

LAPTOP INSTALLATION GUIDE FOR563 : MOBILE DEVICE FORENSICS

Version 1.1

Mandatory Requirements For FOR563 Class:

BASE OPERATING SYSTEM LINUX, MAC OSX, or WINDOWS

A properly configured computer system is required for each student participating in the workshop portion of this course. Before coming to class, download the forensic installation document that will describe the steps in detail to follow to complete the installation. If you do not carefully read and follow these instructions exactly, you are guaranteed to leave the course unsatisfied since you will not be able to accomplish many of the in-class exercises.

You can use any version of **Windows**, **MAC OSX**, or **Linux** as your core operating system that also can install and run VMware virtualization products. You will use VMware with preconfigured virtual forensic workstation built on a Windows XP Professional environment that will enable you to perform hands-on analysis during class. You must have VMware Workstation 7, VMware Fusion 4.0, or VMware Player 4.0 or higher versions installed on your system prior to class beginning. If you do not own a licensed copy of VMware Workstation or Fusion, you can download a free 30-day trial copy from <http://www.vmware.com>. VMware will send you a time-limited serial number if you register for the trial at their website. VMware Player is a free download and works great for the course.

MANDATORY LAPTOP SOFTWARE REQUIREMENTS:

- Download and install VMware Workstation 7, VMware Fusion 4.0, or VMware Player 4.0 or higher versions
- Download and install 7Zip
- Download the viaExtract demo tool. You must create an account and download viaExtract by accessing this link:
<https://viaforensics.com/products/viaextract/>

MANDATORY LAPTOP HARDWARE REQUIREMENTS:

- CPU: 2.0 GHz or higher is recommended (Multi Core Preferred)
- Wireless 802.11 B/G/N Networking Capability
- 2 Gigabyte of RAM minimum (4GB or higher RAM is recommended)
- 40 Gigabytes of Free Space on your Laptop Hard Drive
- The student should have the capability to have Local Administrator Access within their host operating system.

MANDATORY ADDITIONAL ITEMS:

- One USB Thumb Drive (4-8 GB in size)

- One new, old, or used mobile device for an acquisition exercise, such as:
 - Cell phone (Motorola, Samsung, Nokia)
 - GPS device
 - Smartphone (e.g., iPhone, Blackberry, Android, Windows Phone)

If your BASE OPERATING SYSTEM is Windows:

WINDOWS VMWARE INSTALLATION

Go to <http://www.vmware.com> and register to download the latest version of VMware Workstation or Player to run under Windows. You can obtain a free 30-day license if you already do not own a copy of VMware. Download the latest **VMware Workstation 7 for Windows or VMware Player 4.0 or higher** and place it in your "My Documents" directory. Do not download any BETA versions of VMware products for this class; they will be incompatible with the course. Do not download any earlier versions of VMware as the VMware guest machines we distribute for the course are only compatible with the versions we highlighted above or higher. Please make sure that your VMware environment is stable as there will be no time to install or troubleshoot the Windows VMware machine during class. Remember to install VMware tools on your system. VMware support site is located on the web.

If your BASE OPERATING SYSTEM is LINUX

LINUX VMWARE INSTALLATION

You can use any version of Linux that allows you to install and run VMware Workstation 7 for Linux or higher.

Go to <http://www.vmware.com> and register to download the latest version of VMware to run under Linux. You can obtain a free 30-day license if you already do not own a copy of VMware. Download the latest **VMware Workstation 7/VMware Player 4** or higher rpms and place it in your /usr/local/src directory. Do not download any BETA versions of VMware for this class; they will be incompatible with the course. Do not download any earlier versions of VMware as the VMware guest machines we distribute for the course are only compatible with VMware Workstation 6.0/VMware Player 2.5 or higher.

From your command line run the following after your VMware rpm is downloaded to the /usr/local/src directory.

```
#rpm -ivh VMware-workstation-7-45731.i386.rpm (or later version)
```

```
Ensure eth0 is currently not turned on.
```

```
#ifdown eth0
```

```
Wait until installation is complete and run the VMware Configuration Tool.
```

```
#vmware-config.pl
```

```
Execute the following command and answer the following questions prompted to you with the response in BOLD. (press return) means press the return key without typing any value.
```

```
Do you accept? (yes/no) yes
```

```
Thank you.
```

```
Configuring fallback GTK+ 2.4 libraries.
```

```
What directory contains your desktop menu entry files? These files
```

```

have a .desktop file extension.
[/usr/share/applications] [press return]
In which directory do you want to install the mime type icons?
[/usr/share/icons] [press return]
In which directory do you want to install the application's icon?
[/usr/share/pixmaps] [press return]
Trying to find a suitable vmmon module for your running kernel.
None of pre-built vmmon modules for VMware Workstation is suitable for
your running kernel. Do you want this program to try to build the
vmmon module for your system (you need to have a C compiler installed
on your system)?
[yes] yes
Using compiler "/usr/bin/gcc". Use environment variable CC to override.
What is the location of the directory of C header files that match your
running kernel? [/lib/modules/your_kernel_version/build/include] [press
return]
Do you want networking for your virtual machines? (yes/no/help) [yes]
yes
Optional Question if you have more than one Ethernet adapter: Your
computer has multiple Ethernet network interfaces available: eth0,
eth1. Which one do you want to bridge to vmnet0 [eth0] [press return]
Optional Question if you have more than one Ethernet adapter:Do you
wish to configure another bridged network (yes/no) [press return]
Configuring a bridged network for vmnet0.
Do you want to be able to use NAT networking in your virtual machine?
[yes] no
Do you want to be able to use host-only networking in your virtual
machines?
[no] yes
Do you want this program to probe for an unused private subnet?
Do you wish to configure another host-only network? (yes/no) [no] no
Do you want this program to automatically configure your system to
allow your virtual machines to access the host's filesystem?
(yes/no/help) [no] no
Do you want to install the Eclipse Integrated Virtual Debugger [no] no
Do you accept? (yes/no) yes
[press return] for all VMware VIX API questions
# vmware &

```

If your BASE OPERATING SYSTEM is MAC OSX

VMWARE FUSION 4.0 INSTALLATION

You can use any version of Intel Based MAC OSX that allows you to install and run VMware Fusion 4.0. No beta versions are supported. SANS will be handing out one VMware Machine that will be utilized for the course.

Go to <http://www.vmware.com/products/fusion/> and register to download the latest version of VMware Fusion to run under MACOSX. You can obtain a free 30-day license if you already do not own a copy of VMware Fusion. Download the latest **VMware Fusion 4.0** or higher dmg.

Do not download any BETA versions of VMware Fusion for this class; they will be incompatible with the course.