Necessary tools

Let us start with the **installation of SIFT Workstation**.

1. We need to install VirtualBox on your host OS. Start by clicking on the following link (https://www.virtualbox.org/wiki/Downloads) and download VirtualBox for your OS. Next you should also download Oracle VM VirtualBox Extension Pack (found just under the VirtualBox installation).
2. After downloading your VirtualBox, run it and you have to manually add the Extension Pack. Start by hitting *Preferences->Extensions* and on the left side of the window you can add previously downloaded Extension Pack.
3. For the further installation, you have to visit this following link (https://digital-forensics.sans.org/community/downloads), create your account and download SIFT Workstation Virtual Appliance (latest SIFT .ova image).
4. Start VirtualBox one more time and in the top menu try to find *File->Import Appliance*; then in the following window choose your .ova image file; *Next*; give the VM some proper name (e.g. SIFT_Workstation); choose how much computing resources you want to add to this VM and click on *Import.*
5. Click on your newly created SIFT VM and go for *Settings*, here you can anytime change the computing power, but now in the *Display* section try to find *Graphics Controller* and choose *VMSVGA* and secondly navigate to *Network->Adapter 2->Enable Network Adapter*, in the section *Attached to* choose *Host-only Adapter.* Click on *OK.*
6. Now, start your SIFT VM and wait for the necessary things to be installed (do not forget to sign in, login information were mentioned on the following link https://digital-forensics.sans.org/community/downloads). After that you need to run 2 commands on your Ubuntu VM (*sudo apt-get update* and sudo *apt-get install virtualbox-guest-utils*). **NOTE** – Shared folders are not that important in order to complete this laboratory exercise. Next turn off your VM and again go for *Settings* and set-up yours Shared Folders, here you can add a folder that will be shared between guest and host operating systems (choose also the right access).
7. Start you SIFT VM again, sign in and after all the background installation is done, you can create a snapshot of your VM or the so-called clean state. This step is not that important if you doing only this one laboratory exercise. **NOTE** – before creating a snapshot, it is a copy of the current state of memory and disk, so make sure you have a few GB of space. If you want to work with SIFT workstation frequently and create a clean snapshot, navigate yourself to the top right menu *Machine->Take Snapshot.*
8. Congratulations now you have a clean SIFT workstation, which is ready to work.

Next we will install **RegRipper3.0**. Everything you need to know about this installation can be found on the following link (https://dfir-scripts.medium.com/installing-regripper-v2-8-on-ubuntu-26dc8bc8a2d3).

1. The whole script, which will do the installation for you, can be found on following link (https://raw.githubusercontent.com/dfir-scripts/installers/main/RegRipper30-apt-git-Install.sh) , so use command *wget* and the link
2. Change file execution rights *chmod +x name.sh*
3. And run the script, simply *./name.sh*
4. Now you can use RegRipper3.0 by typing command rip.pl.

NOTE – unlike in the document, we have to unfortunately use the command line version of RegRipper, but no worries it is also really simple.

Before running the RegRipper, make sure also to run the plugins_repair.sh (found on following link - https://github.com/57972887/LaboratoryExerciseWR).

Start by typing *rip.pl –r /path/to/hive/file –a > output.txt*, this will parse specified hive file and create output.txt file with findings.

Last but not least, you have to download the image from github repository (https://github.com/57972887/LaboratoryExerciseWR). You can either download only the image or clone the whole repository and then extract the image.