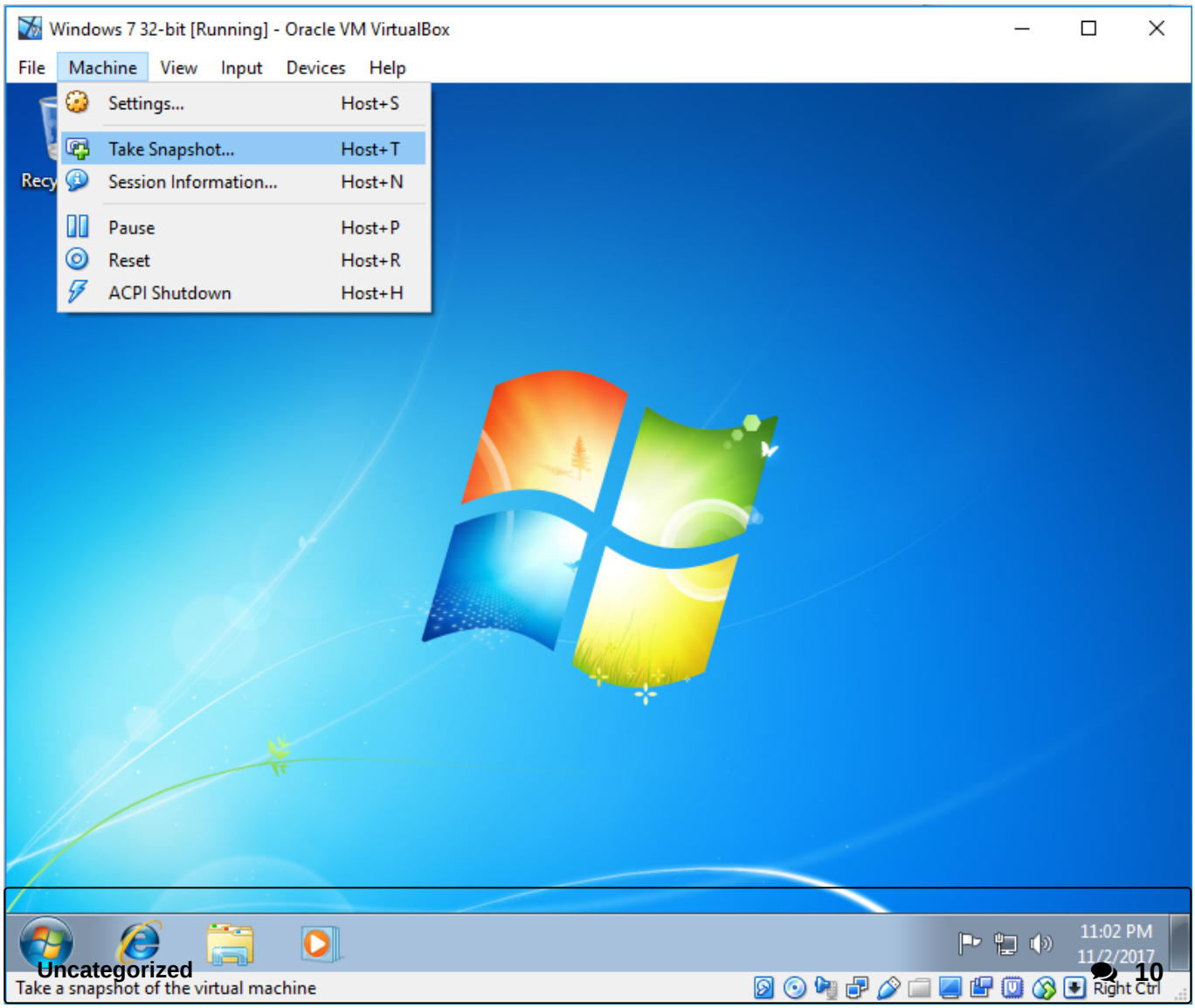
Creating a Simple Free Malware Analysis Environment

By : MalwareTech (https://www.malwaretech.com/author/malwaretech) November 4, 2017 Category : Uncategorized (https://www.malwaretech.com/category/uncategorized) Tags: security (https://www.malwaretech.com/tag/security), tutorials (https://www.malwaretech.com/tag/tutorials), virtual machines (https://www.malwaretech.com/tag/virtual-machines)



Uncategorized 10

Computer Requirements:

- A CPU with AMD-V or Intel VT-x support (pretty much any modern CPU).

- 4 GB RAM (more is better).

