
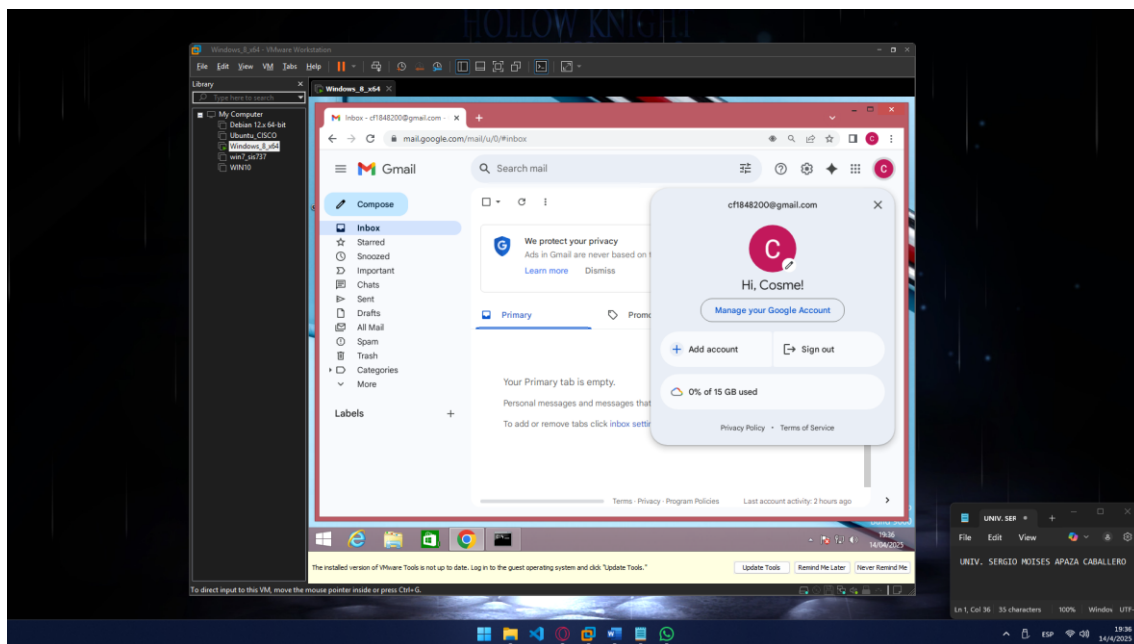
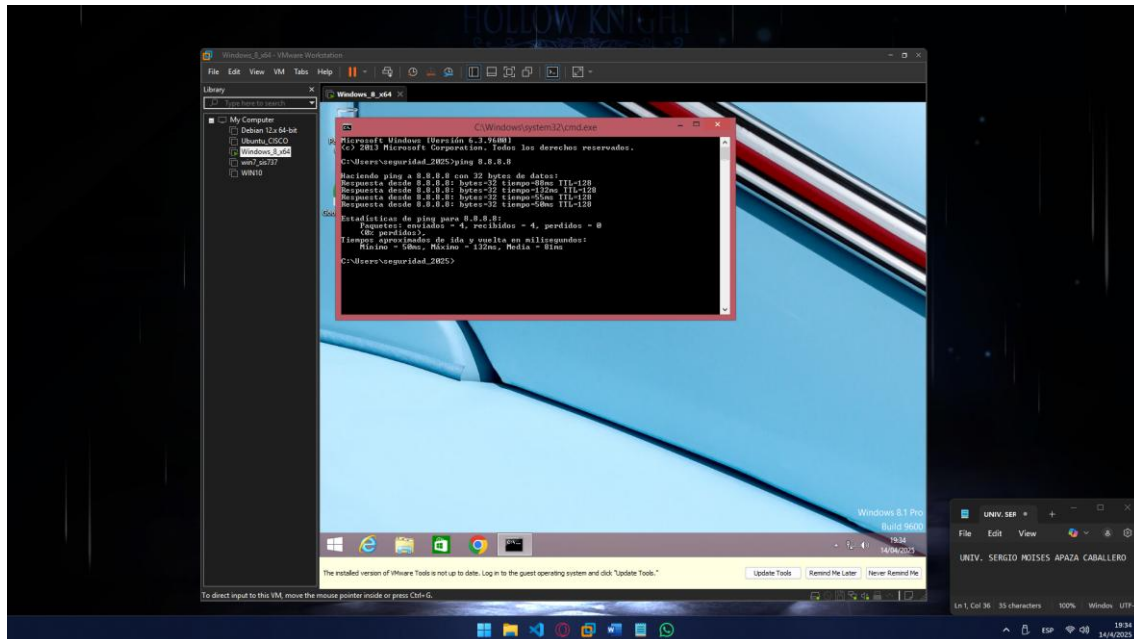
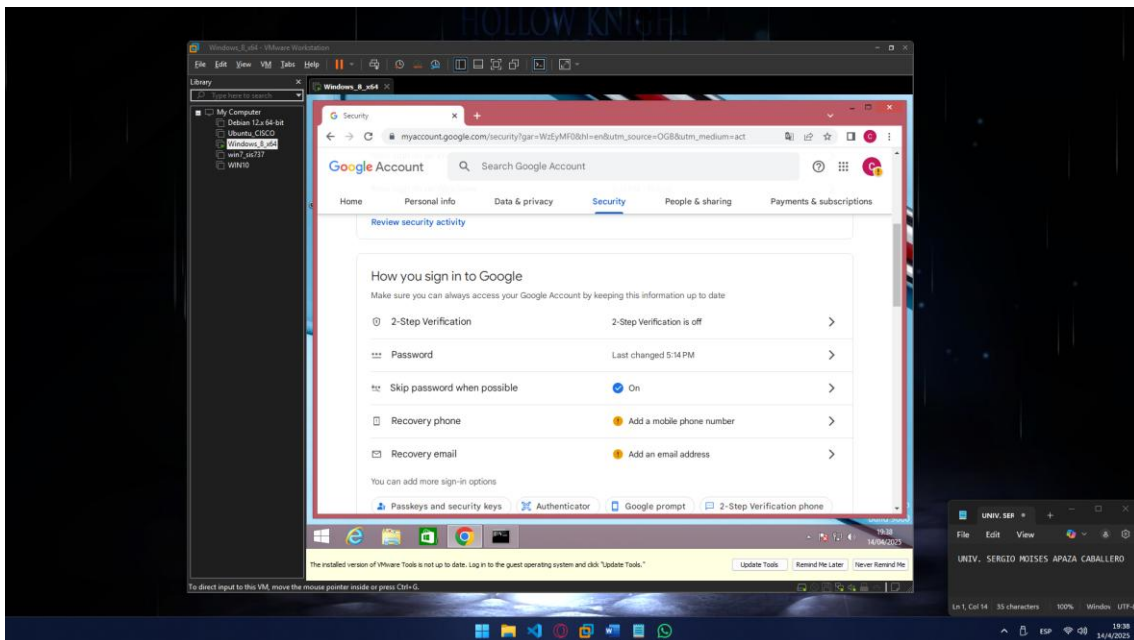
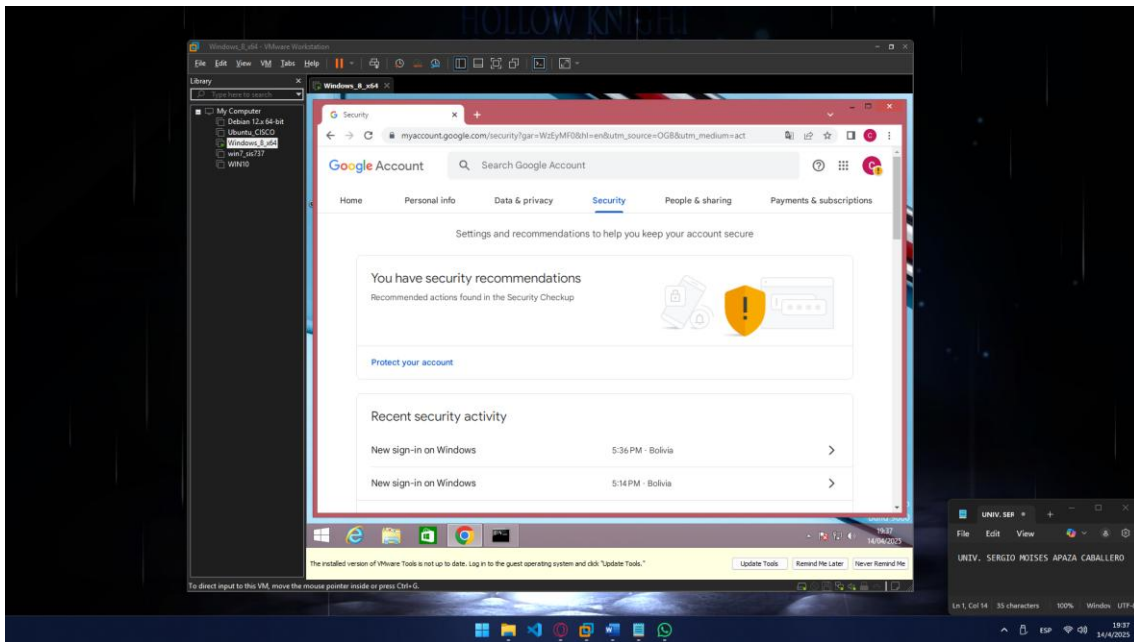


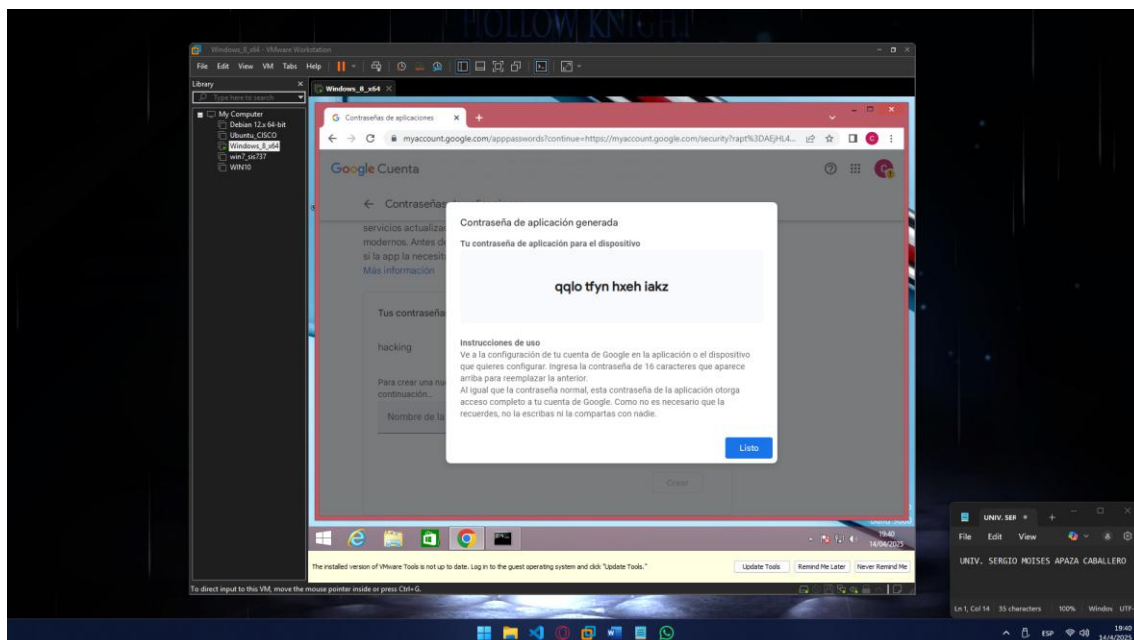
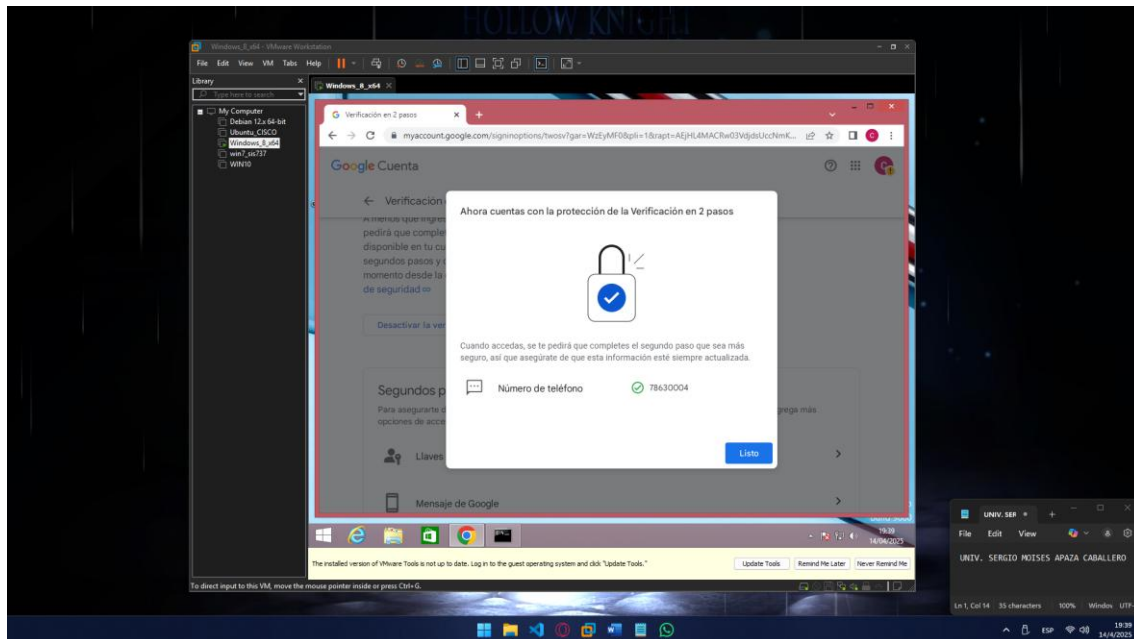
UNIVERSIDAD AUTÓNOMA “TOMAS FRÍAS” CARRERA DE INGENIERÍA DE SISTEMAS				
Materia:	Seguridad de sistemas (SIS-737)			
Docente:	M. Sc. Ing. Javier Alexander Duran Miranda			N Práctica 1
Auxiliar:	Univ. Aldrin Roger Perez Miranda			
Estudiante:	Univ. Sergio Moises Apaza Caballero			
29/03/2025	Fecha publicación			
12/04/2025	Fecha de entrega			
Grupo:	1	Sede:	Potosí	

