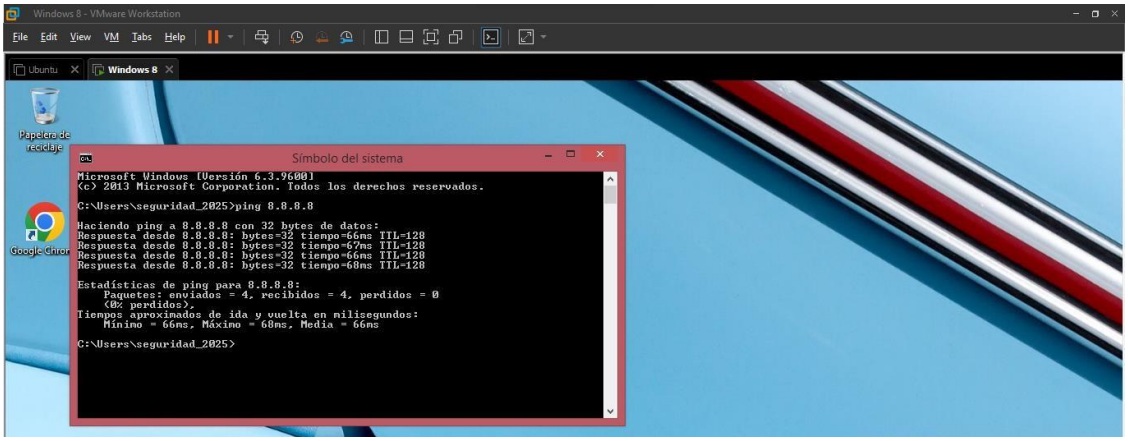
PRACTICA N ° 1 SEGURIDAD DE SISTEMAS SIS-737S1	
Estudiante: Miguel Angel Mollo Porco RU: 66810 Fecha de Entrega: 18/04/2025	
Docente: Ing. J. Alexander Duran M.	Auxiliar: Univ. Aldrin Perez Miranda

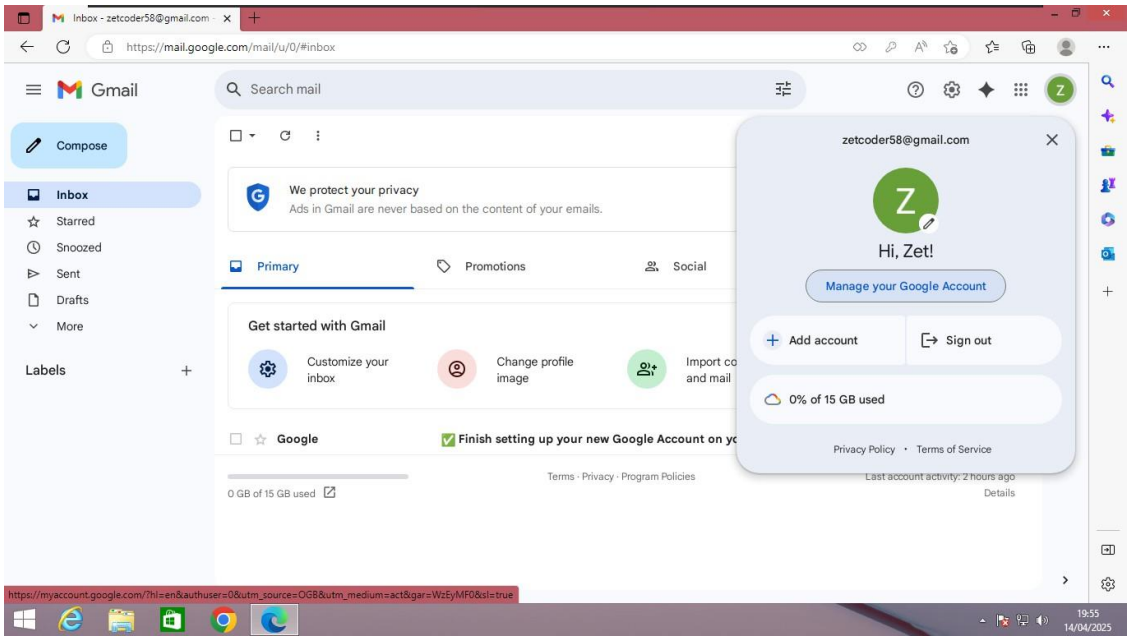
PARTE 1

Modificar parámetros de correo:

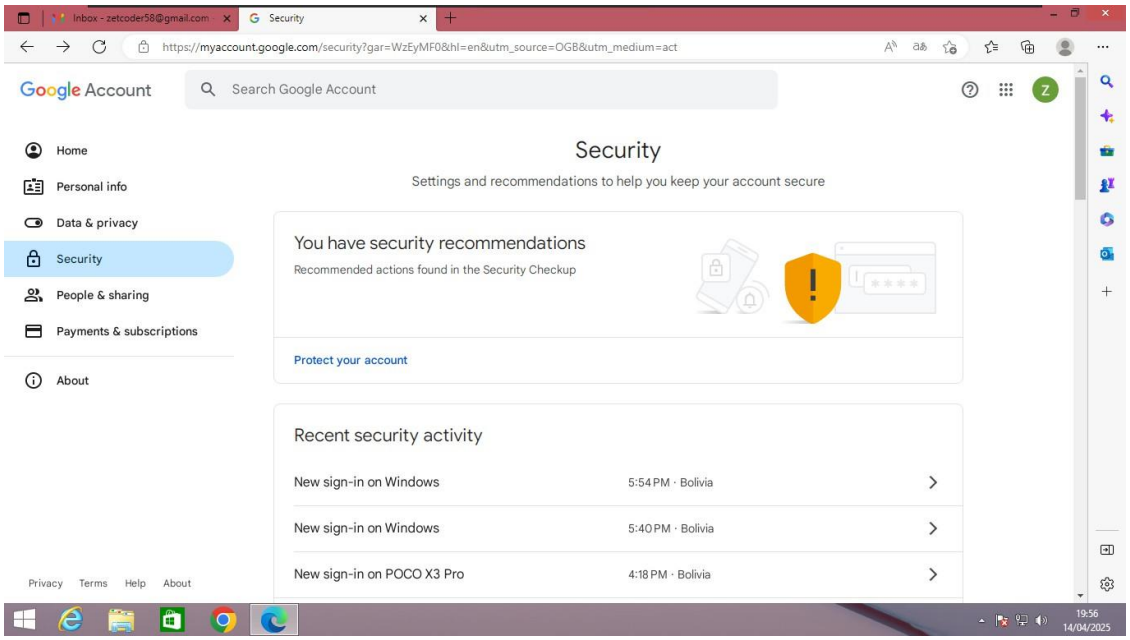
1.



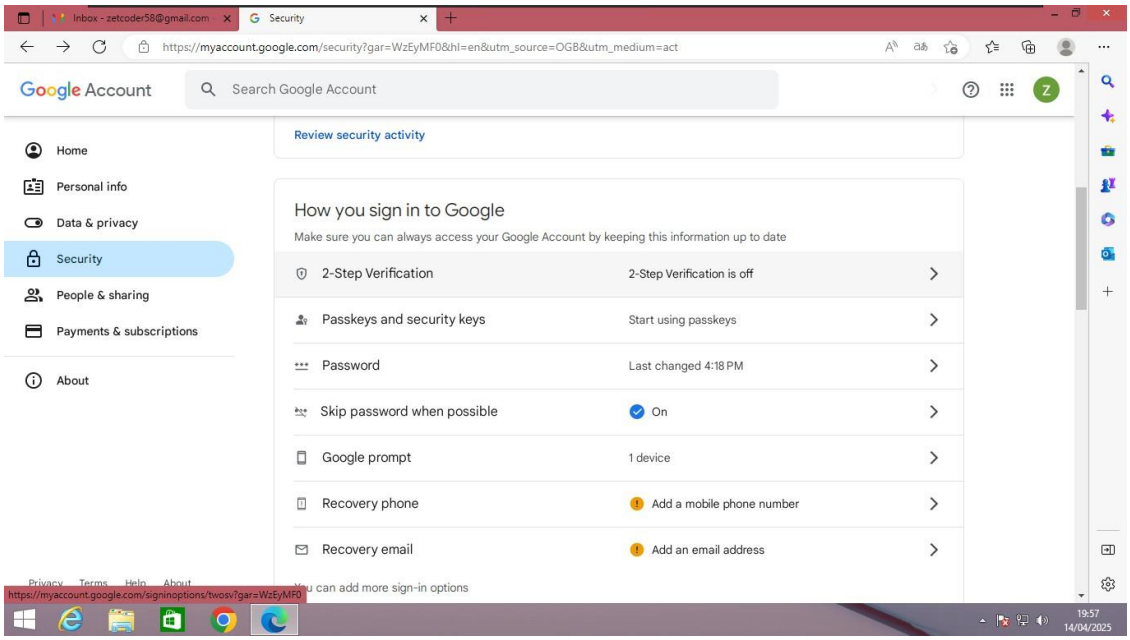
2.


Inbox - zetcoder58@gmail.com
https://mail.google.com/mail/u/0/#inbox
Gmail
Search mail
Compose
Inbox
Starred
Snoozed
Sent
Drafts
More
Labels
We protect your privacy
Ads in Gmail are never based on the content of your emails.
Primary
Promotions
Social
Get started with Gmail
Customize your inbox
Change profile image
Google
0 GB of 15 GB used
zetcoder58@gmail.com
Hi, Zet!
Manage your Google Account
Add account
Sign out
0% of 15 GB used
Privacy Policy · Terms of Service
https://myaccount.google.com/?hl=en&authuser=0&utm_source=OGB&utm_medium=act&gar=WzEyMF0&sl=true

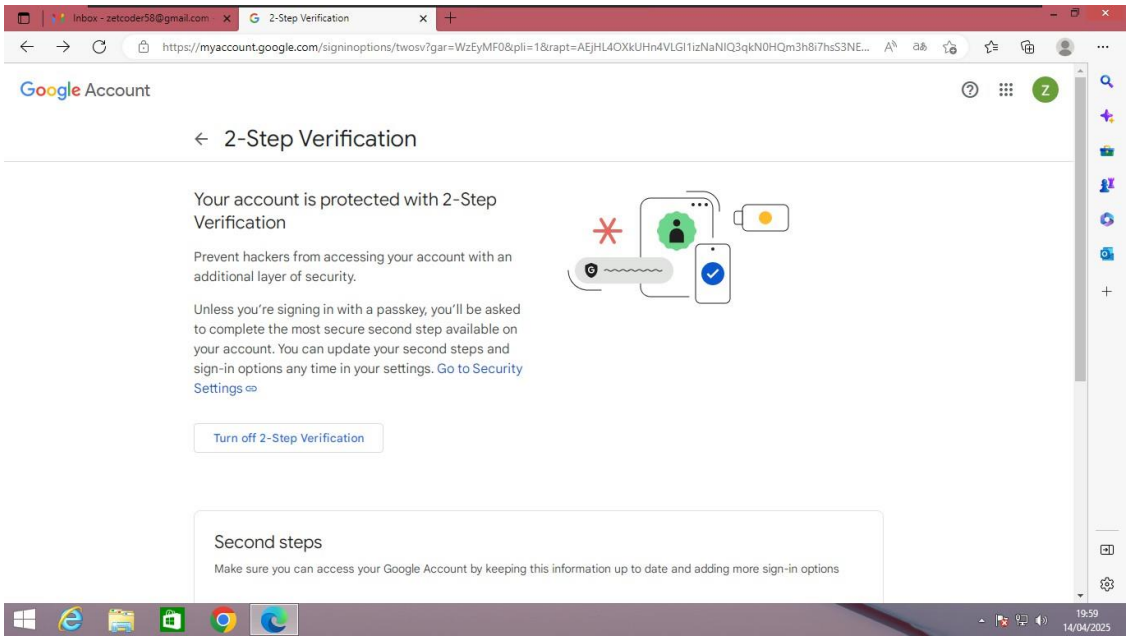
3.


Inbox - zetcoder58@gmail.com
Security
https://myaccount.google.com/security?gar=WzEyMF0&hl=en&utm_source=OGB&utm_medium=act
Google Account
Search Google Account
Home
Personal info
Data & privacy
Security
People & sharing
Payments & subscriptions
About
Privacy Terms Help About
Security
Settings and recommendations to help you keep your account secure
You have security recommendations
Recommended actions found in the Security Checkup
Protect your account
Recent security activity
New sign-in on Windows 5:54 PM · Bolivia
New sign-in on Windows 5:40 PM · Bolivia
New sign-in on POCO X3 Pro 4:18 PM · Bolivia

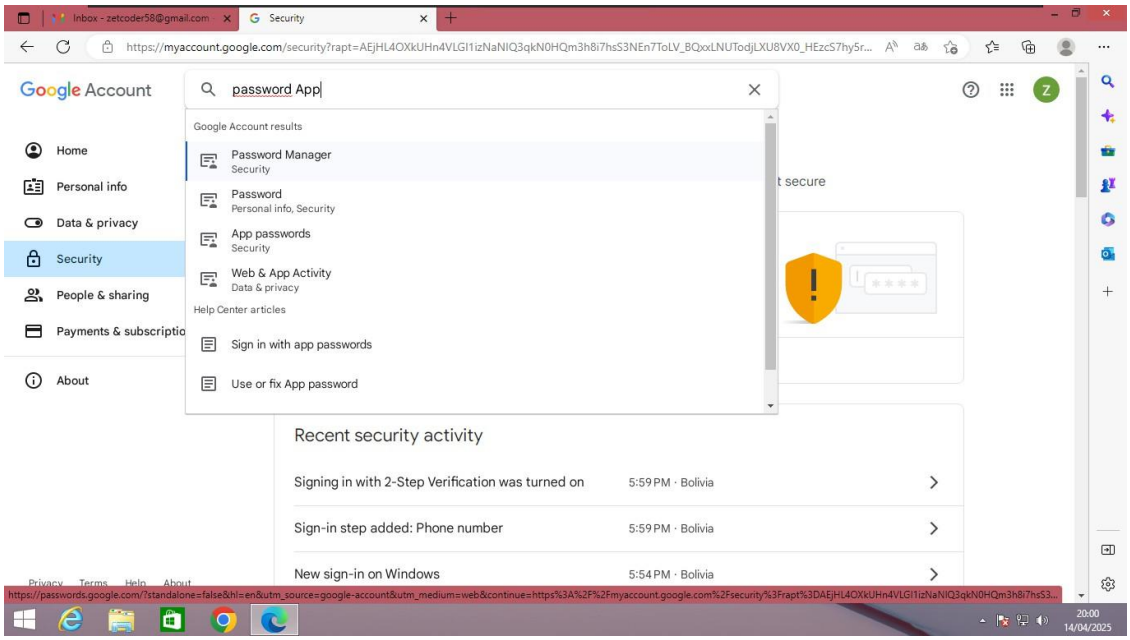
4.



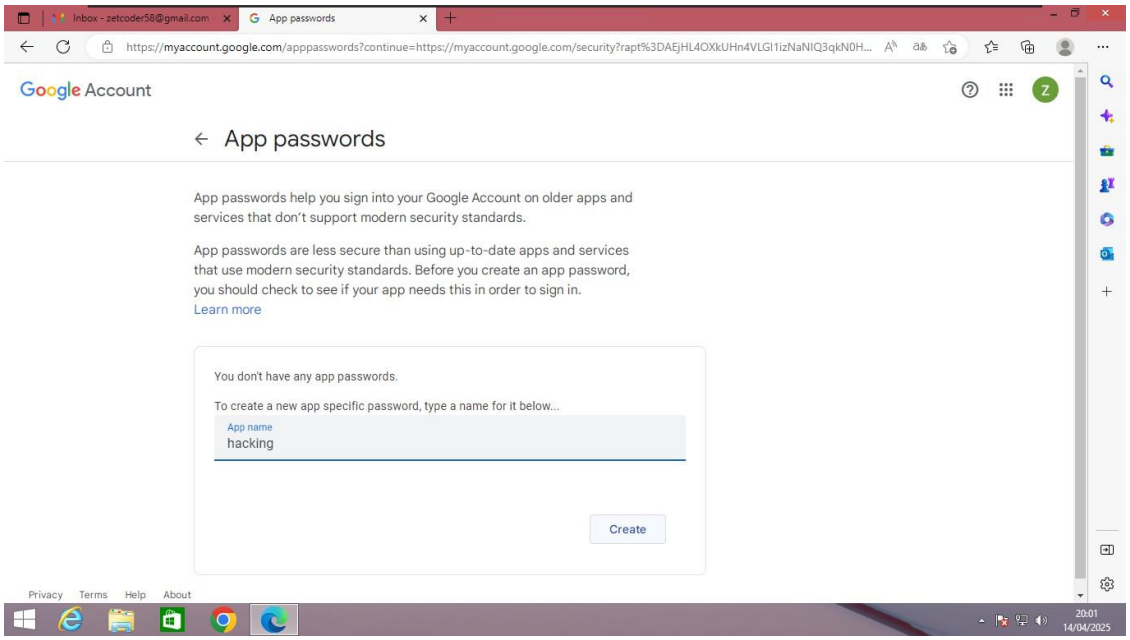
5. activar verificación de 2 pasos



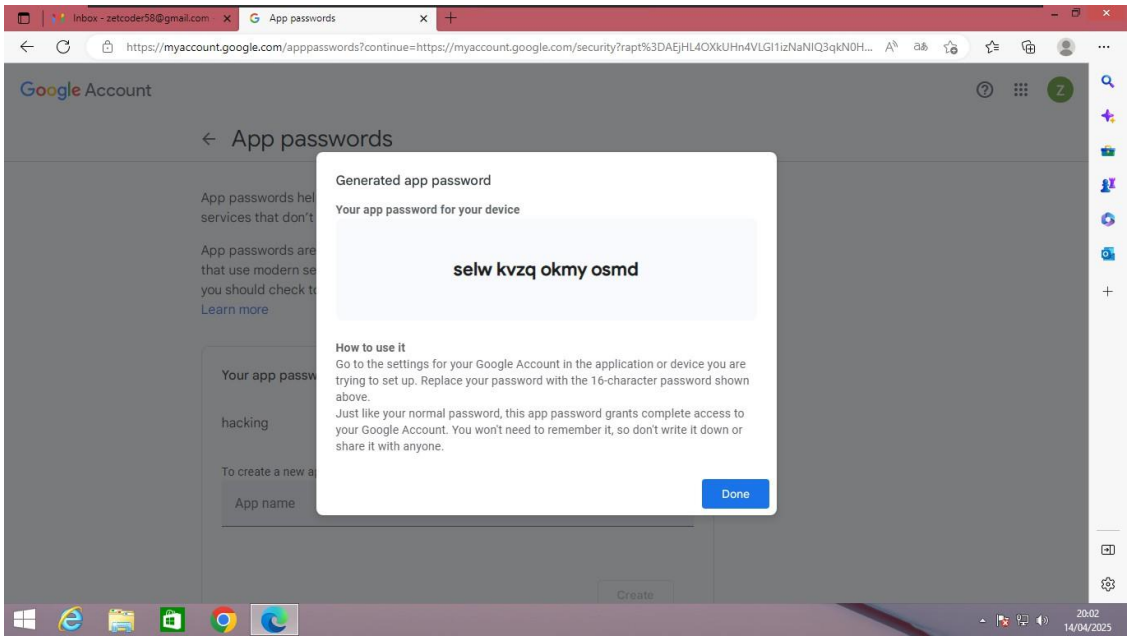
6.


