

LAB 1: INTRODUCTION TO FORENSIC TOOLKITS

INTRODUCTION

The purpose of this lab is to begin to perform a basic forensic examination of a computer. You will learn to identify the various components of a PC, document the physical appearance of devices, note important serial numbers, and learn the basics of booting and using a Linux-based forensic operating system

RESOURCES AND LINKS

- Paladin
 - <http://www.sumuri.com/products/paladin/>
(free registration required for download)
- Hardware Forensic Write Blockers and Disk Duplicators
 - <http://www.tableau.com>
 - <http://www.cru-inc.com/cru-wiebetech/>
 - <http://www.logicubeforensics.com/>
- Other Linux-Based Forensic Operating Systems
 - SANS Investigative Forensic Toolkit (SIFT) Workstation
<https://digital-forensics.sans.org/community/downloads>
 - DEFT Linux
<http://www.deftlinux.net/>
 - Helix3 (free version no longer maintained):
<https://www.e-fense.com/store/index.php? a=viewProd&productId=11>

LAB 1: INTRODUCTION TO FORENSIC TOOLKITS

1. INITIAL PC EXAMINATION

PHYSICAL EXAMINATION

When beginning a forensic examination, the first thing you must do is document the exhibit. This will typically involve a visual examination of the device, noting down identifying marks (especially any visible damage), and may also involve photographs. This documentation helps us later in tying our findings back to the original piece of evidence. It may also help protect you against claims that you have damaged or tampered with the exhibit.

1) **Using the Swinburne computer on your desk.** Note down the following details:

- a) Brand / Make:
- b) Serial Number:
- c) Colour / Description:
- d) Optical Drives (description/brand/etc):
- e) Open the optical drives - do they contain any disks? If so, document these also:
.....
- f) Other Data Storage Devices (e.g. Memory card readers):
.....

LAB 1: INTRODUCTION TO FORENSIC TOOLKITS

INTERNAL COMPONENTS

Identifying the hardware contained within the PC (video cards, memory card readers, optical drives, storage devices.) can also be important. It is important to understand the storage capabilities or external interfaces that a device may contain.

2) Using the following photo. Identify the labeled internal components of a laptop:

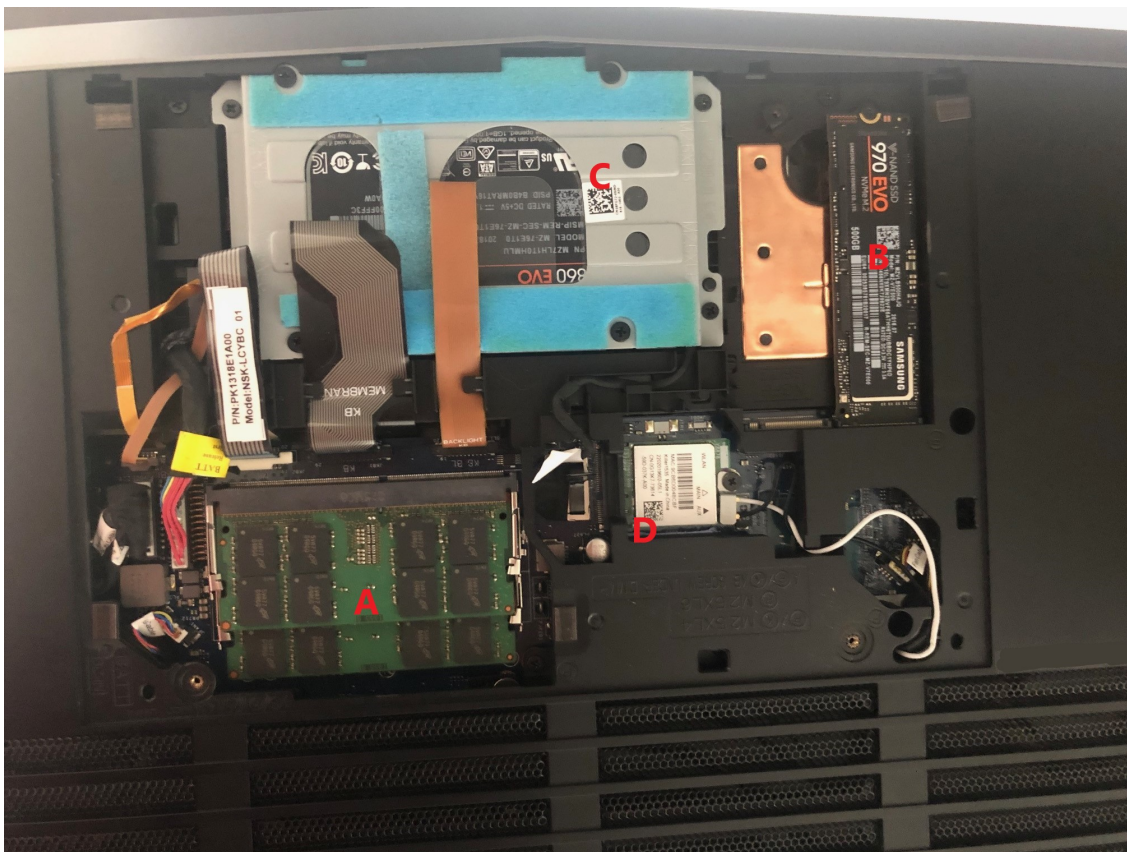


Figure 1. Laptop Internal Components

- a) Component A:
- b) Component B:
- c) Component C:
- d) Component D:

LAB 1: INTRODUCTION TO FORENSIC TOOLKITS

LOCATING AND DOCUMENTING STORAGE DEVICES

When examining a “dead” (powered off) computer, we typically remove the Hard Disk Drives and use a forensic workstation (running a forensic operating system, or with hardware write blocking tools) to examine the contents or take a forensic image of the drives.

Again, the first thing we want to do before commencing a forensic investigation is to document each storage device.

3) **Using the following two photos**, identify the following information:

a) Hard Disk 1:



Figure 2. M.2 Hard Drive

- i) Make:
- ii) Model:
- iii) Serial #:
- iv) Size: Gigabytes

LAB 1: INTRODUCTION TO FORENSIC TOOLKITS

b) Hard Disk 2:



Figure 3. SATA Hard Drive

- i) Make:
- ii) Model:
- iii) Serial #:
- iv) Size: Gigabytes

LAB 1: INTRODUCTION TO FORENSIC TOOLKITS

DOCUMENTING BIOS SETTINGS AND COMPUTER'S DATE AND TIME

The final step in documenting the computer hardware is to attempt to note down and time discrepancies that might be present. Computers keep an internal clock, which is relied upon when programs and operating systems store records of dates and times. If the clock in our evidence is incorrect, this could affect the results of our analysis.

Most PCs have a Basic Input/Output System (BIOS) which is an operating system stored on the motherboard. This basic operating system can be used to configure certain hardware settings, and to also set (and check) the current date and time. You may also want to enter the BIOS to change the "boot priority", to allow you to boot from a forensic live CD.

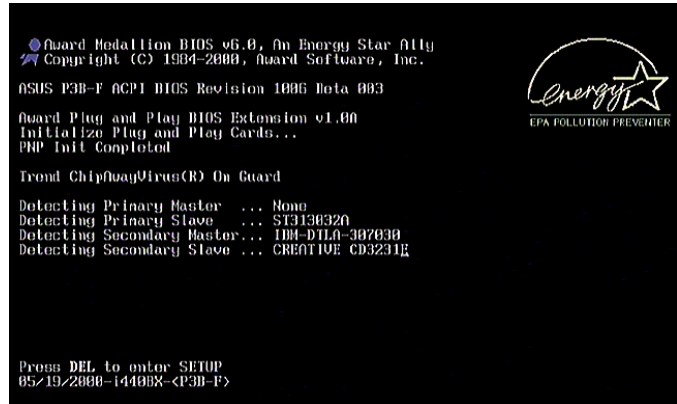


Figure 4. A Typical PC boot screen, showing "Press DEL to enter SETUP" in the bottom left corner