PARTE 1

Modificar parámetros del correo:



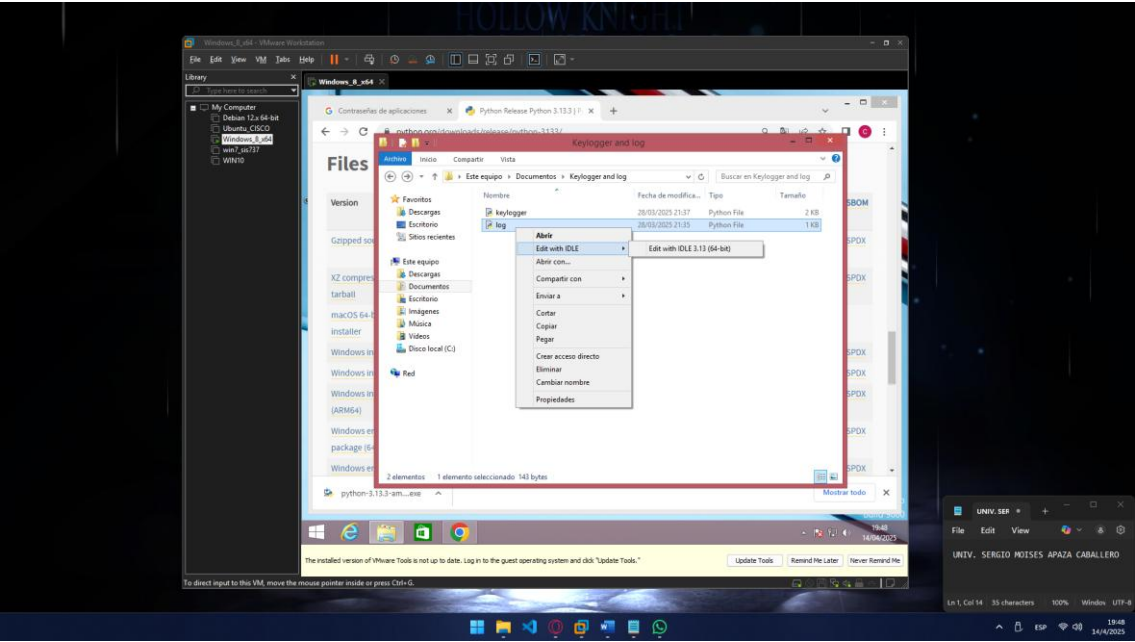
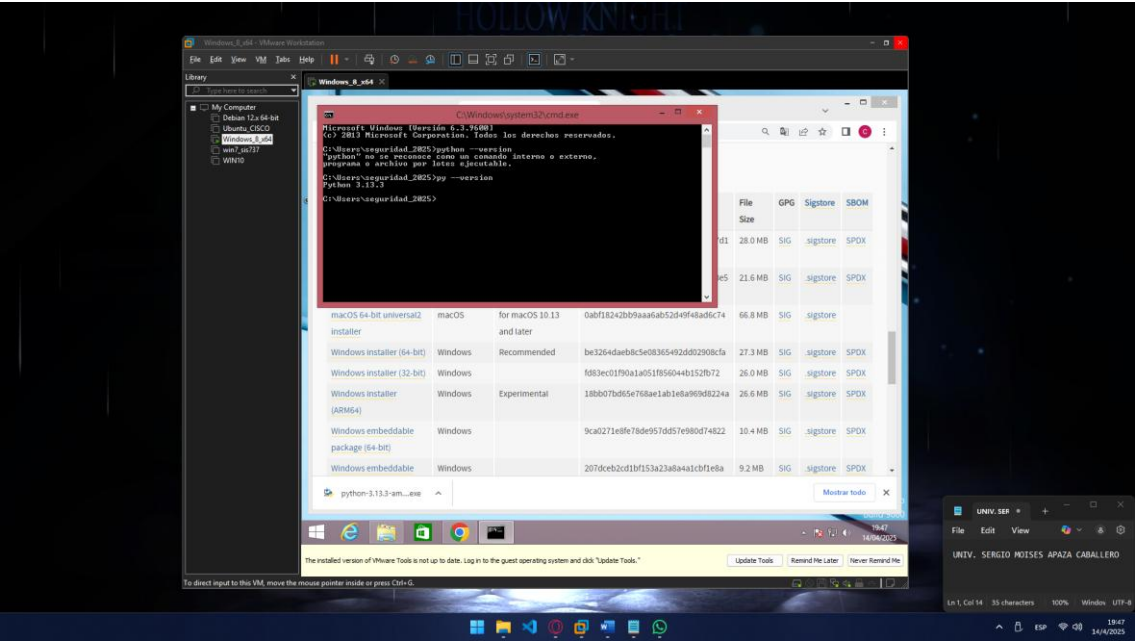


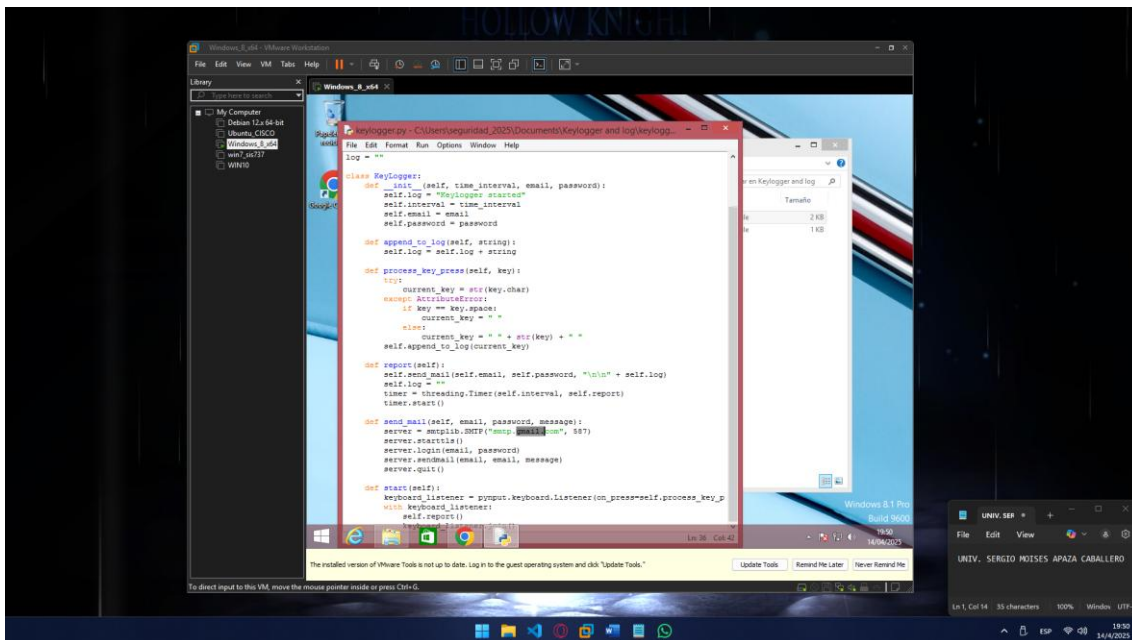
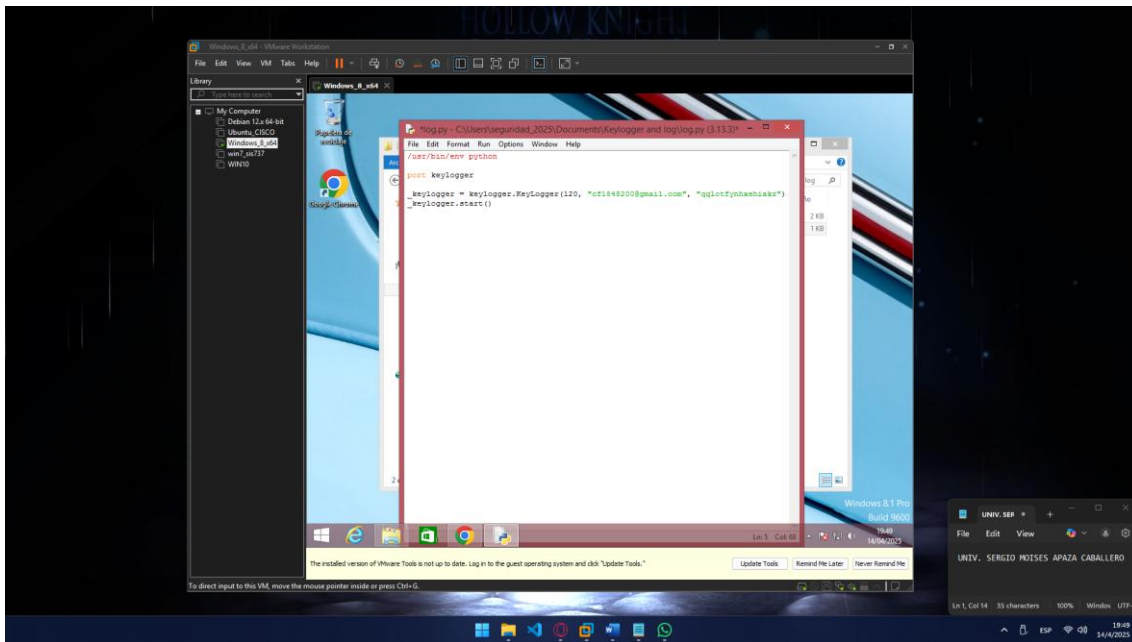


(No le saqué captura, pero si cree con el nombre de hacking)

password: qqlo tfyn hxeh iakz

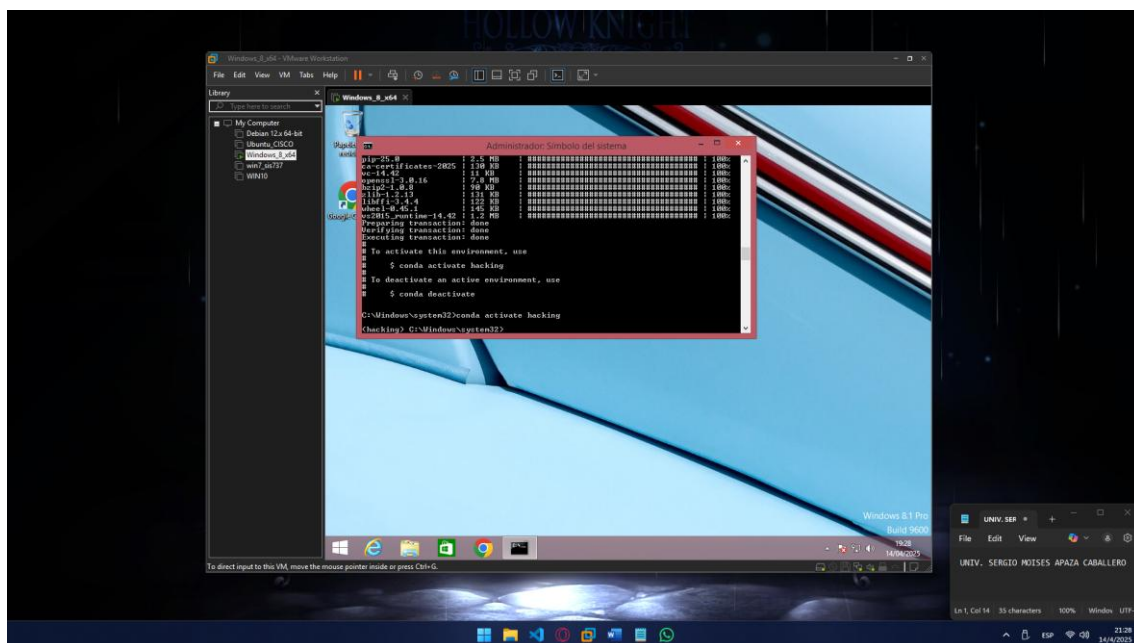
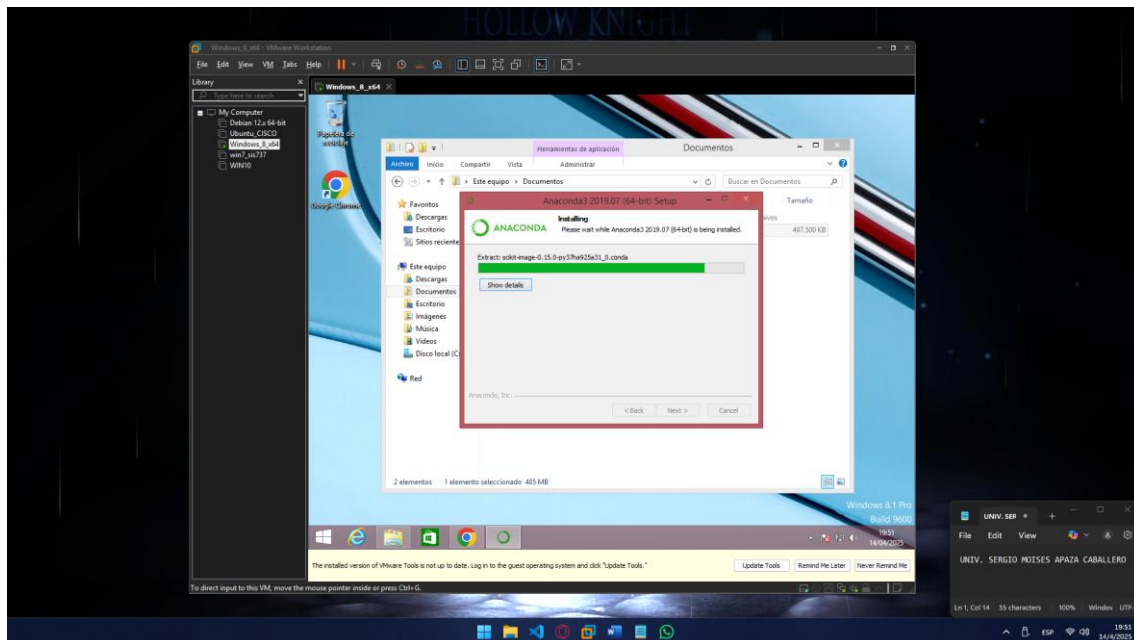
Actualizar los parámetros:

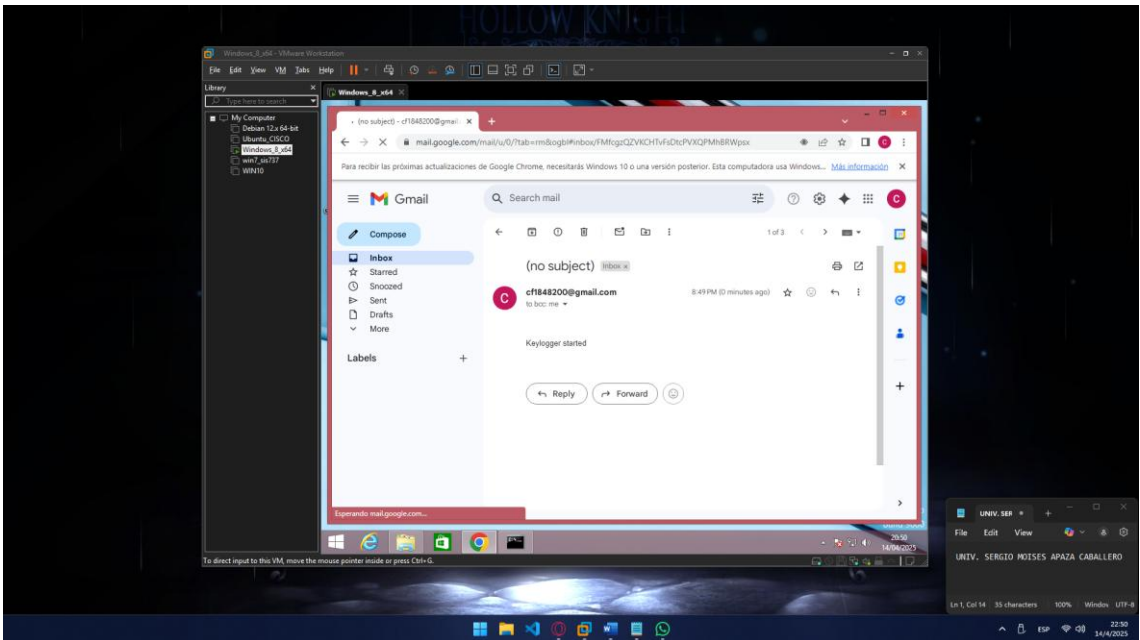
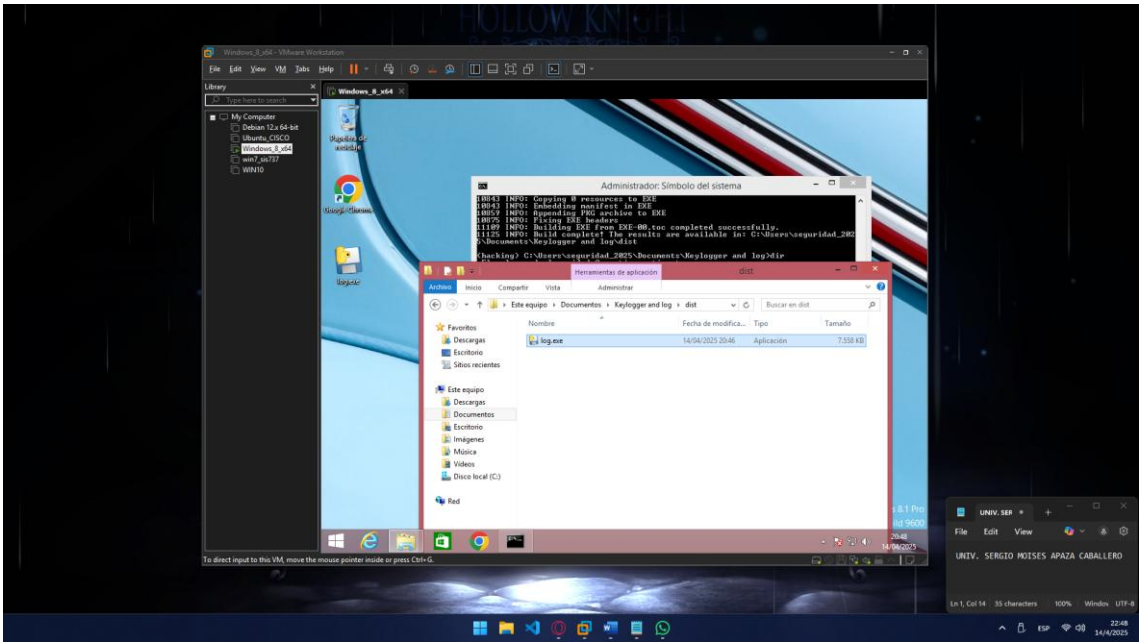




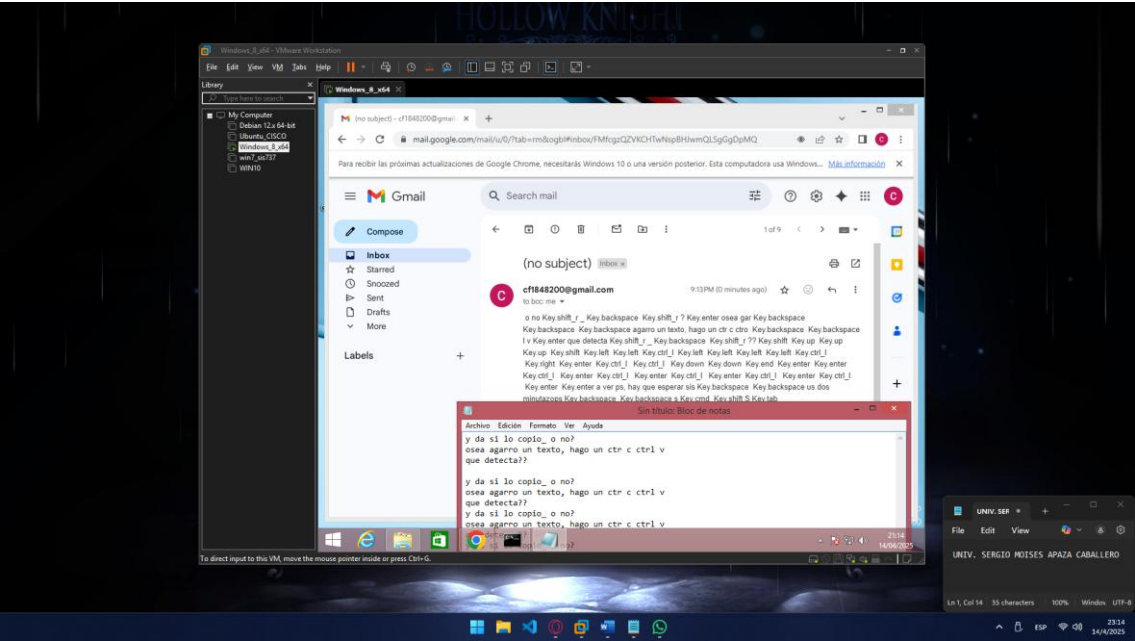
Empaquetamos el archivo ejecutable:

Se instala Anaconda3



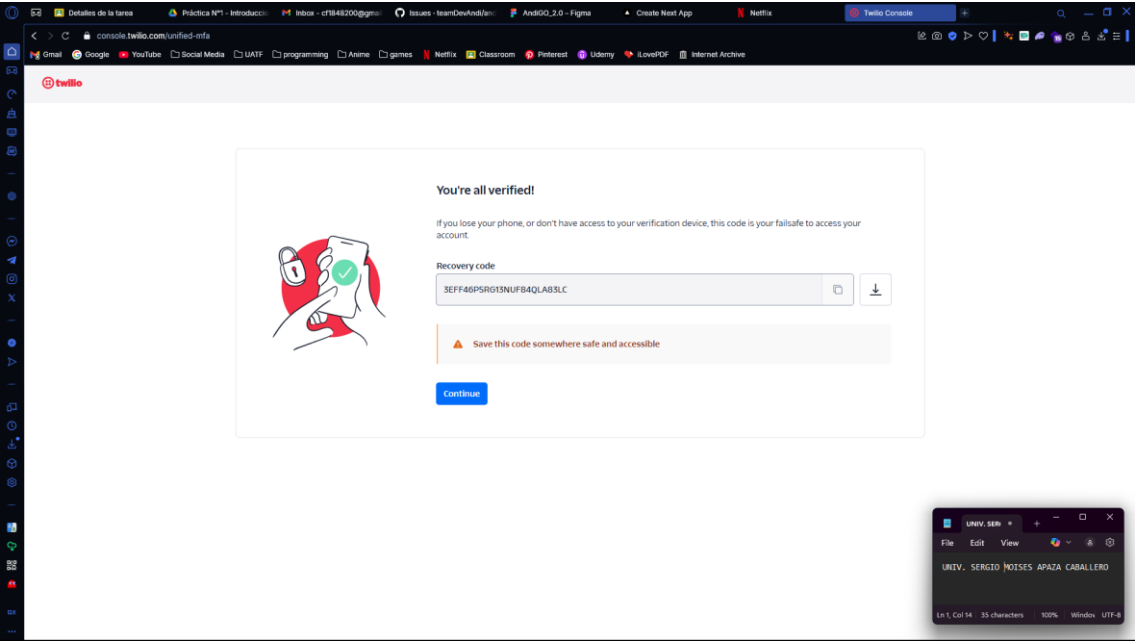


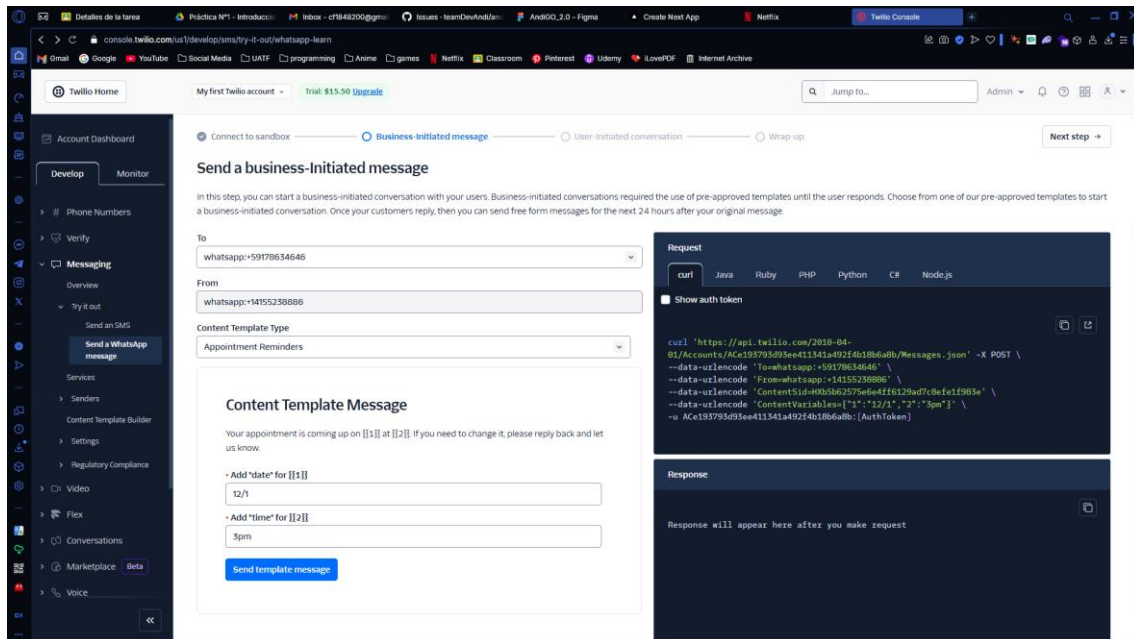
RESULTADO



EVALUACIÓN 1

1) Registrarse en Twilio para obtener credenciales y un número emisor.

