Lab Setup Instructions

These setup instructions contain everything you'll need to get ready for your upcoming SANS class. These can take some time to complete, and may involve downloading large files. So please allow ample time to complete them before you arrive at class - especially if you have limited Internet bandwidth.

If you require assistance with the instructions contained within this document, please contact support@sans.org. Be sure to include the name of your course, and if possible, your order number.

We're looking forward to having you in class!

Lab 0: Getting Started (Complete Prior to Class)

Objectives

- Install and prepare your SIFT Workstation VMware image for use in the class labs.
- Familiarize yourself with the syntax used in the course's labs.
- Time permitting, prepare additional VMware images that will be used in the course.

Before you Arrive in Class or Travel

Several steps must be accomplished before you start class. For those students attending a live class event, this means completing the setup process before you leave. Some steps may require significant download bandwidth and hotel/venue Internet is not suitable for these downloads.

The following steps should be completed prior to the start of class:

Notice

The documents linked to in the steps below are purposely template content designed to be consistent across all SANS courses. As such, you will see screenshots that differ slightly from your course files. However, the file naming conventions and setup processes are the same by design.

1. **Downloading Course Materials**
   - **a.** Follow the guidance at https://sansurl.com/downloading-course-materials for accessing and downloading your course materials.
   - **b.** These files are large and may take a long time to download, depending on your Internet connection and many other factors. If you are attending a live class, you should not rely on Internet access at the event to download these files.
2. **Mounting Course ISOs**
   - **a.** Follow the guidance at https://sansurl.com/mounting-isos for mounting and accessing the the data within the downloaded course ISO files.
   - **b.** The course ISOs are archives that contain important files for your class. The course ISOs are not bootable operating systems.
3. **Decompressing and Booting Virtual Machines**
   - **a.** Follow the guidance at https://sansurl.com/decompressing-booting-vms for decompressing and booting the course VMs.

b. There are three virtual machines used in this course. The SIFT Workstation virtual machine will be used initially and most extensively throughout the class. Decompressing this is the first priority but all three should be extracted and ready to use before class starts.

   i. The FOR572-specific Linux SIFT Workstation will be the primary virtual machine used. Students who have taken other SANS DFIR classes will already be familiar with the SIFT environment, as will students who have downloaded the free SIFT VMware image for their own use. However, this distribution is a customized version built from the main SIFT distribution. We have included a number of network forensic and analysis tools that will be of use in the course and in taking on your daily workload. It also contains the lab evidence needed for your course. This version of the virtual machine is required for your FOR572 course.

   ii. The SOF-ELK® (Security Operations and Forensics) virtual machine consists of a self-contained installation of the Elastic Stack. There are numerous log and other parsers pre-loaded to simplify and streamline your analysis processes. The SOF-ELK project is a free resource for the community, but the version used in FOR572 is specifically matched to your courseware and contains pre-staged evidence files required for the labs.

   iii. The Arkime VM consists of an appliance-based installation of Arkime, and large scale, open source indexed packet capture and search tool. Arkime is a public project. The installation on your virtual machine is matched to your courseware and contains pre-staged evidence files required for the labs.

c. Log into the virtual machines: The **Virtual Machine Credentials** section of at the end of this document contains the credentials for each virtual machine and how they can be used. In particular, note that the SOF-ELK and Arkime virtual machines do not provide a graphical login. It is recommended to use the `ssh` client to access these two VMs from your SIFT Workstation, particularly if you have a non-US keyboard.

4. Review/Complete Specific Course Notes Below

a. The additional instructions below are unique to your course. Follow the remainder of this document once you are able to login to your course VMs.

Foundational Videos and Labs

For students who are not yet comfortable with or would like a brief refresher on the Wireshark, `tshark`, and `tcpdump` tools, you should take some time *before* class to watch some video content designed to bring you up to speed. These are part of a growing collection of public-facing content tailored around FOR572 that is not always necessary for all students. However, it will ensure everyone is equally ready to hit the ground running in class. Consider the following three notional tasks:

1. Using only `tcpdump`, read a 25 GB pcap file and create a new pcap file containing only the packets that are:
   a. Sent to or from the `70.32.97.206` IP address **and**
   b. Sent to or from port TCP/80
2. Using Wireshark, write a display filter that will match only packets with the string `Firefox` contained in the User-Agent field
3. Using `tshark`, create a list of all HTTP `Server:` header values in a given pcap file

The course content assumes a working knowledge of these tools. If you are not reasonably comfortable undertaking any of those notional tasks, it would greatly benefit you to take some time to review the videos and lab material provided here.

1. Videos are on YouTube at `https://for572.com/videos`

2. Introductory labs included in your SIFT Workstation VM's Electronic Workbook:

   a. Bonus Lab 1.0: `tcpdump` and Wireshark Hands-On

Time Zone and Region Settings Within Virtual Machines

Do not change your regional or time settings inside your VMs. Your VMs' system time zones are set to UTC. Timestamps in your course material will reflect the standard ISO 8601 format `YYYY-MM-DD HH:MM:SS` [1] as closely as possible. This avoids confusion from region to region across the globe so wherever you are located, the timestamp will be clear and unambiguous. Some tools may fail if the time zones are changed. Dealing with time zones and regional settings is complex [2].

