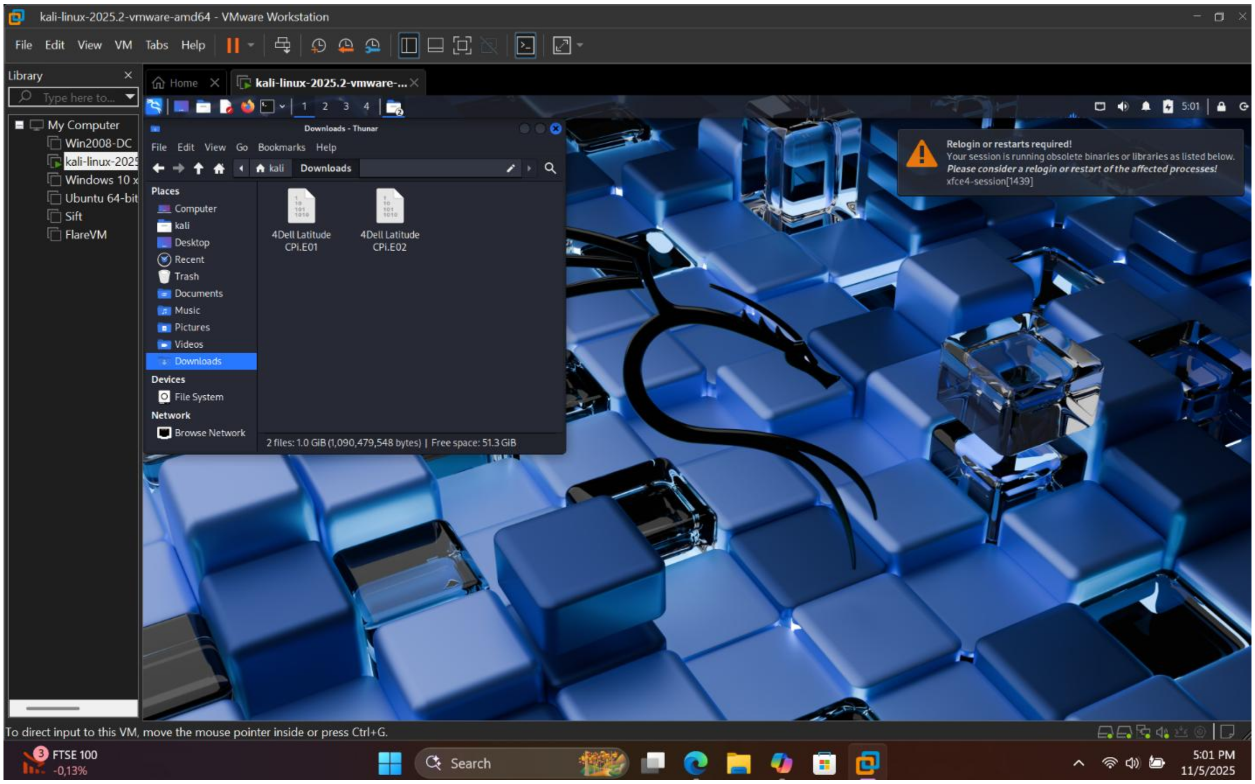
Báo cáo lab 13-FRS

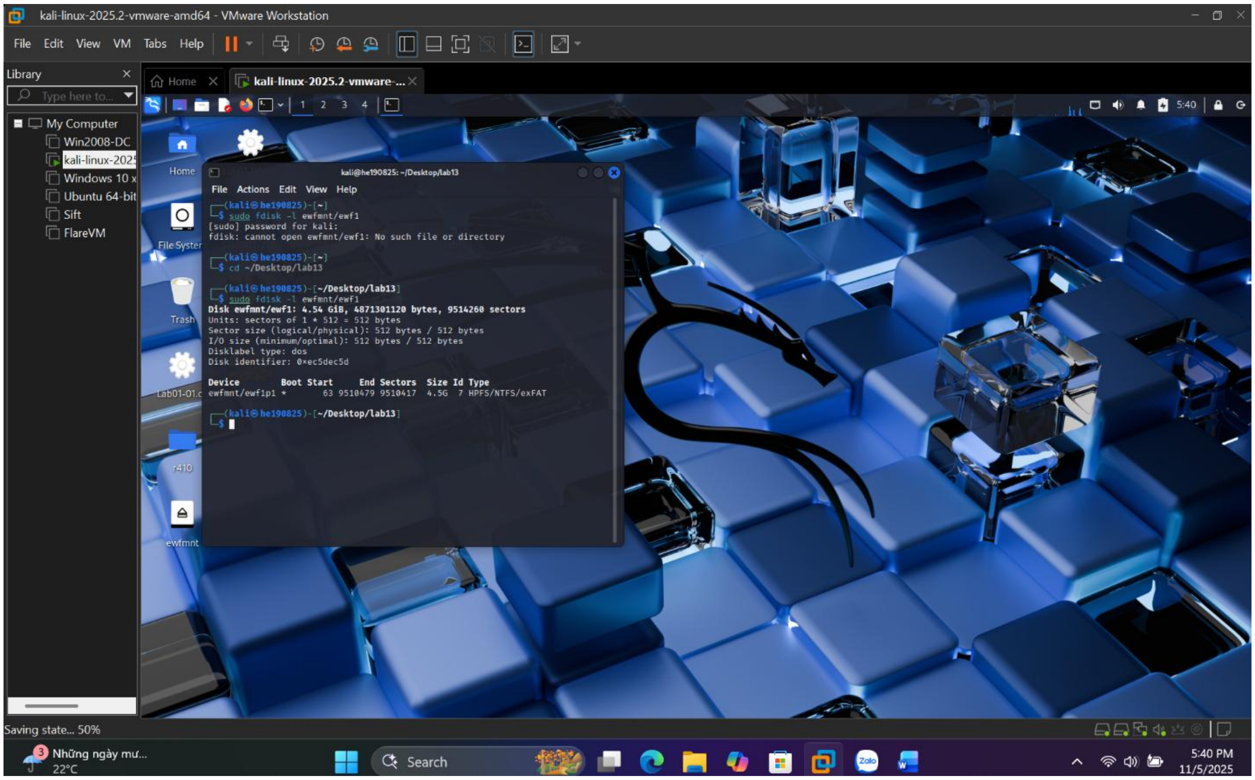
Họ và tên: Hoàng Đình Lâm
MSSV: HE190825



2 files: 1.0 GiB (1,090,479,548 bytes) | Free space: 51.3 GiB

Relogin or restarts required!
Your session is running obsolete binaries or libraries as listed below.
Please consider a relogin or restart of the affected processes!
xfce4-session[1439]

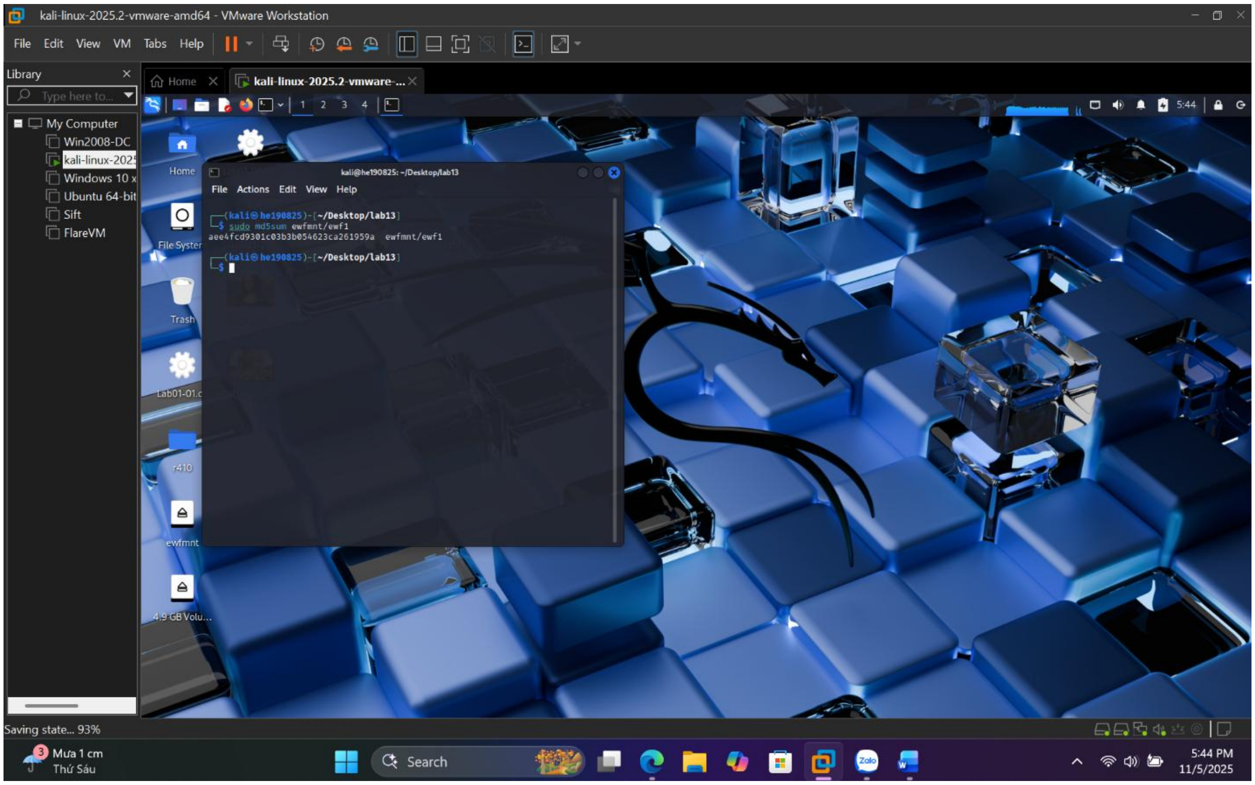
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



```
┌──(kali㉿he190825)-[~]
└─$ sudo fdisk -l ewfmnt/ewf1
[sudo] password for kali:
fdisk: cannot open ewfmnt/ewf1: No such file or directory

┌──(kali㉿he190825)-[~]
└─$ cd ~/Desktop/lab13

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ sudo fdisk -l ewfmnt/ewf1
Disk ewfmnt/ewf1: 4.54 GiB, 4871301120 bytes, 9514260 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0×ec5dec5d

Device         Boot Start     End Sectors  Size Id Type
ewfmnt/ewf1p1 *       63 9510479 9510417  4.5G  7 HPFS/NTFS/exFAT

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ 
```

