

CAINE Installation Guidelines

CAINE (Computer Aided INvestigative Environment) is as a live Linux distribution specifically designed for digital forensics. It is based on Ubuntu 64 bits. The same set of tools covered by Caine can be found in Kali, under the forensics section.

This tutorial is based on Caine v.7.0. The latest release v10.0, but it is unstable. There are also two other releases Caine v 8.0 and 9.0. The installation process for all the release except v10.0 are the same. We are using version 7.0 because of the great support and tutorials available for this version.

Caine v 7.0 works fine on VMWare, so the installation instructions will be based on VMWare, although the same steps can be followed (after creating the VM) whether you are using Virtualbox or VMWare. Virtualbox extensions (shared folder, USB, etc.) do not work well for Caine v7.0. Since these will be important in forensic analysis, it is better to deploy v7.0 on Caine. Caine v6.0 works fine in both VMWare and Virtualbox.

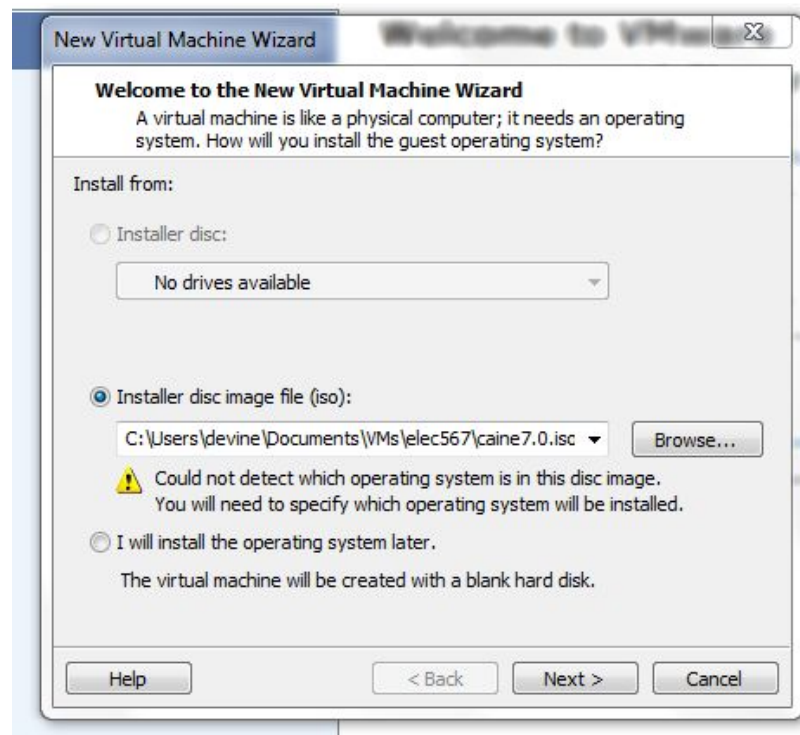
Caine Installation

You can download VMware Workstation player v12 or later, the most recent version is version 15.0

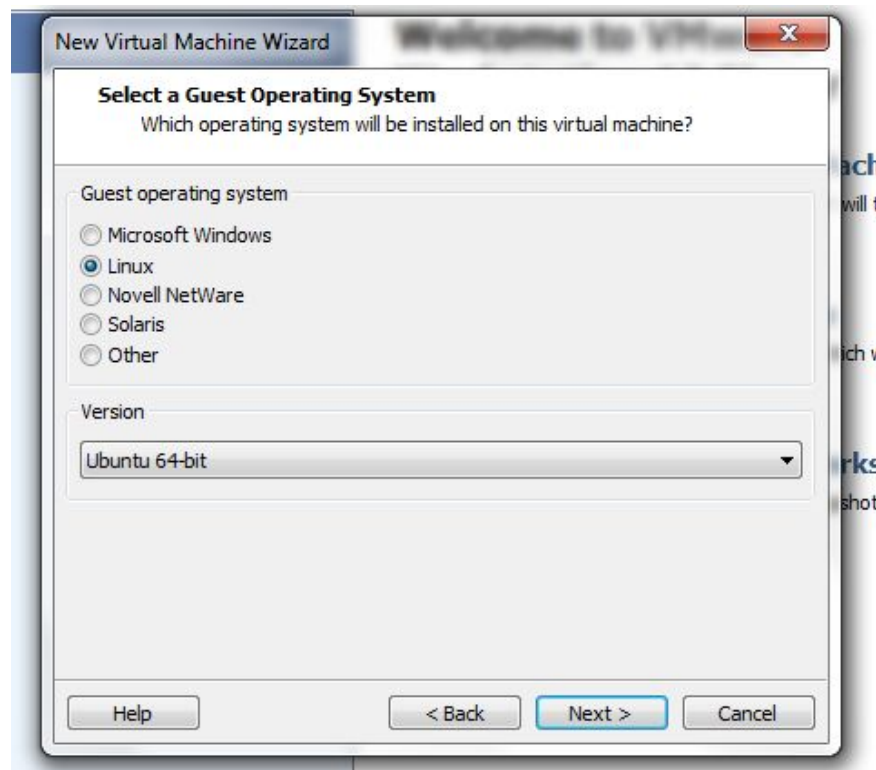
https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/15_0

You can download Caine v7.0 at <https://caine.mirror.garr.it/mirrors/caine/caine7.0.iso>

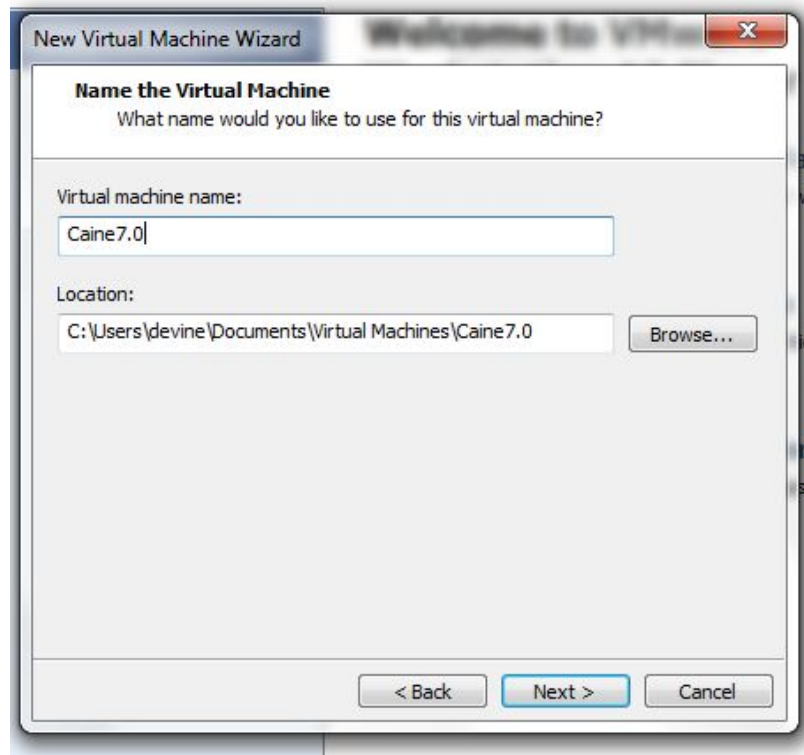
Start VMWare Player, and create a VM by loading the downloaded Caine ISO:



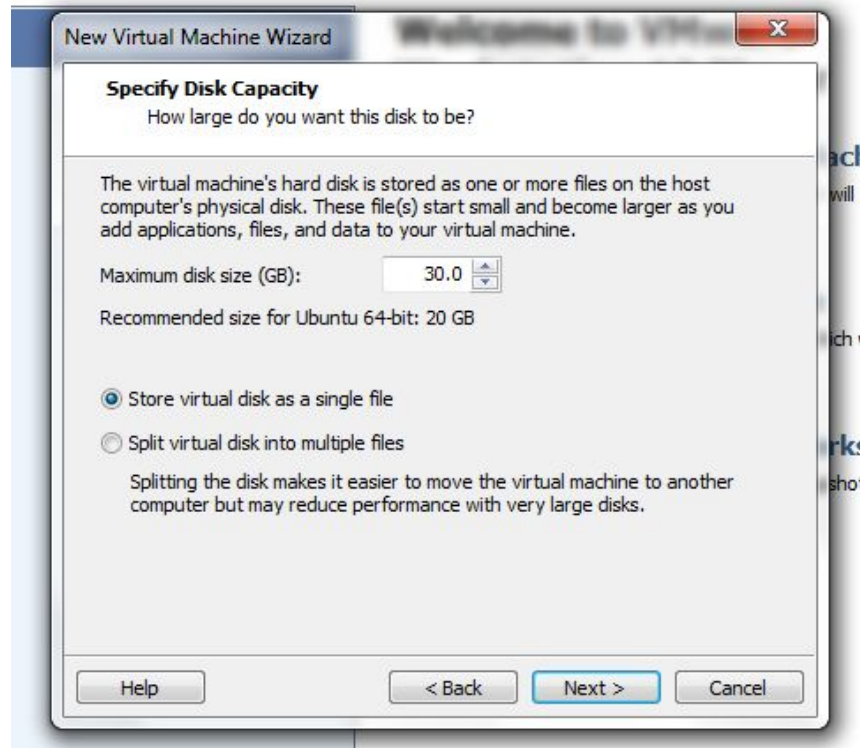
Click Next, and select the Linux as the guest OS and Ubuntu 64 as the version:



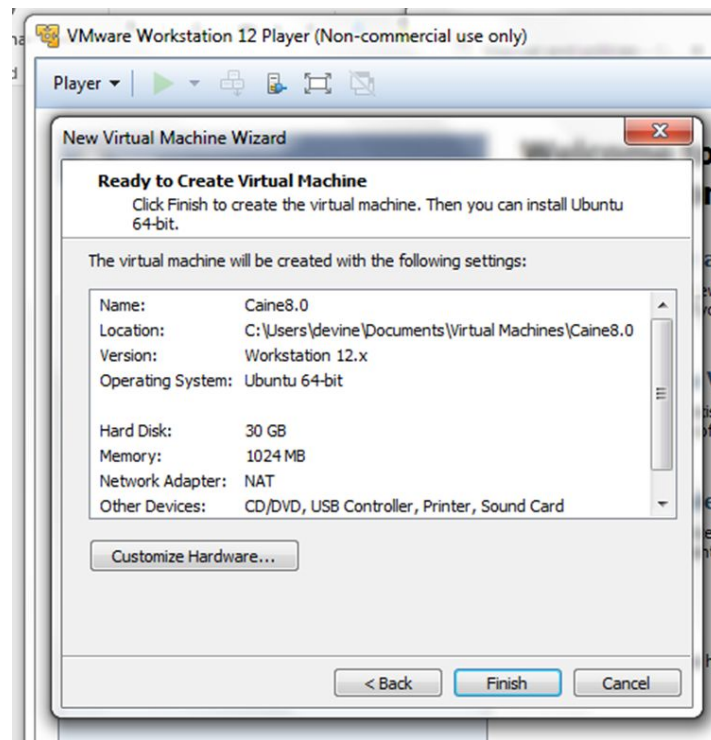
Next, name the VM (any name is fine) and specify the location to store the VM (you can keep the default location):



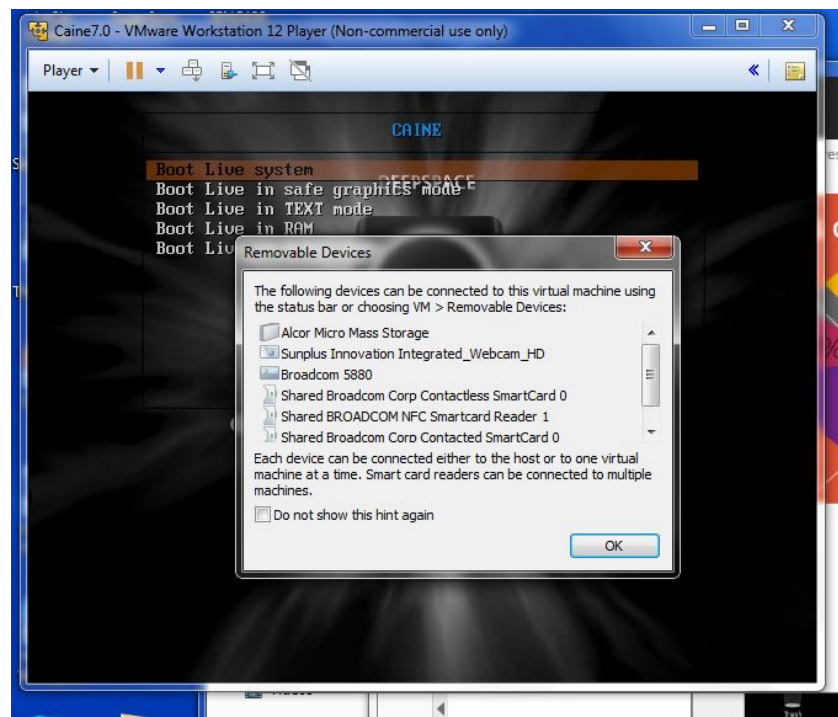
Click Next and specify disk size (30 GB or more), and select Store virtual disk as a single file:



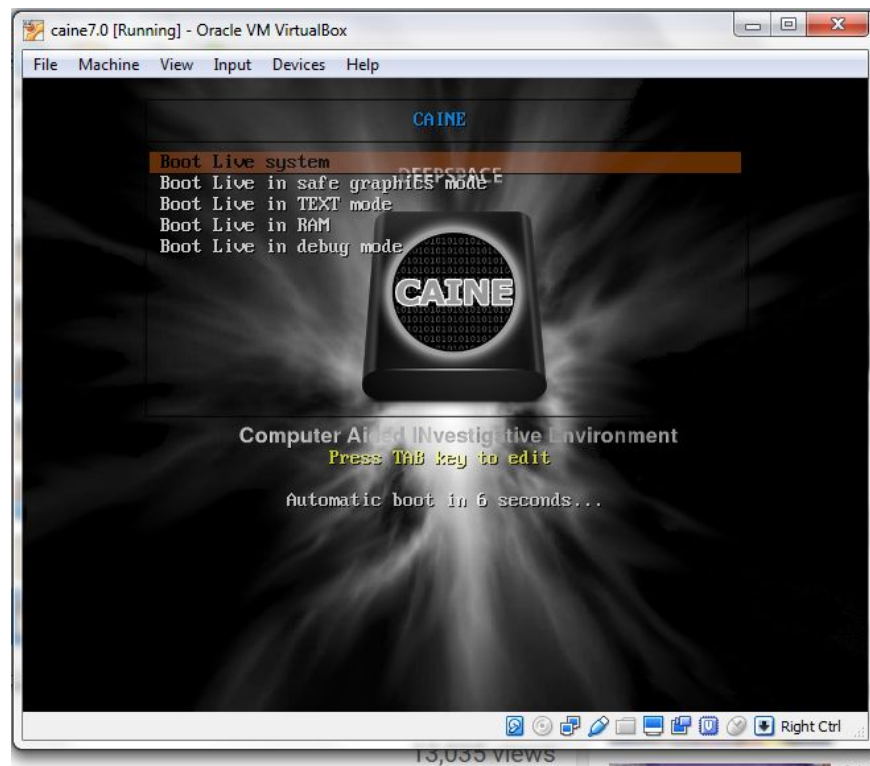
Next, keep the default hardware settings and make sure that memory is at least 4096 MB:



Click Next, to start the VM, and finalize the setup. The following window will be displayed:

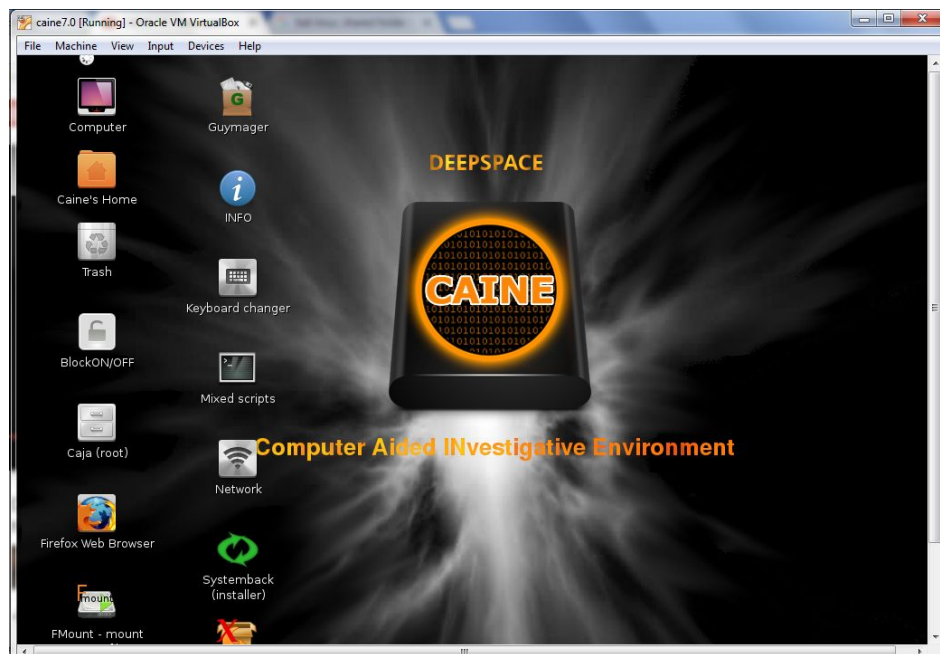


Click Ok, and choose 'Boot Live system' in the displayed start-up menu. Caine will now boot from the Live CD; be patient as this may take a little while.



