|  |
| --- |
| The Wealth of Nations Banjoko Olasehindemi  5th April, 2024 |



Table of Content

Table Contents

Main body ................................................................................….......…………........ 1

1.0 Policies and Procedures ***..................................................................…***……….1

2.0 Excel............................................................................................................... 3

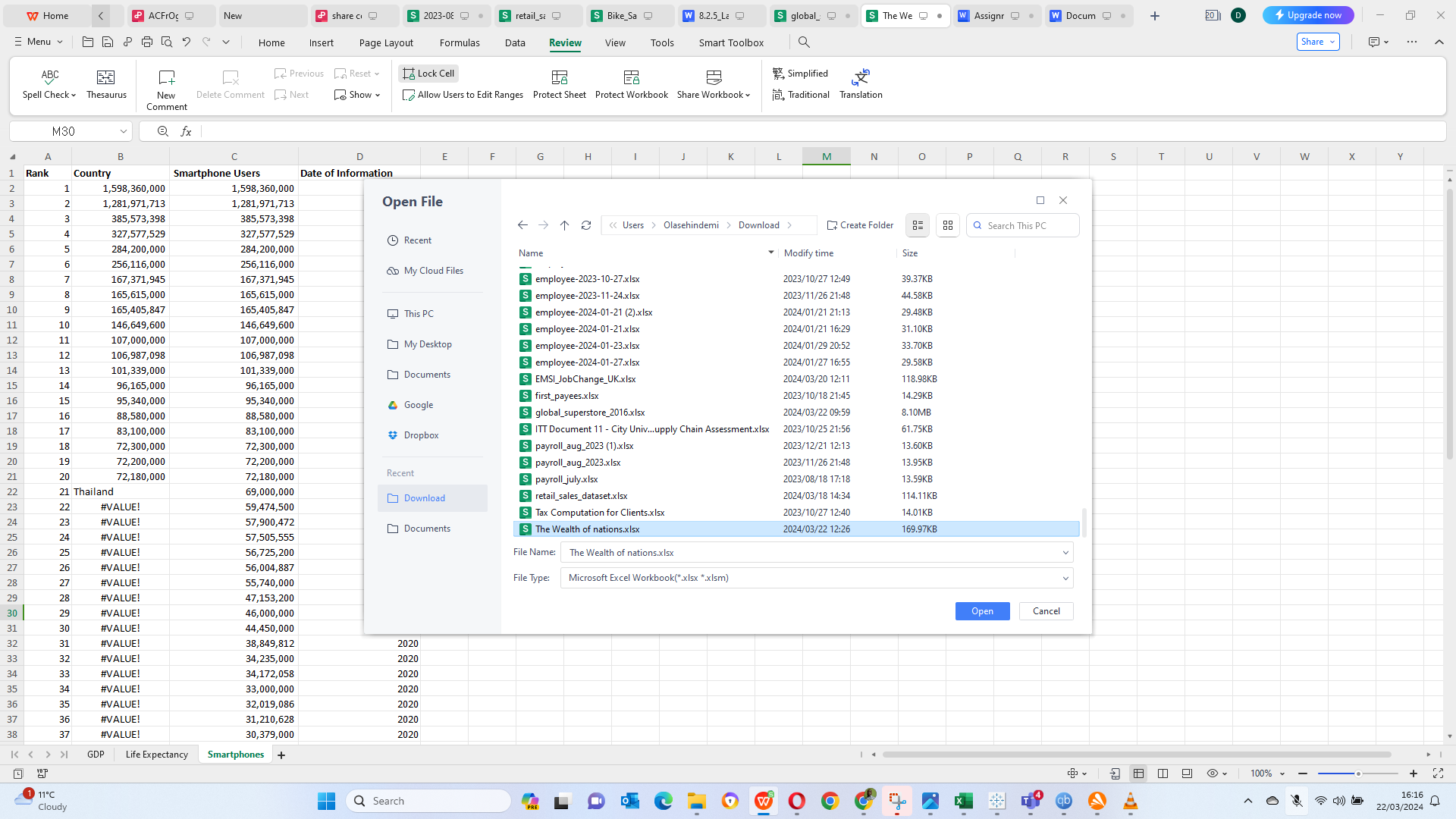
3.0 Tableau ...............................................................……………………………………..…...7

1.0 Policies and Procedures to adhere to while using data

1. PROTECT PASSWORDS: Secure data storage depends on the creation and use of passwords that are needed to gain access to data records. The best storage and encryption technologies can be easily undone by poor password practices. Passwords should be difficult to determine and be protected as carefully as confidential data. They should never be shared or left on slips of paper at work stations or desks. Princeton University’s OIT is an excellent resource for information on [creating and managing passwords](https://informationsecurity.princeton.edu/passwords" \t "https://ria.princeton.edu/human-research-protection/data/_blank).
2. TRAIN AND MONITOR RESEARCH ASSISTANTS: Research assistants who work with confidential data should understand and follow all of the basic data security practices outlined in this section.   This begins with human subject research training which may be completed on line at: [Human Research/training](https://ria.princeton.edu/human-research/training" \t "https://ria.princeton.edu/human-research-protection/data/_blank).  Research assistants and other project staff must be acquainted with procedures and practices described in these guidelines. Principal investigators are directly responsible for training and monitoring project staff, and researchers who work with confidential data. Researchers are encouraged to contact the Office of Research Integrity and Assurance should they have questions about training.
3. RESTRICTED USE SHARED ACCOUNTS OR GROUP LOGIN IDs**:**Anyone who works with confidential electronic data should identify themselves when they log on to the PC or laptop computer that gives them access to the data.   Use of group login IDs violates this principle.   Project managers must make certain that everyone working with confidential data has a unique password that personally identifies them before they can access the data.   For any student or employee working on a Princeton computer, this will be the LDAP login ID and password that person was assigned at matriculation or initial employment. For information on requesting LDAP login IDs and passwords for temporary employees or consultants, click [here](https://princeton.service-now.com/snap/?id=kb_article&sys_id=5b2a27064f9ca20018ddd48e5210c788" \t "https://ria.princeton.edu/human-research-protection/data/_blank).
4. KEEP USER GROUP LISTS UP-TO-DATE:  User groups are a convenient way to grant access to project files stored on a remote server.   The use of user groups simplifies the granting and revoking of access to a research project’s electronic data resources.   By granting access privileges to each of the research project’s electronic folders to the group as a whole, newly authorized members of the project team can obtain access to all related electronic data resources by just being added to the group.   When an individual is no longer a part of the project team, the removal of his or her ID revokes access to all resources. But remember that group members can access resources on any Princeton computer to which the group has access, not just the computers used in your work area. Group membership lists should be reviewed regularly and, when project staff complete their work or leave the project, the user group administrator should update the user group list so that persons no longer working on the project cannot access any shared resources.
5. AVOID USING NON-DESC PCs OR LAPTOPS FOR COLLECTION OR STORAGE OF CONFIDENTIAL RESEARCH DATA:The Desktop Systems Council ([DeSC](http://www.princeton.edu/desc/about-desc/" \t "https://ria.princeton.edu/human-research-protection/data/_blank)) oversees the use and maintenance of computers participating in the managed environments that make up the DeSC Program. The scope of the Council’s activities is to advise the university on standards for the managed computing platforms for institutionally owned computers. Computers outside of the DESC system may lack adequate firewalls, virus protection, and encryption that help protect confidential research data from being stolen.   Computers that are part of the University’s DeSC system maintain up-to-date systems that are designed to keep PCs, laptops and their contents securely protected from theft or unauthorized use.
6. ACTIVATE LOCK OUT FUNCTIONS FOR SCREEN SAVERS: Computers used for data analysis should be configured to "lock out" after 20 minutes of inactivity.   This reduces the risk of theft or unauthorized use of data in situations where a user working with confidential data leaves his or her desk and forgets to logoff the PC. OIT provides instructions on how to configure the automatic lock out feature for Windows PCs.
7. USE SECURE METHODS OF FILE TRANSFER: Transfer of confidential data files between users or between institutions has the potential to result in unintended disclosure. File transfers are often the weakest part of any plan for keeping research data secure. The method used to transfer files should reflect the sensitivity level of the data.   Research files with PII or other confidential information should always be compressed and encrypted before they are transferred from one location to another.   This is especially important when transferring files as attachments to email or as files on physical media such as CDs or flash memory drives.   File compression minimizes the chances of your file transfer failing because your file is too large.   Encryption will ensure that your compressed file cannot be read by anyone who does not have the password that was created when the file was compressed and encrypted. Other secure and convenient methods of file transfer include SharePoint and University-supported Google Drive