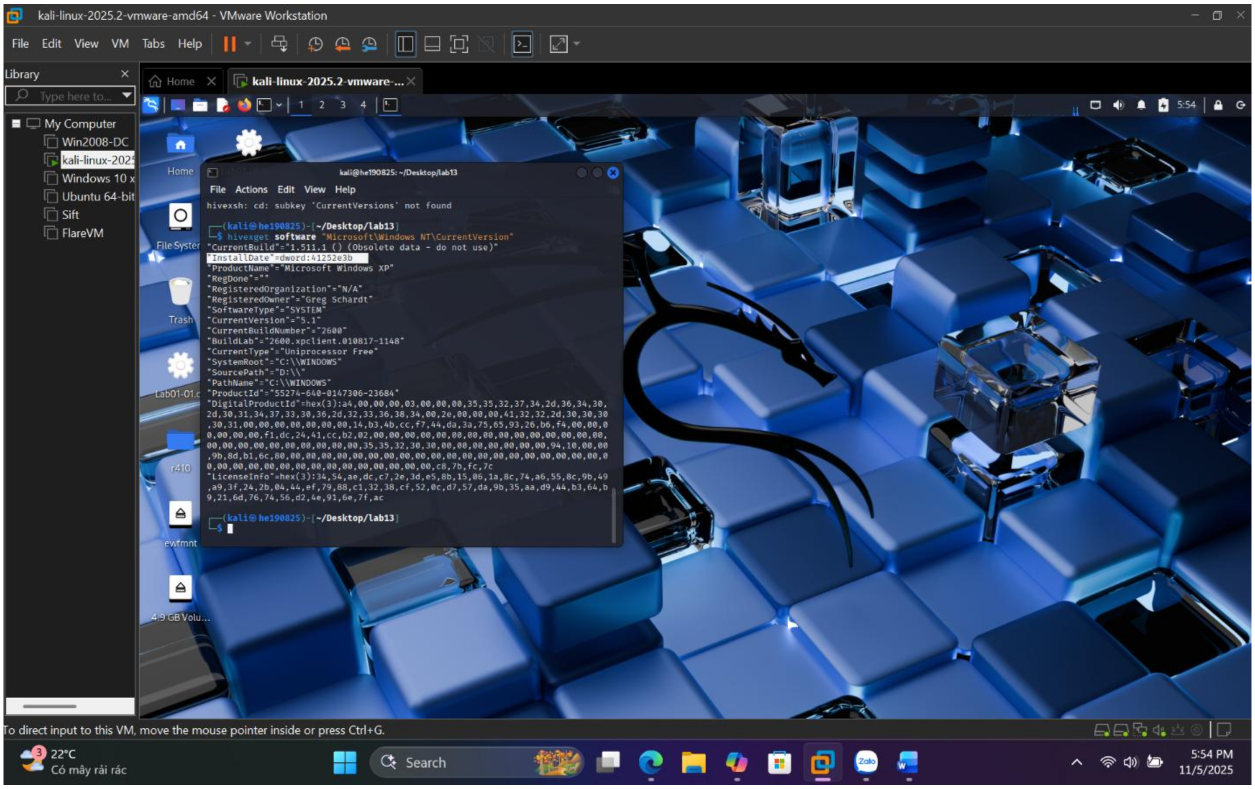
Saving state... 50%

1. What is the image hash? Does the acquisition and verification hash match?

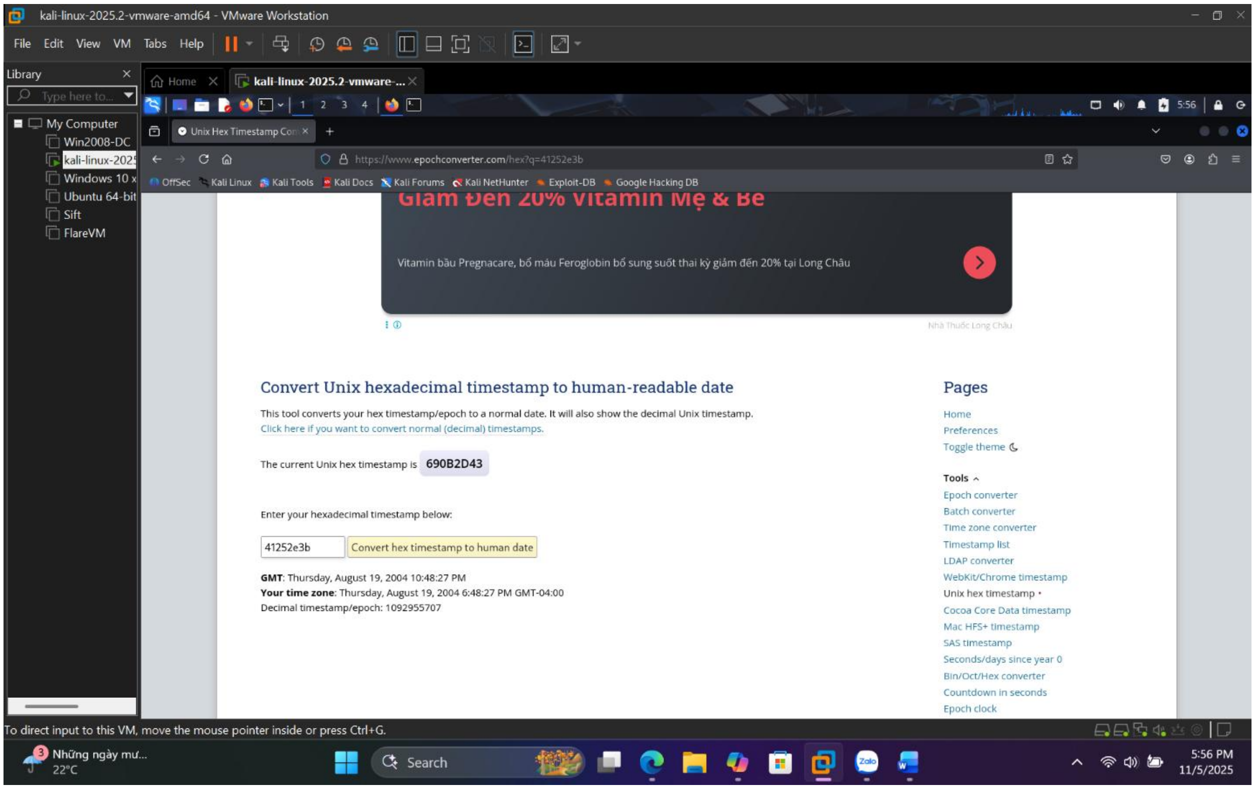


```
┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ sudo md5sum ewfmnt/ewf1
aee4fcd9301c03b3b054623ca261959a  ewfmnt/ewf1

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ 
```

3. When was the install date?


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to...
My Computer
Win2008-DC
kali-linux-2025
Windows 10 x
Ubuntu 64-bit
Sift
FlareVM
Home
kali-linux-2025.2-vmware-...
kali@he190825: ~/Desktop/lab13
File Actions Edit View Help
Home
File System
Trash
Lab01-01.c
r410
ewfmnt
4.9 GB Volu...
5:54
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
22°C
Có mây rải rác
Search
5:54 PM
11/5/2025

```
hivexsh: cd: subkey 'CurrentVersions' not found

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ hivexget software "Microsoft\Windows NT\CurrentVersion"
"CurrentBuild"="1.511.1 () (Obsolete data - do not use)"
"InstallDate"=dword:41252e3b
"ProductName"="Microsoft Windows XP"
"RegDone"=""
"RegisteredOrganization"="N/A"
"RegisteredOwner"="Greg Schardt"
"SoftwareType"="SYSTEM"
"CurrentVersion"="5.1"
"CurrentBuildNumber"="2600"
"BuildLab"="2600.xpclient.010817-1148"
"CurrentType"="Uniprocessor Free"
"SystemRoot"="C:\\WINDOWS"
"SourcePath"="D:\\"
"PathName"="C:\\WINDOWS"
"ProductId"="55274-640-0147306-23684"
"DigitalProductId"=hex(3):a4,00,00,00,03,00,00,00,35,35,32,37,34,2d,36,34,30,
2d,30,31,34,37,33,30,36,2d,32,33,36,38,34,00,2e,00,00,00,41,32,32,2d,30,30,30
,30,31,00,00,00,00,00,00,00,14,b3,4b,cc,f7,44,da,3a,75,65,93,26,b6,f4,00,00,0
0,00,00,00,f1,dc,24,41,cc,b2,02,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,
00,00,00,00,00,00,00,00,00,00,35,35,32,30,30,00,00,00,00,00,00,00,94,10,00,00
,9b,8d,b1,6c,80,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,0
0,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,c8,7b,fc,7c
"LicenseInfo"=hex(3):34,54,ae,dc,c7,2e,3d,e5,8b,15,06,1a,8c,74,a6,55,8c,9b,49
,a9,3f,24,2b,04,44,ef,79,88,c1,32,38,cf,52,0c,d7,57,da,9b,35,aa,d9,44,b3,64,b
9,21,6d,76,74,56,d2,4e,91,6e,7f,ac

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ 
```


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to...
My Computer
Win2008-DC
kali-linux-2025
Windows 10 x
Ubuntu 64-bit
Sift
FlareVM
Home
kali-linux-2025.2-vmware-...
5:56
Unix Hex Timestamp Con
https://www.epochconverter.com/hex?q=41252e3b
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Giảm Đến 20% Vitamin Mẹ & Bé
Vitamin bầu Pregnacare, bổ máu Feroglobin bổ sung suốt thai kỳ giảm đến 20% tại Long Châu
Nhà Thuốc Long Châu
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Những ngày mư...
22°C
Search
5:56 PM
11/5/2025

Convert Unix hexadecimal timestamp to human-readable date

This tool converts your hex timestamp/epoch to a normal date. It will also show the decimal Unix timestamp.
Click here if you want to convert normal (decimal) timestamps.

The current Unix hex timestamp is 690B2D43

Enter your hexadecimal timestamp below:

41252e3b [Convert hex timestamp to human date]

GMT: Thursday, August 19, 2004 10:48:27 PM
Your time zone: Thursday, August 19, 2004 6:48:27 PM GMT-04:00
Decimal timestamp/epoch: 1092955707

