Laboratorio Análisis Estático de Malware

ReadMe: El presente documento describe una guía práctica para la implementación de un laboratorio de análisis estático de malware, orientado al análisis de archivos obtenidos durante investigaciones en foros clandestinos de la Deep Web y la Dark Web. Su objetivo es establecer un entorno seguro que permita verificar la presencia de indicadores de malware antes de descomprimir, abrir o analizar el contenido de los archivos descargados.

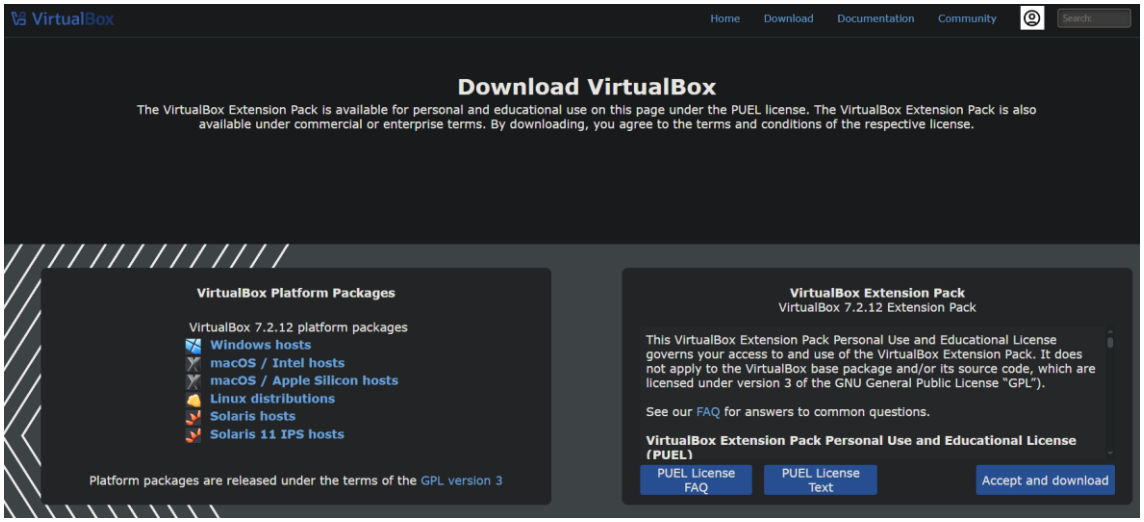
Crear laboratorio con VirtualBox

1) Instalar VirtualBox

Descargar: VirtualBox 7.x.x platform packages y VirtualBox 7.x.x Extension Pack

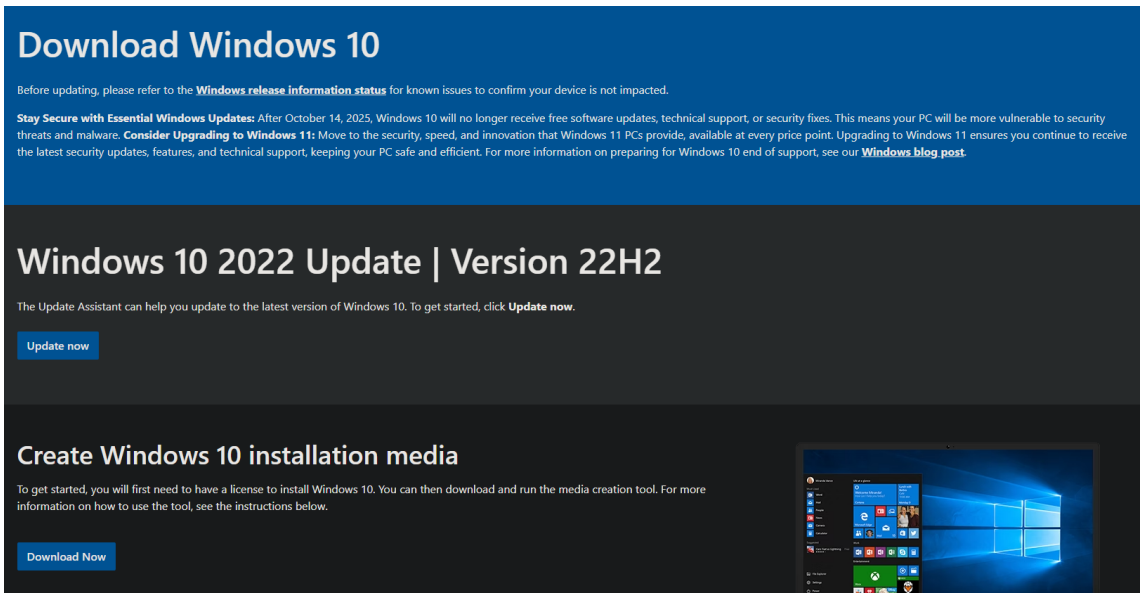
[LATEST]: https://www.virtualbox.org/wiki/Downloads

