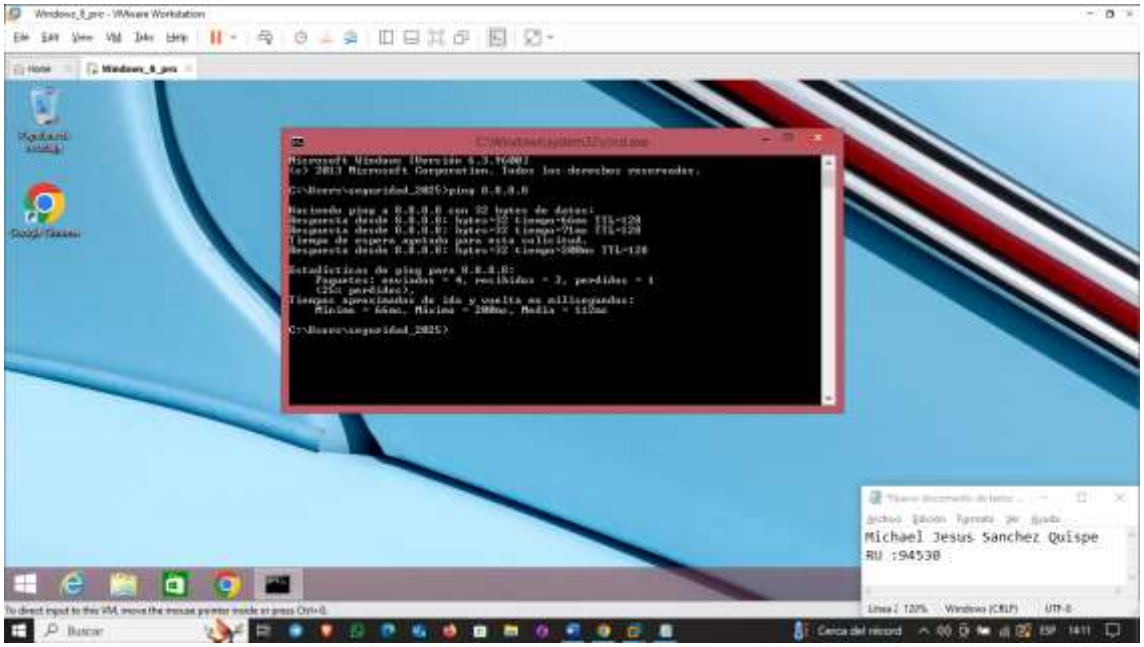
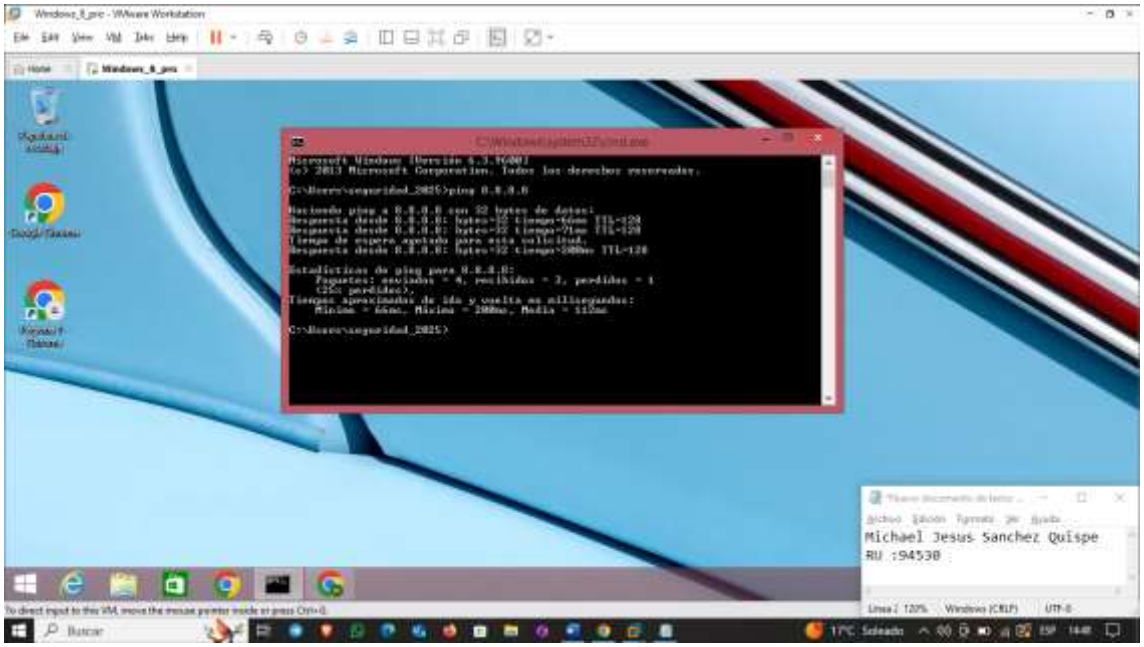
PRACTICA 1

Seguridad de Sistemas (Sis-737)

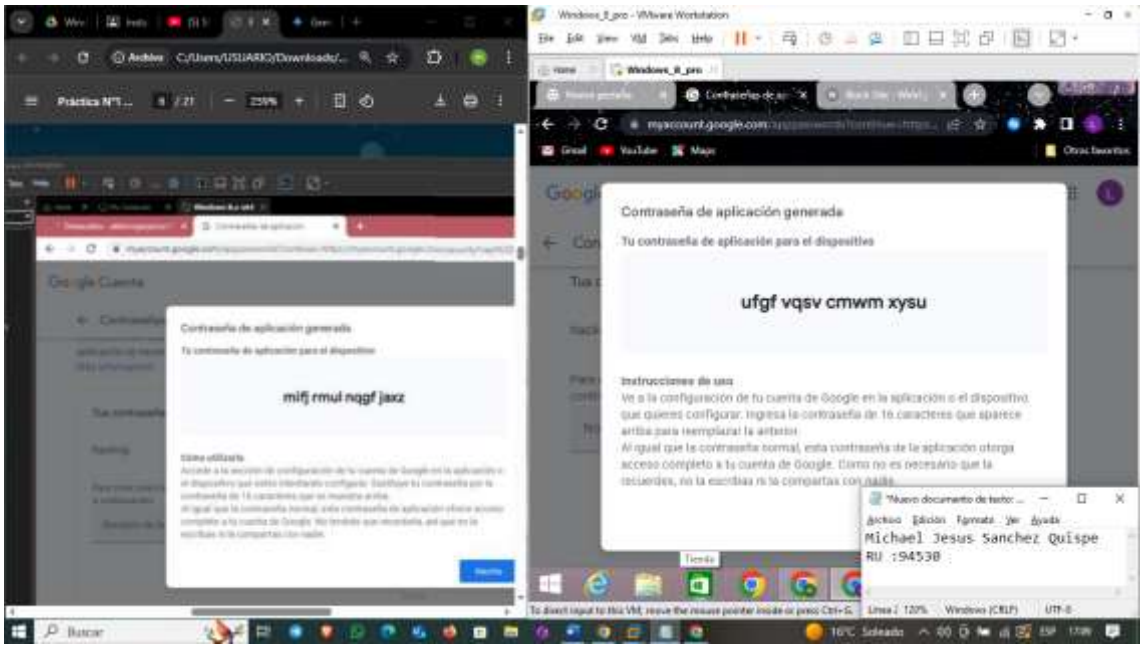
Univ. Michael Jesús Sanchez Quispe

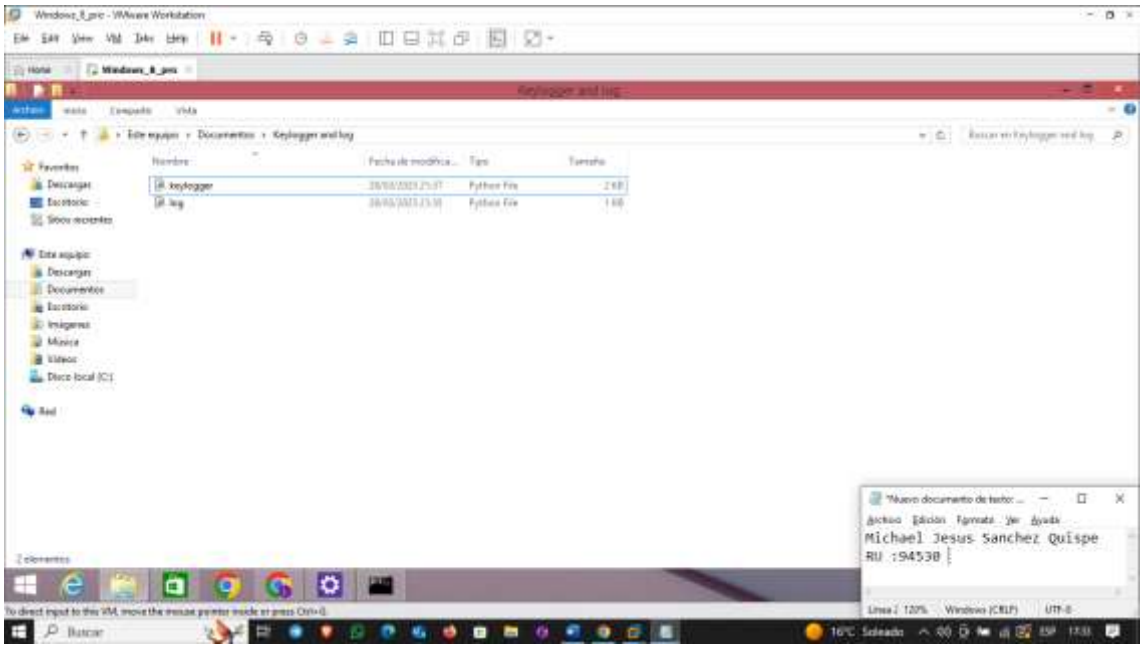
Parte 1



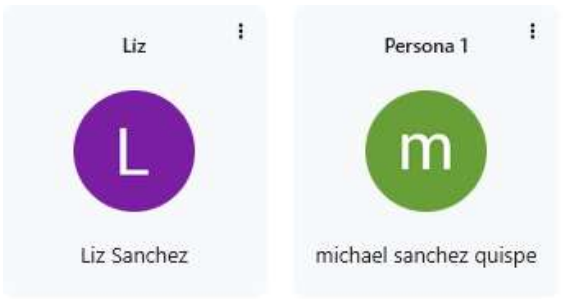


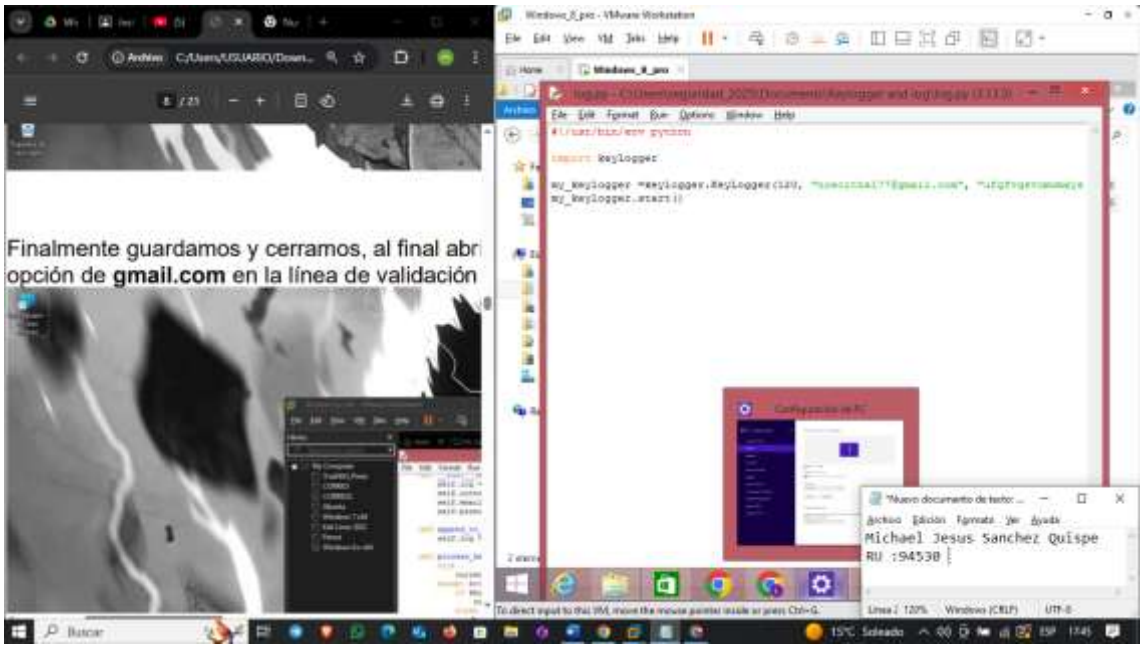
En esta parte el correo inicial no me quería dar permiso debido a que no tenia configurado la verificación en dos pasos asi que use el siguiente correo que tambien me pertenece

