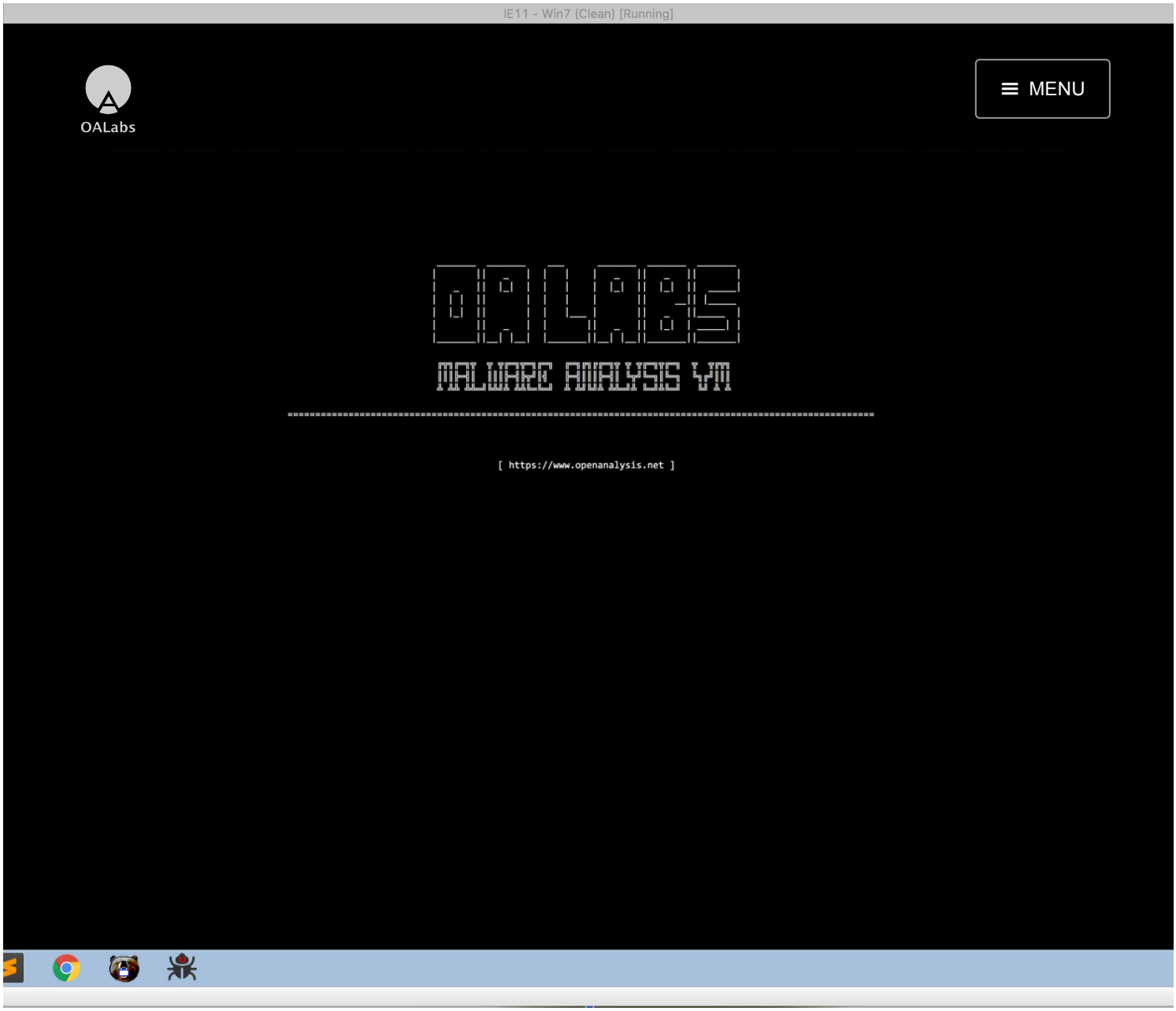


OALabs Malware Analysis Virtual Machine

16 JULY 2018 on Research

A Windows virtual machine (VM) is one of the most important tools available for analyzing malware. A VM allows the flexibility to debug malware live without fear of infecting your host. If the VM is infected it can quickly be reverted to a clean snapshot to continue analysis.

Traditionally malware analysts have had to maintain their own VMs with a collection of analysis tools. But this all changed in 2017 with the release of the excellent FLARE-VM project. FLARE-VM is built on top of the Chocolatey package manager for Windows and provides central management for windows software. We have extended the idea behind the FLARE-VM project and created a specific OALabs-VM installer that will automatically configure a full VM with the tools you need to follow our malware analysis tutorials.

This tutorial provide instructions for the installation and configuration of a free Windows 7 VM with the OAlabs-VM installer. The following steps will be covered in detail.

- Installing VirtualBox
- Downloading a FREE Windows 7 (x86) VM from Microsoft
- Importing the Windows 7 VM into VirtualBox and configuring the settings
- Downloading and executing the OALabs-VM installer script
- An overview of OLabs tools and their location on the VM
- Setting up a 64bit VM for use with the free IDA Disassembler

> ***Watch our installation tutorial here:*** *Malware Analysis VM Setup Tutorial*

Installing Virtual Box

We recommend using VirtualBox as your hypervisor for controlling the malware analysis VMs. VirtualBox has a similar user interface across all host platforms so it will be easier to follow our install guide. It is also free and easy to use.

