Práctica 3: Antivirus LIVE

Vamos a probar una antivirus en versión de arranque o una version en ISO. Que sencillamente es como una unidad que es capaz de iniciarse por si sola para poder leer la unidad infectada.

Como anteriormente describes en la practica hay virus que son capaces de detectar la presencia o los procesos de los típicos antivirus. Entonces este es capaz de detenerse y así evitar ser detectado.

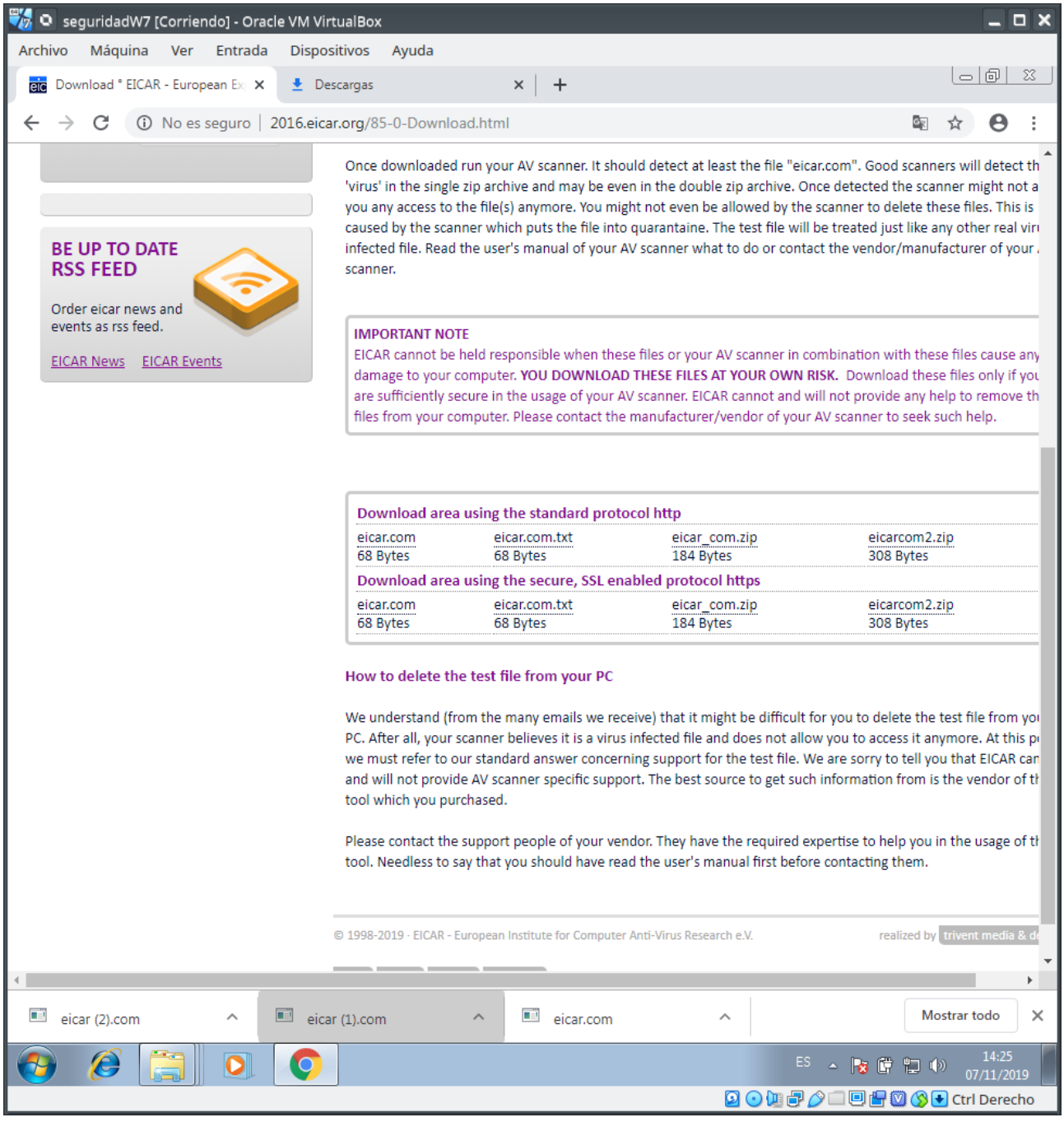
En la practica la vamos hacer muy vulgar y vamos a tirar de imaginación. Primeramente con una maquina virtual con Windows 7 descargaremos el virus de muestra Eicar. Este virus en cuestión seria tan fácil como pasar el antivirus con el sistema en marcha y seria detectado al instante.

