



ETHICAL HACKING V2 LAB SERIES

Lab 22: Registry – Windows Security Account Manager

Document Version: **2021-05-18**

Material in this Lab Aligns to the Following	
Books/Certifications	Chapters/Modules/Objectives
All-In-One CEH Chapters ISBN-13: 978-1260454550	5: Attacking a System 11: Cryptography 101
EC-Council CEH v10 Domain Modules	4: Enumeration 6: System Hacking 20: Cryptography

Copyright © 2021 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and other countries. Google is a registered trademark of Google, LLC.

Contents

Introduction	3
Objectives.....	3
Lab Topology	4
Lab Settings	5
1 Getting to Know FTK Imager	6
2 Locate the SAM File Using FTK Imager	11
3 Accessing the SAM and SYSTEM Registry File from Kali Linux.....	23
4 Extracting Passwords from the SAM File	29

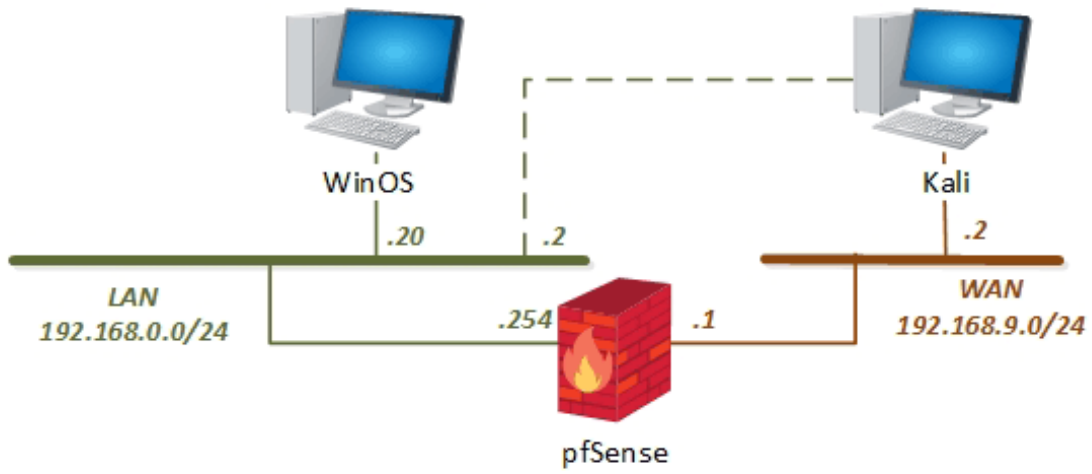
Introduction

The Windows Security Account Manager (SAM) is stored as a file in the Windows operating system. The SAM is part of the Windows Registry and contains information about the user accounts on the computer. This information includes passwords that can be cracked by popular password cracking methods. In this lab, we will go through the exercise of identifying the SAM file and cracking the password using *John The Ripper*.

Objectives

- Identify the location of the file
- Learn what type of data the SAM file stores
- Learn how to parse them
- Understand how to corroborate findings in the registry with files on the source device
- Attempt to crack the users in the SAM

Lab Topology



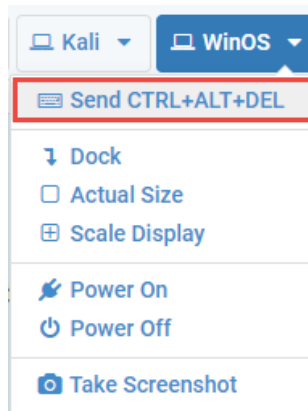
Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address / Subnet Mask	Account (if needed)	Password (if needed)
WinOS	192.168.0.20	Administrator	Train1ng\$
Kali Linux	192.168.9.2 192.168.0.2	root	toor

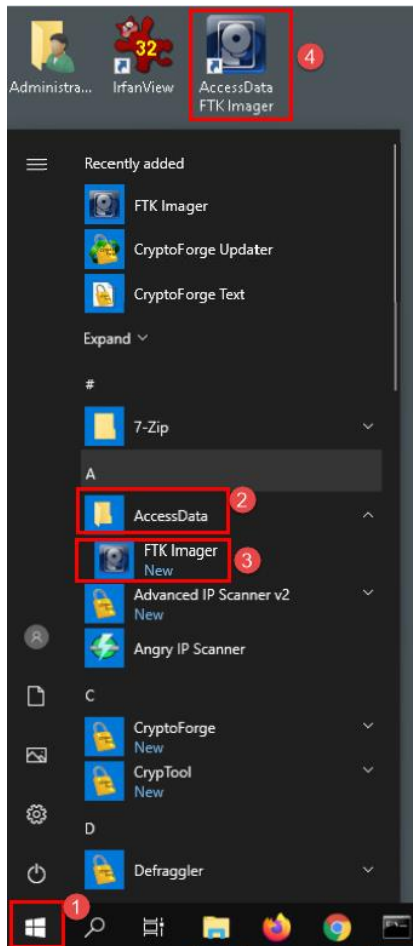
1 Getting to Know FTK Imager

1. Launch the **WinOS** virtual machine to access the graphical login screen.
 - 1.1. Select **Send CTRL+ALT+DEL** from the dropdown menu to be prompted with the login screen.

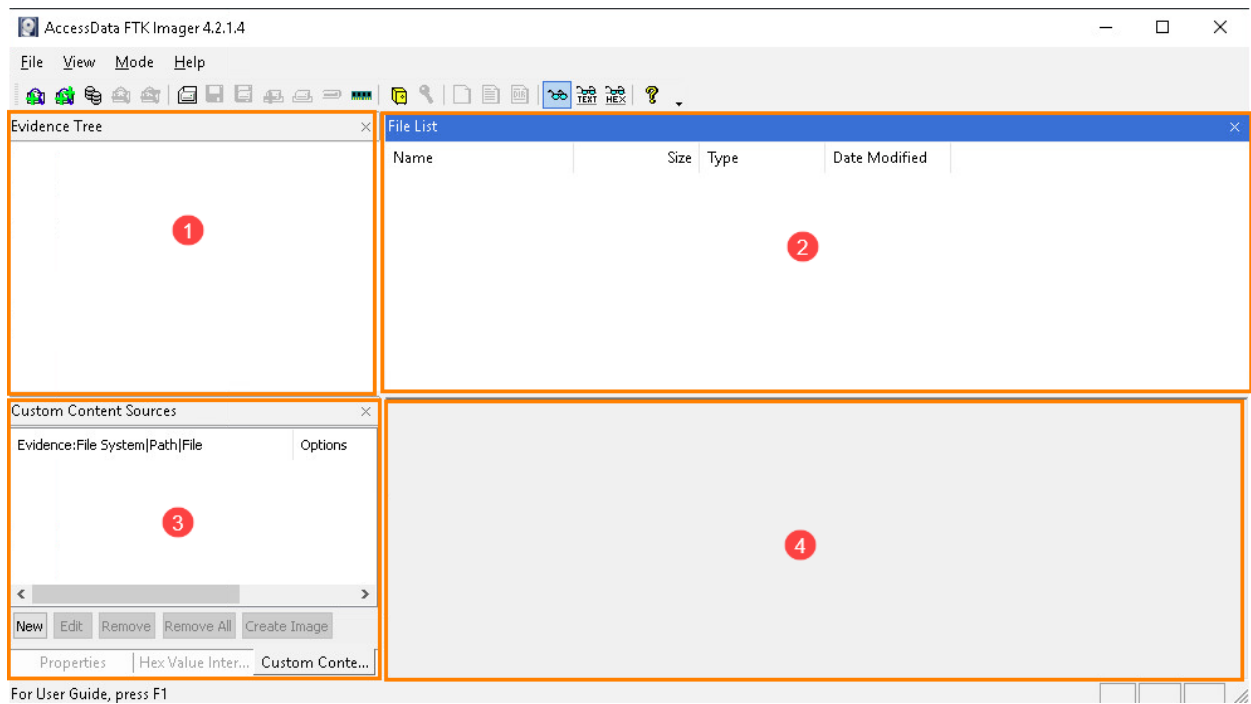


- 1.2. Log in as **Administrator** using the password: **Train1ng\$**

2. Once you are logged into the VM, launch the *FTK Imager* program from the *Windows* menu by navigating to **Start Menu > AccessData > FTK Imager**, as seen in *items 1, 2, and 3* below. Alternatively, you can open it by clicking the icon from the Desktop, as seen in *item 4*.

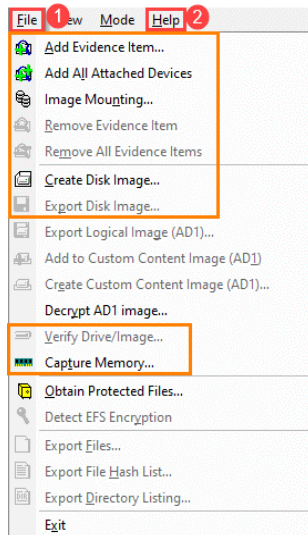











3. The following window will appear. Look at the sections highlighted in red. These are the different areas of the interface.



