1. Instalación y configuración de los entornos virtuales

En este anexo se describe el proceso de instalación de las máquinas virtuales utilizadas en la creación del laboratorio virtual para análisis de malware.

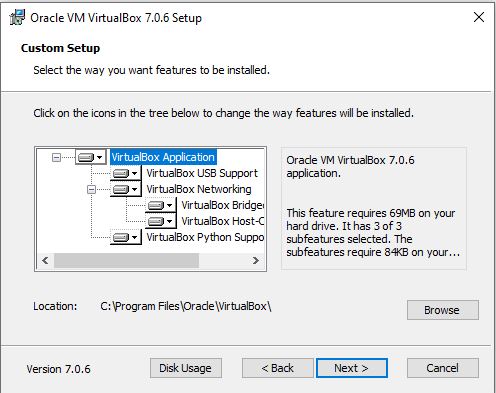
Primero debemos escoger el hipervisor, este paso es muy importante para poder mantener la seguridad al momento de manipular y ejecutar el malware. Sin poner el riesgo el sistema operativo del host físico. El hipervisor que utilizaremos en este piloto experimental es Virtual Box, ya que es de código abierto, se puede descargar libremente, es fácil de usar. Pero lo más importante, nos permite tomar instantáneas del sistema y volver a un estado anterior. Esto será de suma importancia cuando comencemos a ejecutar el malware para su posterior análisis.

Link descarga VirtualBox: <https://www.virtualbox.org/wiki/Downloads>

Instalar VirtualBox en Mac: <https://cs.hofstra.edu/docs/pages/guides/vbox_mac.html>

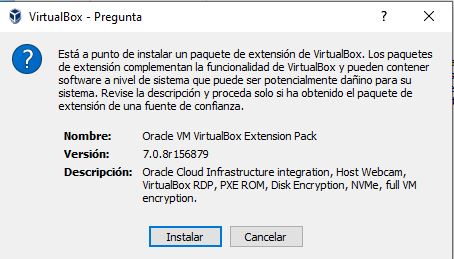
Instalar VirtualBox en Linux: <https://phoenixnap.com/kb/install-virtualbox-on-ubuntu>

Primero debemos descargar el instalador, y luego ejecutarlo como administrador.

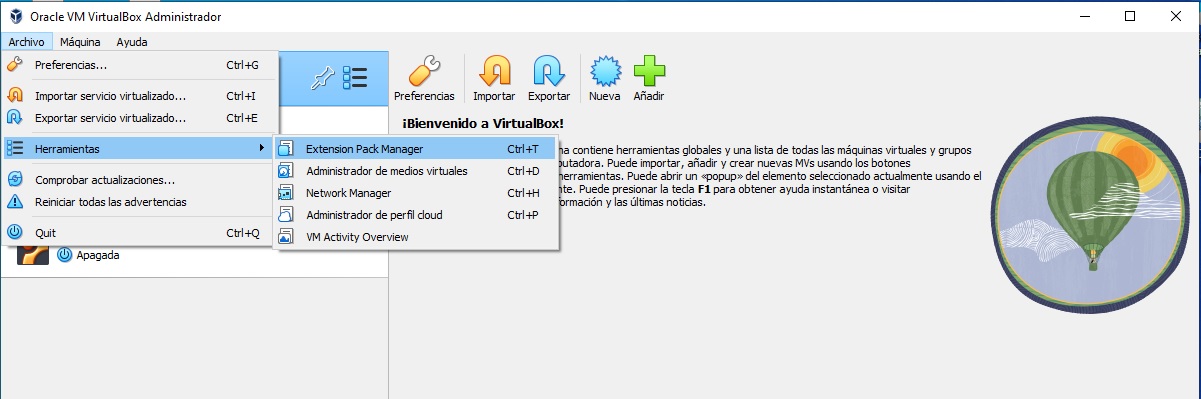


**Fuente:** Elaboración propia

Luego descargamos el paquete de extensiones de Virtual Box.



**Fuente:** Elaboración propia



**Fuente:** Elaboración propia

Al finalizar la instalación debemos ver la siguiente pantalla:

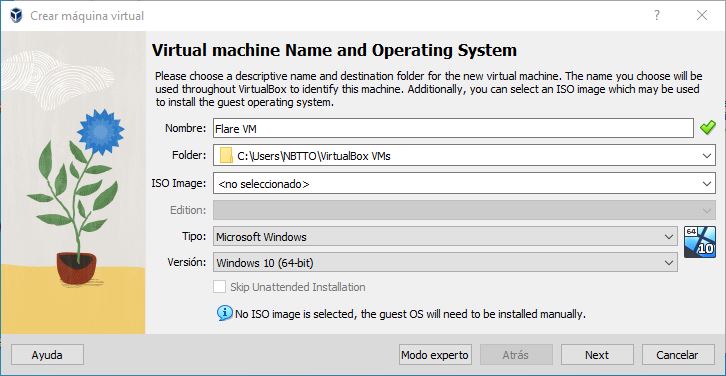
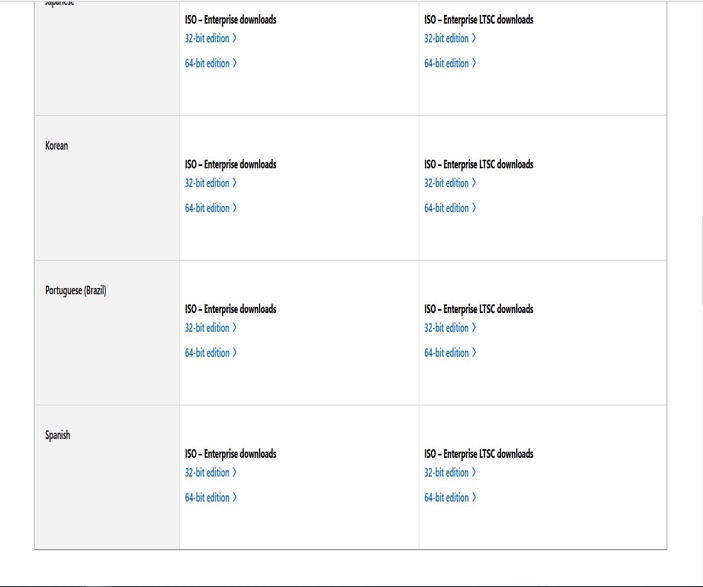


**Fuente:** Elaboración propia

Descargar la imagen ISO de Windows 10 Enterprise de Microsoft:

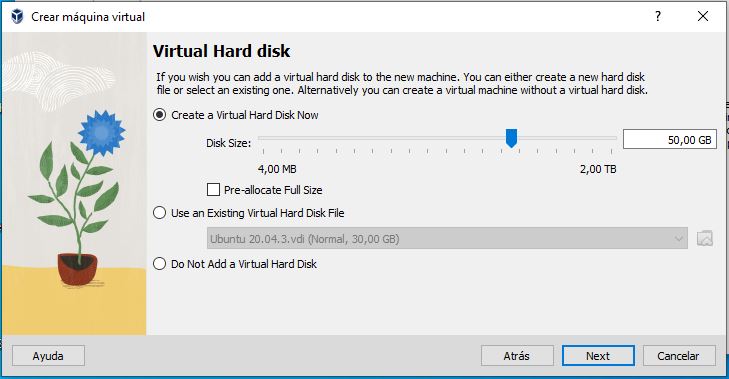
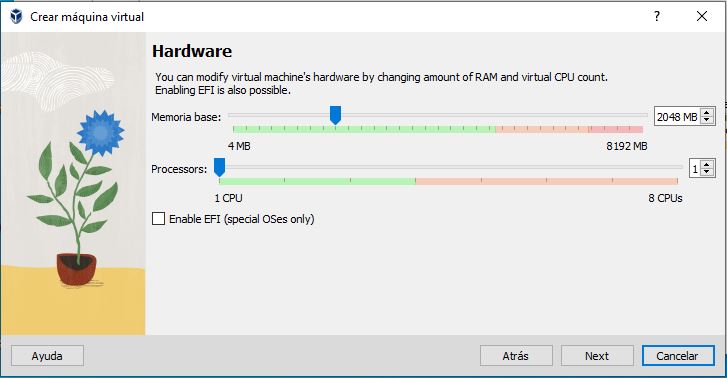
<https://www.microsoft.com/en-us/evalcenter/download-windows-10-enterprise>

En nuestro caso descargaremos la versión de prueba de 64 bit. Dejamos la carpeta por defecto, donde se instalará la máquina virtual.



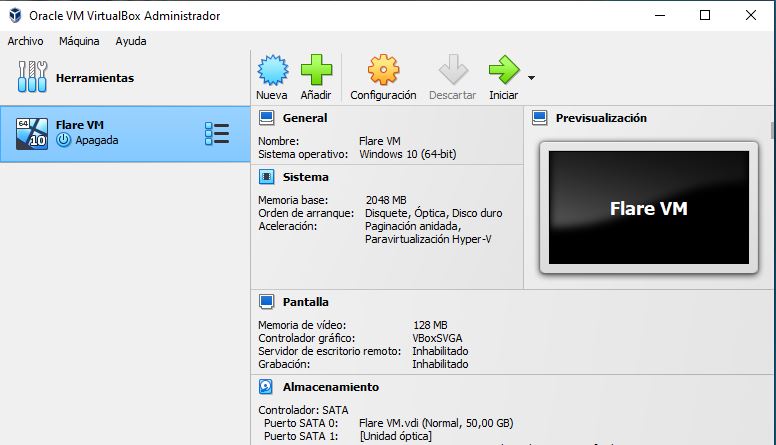
**Fuente:** Elaboración propia

Seleccionamos 2GB de memoria RAM, 1 Procesador, podemos seleccionar 2 procesadores si se tiene la capacidad. Creamos un disco virtual de 50GB.



