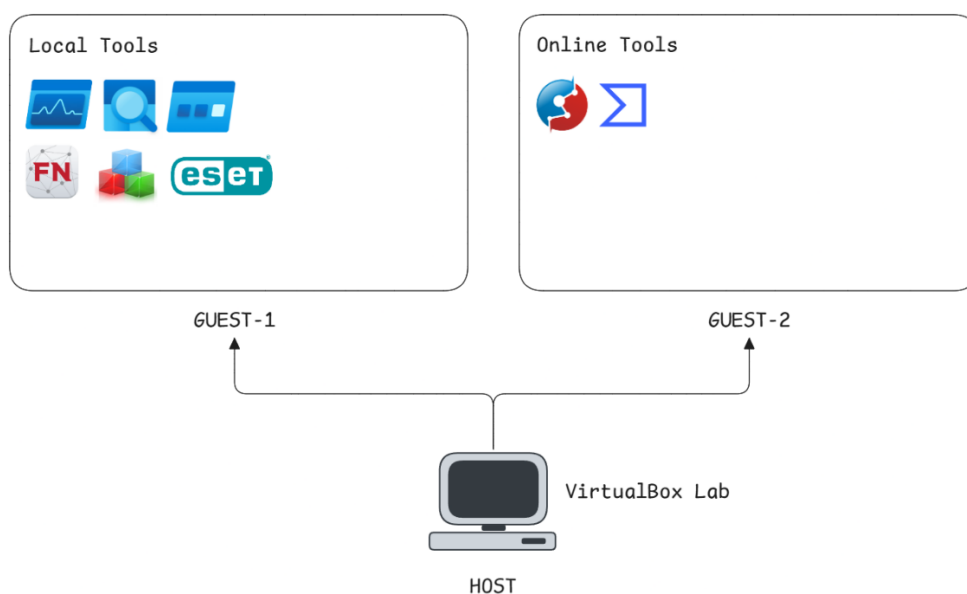


Laboratorio Análisis Dinámico de Malware



ReadMe: el siguiente documento expondrá una guía práctica para crear un laboratorio de análisis de malware. Se listarán todas las herramientas a utilizar, fuentes de descarga e instalación y configuración de las mismas. Además, se darán recomendaciones sobre la configuración del firewall de Windows y capturas de instantáneas del SO y registro antes de ejecutar cualquier análisis en la VM.

Arquitectura de máquinas virtuales



Herramientas Local:

- VirtualBox
- Process Monitor (Sysinternals)
- Process Explorer (Sysinternals)
- Autoruns (Sysinternals)
- FakeNet-NG 3.5
- ESET SysInspector
- RegShot

Herramientas Online:

- Hybrid Analysis
- Virus Total

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>

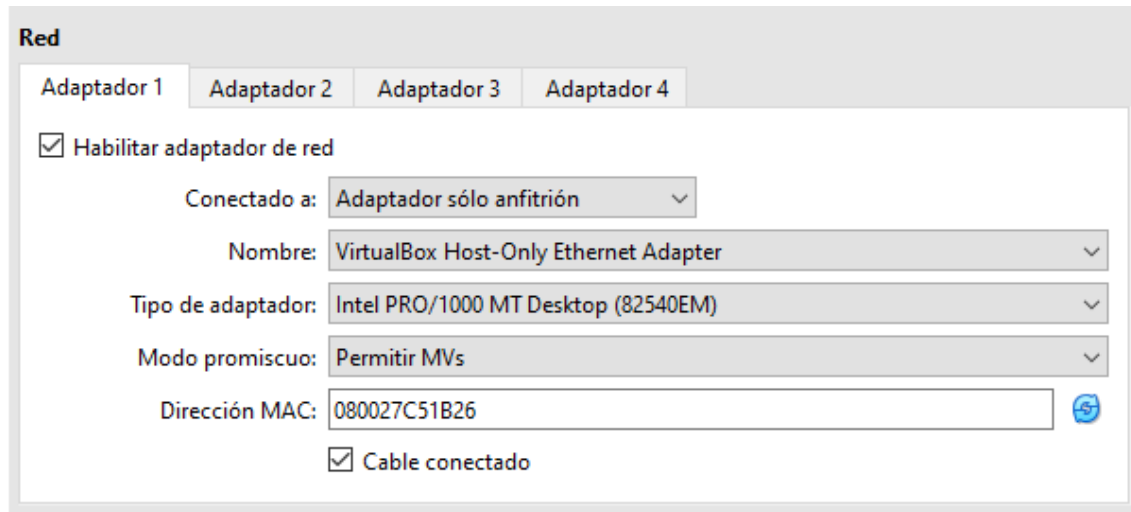
 **NOTA:** Primeramente configuraremos la VM con una configuración de red NAT para poder descargar y compartir por red todas las herramientas para nuestro testing. Finalizada la transferencia de herramientas procederemos a securizar la VM con la siguiente configuración.

