Module	CMP209 – Digital Forensics
Module Lecturer	Dr Karl van der Schyff
Lab No	8
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. The image file is labelled *johnDoe.dd.gz*

AIM OF THIS LAB

The aim of this lab is to:

- Examine the browser data on John Doe's disk image.

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 forensically examine the browser activity of a Windows user.**

Browser analysis – Part 1 – Recovering data from the image

Please read all the lab instructions before starting with your analysis. As stated in the learning outcome, the aim of this lab is to understand (and learn) how to extract a user's web-browsing activity from various files, databases and other digital artefacts that have been left behind as a consequence of normal browsing activity.

For this lab, you have a choice: You can either follow a command line-based approach, or you can select another tool. Some recommendations include:

- Autopsy (already installed on the Ubuntu analysis VM). You can also download and install Autopsy for Windows if you are doing your analysis on Windows.
- WEFA which can be downloaded from the supplementary section for Week 8.
- Any of the tools mentioned in the article by Oh, Lee & Lee (2011). The article is also available in the supplementary section for Week 8.

Remember, whichever route you choose, you should recover and analyse AT LEAST the browsing history, cache, bookmarks, and cookies from the John Doe image.

It is also really important to become increasingly inquisitive. You should be trying to figure out what John Doe has done by trying to figure out what John Doe was viewing and opening. Additionally:

- Keep in mind the kind of crime(s) that you are looking for evidence of.
- Remember that you are not just looking for images of birds, but wider involvement in any bird-related activities. Eventually you will need to recommend if John Doe should be charged and if so whether it is with "*possession of inappropriate images of birds*" and/or "*distribution of inappropriate images of birds*".
- Keep in mind that you should be looking to reconstruct not only what John Doe did, but also how he did it (and possibly why). Essentially, you are looking to prove *mens-rea* (i.e., intention).

1. Ensure that you change to the directory that contains your John Doe image and related files. Up to now the labs have been using the `jd` directory for these files.

2. Then, check the md5 checksum before proceeding.

3. Create a sub-directory called `browser` and change to that directory.

4. Then, create another sub-directory called `ie`. Once created, change to this new sub-directory.

5. As before, mount the johnDoe.dd image file using a loopback approach.

   ```
   sudo losetup -o 32256 /dev/loop30 ~/jd/johnDoe.dd
   sudo mount -o ro -t ntfs /dev/loop30 ~/suspectDrive
   ```

   Ensure that the directory you are mounting the loopback to exists before executing the above command. If not, you will receive errors similar to this:

   ```
   ntfs-3g-mount: bad mount point /home/cmp209/suspectDrive: No such file or directory
   ```

Browser analysis – Part 2

6. Given that John Doe used an old computer running XP, we need to locate the Internet Explorer cache at:

   `Documents and Settings/<username>/Local Settings/Temporary Internet Files/Content.IE5`

   Note: the location above depends on what version of Windows is used and may differ depending on the version of Internet Explorer (IE) in use.

7. Locate the cache file (one of the `index.dat` files – there are several) and use `pasco` to examine its contents for evidence that may be of use. Run these commands:

   ```
   pasco index.dat > ~/jd/index.pasco
   ```

   Then, open the `index.pasco` file in a text editor or spreadsheet program, such as LibreOffice Calc or Excel. Note that there may be several users' data to inspect, so name these files appropriately.

8. Locate the IE History which is at:

   `Documents and Settings/<username>/Local Settings/History/History.IE5.` As before, note that this location will vary depending on the operating system and browser versions in use. The IE cookies file is called `index.dat` and is located in a sub-directory called `Cookies.`

9. It might be easier to find the cookies associated with the John Doe case by using Autopsy. The figure below shows what this area in Autopsy would look like. Just please note that the screenshot used below is from another case study (i.e., not the John Doe case).

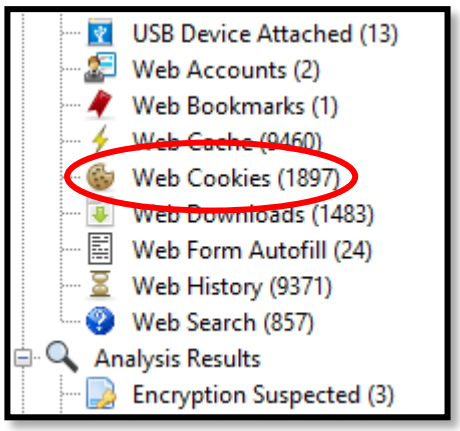

Figure 1

10. You should also use the `find` command to locate all other `index.dat` files. Once located, please investigate their contents using the `strings` command for example.

11. In addition to the above, bookmarks, typed URLs, recently used items, and autocompletion-type data may be available. Use Google as a means to research how these could be located and attempt to recover additional (and useful) evidence. You could also use Bulk Extractor. Just note that I typically use the Windows version of this tool (specifically v1.5.5) and that you will require Java to run it. There is a video lecture in Week 10's MLS webpage which demonstrates how to use Bulk Extractor.

Browser analysis – Part 3 – Cleaning up

12. Unmount the johnDoe image and remove the loopback device:

```
sudo umount ~/suspectDrive
sudo losetup -d /dev/loop30
```

13. Wait a second…maybe John Doe used other browsers in addition to Internet Explorer. How should be gather evidence from them?