To install VirtualBox navigate to the VirtualBox downloads page https://www.virtualbox.org/wiki/Downloads choose the installer package for your operating system. Download and run the installer and follow the install directions.

Installing FREE Windows 7 VM

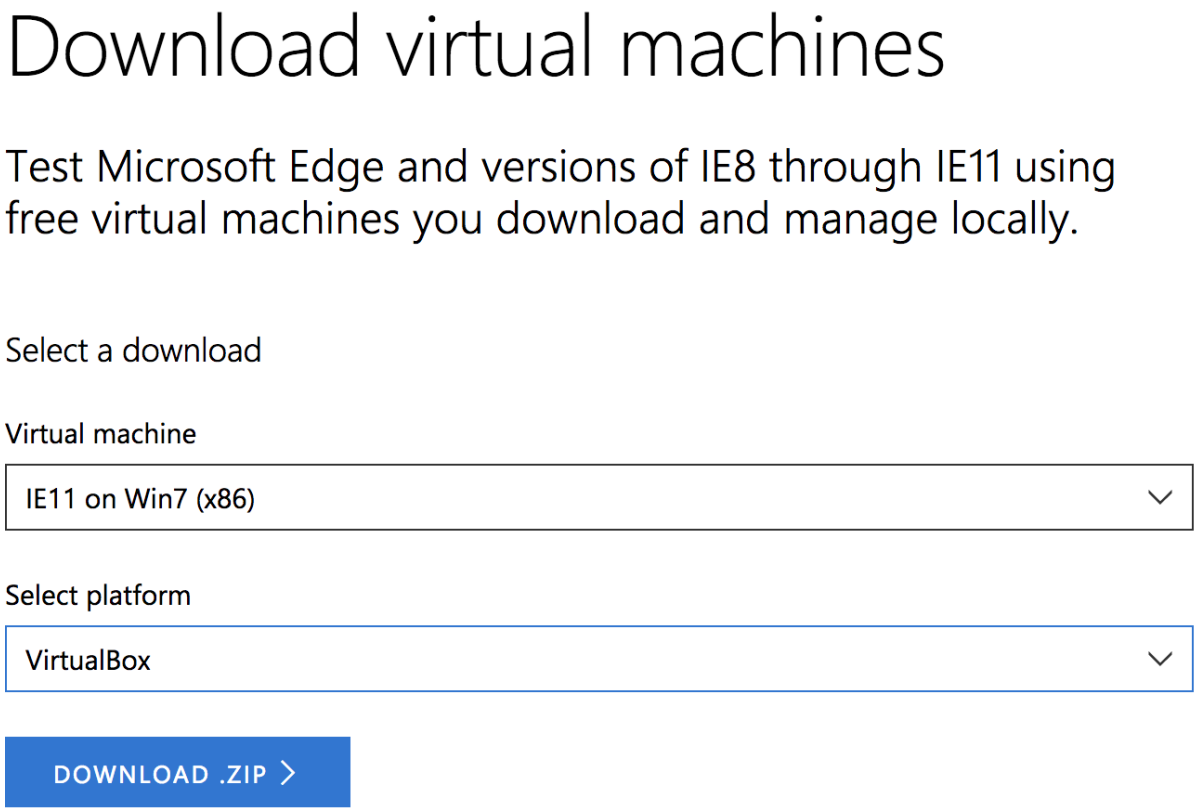
The OALabs-VM installer is intended to be run on the FREE VMs provided by Microsoft for testing the Edge web browser. The installer should still work on any 32bit Windows 7 VM though we have only tested it with the free VMs. We chose to use 32bit Windows 7 and it is simpler to use for debugging 32bit malware which is currently still the majority of windows malware.

The FREE Microsoft VMs have a **limited license that will expire after 90 days**; however, during our install process we will take a snapshot of the VM that can be restored after the 90 day period to extend the license indefinitely.