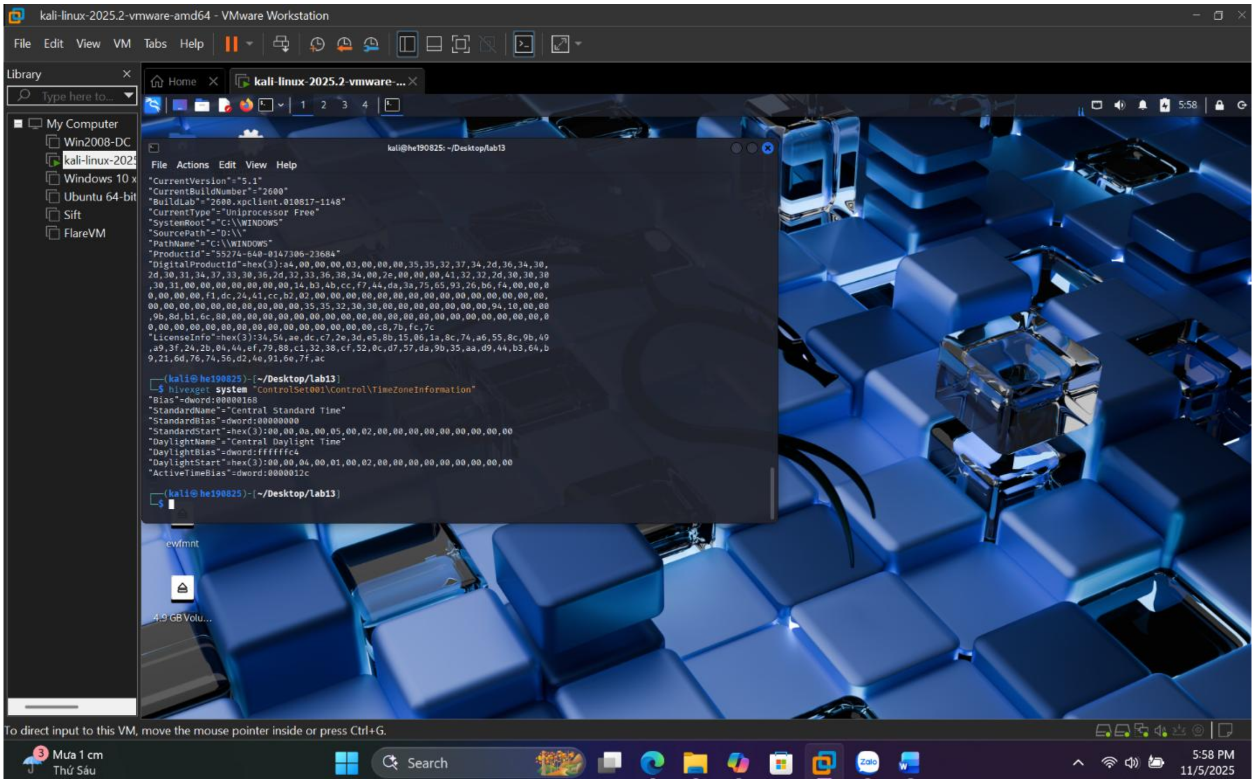
Pages

Home
Preferences
Toggle theme

Tools

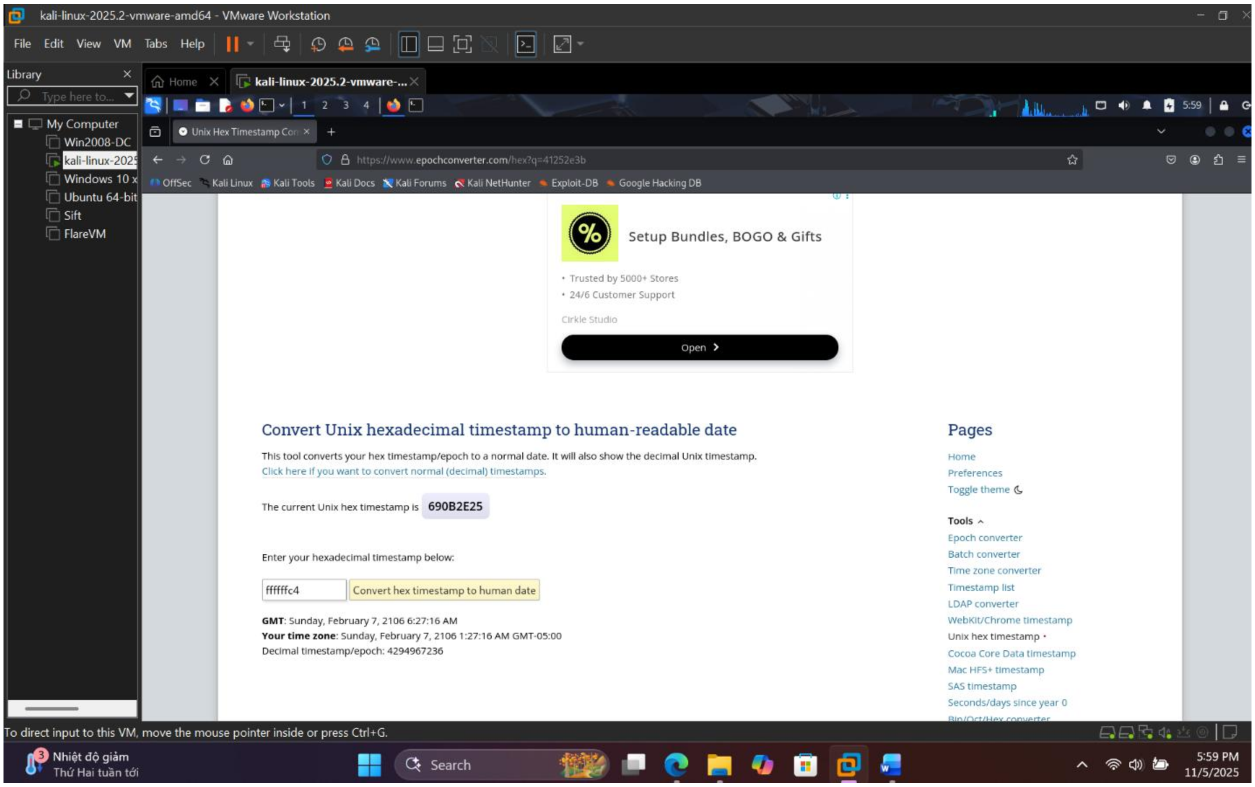
Epoch converter
Batch converter
Time zone converter
Timestamp list
LDAP converter
WebKit/Chrome timestamp
Unix hex timestamp •
Cocoa Core Data timestamp
Mac HFS+ timestamp
SAS timestamp
Seconds/days since year 0
Bin/Oct/Hex converter
Countdown in seconds
Epoch clock

4. What is the timezone settings?



kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Win2008-DC
kali-linux-2025
Windows 10 x
Ubuntu 64-bit
Sift
FlareVM
Home
kali-linux-2025.2-vmware-...
kali@he190825: ~/Desktop/lab13
File Actions Edit View Help
ewfmnt
4.9 GB Volu...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Mưa 1 cm
Thứ Sáu
Search
5:58 PM
11/5/2025

```
"CurrentVersion"="5.1"
"CurrentBuildNumber"="2600"
"BuildLab"="2600.xpclient.010817-1148"
"CurrentType"="Uniprocessor Free"
"SystemRoot"="C:\\WINDOWS"
"SourcePath"="D:\\"
"PathName"="C:\\WINDOWS"
"ProductId"="55274-640-0147306-23684"
"DigitalProductId"=hex(3):a4,00,00,00,03,00,00,00,35,35,32,37,34,2d,36,34,30,
2d,30,31,34,37,33,30,36,2d,32,33,36,38,34,00,2e,00,00,00,41,32,32,2d,30,30,30
,30,31,00,00,00,00,00,00,00,14,b3,4b,cc,f7,44,da,3a,75,65,93,26,b6,f4,00,00,0
0,00,00,00,f1,dc,24,41,cc,b2,02,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,
00,00,00,00,00,00,00,00,00,00,35,35,32,30,30,00,00,00,00,00,00,00,94,10,00,00
,9b,8d,b1,6c,80,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,0
0,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,c8,7b,fc,7c
"LicenseInfo"=hex(3):34,54,ae,dc,c7,2e,3d,e5,8b,15,06,1a,8c,74,a6,55,8c,9b,49
,a9,3f,24,2b,04,44,ef,79,88,c1,32,38,cf,52,0c,d7,57,da,9b,35,aa,d9,44,b3,64,b
9,21,6d,76,74,56,d2,4e,91,6e,7f,ac

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ hivexget system "ControlSet001\Control\TimeZoneInformation"
"Bias"=dword:00000168
"StandardName"="Central Standard Time"
"StandardBias"=dword:00000000
"StandardStart"=hex(3):00,00,0a,00,05,00,02,00,00,00,00,00,00,00,00,00
"DaylightName"="Central Daylight Time"
"DaylightBias"=dword:ffffffc4
"DaylightStart"=hex(3):00,00,04,00,01,00,02,00,00,00,00,00,00,00,00,00
"ActiveTimeBias"=dword:0000012c

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ 
```



Convert Unix hexadecimal timestamp to human-readable date

This tool converts your hex timestamp/epoch to a normal date. It will also show the decimal Unix timestamp.
Click here if you want to convert normal (decimal) timestamps.

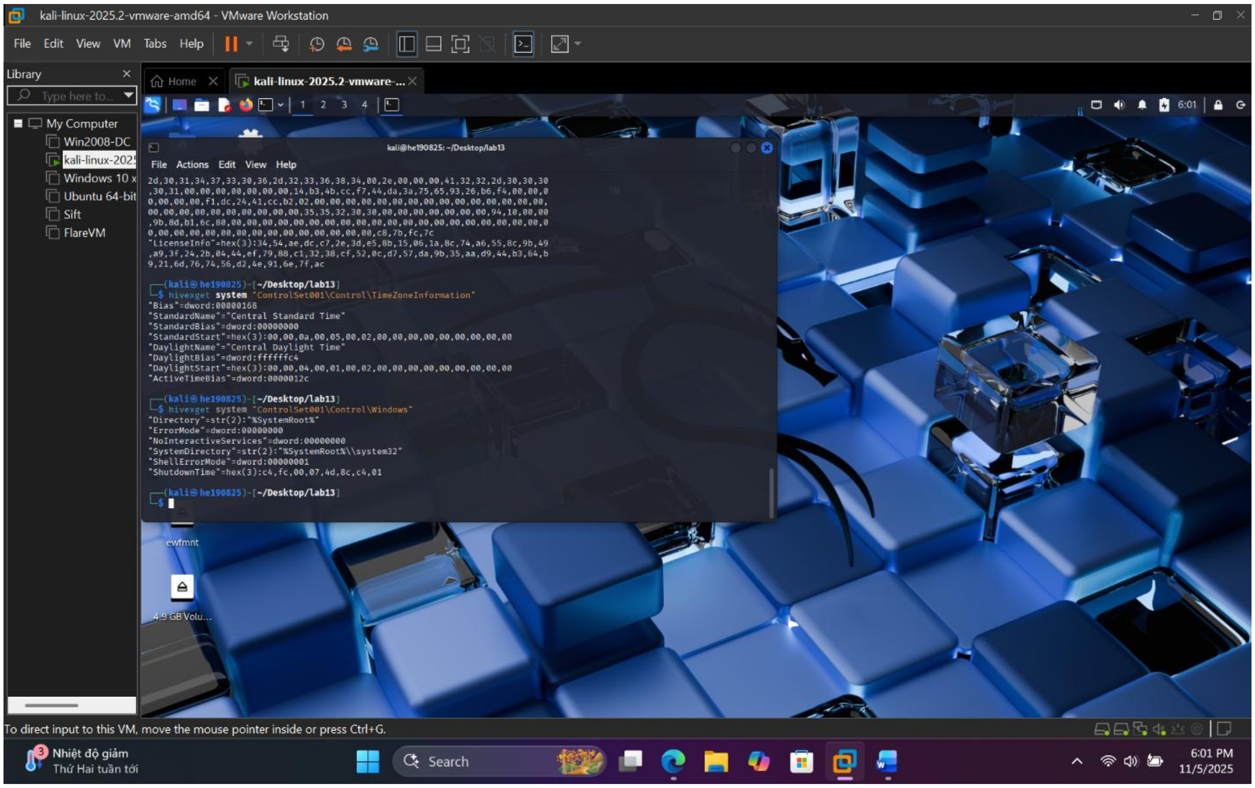
The current Unix hex timestamp is 690B2E25

Enter your hexadecimal timestamp below:

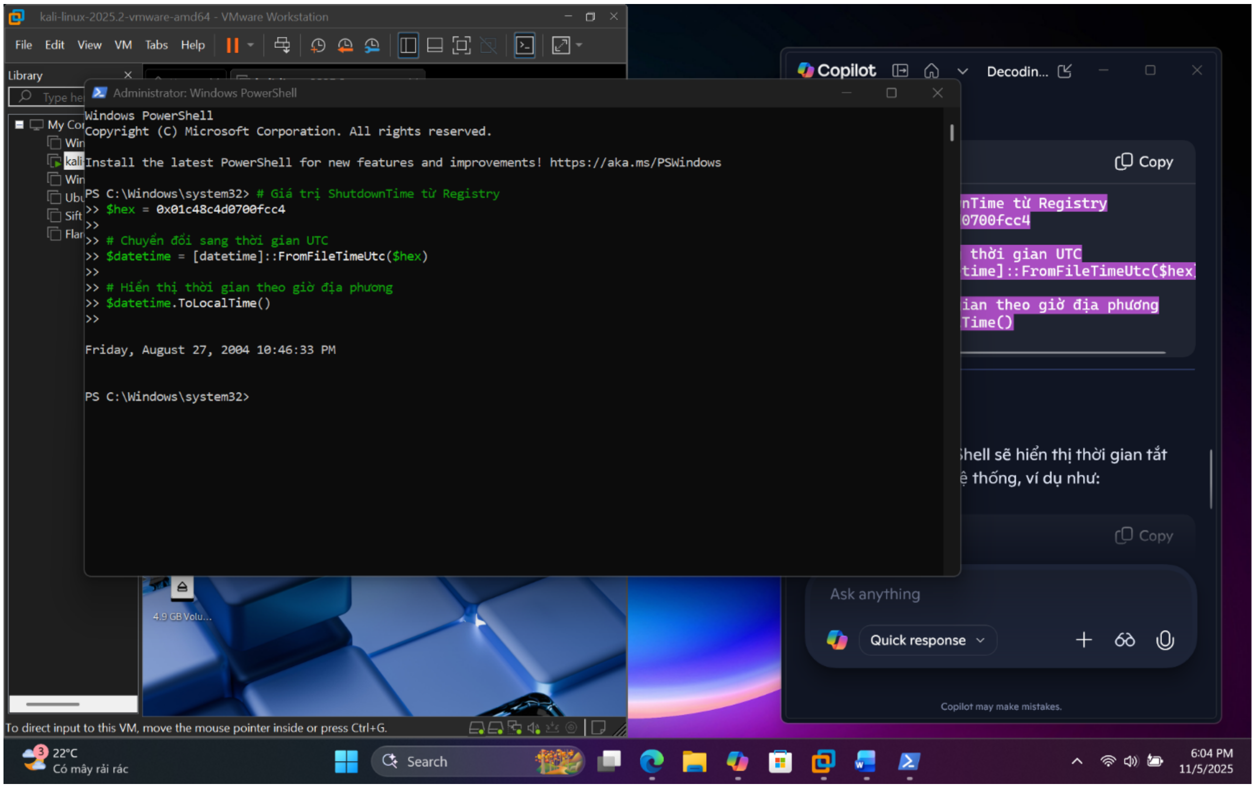
ffffffc4 Convert hex timestamp to human date