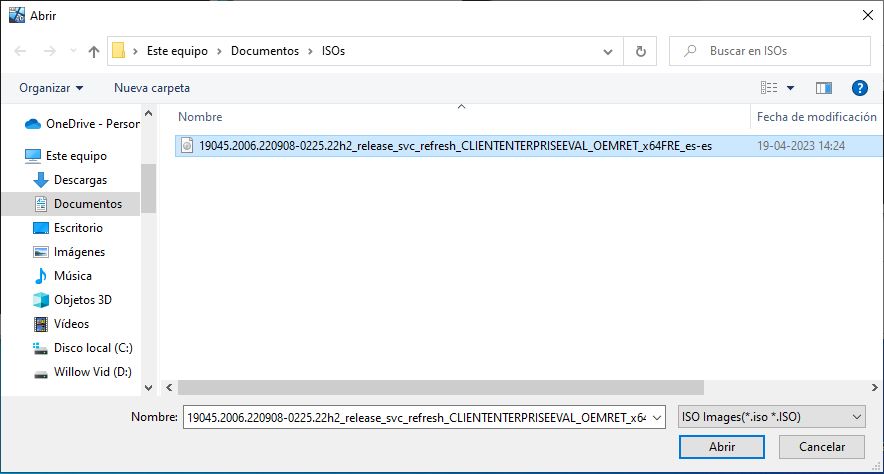
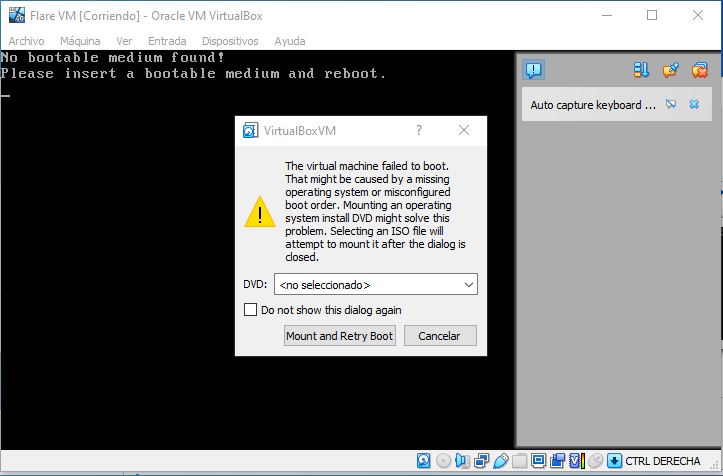
**Fuente:** Elaboración propia

Luego presionamos siguiente y luego crear. Por último, tendremos instalada nuestra máquina virtual corriendo el SO Windows 10, sobre el cual luego instalaremos FlareVM.



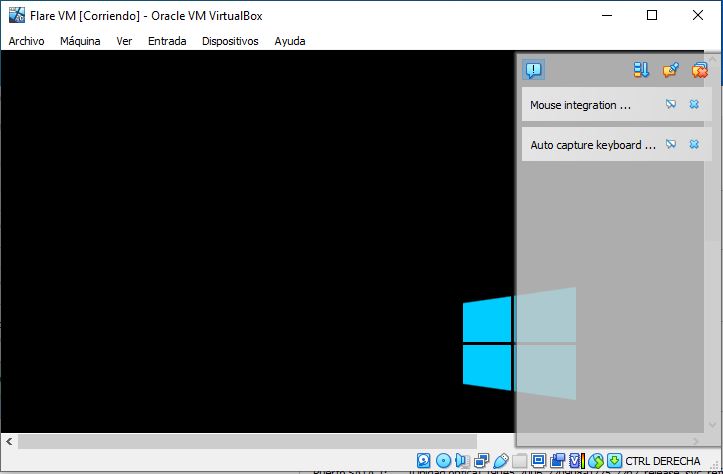
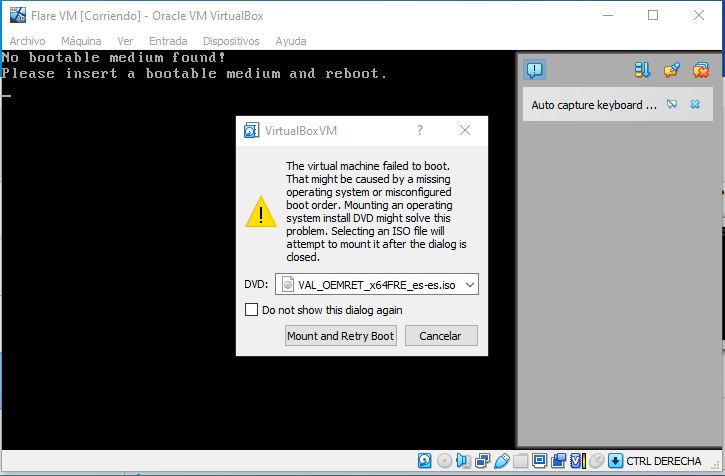
**Fuente:** Elaboración propia

Ahora debemos indicar la ubicación desde donde se arrancará la máquina virtual.



**Fuente:** Elaboración propia

Luego de seleccionar la ISO desde la ruta donde se encuentra el archivo. Seleccionamos “Mount and Retry Boot”.

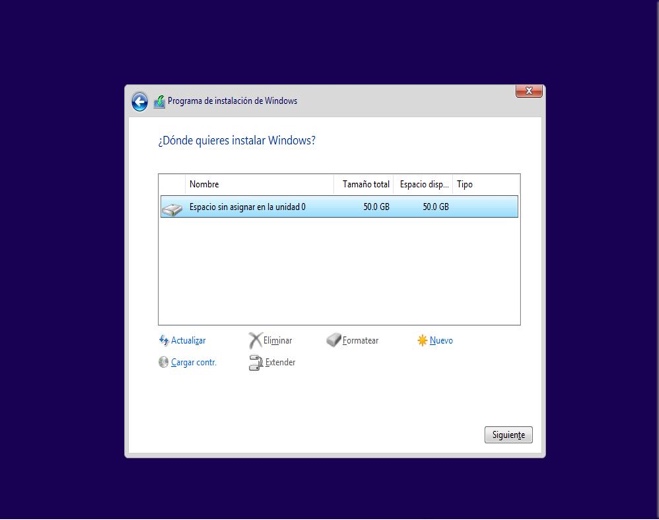
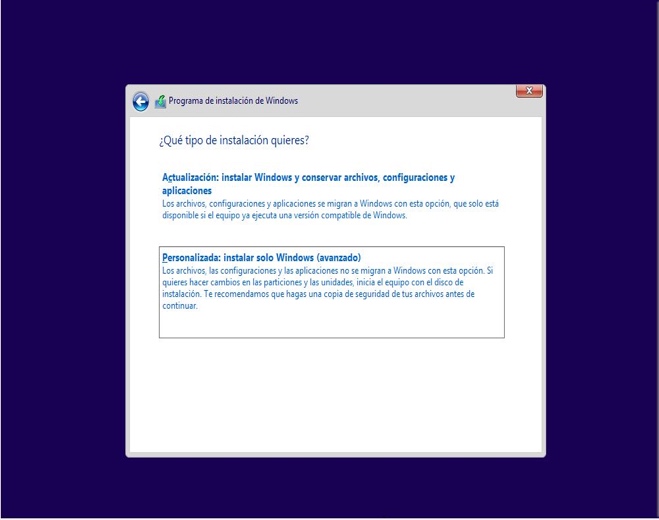
**Fuente:** Elaboración propia

Luego de inicializarse debemos ver la siguiente pantalla, donde seleccionamos el idioma y la configuración del SO Windows 10.