1. Aislamiento de red

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

Después de la instalación:

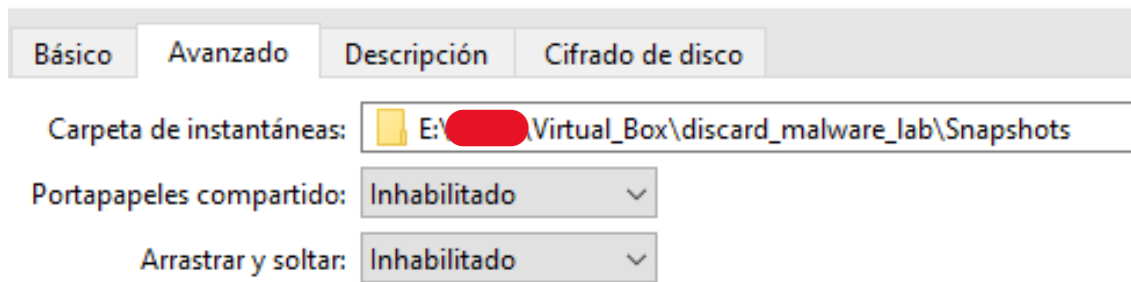
Red → Adaptador **solo-anfitrión (Host-Only Adapter)** sin darle conexión a internet.
Esta configuración de red nos asigna una dirección IP segmentada de la red principal, sin embargo podemos tener visibilidad con la maquina host.



2. Aislamiento de recursos compartidos

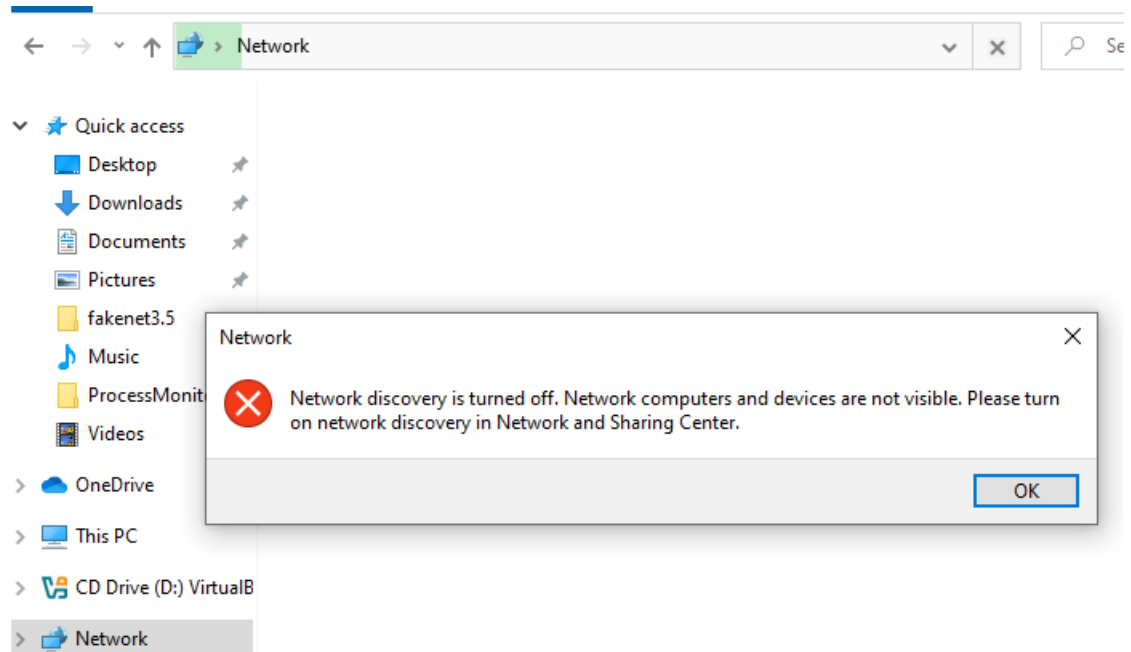
- **Carpetas compartidas** → Desactivado.
- **Arrastrar y soltar (Drag & Drop)** → Desactivado.
- **Portapapeles compartido** → Desactivado.





