Name: _____ Student ID:_____

You will need:
Lab Computer
simpsons_samba_log_simulation.csv

COS30015 IT Security

Lab 11 week 11

This lab is essential preparation for your second technical assignment. Specifically, it relates to part A, helping you gain experience looking through and making sense of what has happened in a log file.

In this example we have a made up log file and structure mimicking the Samba service. Typically a log will have it's own defined structure but there are some usual things you would expect to see. Things such as:

- Time
- Date
- Service
- Alert

The log being investigated in this lab is fictional, but investigating it allows you to practice how you make sense of a large number of recorded actions. To help get you started, the following helps you understand the structure of the log.

Timestamp

Format: yyyy/MM/dd HH:mm:ss.SSS

Example Entries:

2024/09/12 10:00:00.123
2024/09/12 15:45:32.456

Description: This column records the exact date and time when the log entry was created. The timestamp helps in tracking when each action occurred and is useful for chronological analysis of events.

Log Level

Possible Values:

1: Informational - Indicates normal operation or minimal information.
2: Warning - Indicates potential issues or notable events that are not errors.
3: Error - Indicates significant issues or errors that need attention.

Example Entries:

1
2
3

Description: Specifies the severity of the log entry. It helps in filtering and prioritising log messages based on their importance or impact.

Process ID

Format: Integer

Example Entries:

1234
5678

Description: Represents the identifier for the process that generated the log entry. Useful for distinguishing between logs from different processes in a multi-process environment.

Thread ID

Format: Integer

Example Entries:

2345
6789

Description: Represents the identifier for the thread within the process that generated the log entry. This can be used for debugging issues related to specific threads.

Samba Component

Possible Values:

smbd: Samba daemon responsible for file sharing and printer services.
nmbd: Samba daemon responsible for NetBIOS name service.
winbindd: Samba daemon responsible for retrieving user and group information from Windows domain controllers.

Example Entries:

smbd
nmbd
winbindd

Description: Identifies the specific Samba service or module that created the log entry. This helps in understanding which part of the Samba suite is involved.

Message Text

Format: Free-form text

Example Entries:

File 'donuts.txt' uploaded successfully
Error opening file 'springfield_map.png': Permission denied
File 'krusty_comedy_routine.mp4' downloaded successfully

Description: Contains the detailed message about the log entry, providing context on the action performed, any errors encountered, or other relevant information.

IP Address

Format: IPv4 Address

Example Entries:

192.168.1.10
192.168.1.15

Description: Represents the IP address of the client or system that interacted with the Samba service. Useful for tracking which clients are performing actions and for network-based analysis.

User

Possible Values:

Homer_Simpson
Marge_Simpson
Bart_Simpson
Lisa_Simpson
Maggie_Simpson
Ned_Flanders
Mr_Burns
Smithers
Krusty_The_Clown
Apu_Nahasapeemapetilon

Example Entries:

Homer_Simpson
Bart_Simpson

Description: Represents the Simpsons character who performed the action. This helps in identifying which user (character) was involved in each log entry.

Action

Possible Values:

upload: Indicates that a file was uploaded to the server.
download: Indicates that a file was downloaded from the server.
edit: Indicates that a file was edited.
view: Indicates that a file was viewed.

Example Entries:

upload
download
edit
view

Description: Specifies the type of action performed on the file. This column helps categorise the log entry based on the nature of the action.

File Name

Format: filename.extension

Example Entries:

donuts.txt
nuclear_plant_report.xlsx
power-plant-codes.txt

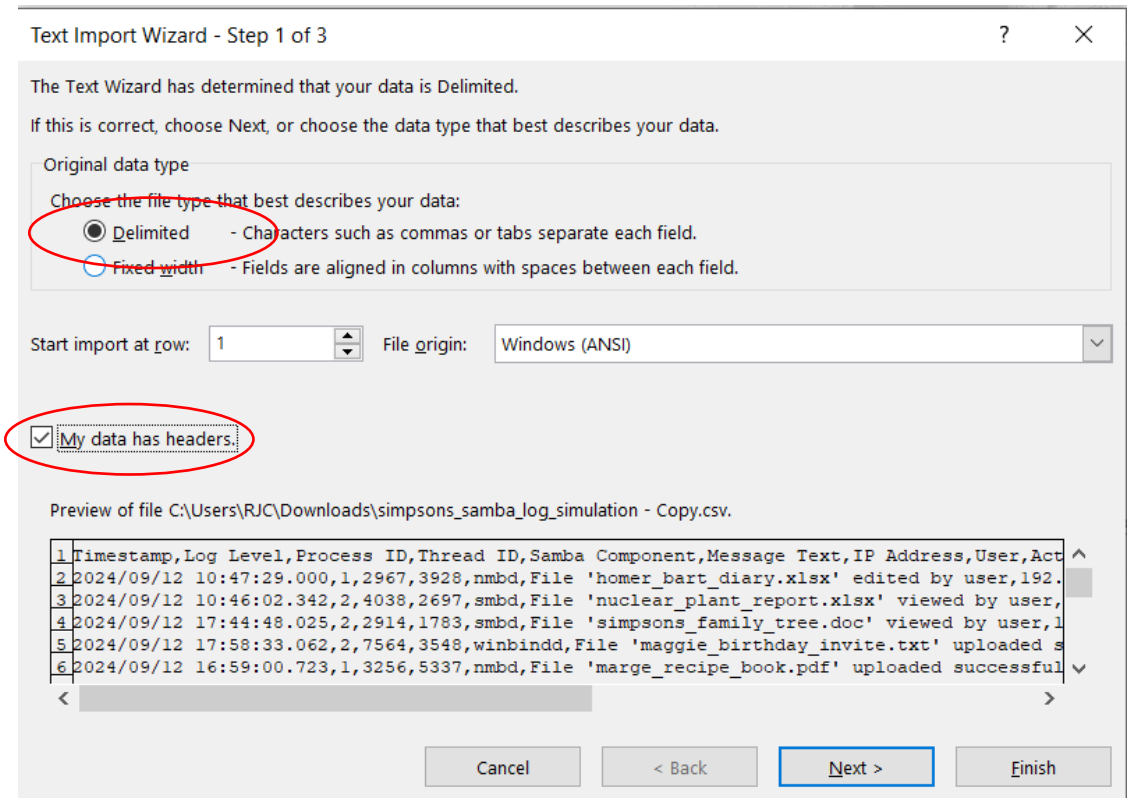
Description: Represents the name of the file involved in the log entry, including its extension. This is crucial for identifying which file the action pertained to.
Summary