Take Snapshots of Virtual Machines (Optional but Recommended)

> **Note**
>
> VMware Player and VMware Fusion Player do not have snapshot capabilities. If you are using either of these virtualization software products, this section cannot be accomplished. Snapshots are very useful to have, so we recommend using VMware Workstation Pro or VMware Fusion.

Consider creating a snapshot in case you need to revert one or more VMs to a known good state. At a minimum, it is recommended to take a snapshot of each virtual machine immediately after extracting it from the archive file. It is also recommended to periodically take snapshots during the class to ensure you can recover from any problems that might occur.

Updating the Electronic Workbook

The electronic workbook content is stored locally in the VM so it is always available, in perpetuity. However, course authors may update the source content with minor fixes, such as correcting typos or clarifying explanations, or add new content such as updated bonus labs. Your electronic workbook will automatically retrieve any updates several minutes after the SIFT VM is booted, as well as at randomized intervals four times per day. If an update is required outside of this schedule, your instructor or OnDemand SME will provide specific instructions.

Do NOT Perform Operating System Updates

It is critical that you **do not** upgrade software within the virtual machine unless specifically directed to do so in the lab instructions. Your virtual machine has been extensively tested in the configuration which it was distributed. SANS cannot ensure your labs will function properly if the software is updated.

Completing the Setup Process

Once you have downloaded all the course materials, decompressed and booted the virtual machines, and reviewed the specific notes above about the course VMs, you will be ready for class!

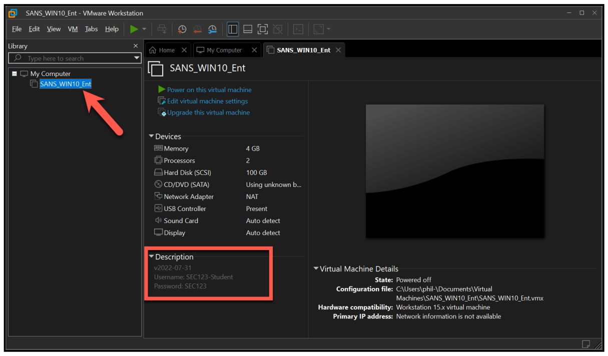
[1] Date and time format - ISO 8601: `https://for572.com/iso8601`

2. The Problem with Time & Time Zones - Computerphile - YouTube `https://for572.com/tz-probs`

Virtual Machine Credentials

The login credentials for all virtual machines used in this class are listed below for quick reference.

All login credentials are also displayed in the respective virtual machine's information panel. Below are screenshots showing the login credentials under VMware Workstation and VMware Fusion, respectively.


SANS_WIN10_Ent - VMware Workstation
File
Edit
View
VM
Tabs
Help
Library
Type here to search
My Computer
SANS_WIN10_Ent
Home
My Computer
SANS_WIN10_Ent
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine

SANS_WIN10_Ent

Devices

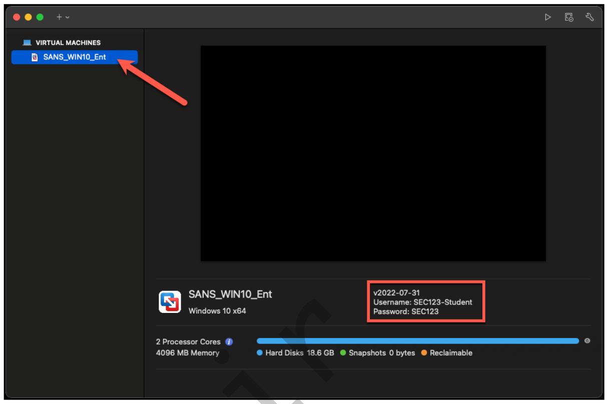
Memory	4 GB
Processors	2
Hard Disk (SCSI)	100 GB
CD/DVD (SATA)	Using unknown b...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Description

v2022-07-31
Username: SEC123-Student
Password: SEC123

Virtual Machine Details

State: Powered off
Configuration file: C:\Users\phil-\Documents\Virtual Machines\SANS_WIN10_Ent\SANS_WIN10_Ent.vmx
Hardware compatibility: Workstation 15.x virtual machine
Primary IP address: Network information is not available



SANS_WIN10_Ent
Windows 10 x64

v2022-07-31
Username: SEC123-Student
Password: SEC123

2 Processor Cores
4096 MB Memory

● Hard Disks 18.6 GB ● Snapshots 0 bytes ● Reclaimable

1. SIFT Workstation

   - Username: `sansforensics`
   - Password: `forensics`

   This user has `sudo` access for all commands on the virtual machine.

2. SOF-ELK®

   - Username: `elk_user`
   - Password: `forensics`

   This user has `sudo` access for all commands on the virtual machine.

   These credentials are for the system account used via either the console or SSH.

   There is no authentication to the Kibana dashboard.

3. Arkime

   - Username: `arkime_user`
   - Password: `forensics`

   This user has `sudo` access for all commands on the virtual machine.

   These credentials are for both the Arkime web interface and system account used via either the console or SSH.