1	Evidence Tree	In this area, the storage device or evidence item will be displayed in a tree format
2	File list	This pane will display the list of files that are selected in the evidence tree pane
3	Properties	This pane contains various details about items selected in either the evidence tree or the file list panes
4	View pane	This is the box located in the bottom-right corner of the FTK Imager window and displays the contents of files selected in the file list pane

4. Now let us look at the menus to see some important options. We will start with the *File* menu. To access this, select the **File** button at the top left corner of the GUI, seen in *item 1* below, which will reveal the menu, as seen below:

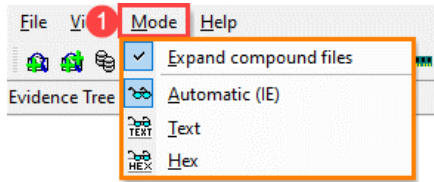


 Add Evidence Item...	The Add Evidence Item option allows the user to add a single evidence item
 Add All Attached Devices	The Add All Attached Devices option allows the user to add all storage devices attached to the computer (<i>Beware as this option only adds live volumes</i>)
 Image Mounting...	The Image Mounting option allows the user to mount an evidence item so that it can be viewed as an attached storage device
 Remove Evidence Item	The Remove Evidence Item option allows a user to remove a single evidence item
 Remove All Evidence Items	The Remove All Evidence Items option allows a user to remove all evidence items that are currently loaded.
 Create Disk Image...	The Create Disk Image option allows a user to create a forensic image of a storage device
 Export Disk Image...	The Export Disk Image option allows a user to create a disk image from a storage device that is already loaded in FTK Imager
 Verify Drive/Image...	The Verify Drive/Image option allows a user to perform a hash comparison of a forensic image
 Capture Memory...	The Capture Memory option allows a user to capture an image of the RAM for the host that FTK Imager is running on



The table above outlines the most common options highlighted in red on the menu. Please refer to the user manual located in the help tab highlighted in *item 2* for definitions on the remainder.

5. Let us look at another important menu. This is the option called *Mode*. To get to it, select the **Mode** button at the top-left corner of the GUI, seen in *item 1* below, to reveal the menu as seen below:



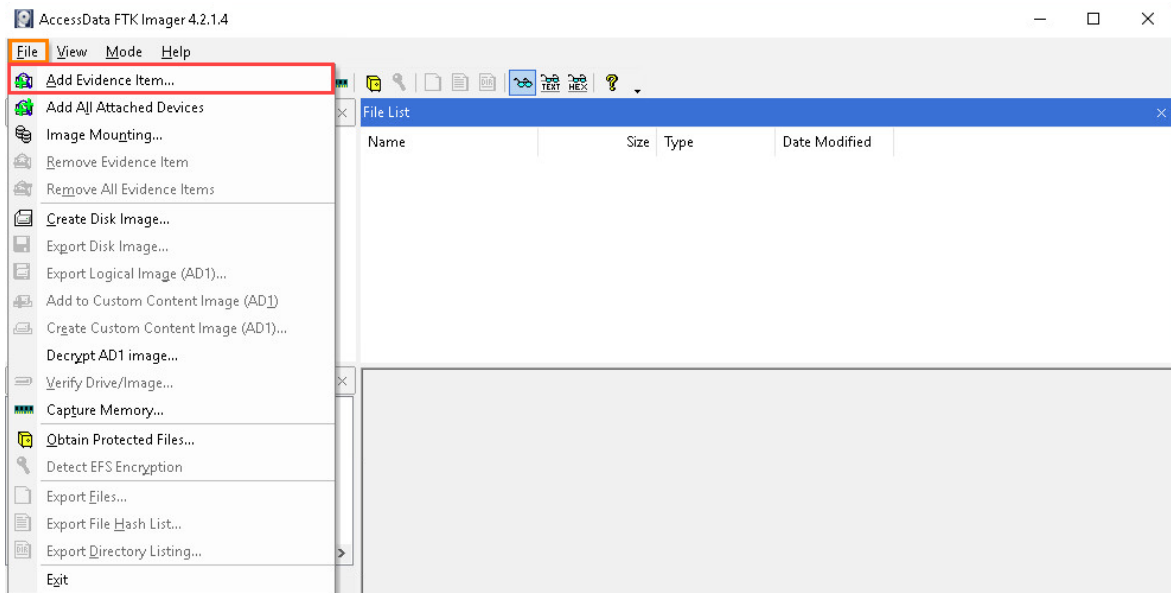
Expand Compound Files	The Expand Compound Files option, Toggles the option to expand compound files such as Zip, tar, etc.
Automatic	The Automatic option affects the view pane and allows the software to choose how to display a file (using IE, Text view, or Hex view).
Text	The Text option switches the view pane to only show selected files in raw text
Hex	The Hex option switches the view pane to only show selected files in Hexadecimal

6. The remaining menus are equally as important, but we will not cover them in this lab. Now, let us move on to the good stuff, creating a forensic image!

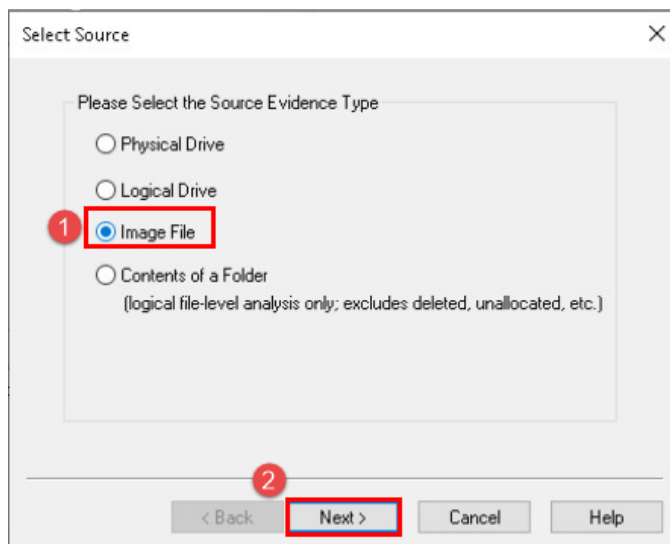
2 Locate the SAM File Using FTK Imager

Now that you are familiar with *FTK Imager*, let us use it to navigate to and extract a SAM file from a disk image. We will also provide instructions on how to extract the file on a live system.

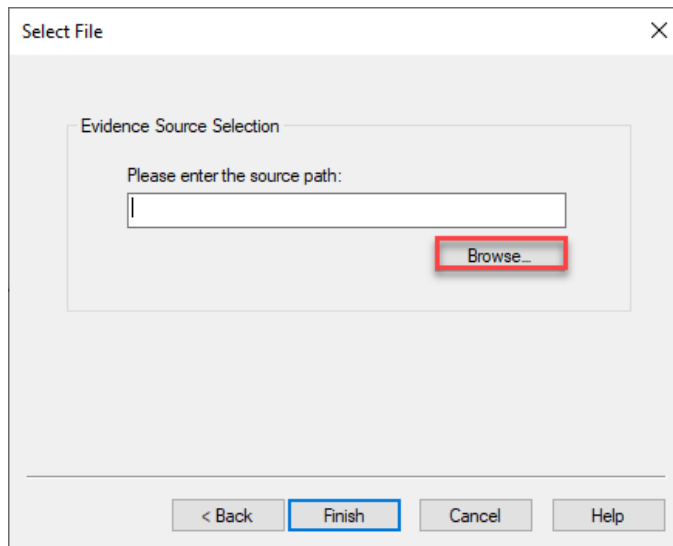
1. *FTK Imager* should already be open. If not, reopen it and navigate to **File > Add Evidence Item** as seen in *items 1 and 2* below. This will open the *Select Source* window that will allow you to choose the disk image file.