Google Account
password App
Google Account results
Password Manager
Security
Password
Personal info, Security
App passwords
Security
Web & App Activity
Data & privacy
Help Center articles
Sign in with app passwords
Use or fix App password
Home
Personal info
Data & privacy
Security
People & sharing
Payments & subscriptio
About
Recent security activity
Signing in with 2-Step Verification was turned on 5:59 PM · Bolivia
Sign-in step added: Phone number 5:59 PM · Bolivia
New sign-in on Windows 5:54 PM · Bolivia

7.


Google Account
App passwords
App passwords help you sign into your Google Account on older apps and services that don't support modern security standards.
App passwords are less secure than using up-to-date apps and services that use modern security standards. Before you create an app password, you should check to see if your app needs this in order to sign in.
Learn more
You don't have any app passwords.
To create a new app specific password, type a name for it below...
App name
hacking
Create
Privacy Terms Help About

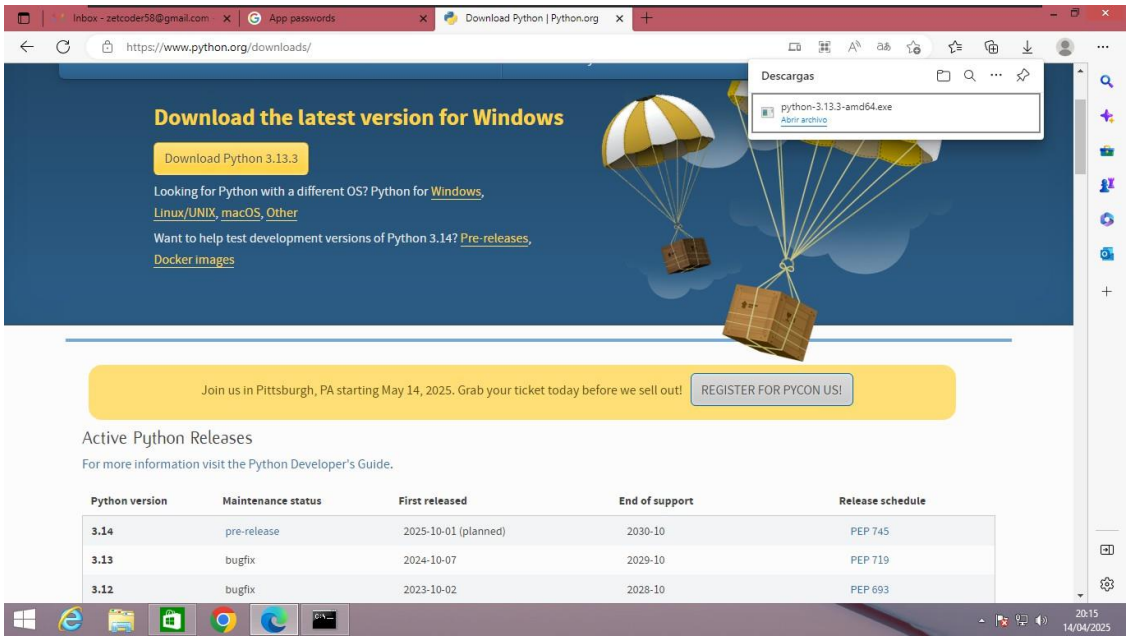
8.

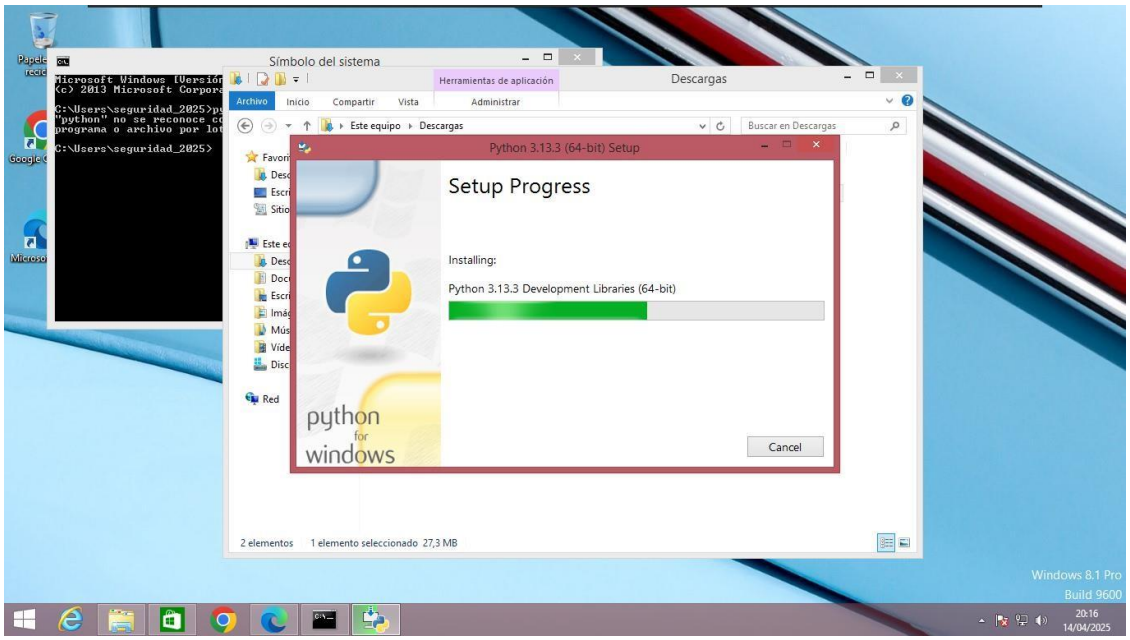


Actualizar Parametros

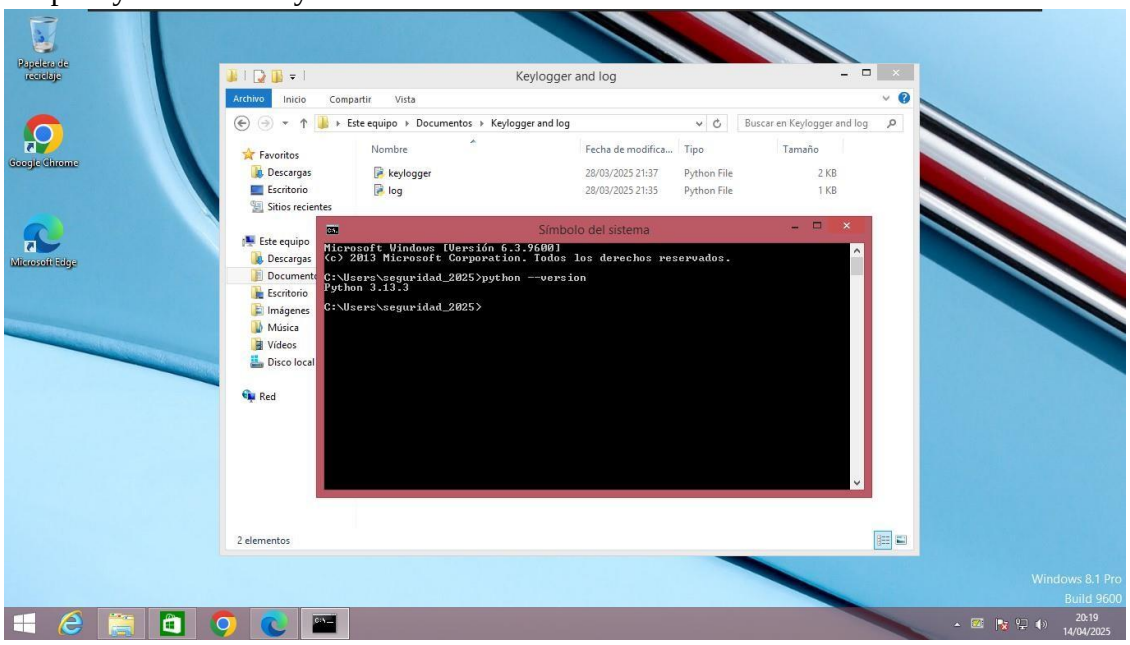
3.

Instalamos Python

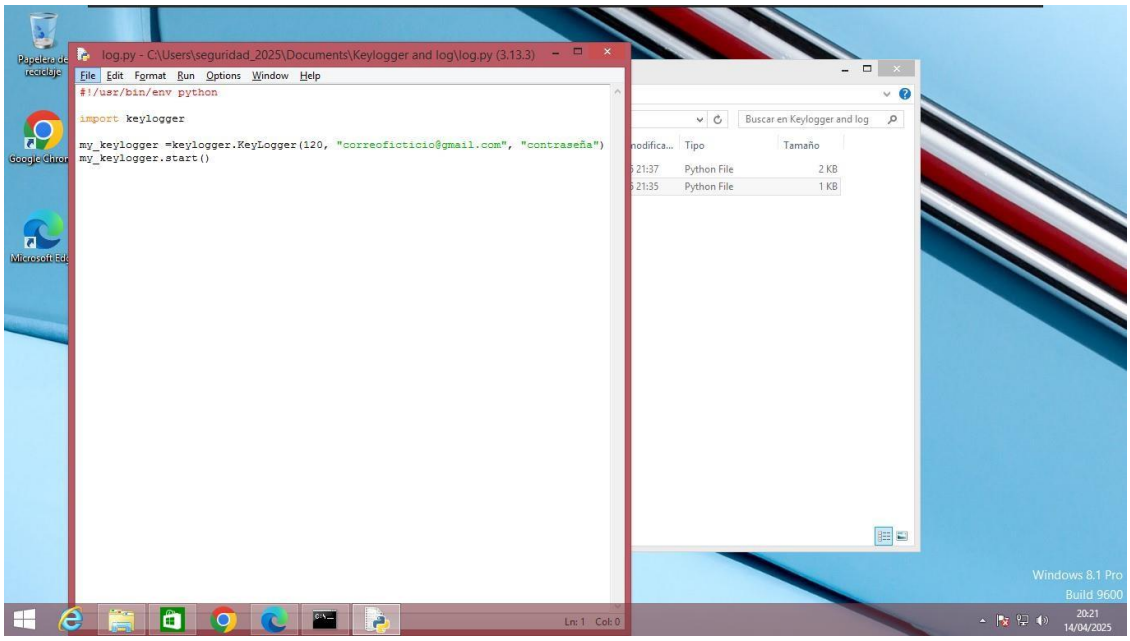




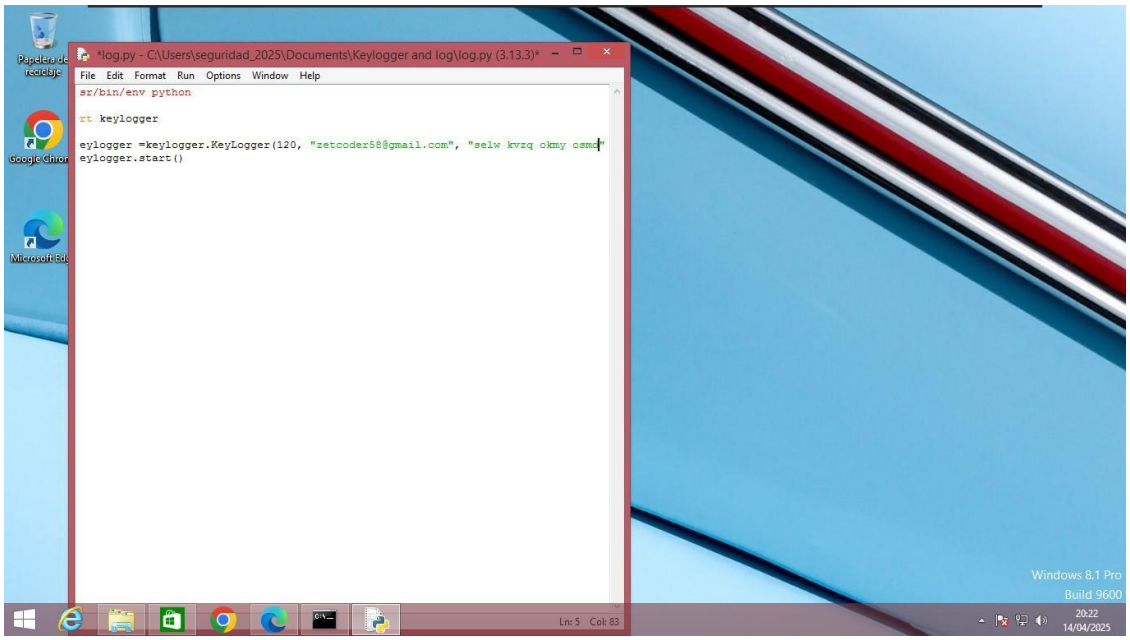
Carpeta y versión de Python:



Edith

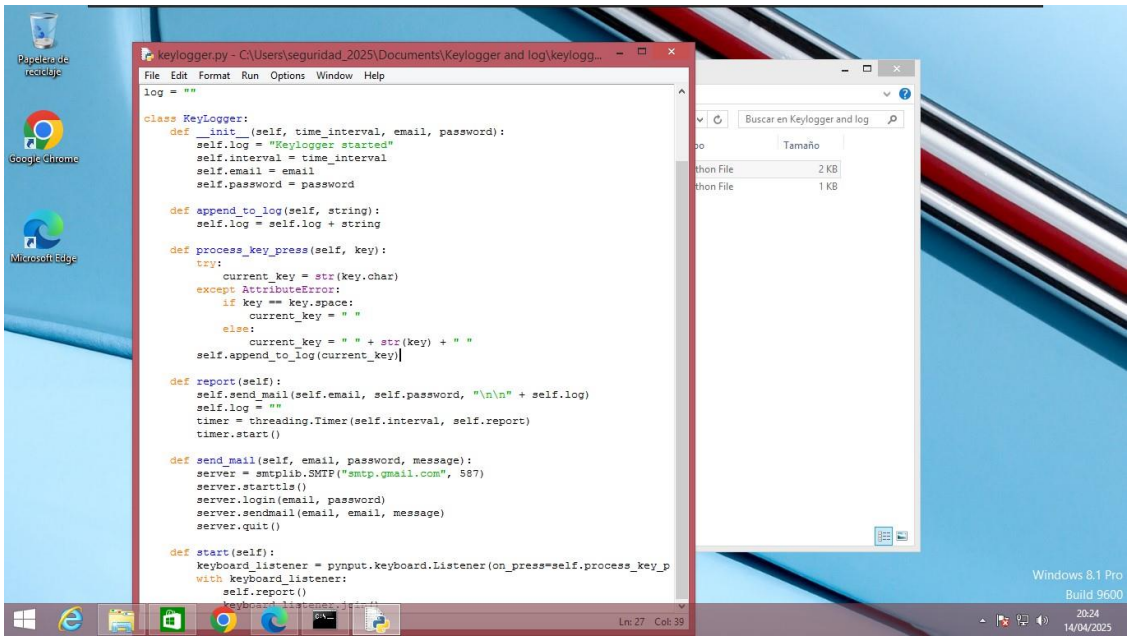


Cambio contraseñas



Guardamos y cerramos

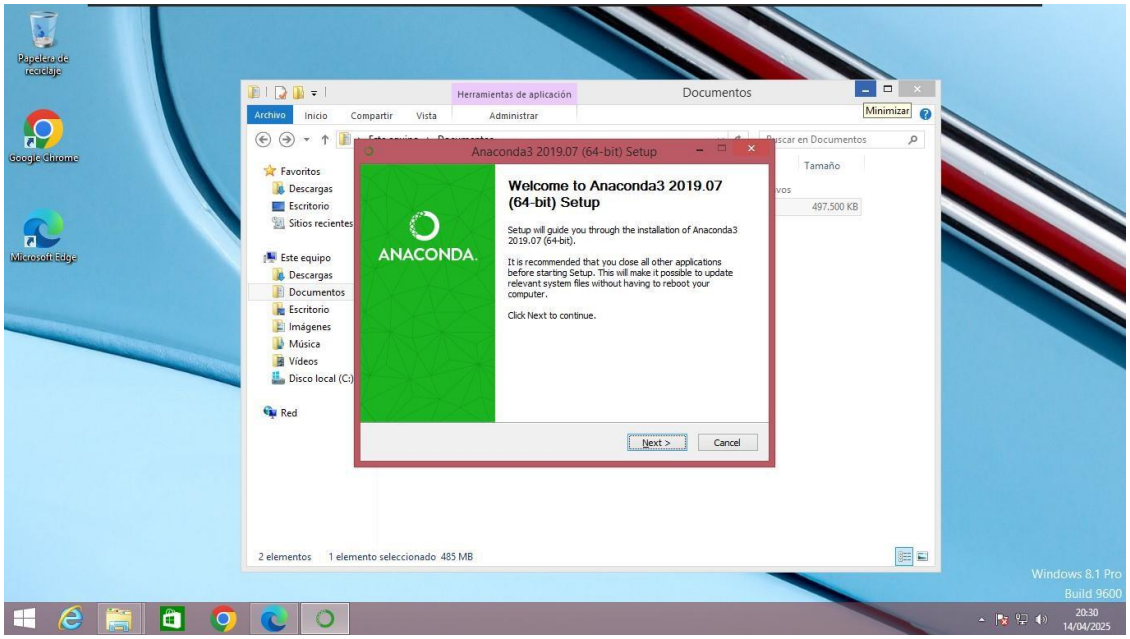
Abriendo keylogger.py

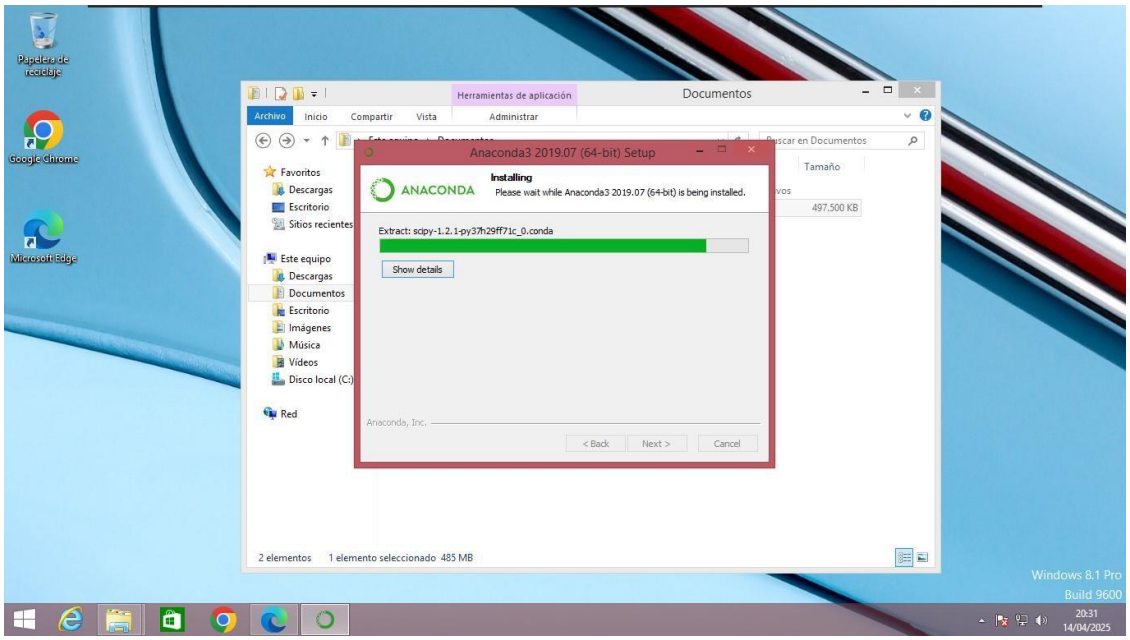


EMPAQUETAMOS EL ARCHIVO EJECUTABLE

4.

