ITP 125 - Lab 06

Deadline

1 minute before the next scheduled lecture.

Objective

Hide your data from people cause you don’t want them to see your dirty little secrets.

Setup

**Installation:**

If you plan to do this lab at home you will need to download and install the following:

**Both (Windows and OSX):**

Veracrypt

<https://veracrypt.codeplex.com>

Procedure

**Symmetric Encryption**

For this lab, remember never to use a password that you typically use for any other account. In addition, remember that you will be working with 2 passwords. The outer volume should have the weaker password. You have make strong passwords for both volumes.

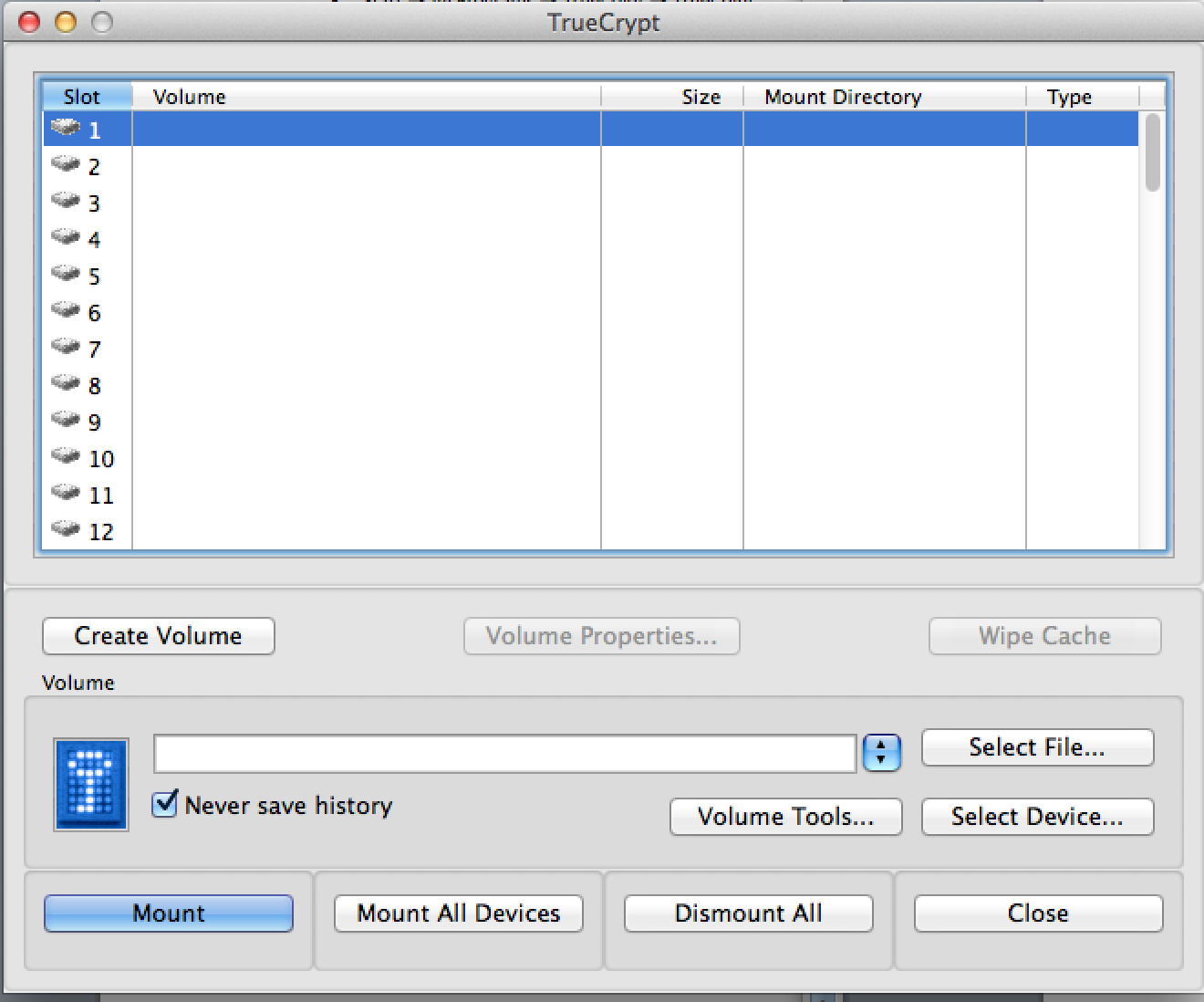
1. The way Veracrypt works is by creating encrypted volumes for you to put files in. So you cannot encrypt a file directly.