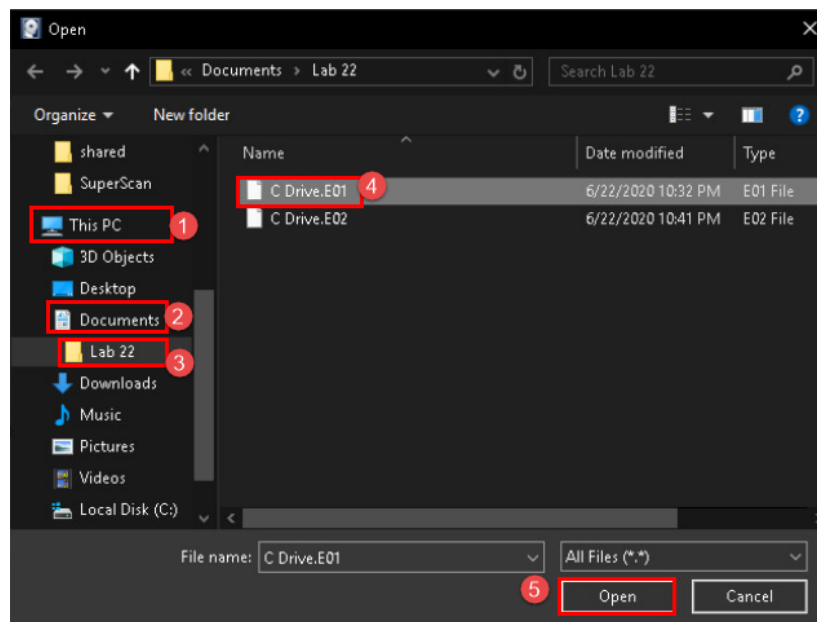
2. You will be brought to the *Select Source* window. Let us select **Image File** and click **Next** as highlighted in *items 1 and 2* below:



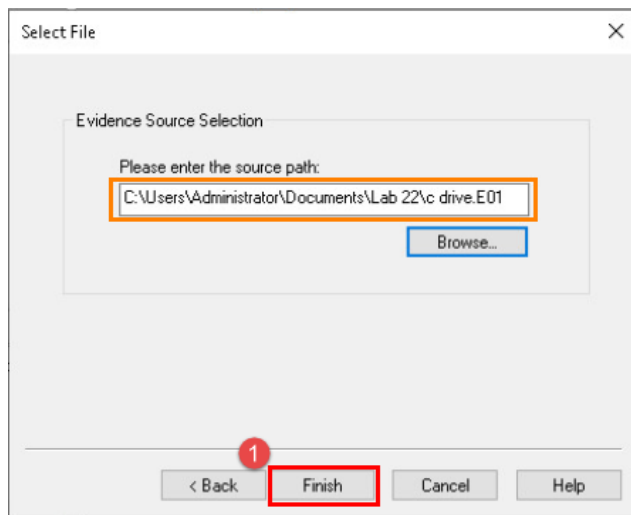
3. In the *Select File* window, click **Browse**, as highlighted in the screenshot below. This will open the *Select File* window, which will allow you to browse to the appropriate disk image file.



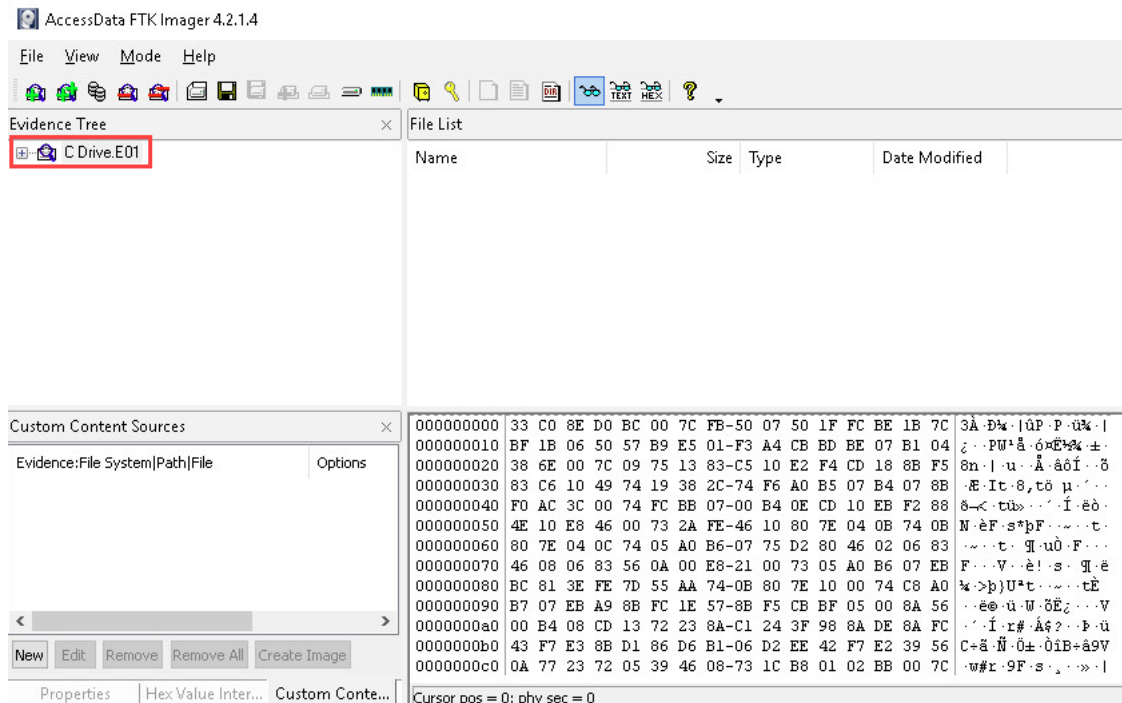
4. You are now at the *Select File* window. Browse to **This PC > Documents > Lab 22**. This will open the folder revealing the image file called *C Drive.E01*. Select the file called **C Drive.E01** and click the **Open** button as highlighted in *items 1, 2, 3, 4, and 5* below.



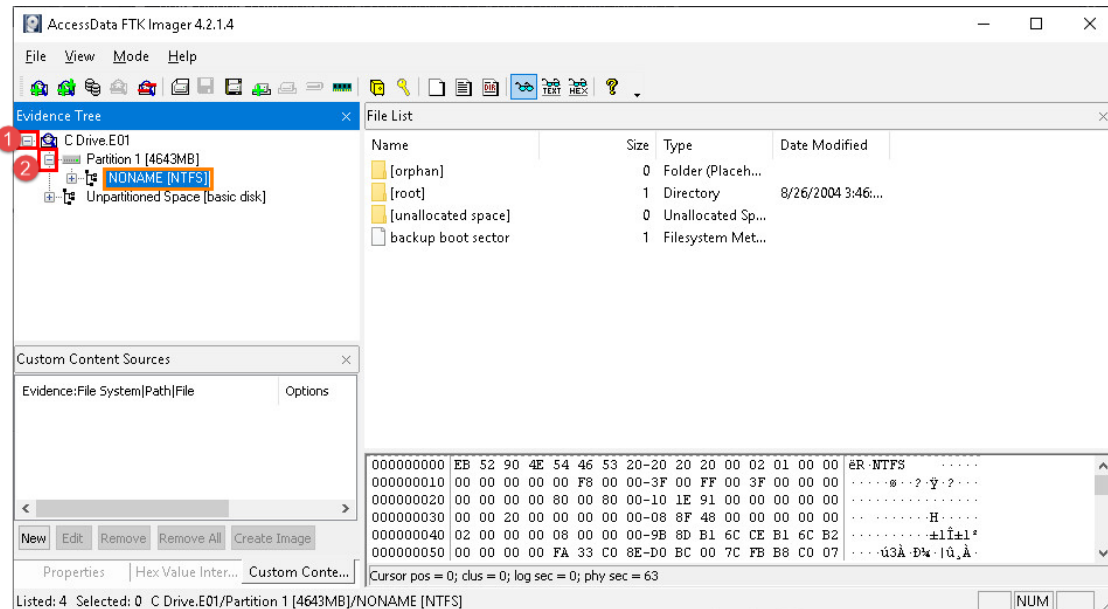
- Review the source path of the file called *C Drive.E01*. In the *Select File* window, click **Finish** highlighted in *item 1* below. This will take you back to the *FTK Imager's* main window, where the image file will be loaded.



