|  |  |
| --- | --- |
| **Mobile Device Security & Forensics**  Diploma in IT  Year 3 (2014/15) Semester 5 | Week 1 |
| Practical 1a |
| **Familiarization with Linux Commands** | |

**OBJECTIVES**

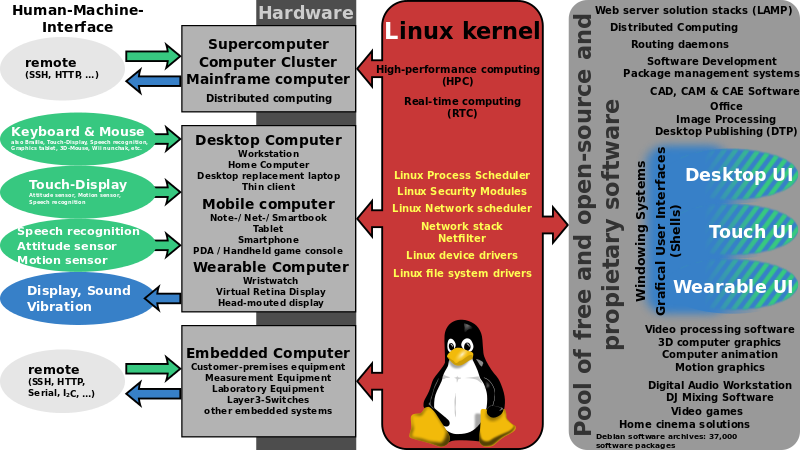
After completing this topic, you should be able to

1. Introduce to Linux
2. Familiarize with the Linux directory structure
3. Use the Command shell for file manipulation
4. Familiarize with Apt-Get command line tool

**Background**

Linux is a Unix-like computer operating system assembled under the model of free and open source software development and distribution. Unix is a multitasking, multi-user computer operating system that exists in many variants. The defining component of Linux is the Linux kernel, an operating system kernel first released on 5 October 1991, by Linus Torvalds.

The main form of distribution are Linux distributions. A Linux distribution (often called distro for short) is an operating system built on top of the Linux kernel and often around a package management system. They can be specific to a certain type of hardware device, like supercomputers (e.g. Rocks Cluster Distribution) or embedded systems (e.g. OpenWrt), or be compiled for various instruction sets and be designed to run on various hardware types (e.g. Debian). A Linux distribution usually includes a very large collection of free and open-source software of all sorts. The software is usually adapted to the distribution and then packaged into software packages by the distribution maintainers. The software packages are available online in so called repositories, on various servers around the world.



Distros that come with a GUI, adapt and package the available free and open-source implementations of one or more of the available windowing systems.

Linux was originally developed as a free operating system for Intel x86-based personal computers. It has since been ported to more computer hardware platforms than any other operating system. It is a leading operating system on servers and other big iron systems such as mainframe computers and supercomputers. As of June 2013, more than 95% of the world's 500 fastest supercomputers run some variant of Linux, including all the 44 fastest. Linux also runs on embedded systems (devices where the operating system is typically built into the firmware and highly tailored to the system) such as mobile phones, tablet computers, network routers, building automation controls, televisions and video game consoles; the Android system in wide use on mobile devices is built on the Linux kernel. Android is an operating system based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones and tablet computers. Initially developed by Android, Inc., which Google backed financially and later bought in 2005, Android was unveiled in 2007 along with the founding of the Open Handset Alliance: a consortium of hardware, software, and telecommunication companies devoted to advancing open standards for mobile devices. The first Android-powered phone was sold in October 2008.

The development of Linux is one of the most prominent examples of free and open source software collaboration: the underlying source code may be used, modified, and distributed — commercially or non-commercially — by anyone under licenses such as the GNU General Public License. Typically, Linux is packaged in a format known as a Linux distribution for desktop and server use. Some popular mainstream Linux distributions include Debian (and its derivatives such as Ubuntu and Linux Mint), Fedora (and its derivatives such as the commercial Red Hat Enterprise Linux and its open equivalent CentOS), Mandriva/Mageia, openSUSE (and its commercial derivative SUSE Linux Enterprise Server), and Arch Linux. Linux distributions include the Linux kernel, supporting utilities and libraries and usually a large amount of application software to fulfill the distribution's intended use. . Ubuntu is a Debian-based Linux operating system, with Unity as its default desktop environment. It is based on free software. We will be using Ubuntu for MDSF module.

