Webinar: Password managers

Exercises

INDEX

FIGURE INDEX

1. PRACTICAL EXERCISES

1.1. Export passwords

In this exercise we are going to save in a file all the stored passwords in order to be able to import them in the future or to have an intermediate structured file that we can use in our favourite programming languages.

1.1.1. Export from BitWarden.

We start the application by entering our master password.
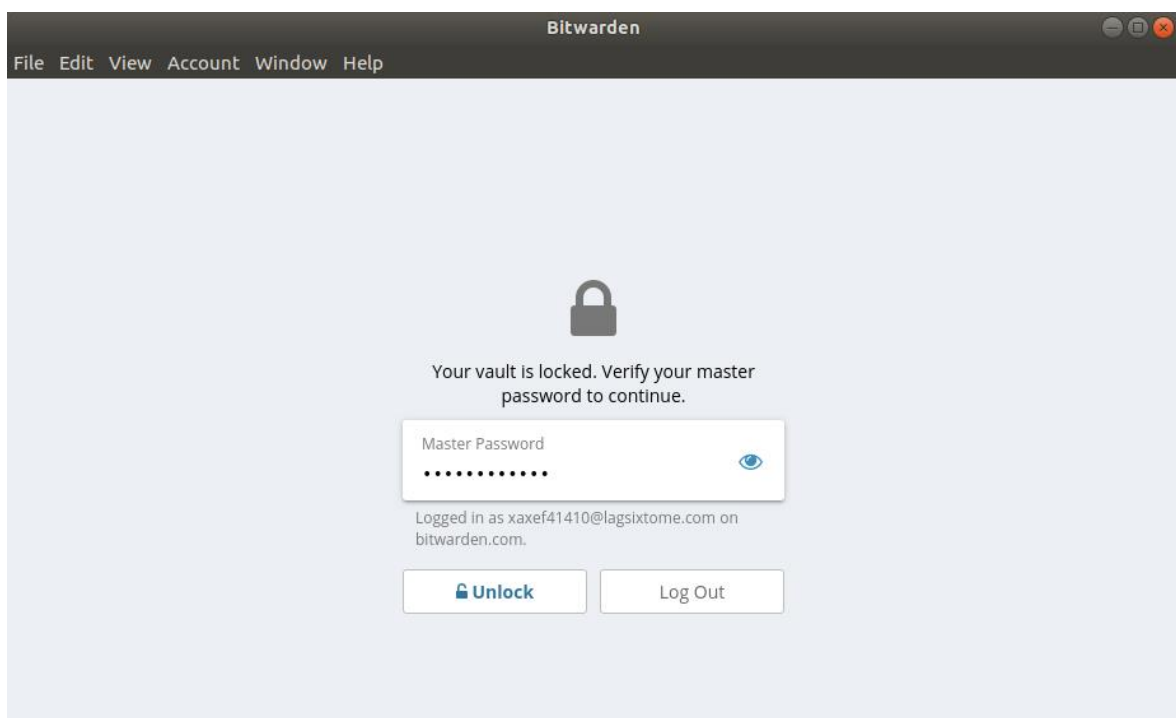
Figure 1 - Start screen with the master password

Once we are authenticated, we click on "File" and "Export Vault".
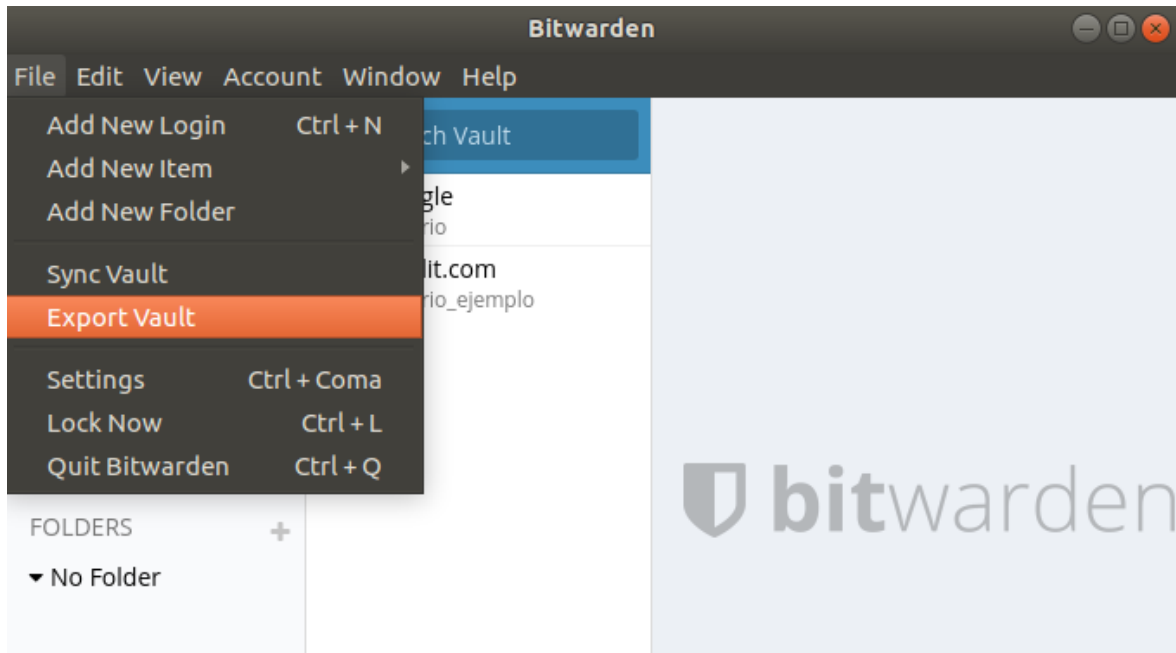
Figure 2 - Export vault