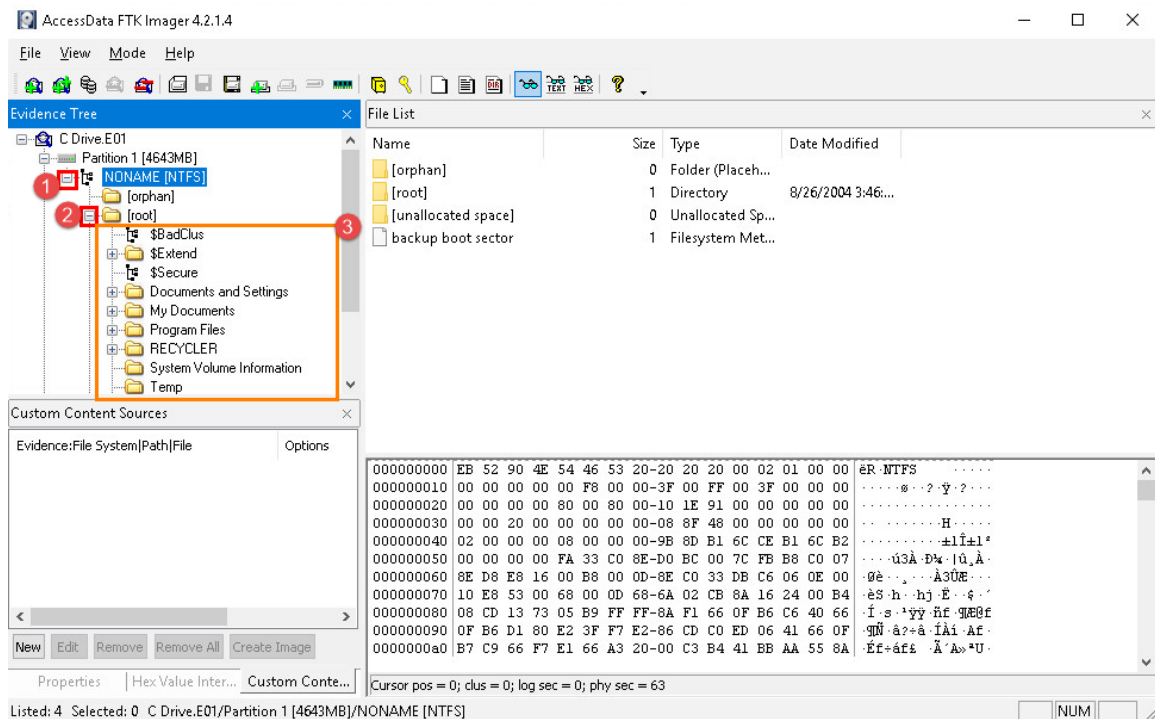
- If you did everything correctly, you will now be back at *FTK Imager's* main window with *C Drive.E01* listed under the *Evidence Tree* Pane. From the *Evidence Tree* pane, click the tree item **C Drive.E01** highlighted below. This will select the image you are going to peruse.



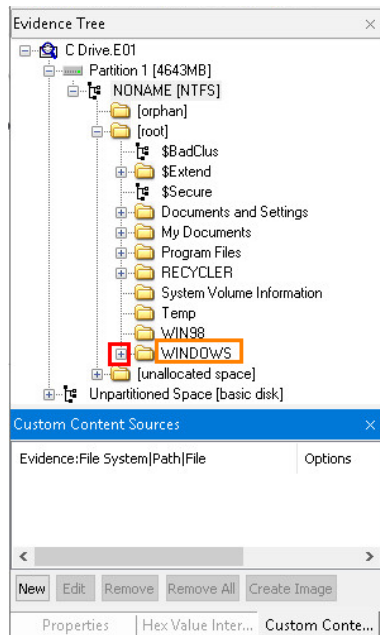
7. We will now browse the disk image file and view its contents. To begin, click the + sign beside the hard drive you added called **C Drive.E01**, as seen in *item 1*. This will expand the tree and display the partition on the drive. Click the + beside Partition 1, as seen in *item 2* below. Now that you can see the partition, let us learn how to identify the operating system files on a normal installation of *Microsoft Windows*.



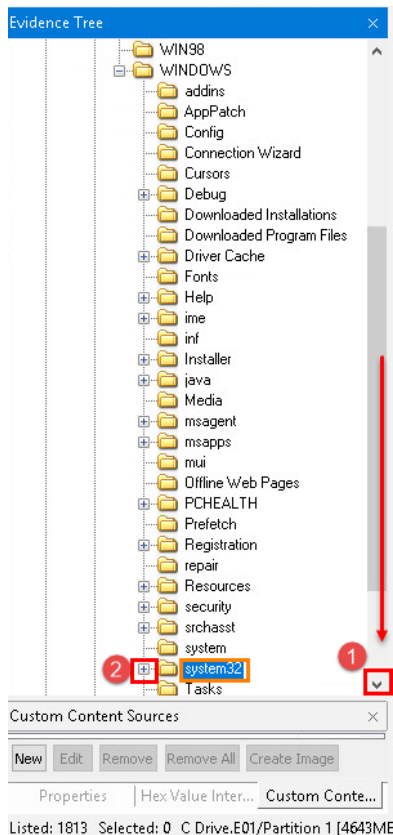
8. You will now be presented with the file system that is being used on the partition. The file system in the screenshot below is called *NONAME [NTFS]*, which indicates that the partition uses the New Technology File System (NTFS) file system. Let us expand the partition by clicking the + beside *NONAME [NTFS]*, as seen in *item 1* below. This will reveal three folders. The first folder is the *orphan* folder, and it contains deleted files that were recovered but have no parent folder. Next, there is the *root* folder that contains the operating system. The last folder is called *unallocated space* and represents free space as files. Let us expand the folder called *root* by clicking the + sign beside it, as seen in *item 2*. This root directory contains the *Microsoft Windows* operating system files, seen in *item 3*, and is represented as the *C:* drive in *Windows File Explorer*.



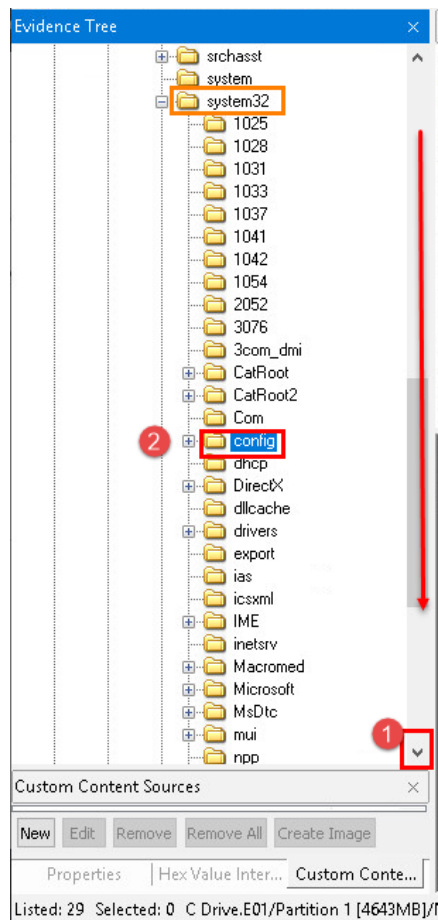
9. Now let us navigate to the folder that contains the **SAM** file. To begin, click the + beside the *Windows* folder to expand it.



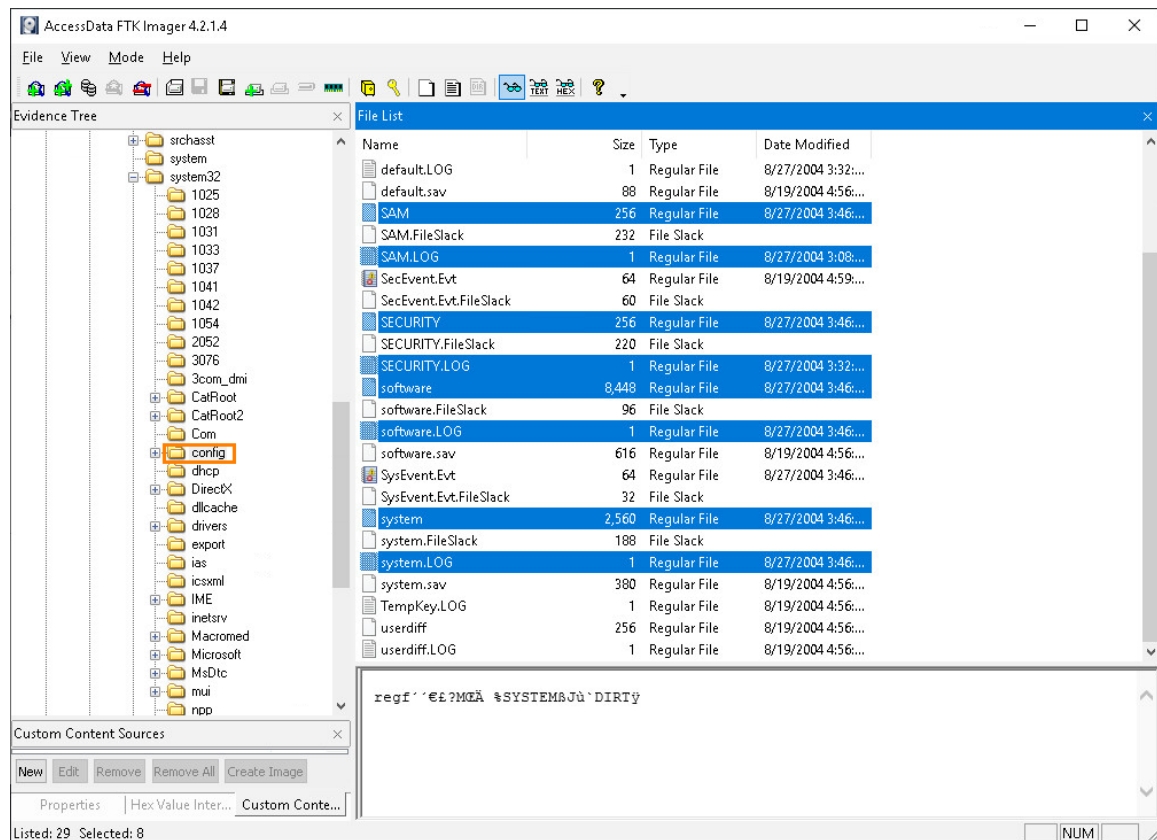
10. The *Windows* folder has many files and folders. The folder that contains the registry files is found in the *System32* folder and may require scrolling down to see it. Scroll until you see the *System32* folder and click the + sign beside it, highlighted as *item 2* below.