Make sure Virtualization (AMD-V or Intel VT-x) is enabled in the BIOS. To do this, you'll need to google "enable virtualization" along with your bios or motherboard version, then follow the steps.

Picking Your Hypervisor

A hypervisor is software that allows you to create a virtual computer (sometimes called a Virtual Machine and abbreviated to VM) which is that is isolated from your real machine. We will use the hypervisor to create a separate Windows installation that can be infected with malware without causing harm to us or our data.

I personally have used about 5 different hypervisors I frequently use because each one has subtle differences that i find makes them better for different tasks, I'll explain what I use each for and why.

- **VMware Workstation Pro –** Very high performance and is probably the best hypervisor to run on a Windows operating system, it's also packed full of extra features which makes it useful for complex virtual networks.
- **VMware Workstation Player –** Stripped back and lightweight version of Pro, great for simple and easy VM setup but doesn't support snapshots which is a major problem for malware analysis. I have this installed on my laptop for on the road demos.
- **KVM –** Runs on Linux and has a cool plugin that allows you to run more VMs that your system has RAM by using memory de-duplication. KVM is great for avoid malware detecting it's in a VM because most malware relies on the presence of VirtualBox or VMWare specific artifacts and doesn't care much for detecting other hypervisors.
- **ESXi –** It's not a hypervisor that you install on your operating system, the hypervisor is the operating system. By having an operating system built around the hypervisor, overhead is reduced because there's no need for any code other than that required to run the hypervisor.
- **VirtualBox** -Allows you to spoof the hardware your VM runs on, avoiding malware figuring out that it's in a VM by probing virtual/physical hardware or firmware version; it's free, easy to set up, and has most of the features paid hypervisors have.

For beginners I'd recommend VirtualBox (https://www.virtualbox.org/wiki/Downloads) because it's free, supports most major operating systems, and has a snapshot feature allowing you to rollback the VM to a saved point. For this reason, I will base the post on VirtualBox.

Picking Your Guest OS

The operating system running inside the Virtual Machine is fairly important and depends on a couple of things, I'll go into details on each.

Your Skill Set
If you're planning to reverse engineer malware and you only understand x86 assembly (or are learning Assembly), then it would make sense to run an x86 Windows installation. The majority of malware runs under WoW64 (Windows' way of running 32-bit binaries on 64-bit systems), so you'll likely be reverse engineering

32-bit code regardless of what architecture you use. In some cases malware will drop a 32-bit or 64-bit payload depending on the architecture, so if you don't know 64-bit assembly, you'll want the 32-bit payload, which means using a 32-bit (x86) operating system.

Your Hardware

A x86_64 CPU can run 32-bit and 64-bit VMs, but a x86 CPU can only run 32-bit VMs, so if your CPU is x86 you should pick a 32-bit operating systems. Older CPUs (especially x86 ones) might not support features required by newer Windows installations, so it'd also be best to stay below Windows 8.

If your computer doesn't have much RAM, you'll be better off running a Windows XP VM as this can run on as little as 256 MB of RAM (make sure to use Service Pack 3 though as it adds some features to the OS which most malware relies on). Windows 7 VMs generally require 1 GB of ram, but you can probably get away with 768 MB (512 MB for Home Edition).

Your Experience

Most malware will work on every Windows system between XP Service Pack 3 and Windows 10, so if you find you're more familiar with XP, then don't be afraid to use it. Windows 10 is very resource intensive and may not be supported by all malware, so for general day to day malware analysis I recommend staying away from Windows 10 unless you absolutely need it for some reason. Windows 10 is also incredibly noisy in terms of internet connected background services, which will fill up your packet capture with useless and irrelevant data.

Your Malware

64-bit operating systems utilize something called DSE (Driver Signature Enforcement) which prevents loading of unsigned kernel drivers, if you're analyzing malware which installs a kernel driver, then a 32-bit operating system is your best bet because it won't have a problem with malware installing unsigned drivers.

What do I use?
I'm actually lucky enough to now have a powerful rackmount server in my basement (courtesy of my employer), so I have a VM of every OS from XP to 10 as well as both 32-bit and 64-bit installations, but previously my personal preference was Windows 7 Ultimate Edition (32-bit) for working with common malware (I use Ultimate for the Remote Desktop feature, but if you're happy using VNC then Home Edition is fine).

It's also important to remember that the VM will be used to run and analyze malware, so not using older operating systems because they're "insecure against hackers/malware" is counter productive when the intention is to infect it with malware.

Setting Up Your Virtual Machine

RAM
I recommended you use the minimum amount suggested by requirements for your chosen operating system.