Por eso de la imaginación, es un virus muy puñetero y nos ha inutilizado la unidad que esta ahora no es capaz de encender. También podemos ser desconfiados y pasar el “antivirus ISO” para comprobar que no tengamos un virus indetectables cuando el sistema este en marcha.

Antes de seguir quiero puntualizar algo, recordar que este tipo de antivirus tiene un problema. Al ser un archivo descargado o instalado no es actualizable. Solo tendrá una base de datos de virus hasta la fecha de su creación, desconozco si el propio programa sera capaz de realizar una conexión a Internet para poderse actualizar. Pero vamos sera buena idea de si lo vamos a utilizar no usar uno que tengamos por el cajón y descargarlo recientemente.

Práctica 3: Antivirus LIVE

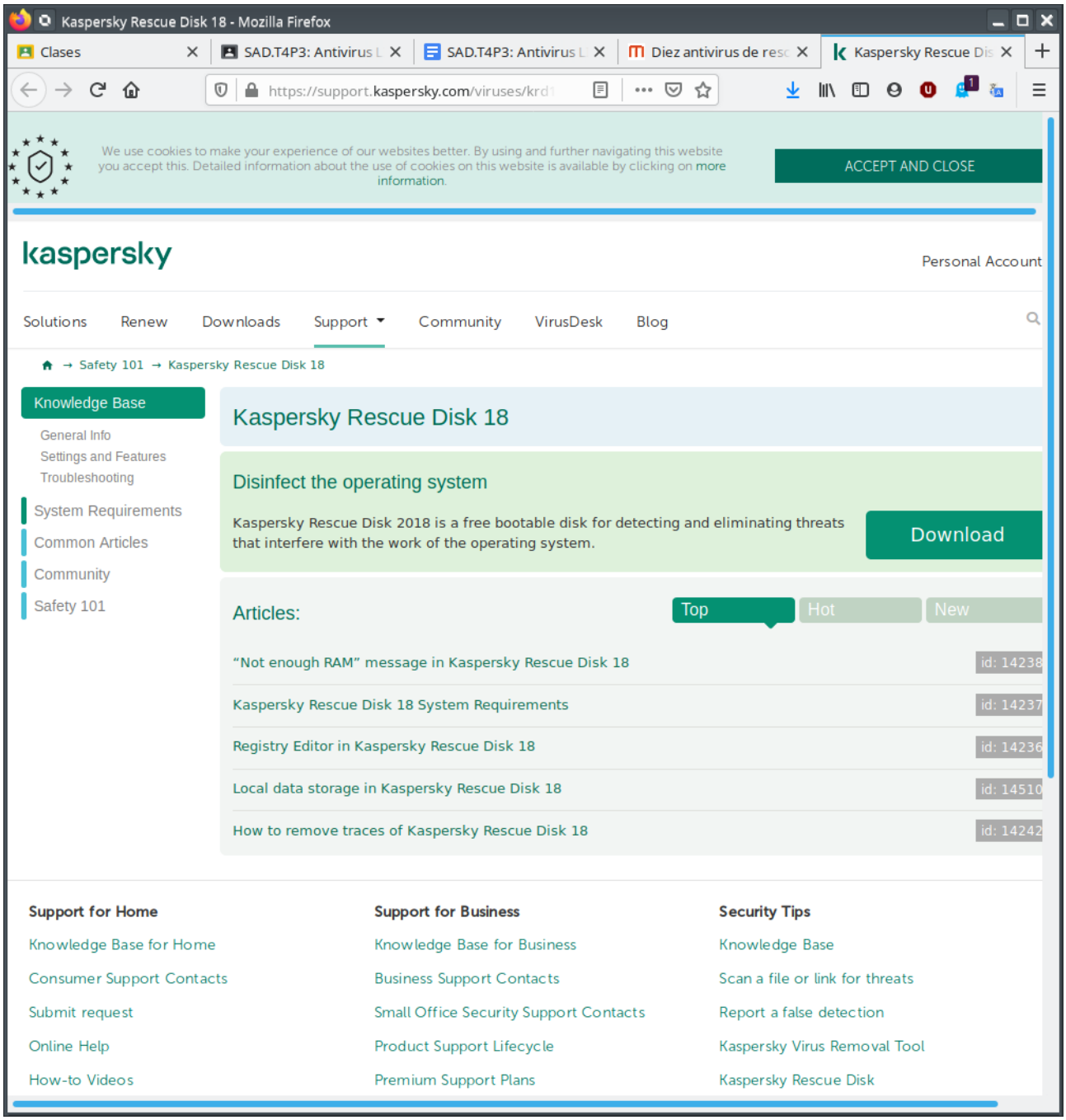
Descargamos Eicar en la maquina de W7



Ya contiene el virus entonces vamos apagarla para después arrancar desde la ISO.