2.0 Excel

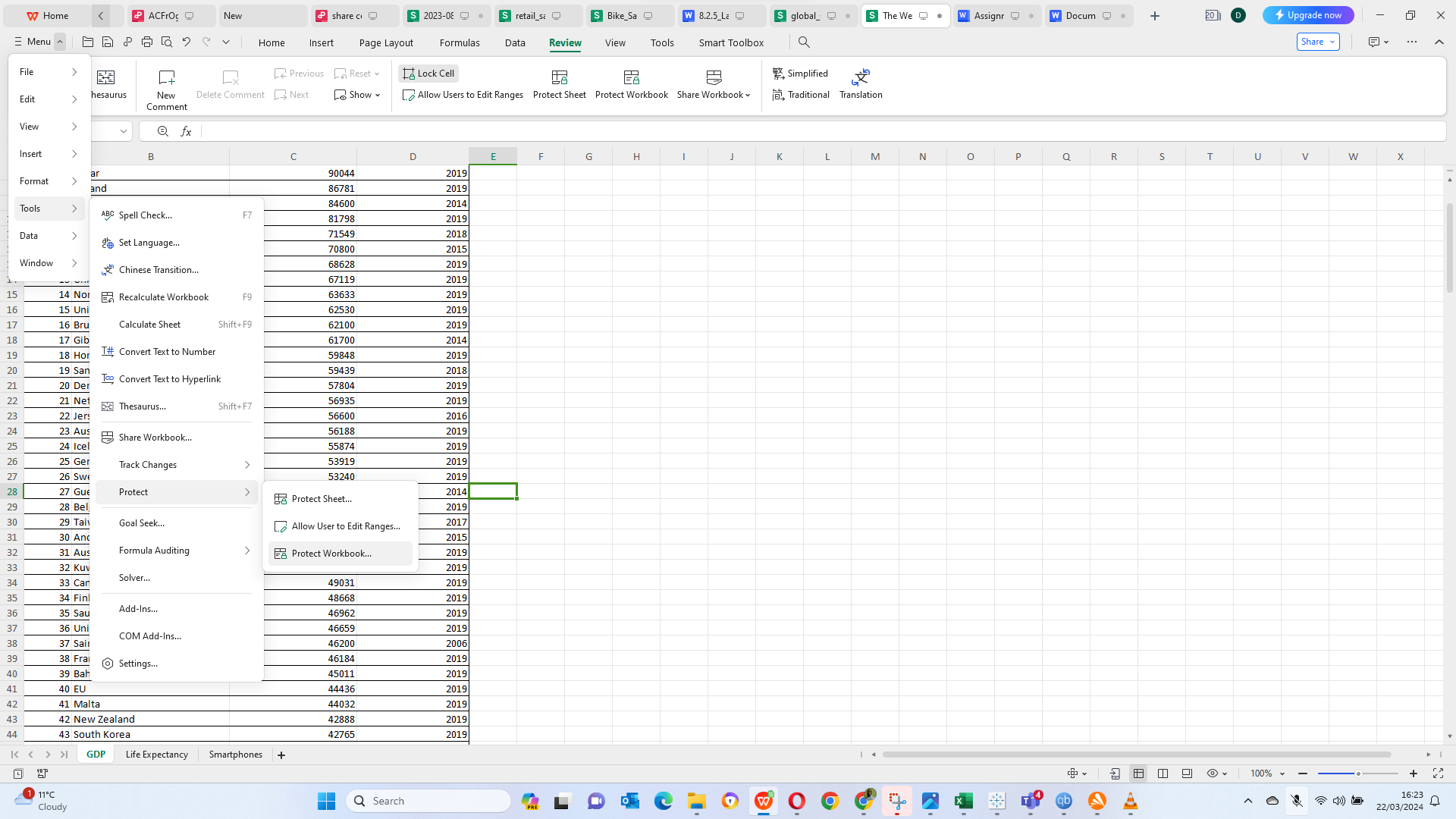
Opening Data on Excel



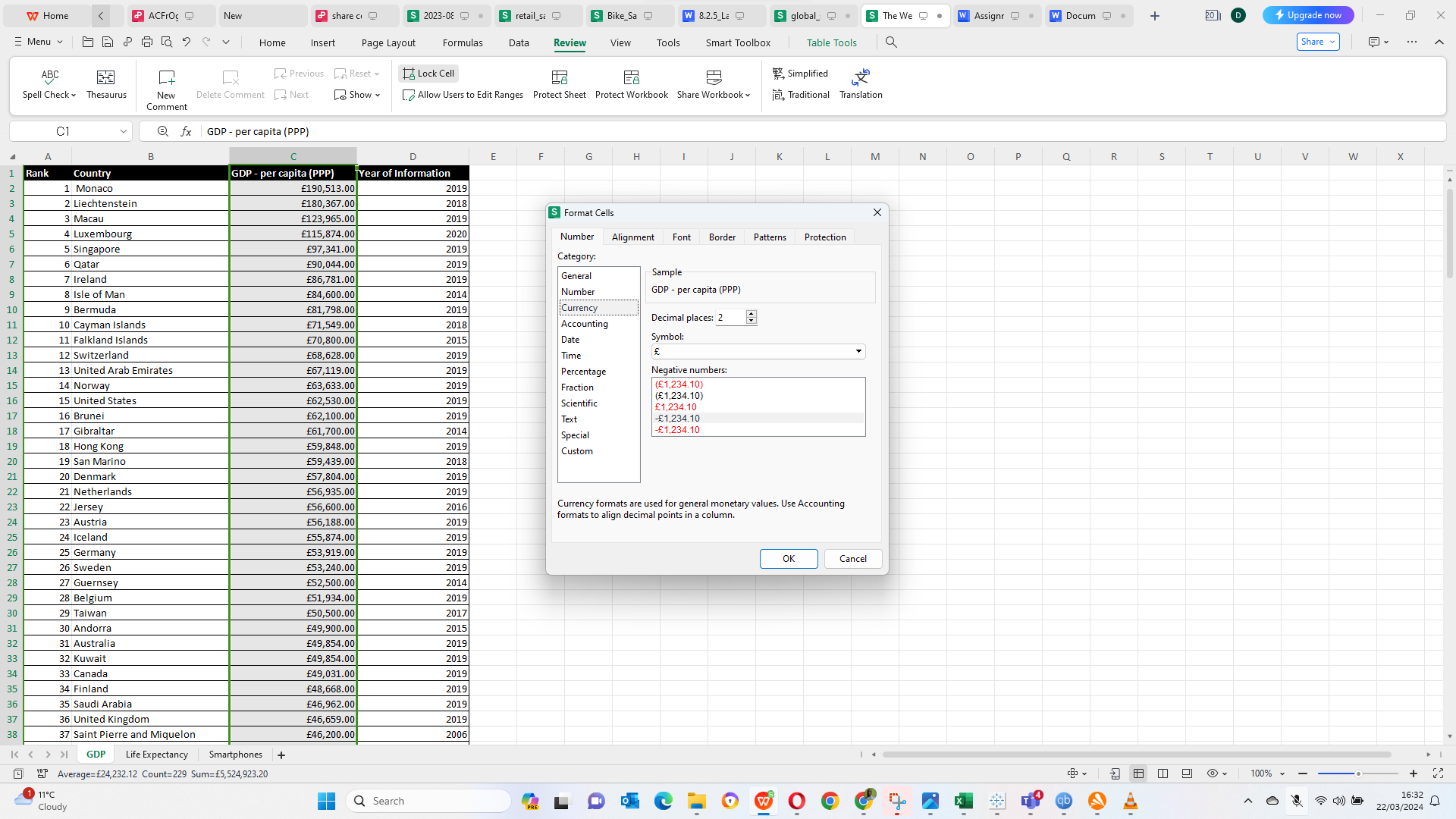
Open the excel table by clicking on