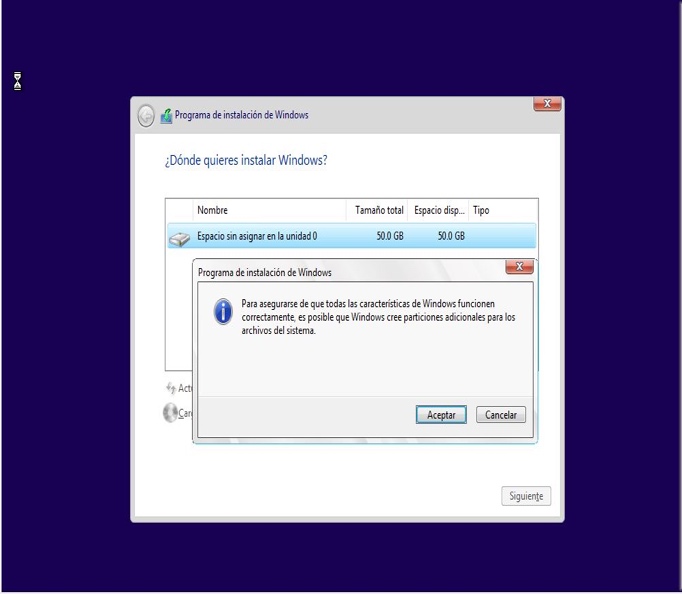
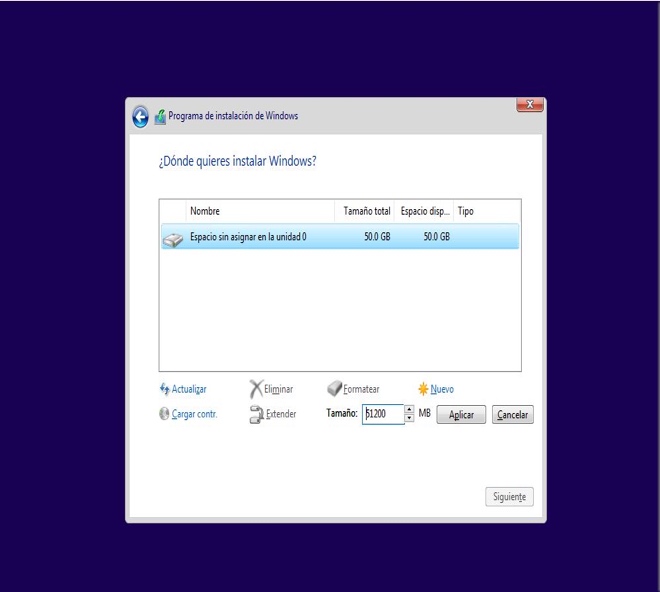
**Fuente:** Elaboración propia

Aceptamos la licencia y luego seleccionamos “Instalación personalizada”. Seleccionamos “New” en “Drive0 Unallocated Space”.



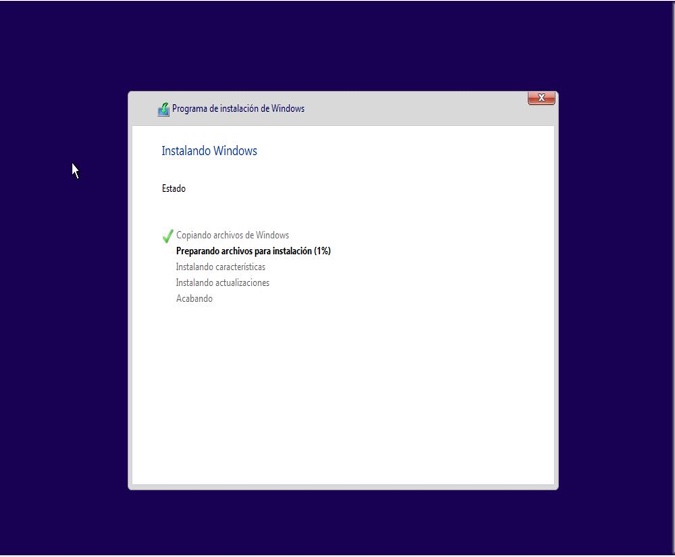
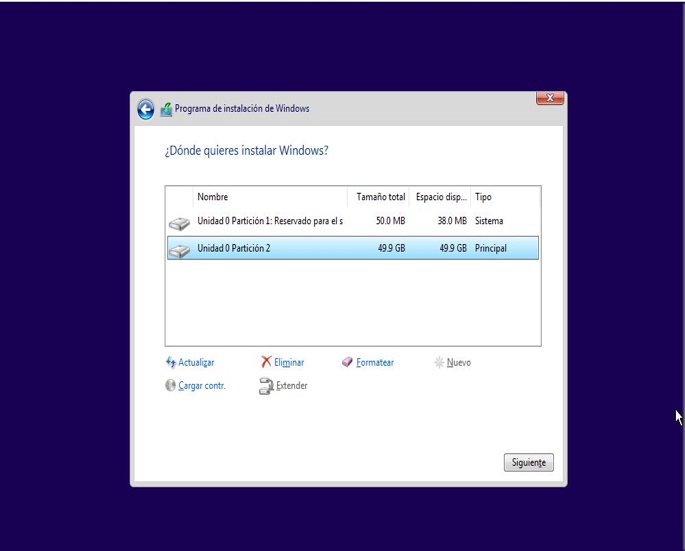
**Fuente:** Elaboración propia

Seleccionamos aplicar, y luego “Aceptar” en la pantalla emergente.



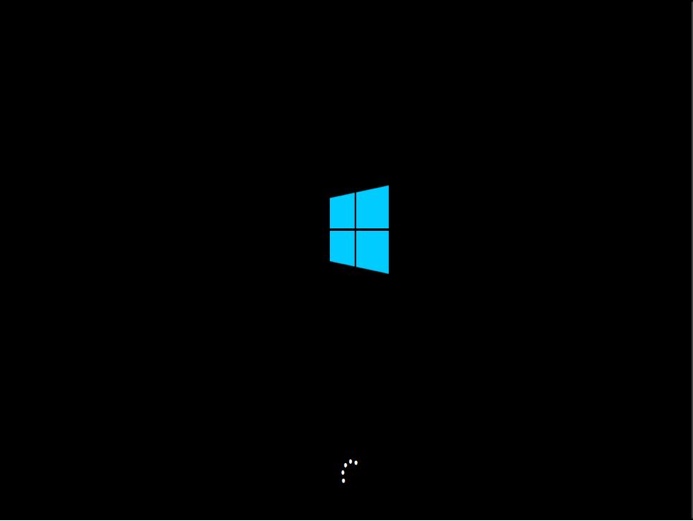
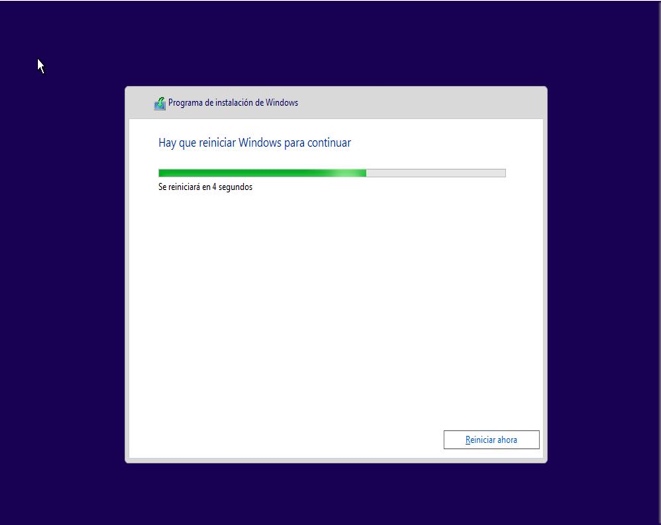
**Fuente:** Elaboración propia

Creará particiones adicionales, luego hacemos clic en “siguiente” y comienza la instalación.



**Fuente:** Elaboración propia

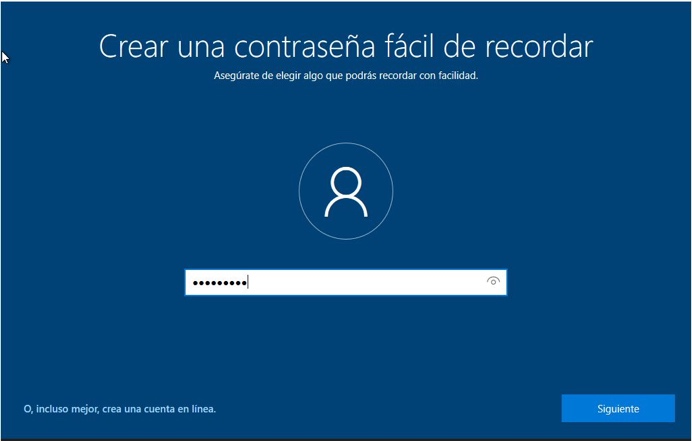
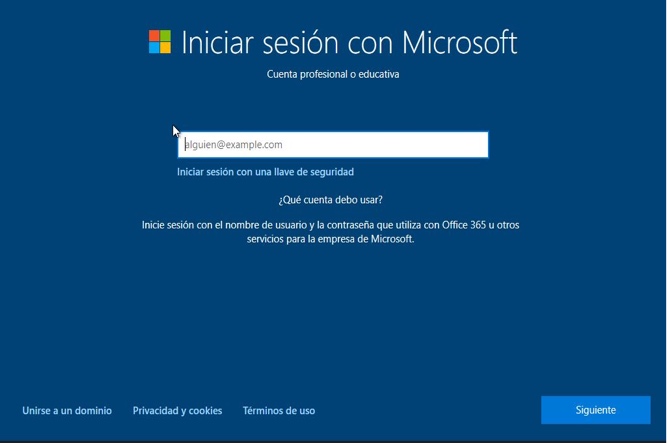
Se comenzará a instalar el SO de la máquina virtual, esto tardará un tiempo para finalizar de ejecutarse. Luego de concluida esta etapa se reiniciará.