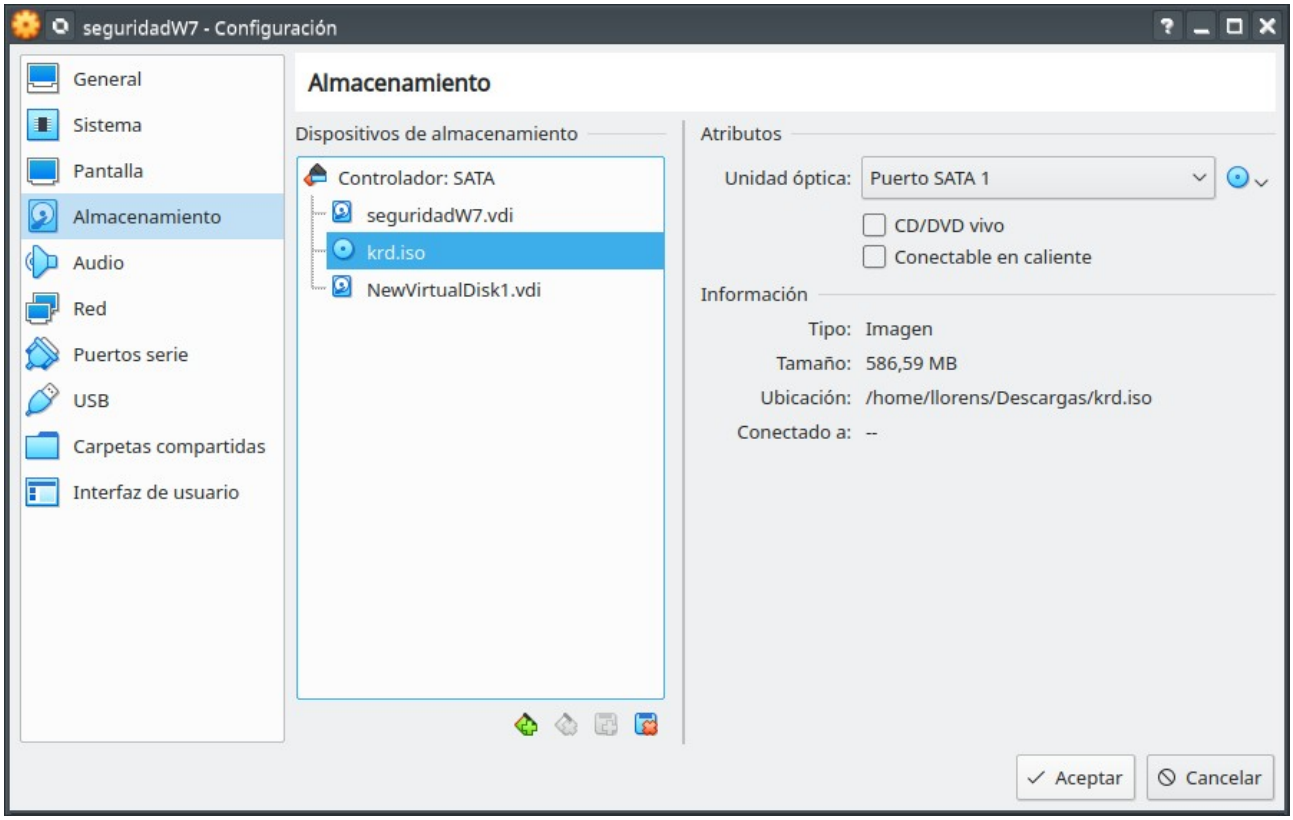
Práctica 3: Antivirus LIVE

Ahora descargaremos la ISO que en esta ocasión seleccione la primera que es Kaspersky Rescue Disk 18



Después si fuera una maquina real deberíamos