[VERSIONS]: https://www.virtualbox.org/wiki/Download_Old_Builds



2) Descargar ISO Windows 10

[SOURCE]: https://www.microsoft.com/en-us/software-download/windows10

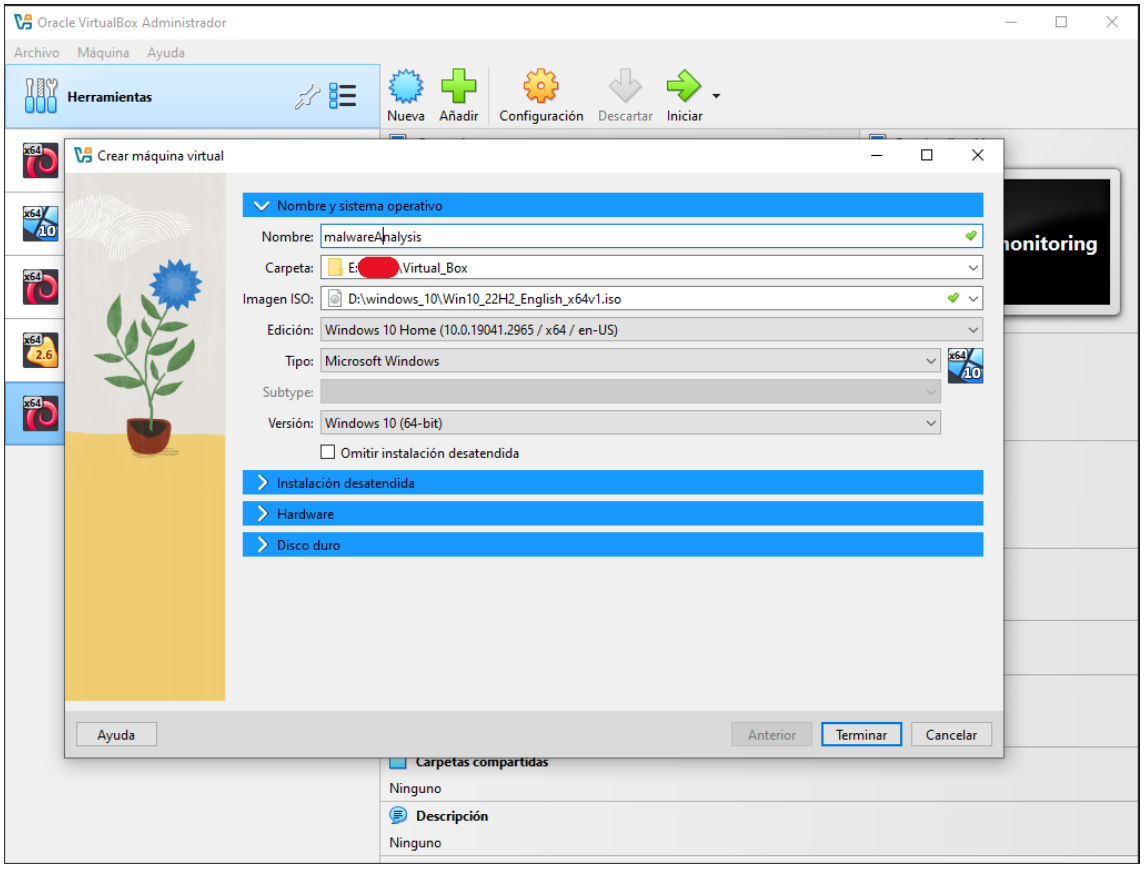


3) Crear VM

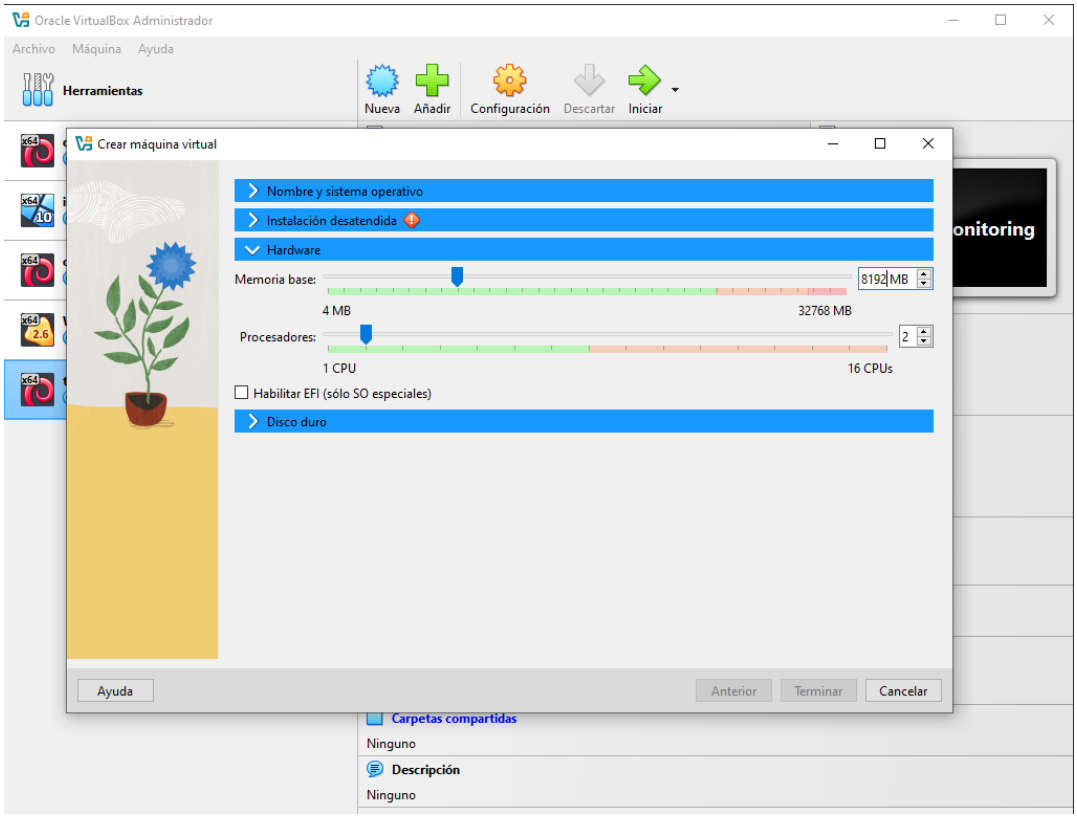
Para iniciar el proceso de instalación de la VM, seguir los siguientes pasos del video, donde se explica paso a paso la configuración.

[YOUTUBE]: https://www.youtube.com/watch?v=hZ5J-wYuIO0

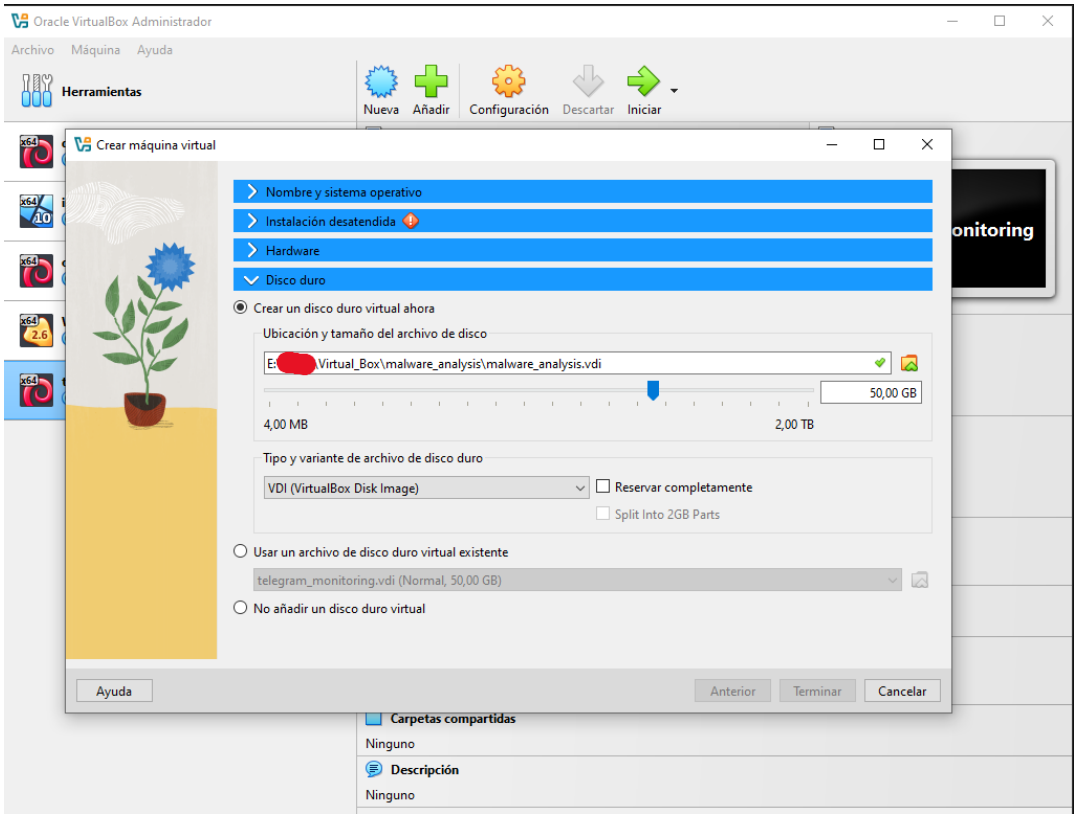
1. Cargar Sistema Operativo:



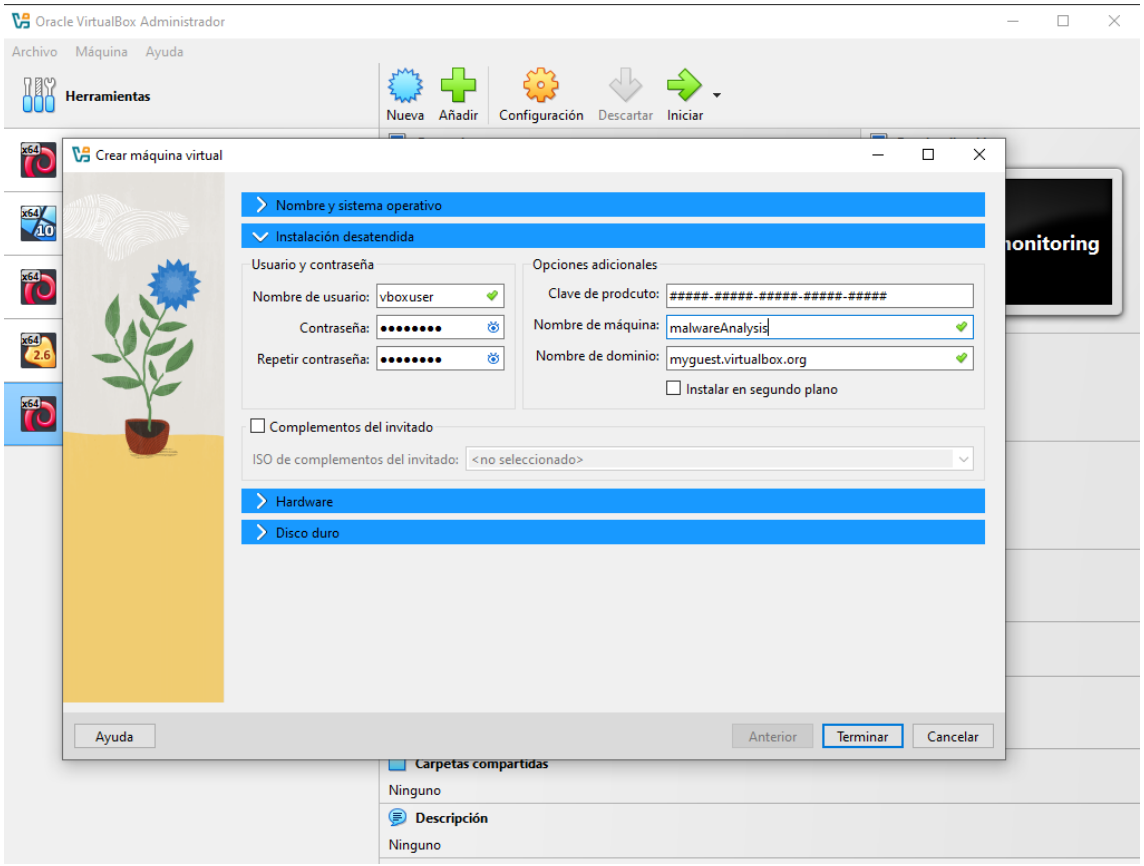
2. Capacidades del Hardware:



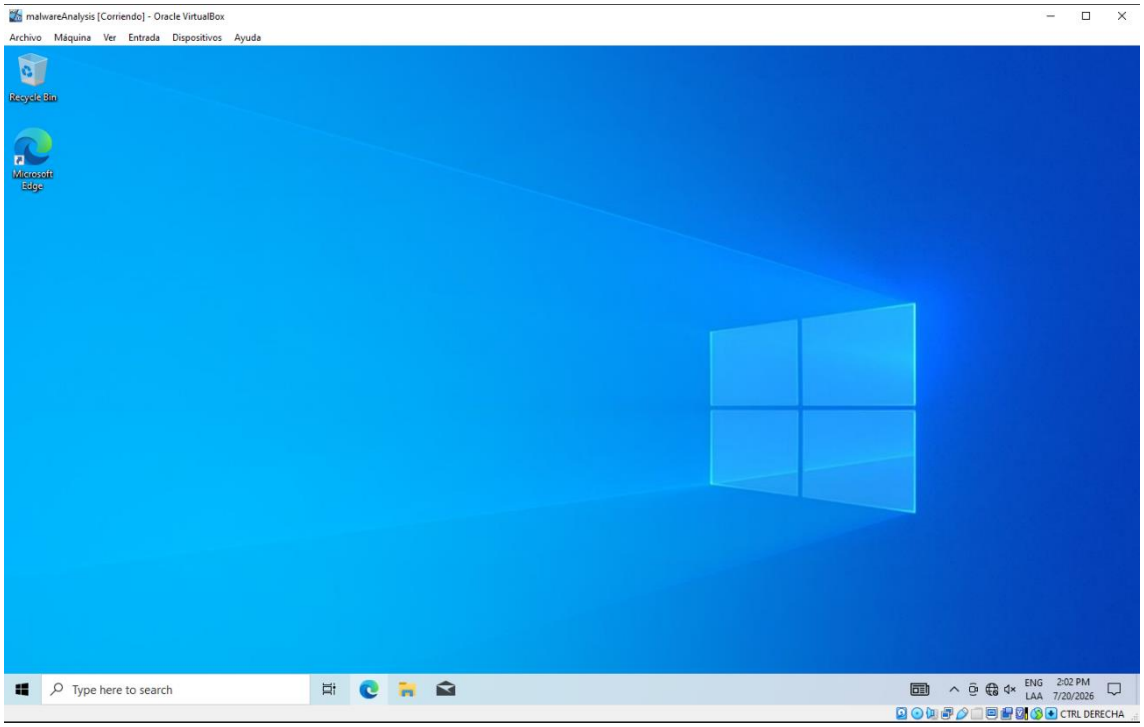
3. Espacio Disco Virtual:



4. Configuración predeterminada:



5. Windows 10 instalado:



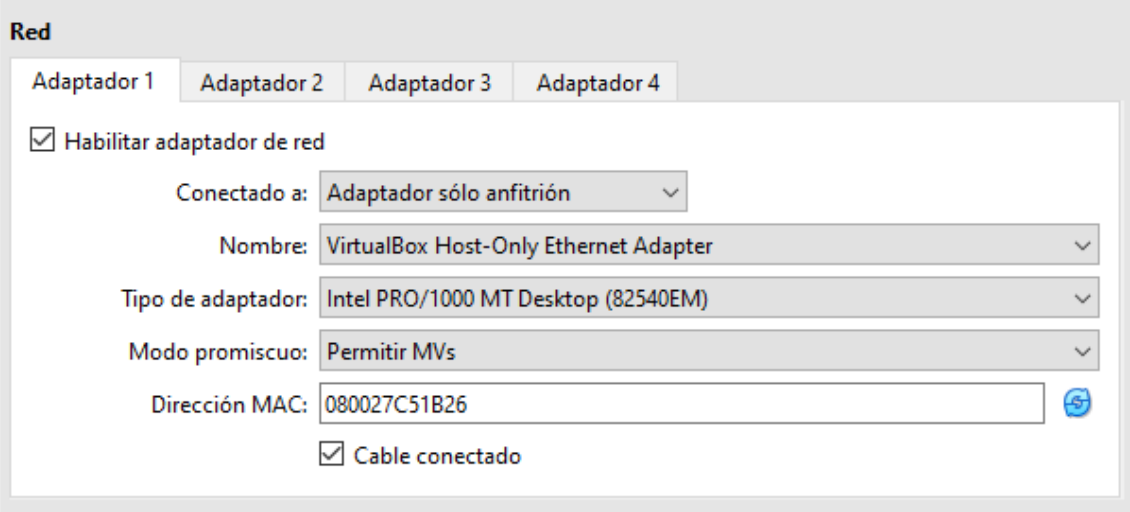
4) Securizar VM

1. Aislamiento de red

Instalación con NAT (solo inicial): para descargar actualizaciones, herramientas, y recursos para testing.

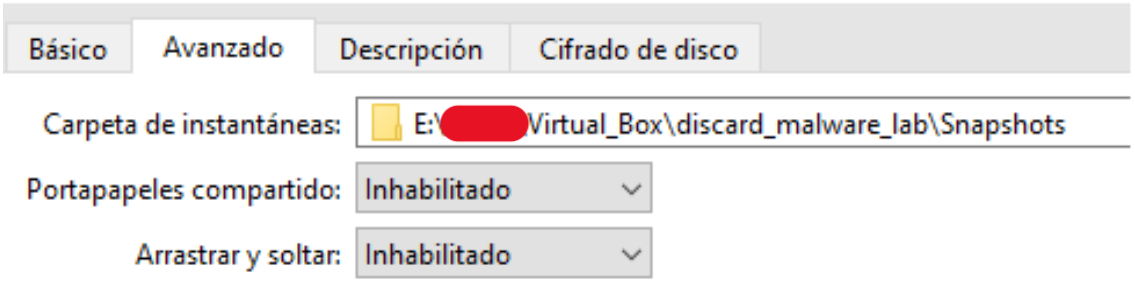
Después de la instalación:

Red → Adaptador **solo-anfitrión (Host-Only Adapter)** sin darle conexión a internet. Esta configuración de red nos asigna una dirección IP segmentada de la red principal, sin embargo podemos tener visibilidad con la maquina host.



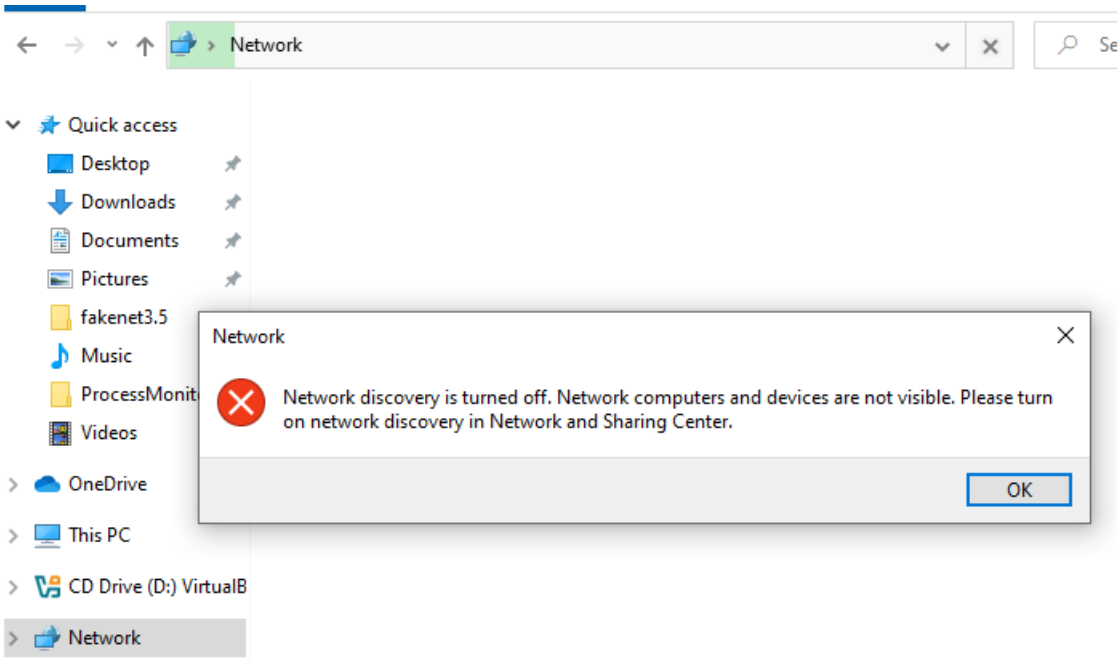
2. Aislamiento de recursos compartidos

- **Carpetas compartidas** → Desactivado.
- **Arrastrar y soltar (Drag & Drop)** → Desactivado.
- **Portapapeles compartido** → Desactivado.