One special thing you can do with this feature is to create hidden volumes. This allows for a volume file to have 2 containers. In other words, you can have a public portion of the file (with things you don’t care too much about), and a hidden portion (with your real secrets).

Start up Veracrypt.

1. We’re going to create a new volume. Do the following

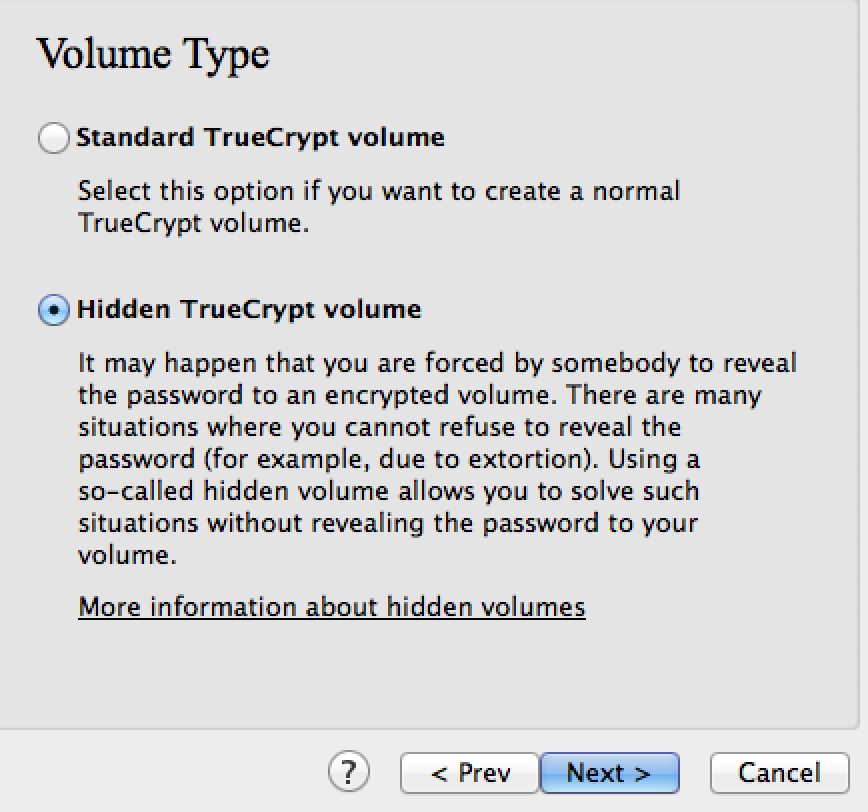
Click on “Create Volume” button



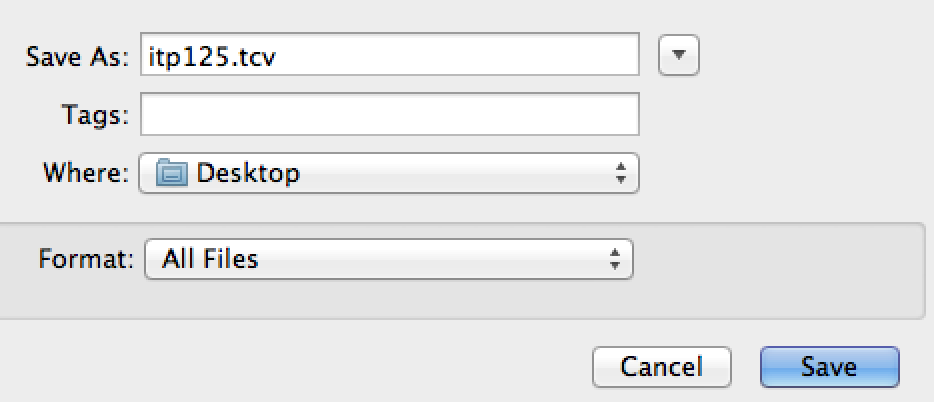
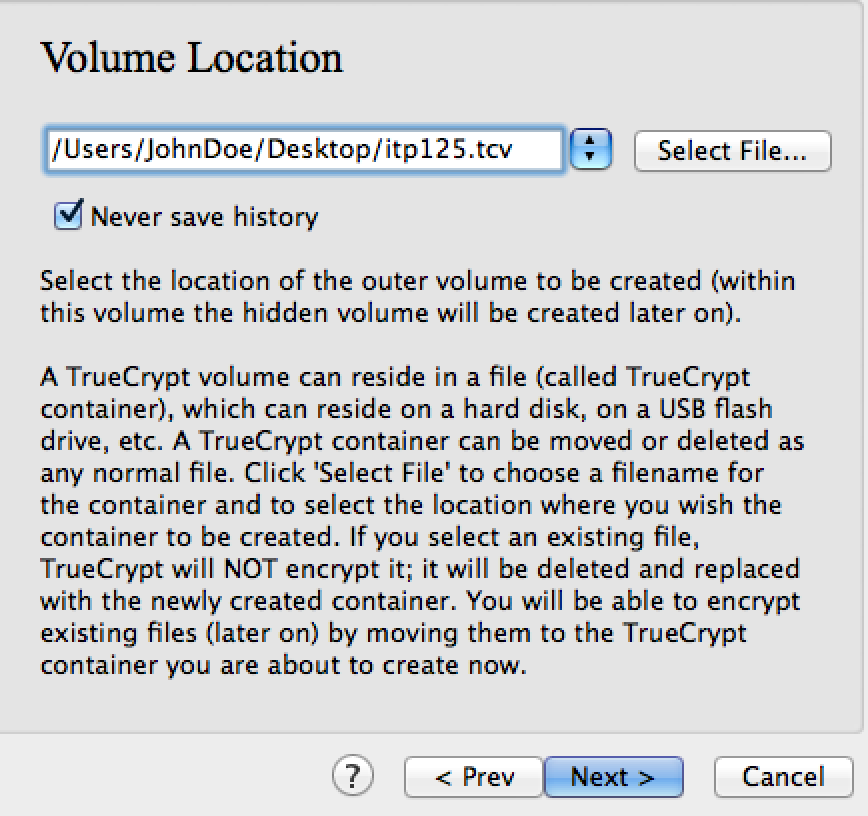
Select “Create an encrypted file container” then press ‘Next’



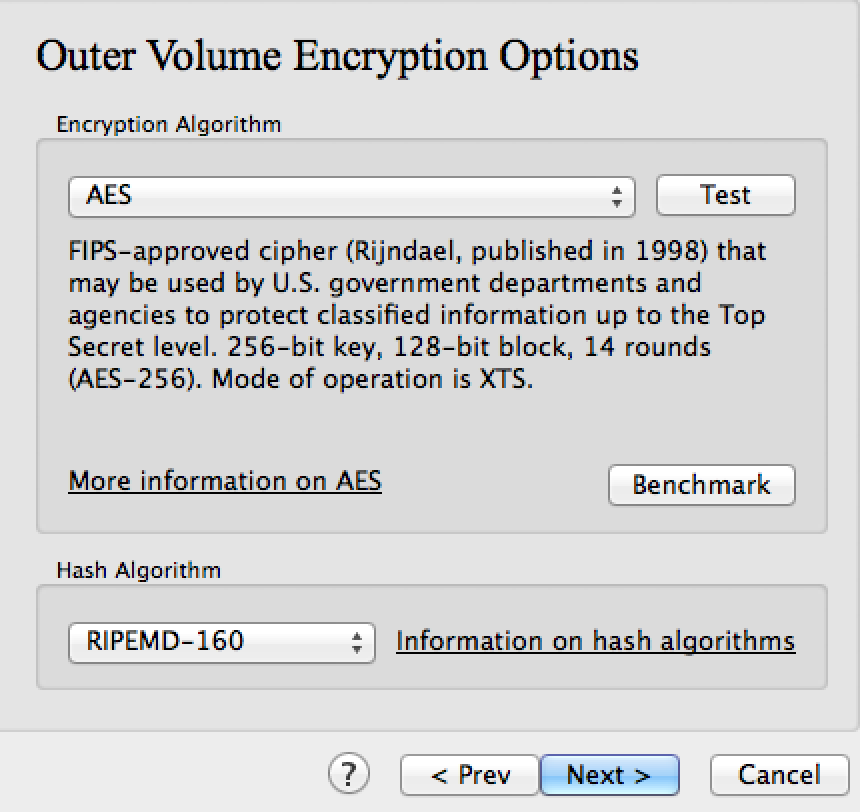
1. Select “Hidden Veracrypt volume” then click on ‘Next’