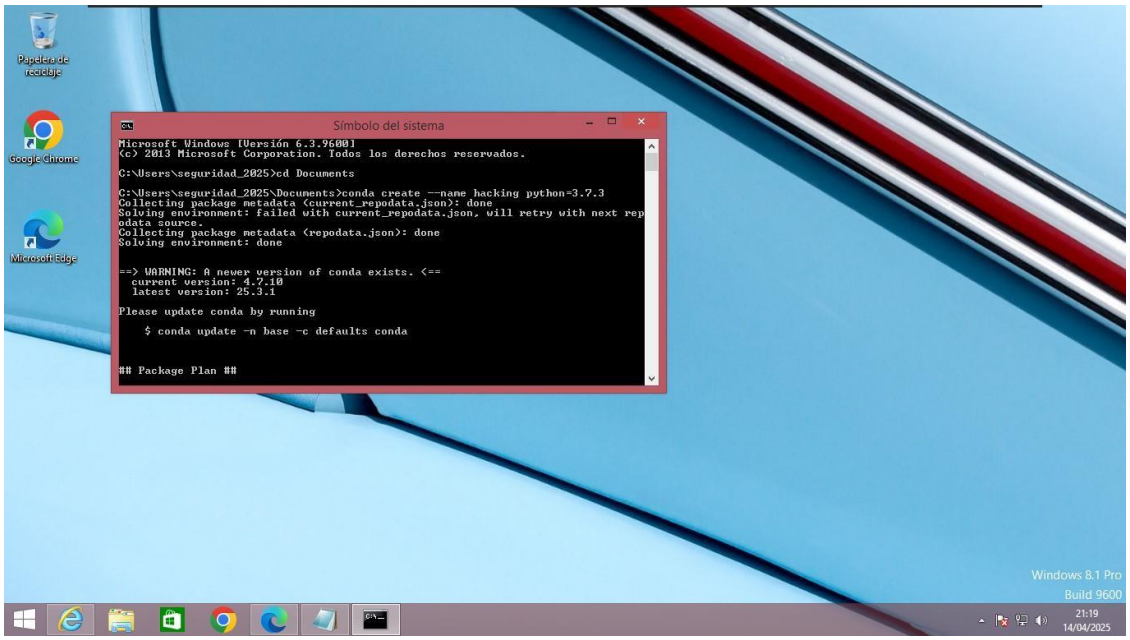
Instalacion Anaconda 3

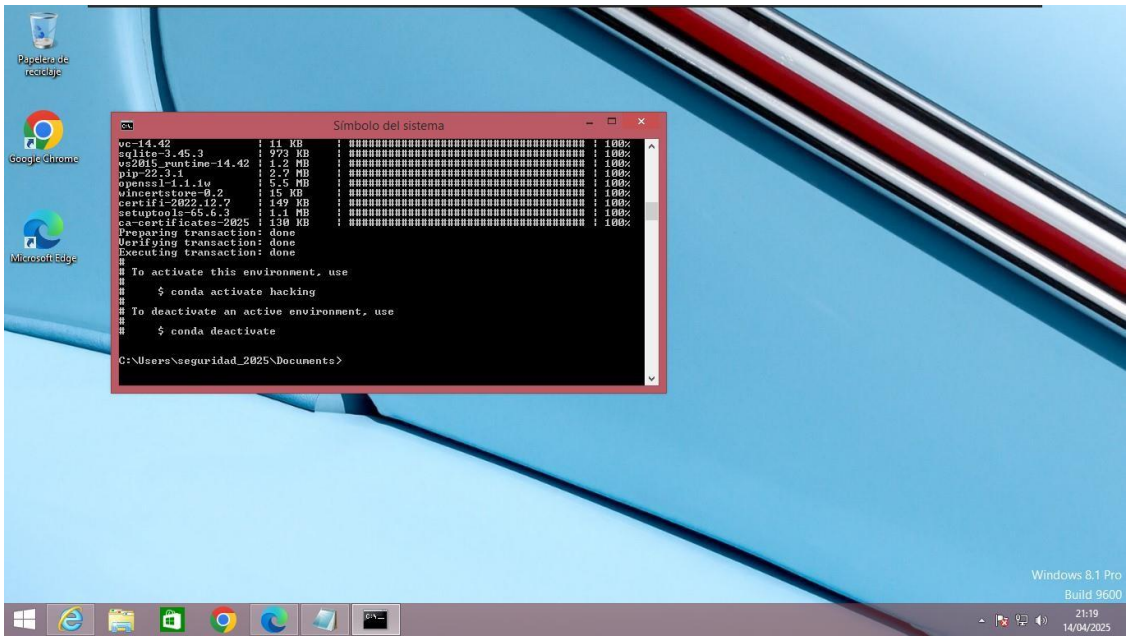




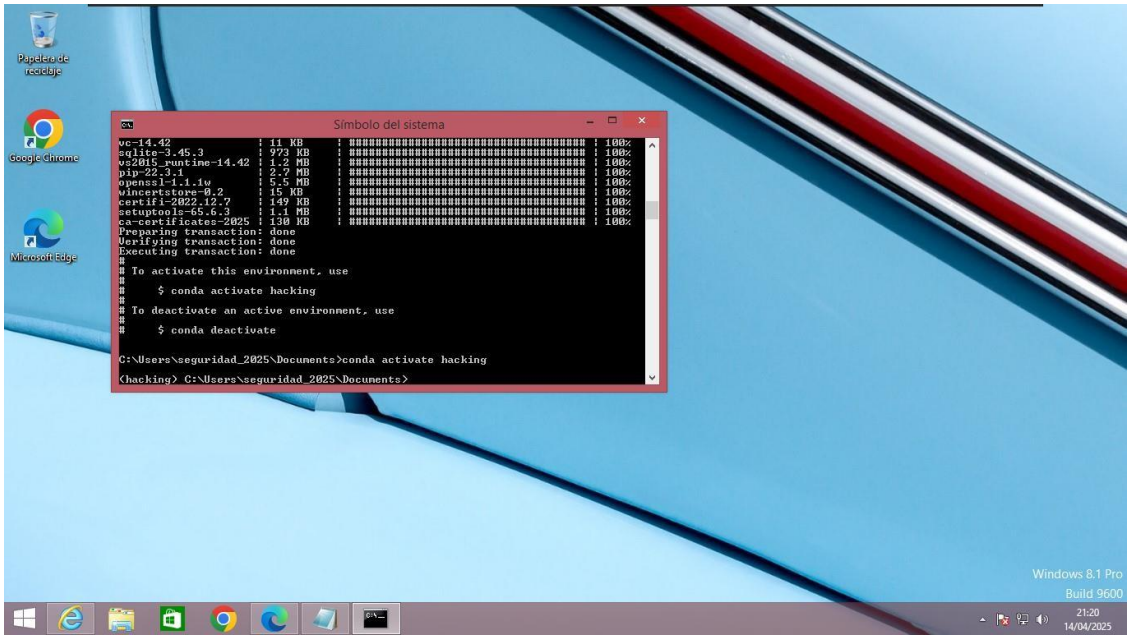
CMD

Crear en Envs hacking

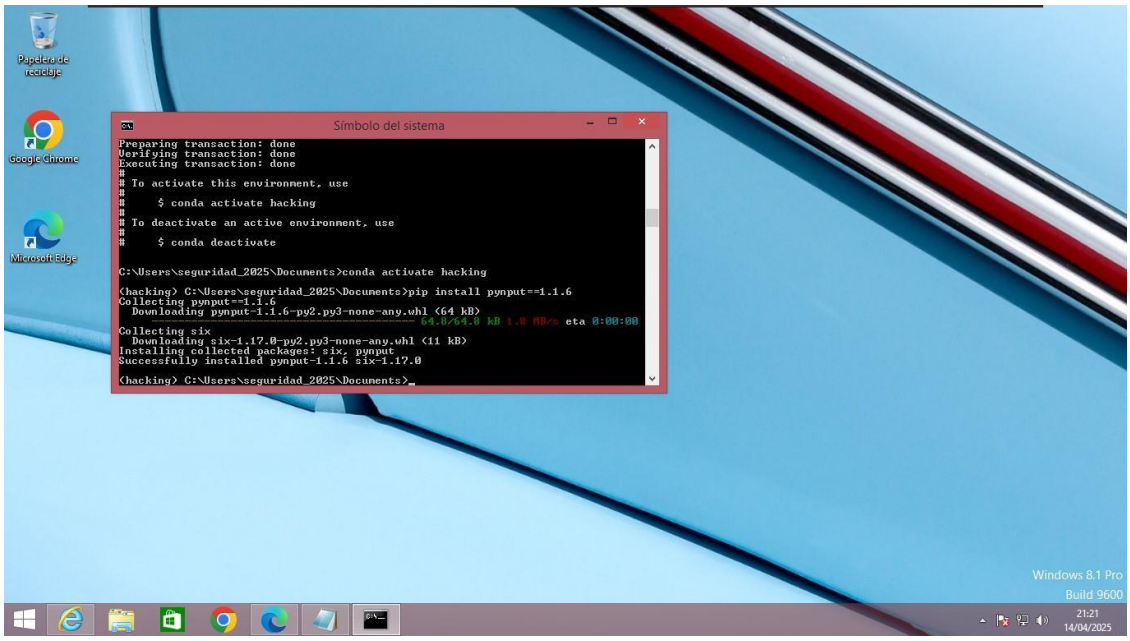




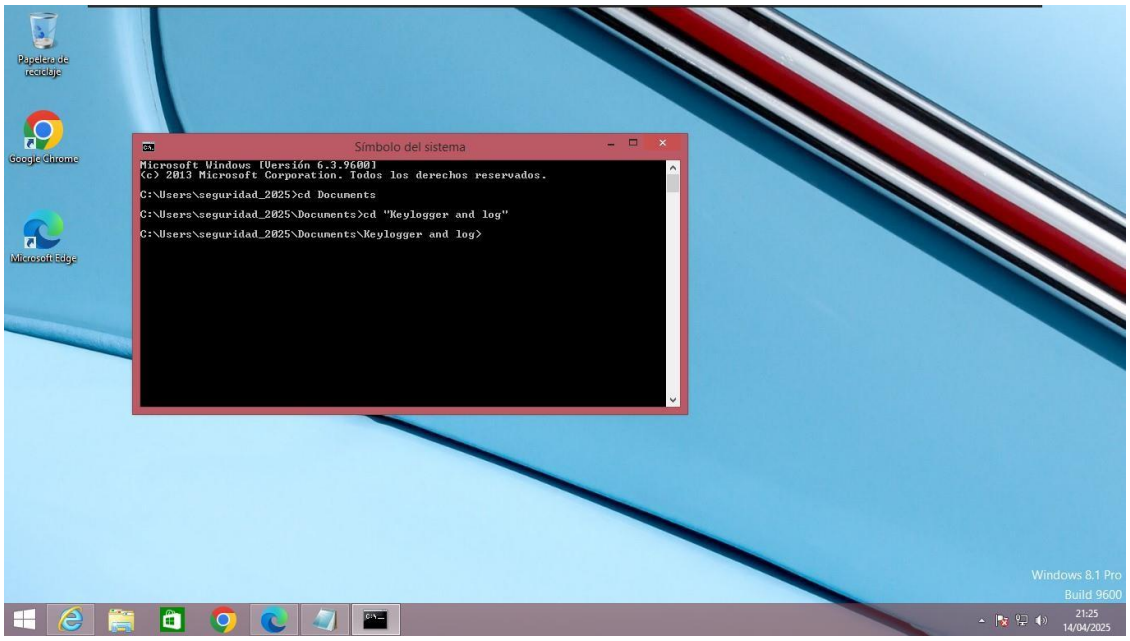
Conda actívate hacking



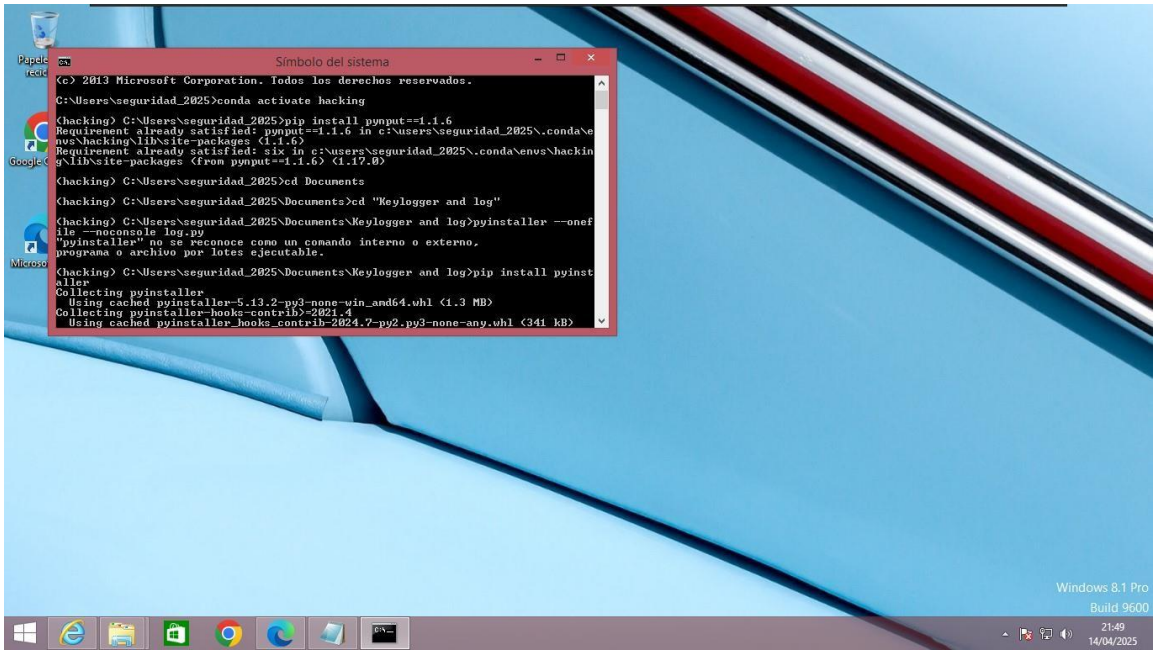
Pip install



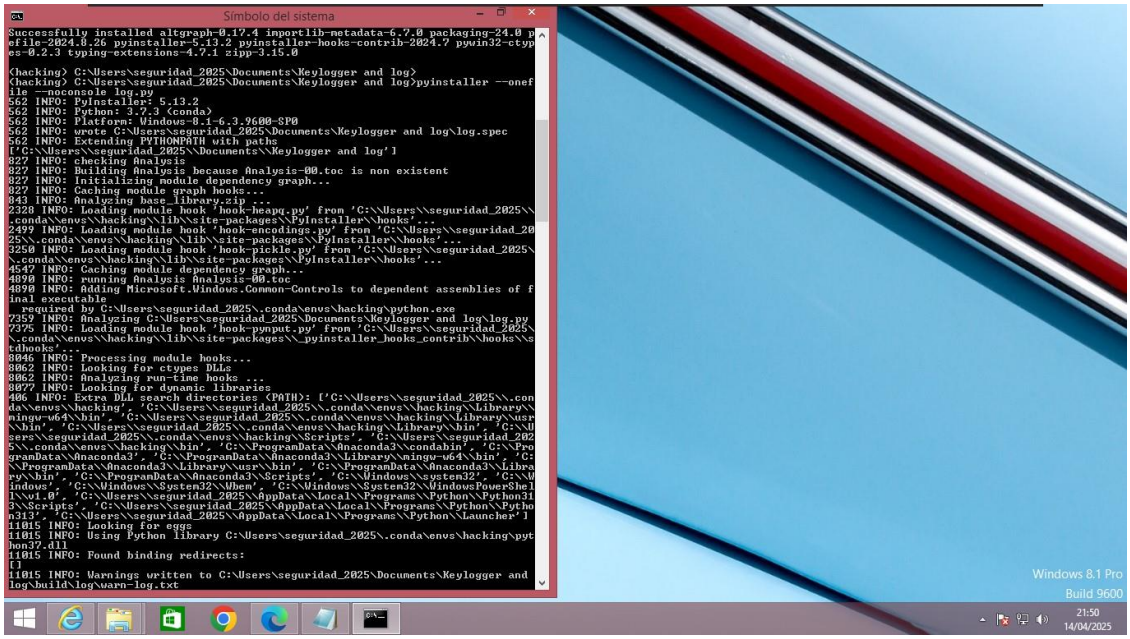
“Keylogger.py” y “log.py”