CPU
The "Processor(s)" option defines how many CPU cores the VM can use. One should be fine, but if you have a CPU with more than a single core, consider setting the limit higher to speed up the VM.

Execution Cap should be left at 100% unless you set the Processor(s) setting to the same number of cores your CPU has, in which case consider lowering the limit to avoid VMs freezing your computer.

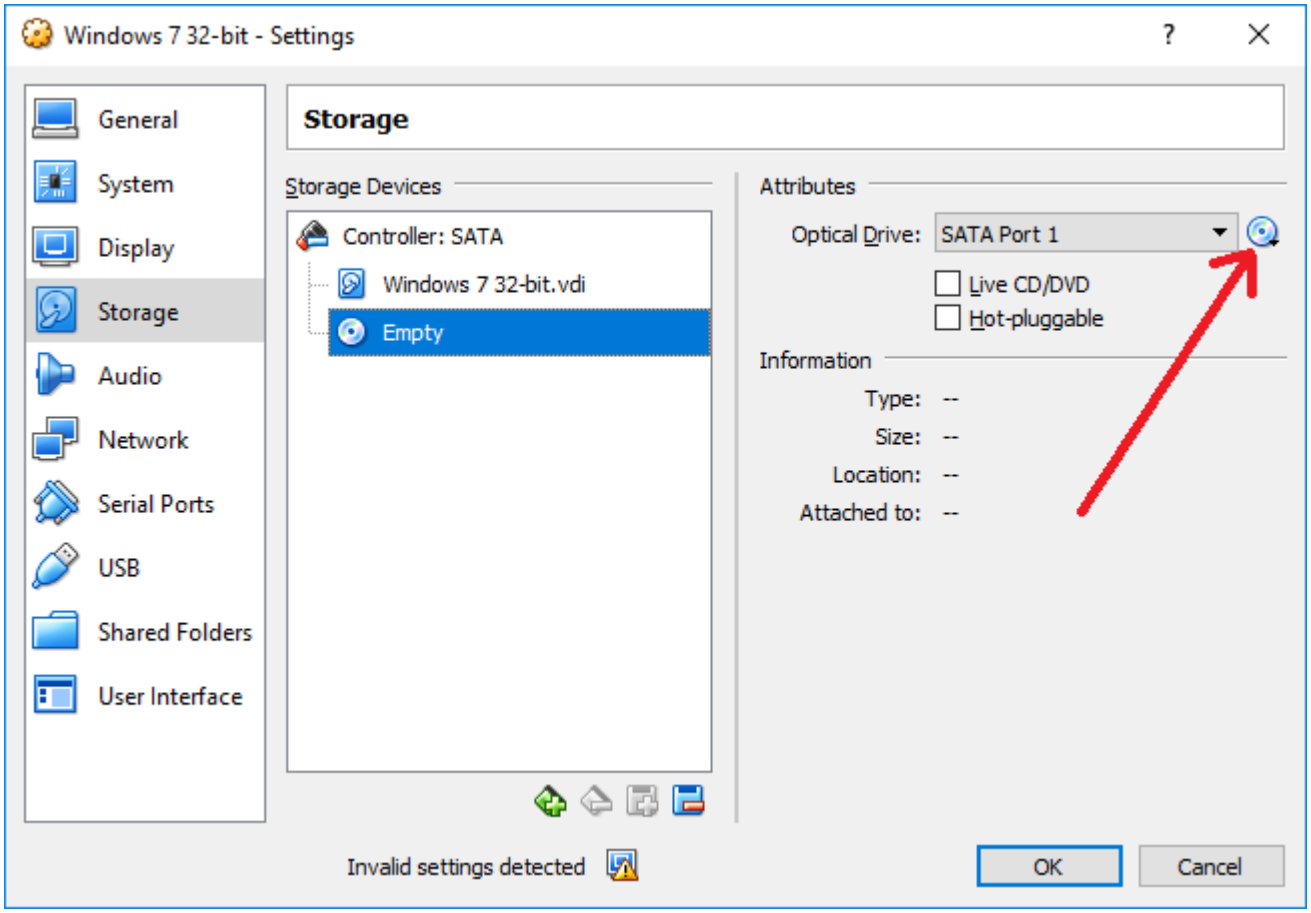
Network
Make sure to select the "NAT" option. It will allow your VM to connect to the internet but not see devices on your real network or talk to other VMs, which is good from a security standpoint.

