Laptop Hardware and Software Technical Requirements

Important! Bring your own laptop and a pre-installed Windows XP 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 (faster the better)
- RAM: Minimum: 4GB of RAM (more RAM the better like 6GB or 8GB)
- 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
- Ethernet Cable
- WiFi

Software

- SIFT - Download the 1.5GB SIFT workstation at: http://computer-forensics.sans.org/community/downloads/
- VMWare Workstation 8 (or newer) or VMWare Fusion (VMWare Player WILL NOT WORK. MUST BE ABLE TO TAKE SNAPSHOTS.
- A Windows XP 32-Bit Virtual Machine installed inside VMWare Workstation or VMWare Fusion.

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.

Notes

Creating a Windows Virtual Machine Using VMware

You will use VMware to simultaneously run multiple virtual machines when performing hands-on exercises. You must have VMware Workstation version 8 or higher installed on your system. If you do not own and cannot purchase VMware Workstation, you can download a free trial copy from VMware. VMware will send you a 30-day serial number if you register for the trial at their Web site.

When analyzing malware, you will make use of a virtual Windows machine running within VMware. You will be asked to infect this virtual machine when examining malicious code. You must create a Windows XP (32-bit) virtual machine using your copy of VMware before coming to class. Note that this involves

not only creating a virtual machine shell using VMware, but also installing your copy of the Windows XP operating system into the virtual machine.

If you don't have Windows XP installation medium, you can obtain a free virtual machine from Microsoft if you are running Windows 7 Professional, Enterprise, or Ultimate on your base system. To do this and to import the virtual machine into VMware, follow instructions here.

Install Windows XP with Service Pack 3 (32-bit) on your virtual machine. Don't install anti-virus software on the Windows virtual machine. Lastly, be sure to install Internet Explorer 8 or higher into your Windows virtual machine.

Shut down your Windows virtual machine and configure it to use the "Host-only" network connection. You can do this by selecting Settings of your virtual machine in VMware, clicking Network Adapter on the Hardware tab, and selecting "Host-only." Then, start the virtual machine and confirm that you received an IP address from the VMware built-in DHCP server. You can do this by typing "ipconfig" on the command prompt within your virtual machine.

Hands-on exercises will involve operating with malicious code. Although VMware will provide you with reasonable isolation, we do not recommend using a production system as your laboratory machine. We expect you to exercise due caution when handling malicious code.

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 XP with Service Pack 3 (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.