**Fuente:** Elaboración propia

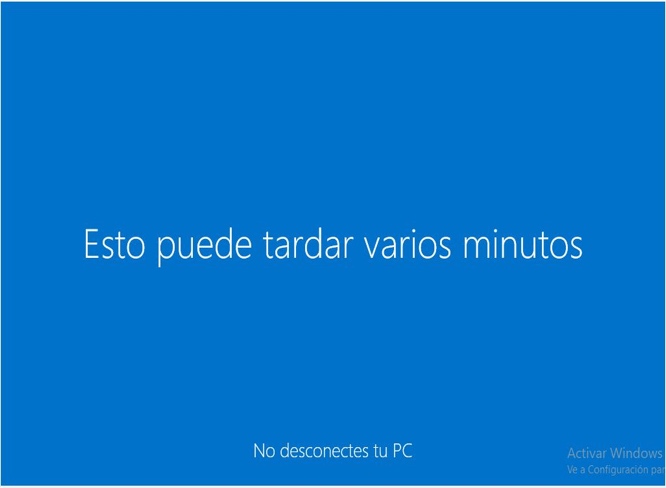
Ahora estamos en la porción de instalación de Windows. Seleccionamos la región donde estamos, en nuestro caso Chile. Seleccionamos también la configuración del teclado. Debemos recordar que esta instalación la realizamos para un laboratorio de Análisis de Malware, a diferencia de un equipo de uso diario.

No necesitamos iniciar sesión con nuestro correo, seleccionamos la opción unirse a un dominio. Agregamos un nombre de usuario, para el cual seleccionamos “Analista”, luego introducimos una contraseña.



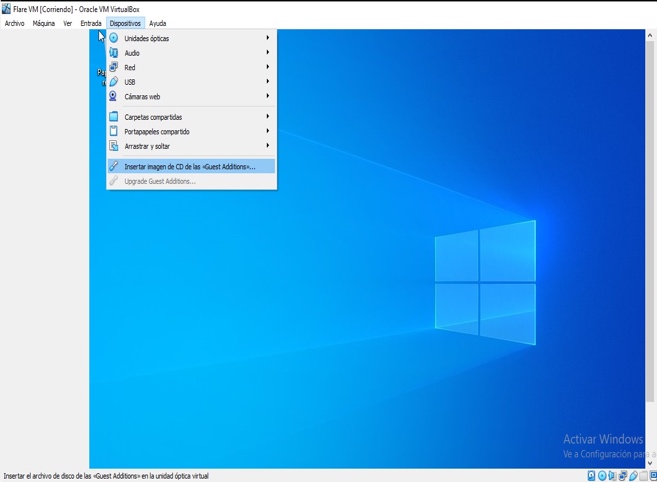
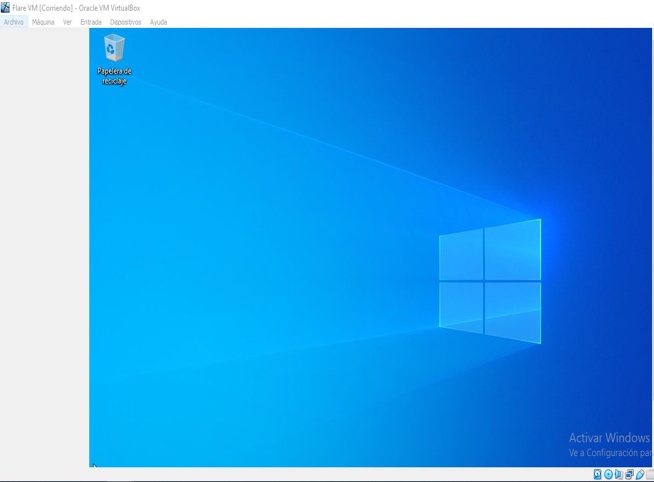
**Fuente:** Elaboración propia

Luego seleccionamos las preguntas de seguridad de recuperación. Pulsamos siguiente luego de llegar a la pantalla donde elegimos la configuración se privacidad para el dispositivo. Aquí seleccionaremos todo en “No”. Por último, pulsamos “Aceptar”.



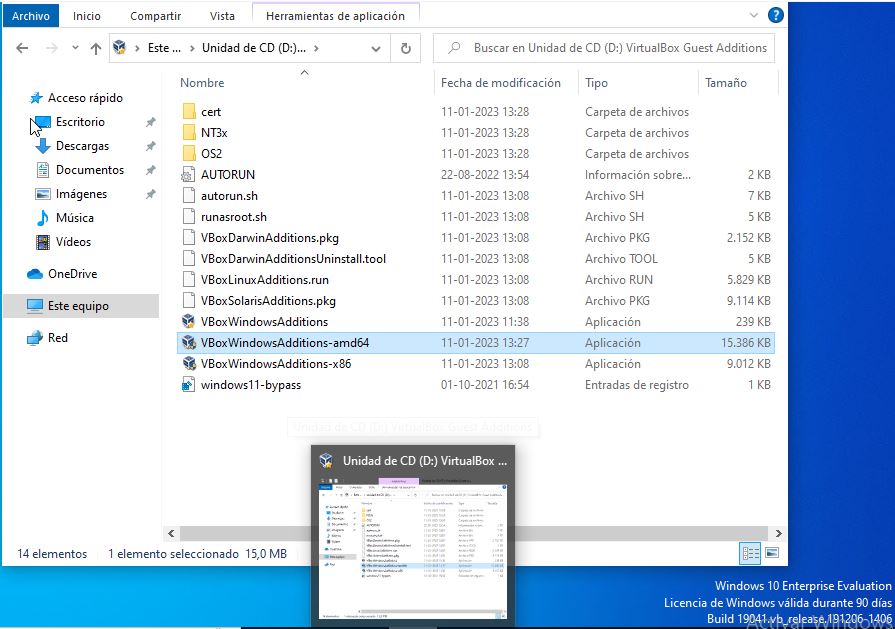
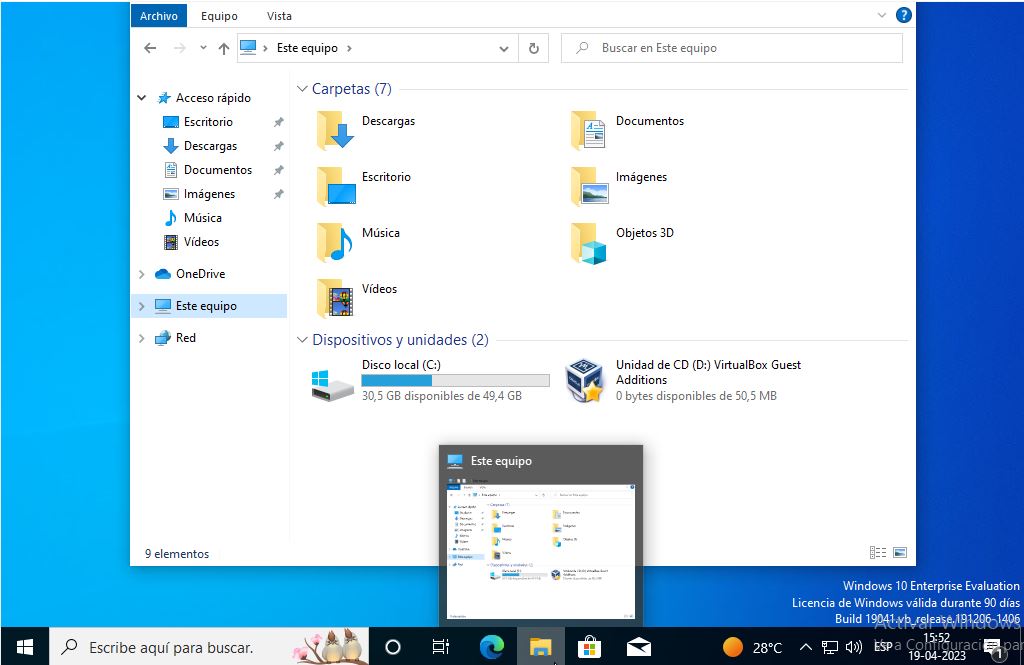
**Fuente:** Elaboración propia

Luego de esperar, cargara el SO Windows 10, y veremos la siguiente pantalla. Para poder hacer que la pantalla de la máquina virtual no se vea pequeña, y podamos agrandarla. Debemos insertar “Guest Additions” imagen de CD. Esto cagara un CD Drive a la máquina virtual.