GMT: Sunday, February 7, 2106 6:27:16 AM
Your time zone: Sunday, February 7, 2106 1:27:16 AM GMT-05:00
Decimal timestamp/epoch: 4294967236

8. When was the last recorded computer shutdown date/time?


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Win2008-DC
kali-linux-2025
Windows 10 x
Ubuntu 64-bit
Sift
FlareVM
Home
kali-linux-2025.2-vmware-...
kali@he190825: ~/Desktop/lab13
File Actions Edit View Help
ewfmnt
4.9 GB Volu...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Nhiệt độ giảm
Thứ Hai tuần tới
Search
6:01 PM
11/5/2025

```
2d,30,31,34,37,33,30,36,2d,32,33,36,38,34,00,2e,00,00,00,41,32,32,2d,30,30,30
,30,31,00,00,00,00,00,00,00,14,b3,4b,cc,f7,44,da,3a,75,65,93,26,b6,f4,00,00,0
0,00,00,00,f1,dc,24,41,cc,b2,02,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,
00,00,00,00,00,00,00,00,00,00,35,35,32,30,30,00,00,00,00,00,00,00,94,10,00,00
,9b,8d,b1,6c,80,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,0
0,00,00,00,00,00,00,00,00,00,00,00,00,00,00,c8,7b,fc,7c
"LicenseInfo"=hex(3):34,54,ae,dc,c7,2e,3d,e5,8b,15,06,1a,8c,74,a6,55,8c,9b,49
,a9,3f,24,2b,04,44,ef,79,88,c1,32,38,cf,52,0c,d7,57,da,9b,35,aa,d9,44,b3,64,b
9,21,6d,76,74,56,d2,4e,91,6e,7f,ac

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ hivexget system "ControlSet001\Control\TimeZoneInformation"
"Bias"=dword:00000168
"StandardName"="Central Standard Time"
"StandardBias"=dword:00000000
"StandardStart"=hex(3):00,00,0a,00,05,00,02,00,00,00,00,00,00,00,00,00
"DaylightName"="Central Daylight Time"
"DaylightBias"=dword:ffffffc4
"DaylightStart"=hex(3):00,00,04,00,01,00,02,00,00,00,00,00,00,00,00,00
"ActiveTimeBias"=dword:0000012c

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ hivexget system "ControlSet001\Control\Windows"
"Directory"=str(2):"%SystemRoot%"
"ErrorMode"=dword:00000000
"NoInteractiveServices"=dword:00000000
"SystemDirectory"=str(2):"%SystemRoot%\\system32"
"ShellErrorMode"=dword:00000001
"ShutdownTime"=hex(3):c4,fc,00,07,4d,8c,c4,01

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ 
```

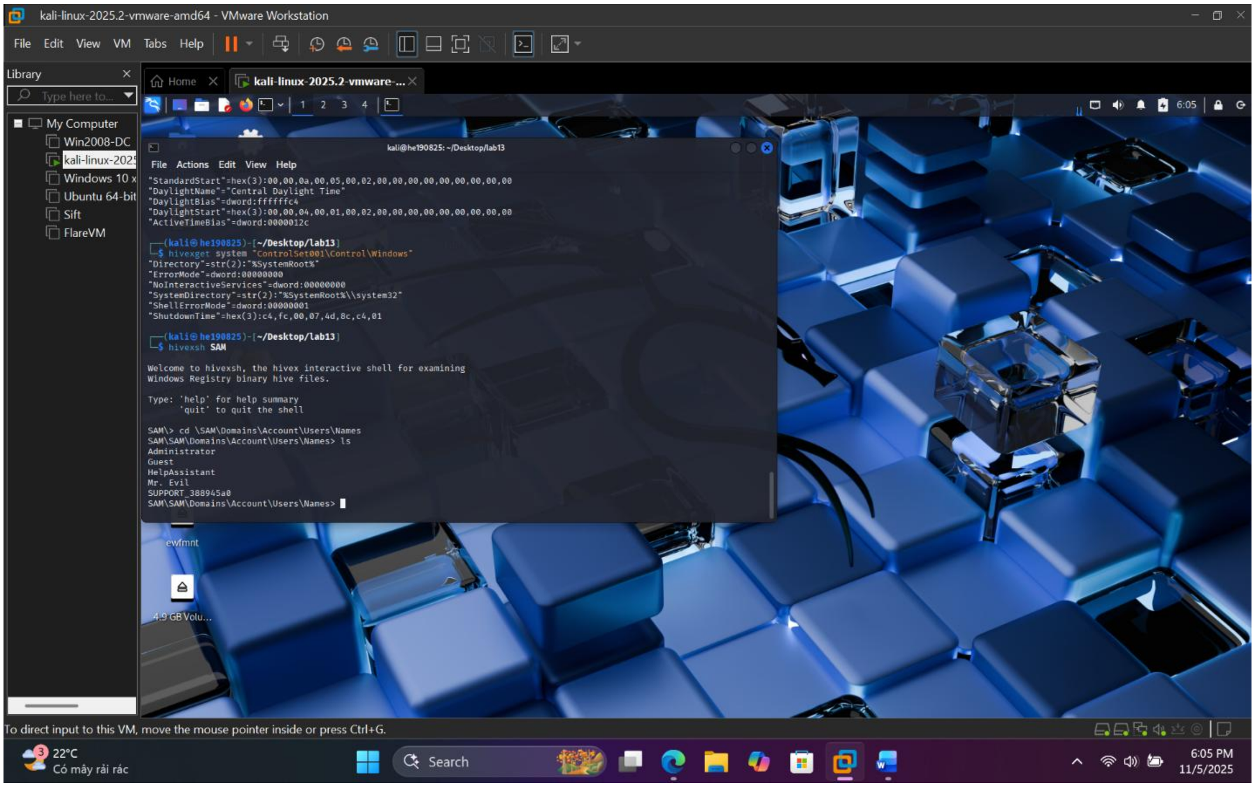

kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Administrator: Windows PowerShell
Copilot
Decodin...
Copy
Copy
Ask anything
Quick response
Copilot may make mistakes.
4.9 GB Volu...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
22°C
Có mây rải rác
Search
6:04 PM
11/5/2025

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> # Giá trị ShutdownTime từ Registry
>> $hex = 0x01c48c4d0700fcc4
>>
>> # Chuyển đổi sang thời gian UTC
>> $datetime = [datetime]::FromFileTimeUtc($hex)
>>
>> # Hiển thị thời gian theo giờ địa phương
>> $datetime.ToLocalTime()
>>

Friday, August 27, 2004 10:46:33 PM


PS C:\Windows\system32>
```

```
nTime từ Registry
0700fcc4

 thời gian UTC
time]::FromFileTimeUtc($hex

ian theo giờ địa phương
Time()
```

hell sẽ hiển thị thời gian tắt
ệ thống, ví dụ như:

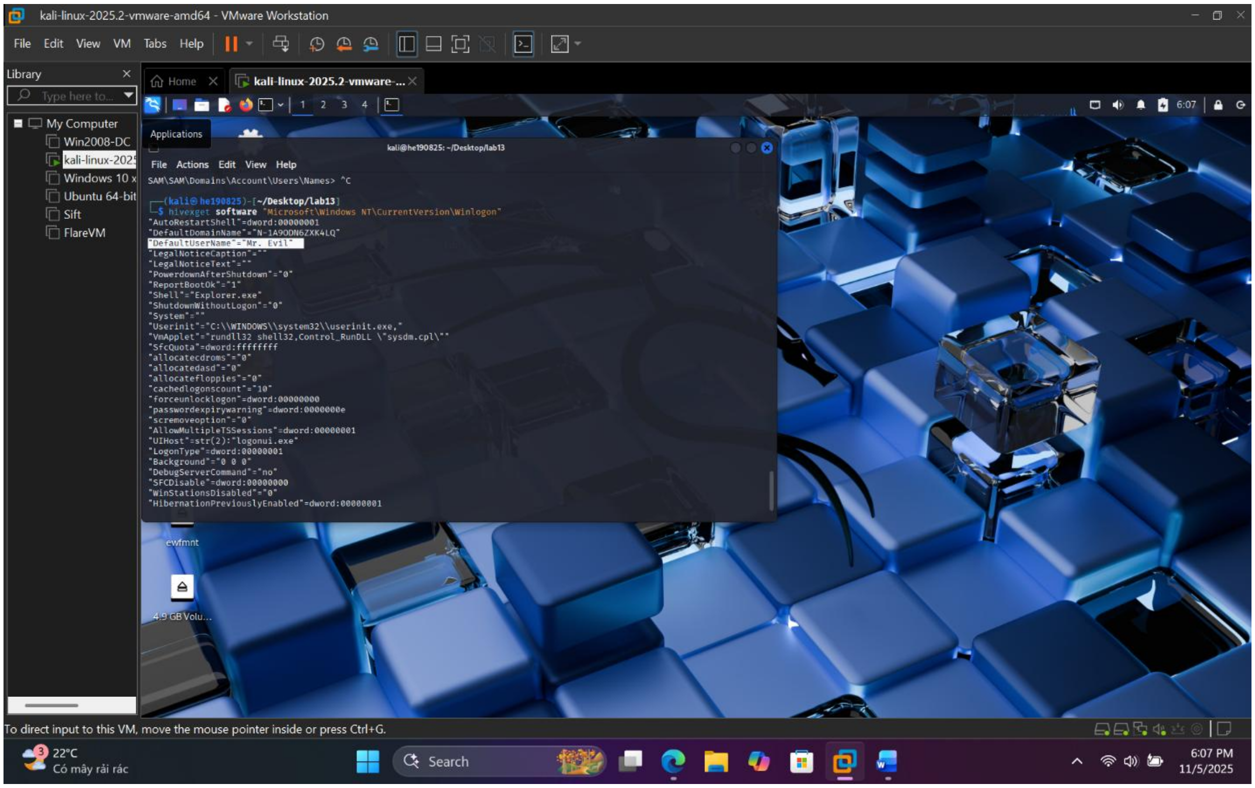
9. How many accounts are recorded (total number)?



kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Win2008-DC
kali-linux-2025
Windows 10 x
Ubuntu 64-bit
Sift
FlareVM
Home
kali-linux-2025.2-vmware-...
kali@he190825: ~/Desktop/lab13
File Actions Edit View Help
ewfmnt
4.9 GB Volu...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
22°C
Có mây rải rác
Search
6:05 PM
11/5/2025

```
"StandardStart"=hex(3):00,00,0a,00,05,00,02,00,00,00,00,00,00,00,00,00
"DaylightName"="Central Daylight Time"
"DaylightBias"=dword:ffffffc4
"DaylightStart"=hex(3):00,00,04,00,01,00,02,00,00,00,00,00,00,00,00,00
"ActiveTimeBias"=dword:0000012c

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ hivexget system "ControlSet001\Control\Windows"
"Directory"=str(2):"%SystemRoot%"
"ErrorMode"=dword:00000000
"NoInteractiveServices"=dword:00000000
"SystemDirectory"=str(2):"%SystemRoot%\\system32"
"ShellErrorMode"=dword:00000001
"ShutdownTime"=hex(3):c4,fc,00,07,4d,8c,c4,01

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ hivexsh SAM

Welcome to hivexsh, the hivex interactive shell for examining
Windows Registry binary hive files.

