Module	CMP209 – Digital Forensics
Module Lecturer	Dr Karl van der Schyff
Lab No	5
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. <u>Thus, all work should be your own.</u>** 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 analysis workstation, which is an Ubuntu VM that can be accessed via VMware Workstation. • You can also download the analysis VM from MLS via the tile labelled "*OneDrive link to analysis VM download files*". • Access to MLS to download the above (and the supplementary docs), but also the John Doe image file (and md5 hash value). The image file is labelled *johnDoe.dd.gz*

AIM OF THIS LAB

The aim of this lab is to:

- Search the contents of the John Doe disk image using certain Linux utilities.

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).
- **How to search the contents of a disk image.**

Physical searching – Part 1 – File-carving and metadata in Linux

1. Change to the `jd` directory which is located within the cmp209 users' home drive. To do this execute the following from the command line once you have logged in as cmp209:

   ```
   cd ~/jd
   ```

2. Place the `johnDoe.dd` image file inside the `jd` folder. You will find a copy of the `johnDoe.dd` image (and the associated MD5 hash value text file) within Week 5's supplementary section on MLS. I have uploaded a few videos as to how you could copy (and extract) the file once copied via Windows workstation using WinSCP. These videos are also on MLS under the resources for Week 5. Once copied and extracted, ensure that the image file is read-only:

   ```
   chmod 400 johnDoe.dd
   ```

3. Let's check the md5 by executing the following. Give this command a few minutes to run.

   ```
   md5sum johnDoe.dd
   ```

   Once executed, the hash value should equal `d63dd1b8917ca28bac7c955fc3b6cd25.` If the hash value is different then something has changed the contents of the image file.

4. From the command line, use `foremost` and `metacam` to find all JPG images taken with a Canon PowerShot camera.

5. Store the images (and any other files you created as part of this task) in a directory called `fileCarving` in your `jd` directory.

Physical searching – Part 2 – Using Autopsy

6. Run `autopsy` using the desktop shortcut. Note that this can be a slow process the first time you run it.

7. Create a new case called `johnDoe` using your name as examiner. Store it in a directory called `autopsy` under your `jd` directory. Use the same case number you used during acquisition. Then, supply the rest of the information required.

8. Add the `johnDoe.dd` image and wait for the ingest modules to complete their analysis. Note, that it is not uncommon for `autopsy` to fail at this point complaining that some of the ingest modules are not valid or could not run. If you struggle with this part on the Linux version of `autopsy`, I strongly encourage you to simply make use of the Windows version. Simply, download and install the Windows version if you decide to take this route.

9. Once the ingest process has completed, perform a keyword search for "birdwatching". Feel free to use other keyword searches as well.

10. Explore the other features of `autopsy`.

Physical searching – Part 3 – Do some more exploration on your own

Remember, the steps outlined thus far will only find a minimal amount of evidence. As an investigator you are responsible for "thinking outside the box". As such, you should think about what other evidence (other

files, for example) there might be to collect. Additional keywords would have to be used for this. What about using other techniques and file types?

Required reading

Download and read the supplementary material. In particular, the information by Brian Carrier (labelled *sleuthkit_brian_carrier.pdf*).