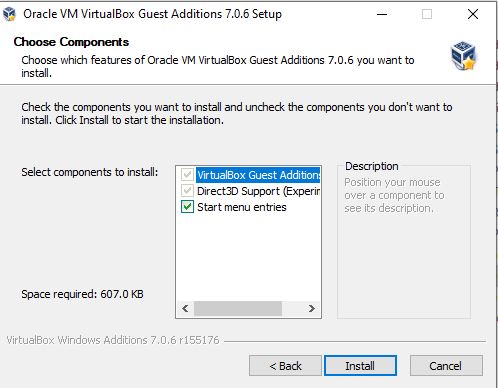
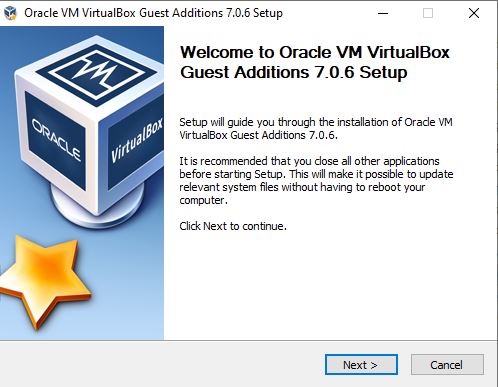
**Fuente:** Elaboración propia

Si vamos a file explorer, este equipo podemos ver “CD Drive (D:) Virtual Box Guest Additions”. Hacemos clic y seleccionamos la opción “Vbox-WindowsAdditions-amd64”.



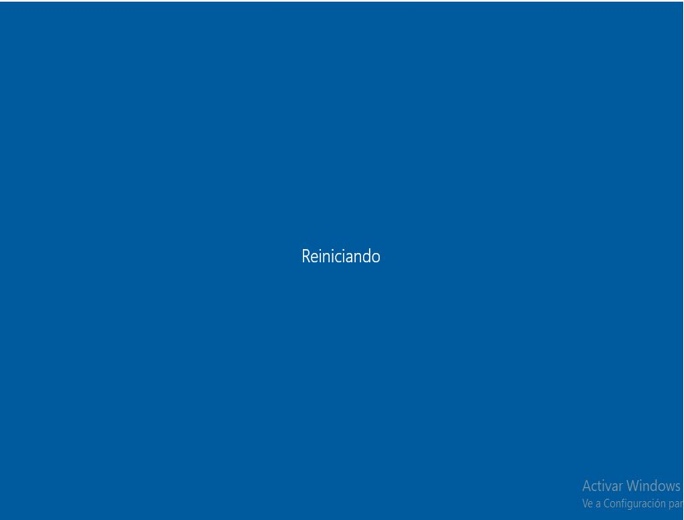
**Fuente:** Elaboración propia

Dejamos todas las opciones predeterminadas haciendo clic en “next”. Luego finalizamos haciendo clic en “Install”.

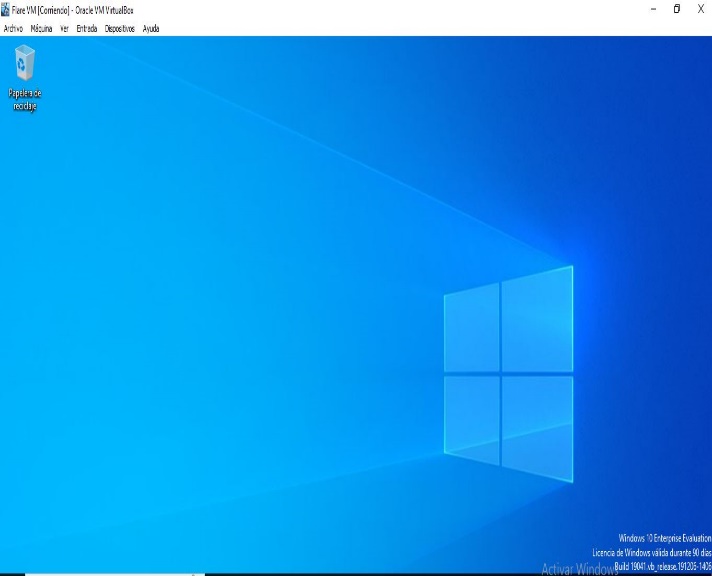
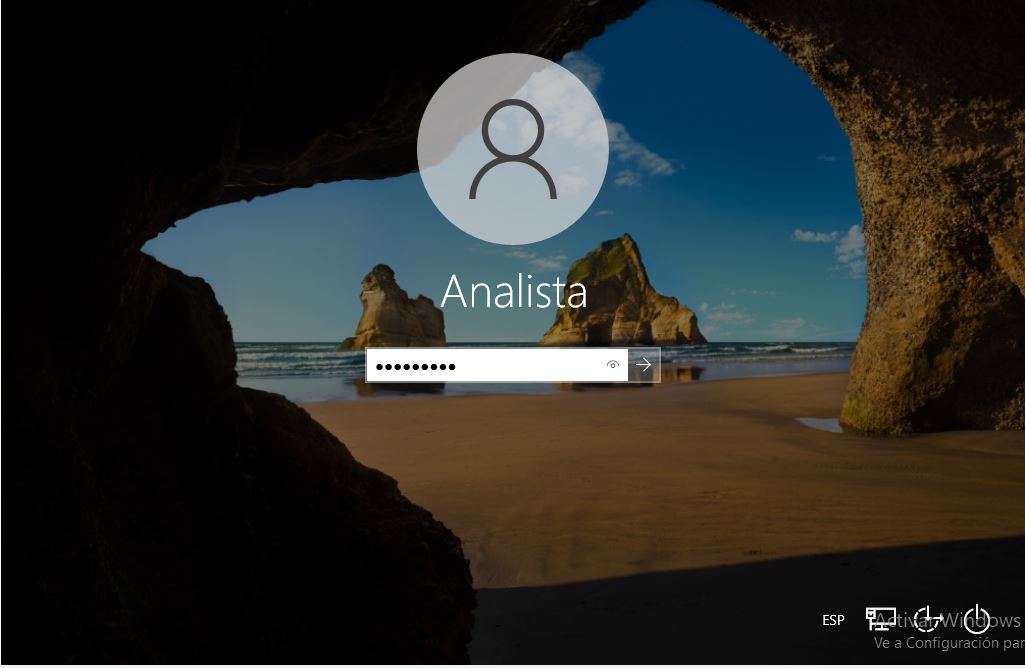


**Fuente:** Elaboración propia

Por último, debemos seleccionar reiniciar el sistema operativo “Reboot now”.

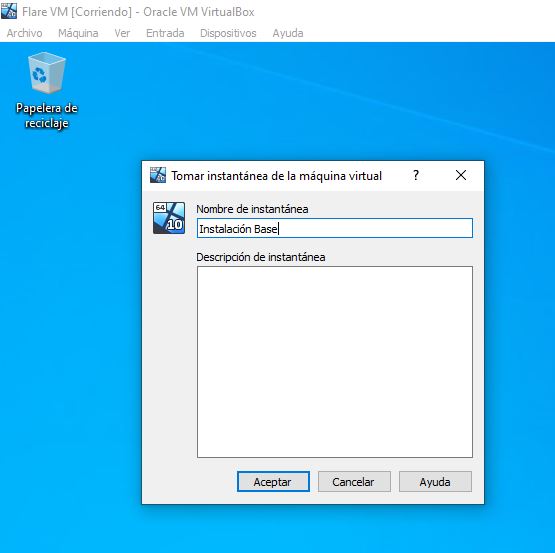
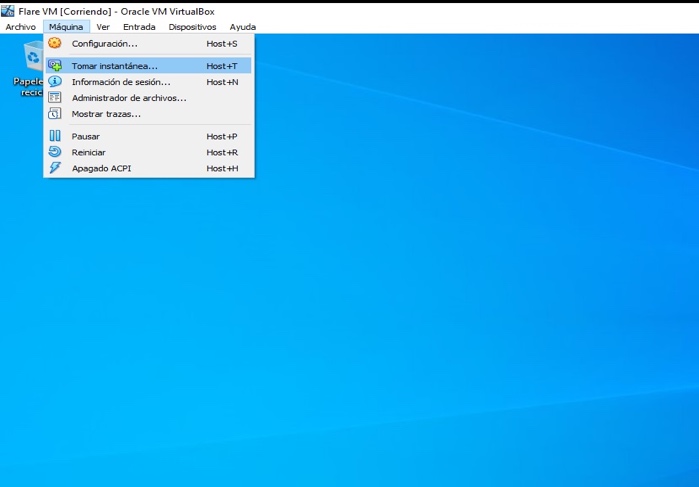
 **Fuente:** Elaboración propia

Las herramientas de la máquina virtual se cargarán como un servicio. Nos pedirá la contraseña de la cuenta. Luego podemos minimizar y volver a expandir la ventana y tendremos la vista en pantalla extendida.



