SIT282/SIT703 Computer Forensics and Investigations

Workshop Session 1

Before undertaking this workshop, you should have read and completed the "Ethics Agreement" posted on CloudDeakin and submit it to the dropbox on the unit site. Failure to do so will result in your being removed from the unit.

Learning Objectives

1. Set up the digital forensic lab by installing VirtualBox and Ubuntu VM.
2. Demonstrate that you can create shared folder(s) between the host machine and the virtual machine.
3. Demonstrate that you can perform basic forensic investigation using Autopsy.

1. Getting started

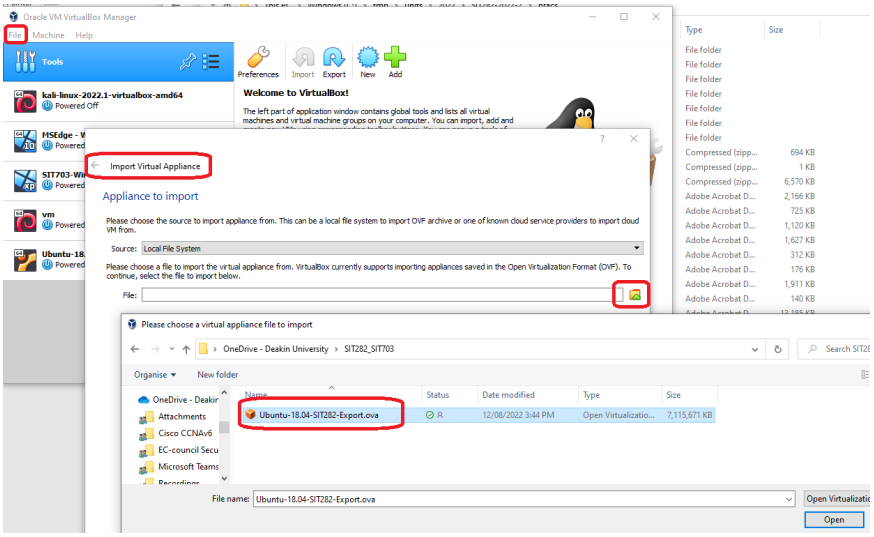
In the first workshop of the unit, you prepare your digital forensic lab by installing virtualbox and Ubuntu VM. For security reasons, almost all of the forensic tools and most of the data files you need for this unit have been packaged in a virtual machine.

We use Oracle VM VirtualBox as the virtualization software in this unit. To get it,

Step 1: Download VirtualBox to your machine from:
https://www.virtualbox.org/
Step 2: Download the virtual machine from:
https://cloudstor.aarnet.edu.au/plus/s/pAy8BEawGLMSdEt/authenticate with code SIT282-Download or the Deakin OneDrive link.

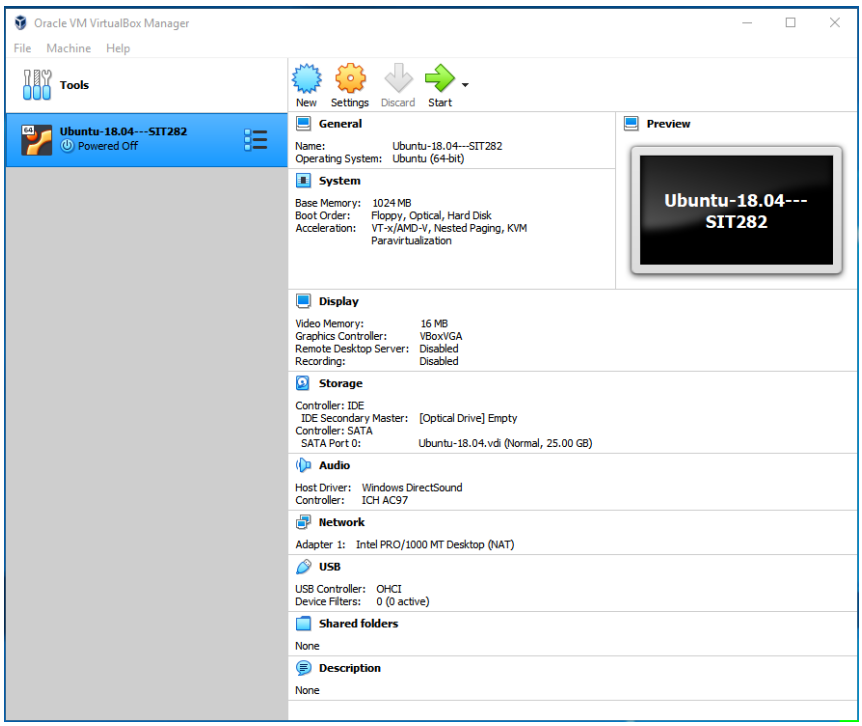
Launch the Virtualbox program on your computer. You should see a screen similar to this:

This is the default interface where no virtual machine is loaded at the moment.