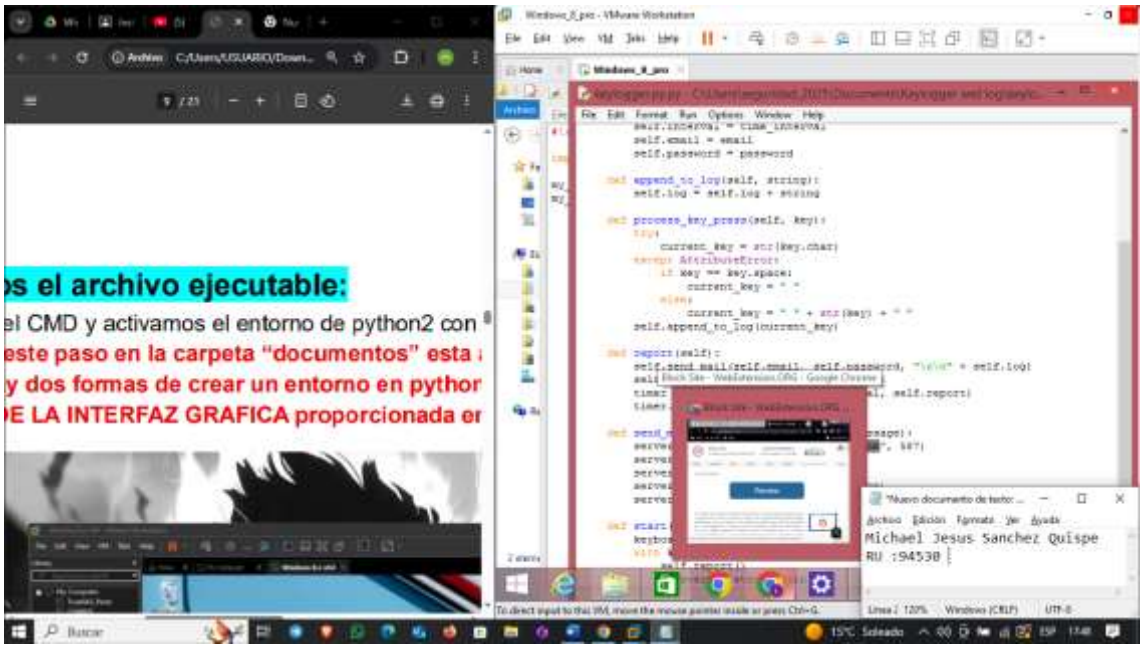


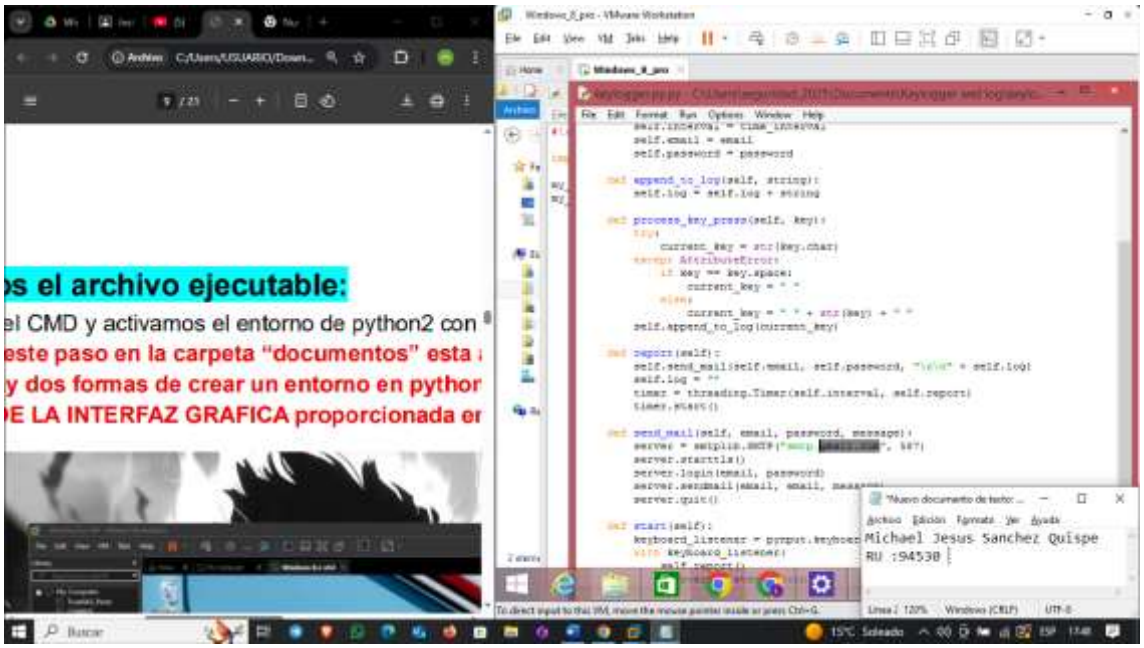


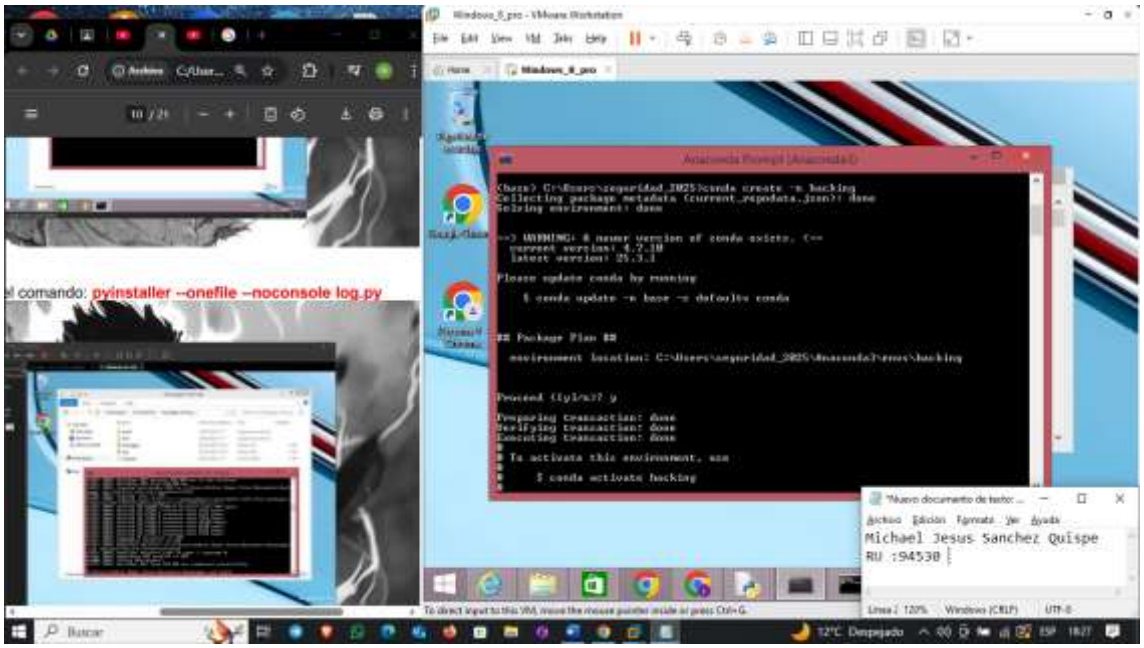
Adjunto prueba

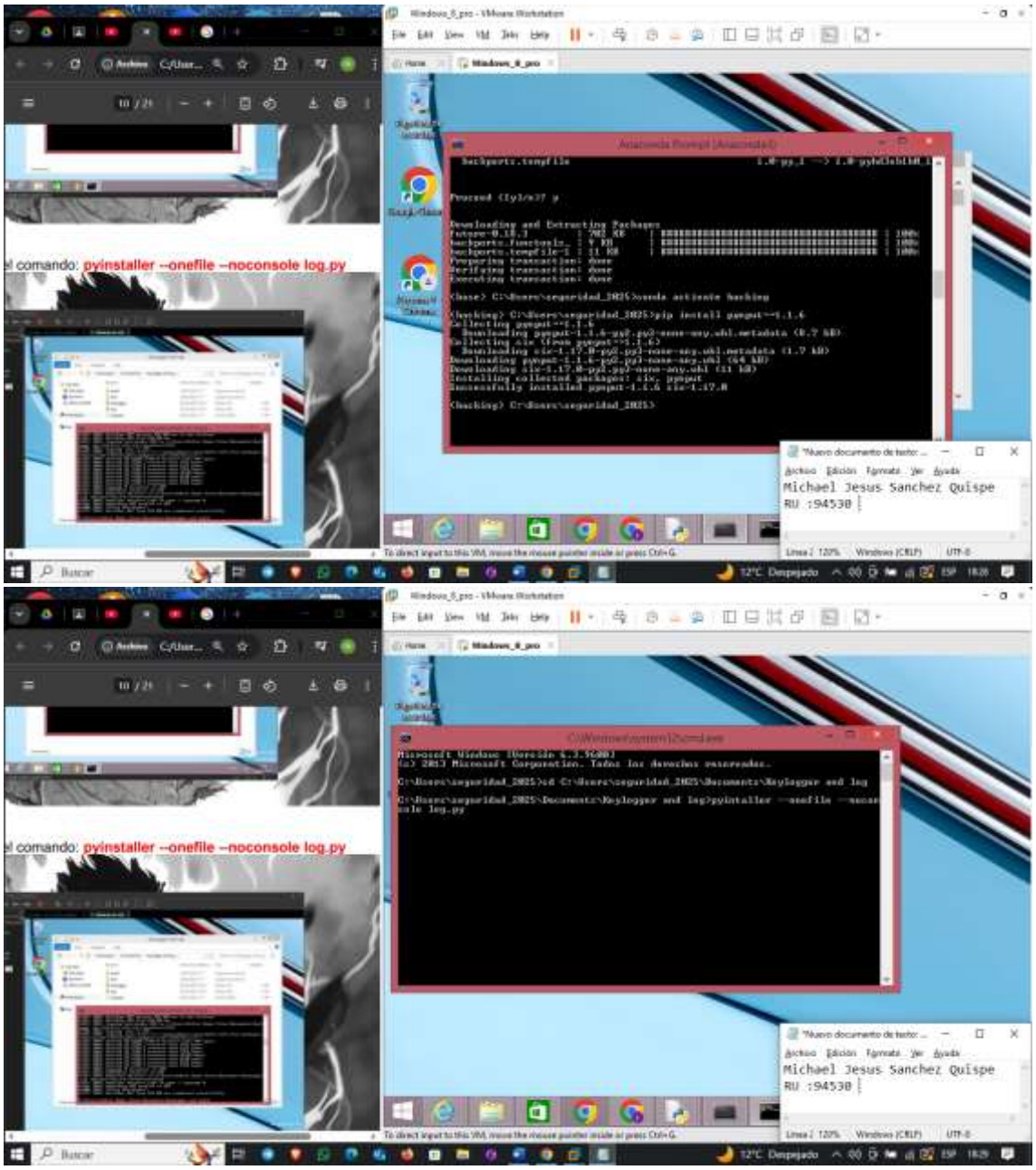



Finalmente guardamos y cerramos, al final abr
opción de gmail.com en la línea de validación
Michael Jesus Sanchez Quispe
RU :94530

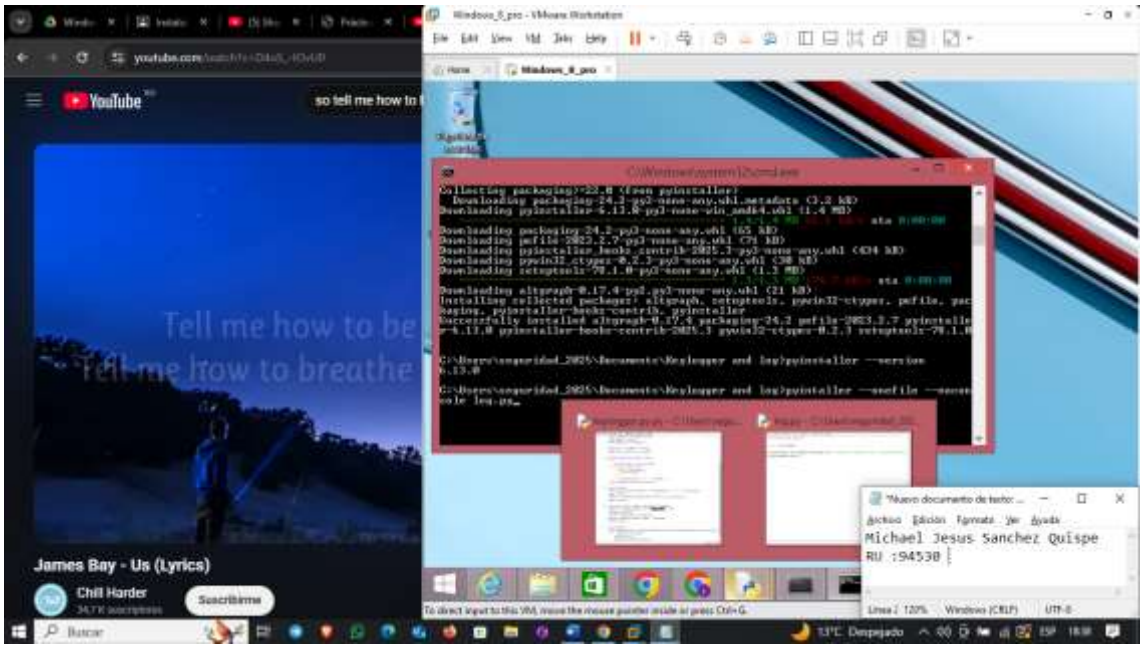

s el archivo ejecutable:
el CMD y activamos el entorno de python2 con
este paso en la carpeta "documentos" esta
y dos formas de crear un entorno en pythor
E LA INTERFAZ GRAFICA proporcionada er
Michael Jesus Sanchez Quispe
RU :94530

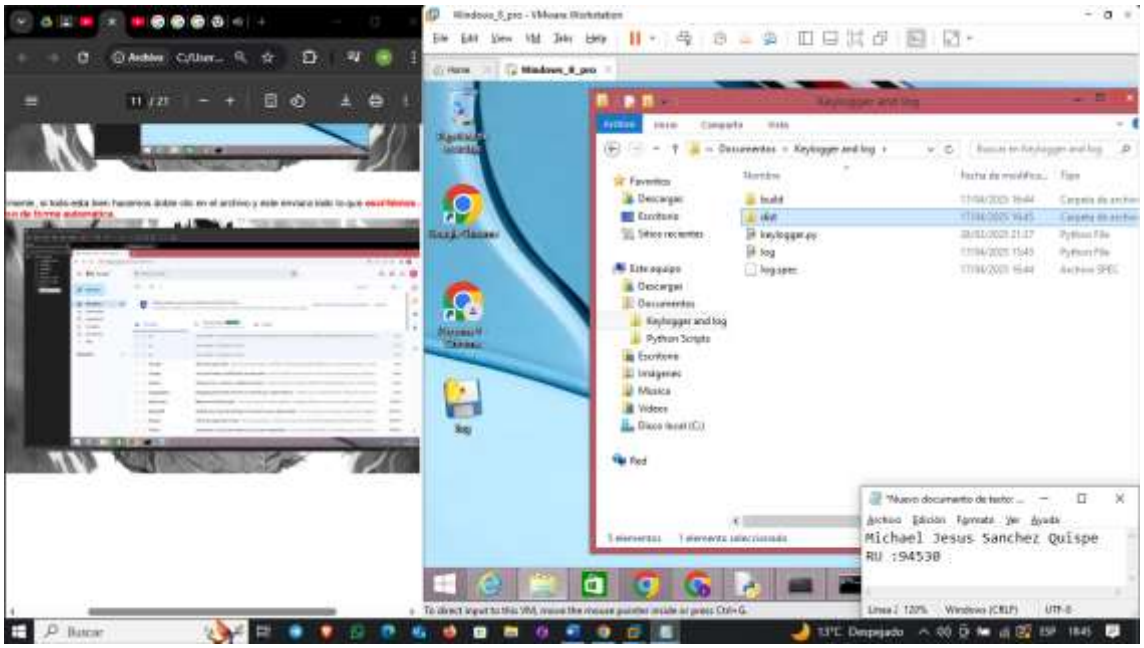

s el archivo ejecutable:
el CMD y activamos el entorno de python2 con
este paso en la carpeta "documentos" esta
y dos formas de crear un entorno en pythor
E LA INTERFAZ GRAFICA proporcionada er
Michael Jesus Sanchez Quispe
RU :94530


el comando: pyinstaller --onefile --noconsole log.py
Michael Jesus Sanchez Quispe
RU :94530

