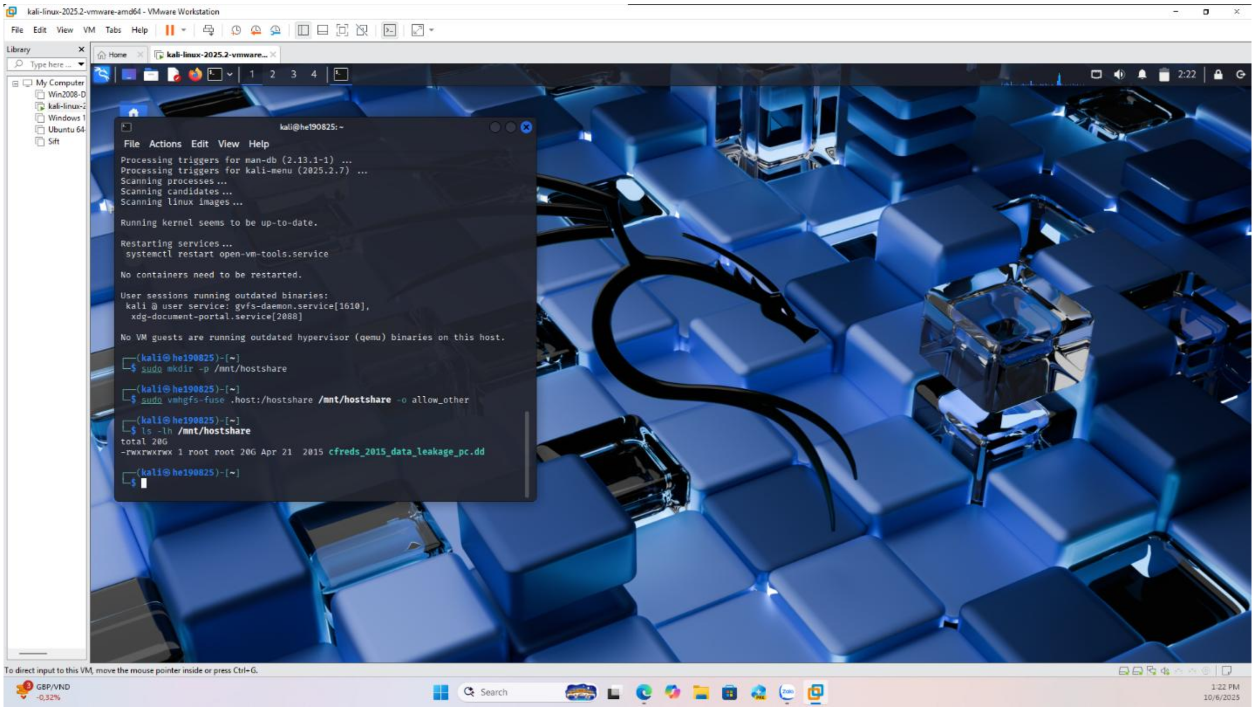
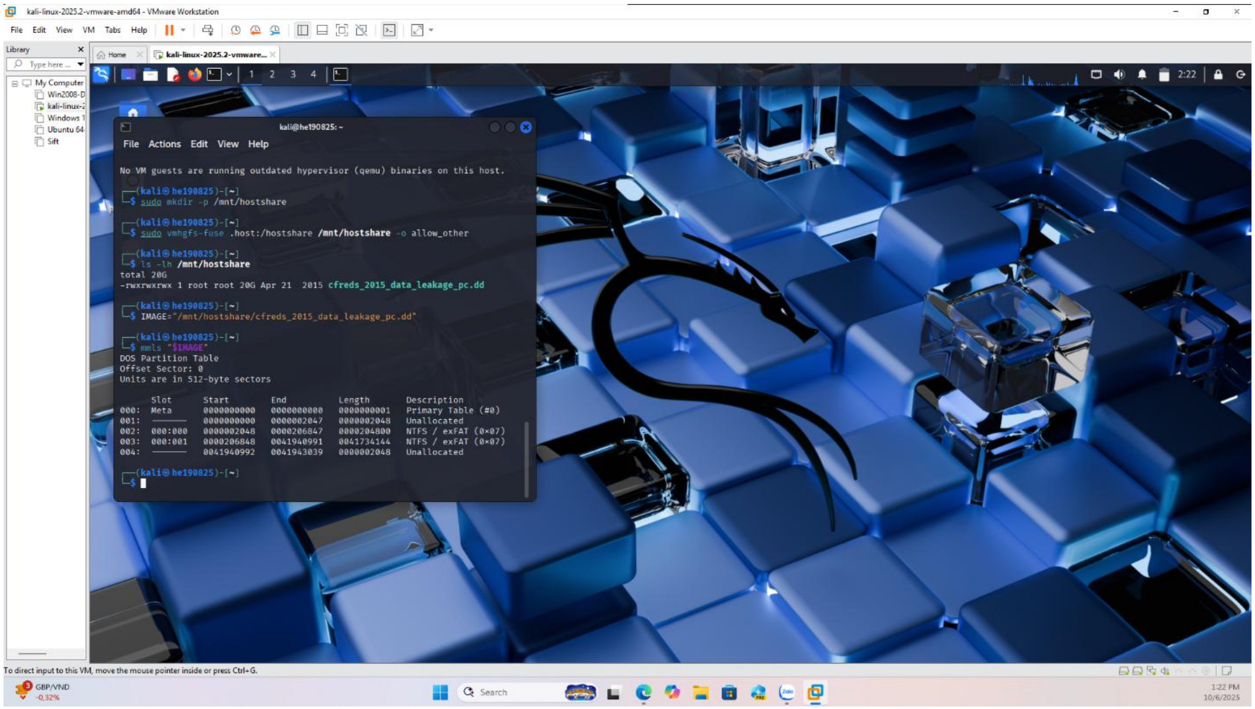
BÁO CÁO LAB 5-FRS