From the VirtualBox top menu “File” > “Import Appliance”, choose the virtual appliance file “Ubuntu-18.04-SIT282-Export.ova”, click “open”, “next”, keep the default settings, then click “Import”. (If you have trouble downloading or installing the virtual machine, please talk to the teaching team ASAP.)

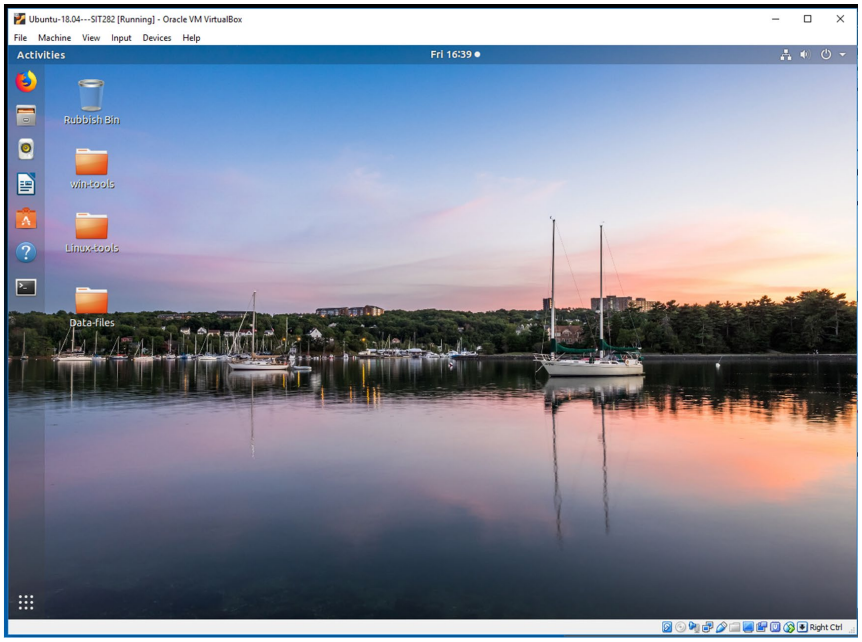
If everything goes well, you should be able to see a screen like this:



Congratulations! You have just installed the Ubuntu virtual machine successfully on your computer.

2. Run This Virtual Machine

Select the Ubuntu VM you just installed, click the green arrow "Start" to run this virtual machine. It should boot normally and no password is needed to log in.



The most commonly used programs in the virtual machine include firefox, file explorer and terminal. They are pinned to the Docker on the left hand side of the interface. Within Ubuntu/Linux, "Terminal" will generally take you to anywhere you want to go.

Now, you can spend some time to get familiar with the Virtualbox and Ubuntu operating system. For the beginners, we recommend you to read this tutorial as a starting point https://archive.org/details/ubuntupocketguide-v1-1 or the same tutorial available on CloudDeakin. If you are an experienced Linux user, you may proceed to the next section.