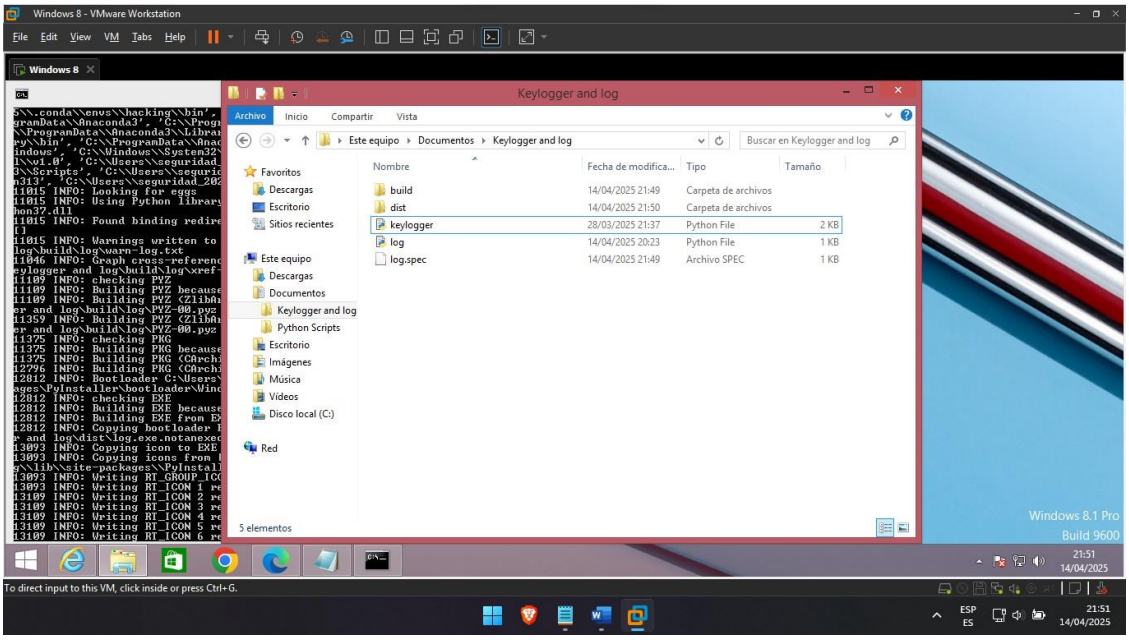
Install pip install pyinstaller



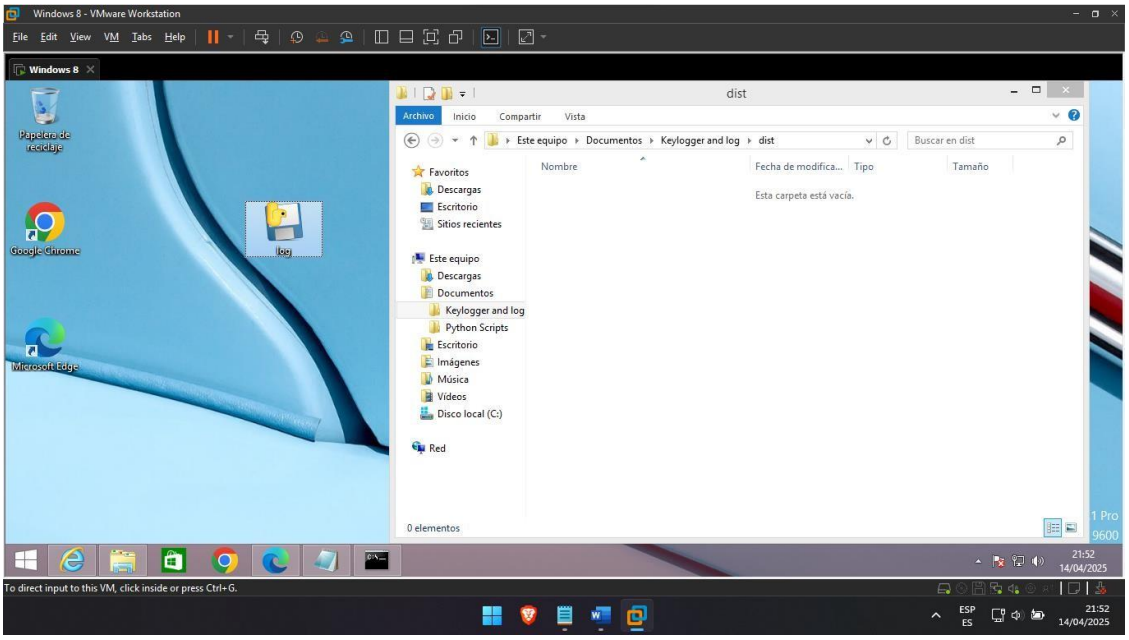
Pyinstaller –onefile –noconsole log.py



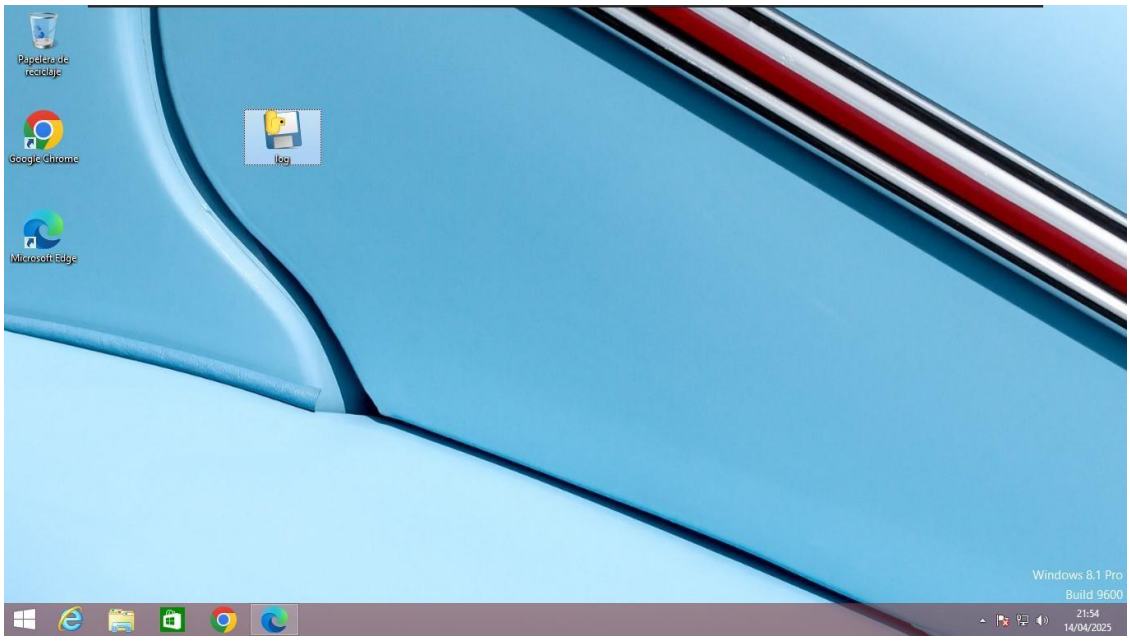
Se crearon carpetas

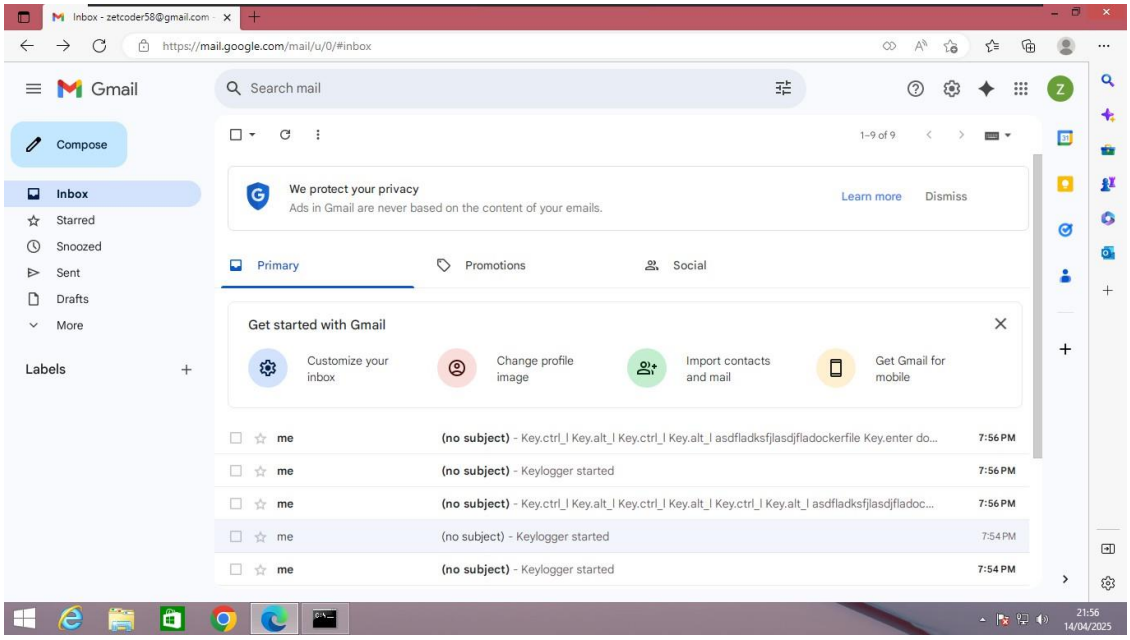


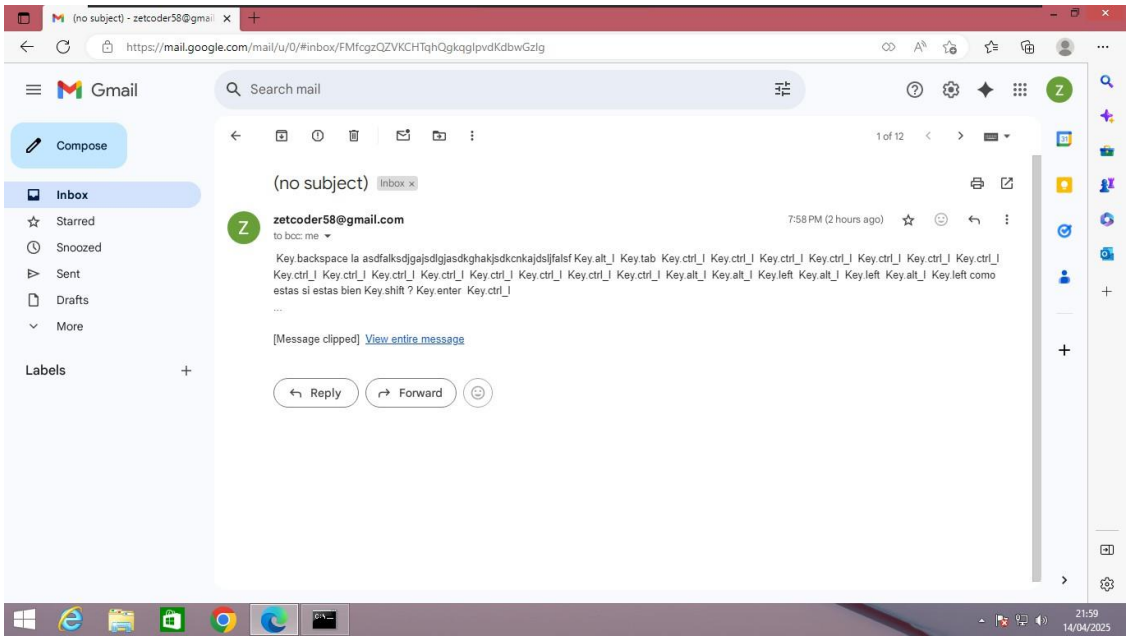
Copeamos al escritorio el archivo de Dist “log.py”