Họ và tên: Hoàng Đình Lâm
MSSV: HE190825
Lớp: IA1905

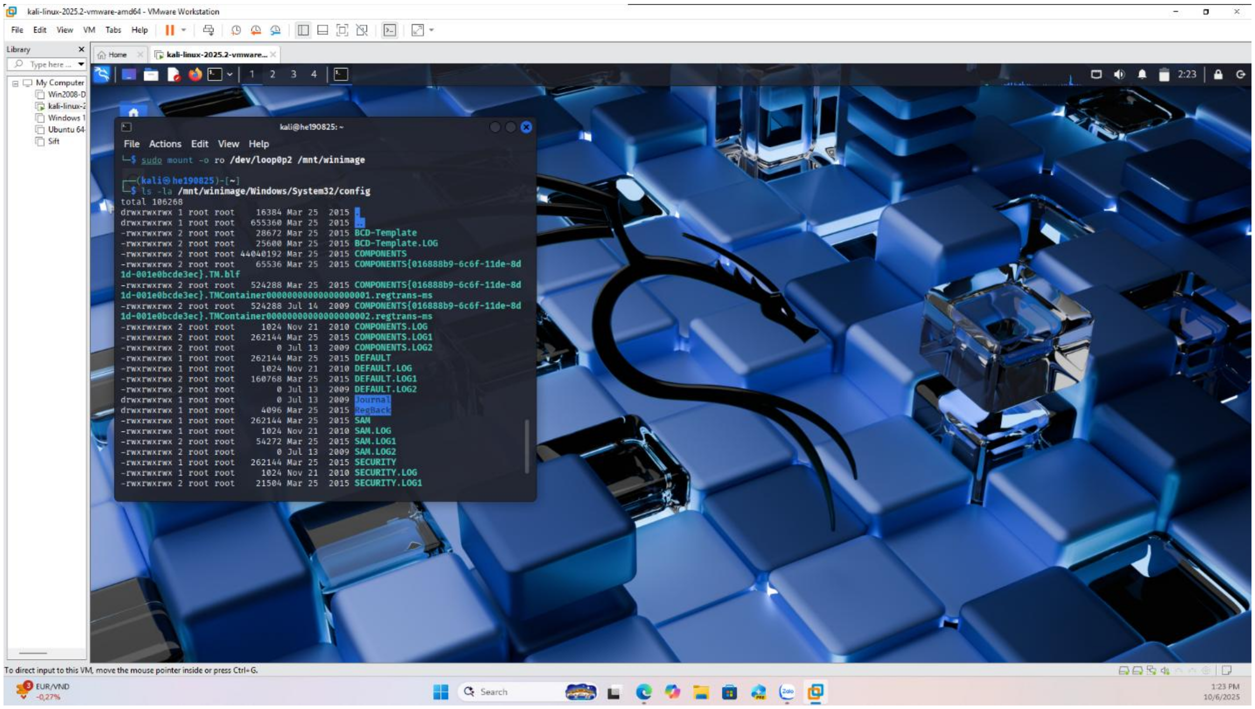

kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Win2008-D
kali-linux-2
Windows 1
Ubuntu 64
Sift
Home
kali-linux-2025.2-vmware...
kali@he190825: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
GBP/VND
-0,32%
Search
1:22 PM
10/6/2025

```
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.2.7) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.

Restarting services...
 systemctl restart open-vm-tools.service

No containers need to be restarted.

User sessions running outdated binaries:
 kali @ user service: gvfs-daemon.service[1610],
  xdg-document-portal.service[2088]

No VM guests are running outdated hypervisor (qemu) binaries on this host.

┌──(kali㉿he190825)-[~]
└─$ sudo mkdir -p /mnt/hostshare

┌──(kali㉿he190825)-[~]
└─$ sudo vmhgfs-fuse .host:/hostshare /mnt/hostshare -o allow_other

┌──(kali㉿he190825)-[~]
└─$ ls -lh /mnt/hostshare
total 20G
-rwxrwxrwx 1 root root 20G Apr 21  2015 cfreds_2015_data_leakage_pc.dd

┌──(kali㉿he190825)-[~]
└─$ 
```

-ShareFolder từ ổ vào win ảo.



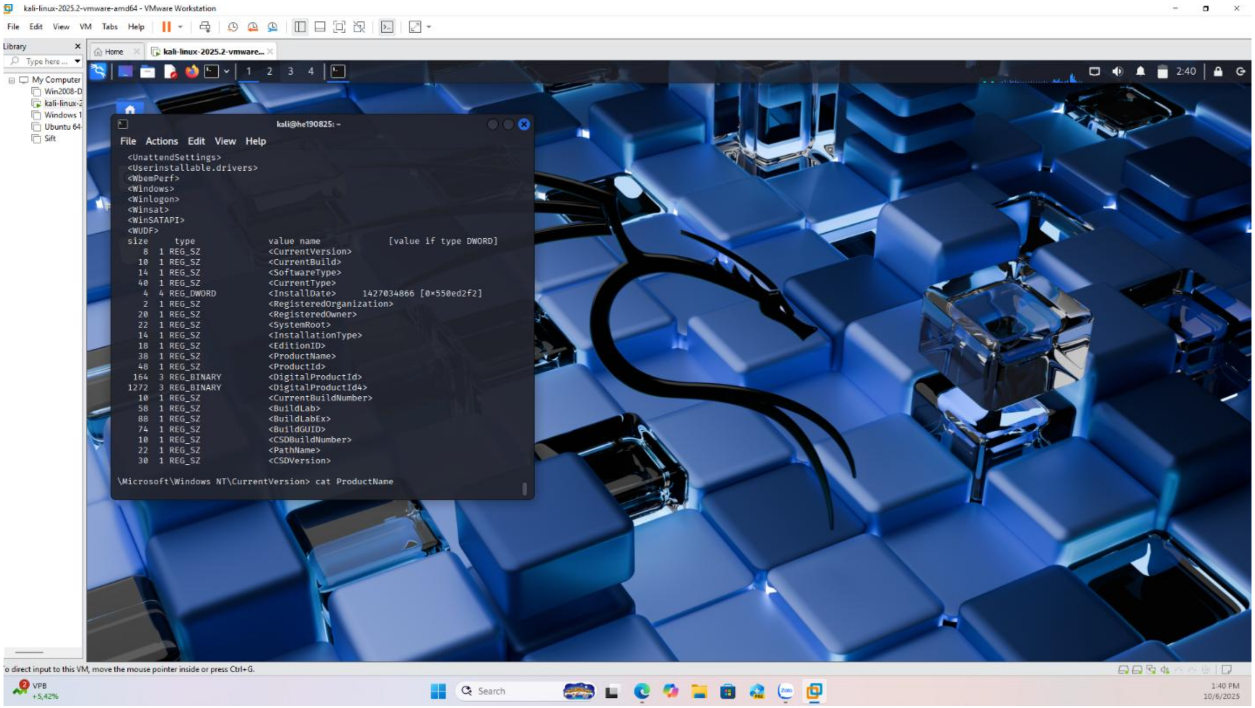
```
No VM guests are running outdated hypervisor (qemu) binaries on this host.

┌──(kali㉿he190825)-[~]
└─$ sudo mkdir -p /mnt/hostshare

┌──(kali㉿he190825)-[~]
└─$ sudo vmhgfs-fuse .host:/hostshare /mnt/hostshare -o allow_other

┌──(kali㉿he190825)-[~]
└─$ ls -lh /mnt/hostshare
total 20G
-rwxrwxrwx 1 root root 20G Apr 21  2015 cfreds_2015_data_leakage_pc.dd

┌──(kali㉿he190825)-[~]
└─$ IMAGE="/mnt/hostshare/cfreds_2015_data_leakage_pc.dd"

┌──(kali㉿he190825)-[~]
└─$ mmls "$IMAGE"
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0000206847   0000204800   NTFS / exFAT (0x07)
003:  000:001   0000206848   0041940991   0041734144   NTFS / exFAT (0x07)
004:  -------   0041940992   0041943039   0000002048   Unallocated

┌──(kali㉿he190825)-[~]
└─$ 
```