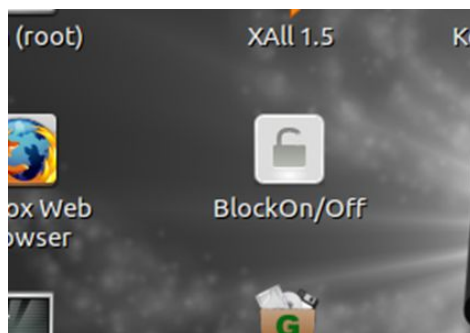
In case where it doesn't boot properly; shutdown the Caine VM, and restart.

After the live CD is booted, the Caine desktop will be displayed, as shown below:

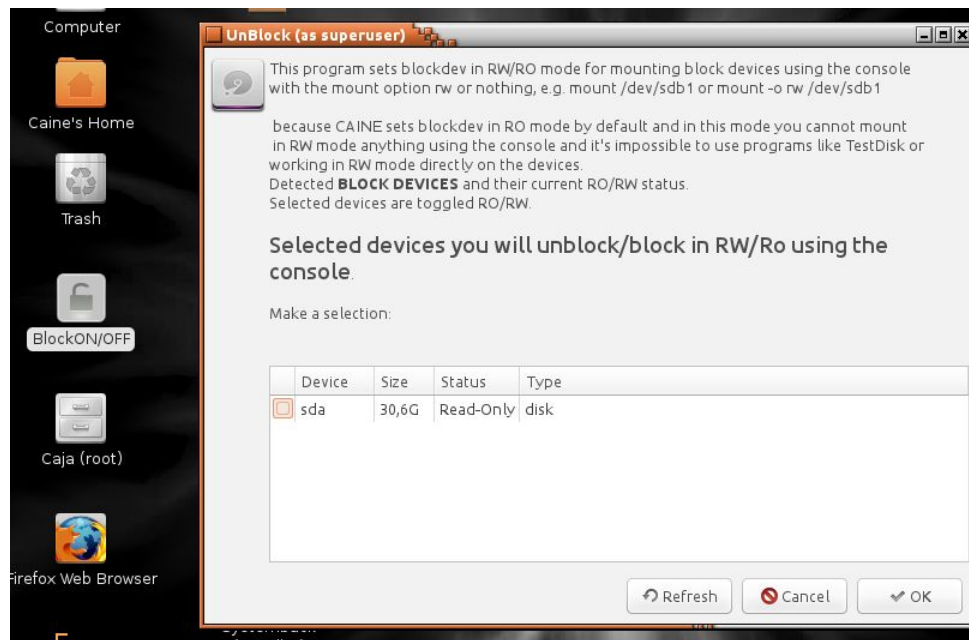


The next step is to install Caine on the virtual disc. This is done using the SystemBack tool which is located on the desktop.

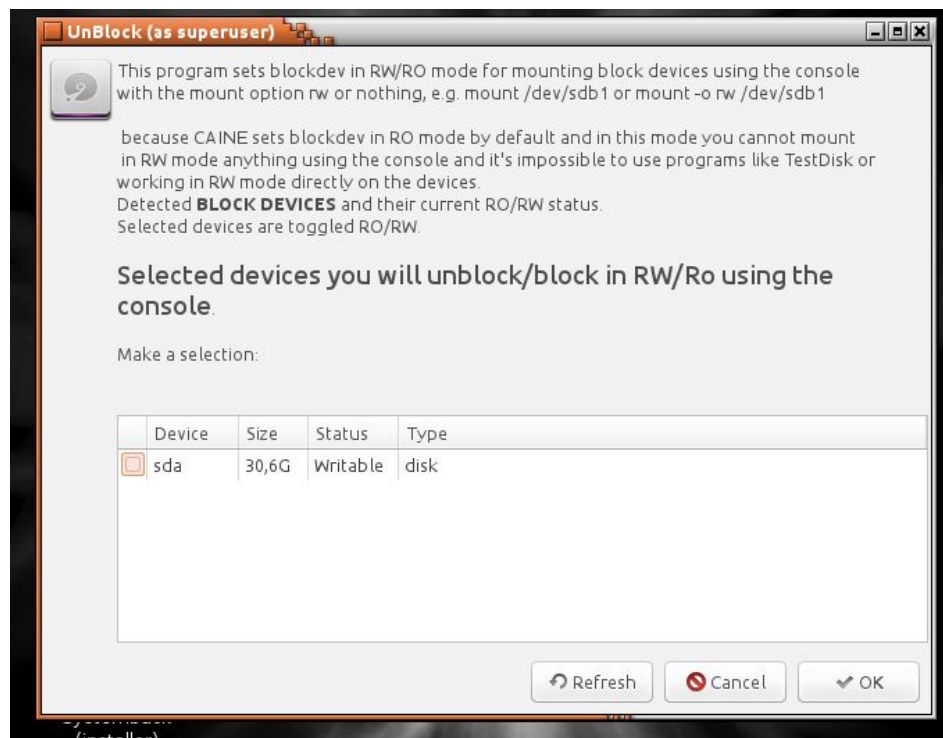
Before we can install Caine on the virtual drive we need to unlock it first with a tool on the desktop named **BlockOn/Off**. Click on the corresponding icon to unlock.



The following panel will be displayed. Select **sda1** (use the small selection box before the device name) and press the OK button:

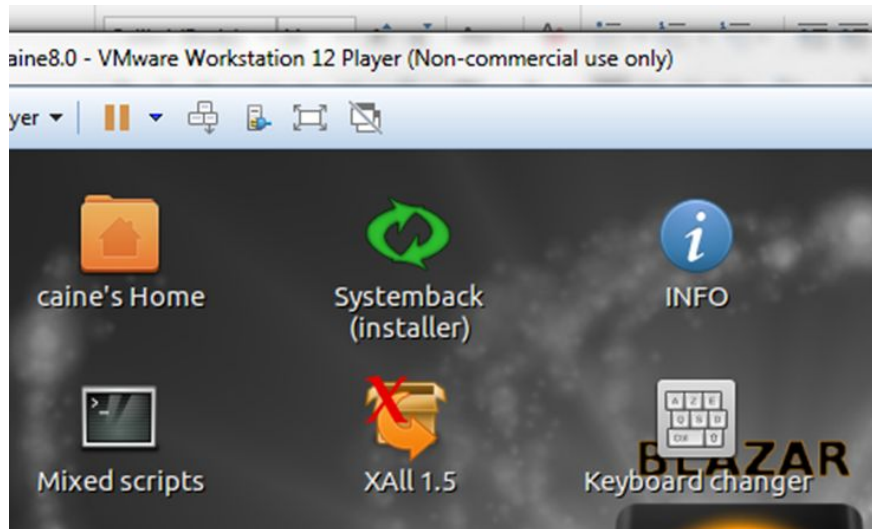


This will change the device status from Read-Only to Writable, as shown below:

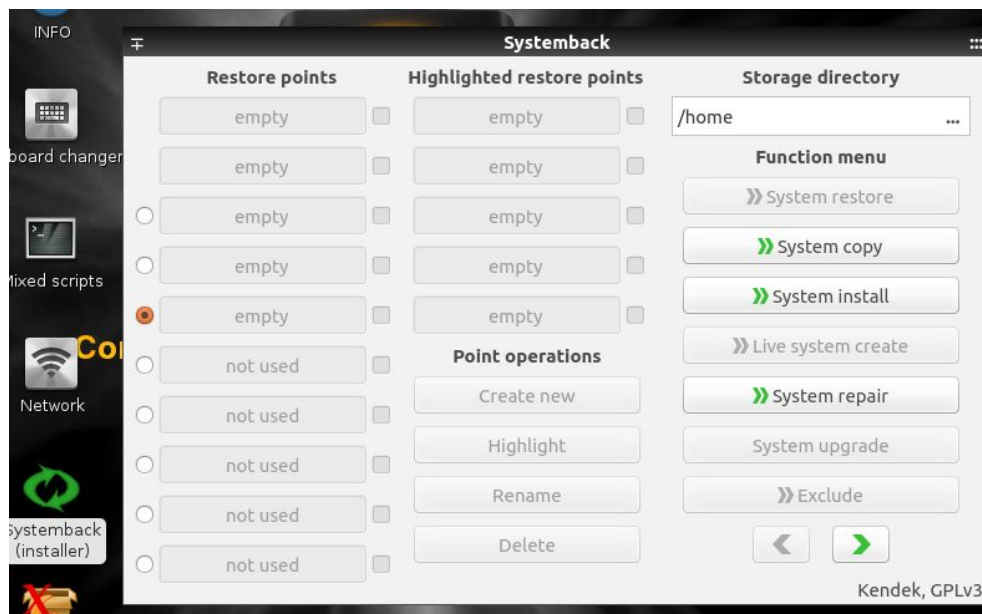


Iconize the above window (don't click on Ok; as it will go back to the previous state; I think this is a bug).

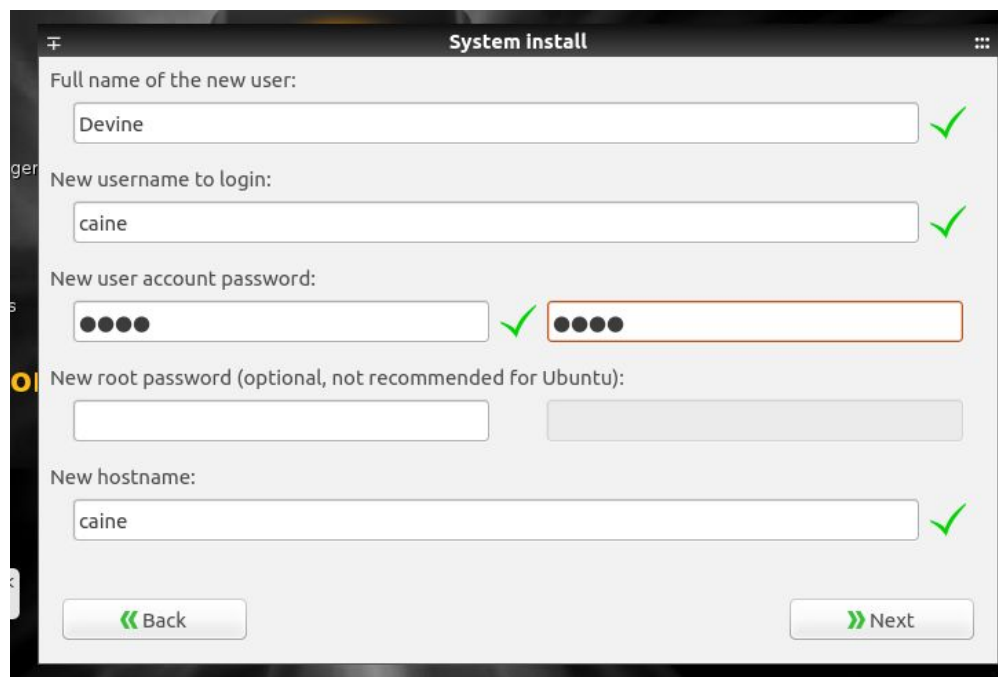
The next step is to start the SystemBack tool, which is located on the desktop:



Click on the Systemback icon, and choose for 'System install' in the menu on the right side of the following window:



The next step, is to create a new system account for the system install. Enter the requested information and press the 'next' button:

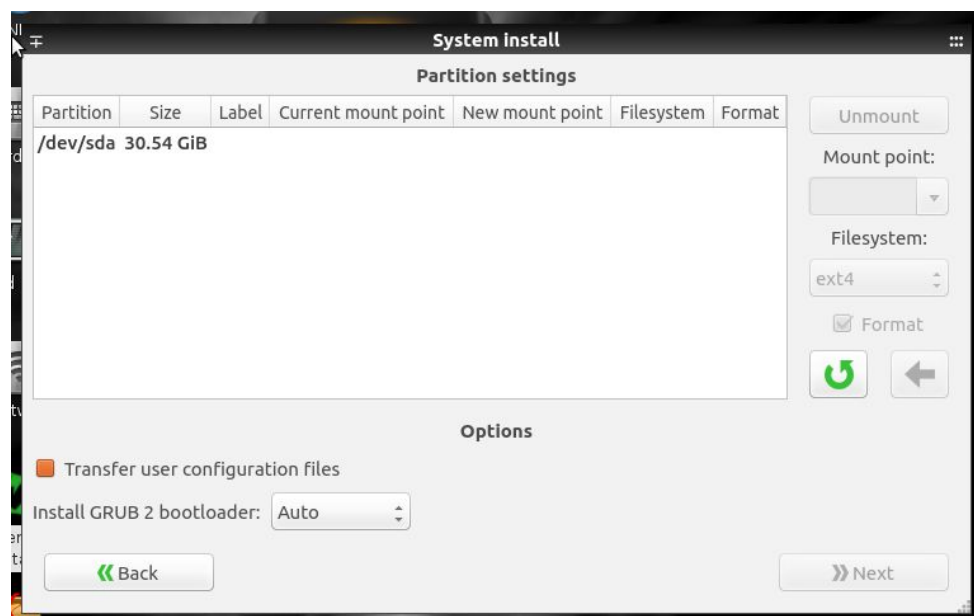


The 'System install' window displays the following configuration fields:

- Full name of the new user: Devine ✓
- New username to login: caine ✓
- New user account password: [masked] ✓ [masked]
- New root password (optional, not recommended for Ubuntu): [empty] [empty]
- New hostname: caine ✓

Navigation buttons: « Back and » Next.

Now, we need to create a partition to install Caine on it.



The 'System install' window shows the 'Partition settings' section with a table of available partitions:

Partition	Size	Label	Current mount point	New mount point	Filesystem	Format
/dev/sda	30.54 GiB					

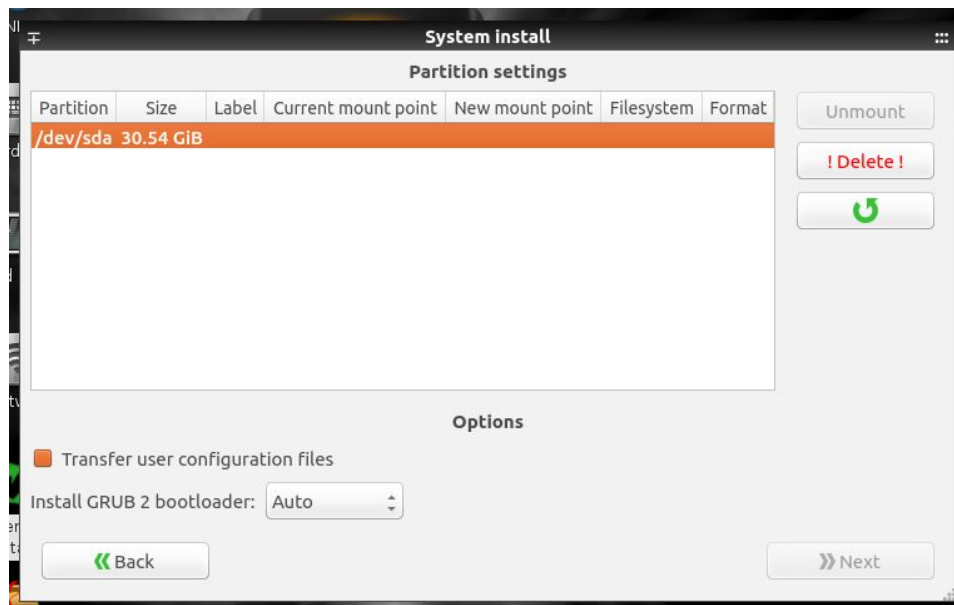
On the right, the 'Mount point' is set to /, the 'Filesystem' is set to ext4, and the 'Format' checkbox is checked. There are 'Unmount', 'Format' (green circular arrow), and 'Back' (grey arrow) buttons.