Doble click al archivo

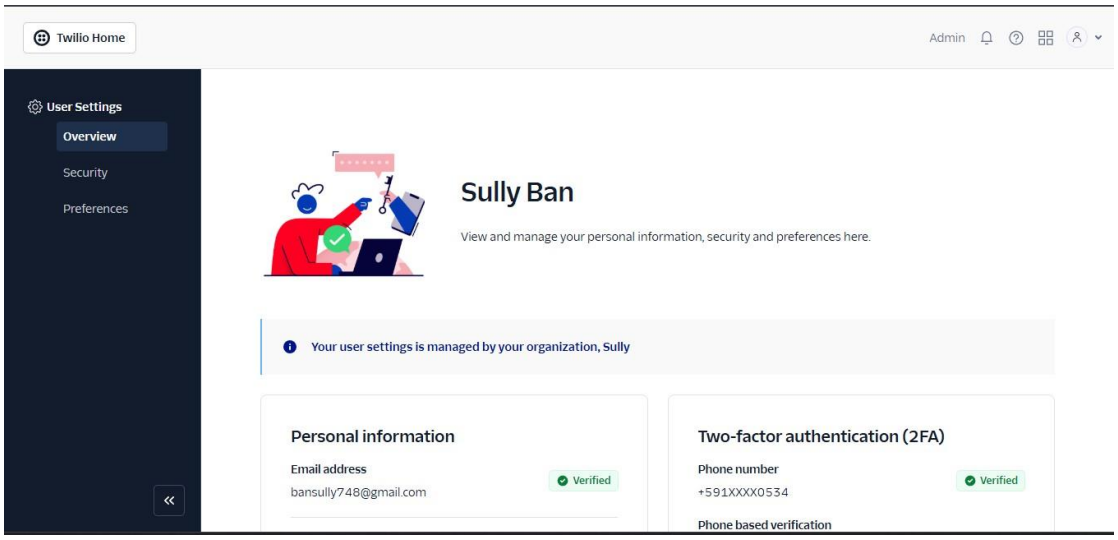


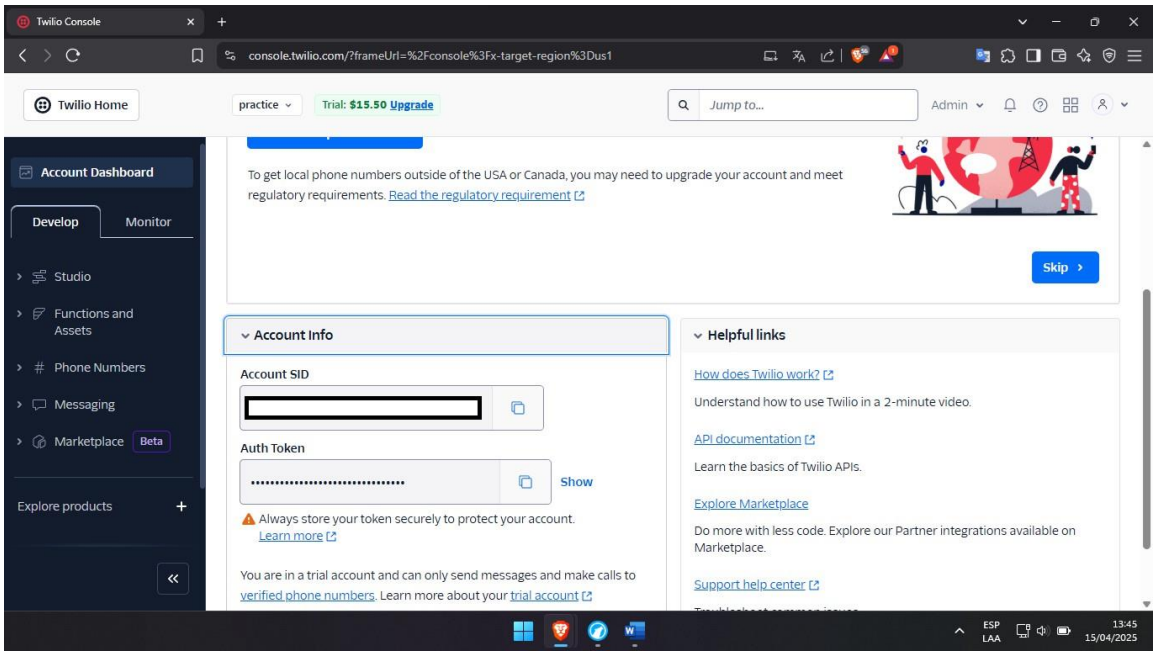




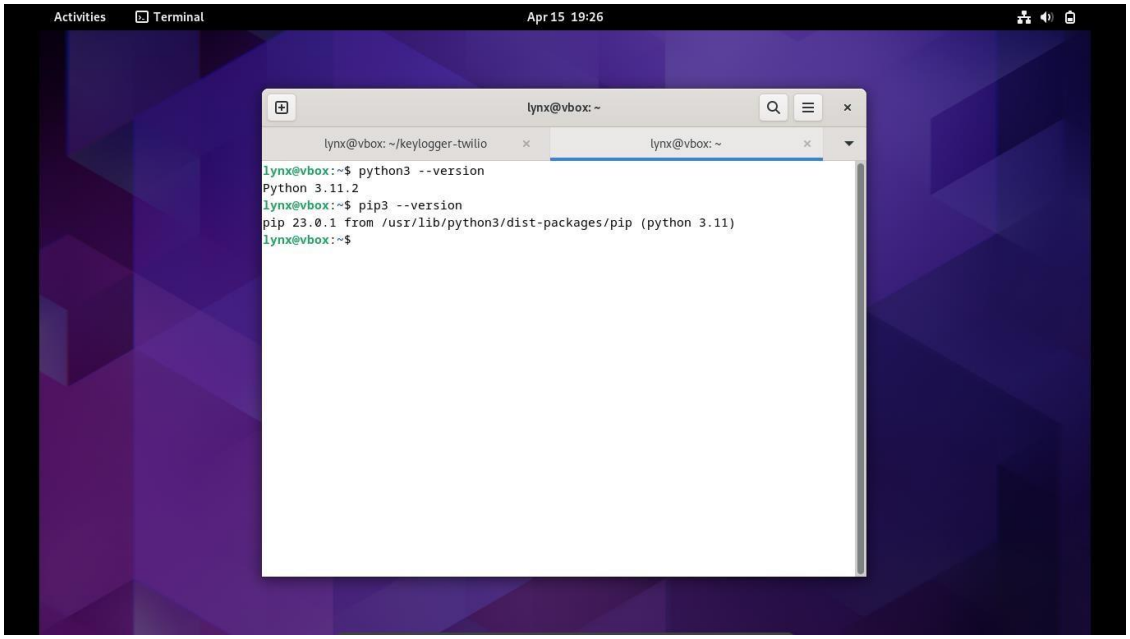
EVALUACION

Nos registramos en twilio

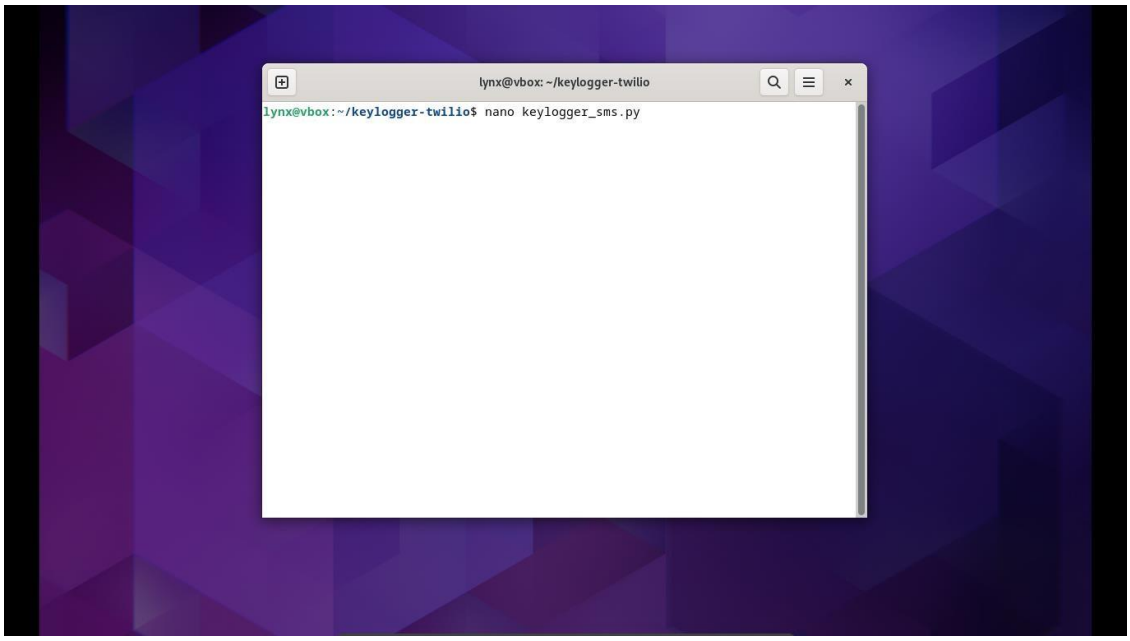




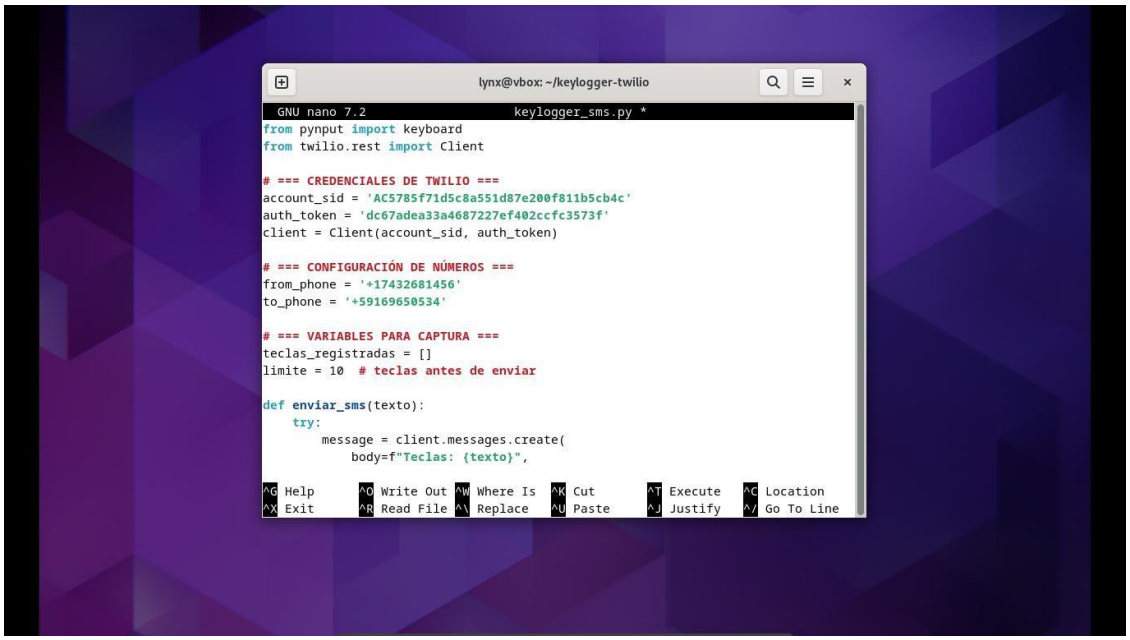
Instalamos python y pip3



En Debian creamos un directorio y creamos un archivo .py

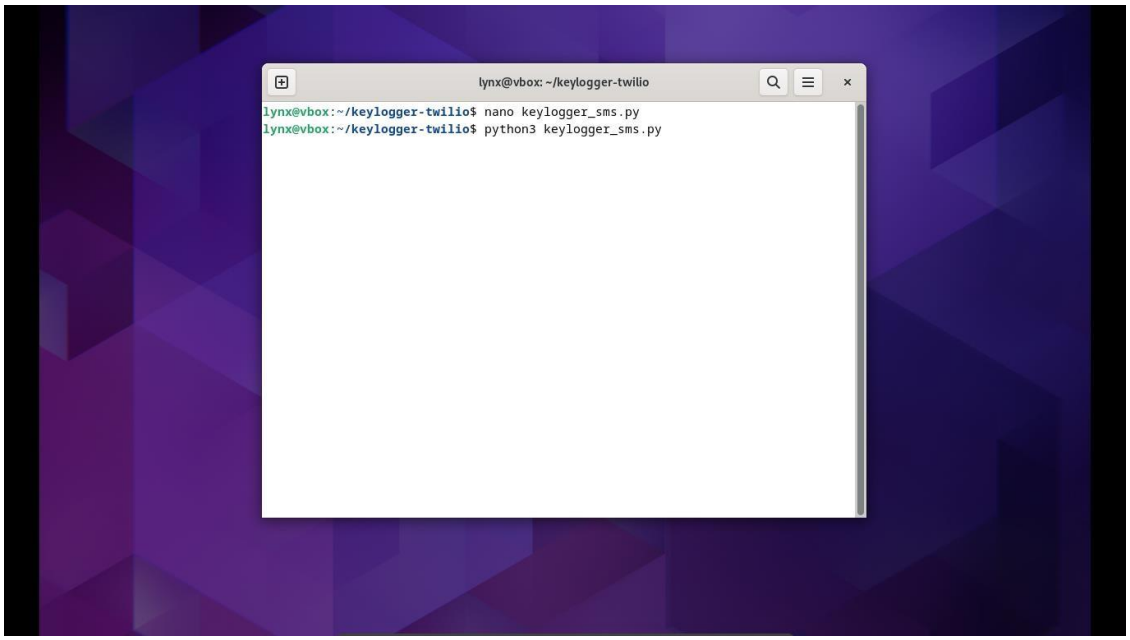


Introducimos el código y ponemos los credenciales que nos dio twilio y guardamos.

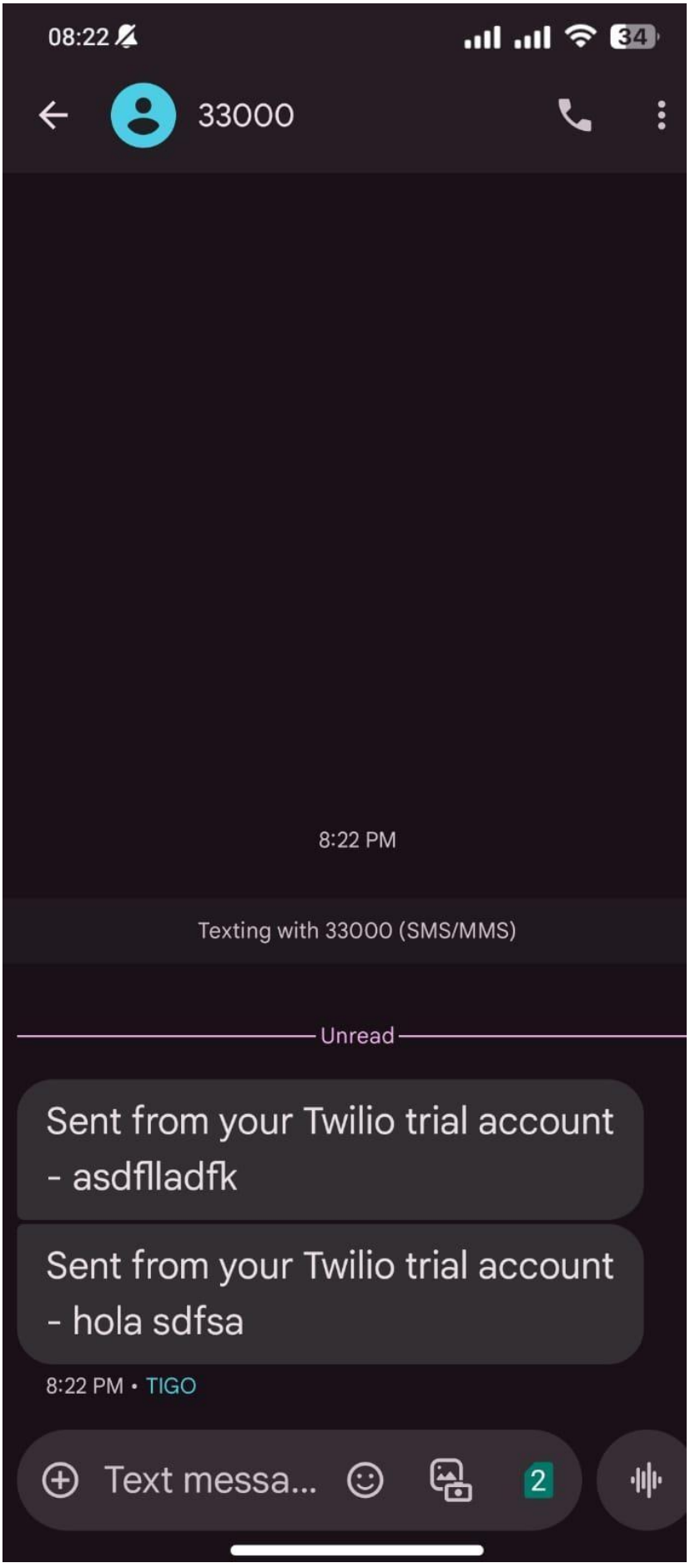


Ejecutamos con el siguiente comando

“python3 keylogger_sms.py”

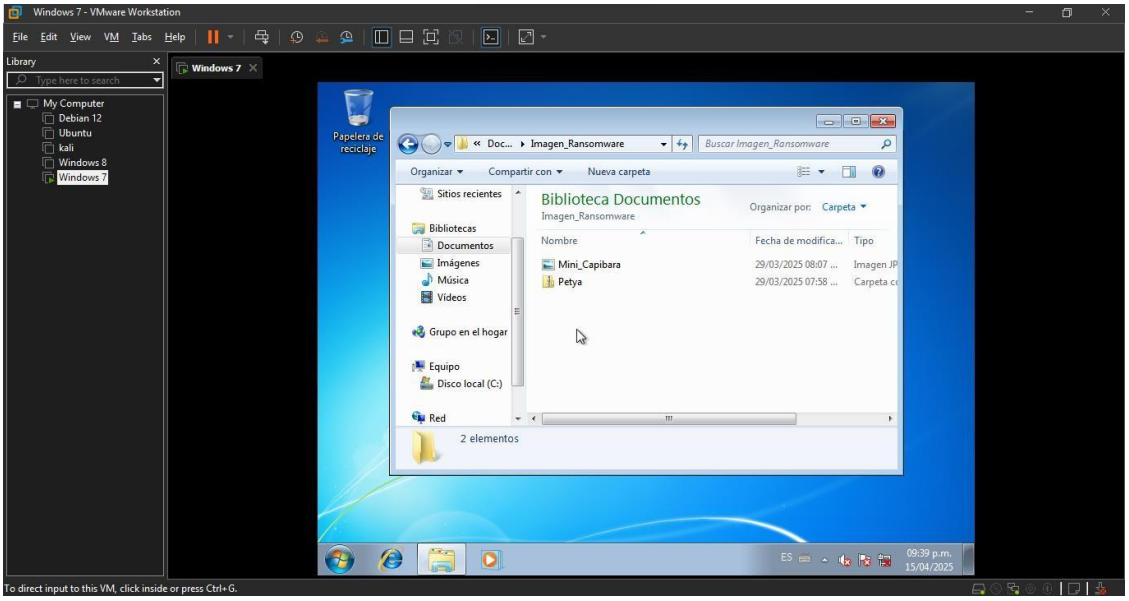


Resultado:

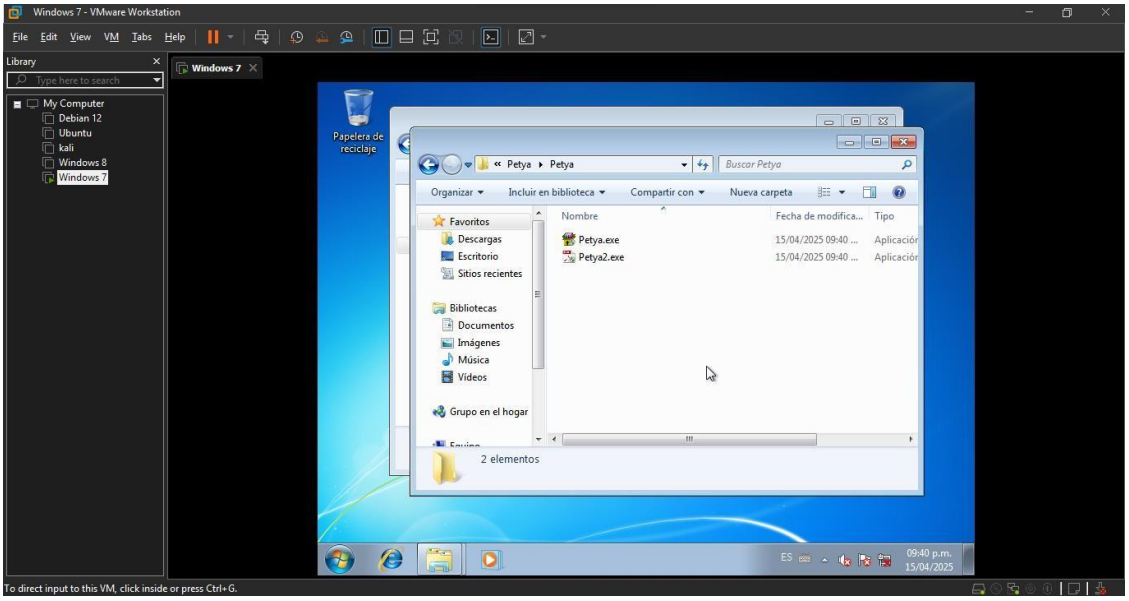

08:22
33000
8:22 PM
Texting with 33000 (SMS/MMS)
Unread
Sent from your Twilio trial account - asdflladfk
Sent from your Twilio trial account - hola sdfsa
8:22 PM • TIGO
Text messa...

PARTE 2

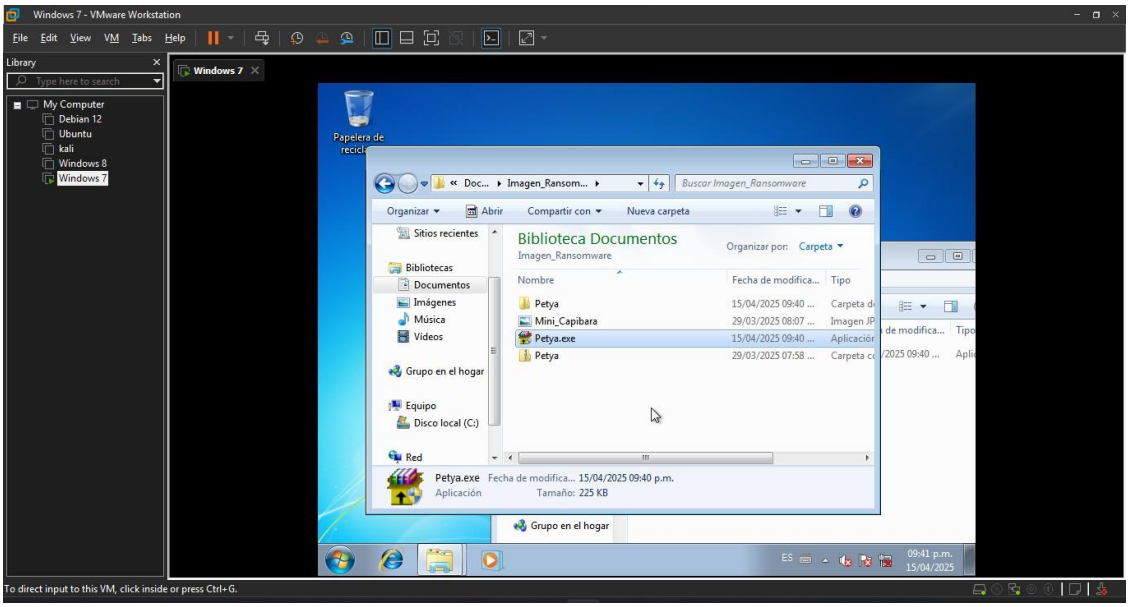
1.


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Debian 12
Ubuntu
kali
Windows 8
Windows 7
Windows 7
Papelera de reciclaje
Doc... ▸ Imagen_Ransomware
Buscar Imagen_Ransomware
Organizar
Compartir con
Nueva carpeta
Sitios recientes
Bibliotecas
Documentos
Imágenes
Música
Videos
Grupo en el hogar
Equipo
Disco local (C:)
Red
Biblioteca Documentos
Imagen_Ransomware
Organizar por: Carpeta
Nombre
Fecha de modifica...
Tipo
Mini_Capibara
29/03/2025 08:07 ...
Imagen JP
Petya
29/03/2025 07:58 ...
Carpeta c
2 elementos
ES
09:39 p.m.
15/04/2025
To direct input to this VM, click inside or press Ctrl+G.

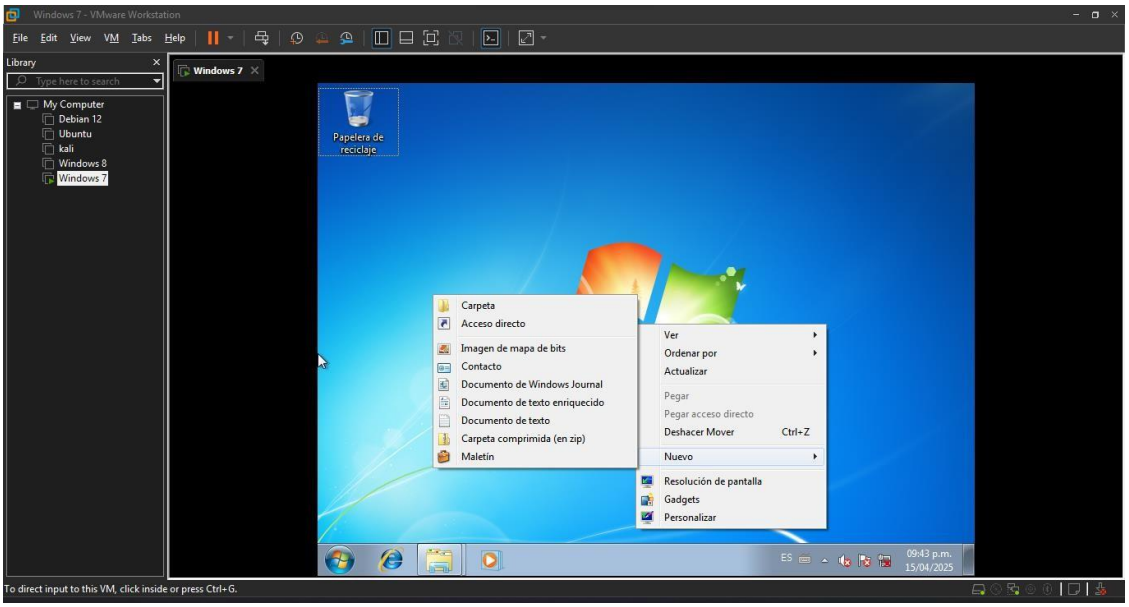
2.