Directorio de Red

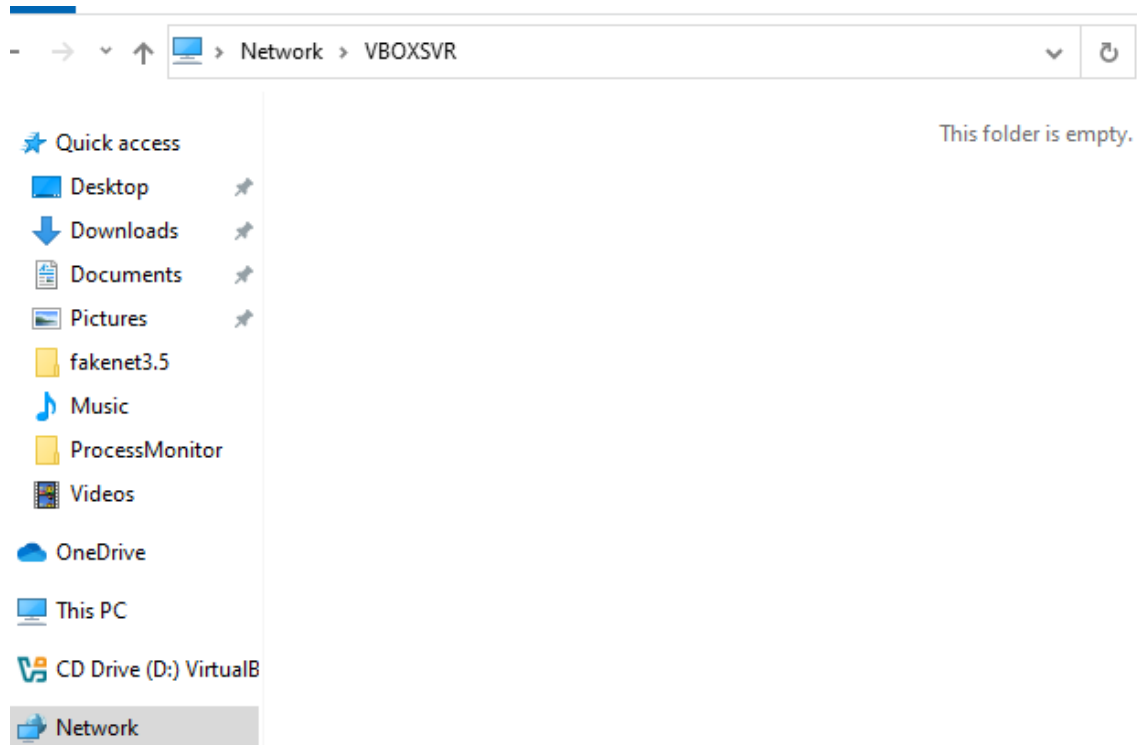
Verificar que el descubrimiento de red este desactivado en el Windows invitado (VM).



Explorador de Archivos

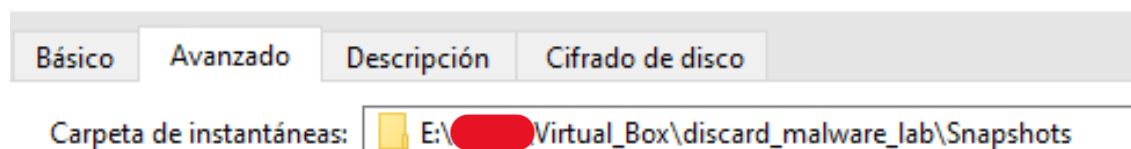
Verificar que no halla carpetas compartidas en el directorio "\\VBOXSVR\" de la unidad de red.

Para verificar esto dirígite 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)