The rest of the options can be left as is. Although it's not required for a simple malware analysis environment, you can harden VirtualBox to prevent malware detecting it's in a VM by using hfireF0x's loader (https://github.com/hfiref0x/VBoxHardenedLoader).

Installing Windows

Windows 7, 8, and 10 ISOs can be gotten here (https://www.microsoft.com/en-us/software-download/home) if you have a valid product key (do not use your product key to activate Windows once installed in the VM or malware could steal your key; instead leave Windows un-activated). Windows XP doesn't seem to be available from the Microsoft site, but I believe it's legal to download Windows ISO torrents as long as the installers are not cracked or patched. Simply don't activate Windows as you don't need any of the benefits of activating when the VMs only purpose is running malware.

You don't need to mount the installer ISO to a CD, simply navigate to the "Storage" category in options, click the CD icon which says "Empty" next to it, click the second CD icon in the top right and select the install ISO.

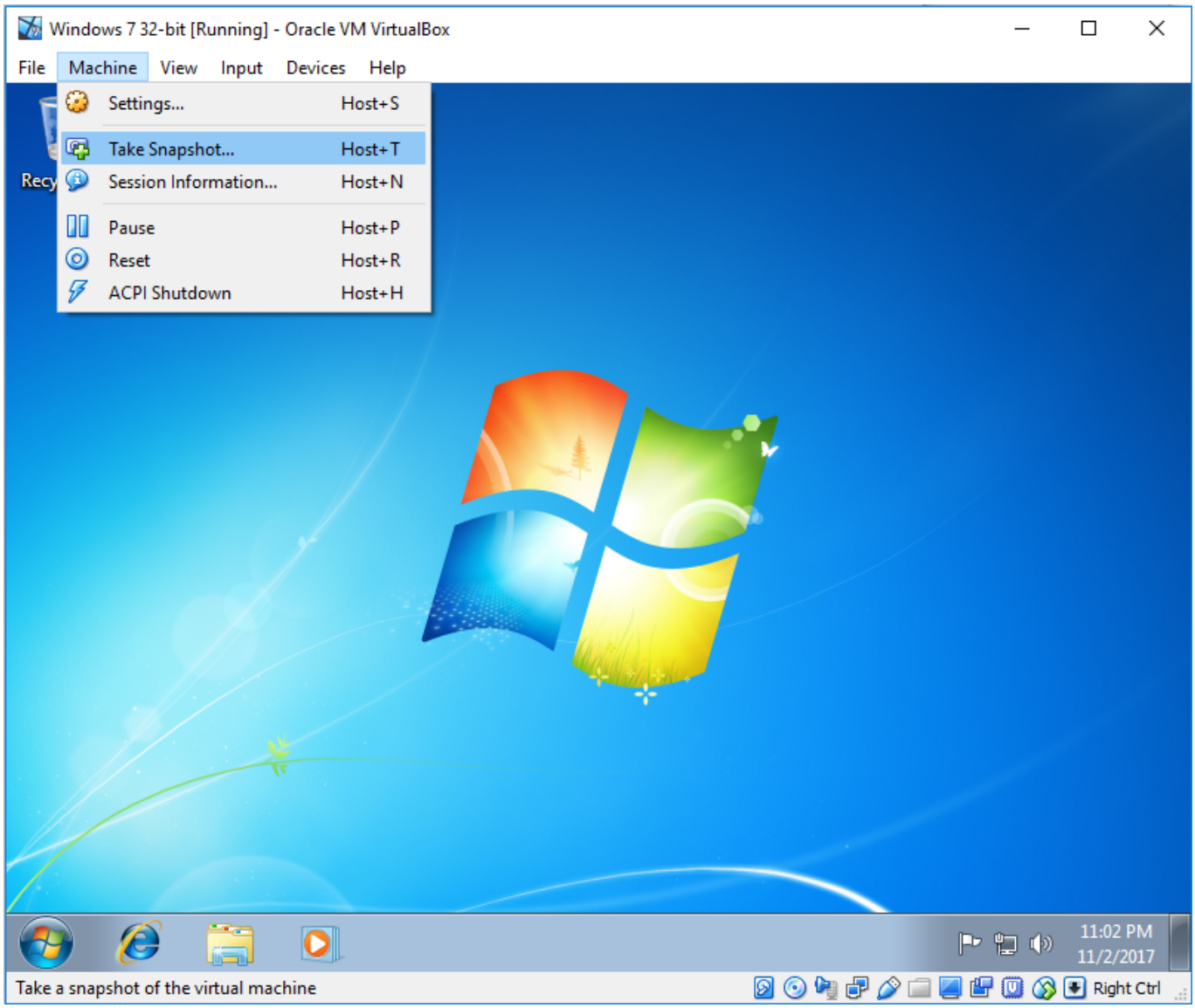


(https://www.malwaretech.com/wp-content/uploads/2017/11/iso.png)

Once you boot the VM it will automatically boot from the ISO. Go through the Windows installation process like you would normally, skip the activation section, and consider changing your computer name and username to make the VM seem less like a research machine. Avoid installing "Guest Additions" as the toolset is commonly used by malware to detect that it's running inside a VM.