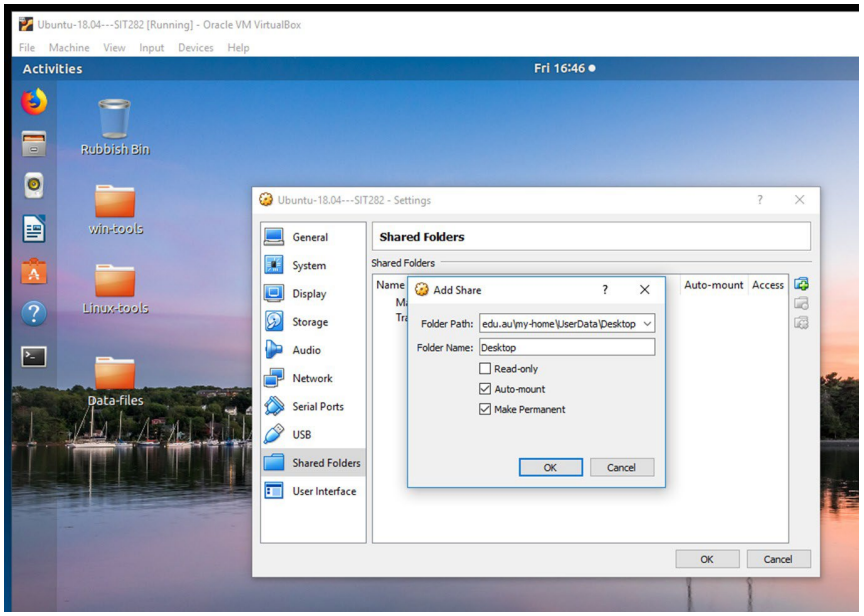
3. Access Your Personal Files

Virtualbox allows you to share files between the host machine and the virtual machine, which is very useful. There are a few approaches:

The first approach is through a USB drive, when you copy files from one system and then paste them to another system. Your USB must be formatted in FAT32 or ex-FAT for compatibility reasons. The Ubuntu VM should be able to recognize most USB drives.

The second approach is through a network share or network drive. Our virtual machine is configured with a NAT network access to your host machine. In most cases, it should have internet access so that you can sync your files to google drive, OneDrive or dropbox.

The third approach is through directory sharing. There are many possible host systems (windows/linux/mac) and we cannot cover all. You are recommended to find solutions from sources similar to this video https://www.youtube.com/watch?v=9-teQnZ8LEY



(Note: This screenshot is for demonstration purposes only. Yours might be different.)

Steps in the video:
1. Switch off the Ubuntu VM, select the Ubuntu VM and go to "Settings" > "Shared Folders" > "+" (top-right), choose "others" from "Folder Path" dropdown, select your target folder (e.g., *sharedfolder*) to share on the host machine, "Folder Name" should appear the same as the target folder automatically, check the "Auto-mount" box, leave "Mount point" empty if you wish as it will be automatically set by virtualbox;

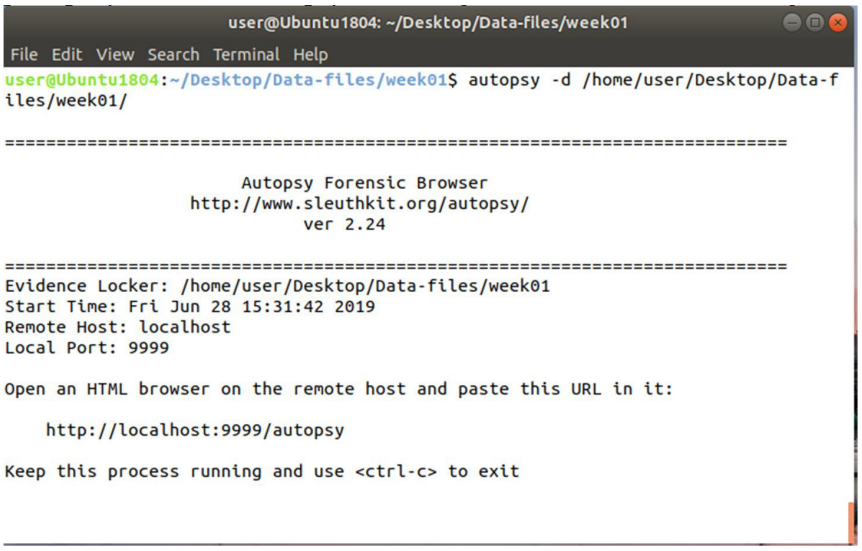
2. Start the Ubuntu VM. You will see the sf_*sharedfolder* appear on the desktop. Open a terminal window, type "**whoami**" to find out who you are (e.g. *user*"), then type "**sudo adduser *user* vboxsf**". Restart the Ubuntu VM. Test the shared folder.

When following the steps above or as instructed by the video, please ensure you add the Ubuntu user "*user*" to the group 'vboxsf'. This will enable the link between the folder on the host machine and on the virtual machine. Enter "*user*" (sudo password) when prompted for password.