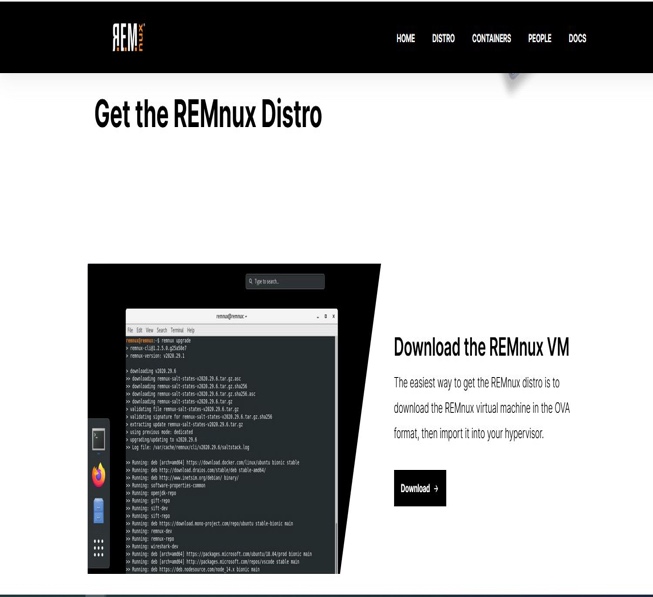
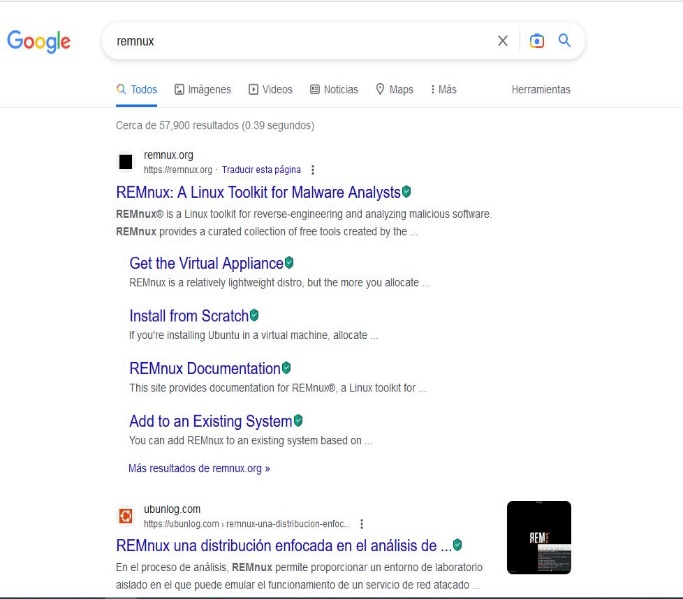
**Fuente:** Elaboración propia

Ahora haremos un paso muy importante. Debemos tomar una instantánea del sistema, ya que luego ejecutaremos malware. La instantánea nos permite volver atrás al estado en que se encontraba la máquina virtual antes de ejecutar el binario.



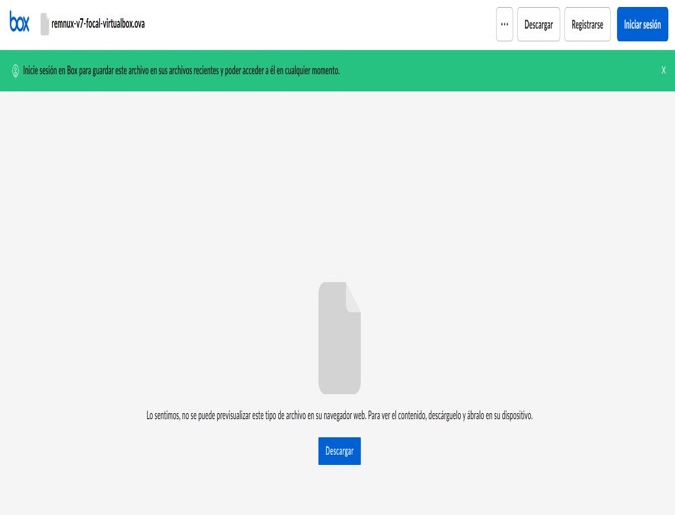
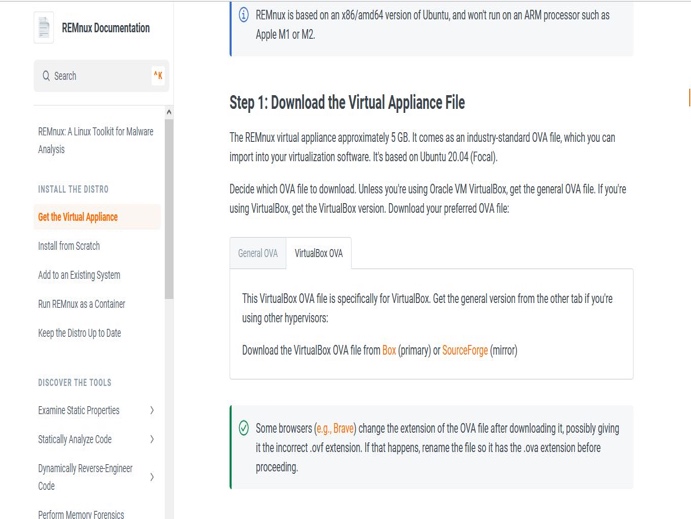
**Fuente:** Elaboración propia

Luego de instalar Flare VM, procederemos a instalar Remnux que es una distribución de Linux especialmente creada para análisis de malware e ingeniería inversa.



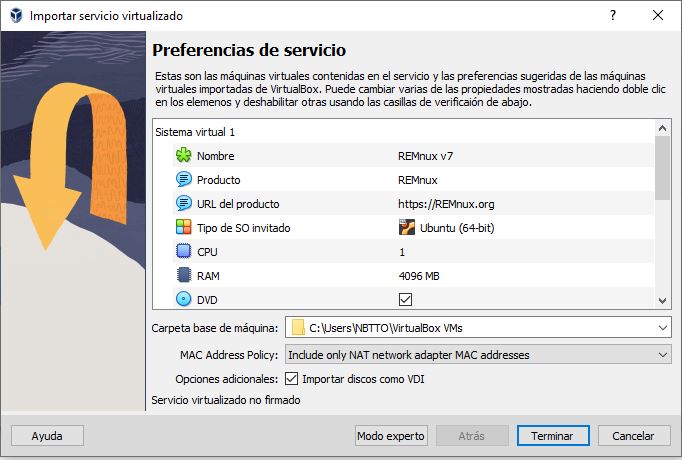
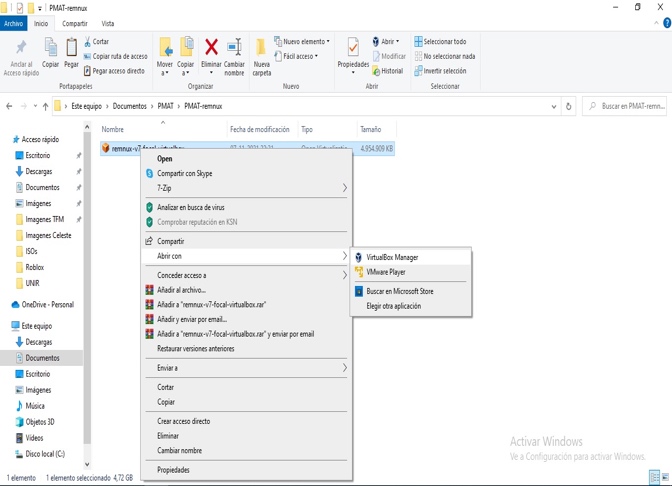
**Fuente:** Elaboración propia

Buscamos la opción de descargar el archivo VirtualBox OVA, lo descargamos de BOX.

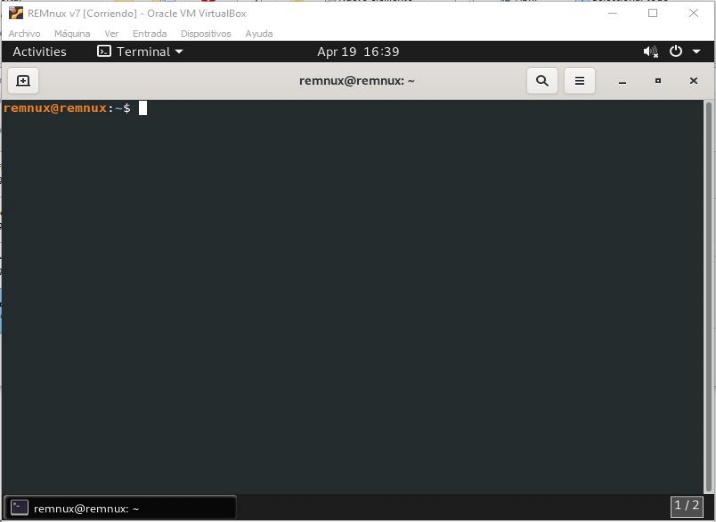
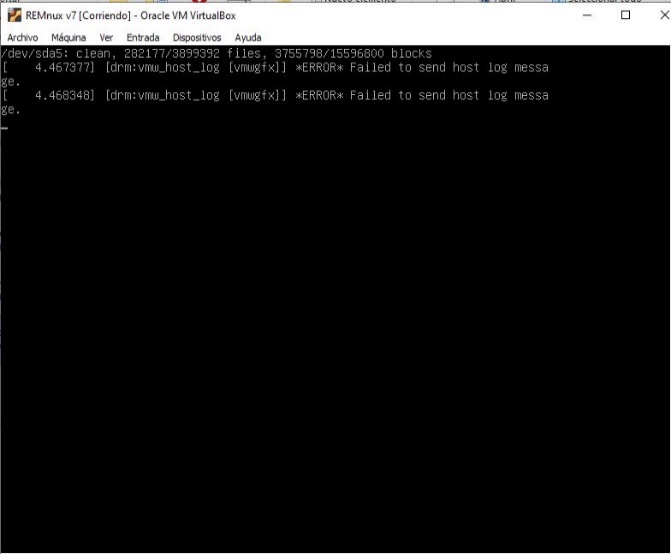


**Fuente:** Elaboración propia

Luego de descargado Remnux lo abriremos con Virtual Box Manager, para importarlo.