A distribution oriented toward desktop use will typically include the windowing systems X11 and Wayland and an accompanying desktop environment such as GNOME or the KDE Software Compilation. Some such distributions may include a less resource intensive desktop such as LXDE or Xfce for use on older or less powerful computers. Because Linux is freely redistributable, anyone may create a distribution for any intended use.

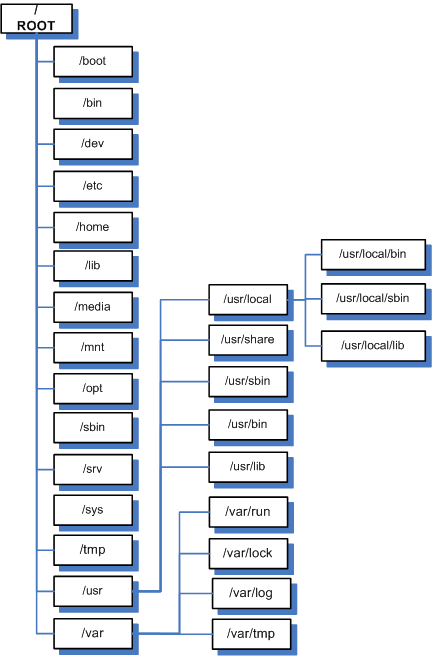
**Resources**

1. PC running Windows 7 OS and Linux ubuntu1110t Virtual Image
2. <http://www.codepuppet.com/2012/06/08/directory-structure-in-linux/>
3. <http://www.debianadmin.com/linux-directory-structure-overview.html>
4. <http://en.wikipedia.org/wiki/Linux>

**Activities**

The directory structure itself resides on what is called a partition – a low-level structure in which files and directories reside. Each directory contains information such as the name, location and size of each file.

The Linux directory structure is a tree structure and is composed of:



**"/" Root**

The Directory Structure starts with the Root file system "/" and is indeed the root directory for the whole structure. The partition where / (the root directory) will be located on a UNIX or UNIX-compatible system.

/boot

The /boot directory contains the Boot loader files including Grub or Lilo, the Kernel, initrd and system.map config files

/sys

This contains the Kernel, Firmware and system related files.

/sbin

Contains the essential System Binaries and System Administration tools essential for the system operation and performance

/bin

Contains the essential binaries for users and those utilities that are required in single user mode. Examples, include cat, ls, cp etc.

/lib

Contains the library files for all the binaries held in the /sbin & /bin directories

/dev

The /dev directory contains the essential system files and drivers.

**/etc**

The /etc/directory contain essential System configuration files including /etc/hosts, /etc/resolv.conf, nsswitch.conf, defaults and network configuration files. These are mostly host specific system and application configuration files.

/home

All the user home directories are held under this directory with the exception of the root home directory which is kept under /root directory. This directory holds users files, personal settings like .profile etc.

/media

A generic mount point for removable media like CD-ROM, USB, Floppies etc

/mnt

A generic mount point for temporary file systems. This comes handy particularly when troubleshooting from CDROM etc wherein you might have to mount the Root file system and edit configurations.

/opt

A rarely used directory in Linux for Optional Software Packages. This is extensively used in UNIX OS like Sun Solaris where the software packages are installed

/usr

A sub hierarchy to the root file system which is a User data directory. Contains user specific utilities and applications. You will again see a lot of important but not critical file systems are mounted. Here you would again find a bin, sbin & lib directory which contains non-critical user and system binaries and related libraries and a share directory. Also found here are the include directory with include files

/usr/sbin

Contains Non-essential Non-critical system binaries and network utilities

/usr/bin

Contains Non-Essential Non-critical command binaries for users.

/usr/lib

Library files for the binaries in /usr/bin & /usr/sbin directory.

/usr/share

A platform-independent shared data directory

/usr/local

A sub hierarchy under the /usr directory which has Local System specific data including user and system binaries and their libraries

/var

The /var directory is mostly mounted as a separate filesystem under the root where in all the variable content like logs, spool files for printers, crontab, at jobs, mail, running process, lock files etc. Care has to be taken in planning this file system and maintenance as this can fill up pretty quickly and when the FileSystem is full can cause system and application operational issues.

/tmp

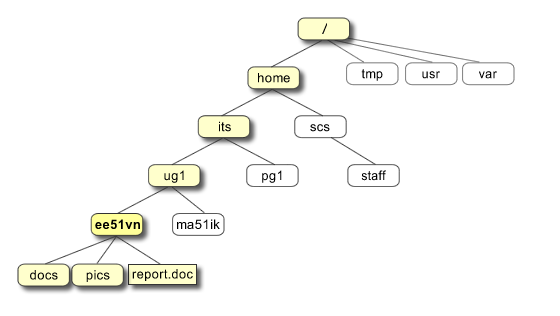
A temporary file system which hold temporary files which are cleared at system reboot. There is also a /var/tmp directory which holds temporary files too. the only difference between the two is that /var/tmp directory holds files that are protected at system reboot. In other words, /var/tmp files are not flushed upon a reboot.