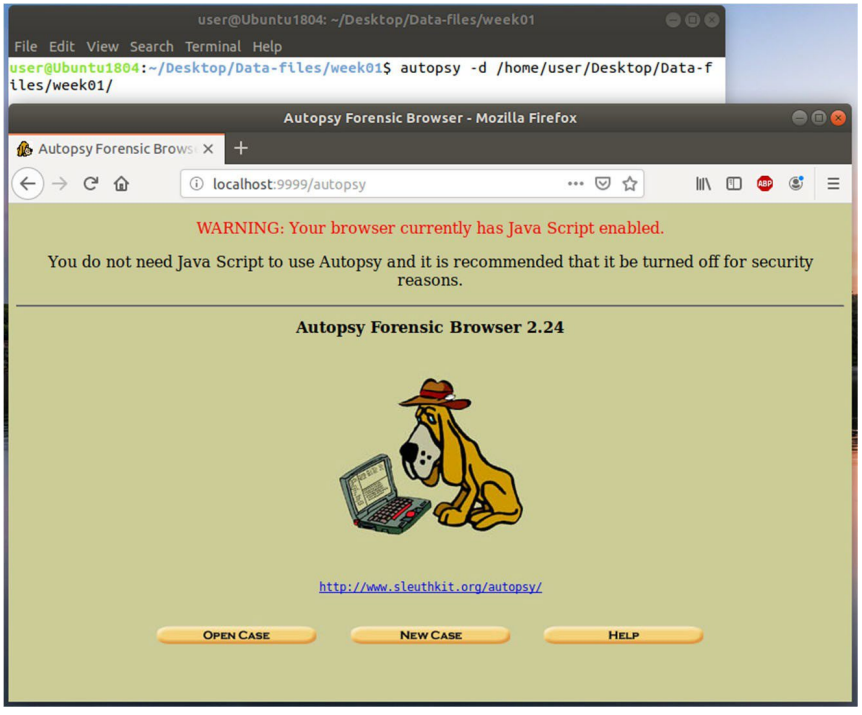
4. Forensic Investigation through Autopsy

Launch a "Terminal" program by clicking the terminal icon on the dock bar (the left side of the interface), then type "**cd ~/Desktop/Data-files/week01**".

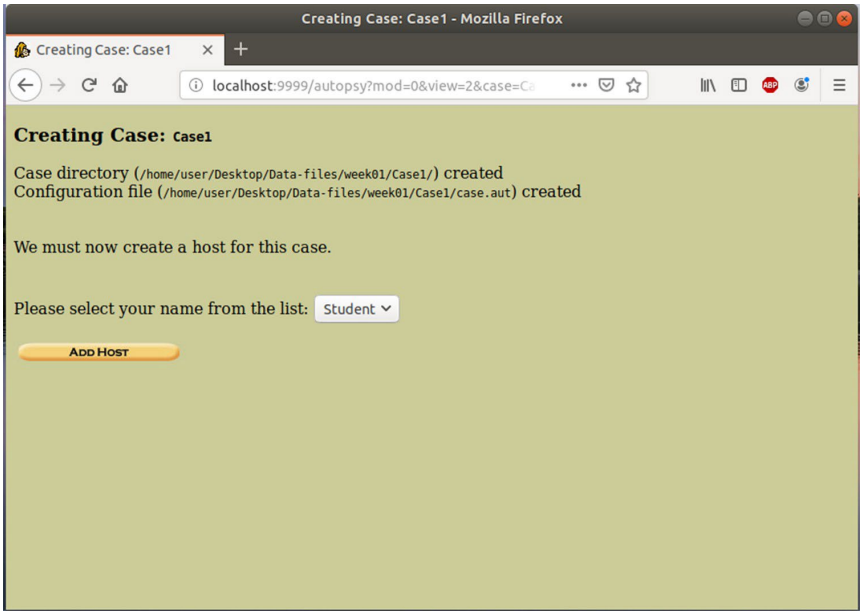
We will use the program named "autopsy" to investigate the first forensic case. Type in the command "**autopsy -d /home/user/Desktop/Data-files/week01/**", then the program prompts you that the autopsy is running and can be accessed through an URL.



Open the URL http://localhost:9999/autopsy in firefox.

