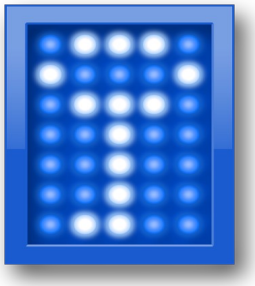
UBC Department of Psychology IT

Securing your data using TrueCrypt

A quick start guide (for OSX)



What is TrueCrypt and why use it?

TrueCrypt is Free and Open Source Software that enables you to encrypt (and therefore secure) your data in a variety of ways. There are 2 main methods of encrypting your data:

- Encrypted file container. Think of this as a "virtual" hard drive on your system that can only be accessed (or even seen) by using TrueCrypt and entering a secure password. You would ideally save, move and store files/folders which contain sensitive data to this secure space. This is the method of encryption that we recommend and will go over in this guide.

- Full-disk encryption. This is ideal in a situation where even the software running on your computer is considered sensitive. For example, if you are on a clinical computer which has an application running which would allow a user to access a health authority database. You would want to encrypt the entire system in this case. This is not ideal for most situations as it will slow down your system significantly.

How to Create and Use a TrueCrypt Container

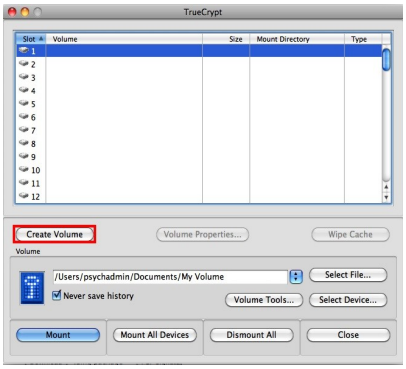
We will go over step-by-step instructions on how to create and access a TrueCrypt volume (file container).

Step 1:

If you have not done so, download and install TrueCrypt: <http://www.truecrypt.org/downloads>. The installer should run automatically but if it does not open and run the installer.

Step 2:

Open TrueCrypt, now found in your Applications folder. The main TrueCrypt window should appear. Click Create Volume.



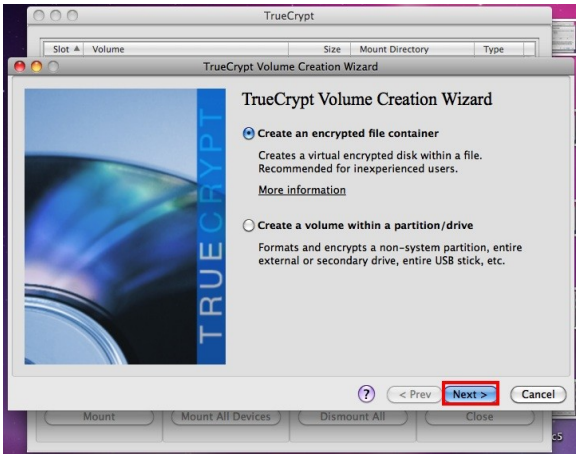
Step 3:

The TrueCrypt Volume Creation Wizard window should appear.

In this step you need to choose where you would like the TrueCrypt volume to be created. A TrueCrypt volume can reside in a file, which is also called container, in a partition or drive. In this tutorial, we will choose the first option and create a TrueCrypt volume within a file.

As the option is selected by default, you can just click **Next**.

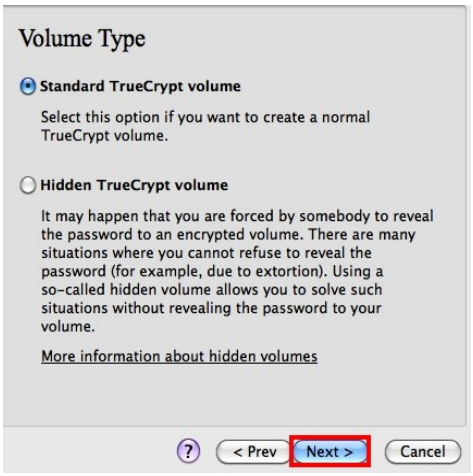
- Note: In the following steps, the screenshots will show only the right-hand part of the Wizard window



Step 4:

In this step you need to choose whether to create a standard or hidden TrueCrypt volume. In this tutorial, we will choose the former option and create a standard TrueCrypt volume.

