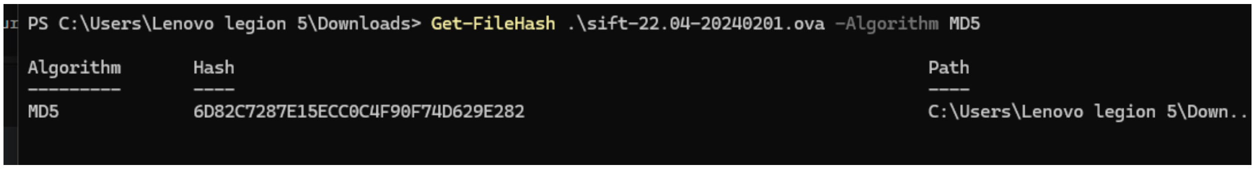
Nguyen Nam Khanhh – HE191159 – IA1902 – IAM302

Lab 5: Sandbox Setup and Configuration

Install SIFT

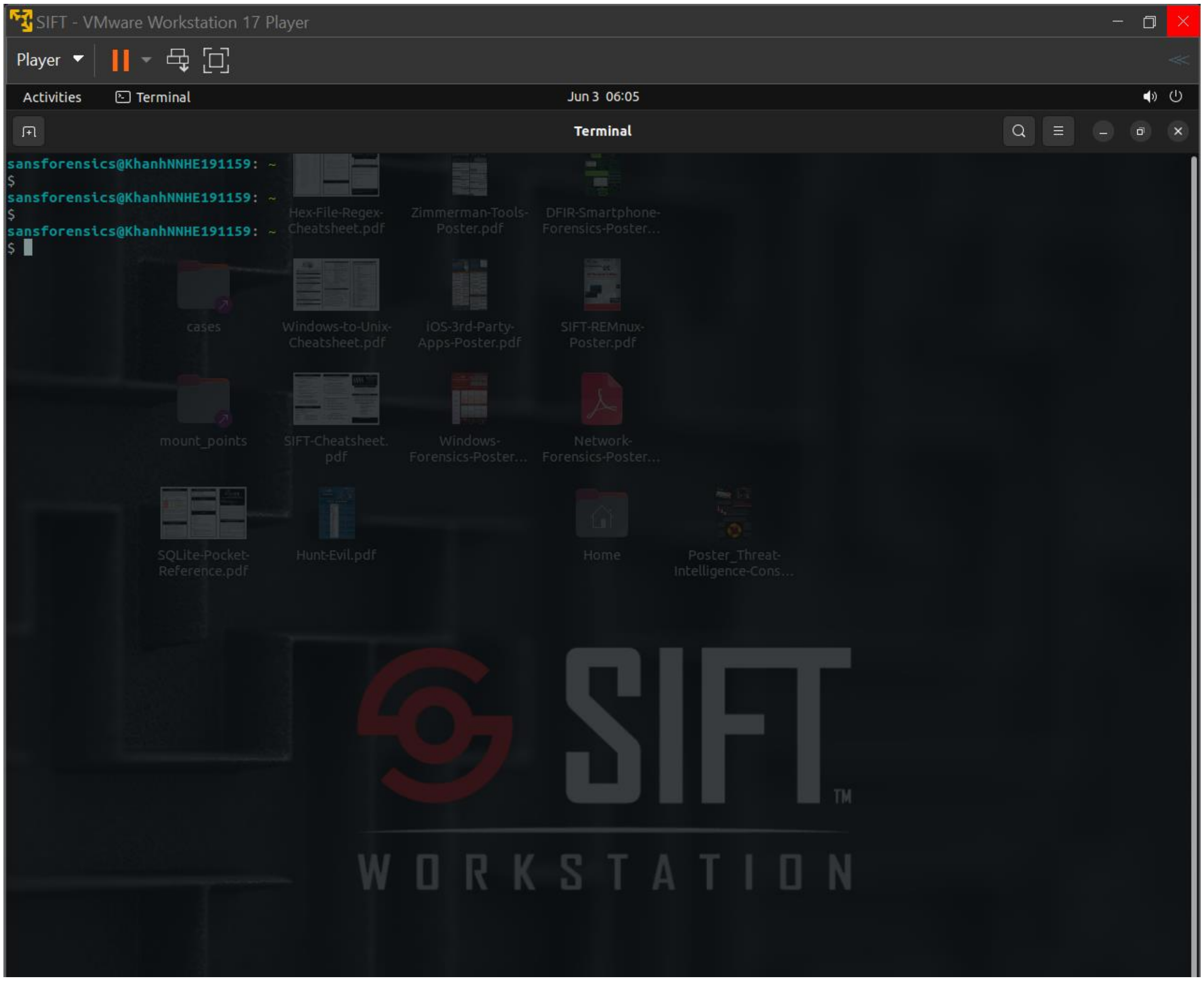
Option 1: SIFT Workstation VM Appliance

Check Hash Values of SIFT



```
ur PS C:\Users\Lenovo legion 5\Downloads> Get-FileHash .\sift-22.04-20240201.ova -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             6D82C7287E15ECC0C4F90F74D629E282                                       C:\Users\Lenovo legion 5\Down..
```

Set up SIFT workstation WM appliance successfully

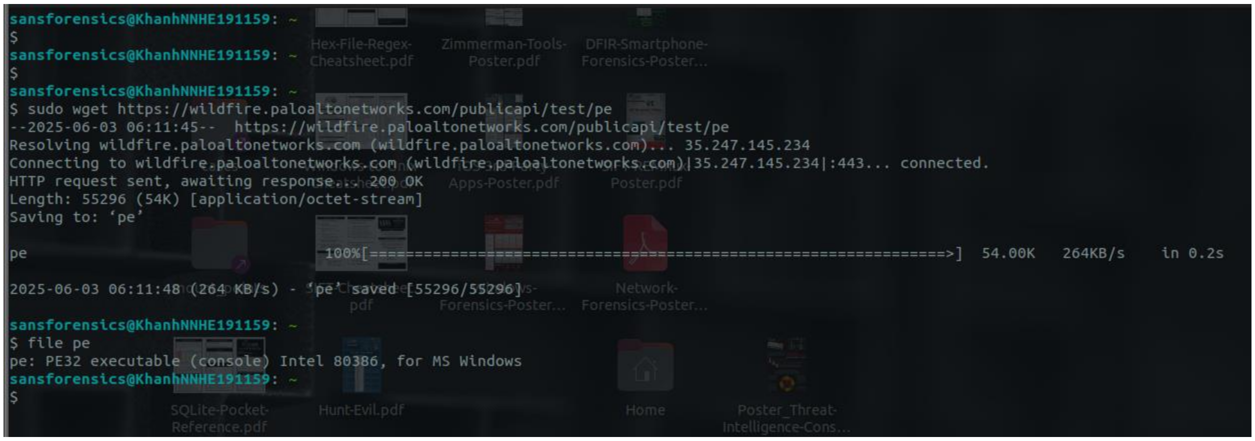


```
sansforensics@KhanhNNHE191159: ~
$
sansforensics@KhanhNNHE191159: ~
$
sansforensics@KhanhNNHE191159: ~
$ █
```

SIFT - VMware Workstation 17 Player
Player
Activities
Terminal
Jun 3 06:05
Terminal
Hex-File-Regex-Cheatsheet.pdf
Zimmerman-Tools-Poster.pdf
DFIR-Smartphone-Forensics-Poster...
cases
Windows-to-Unix-Cheatsheet.pdf
iOS-3rd-Party-Apps-Poster.pdf
SIFT-REMnux-Poster.pdf
mount_points
SIFT-Cheatsheet.pdf
Windows-Forensics-Poster...
Network-Forensics-Poster...
SQLite-Pocket-Reference.pdf
Hunt-Evil.pdf
Home
Poster_Threat-Intelligence-Cons...
SIFT
TM
WORKSTATION

Download 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.

