Module	CMP209 – Digital Forensics
Module Lecturer	Dr Karl van der Schyff
Lab No	4
Due Date	complete before your next lab.

LAB INSTRUCTIONS

WHERE (and what) TO SUBMIT?	• Note that this lab is formative in nature. In other words, although you are expected to complete it, I do not require you to hand it in for assessment. Having said this, I am more than happy to give feedback if you wish to receive it.
WHAT ABOUT USING AI?	• Use of Generative AI Tools such as ChatGPT, DALL-E, Bard etc. is explicitly prohibited for this module's assessment (i.e., the court report). The output gleaned or generated from the tools mentioned and others that are similar relates to sources already published/available. **Also, be aware that the information obtained can be inaccurate or incomplete. Thus, all work should be your own.** If the assessment (i.e., court report) is found to have been plagiarised or to have used unauthorised AI tools, you will be referred to the Student Disciplinary Officer within the School and this may result in an Academic Misconduct charge.

LAB REQUIREMENTS

WHAT DO I NEED TO COMPLETE IT?	• Access to the "bare metal" Linux workstations in the labs. • You can also complete it using a VM, but the process is slightly different. • Access to MLS to download these documents (and the supplementary docs).

AIM OF THIS LAB

The aim of this lab is to:

- Create a verified physical image of a disk.
- Sign the group contract.

CORE LEARNING OUTCOMES

- Increased understanding and competence using the Linux operating system to perform digital forensics.
- Familiarization with the processes required to conduct a digital forensic investigation (read the supplementary docs for this). **In particular, how to make a verified physical image of a disk.**

Preservation and media imaging

1. Please ensure that you follow these using a lab workstation booted into Linux from the GRUB menu. Know that the procedure is slightly different if you are using a VM (but it can be done).

2. Additionally, ensure that you collect a "*suspect hard disk*" from me before continuing with this lab. Note that for the purposes of only this lab the hard disk we will provide you with is the disk seized from John Doe's house. Please consider working in groups if there are not enough physical disks to use.

3. Create a directory called `jd` within the home drive of the user you are logged in as. Note that if you are using the Ubuntu analysis VM, this folder will already exist.

4. Change into that directory using the command to test that it is there:

   ```
   cd /home/admin/jd
   ```

   Note that the above command assumes that the username is `admin`. If you are executing this from another Linux VM (i.e., Kali) your username will differ.

5. If you are using a physical lab workstation, turn it off at this point. Then, attach the suspect hard disk (i.e., the evidence drive) to your lab workstation physically using the appropriate cables we have provided you with (e.g., SATA/IDE/USB). Technically, you should follow this sequence when connecting the evidence drive:
   i. Attach the SATA/IDE/USB cable to the evidence drive.
   ii. Attach the power cable to the evidence drive. You might have to flip a small switch on the cable to enable it to work fully.
   iii. Turn on your lab workstation and boot into the bare metal version of Linux.
   iv. Connect the USB cable to your lab workstation once booted into Linux.

6. At this point you will need to explore the use of the `dmesg` command to find the device name that has been assigned to the evidence drive by the OS. Note that you should be noting the device name and not the partition name. In other words, something like `/dev/sdb` and not `/dev/sdb1` (i.e., there should be no number). Also note that you will most likely have to run this command as root so please include `sudo` in your `dmesg` command (i.e., `sudo dmesg | tail`).

7. The bare metal versions of Linux do not have `dcfldd` installed by default so please install it using this command:

   ```
   sudo apt-get install dcfldd
   ```

8. Once you have the device name, and you have installed `dcfldd`, use it (from the command line) to copy the evidence drive to a file on your workstation's desktop. Note that the following command also creates an MD5 checksum of the original data "*on the fly*".

   ```
   sudo dcfldd if=/dev/sd<whatever letter you found in step
   6> of=/home/admin/jd/johnDoe.dd
   conv=notrunc,noerror,sync hash=md5
   hashlog=/home/admin/jd/johnDoeDrive.md5
   bs=1406916 count=4096
   ```

   Note that the above is one (i.e., a single) command - do not type it on separate lines as listed above.

9. To ensure that the image you have just created is sound (i.e., what is meant by verified or verifiable), you have to calculate its md5sum and compare it with the md5sum of the original evidence drive. In other words, the hashlog file you created in step 8. Run the following two separate commands:

```
cd /home/admin/jd
md5sum johnDoe.dd > johnDoeAfterInitialImaging.md5
```

If these two values do not match, then something has gone wrong. In other words, the MD5 hash value within the hashlog file has to match the output of the above command as they refer to the same image. Always keep this in mind, and regularly check that this hash value has not changed during your investigation. If they do not match, you should technically retry your imaging process. Know that the "*official*" MD5 hash value for this module's case study is listed below and is associated with the `johnDoe.dd` file I have made available under week 5's content on MLS (under supplementary material):

```
d63dd1b8917ca28bac7c955fc3b6cd25
```

It is, however, unlikely (but possible) that your MD5 will match the one above simply because the current lab workstations do not perform write blocking of newly inserted USB storage devices. See Figure 1 below, which provides a screenshot of the output from the `dmesg` command.