✓ To enter the BIOS on most desktop computers, power the computer on, and press the "Delete" key when prompted (other common keys are F2, F10 and F12)

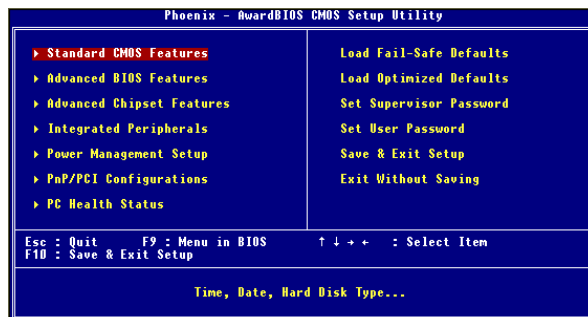


Figure 5. Phoenix AwardBIOS Main Screen

Typical BIOS screens. The first screen may show you the current date and time, or you may need to navigate through various menus to locate it. You should become comfortable with using the keyboard to navigate various BIOSs.

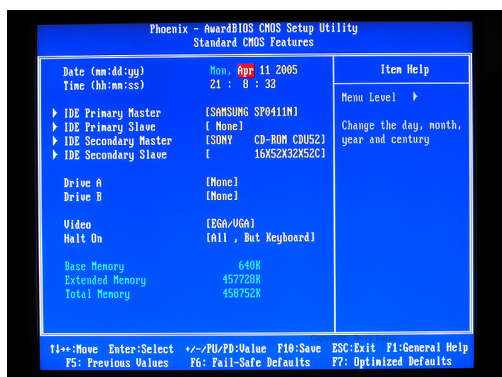


Figure 6. Phoenix AwardBIOS Standard CMOS Features

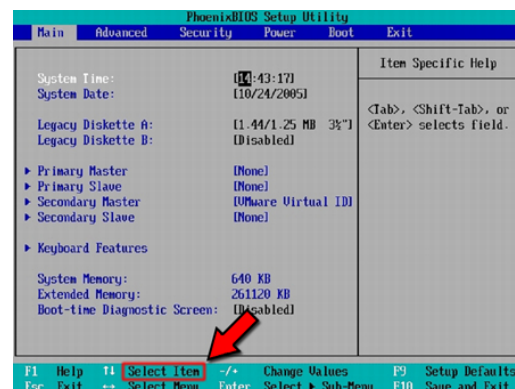


Figure 7. PhoenixBIOS Main Screen

LAB 1: INTRODUCTION TO FORENSIC TOOLKITS

2. FORENSIC TOOLS / PROTECTING THE EVIDENCE

Now we have documented the original evidence and identified and removed the Hard Disk Drives we want to examine the data on them. Of course, we want to be careful to not change any of the data. There are typically two ways to do this - we either need a forensic operating system (one that will only mount our evidence drive as “read only”, as opposed to “read write”), or hardware tools to protect the drive from our non-forensic operating system (e.g. Windows).

These types of hardware tools are typically called “write blockers”. A hardware write blocker is connected between the computer and the evidence drive and literally blocks commands from the operating system to write to the drive, while allowing read commands to flow normally.

Write Blocking



Figure 8. Diagram explaining how a hardware write blocker works

In this lab, we will be using a forensic operating system to view the contents of our own computer hard disks, as we do not have access to hardware write blocking devices.

LAB 1: INTRODUCTION TO FORENSIC TOOLKITS

3. EXAMINING THE EVIDENCE

For this exercise, we will examine the contents of a virtual computer using a Linux-based forensic boot CD. While forensic practitioners will usually prefer to remove the hard disk drives and access them using their own forensic workstation, this is not always possible (or easy!).

A forensic boot CD may often be useful in situations where hard disks cannot easily be removed (e.g. Mac computers, many laptops), computers without removable hard disk drives (e.g. many NetBooks, Macbook Air) or in servers where examining disks individually would prove useless due to hardware RAID. We may also use a forensic boot CD to quickly triage a machine without needing to dismantle it.