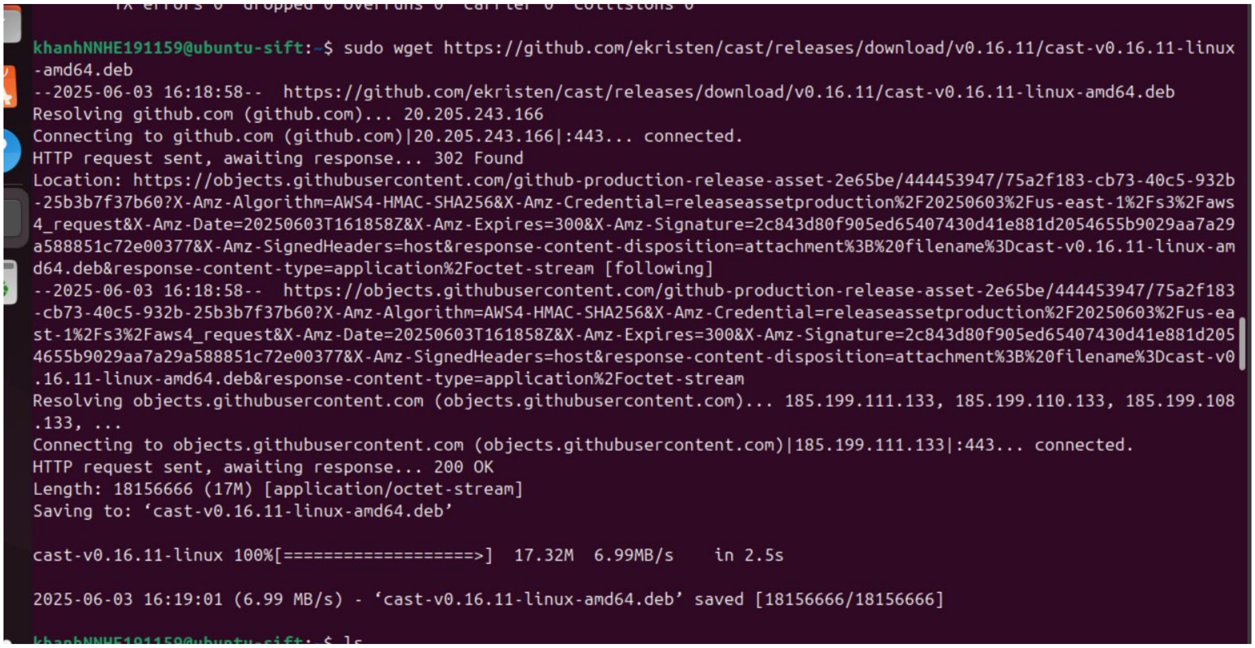


```
sansforensics@KhanhNNHE191159: ~
$
sansforensics@KhanhNNHE191159: ~
$
sansforensics@KhanhNNHE191159: ~
$ sudo wget https://wildfire.paloaltonetworks.com/publicapi/test/pe
--2025-06-03 06:11:45--  https://wildfire.paloaltonetworks.com/publicapi/test/pe
Resolving wildfire.paloaltonetworks.com (wildfire.paloaltonetworks.com)... 35.247.145.234
Connecting to wildfire.paloaltonetworks.com (wildfire.paloaltonetworks.com)|35.247.145.234|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 55296 (54K) [application/octet-stream]
Saving to: ‘pe’

pe                  100%[===================================================================>]  54.00K   264KB/s    in 0.2s

2025-06-03 06:11:48 (264 KB/s) - ‘pe’ saved [55296/55296]

sansforensics@KhanhNNHE191159: ~
$ file pe
pe: PE32 executable (console) Intel 80386, for MS Windows
sansforensics@KhanhNNHE191159: ~
$
```

Hex-File-Regex-Cheatsheet.pdf
Zimmerman-Tools-Poster.pdf
DFIR-Smartphone-Forensics-Poster...
Apps-Poster.pdf
Poster.pdf
Network-Forensics-Poster...
Forensics-Poster...
SQLite-Pocket-Reference.pdf
Hunt-Evil.pdf
Home
Poster_Threat-Intelligence-Cons...

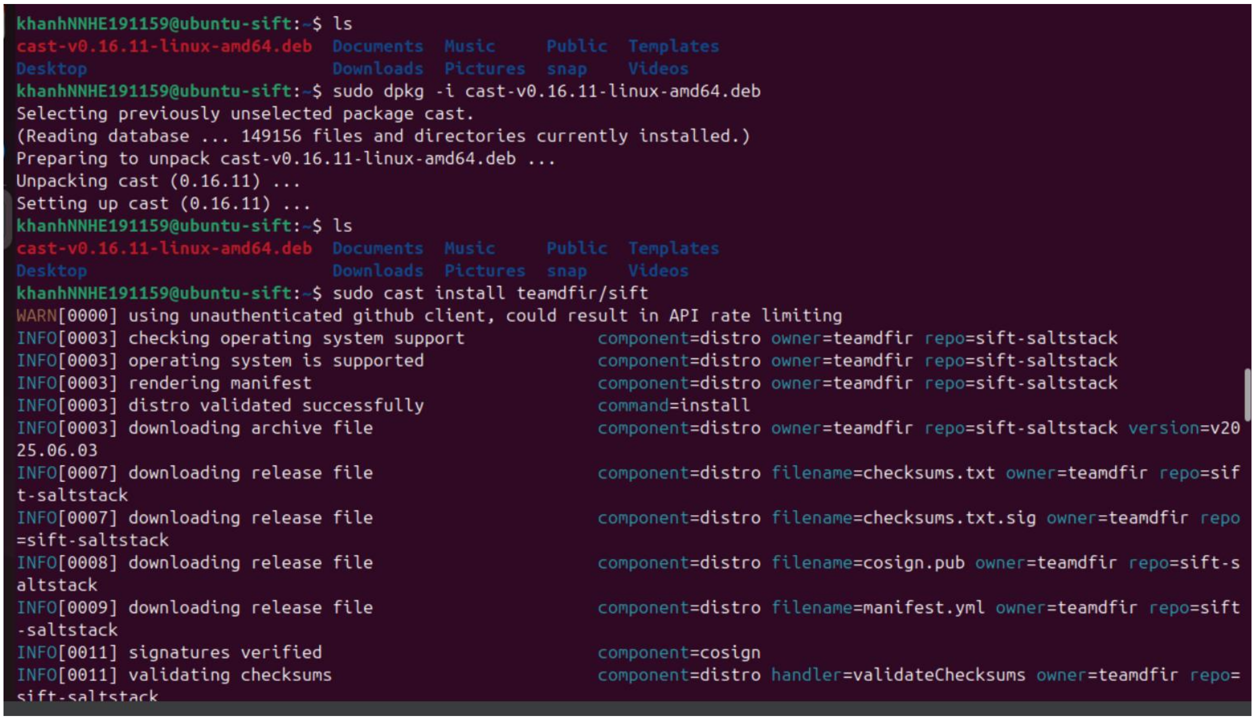
Option 2A: SIFT Easy Installation on Native Ubuntu System

Download Cast into ubuntu



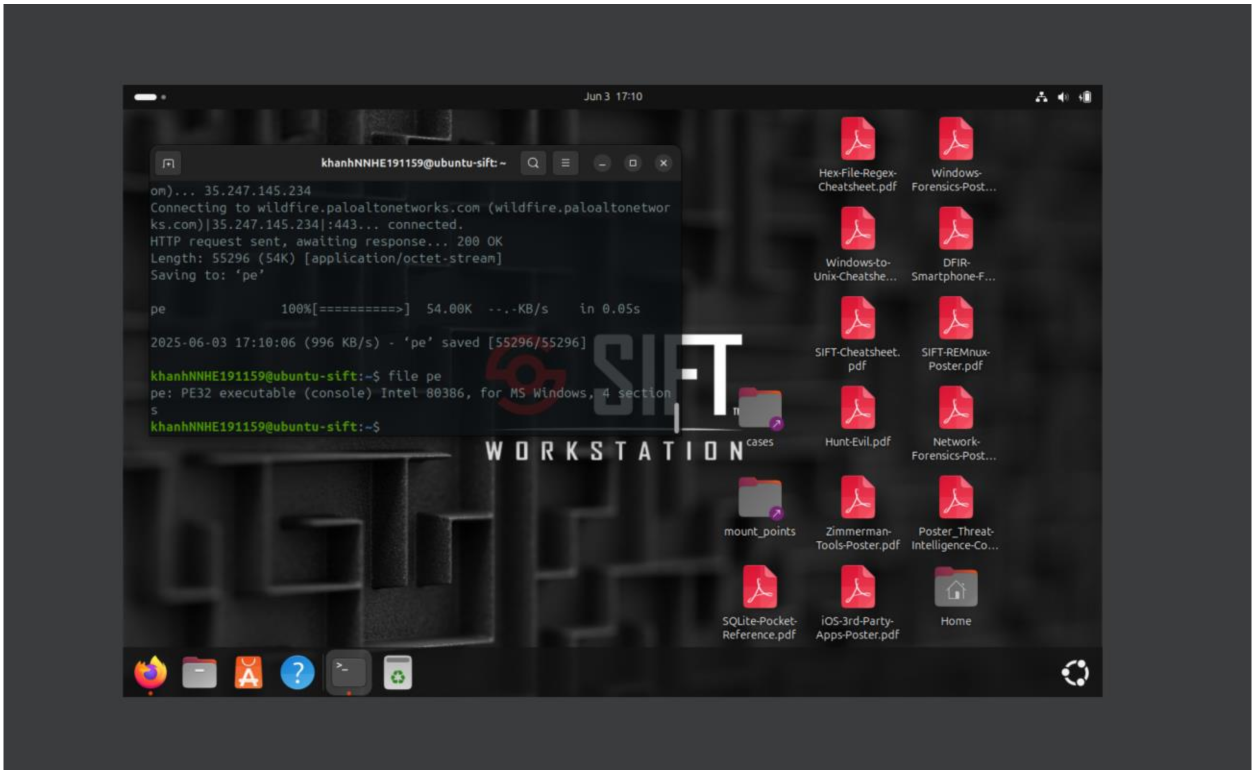
```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

khanhNNHE191159@ubuntu-sift:~$ sudo wget https://github.com/ekristen/cast/releases/download/v0.16.11/cast-v0.16.11-linux
-amd64.deb
--2025-06-03 16:18:58--  https://github.com/ekristen/cast/releases/download/v0.16.11/cast-v0.16.11-linux-amd64.deb
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/444453947/75a2f183-cb73-40c5-932b
-25b3b7f37b60?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20250603%2Fus-east-1%2Fs3%2Faws
4_request&X-Amz-Date=20250603T161858Z&X-Amz-Expires=300&X-Amz-Signature=2c843d80f905ed65407430d41e881d2054655b9029aa7a29
a588851c72e00377&X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3Dcast-v0.16.11-linux-am
d64.deb&response-content-type=application%2Foctet-stream [following]
--2025-06-03 16:18:58--  https://objects.githubusercontent.com/github-production-release-asset-2e65be/444453947/75a2f183
-cb73-40c5-932b-25b3b7f37b60?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20250603%2Fus-ea
st-1%2Fs3%2Faws4_request&X-Amz-Date=20250603T161858Z&X-Amz-Expires=300&X-Amz-Signature=2c843d80f905ed65407430d41e881d205
4655b9029aa7a29a588851c72e00377&X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3Dcast-v0
.16.11-linux-amd64.deb&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.199.108
.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18156666 (17M) [application/octet-stream]
Saving to: ‘cast-v0.16.11-linux-amd64.deb’

cast-v0.16.11-linux 100%[===================>]  17.32M  6.99MB/s    in 2.5s

2025-06-03 16:19:01 (6.99 MB/s) - ‘cast-v0.16.11-linux-amd64.deb’ saved [18156666/18156666]

khanhNNHE191159@ubuntu-sift:~$ ls
```