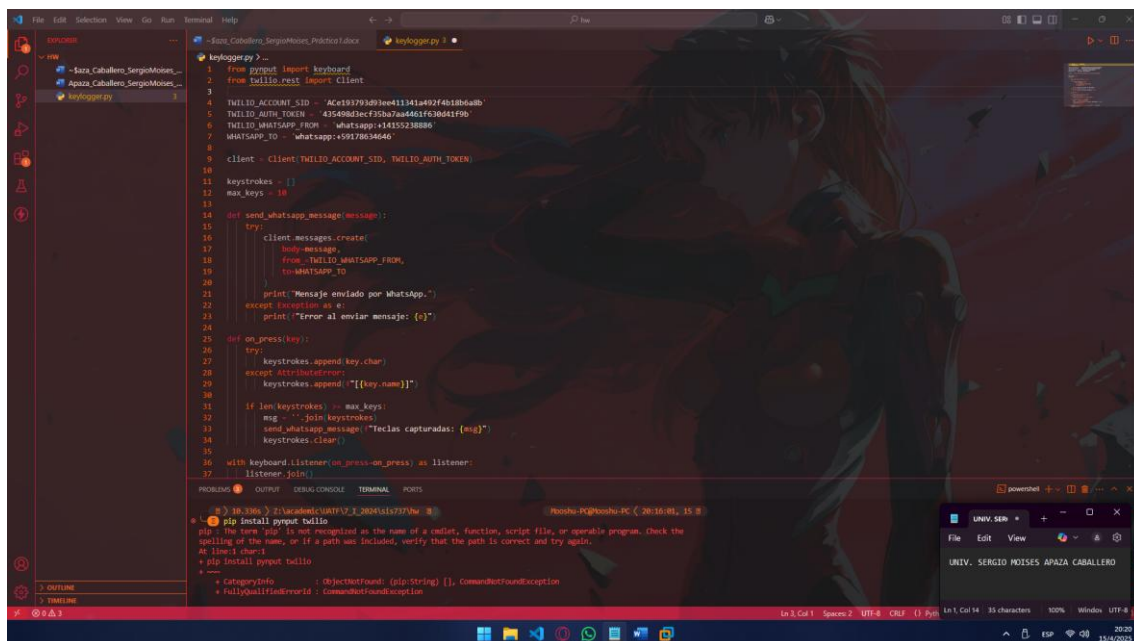




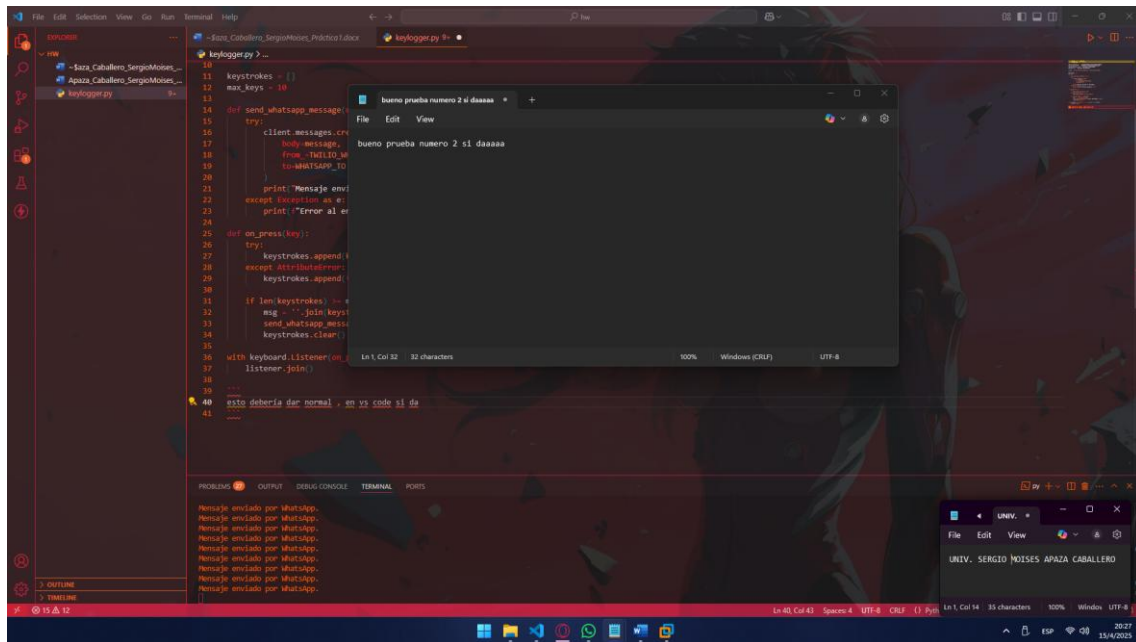
2) Integrar el módulo pynput para capturar teclas y twilio para enviar los datos.

3) Configurar el envío automático cada cierto número de pulsaciones (ej: cada 10 teclas).

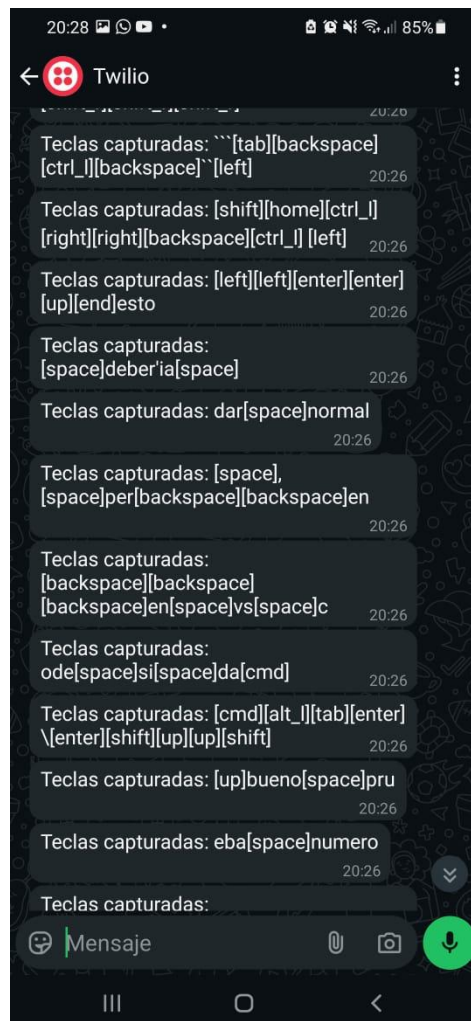
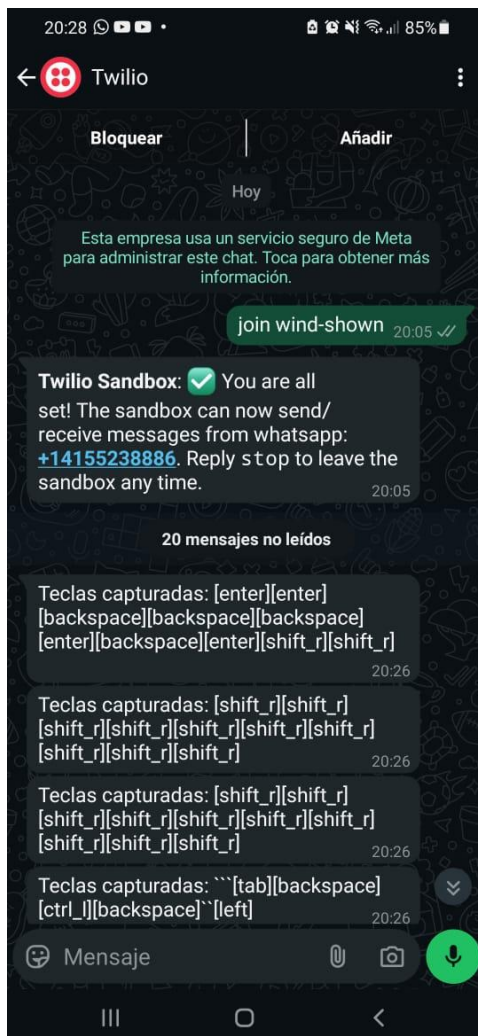
(Ambos incisos están resueltos en el código, por tanto respondo ambos con la misma captura de pantalla)



4) Probar el script en un entorno controlado (nunca en dispositivos ajenos sin consentimiento).



Resultados en whatsapp



20:28

85%

← Twilio

[space][per][backspace][backspace]en

20:26

Teclas capturadas:
[backspace][backspace]
[backspace]en[space]vs[space]c

20:26

Teclas capturadas:
ode[space]si[space]da[cmd]

20:26

Teclas capturadas: [cmd][alt_][tab][enter]
\[enter][shift][up][up][shift]

20:26

Teclas capturadas: [up]bueno[space]pru

20:26

Teclas capturadas: eba[space]numero

20:26

Teclas capturadas:
[space]2[space]si[space]daaa

20:26

Teclas capturadas: aa[print_screen][alt_]
[tab][alt_][tab][ctrl_] [ctrl_]

20:27

Teclas capturadas: [enter][up][down][left]
[left][enter][caps_lock]r[caps_lock]e

20:27

Teclas capturadas: sultados[space]e

20:27

Teclas capturadas: n[space]whatsapp

20:27

Teclas capturadas: [shift][home][ctrl_]
[ctrl_][ctrl_][ctrl_][ctrl_][ctrl_][ctrl_]
[ctrl_]

20:27

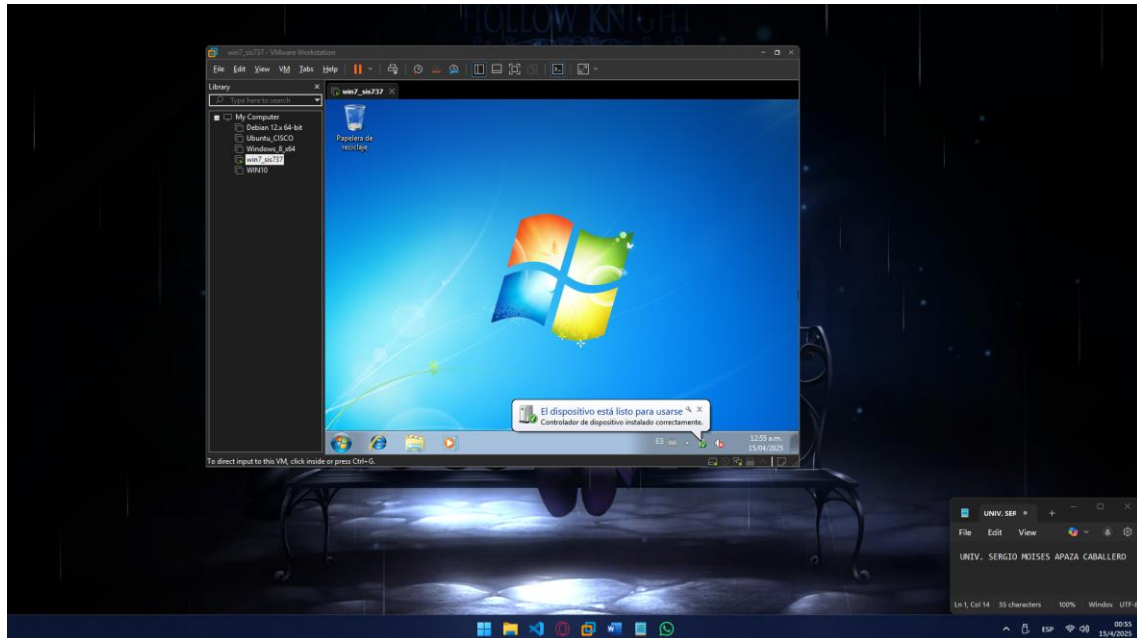
Mensaje



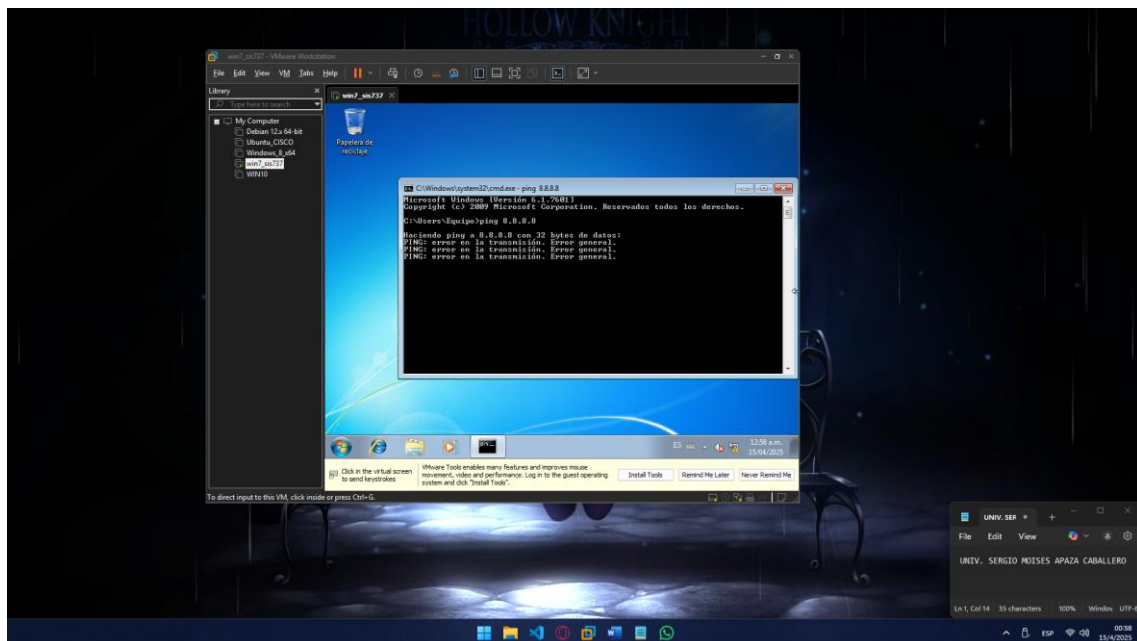
PARTE 2

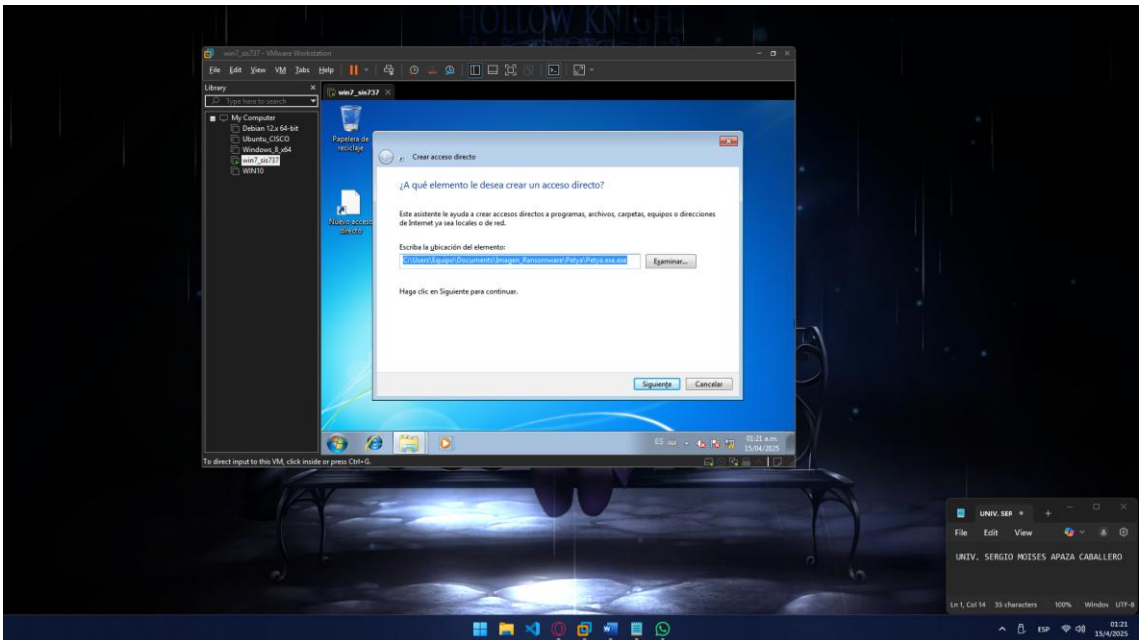
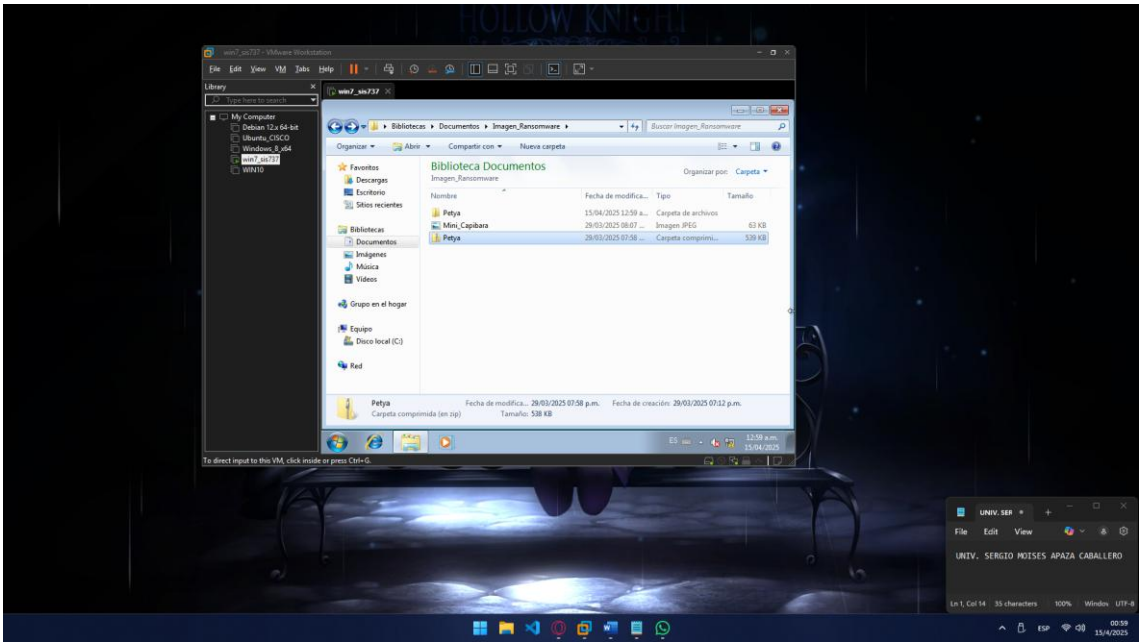
Camuflaje de Malware (Windows 7):

