Module	CMP209 – Digital Forensics
Module Lecturer	Dr Karl van der Schyff
Lab No	7
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 registry 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 registry of a Windows computer.**

Directed searching – Part 1 – Examining the registry

1. Again, check the MD5 hash of your `johnDoe.dd` file. It should be unchanged from when you first created it.

2. Use the loopback mounting technique to mount your `johnDoe.dd` image file. We covered loopback mounting last week. Note that if you receive an error that the device or resource is busy, try and increment your loopback device number. For example, instead of using `/dev/loop30` use `/dev/loop60` etc.

3. Then, create a `registry` directory in your main `jd` working folder. You can create this folder in a different directory (i.e., not your home directory), but then permissions can become problematic.

4. Once created, copy the registry files from the mounted `johnDoe.dd` image to the registry directory you created in step 3. Note that the following command assumes that you mounted the John Doe image under `~/suspectDrive`. It also assumes that you created your registry directory in `/home/cmp209/jd/`

   Execute the following to copy the required files. Note that each pair of commands listed below are actually one command and should thus be types on one line. Also note that there is supposed to be a space after the command specifying the source of the copy operation:

   ```
   sudo cp ~/suspectDrive/WINDOWS/system32/config/SAM
   /home/cmp209/jd/registry

   sudo cp ~/suspectDrive/WINDOWS/system32/config/SECURITY
   /home/cmp209/jd/registry

   sudo cp ~/suspectDrive/WINDOWS/system32/config/software
   /home/cmp209/jd/registry

   sudo cp ~/suspectDrive/WINDOWS/system32/config/system
   /home/cmp209/jd/registry

   sudo cp ~/suspectDrive/Documents\ and\ Settings/johndoe/NTUSER.DAT
   /home/cmp209/jd/registry
   ```

5. Unmount the John Doe image and remove the loopback device.

6. Ensure that you are in the registry directory you created in step 3 before continuing. If not, you could change to this directory by issuing the following command:

   ```
   cd /home/cmp209/jd/registry
   ```

7. Change permissions to give the cmp209 user (your current logged in user account) the required access to the files. Note that these are two separate commands:

   ```
   sudo chown cmp209 SAM SECURITY software system NTUSER.DAT
   chmod u+w SAM SECURITY software system NTUSER.DAT
   ```

8. Use the tool `chntpw` to find a list of user accounts on John Doe's computer. Execute:

   ```
   chntpw -l SAM
   ```

   Ensure that you are in the `/home/cmp209/jd/registry` directory when you execute the above.

9. Run `fred` and load the registry files you were able to retrieve. You can run `fred` using the desktop shortcut or from the command line. Open these files one at a time by navigating to File → Open hive. Once completed, you should see a folder in the tree (on the left) for each registry file. You may also be able to get some use out of `regripper`.

10. Before embarking on any further analyses, you will need to read the article listed under (a) below. I have made it available in the supplementary reading list for this week (together with the other two). The techniques covered by Carvey (2005) are older as they have to match the version of Windows on John Doe's computer. For those interested in reading more widely, consider reading about the newer techniques within articles (b) and (c) listed below.

    a.) Carvey, H. (2005). The Windows Registry as a forensic resource. *Digital Investigation*, 2(3), 201-205.

    b.) Park, J. (2018). TREDE and VMPOP: Cultivating multi-purpose datasets for digital forensics–A Windows registry corpus as an example. *Digital Investigation*, 26, 3-18.

    c.) Singh, A., Venter, H. S., & Ikuesan, A. R. (2020). Windows registry harnesser for incident response and digital forensic analysis. *Australian Journal of Forensic Sciences*, 52(3), 337-353.

11. At this point I would like for you to take note that information about USB devices is typically stored in the following registry location:

    ```
    HKEY_LOCAL_MACHINES\System\CurrentControlSet\Enum\USBSTOR.
    ```

    If you are using `fred` this information will appear under this location:

    ```
    ControlSet002\Enum\USBSTOR
    ```

    The word `ControlSet002` simply means that you are working with the current control set. More importantly, this location contains a unique entry for each device that was ever connected to John Doe's computer. Even more information can be obtained from here:

    ```
    HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Device-Classes\
    {53f56307-b6bf-11d0-94f2-00a0c91efb8b}
    ```

12. In short, find out which USB storage devices have been connected to John Doe's computer.

13. To find out where these devices were mounted (together with their unique id's), investigate:

    ```
    HKEY_LOCAL_MACHINE\System\MountedDevices
    ```

    As well as the following location from the `NTUSER.DAT` file:

    ```
    HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
    ```

List the discovered devices.

14. Which software packages were installed and available to users?

15. You can also use `Autopsy` to perform registry investigations. Open Autopsy and perform a similar registry investigation.

16. What else do you think we could gain by investigating the registry of John Doe's computer? You will have to start thinking broadly at this point and should not be relying solely on the lab exercises.

17. Before completing the lab exercises, please check the MD5 hash of the `johnDoe.dd` image to ensure that you have not changed d it whilst performing the above steps.

Howto install fred

18. As stated, `fred` is already installed on the Ubuntu analysis VM, so please only follow these steps if you are installing it on your own computer or VM.

```
sudo wget -nH -P /etc/apt/sources.list.d/ https://deb.pinguin.lu/deb.pinguin.lu.list

sudo wget -nH -P /usr/share/keyrings/ https://deb.pinguin.lu/deb-pinguin-lu.gpg

sudo apt update

sudo apt install fred

sudo apt install fred-reports
```