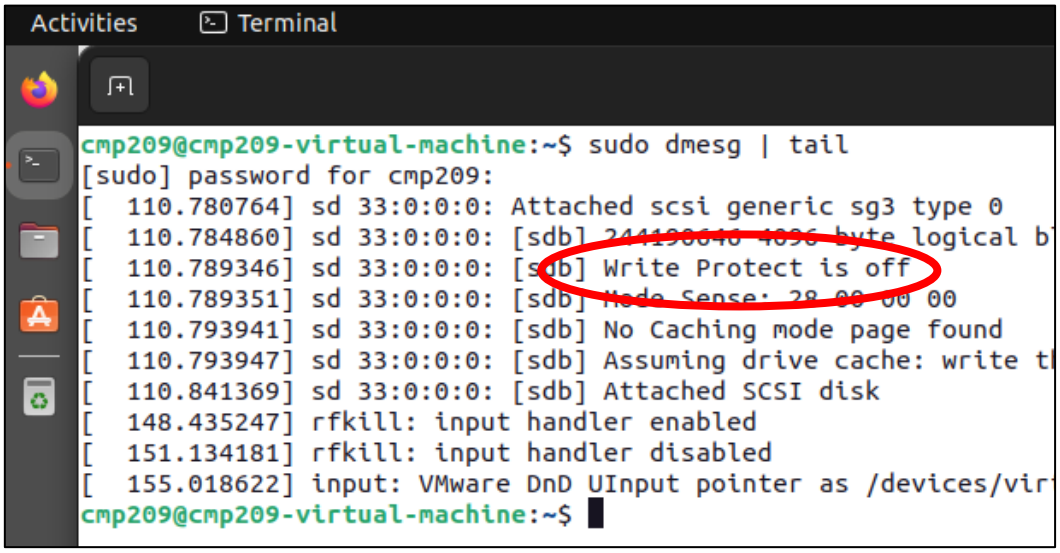

Figure 1.

10. To stop any further changes from taking place, use the `chmod` command (or the file manager) to change the file permissions of the `johnDoe.dd`, `johnDoeDrive.md5` and `johnDoeAfterInitialImaging.md5` files to make them read-only. I will let you research how to perform this.

11. The bare metal Linux workstations may not have the Sleuthkit installed. If this is the case, please install it using the command I provide below. If you are using the Ubuntu analysis VM, `mmls` is already installed so please avoid running this command.

```
sudo apt install sleuthkit
```

12. Once installed, use the `mmls` (and possibly also the `fdisk`) command on your image file to perform a disk or partition audit (see my demonstration videos for this week). Please find answers to the following questions:
    i. What capacity does the disk image report?

ii. What partitions are on the disk?
iii. How much space is unallocated?
iv. Does the sum of the partition sizes and the unallocated space equal the capacity of the disk?

If, for any reason, the `mmls` (or `fdisk`) commands do not work with the mage you have just captured, please use the `johnDoe.dd.gz` file I have made available on MLS (under week 5's supplementary material). Once downloaded, simply extract it (`gzip -d johnDoe.dd.gz`) and use the above commands to perform an audit. If you follow this route, you could simply use the analysis VM, which may be easier to work with.

13. Once you have completed your disk or partition audit, ensure that you keep your copy of the `johnDoe.dd` file somewhere safe (e.g., OneDrive, NTFS USB disk or your analysis VM). In fact, feel free to make more than one copy just in case. Note that you will now use this image in your investigation going forward.

Group contract

14. By now you should have either formed your own group or I would have allocated you to a group. Please sit with the rest of your group and discuss the group contract (in the Lab area for Week 4). Be sure to address all areas of the contract. **I am particularly interested in seeing that all members of the group have been assigned a set of responsibilities.**

15. Once complete, all group members should sign the contract. Once signed, please submit it via the submission link on MLS. I only need to see one submission per group.

Required reading

16. Download and read the supplementary material. In particular,
    i. *How to identify an OS from a disk image (*labelled *determing_the_OS_version_from_image.pdf).*
    ii. Forensic Imaging (a SANS publication).
    iii. Inspect the media imaging log spreadsheet (labelled *media_imaging_log.xlsx*).
    iv. Why software write protection may not always be the best approach (labelled *fallacy_of_software_write_blocking.pdf).*