For this task, you'll need to copy the following files from T:\HED\ICT30010 to your desktop

1. paladin_edge.iso
2. ICT30010-Lab01-WinXPSP3-VM.zip

✓ **Note:** While we are using a virtual computer (VMWare machine) for this exercise, the steps you take would be identical if actually performing this on a real-life PC.

CHECKING / CHANGING BOOT ORDER

In order to boot from a live forensic boot CD, we need to make sure the computer will boot from our CD, and not the internal hard drive (or other media). If we fail to check the boot order, we may inadvertently boot up the suspect's computer, thereby making changes to the original evidence. Since we're going to make changes to the original evidence, we need to carefully document what we're doing.

✓ To enter the BIOS on a VMWare PC, power the computer on, and press the "**F2**" key when prompted. In VMWare, you'll need to ensure the virtual machine has "focus" by first clicking on the screen first. You'll only have a couple of seconds to do this before the PC boots.

- 4) Unzip ICT30010-Lab01-WinXPSP3-VM.zip
- 5) Add the extracted virtual machine to VMWare

LAB 1: INTRODUCTION TO FORENSIC TOOLKITS

- 6) Turn on your VMWare machine and enter the BIOS by pressing “F2”. If you don’t get into the BIOS first time, simply restart the machine and try again (in the real world you would want to immediately disconnect the power to prevent the machine booting, but we’re not too concerned in this case). Note the following:

a) Date and Time:

i) Current Date and Time:

ii) BIOS Date and Time:

iii) Date/Time Difference:

b) Boot Order:

i) First Boot Device:

ii) Second Boot Device:

iii) Third Boot Device:

- 7) Change the boot order so that the optical (CD/DVD) drive is the first boot device. The exact method of doing this will differ for different BIOSs. Ask if you’re not sure. For VMWare, use the arrow keys to move across to the “Boot” menu, then select the “CD-ROM Drive” and press the “+” key until it is the first option. Don’t exit the BIOS just yet!

a) Note the new boot order

i) First Boot Device:

ii) Second Boot Device:

iii) Third Boot Device:

LAB 1: INTRODUCTION TO FORENSIC TOOLKITS

BOOTING THE FORENSIC OPERATING SYSTEM

Now we've changed the boot order, we should be able to boot directly from our forensic CD. In this case, we'll simulate putting a CD in our virtual machine by pointing VMWare to the ISO file containing Paladin.

- 8) With VMWare open click Player -> Removable Devices -> CD/DVD (IDE) -> Settings

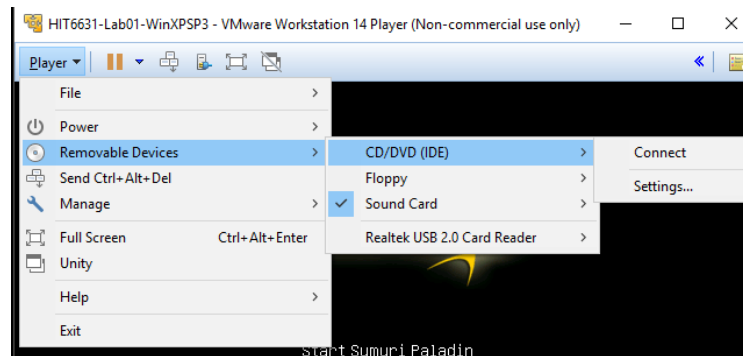


Figure 9. VMWare Removable Devices

- 9) Configure the VMWare virtual CD/DVD Settings

- a) Ensure "Connected" and "Connect at power on" are selected
- b) Select "Use ISO image file" and browse to where the CD/DVD image file is saved