You will again be asked for our master password and a data format for export: "json" or "csv". We proceed to click on the button in the red box.
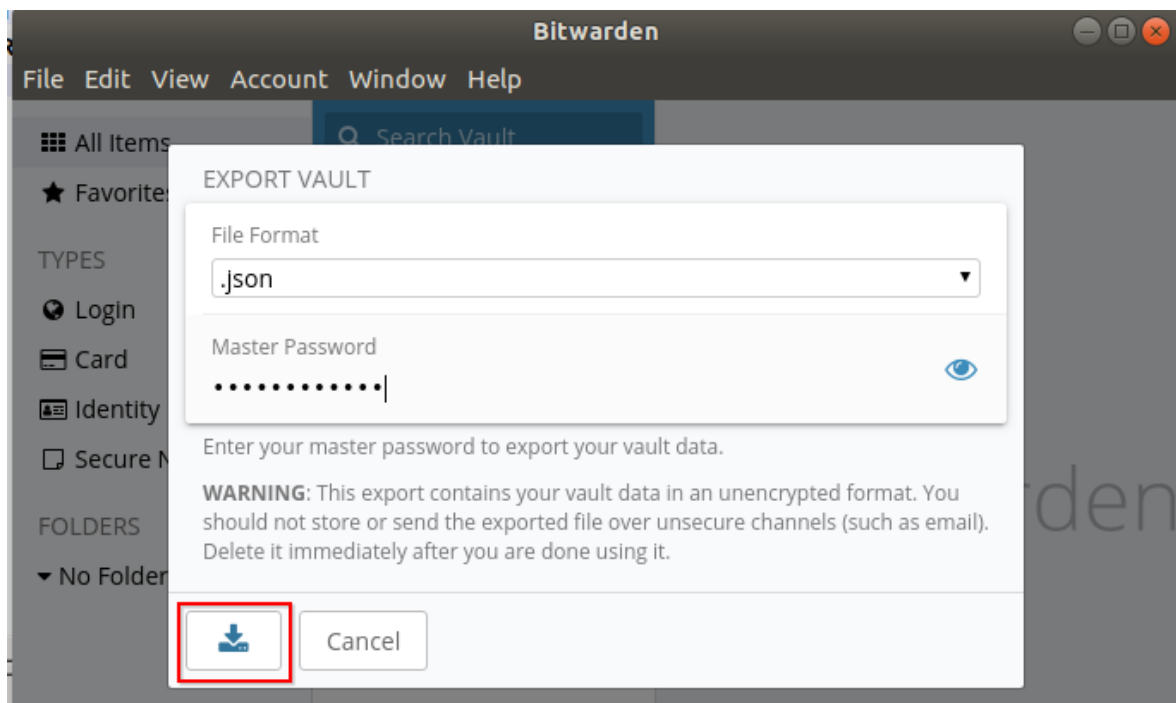
Figure 3 - Export Vault, download

Finally, it will ask us for a file name so that it can be saved to disk. We will have successfully exported the entire safe.

Figure 4 - Export filename

1.1.2. Export from KeePass.

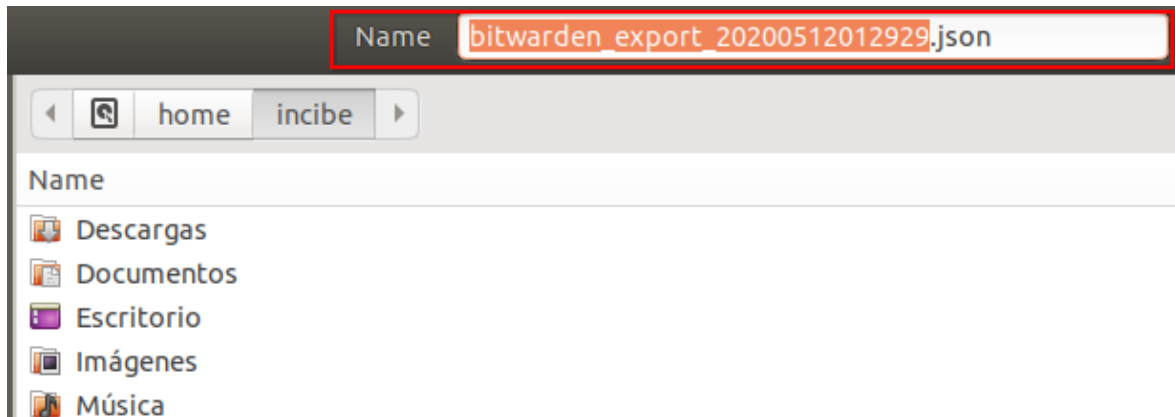We open the KeePass application with our master password and click on "File" and "Export".

