

# Virus Scanning and Backups

In this tutorial we're going to conduct maintenance on an Operating System by scanning the OS for any potential infections and by creating backups. We'll record our findings and *clean* the system by removing infections using the Virus Scanner and restoring Backups where necessary, using the installed OS tools. Follow these steps to conduct the maintenance. Then submit your completed documents for assessment.

All testing will be performed in a *Virtual Machine (VM)*. A VM can be thought of as a computer inside a computer. Essentially, a VM runs on a host computer inside virtualisation-software. We'll use **Virtual Box** to host an instance of the Linux OS. The power of VMs come from the fact that we can sandbox/isolate the VM. We can also save the VM as a file on the host computer, make copies of the file and thus create copies of the VM, with all its files and settings.

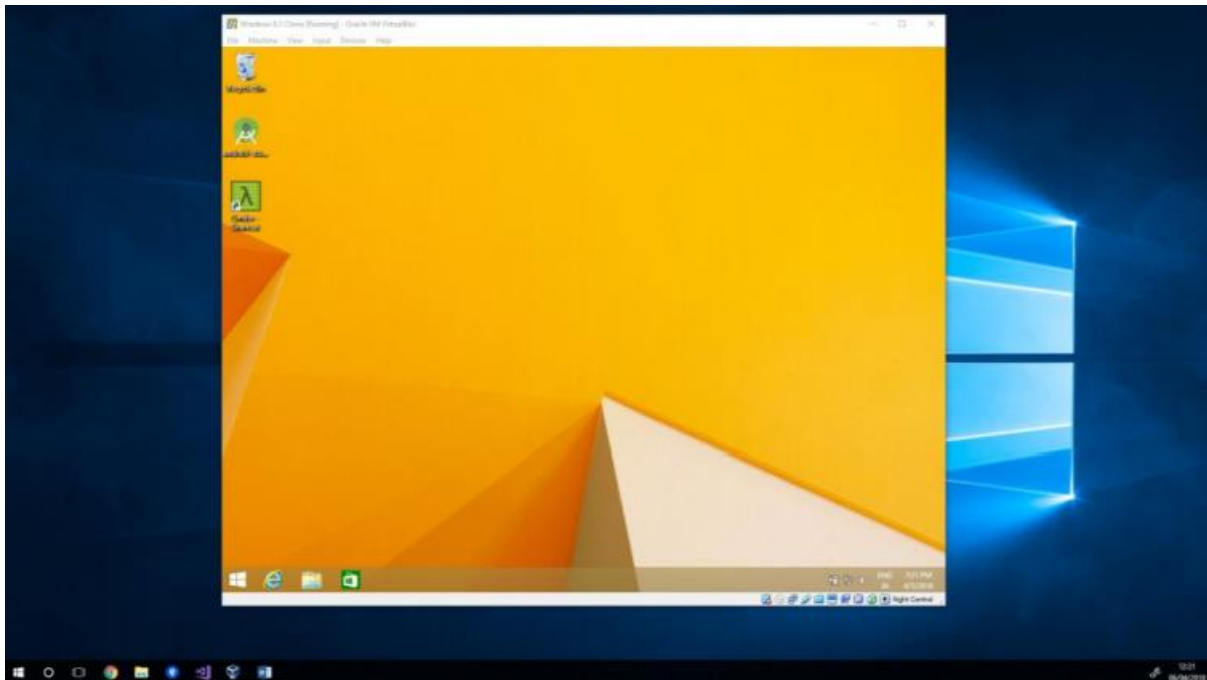
**NOTE:** The document "*Assessment - Virus Scanning and Backups.docx*" *is to be completed and submitted as part of your final assessment*. Make sure you take plenty of screenshots as you work through this tutorial as evidence.

## Contents

Step 1: Installing Virtual Box (Optional).....	2
Step 2: Installing the pre-configured Virtual Machines .....	3
Option 1 (from .ova file): Importing a Virtual Box appliance.....	3
Option 2 (from zip-file): Adding existing Virtual Machines.....	3
About the Virtual Machines .....	4
Step 3: Starting a Virtual Machine .....	5
Step 4: Creating a System Backup.....	6
Step 5: Using Anti-Virus Software (on a <i>CLEAN</i> system).....	8
<i>A note on updating virus signatures</i> .....	8
Step 6: Using Anti-Virus Software (on an <i>INFECTED</i> system) .....	9
Step 7: Restoring a System Backup.....	11
Appendices.....	13
Appendix 1: Finding pre-configured Virtual Machines .....	13
Appendix 2: Creating a New Virtual Machine.....	13
Appendix 3: Installing & Configuring ClamAV .....	14

## Step 1: Installing Virtual Box (Optional)

Note: VirtualBox is already installed on the AIE network. Skip this step if Virtual Box is already installed on your machine.