Type: 'help' for help summary
      'quit' to quit the shell

SAM\> cd \SAM\Domains\Account\Users\Names
SAM\SAM\Domains\Account\Users\Names> ls
Administrator
Guest
HelpAssistant
Mr. Evil
SUPPORT_388945a0
SAM\SAM\Domains\Account\Users\Names>
```

11. Who was the last user to logon to the computer?

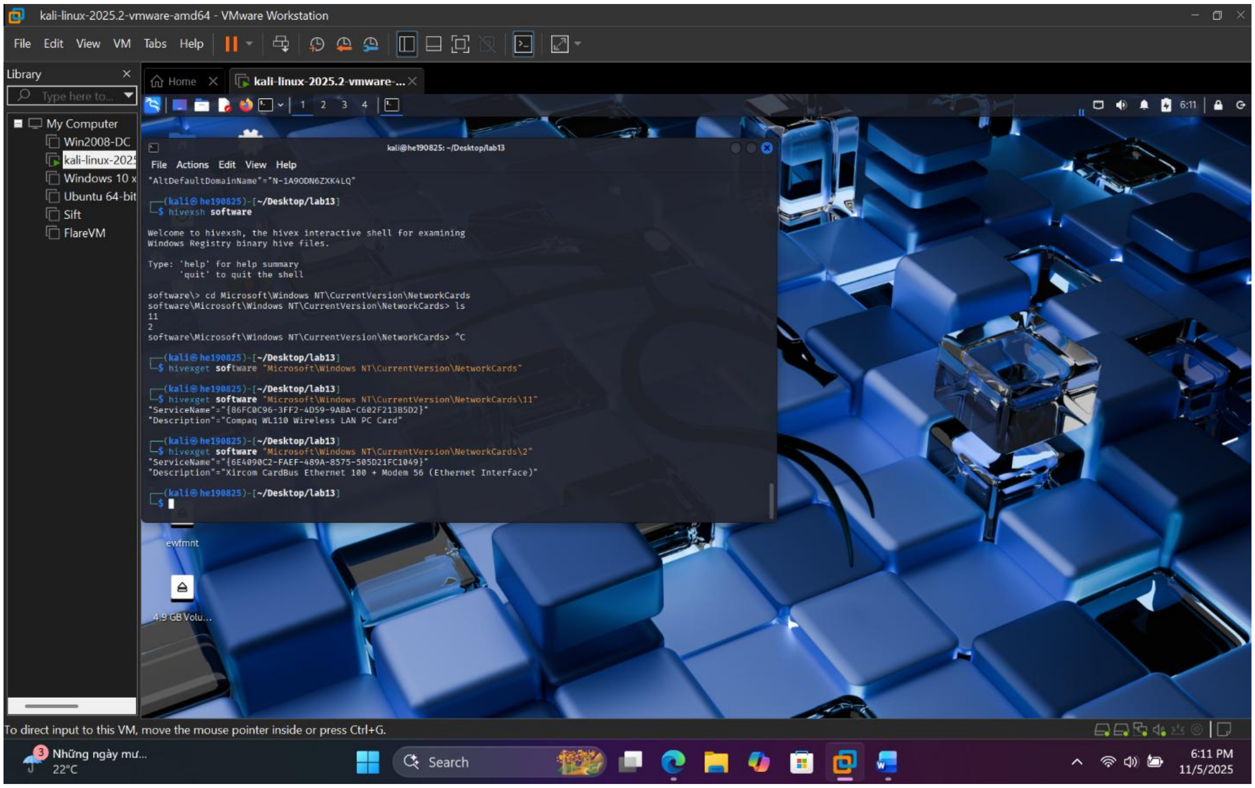


```
SAM\SAM\Domains\Account\Users\Names> ^C

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ hivexget software "Microsoft\Windows NT\CurrentVersion\Winlogon"
"AutoRestartShell"=dword:00000001
"DefaultDomainName"="N-1A9ODN6ZXK4LQ"
"DefaultUserName"="Mr. Evil"
"LegalNoticeCaption"=""
"LegalNoticeText"=""
"PowerdownAfterShutdown"="0"
"ReportBootOk"="1"
"Shell"="Explorer.exe"
"ShutdownWithoutLogon"="0"
"System"=""
"Userinit"="C:\\WINDOWS\\system32\\userinit.exe,"
"VmApplet"="rundll32 shell32,Control_RunDLL \"sysdm.cpl\""
"SfcQuota"=dword:ffffffff
"allocatecdroms"="0"
"allocatedasd"="0"
"allocatefloppies"="0"
"cachedlogonscount"="10"
"forceunlocklogon"=dword:00000000
"passwordexpirywarning"=dword:0000000e
"scremoveoption"="0"
"AllowMultipleTSSessions"=dword:00000001
"UIHost"=str(2):"logonui.exe"
"LogonType"=dword:00000001
"Background"="0 0 0"
"DebugServerCommand"="no"
"SFCDisable"=dword:00000000
"WinStationsDisabled"="0"
"HibernationPreviouslyEnabled"=dword:00000001
```

kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Win2008-DC
kali-linux-2025
Windows 10 x
Ubuntu 64-bit
Sift
FlareVM
Home
kali-linux-2025.2-vmware-...
Applications
kali@he190825: ~/Desktop/lab13
File Actions Edit View Help
ewfmnt
4.9 GB Volu...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
22°C
Có mây rải rác
Search
6:07 PM
11/5/2025

13. List the network cards used by this computer. This same file reports the IP address and

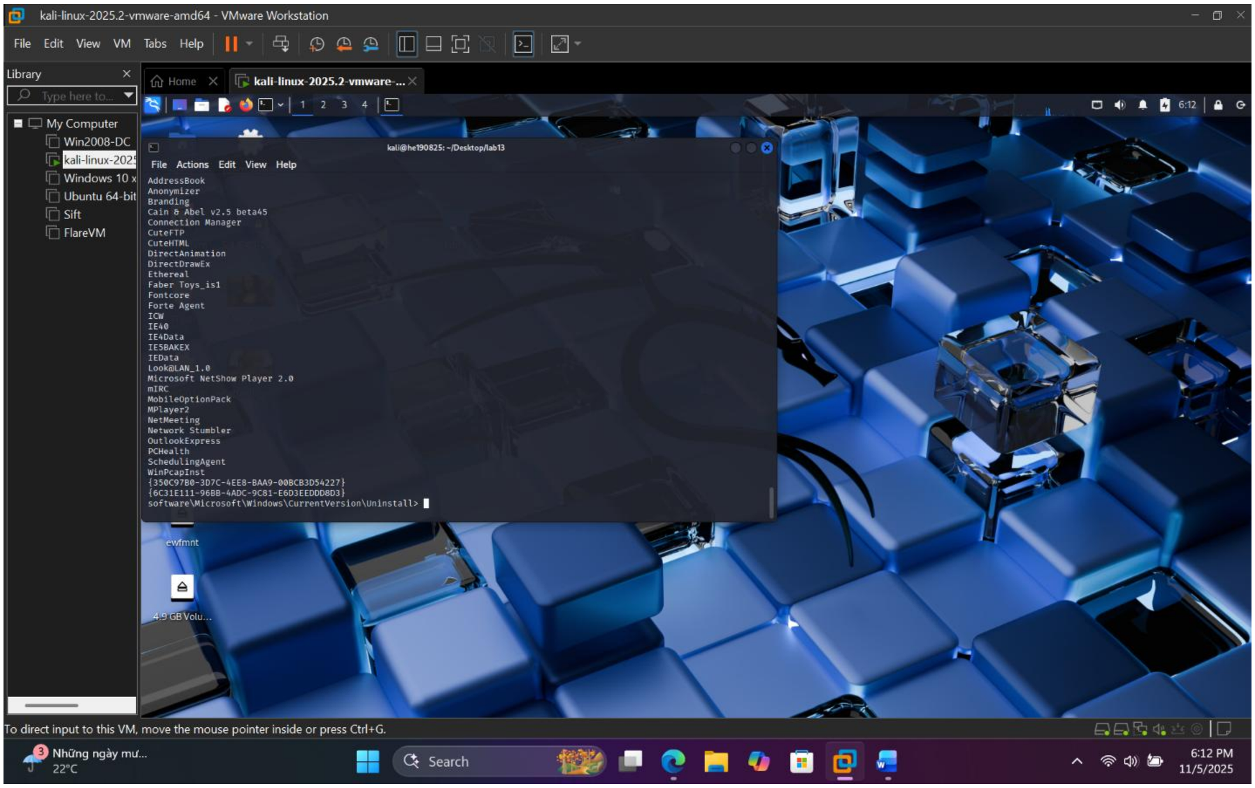
MAC address of the computer. What are they?



kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Win2008-DC
kali-linux-2025
Windows 10 x
Ubuntu 64-bit
Sift
FlareVM
Home
kali-linux-2025.2-vmware-...
kali@he190825: ~/Desktop/lab13
File Actions Edit View Help
ewfmnt
4.9 GB Volu...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Những ngày mư...
22°C
Search
6:11 PM
11/5/2025

```
"AltDefaultDomainName"="N-1A9ODN6ZXK4LQ"

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ hivexsh software

Welcome to hivexsh, the hivex interactive shell for examining
Windows Registry binary hive files.

Type: 'help' for help summary
      'quit' to quit the shell

software\> cd Microsoft\Windows NT\CurrentVersion\NetworkCards
software\Microsoft\Windows NT\CurrentVersion\NetworkCards> ls
11
2
software\Microsoft\Windows NT\CurrentVersion\NetworkCards> ^C

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ hivexget software "Microsoft\Windows NT\CurrentVersion\NetworkCards"

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ hivexget software "Microsoft\Windows NT\CurrentVersion\NetworkCards\11"
"ServiceName"="{86FC0C96-3FF2-4D59-9ABA-C602F213B5D2}"
"Description"="Compaq WL110 Wireless LAN PC Card"

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ hivexget software "Microsoft\Windows NT\CurrentVersion\NetworkCards\2"
"ServiceName"="{6E4090C2-FAEF-489A-8575-505D21FC1049}"
"Description"="Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)"