Figure 5 - Exporting with KeePass
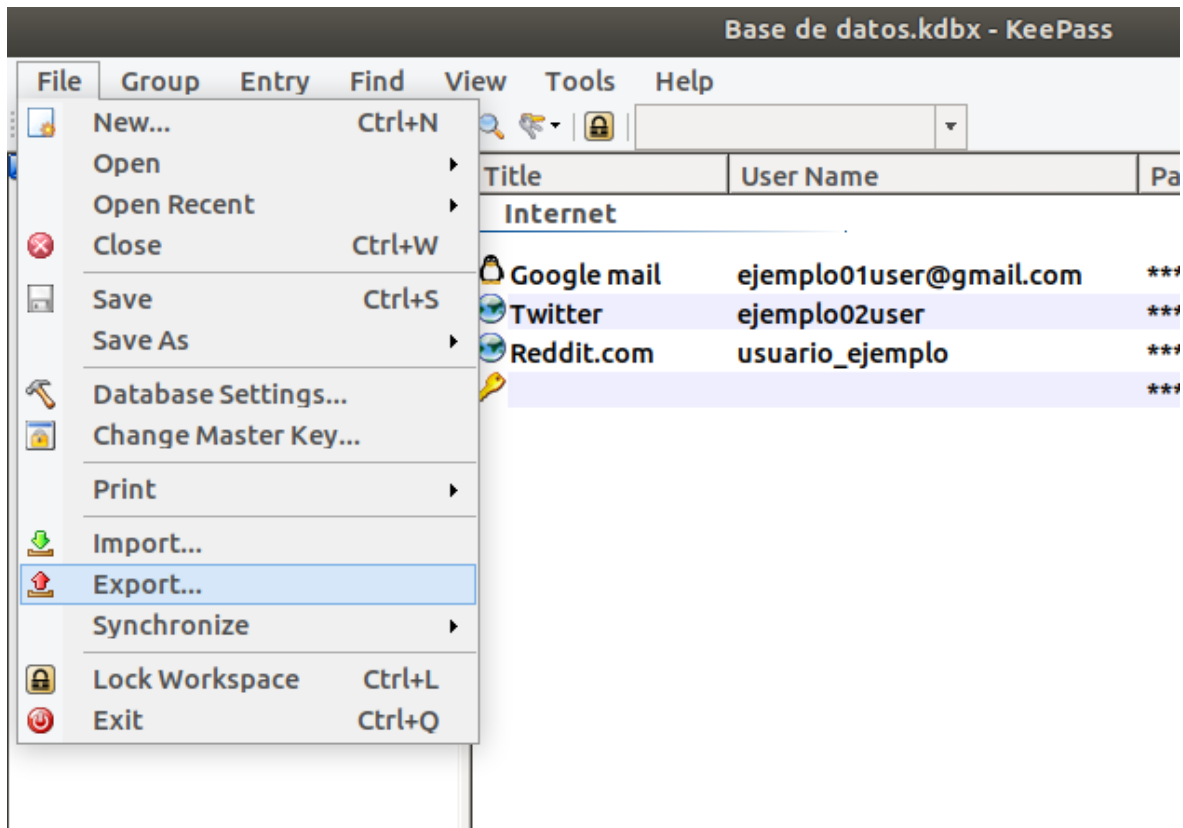
By clicking on "Export" we'll see the export file options available.
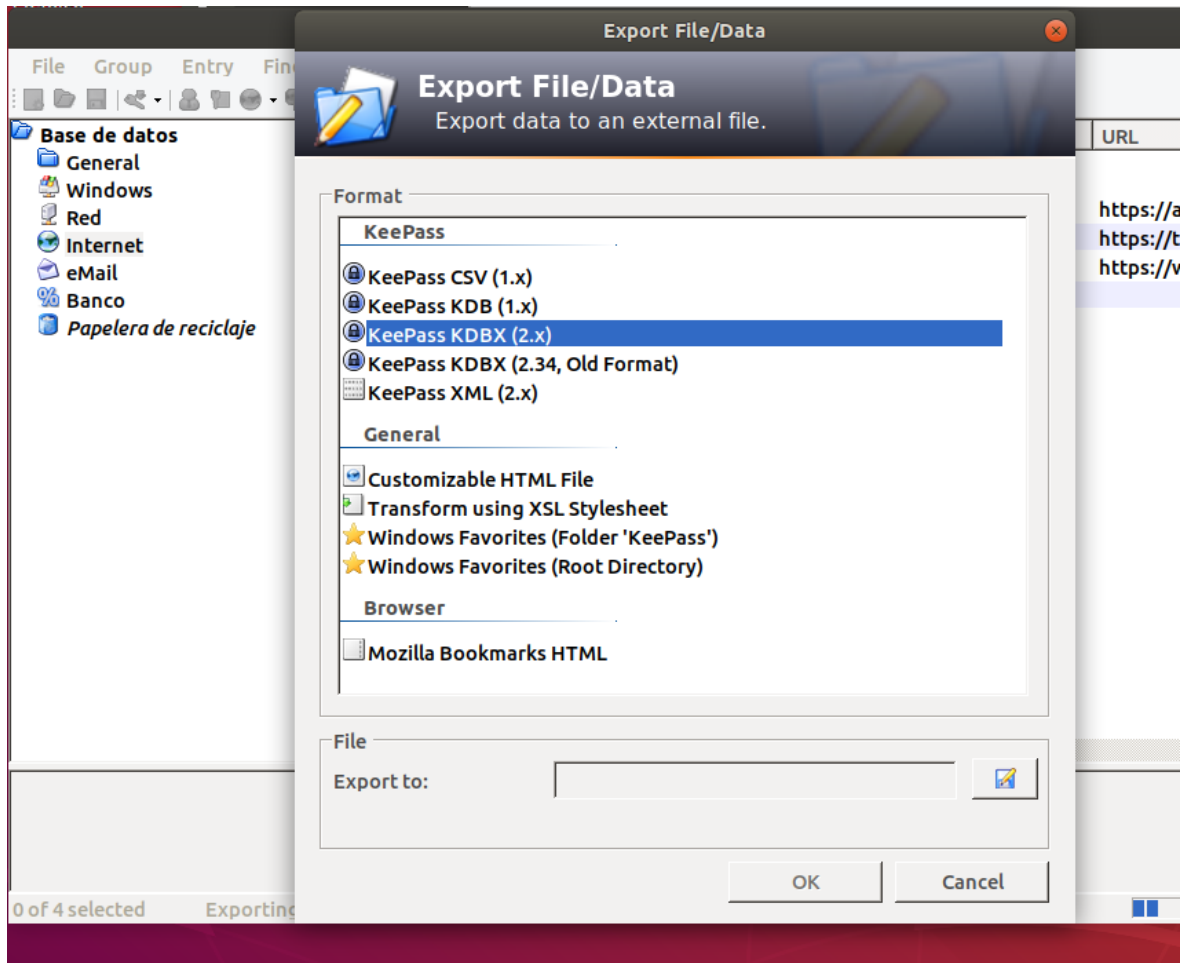
Figure 6 - Options for selecting export files