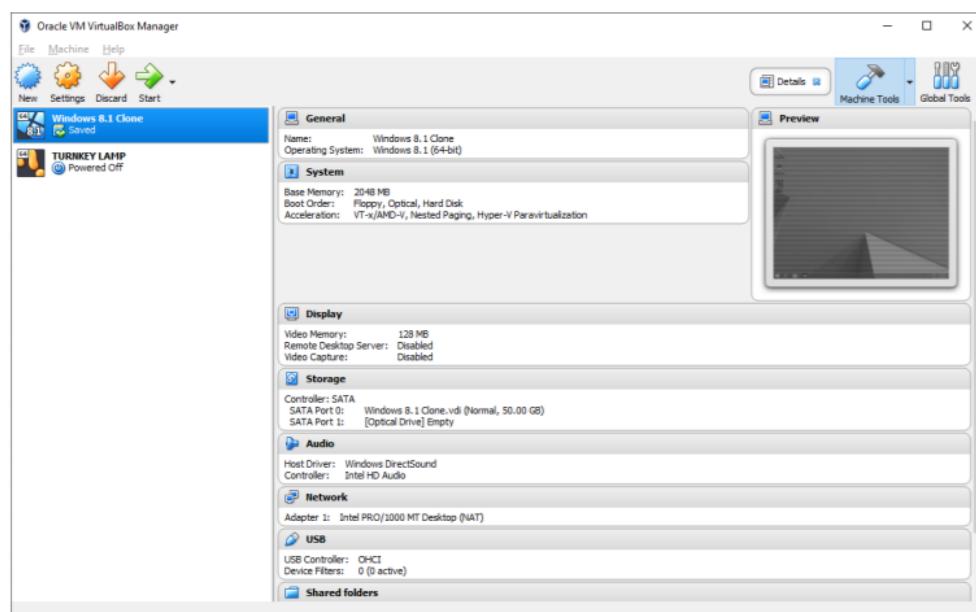


*Windows 8 running within a Virtual Box window on Windows 10*

Visit the VirtualBox website to download the latest version of the software:

<https://www.virtualbox.org/wiki/Downloads>

Install the software and follow the prompts. Once Virtual Box is installed you should see a screen like the following. The list on the left includes your collection of VMs. The right panel shows details for the currently selected VM.



## Step 2: Installing the pre-configured Virtual Machines

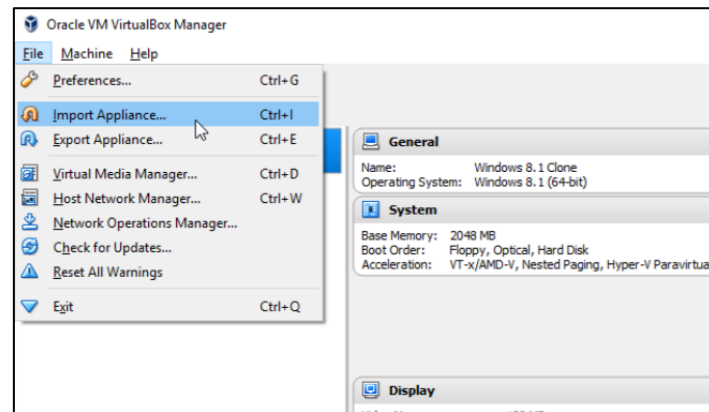
We'll use *pre-configured VMs* for this tutorial which include *Linux Mint* already installed and prepared in different configurations. This will reduce the amount of work required, but feel free to explore creating your own VM and then installing an operating system from an ISO-file outside of class.

1. Download the preconfigured Virtual Machines from *AIE's Canvas Platform*. It will be available in **one of the following formats**:
  - a. **Virtual Box Appliance file** : *LinuxMint-AIE-VirusScanningAndBackups.ova*
  - b. **Standard zip file**: VirtualBox 6.1.2 - Linux 32-bit.zip

### Option 1 (from .ova file): Importing a Virtual Box appliance

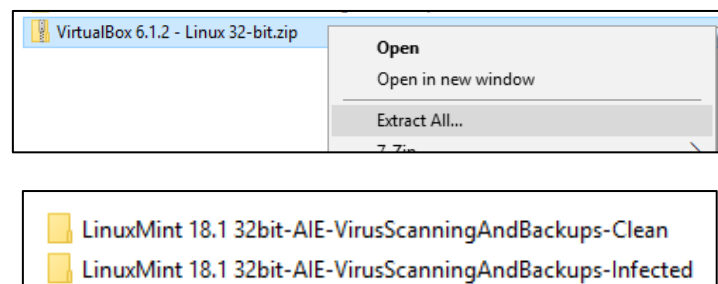
If you downloaded the .ova file, then follow this procedure to add the Virtual Machine to Virtual Box

1. Import the .ova appliance into VirtualBox via the **"File->Import Appliance"** menu

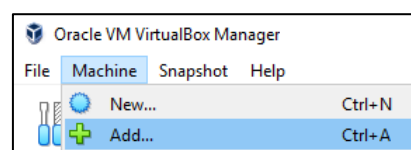



### Option 2 (from zip-file): Adding existing Virtual Machines

1. Extract/Unzip the Virtual Machines from their zip-file to your local computer. This should result in 2 new folders on your computer.



2. In Virtual Box, click the **"Add"** button or use the **"Machine->Add"** menu, and browse to the .vbox file for each Virtual Machine

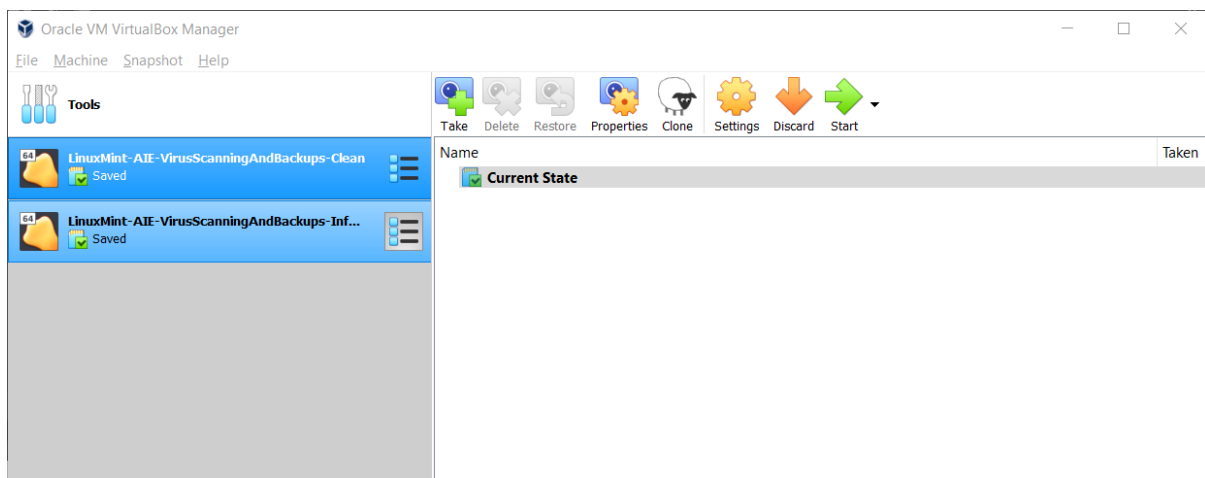


 LinuxMint 18.1 32bit-AIE-VirusScanningAndBackups-Clean.vbox

### About the Virtual Machines

The installed VM Appliance includes **2 separate configurations** of the Linux Mint Operating System. You should now have 2 VMs ready for use which represent Linux installations in different initial states. The names should be something like this:

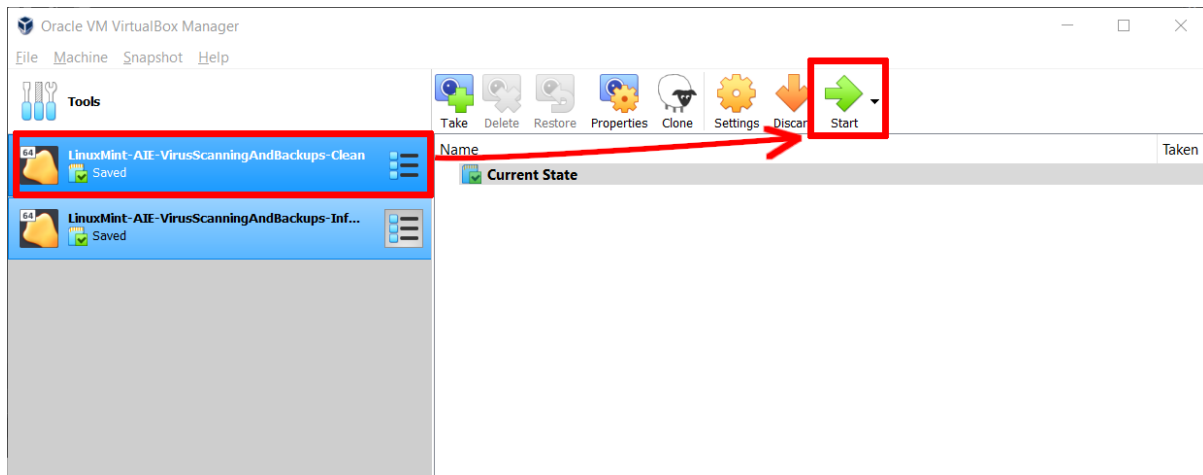
- a. *LinuxMint-AIE-VirusScanningAndBackups-Clean*
- b. *LinuxMint-AIE-VirusScanningAndBackups-Infected*



### Step 3: Starting a Virtual Machine

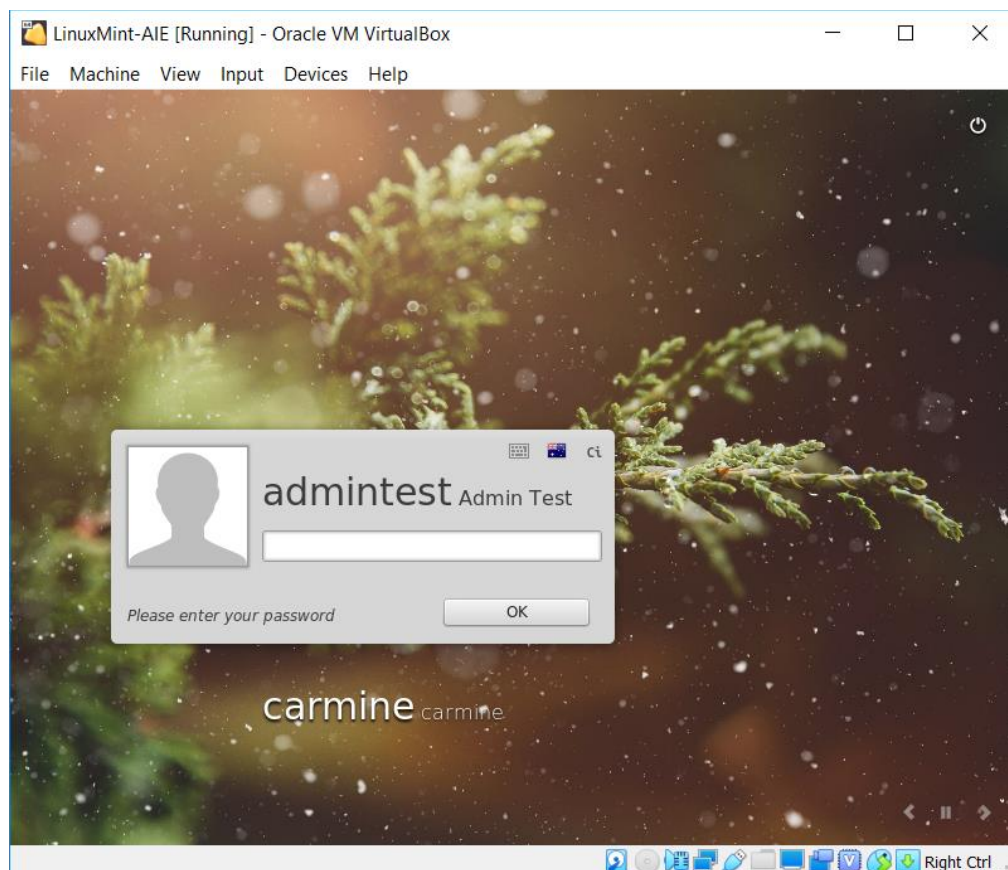
Start the **CLEAN** Virtual Machine by following these steps:

1. Select the “xxx-VirusScanningAndBackups-Clean” Virtual Machine
2. Then press the **Start** button



Once the VM has booted up, you'll be presented with the *Login screen*.