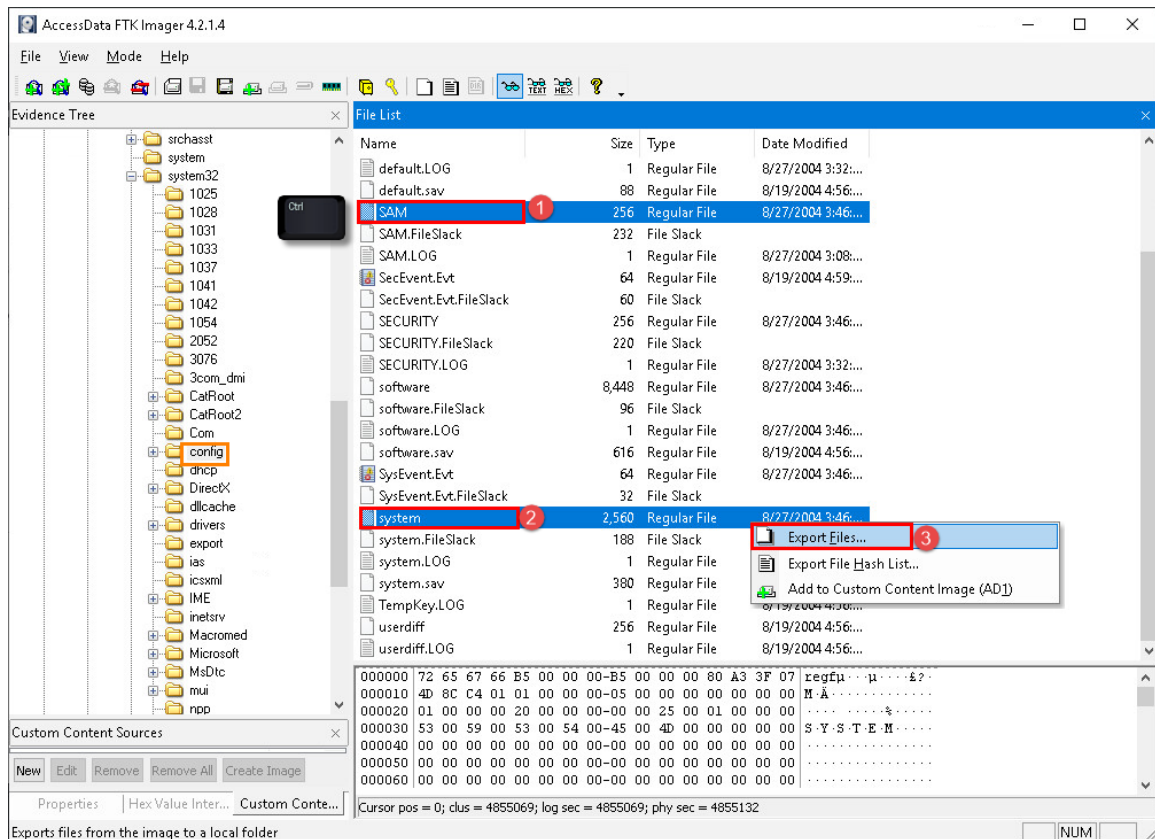
11. The *System32* folder is another folder that has many files and folders. We are looking for the folder called *config*. To get to it, you may need to scroll down in the **File Tree** pane. Once you see the *config* folder, click it as highlighted below:



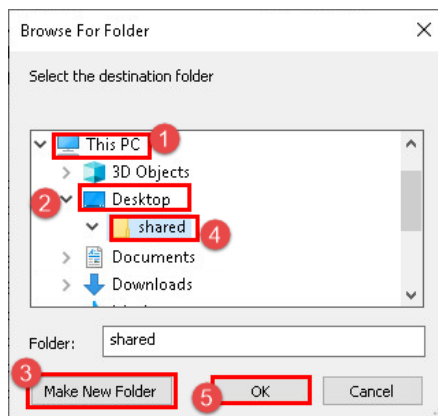
12. Now, let us look in the *File List* pane to identify the registry files. These are the system-wide registry files and are unique because they do not have file extensions. The screenshot below lists the different registry files on this system.



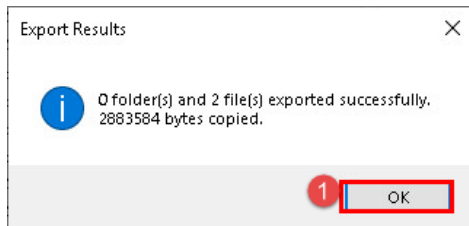
13. Now, let us export the **SAM** and **SYSTEM** files by holding **CTRL +** left-clicking on them, as seen in *items 1* and *2* below. Once the files are highlighted, right-click on the highlighted area and select the **Export Files...** option from the context menu that appears, as seen in *item 3* below. This will open the *Browse For Folder* window, which allows you to browse for the destination of the files.



14. Navigate to the **This PC > Desktop** folders and click the **Make New Folder** button as seen in *items 1, 2, and 3*. Name the folder **shared** and then click **OK** this will export the SAM registry file to the specified folder, as seen in *items 4 and 5* below.

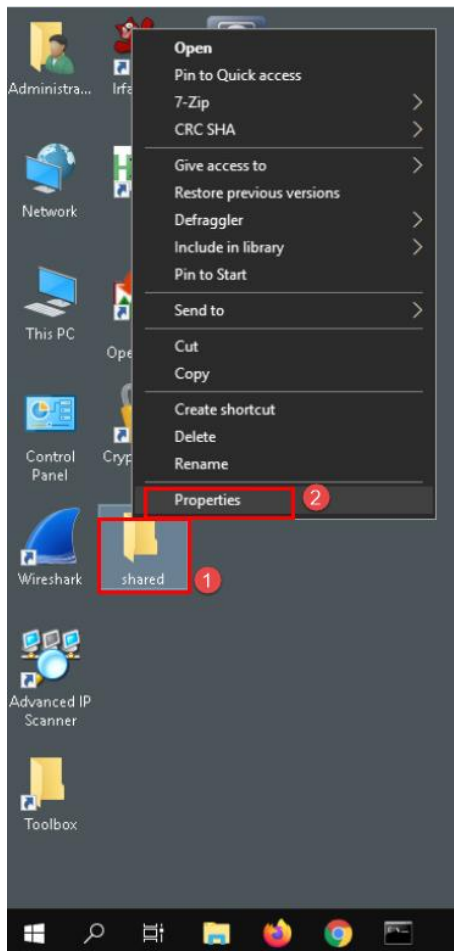


15. You will be prompted with the export results. Click **OK** to continue.

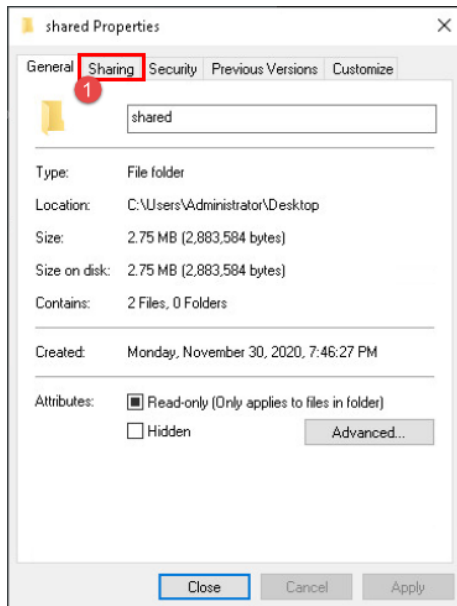


If you were unable to name the folder shared in step 14, please rename the *New folder* on the Desktop as *shared* before proceeding.

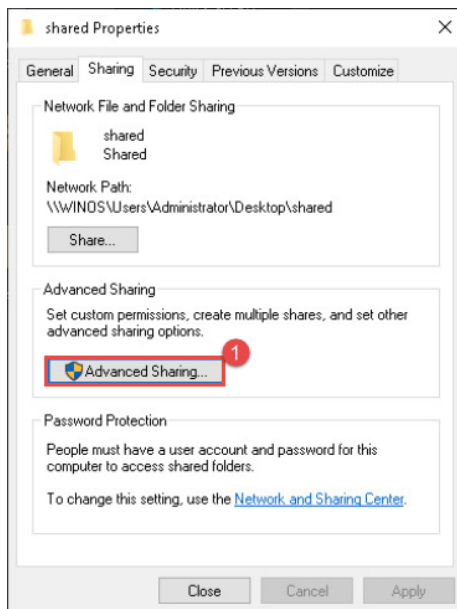
16. Now, let us navigate to the **Desktop** and locate the folder we created called **shared**, as seen in *item 1*. Next, right-click on the folder and select **Properties**, as seen in *item 2* below.