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ 
```

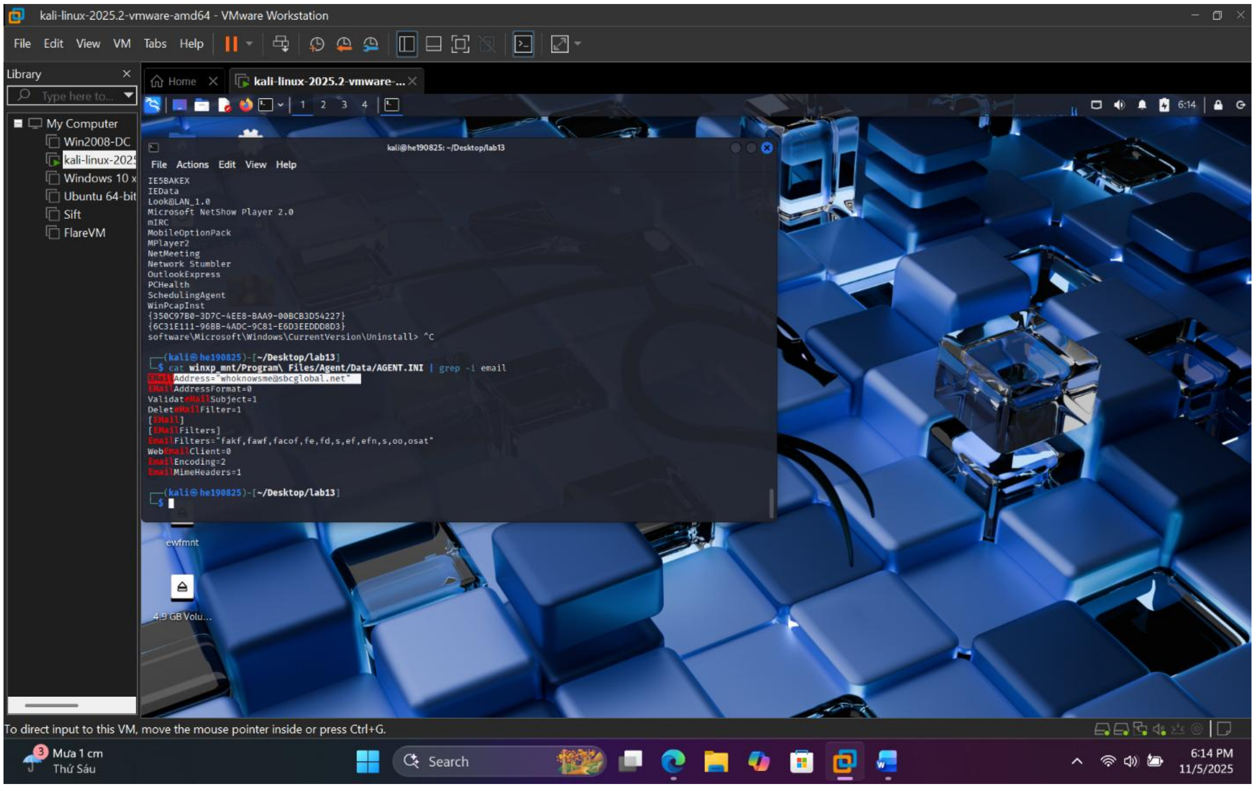
16. Find 6 installed programs that may be used for hacking.



kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Win2008-DC
kali-linux-2025
Windows 10 x
Ubuntu 64-bit
Sift
FlareVM
Home
kali-linux-2025.2-vmware-...
kali@he190825: ~/Desktop/lab13
File Actions Edit View Help
ewfmnt
4.9 GB Volu...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Những ngày mư...
22°C
Search
6:12 PM
11/5/2025

```
AddressBook
Anonymizer
Branding
Cain & Abel v2.5 beta45
Connection Manager
CuteFTP
CuteHTML
DirectAnimation
DirectDrawEx
Ethereal
Faber Toys_is1
Fontcore
Forte Agent
ICW
IE40
IE4Data
IE5BAKEX
IEData
Look@LAN_1.0
Microsoft NetShow Player 2.0
mIRC
MobileOptionPack
MPlayer2
NetMeeting
Network Stumbler
OutlookExpress
PCHealth
SchedulingAgent
WinPcapInst
{350C97B0-3D7C-4EE8-BAA9-00BCB3D54227}
{6C31E111-96BB-4ADC-9C81-E6D3EEDDD8D3}
software\Microsoft\Windows\CurrentVersion\Uninstall> 
```

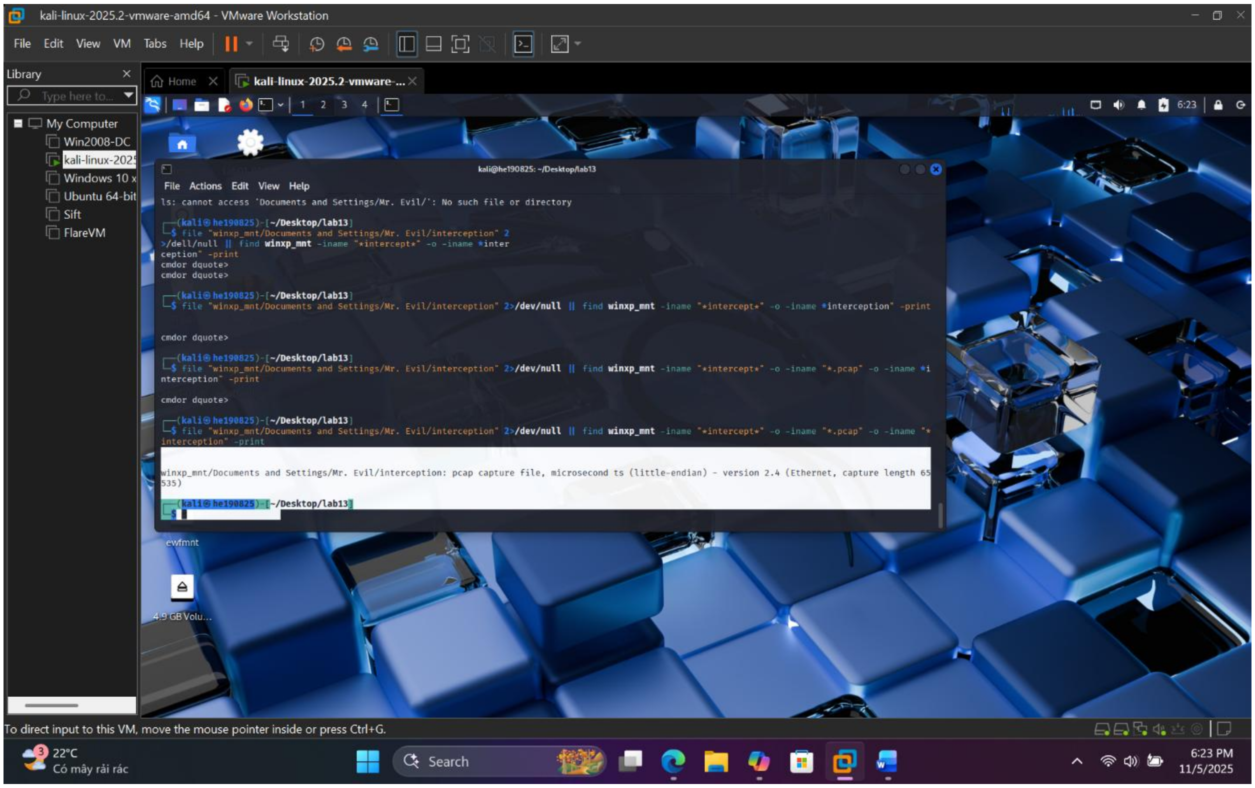
17. What is the SMTP email address for Mr. Evil?


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Win2008-DC
kali-linux-2025
Windows 10 x
Ubuntu 64-bit
Sift
FlareVM
Home
kali-linux-2025.2-vmware-...
kali@he190825: ~/Desktop/lab13
File Actions Edit View Help
ewfmnt
4.9 GB Volu...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Mưa 1 cm
Thứ Sáu
Search
6:14 PM
11/5/2025

```
IE5BAKEX
IEData
Look@LAN_1.0
Microsoft NetShow Player 2.0
mIRC
MobileOptionPack
MPlayer2
NetMeeting
Network Stumbler
OutlookExpress
PCHealth
SchedulingAgent
WinPcapInst
{350C97B0-3D7C-4EE8-BAA9-00BCB3D54227}
{6C31E111-96BB-4ADC-9C81-E6D3EEDDD8D3}
software\Microsoft\Windows\CurrentVersion\Uninstall> ^C

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ cat winxp_mnt/Program\ Files/Agent/Data/AGENT.INI | grep -i email
EMailAddress="whoknowsme@sbcglobal.net"
EMailAddressFormat=0
ValidateMailSubject=1
DeleteMailFilter=1
[EMail]
[EMailFilters]
EmailFilters="fakf,fawf,facof,fe,fd,s,ef,efn,s,oo,osat"
WebEmailClient=0
EmailEncoding=2
EmailMimeHeaders=1

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ 
```

23. Ethereal, a popular “sniffing” program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and re-assembled, the default save directory is that users \My Documents directory. What is the

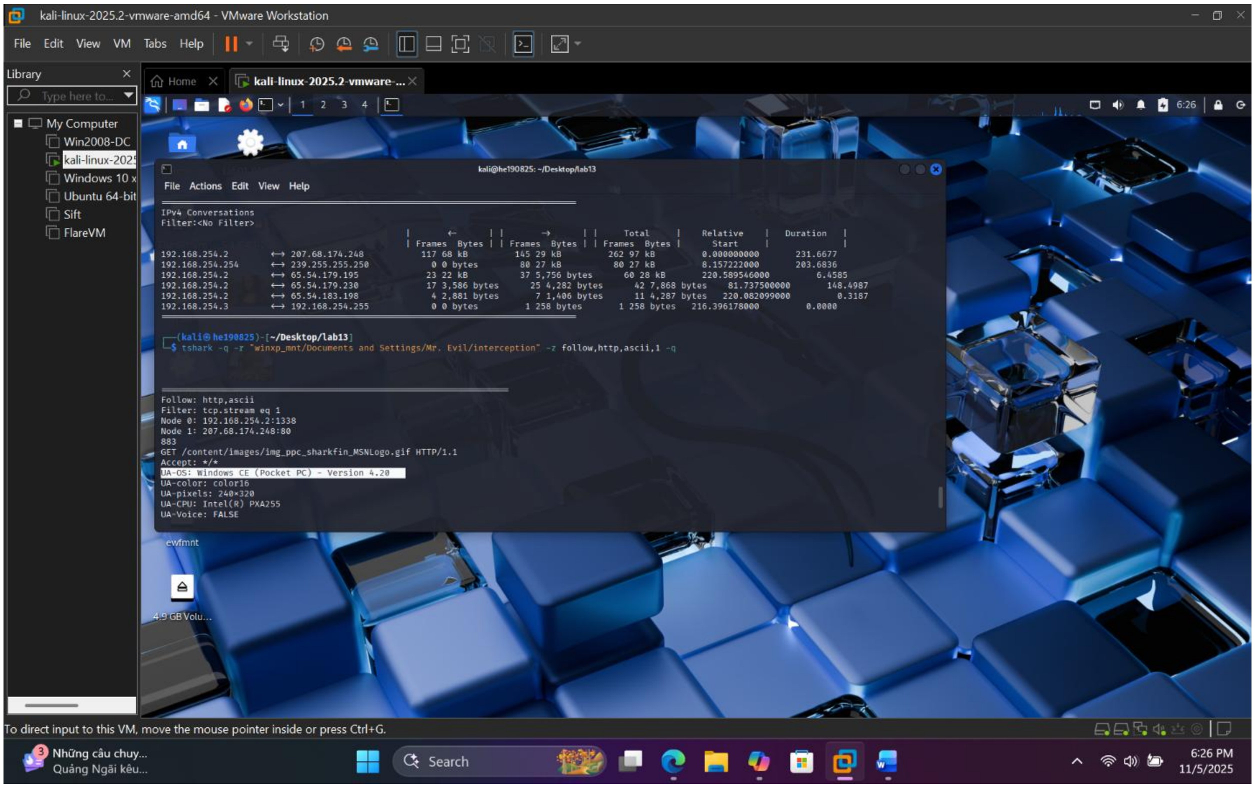
name of the file that contains the intercepted data?


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Win2008-DC
kali-linux-2025
Windows 10 x
Ubuntu 64-bit
Sift
FlareVM
Home
kali-linux-2025.2-vmware-...
kali@he190825: ~/Desktop/lab13
File Actions Edit View Help
ewfmnt
4.9 GB Volu...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
22°C
Có mây rải rác
Search
6:23 PM
11/5/2025

```
ls: cannot access 'Documents and Settings/Mr. Evil/': No such file or directory

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ file "winxp_mnt/Documents and Settings/Mr. Evil/interception" 2
>/dell/null || find winxp_mnt -iname "*intercept*" -o -iname *inter
ception" -print
cmdor dquote>
cmdor dquote>