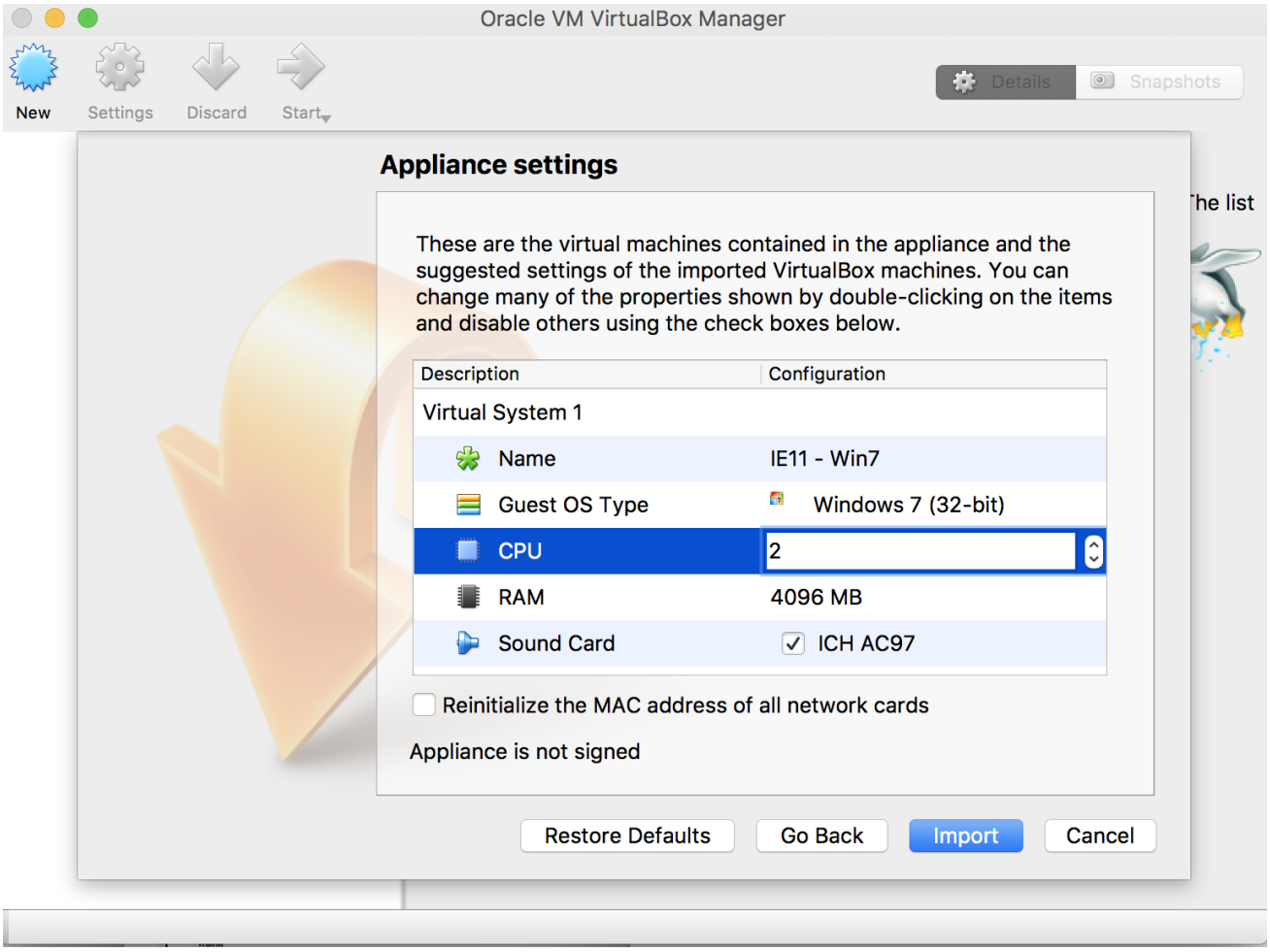
To download the free VMs navigate to the Microsoft VM download page here https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/. Use the drop down menus on the page to select the following VM configuration:

- IE11 on Win7 (x86)
- VirtualBox

Download the `.zip` file and unzip it on you host. The zip folder should contain a `.ova` file.



Next, open VirtualBox and select `File->Import Appliance`. Select that path to the .ova file that you just unzipped and select `Continue`. You will then be asked to select the appliance settings, if possible up the number of CPUs to 2. The rest of the settings should be ok.