The 'Options' section at the bottom includes:

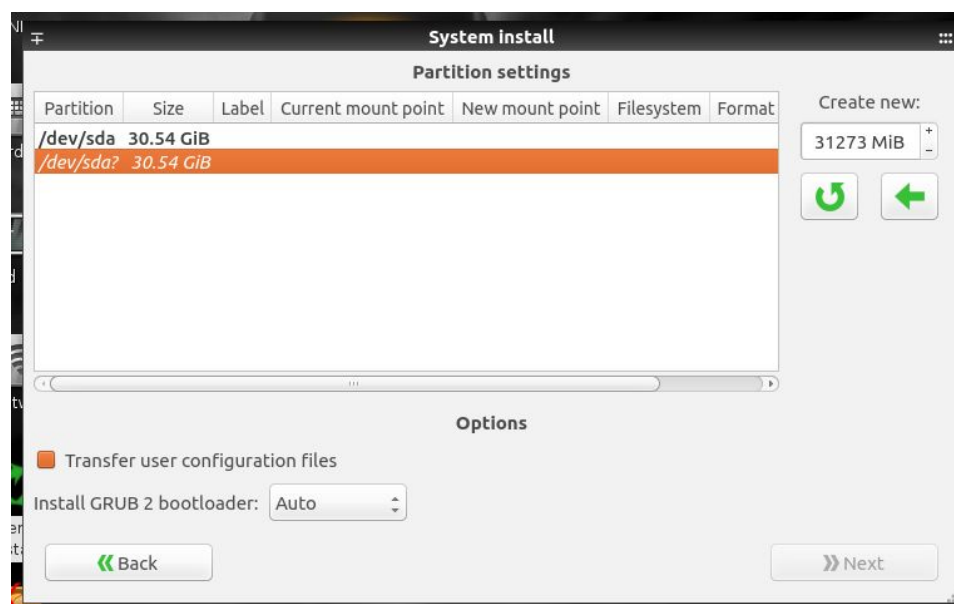
- ☒ Transfer user configuration files
- Install GRUB 2 bootloader: Auto

Navigation buttons: « Back and » Next.

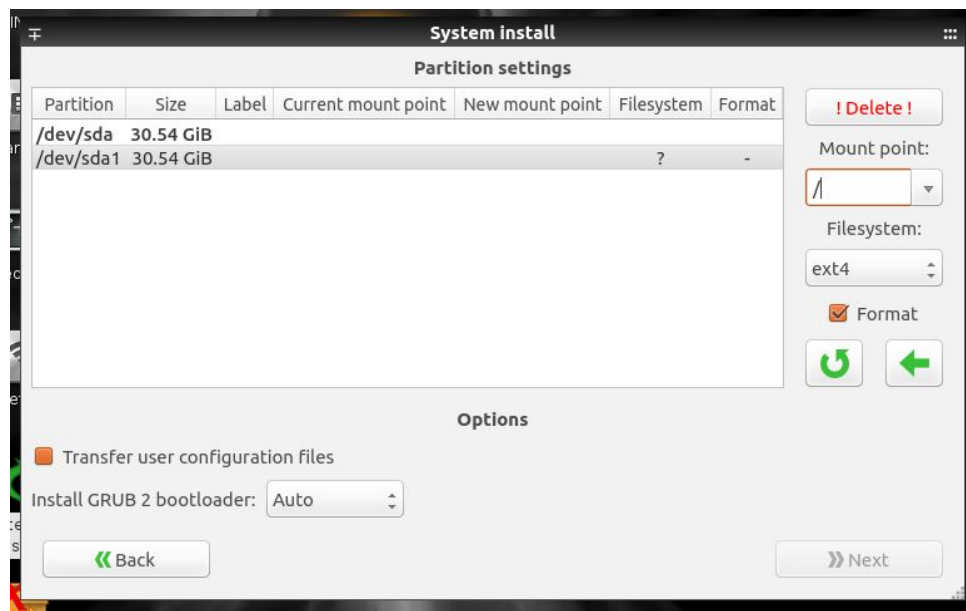
Select the **/dev/sda** partition and press the 'Delete' button.



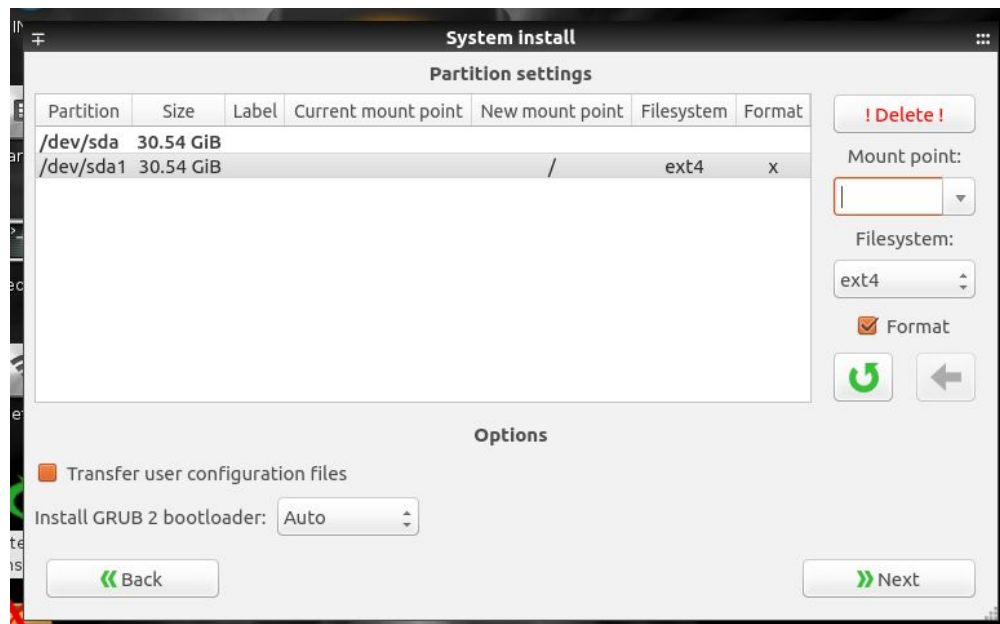
Then select the **/dev/sda?** Partition and press the left arrow button:



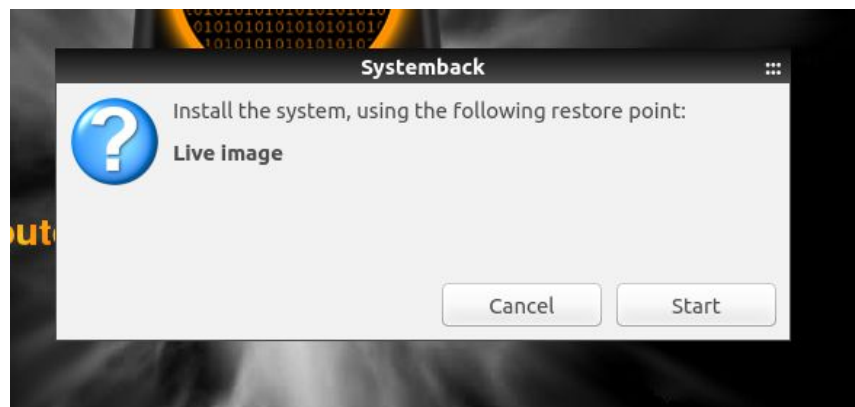
Now, choose the root directory as mount point (**/**) and keep the default filesystem **ext4**, as shown below:



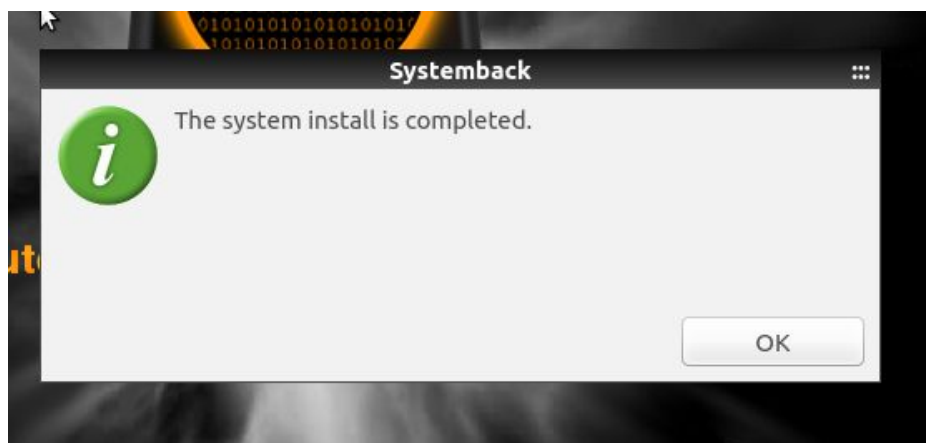
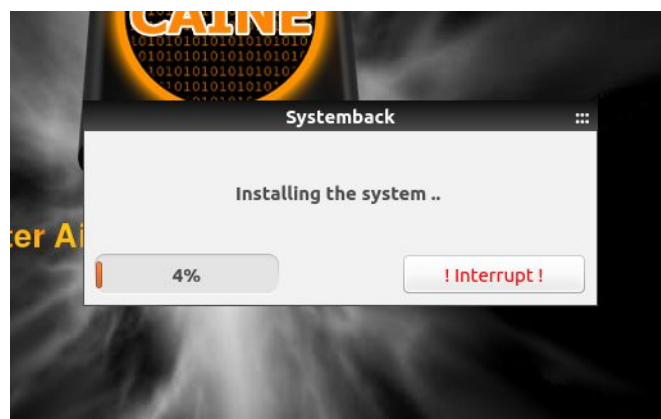
Click the left arrow button again to apply the settings, then click the Next button again to proceed:



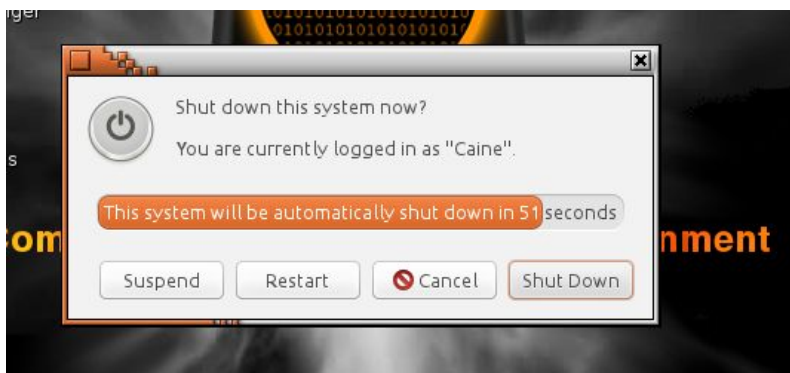
You will now be asked to install the system from the live image with the following dialog screen. Confirm by clicking the Start button:



The installation process will start now:



After the installation process is finished reboot the system:



After rebooting, you can login, and access the Caine Forensics tools by selecting Menu>Forensics Tools. Some of these tools will be covered in class and subsequent tutorials.



Shared Folders

To be able to use features such as shared folders and USB devices, which sometimes are needed in forensic analysis, you need to install and configure VMWare Tools.

At the bottom of the machine, you should see a message asking whether you'd like to install VMWare Tools; accept and start the installation.



Mount the VMware Tools virtual CD-ROM image, by opening a terminal and typing the following:

```
caine@caine:/$ sudo mount /dev/cdrom /cdrom
mount: block device /dev/sr0 is write-protected, mounting read-only
caine@caine:/$
```

Change to a working directory, for example, /tmp; type:

cd /tmp

And then **ls /cdrom**

```
caine@caine:/tmp$ ls /cdrom
manifest.txt      VMwareTools-10.1.6-5214329.tar.gz  vmware-tools-upgrader-64
run_upgrader.sh  vmware-tools-upgrader-32
caine@caine:/tmp$
```

Uncompress the installer, by typing:

tar xzpf /mnt/cdrom/VMwareTools-x.x.x-yyyy.tar.gz

The value x.x.x is the product version number, and yyyy is the build number of the product release.

```
caine@caine:/tmp$ tar xzpf /cdrom/VMwareTools-10.1.6-5214329.tar.gz
caine@caine:/tmp$ ls
config-err-MGCCBs  mounter.4xAZaXx6  vmware-tools-distrib
libgksu-knxv0R    ssh-0fvLHbXCXa6g
caine@caine:/tmp$
```

Next, unmount the CD-ROM image by typing:

umount /dev/cdrom

```
caine@caine:/tmp$ sudo umount /cdrom
caine@caine:/tmp$
```

Run the installer and configure VMware Tools by typing:

cd vmware-tools-distrib

./vmware-install.pl

```
caine@caine:/tmp/vmware-tools-distrib$ cd ..
caine@caine:/tmp$ cd vmware-tools-distrib/
caine@caine:/tmp/vmware-tools-distrib$ sudo ./vmware-install.pl
open-vm-tools packages are available from the OS vendor and VMware recommends
using open-vm-tools packages. See http://kb.vmware.com/kb/2073803 for more
information.
Do you still want to proceed with this installation? [no] yes
```

Follow the prompts to accept the default values.

```
Creating a new VMware Tools installer database using the tar4 format.

Installing VMware Tools.

In which directory do you want to install the binary files?
[/usr/bin]
```

```
Creating a new VMware Tools installer database using the tar4 format.

Installing VMware Tools.

In which directory do you want to install the binary files?
[/usr/bin]

What is the directory that contains the init directories (rc0.d/ to rc6.d/)?
[/etc]

What is the directory that contains the init scripts?
[/etc/init.d]

In which directory do you want to install the daemon files?
[/usr/sbin]

In which directory do you want to install the library files?
[/usr/lib/vmware-tools]

The path "/usr/lib/vmware-tools" does not exist currently. This program is
going to create it, including needed parent directories. Is this what you want?
[yes] yes
```

```
You must restart your X session before any mouse or graphics changes take
effect.

You can now run VMware Tools by invoking "/usr/bin/vmware-toolbox-cmd" from the
command line.

To enable advanced X features (e.g., guest resolution fit, drag and drop, and
file and text copy/paste), you will need to do one (or more) of the following:
1. Manually start /usr/bin/vmware-user
2. Log out and log back into your desktop session
3. Restart your X session.

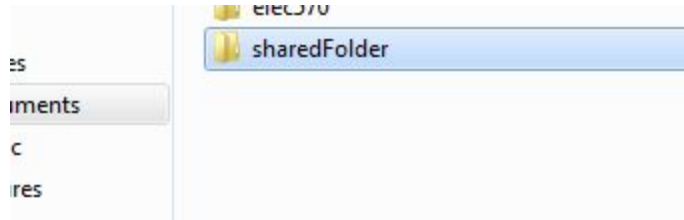
Enjoy,

--the VMware team

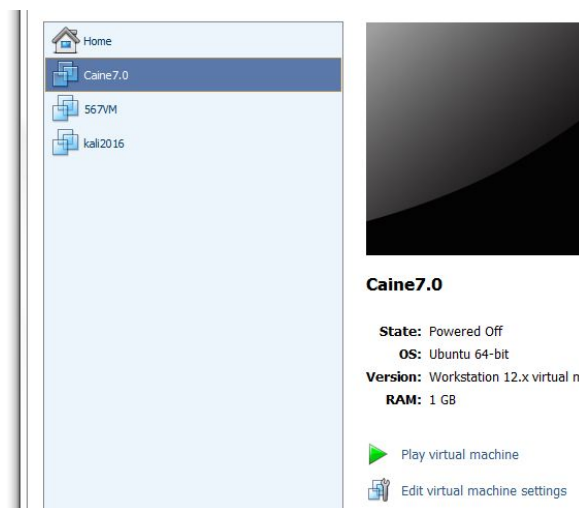
caine@caine:/tmp/vmware-tools-distrib$
```