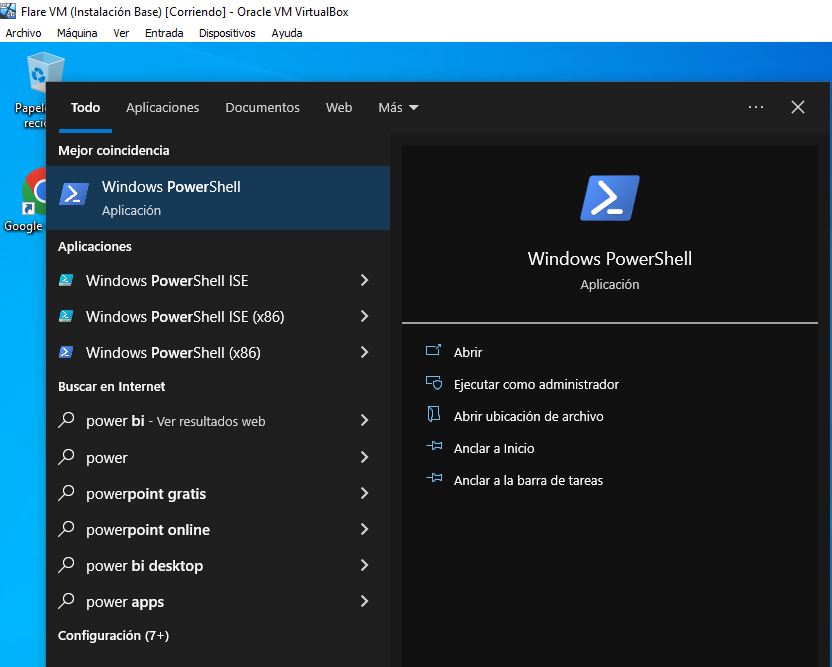
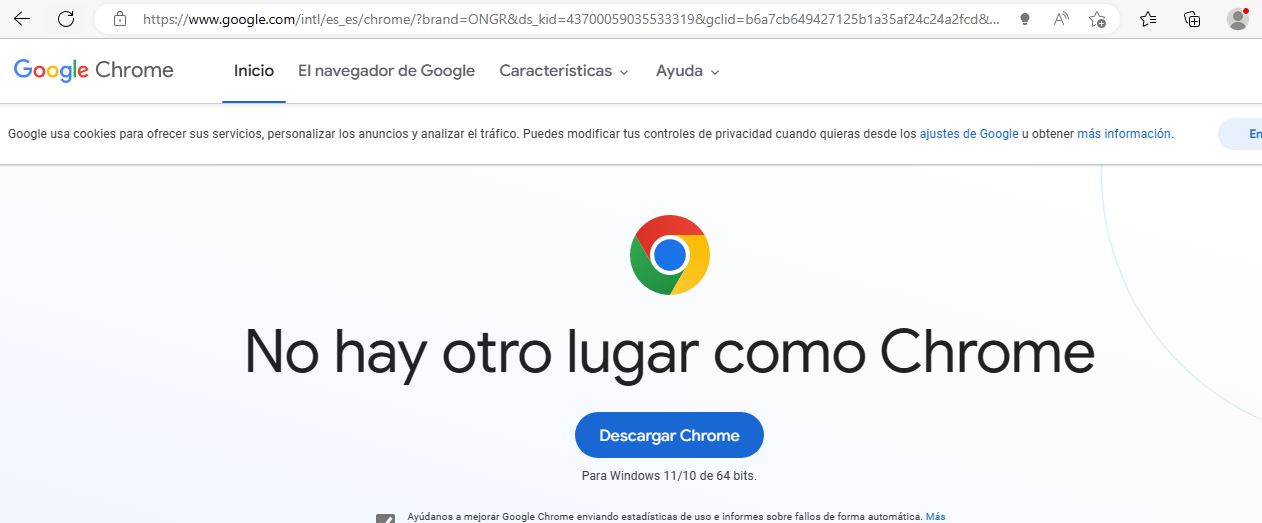
 **Fuente:** Elaboración propia

Al finalizar la importación, comenzamos la máquina virtual.



**Fuente:** Elaboración propia

Descargamos el navegador Chrome. Luego abrimos una terminal de Power Shell como administrador.



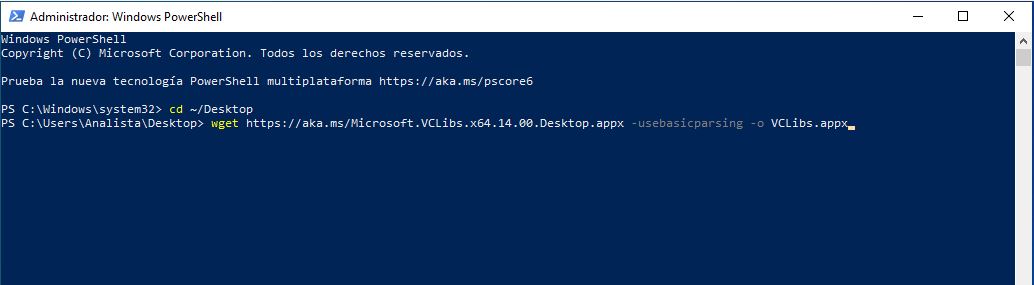
**Fuente:** Elaboración propia

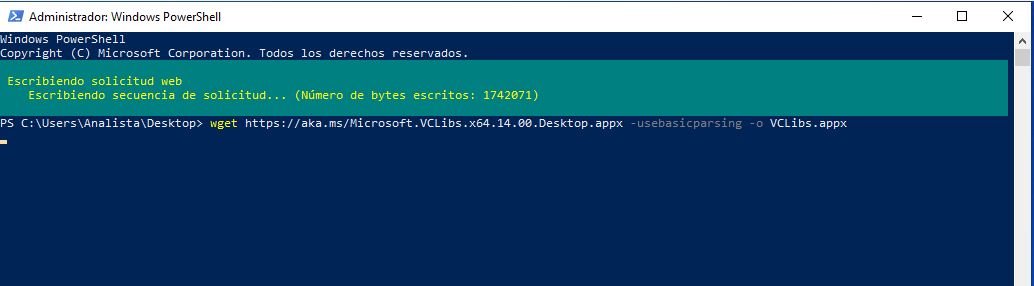
Antes de instalar Flare VM, procedemos a hacer una descarga de algunas herramientas.

Descargar Chrome: [https://www.google.com/chrome/](https://www.google.com/chrome)

Descargar Windows Terminal:

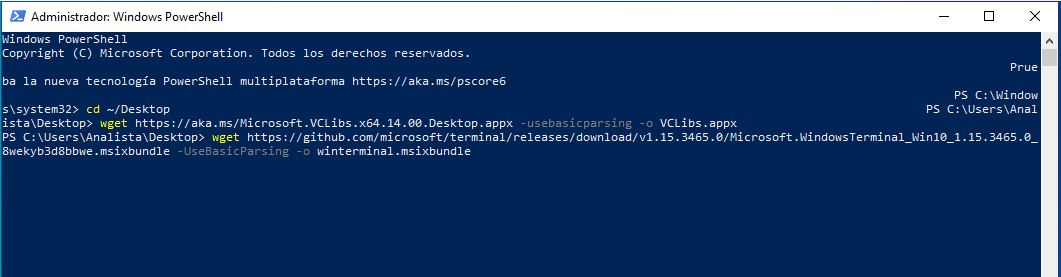
Descargar VCLibs package. En una terminal de PowerShell window, correr: wget https://aka.ms/Microsoft.VCLibs.x64.14.00.Desktop.appx -usebasicparsing -o VCLibs.appx

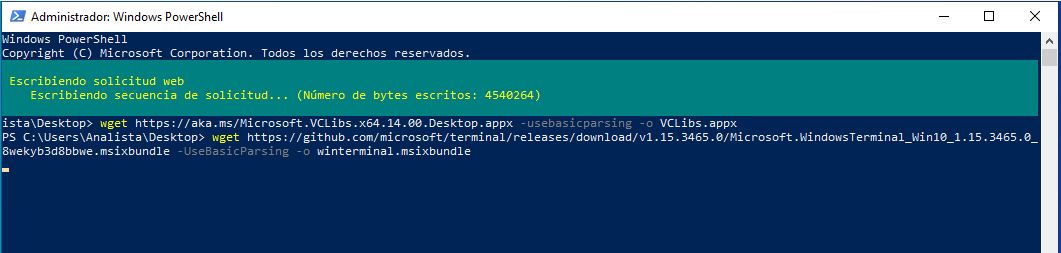




**Fuente:** Elaboración propia

Descargar Windows Terminal MSIX bundle Del siguiente link: wget https://github.com/microsoft/terminal/releases/download/v1.15.3465.0/Microsoft.WindowsTerminal\_Win10\_1.15.3465.0\_8wekyb3d8bbwe.msixbundle -UseBasicParsing -o winterminal.msixbundle





**Fuente:** Elaboración propia

En el terminal de PowerShell, agregar VCLibs package: Add-AppxPackage .\VCLibs.appx

En el terminal de PowerShell, correr: Add-AppxPackage .\winterminal.msixbundle

Deshabilitar en el proxy el auto detectar:

En la Ventana de búsqueda de Windows, escribir “Configuración del proxy”,

Desactivar "Detectar Automáticamente"

Desactivar Protección

Buscar "Defender", abrir Defender y apagarlo.