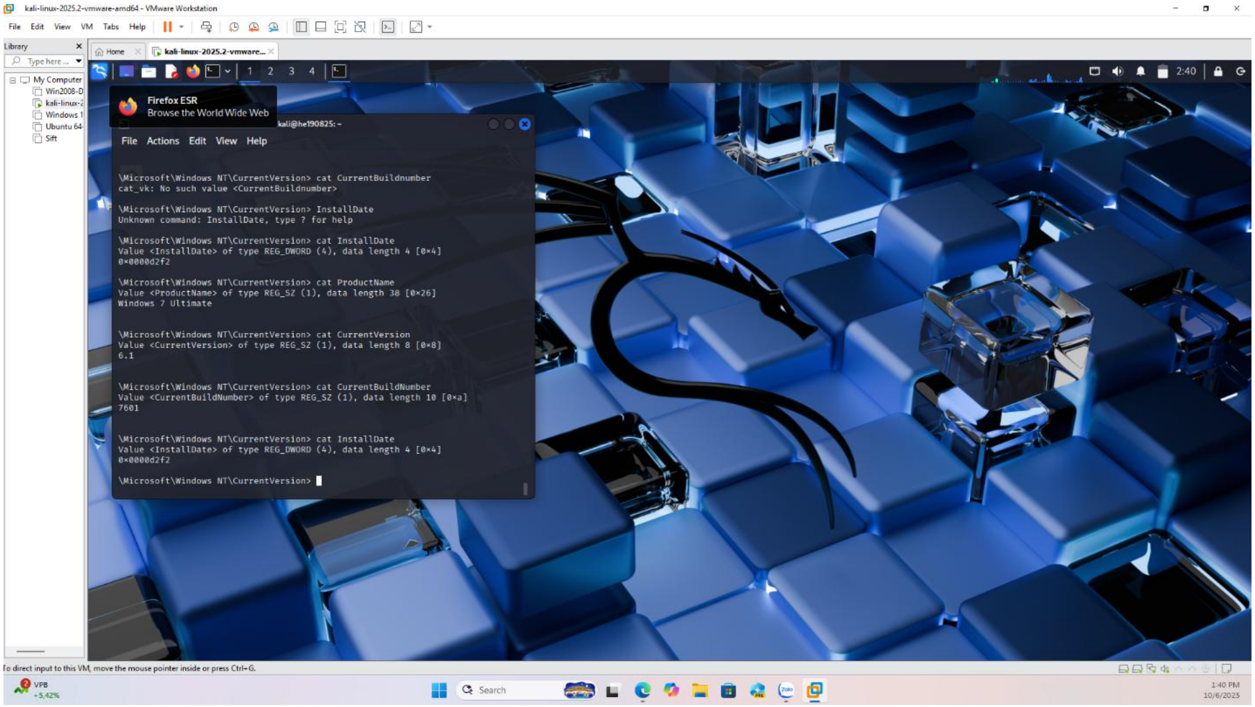
```
└─$ sudo mount -o ro /dev/loop0p2 /mnt/winimage

┌──(kali㉿he190825)-[~]
└─$ ls -la /mnt/winimage/Windows/System32/config
total 106268
drwxrwxrwx 1 root root    16384 Mar 25  2015 .
drwxrwxrwx 1 root root   655360 Mar 25  2015 ..
-rwxrwxrwx 2 root root    28672 Mar 25  2015 BCD-Template
-rwxrwxrwx 2 root root    25600 Mar 25  2015 BCD-Template.LOG
-rwxrwxrwx 2 root root 44040192 Mar 25  2015 COMPONENTS
-rwxrwxrwx 2 root root    65536 Mar 25  2015 COMPONENTS{016888b9-6c6f-11de-8d
1d-001e0bcde3ec}.TM.blf
-rwxrwxrwx 2 root root   524288 Mar 25  2015 COMPONENTS{016888b9-6c6f-11de-8d
1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
-rwxrwxrwx 2 root root   524288 Jul 14  2009 COMPONENTS{016888b9-6c6f-11de-8d
1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
-rwxrwxrwx 2 root root     1024 Nov 21  2010 COMPONENTS.LOG
-rwxrwxrwx 2 root root   262144 Mar 25  2015 COMPONENTS.LOG1
-rwxrwxrwx 2 root root        0 Jul 13  2009 COMPONENTS.LOG2
-rwxrwxrwx 1 root root   262144 Mar 25  2015 DEFAULT
-rwxrwxrwx 1 root root     1024 Nov 21  2010 DEFAULT.LOG
-rwxrwxrwx 2 root root   160768 Mar 25  2015 DEFAULT.LOG1
-rwxrwxrwx 2 root root        0 Jul 13  2009 DEFAULT.LOG2
drwxrwxrwx 1 root root        0 Jul 13  2009 Journal
drwxrwxrwx 1 root root     4096 Mar 25  2015 RegBack
-rwxrwxrwx 1 root root   262144 Mar 25  2015 SAM
-rwxrwxrwx 1 root root     1024 Nov 21  2010 SAM.LOG
-rwxrwxrwx 2 root root    54272 Mar 25  2015 SAM.LOG1
-rwxrwxrwx 2 root root        0 Jul 13  2009 SAM.LOG2
-rwxrwxrwx 1 root root   262144 Mar 25  2015 SECURITY
-rwxrwxrwx 1 root root     1024 Nov 21  2010 SECURITY.LOG
-rwxrwxrwx 2 root root    21504 Mar 25  2015 SECURITY.LOG1
```

1. What is the installed OS information in detail?

-: cd 'Microsoft\Windows NT\CurrentVersion'


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Win2008-D
kali-linux-2
Windows 1
Ubuntu 64
Sift
Home
kali-linux-2025.2-vmware...
kali@he190825: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
VPB
Search
1:40 PM
10/6/2025

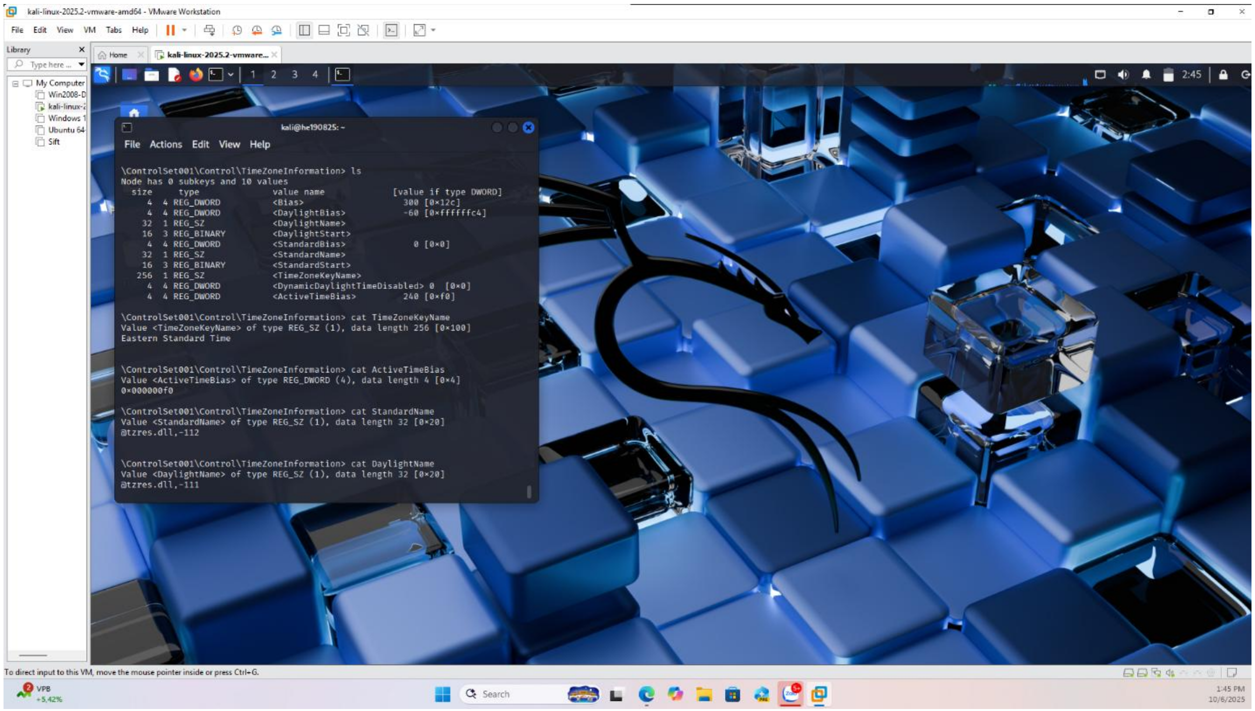
```
 <UnattendSettings>
 <Userinstallable.drivers>
 <WbemPerf>
 <Windows>
 <Winlogon>
 <Winsat>
 <WinSATAPI>
 <WUDF>
 size     type              value name             [value if type DWORD]
    8  1 REG_SZ             <CurrentVersion>
   10  1 REG_SZ             <CurrentBuild>
   14  1 REG_SZ             <SoftwareType>
   40  1 REG_SZ             <CurrentType>
    4  4 REG_DWORD          <InstallDate>     1427034866 [0×550ed2f2]
    2  1 REG_SZ             <RegisteredOrganization>
   20  1 REG_SZ             <RegisteredOwner>
   22  1 REG_SZ             <SystemRoot>
   14  1 REG_SZ             <InstallationType>
   18  1 REG_SZ             <EditionID>
   38  1 REG_SZ             <ProductName>
   48  1 REG_SZ             <ProductId>
  164  3 REG_BINARY         <DigitalProductId>
 1272  3 REG_BINARY         <DigitalProductId4>
   10  1 REG_SZ             <CurrentBuildNumber>
   58  1 REG_SZ             <BuildLab>
   88  1 REG_SZ             <BuildLabEx>
   74  1 REG_SZ             <BuildGUID>
   10  1 REG_SZ             <CSDBuildNumber>
   22  1 REG_SZ             <PathName>
   30  1 REG_SZ             <CSDVersion>

\Microsoft\Windows NT\CurrentVersion> cat ProductName
```


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Win2008-D
kali-linux-2
Windows 1
Ubuntu 64
Sift
Home
kali-linux-2025.2-vmware...
Firefox ESR
Browse the World Wide Web
kali@he190825: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
VPB
Search
1:40 PM
10/6/2025

```
\Microsoft\Windows NT\CurrentVersion> cat CurrentBuildnumber
cat_vk: No such value <CurrentBuildnumber>

\Microsoft\Windows NT\CurrentVersion> InstallDate
Unknown command: InstallDate, type ? for help

\Microsoft\Windows NT\CurrentVersion> cat InstallDate
Value <InstallDate> of type REG_DWORD (4), data length 4 [0×4]
0×0000d2f2

\Microsoft\Windows NT\CurrentVersion> cat ProductName
Value <ProductName> of type REG_SZ (1), data length 38 [0×26]
Windows 7 Ultimate


\Microsoft\Windows NT\CurrentVersion> cat CurrentVersion
Value <CurrentVersion> of type REG_SZ (1), data length 8 [0×8]
6.1


\Microsoft\Windows NT\CurrentVersion> cat CurrentBuildNumber
Value <CurrentBuildNumber> of type REG_SZ (1), data length 10 [0×a]
7601


\Microsoft\Windows NT\CurrentVersion> cat InstallDate
Value <InstallDate> of type REG_DWORD (4), data length 4 [0×4]
0×0000d2f2

\Microsoft\Windows NT\CurrentVersion> 
```

2. What is the time zone setting?

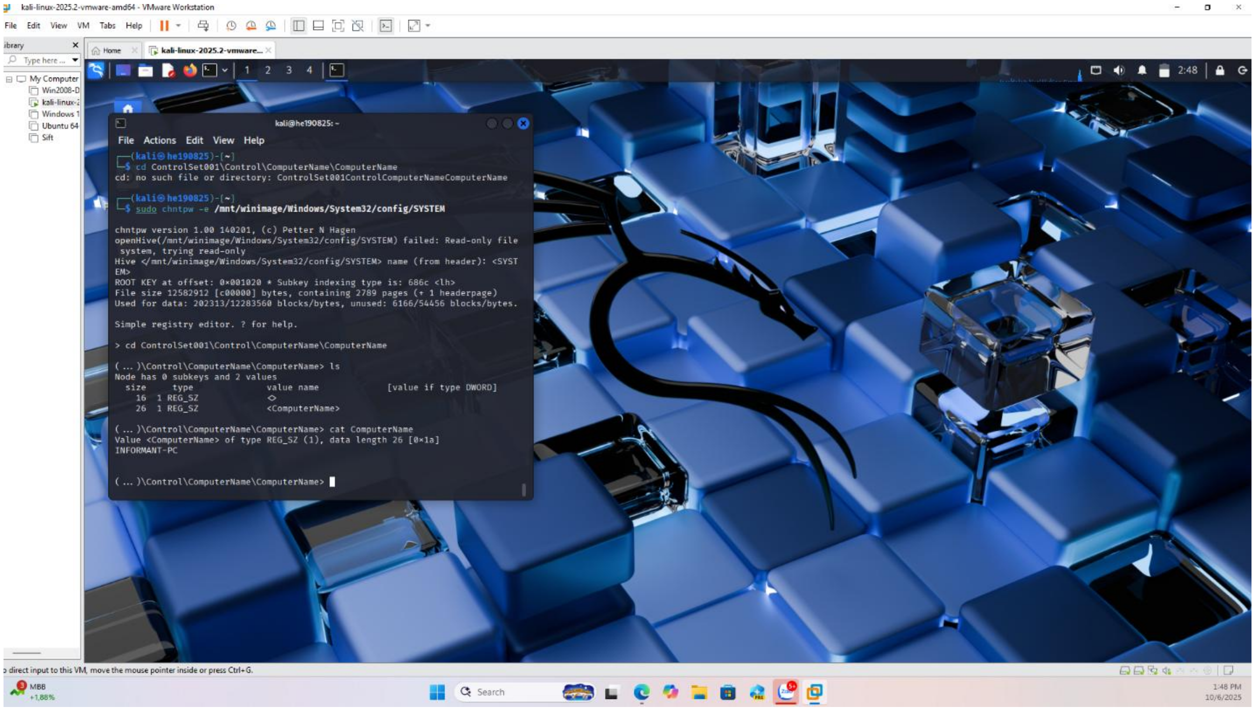
```
sudo chntpw -e "$WORK/SYSTEM"
cd CurrentControlSet\Control\TimeZoneInformation
ls
```



kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Win2008-D
kali-linux-2
Windows 1
Ubuntu 64
Sift
Home
kali-linux-2025.2-vmware...
kali@he190825: ~
File Actions Edit View Help
2:45
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
VPB
+5.42%
Search
1:45 PM
10/6/2025

```
\ControlSet001\Control\TimeZoneInformation> ls
Node has 0 subkeys and 10 values
  size     type              value name             [value if type DWORD]
     4  4 REG_DWORD          <Bias>                   300 [0×12c]
     4  4 REG_DWORD          <DaylightBias>           -60 [0×ffffffc4]
    32  1 REG_SZ             <DaylightName>
    16  3 REG_BINARY         <DaylightStart>
     4  4 REG_DWORD          <StandardBias>             0 [0×0]
    32  1 REG_SZ             <StandardName>
    16  3 REG_BINARY         <StandardStart>
   256  1 REG_SZ             <TimeZoneKeyName>
     4  4 REG_DWORD          <DynamicDaylightTimeDisabled> 0  [0×0]
     4  4 REG_DWORD          <ActiveTimeBias>         240 [0×f0]

\ControlSet001\Control\TimeZoneInformation> cat TimeZoneKeyName
Value <TimeZoneKeyName> of type REG_SZ (1), data length 256 [0×100]
Eastern Standard Time


\ControlSet001\Control\TimeZoneInformation> cat ActiveTimeBias
Value <ActiveTimeBias> of type REG_DWORD (4), data length 4 [0×4]
0×000000f0

\ControlSet001\Control\TimeZoneInformation> cat StandardName
Value <StandardName> of type REG_SZ (1), data length 32 [0×20]
@tzres.dll,-112


\ControlSet001\Control\TimeZoneInformation> cat DaylightName
Value <DaylightName> of type REG_SZ (1), data length 32 [0×20]
@tzres.dll,-111
```

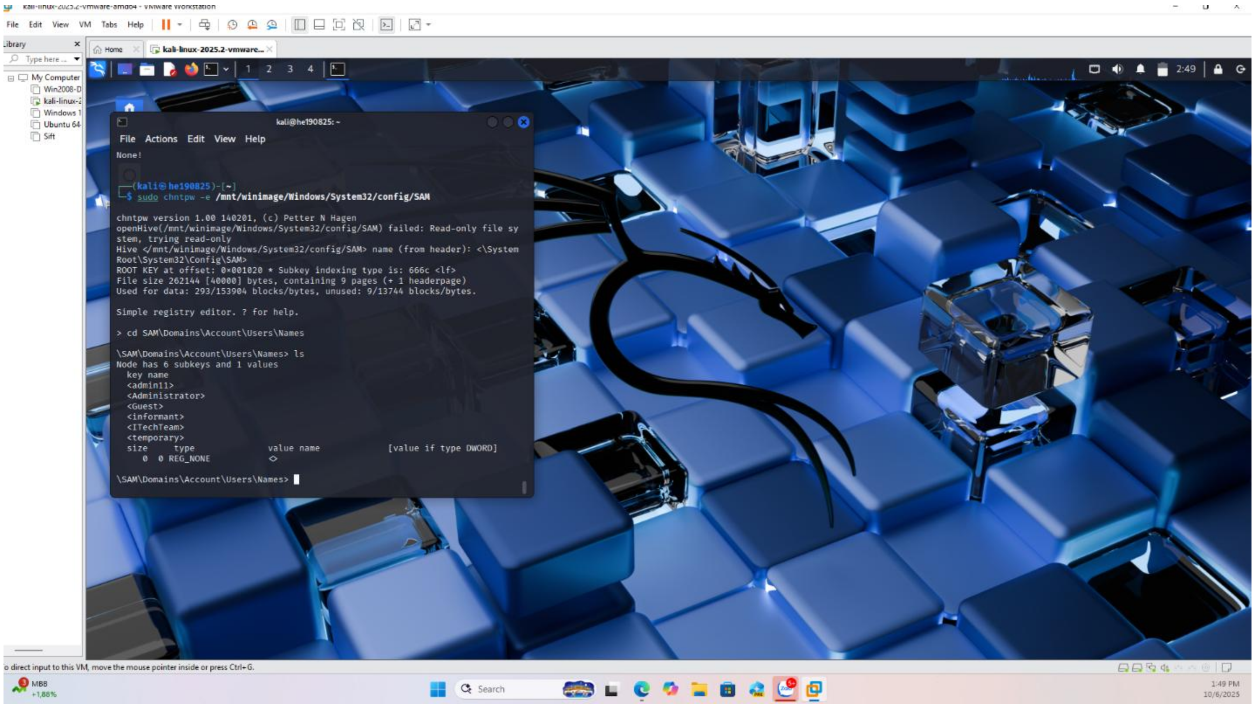
3. What is the computer name?



kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
ibrary
My Computer
Win2008-D
kali-linux-2
Windows 1
Ubuntu 64
Sift
Home
kali-linux-2025.2-vmware...
kali@he190825: ~
File Actions Edit View Help
2:48
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.
MBB
+1.88%
Search
1:48 PM
10/6/2025

```
┌──(kali㉿he190825)-[~]
└─$ cd ControlSet001\Control\ComputerName\ComputerName
cd: no such file or directory: ControlSet001ControlComputerNameComputerName

┌──(kali㉿he190825)-[~]
└─$ sudo chntpw -e /mnt/winimage/Windows/System32/config/SYSTEM

chntpw version 1.00 140201, (c) Petter N Hagen
openHive(/mnt/winimage/Windows/System32/config/SYSTEM) failed: Read-only file
 system, trying read-only
Hive </mnt/winimage/Windows/System32/config/SYSTEM> name (from header): <SYST
EM>
ROOT KEY at offset: 0×001020 * Subkey indexing type is: 686c <lh>
File size 12582912 [c00000] bytes, containing 2789 pages (+ 1 headerpage)
Used for data: 202313/12283560 blocks/bytes, unused: 6166/54456 blocks/bytes.

Simple registry editor. ? for help.

> cd ControlSet001\Control\ComputerName\ComputerName

( ... )\Control\ComputerName\ComputerName> ls
Node has 0 subkeys and 2 values
  size     type              value name             [value if type DWORD]
    16  1 REG_SZ             <>
    26  1 REG_SZ             <ComputerName>

( ... )\Control\ComputerName\ComputerName> cat ComputerName
Value <ComputerName> of type REG_SZ (1), data length 26 [0×1a]
INFORMANT-PC


( ... )\Control\ComputerName\ComputerName> █
```