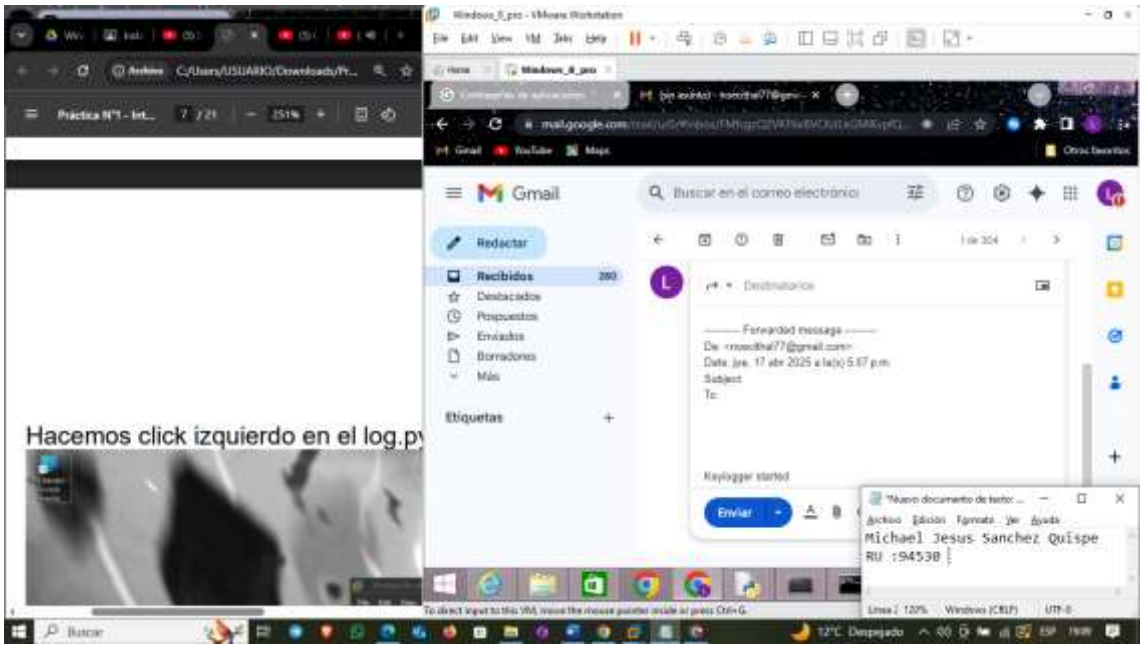


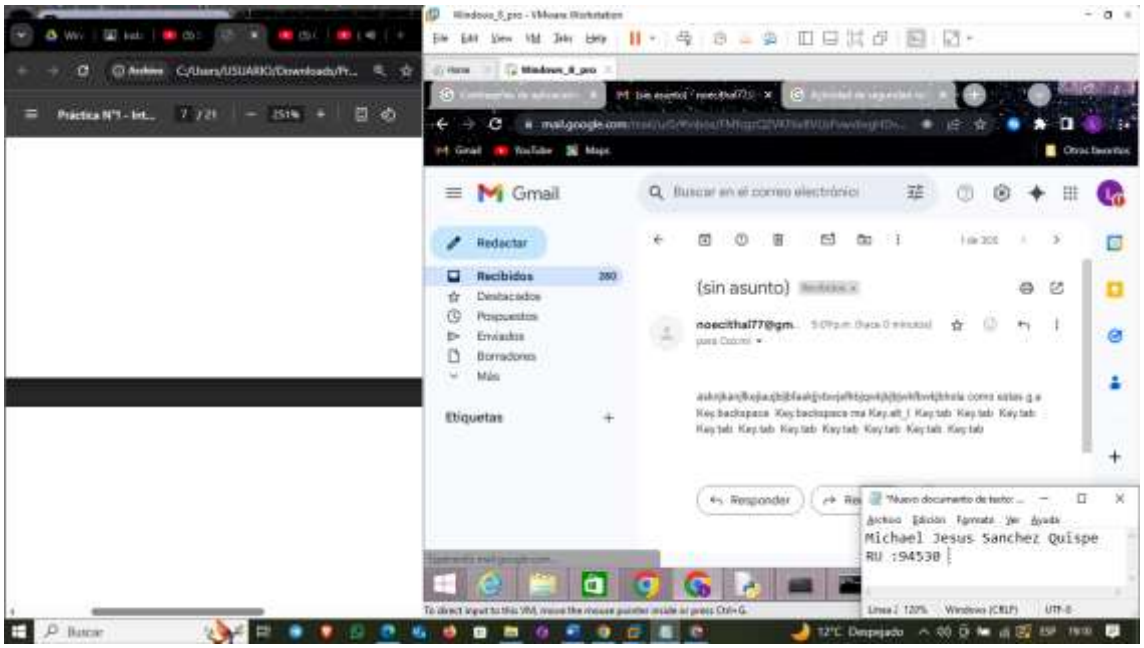
Hasta este punto ya se hicieron todas las instalaciones necesarias tanto de anaconda3 como de `pyinstaller` y tambien Python





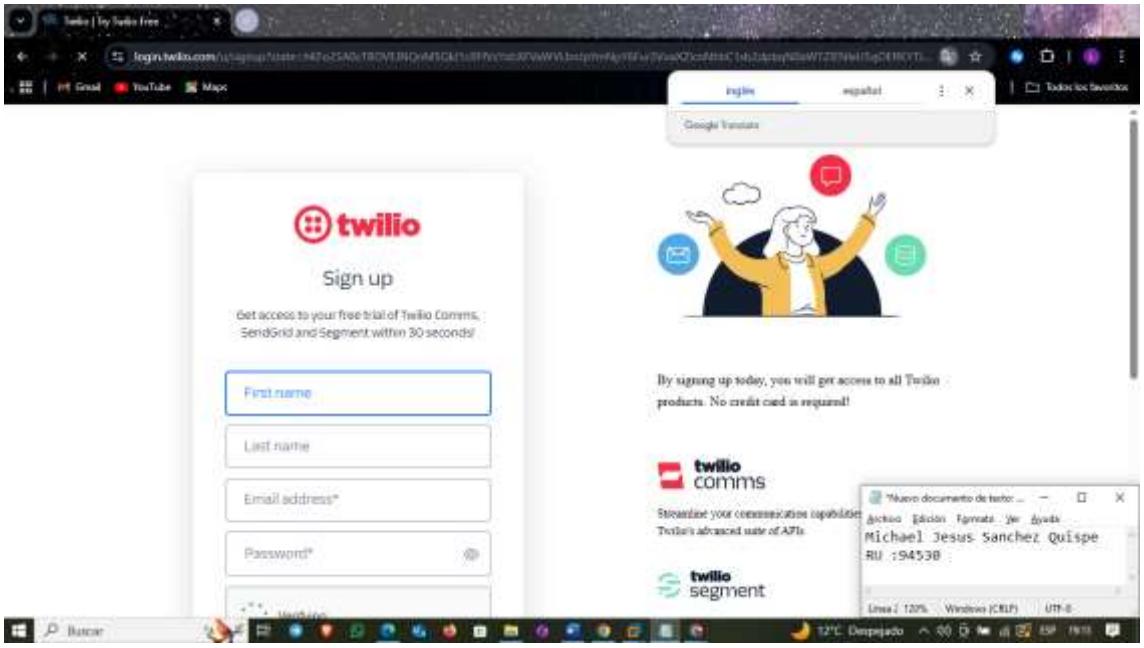
Y por ultimo a continuación los resultados se muestran como todo lo que se escribe en el teclado llega al correo electrónico asociado en la parte 1 de la practica

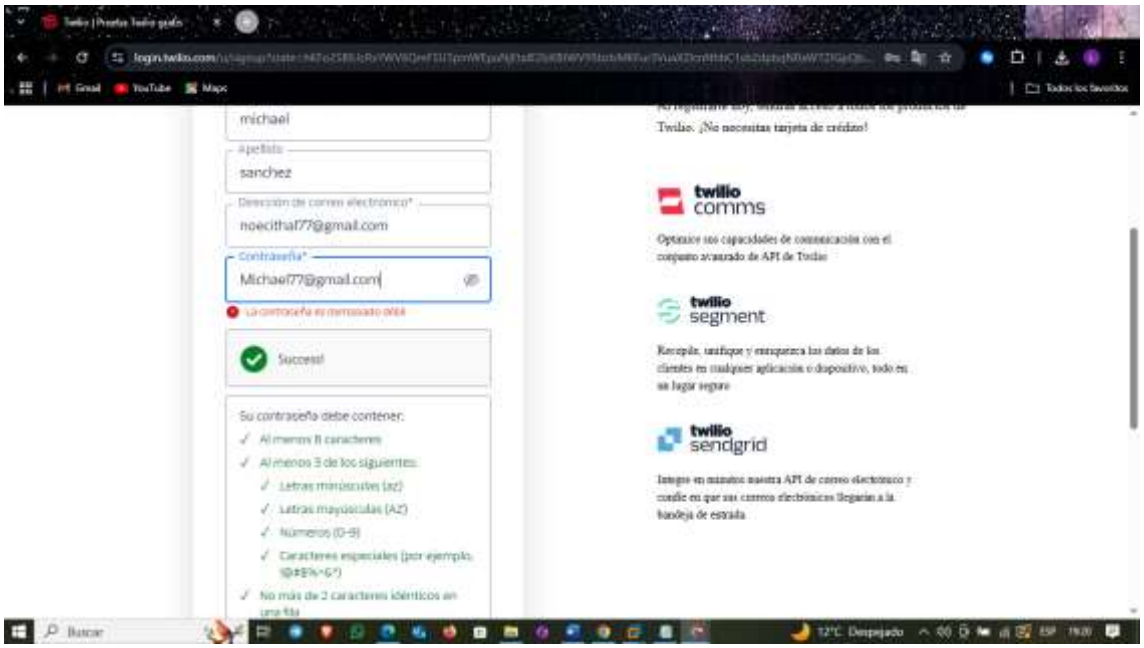

Hacemos click izquierdo en el log.py
Gmail
Buscar en el correo electrónico
Redactar
Recibidos
Destacados
Pospuestos
Enviados
Borradores
Más
Etiquetas
Keylogger started
Enviar
Michael Jesus Sanchez Quispe
RU :94530


Gmail
Buscar en el correo electrónico
Redactar
Recibidos
Destacados
Pospuestos
Enviados
Borradores
Más
Etiquetas
(sin asunto)
Responder
Michael Jesus Sanchez Quispe
RU :94530

Evaluación 1

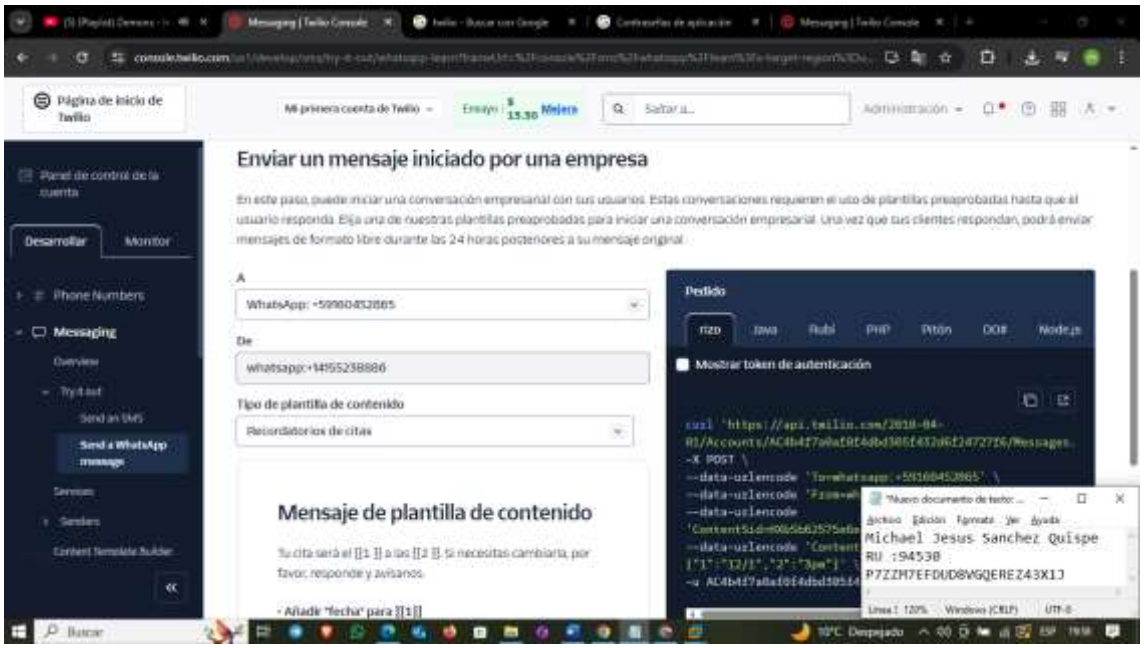
primero nos registramos



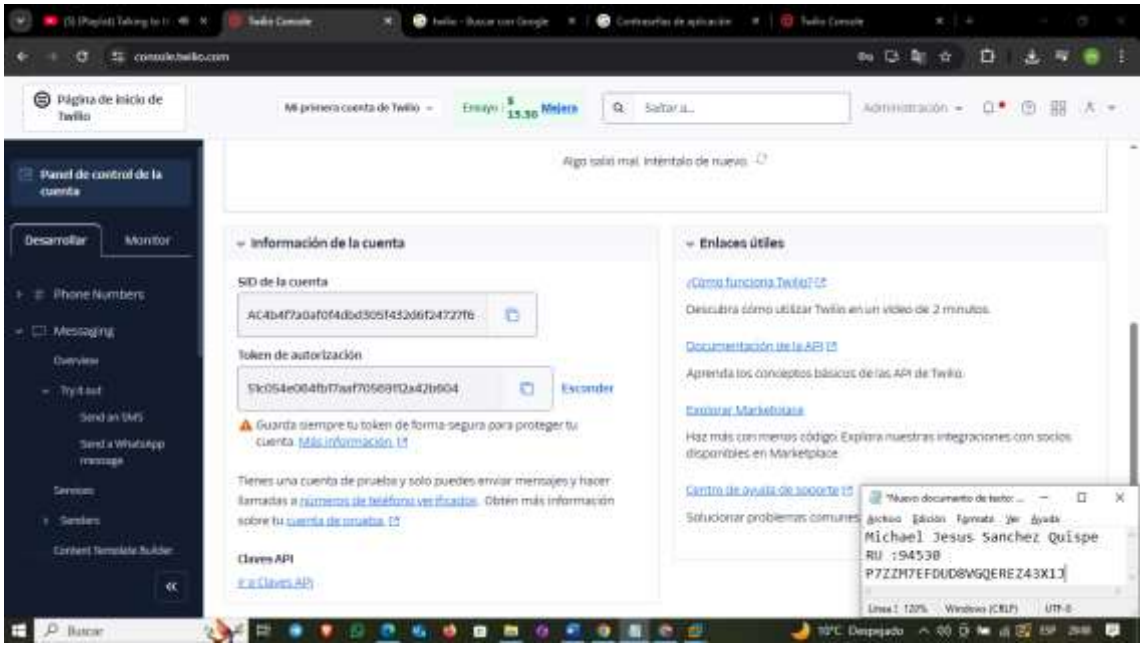


Para este use mi otra cuenta debido a que la primera me daba lo siguiente

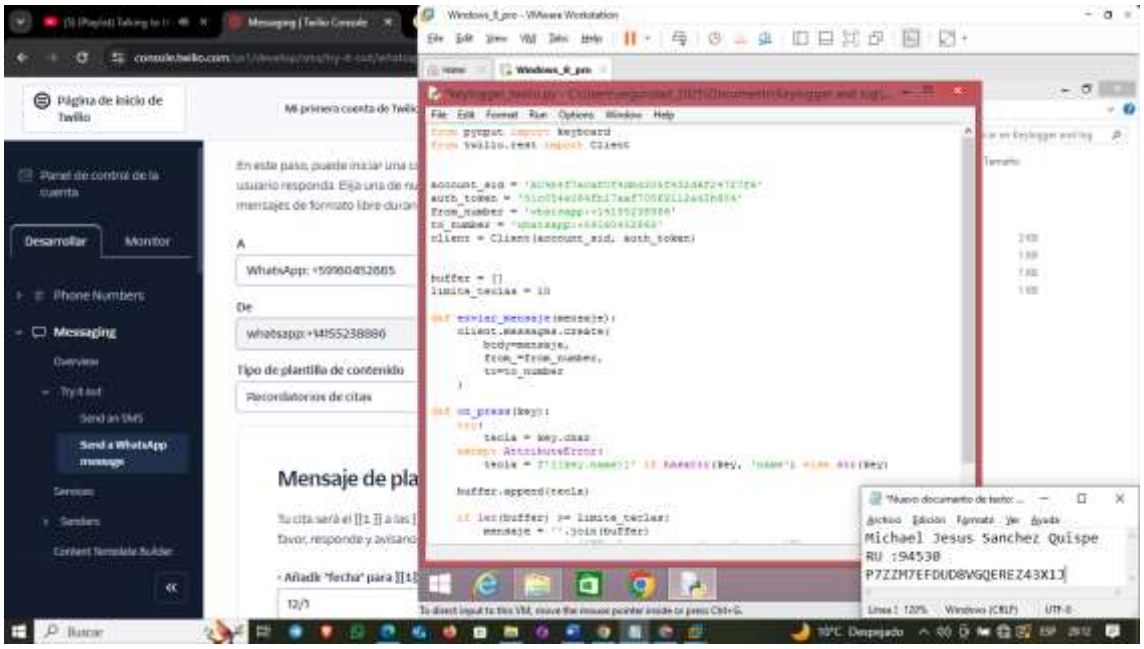
Aquí obtuve el numero para realizar la prueba y escaneando un codigo QR me lanxo al chat con el numero