preparar una memoria USB o quemar un CD/DVD con la ISO.

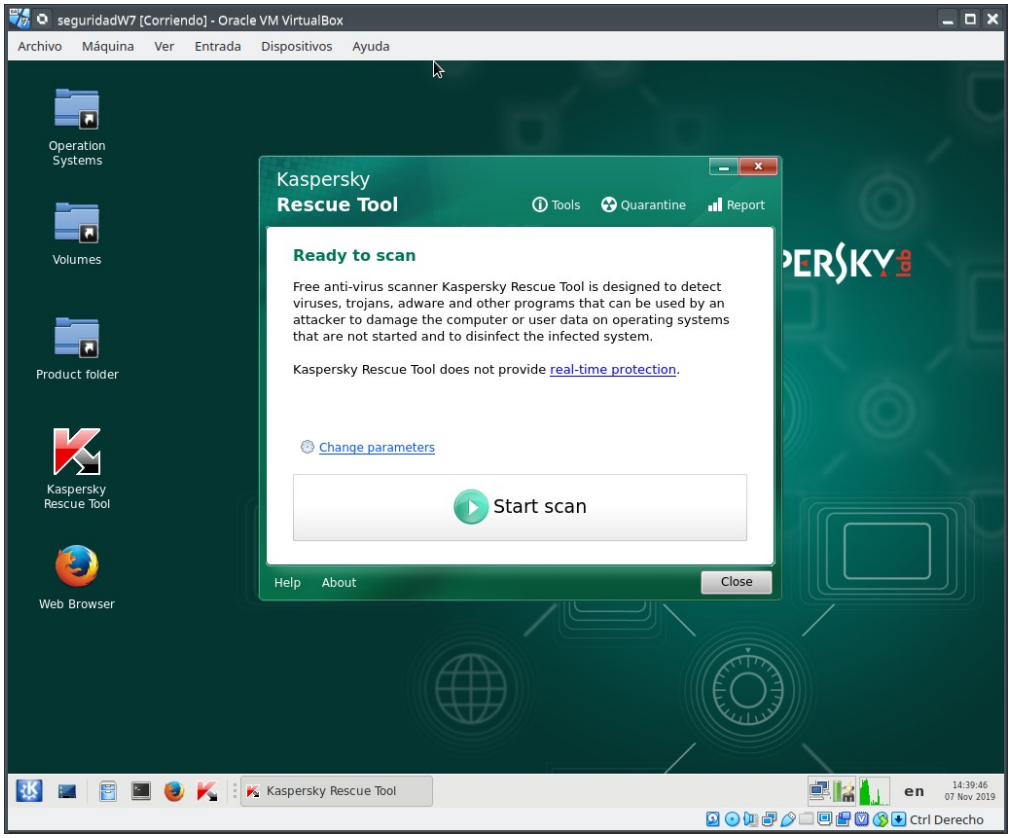
Práctica 3: Antivirus LIVE



Como se muestra en la captura de arriba seleccionamos la ISO y encendemos la maquina.