If we want to exchange with another entity or person, we will provide them with the latest version of the new KBDX format, in this case KeePass KDBX 2.x. Afterwards, we will select where we want to save the file and we will have it available in that location.
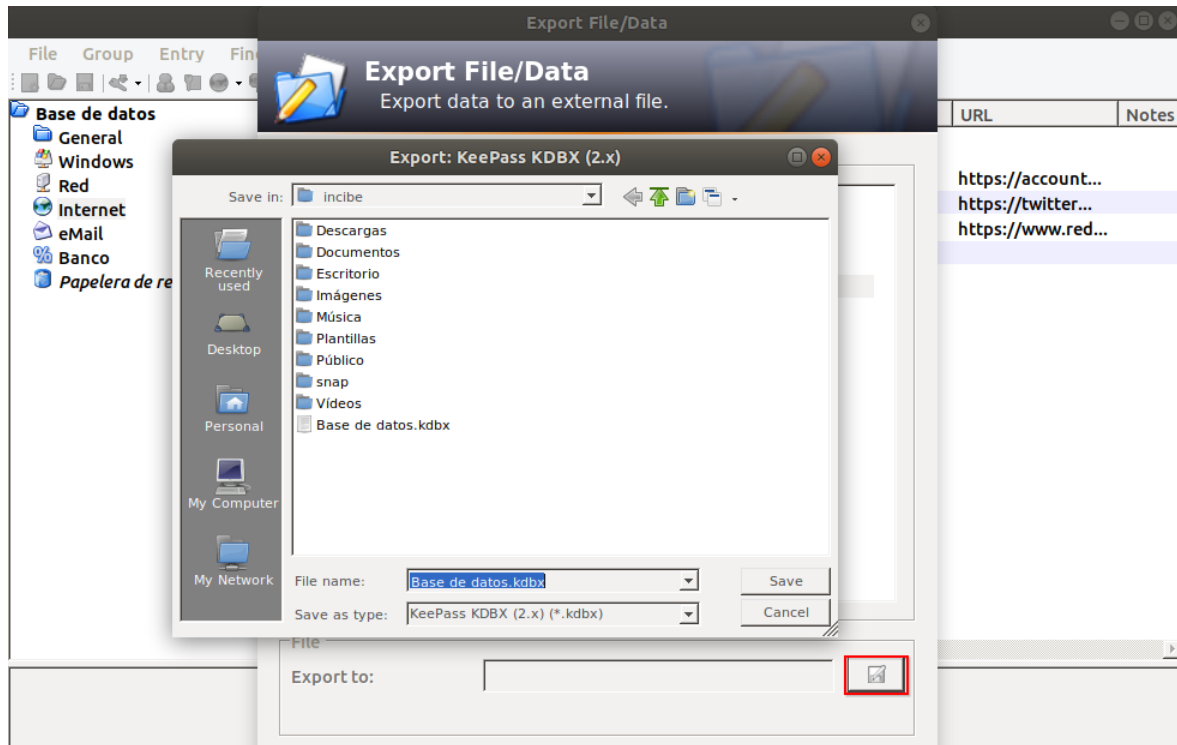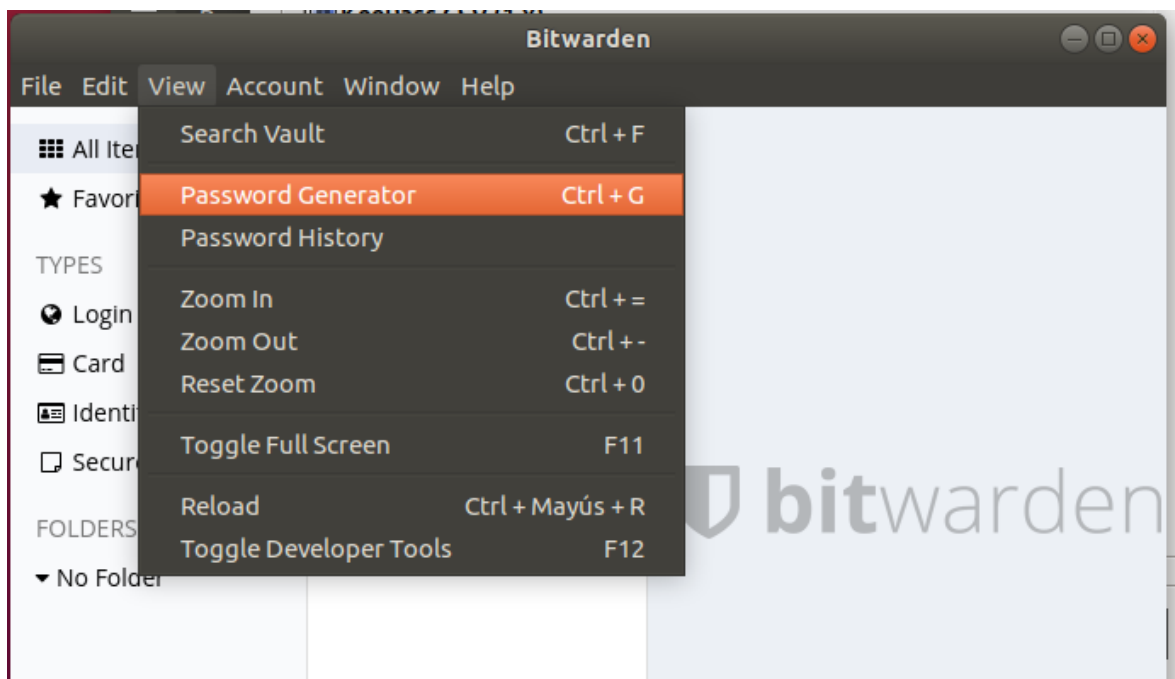
Figure 7 - Location of the export file

2. RESEARCH INVESTIGATION

2.1. Using the Password Generator

In this exercise we will see how we can make use of the password generator for both BitWarden and KeePass.