Directorio de Red

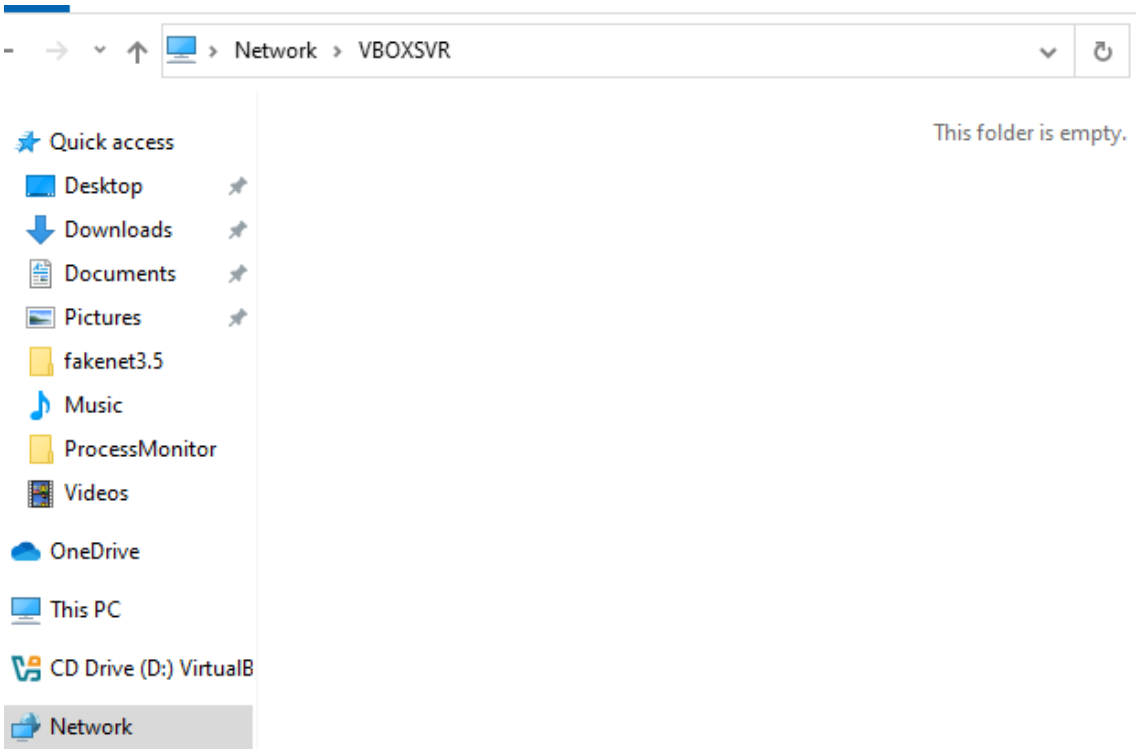
Verificar que el descubrimiento de red este desactivado en el Windows invitado (VM).



Explorador de Archivos

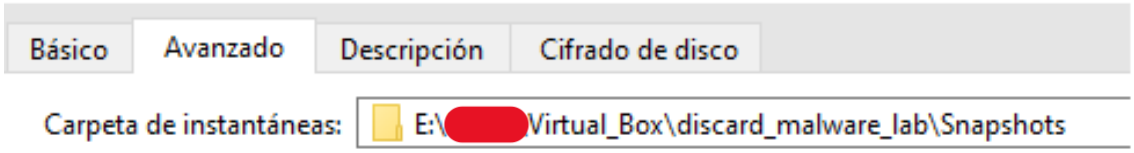
Verificar que no halla carpetas compartidas en el directorio “\\VBOXSVR\” de la unidad de red.

Para verificar esto dirigite a al explorador de archivos → Network → y en la barra superior escribir ““\\VBOXSVR\”. Si la carpeta esta vacia significa que no existe ningun archivo compartido.



3. Configuración de almacenamiento

- Guardar el **disco virtual (VDI)** de la VM en un directorio **separado** del resto de tus documentos. Utilizar una partición de disco diferente del directorio personal de trabajo.
- No utilizar discos compartidos ni rutas de red mapeadas entre host y VM.



Arquitectura de carpetas:

C:*Windows* (Instalación de SO)

D:*<TuUsuario>* (Directorio personal)

E:\ *<TuUsuario>* (Laboratorio Virtual)

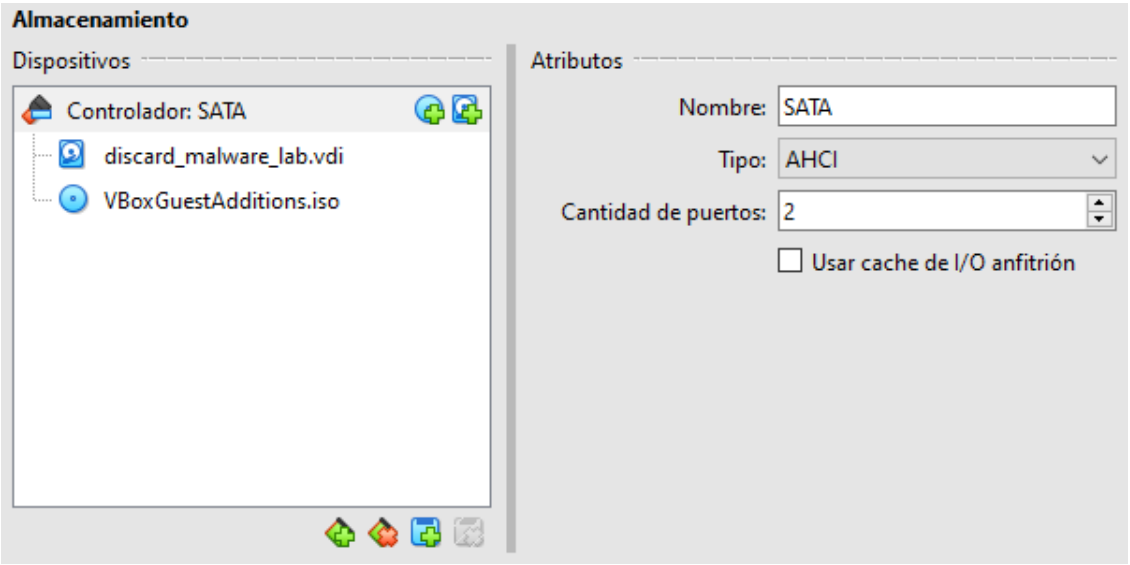
discard_malware_lab

malware_lab_1

malware_lab_2

Instalación del VDI:

El disco virtual (.vdi) debe estar guardado dentro de la carpeta de su VM correspondiente.

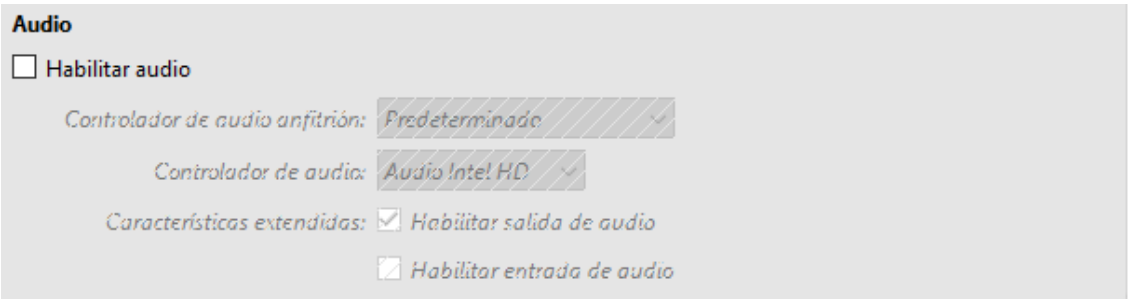


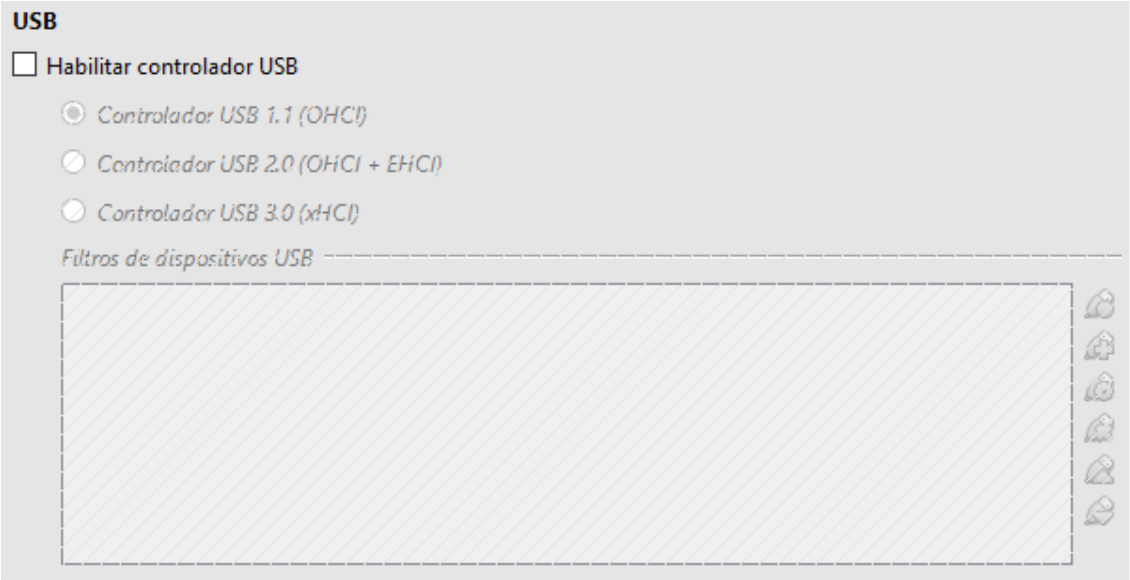
E:\ *<TuUsuario>* (Laboratorio Virtual)