- Use the AIE **admintest** account, **password** “admin1234”



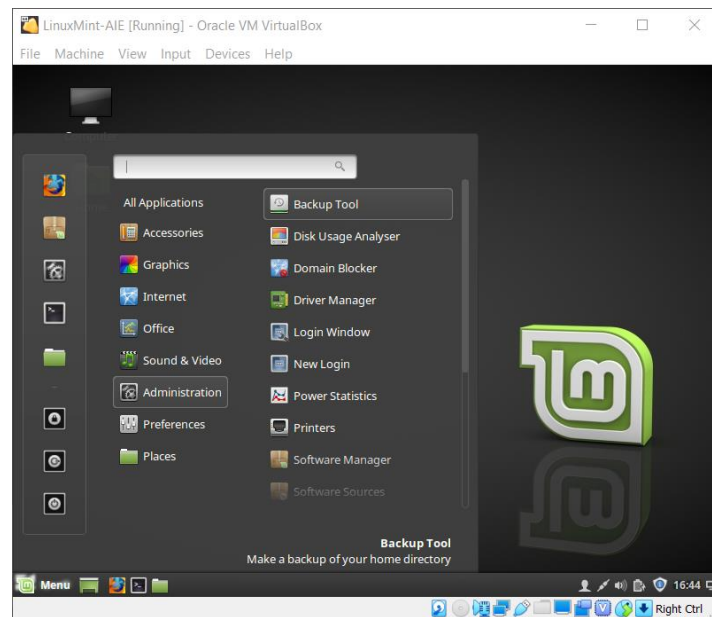
## Step 4: Creating a System Backup

Our first step is to **create a backup** of our *Documents* directory using the *Linux Backup Tool*. Backups are an important part of any maintenance process to ensure that we can restore our system to a previous state should it ever become corrupted or compromised.

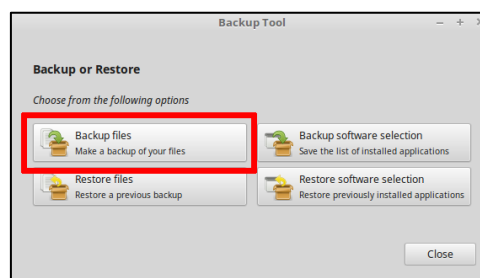
Note that this VM already has a previous backup created - two existing folders on the VM Desktop with *briefcase icons* indicating they're *Backup Archives*.

**Let's create a new backup** by following these steps:

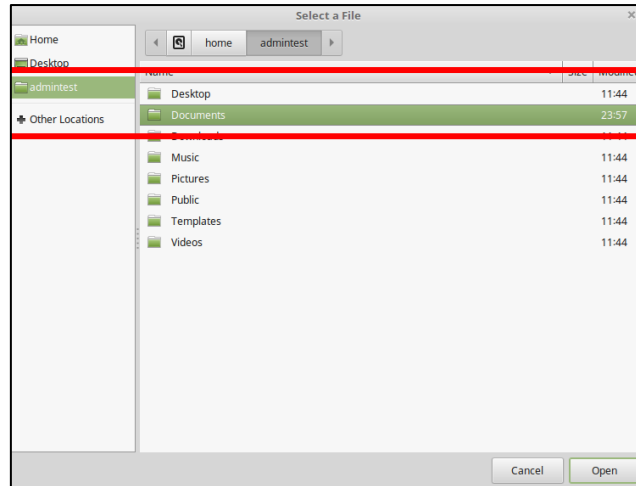
1. Open the **Backup Tool** from the **Administration** sub-menu
  - a. You'll need to re-enter the admin password to manage this software



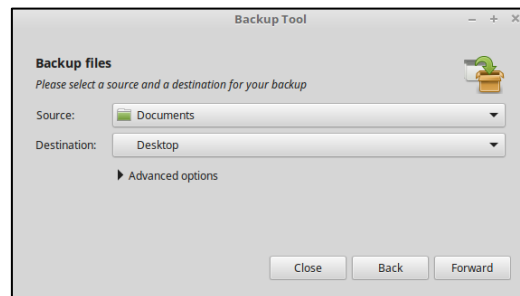
2. We'll be making a backup of our files; Select the "**Backup Files**" option
  - a. Note that you can also make backups of installed applications



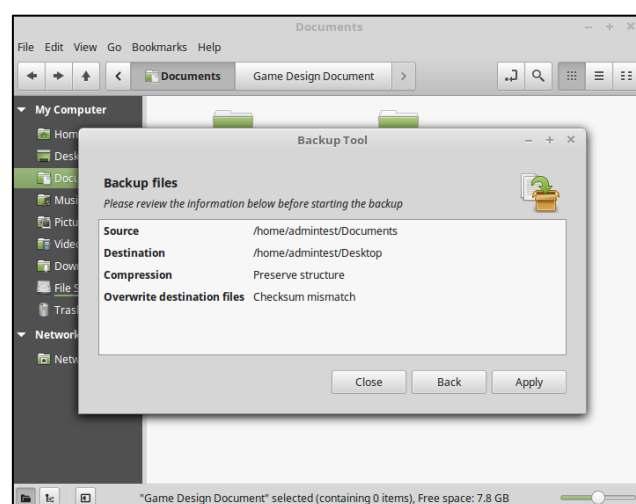
3. For the **Source** option, select "**Other**". Then select the "**admintest->Documents**" folder. This is the *Documents* folder for the *admintest* account.



4. For the **Destination** option, select “**Other**”. Then select the “**admintest->Desktop**” folder. Normally we’d select a secure server as our backup destination to ensure it remains safe. But for this test, we’ll simply store our backup on the Desktop.



5. Press the **Forward** button to continue with the Backup wizard
6. Check that you have the following settings, and then press the **Apply** button to start the backup



7. You’ll receive a message indicating that the backup was a success!
8. Feel free to explore the Backup Tool in greater detail and try backing up other folders. Note that the Backup Tool ignores empty folders.