2.1.1. Password generator in BitWarden

We open BitWarden, authenticate ourselves with the master password and access the "View" and "Password" menu.

Figure 8 - Password generator in BitWarden

In BitWarden we have two options: "Password" and "Passphrase". The difference between the two is the readability provided by the second option, since it will build a readable sentence in blocks of columns that we define. The generator allows us to generate passwords between a set of length defined by us between special characters, upper or lower case, numbers, etc....
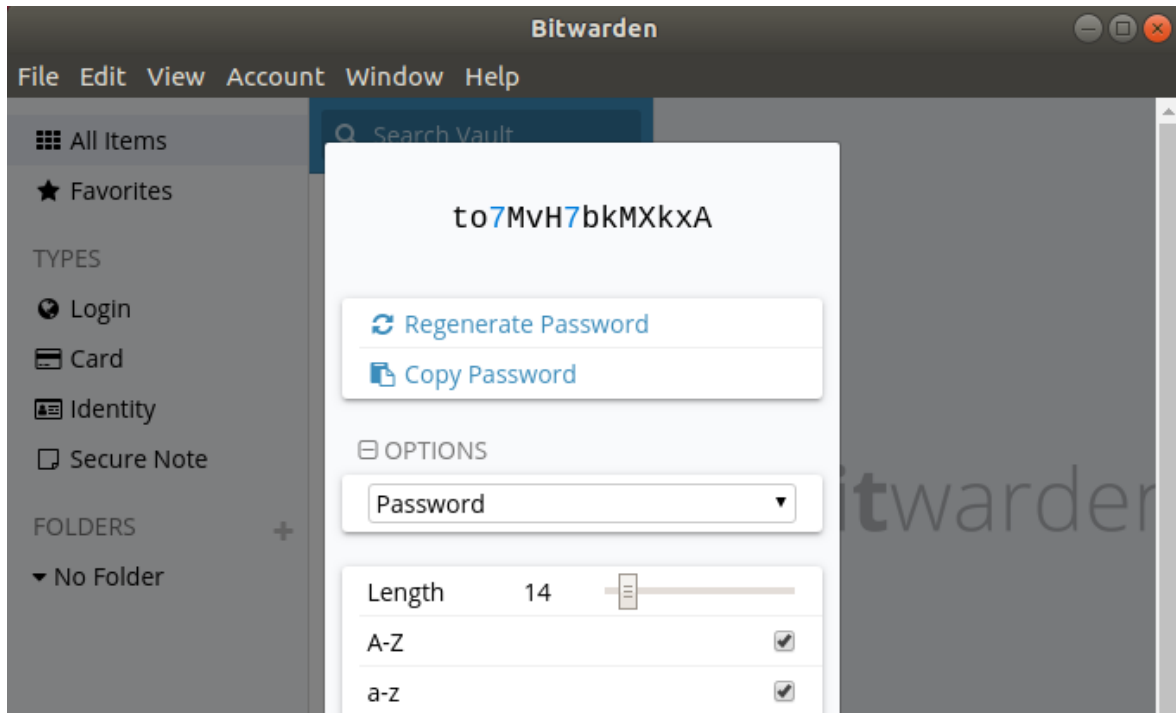
Figure 9 - Classical password generation with options

In the second option, "passphrase" we see that it constructs three words separated by a hyphen so that we can easily remember it. In any case, in both options, we have the possibility to save the password in the clipboard with "Copy password".
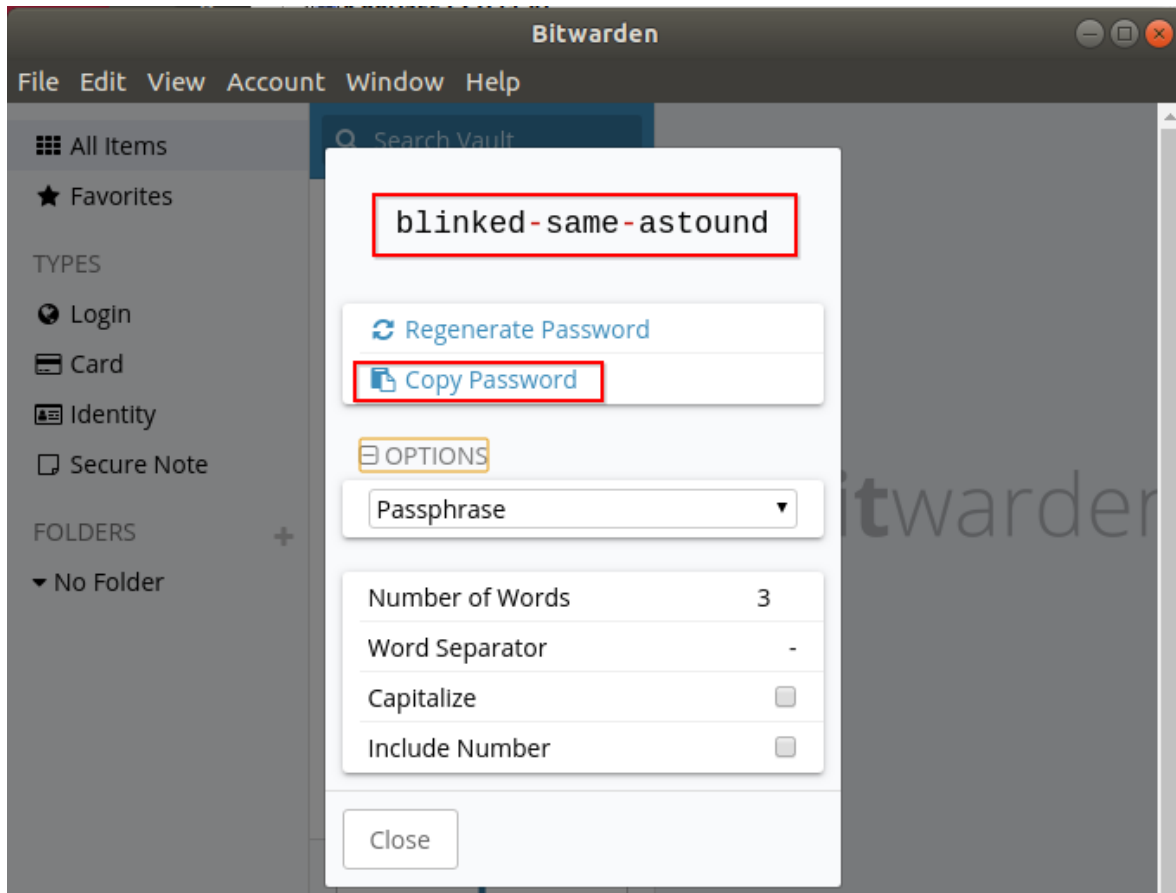
Figure 10 - Passwordphrase