At the end, **shutdown the machine.**

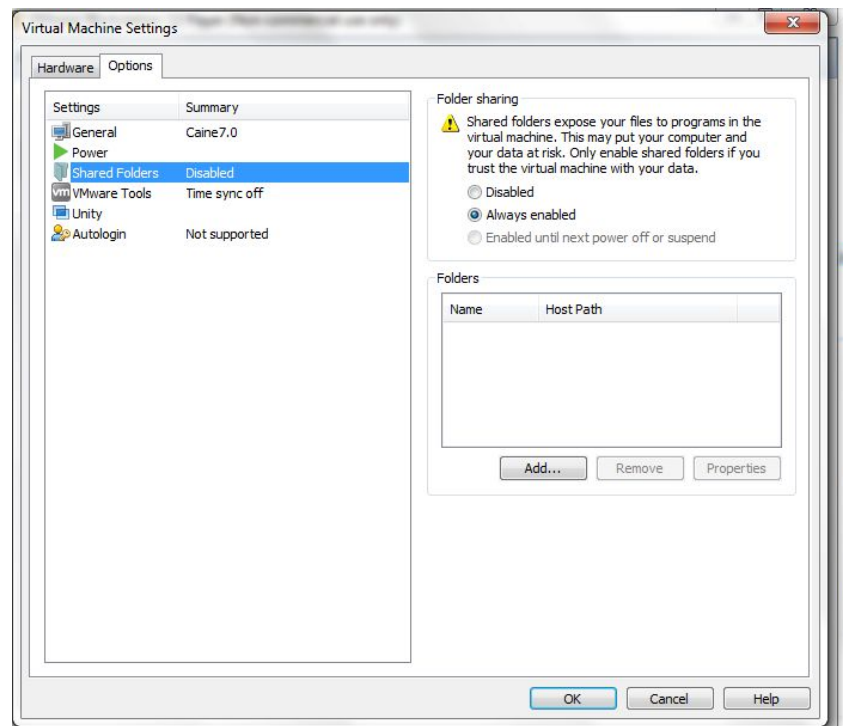
Next, create a folder in your Windows file system that you want to use as the share. I've created one that I called **sharedFolder** (you can use any name and location):



Select your VM in VMware Player and click *Edit virtual machine settings*



In the Options tab click *Shared Folders* in the left hand pane



Click *Always enabled* in the right pane and click *Add...*

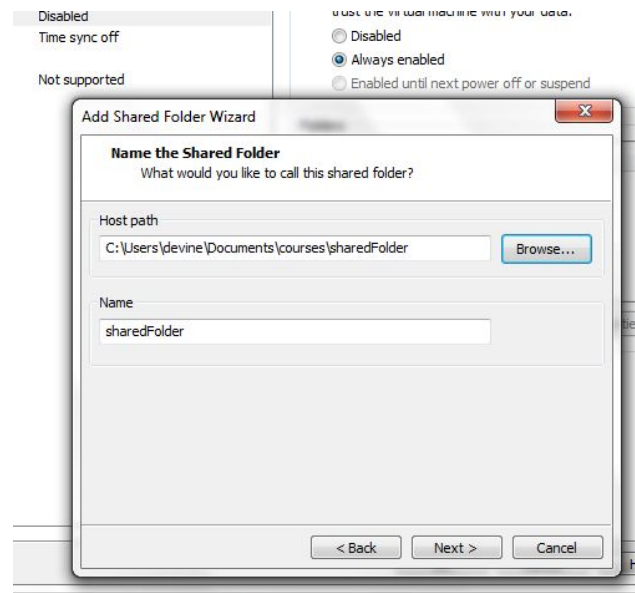
This will take you into the “Add Shared Folder Wizard”

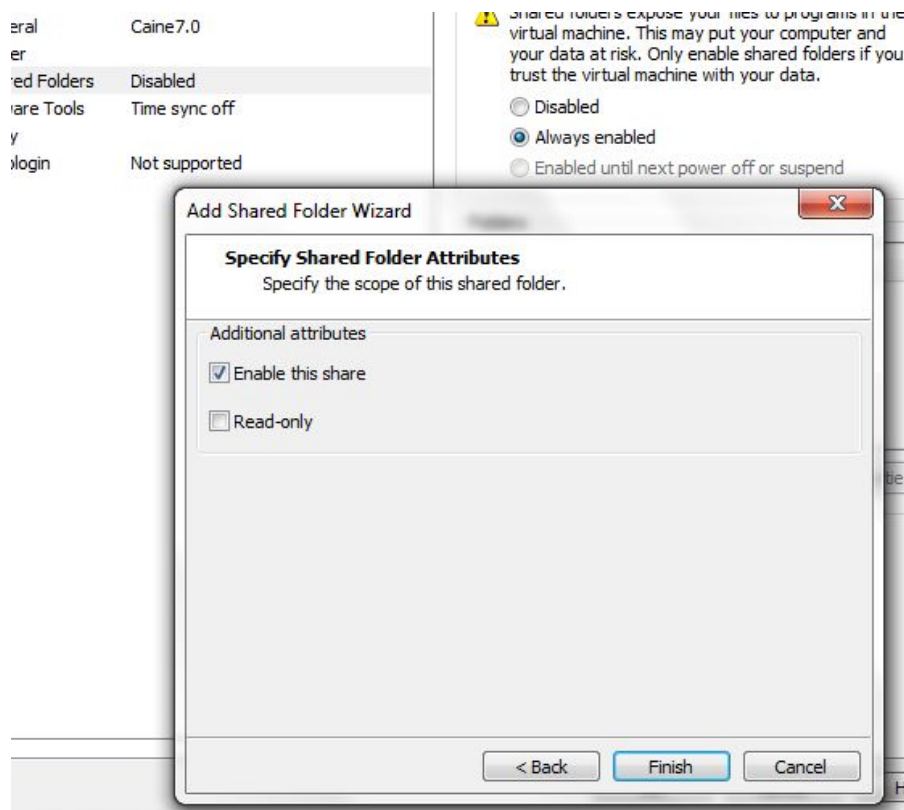


Click *Next* and follow the prompts selecting the folder you created in Step 1

Also name the share – this is the name that the folder will have in Caine

You will come back to the Settings screen with your share added





Click OK to close the settings.

Play the VM to boot Caine.

Shared folders in Ubuntu appear in the location **/mnt/hgfs** but you probably won't be able to see it.

To check if Ubuntu is aware that there is a shared folder available, run this command in a terminal window:

vmware-hgfsclient

This will output the share name into the terminal window as follows:

```
caine@caine:/$ vmware-hgfsclient
sharedFolder
caine@caine:/$
```

Now we need to run the VMWare config tools. In terminal enter:

sudo vmware-config-tools.pl

Follow the prompts, accepting the default values:

```
caine@caine:/$ sudo vmware-config-tools.pl
Initializing...

Making sure services for VMware Tools are stopped.
```

```
To enable advanced X features (e.g., guest resolution fit, drag and drop, and
file and text copy/paste), you will need to do one (or more) of the following:
1. Manually start /usr/bin/vmware-user
2. Log out and log back into your desktop session
3. Restart your X session.

Enjoy,

--the VMware team

caine@caine:/$
```

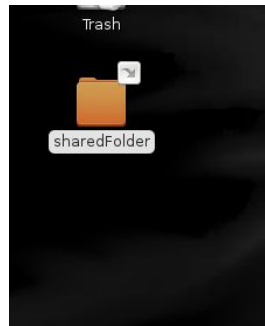
At the end, you can check to see that your folder is now showing in the `/mnt/hgfs` directory:

```
caine@caine:/$ cd /mnt/hgfs
caine@caine:/mnt/hgfs$ ls
sharedFolder
caine@caine:/mnt/hgfs$
```

To share folder permissions across Caine Virtual Machine & Windows Host, and get quick access to the folder from your Ubuntu desktop, enter this into a terminal (replace in the command the name of the shared directory and the name of the folder on Caine as you see fit):

```
caine@caine:/mnt/hgfs$ ln -s /mnt/hgfs/shared-directory ~/Desktop/sharedFolder
caine@caine:/mnt/hgfs$ ln -s /mnt/hgfs/sharedFolder ~/Desktop/sharedFolder
caine@caine:/mnt/hgfs$
```

After doing that, the Windows shared folder is now fully accessible and usable from your Caine VM:

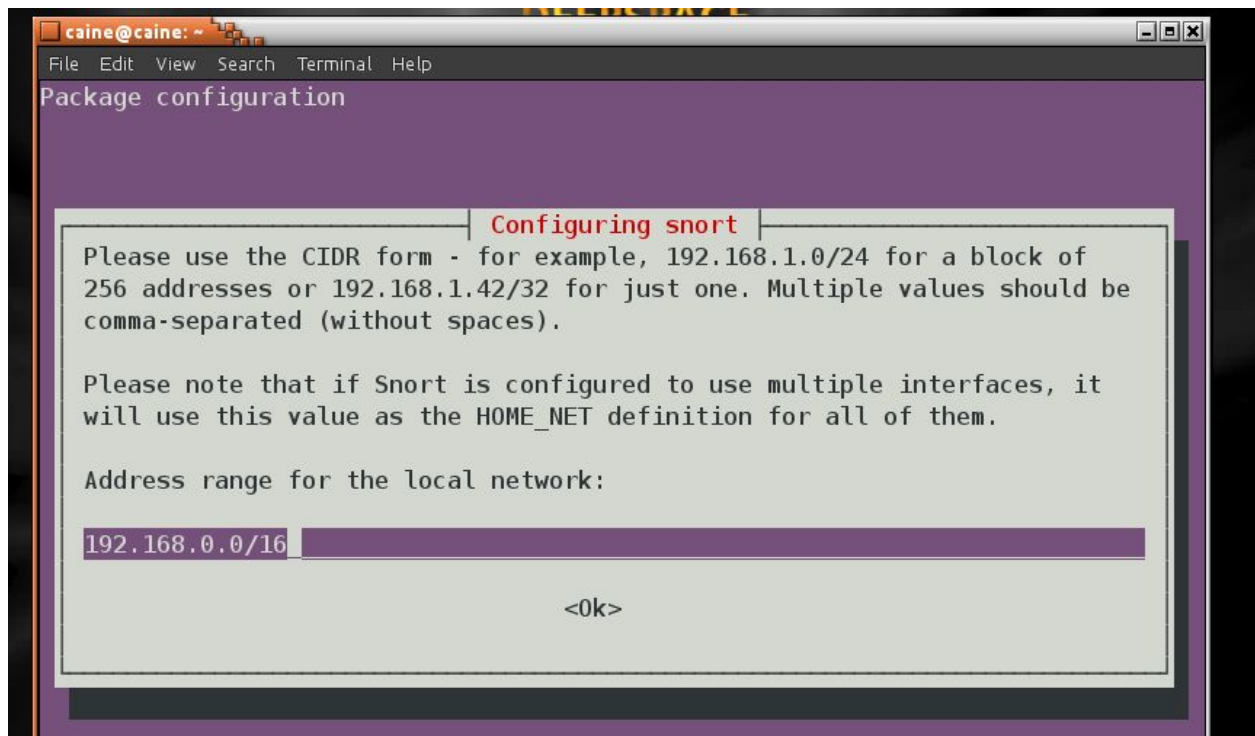


Snort Installation (Optional)

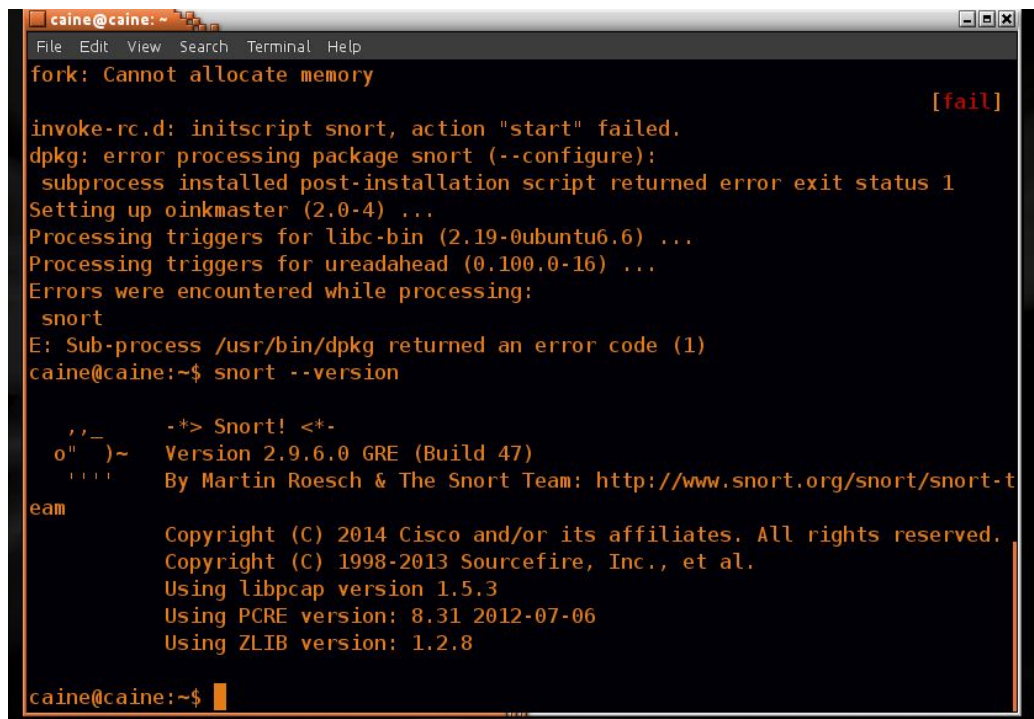
Snort will be used later in network forensics analysis; however, it is not installed by default on Caine. You can check, whether snort is installed as follows, and if not start the installation:

```
caine@caine: ~  
File Edit View Search Terminal Help  
caine@caine:~$ snort --version  
The program 'snort' is currently not installed. You can install it by typing:  
sudo apt-get install snort  
caine@caine:~$ sudo apt-get install snort  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following extra packages will be installed:  
  libdaq2 libdumbnet1 oinkmaster snort-common snort-common-libraries  
  snort-rules-default  
Suggested packages:  
  snort-doc  
The following NEW packages will be installed:  
  libdaq2 libdumbnet1 oinkmaster snort snort-common snort-common-libraries  
  snort-rules-default  
0 upgraded, 7 newly installed, 0 to remove and 626 not upgraded.  
Need to get 1.373 kB of archives.  
After this operation, 7.199 kB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

Select Y [Yes], and next click Ok, keeping the default:



The installation will continue and complete:



Next, configure snort to display its output in CSV format. First, you can install a text editor like Leafpad as follows:

```
caine@caine:~$ leafpad -h
The program 'leafpad' is currently not installed. You can install it by typing:
sudo apt-get install leafpad
caine@caine:~$ sudo apt-get install leafpad
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  evince-gtk
The following NEW packages will be installed:
  leafpad
```

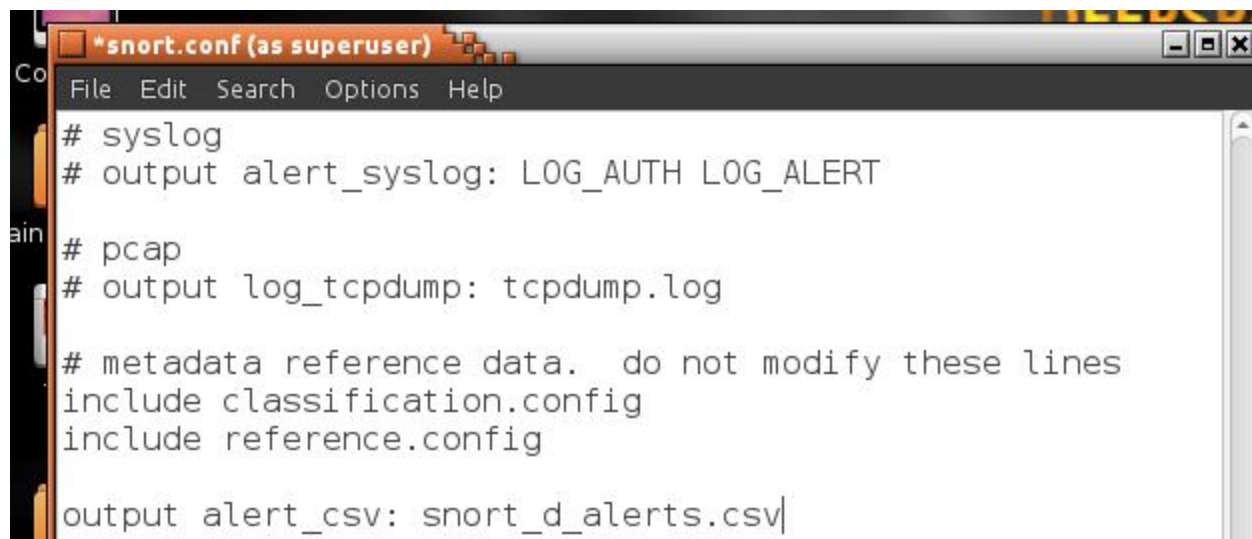
Next, open the snort configuration file using leafpad (any other text editor will be fine):

```
caine@caine:/etc/snort$ sudo leafpad snort.conf

(leafpad:14395): IBUS-WARNING **: The owner of /home/caine/.config/ibus/bus is not root!
```

Enter the following line and save/close the file:

Output alert_csv: snort_d_alerts.csv



Snort will be covered in more details later.