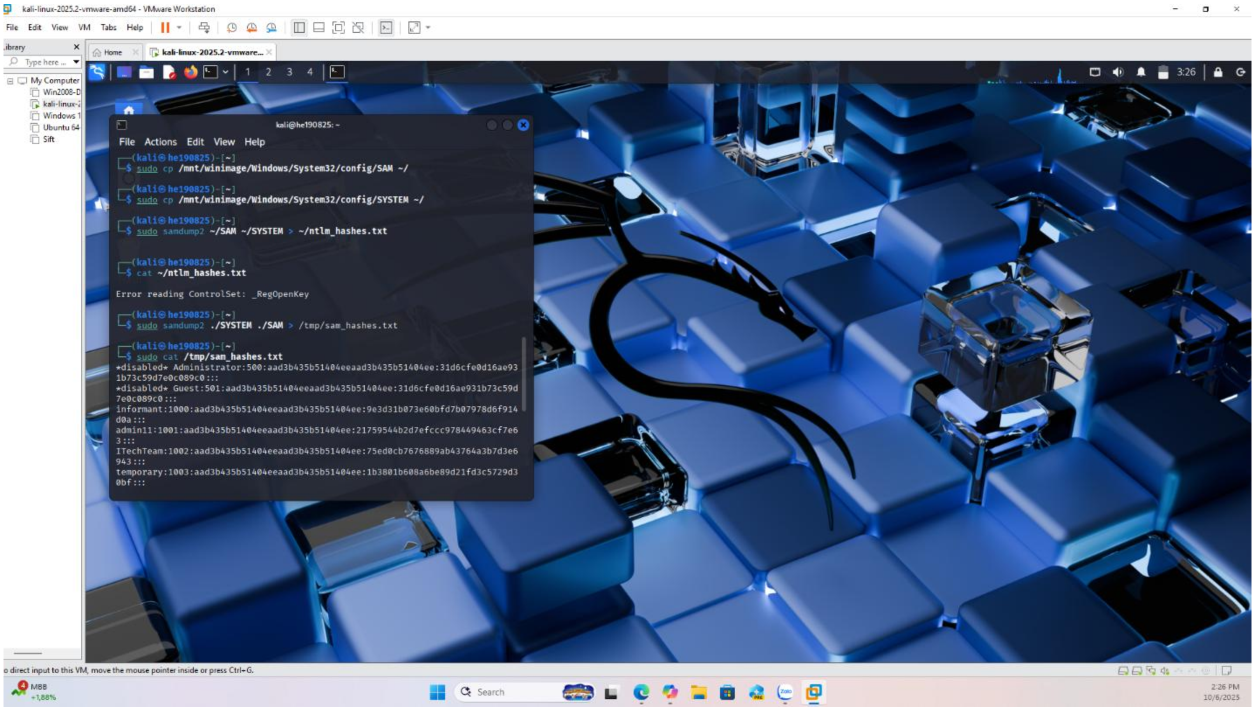
4. How many accounts does the system have?



```
None!

┌──(kali㉿he190825)-[~]
└─$ sudo chntpw -e /mnt/winimage/Windows/System32/config/SAM

chntpw version 1.00 140201, (c) Petter N Hagen
openHive(/mnt/winimage/Windows/System32/config/SAM) failed: Read-only file sy
stem, trying read-only
Hive </mnt/winimage/Windows/System32/config/SAM> name (from header): <\System
Root\System32\Config\SAM>
ROOT KEY at offset: 0×001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 9 pages (+ 1 headerpage)
Used for data: 293/153904 blocks/bytes, unused: 9/13744 blocks/bytes.

Simple registry editor. ? for help.

> cd SAM\Domains\Account\Users\Names

\SAM\Domains\Account\Users\Names> ls
Node has 6 subkeys and 1 values
  key name
  <admin11>
  <Administrator>
  <Guest>
  <informant>
  <ITechTeam>
  <temporary>
  size     type              value name             [value if type DWORD]
     0  0 REG_NONE           <>

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

5.

What are the NTLM password hashes of these accounts?



```
┌──(kali㉿he190825)-[~]
└─$ sudo cp /mnt/winimage/Windows/System32/config/SAM ~/

┌──(kali㉿he190825)-[~]
└─$ sudo cp /mnt/winimage/Windows/System32/config/SYSTEM ~/

