Abertay University

Module	CMP209 – Digital Forensics
Module Lecturer	Dr Karl van der Schyff
Lab No	3
Due Date	complete before your next lab.
LAB INSTRUCTIONS	
WHERE (and what) TO SUBMIT? WHAT ABOUT USING AI?	• Please complete the regular expression exercises on your own. • 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 do wish to receive it. • 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 a Linux operating system that has Internet connectivity. Either your own, or the Ubuntu analysis VM on the lab workstations. • 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 documents).

AIM OF THIS LAB

The aim of this lab is to:

- Familiarise students with the Linux command line interface (CLI).

CORE LEARNING OUTCOMES

- Increased understanding and competence using the Linux operating system and the associated command line interface (CLI).
- Familiarization with the processes required to conduct a digital forensic investigation (read the supplementary docs for this). **In particular, the acquisition (now specifically searching) of evidence by using regular expressions.**

Understanding of the Linux CLI

1. Download and open the *Linux-Fu* document from MLS. You will find this document within the Labs section of the Week 3 Teaching Material (i.e., the same place you found this lab).

2. Once opened, please complete Section 5 (Redirection, pipes, filters), and Section 6 (Searching).

Required reading

3. Download and read the supplementary material. In particular,
    a. *An Intro to Regular Expressions.* I have made a downloadable cheat sheet available for easy reference (labelled *reg_exp_cheat_sheet*).
    b. A pdf file containing a decent list of file signatures. Very useful!
    c. A hexadecimal cheat sheet (also contains some reg exp content). Also, very useful.
    d. *The Law Enforcement and Forensic Examiner's Introduction to Linux.* It has recently been revised and is now very comprehensive.
    e. Sleuthkit and Autopsy by Brian Carrier. Labelled as *sleuthkit_brian_carrier.*