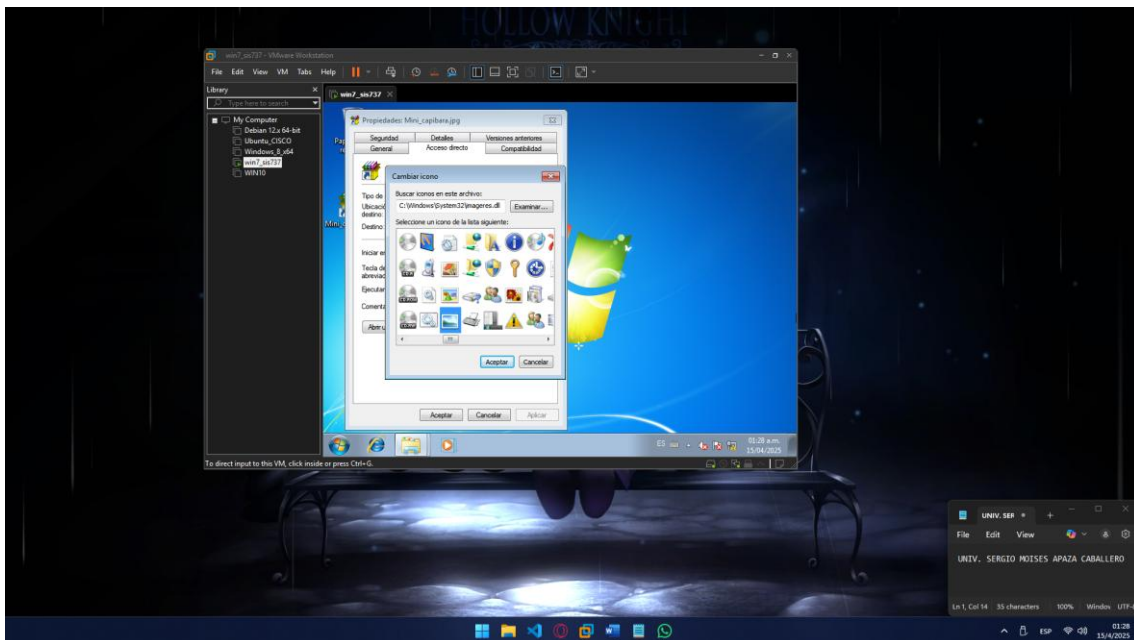
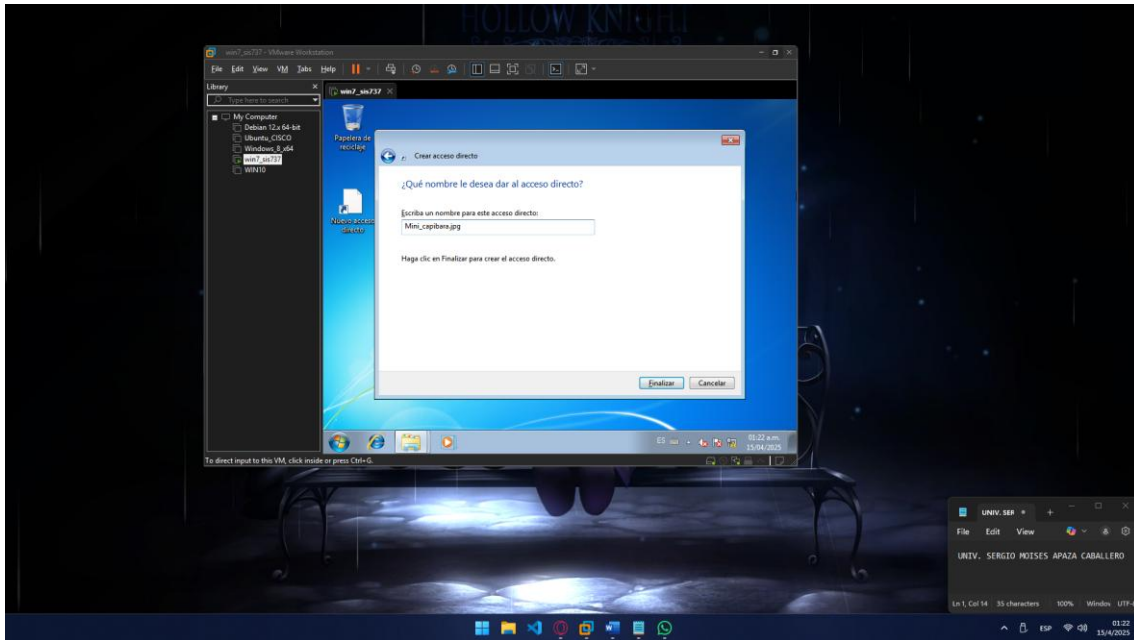
Empezamos

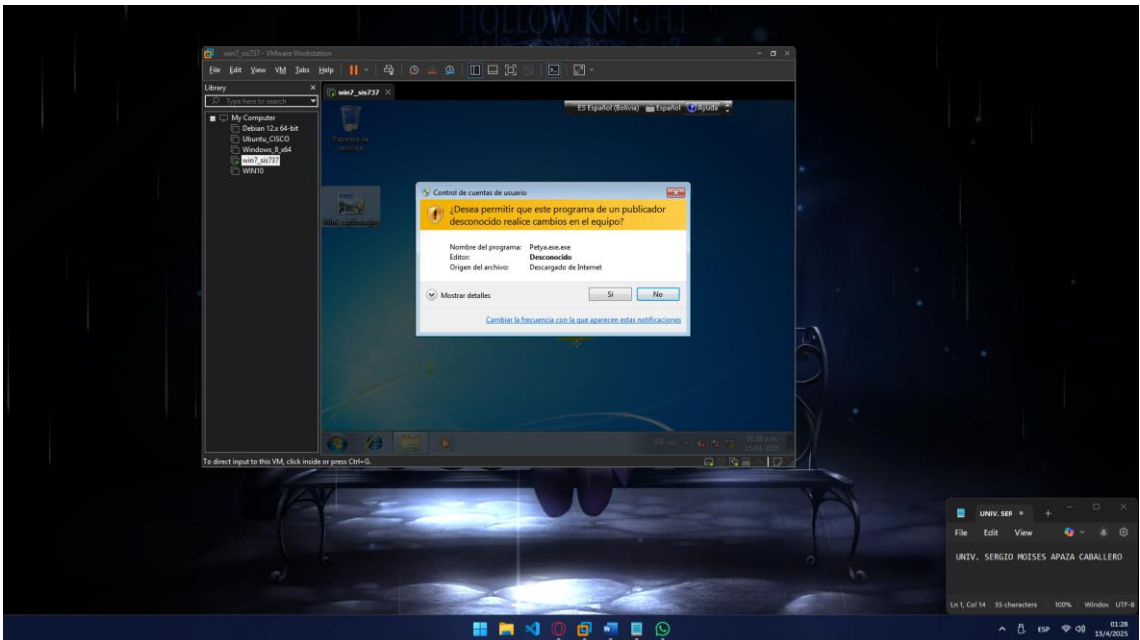
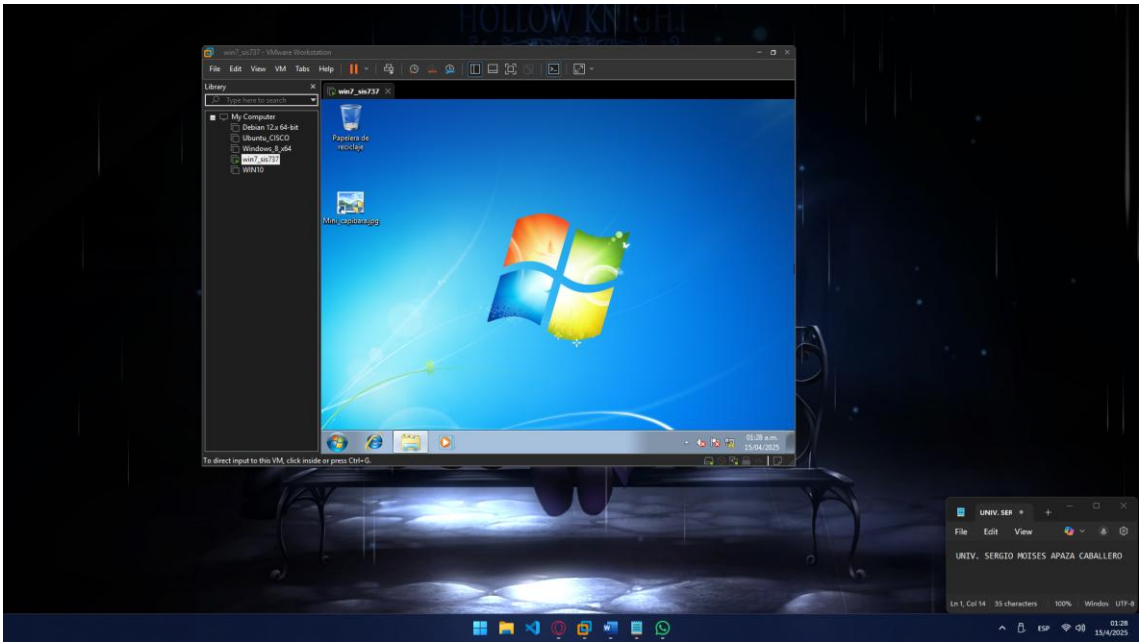


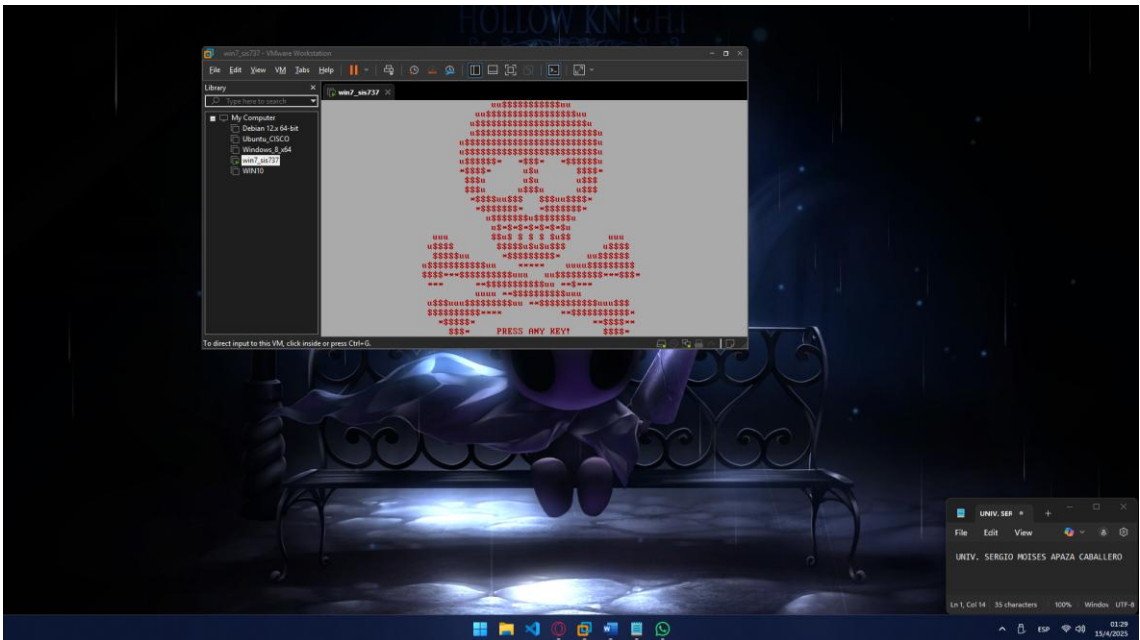
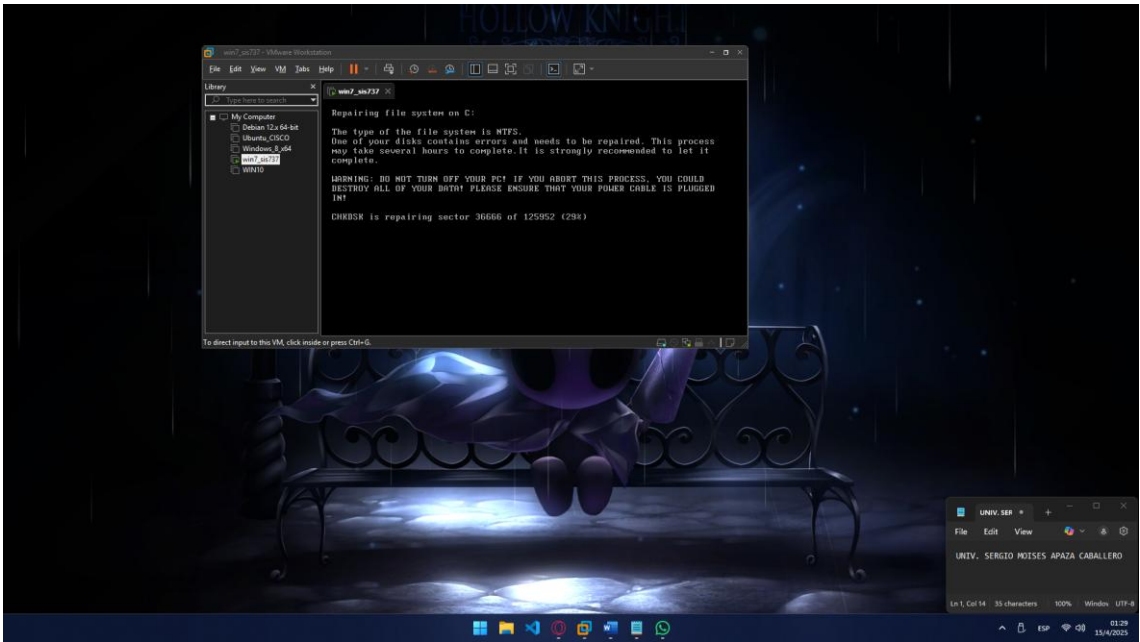
Sin conexión a internet