As the option is selected by default, you can just click Next.

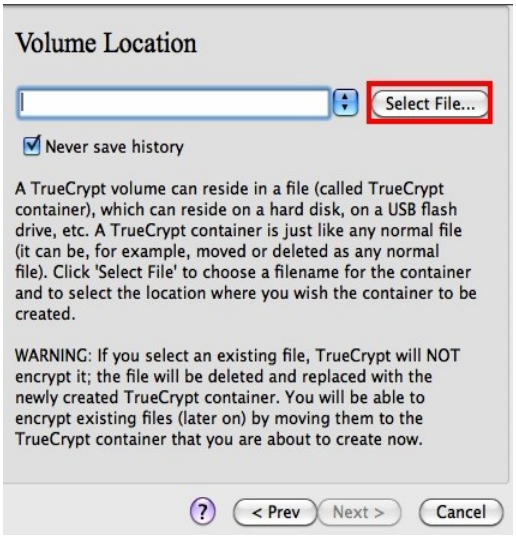


Step 5:

In this step you have to specify where you would like the TrueCrypt volume (file container) to be created. Note that a TrueCrypt container is just like any normal file. It can be moved or deleted as any normal file. It also needs a filename, which you will choose in the next step.

Click Select File.

The standard OSX file selector should appear (while the window of the TrueCrypt Volume Creation Wizard remains open in the background).

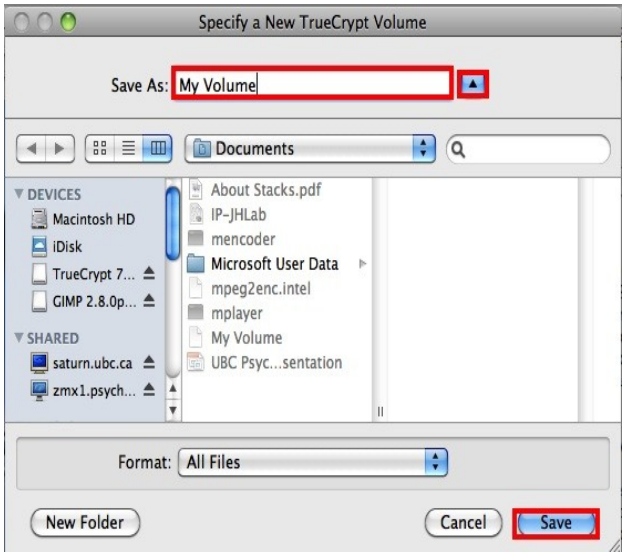


Step 6:

In this tutorial, we will create our TrueCrypt volume in the folder *Documents* and the filename of the volume (container) will be *My Volume* (as can be seen in the screenshot below). You may, of course, choose any other filename and location you like (for example, on a USB memory stick).

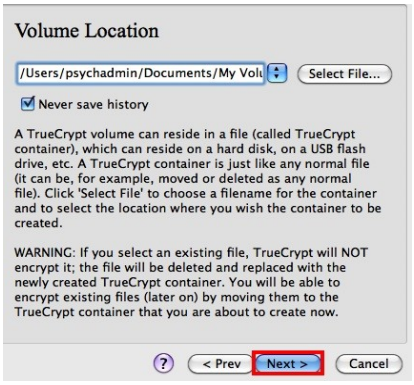
Select the desired path (where you wish the container to be created) in the file selector.

Type the desired container filename in the File name box. Click Save. The file selector window should disappear and you will be returned to the Volume Creation Wizard.



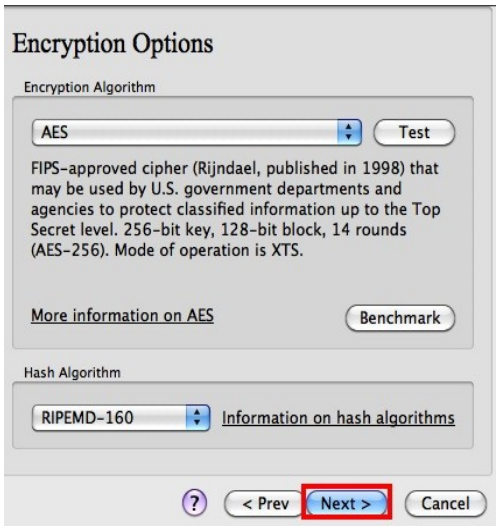
Step 7:

In the Volume Creation Wizard window, click Next.