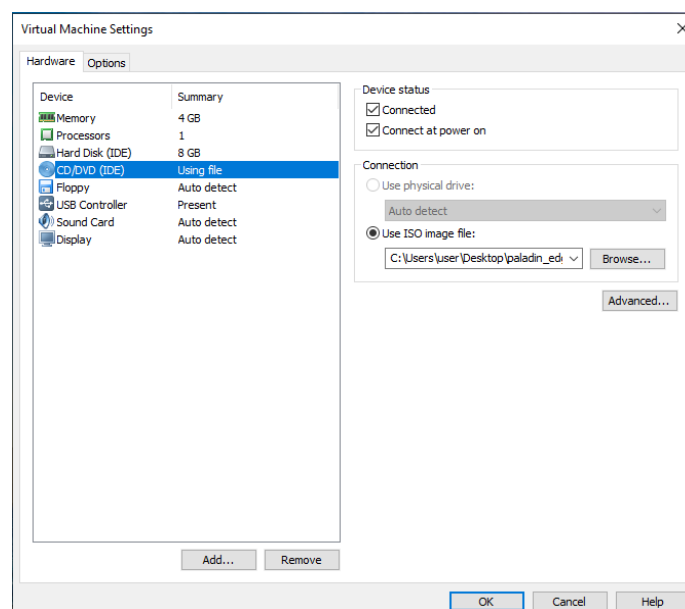


Figure 10. VMWare CD/DVD Settings

LAB 1: INTRODUCTION TO FORENSIC TOOLKITS

- 10) Now the Paladin boot CD is “in” your virtual PC, power it on. If you’re still in the BIOS, you should simply be able to “Exit Saving Changes” (under the “Exit” Menu). You will be prompted to select a boot option (as below). If Windows starts to boot, you have most likely not set your boot order correctly.

✓ While it’s not critical for this exercise if Windows boots (simply restart, check the BIOS settings and try again), if this were a real investigation you may have just changed a large number of files on the Windows computer!