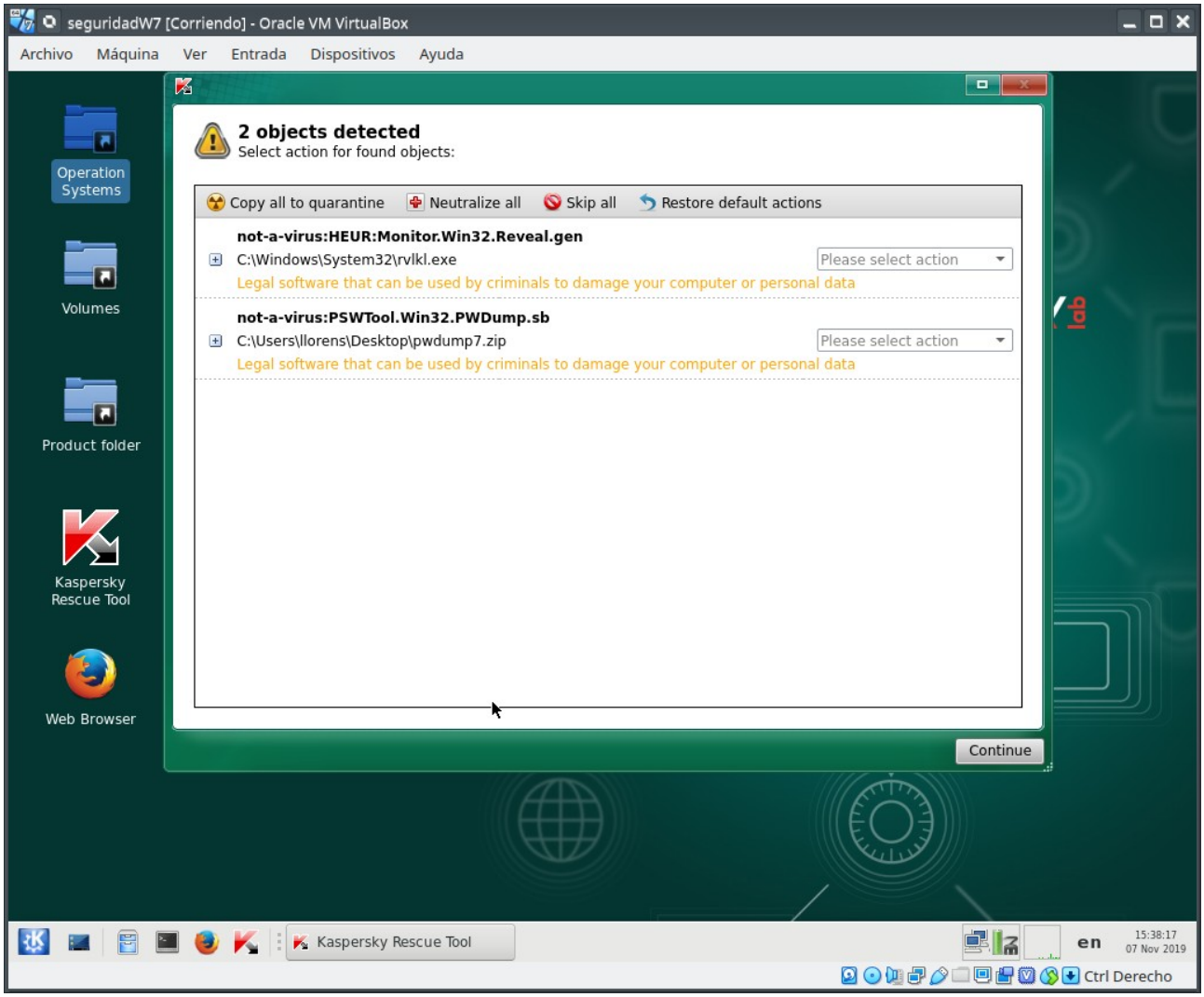
Práctica 3: Antivirus LIVE

Después de aceptar los términos de uso, etc. Aparecerá el antivirus



Pulsamos “Start Scan” y esperamos a ver si encuentra algo

Práctica 3: Antivirus LIVE



Curiosamente el virus que yo mencione no lo encontró, pero si que encontró 2 que si que conozco (no se si estaré en lo cierto)

