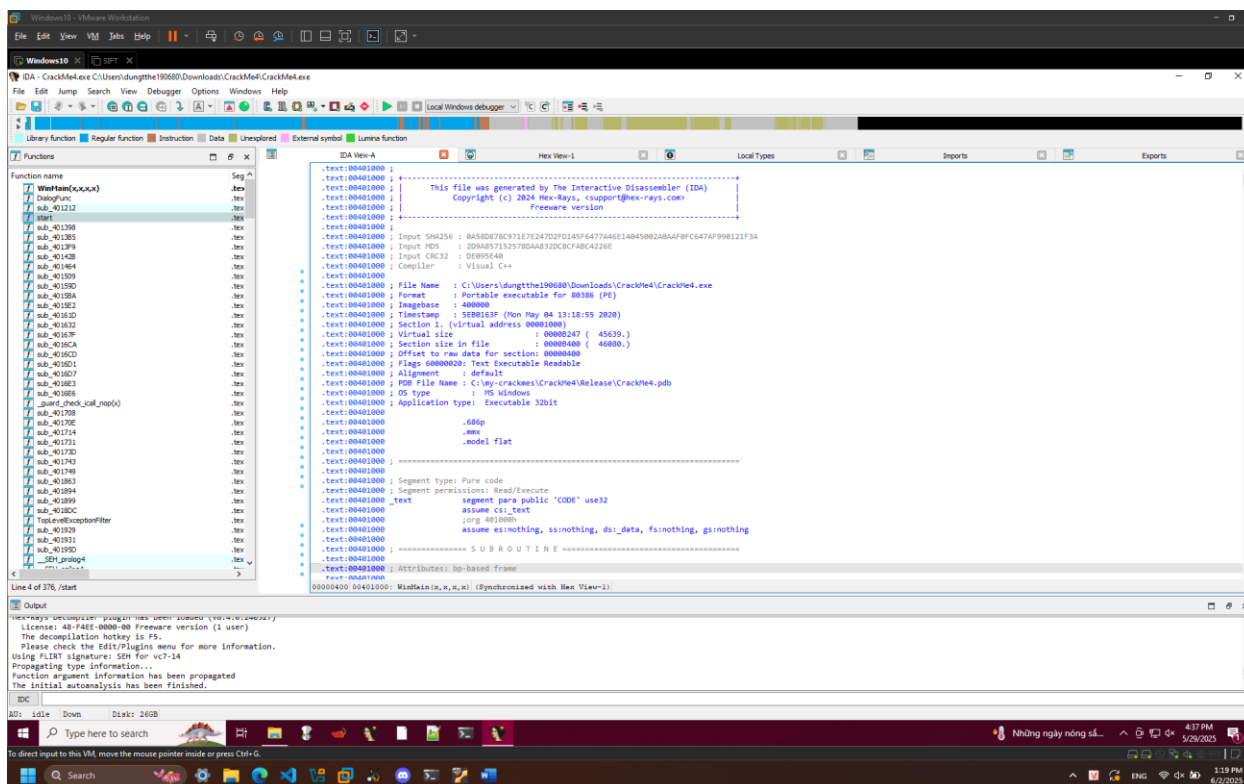
```
dungtthe190680@dungtthe11: ~  
Verified OK  
dungtthe190680@dungtthe190680:~$ cosign verify-blob --key sift-cli.pub --signature sift-cli-linux.sig sift-cli-linux  
Verified OK  
dungtthe190680@dungtthe190680:~$ sudo mv sift-cli-linux /usr/local/bin/sift  
dungtthe190680@dungtthe190680:~$ chmod 755 /usr/local/bin/sift  
dungtthe190680@dungtthe190680:~$ sudo sift install  
> sift-cli@1.14.0-rc140-g9582d2b  
> sift-version: not installed  
  
> mode: desktop  
> downloading v2024.11.14  
>> downloading sift-saltstack-v2024.11.14.tar.gz.asc  
>> downloading sift-saltstack-v2024.11.14.tar.gz.sha256  
>> downloading sift-saltstack-v2024.11.14.tar.gz.sha256.asc  
>> downloading sift-saltstack-v2024.11.14.tar.gz  
> validating file sift-saltstack-v2024.11.14.tar.gz
```