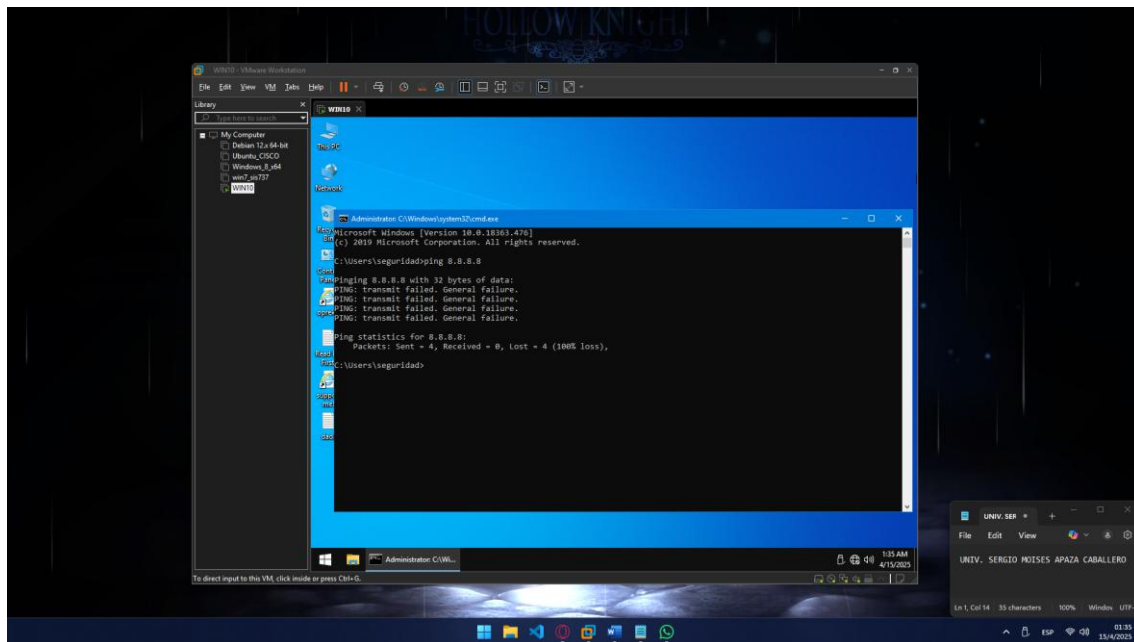




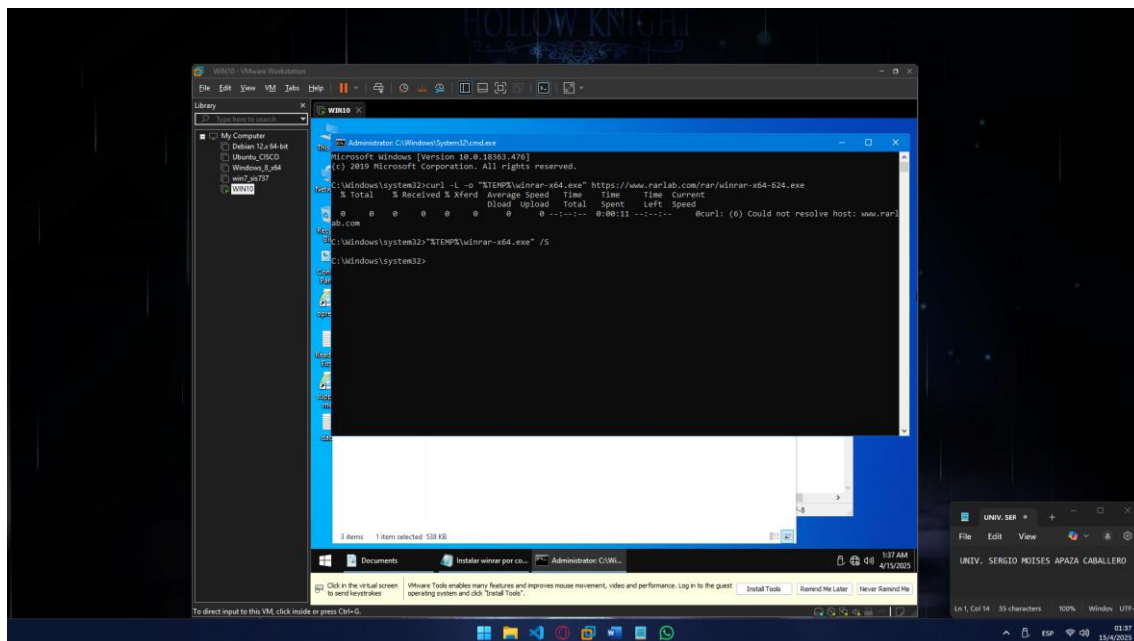


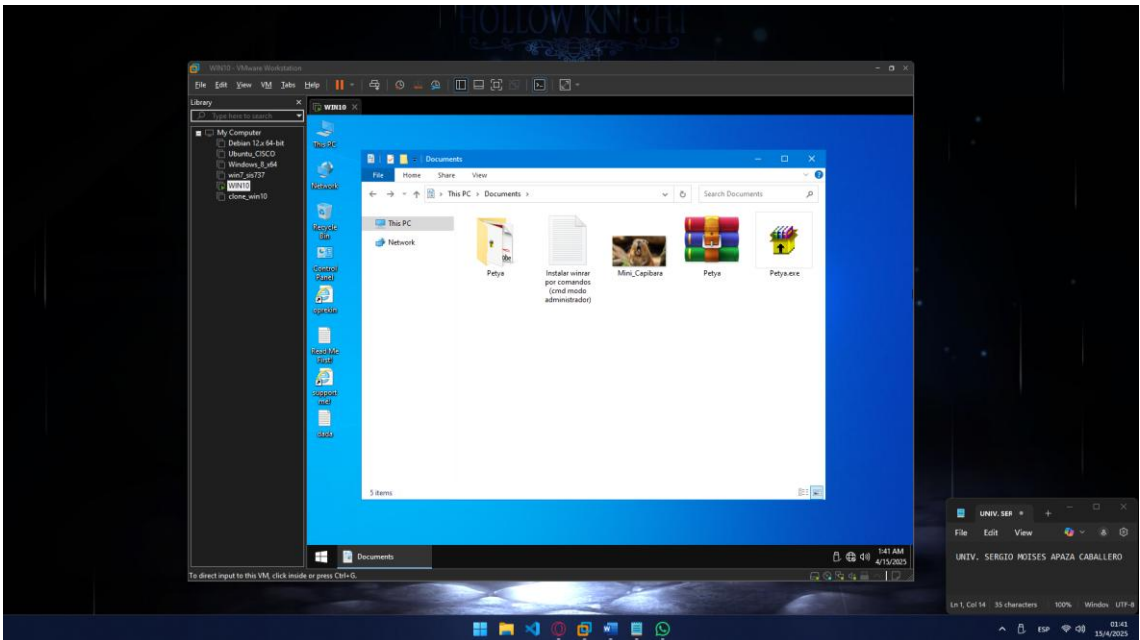
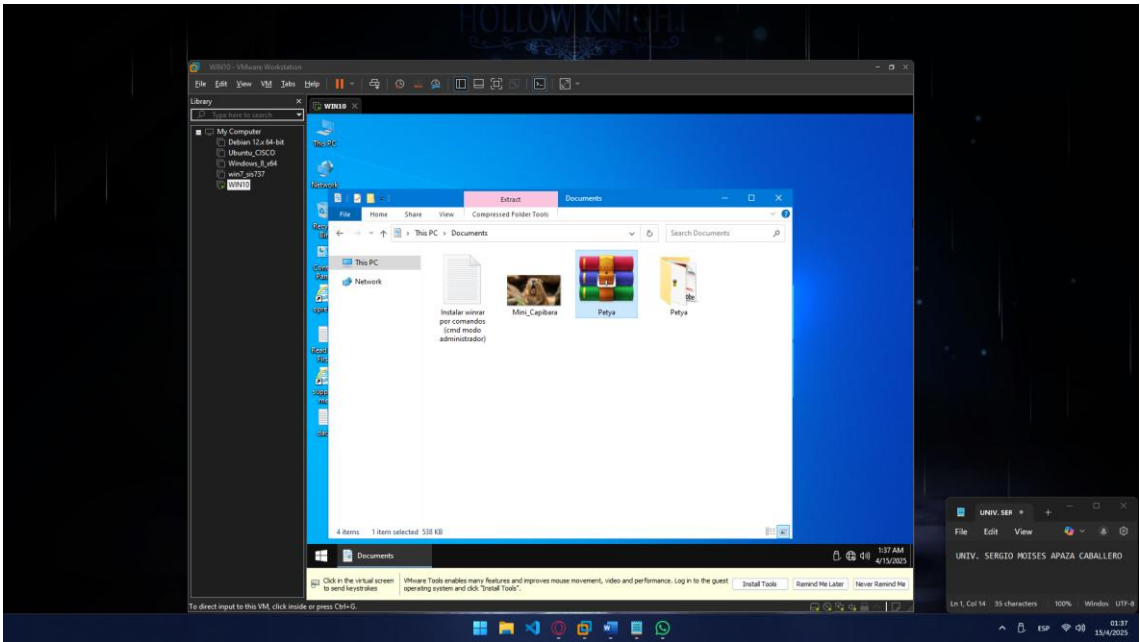


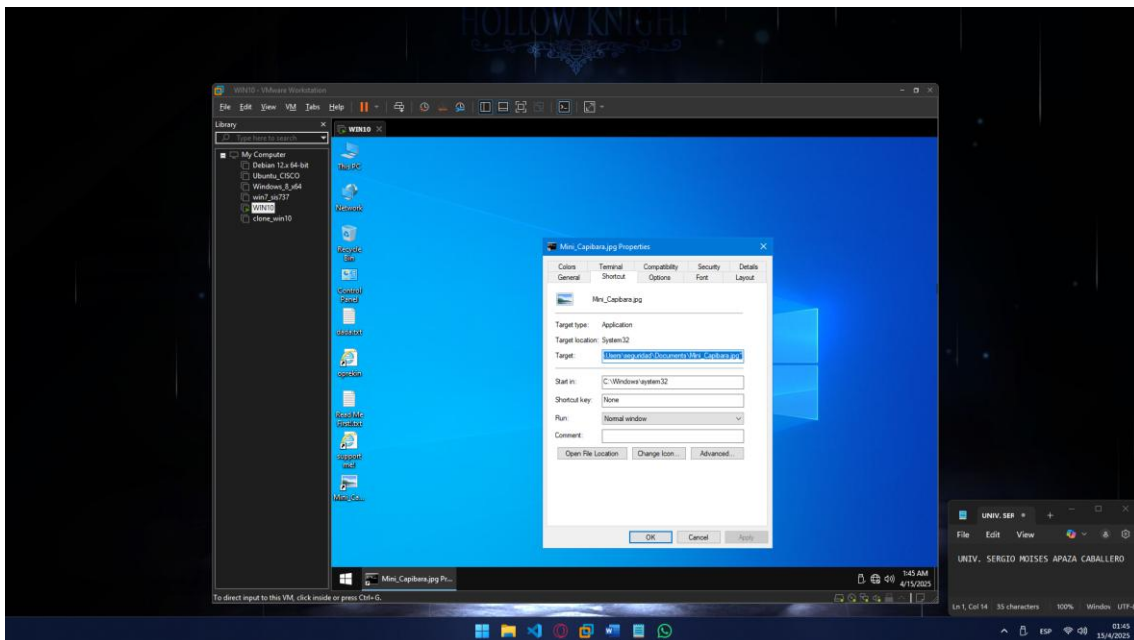
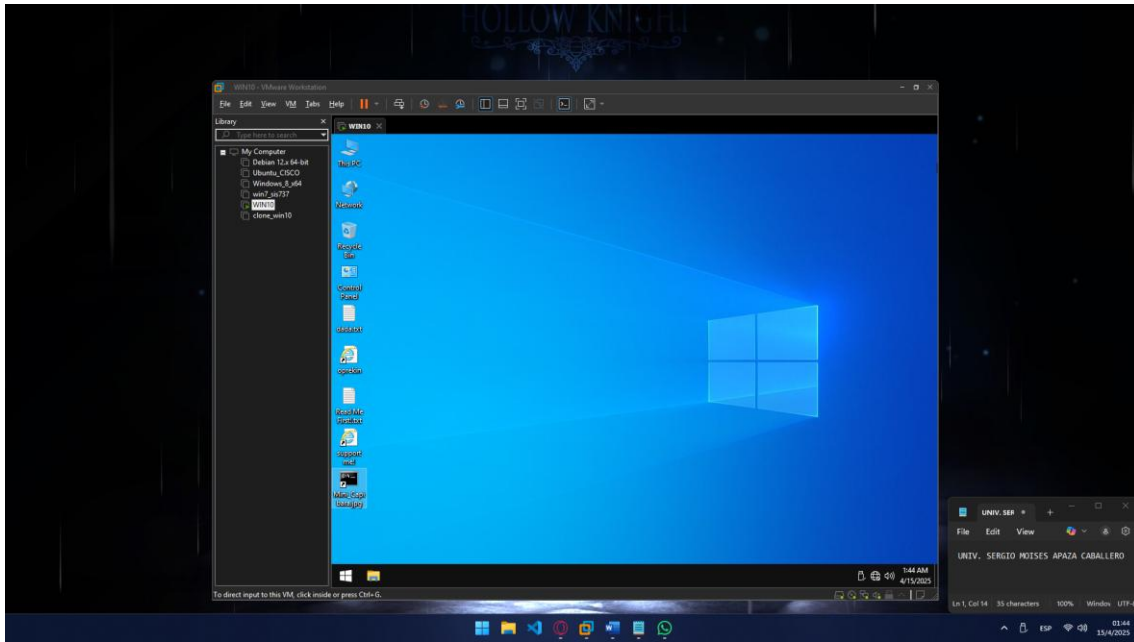
En efecto, no tiene conexión a internet