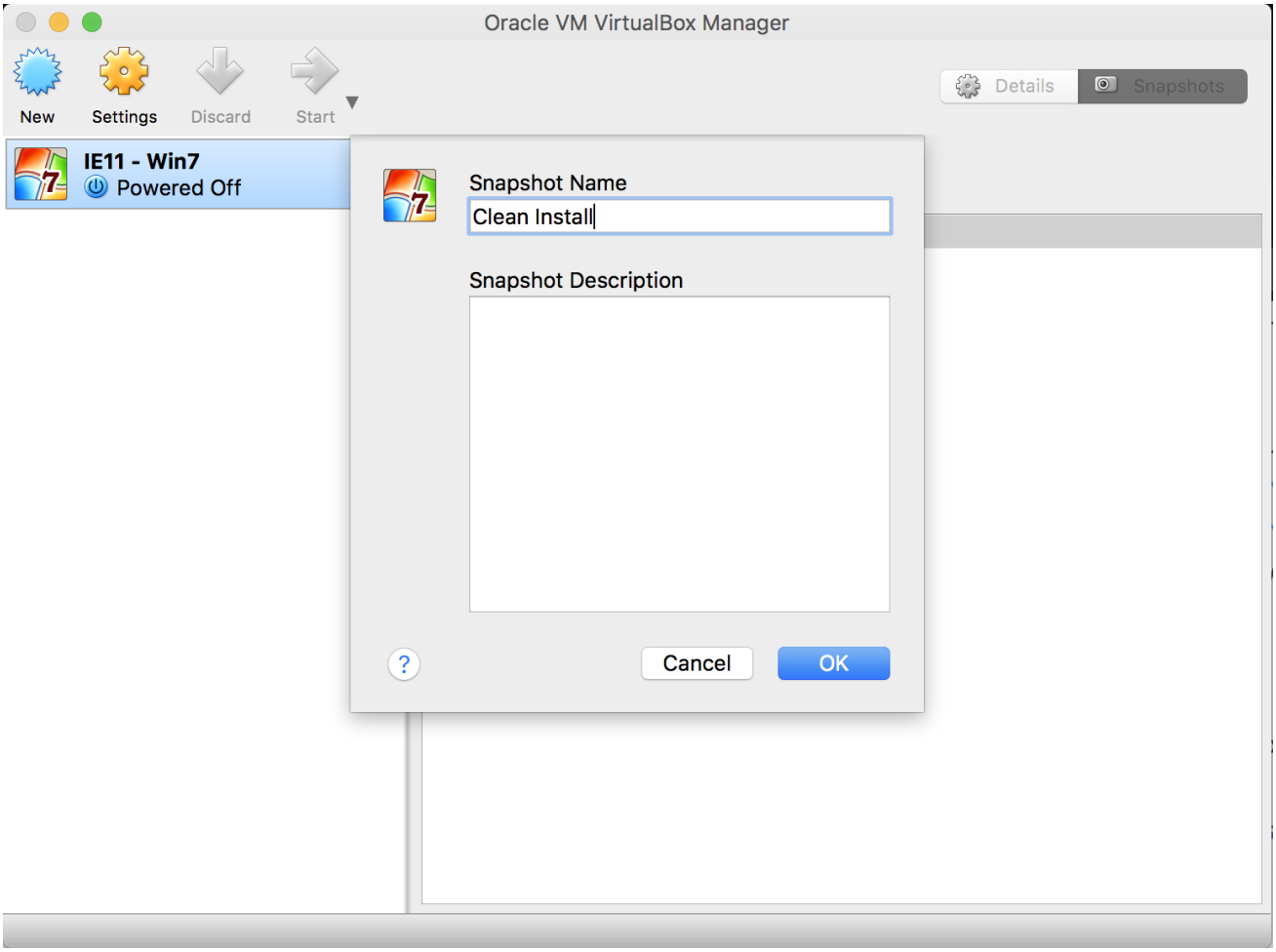


Finally click `Import` to import the VM. This may take some time.

Once the VM has been imported you should take a snapshot **before you power it on**.

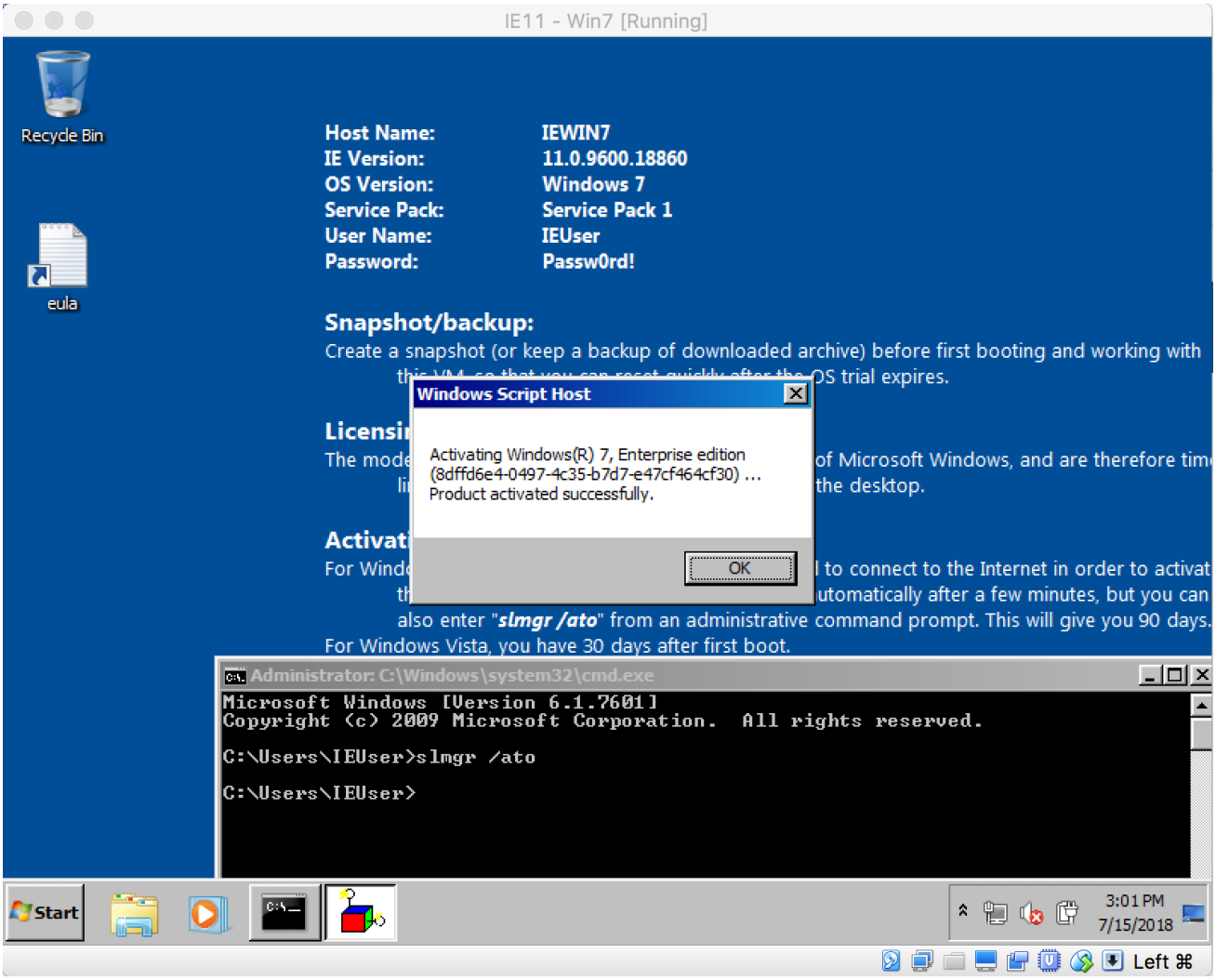
Snapshot/backup:
Create a snapshot (or keep a backup of downloaded archive) before first booting and working with this VM, so that you can reset quickly after the OS trial expires.