*discard_malware_lab**discard_malware_lab.vdi*

4. Deshabilitar USB y dispositivos

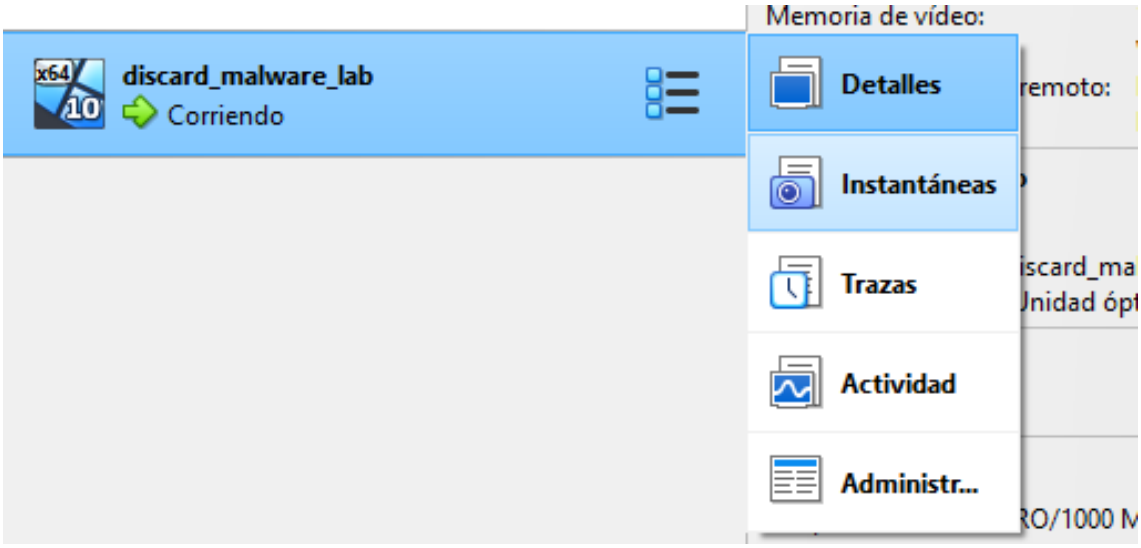
- **USB**: Desactivar el soporte de USB en la VM.
- **Audio y Cámara**: Si no los necesitas, desactívalos en configuración → Audio / USB.



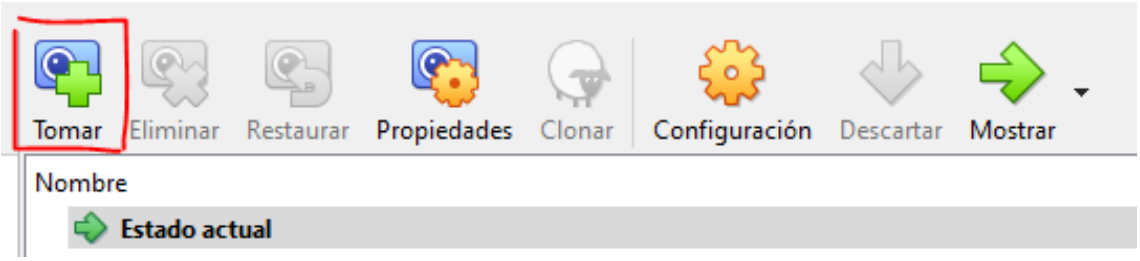


5. Snapshots (Backup)

Una vez tengas el Windows 10 recién instalado y limpio, crea un snapshot. Así puedes volver a un estado limpio sin reinstalar todo desde cero.



Seleccionar <Tu maquina virtual> → Instantáneas → Tomar



⚒️ Instalar Herramientas Locales:

Una vez terminada la instalación de nuestra máquina virtual, procederemos a instalar todas nuestras herramientas para analizar archivos estáticos.

Para esta sección la configuración de red debe ser NAT, luego de la instalación de las herramientas volver a Only Host o deshabilitar por completo el adaptador de red. En caso de tener las herramientas previamente descargadas (recomendado), compartirlas mediante pendrive al laboratorio de malware (VM).

1. Detect It Easy

https://www.detectiteasy.com/download-for-windows

2. Malcat

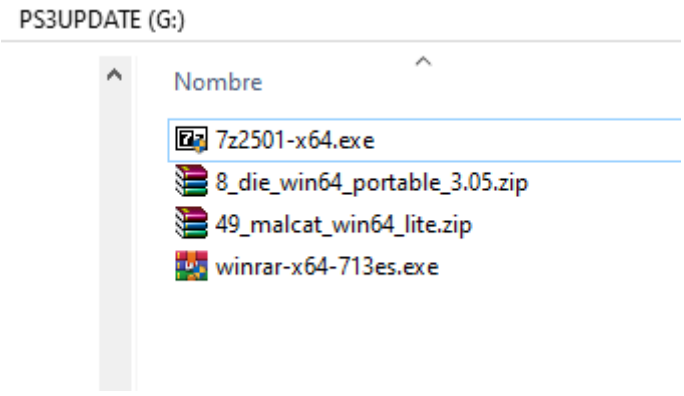
https://malcat.fr/download.html

3. 7z

https://www.7-zip.org/download.html

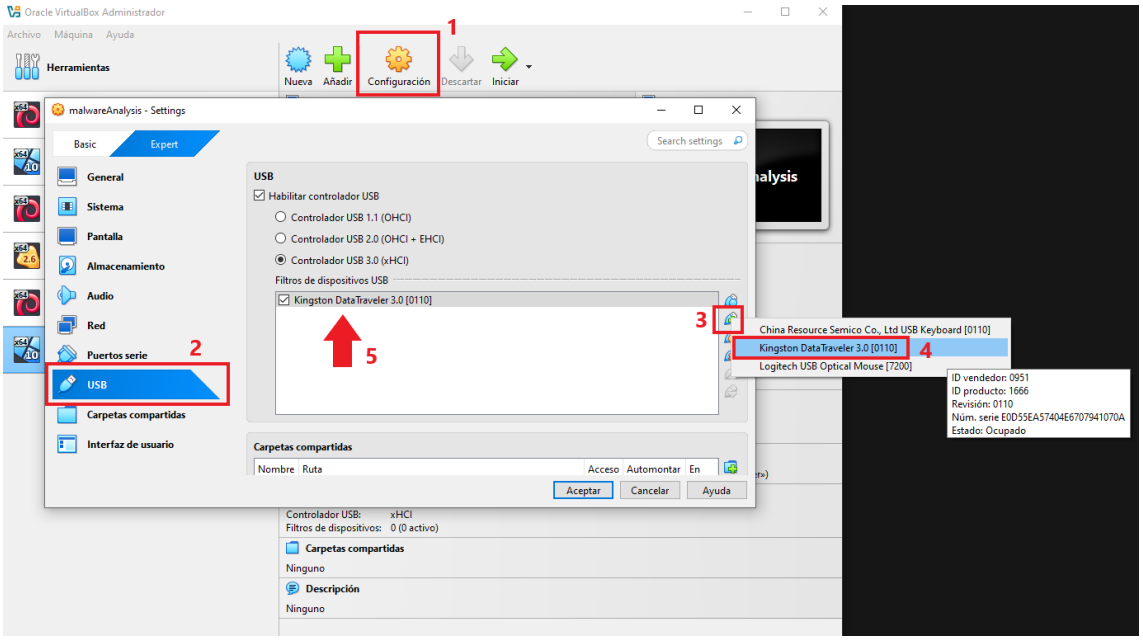
1. Compartir herramientas con pendrive

En el caso de ya tener previamente descargadas las herramientas, transferirlas a un pendrive.