file -open - select The wealth of Nation and click on Open

GDP TASK

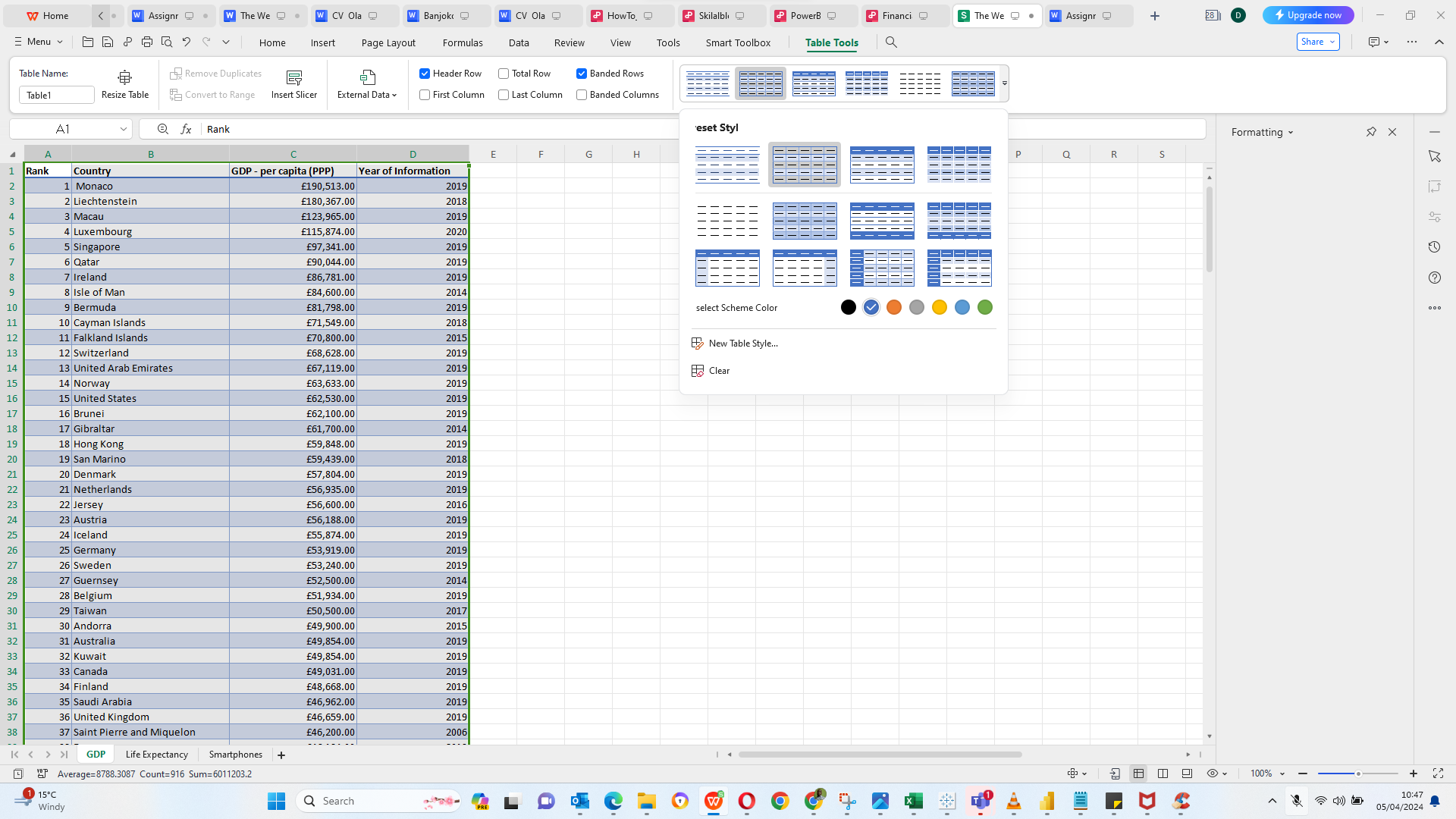
1. Set a password to protect the workbook