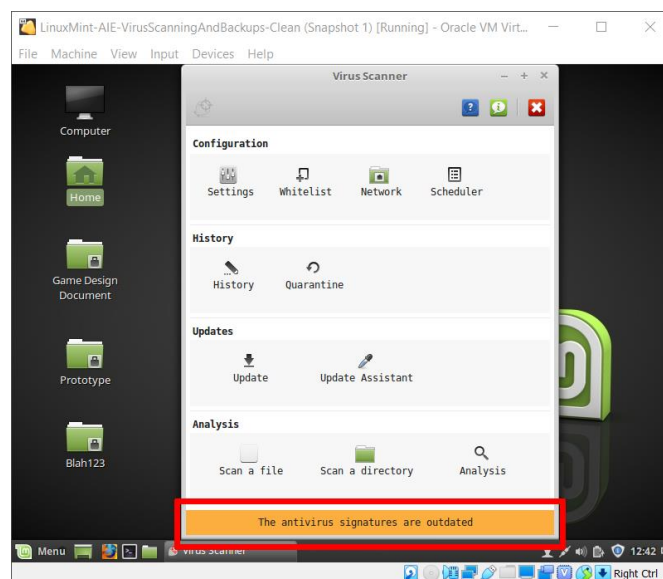


## Step 5: Using Anti-Virus Software (on a *CLEAN* system)

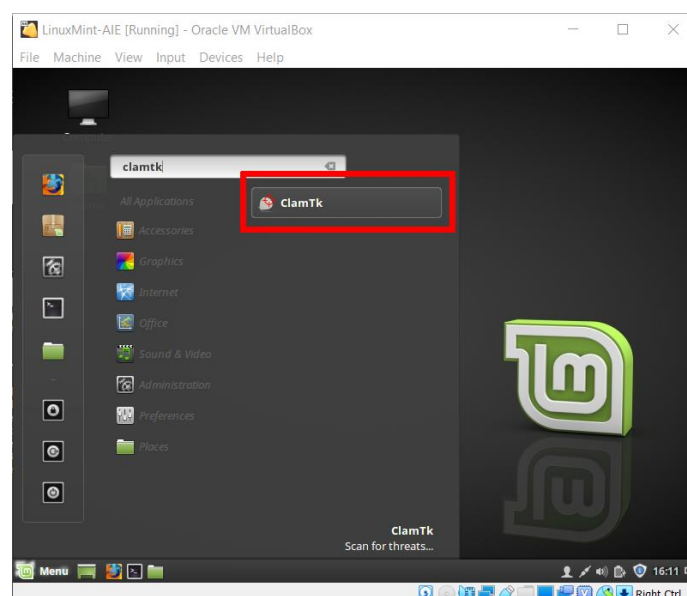
*ClamAV* has already been installed on the Virtual Machines and we'll use it for this tutorial. We'll run the Anti-Virus software using the ClamTk user-interface. We'll continue to work with the “**xxx-AIE-VirusScanningAndBackups-Clean**” Virtual Machine for this step.

### A note on updating virus signatures

Anti-Virus software maintain a database of *signatures* for the latest known infections. It's important to keep these signatures up-to-date to ensure the anti-virus software can monitor/detect the latest threats. ClamTk indicates when the signatures are out-of-date on its status-bar. Use the **Update** button to refresh the AV database (a network connection is required).