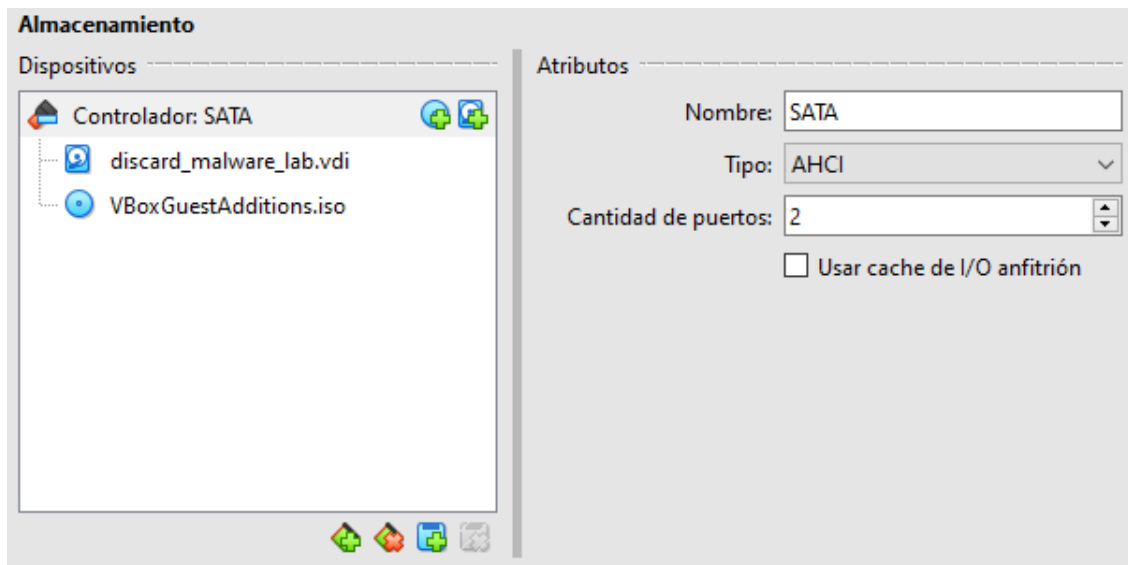
\discard_malware_lab

\malware_lab_1

\malware_lab_2

Instalación del VDI:

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

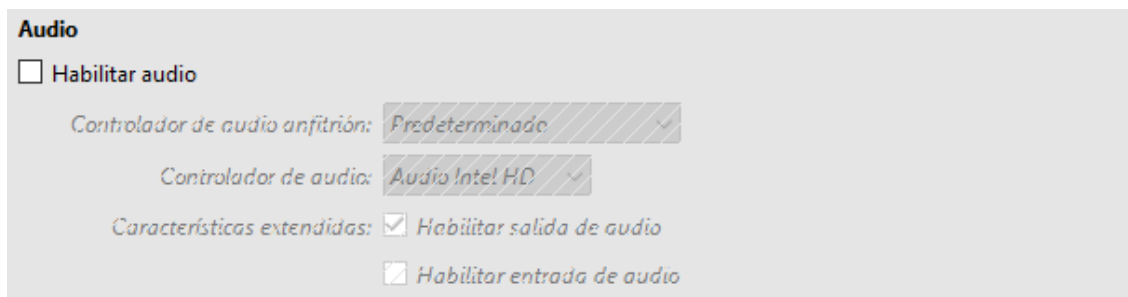


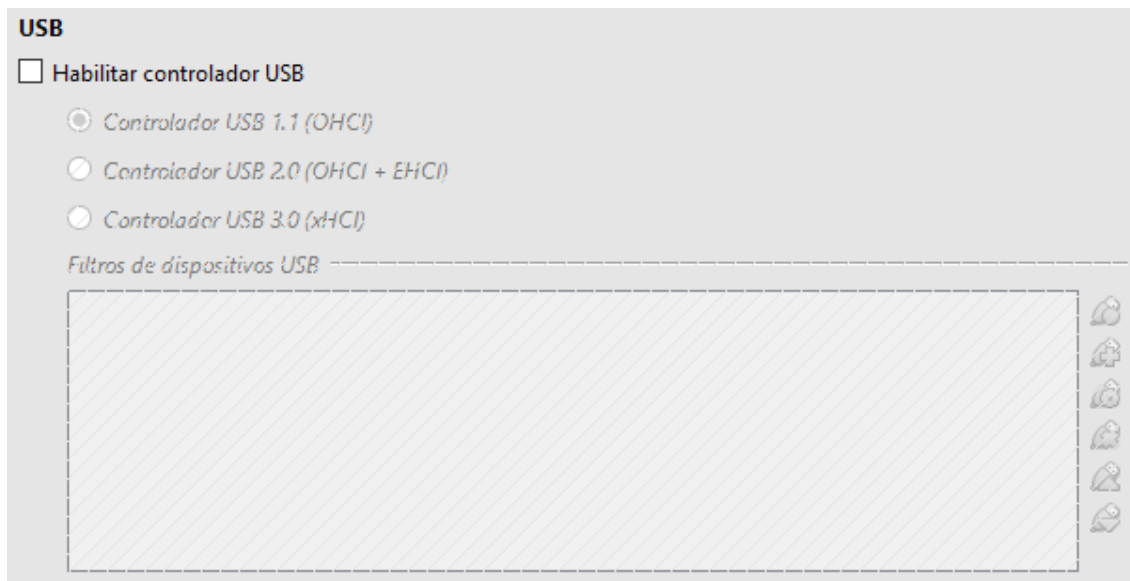
E:\ <TuUsuario> (Laboratorio Virtual)