1. Under “Volume Location”, press the “Select File…” button 🡪 Select your ‘Desktop’ 🡪 Create a new file called “itp125.tcv” 🡪 click on ‘Save’

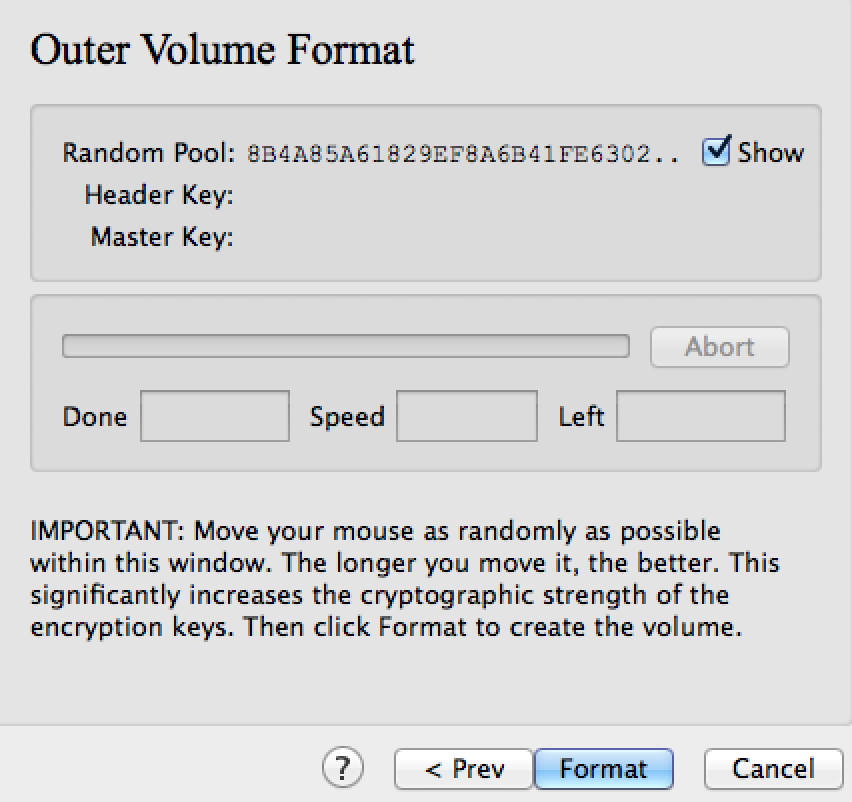
  
  