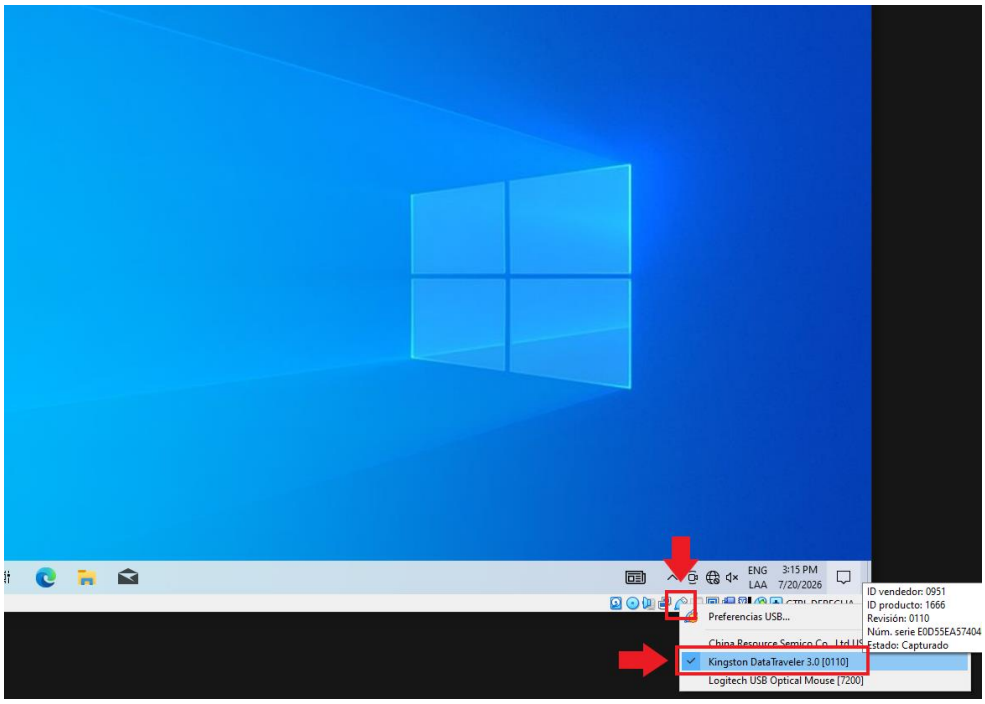
2. Habilitar pendrive en VM

1. Colocar pendrive en PC
2. Abrir configuración de nuestra VM
3. Seleccionar opción USB
4. Habilitar controlador USB
5. Incluir nuestra unidad USB (pendrive)
6. Aceptar los cambios (Aceptar)