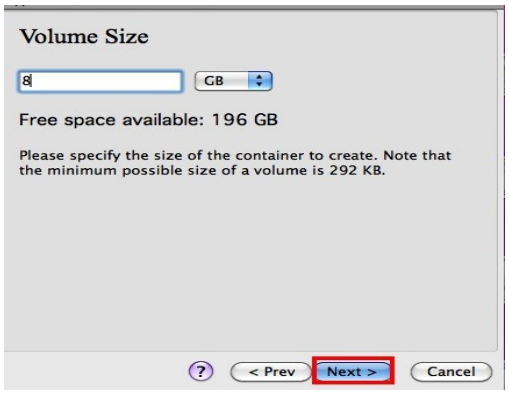
Step 8:

Then you will see some fairly advanced encryption settings. Leave at default and click Next.



Step 9:

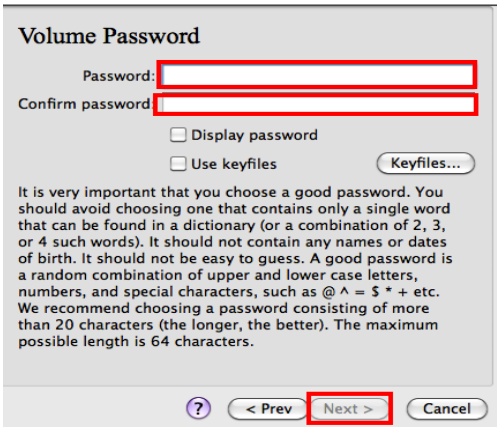
Here we specify the size of our TrueCrypt container, you will want to set it to a large enough size to store all of your data. I would recommend the size of an average thumb drive, **8GB**. After you type the desired size in the input field (marked with a red rectangle) and select the appropriate radio button (KB, MB or GB), click Next.



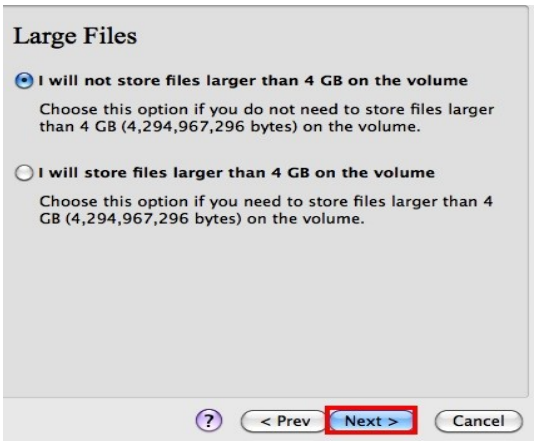
Step 10:

This is one of the most important steps. Here you have to choose a good volume password.
Read carefully the information displayed in the Wizard window about what is considered a good password. After you choose a good password, type it in the first input field. Then re-type it in the input field below the first one and click Next.

Note: The button Next will be disabled until passwords in both input fields are the same.



It will then show the below “Large Files” window. Leave as default and click next.

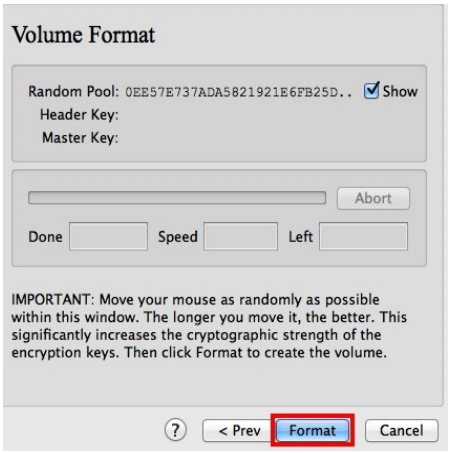


Step 11:

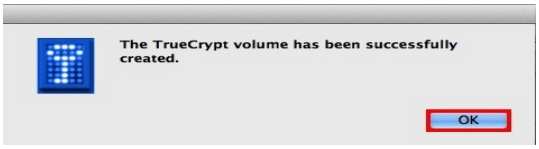
The next screen will ask what format you would like your storage container to be. Leave as default (FAT) unless you are going to store files larger than 4GB. If you are, select Mac OS Extended. Click next.