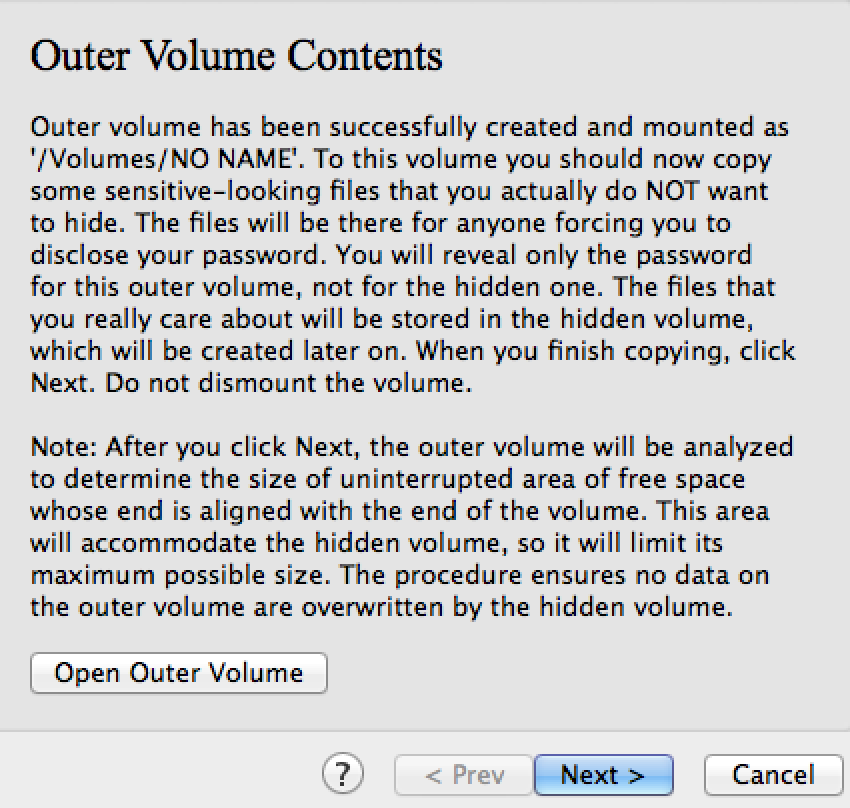
1. Under the “Outer Volume” window leave the default options and click on ‘Next’