17. The folder's properties window will appear. Next, select the tab **Sharing** as seen in item 1 below.

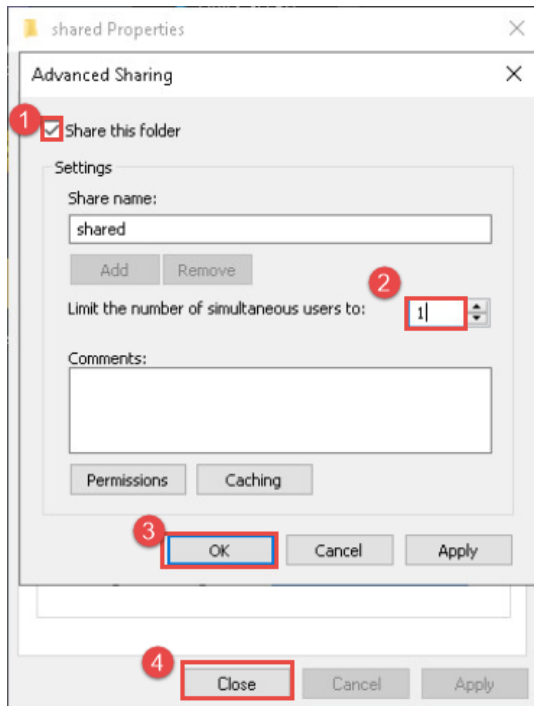


18. Let us set custom permissions for the folder. Select **Advanced Sharing...** as seen in item 1 below. This will open the *Advanced Sharing* window.



If prompted by a User Account Control warning, click **YES**.

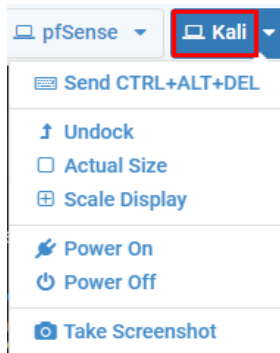
19. In the *Advanced Sharing* window, select the checkbox beside **Share this folder**, as seen in *item 1*. Now, let us reduce the number of users that can access the shared folder. Change the value to one (1), click **OK**, and then **Close** as highlighted in *items 2, 3, and 4* below.



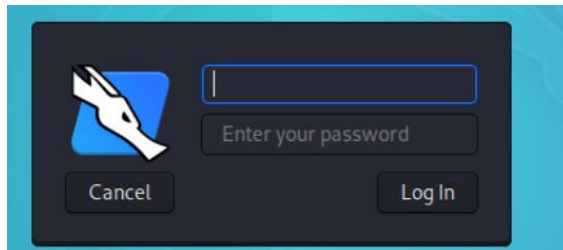
3 Accessing the SAM and SYSTEM Registry File from Kali Linux

Once the SAM and SYSTEM registry files are extracted from the Forensic Image file, we will need to copy them over to our Kali Linux environment. Both files are needed to extract the password hashes. In Kali Linux, we can use several tools to get this done but before we do that, let's get the files.

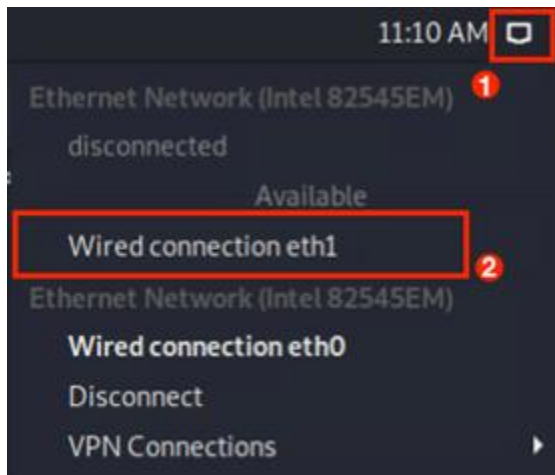
1. Launch the **Kali Linux** virtual machine to access the graphical login screen.



- 1.1. Log in as **root** using the password: **toor**

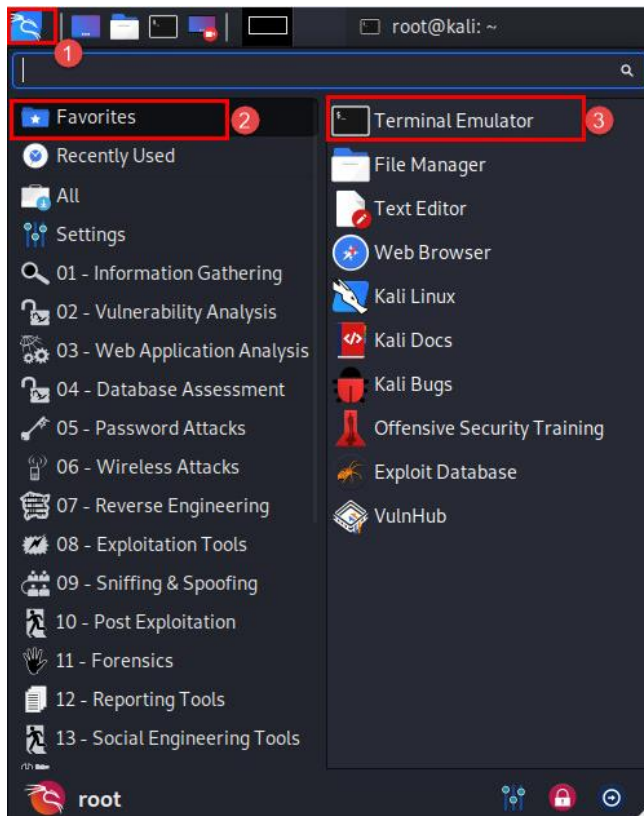


2. Before starting the lab, ensure that the host machine is on the same network as the target machine. Select the **Ethernet network connection** from the navigation panel, as seen in *item 1*. Then click **Wired connection eth1** to enable Kali Linux to configure with the IP address 192.168.0.2, as seen in *item 2*.



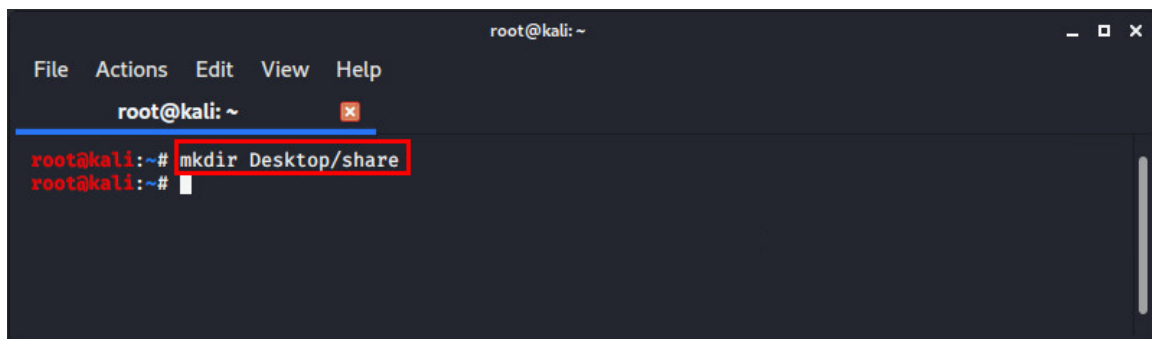
The target machine is on the network 192.168.0.0/24. The Kali Linux VM is configured with both IP address and can easily be interchanged.

3. Let us start by launching **Terminal Emulator**. To do this, navigate to **Whisker Menu > Favorites > Terminal Emulator** as seen in items **1**, **2**, and **3** below.