This will allow you to restore to the snapshot after the 90 day license expires and follow the OALabs-VM installation steps in the next section to re-create your analysis VM. We have labeled the snapshot `Clean Install`.

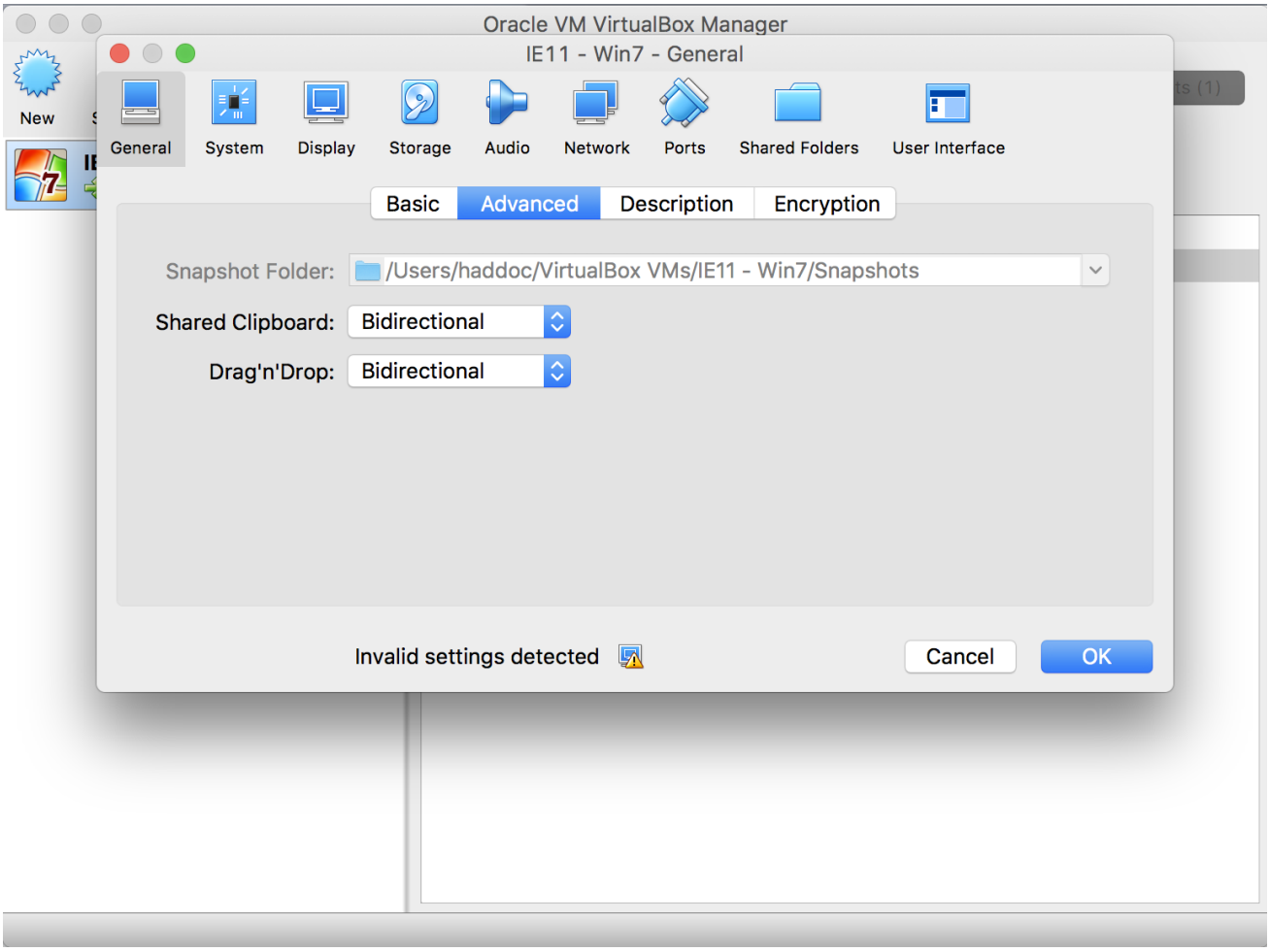


After taking the snapshot you will need to power on the VM and register the 90 day license.

- Power on the VM.
- Ignore any prompts to reboot the VM, choose `Restart Later`.
- Take note of the user name and password (on the wallpaper).
  - This is usually IEUser:Passw0rd!
- Open `cmd.exe` and activate the 90 day license by typing in `slmgr /ato`.
- Wait for the activation confirmation pop-up and close it.