Move your mouse as randomly as possible within the Volume Creation Wizard window at least for 30 seconds. The longer you move the mouse, the better. This significantly increases the cryptographic strength of the encryption keys (which increases security).

Click Format.

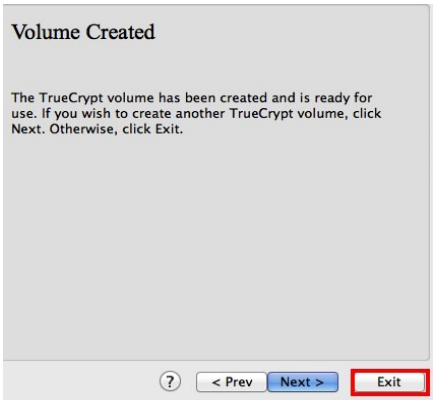


Volume creation should begin. TrueCrypt will now create a file called *My Volume* in the folder *D:\My Documents* (as we specified in Step 6). This file will be a TrueCrypt container (it will contain the encrypted TrueCrypt volume). Depending on the size of the volume, the volume creation may take a long time. After it finishes, the following dialog box will appear:



Click **OK** to close the dialog box.

Step 12:



We have just successfully created a TrueCrypt volume (file container).

In the TrueCrypt Volume Creation Wizard window, click **Exit**.

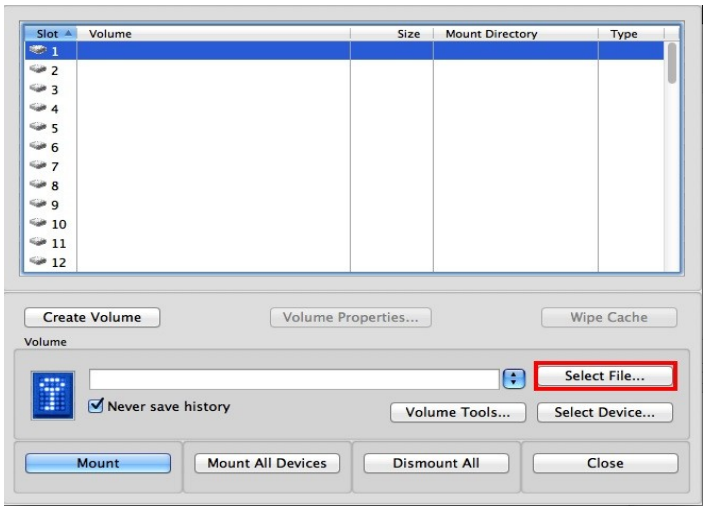
The Wizard window should disappear.

In the remaining steps, we will mount the volume we just created. We will return to the main TrueCrypt window (which should still be open, but if it is not, repeat Step 1 to launch TrueCrypt and then continue from Step 13.)

Step 13:

Select a slot number from the following list (marked with a red rectangle). This will be the slot to which the TrueCrypt container will be mounted.

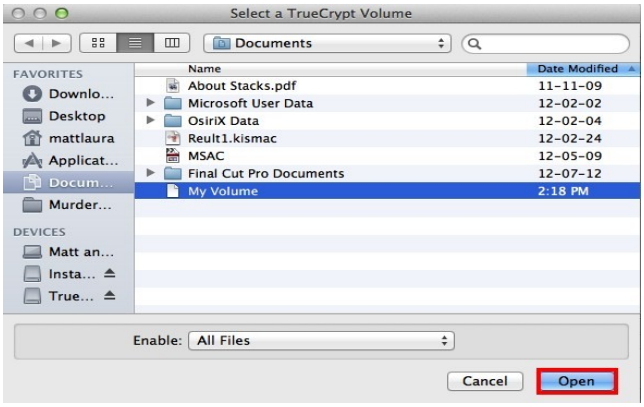
Note: In this tutorial, we chose the Slot 1, but you may of course choose any other available slot.



Click **Select File**.

The standard file selector window should appear.

Step 14:



In the file selector, browse to the container file (which we created in Steps 6-11) and select it.

Click **Open** (in the file selector window).