\discard_malware_lab\discard_malware_lab.vdi

4. Deshabilitar USB y dispositivos

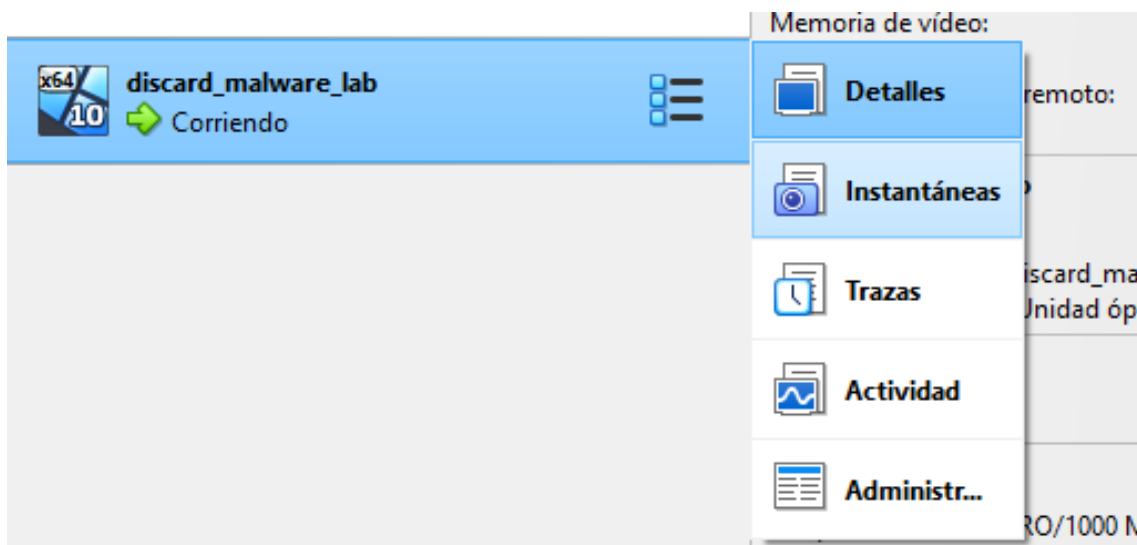
- **USB:** Desactivar el soporte de USB en la VM.
- **Audio y Cámara:** Si no los necesitas, desactívalos en configuración → Audio / USB.



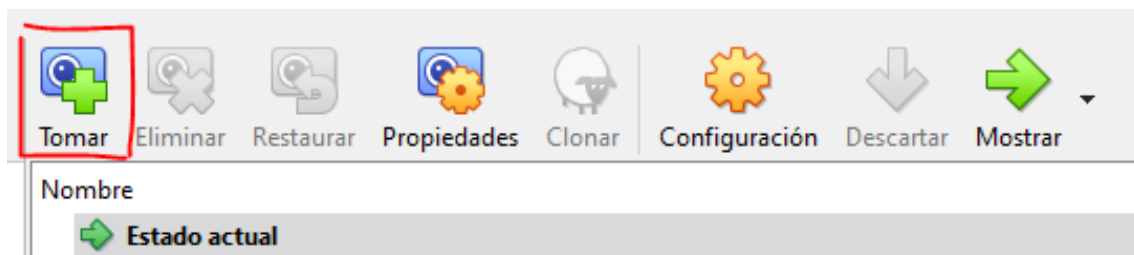


5. Snapshots (Backup)

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 malware.

Para esta sección la configuración de red debe ser NAT, luego de la instalación de las herramientas volver a Only Host.

1. Process Monitor (Sysinternals)

<https://learn.microsoft.com/es-es/sysinternals/downloads/procmon>

2. Process Explorer (Sysinternals)

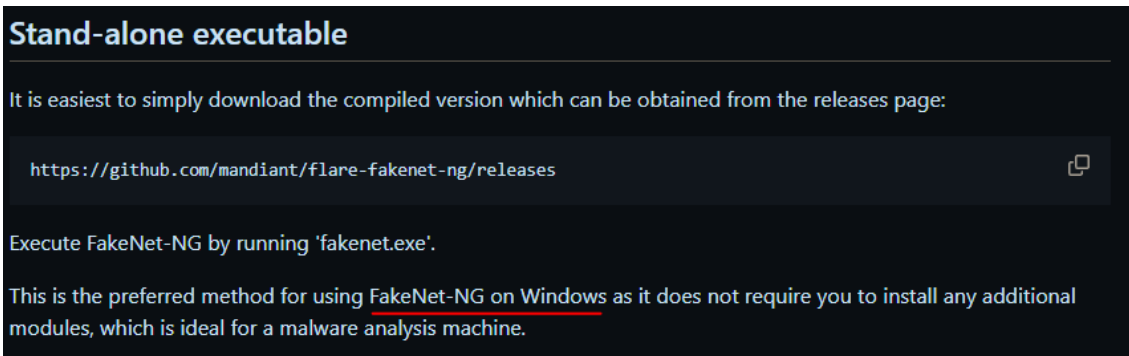
<https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer>