Execute Cast tools to automatically install latest version of SIFT on Github.



```
khanhNNHE191159@ubuntu-sift:~$ ls
cast-v0.16.11-linux-amd64.deb  Documents  Music     Public  Templates
Desktop                        Downloads  Pictures  snap    Videos
khanhNNHE191159@ubuntu-sift:~$ sudo dpkg -i cast-v0.16.11-linux-amd64.deb
Selecting previously unselected package cast.
(Reading database ... 149156 files and directories currently installed.)
Preparing to unpack cast-v0.16.11-linux-amd64.deb ...
Unpacking cast (0.16.11) ...
Setting up cast (0.16.11) ...
khanhNNHE191159@ubuntu-sift:~$ ls
cast-v0.16.11-linux-amd64.deb  Documents  Music     Public  Templates
Desktop                        Downloads  Pictures  snap    Videos
khanhNNHE191159@ubuntu-sift:~$ sudo cast install teamdfir/sift
WARN[0000] using unauthenticated github client, could result in API rate limiting
INFO[0003] checking operating system support             component=distro owner=teamdfir repo=sift-saltstack
INFO[0003] operating system is supported                 component=distro owner=teamdfir repo=sift-saltstack
INFO[0003] rendering manifest                            component=distro owner=teamdfir repo=sift-saltstack
INFO[0003] distro validated successfully                 command=install
INFO[0003] downloading archive file                      component=distro owner=teamdfir repo=sift-saltstack version=v20
25.06.03
INFO[0007] downloading release file                      component=distro filename=checksums.txt owner=teamdfir repo=sif
t-saltstack
INFO[0007] downloading release file                      component=distro filename=checksums.txt.sig owner=teamdfir repo
=sift-saltstack
INFO[0008] downloading release file                      component=distro filename=cosign.pub owner=teamdfir repo=sift-s
altstack
INFO[0009] downloading release file                      component=distro filename=manifest.yml owner=teamdfir repo=sift
-saltstack
INFO[0011] signatures verified                           component=cosign
INFO[0011] validating checksums                          component=distro handler=validateChecksums owner=teamdfir repo=
sift-saltstack
```

Congrats -- you now have a SIFT workstation!



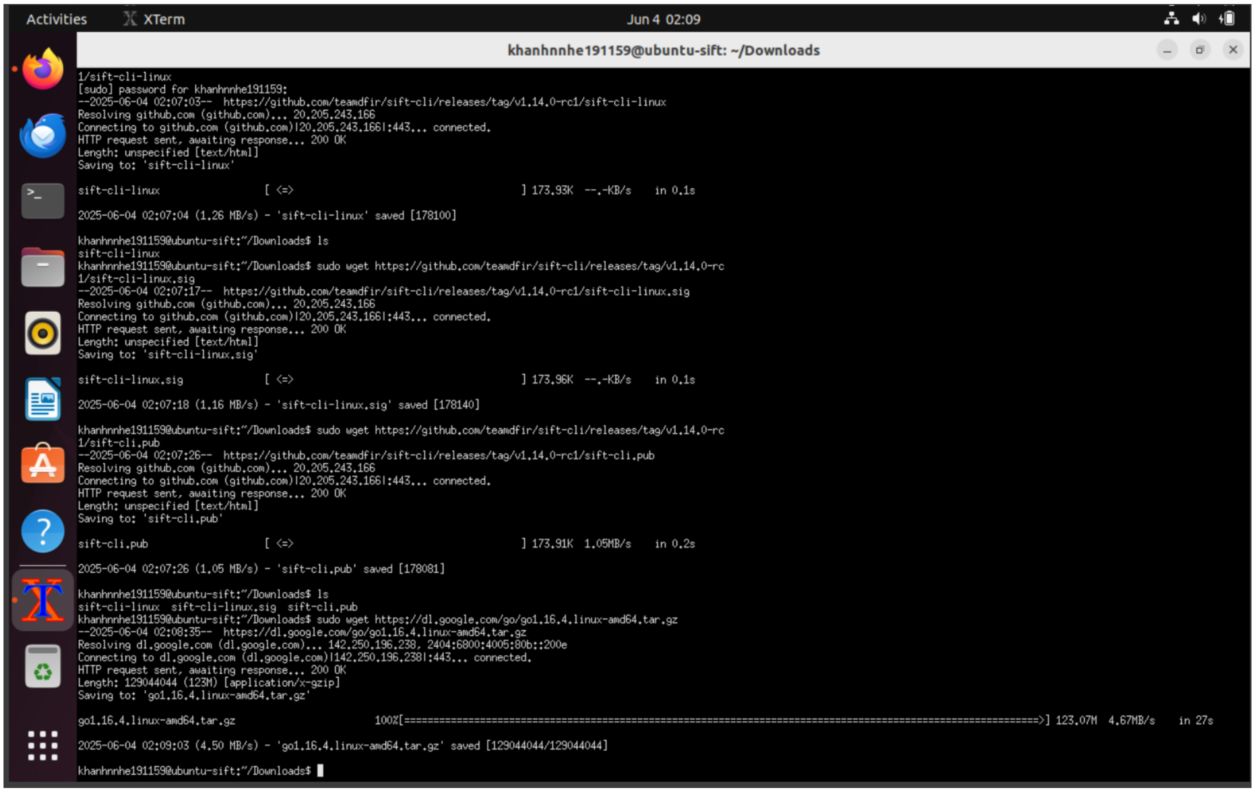
Jun 3 17:10
khanhNNHE191159@ubuntu-sift: ~
SIFT
WORKSTATION
Hex-File-Regex-Cheatsheet.pdf
Windows-Forensics-Post...
Windows-to-Unix-Cheatshe...
DFIR-Smartphone-F...
SIFT-Cheatsheet.pdf
SIFT-REMnux-Poster.pdf
cases
Hunt-Evil.pdf
Network-Forensics-Post...
mount_points
Zimmerman-Tools-Poster.pdf
Poster_Threat-Intelligence-Co...
SQLite-Pocket-Reference.pdf
iOS-3rd-Party-Apps-Poster.pdf
Home

```
om)... 35.247.145.234
Connecting to wildfire.paloaltonetworks.com (wildfire.paloaltonetwor
ks.com)|35.247.145.234|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 55296 (54K) [application/octet-stream]
Saving to: ‘pe’

pe                  100%[==========>]  54.00K  --.-KB/s    in 0.05s

2025-06-03 17:10:06 (996 KB/s) - ‘pe’ saved [55296/55296]

khanhNNHE191159@ubuntu-sift:~$ file pe
pe: PE32 executable (console) Intel 80386, for MS Windows, 4 section
s
khanhNNHE191159@ubuntu-sift:~$
```

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

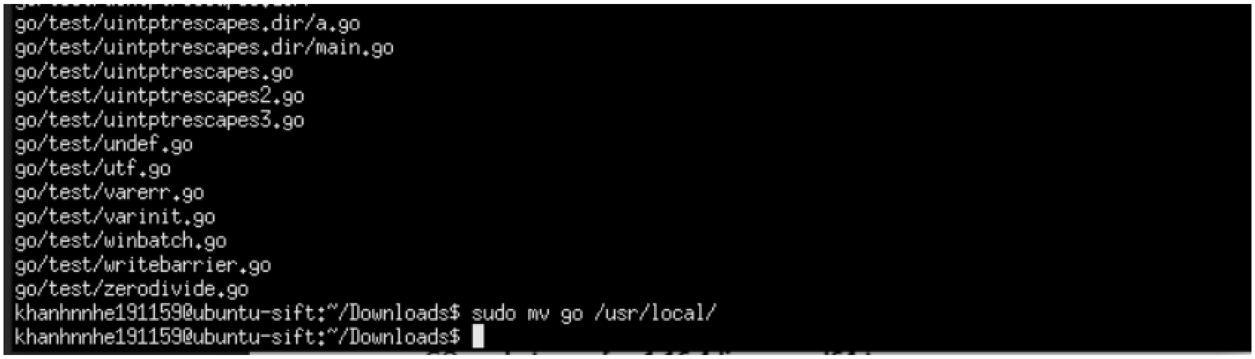
(Download SIFT manually)