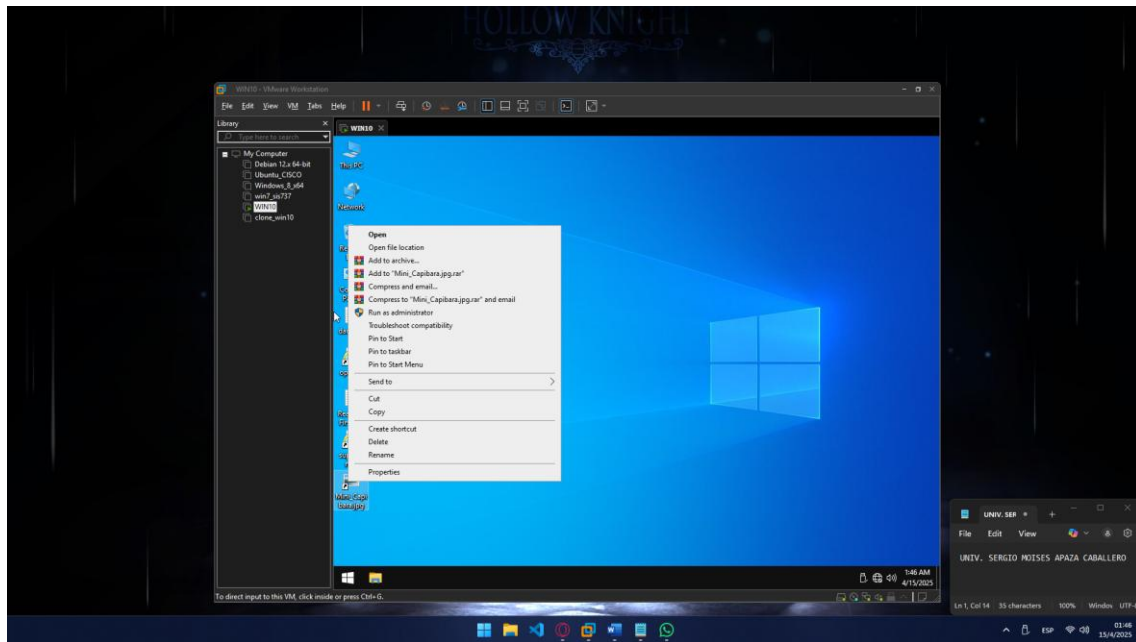


Instalamos winrar mediante comandos (cmd como administrador)

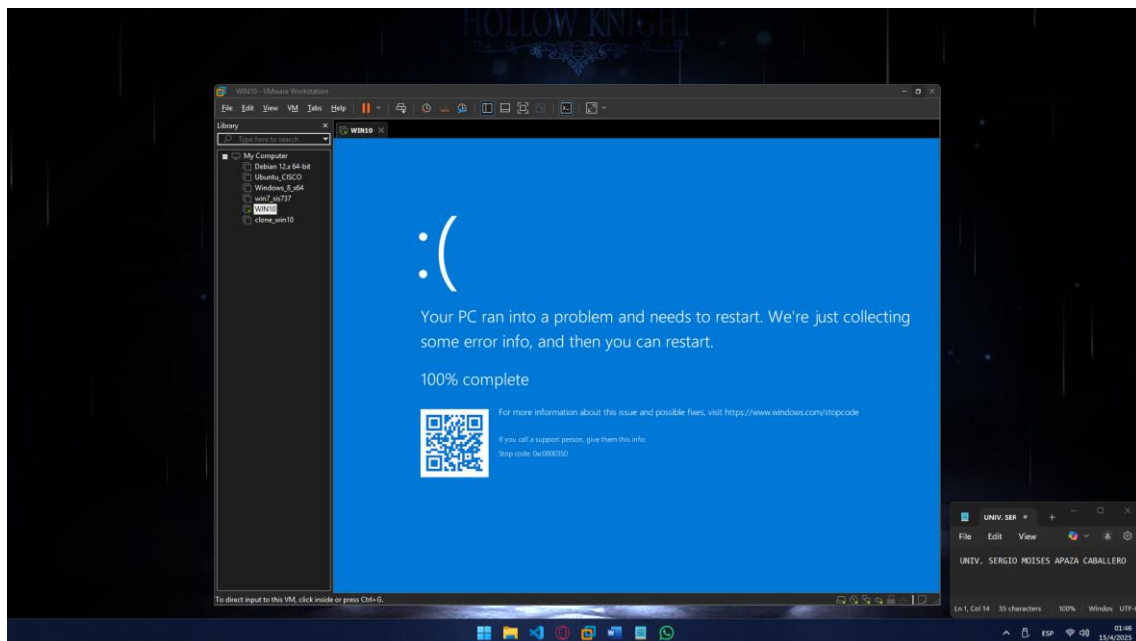




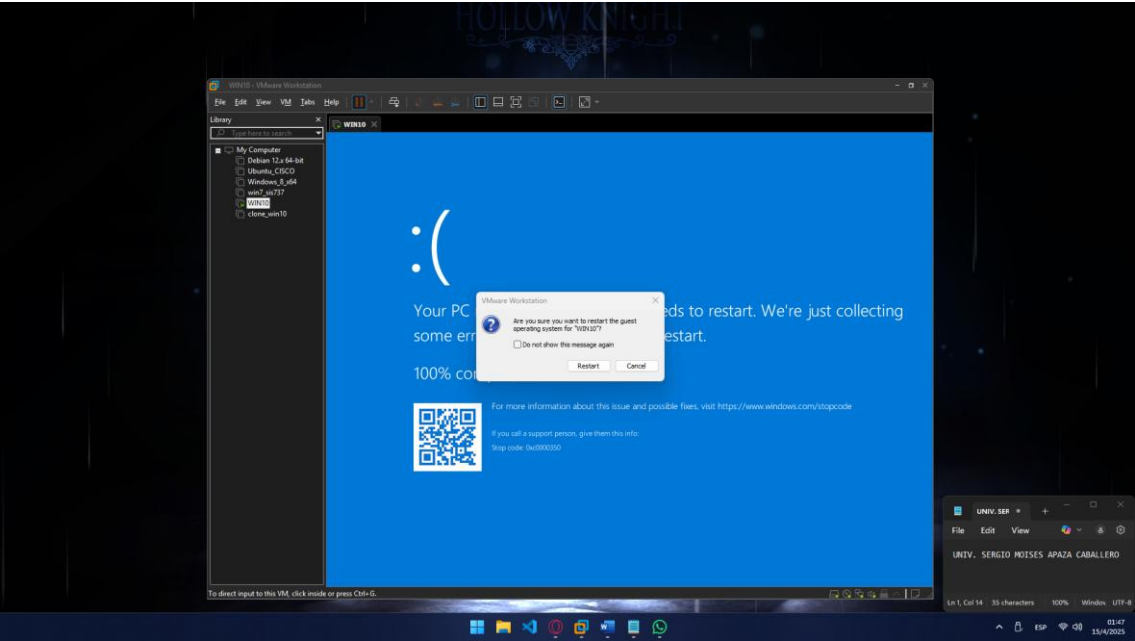




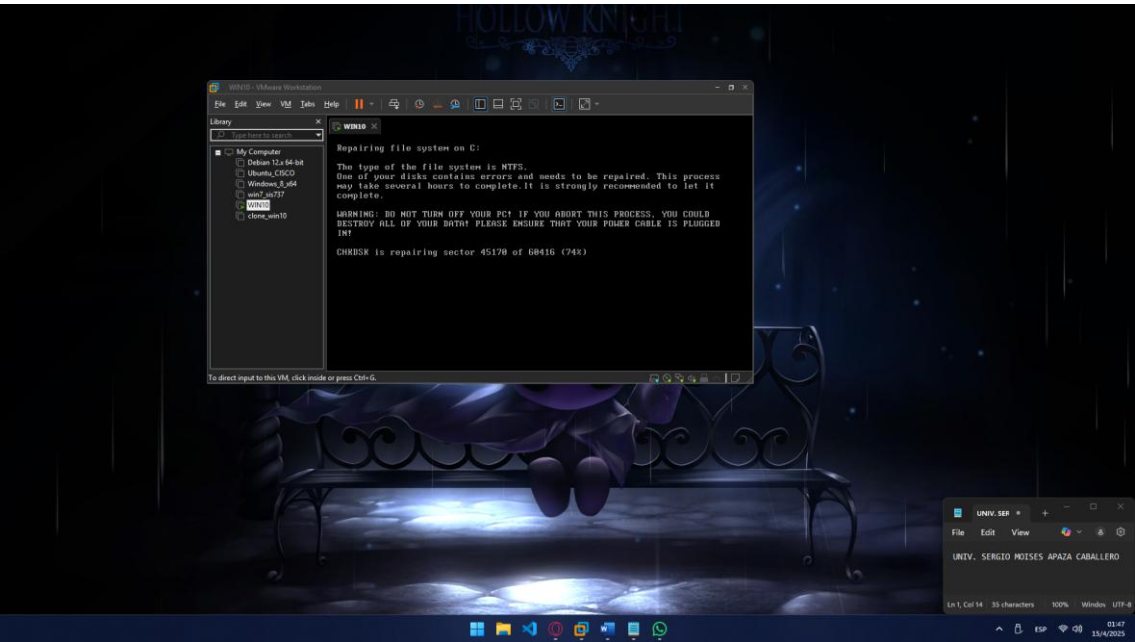
Pantalla azul de la muerte :(



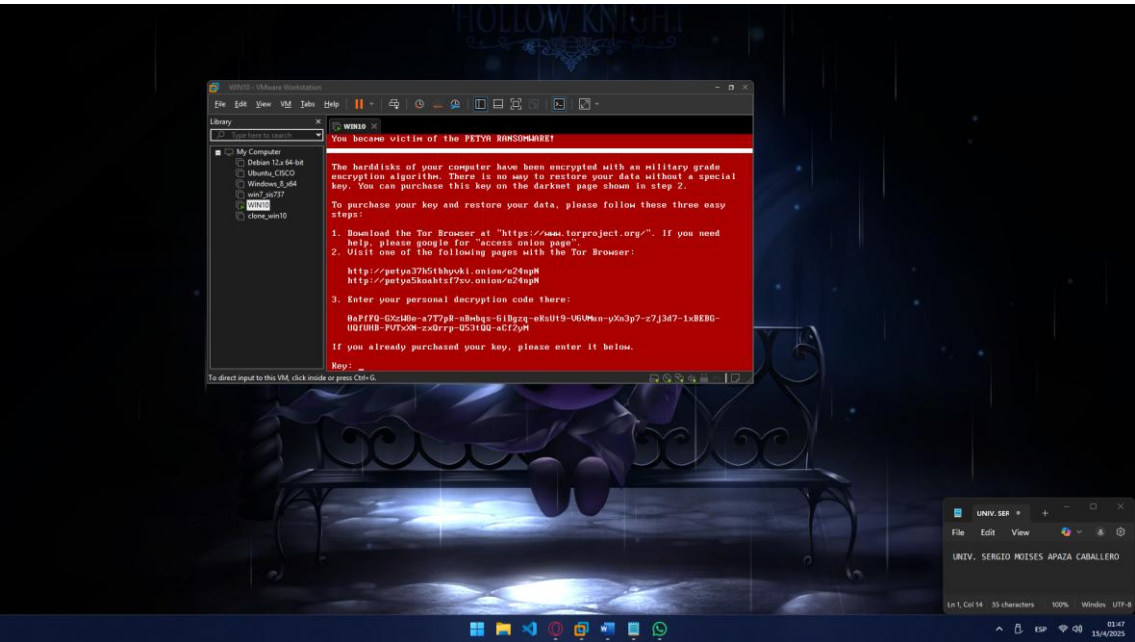
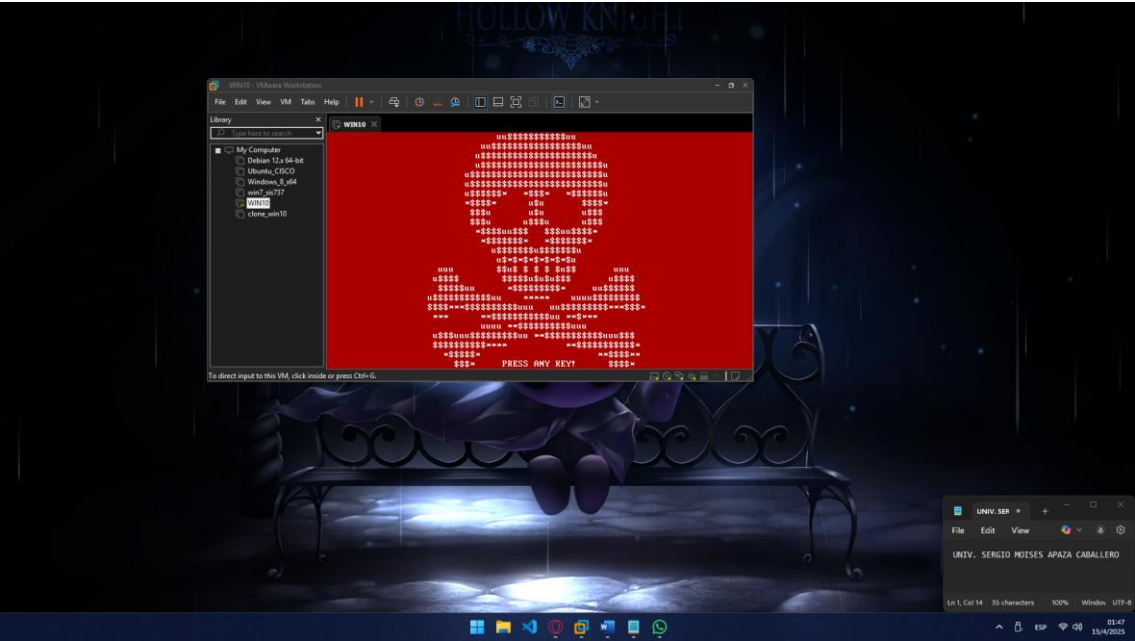
Reiniciamos