The virtual (psuedo) file system /proc resides in the memory and is mounted under the Root holding kernel and process stats in text file formats.

**Task 1: Navigating Linux File Directory**

Which directory houses the super user’s home?

|  |
| --- |
| **/root** |



In the diagram above, we see that the home directory of the undergraduate student **"ee51vn"** contains two sub-directories (**docs** and **pics**) and a file called **report.doc**.

Write down the full path to the file report.doc.

|  |
| --- |
| **/home/its/ug1/ee51vn/report.doc** |

Identify the Linux directory and corresponding file where user account information is stored?

|  |
| --- |
| /media/etc/passwd |

**Task 2: Familiarization with Linux Commands**

<http://linuxcommand.org/learning_the_shell.php>

A Linux shell is a program that takes your commands from the keyboard and gives them to the Linux operating system to perform. In the old days, it was the only user interface available on a Unix computer. Nowadays, we have *graphical user interfaces (GUIs)* in addition to *command line interfaces (CLIs)* such as the shell.

On most Linux systems a program called [bash](http://linuxcommand.org/man_pages/bash1.html) (which stands for Bourne Again SHell, an enhanced version of the original Bourne shell program, sh, written by Steve Bourne) acts as the shell program. There are several additional shell programs available on a typical Linux system. These include: [ksh](http://linuxcommand.org/man_pages/ksh1.html), [tcsh](http://linuxcommand.org/man_pages/tcsh1.html) and [zsh](http://linuxcommand.org/man_pages/zsh1.html).

The table below shows the basic commands used in MS-DOS and Linux. Focus on the Linux commands which you will use for the remaining of this practical session.

| **Command's Purpose** | MS-DOS | **Linux** | **Basic Linux Example** |
| --- | --- | --- | --- |
| Copies files | copy | cp | cp *thisfile.txt* /home/*thisdirectory* |
| Moves files | move | mv | mv *thisfile.txt* /home/*thisdirectory* |
| Lists files | dir | ls | ls |
| Clears screen | cls | clear | clear |
| Closes prompt window | exit | exit | exit |
| Displays or sets date | date | date | date |
| Deletes files | del | rm | rm *thisfile.txt* |
| "Echoes" output on the screen | echo | echo | echo *this message* |
| Edits files with simple text editor | edit | pico | pico *thisfile.txt* |
| Compares the contents of files | fc | diff | diff *file1* *file2* |
| Finds a string of text in a file | find | grep | grep *this word or phrase* *thisfile.txt* |
| Formats a diskette | format a: (if diskette is in A:) | mke2fs (or mformat) | /sbin/mke2fs /dev/fd0 (/dev/fd0 is the Linux equivalent of A:) |
| Displays command help | *command* /? | man | man *command* |
| Creates a directory | mkdir | mkdir | mkdir *directory* |
| View a file | more | less | less *thisfile.txt* |
| Renames a file | ren | mv | mv *thisfile.txt* *thatfile.txt* |
| Displays your location in the file system | chdir | pwd | pwd |
| Changes directories with a specified path (*absolute path*) | cd *pathname* | cd *pathname* | cd */directory/directory* |
| Changes directories with a *relative path* | cd .. | cd .. | cd .. |
| Displays the time | time | date | date |
| Shows amount of RAM and use | mem | free | free |
| Notes : a. Pico is a simple text editor; other editors you can use in place of **Pico** include **Emacs** and **vi**. b. This formats a disk for the DOS filesystem. c. You can also use info for some commands. d. The more pager can also be used to page through a file a screen at a time. e. The mv command can both move a file and, if you want to rename a file in the same directory, you "move" that file to the same directory with a new name, as in this example. | | | |

Basic examples of how the command are used at the Linux shell prompt are also provided. Note that these commands usually have a number of options. To learn more about each command, read its associated man page (for example, type **man ls** at the shell prompt to read about the ls command).