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

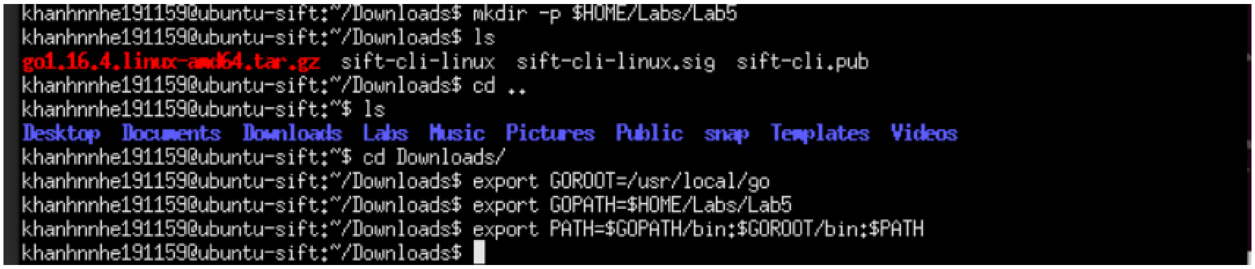


```
1/sift-cli-linux
[sudo] password for khanhnnhe191159:
--2025-06-04 02:07:03--  https://github.com/teamdfir/sift-cli/releases/tag/v1.14.0-rc1/sift-cli-linux
Resolving github.com (github.com)... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'sift-cli-linux'

sift-cli-linux              [ <=>                              ] 173.93K  --.-KB/s    in 0.1s

2025-06-04 02:07:04 (1.26 MB/s) - 'sift-cli-linux' saved [178100]

khanhnnhe191159@ubuntu-sift:~/Downloads$ ls
sift-cli-linux
khanhnnhe191159@ubuntu-sift:~/Downloads$ sudo wget https://github.com/teamdfir/sift-cli/releases/tag/v1.14.0-rc
1/sift-cli-linux.sig
--2025-06-04 02:07:17--  https://github.com/teamdfir/sift-cli/releases/tag/v1.14.0-rc1/sift-cli-linux.sig
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... 200 OK
Length: unspecified [text/html]
Saving to: 'sift-cli-linux.sig'

sift-cli-linux.sig          [ <=>                              ] 173.96K  --.-KB/s    in 0.1s

2025-06-04 02:07:18 (1.16 MB/s) - 'sift-cli-linux.sig' saved [178140]

khanhnnhe191159@ubuntu-sift:~/Downloads$ sudo wget https://github.com/teamdfir/sift-cli/releases/tag/v1.14.0-rc
1/sift-cli.pub
--2025-06-04 02:07:26--  https://github.com/teamdfir/sift-cli/releases/tag/v1.14.0-rc1/sift-cli.pub
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... 200 OK
Length: unspecified [text/html]
Saving to: 'sift-cli.pub'

sift-cli.pub                [ <=>                              ] 173.91K  1.05MB/s    in 0.2s

2025-06-04 02:07:26 (1.05 MB/s) - 'sift-cli.pub' saved [178081]

khanhnnhe191159@ubuntu-sift:~/Downloads$ ls
sift-cli-linux  sift-cli-linux.sig  sift-cli.pub
khanhnnhe191159@ubuntu-sift:~/Downloads$ sudo wget https://dl.google.com/go/go1.16.4.linux-amd64.tar.gz
--2025-06-04 02:08:35--  https://dl.google.com/go/go1.16.4.linux-amd64.tar.gz
Resolving dl.google.com (dl.google.com)... 142.250.196.238, 2404:6800:4005:80b::200e
Connecting to dl.google.com (dl.google.com)|142.250.196.238|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 129044044 (123M) [application/x-gzip]
Saving to: 'go1.16.4.linux-amd64.tar.gz'

go1.16.4.linux-amd64.tar.gz            100%[===================================================================================================>] 123.07M  4.67MB/s    in 27s

2025-06-04 02:09:03 (4.50 MB/s) - 'go1.16.4.linux-amd64.tar.gz' saved [129044044/129044044]

khanhnnhe191159@ubuntu-sift:~/Downloads$ █
```

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

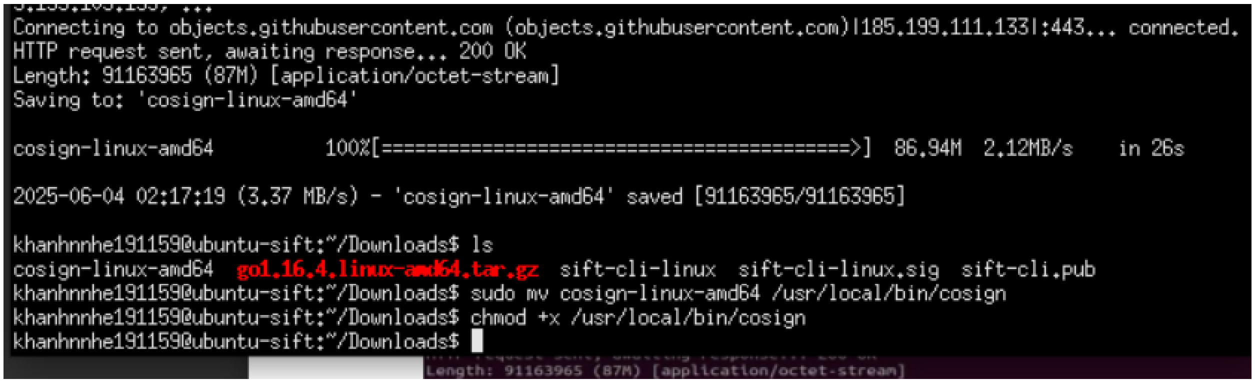


```
go/test/uintptrescapes.dir/a.go
go/test/uintptrescapes.dir/main.go
go/test/uintptrescapes.go
go/test/uintptrescapes2.go
go/test/uintptrescapes3.go
go/test/undef.go
go/test/utf.go
go/test/varerr.go
go/test/varinit.go
go/test/winbatch.go
go/test/writebarrier.go
go/test/zerodivide.go
khanhnnhe191159@ubuntu-sift:~/Downloads$ sudo mv go /usr/local/
khanhnnhe191159@ubuntu-sift:~/Downloads$ █
```



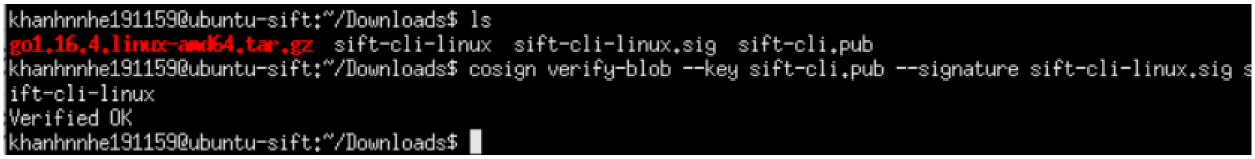
```
khanhnnhe191159@ubuntu-sift:~/Downloads$ mkdir -p $HOME/Labs/Lab5
khanhnnhe191159@ubuntu-sift:~/Downloads$ ls
go1.16.4.linux-amd64.tar.gz  sift-cli-linux  sift-cli-linux.sig  sift-cli.pub
khanhnnhe191159@ubuntu-sift:~/Downloads$ cd ..
khanhnnhe191159@ubuntu-sift:~$ ls
Desktop  Documents  Downloads  Labs  Music  Pictures  Public  snap  Templates  Videos
khanhnnhe191159@ubuntu-sift:~$ cd Downloads/
khanhnnhe191159@ubuntu-sift:~/Downloads$ export GOROOT=/usr/local/go
khanhnnhe191159@ubuntu-sift:~/Downloads$ export GOPATH=$HOME/Labs/Lab5
khanhnnhe191159@ubuntu-sift:~/Downloads$ export PATH=$GOPATH/bin:$GOROOT/bin:$PATH
khanhnnhe191159@ubuntu-sift:~/Downloads$ █
```