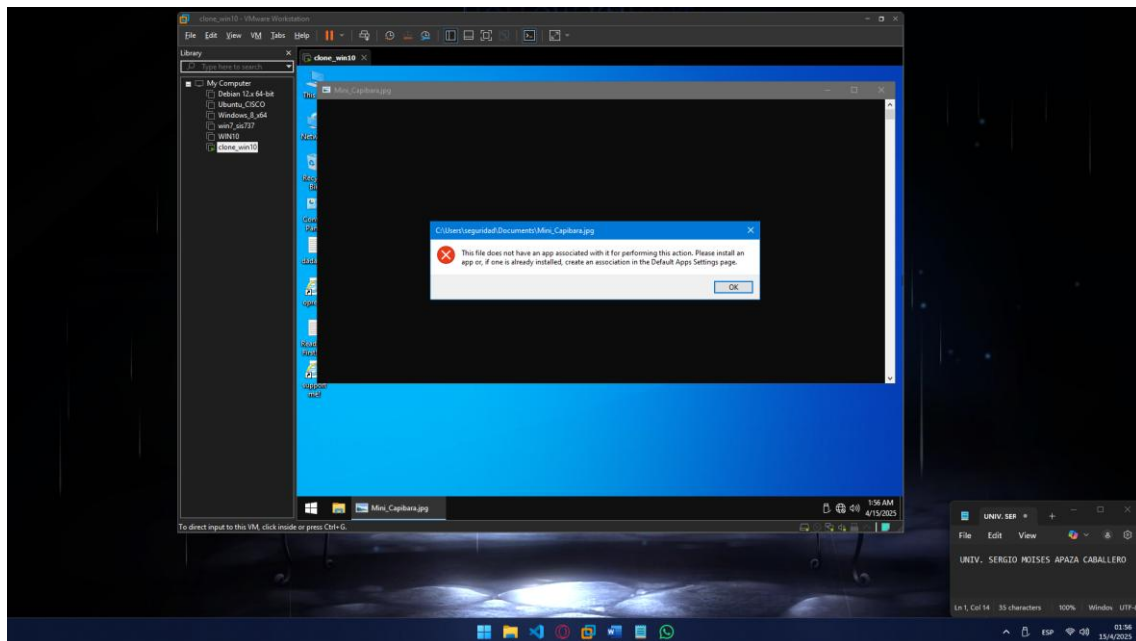
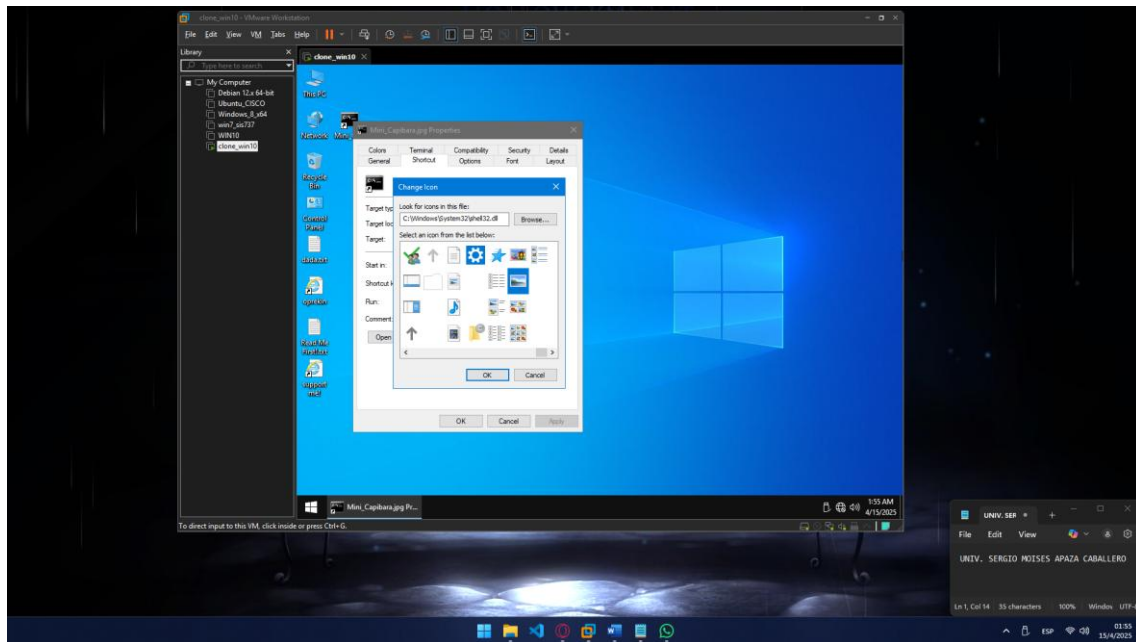
Intenta reparar...

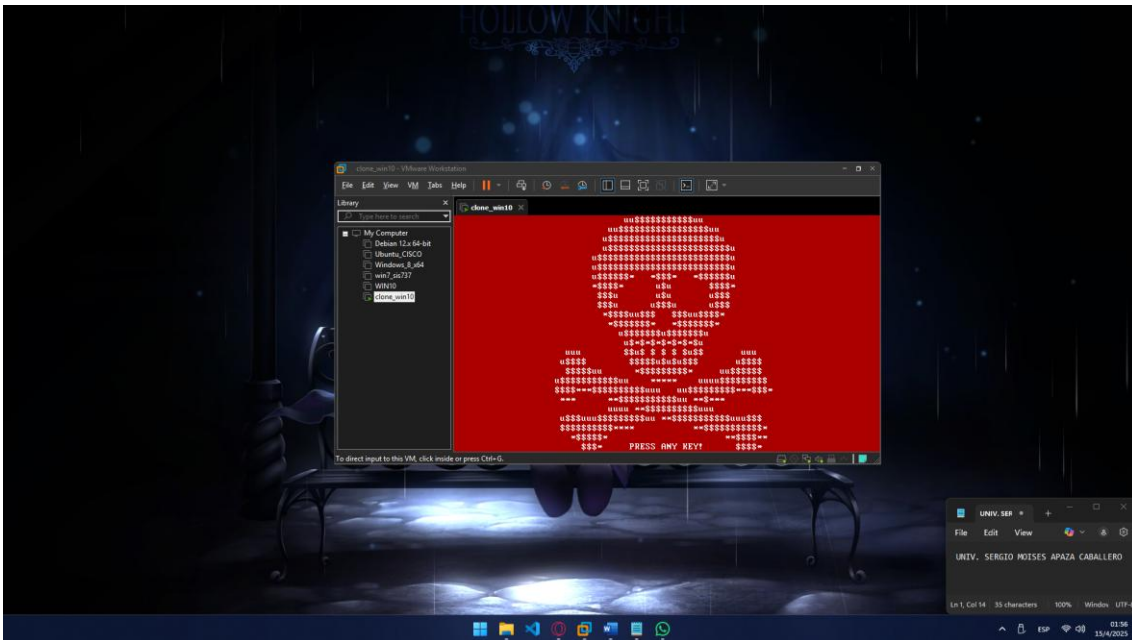
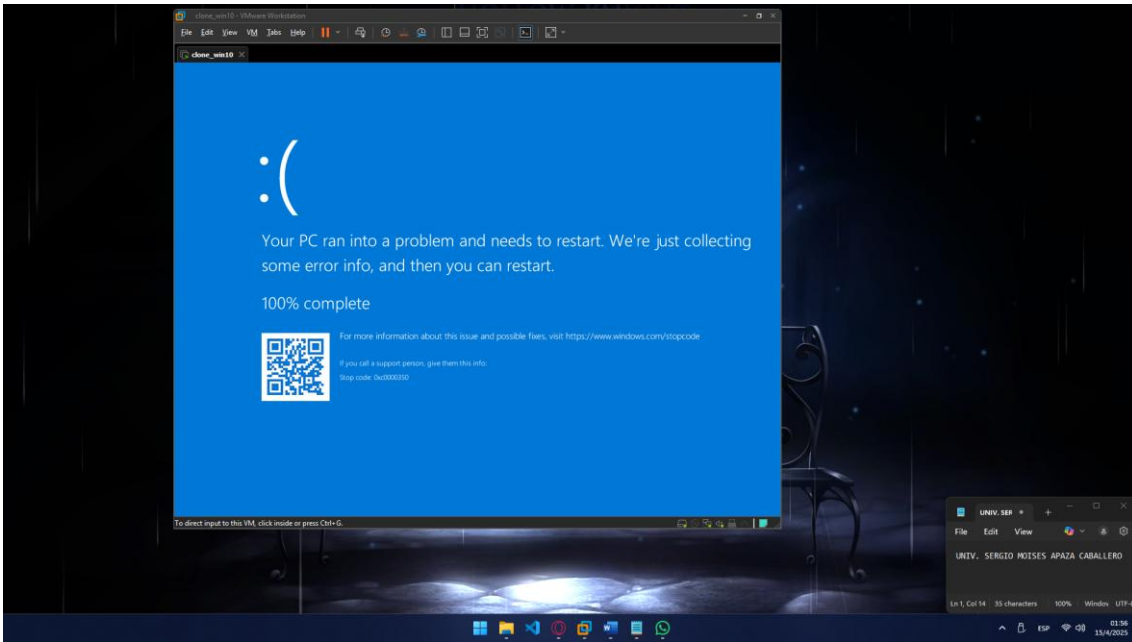


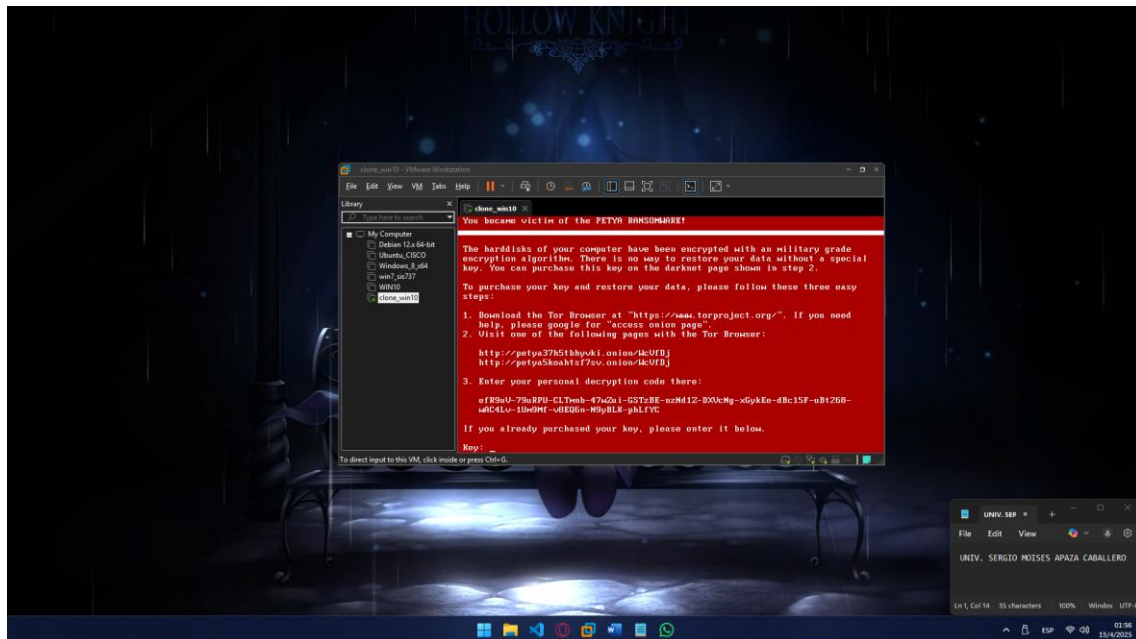
Pero no lo logra



Igualmente, quise comprobar el sistema como tal con petya2 (igualmente venía ese archivo) y seguí los mismos pasos, pero con petya 2 (esto en una VM que cloné antes de infectarla).







El resultado es el mismo, solo cambia el ID de encriptación

1. ¿Se ejecutó correctamente el ransomware en Windows 10?

Si, sin problemas; solo tuvo que cambiarse el directorio al crear el acceso directo, pues no era exactamente el mismo.

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

La pantalla azul, tratando de recolectar información, para después permitirme reiniciar. Como tal, no hubo ningún sistema de protección activa que me advirtiera respecto al peligro de este ransomware.

3. ¿Hubo diferencias notables en comparación con Windows 7?

Simplemente la pantalla azul que apareció al ejecutar el ransomware.

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

Se le da permisos de administrador, lo cual le da más privilegios y más accesos al sistema.