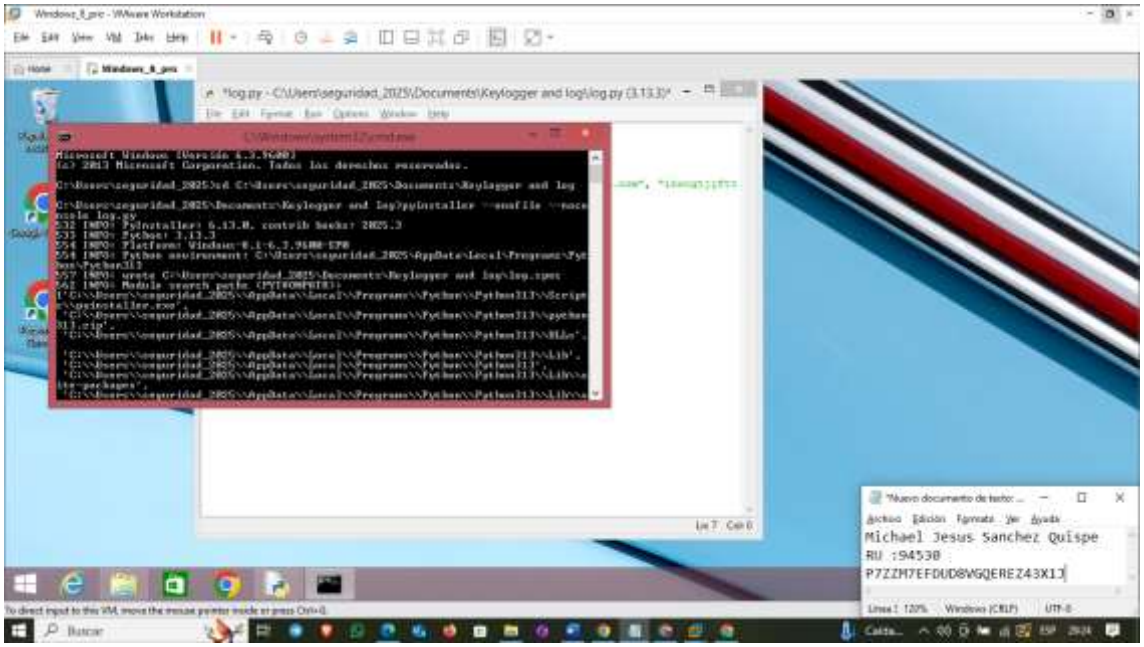


Como tambien mi SID y Token

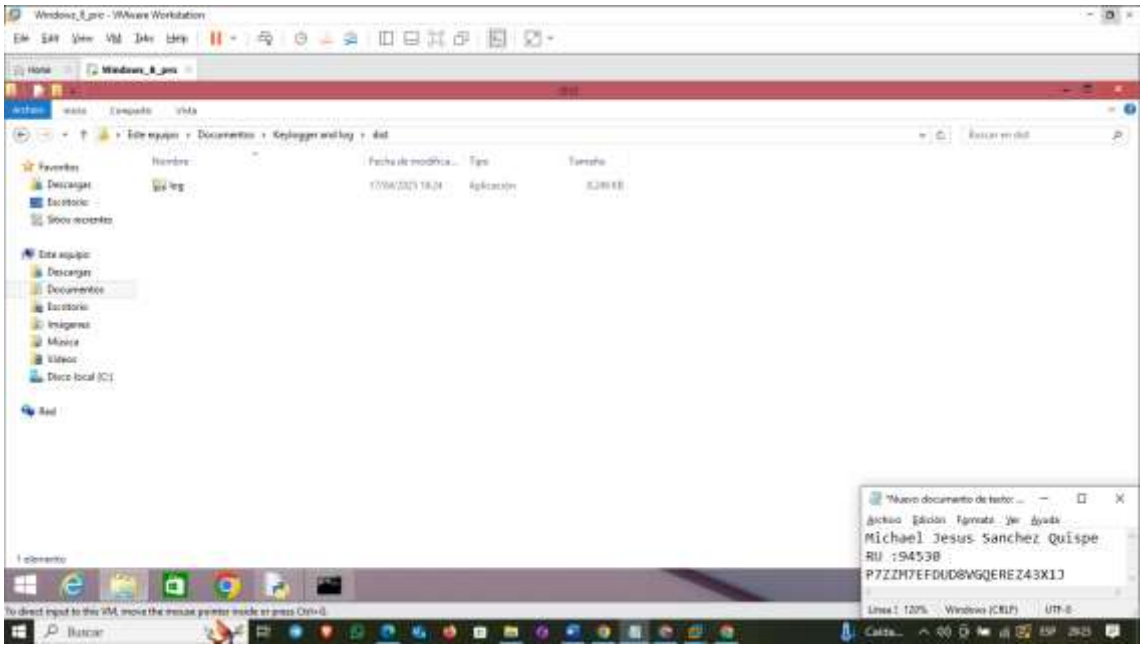


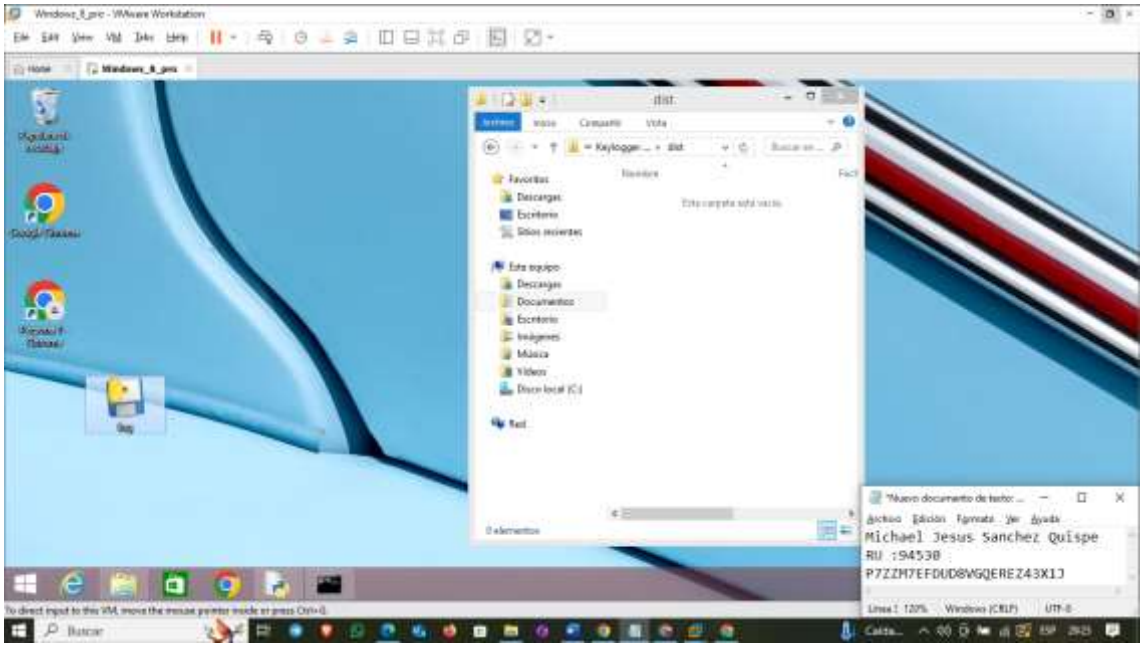
En esta parte cree otro archivo .py para poner el codigo de la evaluación la cual trabaja con twilio

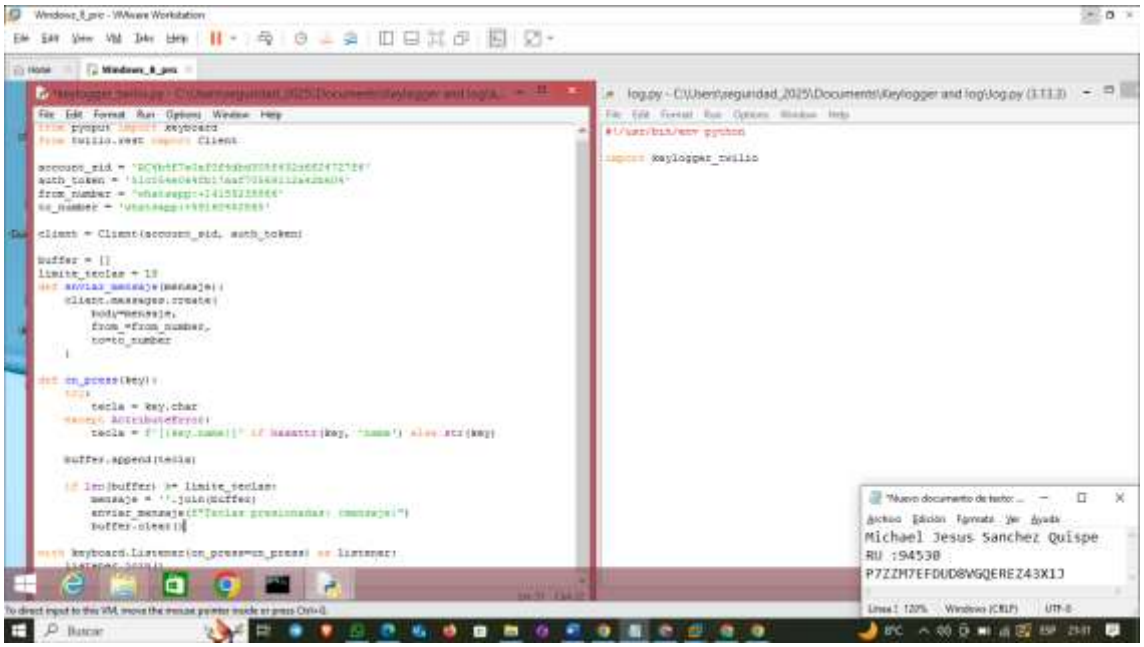


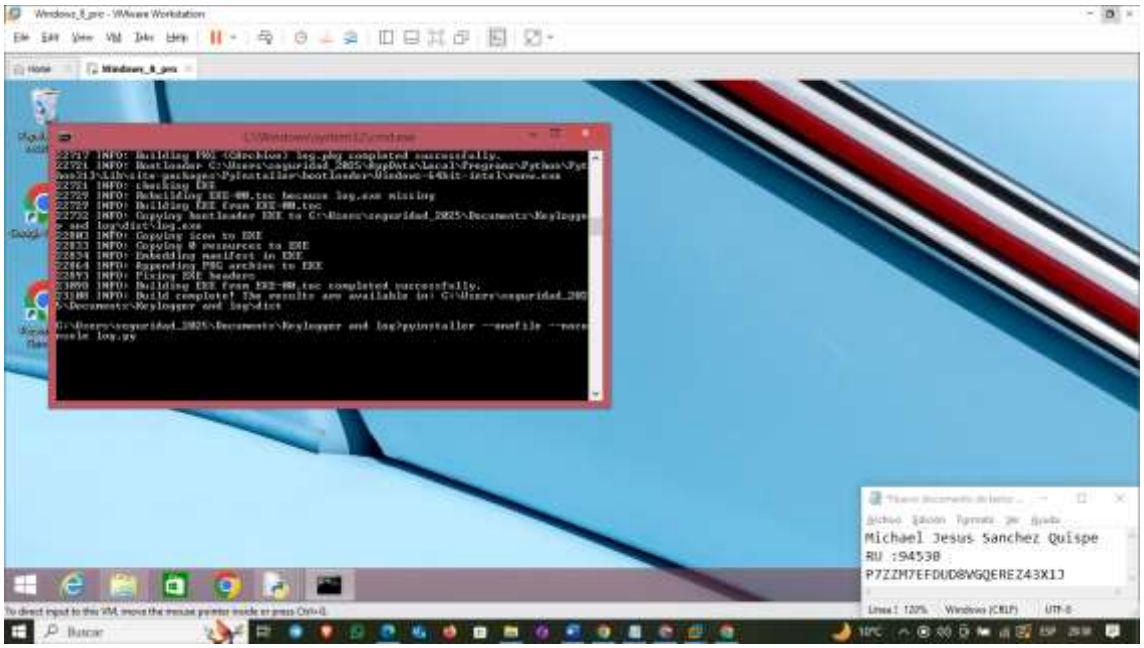


Use el archivo y la misma maquina virtual y el archivo log solo para importar keylogger_twilio