Environment Setup

As soon as Windows is installed you should take a snapshot by clicking “Machine” > “Take Snapshot”, this will create an image of the current VM state so you can rollback later or create new VMs from the same image. A snapshot is like creating a copy of your VM’s hard disk and RAM content; when you “roll back” to a snapshot, it’s like overwriting the hard disk and RAM with the data saved during the snapshot, undoing any changes, and of course malware infections that happened after the snapshot was taken).



(https://www.malwaretech.com/wp-content/uploads/2017/11/vm_snapshot.png)

Now it’s time to pick and install your analysis tools, fo you’re not sure what to install, here is a list of my suggestions to get started:

Disassemblers / Debuggers

- OllyDbg (http://ollydbg.de/)
- WinDbg (Installed as part of the Windows SDK) (https://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=8279)
- x64Dbg (https://sourceforge.net/projects/x64dbg/files/snapshots/)
- IDA (Freeware Edition) (https://www.hex-rays.com/products/ida/support/download_freeware.shtml)

- Radare2 (http://rada.re/r/)

PE Tools

- PE Explorer (http://www.heaventools.com/overview.htm)
- Explorer Suite (http://www.ntcore.com/exsuite.php)
- PEStudio (https://www.winitor.com/binaries.html)

Process Tools

- Process Hacker (http://processhacker.sourceforge.net/)
- ProcMon (https://docs.microsoft.com/en-us/sysinternals/downloads/procmon)
- Process Explorer (https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer)
- Process Dump (http://split-code.com/processdump.html)
- User Mode Process Dumper (https://www.microsoft.com/en-us/download/details.aspx?id=4060)

Network Tools

- Wireshark (https://www.wireshark.org/download.html)
- Fiddler (https://www.telerik.com/fiddler)
- mitmproxy (http://docs.mitmproxy.org/en/stable/install.html)

Other

- HxD (Hex Editor) (https://mh-nexus.de/en/hxd/)
- PaFish (Testing for VM detection) (https://github.com/a0rtega/pafish)
- oledump (Extract Macros from Office Documents) (https://blog.didierstevens.com/programs/oledump-py/)
- olevba (VBA Macro Extractor) (https://www.decalage.info/python/olevba)
- Strings (Extracts ASCII and Unicode Text from Files) (https://docs.microsoft.com/en-us/sysinternals/downloads/strings)

Once you're done installing your favorite tools, create another snapshot and you're ready to go (when you want to install new tools, simply rollback to this snapshot, install your new tools, then create a new snapshot and delete the old one).

Warnings

- There's no recorded cases of malware using zero-day exploits to escape a virtual machine, you should be safe if you practice good VM hygiene. Never plug USB devices into your virtual machine, assume

every file in your VM has been infected and never transfer files that are infectable outside your virtual machine, don't log into any servers inside an infected VM.

- Be careful when using features such as "Shared Folders" to share folders between your computer and the VM. Anything in these folders can easily be stolen, infected, or destroyed by malware inside the VM.
- Don't run malware samples you're not familiar with on an internet connect VM. Malware can launch DDoS attacks, hack computers, and commit financial fraud from your IP address; your front door is much nicer when it hasn't been knocked off its hinges by law enforcement.
- If you run a VPN inside your VM it can be disabled or bypassed by malware, exposing your real IP address. Criminals will generally not target researcher, but if you want to hide your IP address then you should run the VPN on your computer and not inside your VM.
- Avoid storing executable malware samples where they can be accidentally run. Either rename files to something non-executable (like .bin or .malware) before they touch your computer, or store them on a webserver in a non-executable directory.
- Anything you put inside your VM can and probably will be stolen by malware you run inside it, use common sense.
- Use snapshots to save your progress while doing analysis. If you're taking notes in your VM and it crashes or gets encrypted by ransomware, your data will be lost if you haven't backed it up.
- Anti-viruses will still scan and delete non-executable malware samples or even your notes if they match malicious signatures, whitelist the folder you save your research in.