Name: _____ Student ID:_____

Task 1 Import data

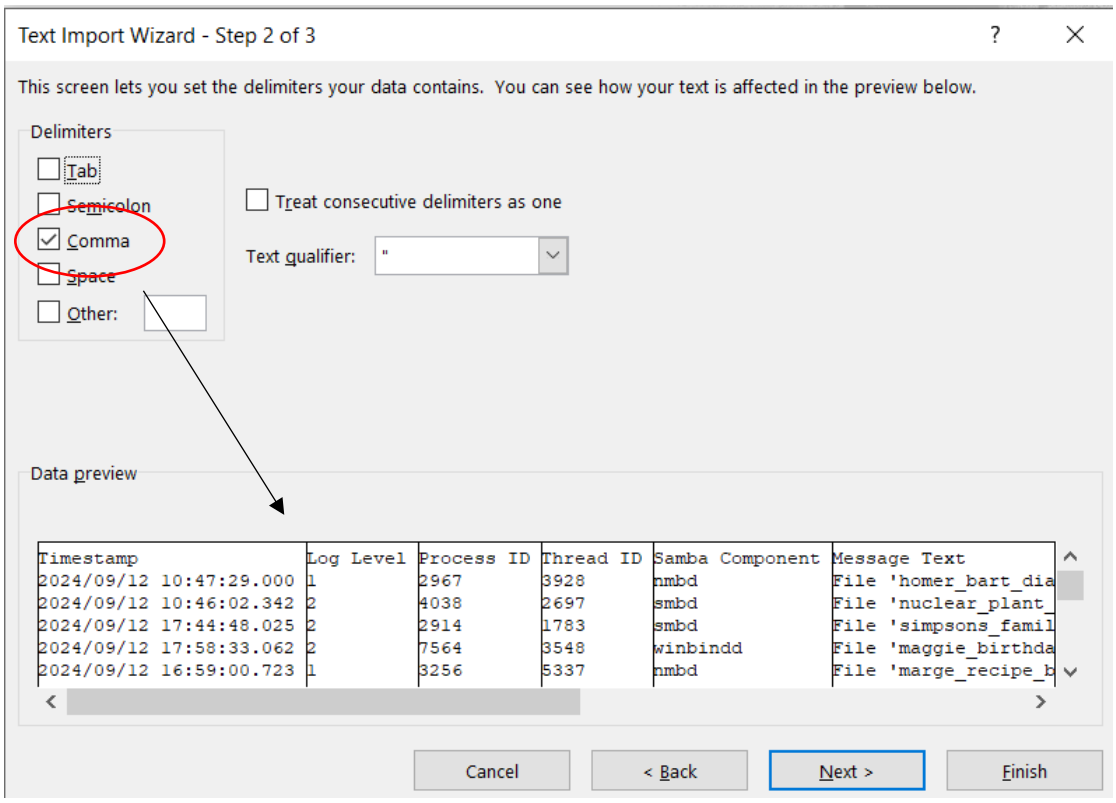
You can either use Excel to analyse the log file. Open Excel and then open the file, the Import Wizard should be prompted automatically. Consult your tutor or the Internet if it doesn't.

Step 1: Choose that the file is delimited (it's a csv), select that is has headers



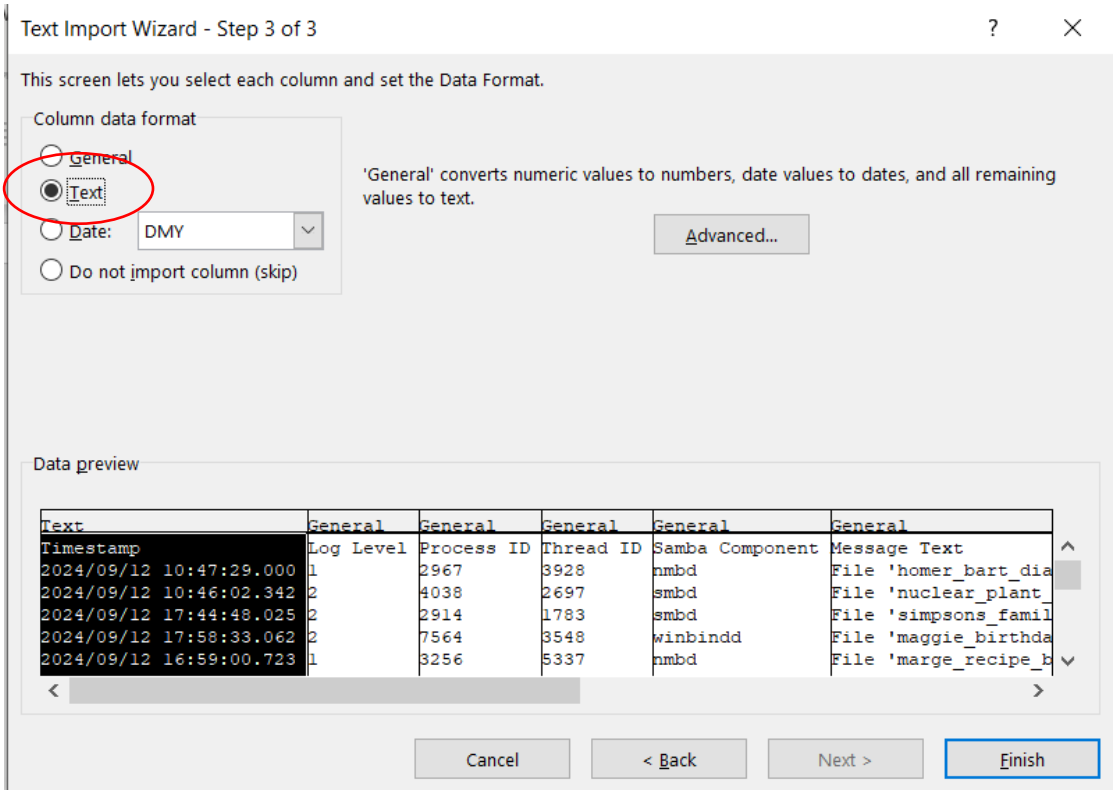
Step 2: Choose the delimiter type as comma