*http://www.centos.org/docs/2/rhl-gsg-en-7.2/ch-doslinux.html*

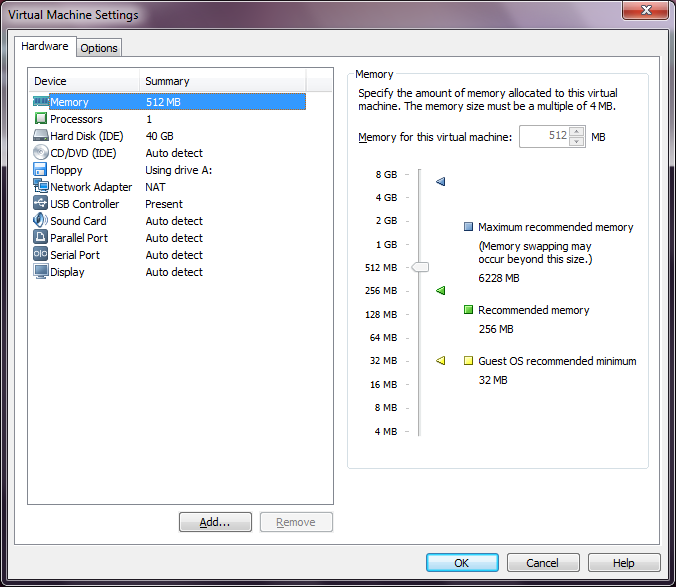
Carry out research online to find out the difference in using a forward slash and backslash in navigating file systems of Linux versus Windows? Also what is the difference between ./ and ../ in Linux?

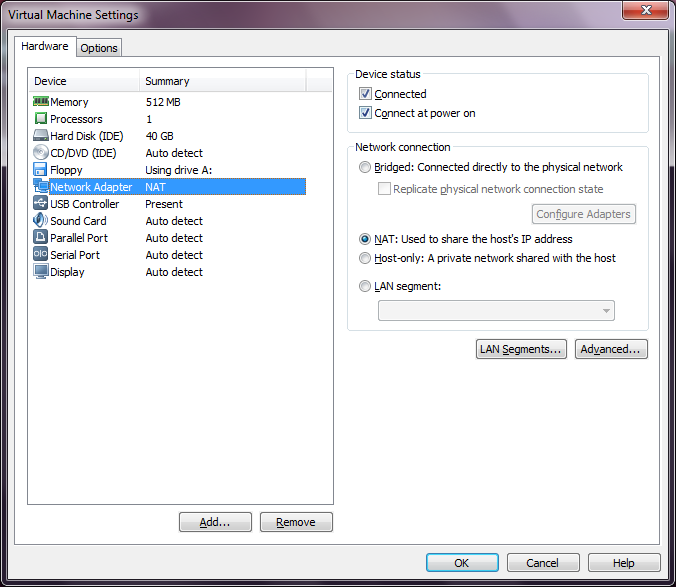
.DOS and Windows uses backslash for Microsoft Operating systems whereas UNIX-based operation system uses forward slash.

The difference between ./ and ../ in Linux is that ./ means is to show the current working directory whereas the ../ means to go back to the parent directory.

On the Lab PC, run VMware Player (either from VMware Player desktop icon or Start->All Programs->VMware->VMware Player)

In VMware Player, Go to Virtual Machine Settings (CTRL-D) and verified that:





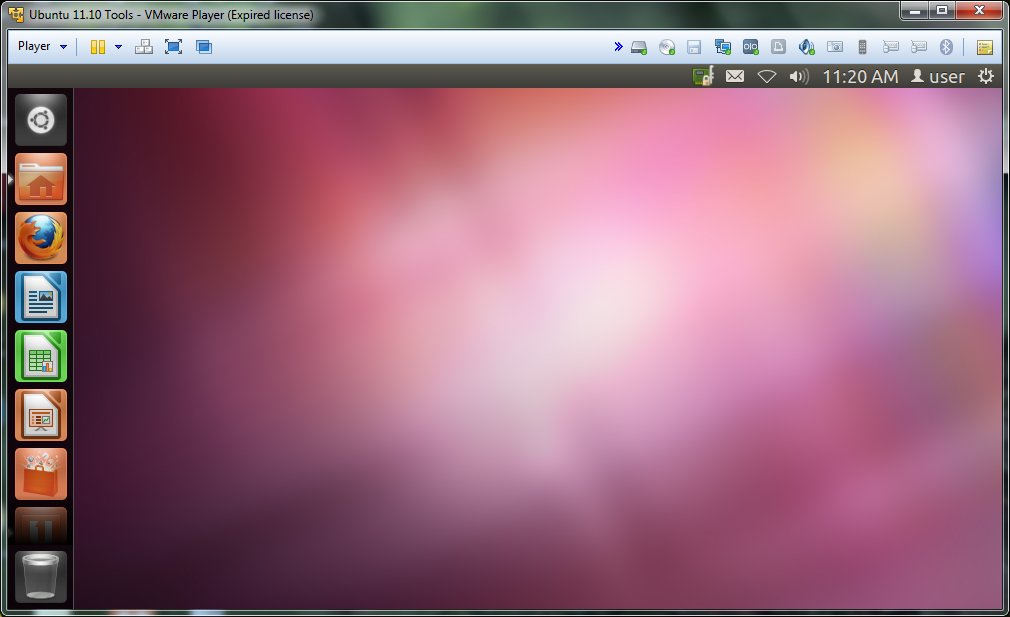
Select Player->File->Open and browse to <Drive Letter: location in Lab Machine HDD> -> ubuntu1110t-> Ubuntu1110 and Ubuntu.vmx. This loads the VM image of Ubuntu (a version of Linux OS).