3. Autoruns (Sysinternals)

<https://learn.microsoft.com/es-es/sysinternals/downloads/autoruns>

4. FakeNet-NG 3.5

<https://github.com/mandiant/flare-fakenet-ng>



Stand-alone executable

It is easiest to simply download the compiled version which can be obtained from the releases page:


<https://github.com/mandiant/flare-fakenet-ng/releases>

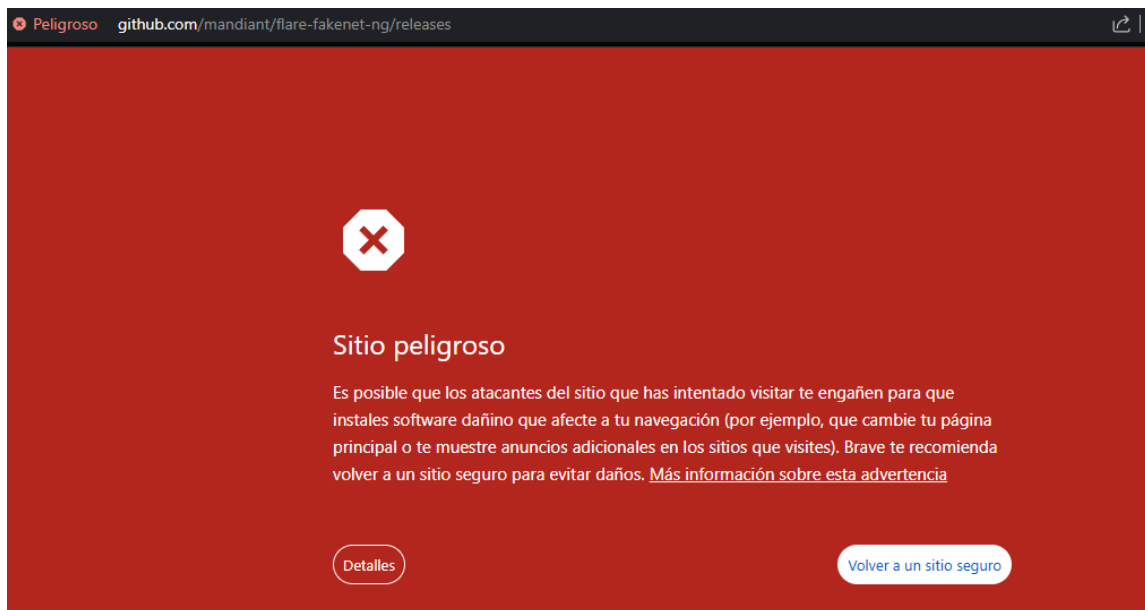
Execute FakeNet-NG by running 'fakenet.exe'.

This is the preferred method for using FakeNet-NG on Windows as it does not require you to install any additional modules, which is ideal for a malware analysis machine.

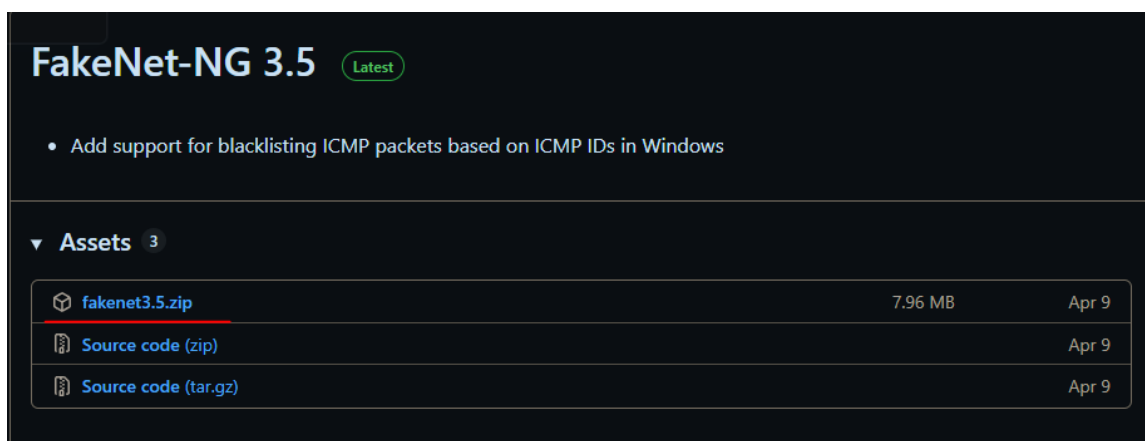
La documentación recomienda para sistemas Windows la instalación del ejecutable "fakenet.exe". Para esto nos dirigimos a la siguiente url:

<https://github.com/mandiant/flare-fakenet-ng/releases>

 **NOTA:** Al navegar por la URL, el navegador nos lanzara una alerta de posible amenaza debido a que este usa listas de reputación (Safe Browsing de Google y filtros propios) las cuales marcan como "herramienta de hacking", o "reverse engineering" y el navegador lanza esta advertencia, aunque el proyecto sea legítimo.