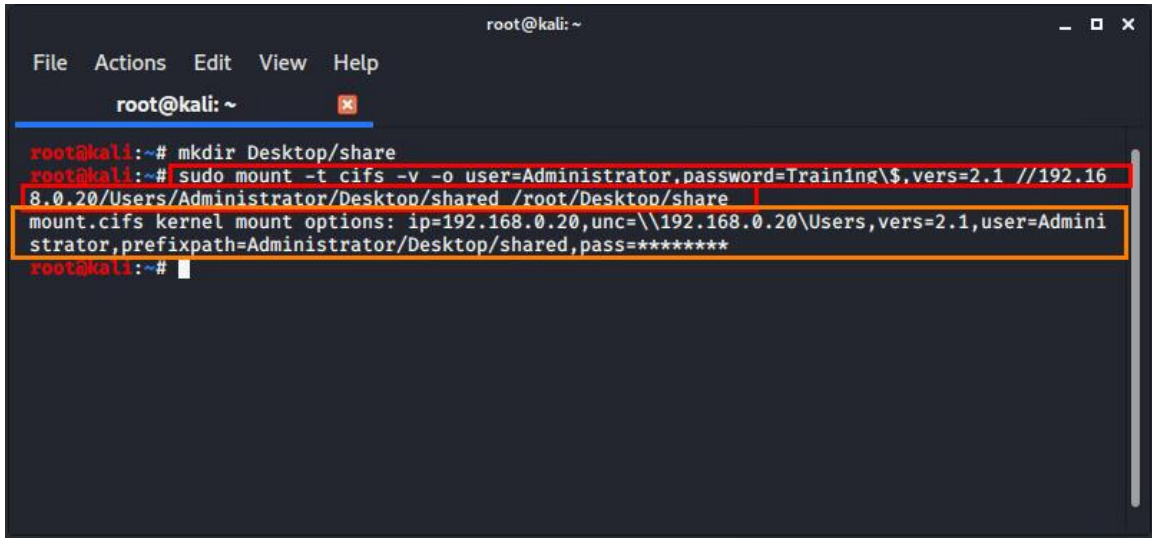
4. To create a folder called **share** on the Desktop, type the command **mkdir Desktop/share** and press **Enter**. We will use this folder as the mount point to access the registry files from Windows VM.

```
root@kali:~# mkdir Desktop/share
```



5. Now, Type the command `sudo mount -t cifs -v -o user=Administrator,password=Train1ng\$,vers=2.1 //192.168.0.20/Users/Administrator/Desktop/shared /root/Desktop/share/` and press **Enter**. If done correctly, you should now have access to the files.

```
root@kali:~# sudo mount -t cifs -v -o user=Administrator,password=Train1ng\$,vers=2.1 //192.168.0.20/Users/Administrator/Desktop/shared /root/Desktop/share/
```

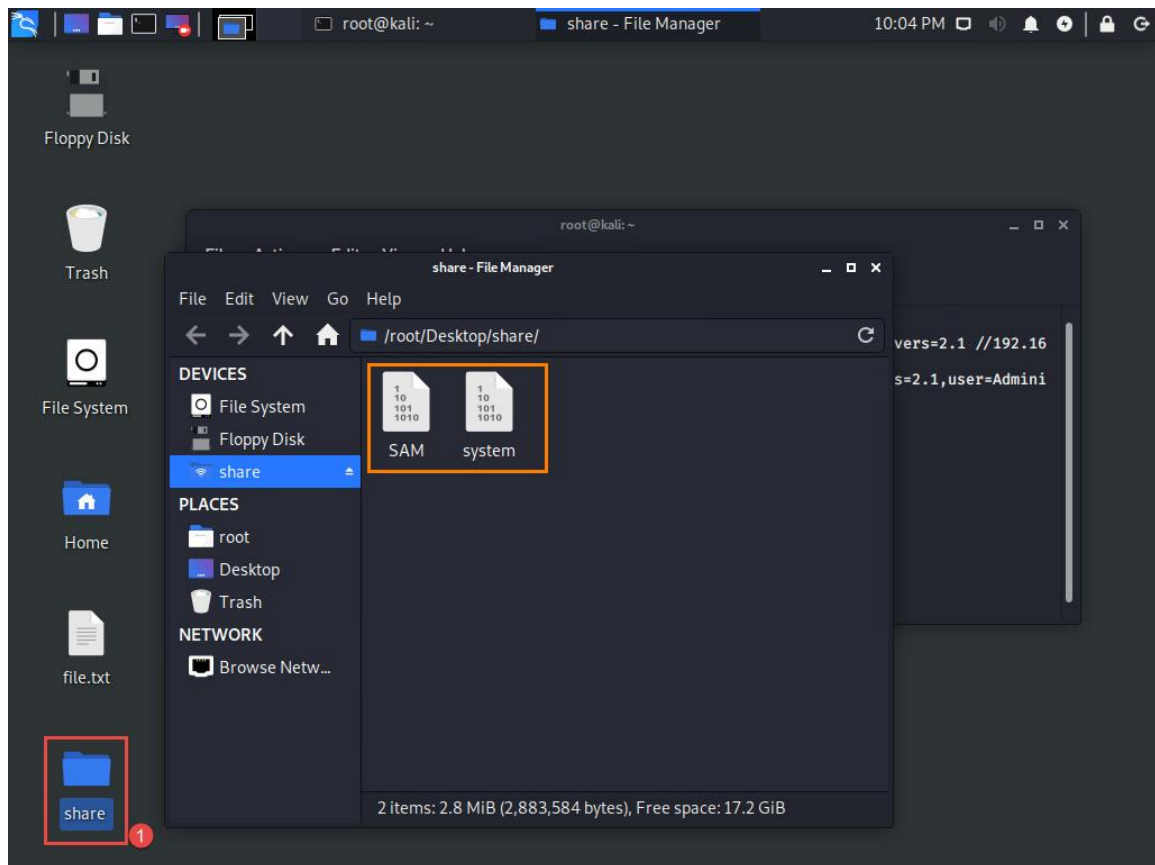


```
root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali:~# mkdir Desktop/share
root@kali:~# sudo mount -t cifs -v -o user=Administrator,password=Train1ng\$,vers=2.1 //192.168.0.20/Users/Administrator/Desktop/shared /root/Desktop/share
mount.cifs kernel mount options: ip=192.168.0.20,unc=\\192.168.0.20\Users,vers=2.1,user=Administrator,prefixpath=Administrator/Desktop/shared,pass=*****
root@kali:~#
```

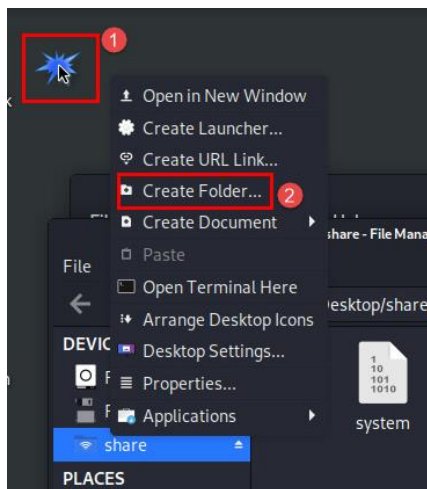


This command will mount the shared folder from the Windows VM to the created folder in Kali Linux.

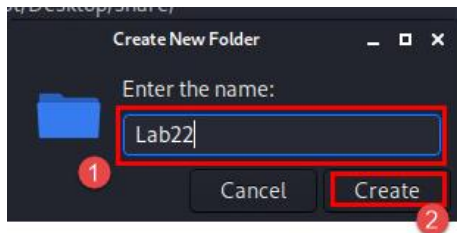
6. Navigate to the **Desktop** and double-click the folder **share**, as seen in *item 1* below. It will open the folder's *File Manager* window. Here you should see both **SAM** and **SYSTEM** registry files previously extracted from the Forensics Image file.



7. Let us create a permanent location to store these files. To do this, select anywhere on the Desktop and right-click as seen in *item 1*. This will open a submenu, select **Create Folder...** as seen in *item 2* below. This will open a *Create New Folder* window.

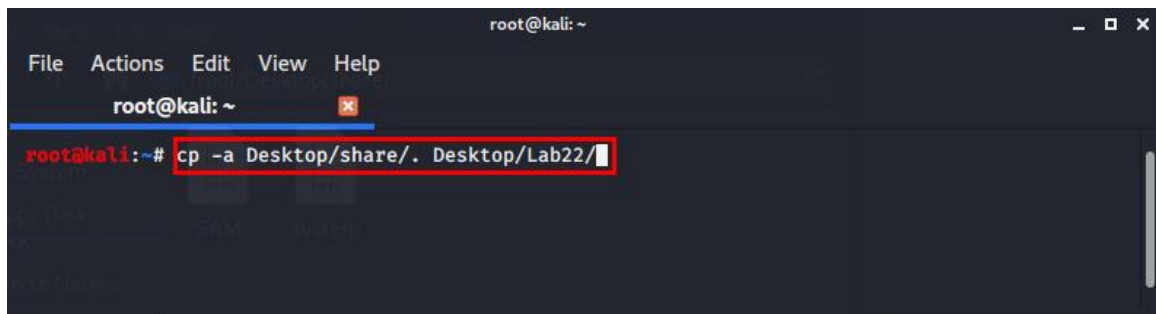


8. Name the folder **Lab22** and select **Create**, as seen in *items 1 and 2* below.



9. Switch to the command line terminal. Type the command `cp -a Desktop/share/. Desktop/Lab22` and press **Enter**. This will copy the contents of the folder **share** to the newly created folder **Lab22**.

```
root@kali:~# cp -a Desktop/share/. Desktop/Lab22
```