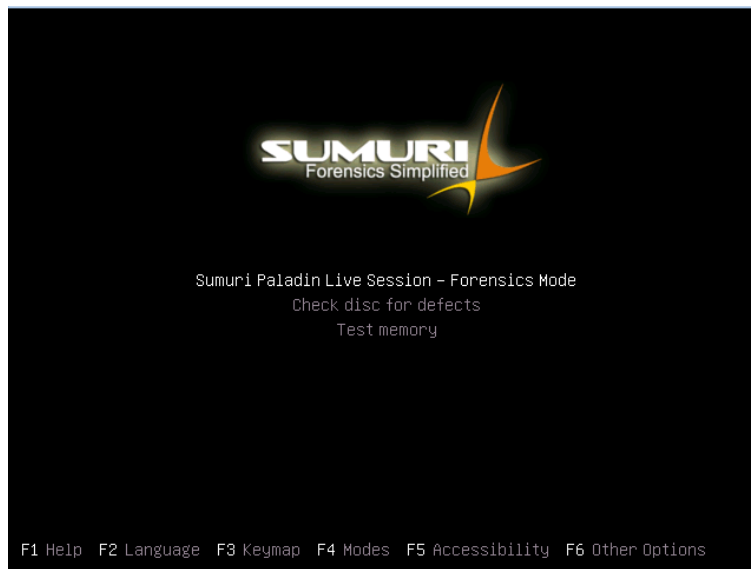



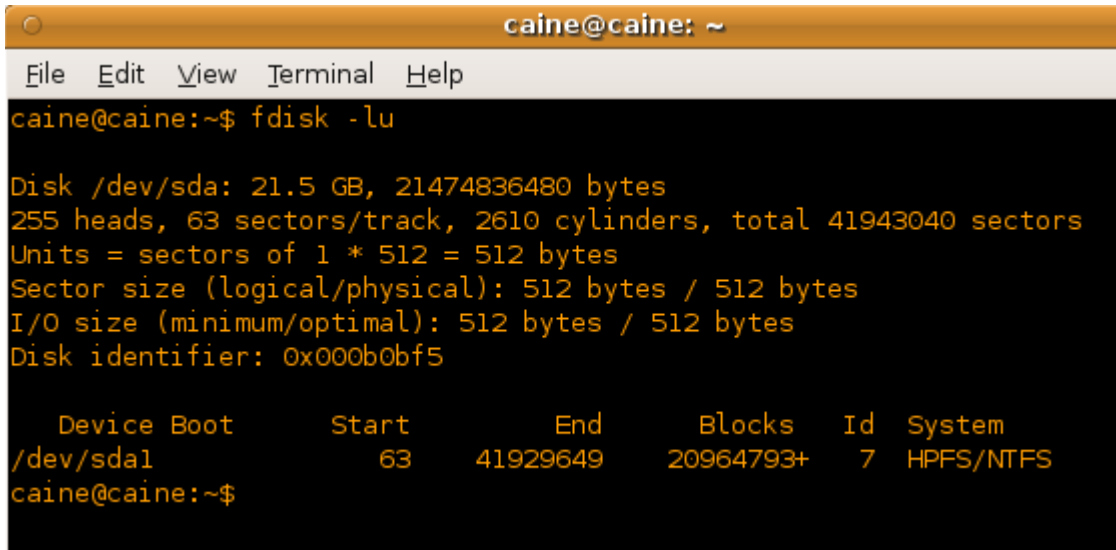
Figure 11. Paladin Boot Menu

- 11) Select the “Sumuri Paladin Live Session – Forensic Mode”
- 12) When Paladin finishes booting, you will see a customized Linux desktop.



LAB 1: INTRODUCTION TO FORENSIC TOOLKITS

- 13) Under the “App” menu, select open a terminal window by clicking the  icon.
- 14) It is important to determine and document the path of the windows hard disk, and the size and name of any partitions as this is the starting point of any investigation
 - a) The following screen shot and table are an example output



```
caine@caine: ~
File Edit View Terminal Help
caine@caine:~$ fdisk -lu

Disk /dev/sda: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders, total 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000b0bf5

   Device Boot      Start         End      Blocks    Id  System
/dev/sda1             63      41929649      20964793+    7  HPFS/NTFS
caine@caine:~$
```

Figure 12. Example Output from fdisk -lu

Partition (e.g. /dev/hda1)	Partition Type (e.g. NTFS/FAT)	Start Sector	End Sector	Total Sectors (End - Start + 1)	Total Size (MB)
/dev/sda1	HPFS/NTFS	63	41,929,649	41,929,587	(Total Sectors * Sector Size) / 1024/1024 = 20,474

Note: Often in computer forensics, sizes are represented in bytes. Sometimes wish to convert these to a different unit of measure such as kilobytes, megabytes etc., to achieve this we simply divide by 1024 until we reach the desired value (rounding up to the nearest whole value)

Eg.

Size in bytes = Total Sectors * Sector Size = 21,467,948,544

Size in kilobytes = 21,467,948,544 / 1024 = 20,964,794

Size in megabytes = 20,964,794 / 1024 = 20,474

Size in gigabytes = 20,473 / 1024 = 20

LAB 1: INTRODUCTION TO FORENSIC TOOLKITS

- b) Open a terminal and run the command `“sudo fdisk -lu”`

This command says: as the superuser/administrator (‘sudo’) - list all partitions (‘fdisk -l’), with sizes shown in sectors (final ‘u’ flag)

✓ If you forget the “sudo”, this command may not work. This is because many commands in Linux require “root” privileges (like Administrator in Windows). Without prefixing a command with “sudo”, all commands will be run as a normal user.

- c) Identify the internal operating system drive, and note the device name for this disk, pay attention to the fact that Paladin reports two different disks, one is the CD media that we booted from to launch paladin, the other is the windows disk

.....

✓ Remember that linux typically names disks “/dev/sda” or “/dev/hda”, while partitions are typically named “/dev/sda1”, “/dev/hda2”, etc.

- d) Note the sector size for the windows disk drive: bytes
(Hint: see the line that begins ‘Units = ‘)
- e) Note the details of all partitions below, you will need a calculator to work out the total size – there’s one built into Paladin (App Menu -> Accessories)

Partition (e.g. /dev/hda1)	Partition Type (e.g. NTFS/FAT)	Start Sector	End Sector	Total Sectors (End-Start+1)	Total Size (MB)

15) We’ll now mount the internal drive’s partition as read-only.

- a) Open a terminal window
- b) Now, we need to create a mount point. This is a directory in the filesystem which will represent the mounted volume. The Windows equivalent would be a drive letter (e.g. “C:”).
- c) Run the command `“sudo mkdir /media/windows”`.