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



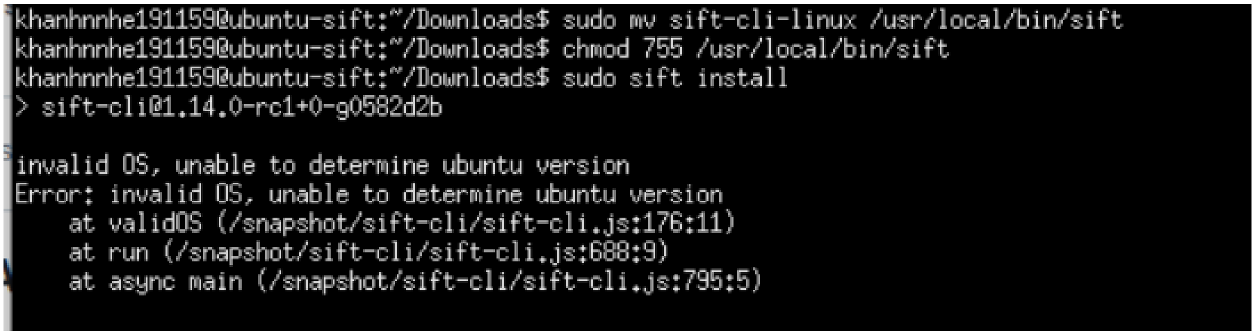
```
5.199.109.153, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 91163965 (87M) [application/octet-stream]
Saving to: 'cosign-linux-amd64'

cosign-linux-amd64         100%[=========================================>]  86.94M  2.12MB/s    in 26s

2025-06-04 02:17:19 (3.37 MB/s) - 'cosign-linux-amd64' saved [91163965/91163965]

khanhnnhe191159@ubuntu-sift:~/Downloads$ ls
cosign-linux-amd64  go1.16.4.linux-amd64.tar.gz  sift-cli-linux  sift-cli-linux.sig  sift-cli.pub
khanhnnhe191159@ubuntu-sift:~/Downloads$ sudo mv cosign-linux-amd64 /usr/local/bin/cosign
khanhnnhe191159@ubuntu-sift:~/Downloads$ chmod +x /usr/local/bin/cosign
khanhnnhe191159@ubuntu-sift:~/Downloads$ 
Length: 91163965 (87M) [application/octet-stream]
```

Verified successfully!



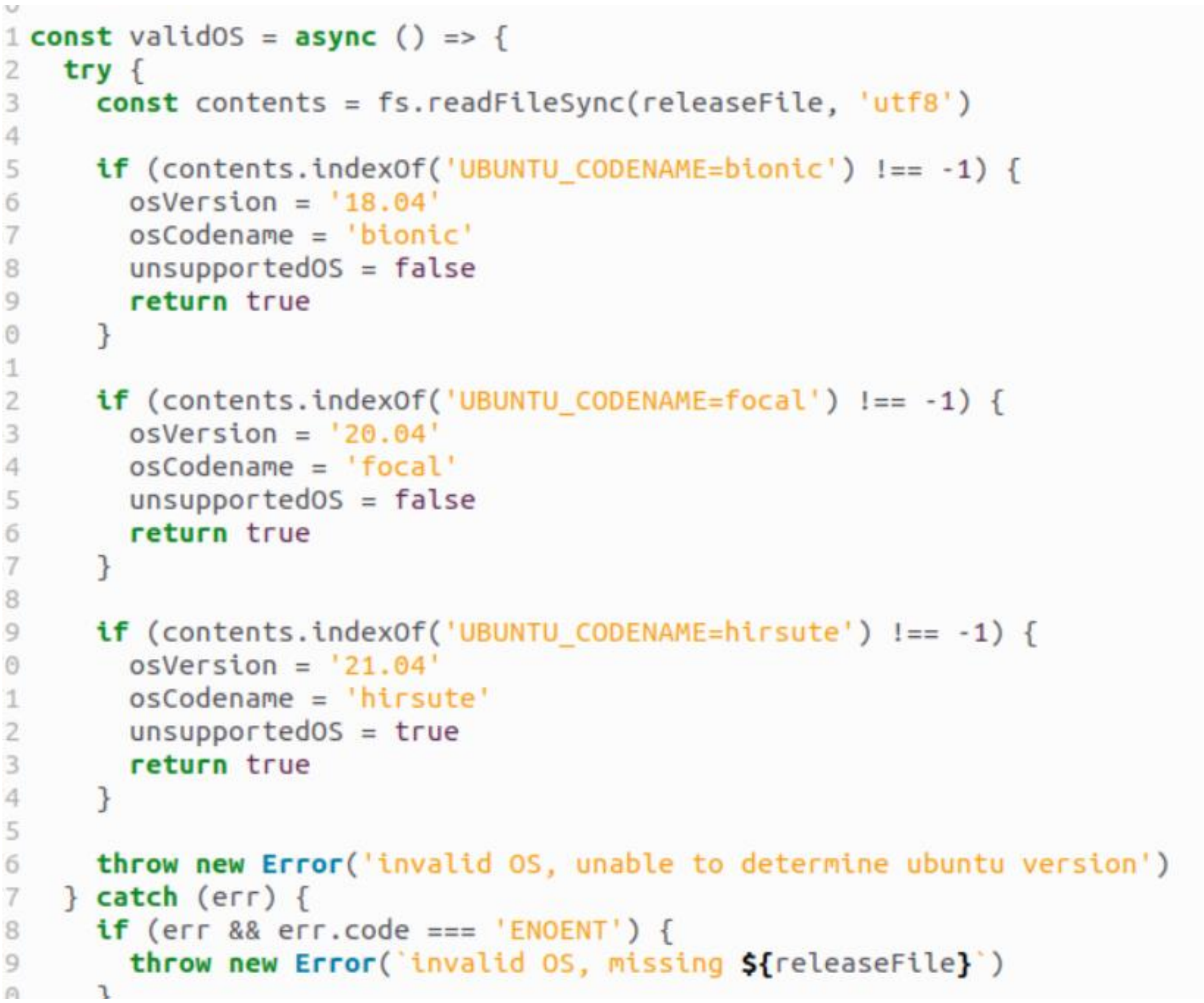
```
khanhnnhe191159@ubuntu-sift:~/Downloads$ ls
go1.16.4.linux-amd64.tar.gz  sift-cli-linux  sift-cli-linux.sig  sift-cli.pub
khanhnnhe191159@ubuntu-sift:~/Downloads$ cosign verify-blob --key sift-cli.pub --signature sift-cli-linux.sig s
ift-cli-linux
Verified OK
khanhnnhe191159@ubuntu-sift:~/Downloads$ 
```

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



```
khanhnnhe191159@ubuntu-sift:~/Downloads$ sudo mv sift-cli-linux /usr/local/bin/sift
khanhnnhe191159@ubuntu-sift:~/Downloads$ chmod 755 /usr/local/bin/sift
khanhnnhe191159@ubuntu-sift:~/Downloads$ sudo sift install
> sift-cli@1.14.0-rc1+0-g0582d2b

invalid OS, unable to determine ubuntu version
Error: invalid OS, unable to determine ubuntu version
    at validOS (/snapshot/sift-cli/sift-cli.js:176:11)
    at run (/snapshot/sift-cli/sift-cli.js:688:9)
    at async main (/snapshot/sift-cli/sift-cli.js:795:5)
```