Desactivar AV/Defender en GPO

En la barra de búsqueda de Windows, buscar "Editar directiva de grupo"

En GPO, navegar hacia → Plantillas Administrativas → Componentes de Windows → Antivirus de Microsoft Defender → Habilitar “Apagar Microsoft Defender Antivirus”

Deshabilitar el Firewall de Windows

GPO → Plantillas Administrativas → Network → Conexiones de red → Firewall de Windows Defender → Perfil de Dominio → Deshabilitar “Proteger todas las redes”

Hacer lo mismo para el perfil estándar.

¡Tomar una instantánea!

Descargar e instalar FLARE-VM:

En PowerShell correr: (New-Object net.webclient).DownloadFile('https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1',"$([Environment]::GetFolderPath("Desktop"))\install.ps1")

Cambiar de directorio a escritorio

Correr: Unblock-File .\install.ps1

Correr: Set-ExecutionPolicy Unrestricted

Aceptar el prompt para cambiar la ExecPol a unrestricted.

Correr: .\install.ps1 -customConfig https://raw.githubusercontent.com/HuskyHacks/PMAT-labs/main/config.xml

Sigue el resto de las ventanas emergentes para finalizar con la instalación.

Cuando la instalación termine toma otra instantánea.

**Instalación de herramientas adicionales en Flare VM.**

Luego de instalado FlareVM, instalaremos las siguientes herramientas adicionales las cuales no vienen incluidas por defecto en la versión de FlareVM que hemos instalado.

Process Hacker es un visor de procesos gratuito y de código abierto. Esta herramienta multiusos es muy útil con la depuración, detección de malware y monitorización del sistema.

Características:

* Visión clara de los procesos en ejecución y el uso de recursos
* Información detallada del sistema y gráficos
* Visualiza y edita servicios
* Otras funciones útiles para depurar y analizar software

La herramienta puede ser descargada del siguiente enlace:

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

La segunda herramienta que instalaremos es Process Dump. Es una herramienta de línea de comandos de ingeniería inversa de Windows para volcar componentes de memoria de malware al disco para su análisis. A menudo, los archivos de malware se empaquetan y ofuscan antes de ejecutarse para evitar los escáneres antivirus. Sin embargo, cuando estos archivos se ejecutan, suelen desempaquetar o inyectar una versión limpia del código malicioso en la memoria. Una tarea común para los investigadores de malware cuando analizan malware es volcar este código desempaquetado de la memoria al disco para escanearlo con productos AV o para analizarlo con herramientas de análisis estático como IDA.

Process Dump funciona para sistemas operativos Windows de 32 y 64 bits y puede volcar componentes de memoria de procesos específicos o de todos los procesos que se estén ejecutando en ese momento. Process Dump admite la creación y el uso de una base de datos clean-hash, de modo que se puede omitir el volcado de todos los archivos limpios, como kernel32.dll.

Sus principales características son:

* Vuelca el código de un proceso específico o de todos los procesos.
* Encuentra y vuelca módulos ocultos que no están correctamente cargados en los procesos.
* Encuentra y vuelca trozos de código sueltos incluso si no están asociados a un archivo PE.
* Construye una cabecera PE y una tabla de importación para los trozos.
* Reconstruye las importaciones utilizando un enfoque agresivo.
* Puede ejecutarse en modo de monitorización de volcado cerrado ('-closemon'), donde los procesos se pausarán y volcarán justo antes de que terminen.
* Es multihilo, por lo que cuando se vuelcan todos los procesos en ejecución se hace bastante rápido.
* Puede generar una base de datos hash limpia. Genere esto antes de que una máquina sea infectada con malware para que Process Dump sólo vuelque los nuevos componentes maliciosos del malware.

Se puede descargar del siguiente repositorio en github:

<https://github.com/glmcdona/Process-Dump>

La tercera herramienta es HxD es un editor hexadecimal rápido y cuidadosamente diseñado que, además de la edición en disco en bruto y la modificación de la memoria principal (RAM), maneja archivos de cualquier tamaño.

La interfaz fácil de usar ofrece funciones como buscar y reemplazar, exportar, sumas de comprobación/dígitos, inserción de patrones de bytes, un triturador de archivos, concatenación o división de archivos, estadísticas y mucho más.

Las unidades y la memoria pueden editarse del mismo modo que un archivo normal, incluida la posibilidad de deshacer. Además, las secciones de memoria definen una región plegable y las secciones inaccesibles se ocultan por defecto.

Además, se ha hecho un gran esfuerzo para que las operaciones sean rápidas y eficientes, en lugar de obligarle a utilizar funciones especializadas por razones técnicas o limitar arbitrariamente el tamaño de los archivos. Esto incluye una interfaz sensible e indicadores de progreso para operaciones largas.

Se puede descargar del siguiente enlace:

<https://mh-nexus.de/en/downloads.php?product=HxD20>

La cuarta herramienta es PE Explorer, es el programa con más funciones para inspeccionar el funcionamiento interno de su propio software y, lo que es más importante, de aplicaciones y bibliotecas de Windows de terceros para las que no dispone de código fuente. Una vez que haya seleccionado el archivo que desea examinar, PE Explorer analizará el archivo y mostrará un resumen de la información del encabezado PE, y todos los recursos contenidos en el archivo PE. A partir de aquí, la herramienta le permite explorar los elementos específicos dentro de un archivo ejecutable.

Además de ser un eficaz Editor de Recursos, PE Explorer también proporciona varias herramientas que lo elevan a la categoría de Power Coder: una Búsqueda de Sintaxis de Funciones API, un Explorador de Dependencias, un Editor de Secciones y un Desensamblador potente pero fácil de usar para generar volcados de código anotados. PE Explorer está pensado para ser utilizado en varios escenarios como el desarrollo de software, prácticas forenses, ingeniería inversa, análisis de seguridad binaria extensivos y procesos de auditoría binaria, lo que sea. Con PE Explorer, puede ver, examinar y editar archivos EXE y DLL, o corregir y reparar las estructuras internas de cualquier PE (portable executable) archivos con el clic de un botón.

Se puede descargar del siguiente enlace:

<http://www.pe-explorer.com/>

La quinta herramienta es Resource Hacker, un editor de recursos para aplicaciones Windows® de 32 y 64 bits. Es tanto un compilador de recursos (para archivos \*.rc), como un descompilador - permitiendo la visualización y edición de recursos en ejecutables (\*.exe; \*.dll; \*.scr; etc) y bibliotecas de recursos compilados (\*.res, \*.mui). Aunque Resource Hacker™ es principalmente una aplicación GUI, también ofrece muchas opciones para compilar y descompilar recursos desde la línea de comandos.

Se puede descargar del siguiente enlace:

<http://www.angusj.com/resourcehacker/>

La sexta herramienta es CyberChef, una aplicación web sencilla e intuitiva para realizar todo tipo de operaciones "cibernéticas" dentro de un navegador web. Estas operaciones incluyen codificaciones sencillas como XOR y Base64, codificaciones más complejas como AES, DES y Blowfish, creación de volcados binarios y hexadecimales, compresión y descompresión de datos, cálculo de hashes y sumas de comprobación, análisis sintáctico de IPv6 y X.509, cambio de codificaciones de caracteres y mucho más.

La herramienta está diseñada para que los analistas, tanto técnicos como no técnicos, puedan manipular datos de forma compleja sin tener que lidiar con herramientas o algoritmos complejos. Fue concebida, diseñada, construida y mejorada incrementalmente por un analista en su 10% de tiempo de innovación a lo largo de varios años.

Se puede acceder a la herramienta a través del siguiente enlace:

<https://gchq.github.io/CyberChef/>

Se puede también acceder al repositorio de Github con el siguiente enlace:

<https://github.com/gchq/CyberChef>

La séptima herramienta es ExEinfo PE, es un software que permite examinar los archivos .exe y ver sus propiedades, así como realizar ediciones en cualquier archivo ejecutable de Windows. Puedes cambiar o editar el nombre del archivo, simplemente abre el .exe o bórralo. **Exeinfo PE** también le permite ver el tamaño así como el tamaño de otros archivos dentro del ejecutable.

Se puede descargar del siguiente enlace:

<https://github.com/ExeinfoASL/ASL>

La octava herramienta es Gmer, una aplicación que detecta y elimina rootkits.

Escanea en busca de:

* procesos ocultos
* hilos ocultos
* módulos ocultos
* servicios ocultos
* archivos ocultos
* Sectores de disco ocultos (MBR)
* flujos de datos alternativos ocultos
* claves de registro ocultas
* controladores SSDT
* controladores que enganchan IDT
* controladores que enganchan llamadas IRP
* ganchos en línea

Se puede descargar del siguiente enlace:

<http://www.gmer.net/>