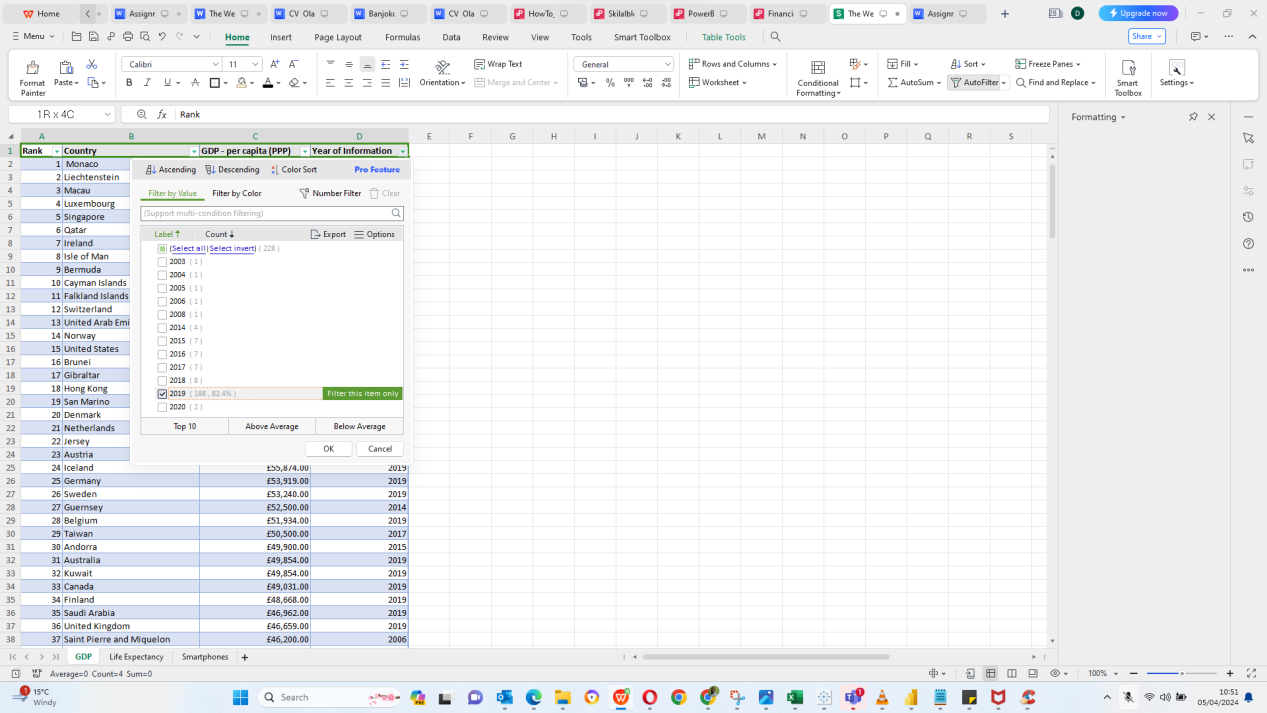
1. Highlight column C and change the data to display in British Pound symbol



1. Turn the GDP sheet into a table.

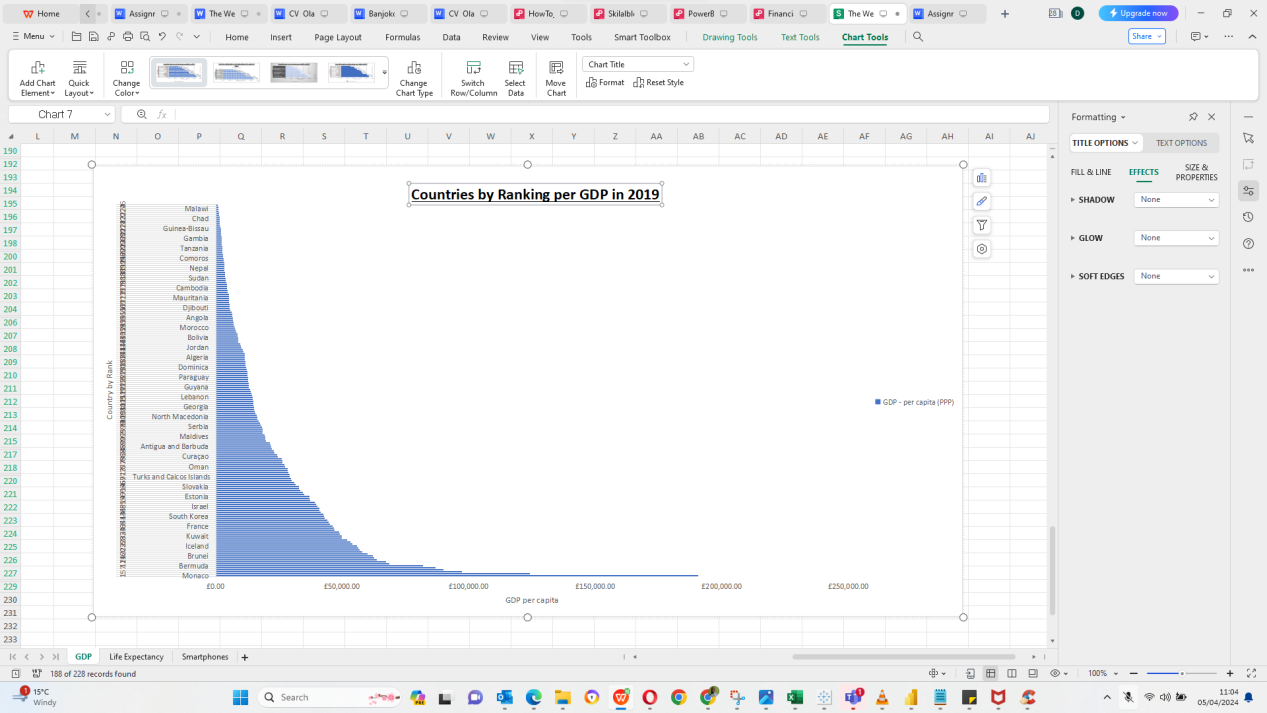


1. Filter the table to display only the information for 2019

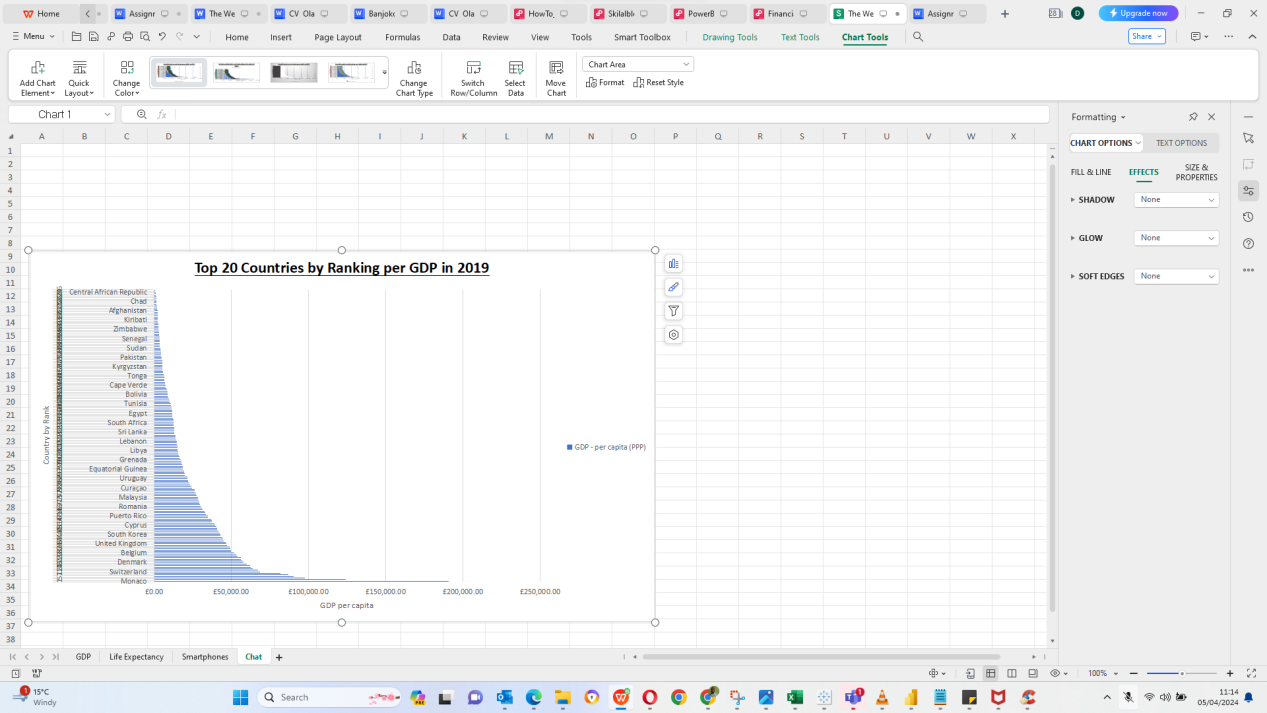


5. Create a chart that will only display the following data ‘Rank, Country and GDP - per capita (PPP). The chart can be anything as long as it is suitable.