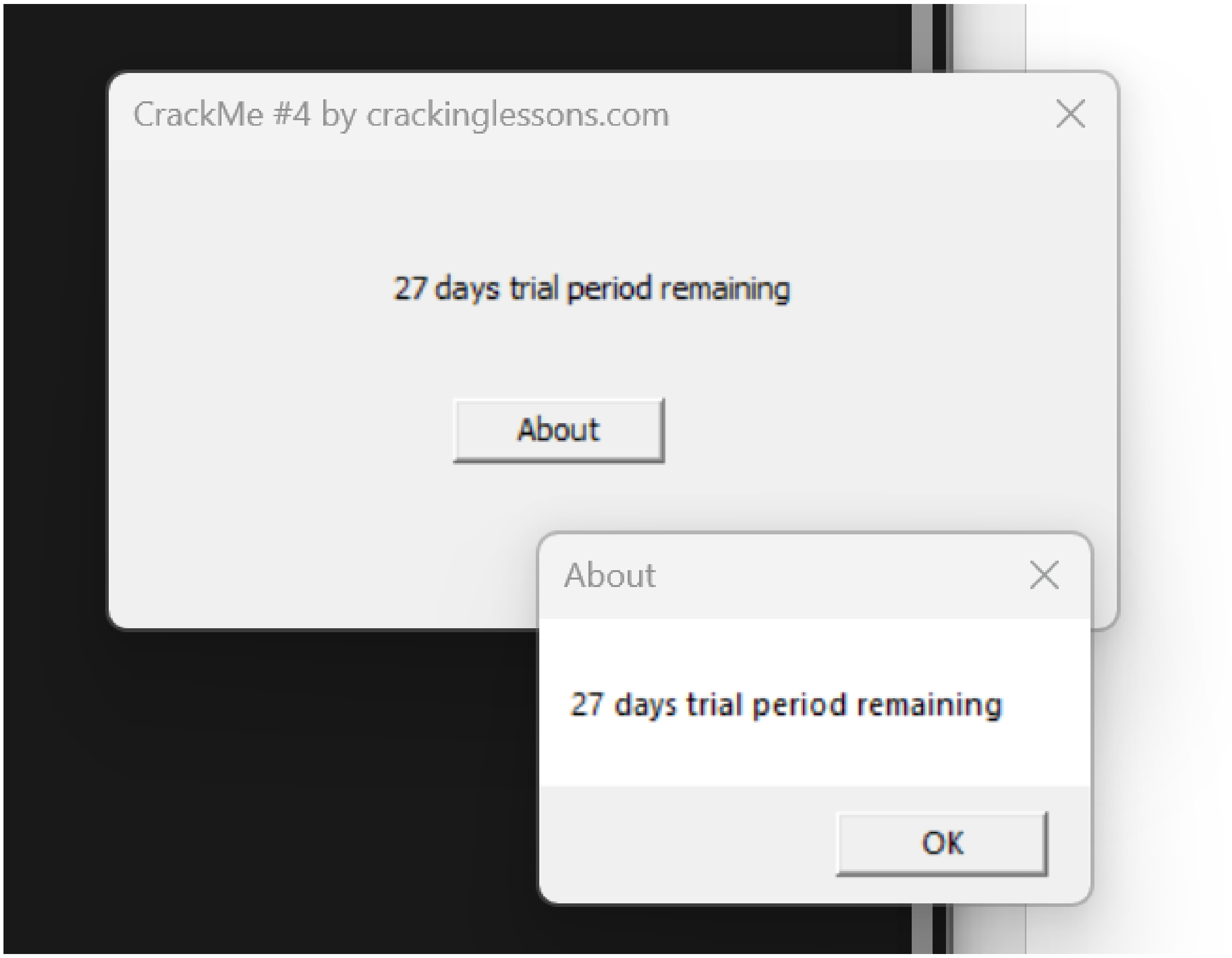
Notice: when install SIFT manually, i got stuck in invalid OS version error and trying change many version 22.04, 24.04 and having same error. So i inspected to source code of SIFT on Github and found that the code only checks 3 versions of Ubuntu: bionic (18.04), focal (20.04), and hirsute (21.04 not 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.



```
const validOS = async () => {
  try {
    const contents = fs.readFileSync(releaseFile, 'utf8')

    if (contents.indexOf('UBUNTU_CODENAME=bionic') !== -1) {
      osVersion = '18.04'
      osCodename = 'bionic'
      unsupportedOS = false
      return true
    }

    if (contents.indexOf('UBUNTU_CODENAME=focal') !== -1) {
      osVersion = '20.04'
      osCodename = 'focal'
      unsupportedOS = false
      return true
    }

    if (contents.indexOf('UBUNTU_CODENAME=hirsute') !== -1) {
      osVersion = '21.04'
      osCodename = 'hirsute'
      unsupportedOS = true
      return true
    }

    throw new Error('invalid OS, unable to determine ubuntu version')
  } catch (err) {
    if (err && err.code === 'ENOENT') {
      throw new Error(`invalid OS, missing ${releaseFile}`)
    }
```

CRACK ME 4

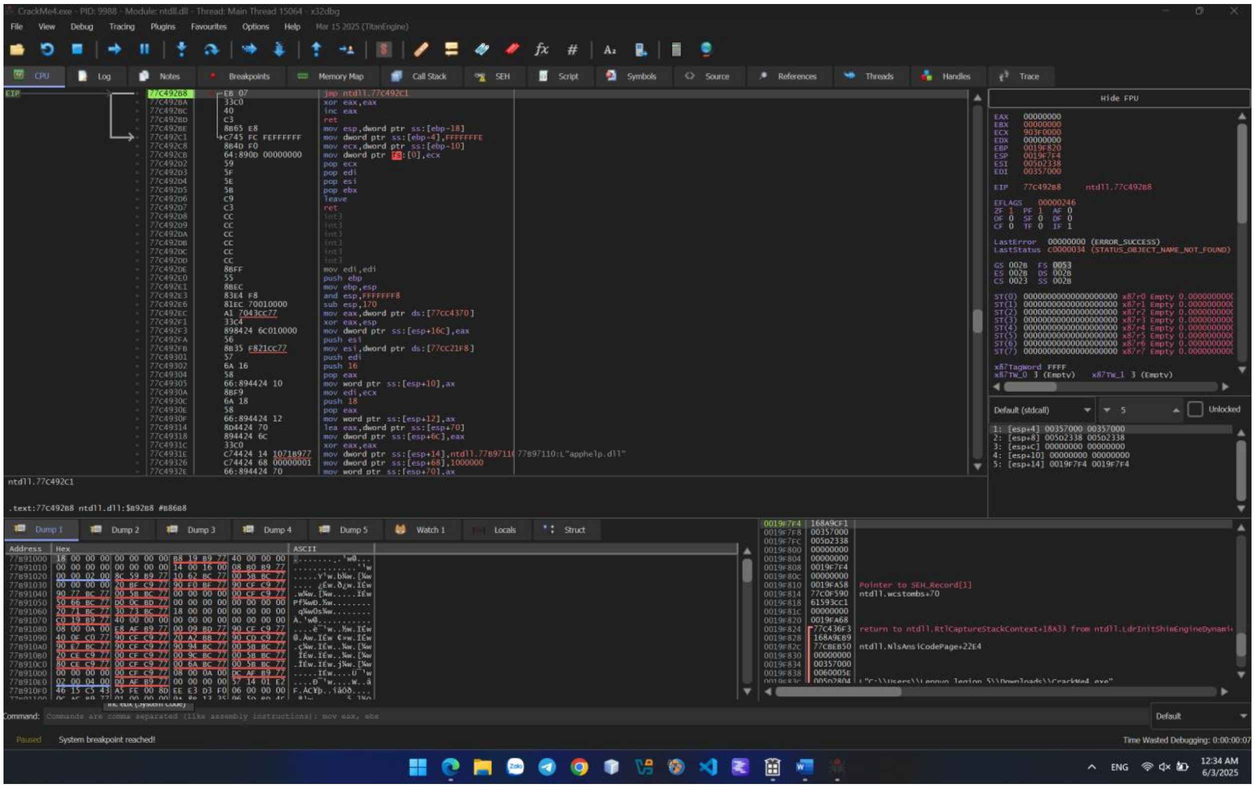
1. Crack it to extend beyond 30 days
2. In the About screen – also extend it to beyond 30 days



27 days trial period remaining

27 days trial period remaining

Open CrackMe4.exe in x32dbg to analyze.