The logon credential for standard user is:

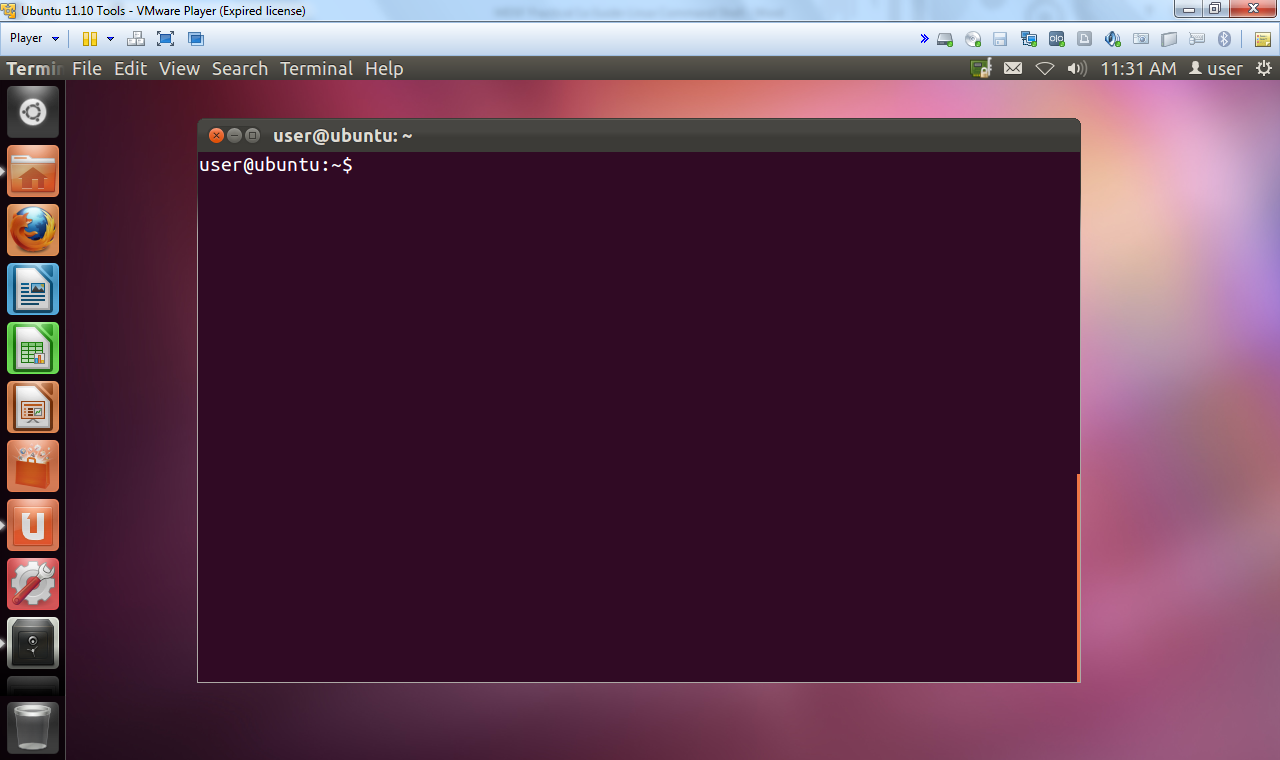
*username:* **user**

*password:* **password**

You should see the screen capture below when Ubuntu boots up fully:



Bring up a terminal shell (either do a search under Dash of “Terminal” to bring it up or click the Terminal icon on the right task bar if available):



Noticed the $ prompt, it indicate that you are login as non root user. root is the user name or account that by default has access to all commands and files on a Linux or other Unix-like operating system. It is also referred to as the root account, root user and the superuser.