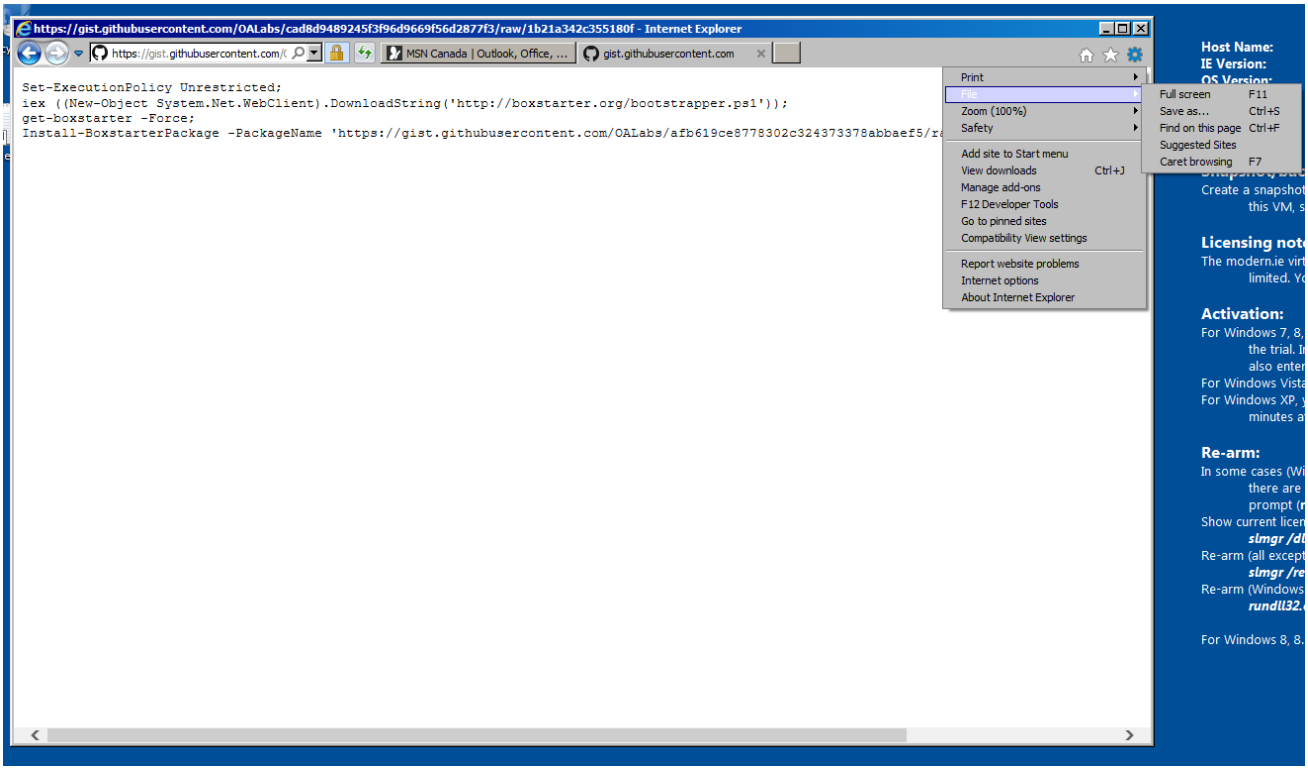


PRO-TIP: If you want to use the clipboard to copy text between your host the the VM you can enable these settings in `Settings->Advanced->Shared Clipboard`. But, remember if you have this enabled and you are analyzing malware in the VM that steals data from the clipboard you should disable this first.