LAB 1: INTRODUCTION TO FORENSIC TOOLKITS

- d) Now we can mount our drive. Look back and check what the device name for your windows partition was (in the table above). Run the command

`sudo mount -o ro,loop /dev/sda1 /media/windows`
replacing `"/dev/sda1"` with the device name of your windows partition, if necessary.

✓ The `"mount"` command tells the operating system to connect to the drive partition (`/dev/sda1`, in the example above) and read its file system. The `"-o ro,loop"` options tells mount to make sure changes can't be made to the partition.

- 16) Change to the `/media/windows` directory by entering the command `"cd /media/windows"`.

- 17) Attempt to create new file in the root of the windows drive by typing `"touch newfile.txt"`. What error message do you receive?

.....

- 18) Why can't we create the file? (*hint*: what options did we use when running 'mount'?)

.....

- 19) Get a directory listing of all files in the root of the Windows partition by typing the command `"ls"`. What folder might contain user-created files and documents?

.....

- 20) Change into this directory using the `"cd"` command.

✓ *Hint*: file and directory names in Linux are case sensitive. Also, you may need to enclose the directory name in quotes if it contains spaces. (e.g. `cd "Program Files"`).

- 21) Run the command `"pwd"`. What is the full path to the current directory?

.....

.....

- 22) Run `"ls"` again to list all the user folders under the current directory. Paladin will highlight folders in green. Write down the folders you've found

.....

Linux Command Cheat Sheet:

ls	list files in the current directory
ls -al	list all files (including hidden) with additional details
cd <i>dir</i>	change directory to <i>dir</i>
cd	change to home
pwd	show current directory
mkdir <i>dir</i>	create a directory <i>dir</i>
rm <i>file</i>	delete <i>file</i>
rm -r <i>dir</i>	delete directory <i>dir</i>
cp <i>file1 file2</i>	copy <i>file1</i> to <i>file2</i>
mv <i>file1 file2</i>	rename or move <i>file1</i> to <i>file2</i>
more <i>file</i>	output the contents of <i>file</i>
head <i>file</i>	output the first 10 lines of <i>file</i>
tail <i>file</i>	output the last 10 lines of <i>file</i>
touch <i>file</i>	create or update the time on <i>file</i>
sudo <i>command</i>	run <i>command</i> as root
date	show the current date and time
man <i>cmd</i>	show the manual for <i>cmd</i>

LAB 1: INTRODUCTION TO FORENSIC TOOLKITS

- 23) Use the `cd` command to change to the Test User folder
- 24) Run `ls -al NTUSER.DAT`. This prints the directory listing for the NTUSER.DAT file in a “long” format with additional information.

✓ The NTUSER.DAT file stores a user’s “registry” settings, which are regularly changed and updated while a user is logged on.

- 25) Note the date and time stamp associated with this file. This is the “Last Written” date – it reflects when the last time the contents of this file were modified.

.....

- 26) What do you think the significance of this date might be? (See the description of NTUSER.DAT above)

.....

- 27) Close the Terminal window (click the “x”, or type “exit” and press enter)

- 28) Click on the “Mounted Media” folder icon on the task bar and then double click on “windows”. This will open a GUI browser for the windows disk (similar to windows explorer).

- 29) Locate the NTUSER.DAT file you examined earlier. Right click on the file, and select “Properties”. Check that the Modified date is the same as the date you observed earlier.

- 30) What other date does the properties window provide?

.....

- 31) What do you think the significance of this date is?

.....

- 32) Unmount the windows partition by accessing the terminal and running the command `sudo umount /media/windows`

- 33) Before we finish using Paladin today, open up the Paladin toolbox program from the icon on the taskbar. We used the terminal and the “mount” command to view our windows partition. Can you work out how you could have achieved this using the toolbox?

- 34) With the device either mounted via the command “mount” or via the Paladin toolbox, navigate the filesystem and try to locate a potential password.

Hint: Have a look for a file containing passwords.

.....

- 35) Shutdown Paladin by clicking the power icon in the App Menu