CrackMe4.exe - PID: 9988 - Module: ntdll.dll - Thread: Main Thread 15064 - x32dbg
File View Debug Tracing Plugins Favourites Options Help Mar 15 2025 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Default (stdcall) 5 Unlocked
Default

```
EIP  77C492B8   EB 07              jmp ntdll.77C492C1
     77C492BA   33C0               xor eax,eax
     77C492BC   40                 inc eax
     77C492BD   C3                 ret
     77C492BE   8B65 E8            mov esp,dword ptr ss:[ebp-18]
     77C492C1   C745 FC FEFFFFFF   mov dword ptr ss:[ebp-4],FFFFFFFE
     77C492C8   8B4D F0            mov ecx,dword ptr ss:[ebp-10]
     77C492CB   64:890D 00000000   mov dword ptr fs:[0],ecx
     77C492D2   59                 pop ecx
     77C492D3   5F                 pop edi
     77C492D4   5E                 pop esi
     77C492D5   5B                 pop ebx
     77C492D6   C9                 leave
     77C492D7   C3                 ret
     77C492D8   CC                 int3
     77C492D9   CC                 int3
     77C492DA   CC                 int3
     77C492DB   CC                 int3
     77C492DC   CC                 int3
     77C492DD   CC                 int3
     77C492DE   8BFF               mov edi,edi
     77C492E0   55                 push ebp
     77C492E1   8BEC               mov ebp,esp
     77C492E3   83E4 F8            and esp,FFFFFFF8
     77C492E6   81EC 70010000      sub esp,170
     77C492EC   A1 7043CC77        mov eax,dword ptr ds:[77CC4370]
     77C492F1   33C4               xor eax,esp
     77C492F3   898424 6C010000    mov dword ptr ss:[esp+16C],eax
     77C492FA   56                 push esi
     77C492FB   8B35 F821CC77      mov esi,dword ptr ds:[77CC21F8]
     77C49301   57                 push edi
     77C49302   6A 16              push 16
     77C49304   58                 pop eax
     77C49305   66:894424 10       mov word ptr ss:[esp+10],ax
     77C4930A   8BF9               mov edi,ecx
     77C4930C   6A 18              push 18
     77C4930E   58                 pop eax
     77C4930F   66:894424 12       mov word ptr ss:[esp+12],ax
     77C49314   8D4424 70          lea eax,dword ptr ss:[esp+70]
     77C49318   894424 6C          mov dword ptr ss:[esp+6C],eax
     77C4931C   33C0               xor eax,eax
     77C4931E   C74424 14 1071B977 mov dword ptr ss:[esp+14],ntdll.77B97110   77B97110:L"apphelp.dll"
     77C49326   C74424 68 00000001 mov dword ptr ss:[esp+68],1000000
     77C4932E   66:894424 70       mov word ptr ss:[esp+70],ax

ntdll.77C492C1

.text:77C492B8 ntdll.dll:$B92B8 #B86B8
```

```
EAX   00000000
EBX   00000000
ECX   903F0000
EDX   00000000
EBP   0019F820
ESP   0019F7F4
ESI   005D2338
EDI   00357000

EIP   77C492B8     ntdll.77C492B8

EFLAGS   00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError   00000000 (ERROR_SUCCESS)
LastStatus  C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) 00000000000000000000 x87r0 Empty 0.000000000000
ST(1) 00000000000000000000 x87r1 Empty 0.000000000000
ST(2) 00000000000000000000 x87r2 Empty 0.000000000000
ST(3) 00000000000000000000 x87r3 Empty 0.000000000000
ST(4) 00000000000000000000 x87r4 Empty 0.000000000000
ST(5) 00000000000000000000 x87r5 Empty 0.000000000000
ST(6) 00000000000000000000 x87r6 Empty 0.000000000000
ST(7) 00000000000000000000 x87r7 Empty 0.000000000000

x87TagWord FFFF
x87TW_0 3 (Empty)   x87TW_1 3 (Empty)

1: [esp+4] 00357000 00357000
2: [esp+8] 005D2338 005D2338
3: [esp+C] 00000000 00000000
4: [esp+10] 00000000 00000000
5: [esp+14] 0019F7F4 0019F7F4
```

```
Address   Hex                                               ASCII
77B91000  18 00 00 00 00 00 00 00 B8 19 B9 77 40 00 00 00  ........¸.¹w@...
77B91010  00 00 00 00 00 00 00 00 14 00 16 00 08 B0 B9 77  ..............°¹w
77B91020  00 00 02 00 8C 59 B9 77 10 62 BC 77 00 5B BC 77  .....Y¹w.b¼w.[¼w
77B91030  00 00 00 00 20 BF C9 77 90 F0 BF 77 90 CF C9 77  .... ¿Éw.ð¿w.ÏÉw
77B91040  90 77 BC 77 00 5B BC 77 00 00 00 00 00 CF C9 77  .w¼w.[¼w.....ÏÉw
77B91050  50 66 BC 77 D0 0C BD 77 00 00 00 00 00 00 00 00  Pf¼wÐ.½w........
77B91060  20 71 BC 77 30 73 BC 77 18 00 00 00 00 00 00 00   q¼w0s¼w........
77B91070  C0 19 B9 77 40 00 00 00 00 00 00 00 00 00 00 00  À.¹w@...........
77B91080  08 00 0A 00 E8 AF B9 77 00 09 BD 77 90 CF C9 77  ....è¯¹w..½w.ÏÉw
77B91090  40 0E C0 77 90 CF C9 77 20 A2 BB 77 90 CD C9 77  @.Àw.ÏÉw ¢»w.ÍÉw
77B910A0  90 E7 BC 77 90 CF C9 77 90 94 BC 77 00 5B BC 77  .ç¼w.ÏÉw..¼w.[¼w
77B910B0  20 CE C9 77 00 CF C9 77 00 9C BC 77 00 5B BC 77   ÎÉw.ÏÉw..¼w.[¼w
77B910C0  80 CE C9 77 00 CF C9 77 00 6A BC 77 00 5B BC 77  .ÎÉw.ÏÉw.j¼w.[¼w
77B910D0  00 00 00 00 00 CF C9 77 08 00 0A 00 DC AF B9 77  .....ÏÉw....Ü¯¹w
77B910E0  02 00 04 00 D0 AF B9 77 00 00 00 00 57 14 01 E2  ....Ð¯¹w....W..â
77B910F0  46 15 C5 43 A5 FE 00 8D EE E3 D3 F0 06 00 00 00  F.ÅC¥þ..îãÓð....
```

```
0019F7F4  168A9CF1
0019F7F8  00357000
0019F7FC  005D2338
0019F800  00000000
0019F804  00000000
0019F808  0019F7F4
0019F80C  00000000
0019F810  0019FA58  Pointer to SEH_Record[1]
0019F814  77C0F590  ntdll.wcstombs+70
0019F818  61593CC1
0019F81C  00000000
0019F820  0019FA68
0019F824  77C436F3  return to ntdll.RtlCaptureStackContext+18A33 from ntdll.LdrInitShimEngineDynami
0019F828  168A9EB9
0019F82C  77CBEB50  ntdll.NlsAnsiCodePage+22E4
0019F830  00000000
0019F834  00357000
0019F838  0060005E
0019F83C  005D2804  L"C:\\Users\\Lenovo Legion 5\\Downloads\\CrackMe4.exe"
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

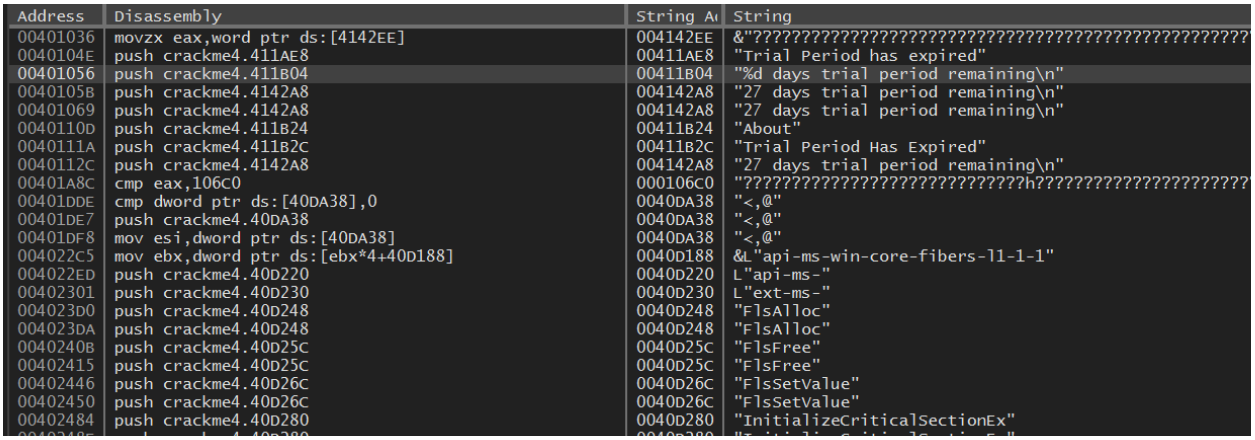
Paused System breakpoint reached!

Time Wasted Debugging: 0:00:00:07

12:34 AM
6/3/2025

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

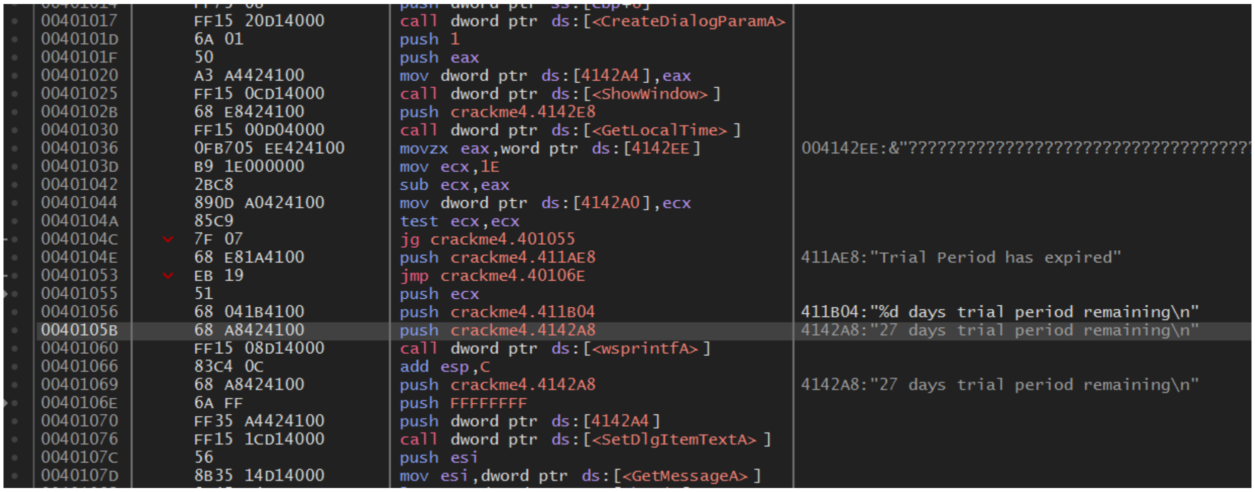
Choose Search for > Current Module > typing “27 days trial period remaining” and find related strings.



Address	Disassembly	String Ad	String
00401036	movzx eax,word ptr ds:[4142EE]	004142EE	&"??"
0040104E	push crackme4.411AE8	00411AE8	"Trial Period has expired"
00401056	push crackme4.411B04	00411B04	"%d days trial period remaining\n"
0040105B	push crackme4.4142A8	004142A8	"27 days trial period remaining\n"
00401069	push crackme4.4142A8	004142A8	"27 days trial period remaining\n"
0040110D	push crackme4.411B24	00411B24	"About"
0040111A	push crackme4.411B2C	00411B2C	"Trial Period Has Expired"
0040112C	push crackme4.4142A8	004142A8	"27 days trial period remaining\n"
00401A8C	cmp eax,106C0	000106C0	"??????????????????????????h?????????????"
00401DDE	cmp dword ptr ds:[40DA38],0	0040DA38	"<,@"
00401DE7	push crackme4.40DA38	0040DA38	"<,@"
00401DF8	mov esi,dword ptr ds:[40DA38]	0040DA38	"<,@"
004022C5	mov ebx,dword ptr ds:[ebx*4+40D188]	0040D188	&L"api-ms-win-core-fibers-l1-1-1"
004022ED	push crackme4.40D220	0040D220	L"api-ms-"
00402301	push crackme4.40D230	0040D230	L"ext-ms-"
004023D0	push crackme4.40D248	0040D248	"FlsAlloc"
004023DA	push crackme4.40D248	0040D248	"FlsAlloc"
0040240B	push crackme4.40D25C	0040D25C	"FlsFree"
00402415	push crackme4.40D25C	0040D25C	"FlsFree"
00402446	push crackme4.40D26C	0040D26C	"FlsSetValue"
00402450	push crackme4.40D26C	0040D26C	"FlsSetValue"
00402484	push crackme4.40D280	0040D280	"InitializeCriticalSectionEx"

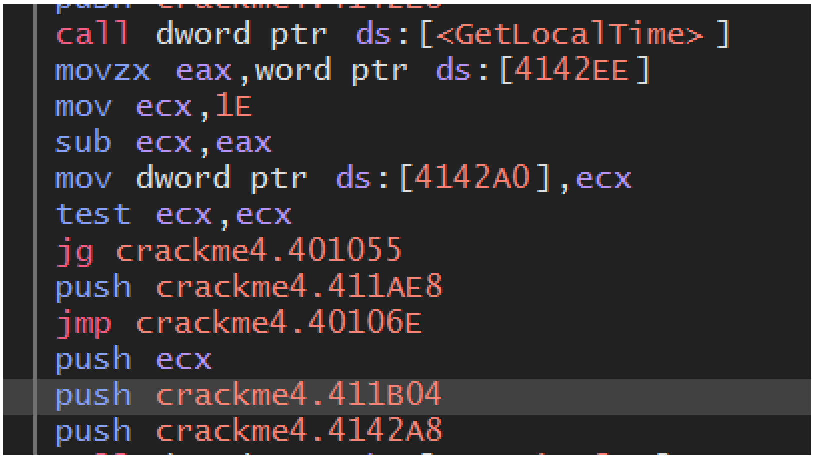
Notice the string "%d days trial period remaining\n" and inspect to the assembly code of these string.

Analyze above and below code of this string.