## CrackMe #4

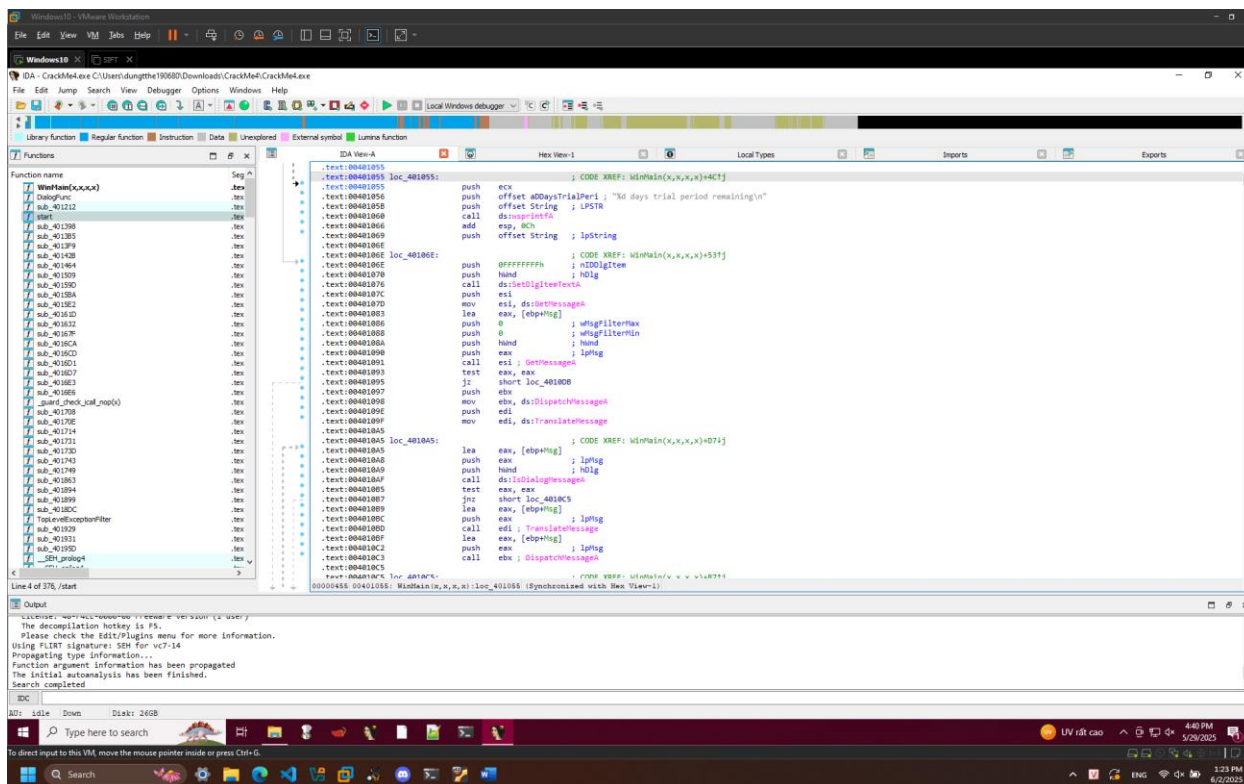
Đầu tiên em thử chạy chương trình và nhận được thông báo có từ khóa “remaining”:



Sau đó em mở phần mềm IDA và tiến hành dịch ngược file:



Em search từ khóa “remaining” và được điều hướng đến đoạn code này:



The screenshot displays a Windows 10 Virtual Machine (VM) environment. The primary window is IDA Pro, which is decompiling a binary file. The main pane shows assembly code for a function named `WinMain@.00000000`. The code includes instructions for setting up a trial period, displaying a message box, and handling user input. The assembly code is as follows:

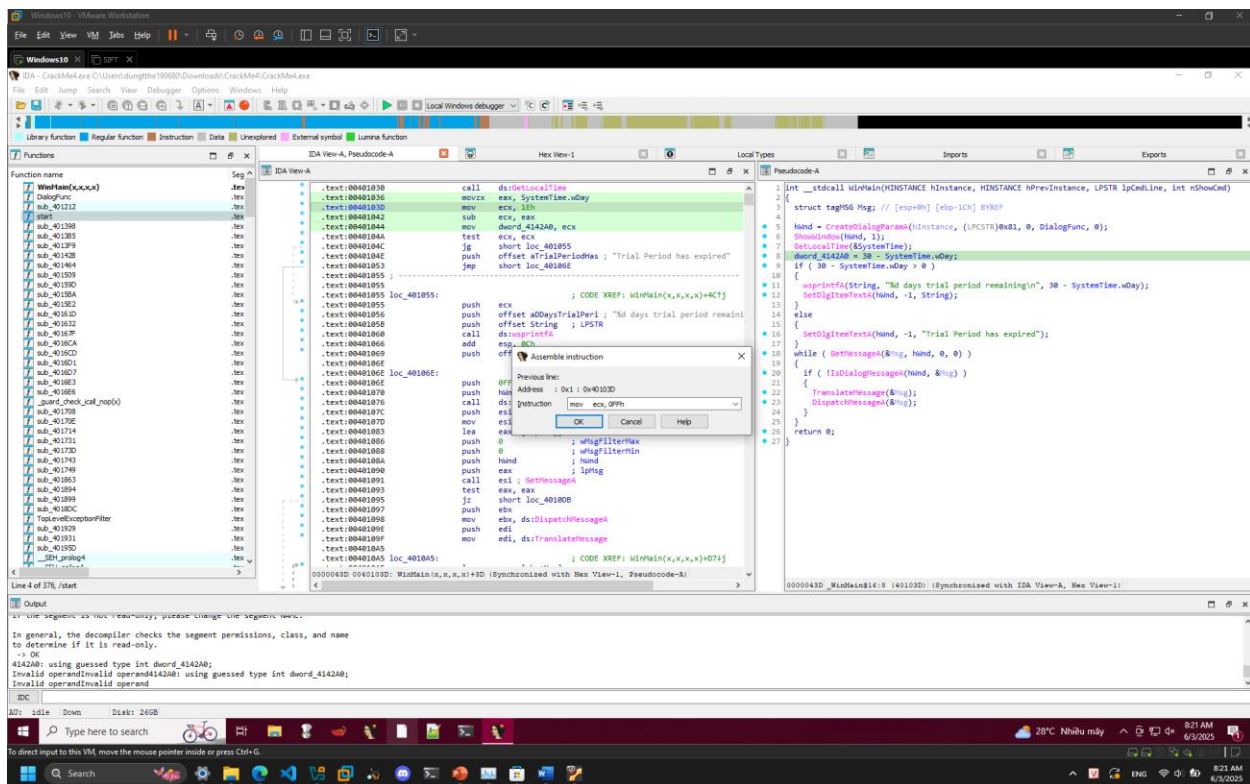
```

.text:00401036 movzx ecx, SystemTime.wDay
.text:0040103D mov ecx, 15h
.text:00401042 sub rcx, ecx
.text:00401044 mov dword_414240, ecx
.text:00401046 test ecx, ecx
.text:0040104C jg short loc_401055
.text:0040104E push offset a"Trial Period has expired"
.text:00401053 short loc_40106C
.text:00401055 ; CODE XREF: WinMain(x,x,x,x)+4C71
.text:00401055 loc_401055: push ecx
.text:00401056 push offset a0DaysTrialPeri ; "3d days trial period remaini
.text:0040105B push offset String ; LPSTR
.text:0040105D call dispatchMsg
.text:00401062 add esp, 0Ch
.text:00401064 push offset String ; lpstrng
.text:00401066 call dispatchMsg
.text:0040106C ; CODE XREF: WinMain(x,x,x,x)+5371
.text:0040106C loc_40106C: push 0FFFFFFFh
.text:0040106E push Hand
.text:00401070 call ds?SetDlgItemText@
.text:00401072 push esi
.text:00401074 mov esi, ds?GetDlgItem@
.text:00401076 lea eax, [ebp+arg_4]
.text:00401078 push 0
.text:0040107A push 0
.text:0040107C push Hand
.text:0040107E push eax
.text:00401080 call ds?SendMessage@
.text:00401082 test eax, eax
.text:00401084 call esi
.text:00401086 push 0
.text:00401088 push 0
.text:0040108A push Hand
.text:0040108C push eax
.text:0040108E call ds?SendMessage@
.text:00401090 test eax, eax
.text:00401092 call esi
.text:00401094 push ebx
.text:00401096 mov ebx, ds?DispatchMessage@
.text:00401098 edi
.text:0040109A mov edi, ds?TranslateMessage@
.text:0040109C ; CODE XREF: WinMain(x,x,x,x)+0714
.text:0040109E lea eax, [ebp+arg_4]

```

The Windows 10 desktop in the background shows a taskbar with various applications and a system tray with a clock showing 5:01 PM on 5/26/2023.





Lưu lại và chạy chương trình thì được thông báo số ngày còn lại là  $255 - 3 (3/6) = 252$  ngày:

