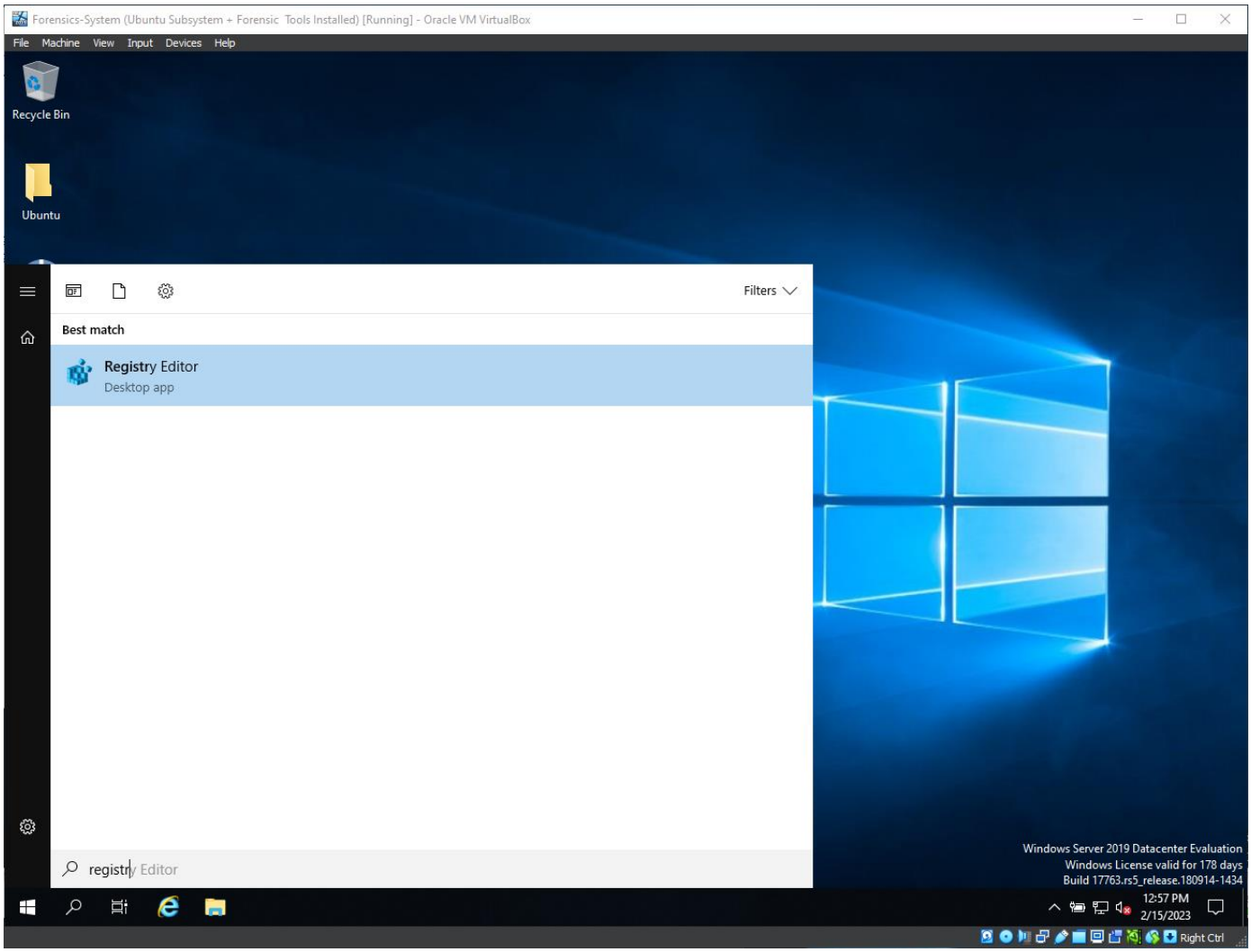
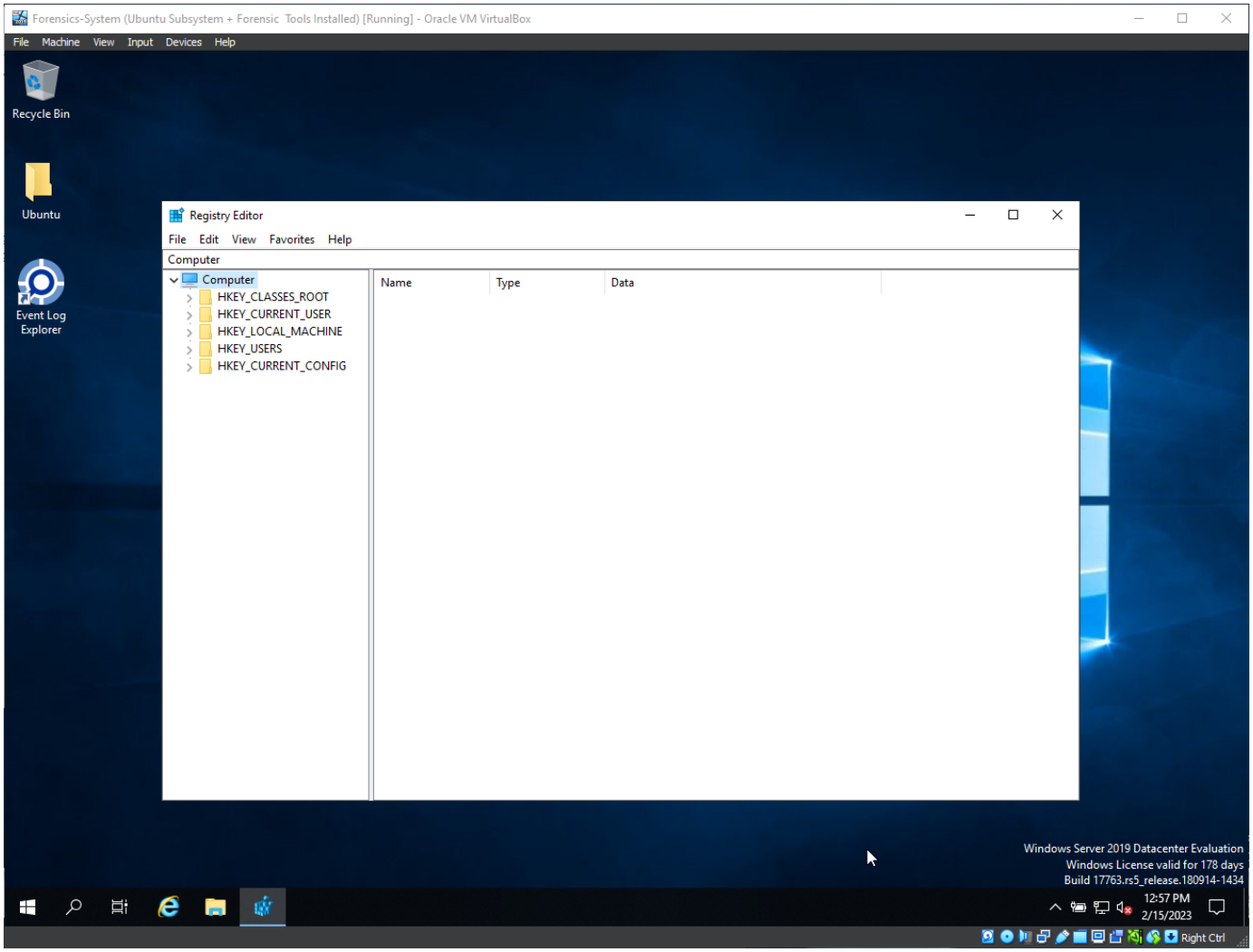
Windows Registry Analysis:

- Overview
- Registry Explorer – Investigation Start
- RegRipper
- SIDs
- User Accounts, groups and profiles

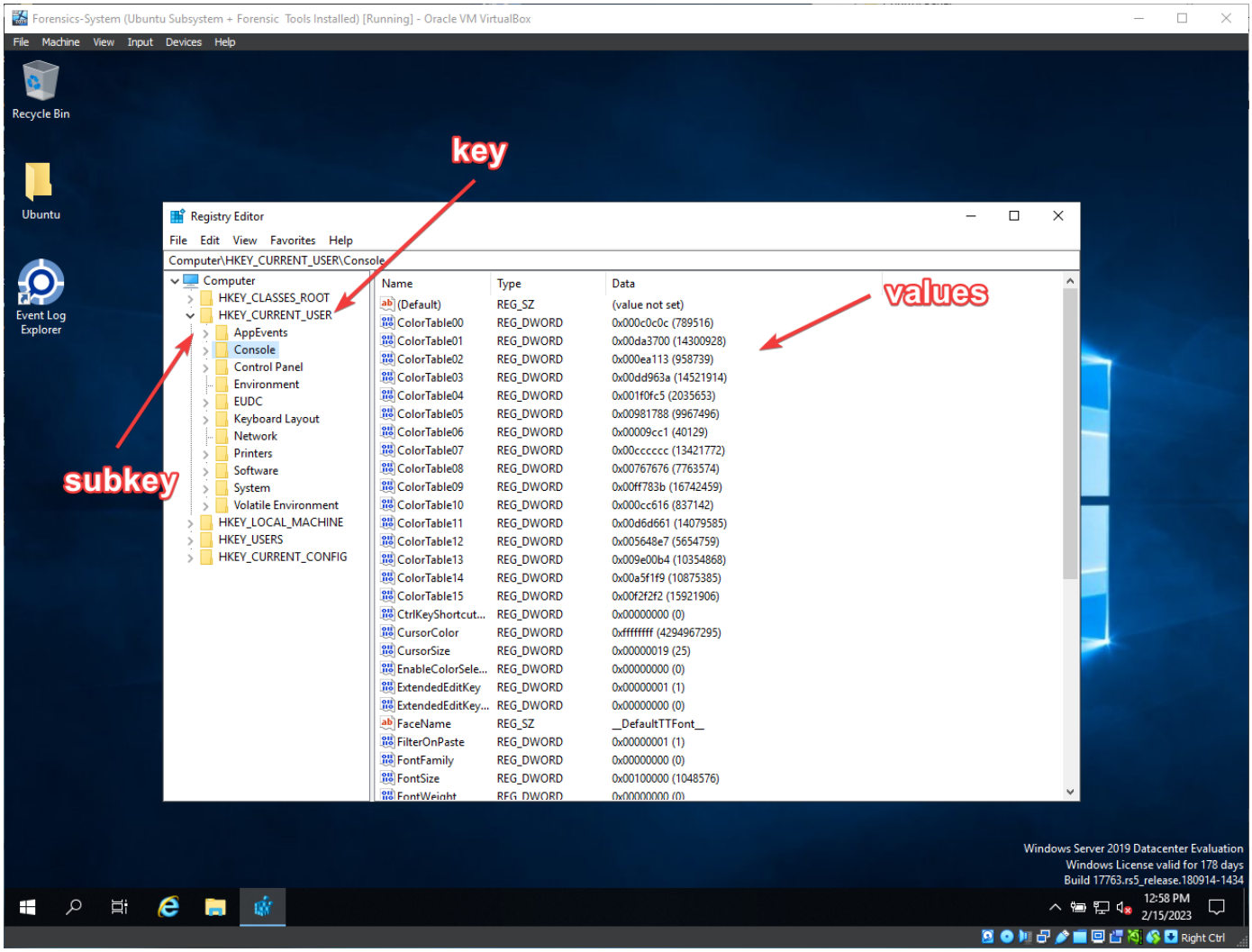
Overview

- Registry Editor:

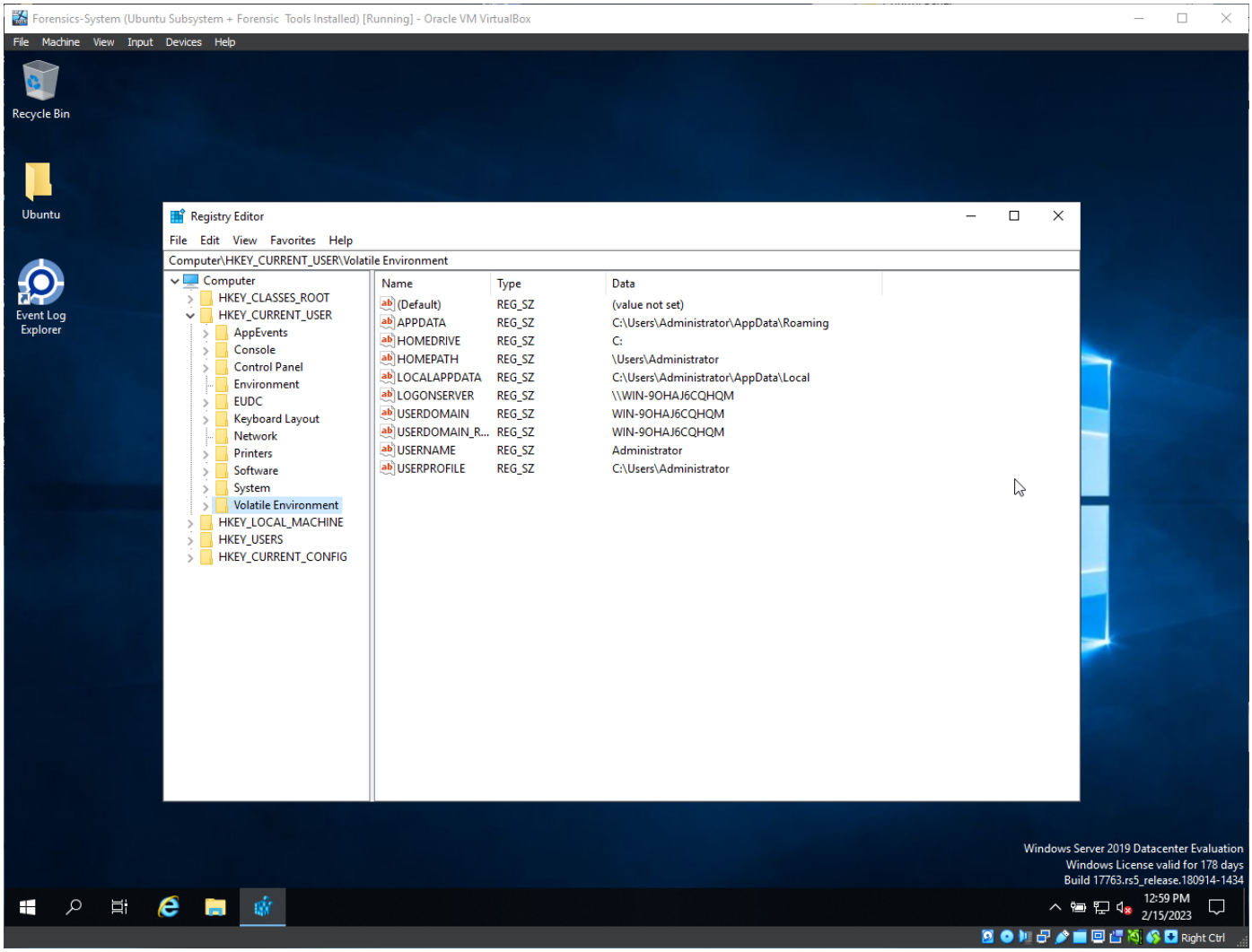




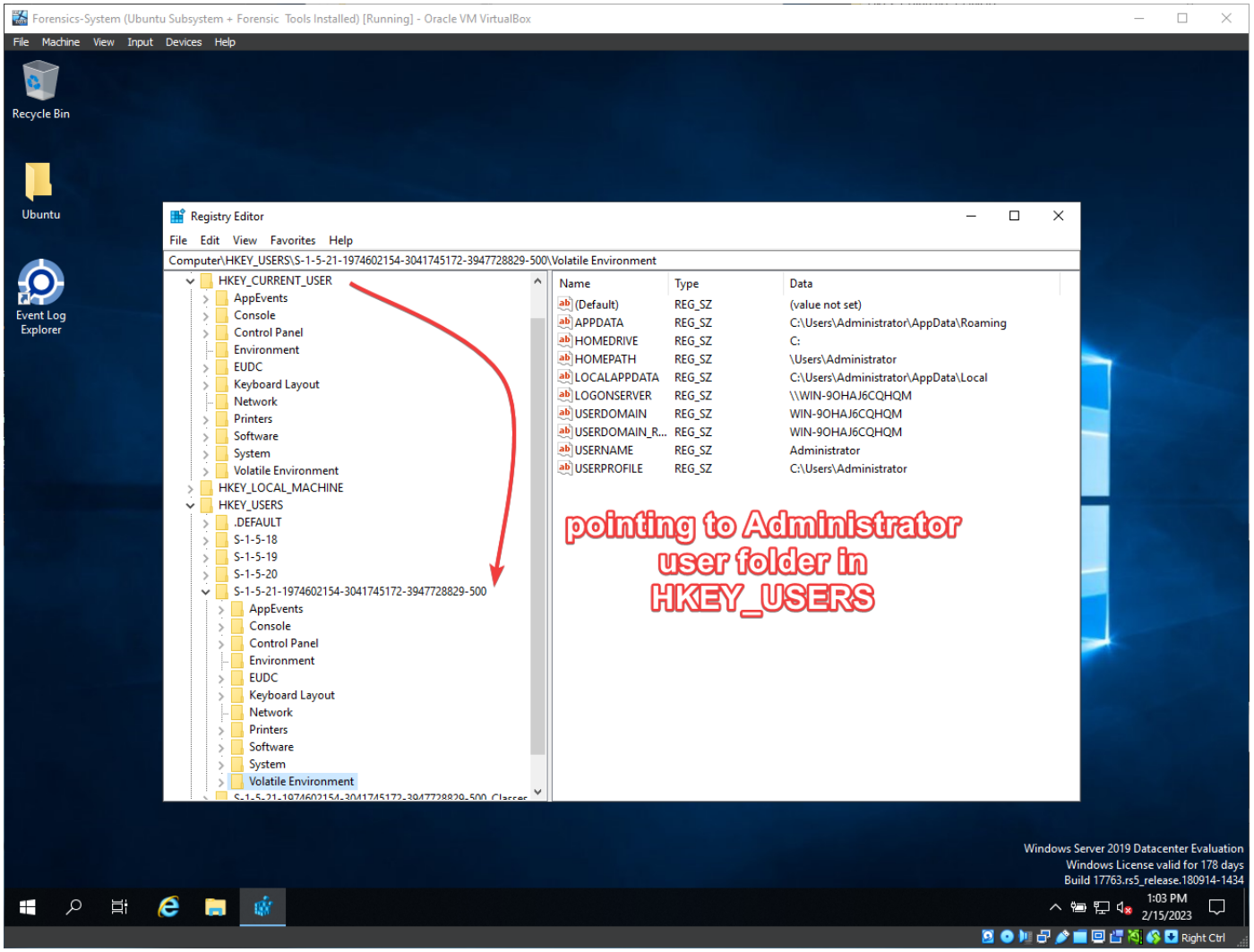
- The registry is the same as a database of key value pairs.



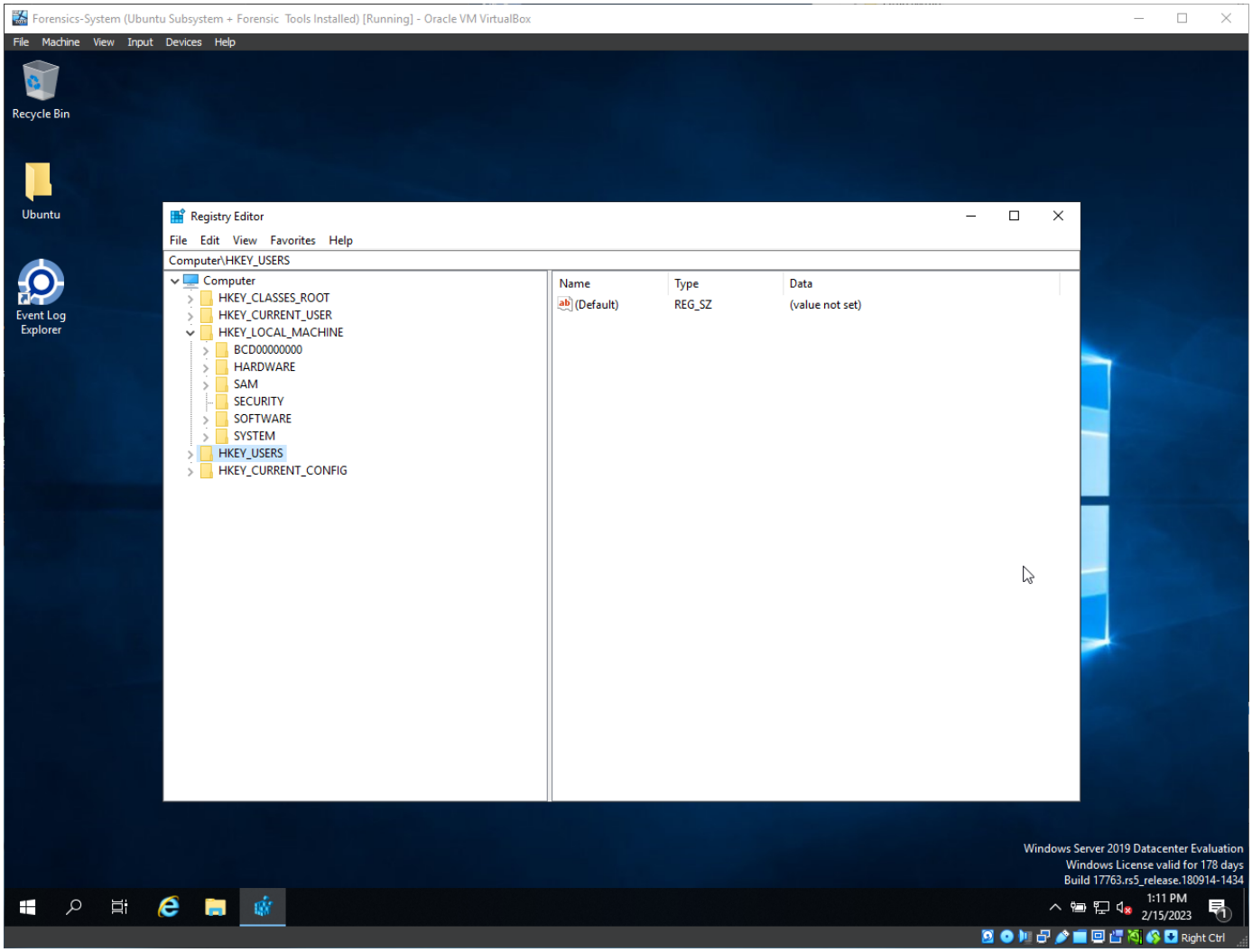
- HKEY_CURRENT_USER represents the user that is logged in.
- Applications, usually take information (user sistem settings or preferences)that it needs from this subkey.



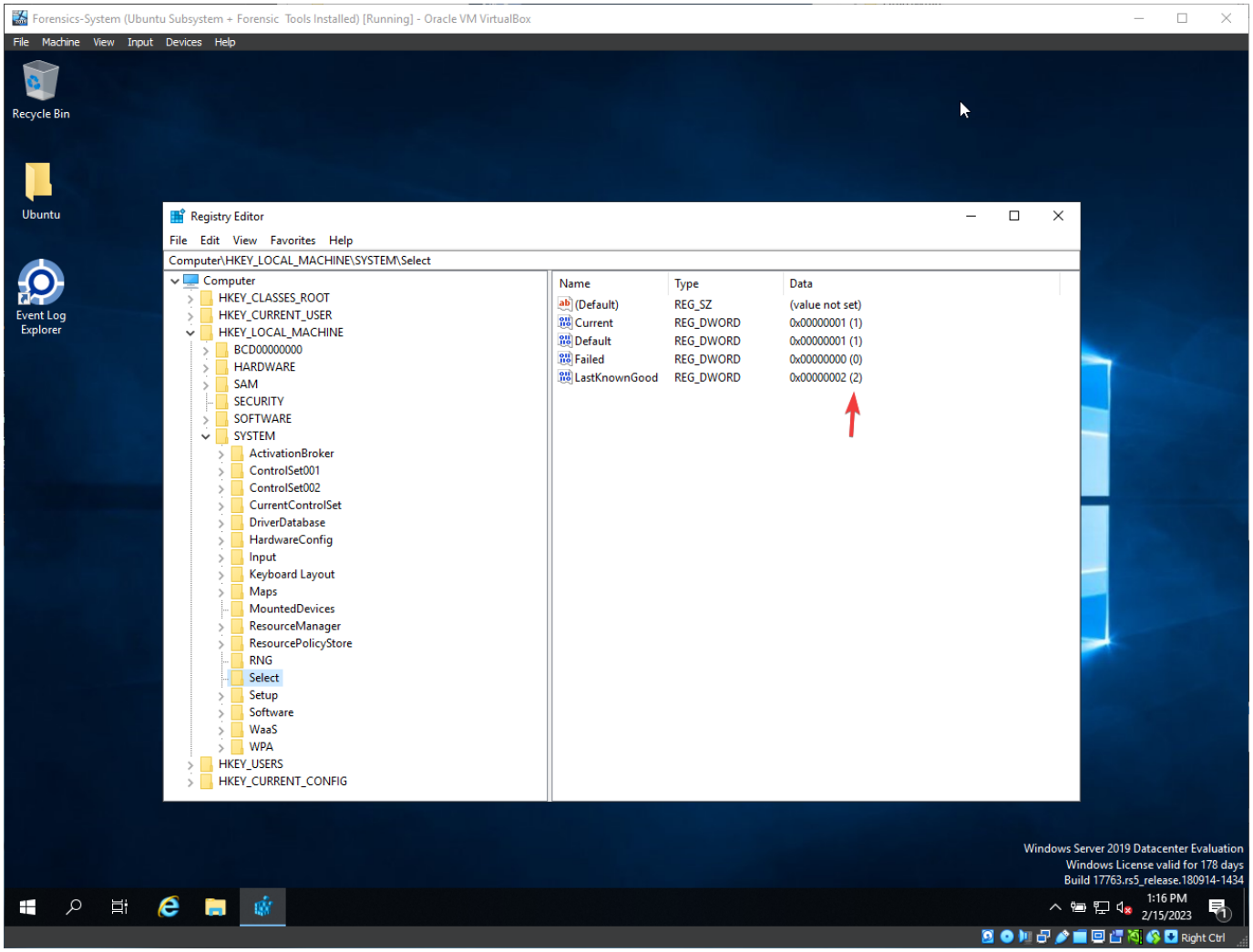
- HKEY_CURRENT_USER is a symbolic link . The information comes from HKEY_USERS registry key.



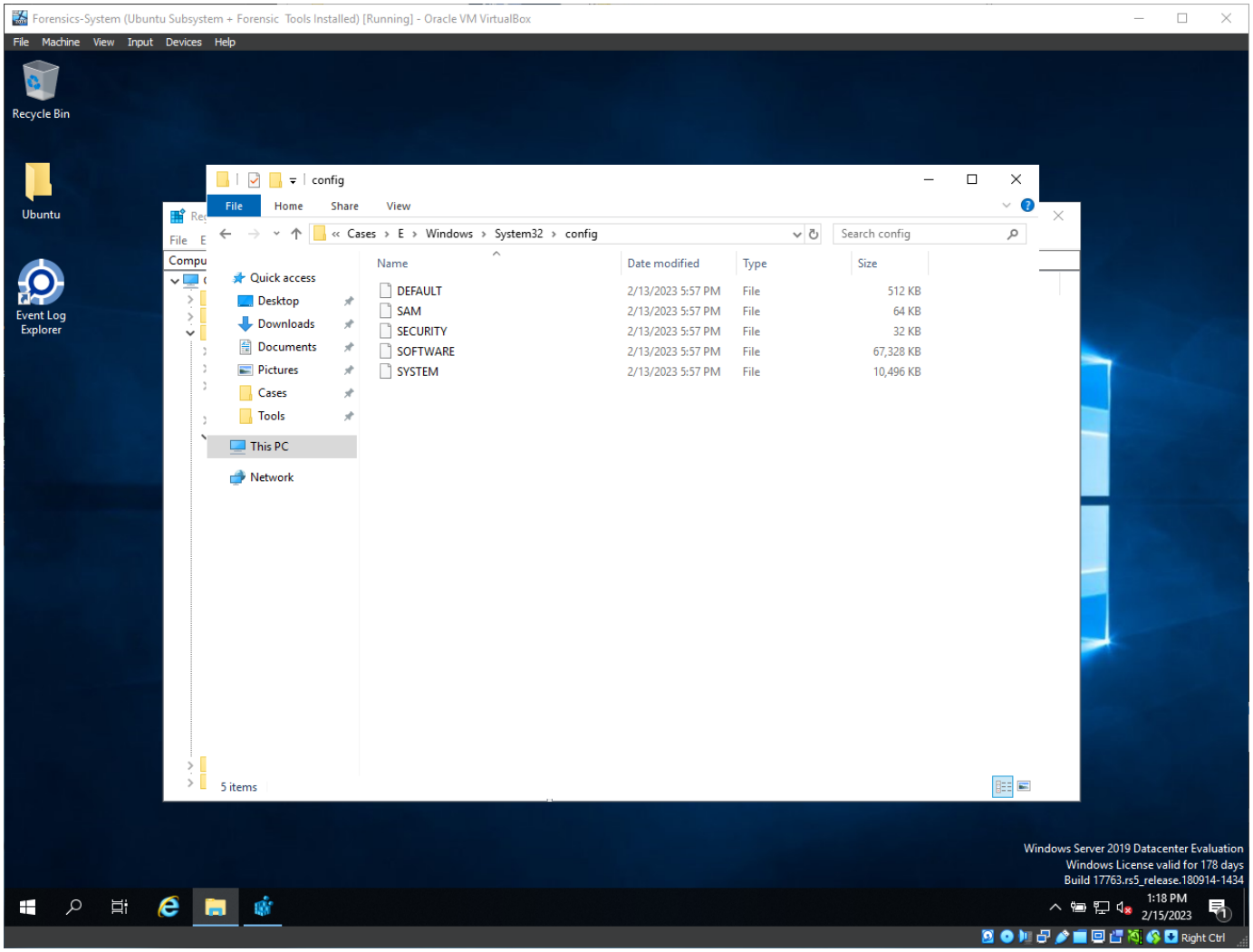
- HKEY_USERS has informations about users of the operating system.
- S, from S-1-5-18 comes from SID (Security Identifier)
- The information comes from WIndows User Profile, for the windows to have a profile , you need to be logged in interactively , with mouse and keyboard and graphical access , in order to have windows create a profile for you.
- For Windows System Settings, these are mostly stored in HKEY_LOCAL_MACHINE.



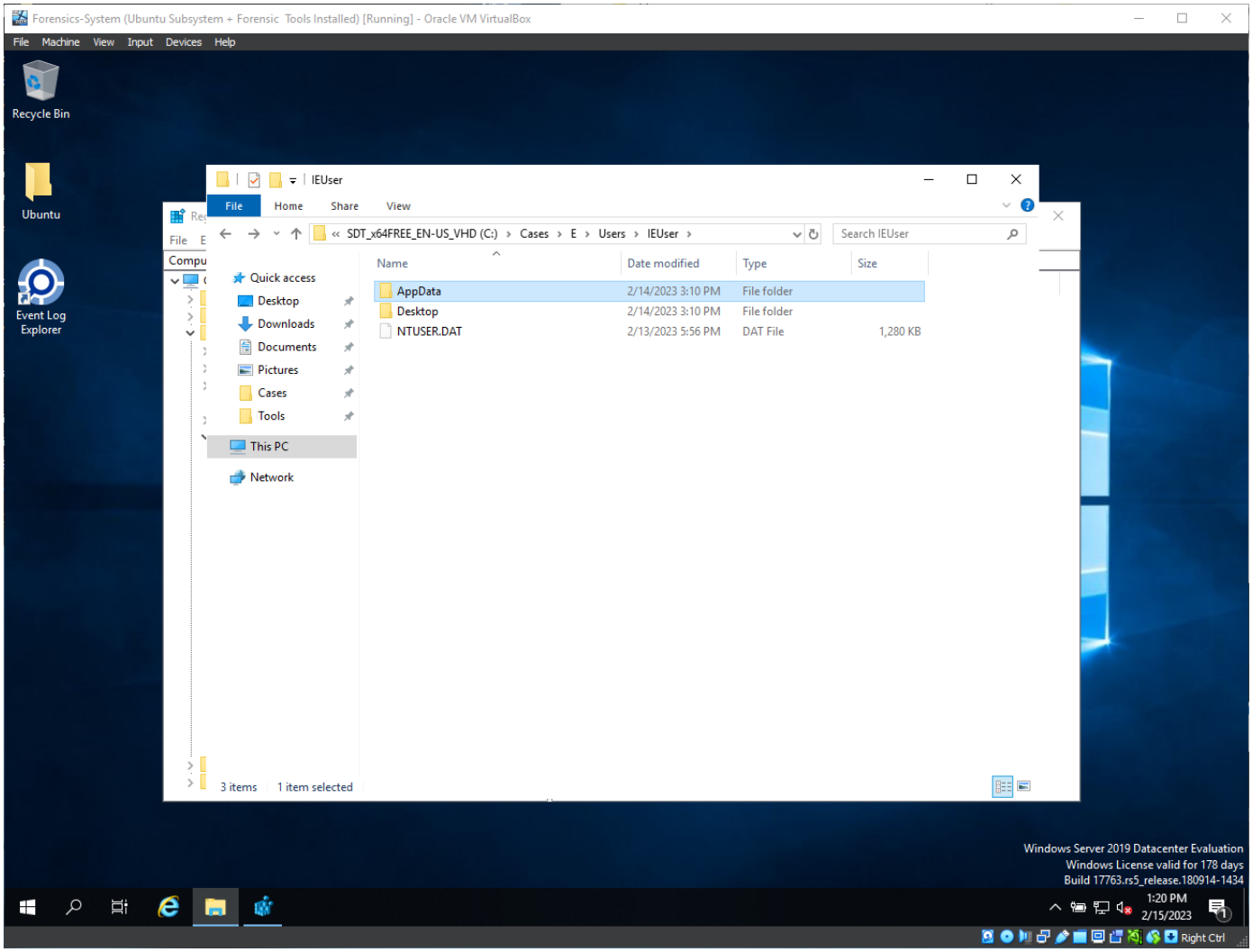
- These files will have an important impact in further forensic analysis.
- In System, is stored information about device drives and service configuration. Important thing to remember, there exists 2 subkeys, ControlSet001 and ControlSet002, Windows will use one of those , in part of its configuration settings.
- We can find the active Control Set from here:

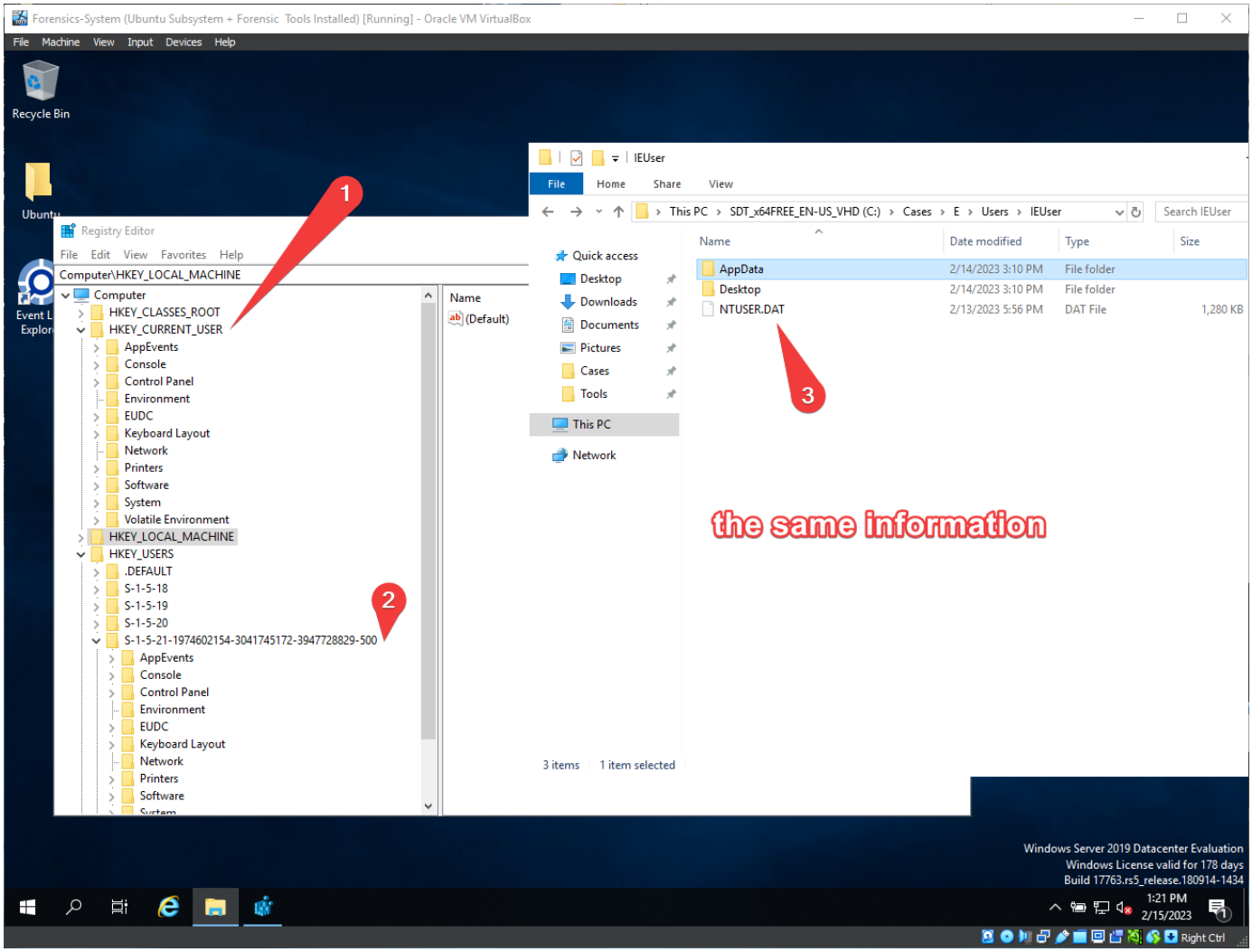


- Registry hives from the evidence:

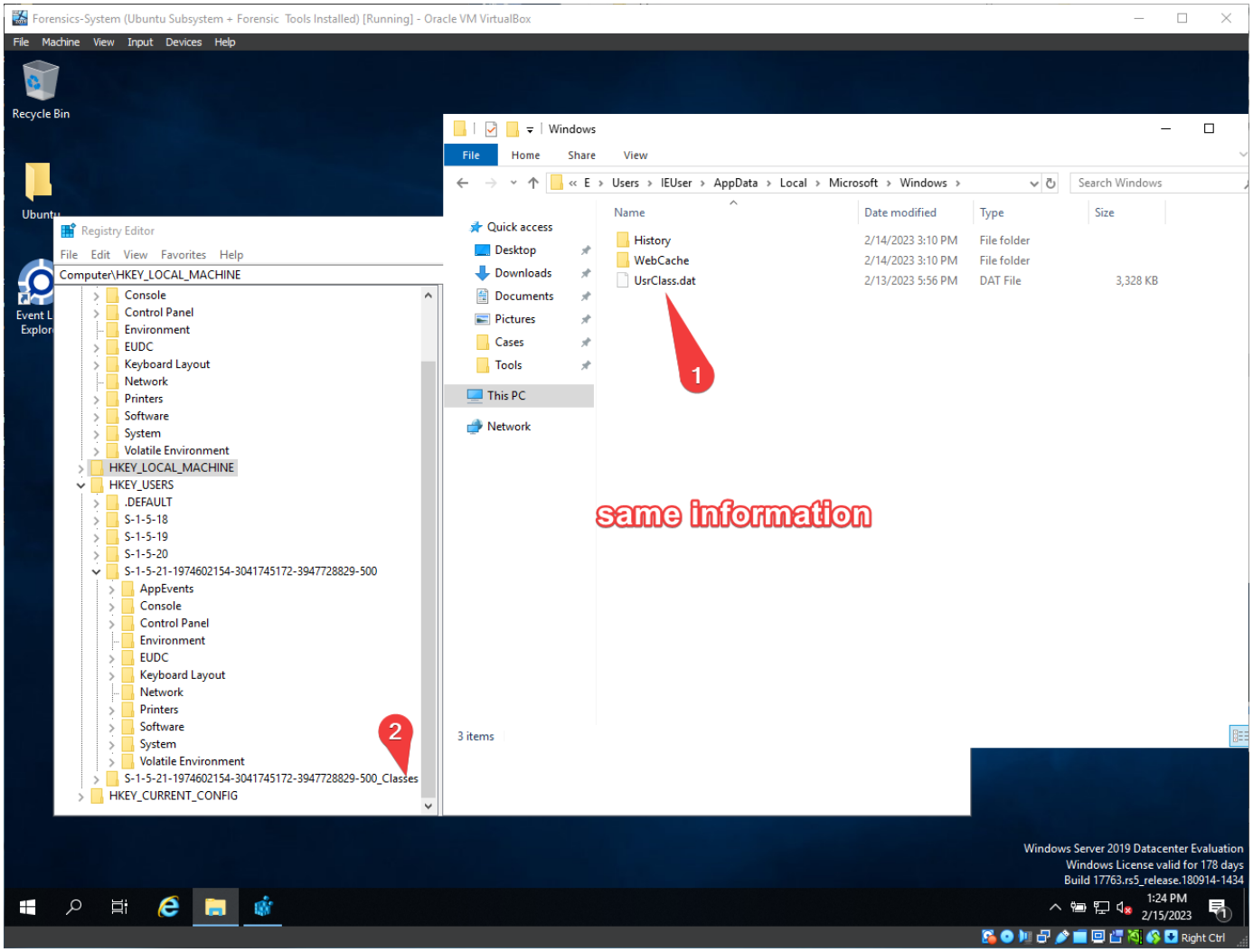


- An user has his particular settings, only if there exists a user profile in the system.
- Location of NTUSER.DAT


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Ubuntu
Event Log Explorer
IEUser
File Home Share View
SDT_x64FREE_EN-US_VHD (C:) › Cases › E › Users › IEUser ›
Search IEUser
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
Size
AppData 2/14/2023 3:10 PM File folder
Desktop 2/14/2023 3:10 PM File folder
NTUSER.DAT 2/13/2023 5:56 PM DAT File 1,280 KB
3 items 1 item selected
Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
1:20 PM
2/15/2023
Right Ctrl

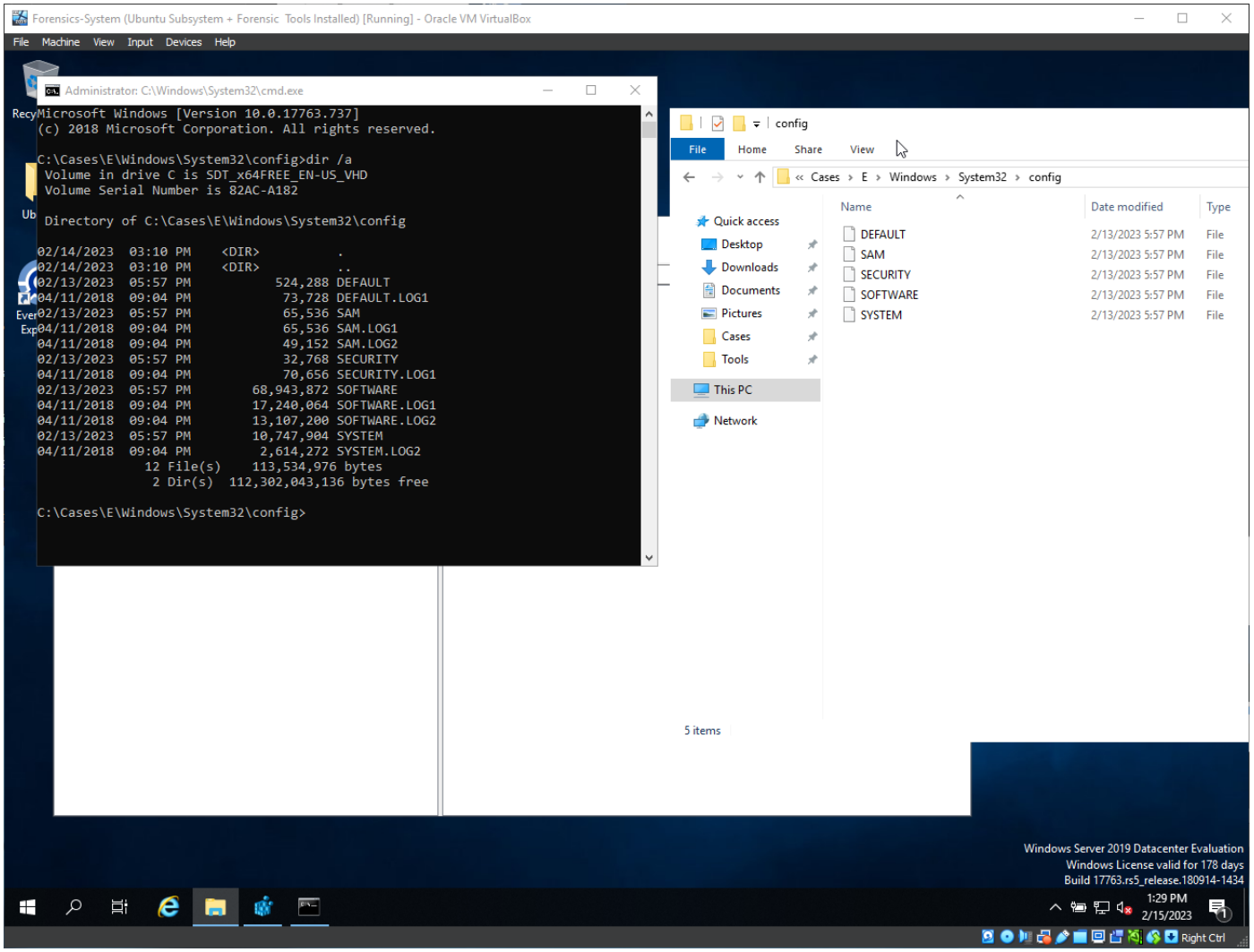


- Another important file for forensic analysis of the user, is users Classes.
- Location of UsrClass.dat



- System registry hives:
  - SAM
  - SECURITY
  - SOFTWARE
  - SYSTEM
- User registry hives:
  - NTUSER.DAT
  - UsrClass.dat

- Transaction logs keeps track of changes and RW to the registry hives only on specific events , for example shutting down the computer.


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Cases\E\Windows\System32\config>dir /a
Volume in drive C is SDT_x64FREE_EN-US_VHD
Volume Serial Number is 82AC-A182
Directory of C:\Cases\E\Windows\System32\config
02/14/2023 03:10 PM <DIR> .
02/14/2023 03:10 PM <DIR> ..
02/13/2023 05:57 PM 524,288 DEFAULT
04/11/2018 09:04 PM 73,728 DEFAULT.LOG1
02/13/2023 05:57 PM 65,536 SAM
04/11/2018 09:04 PM 65,536 SAM.LOG1
04/11/2018 09:04 PM 49,152 SAM.LOG2
02/13/2023 05:57 PM 32,768 SECURITY
04/11/2018 09:04 PM 70,656 SECURITY.LOG1
02/13/2023 05:57 PM 68,943,872 SOFTWARE
04/11/2018 09:04 PM 17,240,064 SOFTWARE.LOG1
04/11/2018 09:04 PM 13,107,200 SOFTWARE.LOG2
02/13/2023 05:57 PM 10,747,904 SYSTEM
04/11/2018 09:04 PM 2,614,272 SYSTEM.LOG2
12 File(s) 113,534,976 bytes
2 Dir(s) 112,302,043,136 bytes free
C:\Cases\E\Windows\System32\config>
config
File Home Share View
« Cases › E › Windows › System32 › config
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
DEFAULT 2/13/2023 5:57 PM File
SAM 2/13/2023 5:57 PM File
SECURITY 2/13/2023 5:57 PM File
SOFTWARE 2/13/2023 5:57 PM File
SYSTEM 2/13/2023 5:57 PM File
5 items
Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
1:29 PM
2/15/2023
Right Ctrl

The following table lists the standard hives and their supporting files.

Registry hive	Supporting files
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav
HKEY_CURRENT_USER	Ntuser.dat, Ntuser.dat.log
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_USERS\.DEFAULT	Default, Default.log, Default.sav

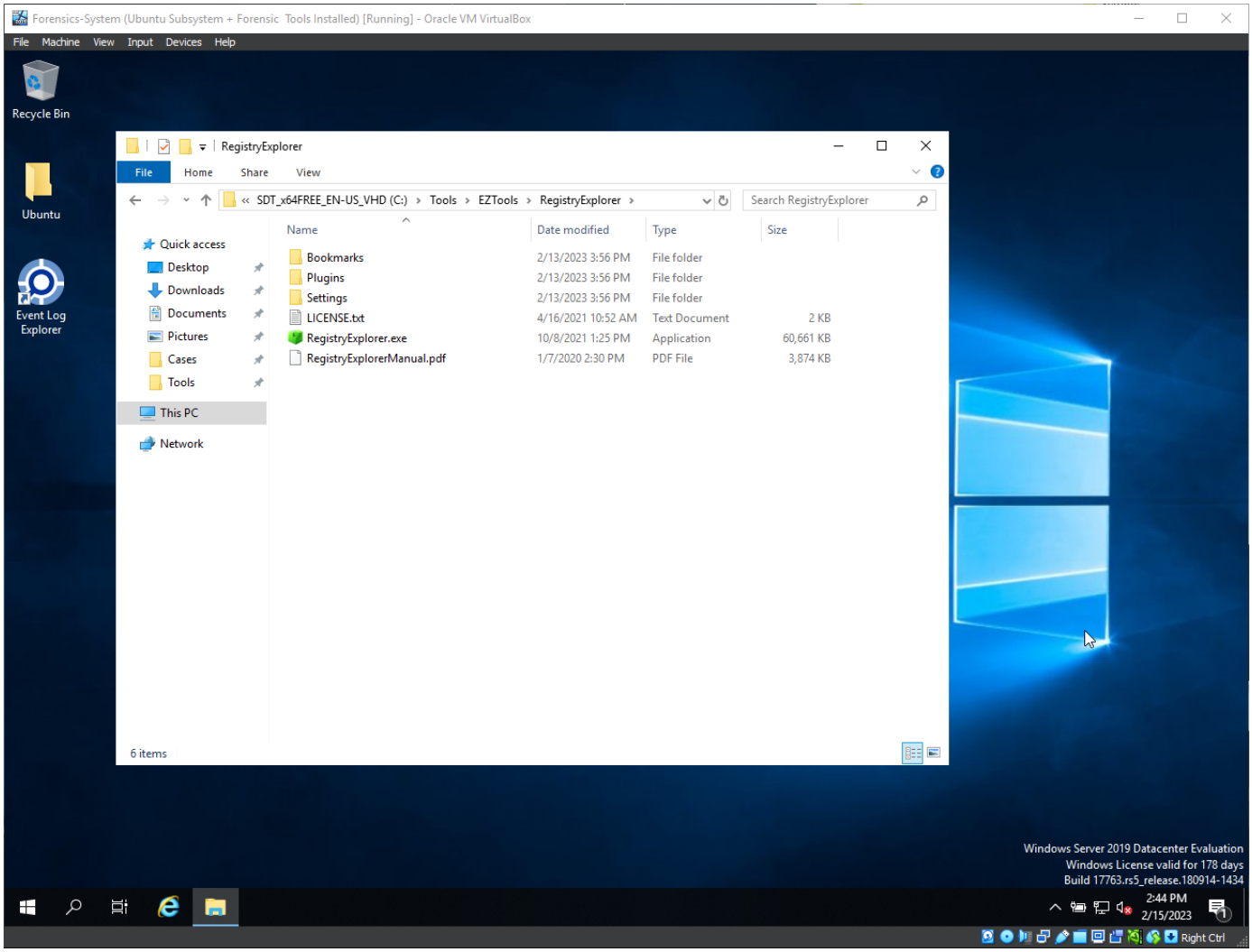
Recommended content

- A registry hive can be “dirty” , that means that the hive hasn’t wrote the latest updates from the transaction logs . If you haven’t turned off the virtual machine , there is a need to merge the transaction logs with the registry hive, in order to create a new one that is updated,.

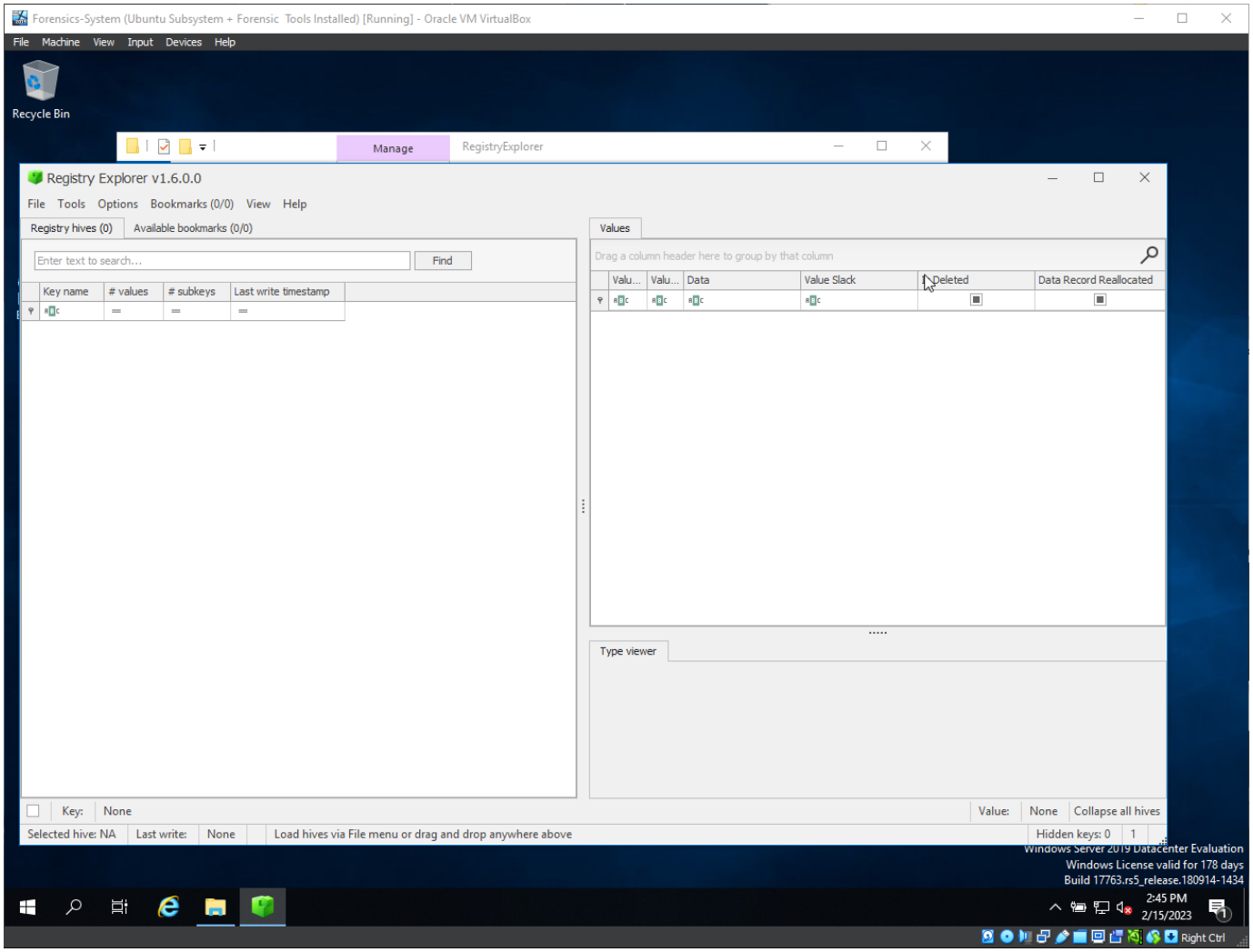
Registry Explorer

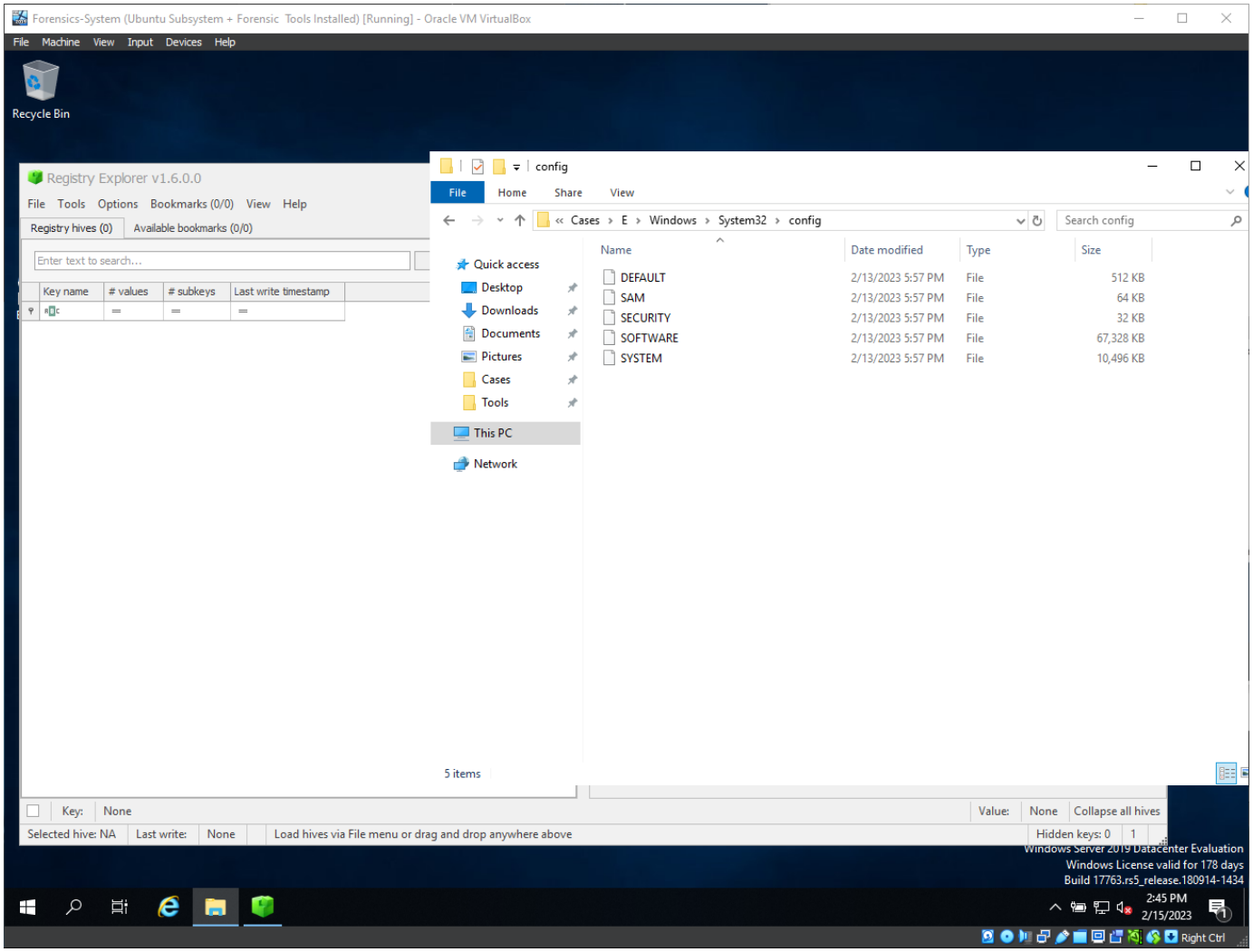
- We will use two tools for parsing registry hives:
  - Registry Explorer
  - RegRipper

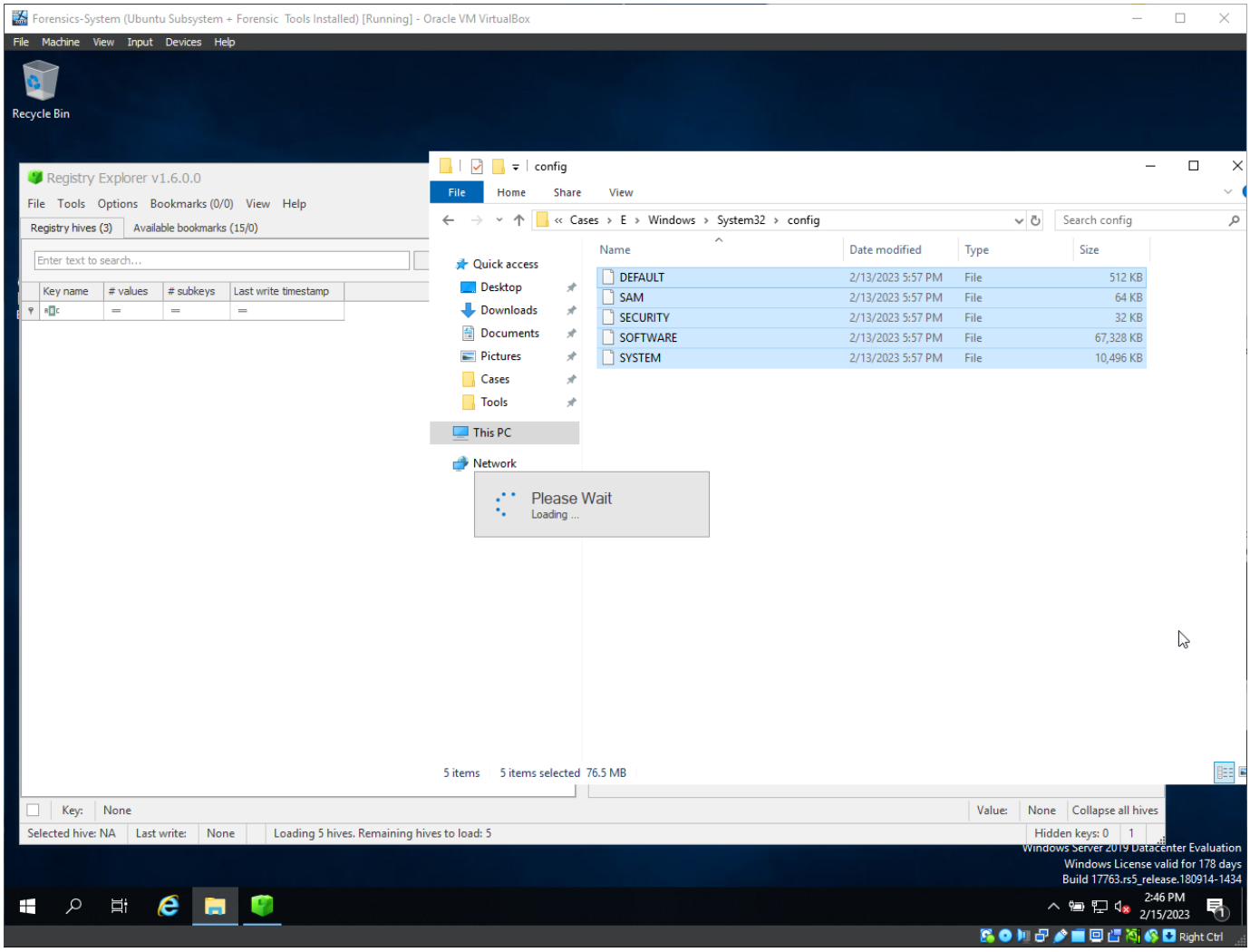
- Registry Explorer:

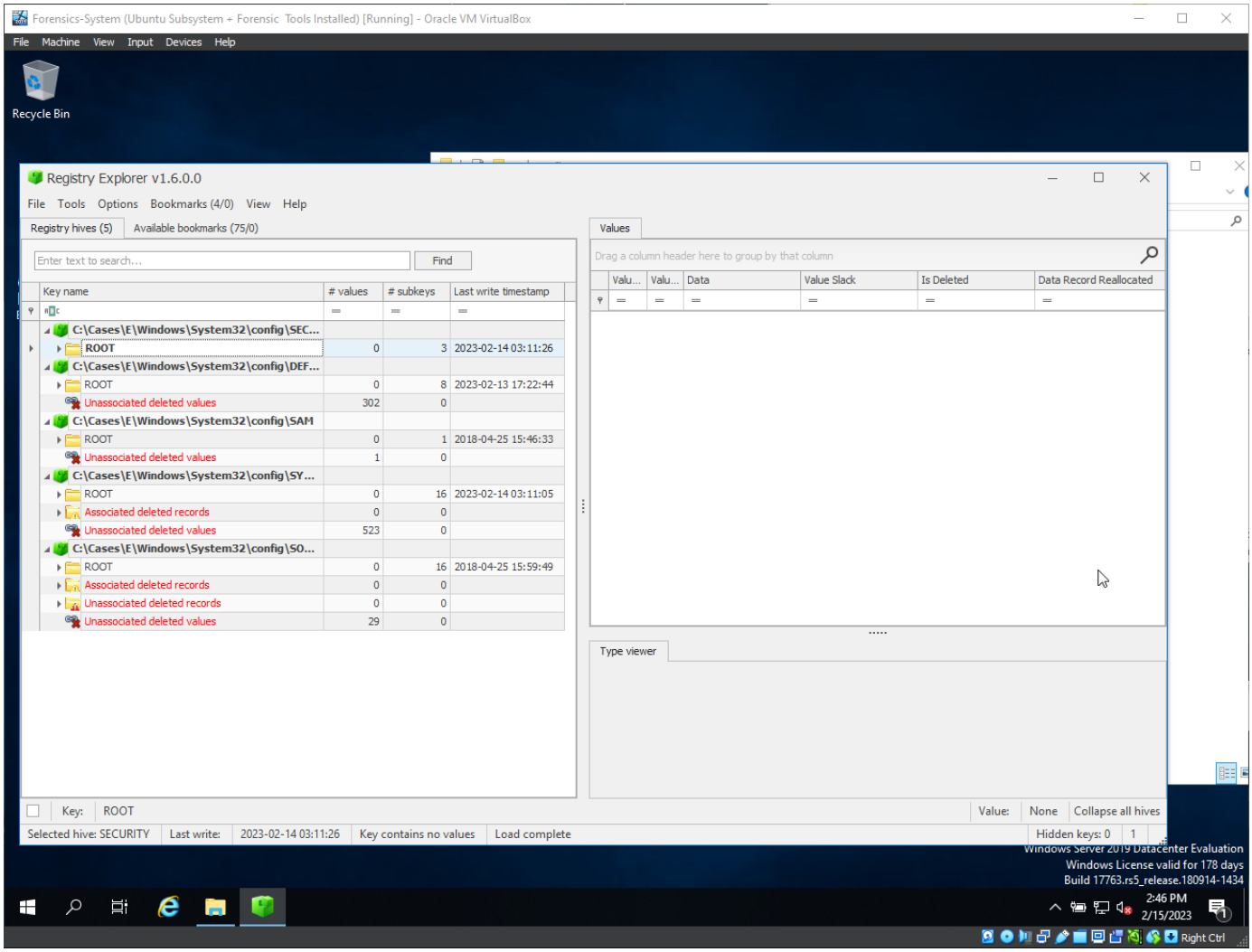


- Drag and drop the system registry files:

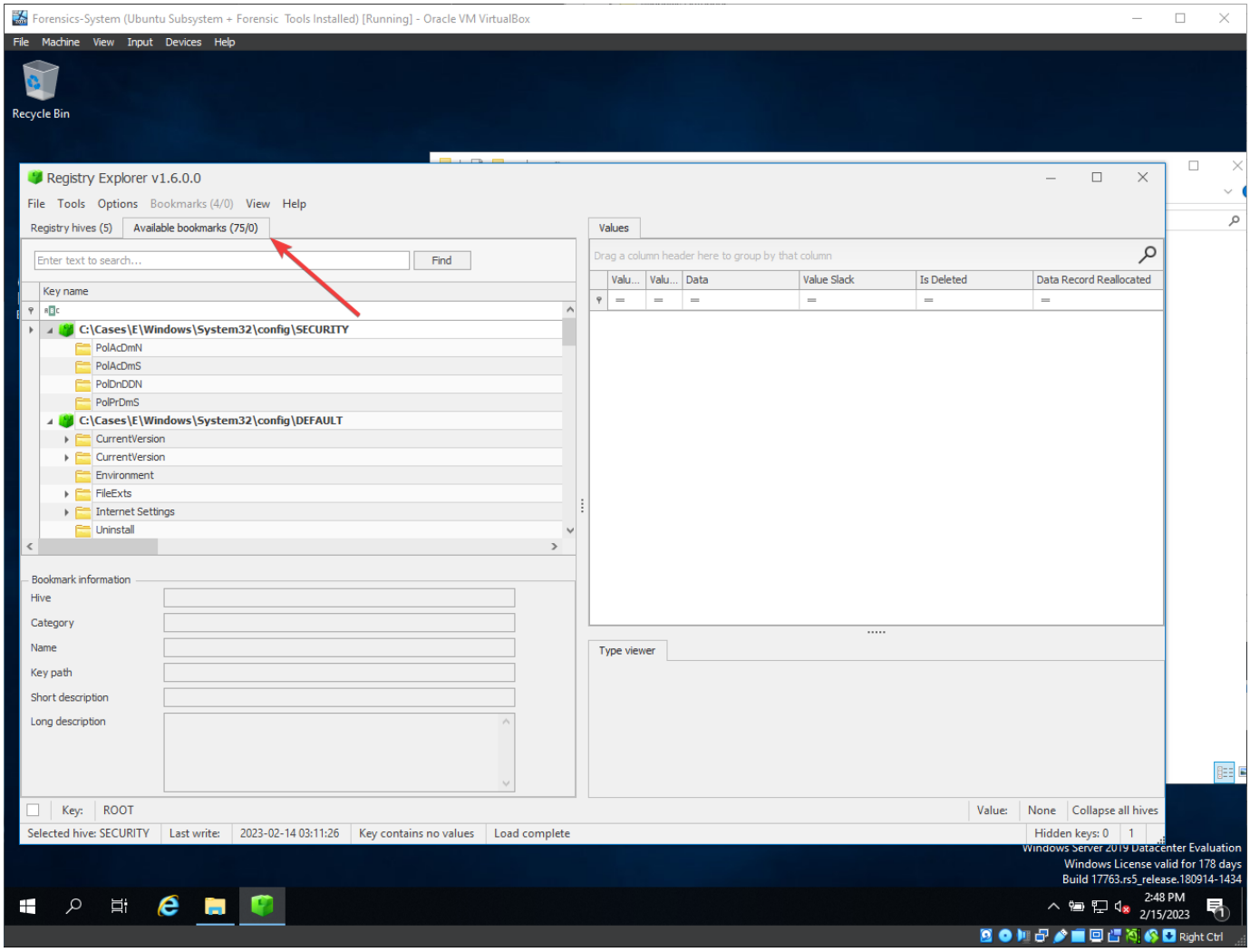

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Manage
RegistryExplorer
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (0/0) View Help
Registry hives (0)
Available bookmarks (0/0)
Enter text to search...
Find
Key name
values
subkeys
Last write timestamp
Values
Drag a column header here to group by that column
Valu...
Valu...
Data
Value Slack
Deleted
Data Record Reallocated
Type viewer
Key: None
Value: None
Collapse all hives
Selected hive: NA
Last write:
None
Load hives via File menu or drag and drop anywhere above
Hidden keys: 0
Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
2:45 PM
2/15/2023
Right Ctrl


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (0/0) View Help
Registry hives (0)
Available bookmarks (0/0)
Enter text to search...
Key name
values
subkeys
Last write timestamp
config
File
Home
Share
View
Cases › E › Windows › System32 › config
Search config
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
Size
DEFAULT 2/13/2023 5:57 PM File 512 KB
SAM 2/13/2023 5:57 PM File 64 KB
SECURITY 2/13/2023 5:57 PM File 32 KB
SOFTWARE 2/13/2023 5:57 PM File 67,328 KB
SYSTEM 2/13/2023 5:57 PM File 10,496 KB
5 items
Key: None
Value: None
Collapse all hives
Selected hive: NA
Last write:
None
Load hives via File menu or drag and drop anywhere above
Hidden keys: 0
Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
2:45 PM
2/15/2023
Right Ctrl


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (0/0) View Help
Registry hives (3) Available bookmarks (15/0)
Enter text to search...
Key name # values # subkeys Last write timestamp
config
File Home Share View
Cases › E › Windows › System32 › config
Search config
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name Date modified Type Size
DEFAULT 2/13/2023 5:57 PM File 512 KB
SAM 2/13/2023 5:57 PM File 64 KB
SECURITY 2/13/2023 5:57 PM File 32 KB
SOFTWARE 2/13/2023 5:57 PM File 67,328 KB
SYSTEM 2/13/2023 5:57 PM File 10,496 KB
Please Wait
Loading ...
5 items 5 items selected 76.5 MB
Key: None
Value: None Collapse all hives
Selected hive: NA Last write: None
Loading 5 hives. Remaining hives to load: 5
Hidden keys: 0 1
Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
2:46 PM
2/15/2023
Right Ctrl



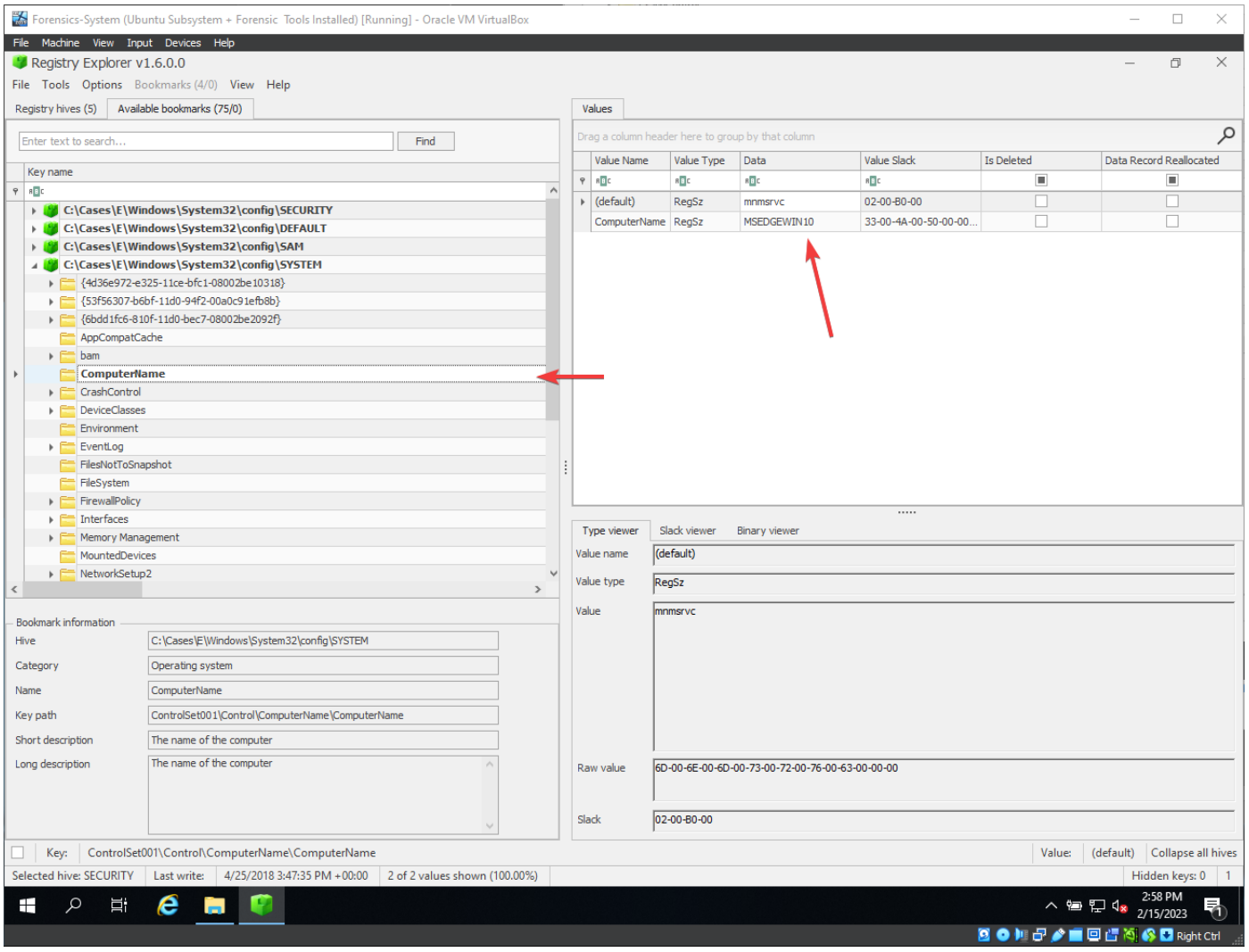
- For better structure, there exists bookmarks:



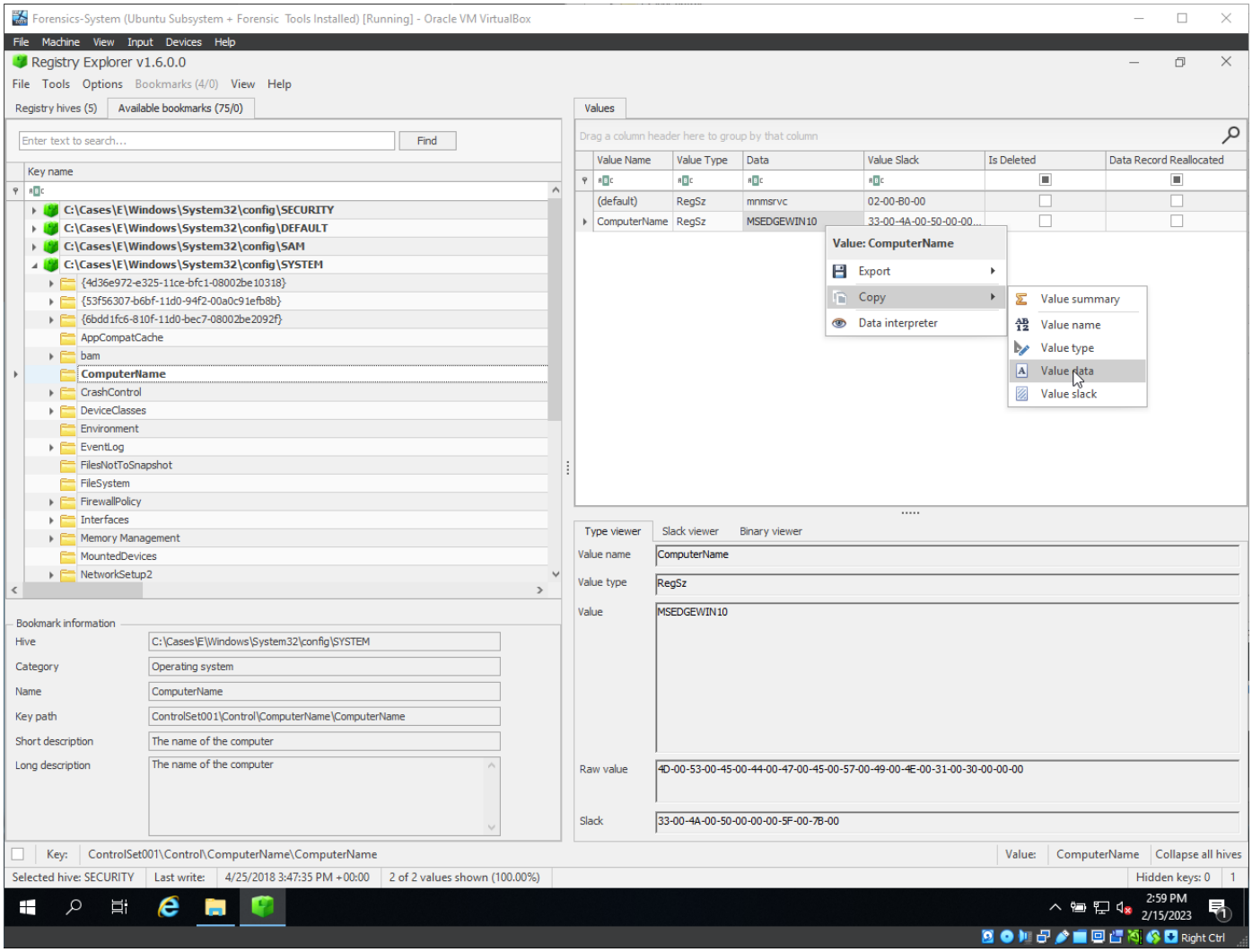
Starting Investigation

- We will start the investigation by searching for basic information about the system, for each information requested, there exists a location where you can find the information:
- Find System Information:
    - Computer name
        - HKLM\System\CurrentControlSet\Control\Computer name\
    - Windows Version
        - HKLM\Software\Microsoft\Windows NT\Currentversion\
    - Timezone

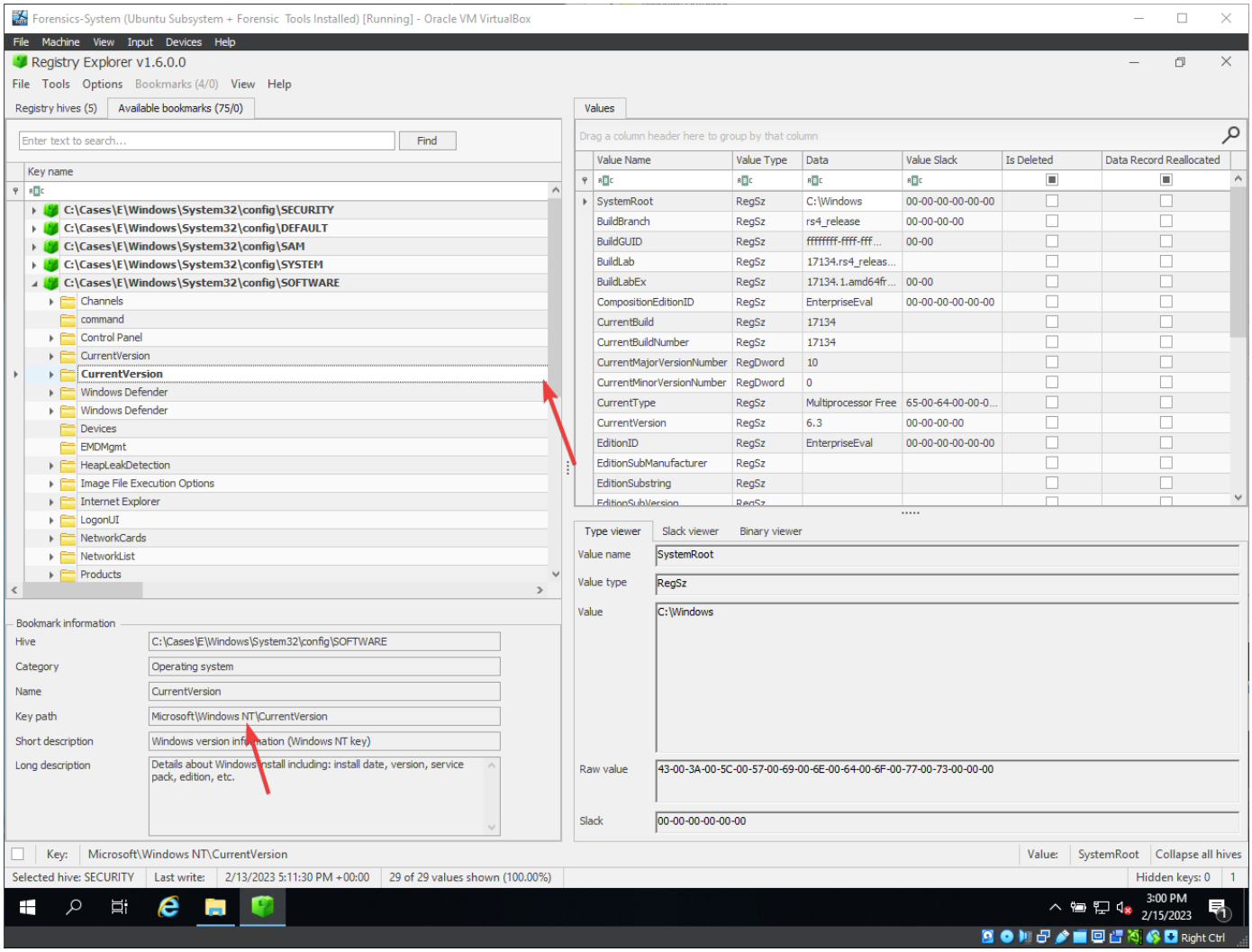
        - HKLM\System\CurrentControlSet\Control\TimeZone Information\
    - Network Information
        - HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{interface-name}
    - Shutdown time
        - HKLM\System\ControlSet001\Control\Windows\ShutdownTime
    - Defender settings
        - HKLM\Software\Microsoft\Windows Defender\
- Computer name:



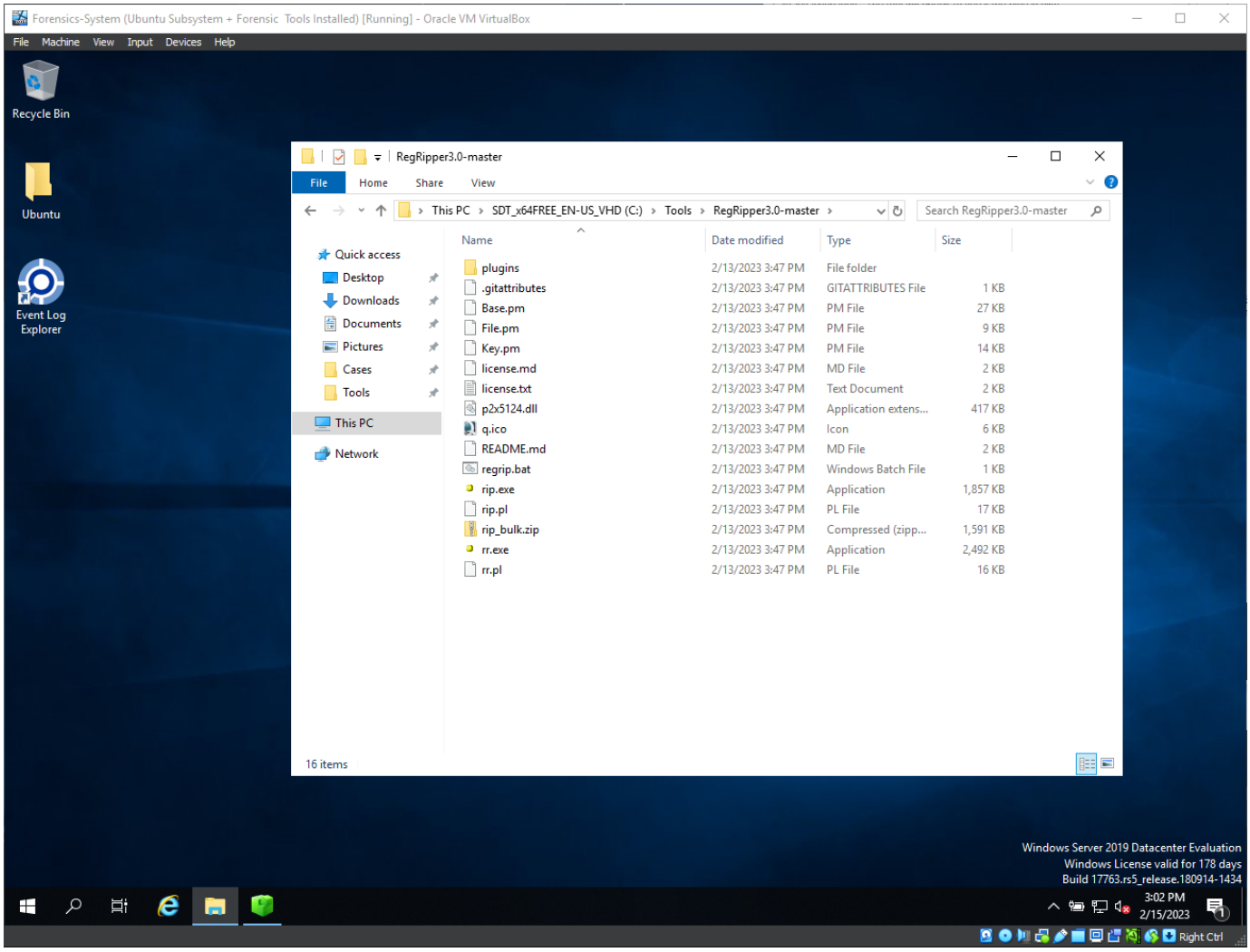
- You can copy and paste the data:



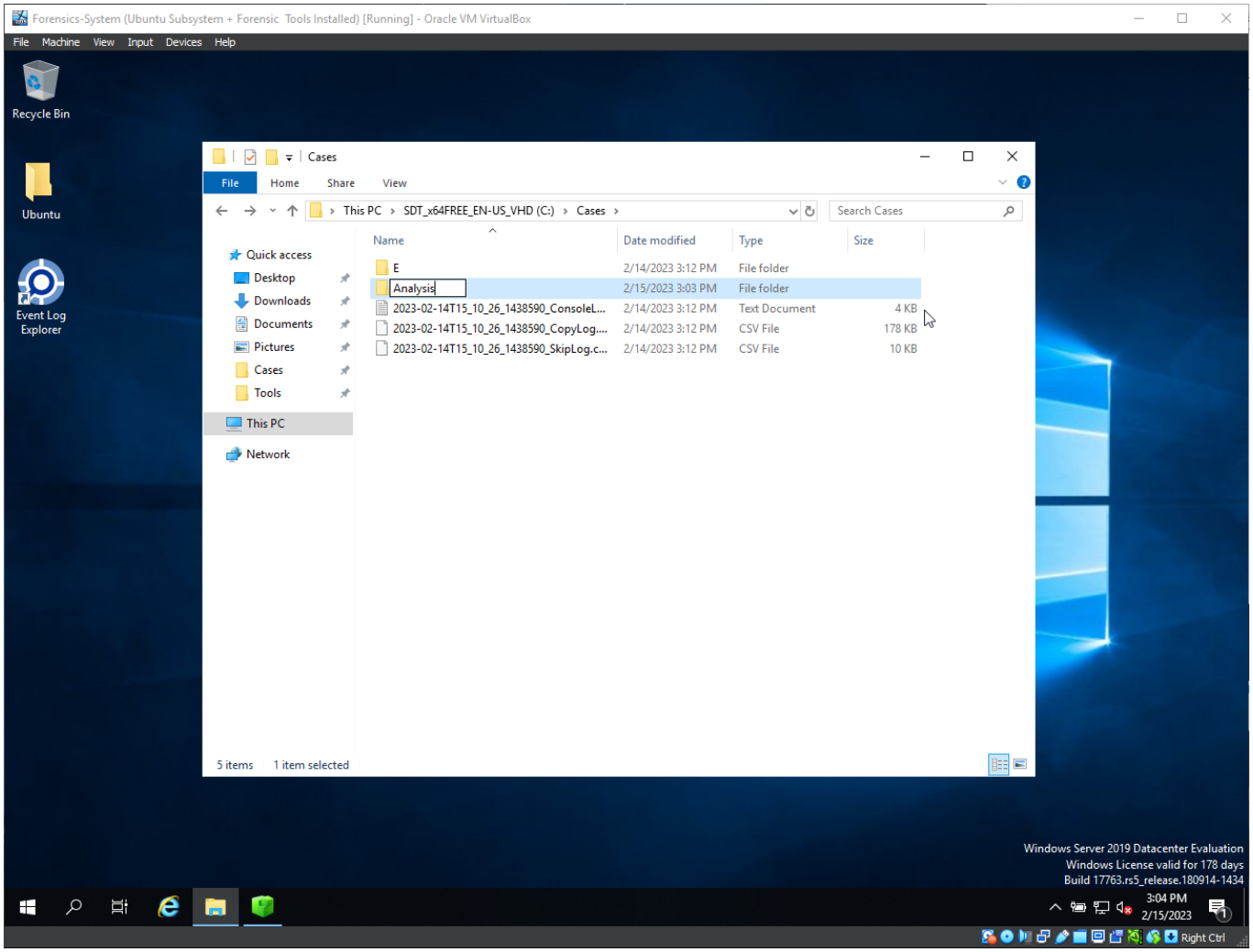
- Answer : MSEDGEWIN10
- Windows Version:



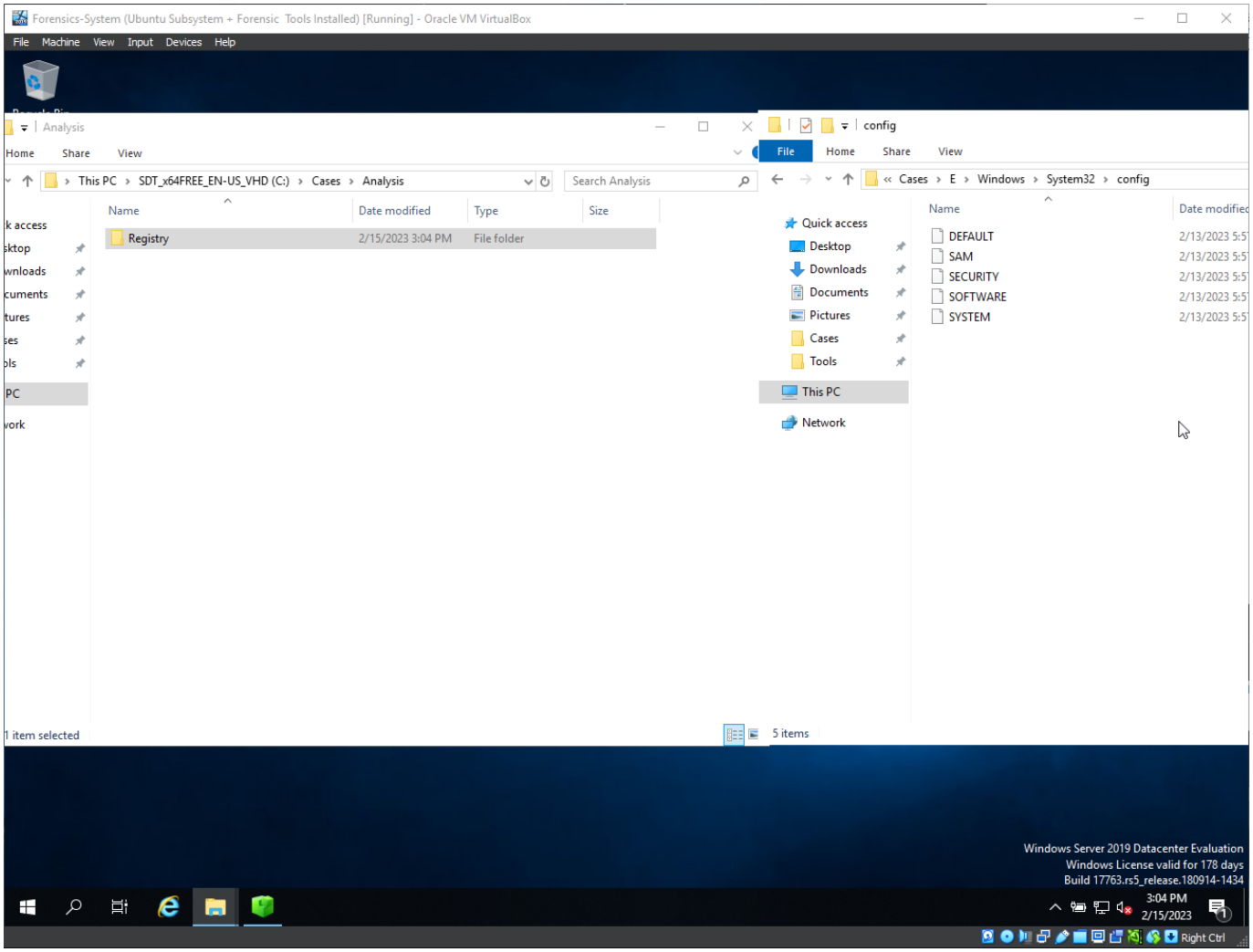
- For easier transfer of evidence data, we will use RegRipper because of easier text structure:

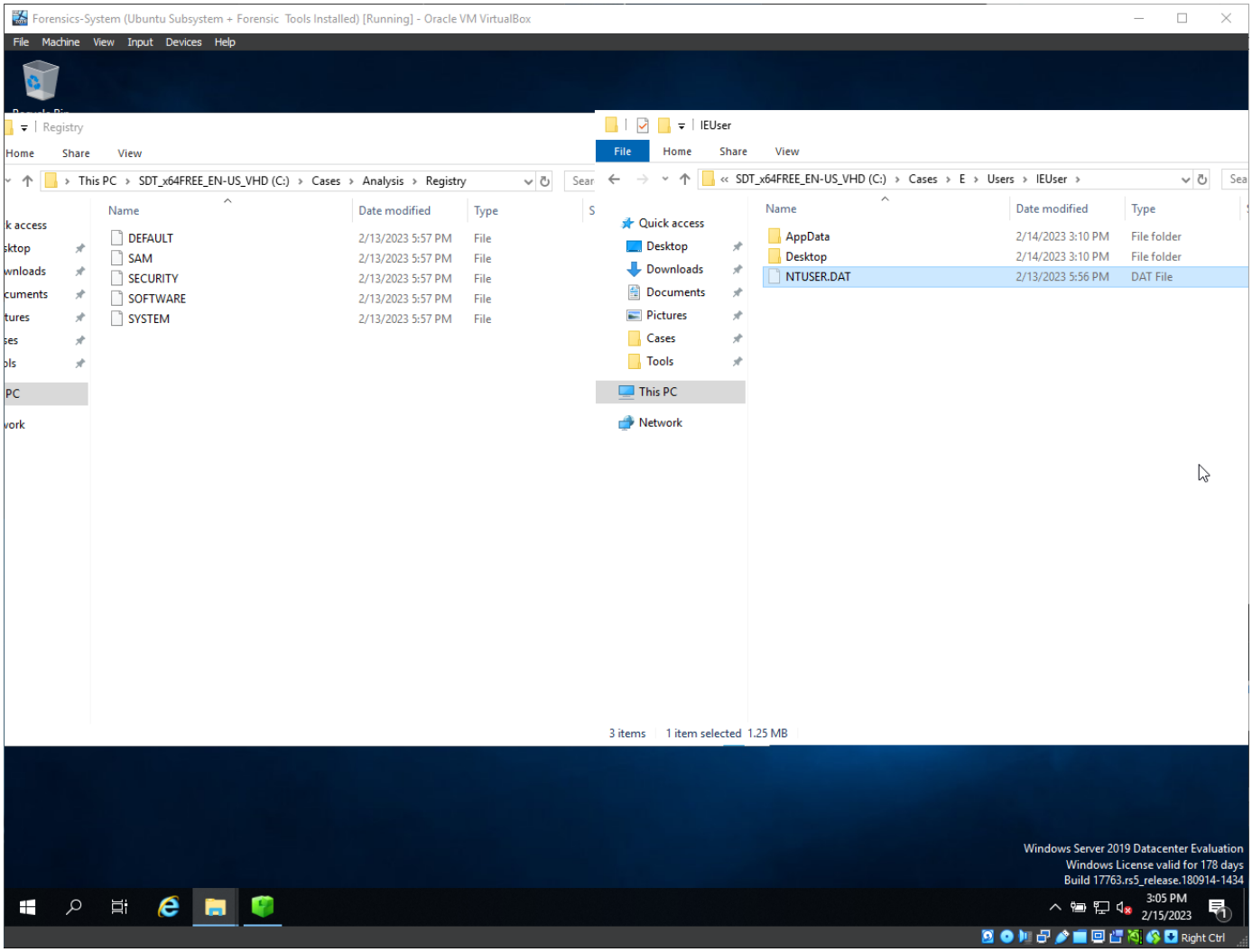


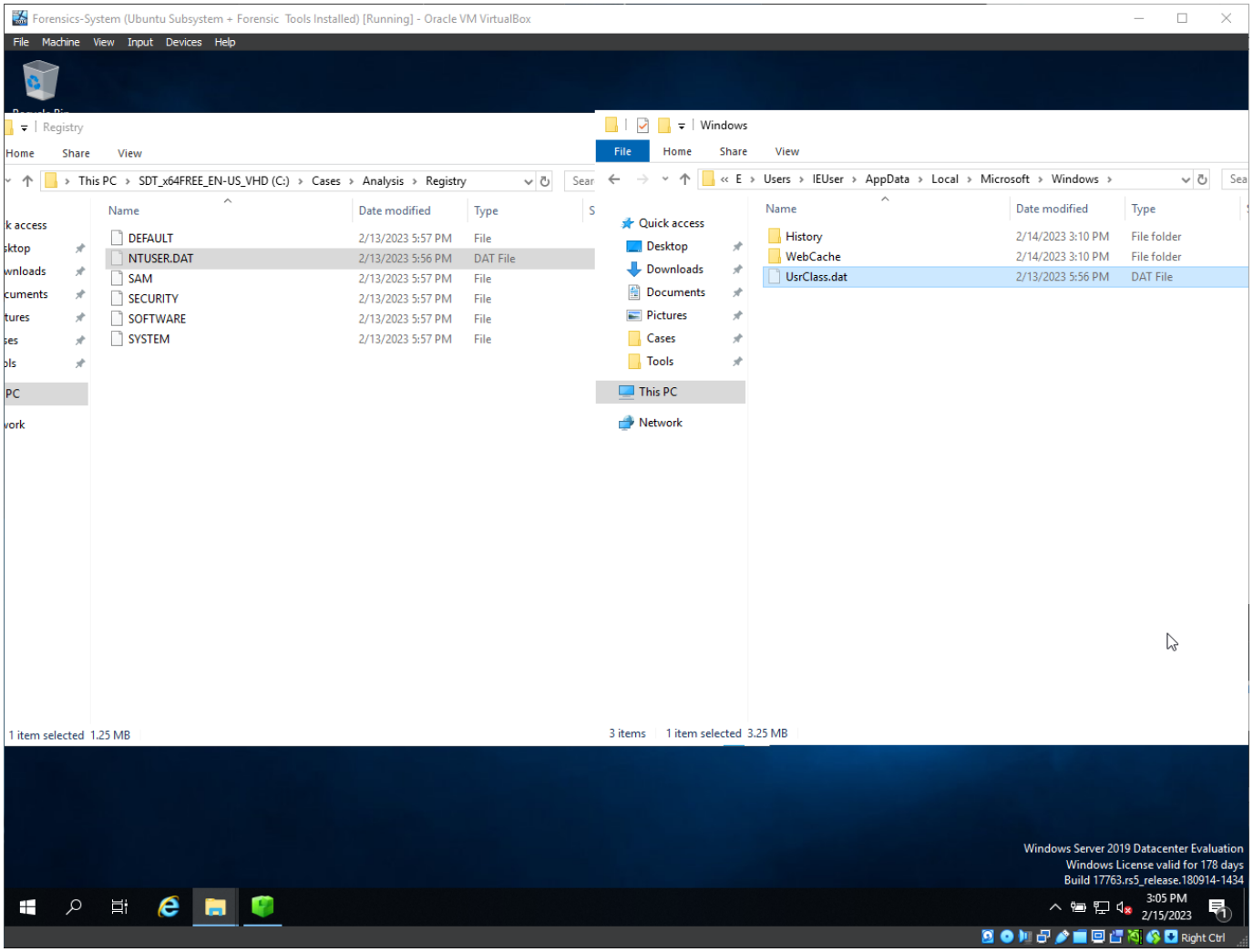
- Create a folder for data analysis , under C:\Cases for gathering information purposes:



- Copy registry system hives and user data hives:

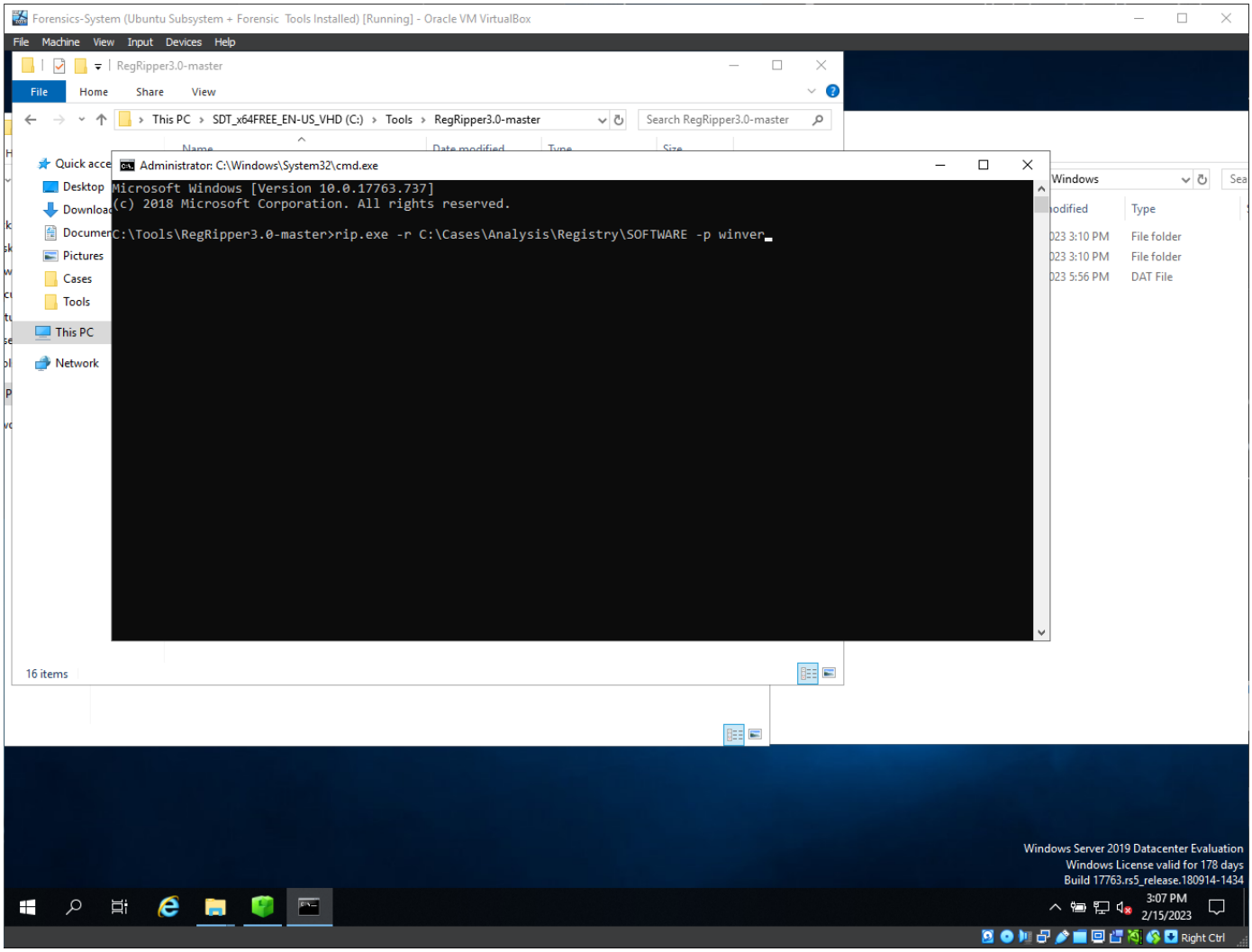

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Analysis
Home Share View
This PC › SDT_x64FREE_EN-US_VHD (C:) › Cases › Analysis
Search Analysis
Name Date modified Type Size
Registry 2/15/2023 3:04 PM File folder
1 item selected
config
File Home Share View
« Cases › E › Windows › System32 › config
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name Date modified
DEFAULT 2/13/2023 5:5
SAM 2/13/2023 5:5
SECURITY 2/13/2023 5:5
SOFTWARE 2/13/2023 5:5
SYSTEM 2/13/2023 5:5
5 items
Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
3:04 PM
2/15/2023
Right Ctrl

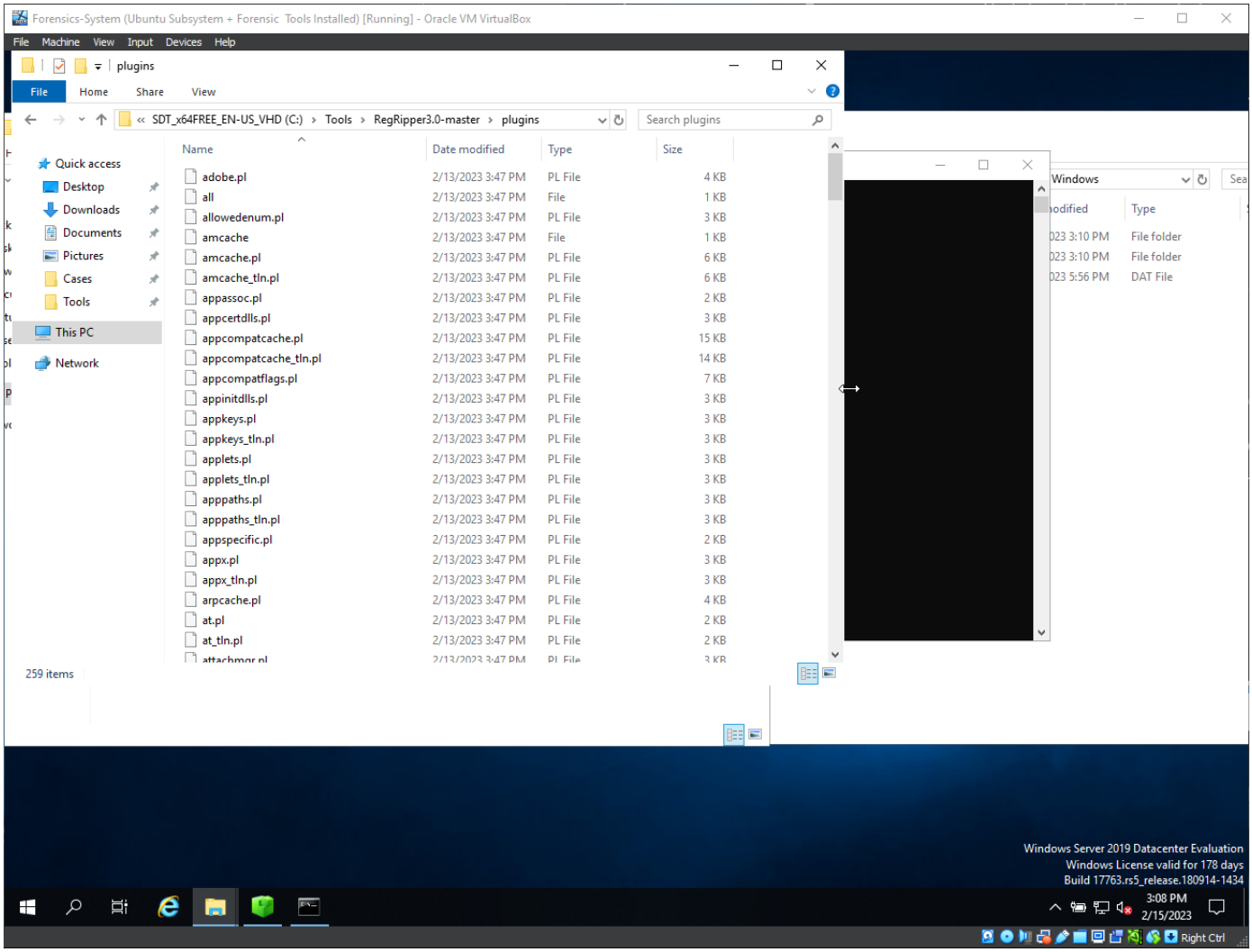

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Registry
Home Share View
This PC › SDT_x64FREE_EN-US_VHD (C:) › Cases › Analysis › Registry
Name Date modified Type
DEFAULT 2/13/2023 5:57 PM File
SAM 2/13/2023 5:57 PM File
SECURITY 2/13/2023 5:57 PM File
SOFTWARE 2/13/2023 5:57 PM File
SYSTEM 2/13/2023 5:57 PM File
IEUser
File Home Share View
SDT_x64FREE_EN-US_VHD (C:) › Cases › E › Users › IEUser
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name Date modified Type
AppData 2/14/2023 3:10 PM File folder
Desktop 2/14/2023 3:10 PM File folder
NTUSER.DAT 2/13/2023 5:56 PM DAT File
3 items 1 item selected 1.25 MB
Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
3:05 PM
2/15/2023
Right Ctrl

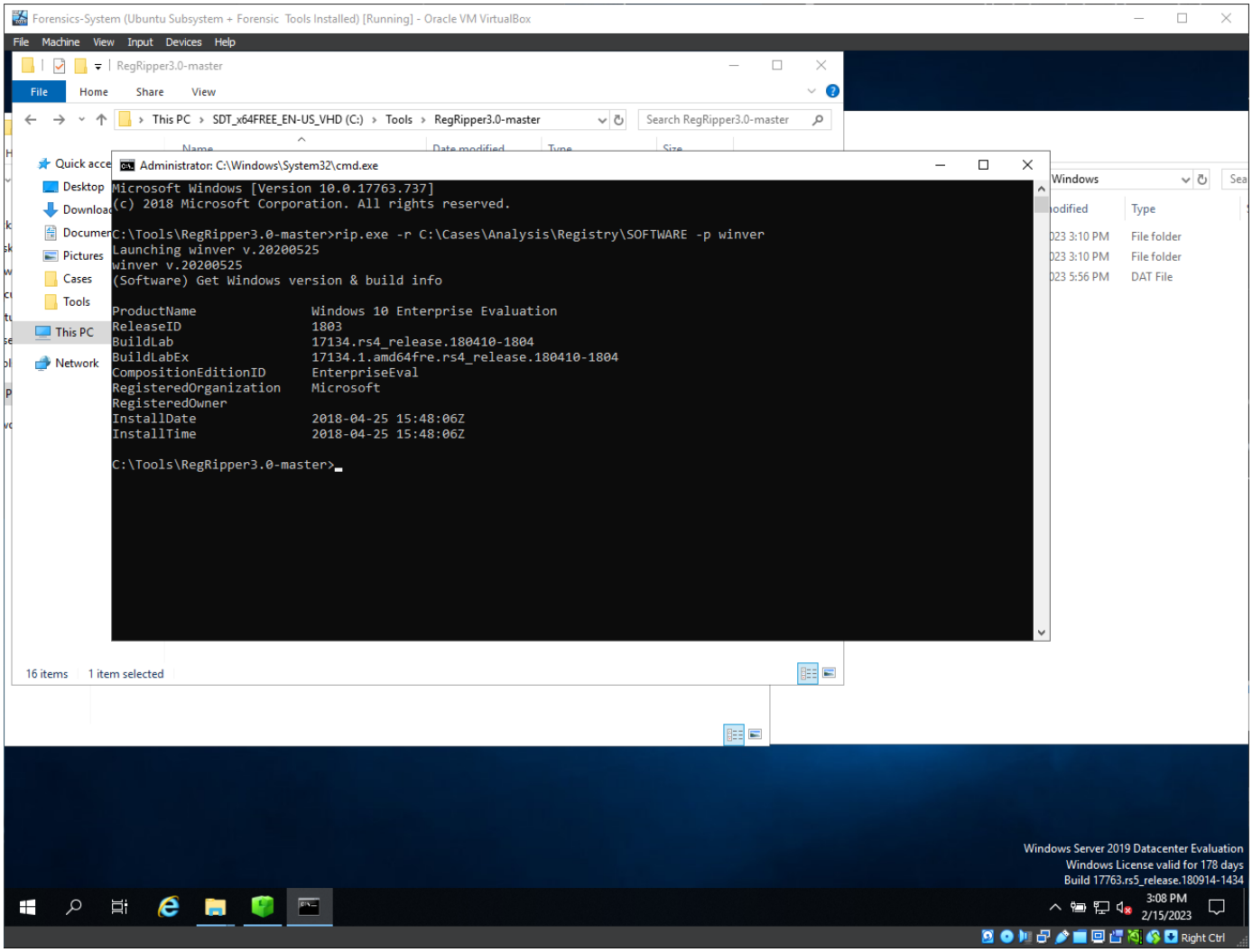


RegRipper

- Using regripper for Windows Information, -p comes from the plugin used by the application to search for windows version, there are multiple plugins that this software uses for data gathering:


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
RegRipper3.0-master
File Home Share View
This PC › SDT_x64FREE_EN-US_VHD (C:) › Tools › RegRipper3.0-master
Search RegRipper3.0-master
Quick acce
Desktop
Downloa
Documen
Pictures
Cases
Tools
This PC
Network
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Tools\RegRipper3.0-master>rip.exe -r C:\Cases\Analysis\Registry\SOFTWARE -p winver
Windows
Type
023 3:10 PM File folder
023 3:10 PM File folder
023 5:56 PM DAT File
16 items
Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
3:07 PM
2/15/2023
Right Ctrl


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
plugins
File Home Share View
SDT_x64FREE_EN-US_VHD (C:) › Tools › RegRipper3.0-master › plugins
Search plugins
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
Size
adobe.pl 2/13/2023 3:47 PM PL File 4 KB
all 2/13/2023 3:47 PM File 1 KB
allowedenum.pl 2/13/2023 3:47 PM PL File 3 KB
amcache 2/13/2023 3:47 PM File 1 KB
amcache.pl 2/13/2023 3:47 PM PL File 6 KB
amcache_tln.pl 2/13/2023 3:47 PM PL File 6 KB
appassoc.pl 2/13/2023 3:47 PM PL File 2 KB
appcertdlls.pl 2/13/2023 3:47 PM PL File 3 KB
appcompatcache.pl 2/13/2023 3:47 PM PL File 15 KB
appcompatcache_tln.pl 2/13/2023 3:47 PM PL File 14 KB
appcompatflags.pl 2/13/2023 3:47 PM PL File 7 KB
appinitdlls.pl 2/13/2023 3:47 PM PL File 3 KB
appkeys.pl 2/13/2023 3:47 PM PL File 3 KB
appkeys_tln.pl 2/13/2023 3:47 PM PL File 3 KB
applets.pl 2/13/2023 3:47 PM PL File 3 KB
applets_tln.pl 2/13/2023 3:47 PM PL File 3 KB
apppaths.pl 2/13/2023 3:47 PM PL File 3 KB
apppaths_tln.pl 2/13/2023 3:47 PM PL File 3 KB
appspecific.pl 2/13/2023 3:47 PM PL File 2 KB
appx.pl 2/13/2023 3:47 PM PL File 3 KB
appx_tln.pl 2/13/2023 3:47 PM PL File 3 KB
arpcache.pl 2/13/2023 3:47 PM PL File 4 KB
at.pl 2/13/2023 3:47 PM PL File 2 KB
at_tln.pl 2/13/2023 3:47 PM PL File 2 KB
259 items
Windows
Type
File folder
File folder
DAT File
Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
3:08 PM
2/15/2023
Right Ctrl



- Answer :

ProductName Windows 10 Enterprise Evaluation

ReleaseID 1803

BuildLab 17134.rs4_release.180410-1804

BuildLabEx 17134.1.amd64fre.rs4_release.180410-1804

CompositionEditionID EnterpriseEval

RegisteredOrganization Microsoft

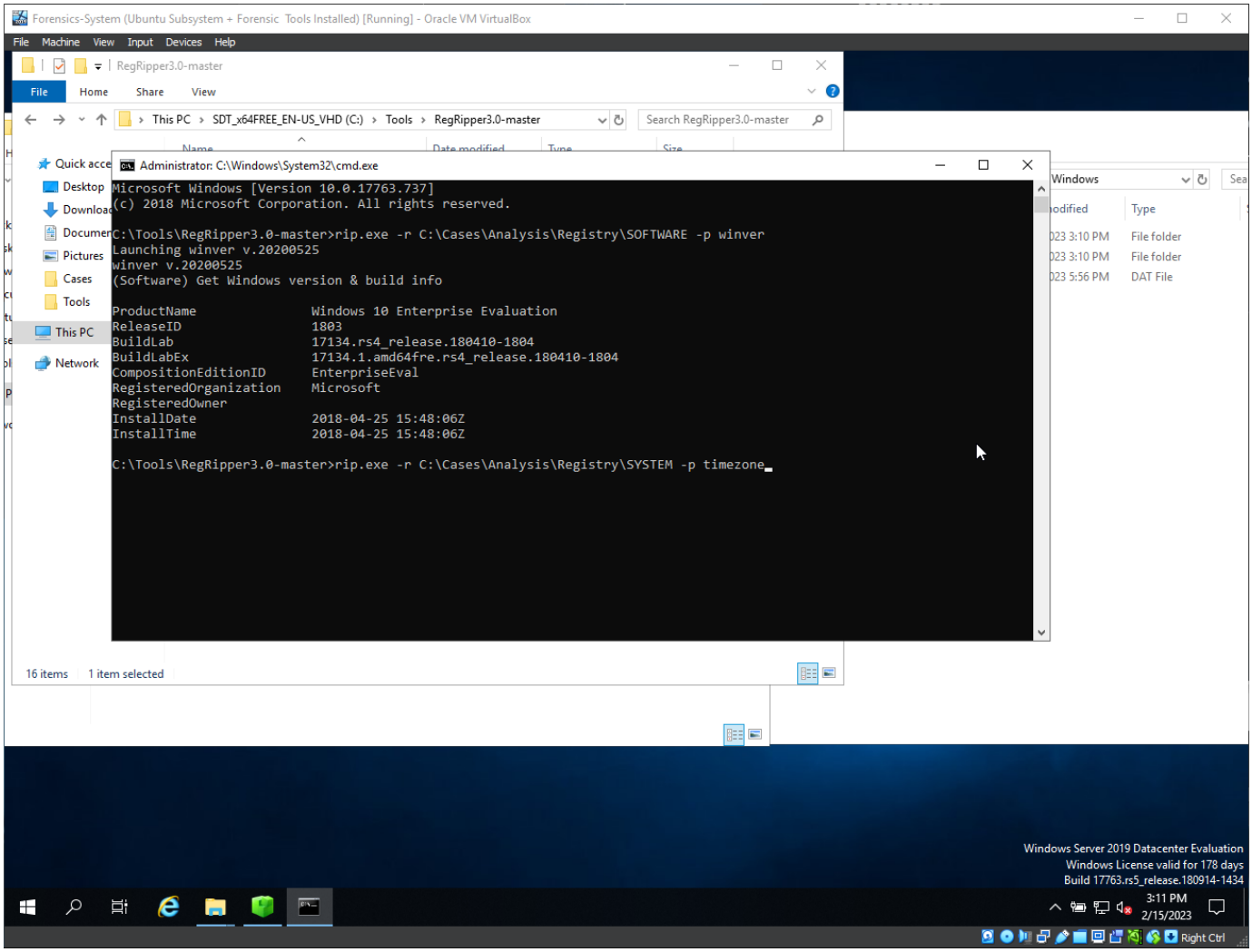
RegisteredOwner

InstallDate 2018-04-25 15:48:06Z

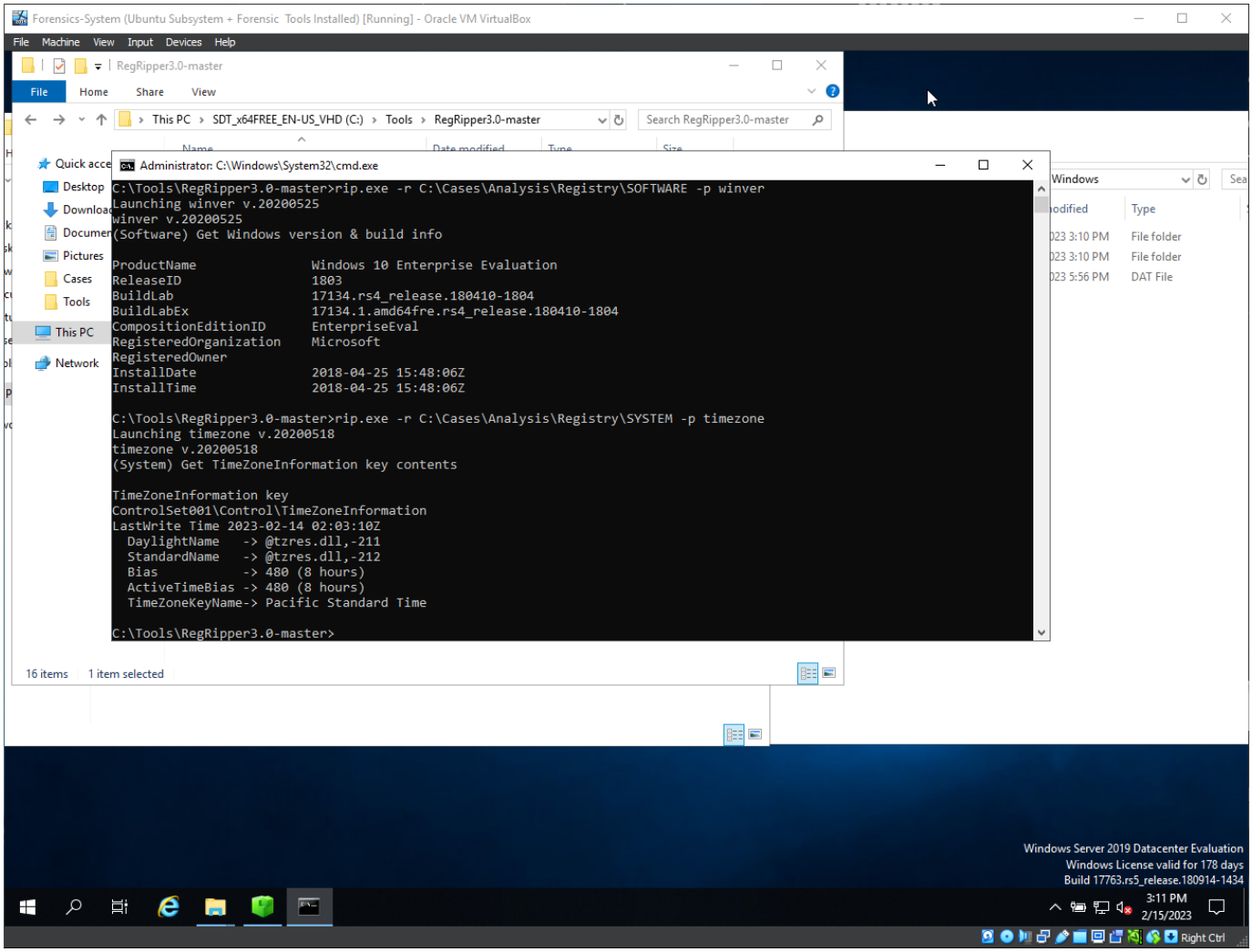
InstallTime 2018-04-25 15:48:06Z

- You can search for different kinds of plugins that regripper uses for parsing at : https://hexacorn.com/tools/3r.html

- Timezone:



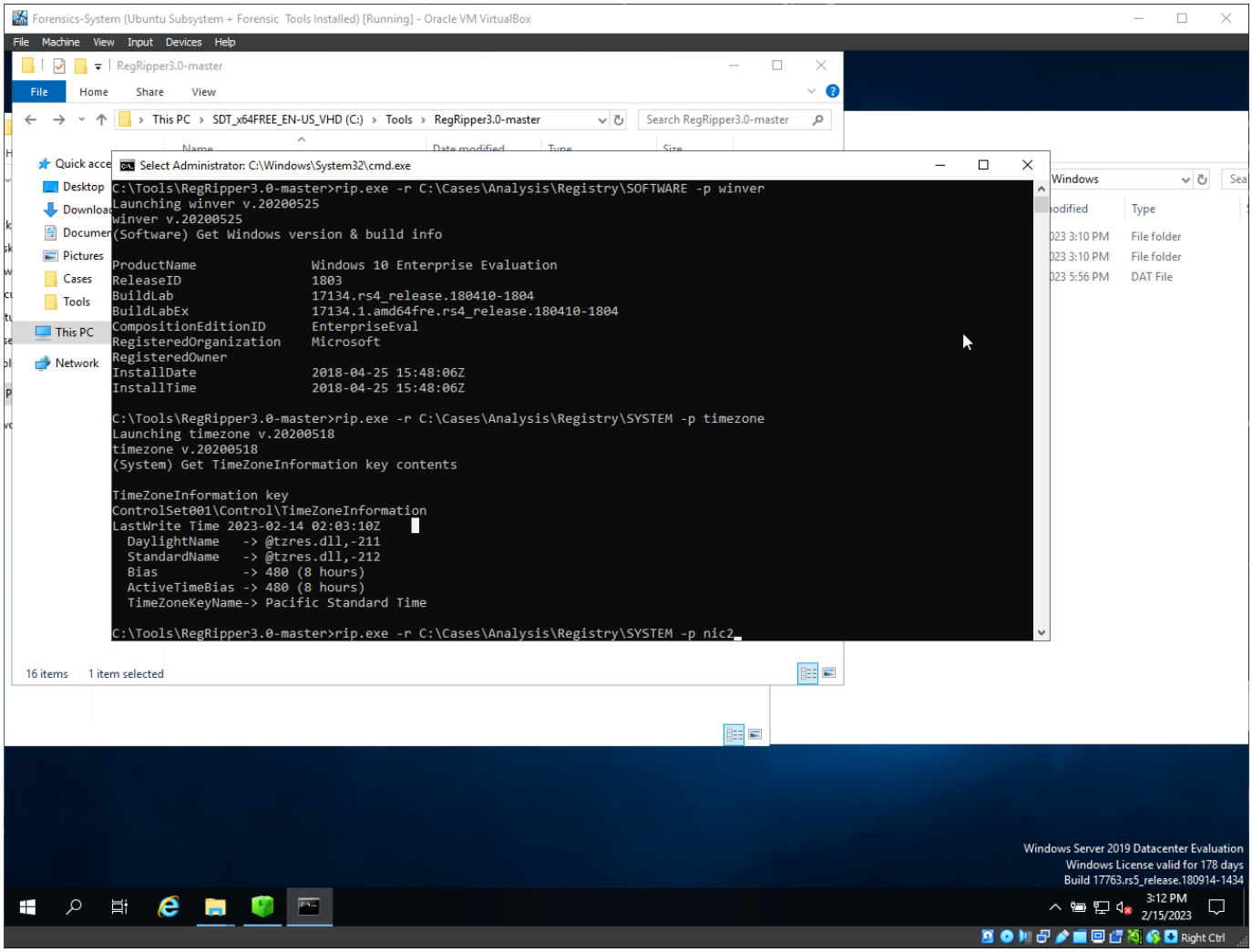
- Pay attention at details, the registry is changed from SOFTWARE to SYSTEM.