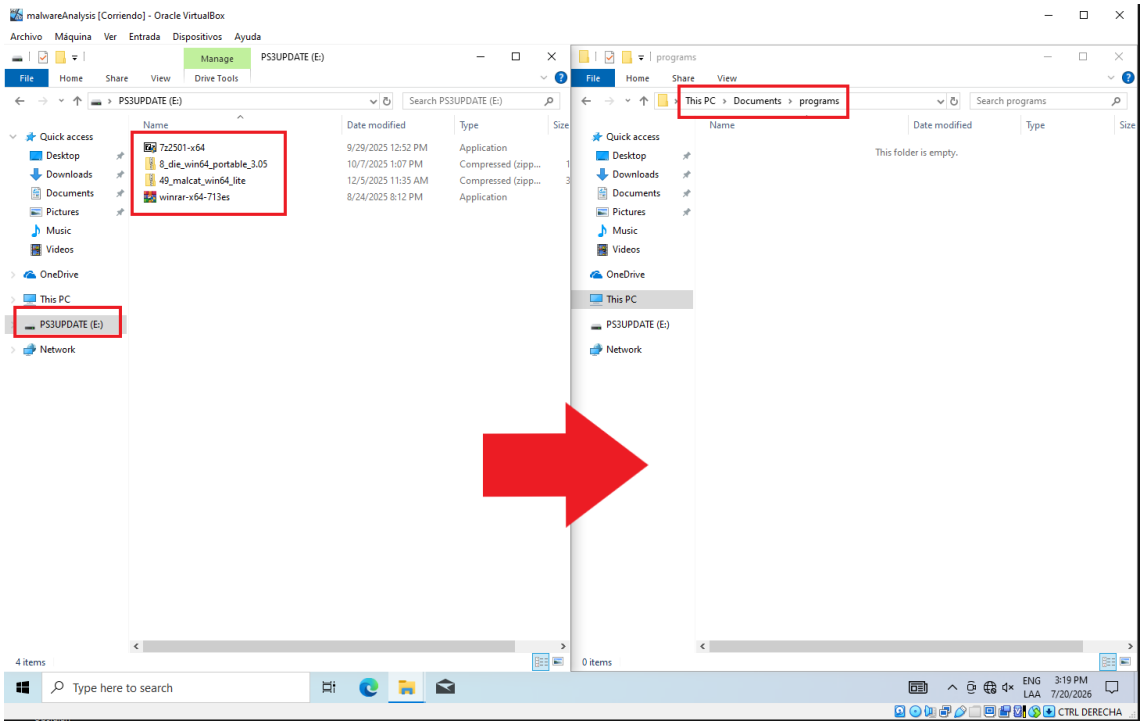


3. Compartir herramientas en la VM

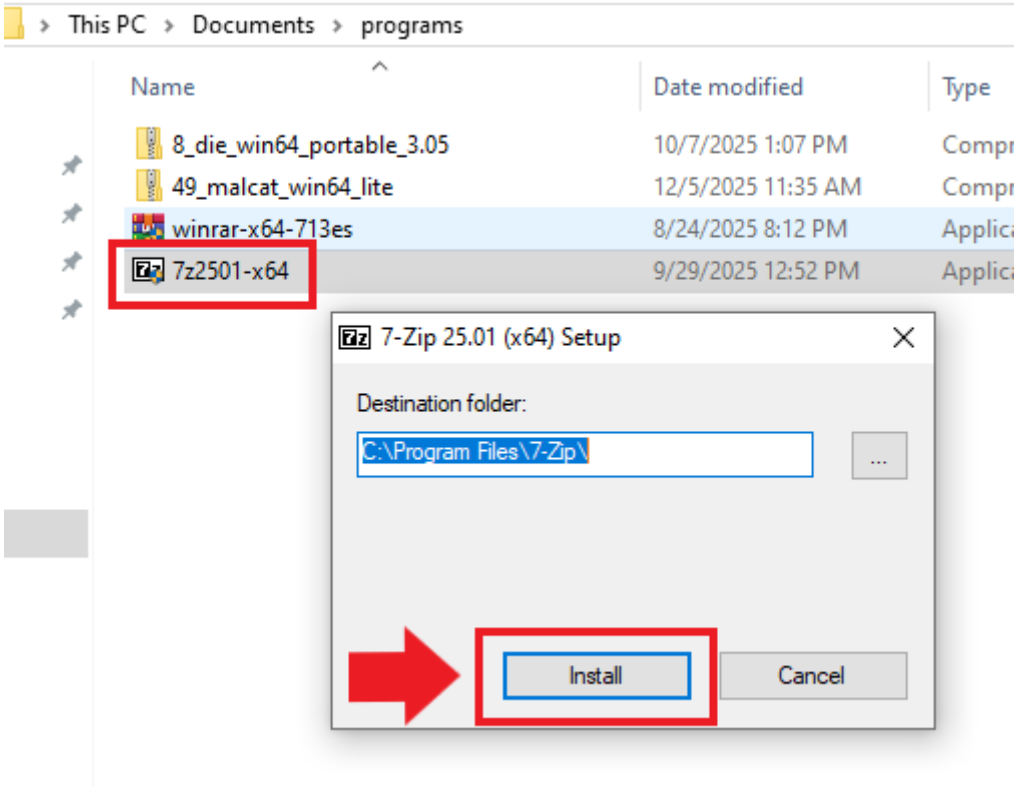
1. Incorporar pendrive en VM



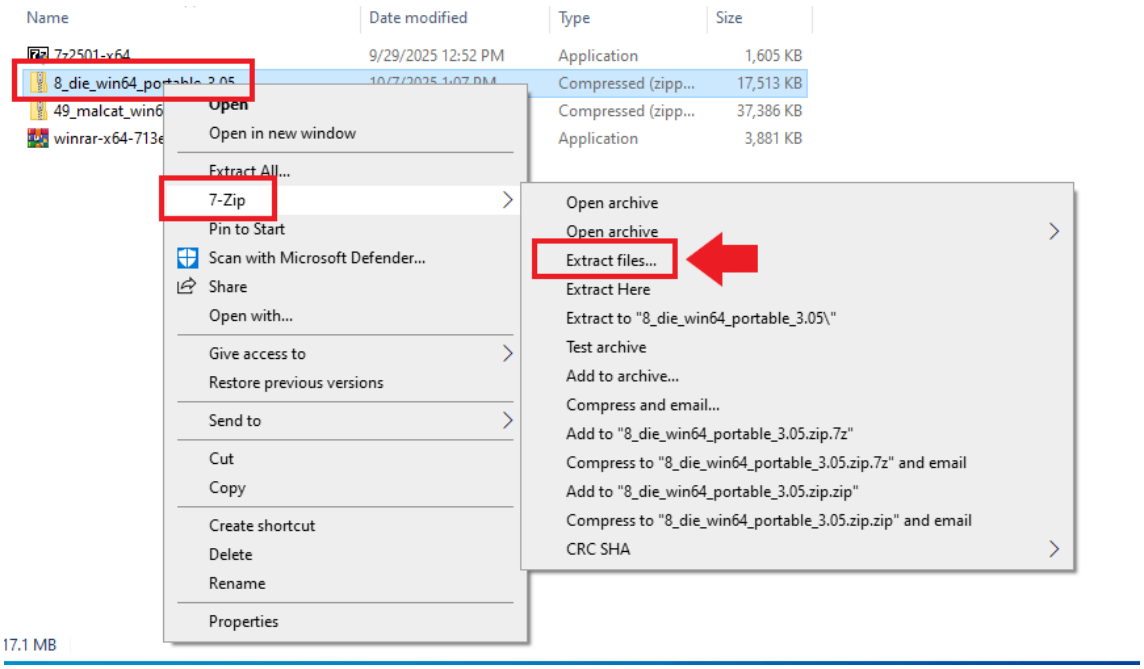
2. Transferir herramientas

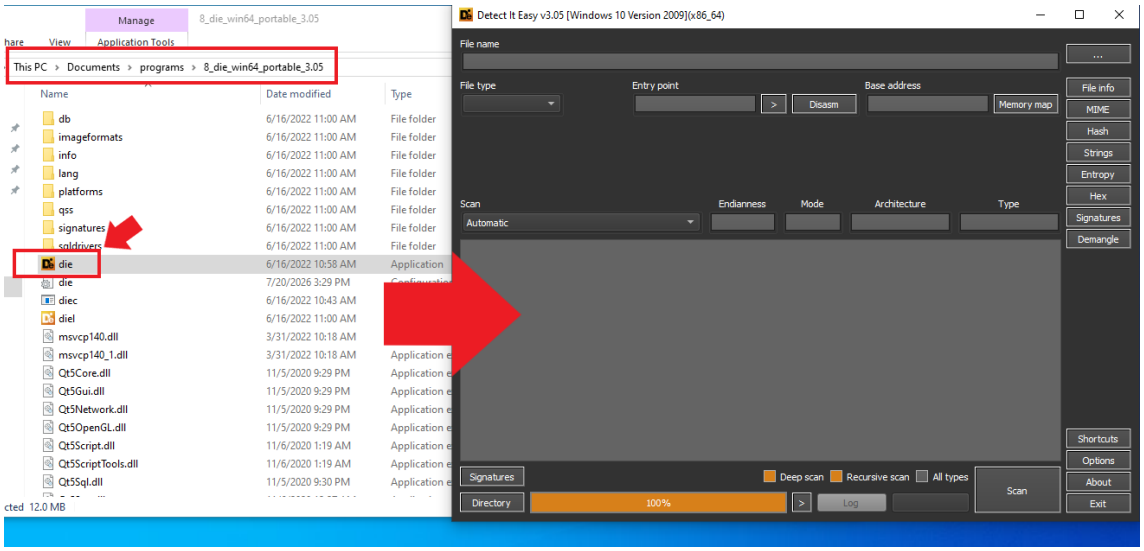


4. Instalar 7z

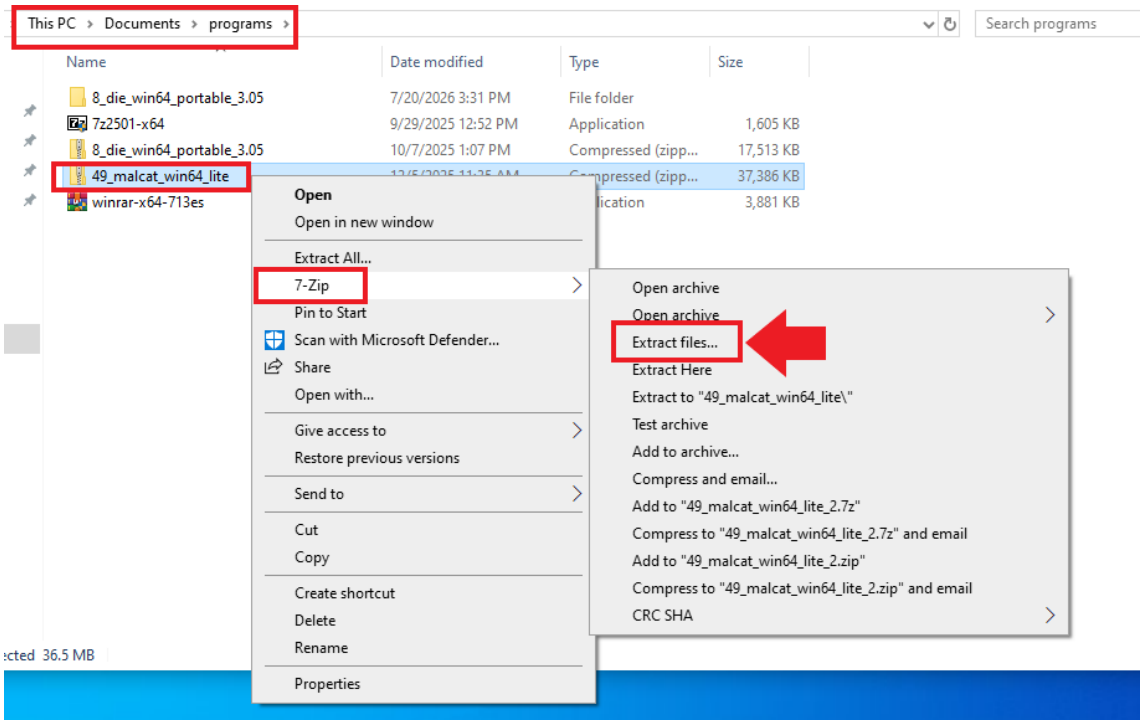


5. Instalar Detec It Easy (DIE)

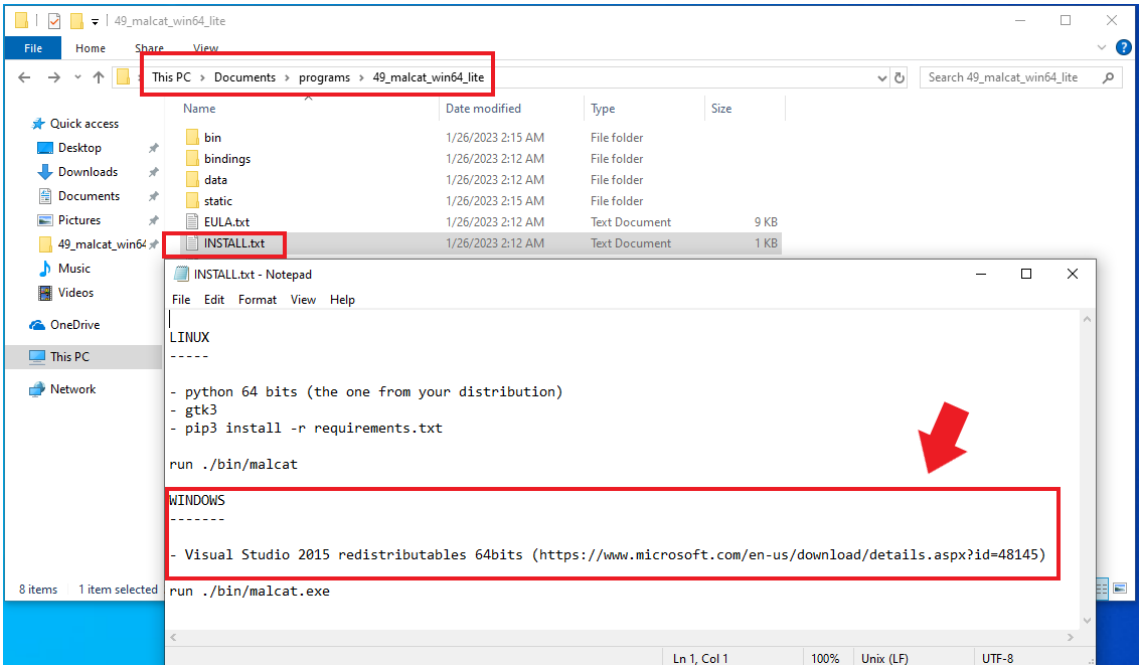




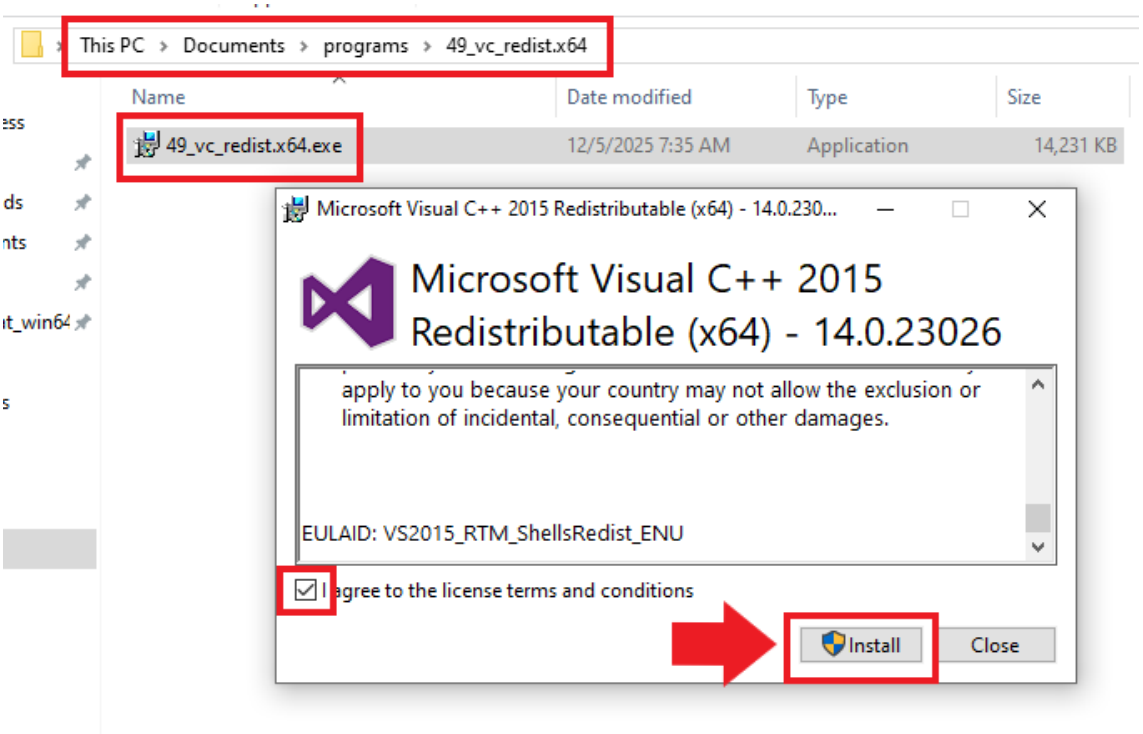
6. Instalar Malcat



