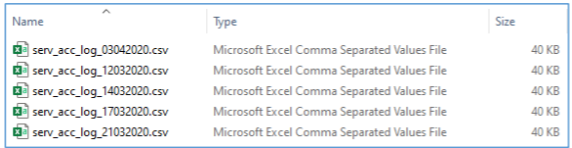
# **Assignment Description**

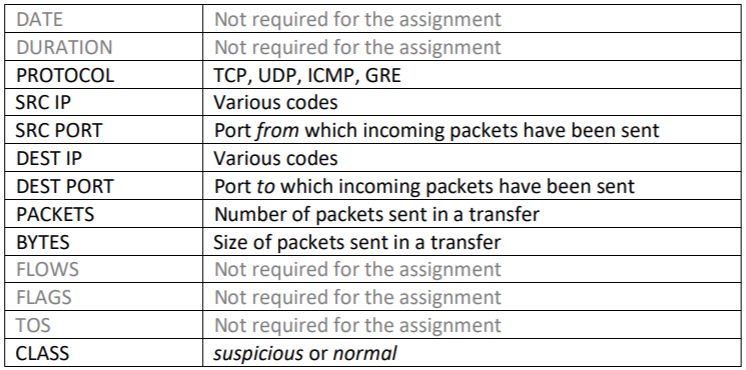
Having completed two main portfolio activities, you are now required to further develop your shell scripting skills by developing a script that automates a task commonly performed by Linux administrators - the analysis of server access logs to identify and report upon suspicious activity.

To develop and test your script, you have been provided with a set of five (5) server access logs.



*All the above log files will be in the same folder as the bash script.*

Each server access log contains 500 records organised into the following columns:

**

## **Write the Code**

### Functional Requirements

Your server access log must provide the user with the following functionality:

1. Run a search on available server access logs based on one (1), two (2) and three (3) field criteria inputs.
2. Give the user the option to a) search all server access logs available in a directory, or b) search just one (1) specific log of the user’s choice.
3. Export the results of any search to a text file and destination directory of the user’s choosing. Where the file and/or destination directory nominated by the user are non-existent, your script will create them.
4. Any records in which the CLASS field is set to normal are to be automatically excluded from the search results printed to the screen.
5. When the PACKETS and/or BYTES fields are used as search criteria, the user should be able to choose greater than (-gt), less than (-lt), equal to (-eq) or not equal to !(-eq) the specific value they provide.
6. When the PACKETS and/or BYTES fields are used as search criteria, totals for each of these should also be calculated and displayed as the final row of the search results printed to the screen.
7. When the SRC IP or DEST IP fields are used as search criteria, the user should only need provide a partial search string rather than a complete value, e.g., search using the partial string EXT rather than the exact value EXT\_SERVER.

### Usability, Reliability and Efficiency Requirements

1. All string-based searches should be case insensitive.
2. The results of any search are to be printed to the screen in a columnar format, uniformly aligned and spaced.
3. All user inputs are to be fully validated and sanitised as required to ensure the correct execution of subsequent code.
4. The script is to display a high level of abstraction, i.e., the hard coding of values is to be avoided.
5. The efficiency of your code will also be considered, hence the degree of thought you apply to the selection of and interaction between shell script elements such as logical tests, control structures (if-elif-fi, loops, arrays), functions, command substitution, regular expressions, piping, redirection, and utilities, e.g., awk, is important.
6. The user must be able to conduct as many search operations as they wish without the script terminating. Hence, the script must continue to run until the user specifically chooses to terminate it via a menu option.
7. All menus, options and prompts are to be easily understood and require minimal input from the user in response.
8. Sound code structure and full commenting will be examined by your tutor and factor into your grade.

### Enhanced Functionality

Enhance the functionality of your server access log analysis tool by devising and coding one (1) additional feature that is not available as one of the default features listed under the **Functional Requirements** section of this brief. This additional feature is to allow the user to work with the server access logs in a useful and meaningful way that adds genuine value to the analysis tool. An example might be to provide the user with the ability to send a server access log analysis report to a specified email address instead of the default option of storing it as a text file in each directory.

*My enhanced functionality is that the code can automatically search all .csv files in the directory and let the search run on all of them simultaneously or any one at a time. This allows for the code to work in real life scenarios where someone might have to search through all the log files at once rather than just one or five of them at a given time. This also greatly improves the efficiency of the user and lets them save a lot of time.*