Question (BitWarden): How would you generate a 5-column "passphrase" key?

2.1.2. KeePass Password Generator

Once authenticated with the master password, we proceed to click on "Tools" and "Generate password".
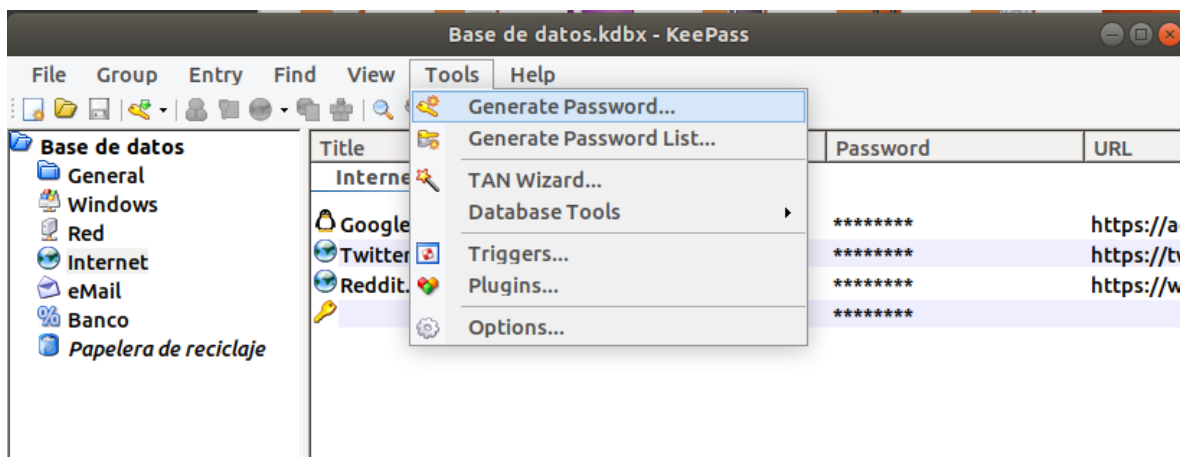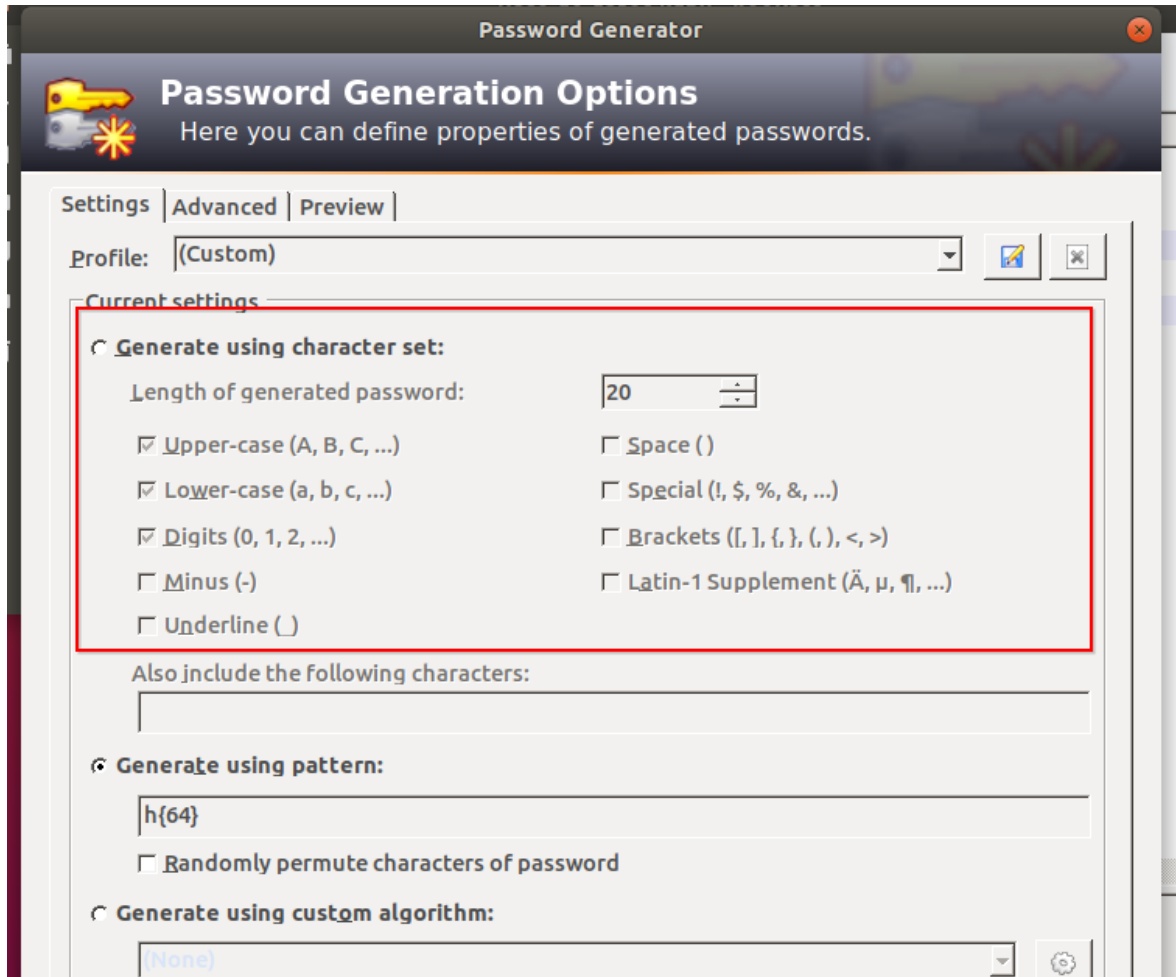