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Debian 12
Ubuntu
kali
Windows 8
Windows 7
Windows 7
Papelera de reciclaje
Petya ▸ Petya
Buscar Petya
Organizar
Incluir en biblioteca
Compartir con
Nueva carpeta
Favoritos
Descargas
Escritorio
Sitios recientes
Bibliotecas
Documentos
Imágenes
Música
Videos
Grupo en el hogar
Nombre
Fecha de modifica...
Tipo
Petya.exe
15/04/2025 09:40 ...
Aplicación
Petya2.exe
15/04/2025 09:40 ...
Aplicación
2 elementos
ES
09:40 p.m.
15/04/2025
To direct input to this VM, click inside or press Ctrl+G.

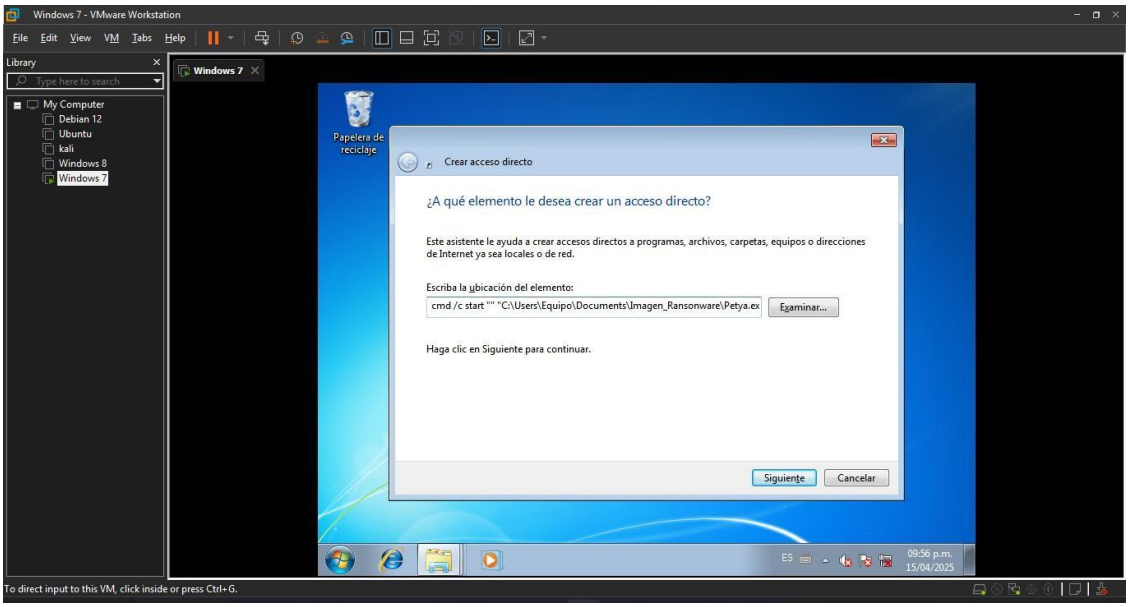
3. petya.exe


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Debian 12
Ubuntu
kali
Windows 8
Windows 7
Windows 7
Papelera de reciclaje
Biblioteca Documentos
Imagen_Ransomware
Organizar por: Carpeta
Nombre
Fecha de modifica...
Tipo
Petya
Mini_Capibara
Petya.exe
Petya
15/04/2025 09:40 ...
29/03/2025 08:07 ...
29/03/2025 07:58 ...
Sitios recientes
Bibliotecas
Documentos
Imágenes
Música
Vídeos
Grupo en el hogar
Equipo
Disco local (C:)
Red
Petya.exe Fecha de modifica... 15/04/2025 09:40 p.m.
Aplicación Tamaño: 225 KB
09:41 p.m.
15/04/2025
To direct input to this VM, click inside or press Ctrl+G.

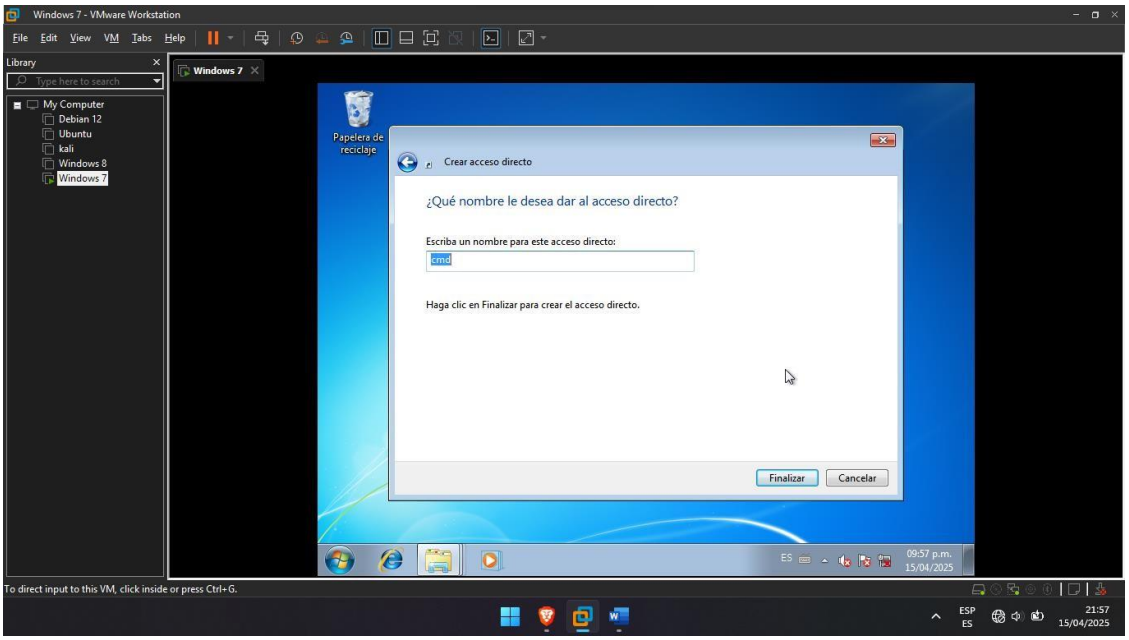
4.


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Debian 12
Ubuntu
kali
Windows 8
Windows 7
Windows 7
Papelera de reciclaje
Carpeta
Acceso directo
Imagen de mapa de bits
Contacto
Documento de Windows Journal
Documento de texto enriquecido
Documento de texto
Carpeta comprimida (en zip)
Maletín
Ver
Ordenar por
Actualizar
Pegar
Pegar acceso directo
Deshacer Mover Ctrl+Z
Nuevo
Resolución de pantalla
Gadgets
Personalizar
09:43 p.m.
15/04/2025
To direct input to this VM, click inside or press Ctrl+G.

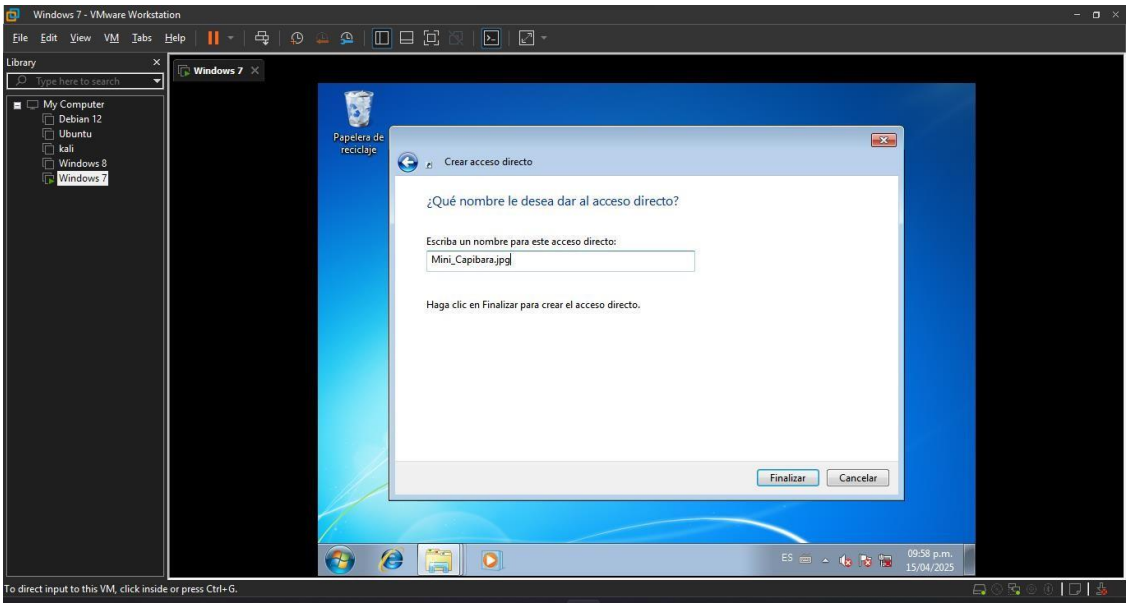
5.


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Debian 12
Ubuntu
kali
Windows 8
Windows 7
Windows 7
Papelera de reciclaje
Crear acceso directo
¿A qué elemento le desea crear un acceso directo?
Este asistente le ayuda a crear accesos directos a programas, archivos, carpetas, equipos o direcciones de Internet ya sea locales o de red.
Escriba la ubicación del elemento:
cmd /c start "" "C:\Users\Equipo\Documents\Imagen_Ransonware\Petya.ex
Examinar...
Haga clic en Siguiente para continuar.
Siguiente
Cancelar
ES
09:56 p.m.
15/04/2025
To direct input to this VM, click inside or press Ctrl+G.

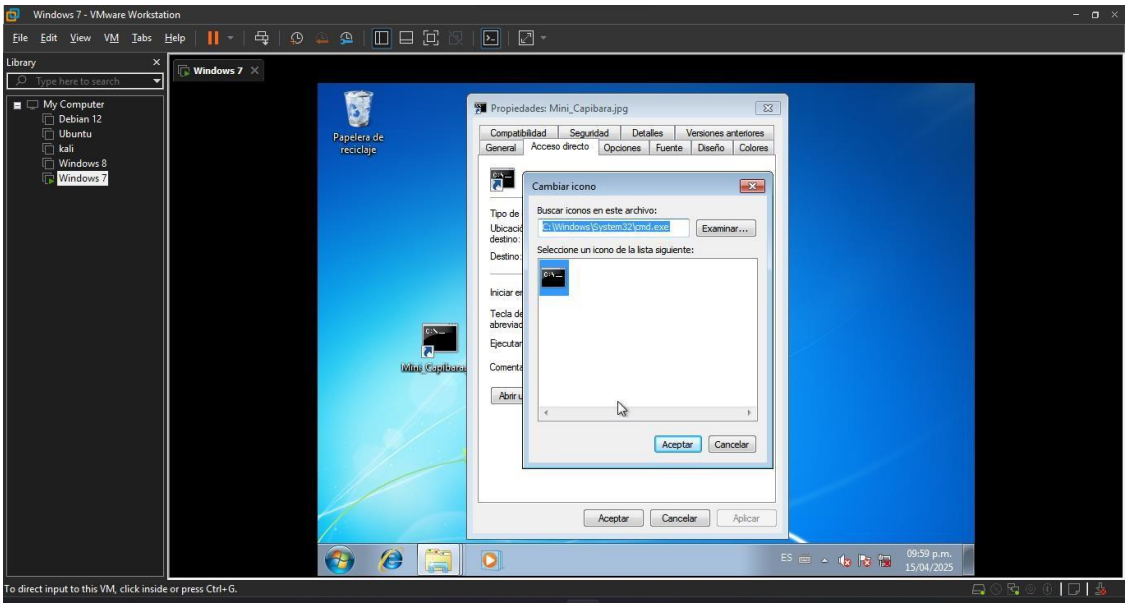
6.

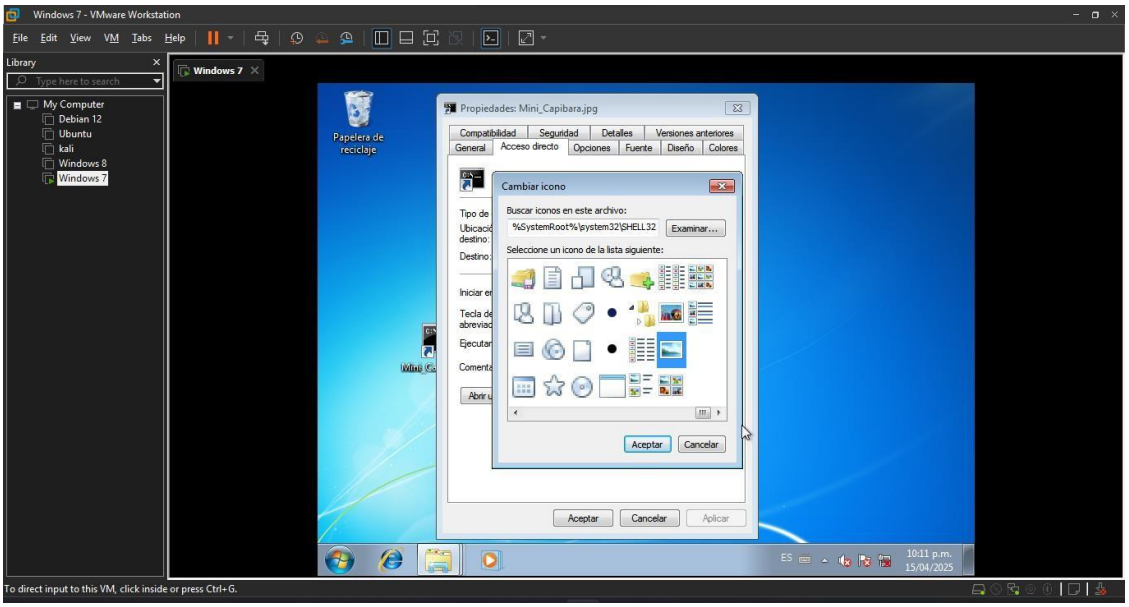

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Debian 12
Ubuntu
kali
Windows 8
Windows 7
Windows 7
Papelera de reciclaje
Crear acceso directo
¿Qué nombre le desea dar al acceso directo?
Escriba un nombre para este acceso directo:
cmd
Haga clic en Finalizar para crear el acceso directo.
Finalizar
Cancelar
ES
09:57 p.m.
15/04/2025
To direct input to this VM, click inside or press Ctrl+G.
ESP
ES
21:57
15/04/2025

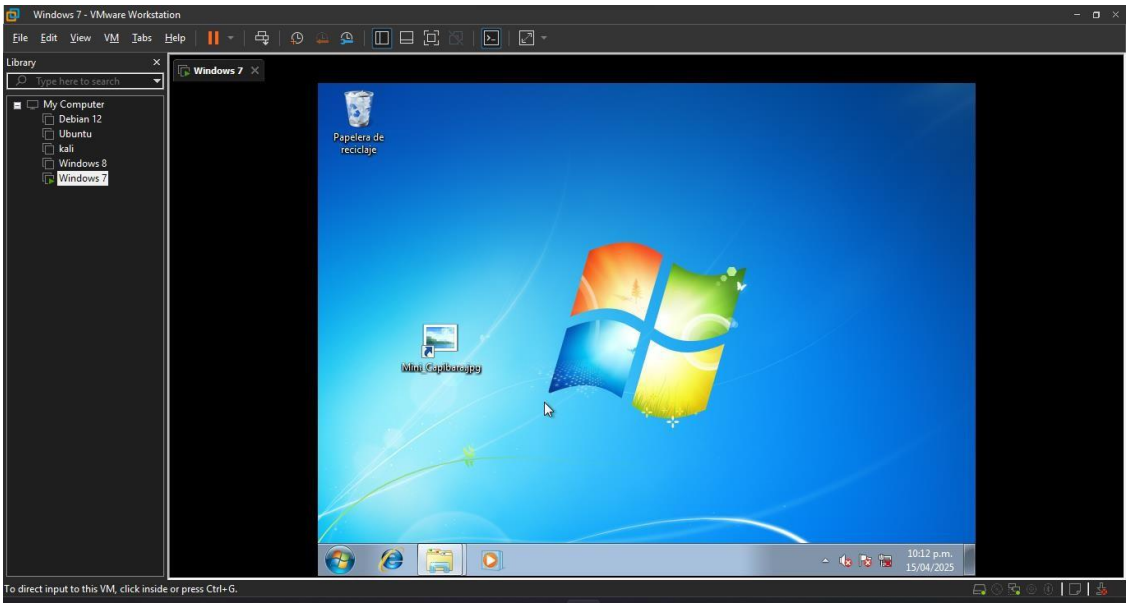
7.

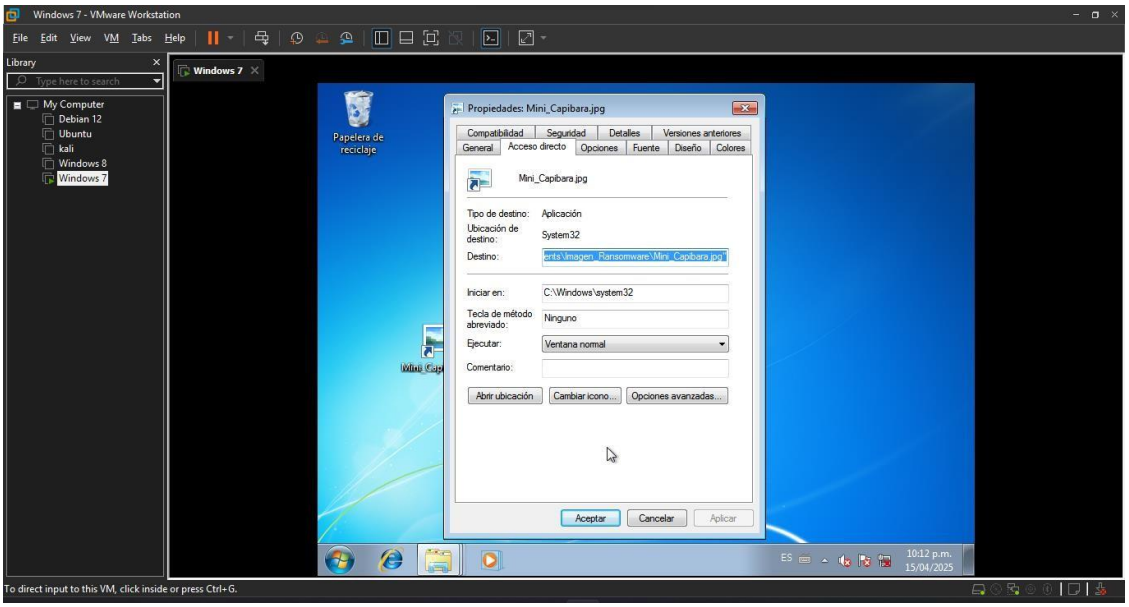

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Debian 12
Ubuntu
kali
Windows 8
Windows 7
Windows 7
Papelera de reciclaje
Crear acceso directo
¿Qué nombre le desea dar al acceso directo?
Escriba un nombre para este acceso directo:
Mini_Capibara.jpg
Haga clic en Finalizar para crear el acceso directo.
Finalizar
Cancelar
ES
09:58 p.m.
15/04/2025
To direct input to this VM, click inside or press Ctrl+G.