6. Using your creative skills edit the chart a. Add a title

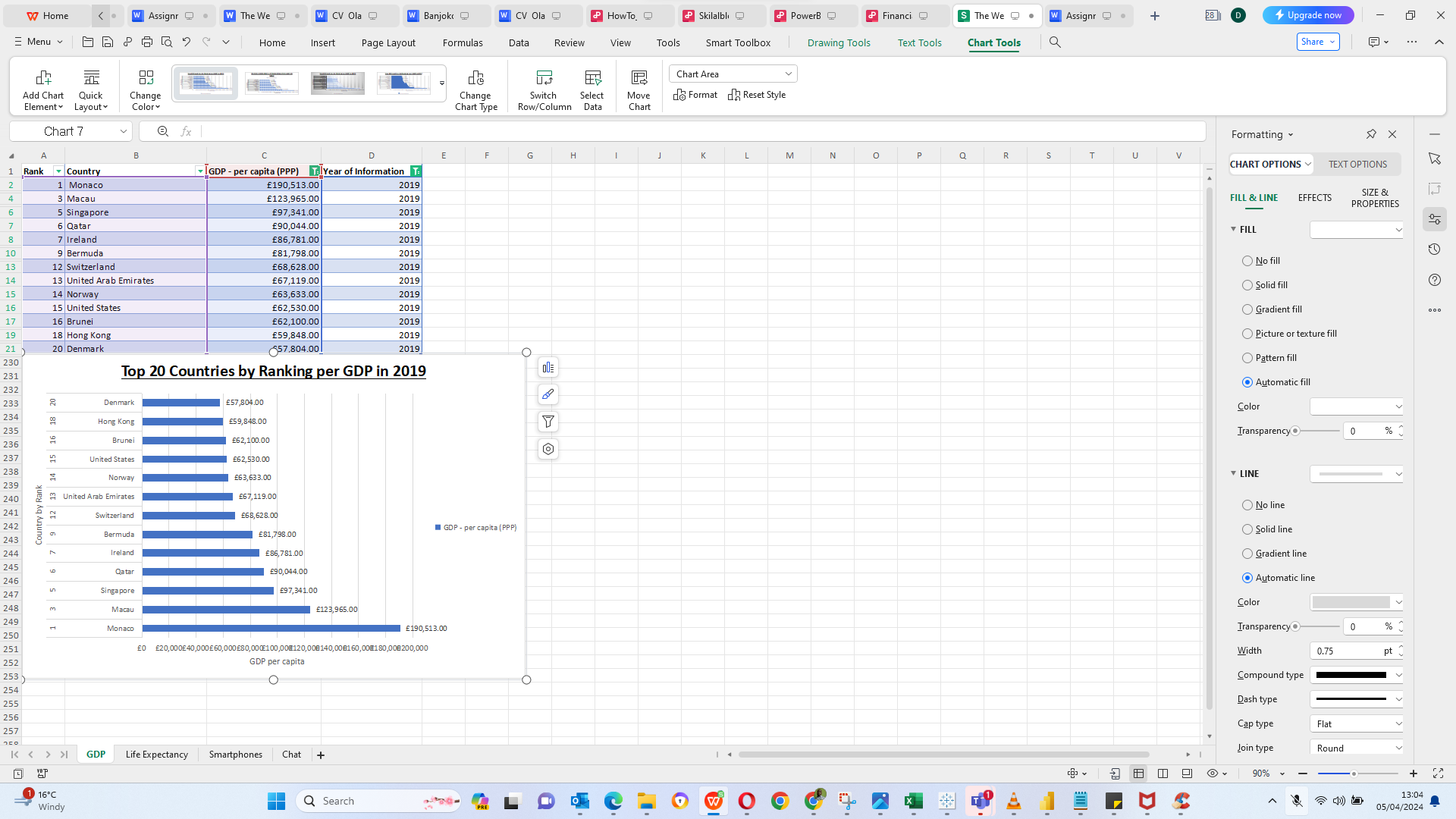


7. Move the chart to a new sheet tab and label with a suitable name

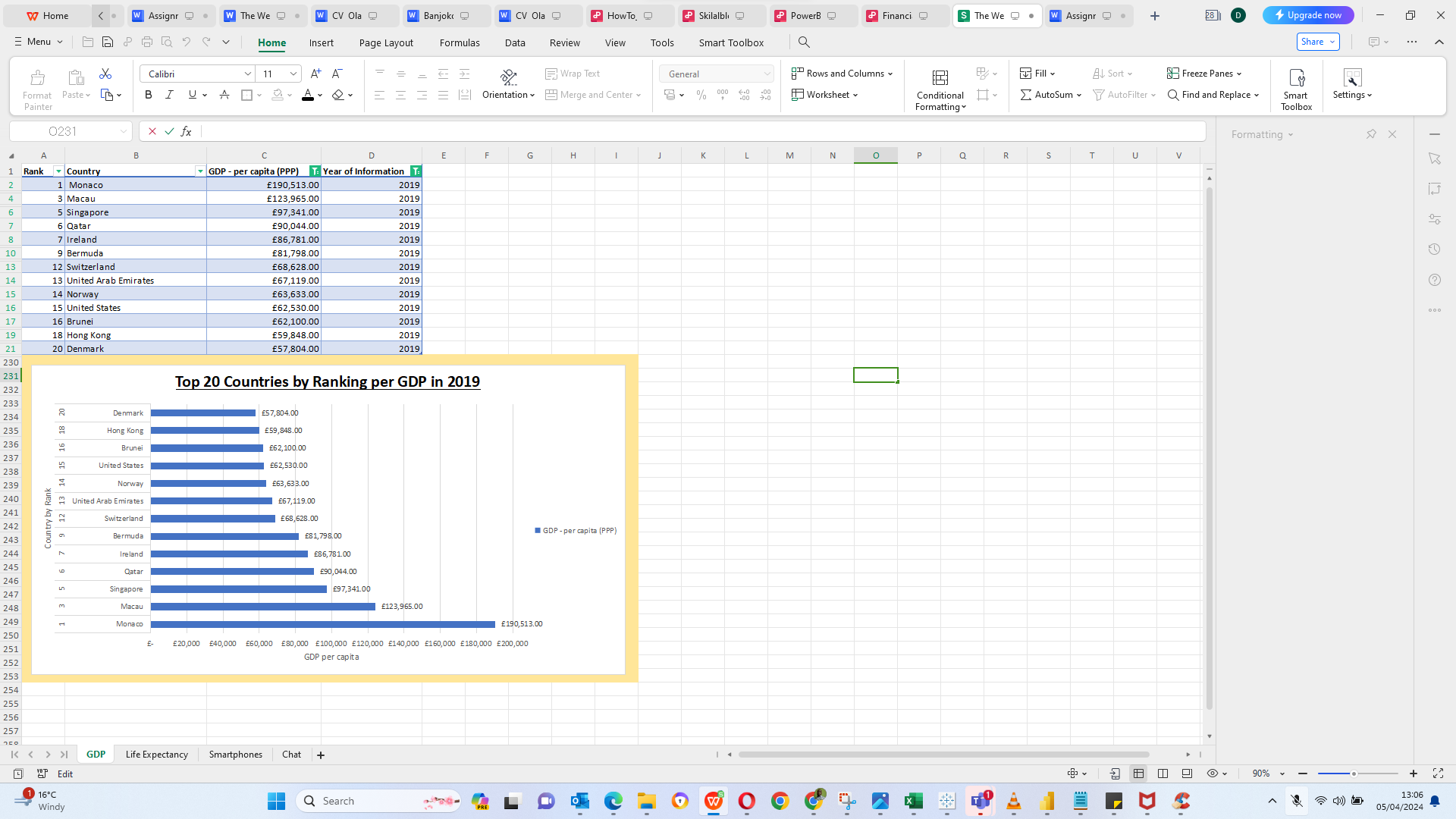


8. Create a sort for the top 20 highest ranking counties