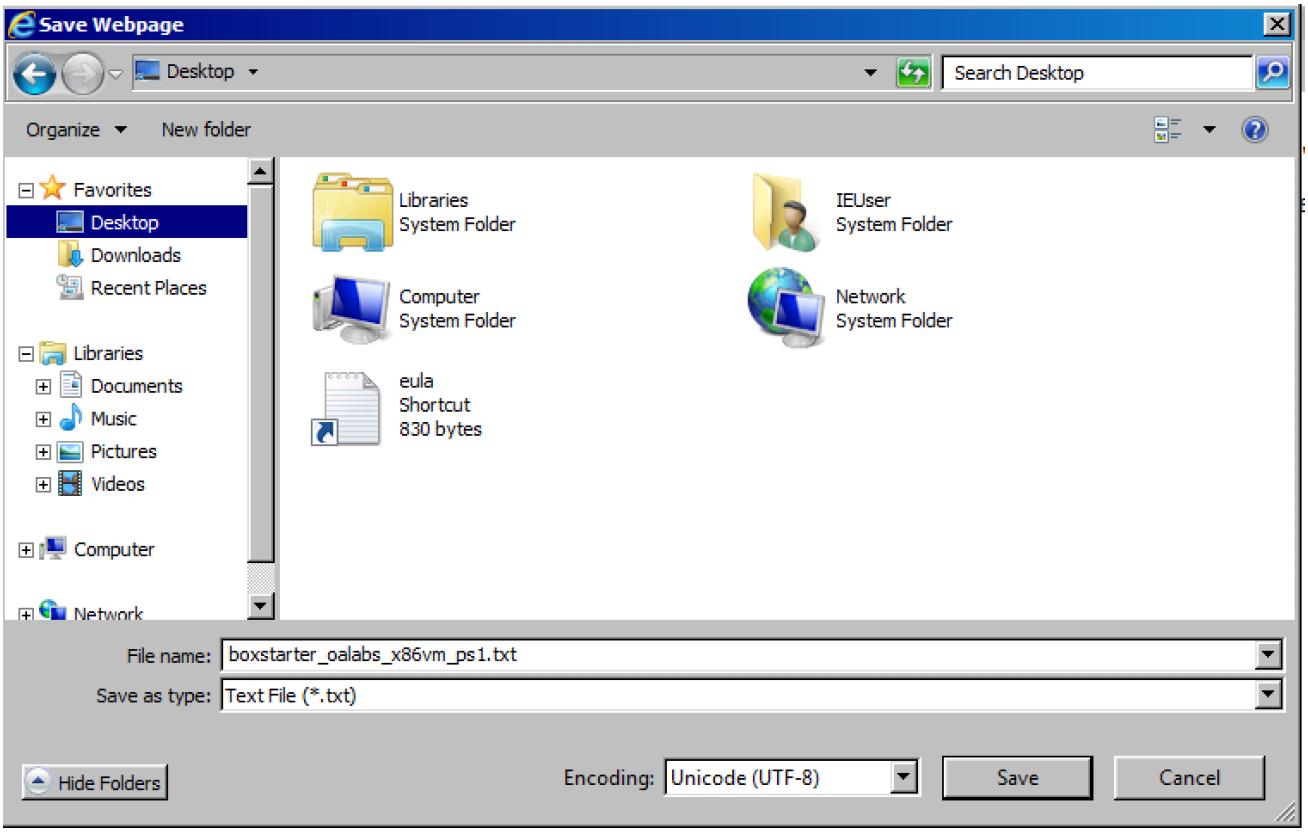


Installing OALabs-VM Tools

Installing the OALabs-VM tools is a simple three step process. First, open Internet Explorer in the VM and browse to the following OALabs Boxstarter gist: https://gist.github.com/OALabs/cad8d9489245f3f96d9669f56d2877f3. This gist contains a Powershell script that will initiate the installer process. Download the script as as a text file by clicking on the `Raw` button in the github interface and then choosing `File->Save As...` in Internet Explorer.

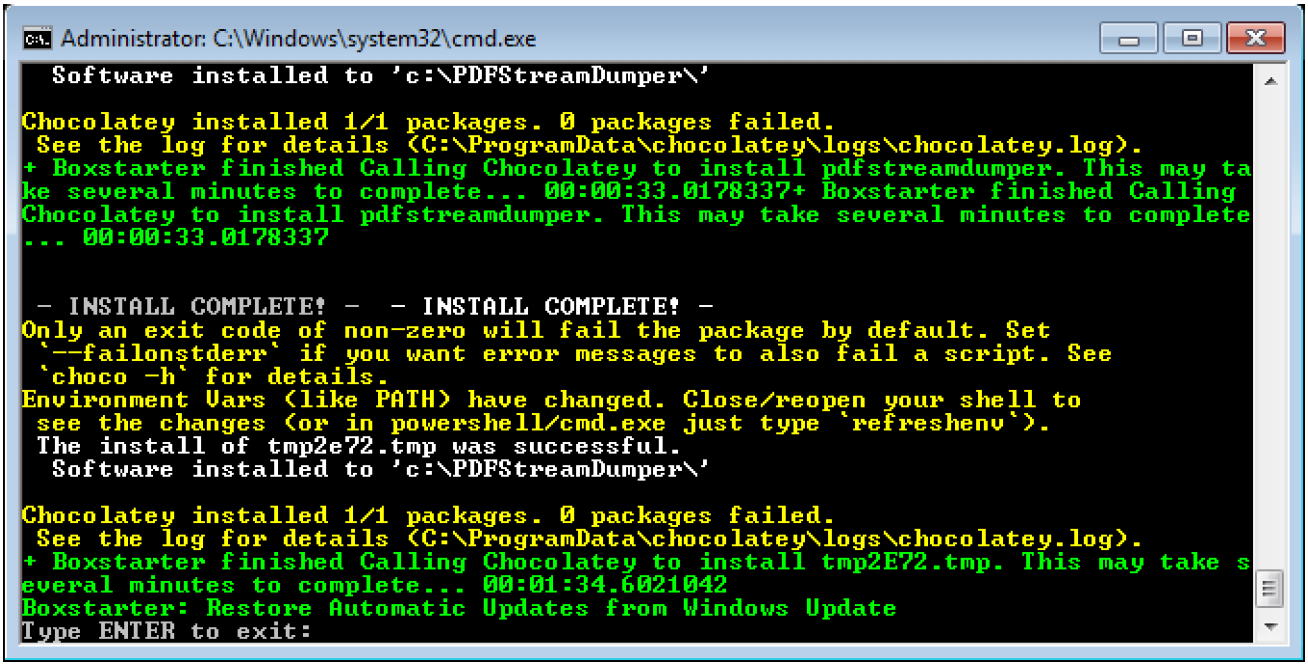


Make sure to save the file to your Desktop **as a** `.txt` **file** and close Internet Explorer.