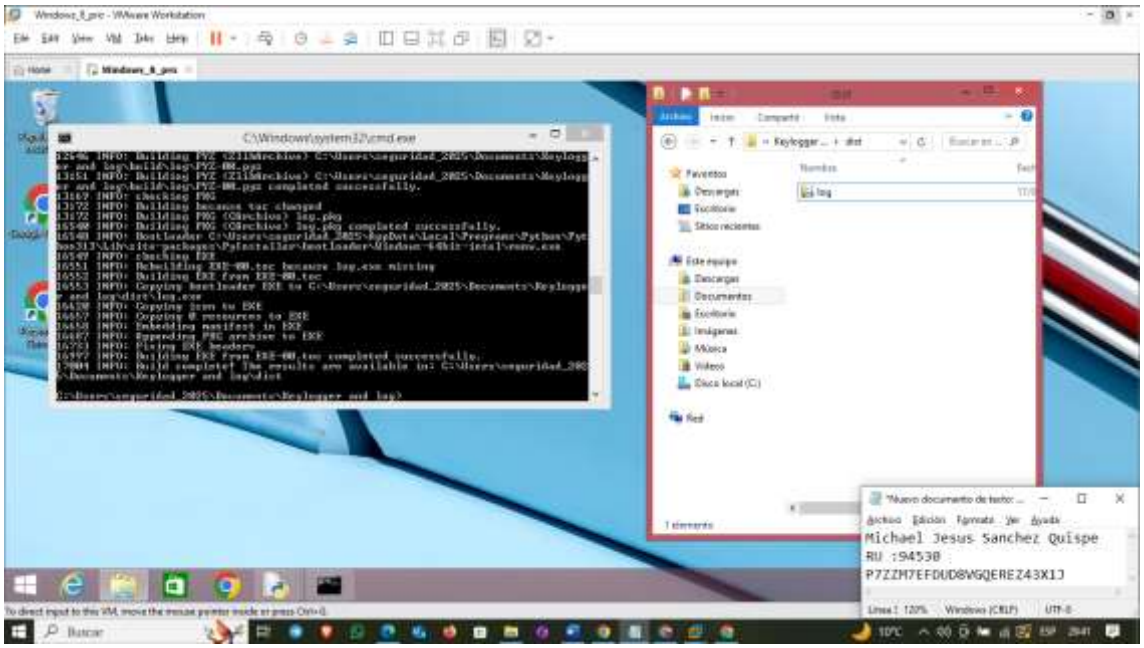


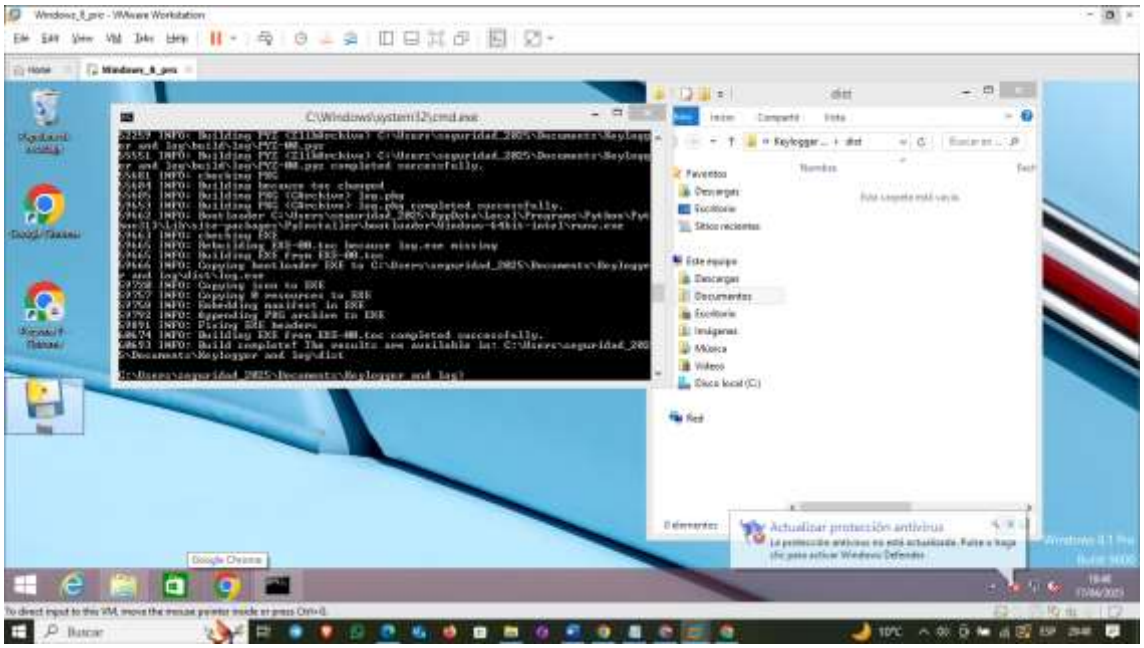




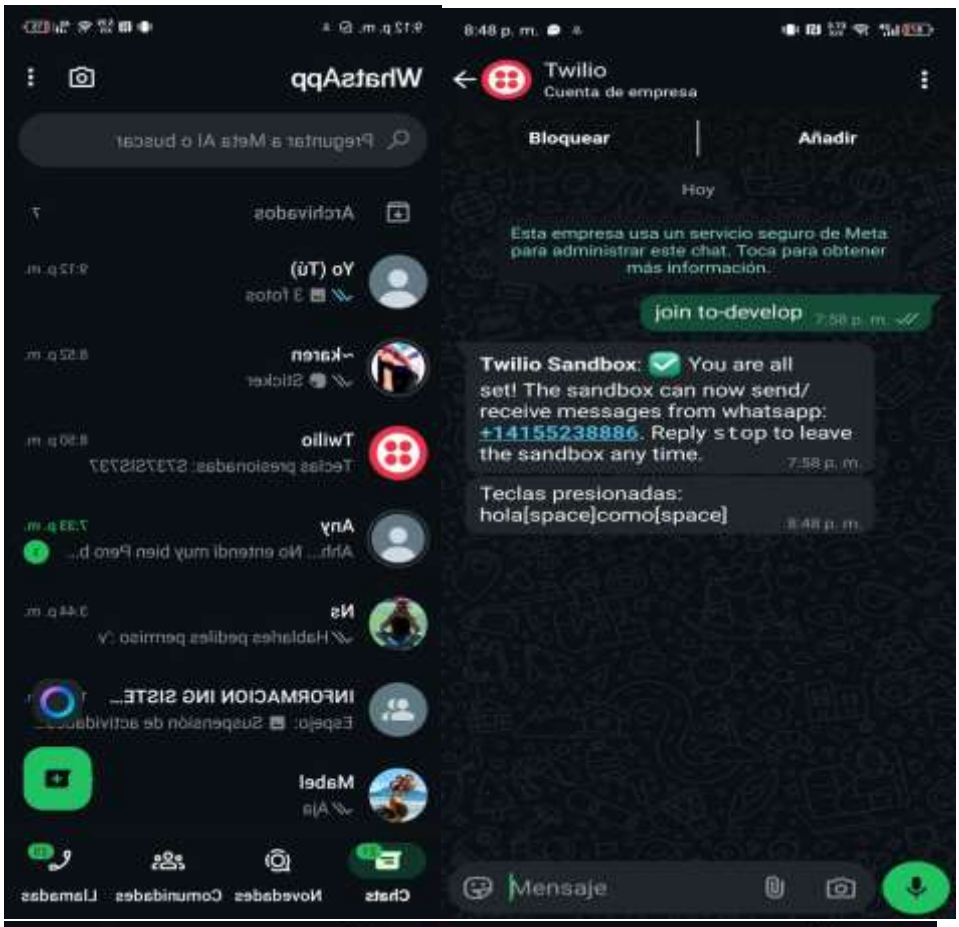


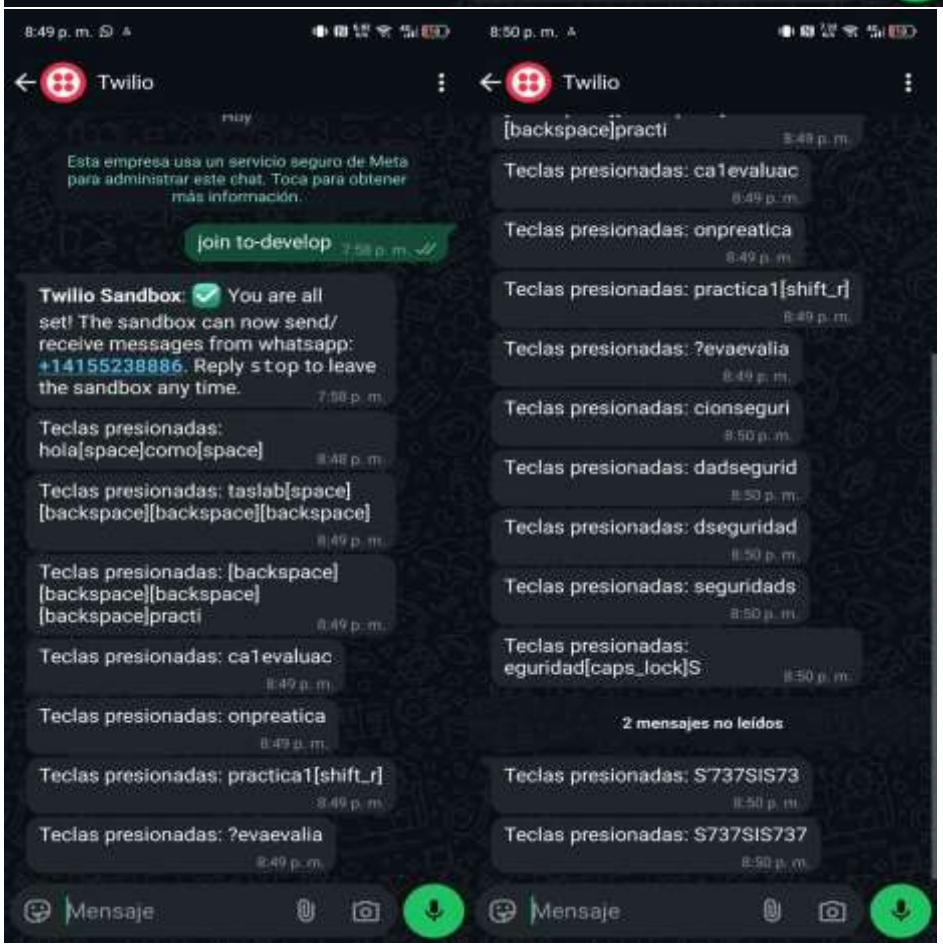
pyinstaller --onefile --noconsole log.py use este comando para generar el ejecutable y empaquetar todo en un .exe



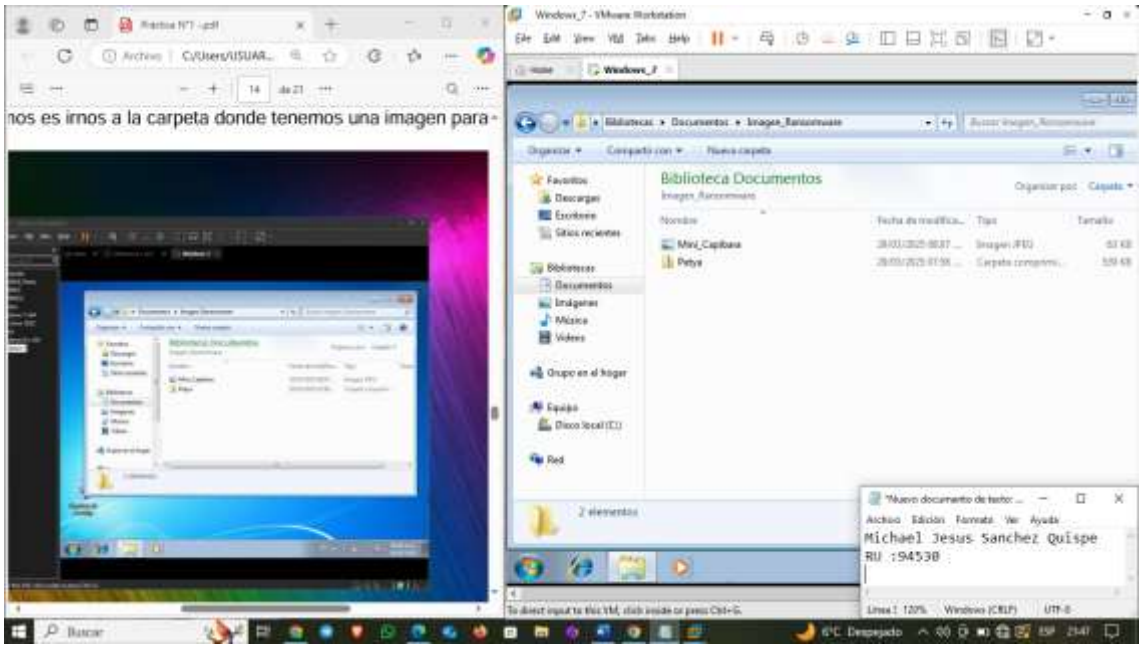


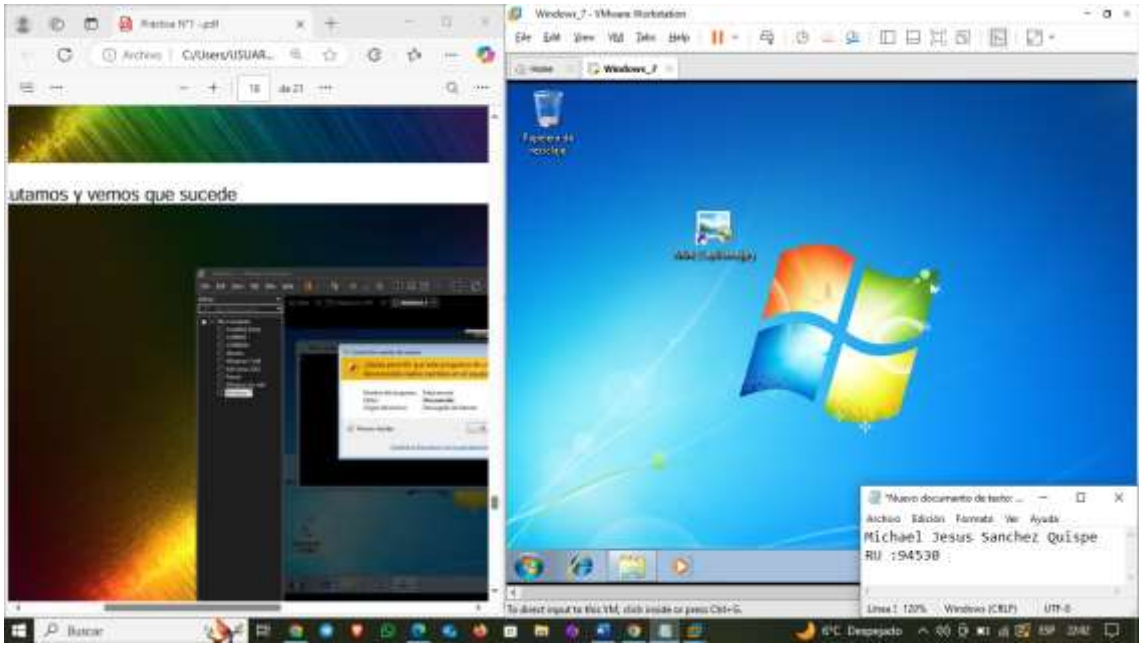
Y a continuación adjunto el chat de twilio en mi watsApp totalmente funcional.