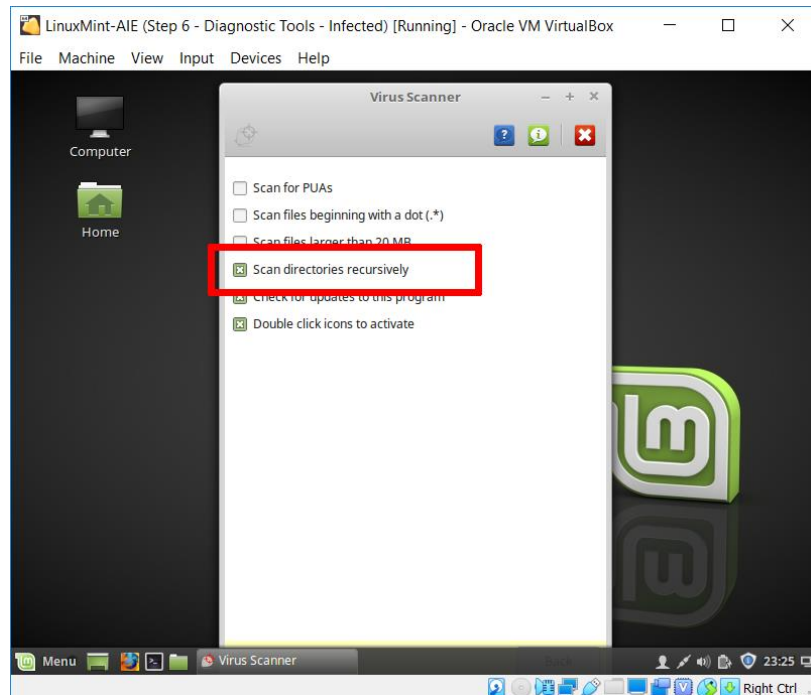


1. Search & open the “**ClamTk**” application from the *Taskbar Menu*

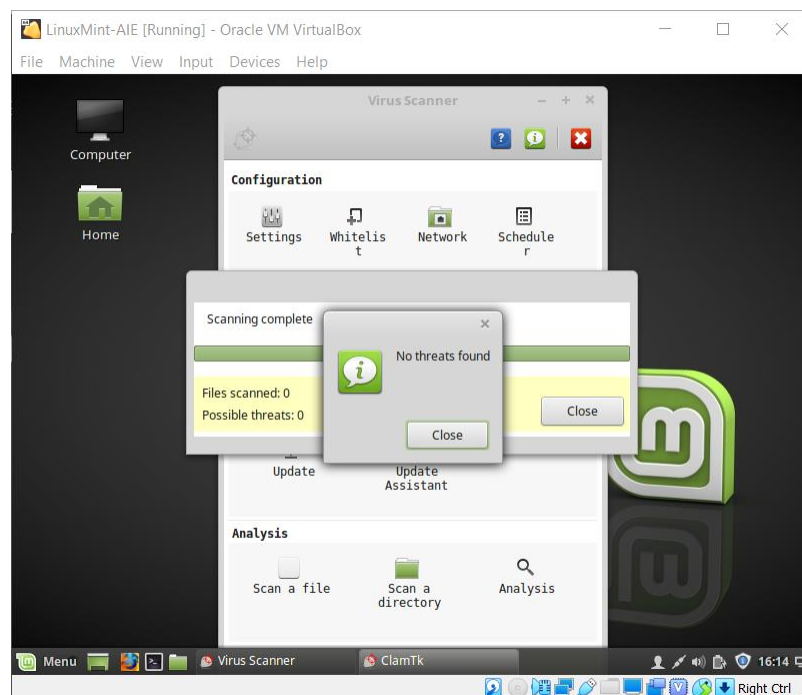




2. Open the “**Settings**” menu and enable the “**Scan directories recursively**” option, so that the scanner will check all sub folders in the selected directory



3. From the ClamTK main menu, select the “**Scan a Directory**” option, then select “**admintest**” folder to commence the scan.
4. Wait for the scan to complete ... this may take some time.
5. You should see output like this indicating that the system is currently clean:

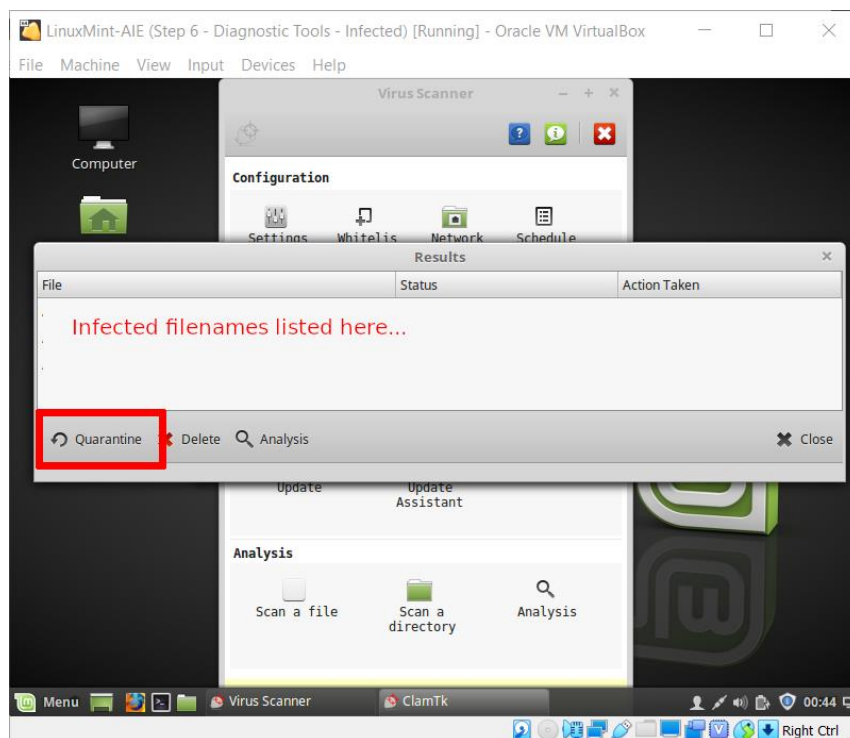


## Step 6: Using Anti-Virus Software (on an *INFECTED* system)

*Notes about this VM:* This VM has the ClamAV Anti-Virus Software already installed and has special *test-files* installed to check the Anti-Virus software. This VM **does not include any actual viruses or malicious software** – only test-files. Anti-virus test files can be sourced from the following website: [https://www.eicar.org/?page\\_id=3950](https://www.eicar.org/?page_id=3950)

We're now going to start a *different* Virtual Machine with test-files already installed for the Anti-Virus software to detect. Follow these steps, just like in Step 1:

1. Shutdown the currently running VM (The one started in Step 1)
2. Select the “**xxx-AIE-VirusScanningAndBackups-Infected**” Virtual Machine
3. Then press the **Start** button
4. Once the Virtual Machine is running, open the **ClamTK** Anti-Virus software.
5. **Perform an anti-virus scan** on the “**admintest**” home folder
6. **Record the results of the scan**, including infections detected and their locations.
  - a. You should locate three separate infected files
  - b. Record the infected filenames, and their folders
  - c. Take a screenshot of your results
7. **Quarantine** each infected file and **request supervisor approval** before deleting.

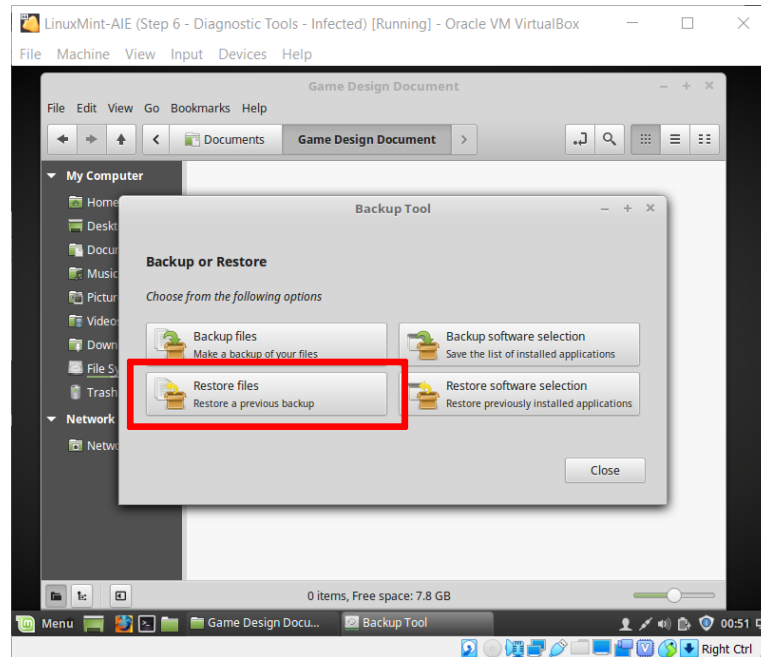


8. After receiving confirmation from a supervisor, you may **delete the infected files** from the “**History->Quarantine**” menu

