

Laptop Hardware and Software Technical Requirements



Important! Bring your own laptop and a pre-installed Windows 7 virtual machine!

A properly configured laptop is required to participate in this Camp. Prior to the start of Camp, you must install the necessary software as described below. If you do not carefully read and follow these instructions, you are guaranteed to leave the Camp unsatisfied, since you will not be able to participate in hands on-exercises that are essential to this Camp.

Hardware

- CPU: At least 2GHz CPU single core (faster the better)
- RAM: Minimum: 4GB of RAM (more RAM the better like 8GB or 16GB)
- Hard Disk Space: At least 30GB of FREE Hard Drive Space (more space is recommended)
- Ethernet network interface card (NIC) or built-in Ethernet network port
- CAT 5, CAT 5e or CAT6 Ethernet Cable
- WiFi

Software

- SIFT - Download the 1.5GB SIFT workstation at: <http://computer-forensics.sans.org/community/downloads/>
- Backtrack or Kali Linux
- VMWare Workstation 8 (or newer) or VMWare Fusion (VMWare Player WILL NOT WORK. MUST BE ABLE TO TAKE SNAPSHOTS.
- A 32 bit **Windows 7 Service Pack 0** or **Windows 7 Service Pack 1** Unpatched with Internet Explorer 8 Virtual Machine with installed inside VMWare Workstation or VMWare Fusion.
- You must download and install Debugging Tools for Windows 7 from this link: <http://www.microsoft.com/en-us/download/details.aspx?id=3138>

***You only need to install the debugging tools and not the entire SDK

- You must download the course tools from the following link and bring it to class: <https://www.dropbox.com/s/0vrz7iueaa0dafo/760.5.zip>

Misc Requirements

- 100% **administrative control** over the host OS (Windows XP, Windows 7, Windows 8, Mac OS X, Gentoo, Ubuntu, etc.) in order to disable any antivirus suites, host-based IDS (HIDS), firewalls, etc.

Final Checklist

Review the following checklist when leaving for the training event to make sure that your laptop is prepared for the Camp:

	Your laptop meets hardware requirements outlined in this note.
	VMware Workstation 8 or higher is installed.
	The VMware Workstation license will not expire before the class (if using a trial copy).
	You created a VMware virtual machine running Windows 7 with Service Pack 0 or Service Pack 1 (32-bit) and Internet Explorer 8 installed.
	Your Windows virtual machine is using "Host-only" network connection and is able to obtain an IP address from the DHCP server built into VMware.

Important note:

In preparation for the Reverse Engineering Malware class:

- Within the virtual machine you create, please have the following tools:
 - The latest Sysinternals Suite (can be downloaded [here](#)).
 - OllyDbg v1.10 (can be downloaded [here](#)).
 - Regshot (can be downloaded [here](#)).
- Please also download and extract the REMnux 5.0 virtual appliance from [here](#).

If you have any questions regarding the configuration of your laptop prior to class, please email the instructor, Anuj Soni, at anuj.soni@gmail.com.