The root directory is the top level directory on a system. That is, it is the directory in which all other directories, including their subdirectories, and files reside. The root directory is designated by a forward slash ( / ).

/root (pronounced slash root), which is the root user's home directory. A home directory is the primary repository of a user's files, including that user's configuration files, and it is usually the directory in which a user finds itself when it logs into a system. /root is a subdirectory of the root directory, as indicated by the forward slash that begins its name, and should not to be confused with that directory. Home directories for users other than root are by default created in the /home directory, which is another standard subdirectory of the root directory.

Root privileges are the powers that the root account has on the system. The root account is the most privileged on the system and has absolute power over it (i.e., complete access to all files and commands). Among root's powers are the ability to modify the system in any way desired and to grant and revoke access permissions (i.e., the ability to read, modify and execute specific files and directories) for other users, including any of those that are by default reserved for root.

[*http://www.linfo.org/root.html*](http://www.linfo.org/root.html)

What is your present working directory? Type in ***ls*** in the shell prompt, what is the outcome?

|  |
| --- |
| /root  root@ict-ThichCentre-M58e:~ |

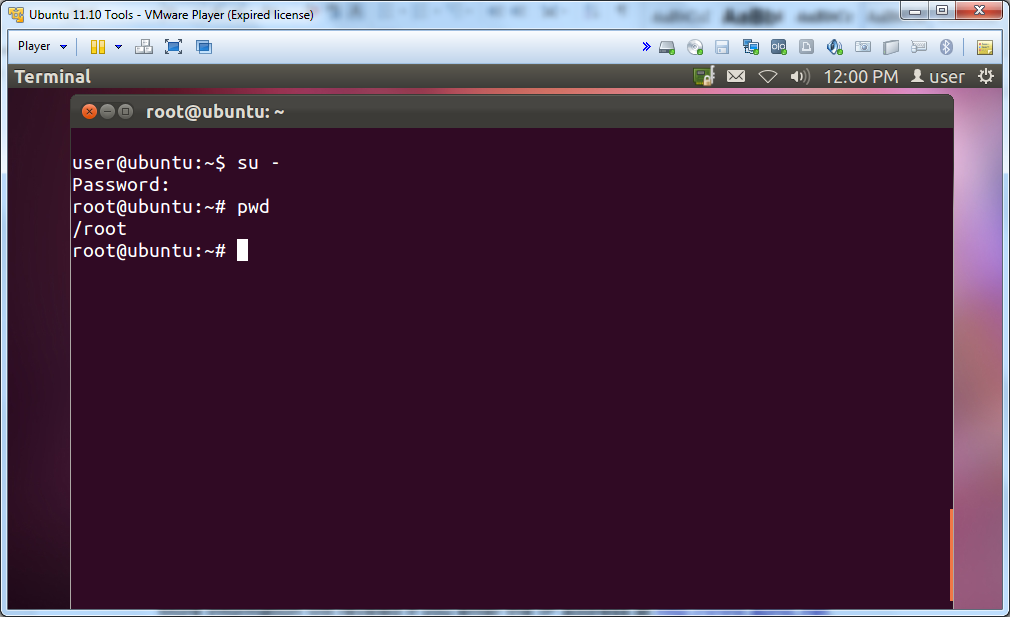
Change to be root user by typing ***su -*** and entering ***password*** when prompted for superuser password. Command **su** be used with a hyphen by administrators (**su -**, which is identical to su - root), which can be used to start a login shell. This way users can assume the user environment of the target user.

The logon credential for administrative user is:

*username:* **root**

*password:* **password**

Issue the pwd command to view your current directory. You should see the screen below:



**Creating folder and file manipulation**

Create a folder <your name> under /home/user using the command:

mkdir /home/user/<your name>

Change directory to <your name>. How do you do this?