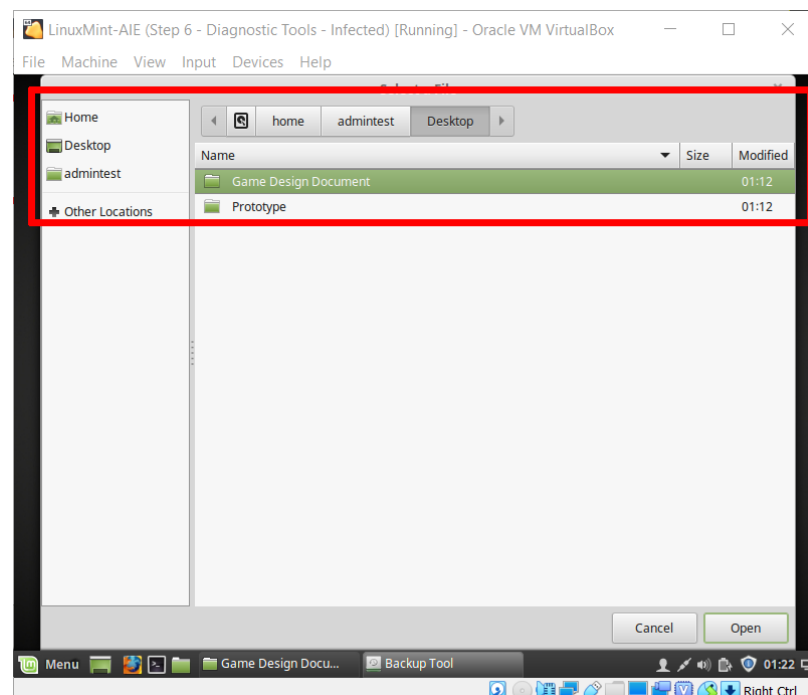
## Step 7: Restoring a System Backup

Some of the infected files from the previous step were in the Documents folder. We'll need to use a *backup* to restore the original files. Follow these steps to restore files from a backup:

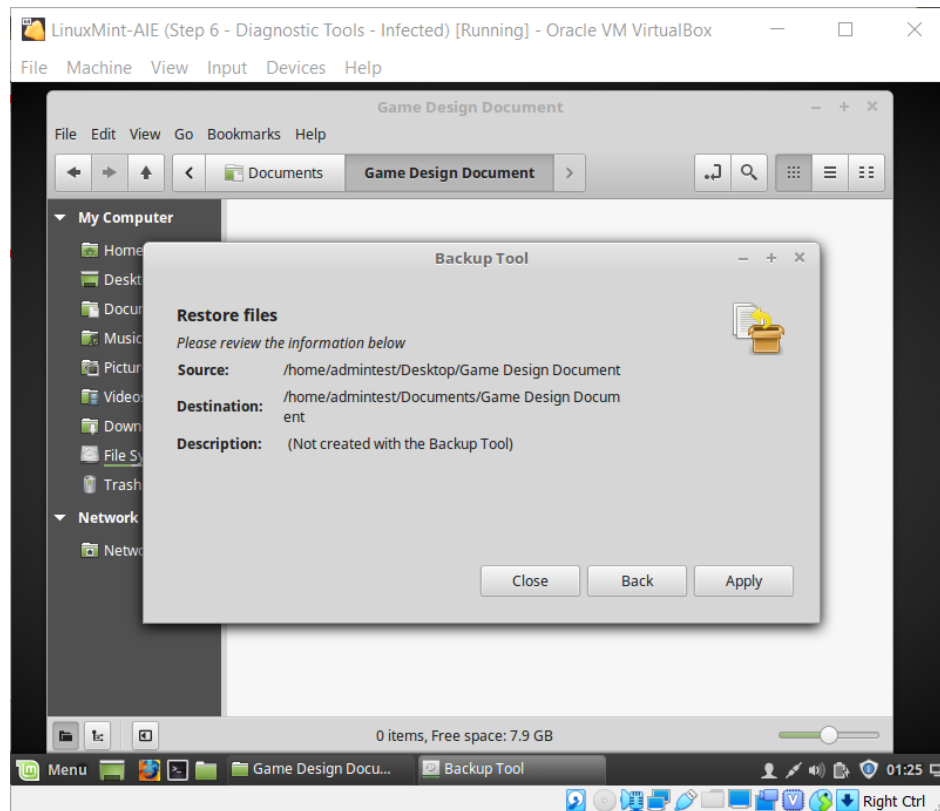
1. Open the Backup Tool from the Menu, just like in Step 4.
2. Select the “Restore files” option



3. Make sure that the “Directory” option is selected
4. Press the “Source” button and select “Other” location. **Navigate to “/home/admintest/Desktop/Game Design Document/”**



5. Press the **“Destination”** button and select **“Other”** location. **Navigate** to the **“/home/admintest/Documents/Game Design Document”** folder.
6. The *Restore Files* settings should look like this:



7. Press the **Apply** button to complete the restore.
8. Check that the **“GDD.txt”** file has been restored in the **“Documents/Game Design Document”** directory.