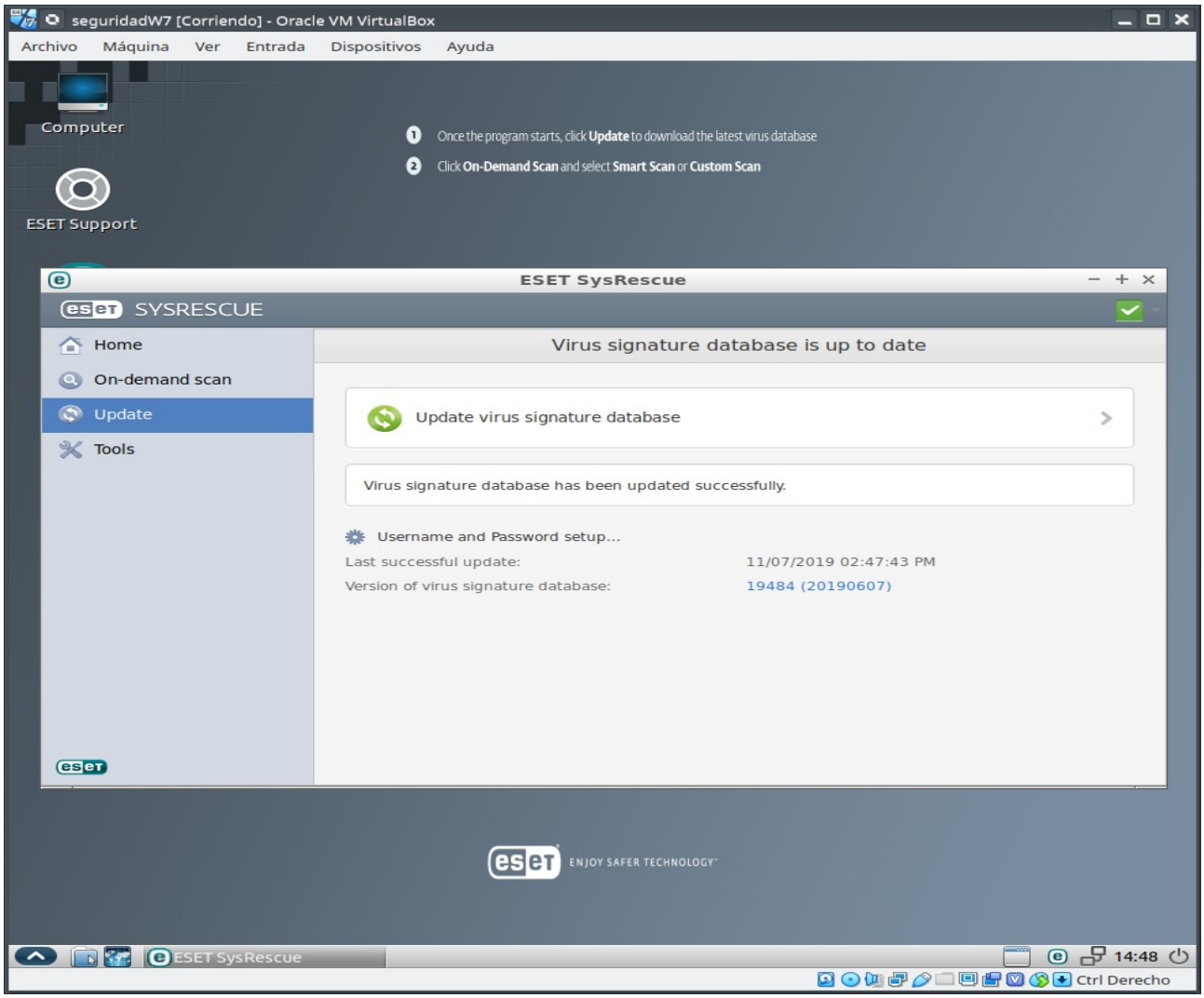
El primero es un un parche para validar Windows, normalmente estos tipos activadores como nada en la vida es gratis. Suelen usarlo para que tu maquina sea una de las tantas que tienen para realizar ataques Ddos para tumbar webs, servicios, etc.