8.

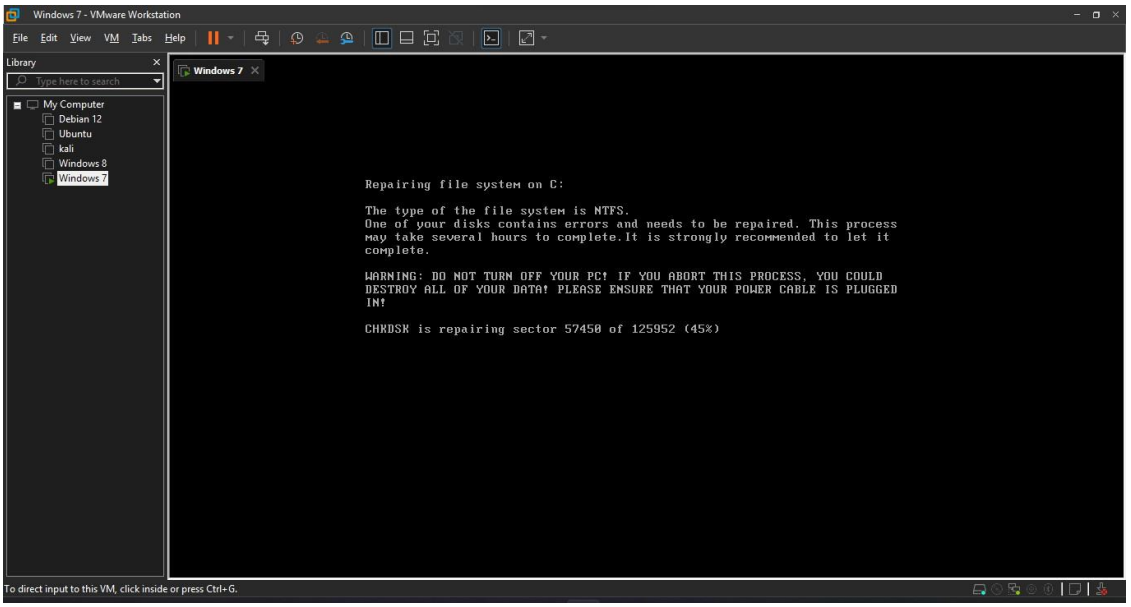

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Debian 12
Ubuntu
kali
Windows 8
Windows 7
Windows 7
Papelera de reciclaje
Mini Capibara
Propiedades: Mini_Capibara.jpg
Compatibilidad Seguridad Detalles Versiones anteriores
General Acceso directo Opciones Fuente Diseño Colores
Cambiar icono
Buscar iconos en este archivo:
C:\Windows\System32\cmd.exe
Examinar...
Seleccione un icono de la lista siguiente:
Aceptar
Cancelar
Aceptar
Cancelar
Aplicar
ES
09:59 p.m.
15/04/2025
To direct input to this VM, click inside or press Ctrl+G.


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Debian 12
Ubuntu
kali
Windows 8
Windows 7
Windows 7
Papelera de reciclaje
Propiedades: Mini_Capibara.jpg
Compatibilidad Seguridad Detalles Versiones anteriores
General Acceso directo Opciones Fuente Diseño Colores
Cambiar icono
Buscar iconos en este archivo:
%SystemRoot%\system32\SHELL32
Examinar...
Seleccione un icono de la lista siguiente:
Aceptar
Cancelar
Aceptar
Cancelar
Aplicar
ES
10:11 p.m.
15/04/2025
To direct input to this VM, click inside or press Ctrl+G.

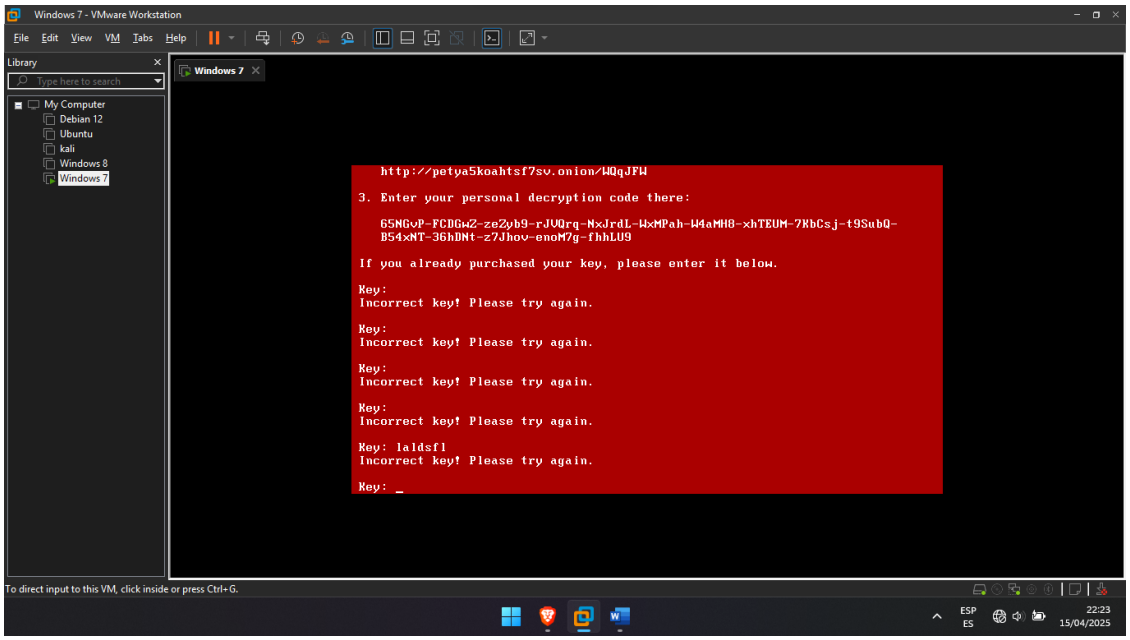

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Debian 12
Ubuntu
kali
Windows 8
Windows 7
Windows 7
Papelera de reciclaje
Mini Capibara.jpg
10:12 p.m.
15/04/2025
To direct input to this VM, click inside or press Ctrl+G.



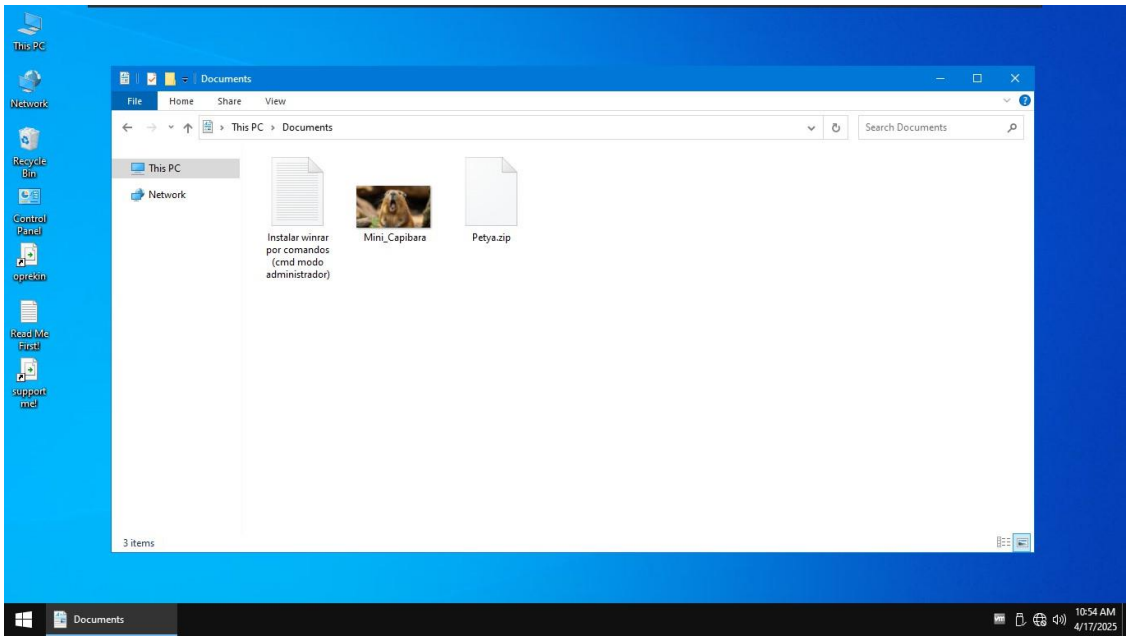
Ejecutamos

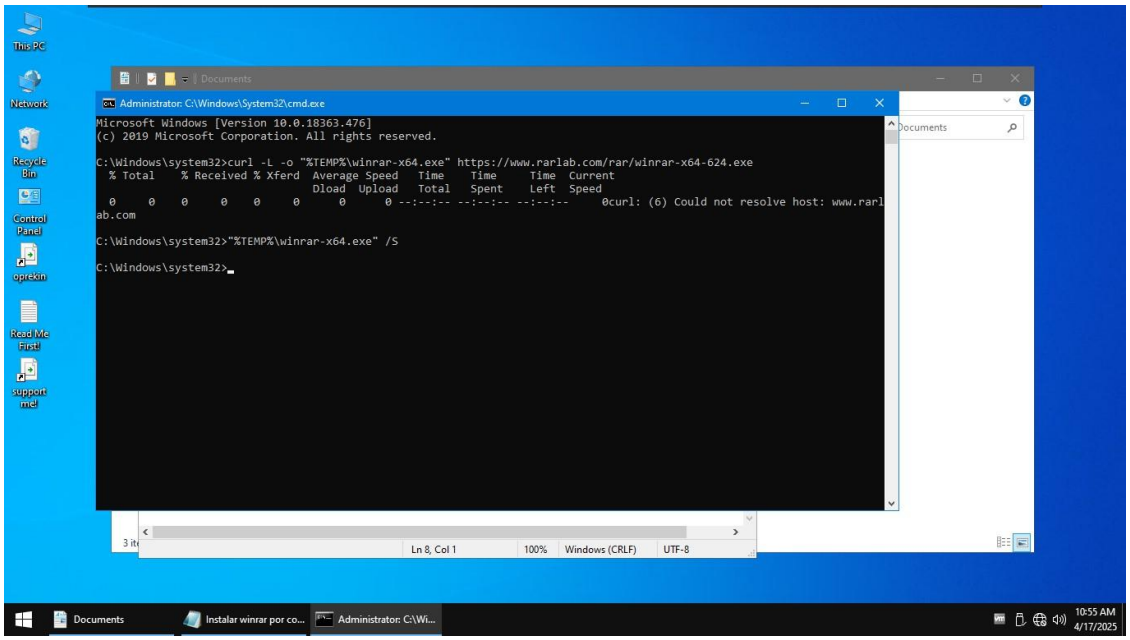


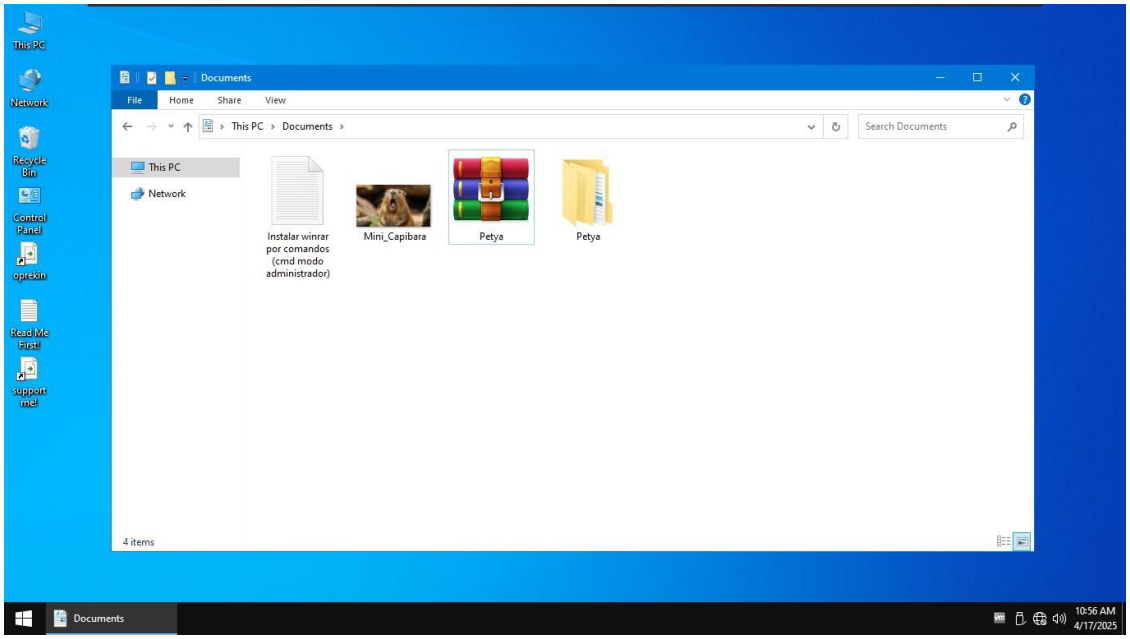
Se reinicio la MV y empezó a cargar una barra


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Debian 12
Ubuntu
kali
Windows 8
Windows 7
Windows 7
http://petya5koahtsf7sv.onion/WQqJFW
3. Enter your personal decryption code there:
65NGvP-FCDGw2-ze2yb9-rJVQrq-MxJrdL-WxMPah-W4aMH8-xhTEUM-7KbCsj-t9SubQ-B54xNT-36hDNt-z7Jhov-enoM7g-fhhLU9
If you already purchased your key, please enter it below.
Key:
Incorrect key! Please try again.
Key:
Incorrect key! Please try again.
Key:
Incorrect key! Please try again.
Key:
Incorrect key! Please try again.
Key: laldsfl
Incorrect key! Please try again.
Key: _
To direct input to this VM, click inside or press Ctrl+G.
ESP
ES
22:23
15/04/2025

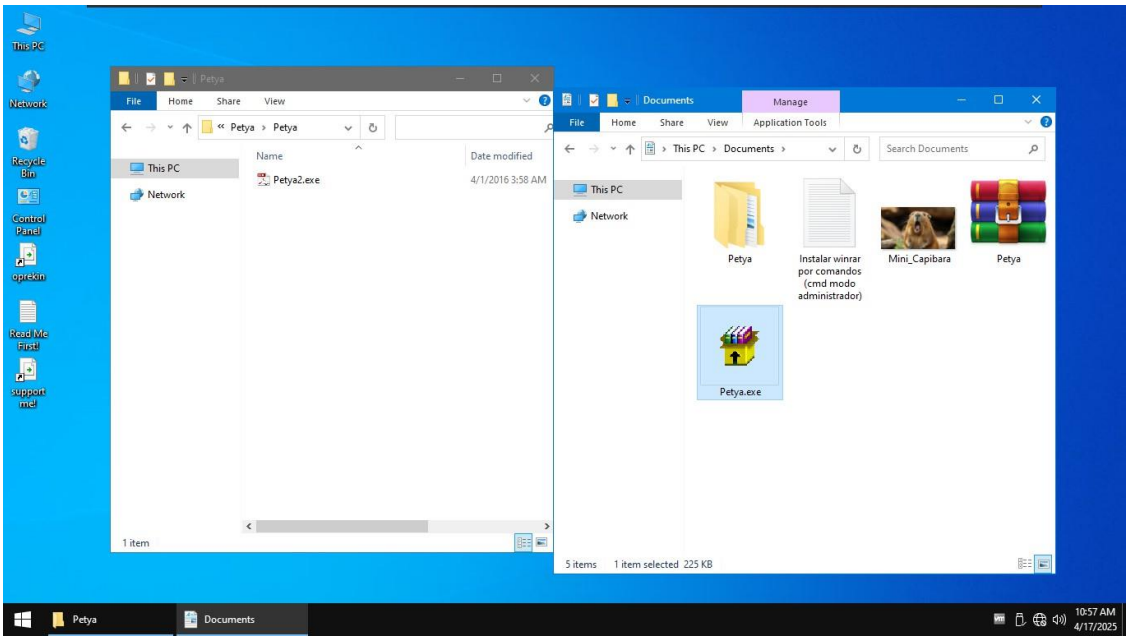
Evaluación


This PC
Network
Recycle Bin
Control Panel
oprekin
Read Me First!
support me!
Documents
File Home Share View
This PC › Documents
Search Documents
This PC
Network
Instalar winrar por comandos (cmd modo administrador)
Mini_Capibara
Petya.zip
3 items
Documents
10:54 AM
4/17/2025