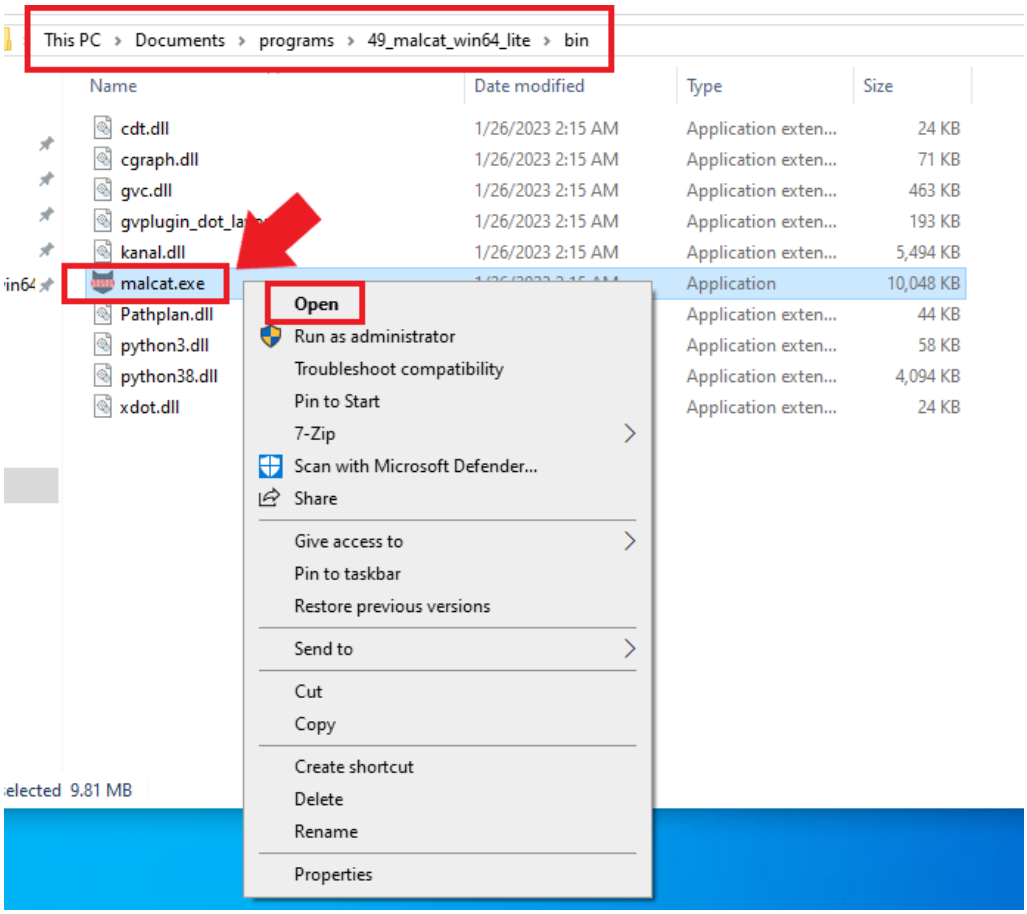
1. Descargar Visual Studio 2015

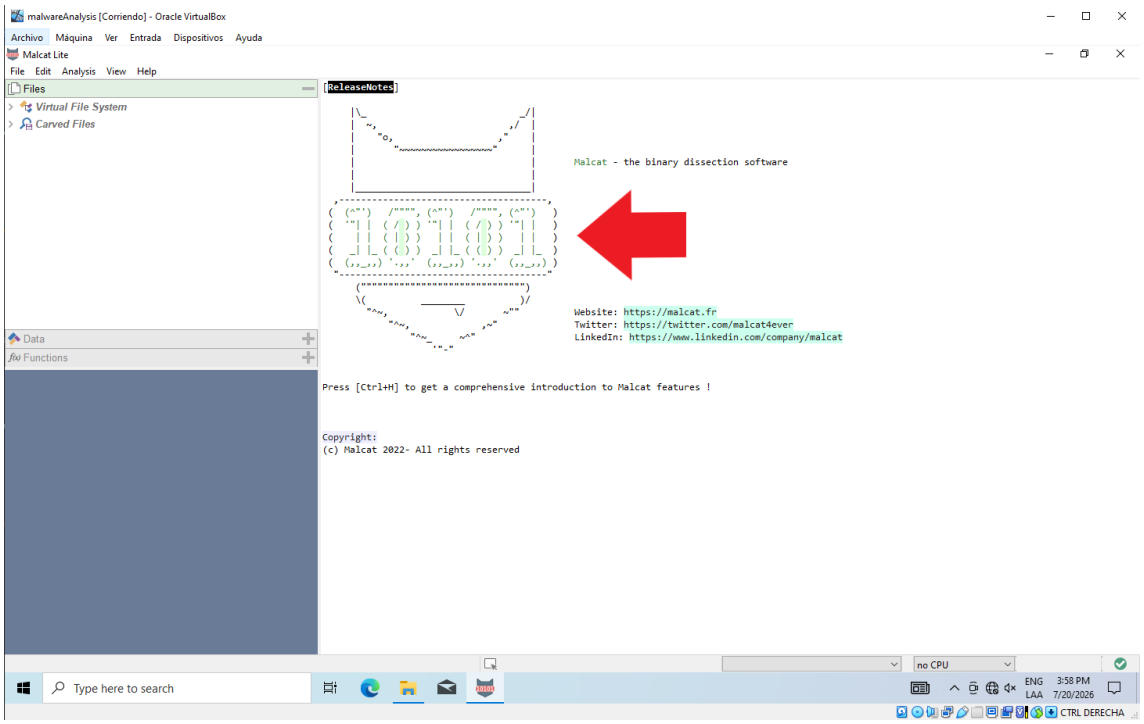


2. Instalar Visual Studio 2015



3. Instalar Malcat





Finalizada la etapa de instalación de herramientas, toma de instantáneas del SO y registro de Windows, ahora podemos iniciar la fase de análisis estático de malware.

Contacto

https://www.linkedin.com/in/david-padron-9a74aa323/

https://github.com/FeathersMcgr4w

https://davidpadron.info