Y el segundo es Pwdump de la practicas anteriores que lo detecta como virus, pero simplemente es para poder descifrar contraseñas de Windows.

Voy a probar otra ISO a ver si lo detecta….

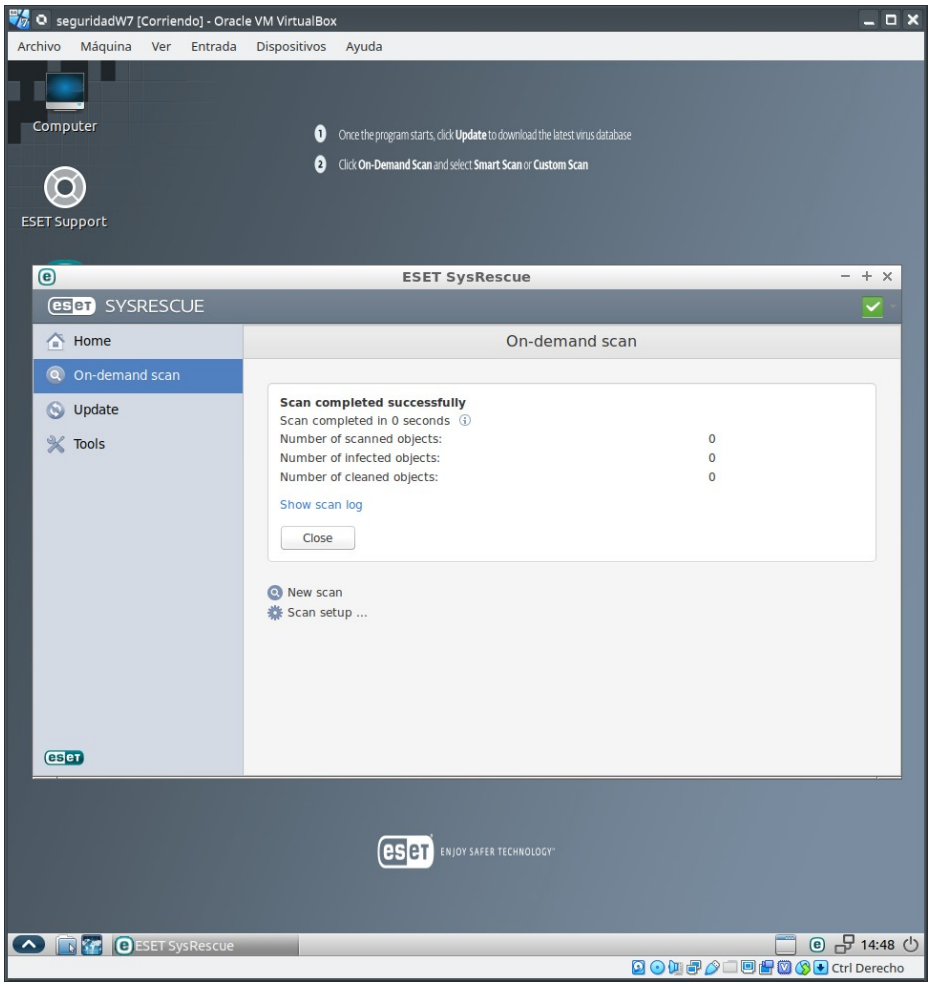
Práctica 3: Antivirus LIVE

Repetiremos los pasos anteriores y esta vez arrancare ESES SysRescue, al dato curioso que esta ISO si que permite actualizar la base de datos. Imaginaros que es del año 2018 y estamos acabando el 2019. Es un dato importante