Figure 11 - Password generation option in KeePass

In this case, the options and preferences are much broader than in BitWarden and include the function to generate a certain number of passwords, in case we might need them. For example, for the "custom" profile we have the following options.

Figure 12 - Password generation options

Question (KeePass): How would you generate a 256-bit Hex key?

3. SOLUTION

Question: How would you generate a five (5) column "passphrase" type key?

In this case we would go to "View", "Password Generator" (CTRL+G) select "Word Numbers" and set it to four. Later we can set the separate one or leave it as a dash.
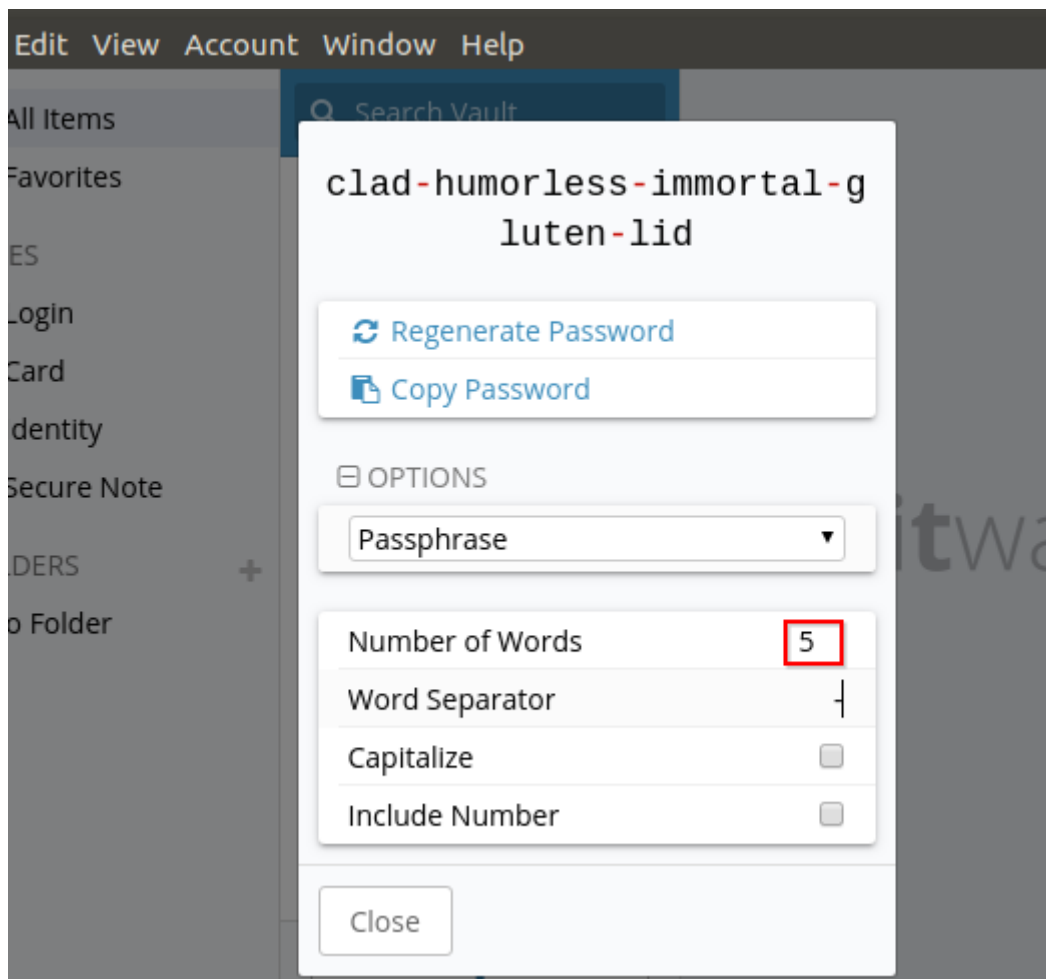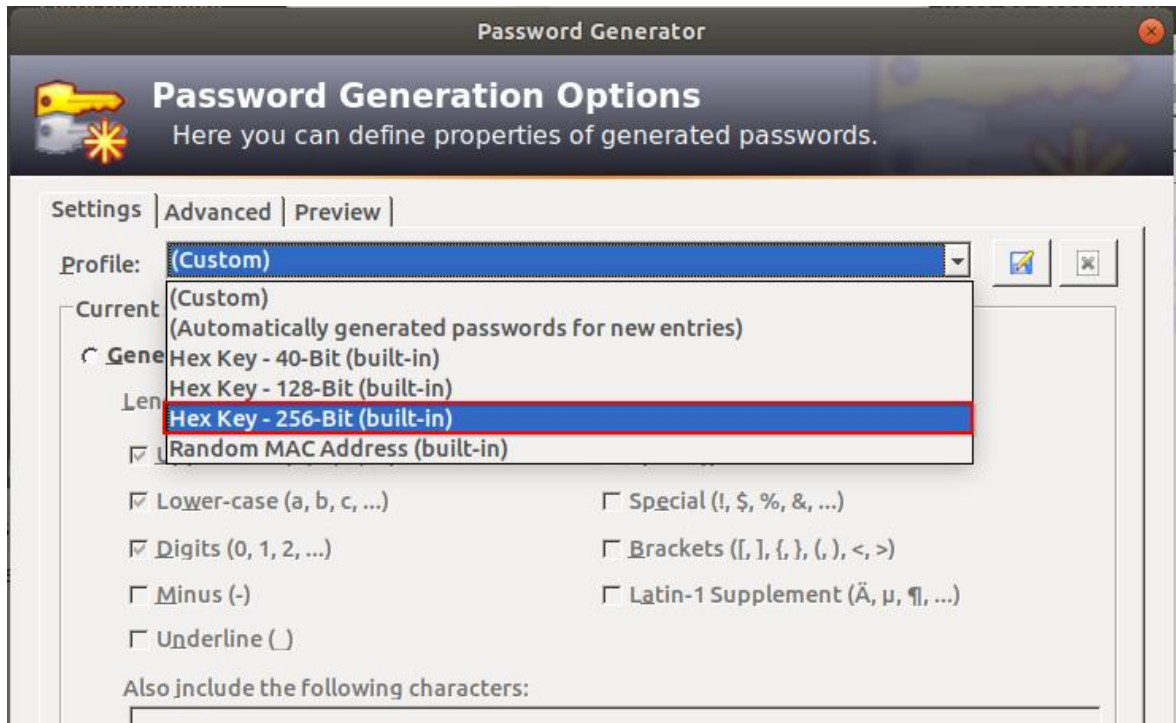