Descargar el archivo comprimido “fakenet3.5.zip”



5. ESET SysInspector

https://download.eset.com/com/eset/tools/diagnosis/sysinspector/latest/sysinspector_nt64_esl.exe

6. RegShot

<https://sourceforge.net/projects/regshot/>

<https://github.com/Seabreg/Regshot>

Instalación FakeNet-NG

Antes de realizar el descomprimido del archivo “fakenet3.5.zip”, se deberá desactivar el análisis en tiempo real del firewall de Windows y además generar una excepción especificando el binario ejecutable “fakenet.exe”.

Deshabilitar Firewall:

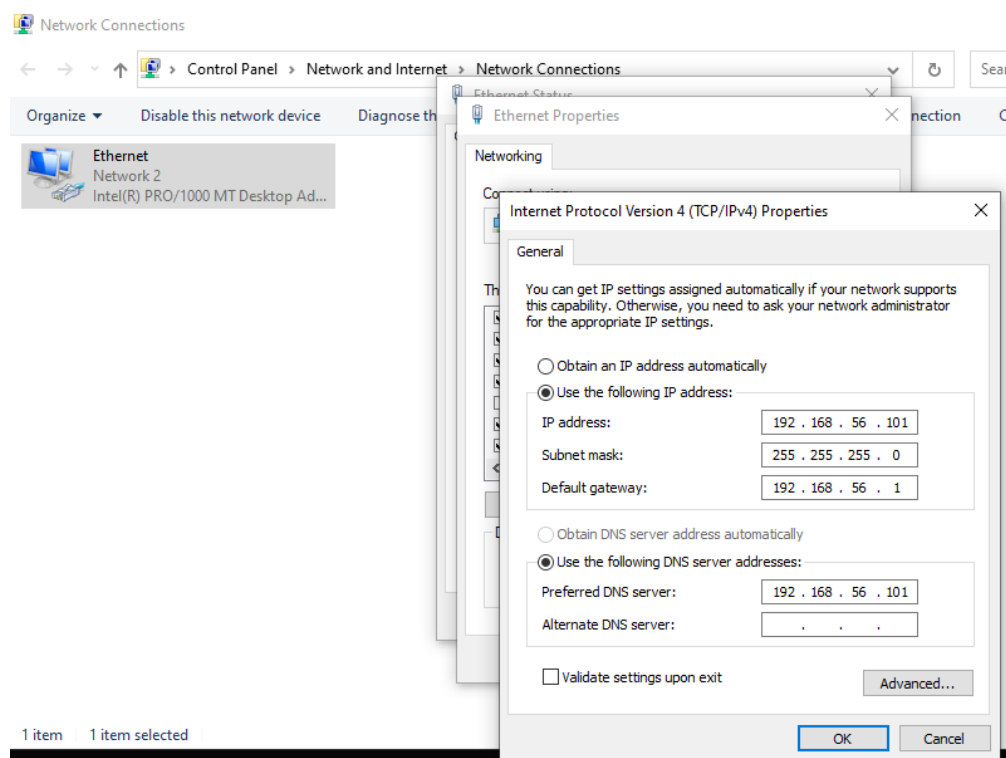
Windows Security → Virus & threat protection → Virus & threat protection settings → Manage settings → Real-time protection (*OFF*)

Habilitar Excepción:

Windows Security → Virus & threat protection → Virus & threat protection settings → Manage settings → Exclusions → Add or remove exclusions → + Add an exclusion

Conexión de red

En este paso verificamos que nuestra conexión de red sea “*Only Host*”. Esta configuración habilita la tarjeta de red para asignarnos una dirección de red segmentada de la red general, la cual utilizara *fakenet* para simular el entorno de red falso.