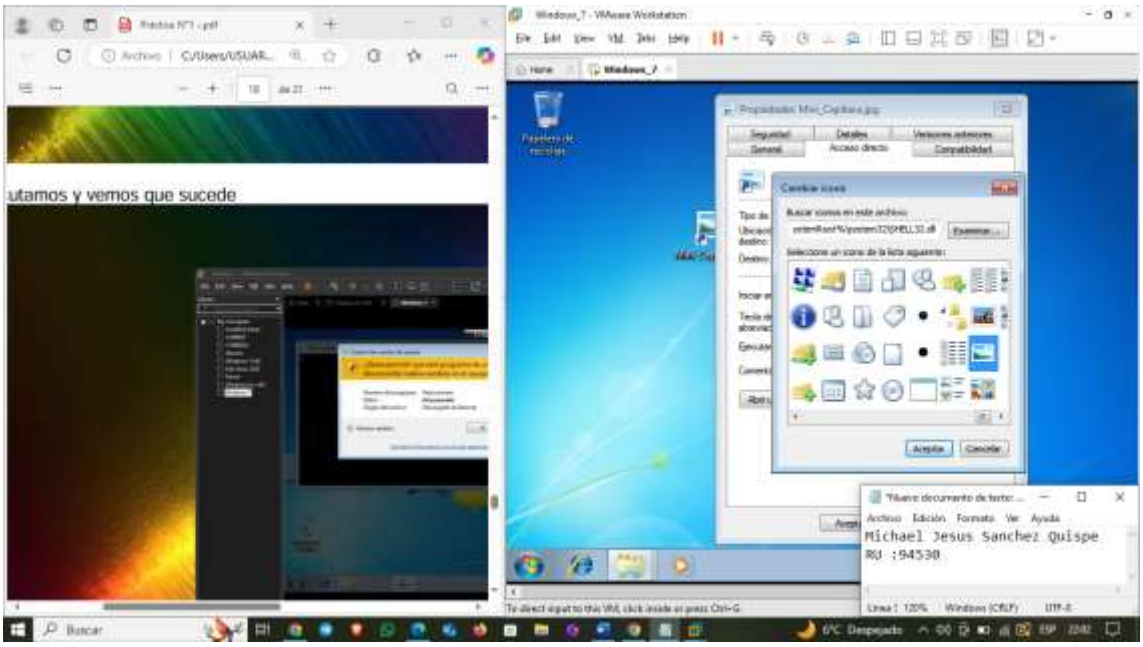

Twilio
Cuenta de empresa
Bloquear
Añadir
Hoy
Esta empresa usa un servicio seguro de Meta para administrar este chat. Toca para obtener más información.
join to-develop
Twilio Sandbox: You are all set! The sandbox can now send/ receive messages from whatsapp: +14155238886. Reply stop to leave the sandbox any time.
Teclas presionadas: hola[space]como[space]
Mensaje


Twilio
Esta empresa usa un servicio seguro de Meta para administrar este chat. Toca para obtener más información.
join to-develop
Twilio Sandbox: You are all set! The sandbox can now send/ receive messages from whatsapp: +14155238886. Reply stop to leave the sandbox any time.
Teclas presionadas: hola[space]como[space]
Teclas presionadas: taslab[space][backspace][backspace][backspace]
Teclas presionadas: [backspace][backspace][backspace][backspace]practi
Teclas presionadas: ca1evaluac
Teclas presionadas: onpreatica
Teclas presionadas: practica1[shift_r]
Teclas presionadas: ?evaevalia
Mensaje
Twilio
[backspace]practi
Teclas presionadas: ca1evaluac
Teclas presionadas: onpreatica
Teclas presionadas: practica1[shift_r]
Teclas presionadas: ?evaevalia
Teclas presionadas: cionseguri
Teclas presionadas: dadsegurid
Teclas presionadas: dseguridad
Teclas presionadas: seguridads
Teclas presionadas: eguridad[caps_lock]S
2 mensajes no leídos
Teclas presionadas: S737SIS73
Teclas presionadas: S737SIS737
Mensaje

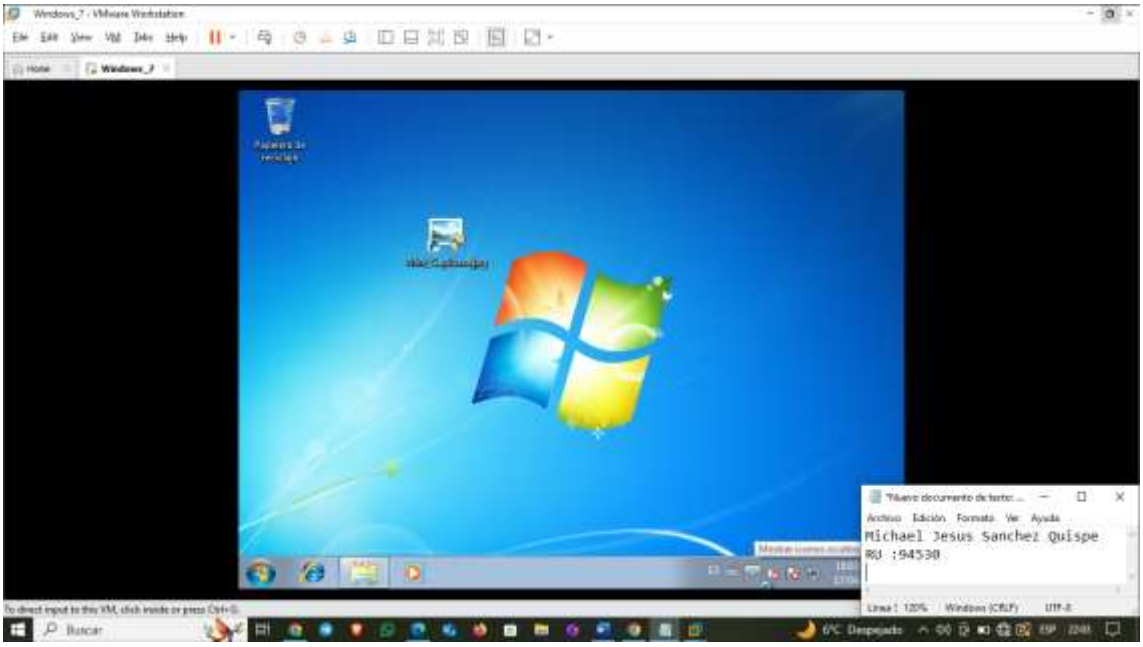
Parte 2

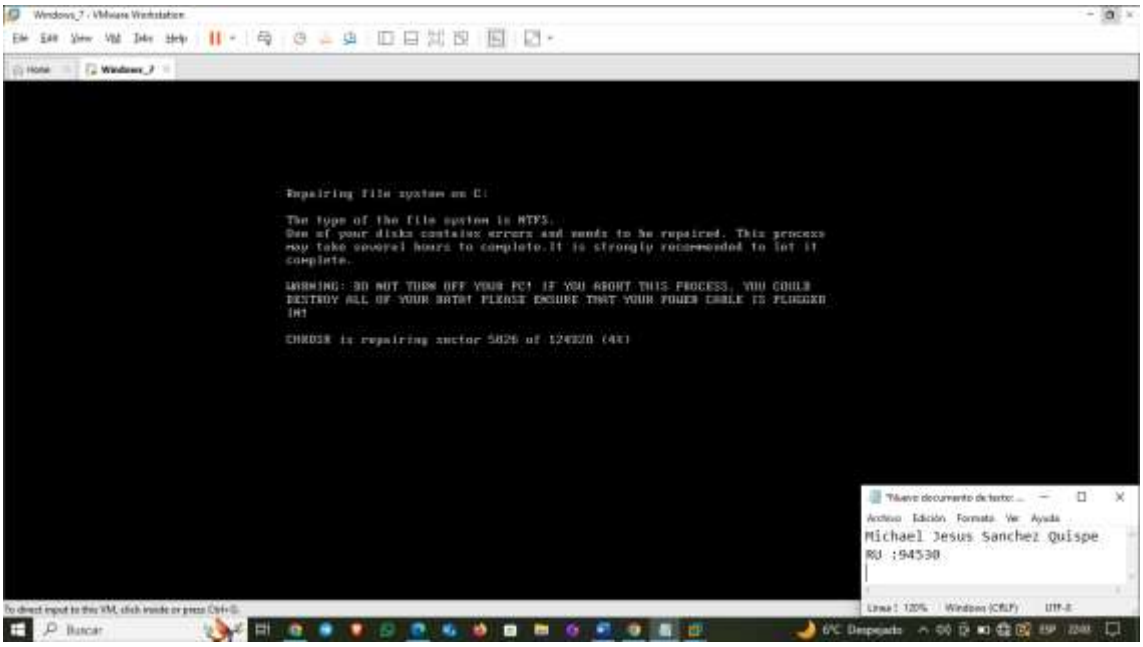

nos es irnos a la carpeta donde tenemos una imagen para
Biblioteca Documentos
Michael Jesus Sanchez Quispe
RU :94530

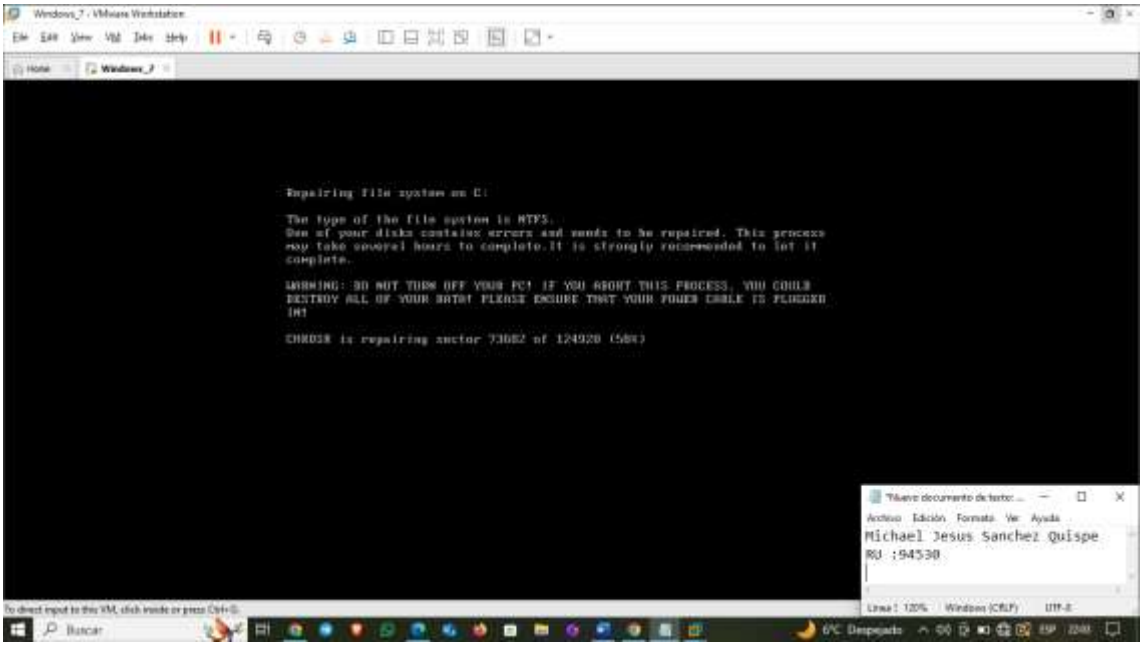

utamos y vemos que sucede
Michael Jesus Sanchez Quispe
RU :94530

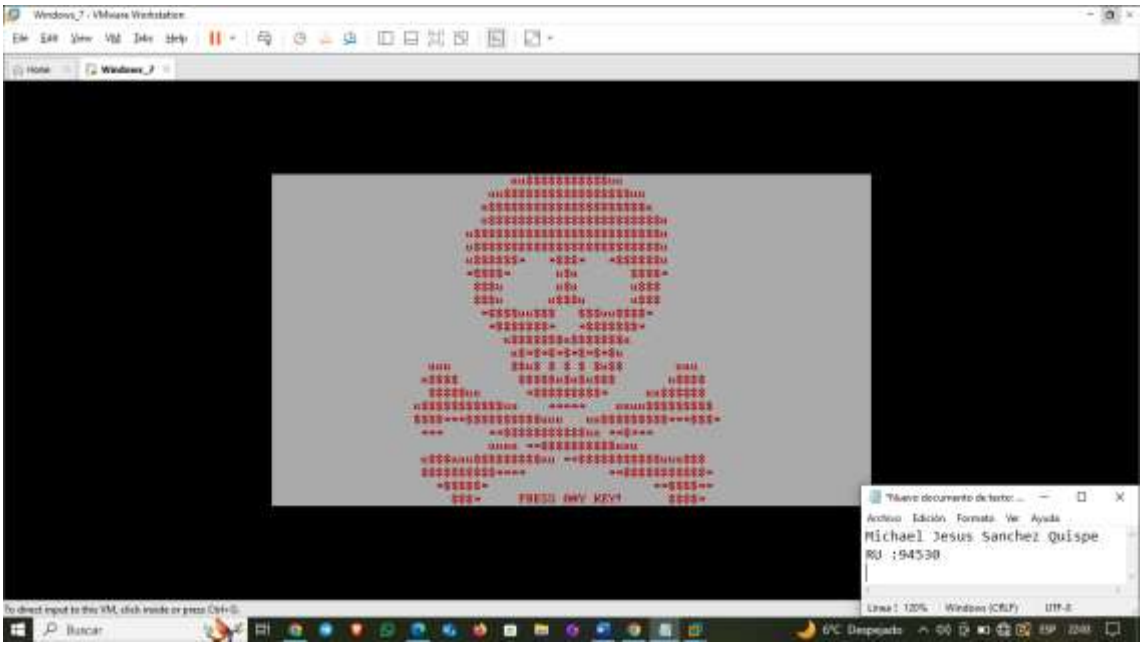


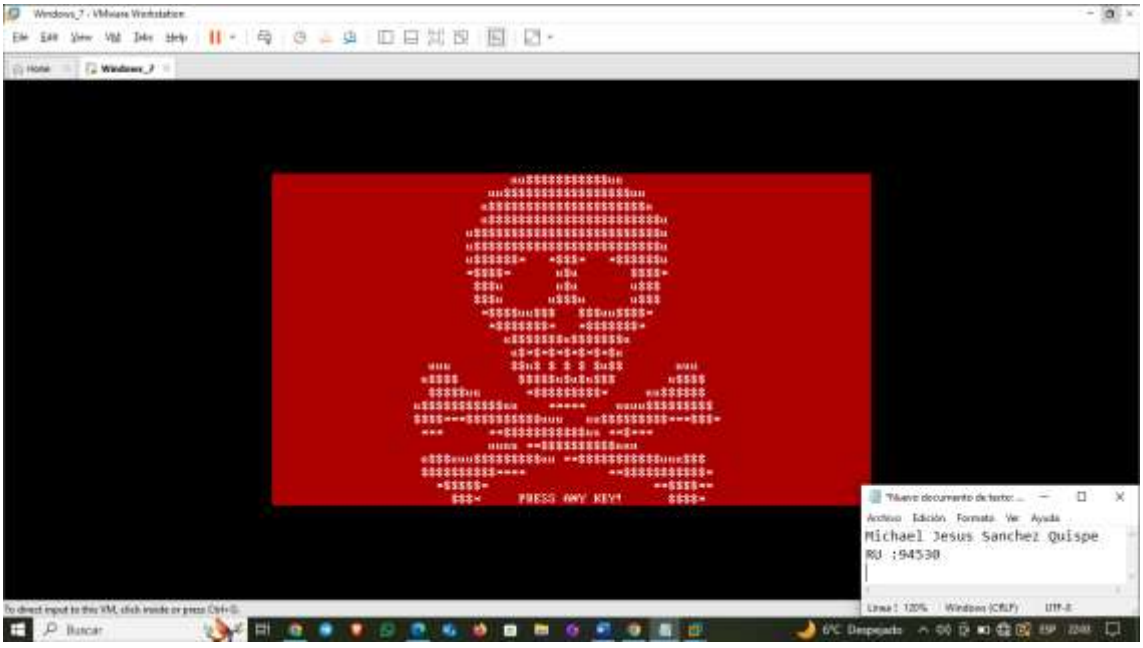
Me falto adjuntar la captura del comando pero despues de correrlo me di cuenta que no se capturo esa