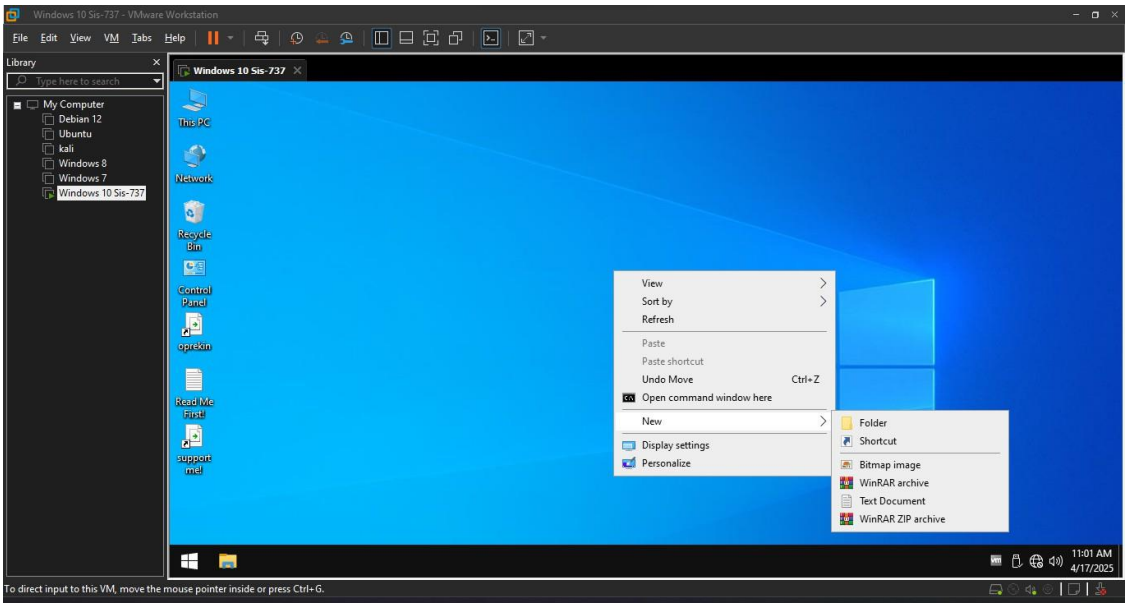

This PC
Network
Recycle Bin
Control Panel
oprekin
Read Me First!
support me!
Documents
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18363.476]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Windows\system32>curl -L -o "%TEMP%\winrar-x64.exe" https://www.rarlab.com/rar/winrar-x64-624.exe
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0curl: (6) Could not resolve host: www.rarlab.com
C:\Windows\system32>"%TEMP%\winrar-x64.exe" /S
C:\Windows\system32>
Ln 8, Col 1
100%
Windows (CRLF)
UTF-8
Documents
Instalar winrar por co...
Administrator: C:\Wi...
10:55 AM
4/17/2025


This PC
Network
Recycle Bin
Control Panel
oprekin
Read Me First!
support me!
Documents
File
Home
Share
View
This PC › Documents ›
Search Documents
This PC
Network
Instalar winrar por comandos (cmd modo administrador)
Mini_Capibara
Petya
Petya
4 items
Documents
10:56 AM
4/17/2025

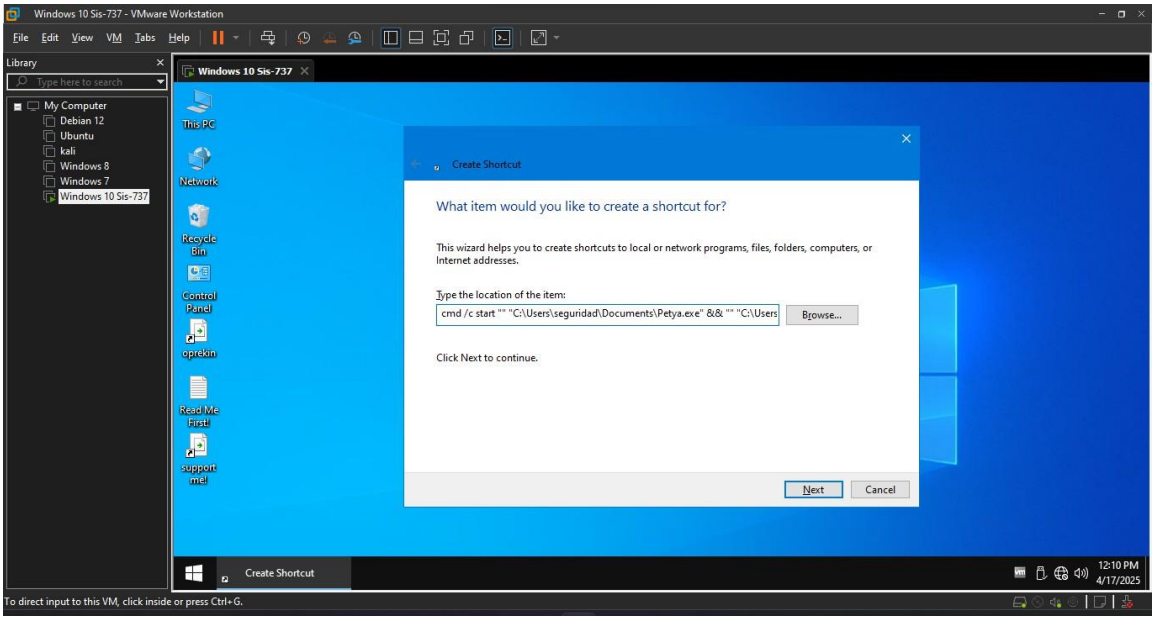
Movemos Petya.exe



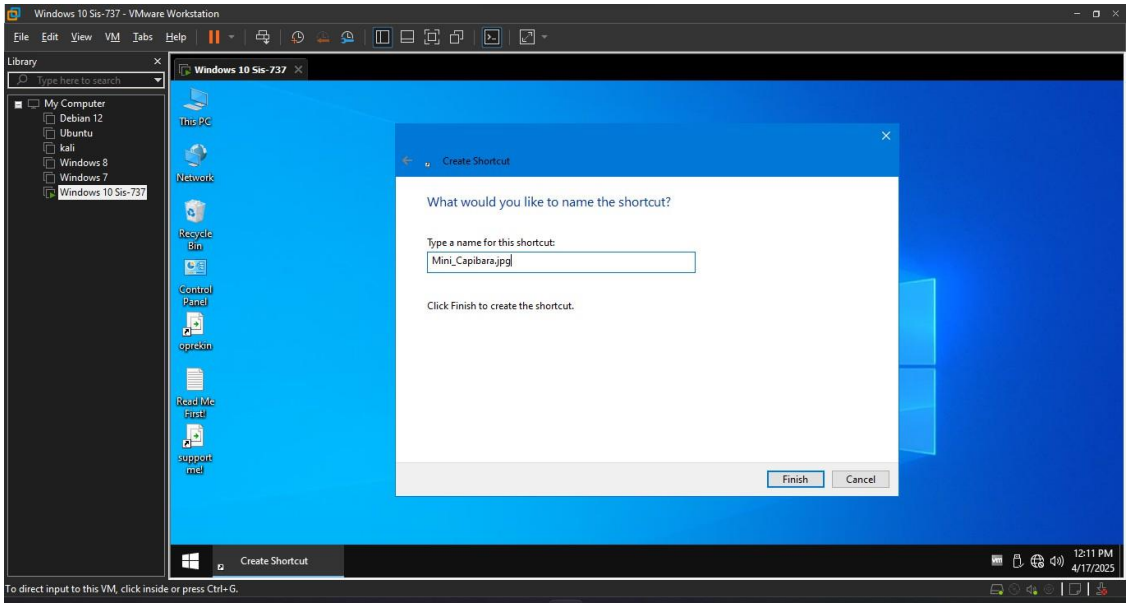
Crear acceso directo



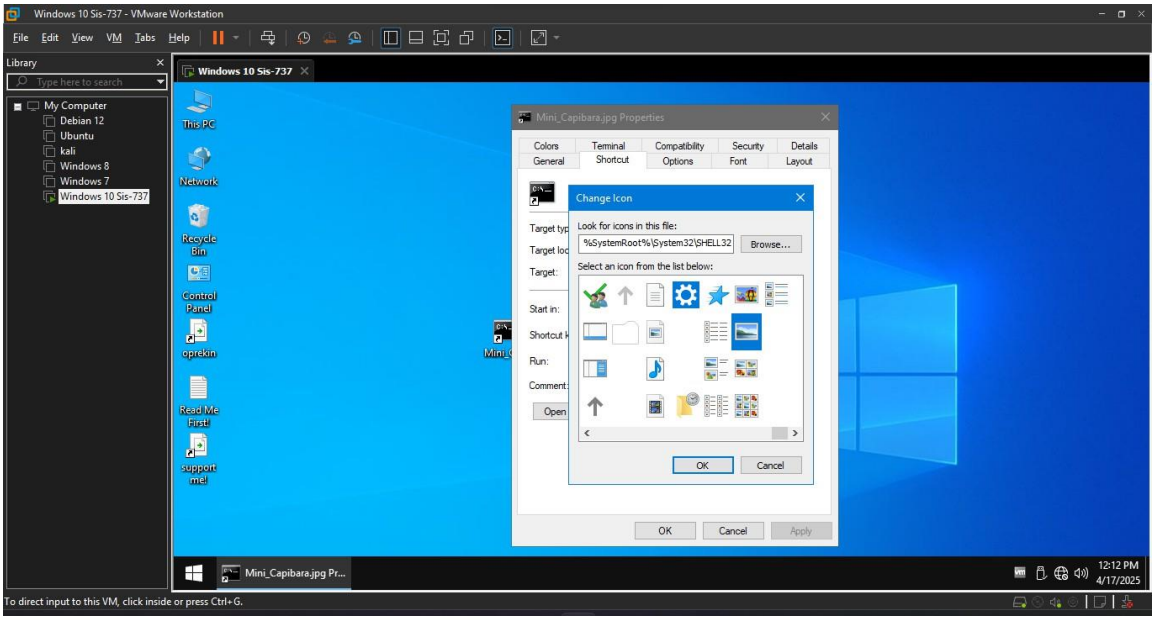
Colocamos la ruta

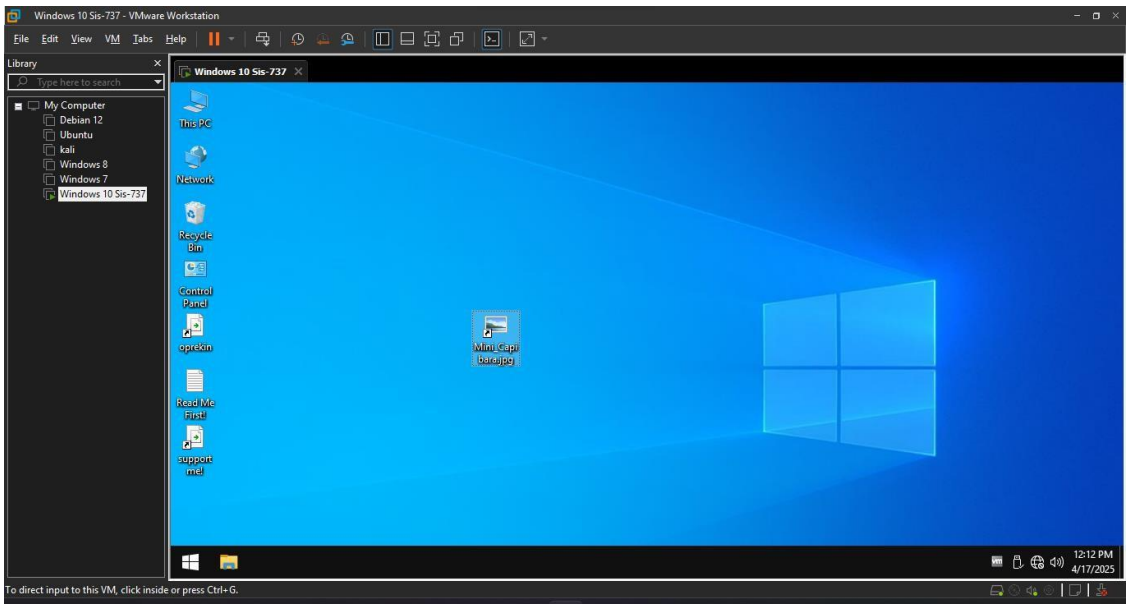


Asignamos un nombre

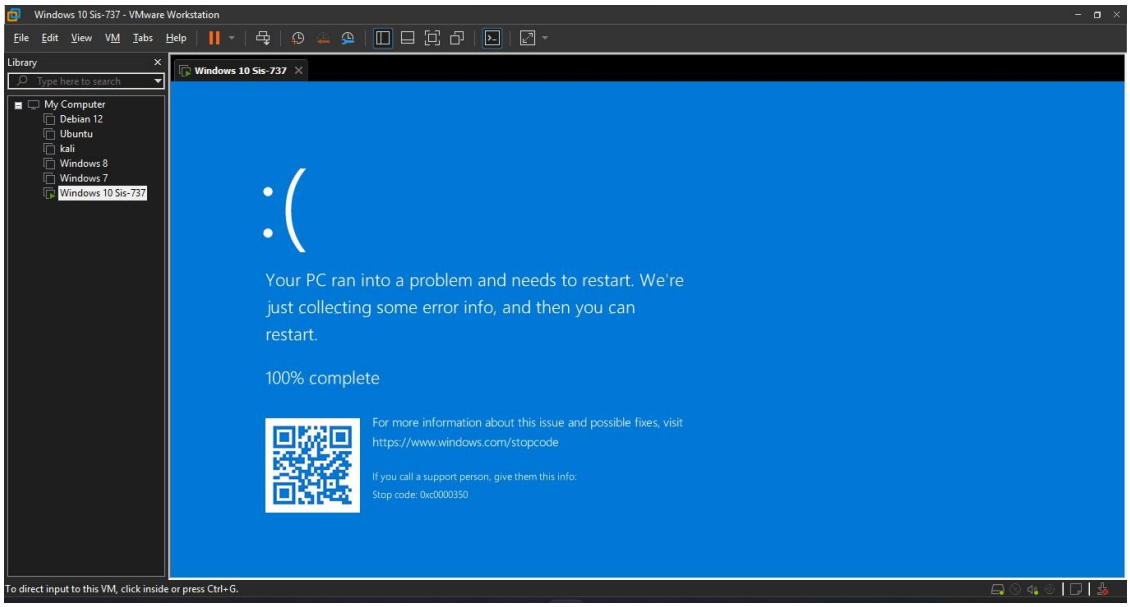


Cambiamos de icono



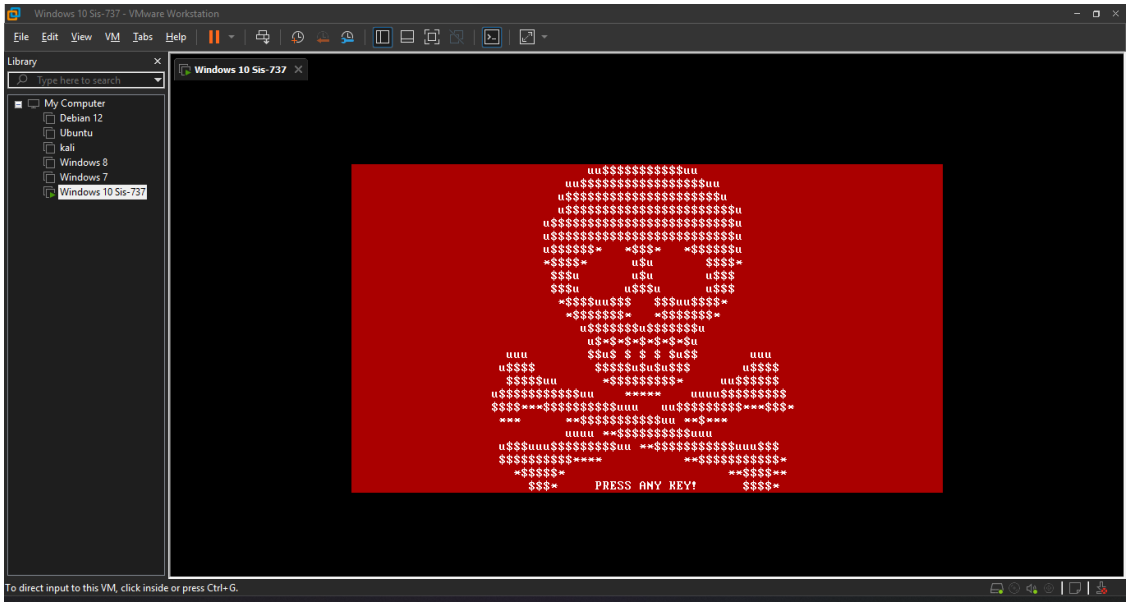


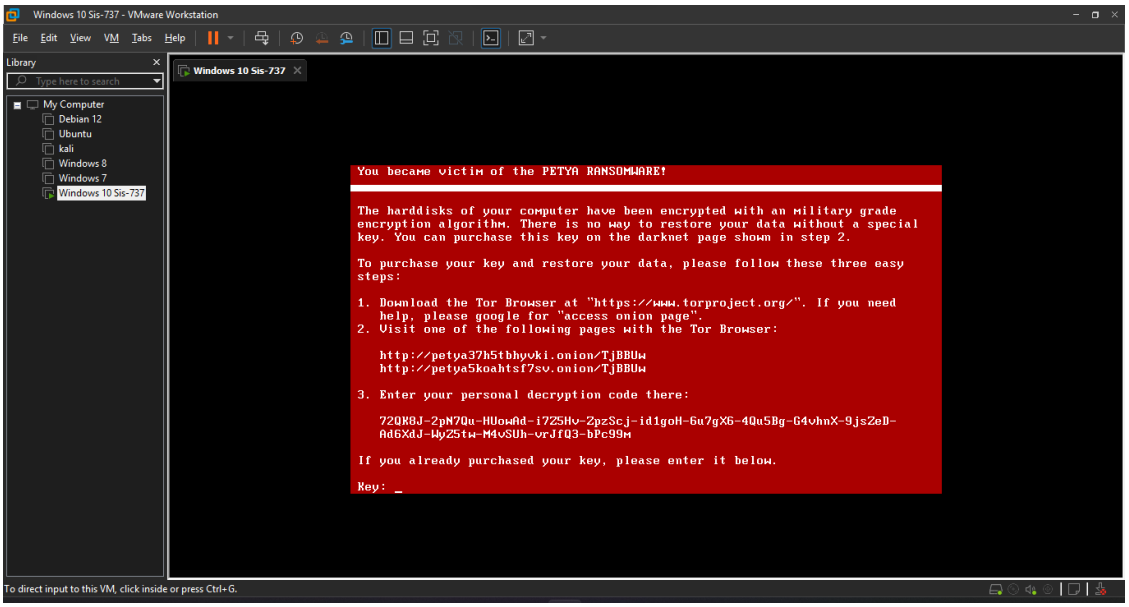
Ejecución del acceso directo



Lo reiniciamos la MV

y se encripto el sistema





Preguntas:

¿Se ejecutó correctamente el ransomware en Windows 10?

Si se ejecutó correctamente

¿El sistema se encriptó o hubo alguna protección activa que lo impidió?

El sistema se encripto esto porque la MV proporcionada no tenia instalado Windows Defender y Firewall.

¿Hubo diferencias notables en comparación con Windows 7?

Solo hubo una diferencia la cual fue la pantalla azul de Windows que nos pedía que reiniciemos el equipo y ahí procedió a encriptarse el sistema.

¿Explique que sucede si se abre el acceso directo como administrador?

Al ejecutar el acceso directo como administrador no es lo mismo que ejecutarlo sin privilegios, porque Petya.exe requiere permisos elevados para realizar sus operaciones. Sin privilegios Petya.exe puede ser que falle mientras como administrador debería de funcionar.

En nuestro caso funciono al ejecutarlo sin privilegios porque no se contaba con firewall y Windows defender o en otro caso desactivados.