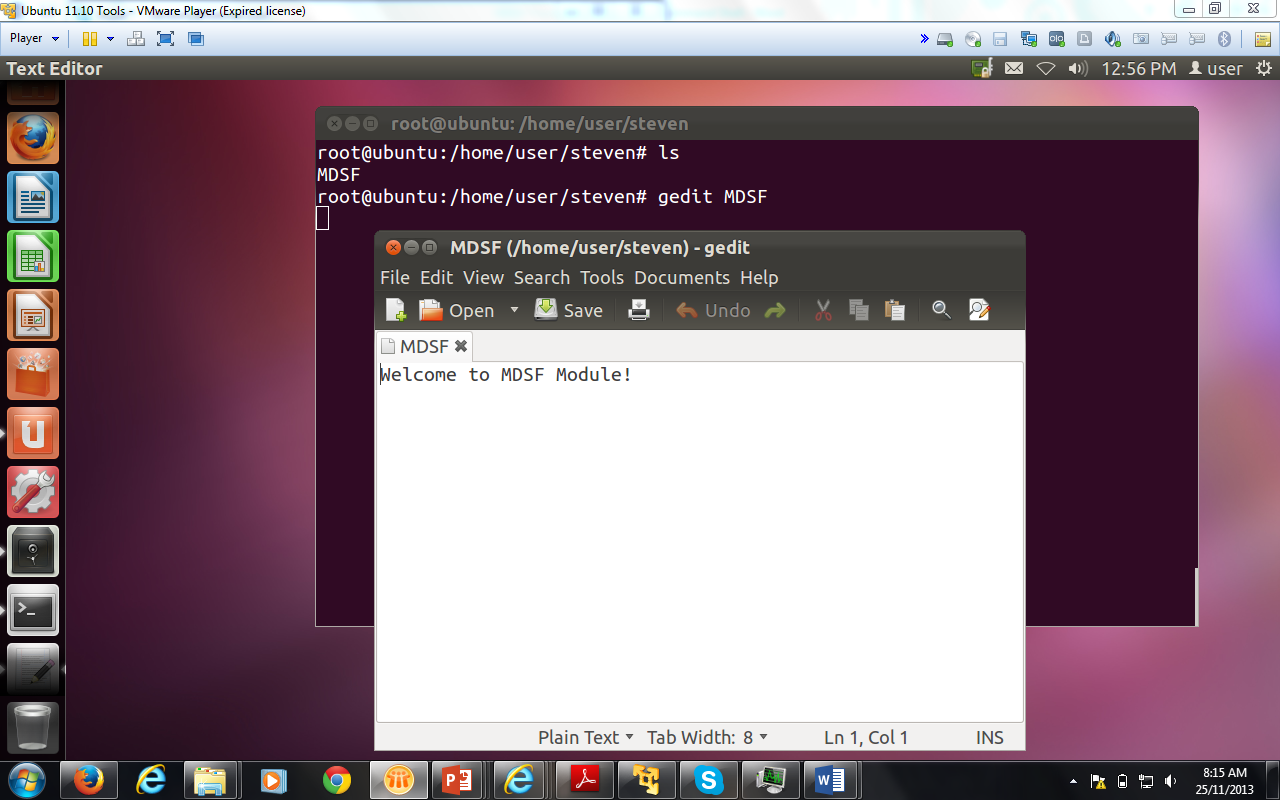
|  |
| --- |
| Cd /home/user/<your name> |

In <your name> directory, create a text document named MDSF and input some text. We are using text editor gedit, which is commonly used for the GNOME desktop environment.

Type **gedit MDSF** and enterthe text :’*Welcome to MDSF Module*!’ in the document. Save and exit from the document editor. Check that the text document is in the correct directory and path. How do you do this?

|  |
| --- |
| Pwd – for correct directory |

You should be able to view the MDSF text document under /home/user/<your name>:



Move the MDSF text document to /tmp directory, how do you perform this action?

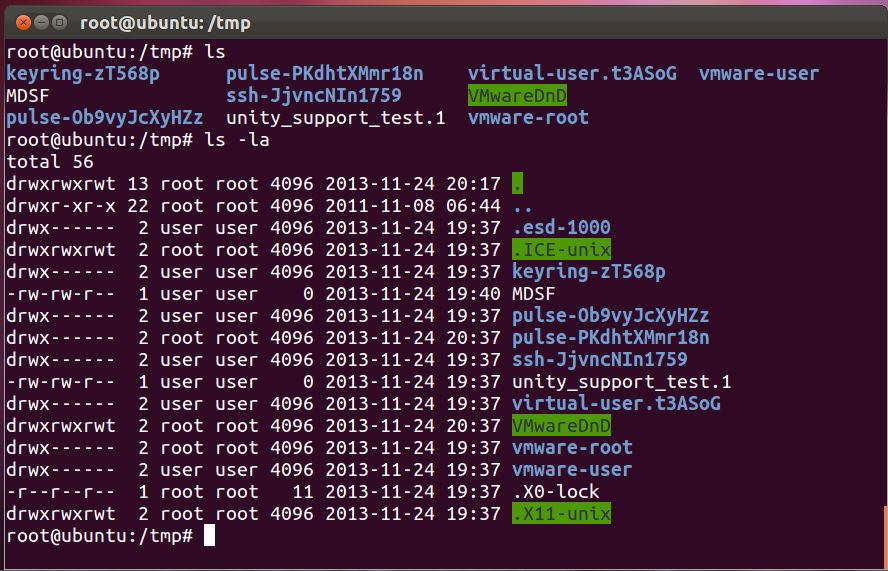
|  |
| --- |
| #mv /home/user/MSDF /home/user/tmp  Or  #mv MSDF tmp |