┌──(kali㉿he190825)-[~]
└─$ sudo samdump2 ~/SAM ~/SYSTEM > ~/ntlm_hashes.txt


┌──(kali㉿he190825)-[~]
└─$ cat ~/ntlm_hashes.txt

Error reading ControlSet: _RegOpenKey

┌──(kali㉿he190825)-[~]
└─$ sudo samdump2 ./SYSTEM ./SAM > /tmp/sam_hashes.txt

┌──(kali㉿he190825)-[~]
└─$ sudo cat /tmp/sam_hashes.txt
*disabled* Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae93
1b73c59d7e0c089c0:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d
7e0c089c0:::
informant:1000:aad3b435b51404eeaad3b435b51404ee:9e3d31b073e60bfd7b07978d6f914
d0a:::
admin11:1001:aad3b435b51404eeaad3b435b51404ee:21759544b2d7efccc978449463cf7e6
3:::
ITechTeam:1002:aad3b435b51404eeaad3b435b51404ee:75ed0cb7676889ab43764a3b7d3e6
943:::
temporary:1003:aad3b435b51404eeaad3b435b51404ee:1b3801b608a6be89d21fd3c5729d3
0bf:::
```

6. What are included in UserAssist?

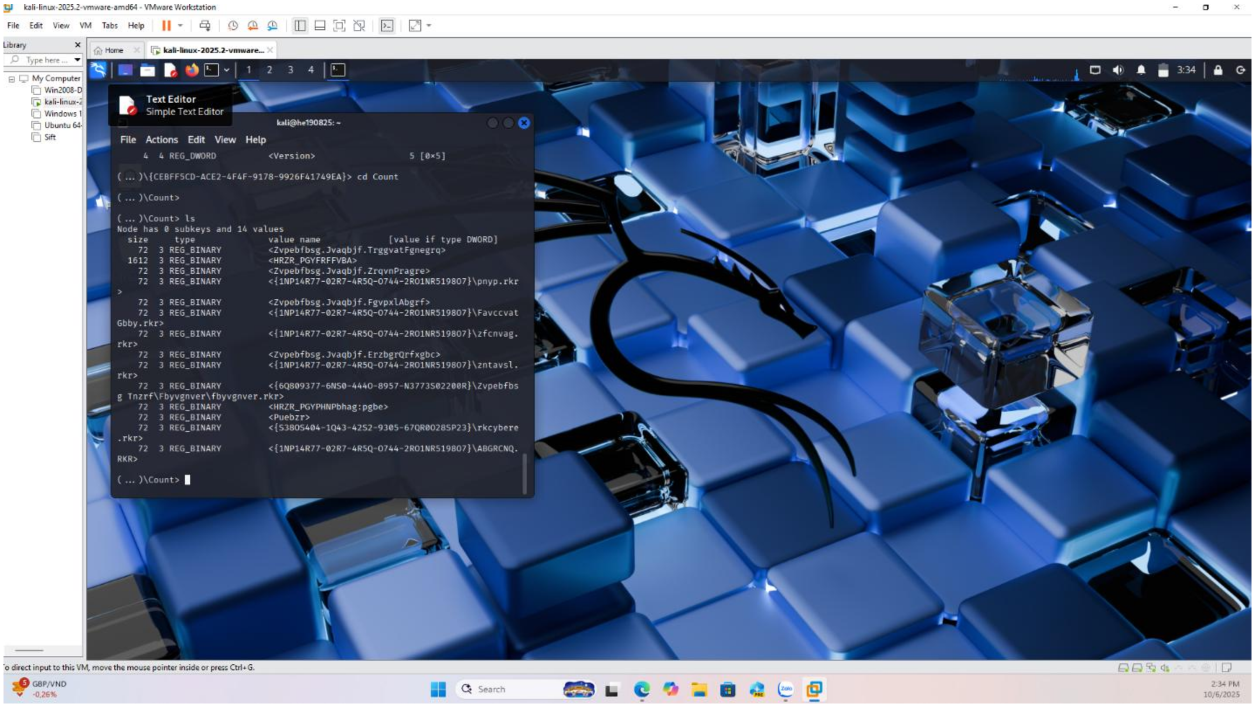
-sử dung admin 11

-sau đó tìm ra 2 GUID

-sao chép 2 GUID đó vào nano userassist_raw.txt

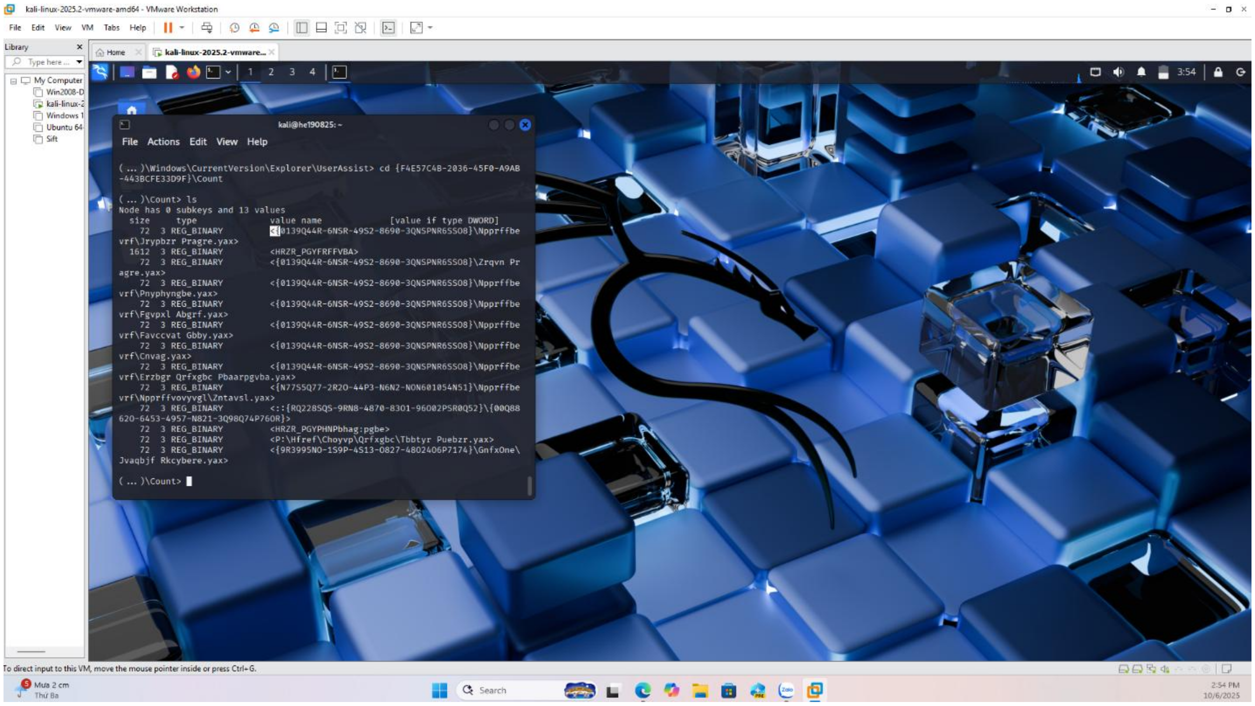
-sed 's/[<>]//g' ~/userassist_raw.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m' > ~/userassist_decoded.txt

cat ~/userassist_decoded.txt



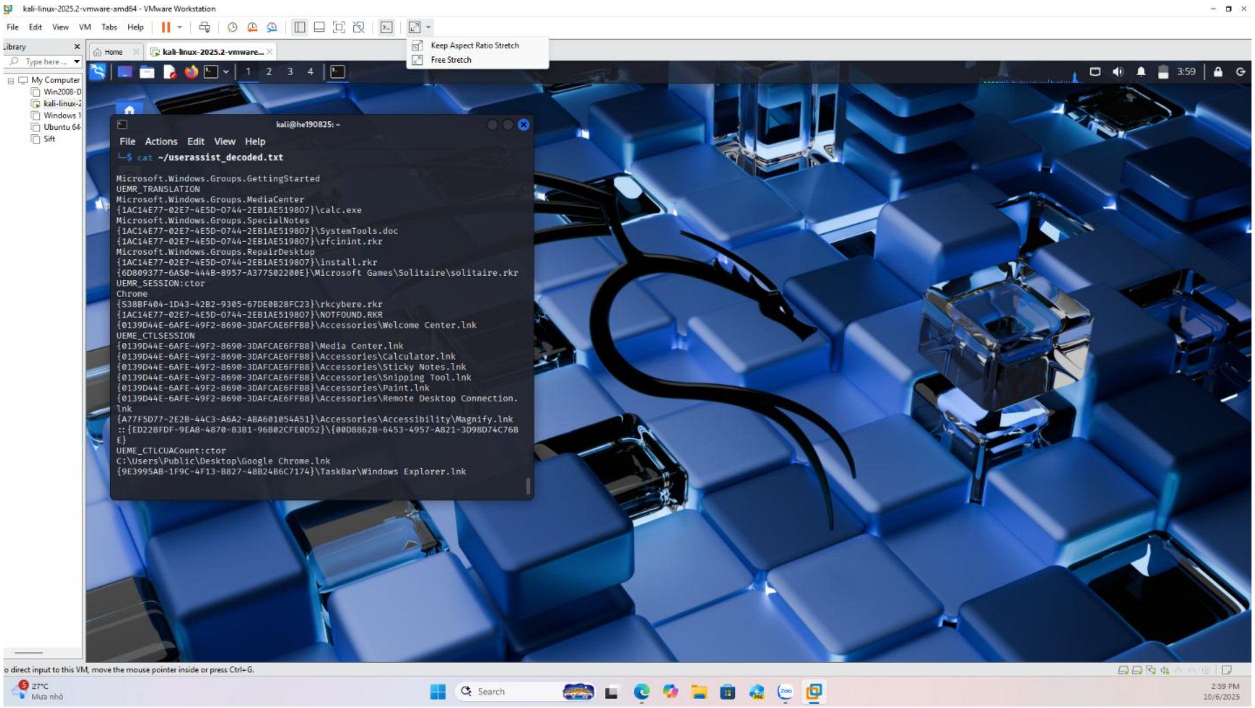
kali-linux-2025.2-vmware-amd64 - VMware Workstation
Text Editor
Simple Text Editor
kali@he190825: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
GBP/VND
-0.26%
2:34 PM
10/6/2025