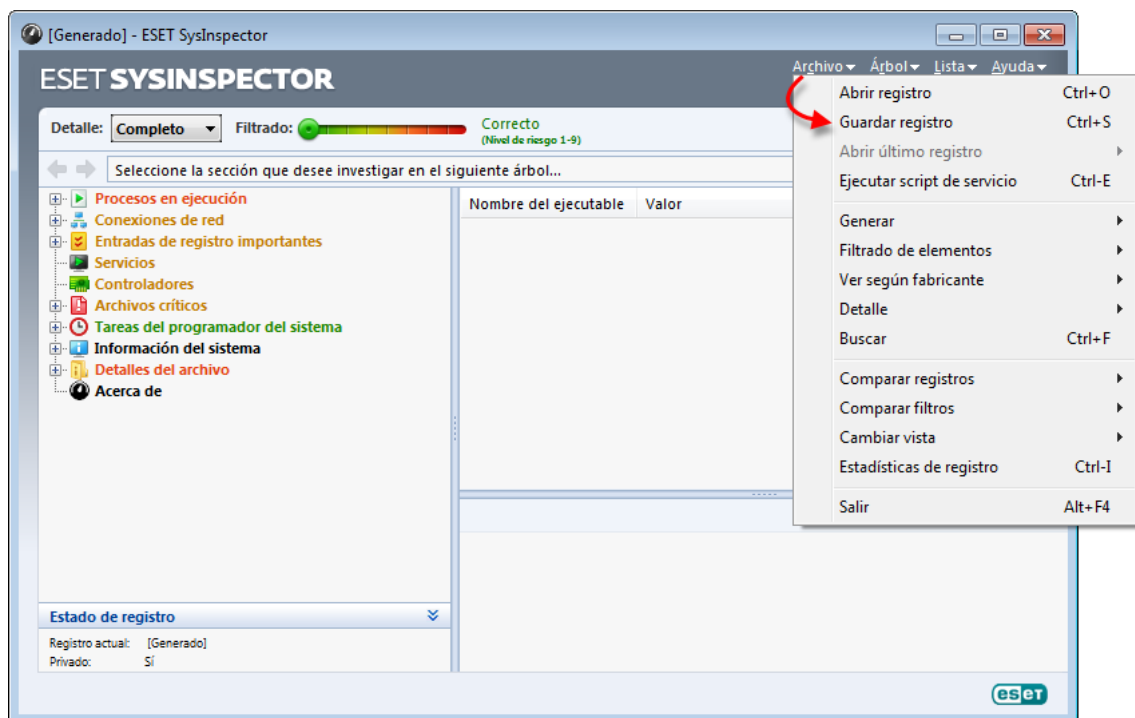


Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . :  
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter  
Physical Address. . . . . : 08-00-27-C5-1B-26  
DHCP Enabled. . . . . : No  
Autoconfiguration Enabled . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::3770:3d96:3ec2:4b2b%5(Preferred)  
IPv4 Address. . . . . : 192.168.56.101(Preferred)  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.56.1  
DHCPv6 IAID . . . . . : 101187623  
DHCPv6 Client DUID. . . . . : 00-01-00-01-30-4B-5A-7C-08-00-27-C5-1B-26  
DNS Servers . . . . . : 192.168.56.101  
NetBIOS over Tcpip. . . . . : Enabled
```

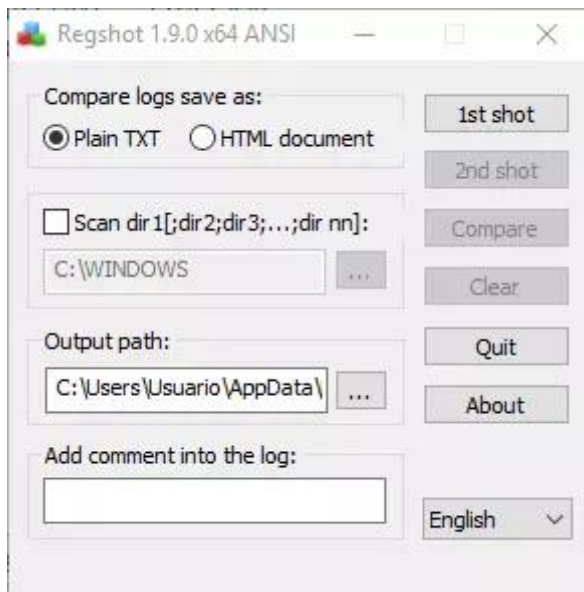
Snapshot Eset SysInspector

Ejecutar el primer análisis de toda la maquina virgen con la herramienta Eset SysInspector. Luego guardar un backup del archivo de registro: Archivo → Guardar registro.



Regshot

Ejecutar una captura del registro de Windows con la herramienta regshot.



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

Contacto

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

 <https://github.com/FeathersMcgr4w>

 <https://feathersmcgr4w.github.io/cyber-portfolio/>