9. Next create a new Bar chart to display the 20 highest ranking countries

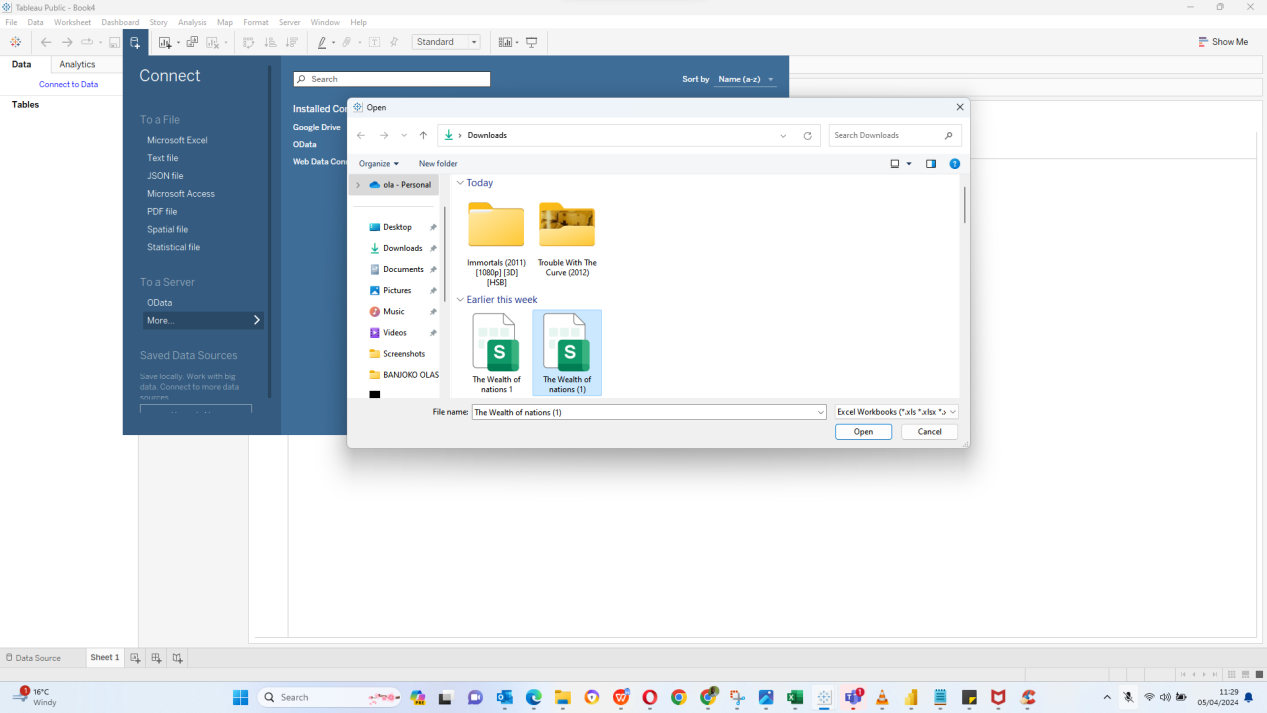


1. Colour the background by highlighting the area underneath the table. Find the add a fill colour icon and select a colour.