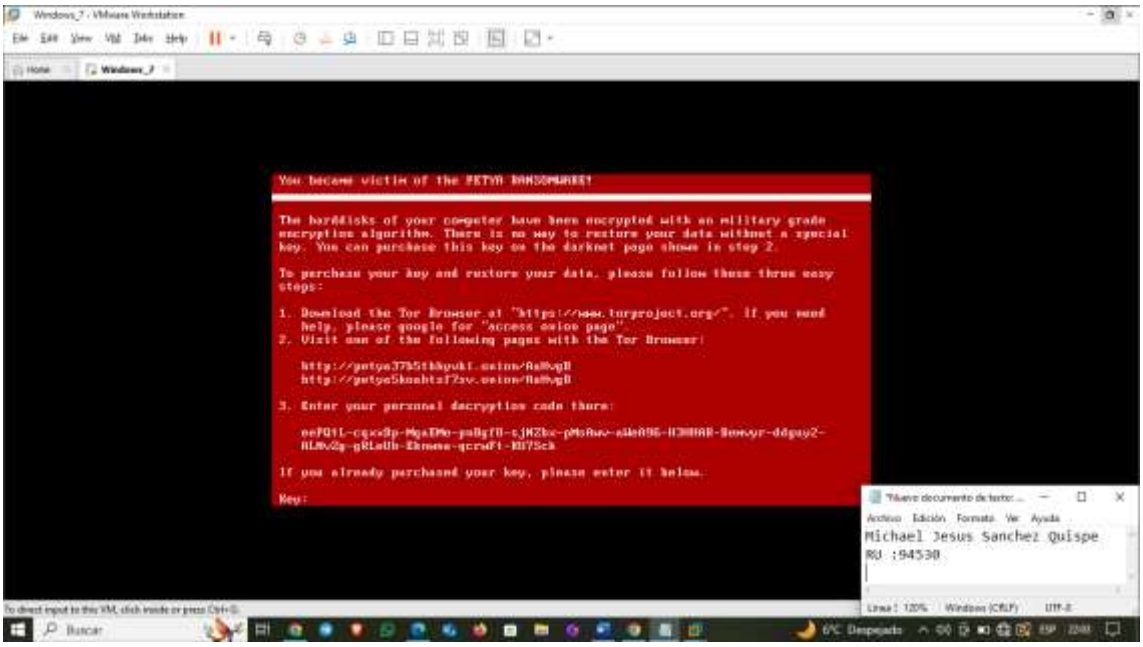



Windows_7 - VMware Workstation
Repairing file system on C:
The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete.It is strongly recommended to let it
complete.
WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!
CHKDSK is repairing sector 5826 of 124920 (4%)
Michael Jesus Sanchez Quispe
RU :94530


Windows_7 - VMware Workstation
Repairing file system on C:
The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete.It is strongly recommended to let it
complete.
WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!
CHKDSK is repairing sector 73082 of 124920 (58%)
Michael Jesus Sanchez Quispe
RU :94530