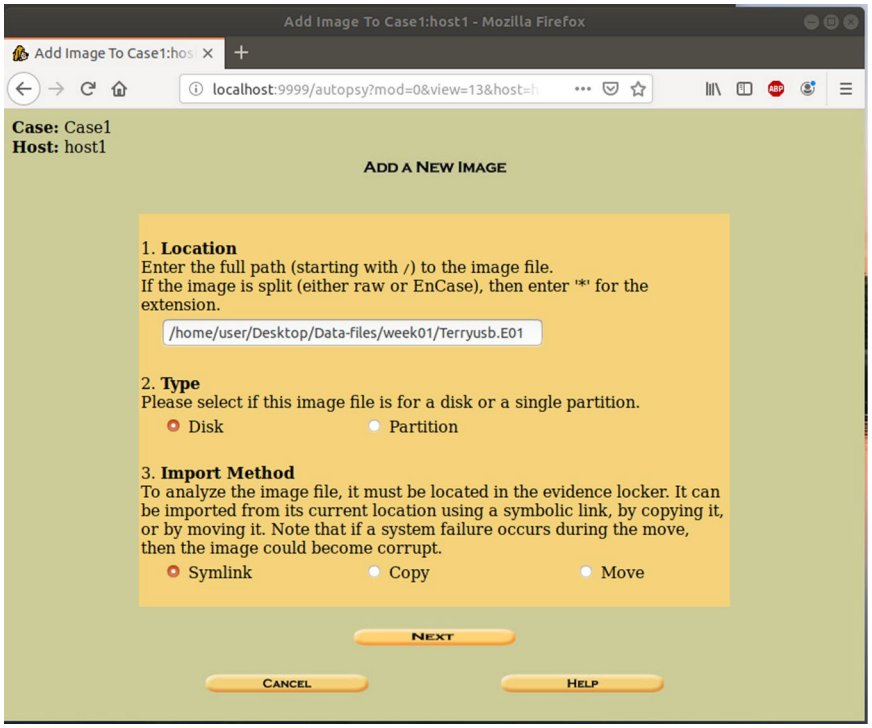


Then click the “New Case” button and name the case and investigator(s). Click the “New Case” button again, add the host.

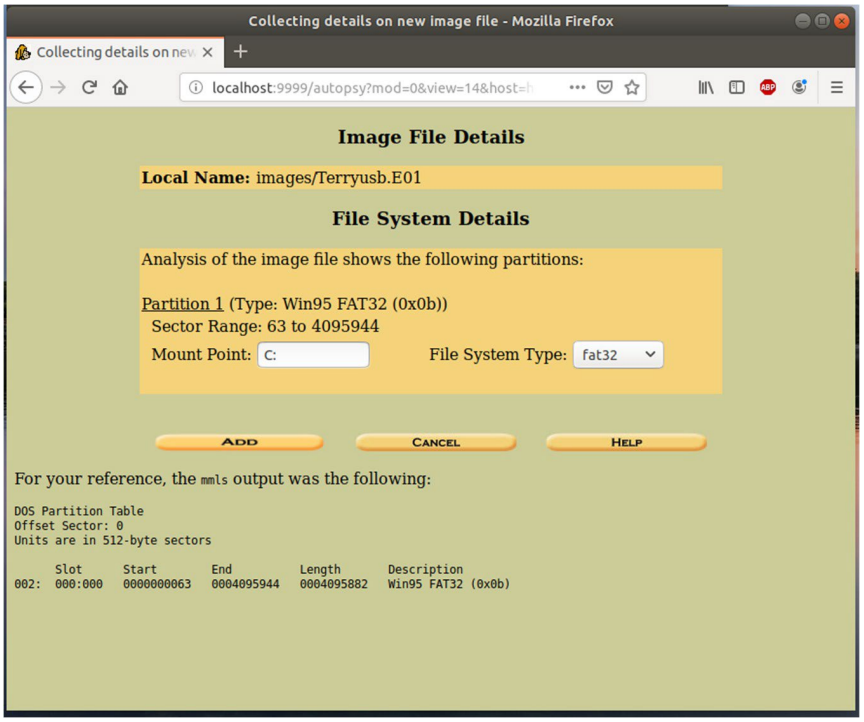


Click the "Add Host" button and use the default settings. Then add the forensic image by clicking the "Add Image" button and then the "Add Image File" button on the next page:

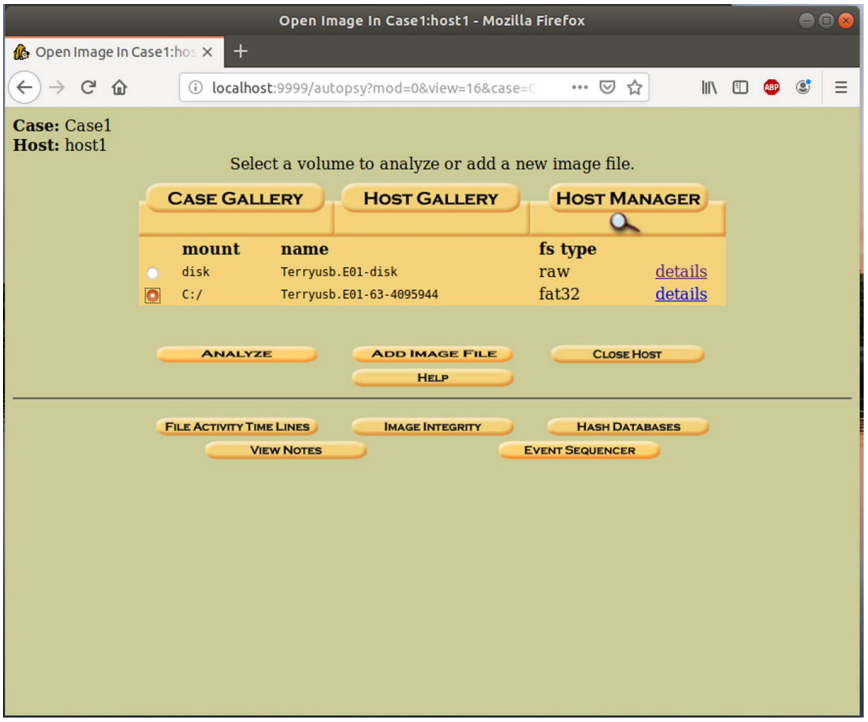
Fill in the entire path and file name (e.g., /home/user/Desktop/Data-files/week01/Terryusb.E01") to the location textbox before clicking the button "Next".



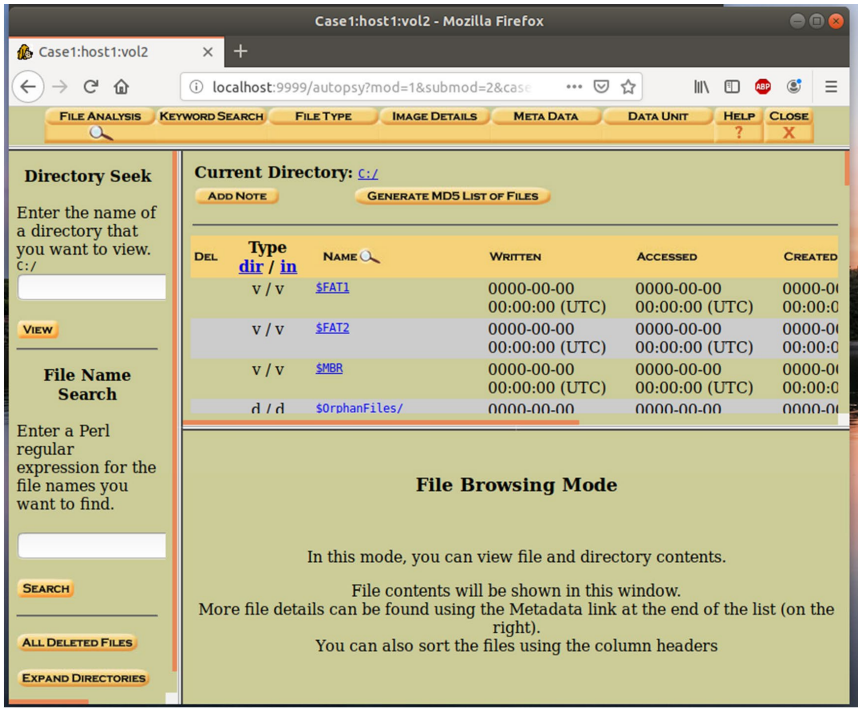
Now click the “Add” button and the “Ok” button:



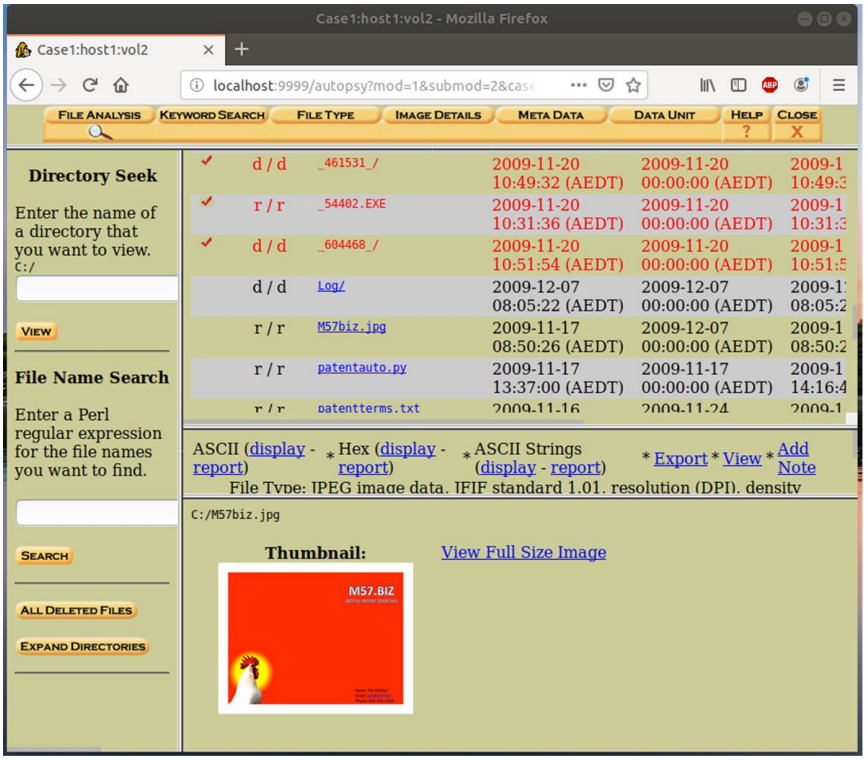
Now the image is properly loaded.



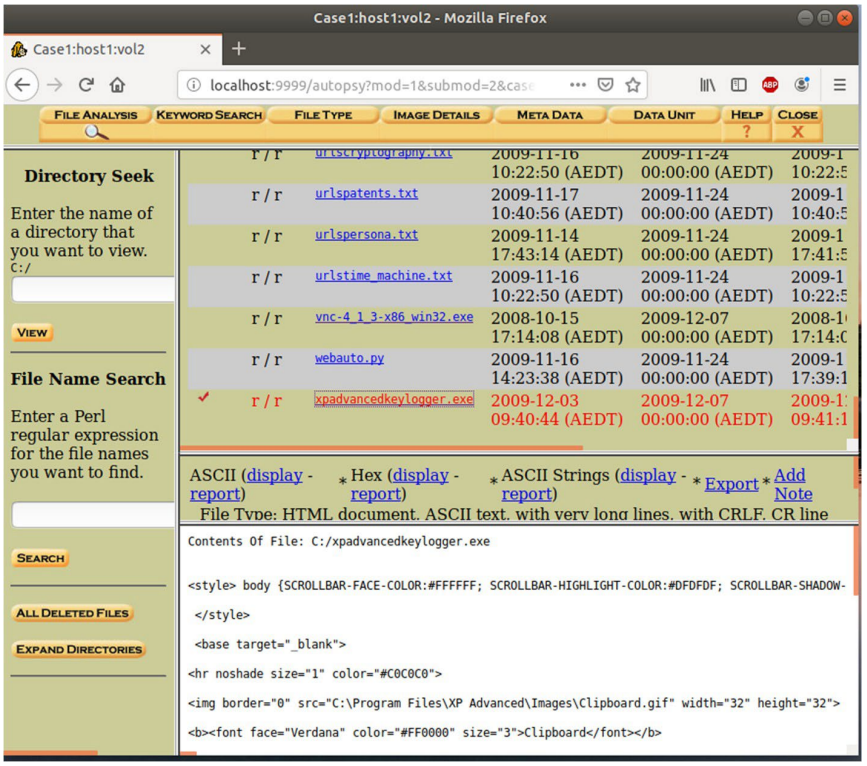
Ensure you check the C:/ option under ‘mount’. After clicking the “Analyze” button, we will see a few options. We check the “file analysis” first.



Spend 10 minutes or so to explore the files and items in the case. For example, you can find an image file in the drive:



Navigate to the bottom of the list, locate file named “xpadvancedkeylogger.exe”. Click it and you will find its contents shown as an html file in the bottom panel.



Spend 30 minutes or so to go through every item in this case. Look for anything that is odd to you. Explore other functions besides of “file analysis” (refer to the official site for more info about Autopsy 2 functions http://www.sleuthkit.org/autopsy/help/index.html) and see what information you can get. (Note: We will perform further investigation into this case later.)

After you have found a few things, take some notes of your findings. Quit the autopsy and shut down the virtual machine.