Linux Basic Commands

Some useful commands for Linux (using the shell/terminal).

1. Open the 'Ubuntu-2013' (Linux virtual machine). Type Ubuntu in the Windows Start/Search box.

   If the root password is required it is **`90opl;./`**

2. Open a 'Terminal' (click the black icon on the top menu bar with >_ in it).

Navigating the file system

3. Use the following commands in the table below to navigate the filesystem. Try each of these commands and make sure you understand what they do.

Command	**Description**
`pwd`	Prints the name of the current directory
`ls -l`	Lists the names (and other details) of files and directories in the current directory
`cd <dir>`	Change directory to the given directory name[1]. If <dir> is omitted, changes to the user's home directory.
`mkdir <dir>`	Create a directory with the given name
`cp <file1> <file2>` `cp <file> <dir>`	Make a copy of <file1> named <file2> Make a copy of <file> in the directory <dir>
`mv <file1> <file2>` `mv <file> <dir>`	Rename (move) <file1> with the new name <file2> Move the file <file> to the directory <dir>
`rm <file>`	Remove (delete) a file

[1] Wherever you see <dir> or <file>, replace it with the name of the desired directory or file.

`rmdir <dir>`	Remove (delete) an empty directory
`zip –r <zipfile> <dir>`	Create a compressed zip file called <zipfile> which contains all the files in the directory <dir>

Some special file and directory characters:

Command	**Description**
/	The 'root' directory
.	The current directory
..	The parent directory
~	The current user's home directory
*	A regular expression that matches all (well almost all – see below) files and directories in the current directory
.<file> .<dir>	Files and directories whose names start with '.' are hidden in th sense that they are not listed with default ls options (and they are not included when a * is used)

Getting help

4. You can obtain detailed help for any command using the 'man' command. For example, try running the command:

```
> man ls
```

What is the option for listing *all* files in a directory (including ones which start with a '.')?

Downloading files.

5. Of course you can start the Firefox browser to do normal web browsing. But, you can also download files from the terminal using the 'wget' command. What is the name of the file created after running the following commands?

```
> mkdir prac1
> cd prac1
> wget http://www.imdb.com/index.html
```

```
> ls
```

Viewing files.

6. Try out commands such as ‘cat’, ‘less’ and ‘pico’ to view the contents of a text file. ‘pico’ will also let you edit a text file.

   Try to create a new file using ‘pico’ which contains the text “Hello world!”

Simple commands that might be useful for ‘forensic’ purposes.

The following commands could be useful when hunting for specific pieces of information during a forensic investigation. Read the man pages for these commands and think about why they might be useful to a forensic investigator.

Command	**Description**
`find`	A command which traverses the filesystem looking for files and directories that match the criteria you specify
`file`	Attempts to determine the file type
`strings`	Extracts all textual strings from a file
`grep`	Searches, line by line through a file looking for matches in a regular expression
`xxd`	Display the contents of a file in hexadecimal
`dd`	Extract contents from a file using an offset, a block size and a block count

7. What is the `find` command to locate all files which have the extension ‘.jpg’. (Hint: read the ‘man’ page.)

8. What is the `find` command to find all files *modified* in the past 30 days?

9. Using the `file` command determine the *type* of the following files:

   - the file downloaded with ‘wget’ in Question 5 above
   - /bin/ls
   - /usr/share/backgrounds/Begonia_by_fatpoint21.jpg

10. Extract the textual strings from each of the same three files. By using command line redirection, save the results to a file with the extension ‘.strings’.