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ file "winxp_mnt/Documents and Settings/Mr. Evil/interception" 2>/dev/null || find winxp_mnt -iname "*intercept*" -o -iname *interception" -print


cmdor dquote>

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ file "winxp_mnt/Documents and Settings/Mr. Evil/interception" 2>/dev/null || find winxp_mnt -iname "*intercept*" -o -iname "*.pcap" -o -iname *i
nterception" -print

cmdor dquote>

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ file "winxp_mnt/Documents and Settings/Mr. Evil/interception" 2>/dev/null || find winxp_mnt -iname "*intercept*" -o -iname "*.pcap" -o -iname "*
interception" -print

winxp_mnt/Documents and Settings/Mr. Evil/interception: pcap capture file, microsecond ts (little-endian) - version 2.4 (Ethernet, capture length 65
535)

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$
```

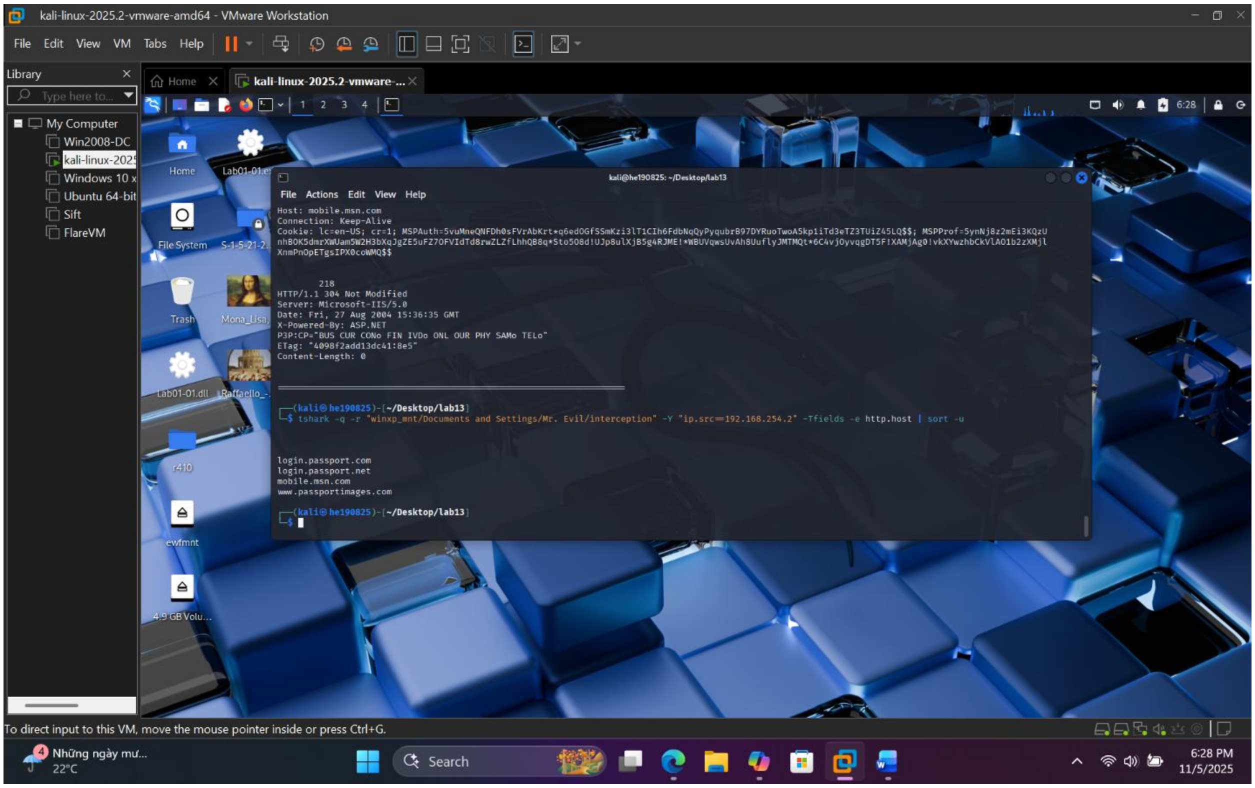
24. Viewing the file in a text format reveals much information about who and what was intercepted. What type of wireless computer was the victim (person who had his internet

surfing recorded) using?



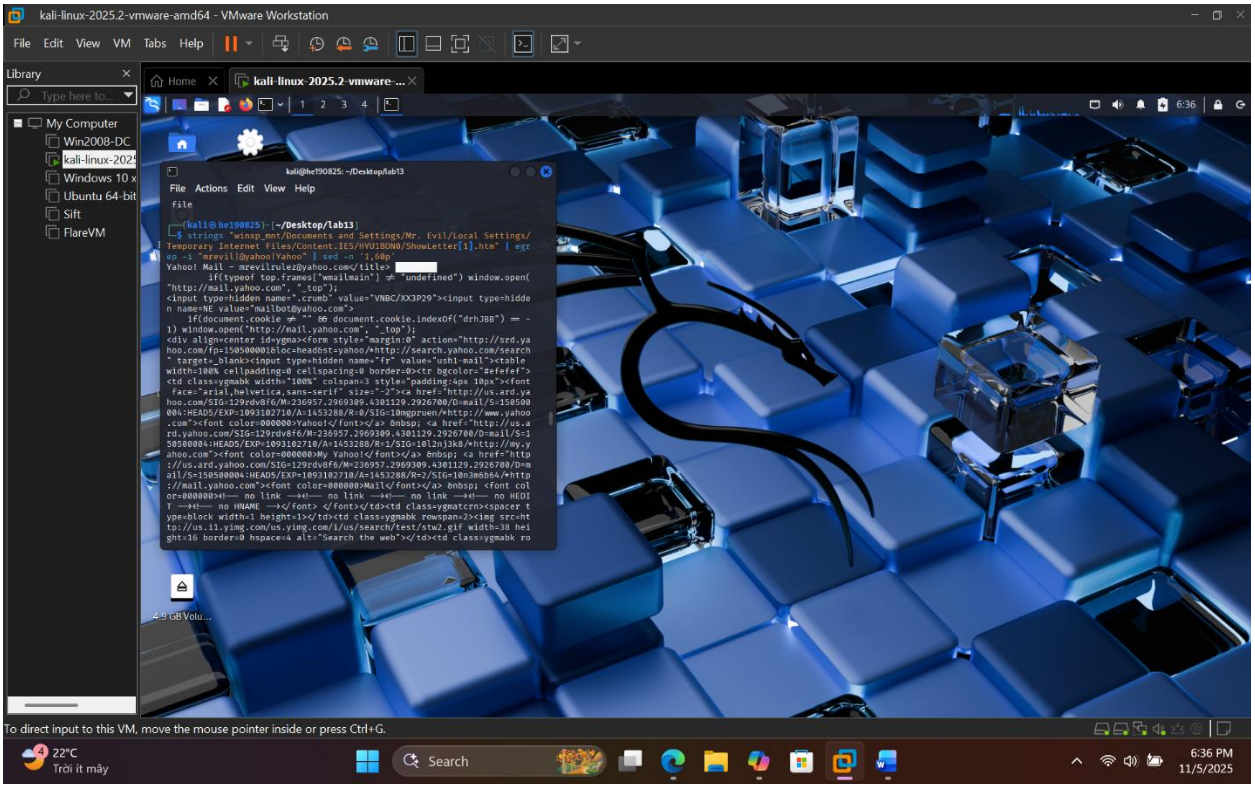
```
kali@he190825: ~/Desktop/lab13

IPv4 Conversations
Filter:<No Filter>
                                                   |       ←      | |       →      | |     Total    |    Relative    |   Duration   |
                                                   | Frames  Bytes | | Frames  Bytes | | Frames  Bytes |      Start     |              |
192.168.254.2         ⟷ 207.68.174.248            117 68 kB          145 29 kB          262 97 kB         0.000000000        231.6677
192.168.254.254       ⟷ 239.255.255.250             0 0 bytes         80 27 kB           80 27 kB         8.157222000        203.6836
192.168.254.2         ⟷ 65.54.179.195              23 22 kB           37 5,756 bytes     60 28 kB       220.589546000          6.4585
192.168.254.2         ⟷ 65.54.179.230              17 3,586 bytes     25 4,282 bytes     42 7,868 bytes    81.737500000        148.4987
192.168.254.2         ⟷ 65.54.183.198               4 2,881 bytes      7 1,406 bytes     11 4,287 bytes   220.082099000          0.3187
192.168.254.3         ⟷ 192.168.254.255             0 0 bytes          1 258 bytes        1 258 bytes   216.396178000         0.0000

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ tshark -q -r "winxp_mnt/Documents and Settings/Mr. Evil/interception" -z follow,http,ascii,1 -q


Follow: http,ascii
Filter: tcp.stream eq 1
Node 0: 192.168.254.2:1338
Node 1: 207.68.174.248:80
883
GET /content/images/img_ppc_sharkfin_MSNLogo.gif HTTP/1.1
Accept: */*
UA-OS: Windows CE (Pocket PC) - Version 4.20
UA-color: color16
UA-pixels: 240×320
UA-CPU: Intel(R) PXA255
UA-Voice: FALSE
```

25. What websites was the victim accessing?



```
kali@he190825: ~/Desktop/lab13

Host: mobile.msn.com
Connection: Keep-Alive
Cookie: lc=en-US; cr=1; MSPAuth=5vuMneQNFDh0sFVrAbKrt*q6edOGfSSmKzi3lT1CIh6FdbNqQyPyqubrB97DYRuoTwoA5kp1iTd3eTZ3TUiZ45LQ$$; MSPProf=5ynNj8z2mEi3KQzU
nhBOK5dmrXWUam5W2H3bXqJgZE5uFZ7OFVIdTd8rwZLZfLhhQB8q*Sto5O8d!UJp8ulXjB5g4RJME!*WBUVqwsUvAh8UuflyJMTMQt*6C4vjOyvqgDT5F!XAMjAg0!vkXYwzhbCkVlAO1b2zXMjl
XnmPnOpETgsIPX0coWMQ$$


       218
HTTP/1.1 304 Not Modified
Server: Microsoft-IIS/5.0
Date: Fri, 27 Aug 2004 15:36:35 GMT
X-Powered-By: ASP.NET
P3P:CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"
ETag: "4098f2add13dc41:8e5"
Content-Length: 0


┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ tshark -q -r "winxp_mnt/Documents and Settings/Mr. Evil/interception" -Y "ip.src==192.168.254.2" -Tfields -e http.host | sort -u


login.passport.com
login.passport.net
mobile.msn.com
www.passportimages.com

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$
```

26. Search for the main users web based email address. What is it?

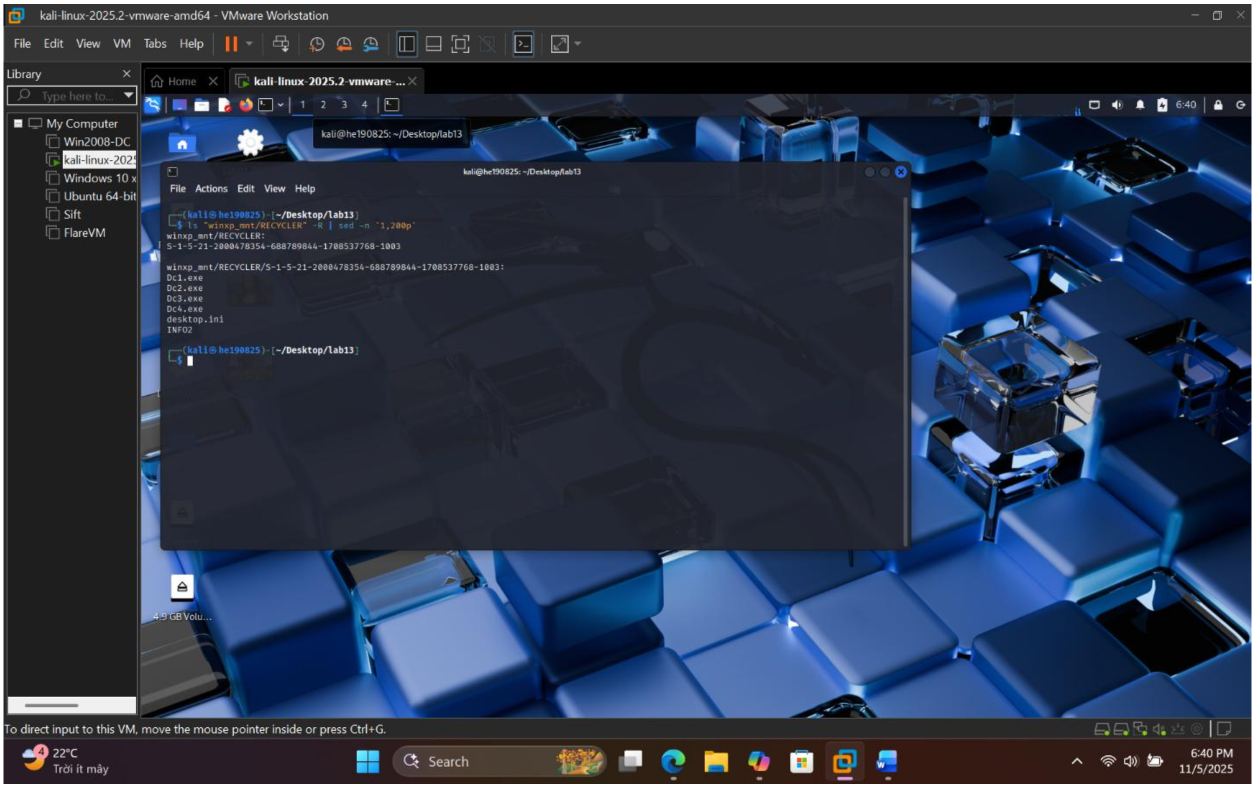


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to...
My Computer
Win2008-DC
kali-linux-2025
Windows 10 x
Ubuntu 64-bit
Sift
FlareVM
Home
kali-linux-2025.2-vmware-...
1 2 3 4
6:36
kali@he190825: ~/Desktop/lab13
File Actions Edit View Help
4.9 GB Volu...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
22°C
Trời ít mây
Search
6:36 PM
11/5/2025

```
 file

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ strings "winxp_mnt/Documents and Settings/Mr. Evil/Local Settings/
Temporary Internet Files/Content.IE5/HYU1BON0/ShowLetter[1].htm" | egr
ep -i "mrevil|@yahoo|Yahoo" | sed -n '1,60p'
Yahoo! Mail - mrevilrulez@yahoo.com</title>
        if(typeof top.frames["wmailmain"] != "undefined") window.open(
"http://mail.yahoo.com", "_top");
<input type=hidden name=".crumb" value="VNBC/XX3P29"><input type=hidde
n name=NE value="mailbot@yahoo.com">
    if(document.cookie != "" && document.cookie.indexOf("drhJBB") == -
1) window.open("http://mail.yahoo.com", "_top");
<div align=center id=ygma><form style="margin:0" action="http://srd.ya
hoo.com/fp=150500001&loc=head&st=yahoo/*http://search.yahoo.com/search
" target=_blank><input type=hidden name="fr" value="ush1-mail"><table
width=100% cellpadding=0 cellspacing=0 border=0><tr bgcolor="#efefef">
<td class=ygmabk width="100%" colspan=3 style="padding:4px 10px"><font
 face="arial,helvetica,sans-serif" size="-2"><a href="http://us.ard.ya
hoo.com/SIG=129rdv8f6/M=236957.2969309.4301129.2926700/D=mail/S=150500
004:HEAD5/EXP=1093102710/A=1453288/R=0/SIG=10mgpruen/*http://www.yahoo
.com"><font color=000000>Yahoo!</font></a> &nbsp; <a href="http://us.a
rd.yahoo.com/SIG=129rdv8f6/M=236957.2969309.4301129.2926700/D=mail/S=1
50500004:HEAD5/EXP=1093102710/A=1453288/R=1/SIG=10l2nj3k8/*http://my.y
ahoo.com"><font color=000000>My Yahoo!</font></a> &nbsp; <a href="http
://us.ard.yahoo.com/SIG=129rdv8f6/M=236957.2969309.4301129.2926700/D=m
ail/S=150500004:HEAD5/EXP=1093102710/A=1453288/R=2/SIG=10n3m6b64/*http
://mail.yahoo.com"><font color=000000>Mail</font></a> &nbsp; <font col
or=000000><!-- no link --><!-- no link --><!-- no link --><!-- no HEDI
T --><!-- no HNAME --></font> </font></td><td class=ygmatcrn><spacer t
ype=block width=1 height=1></td><td class=ygmabk rowspan=2><img src=ht
tp://us.i1.yimg.com/us.yimg.com/i/us/search/test/stw2.gif width=38 hei
ght=16 border=0 hspace=4 alt="Search the web"></td><td class=ygmabk ro
```

28. How many executable files are in the recycle bin?

4

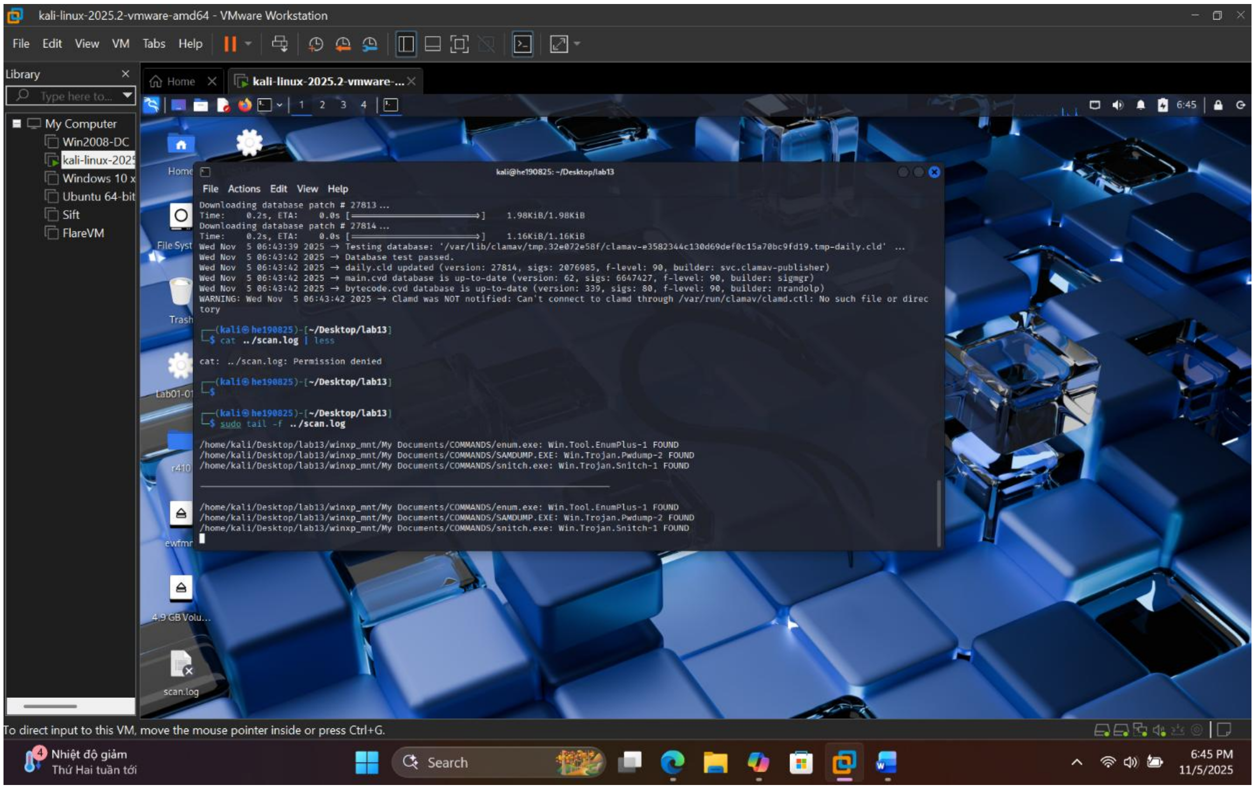


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Win2008-DC
kali-linux-2025
Windows 10 x
Ubuntu 64-bit
Sift
FlareVM
Home
kali-linux-2025.2-vmware-...
kali@he190825: ~/Desktop/lab13
File Actions Edit View Help
4.9 GB Volu...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
22°C
Trời ít mây
Search
6:40 PM
11/5/2025

```
┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ ls "winxp_mnt/RECYCLER" -R | sed -n '1,200p'
winxp_mnt/RECYCLER:
S-1-5-21-2000478354-688789844-1708537768-1003

winxp_mnt/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003:
Dc1.exe
Dc2.exe
Dc3.exe
Dc4.exe
desktop.ini
INFO2

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ 
```

31. Perform a Anti-Virus check. Are there any viruses on the computer?

-Có


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Win2008-DC
kali-linux-2025
Windows 10 x
Ubuntu 64-bit
Sift
FlareVM
Home
kali-linux-2025.2-vmware-...
kali@he190825: ~/Desktop/lab13
File Actions Edit View Help
Home
File Syst
Trash
Lab01-01
r410
ewfmr
4.9 GB Volu...
scan.log
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Nhiệt độ giảm
Thứ Hai tuần tới
Search
6:45 PM
11/5/2025

```
Downloading database patch # 27813 ...
Time:    0.2s, ETA:    0.0s [========================>]    1.98KiB/1.98KiB
Downloading database patch # 27814 ...
Time:    0.2s, ETA:    0.0s [========================>]    1.16KiB/1.16KiB
Wed Nov  5 06:43:39 2025 → Testing database: '/var/lib/clamav/tmp.32e072e58f/clamav-e3582344c130d69def0c15a70bc9fd19.tmp-daily.cld' ...
Wed Nov  5 06:43:42 2025 → Database test passed.
Wed Nov  5 06:43:42 2025 → daily.cld updated (version: 27814, sigs: 2076985, f-level: 90, builder: svc.clamav-publisher)
Wed Nov  5 06:43:42 2025 → main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
Wed Nov  5 06:43:42 2025 → bytecode.cvd database is up-to-date (version: 339, sigs: 80, f-level: 90, builder: nrandolp)
WARNING: Wed Nov  5 06:43:42 2025 → Clamd was NOT notified: Can't connect to clamd through /var/run/clamav/clamd.ctl: No such file or direc
tory

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ cat ../scan.log | less

cat: ../scan.log: Permission denied

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ 

┌──(kali㉿he190825)-[~/Desktop/lab13]
└─$ sudo tail -f ../scan.log

/home/kali/Desktop/lab13/winxp_mnt/My Documents/COMMANDS/enum.exe: Win.Tool.EnumPlus-1 FOUND
/home/kali/Desktop/lab13/winxp_mnt/My Documents/COMMANDS/SAMDUMP.EXE: Win.Trojan.Pwdump-2 FOUND
/home/kali/Desktop/lab13/winxp_mnt/My Documents/COMMANDS/snitch.exe: Win.Trojan.Snitch-1 FOUND

───────────────────────────────────────────────────────────────────────────


/home/kali/Desktop/lab13/winxp_mnt/My Documents/COMMANDS/enum.exe: Win.Tool.EnumPlus-1 FOUND
/home/kali/Desktop/lab13/winxp_mnt/My Documents/COMMANDS/SAMDUMP.EXE: Win.Trojan.Pwdump-2 FOUND
/home/kali/Desktop/lab13/winxp_mnt/My Documents/COMMANDS/snitch.exe: Win.Trojan.Snitch-1 FOUND
█
```