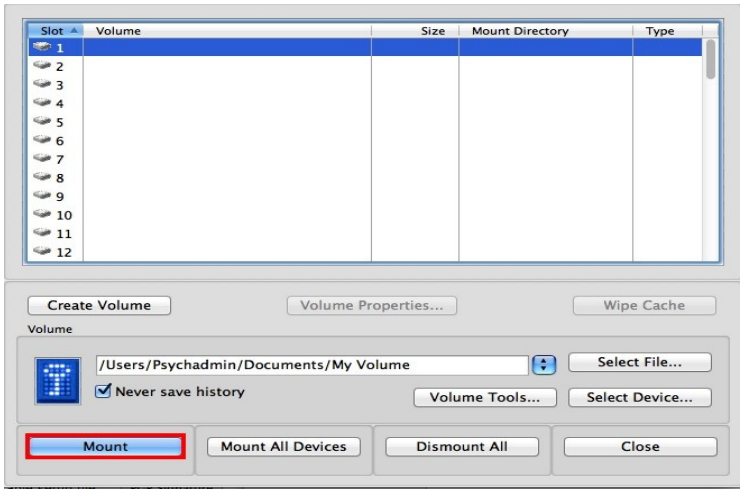
The file selector window should disappear.

In the following steps, we will return to the main TrueCrypt window.

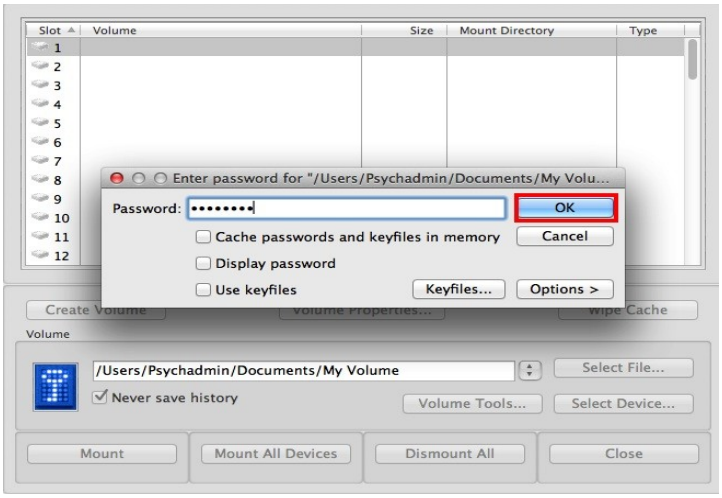
Step 15:

In the main TrueCrypt window, click Mount.

The password prompt dialog window should appear.



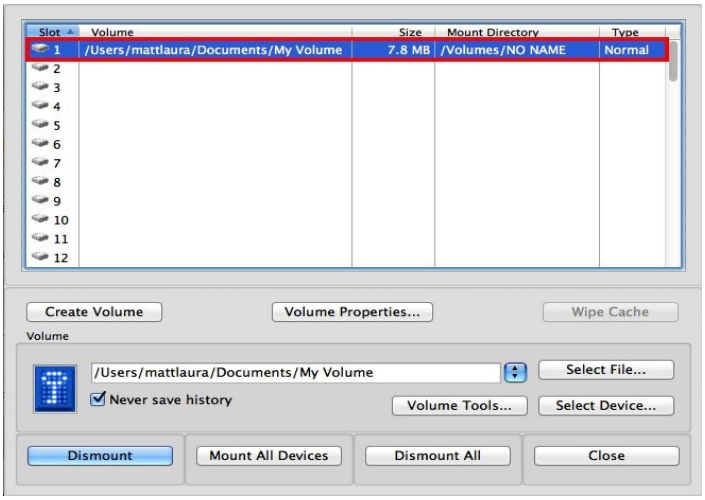
Step 16:



Type the password (which you specified in Step 10) in the password input field. Click **OK**.

TrueCrypt will now attempt to mount the volume. If the password is incorrect (for example, if you typed it incorrectly), TrueCrypt will notify you and you will need to repeat the previous step (type the password again and click **OK**). If the password is correct, the volume will be mounted.