Name: _____ Student ID:_____



Your data should appear as above

Step 3: Column 1 can be marked as text

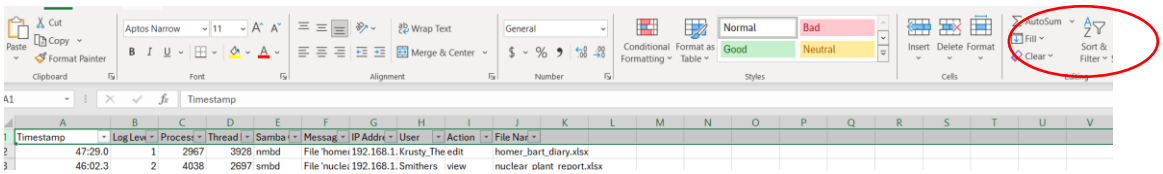


Your data is imported no, ignore the possible data loss warming.

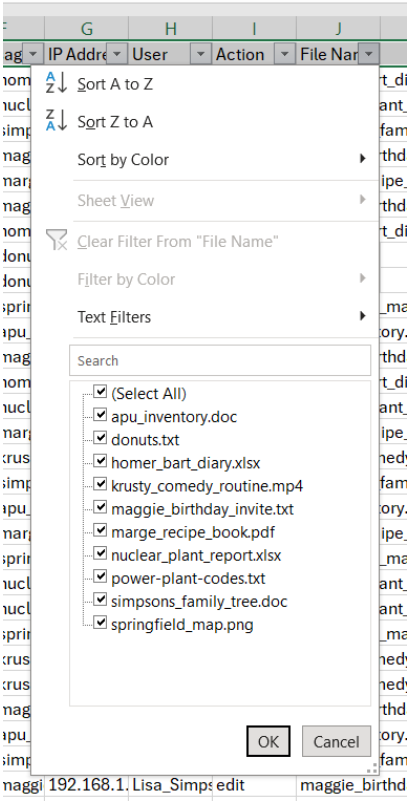
Name: _____ Student ID:_____

Task 2: Analyse your data

Select the top row of column headings, from Sort & Filer select filter



Exploring the file can now be achieved by filtering based on the conditions you set. For example, selecting the drop down menu for File name, we can observe that there are 10 unique files recorded in the log



By deselecting or selecting identified entries here we can filter the log. This can be applied to other columns also and in combination. Don't forget to clear your filters (select everything again in a filtered column) when you are answering a different question when required.

1. **What file types are recorded in the Samba share log?**

Name: _____ Student ID:_____

Now use a combination of filters or pivots to answer the following questions.

2. **How many unique users are recorded in the log file? What account names can be identified?**

3. **What is the first and last timestamp in the log file?**

4. **What files were edited?**

5. **Who edited these files?**

Name: _____ Student ID:_____

6. **What files were edited, and how many times?**

7. **What files were uploaded, and how many times?**

8. **What files were viewed by Krusty the Clown, and how many times?**

9. **Which IP was used the fewest amount of times?**

Name: _____ Student ID:_____

10. It appears a file was edited 15 times. What file had so many edits?

11. What files were viewed from 192.168.1.20?

12. What files were uploaded but not edited?

13. It appears someone has been editing the Simpson family tree. Who could have edited it?

Name: _____ Student ID:_____

14. **Someone has edited Krusty's comedy routine video which must be the reason he didn't perform well. Who edited, and who edited it last and at what time?**

15. **Someone has stolen an important file only downloaded once. What is this file, who downloaded it and at what time?**