Check that the MDF document is no longer in the /home/user/steven directory and is instead in the /tmp directory.

|  |
| --- |
| /ls in the steven directory and /ls in the /tmp directory |

When you wish to view more detailed information about files and directories, you can use the ls command with flags:’-a’ which shows all files and ‘-l’ which shows the details such as permissions, links etc

Issue the **ls –la** command in the shell and you observe:



You are looking at the details associated with the /tmp directory. Noticed the difference between the directory listing of **ls** and **ls –al**

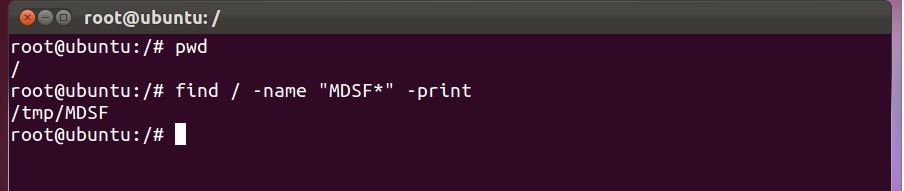
The **ls –la** command displays the file’s group and owner, file size (in bytes), date and time of creation/last modification as well as the file’s permission settings which determine who can read, write or execute the file.

**Finding Files**

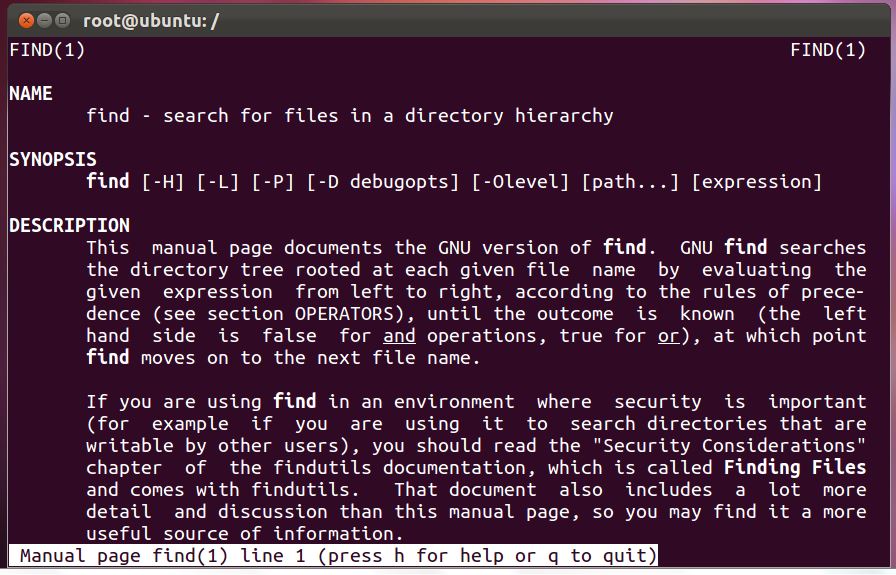
The find command is very useful for locating files (and directories).

Change directory to **/** by issuing **cd /**

Locate the MDSF text document by issuing the **find / -name “MDSF\*” –print** command



Issue the **man find** command to look at other options of using the find command via on-line manual pages.



The man command can be used to look up options of all available commands in Linux.

<http://linux.about.com/od/commands/l/blcmdl1_man.htm>

Remove the MDSF file as well as <your name> folder. How do you do this?

|  |
| --- |
| #rm MSDF\*(already in the tmp directory)  #mkdir \home\user\yourname |

**Task 3: Familiarization with Apt-Get tool**

The apt-get command is a powerful command-line tool, which works with Ubuntu's Advanced Packaging Tool (APT) performing such functions as installation of new software packages, upgrade of existing software packages, updating of the package list index, and even upgrading the entire Ubuntu system.

Being a simple command-line tool, apt-get has numerous advantages over other package management tools available in Ubuntu for server administrators.

Install a Package: Installation of packages using the apt-get tool is quite simple. For example, to install the network scanner nmap, type the following:

**sudo apt-get install nmap**

For further information about the use of APT, read the comprehensive Debian APT User Manual or type:

**apt-get help**

- The End -