```
     4  4 REG_DWORD          <Version>                    5 [0x5]

( ... )\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}> cd Count

( ... )\Count>

( ... )\Count> ls
Node has 0 subkeys and 14 values
  size     type              value name             [value if type DWORD]
    72  3 REG_BINARY         <Zvpebfbsg.Jvaqbjf.TrggvatFgnegrq>
  1612  3 REG_BINARY         <HRZR_PGYFRFFVBA>
    72  3 REG_BINARY         <Zvpebfbsg.Jvaqbjf.ZrqvnPragre>
    72  3 REG_BINARY         <{1NP14R77-02R7-4R5Q-O744-2RO1NR519807}\pnyp.rkr
>
    72  3 REG_BINARY         <Zvpebfbsg.Jvaqbjf.FgvpxlAbgrf>
    72  3 REG_BINARY         <{1NP14R77-02R7-4R5Q-O744-2RO1NR519807}\Favccvat
Gbby.rkr>
    72  3 REG_BINARY         <{1NP14R77-02R7-4R5Q-O744-2RO1NR519807}\zfcnvag.
rkr>
    72  3 REG_BINARY         <Zvpebfbsg.Jvaqbjf.ErzbgrQrfxgbc>
    72  3 REG_BINARY         <{1NP14R77-02R7-4R5Q-O744-2RO1NR519807}\zntavsl.
rkr>
    72  3 REG_BINARY         <{6Q809377-6NS0-444O-8957-N3773S02200R}\Zvpebfbs
g Tnzrf\Fbyvgnver\fbyvgnver.rkr>
    72  3 REG_BINARY         <HRZR_PGYPHNPbhag:pgbe>
    72  3 REG_BINARY         <Puebzr>
    72  3 REG_BINARY         <{S380S404-1Q43-42S2-9305-67QR0028SP23}\rkcybere
.rkr>
    72  3 REG_BINARY         <{1NP14R77-02R7-4R5Q-O744-2RO1NR519807}\ABGRCNQ.
RKR>

( ... )\Count> █
```



kali-linux-2025.2-vmware-amd64 - VMware Workstation
kali@he190825: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Mưa 2 cm
Thứ Ba
2:54 PM
10/6/2025

```
( ... )\Windows\CurrentVersion\Explorer\UserAssist> cd {F4E57C4B-2036-45F0-A9AB
-443BCFE33D9F}\Count

( ... )\Count> ls
Node has 0 subkeys and 13 values
  size     type              value name             [value if type DWORD]
    72  3 REG_BINARY         <{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\Npprffbe
vrf\Jrypbzr Pragre.yax>
  1612  3 REG_BINARY         <HRZR_PGYFRFFVBA>
    72  3 REG_BINARY         <{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\Zrqvn Pr
agre.yax>
    72  3 REG_BINARY         <{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\Npprffbe
vrf\Pnyphyngbe.yax>
    72  3 REG_BINARY         <{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\Npprffbe
vrf\Fgvpxl Abgrf.yax>
    72  3 REG_BINARY         <{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\Npprffbe
vrf\Favccvat Gbby.yax>
    72  3 REG_BINARY         <{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\Npprffbe
vrf\Cnvag.yax>
    72  3 REG_BINARY         <{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\Npprffbe
vrf\Erzbgr Qrfxgbc Pbaarpgvba.yax>
    72  3 REG_BINARY         <{N77S5Q77-2R2O-44P3-N6N2-NON601054N51}\Npprffbe
vrf\Npprffvovyvgl\Zntavsl.yax>
    72  3 REG_BINARY         <::{RQ228SQS-9RN8-4870-83O1-96OO2PSR0Q52}\{00Q88
620-6453-4957-N821-3Q98Q74P76OR}>
    72  3 REG_BINARY         <HRZR_PGYPHNPbhag:pgbe>
    72  3 REG_BINARY         <P:\Hfref\Choyvp\Qrfxgbc\Tbbtyr Puebzr.yax>
    72  3 REG_BINARY         <{9R3995NO-1S9P-4S13-O827-4802406P7174}\GnfxOne\
Jvaqbjf Rkcybere.yax>

( ... )\Count> █
```


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Keep Aspect Ratio Stretch
Free Stretch
Library
Type here ...
My Computer
Win2008-D
kali-linux-2
Windows 1
Ubuntu 64-
Sift
Home
kali-linux-2025.2-vmware...
1 2 3 4
3:59
kali@he190825: ~
File Actions Edit View Help
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.
27°C
Mưa nhỏ
Search
2:59 PM
10/6/2025

```
└─$ cat ~/userassist_decoded.txt

Microsoft.Windows.Groups.GettingStarted
UEMR_TRANSLATION
Microsoft.Windows.Groups.MediaCenter
{1AC14E77-02E7-4E5D-0744-2EB1AE519807}\calc.exe
Microsoft.Windows.Groups.SpecialNotes
{1AC14E77-02E7-4E5D-0744-2EB1AE519807}\SystemTools.doc
{1AC14E77-02E7-4E5D-0744-2EB1AE519807}\zfcinint.rkr
Microsoft.Windows.Groups.RepairDesktop
{1AC14E77-02E7-4E5D-0744-2EB1AE519807}\install.rkr
{6D809377-6AS0-444B-8957-A377S02200E}\Microsoft Games\Solitaire\solitaire.rkr
UEMR_SESSION:ctor
Chrome
{S38BF404-1D43-42B2-9305-67DE0B28FC23}\rkcybere.rkr
{1AC14E77-02E7-4E5D-0744-2EB1AE519807}\NOTFOUND.RKR
{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Welcome Center.lnk
UEME_CTLSESSION
{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Media Center.lnk
{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Calculator.lnk
{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Sticky Notes.lnk
{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Snipping Tool.lnk
{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Paint.lnk
{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Remote Desktop Connection.
lnk
{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Accessories\Accessibility\Magnify.lnk
::{ED228FDF-9EA8-4870-83B1-96B02CFE0D52}\{00D8862B-6453-4957-A821-3D98D74C76B
E}
UEME_CTLCUACount:ctor
C:\Users\Public\Desktop\Google Chrome.lnk
{9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Windows Explorer.lnk
```