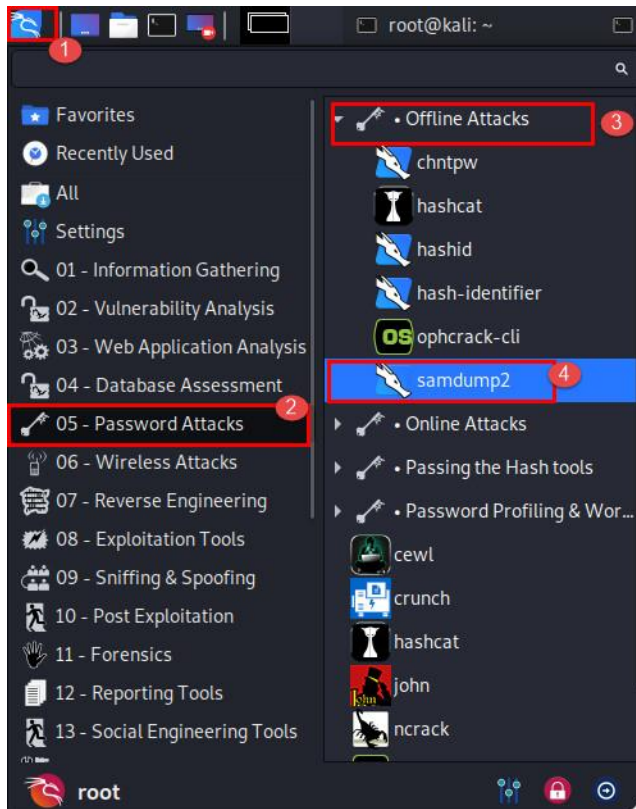


10. We are now done with this exercise. Move on to the next section, where we will attempt to gain the user account password from the SAM file.

4 Extracting Passwords from the SAM File

Let us use the command line tool *samdump2* and *John the Ripper* to achieve our goal.

1. Let us start by launching **samdump2**. To do this, navigate to **Whisker Menu > Password Attacks > Offline Attacks > samdump2** as seen in *items 1, 2, 3, and 4* below.



2. This will open a terminal emulator. Type the command `samdump2 -o Desktop/Lab22/hash.txt Desktop/Lab22/system Desktop/Lab22/SAM` and press **Enter**.

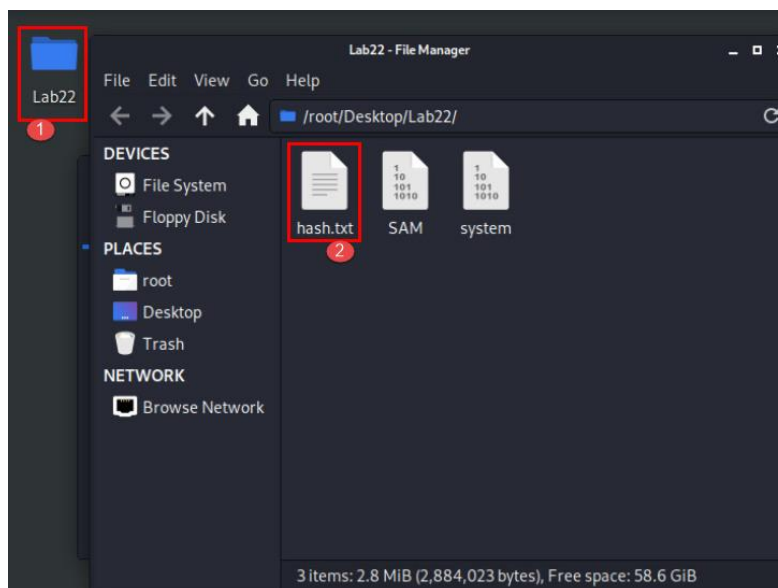
```
root@kali:~# samdump2 -o Desktop/Lab22/hash.txt Desktop/Lab22/system Desktop/Lab22/SAM
```

3. A breakdown of this command can be seen in the table below.

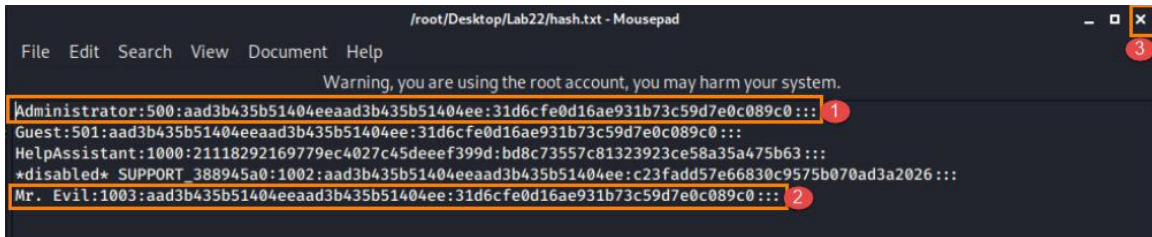
```
root@kali:~# 1 samdump2 2 -o Desktop/Lab22/hash.txt 3 Desktop/Lab22/system 4 Desktop/Lab22/SAM
```

1	<i>Item 1</i> is the command that fetches the SYSKEY and extracts the hashes from the SAM file
2	<i>Item 2</i> is the option tag that outputs the parsed data to the provided file
3	<i>Item 3</i> is the path for the System registry file
4	<i>Item 4</i> is the path for the SAM registry file

4. Let us look at the parsed results. Navigate to the **Desktop** and open the folder **Lab22** highlighted in *item 1*. Then, double-click the output file **hash.txt**, as seen in *item 2* below.



5. A *Mousepad* window should open, displaying the contents of the file. We are only interested in the accounts highlighted as *items 1* and *2*, the **Administrator** and **Mr. Evil**. After observing the hashes for both, click the **X** to the right of the window to close it, as seen in *item 3* below.



```

/root/Desktop/Lab22/hash.txt - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: 1
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:21118292169779ec4027c45deef399d:bd8c73557c81323923ce58a35a475b63:::
*disabled* SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:c23fadd57e66830c9575b070ad3a2026:::
Mr. Evil:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: 2

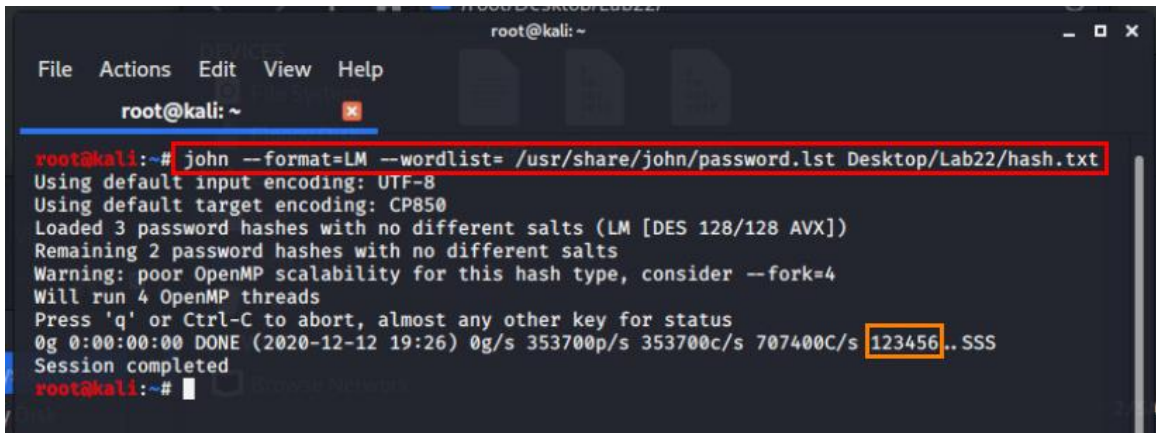
```



Both hashes are the same, indicating that the passwords are identical.

6. Go back to the terminal emulator. Type the command `john --format=LM --wordlist=/usr/share/john/password.lst Desktop/Lab22/hash.txt` and press **Enter**.

```
root@kali:~# john --format=LM --wordlist=
/usr/share/john/password.lst Desktop/Lab22/hash.txt
```



```

root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali:~# john --format=LM --wordlist= /usr/share/john/password.lst Desktop/Lab22/hash.txt
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 3 password hashes with no different salts (LM [DES 128/128 AVX])
Remaining 2 password hashes with no different salts
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2020-12-12 19:26) 0g/s 353700p/s 353700c/s 707400C/s 123456..SSS
Session completed
root@kali:~#

```



This process will only work on the earlier versions of Windows XP/NT/Vista.

7. The results indicated that the password is **123456**. You are now at the end of the lab. Close all the open programs and windows.