Figure 13 - Generation of 5-column passphrase

Question (KeePass): How would you generate a 256-bit Hex key?

In this case we would change the custom profile to a "256-Bit Hex Key (Integrated)" profile as shown in the image below.

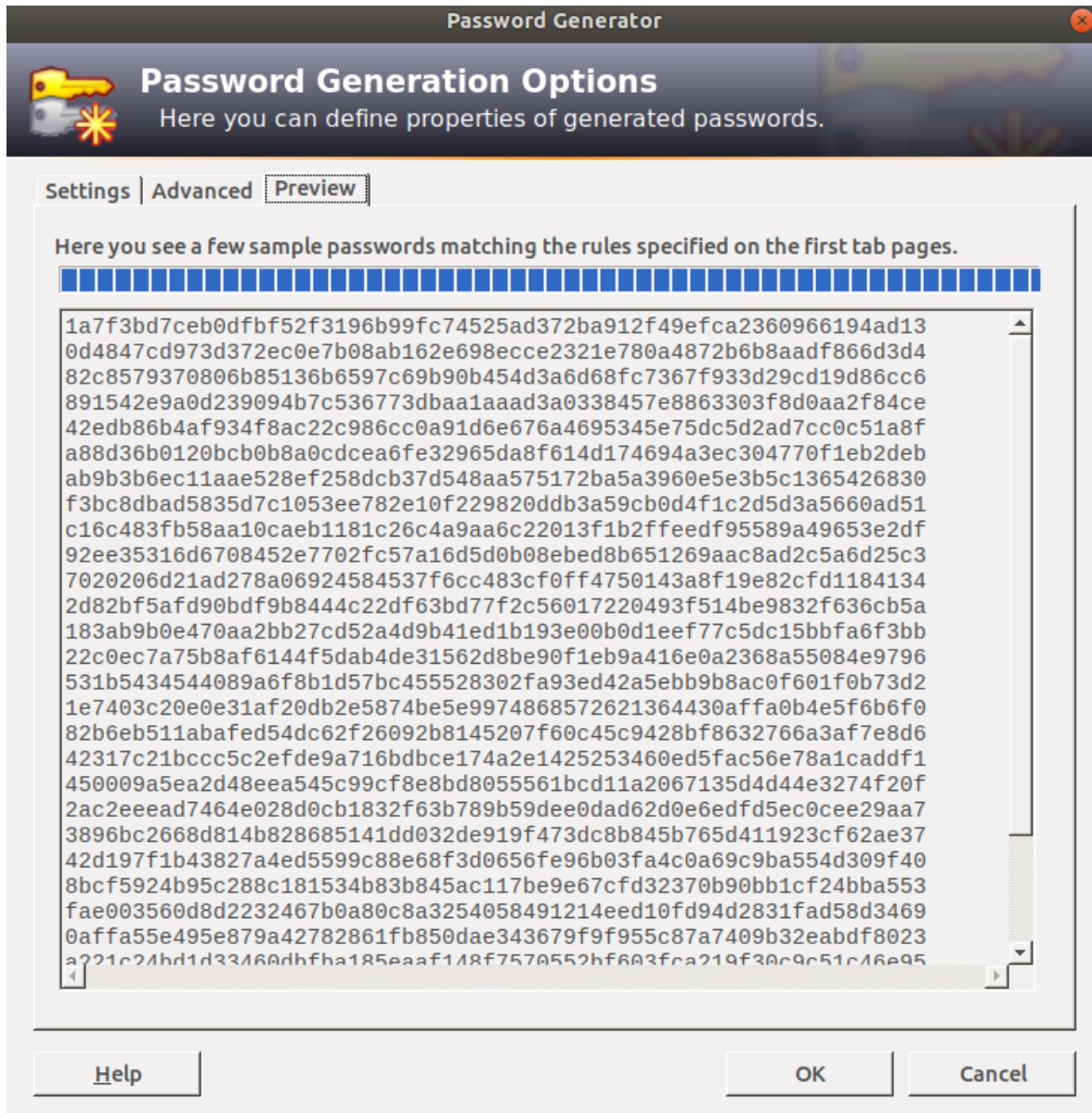*Figure 14 - 256-Bit Hex generation*

To see the result, let's go to the "Preview" tab.

Figure 15 - Password generation preview