## Appendices

### Appendix 1: Finding pre-configured Virtual Machines

Other pre-configured VMs are available from TechNetwork by Oracle and TurnKeyLinux:

<https://www.oracle.com/technetwork/community/developer-vm/index.html>

<https://www.turnkeylinux.org/>

Windows 10 installers can be found on the Microsoft support website. Note that you should download the .iso installer file to install the OS into a new VM:

<https://support.microsoft.com/en-us/hub/4338813/windows-help?os=windows-10>

Linux installers can be found in many different distros. Linux Mint is a great distro with a clean, simple interface:

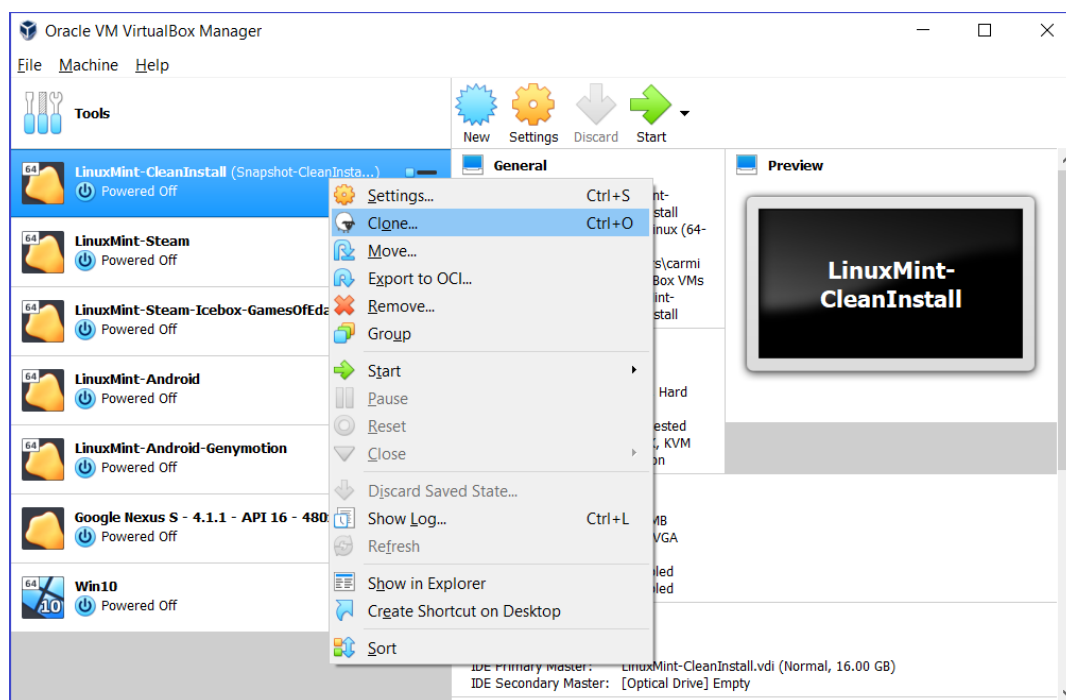
<https://www.linuxmint.com/>

### Appendix 2: Creating a New Virtual Machine

Note: We'll use a pre-configured VM for this tutorial to limit the amount of work required. But feel free to install VirtualBox at home and explore VMs in more depth.

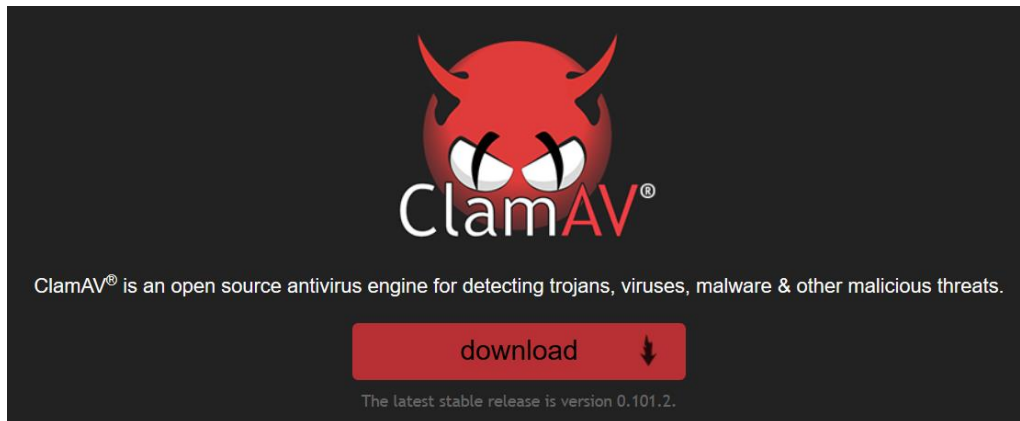
To create a new VM, simply press the **New** button and follow the wizard to specify what sort of hardware you'd like the new VM to simulate including hard-disk size and memory. This is a quick process – Note that no Operating System has yet been installed. Other settings can be modified once the VM has been created via the **Settings** button.

You can also **Clone** an existing VM from your list of available VMs to create an exact copy of an existing VM. The cloned VM can then be started as a separate machine.



## Appendix 3: Installing & Configuring ClamAV

ClamAV is a popular Open-Source Anti-Virus software for Linux, available from <https://www.clamav.net/>.



There's lots of alternatives for Virus Protection Software on Linux. Linux OS is vulnerable to malicious attacks, just like Windows, and as such should be protected from viruses, malware and rootkits

To install ClamAV into a clean Linux Distro follow these steps:

1. Open a Linux Terminal
2. Type "**sudo apt-get update**" to update the OS
3. Type "**sudo apt-get install clamav**" to install ClamAV
4. Type "**sudo apt-get install clamtk**" to install a third-party GUI for ClamAV
5. Type "**sudo freshclam**" to download the latest ClamAV virus-definition files

This website has a good description of the process:

<https://www.linux.com/learn/intro-to-linux/2017/9/security-tools-check-viruses-and-malware-linux>