```
00401017    FF15 20D14000    call dword ptr ds:[<CreateDialogParamA>
0040101D    6A 01            push 1
0040101F    50               push eax
00401020    A3 A4424100      mov dword ptr ds:[4142A4],eax
00401025    FF15 0CD14000    call dword ptr ds:[<ShowWindow> ]
0040102B    68 E8424100      push crackme4.4142E8
00401030    FF15 00D04000    call dword ptr ds:[<GetLocalTime> ]
00401036    0FB705 EE424100  movzx eax,word ptr ds:[4142EE]           004142EE:&"???????????????????????????????????
0040103D    B9 1E000000      mov ecx,1E
00401042    2BC8             sub ecx,eax
00401044    890D A0424100    mov dword ptr ds:[4142A0],ecx
0040104A    85C9             test ecx,ecx
0040104C    7F 07            jg crackme4.401055
0040104E    68 E81A4100      push crackme4.411AE8                     411AE8:"Trial Period has expired"
00401053    EB 19            jmp crackme4.40106E
00401055    51               push ecx
00401056    68 041B4100      push crackme4.411B04                     411B04:"%d days trial period remaining\n"
0040105B    68 A8424100      push crackme4.4142A8                     4142A8:"27 days trial period remaining\n"
00401060    FF15 08D14000    call dword ptr ds:[<wsprintfA> ]
00401066    83C4 0C          add esp,C
00401069    68 A8424100      push crackme4.4142A8                     4142A8:"27 days trial period remaining\n"
0040106E    6A FF            push FFFFFFFF
00401070    FF35 A4424100    push dword ptr ds:[4142A4]
00401076    FF15 1CD14000    call dword ptr ds:[<SetDlgItemTextA> ]
0040107C    56               push esi
0040107D    8B35 14D14000    mov esi,dword ptr ds:[<GetMessageA> ]
```

Notice these some line of code.



```
call dword ptr ds:[<GetLocalTime> ]
movzx eax,word ptr ds:[4142EE]
mov ecx,1E
sub ecx,eax
mov dword ptr ds:[4142A0],ecx
test ecx,ecx
jg crackme4.401055
push crackme4.411AE8
jmp crackme4.40106E
push ecx
push crackme4.411B04
push crackme4.4142A8
```

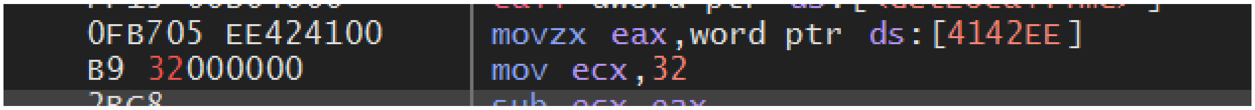
Function GetLocalTime get time of system and move to EAX.

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

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

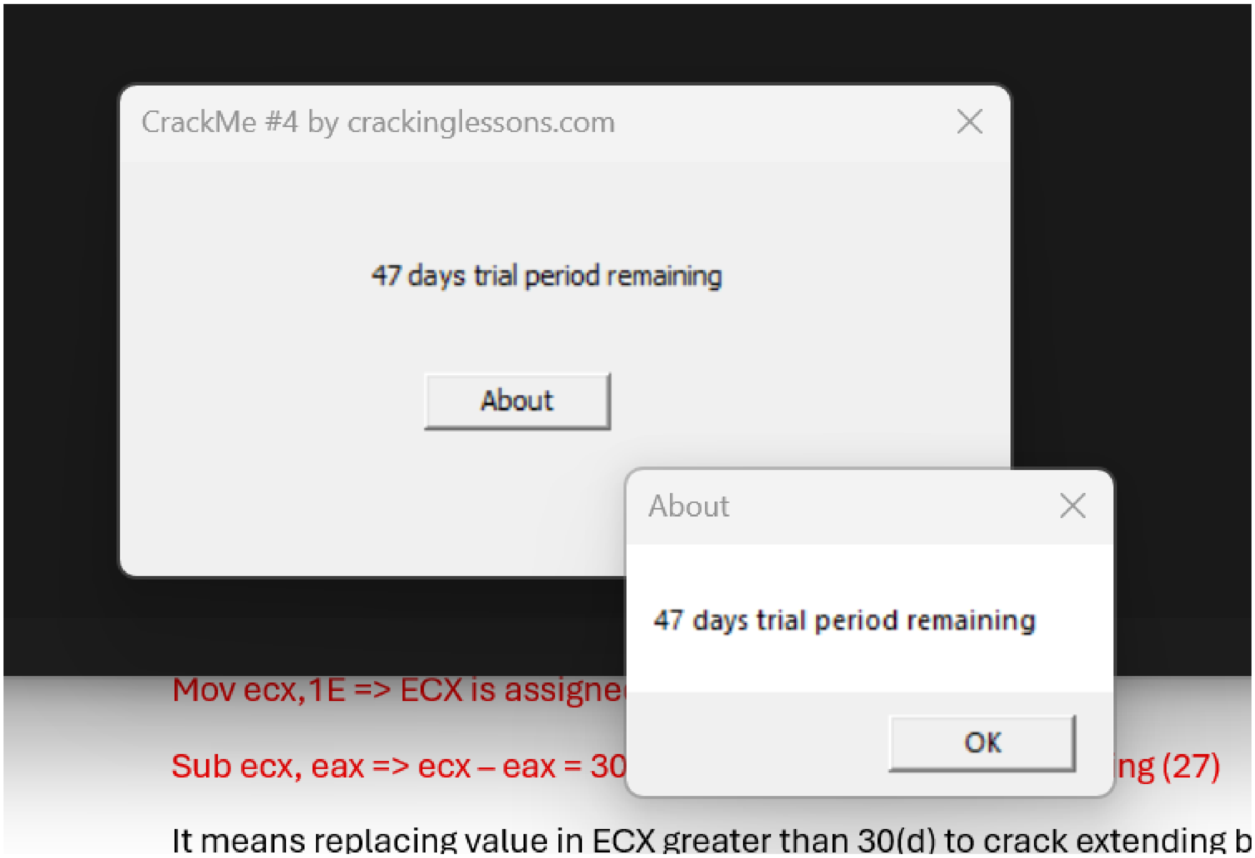
It means replacing value in ECX greater than 30(d) to crack extending beyond 30 days.

Decison change it to another value greater than 1E, such 32 (50 in decimal).



```
0FB705 EE424100    movzx eax,word ptr ds:[4142EE]
B9 32000000        mov ecx,32
```

Patch it and run to check the result.



47 days trial period remaining

47 days trial period remaining

Mov ecx,1E => ECX is assigne

Sub ecx, eax => ecx – eax = 30 ng (27)

It means replacing value in ECX greater than 30(d) to crack extending b

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!