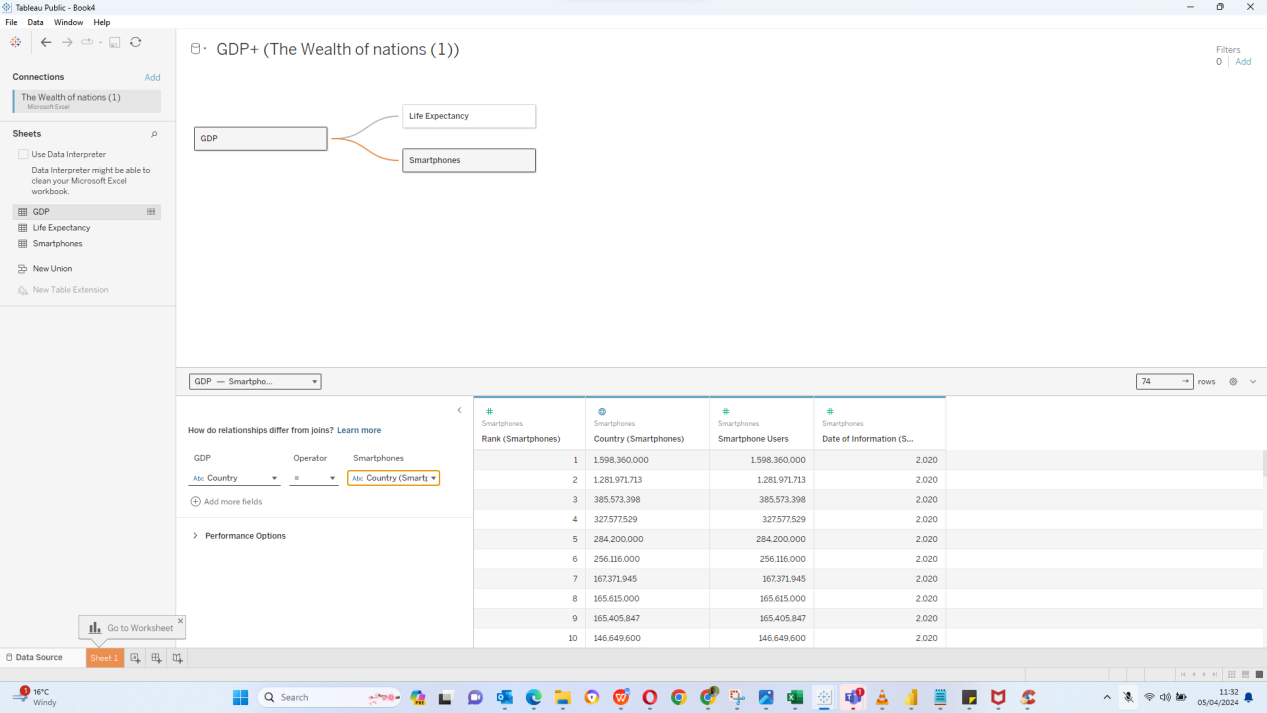


3.0 Tableau

Importing Data

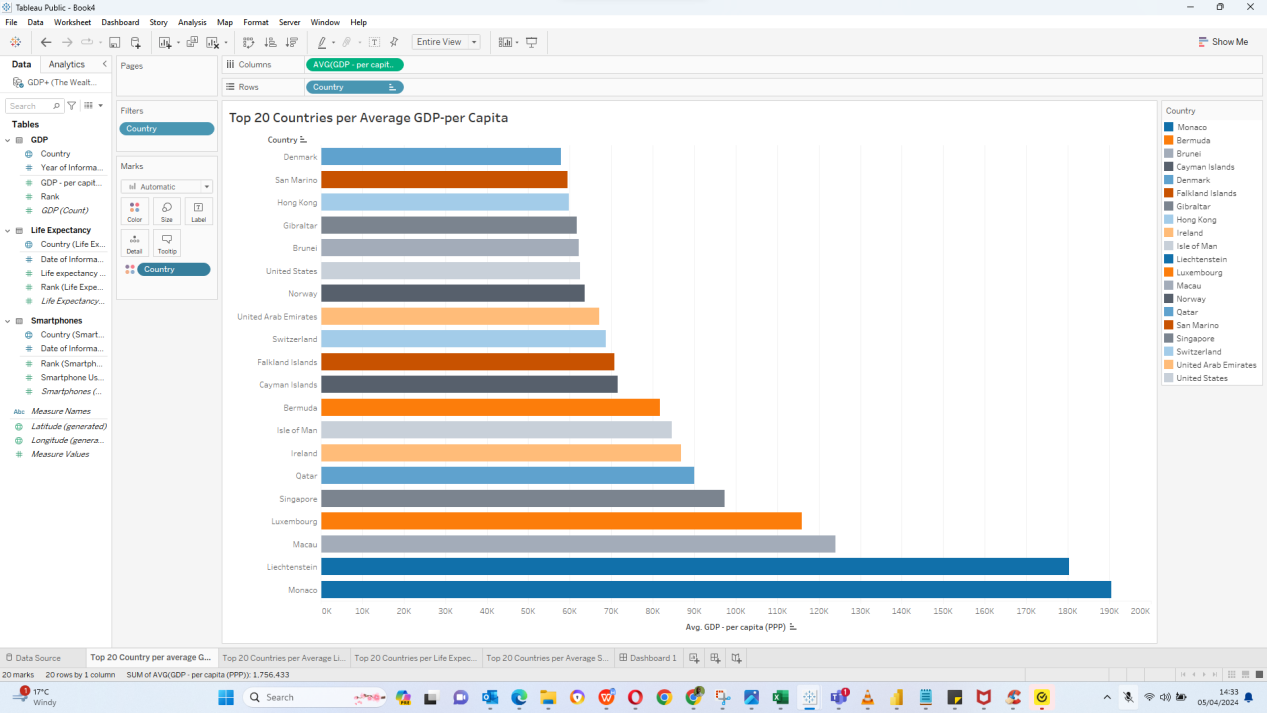


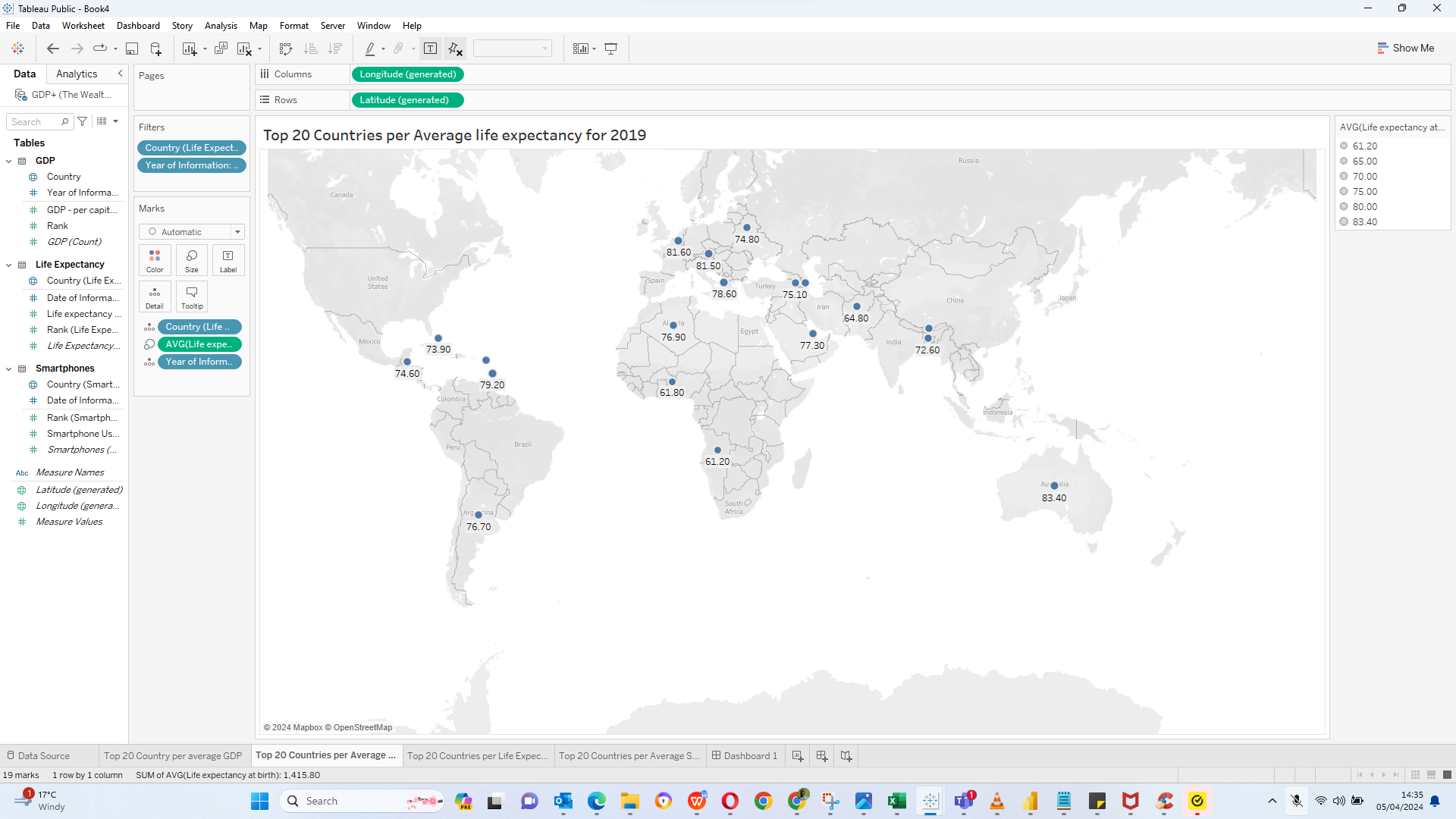
Setting Relationship

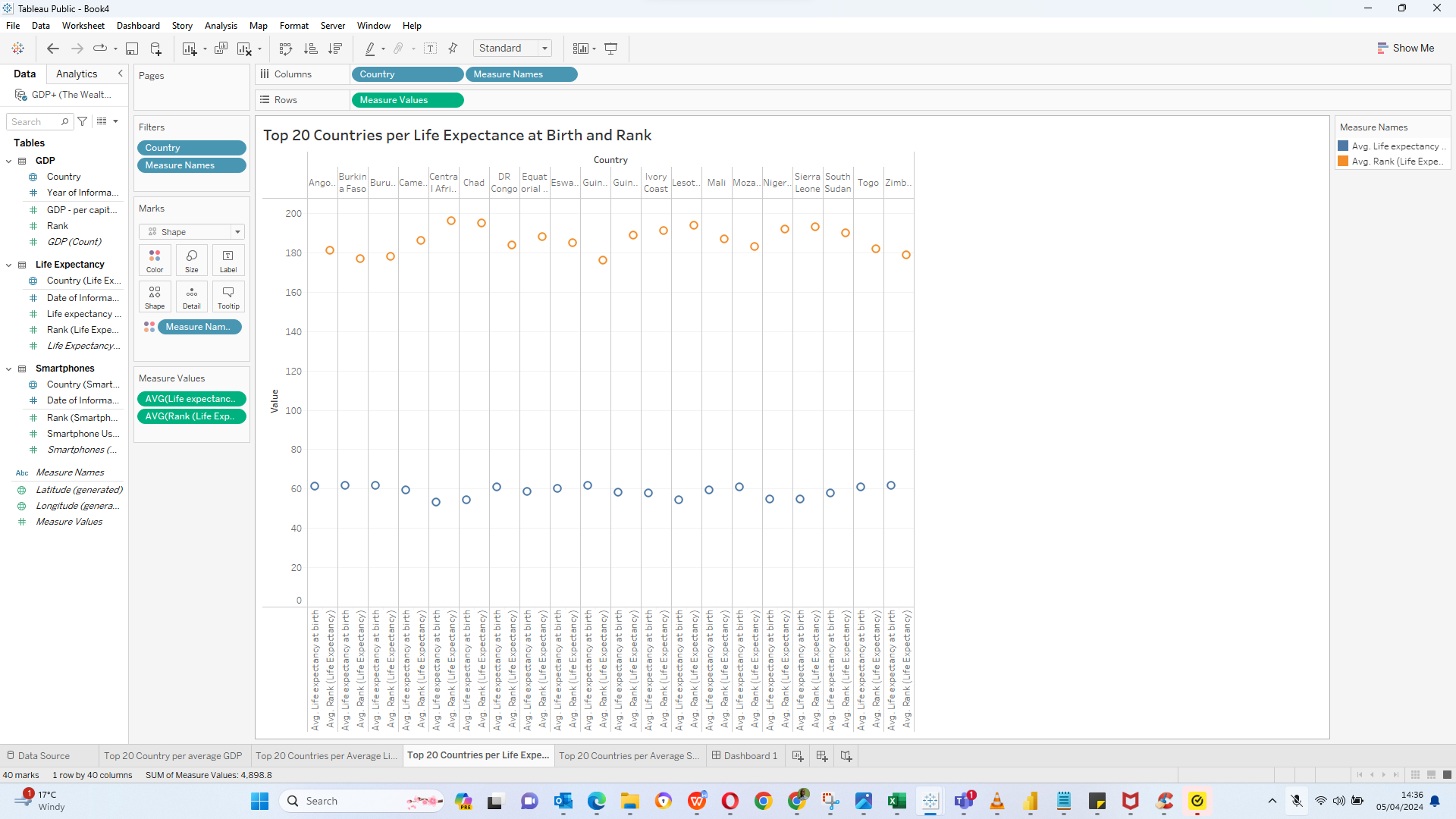


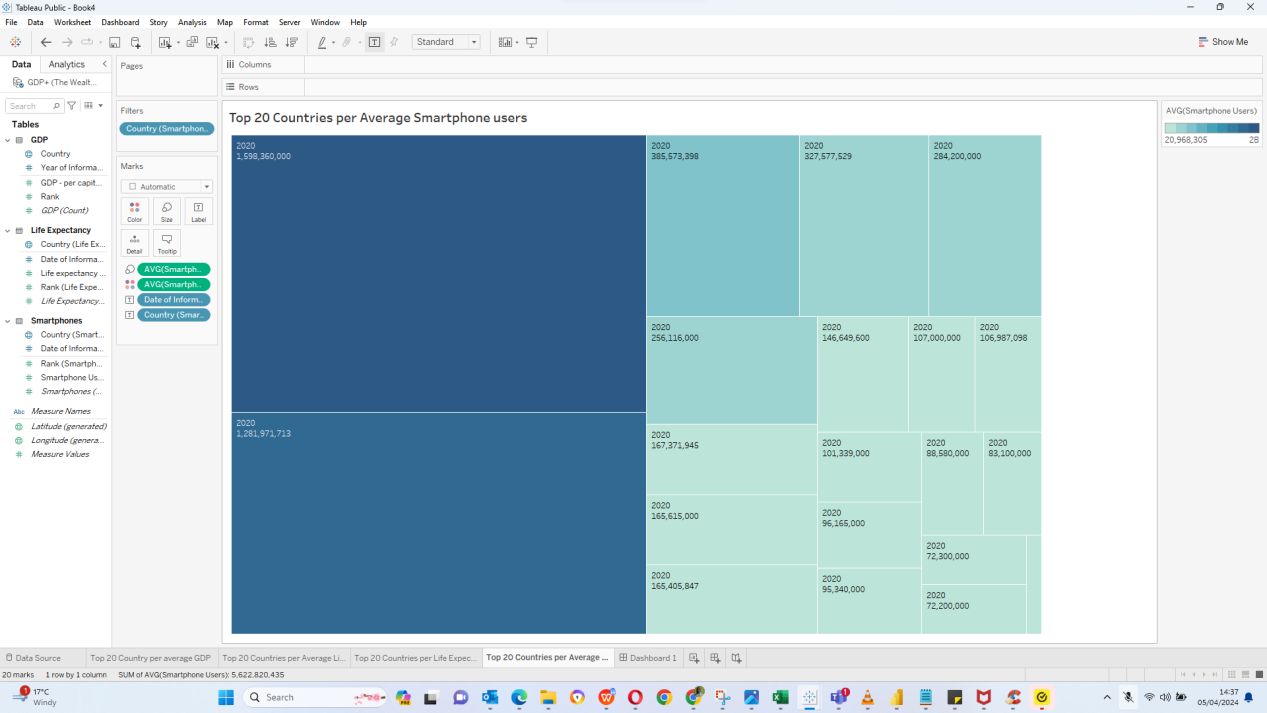
1. Checking Data Types

4) Build charts



[](https://publi)





Use the link below for Answers to Question 5 and 6

https://public.tableau.com/views/Book4\_17123246103410/Dashboard1?:language=en-US&publish=yes&:sid=&:display\_count=n&:origin=viz\_share\_link