- Answer :

TimeZoneKeyName-> Pacific Standard Time

- Network Information:



- Answer :

DhcpIPAddress 10.0.2.15

DhcpSubnetMask 255.255.255.0

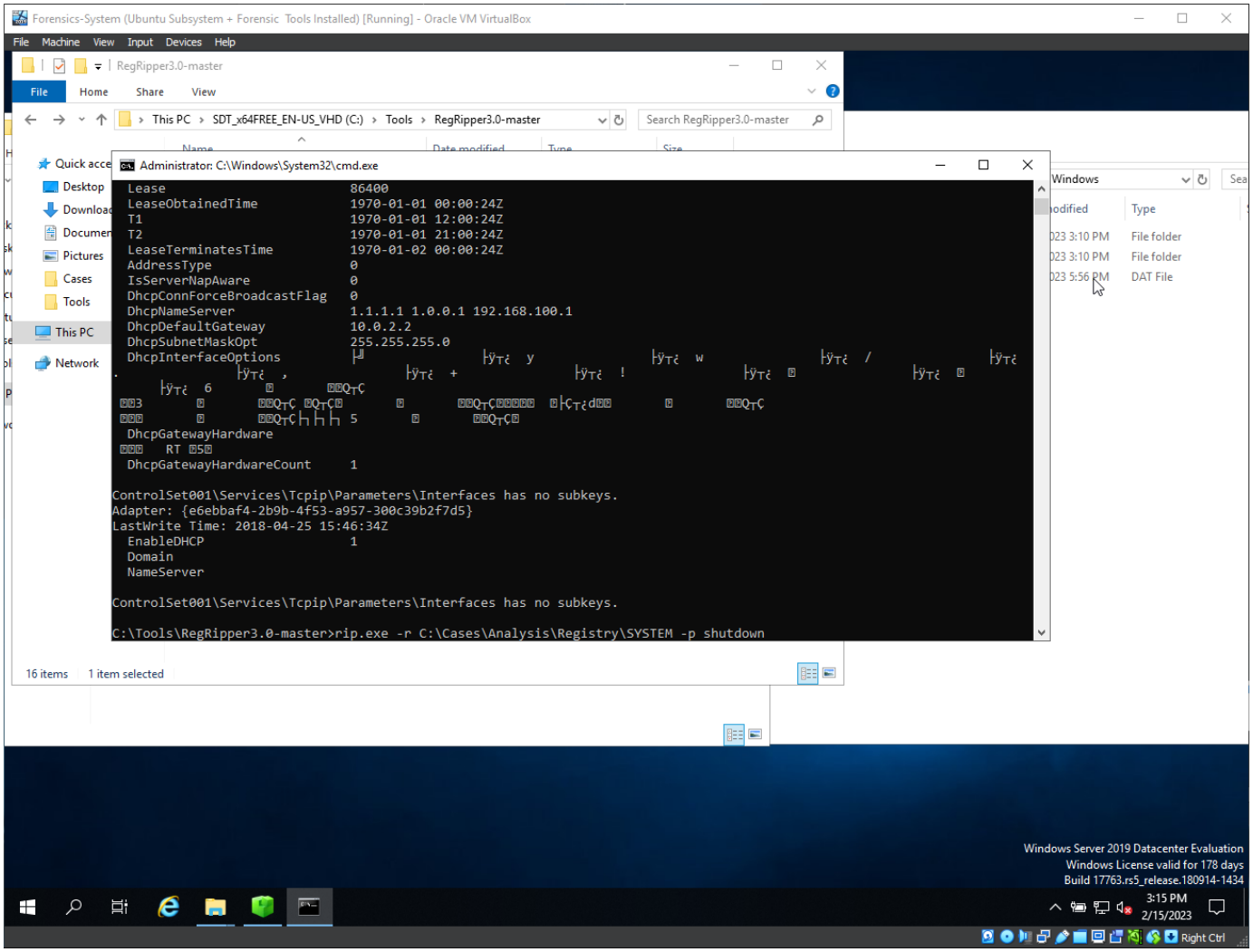
DhcpServer 10.0.2.2

DhcpNameServer 1.1.1.1 1.0.0.1 192.168.100.1

DhcpDefaultGateway 10.0.2.2

DhcpSubnetMaskOpt 255.255.255.0

- Shutdown time:

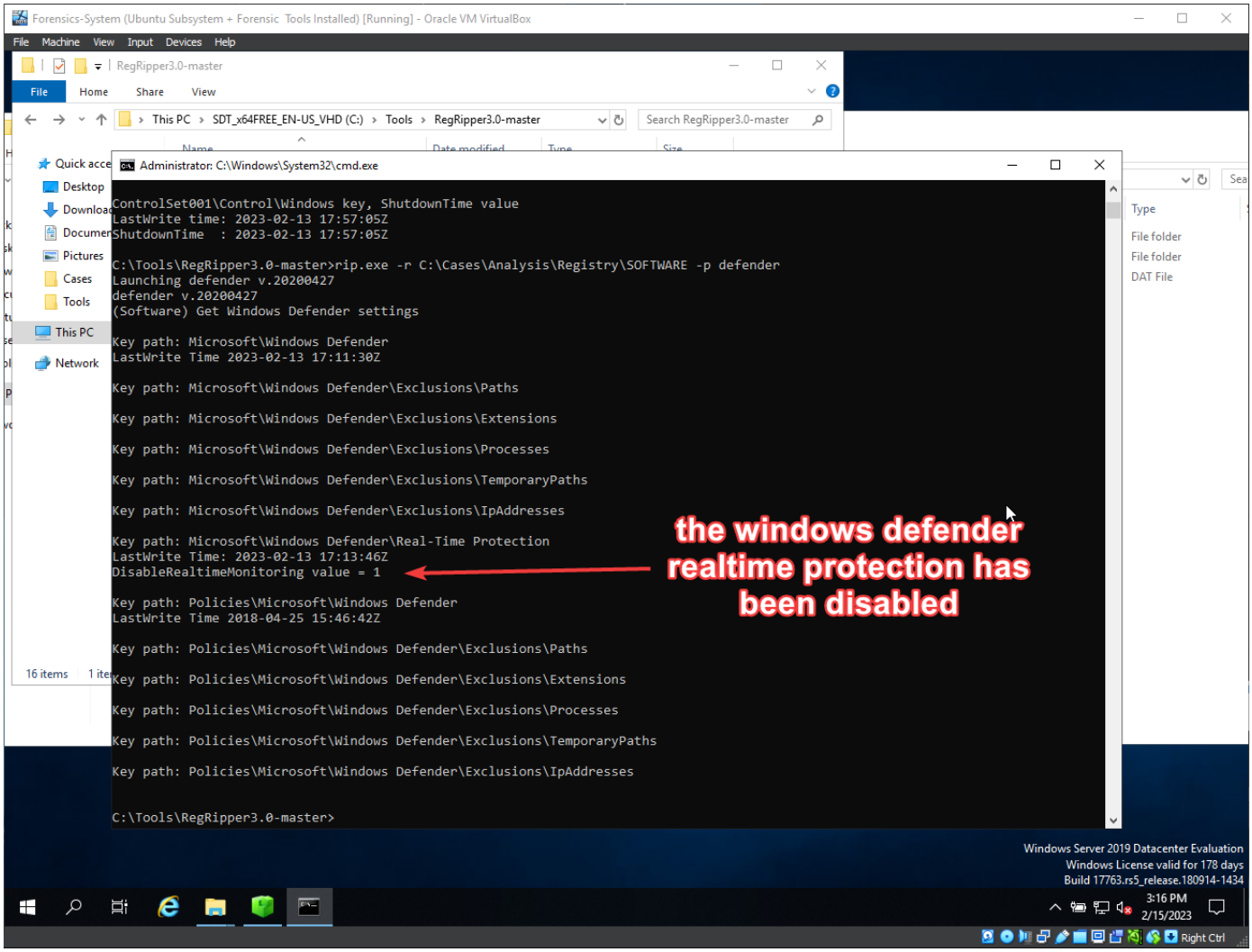


- Answer :

LastWrite time: 2023-02-13 17:57:05Z

ShutdownTime : 2023-02-13 17:57:05Z

- Defender settings:



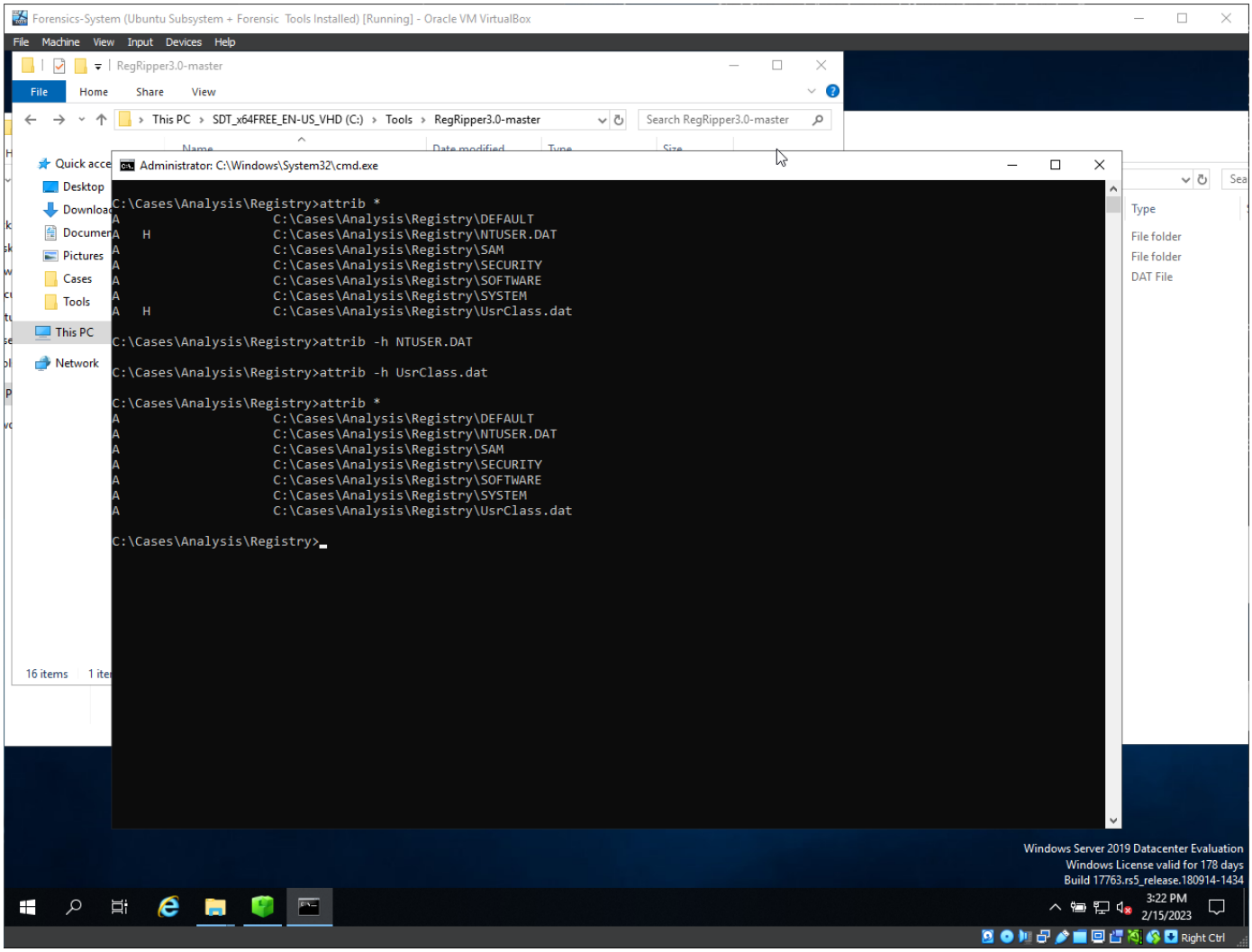
- Answer :

Key path: Microsoft\Windows Defender\Real-Time Protection

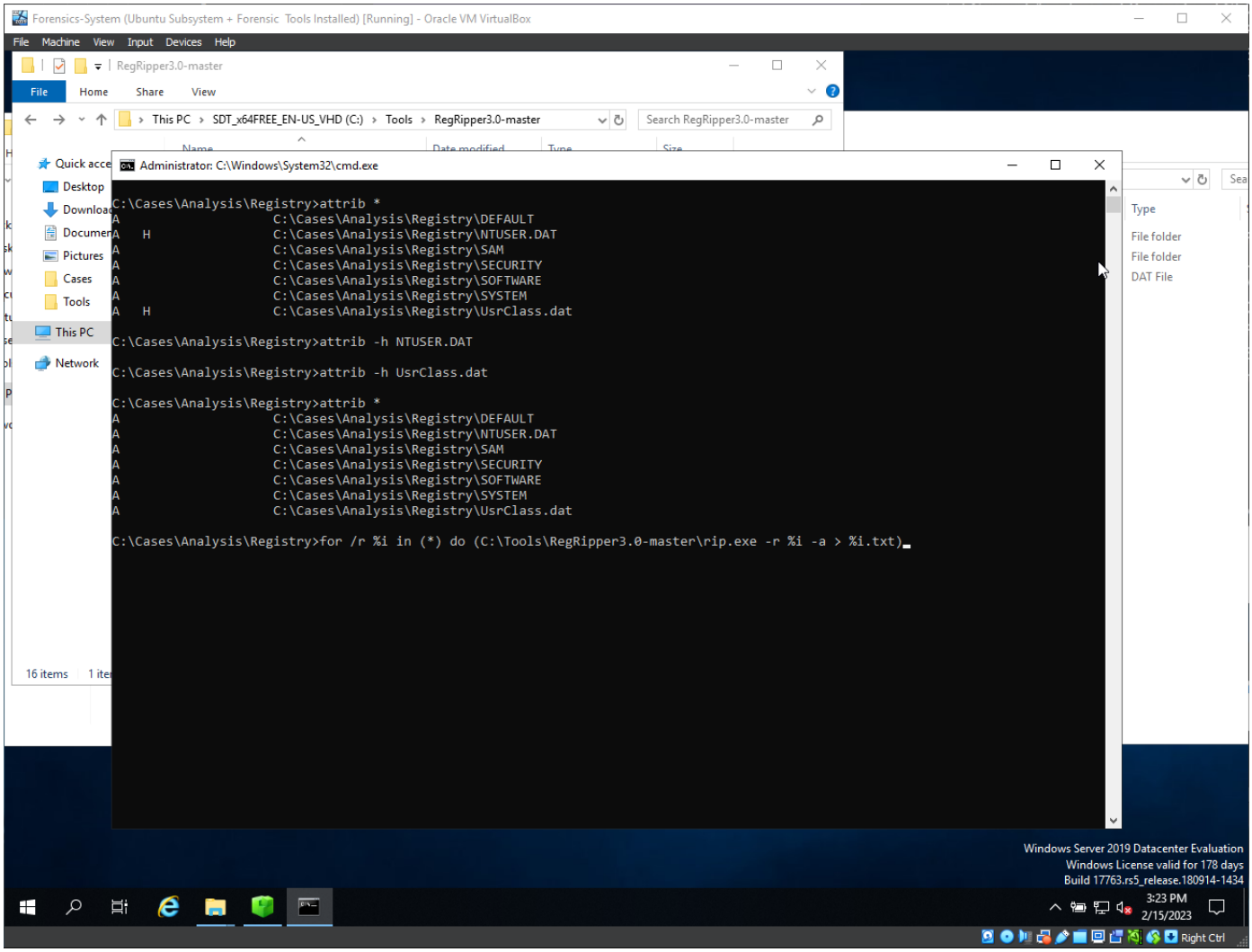
LastWrite Time: 2023-02-13 17:13:46Z

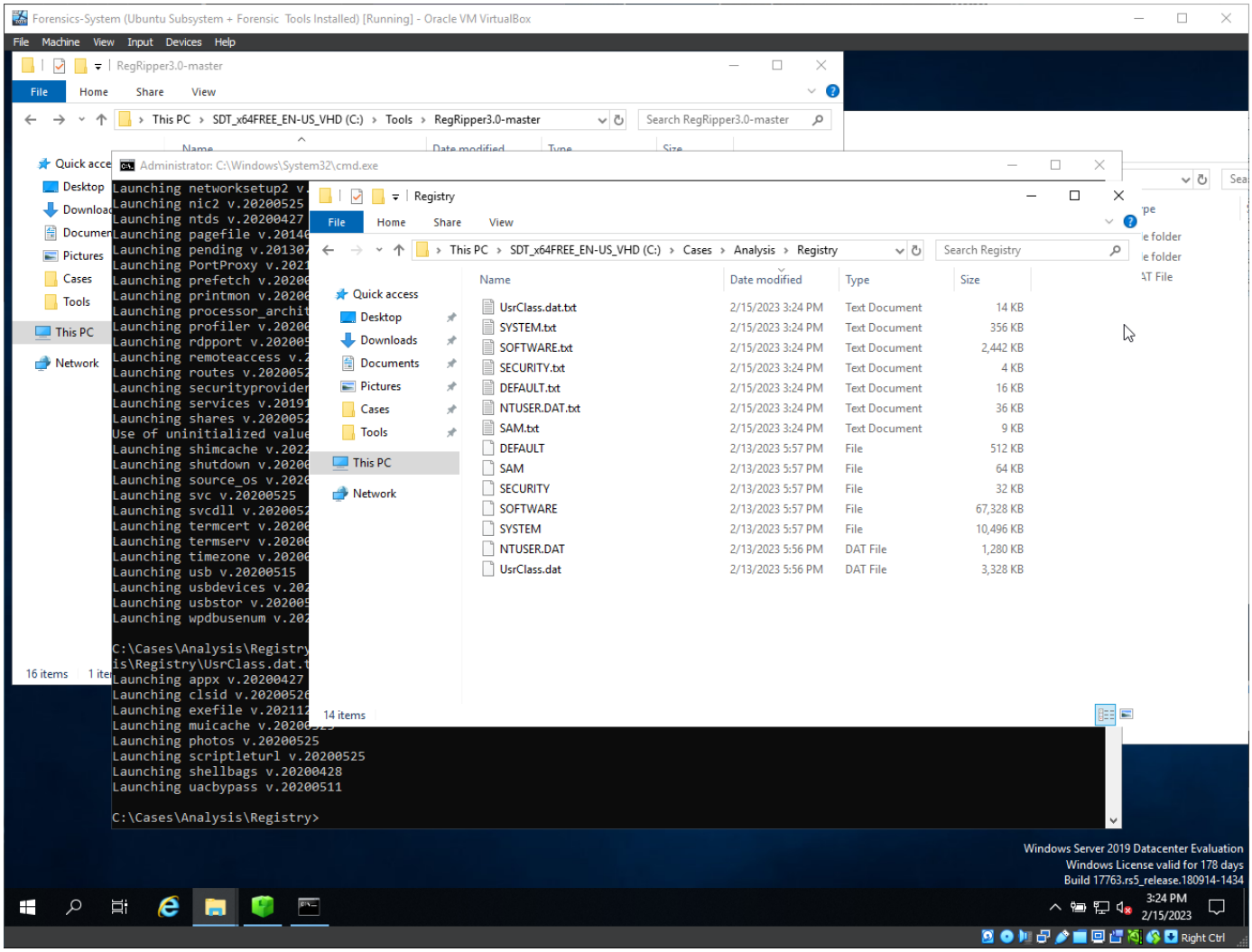
DisableRealtimeMonitoring value = 1

- Parsing all registry hives with RegRipper:
- Unhid the two user registries:

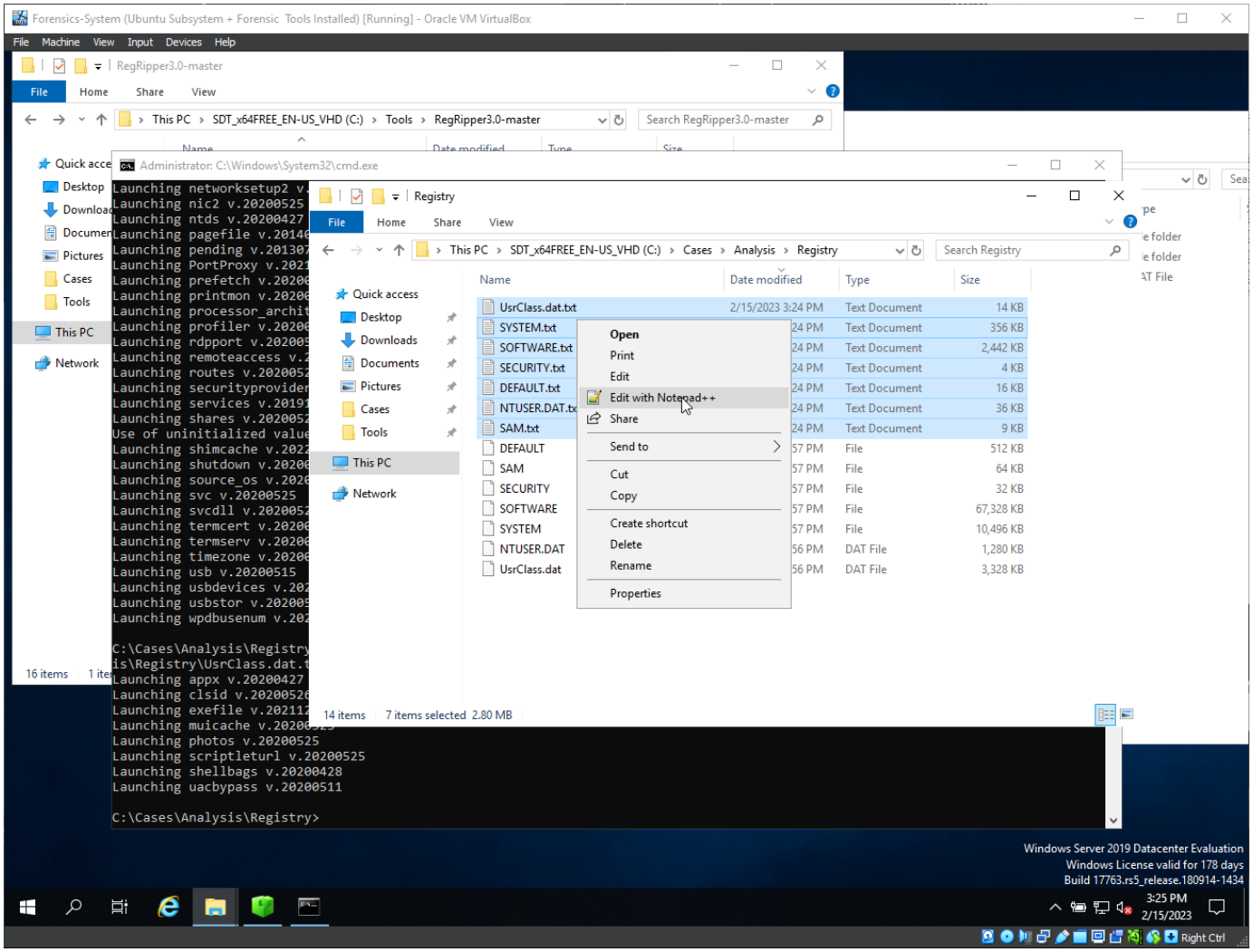


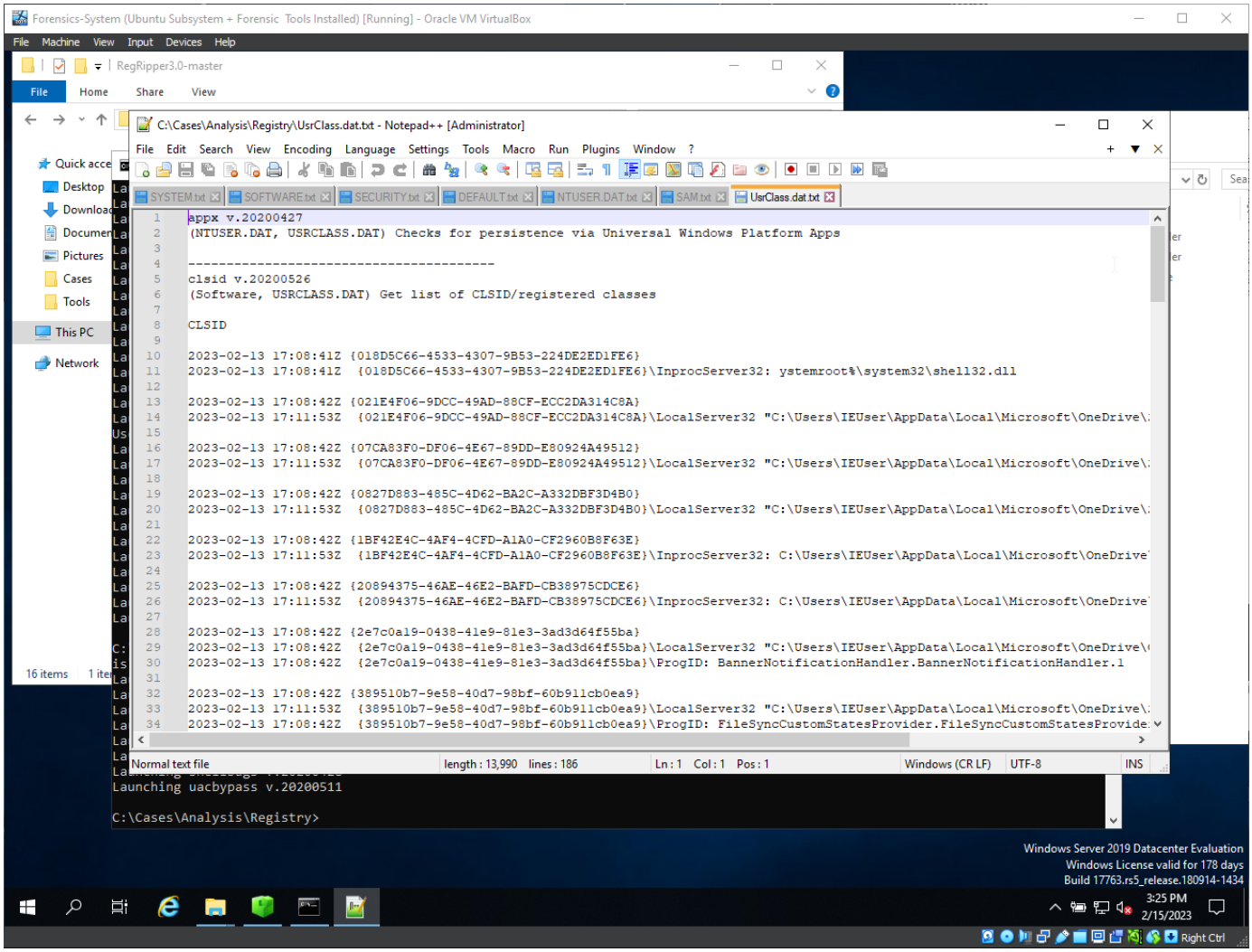
- Parse all the hives and put them into text files:


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
RegRipper3.0-master
File Home Share View
This PC › SDT_x64FREE_EN-US_VHD (C:) › Tools › RegRipper3.0-master
Search RegRipper3.0-master
Quick acce
Desktop
Downloa
Documen
Pictures
Cases
Tools
This PC
Network
16 items
Administrator: C:\Windows\System32\cmd.exe
C:\Cases\Analysis\Registry>attrib *
A C:\Cases\Analysis\Registry\DEFAULT
A H C:\Cases\Analysis\Registry\NTUSER.DAT
A C:\Cases\Analysis\Registry\SAM
A C:\Cases\Analysis\Registry\SECURITY
A C:\Cases\Analysis\Registry\SOFTWARE
A C:\Cases\Analysis\Registry\SYSTEM
A H C:\Cases\Analysis\Registry\UsrClass.dat
C:\Cases\Analysis\Registry>attrib -h NTUSER.DAT
C:\Cases\Analysis\Registry>attrib -h UsrClass.dat
C:\Cases\Analysis\Registry>attrib *
A C:\Cases\Analysis\Registry\DEFAULT
A C:\Cases\Analysis\Registry\NTUSER.DAT
A C:\Cases\Analysis\Registry\SAM
A C:\Cases\Analysis\Registry\SECURITY
A C:\Cases\Analysis\Registry\SOFTWARE
A C:\Cases\Analysis\Registry\SYSTEM
A C:\Cases\Analysis\Registry\UsrClass.dat
C:\Cases\Analysis\Registry>for /r %i in (*) do (C:\Tools\RegRipper3.0-master\rip.exe -r %i -a > %i.txt)
Type
File folder
File folder
DAT File
Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
3:23 PM
2/15/2023
Right Ctrl



- Open all with Notepad++:


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
RegRipper3.0-master
File Home Share View
This PC › SDT_x64FREE_EN-US_VHD (C:) › Tools › RegRipper3.0-master
Search RegRipper3.0-master
Administrator: C:\Windows\System32\cmd.exe
Launching networksetup2 v.
Launching nic2 v.20200525
Launching ntds v.20200427
Launching pagefile v.20146
Launching pending v.201307
Launching PortProxy v.2021
Launching prefetch v.20206
Launching printmon v.20206
Launching processor_archit
Launching profiler v.20206
Launching rdpport v.202005
Launching remoteaccess v.2
Launching routes v.2020052
Launching securityprovider
Launching services v.20191
Launching shares v.2020052
Use of uninitialized value
Launching shimcache v.2022
Launching shutdown v.20206
Launching source_os v.2020
Launching svc v.20200525
Launching svcdll v.2020052
Launching termcert v.20206
Launching termserv v.20206
Launching timezone v.20206
Launching usb v.20200515
Launching usbdevices v.202
Launching usbstor v.202005
Launching wpdbusenum v.202
C:\Cases\Analysis\Registry
is\Registry\UsrClass.dat.t
Launching appx v.20200427
Launching clsid v.20200526
Launching exefile v.202112
Launching muicache v.20200
Launching photos v.20200525
Launching scriptleturl v.20200525
Launching shellbags v.20200428
Launching uacbypass v.20200511
C:\Cases\Analysis\Registry>
Registry
File Home Share View
This PC › SDT_x64FREE_EN-US_VHD (C:) › Cases › Analysis › Registry
Search Registry
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
Size
UsrClass.dat.txt 2/15/2023 3:24 PM Text Document 14 KB
SYSTEM.txt 24 PM Text Document 356 KB
SOFTWARE.txt 24 PM Text Document 2,442 KB
SECURITY.txt 24 PM Text Document 4 KB
DEFAULT.txt 24 PM Text Document 16 KB
NTUSER.DAT.tx 24 PM Text Document 36 KB
SAM.txt 24 PM Text Document 9 KB
DEFAULT 57 PM File 512 KB
SAM 57 PM File 64 KB
SECURITY 57 PM File 32 KB
SOFTWARE 57 PM File 67,328 KB
SYSTEM 57 PM File 10,496 KB
NTUSER.DAT 56 PM DAT File 1,280 KB
UsrClass.dat 56 PM DAT File 3,328 KB
Open
Print
Edit
Edit with Notepad++
Share
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
14 items 7 items selected 2.80 MB
16 items
Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
3:25 PM
2/15/2023
Right Ctrl



SIDs

- Example of SID: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers

`S-1-5-32-544`

This SID has four components:

- A revision level (1)
- An identifier authority value (5, NT Authority)
- A domain identifier (32, Builtin)
- A relative identifier (544, Administrators)

`S-1-5-21-1004336348-1177238915-682003330-512`

The SID for Contoso\Domain Admins has:

- A revision level (1)
- An identifier authority (5, NT Authority)
- A domain identifier (21-1004336348-1177238915-682003330, Contoso)
- A relative identifier (512, Domain Admins)

- Well known SIDs:

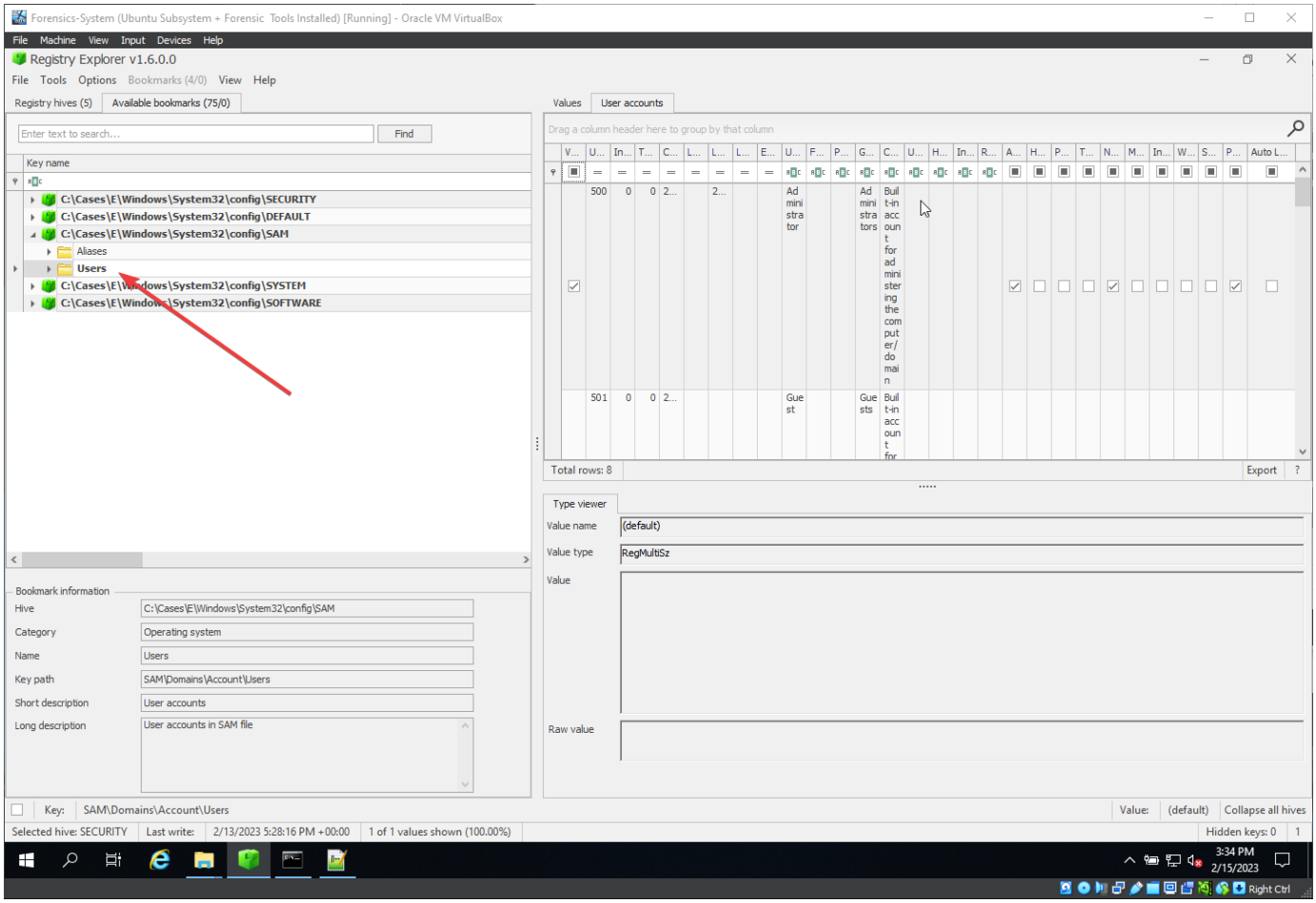
SID	Display name	Description
S-1-5-1	Dialup	A group that includes all users who are signed in to the system via dial-up connection.
S-1-5-113	Local account	You can use this SID when you're restricting network sign-in to local accounts instead of "administrator" or equivalent. This SID can be effective in blocking network sign-in for local users and groups by account type regardless of what they're named.
S-1-5-114	Local account and member of Administrators group	You can use this SID when you're restricting network sign-in to local accounts instead of "administrator" or equivalent. This SID can be effective in blocking network sign-in for local users and groups by account type regardless of what they're named.
S-1-5-2	Network	A group that includes all users who are signed in via a network connection. Access tokens for interactive users don't contain the Network SID.
S-1-5-3	Batch	A group that includes all users who have signed in via batch queue facility, such as task scheduler jobs.
S-1-5-4	Interactive	A group that includes all users who sign in interactively. A user can start an interactive sign-in session by opening a Remote Desktop Services connection from a remote computer, or by using a remote shell such as Telnet. In each case, the user's access token contains the Interactive SID. If the user signs in by using a Remote Desktop Services connection, the user's access token also contains the Remote Interactive Logon SID.
S-1-5-5-*X*-*Y*	Logon Session	The *X* and *Y* values for these SIDs uniquely identify a particular sign-in session.
S-1-5-6	Service	A group that includes all security principals that have signed in as a service.
S-1-5-7	Anonymous Logon	A user who has connected to the computer without supplying a user name and password. The Anonymous Logon identity is different from the identity that's used by Internet Information Services (IIS) for anonymous web access. IIS uses an

User Accounts, groups and profiles

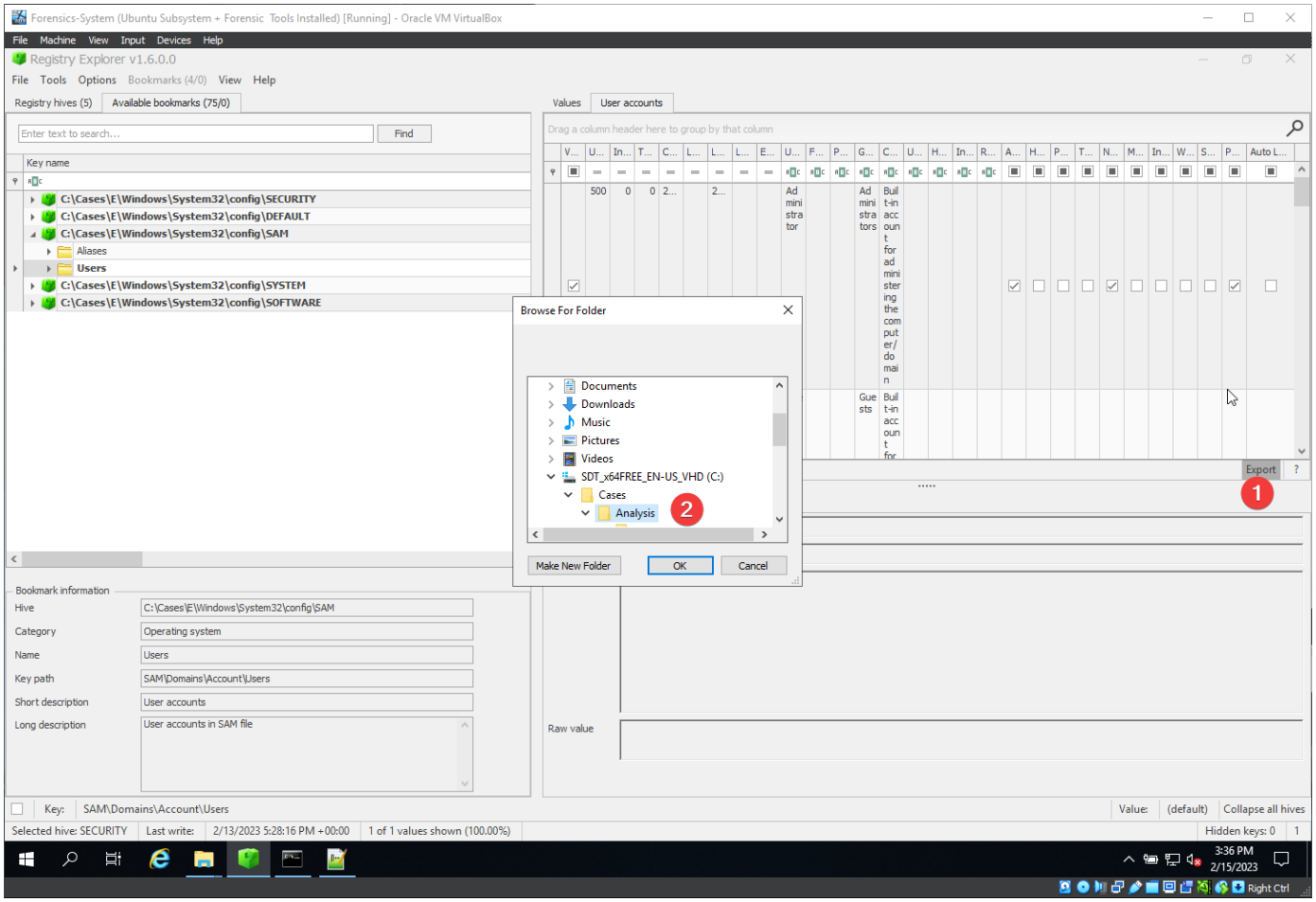
- Find Information about Users,Groups and User Profiles:
  - Active accounts during the attack timeframe:
  - Accounts created
  - Administrator group members

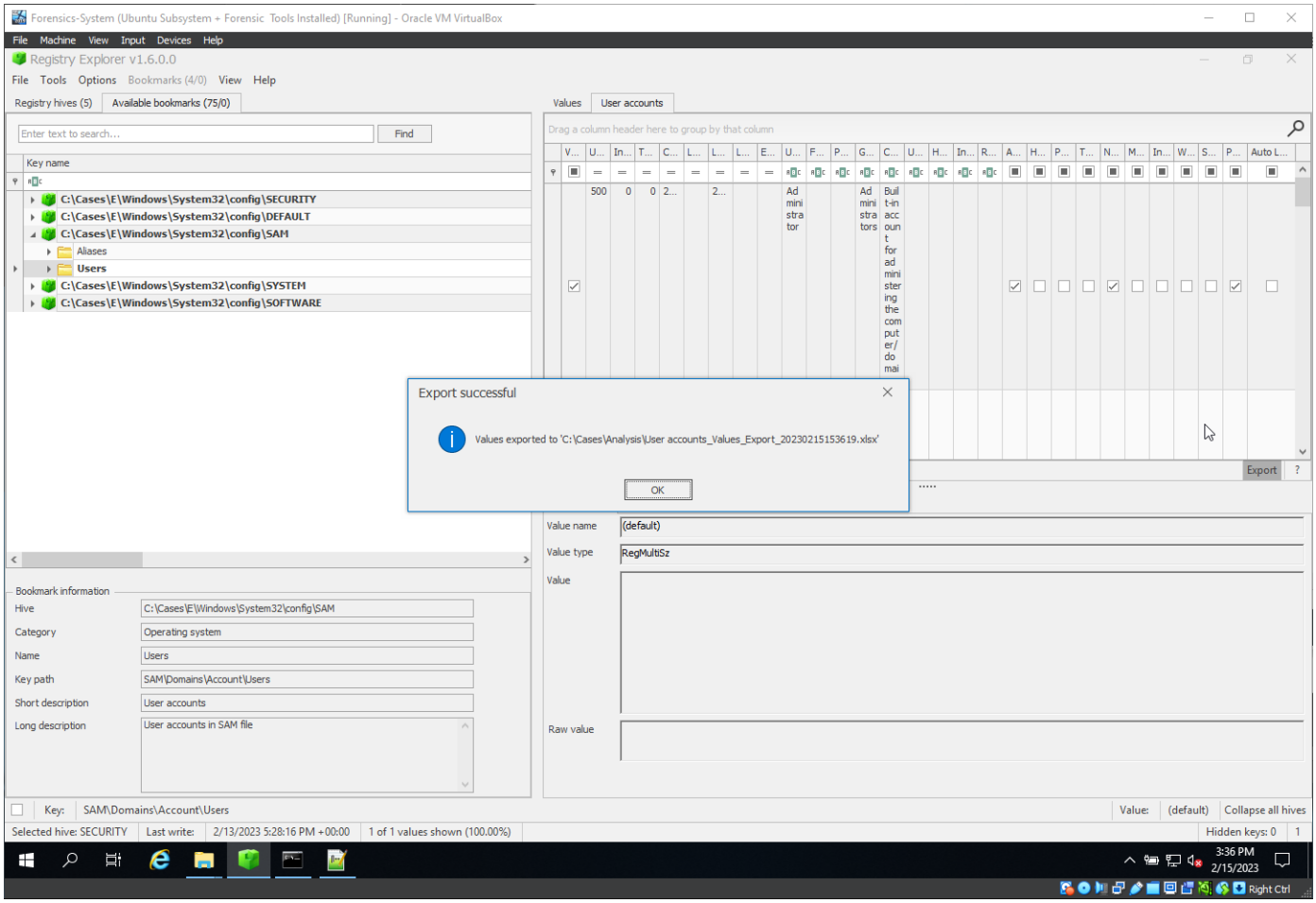
- What users have Windows Profiles

- You can go back to Registry Explorer:

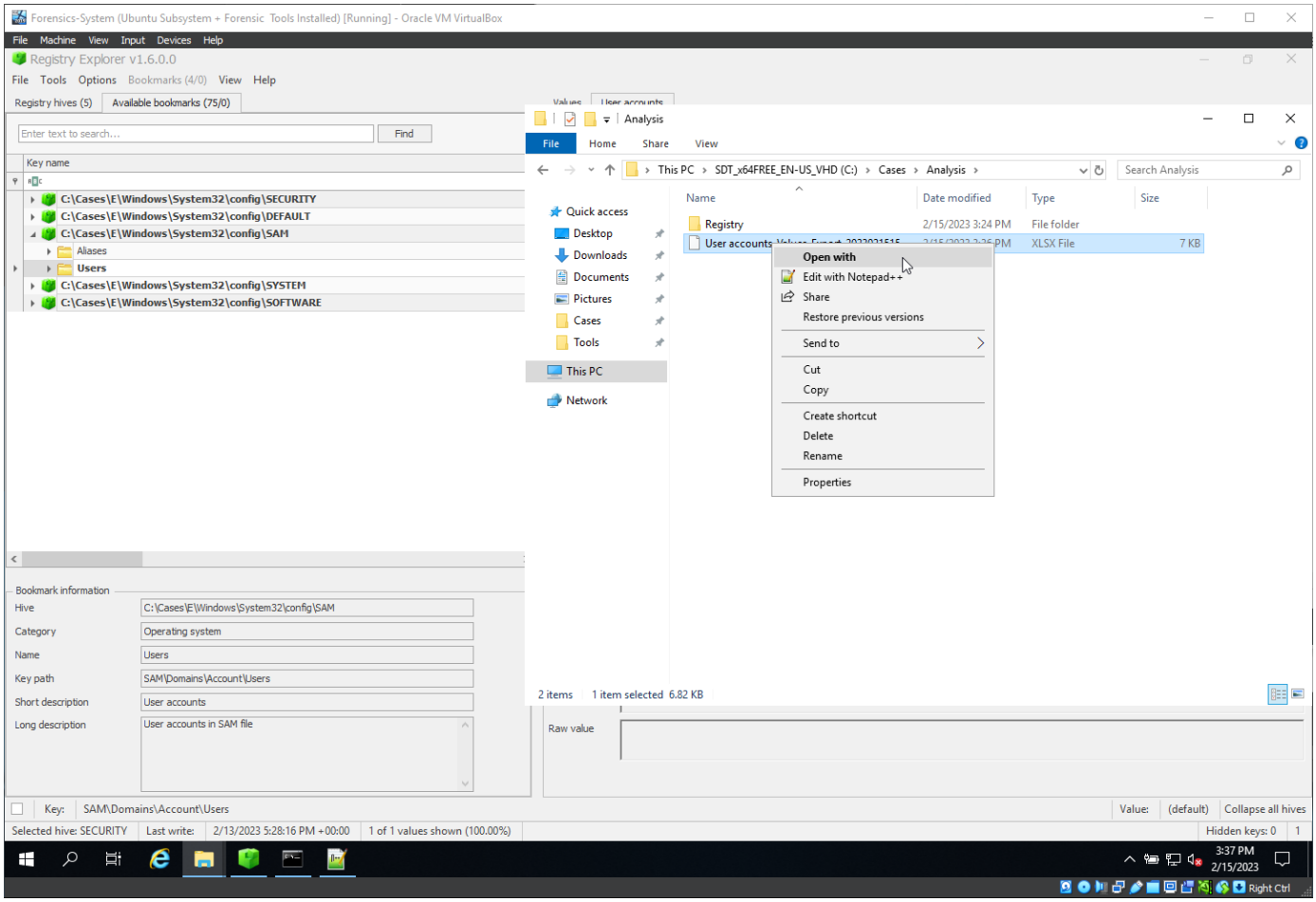


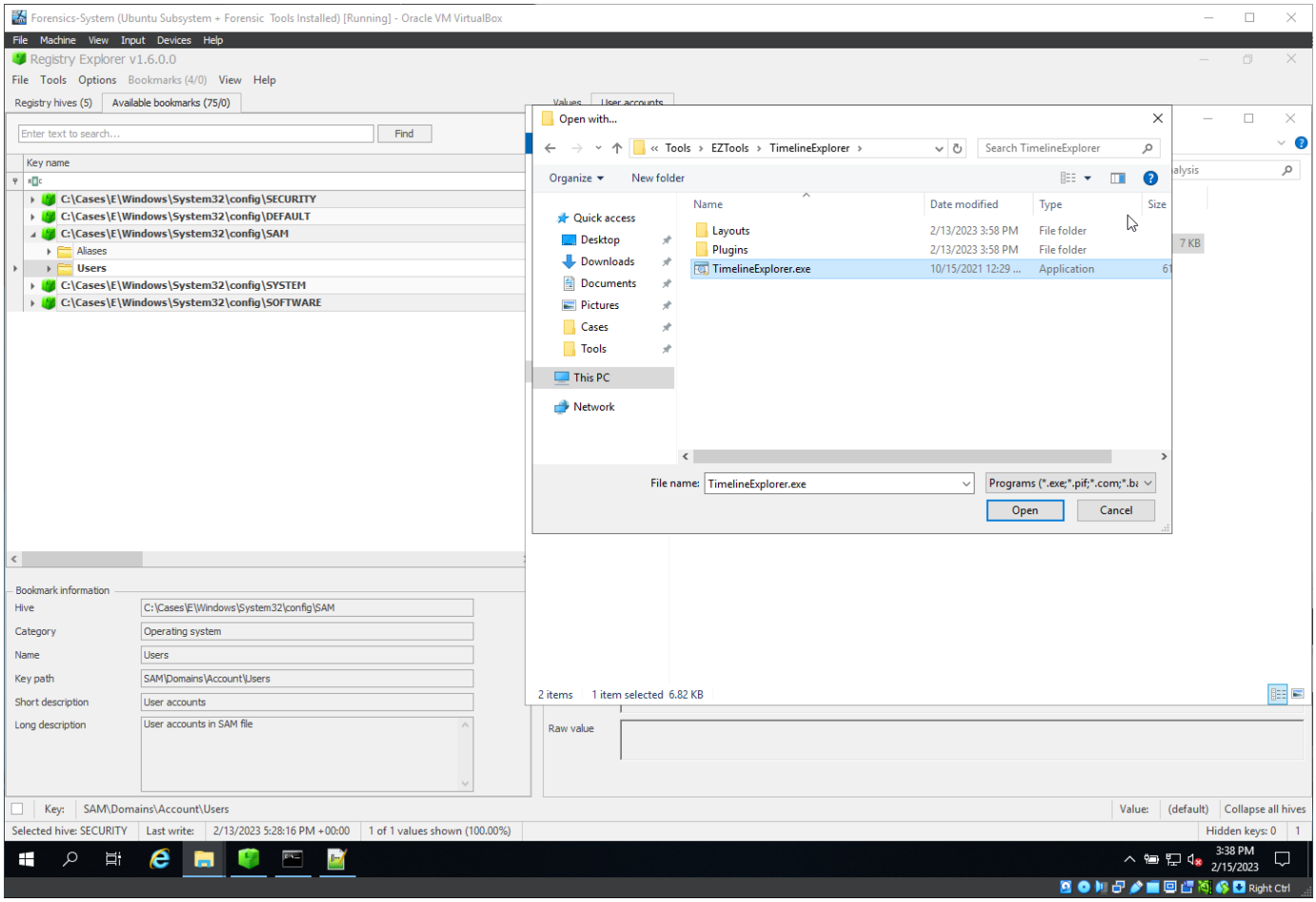
- For better analysis, it is better to export it to XLSX type file:

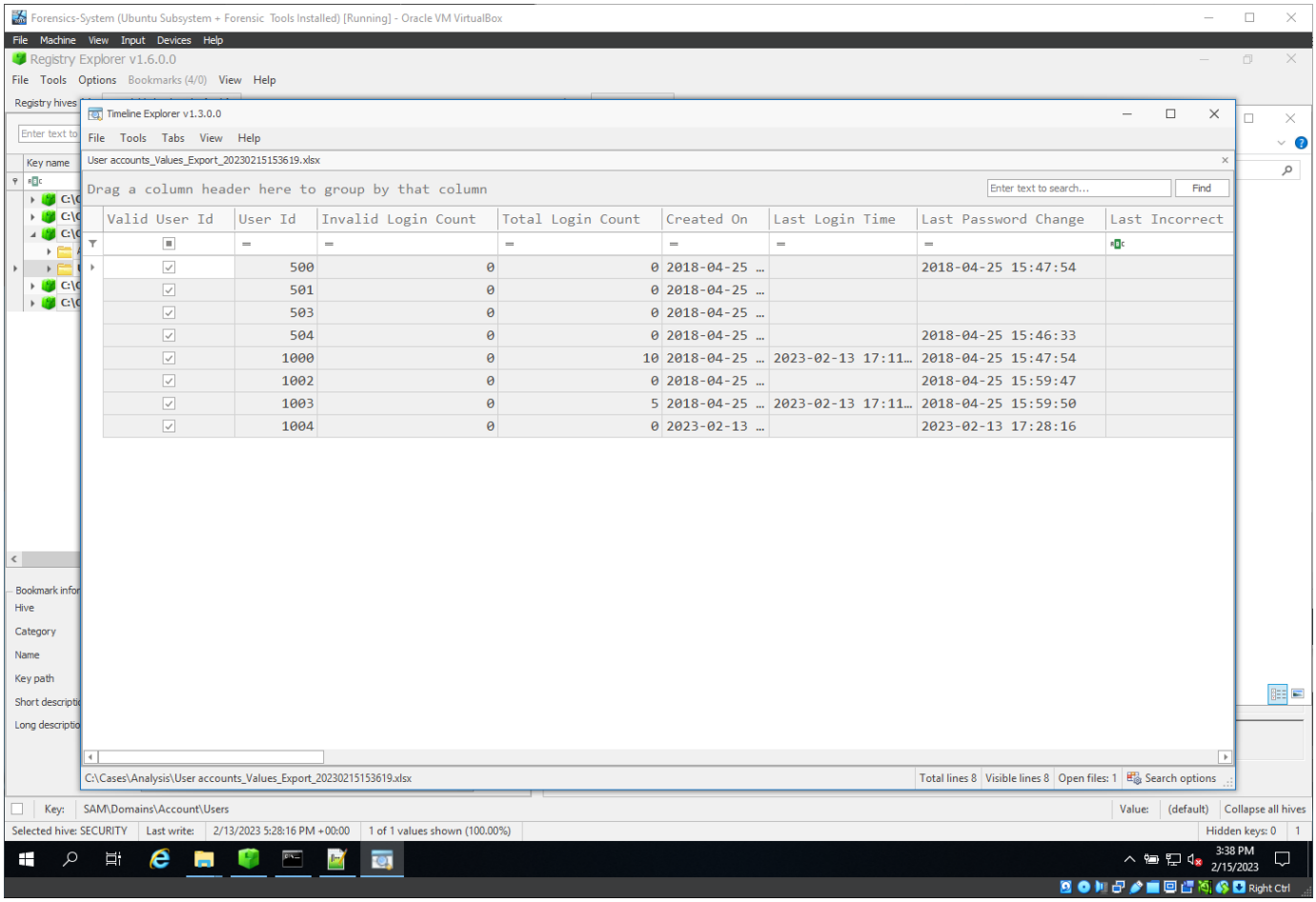

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (4/0) View Help
Registry hives (5)
Available bookmarks (75/0)
Enter text to search...
Find
Key name
C:\Cases\E\Windows\System32\config\SECURITY
C:\Cases\E\Windows\System32\config\DEFAULT
C:\Cases\E\Windows\System32\config\SAM
Aliases
Users
C:\Cases\E\Windows\System32\config\SYSTEM
C:\Cases\E\Windows\System32\config\SOFTWARE
Values
User accounts
Drag a column header here to group by that column
Export
1
Browse For Folder
Documents
Downloads
Music
Pictures
Videos
SDT_x64FREE_EN-US_VHD (C:)
Cases
Analysis
2
Make New Folder
OK
Cancel
Bookmark information
Hive C:\Cases\E\Windows\System32\config\SAM
Category Operating system
Name Users
Key path SAM\Domains\Account\Users
Short description User accounts
Long description User accounts in SAM file
Raw value
Key: SAM\Domains\Account\Users
Value: (default)
Collapse all hives
Selected hive: SECURITY
Last write: 2/13/2023 5:28:16 PM +00:00
1 of 1 values shown (100.00%)
Hidden keys: 0
3:36 PM
2/15/2023
Right Ctrl



- For better viewing, there exists an application in EZTools, TimelineExplorer:


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (4/0) View Help
Registry hives (5)
Available bookmarks (75/0)
Enter text to search...
Find
Key name
C:\Cases\E\Windows\System32\config\SECURITY
C:\Cases\E\Windows\System32\config\DEFAULT
C:\Cases\E\Windows\System32\config\SAM
Aliases
Users
C:\Cases\E\Windows\System32\config\SYSTEM
C:\Cases\E\Windows\System32\config\SOFTWARE
Bookmark information
Hive
C:\Cases\E\Windows\System32\config\SAM
Category
Operating system
Name
Users
Key path
SAM\Domains\Account\Users
Short description
User accounts
Long description
User accounts in SAM file
Analysis
File Home Share View
This PC › SDT_x64FREE_EN-US_VHD (C:) › Cases › Analysis ›
Search Analysis
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
Size
Registry
2/15/2023 3:24 PM
File folder
User accounts
XLSX File
7 KB
Open with
Edit with Notepad++
Share
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
2 items
1 item selected 6.82 KB
Raw value
Key: SAM\Domains\Account\Users
Value: (default)
Collapse all hives
Selected hive: SECURITY
Last write: 2/13/2023 5:28:16 PM +00:00
1 of 1 values shown (100.00%)
Hidden keys: 0
3:37 PM
2/15/2023
Right Ctrl


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (4/0) View Help
Registry hives (5)
Available bookmarks (75/0)
Enter text to search...
Find
Key name
C:\Cases\E\Windows\System32\config\SECURITY
C:\Cases\E\Windows\System32\config\DEFAULT
C:\Cases\E\Windows\System32\config\SAM
Aliases
Users
C:\Cases\E\Windows\System32\config\SYSTEM
C:\Cases\E\Windows\System32\config\SOFTWARE
Bookmark information
Hive
C:\Cases\E\Windows\System32\config\SAM
Category
Operating system
Name
Users
Key path
SAM\Domains\Account\Users
Short description
User accounts
Long description
User accounts in SAM file
Open with...
Tools › EZTools › TimelineExplorer ›
Search TimelineExplorer
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
Size
Layouts
2/13/2023 3:58 PM
File folder
Plugins
2/13/2023 3:58 PM
File folder
TimelineExplorer.exe
10/15/2021 12:29 ...
Application
File name: TimelineExplorer.exe
Programs (*.exe;*.pif;*.com;*.bi
Open
Cancel
2 items
1 item selected 6.82 KB
Raw value
Key: SAM\Domains\Account\Users
Value: (default)
Collapse all hives
Selected hive: SECURITY
Last write: 2/13/2023 5:28:16 PM +00:00
1 of 1 values shown (100.00%)
Hidden keys: 0
3:38 PM
2/15/2023
Right Ctrl



- Active accounts during the attack timeframe:
- Answer :

Username : IEUser [1000]

SID : S-1-5-21-1058341133-2092417715-4019509128-1000

Full Name : IEUser

User Comment : IEUser

Account Type :

Account Created : Wed Apr 25 15:47:54 2018 Z

Name :

Last Login Date : Mon Feb 13 17:11:34 2023 Z

Pwd Reset Date : Wed Apr 25 15:47:54 2018 Z

Pwd Fail Date : Never

Login Count : 10

--> Password does not expire

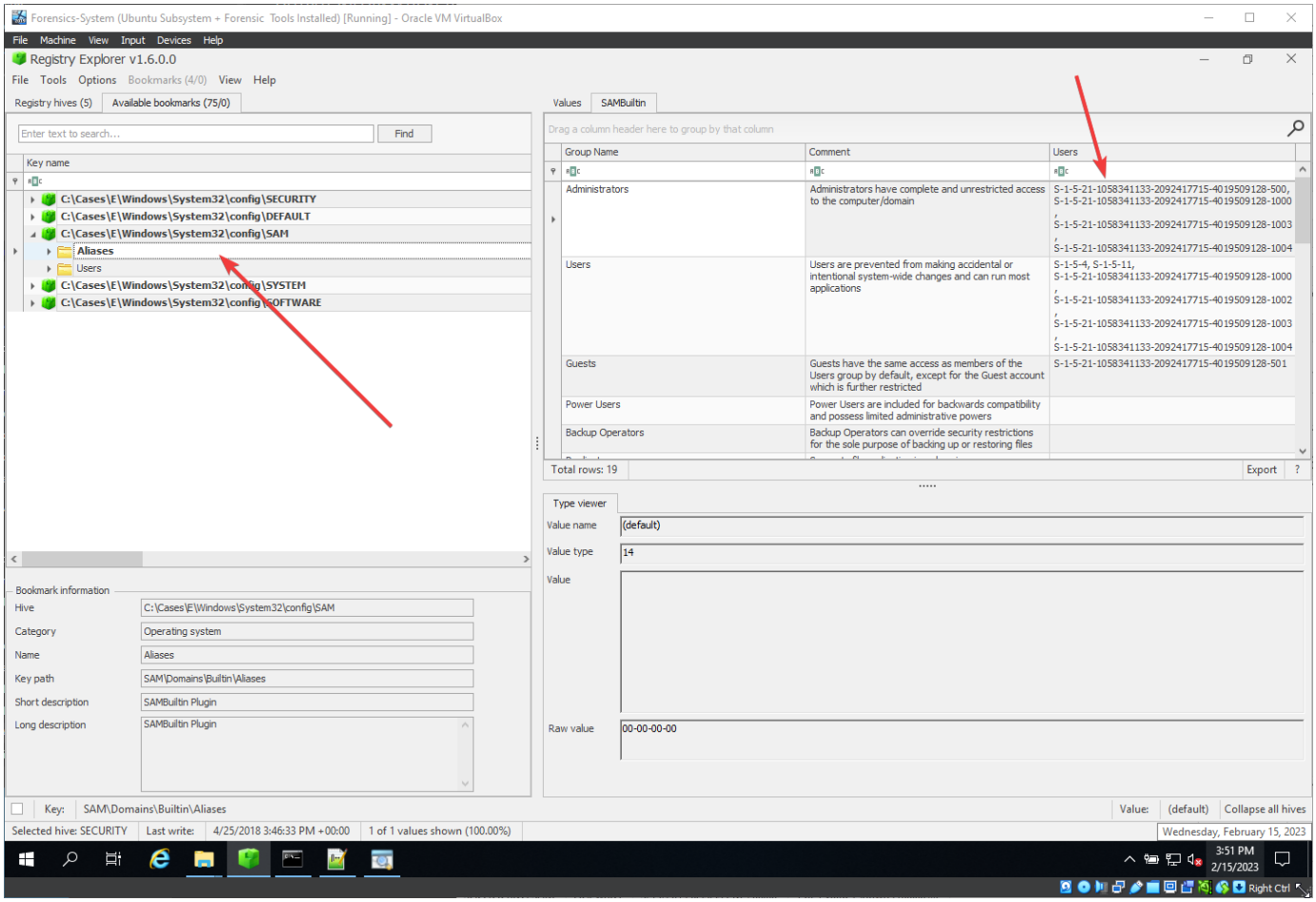
--> Normal user account

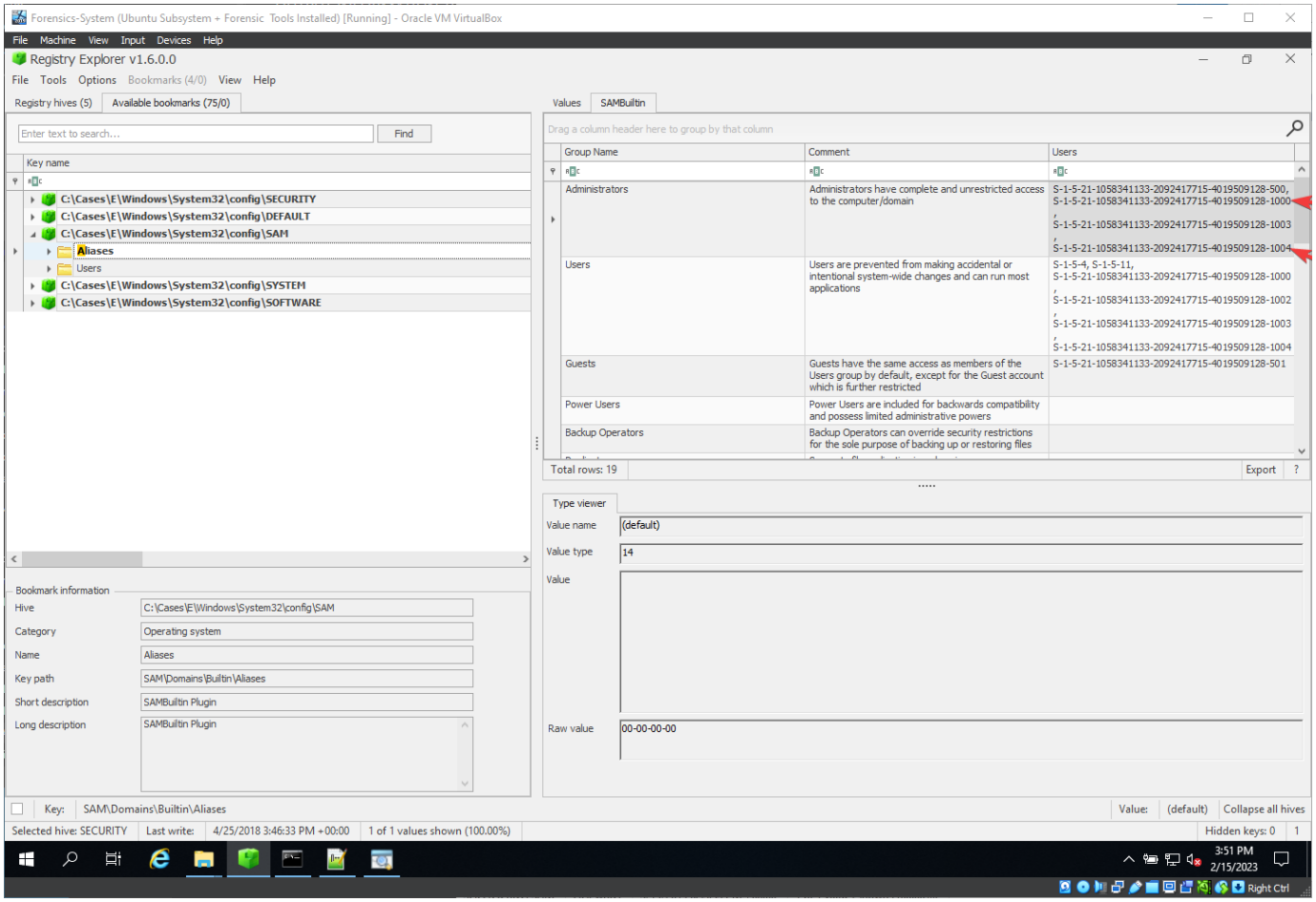
- Accounts created
- Answer :

Username : art-test [1004]

Account Created : Mon Feb 13 17:28:16 2023 Z

- Administrator group members


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (4/0) View Help
Registry hives (5)
Available bookmarks (75/0)
Enter text to search...
Find
Key name
C:\Cases\E\Windows\System32\config\SECURITY
C:\Cases\E\Windows\System32\config\DEFAULT
C:\Cases\E\Windows\System32\config\SAM
Aliases
Users
C:\Cases\E\Windows\System32\config\SYSTEM
C:\Cases\E\Windows\System32\config\SOFTWARE
Values
SAMBuiltin
Drag a column header here to group by that column
Group Name
Comment
Users
Administrators
Administrators have complete and unrestricted access to the computer/domain
S-1-5-21-1058341133-2092417715-4019509128-500, S-1-5-21-1058341133-2092417715-4019509128-1000, S-1-5-21-1058341133-2092417715-4019509128-1003, S-1-5-21-1058341133-2092417715-4019509128-1004
Users
Users are prevented from making accidental or intentional system-wide changes and can run most applications
S-1-5-4, S-1-5-11, S-1-5-21-1058341133-2092417715-4019509128-1000, S-1-5-21-1058341133-2092417715-4019509128-1002, S-1-5-21-1058341133-2092417715-4019509128-1003, S-1-5-21-1058341133-2092417715-4019509128-1004
Guests
Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
S-1-5-21-1058341133-2092417715-4019509128-501
Power Users
Power Users are included for backwards compatibility and possess limited administrative powers
Backup Operators
Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
Total rows: 19
Export
Type viewer
Value name
(default)
Value type
1-4
Value
Raw value
00-00-00-00
Bookmark information
Hive
C:\Cases\E\Windows\System32\config\SAM
Category
Operating system
Name
Aliases
Key path
SAM\Domains\Builtin\Aliases
Short description
SAMBuiltin Plugin
Long description
SAMBuiltin Plugin
Key:
SAM\Domains\Builtin\Aliases
Value:
(default)
Collapse all hives
Selected hive: SECURITY
Last write:
4/25/2018 3:46:33 PM +00:00
1 of 1 values shown (100.00%)
Wednesday, February 15, 2023
3:51 PM
2/15/2023
Right Ctrl

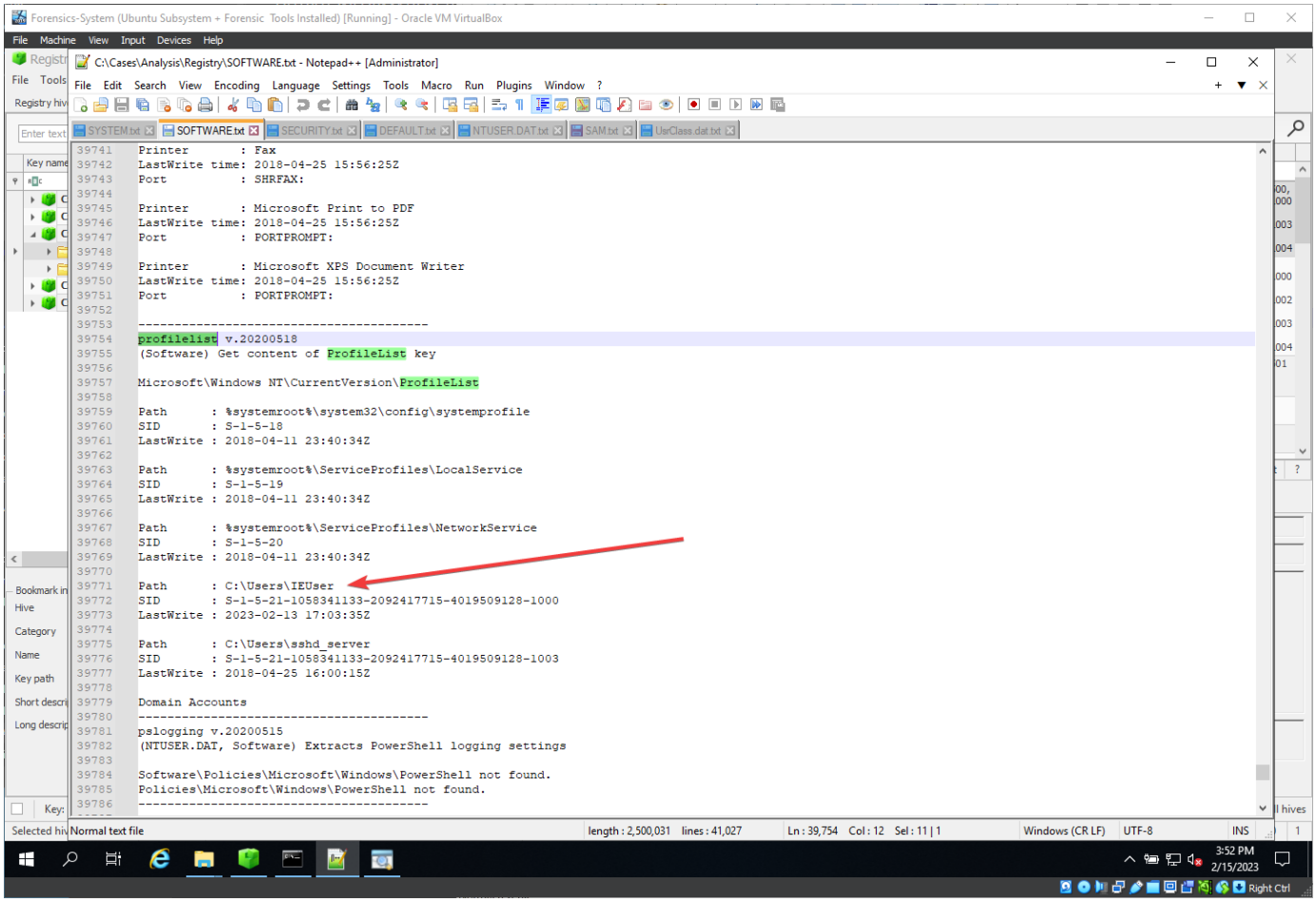


- Answer :

IEUser [1000]

art-test [1004]

- What users have Windows Profiles
- Using profilelist plugin from regripper



- Answer :

Path : C:\Users\IEUser

SID : S-1-5-21-1058341133-2092417715-4019509128-1000

LastWrite : 2023-02-13 17:03:35Z