Locate the saved file and change the file extension to `.ps1` so it can be run as a Powershell script. Then right click on the file and choose `Run with PowerShell`. This will start the installer.

The installation process may take some time as it needs to download multiple software packages. During the install it is normal for the VM to automatically reboot multiple times. Some package may also open an installer screen which you will need to click through. Simply select the default setting and click through to allow the install to proceed. Once the install has finished the script will prompt you to click `Enter` to complete the install and close the PowerShell window.



PRO-TIP: Once you have completed the OALabs-VM install you should take a second snapshot of the VM. We usually label this snapshot `Clean With Tools`. This snapshot will now be the base image that you start with when you start each new malware analysis task. After each analysis is complete you can restore this snapshot and the VM will be ready to go with the tools installed.

OALabs Tools Overview

The OALabs-VM installer will only install a select few tools that we use during our tutorials. However, the installer also installs the Chocolatey package manager so it is easy to install additional software from the Chocolatey software repository. An overview of the OALabs-VM tools is provided below.

Checksum

Checksum is a command line tool that can be used to display checksum hashes for files. For example, `checksum -t sha256 <file>` will display the SHA256 hash of the file.

7zip

7zip is a decompression utility that can be used to decompress multiple archive types. This utility is installed in `%programfiles%\7zip` on the VM and is accessible from the Start Menu. For more details see the 7zip website.

Process Explorer

Process explorer is a utility for exploring the running processes on Windows. It is available from the Start Menu. Many malware samples will check for the string `procexp` in running processes as an anti-analysis trick so we have cloned the procexp binary to `pexp.exe`. This clone is also available from the start Menu and is recommended for use when debugging malware. For more details see the Process Explorer website.

Resource Hacker

Resource Hacker is a simple utility used to extract the resources from a PE file. It is available from both the Start Menu and pinned to the Task Bar. For more details see the Resource Hacker website.

HxD

HxD is a hex editor. It has been installed to `%programfiles%\hxd` and is also available from both the Start Menu and pinned to the Task Bar. For more details see the HxD website.

Sublime Text 3

Sublime is an excellent text editor. It has been installed to `%programfiles%\Sublime Text 3` and is also available from both the Start Menu and pinned to the Task Bar. For more details see the Sublime Text website.

Google Chrome

This is the standard Google Chrome install. Enough said.

PEBear

PEBear is our go-to PE viewer and editor developed by Hasherezade. It is available from both the Start Menu and pinned to the Task Bar. For more details check out hasherezade's post about PEBear.

LordPE

LordPE is a PE viewer and editor similar to PEBear... but retro cool! We don't use it that often but many analysts prefer it so we have included it just in case. It is available

from both the Start Menu. For usage instructions check out the aldeid wiki post about LordPE.

x64dbg (x32dbg)

We have installed x32dbg the 32bit version of x64dbg. This is the debugger that we use for most of our tutorials and it should be suitable for most tasks. We plan on updating the version installed soon. It has been installed to `%programfiles%\x64dbg\release\x32`. This install location also contains the `plugins` and `db` folders which you may need to access if you install any plugins or want to erase past analysis databases. x32dbg is also available from both the Start Menu and pinned to the Task Bar. For more details check out the x64dbg website.

Python2

This is the standard Python 2.7 install and the paths have been set so it is available from the command line. Pip the python package manager is also installed.

strings.py

Strings.py is a custom strings tool written in python by Willi Ballenthin. It is available from the command line. The source for this file is available as a gist here.

Document Tools

The following document analysis tools are also installed.

- oletools
- offvis
- officemalscanner
- pdfid
- pdfparser
- pdfstreamdumper

Installing FREE IDA Disassembler(x64)

As mentioned above we have configured the OALabs-VM installer to be used with a Windows 7 32bit VM. Unfortunately the free version of the IDA disassembler will only run on 64bit Windows. This means that we have to configure a separate VM for use with IDA. Our recommendation is to download a second FREE VM from Microsoft: https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/. This time select the Windows 10 64bit VM.

Download virtual machines

Test Microsoft Edge and versions of IE8 through IE11 using free virtual machines you download and manage locally.

Select a download

Virtual machine

MSEdge on Win10 (x64) Stable (17.17134)

Select platform

VirtualBox

DOWNLOAD .ZIP >

Follow the same VirtualBox Appliance Import instructions as above and add import the Windows 10 64bit VM into VirtualBox. Once you have imported and configured the VM download and install the free IDA disassembler from the Hex-Rays website https://www.hex-rays.com/products/ida/support/download_freeware.shtml .

Installing All The Tools! With FLARE-VM

If you find the OAlabs-VM installer is missing some of your favorite tools you can install a much larger set of analysis tools using the FLARE-VM install. There is also an excellent tutorial video from RingZeroLabs that will walk you though both the installation of the FREE Windows VM and FLARE-VM.

Sergei Frankoff

Sergei a co-founder of Open Analysis, and volunteers as a malware researcher. His focus is reverse engineering malware and building automation tools for malware analysis.

Share this post

https://www.openanalysis.net