Step 17:



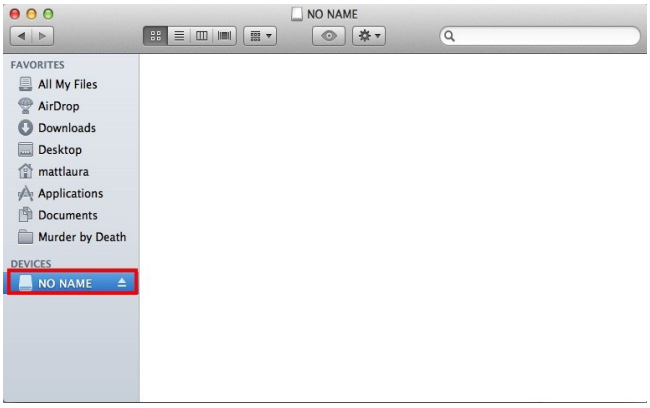
We have just successfully mounted the container in Slot 1. It will appear on your system as NO NAME..

The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves like a real disk. You can save (or copy, move, etc.) files to this virtual disk and they will be encrypted on the fly as they are being written.

Important: Note that when you open a file stored on a TrueCrypt volume (or when you write/copy a file to/from the TrueCrypt volume) you will not be asked to enter the password again. You need to enter the correct password only when mounting the volume.

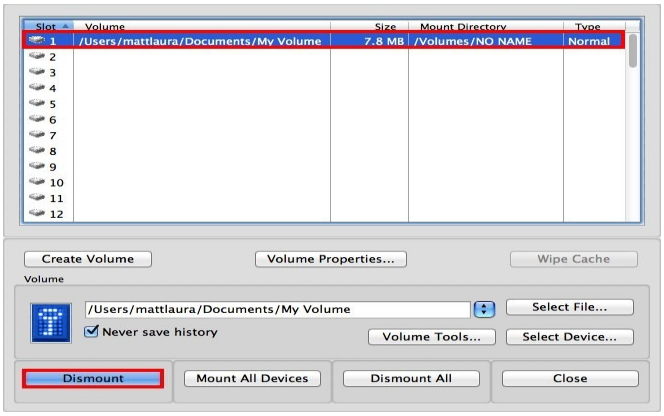
You can open the mounted volume, for example, by double-clicking the item marked with a red rectangle in the screenshot above.

You can also browse to the mounted volume the way you normally browse to any other types of volumes. For example, by opening *Finder* and click on *NO NAME*. It appears in *Finder* much like a USB drive would.



You can copy files (or folders) to and from the TrueCrypt volume just as you would copy them to any normal disk (for example, by simple drag-and-drop operations).

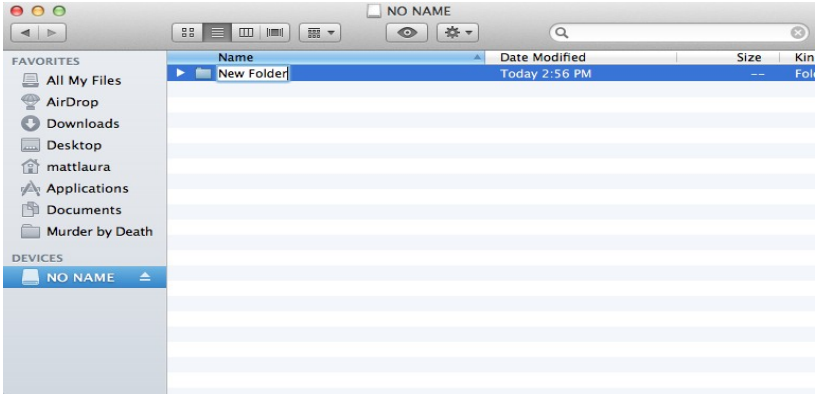
If you want to close the volume and make files stored on it inaccessible, either restart your operating system or dismount the volume. To do so, follow these steps:



Select the volume from the list of mounted volumes in the main TrueCrypt window (marked with a red rectangle in the screenshot above) and then click **Dismount** (also marked with a red rectangle in the screenshot above). To make files stored on the volume accessible again, you will have to mount the volume. To do so, repeat Steps 13-16.

Step 18 - Practice

Let's practice using the drive. As said before you can use the encrypted storage container exactly as you would a USB drive. You can drag files to it by using *Finder* or select it as your *Save To:* destination when using a program such as *MS Word.* You can even create folders in it as shown in the screenshot below.



Step 19 - We're Done

You can now feel confident that the data stored in your encrypted virtual drive is safe. If you have any questions or concerns please contact Psychology IT at <matthew.smith@psych.ubc.ca>.