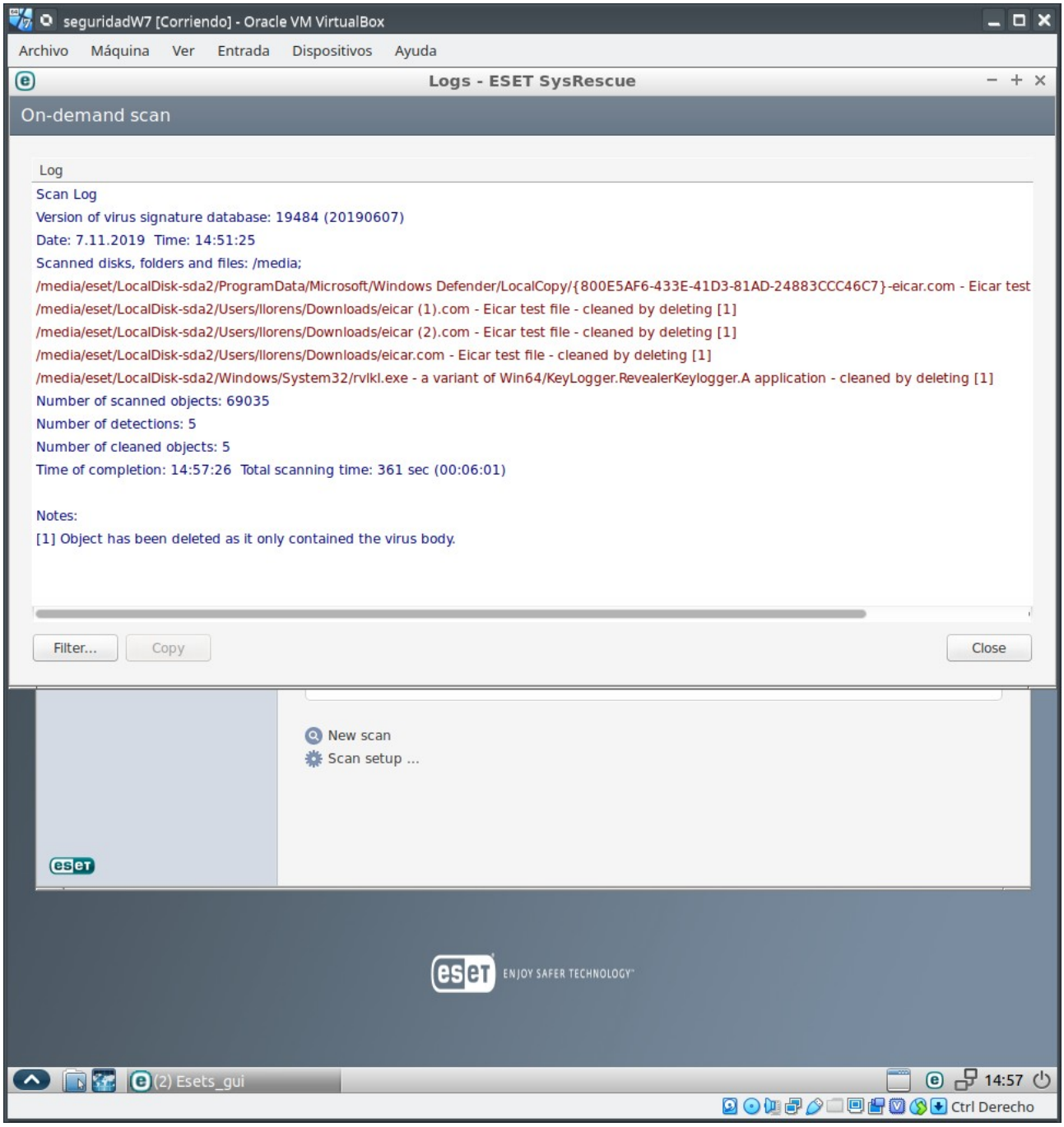
Práctica 3: Antivirus LIVE

Una vez actualizada volvemos a realizar una escaner



Práctica 3: Antivirus LIVE

Y sin desmerecer a Karpesky, tampoco mire si se podía actualizar la base de datos. El punto se lo lleva ESET ya que por su facilidad de interfaz que permite actualizar el antivirus y encontrar lo que Karpesky no fue capaz de encontrar.



Después pues ya seleccionamos lo que deseamos realizar. Eliminar (si es que se puede) o aislar el peligro y ponerlo en cuarentena.