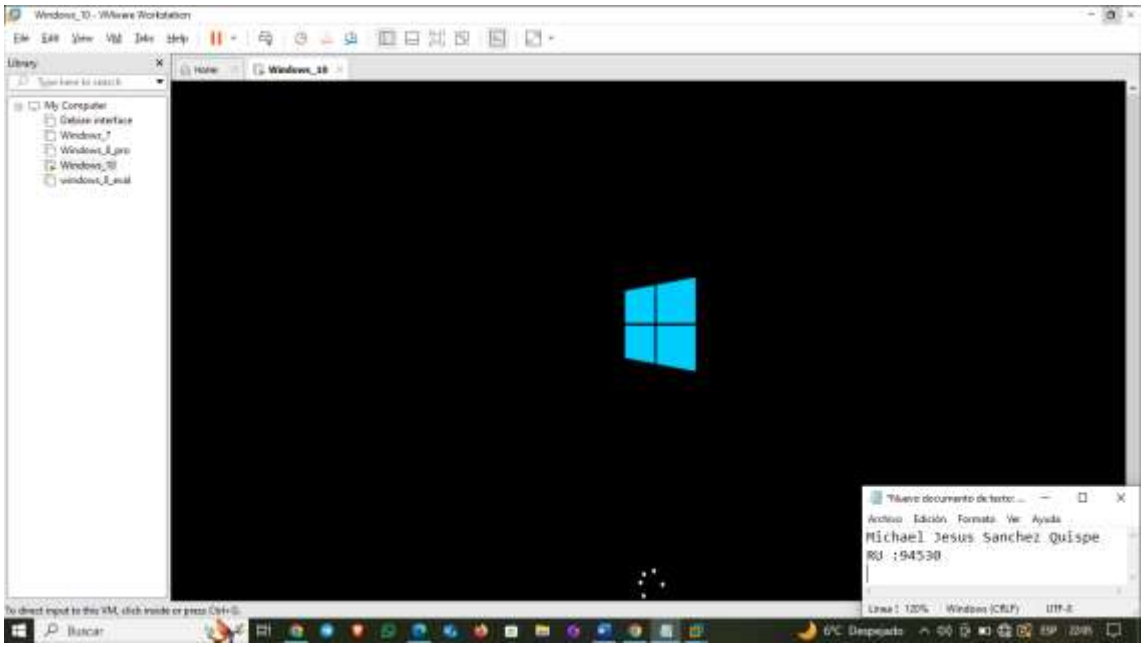

Michael Jesus Sanchez Quispe
RU :94530

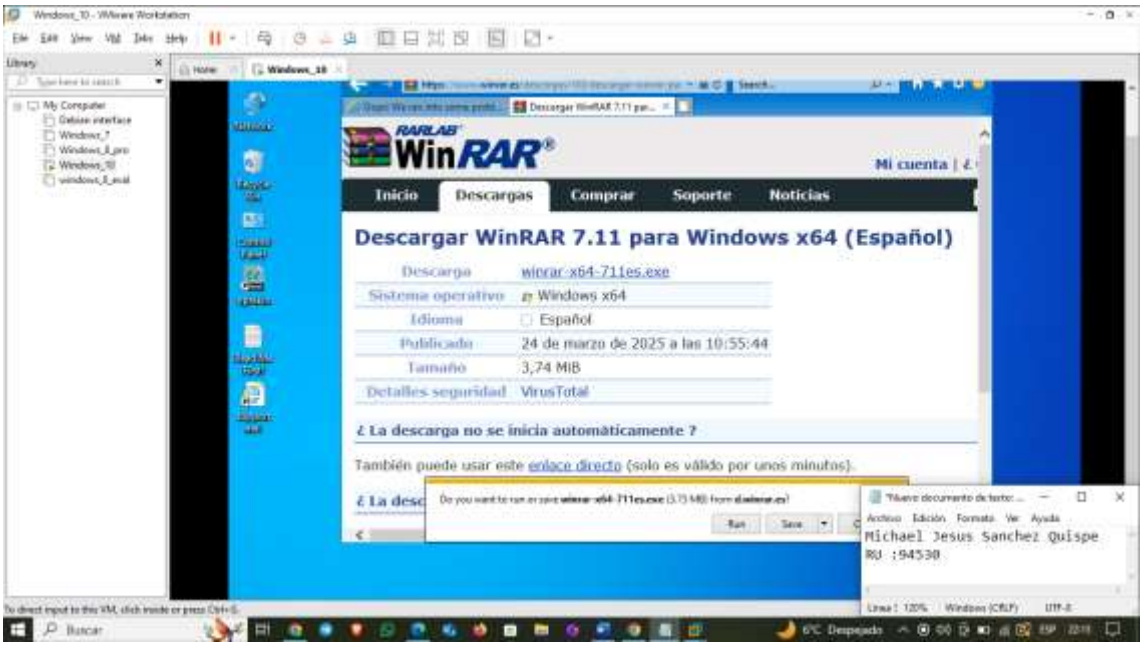

Michael Jesus Sanchez Quispe
RU :94530



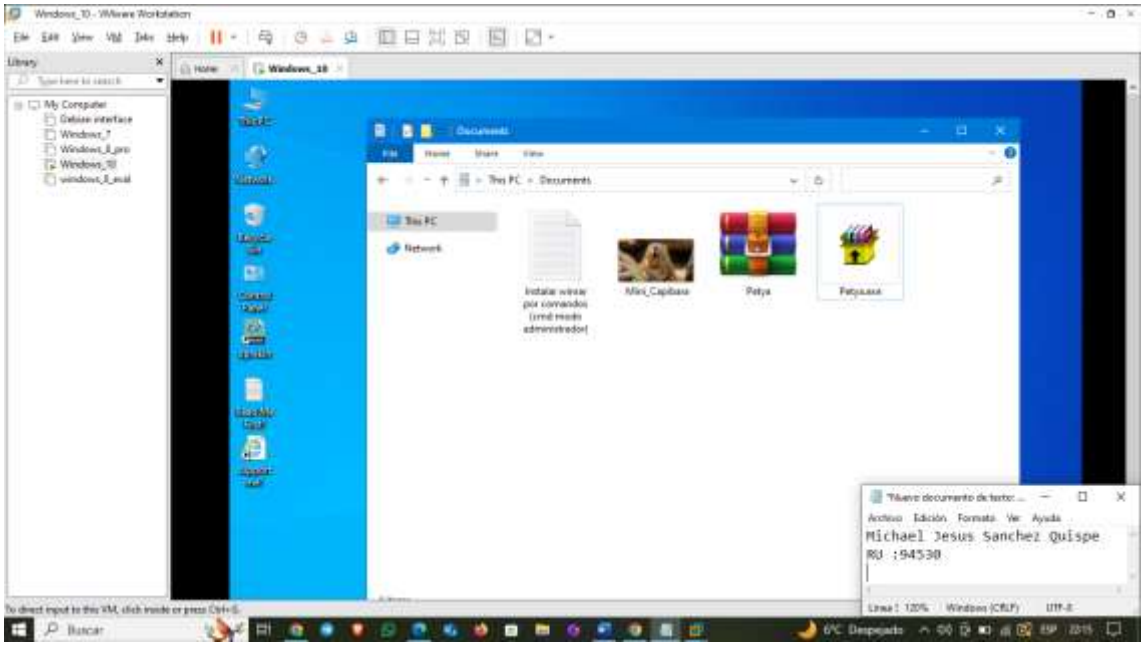
Evaluación 2

Hacemos el uso del Ransomware en un sistema operativo Windows 10

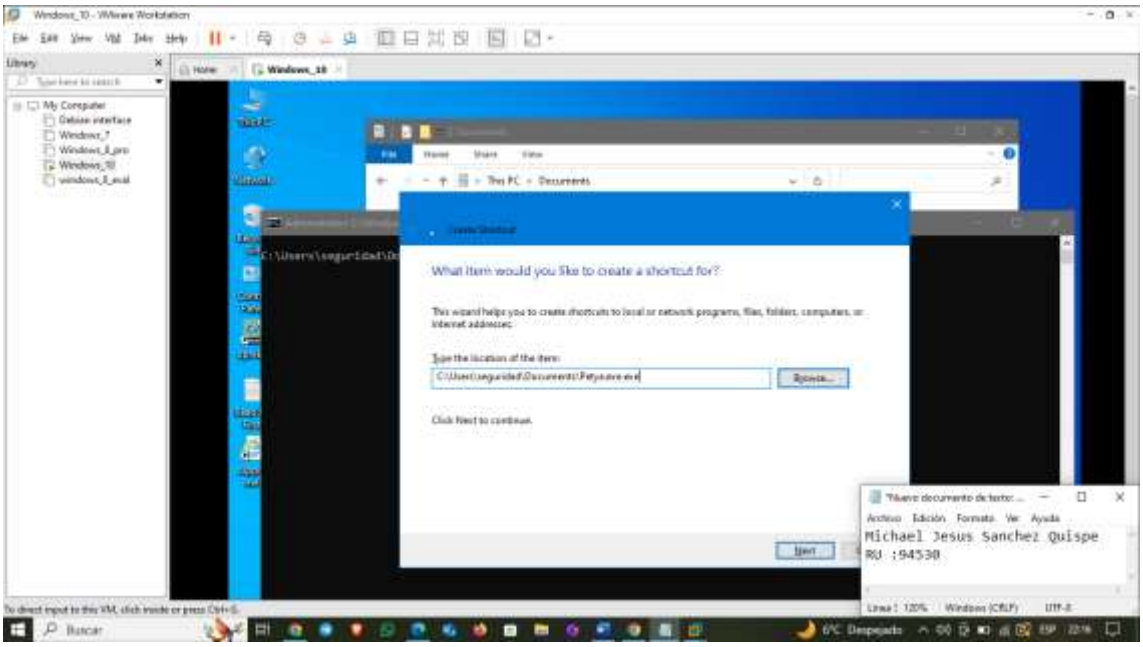




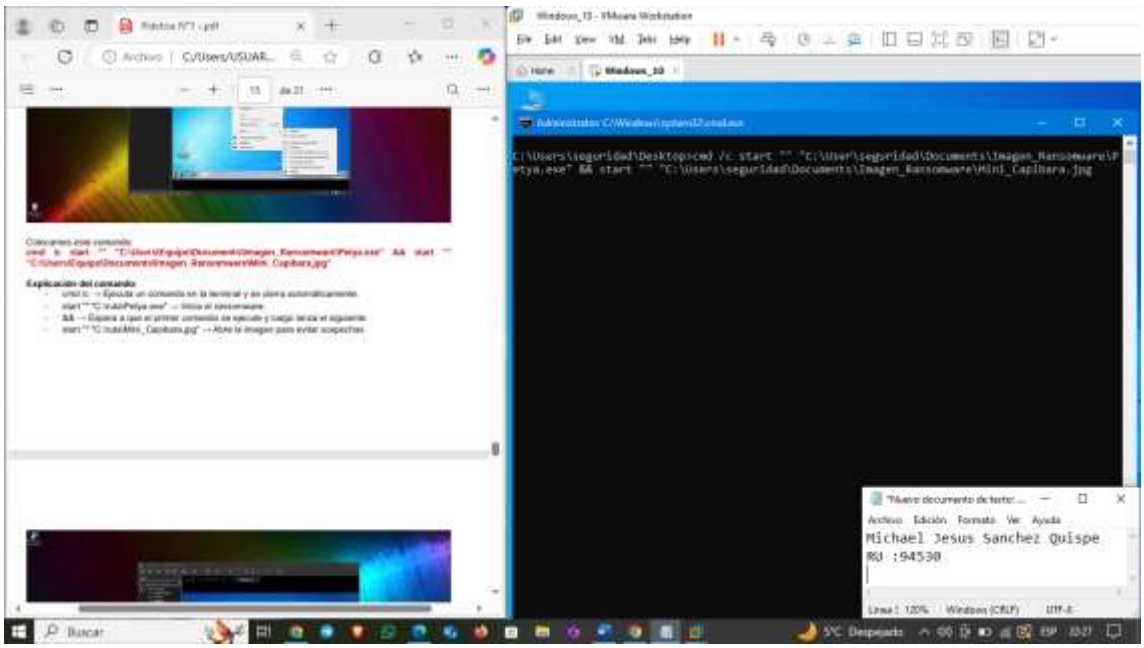
Descomprimimos el archivo Penya,exe

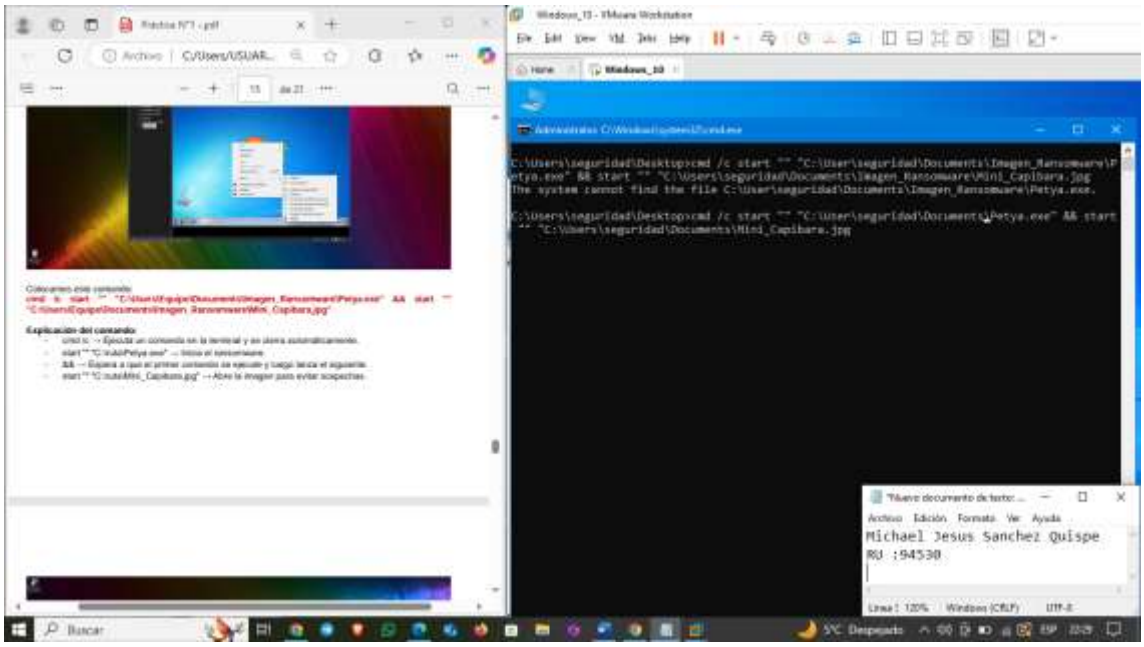


Creamos el acceso directo donde se encargara de ejecutarlo en parte

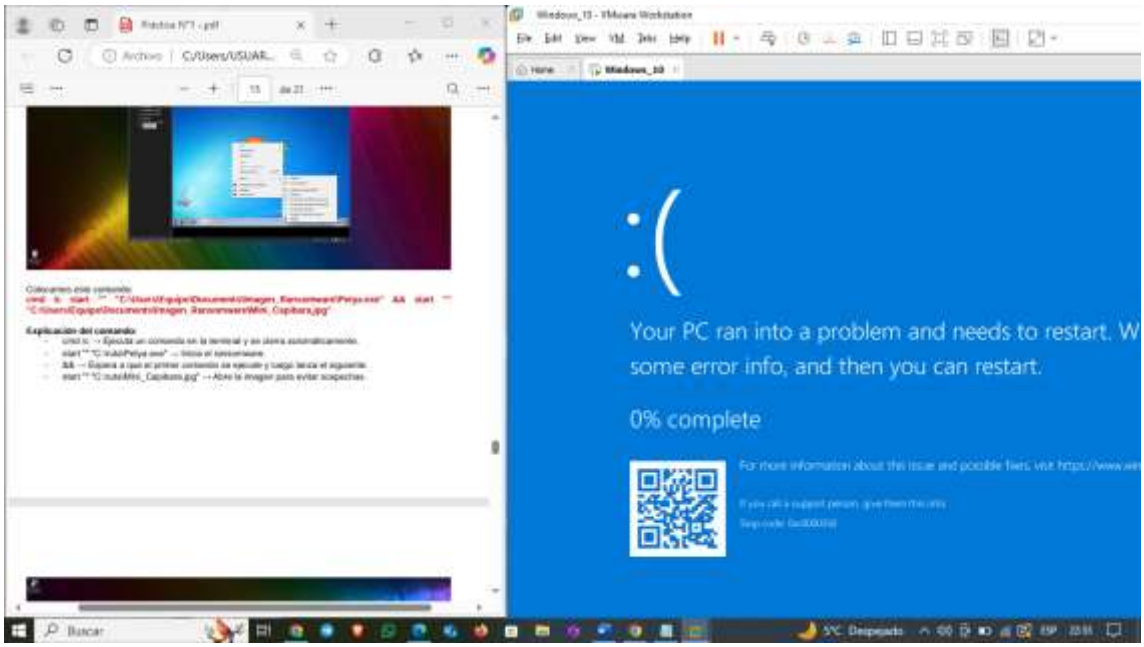


Hacemos el uso de comandos para ejecutarlo

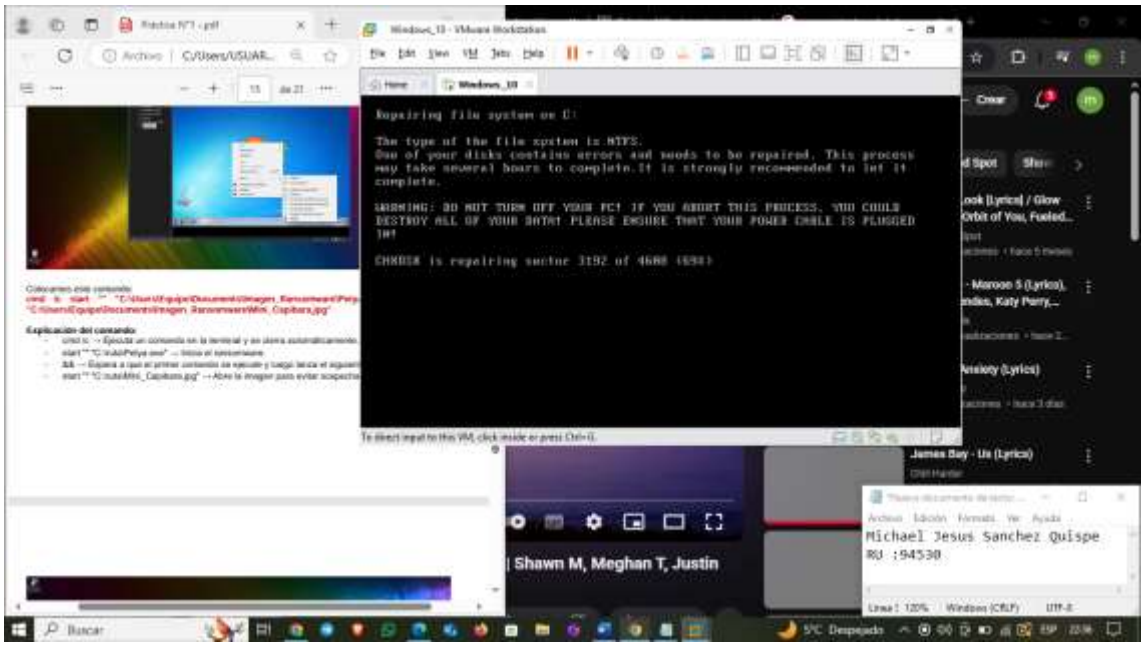


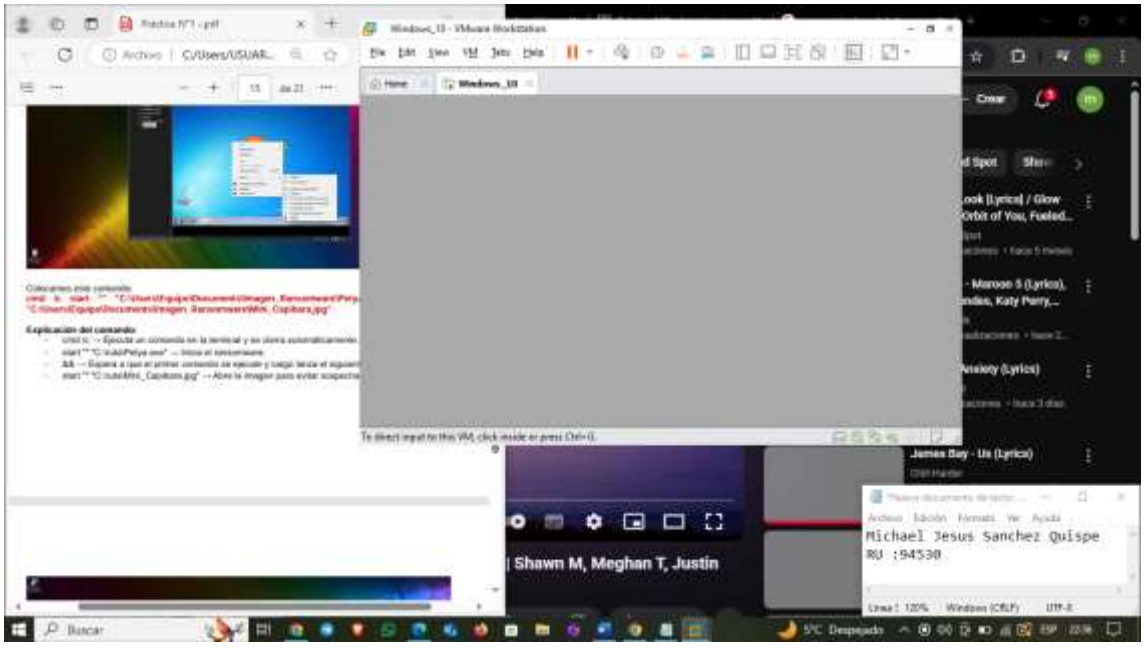


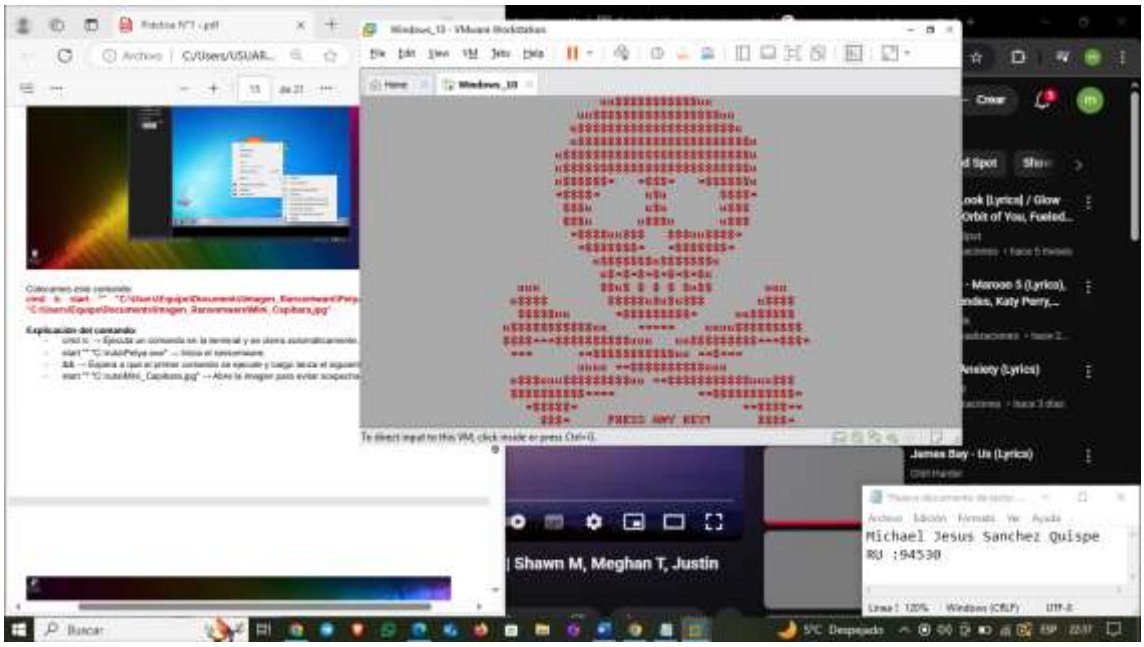
Al hacer uso del comando la maquina de intento defender el equipo y lo reinie

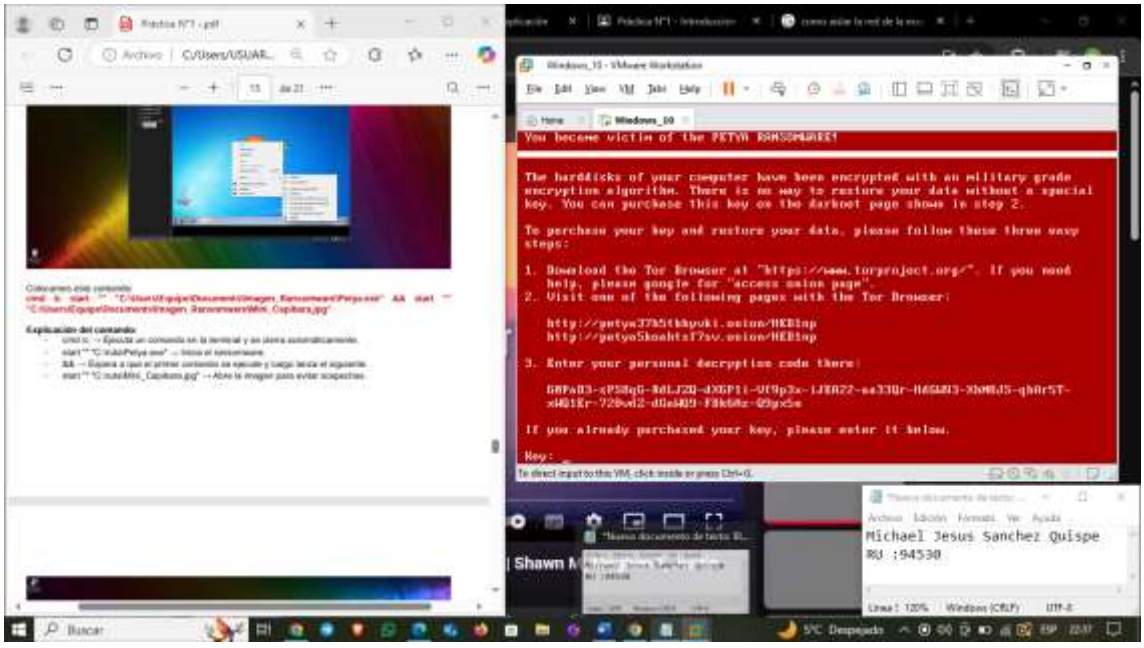


Ni bien se reinicio directamente se ejecuto el Penya.exe


Repairing file system on C:
The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete.It is strongly recommended to let it
complete.
WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!
CHKDSK is repairing sector 3192 of 4688 (68%)
Shawn M, Meghan T, Justin
Michael Jesus Sanchez Quispe
RU :94530


Shawn M, Meghan T, Justin
Michael Jesus Sanchez Quispe
RU :94530





Y observamos que el resultado es el mismo la encriptación de la información del usuario.

o ¿Se ejecutó correctamente el ransomware en Windows 10?

si se ejecuto como en el anterior sistema operativo solo que tardo mas e intento parar el sistema

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

Ninguna protección impidió la encriptación de los datos ni siquiera siendo una versión mas avanzada del sistema operativo

o ¿Hubo diferencias notables en comparación con Windows 7?

Windows 10, al estar más actualizado y con más medidas de seguridad activadas por defecto, puede detectar o bloquear parcialmente la ejecución del ransomware. Windows 7 es mucho más vulnerable.

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

Ejecutarlo como administrador facilita al ransomware tomar el control total del sistema , haciendo mucho más efectivo el cifrado del disco y bloqueando por completo el acceso al equipo y afectándolo mas