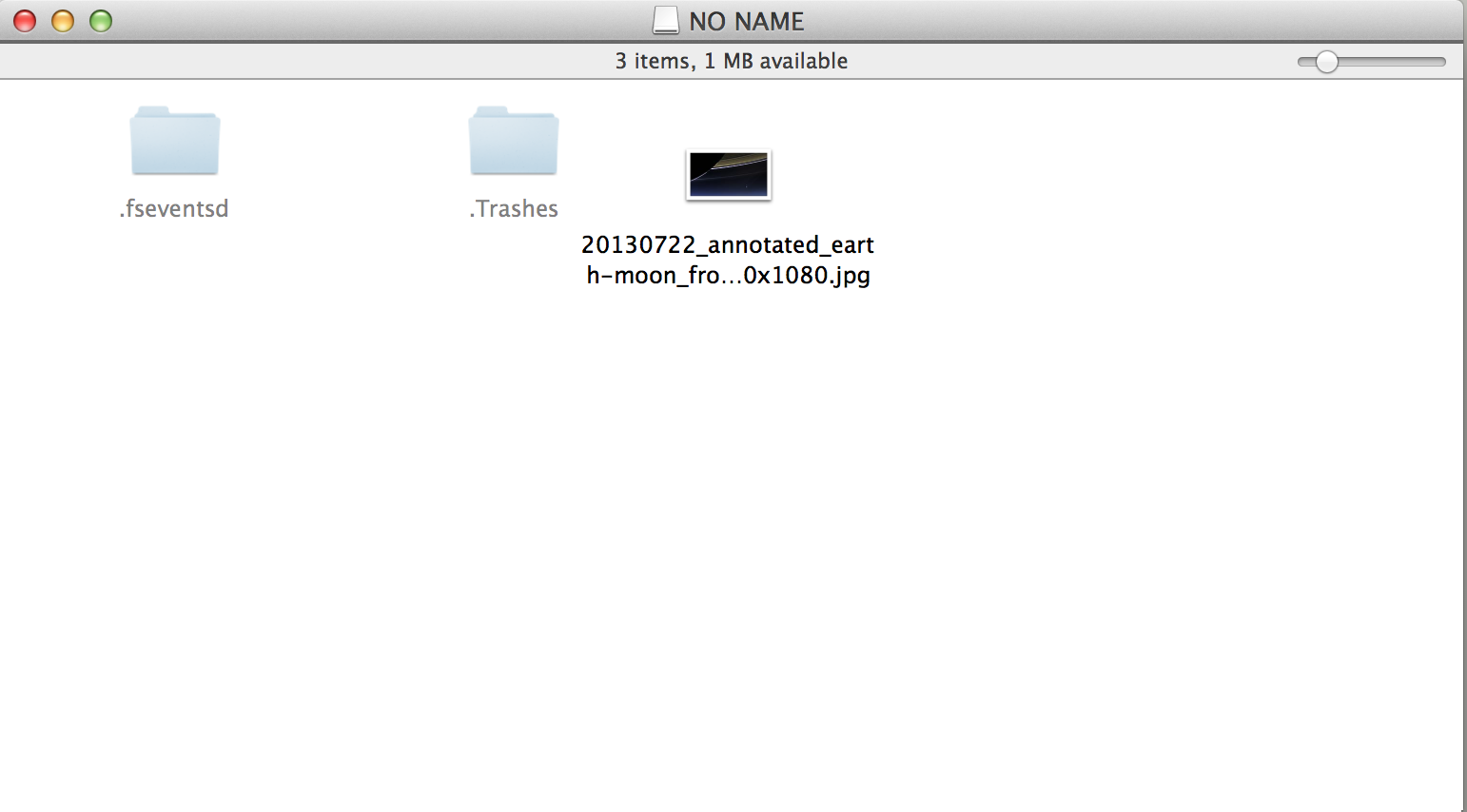


1. Under the “Outer Volume Size”, type in 2 MB then press ‘Next’

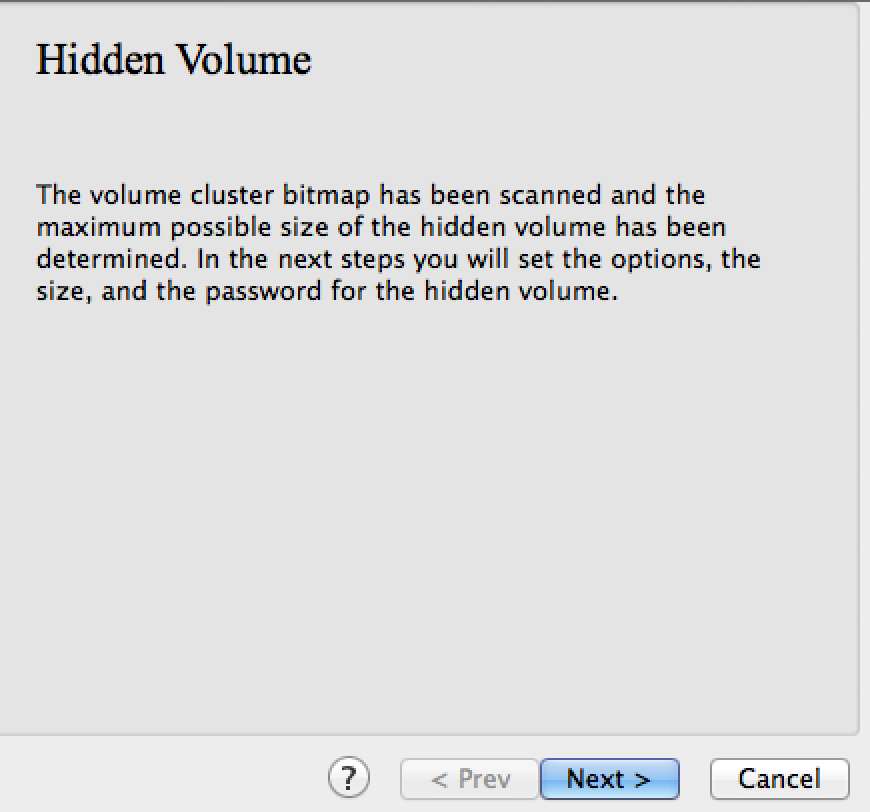


1. Under the “Outer Volume Password”, type in any password you can remember then click on ‘Next’. **Note:** in the picture, the option of “display password” is checked. You really shouldn’t be doing this.   
   
2. Under the “Outer Volume Format”, move the mouse for a while. When you are tired, click on ‘Format’  
     
   
3. Under the window “Outer Volume Contents”, click on the button “Open Outer Volume” and start placing file that you do not care much for.   
     
   When you are satisfied with the files placed in the outer volume, click on ‘Next’  
     
   **Note:** Keep total size of all the files to be less then 1MB.





1. Under the “Hidden Volume”, click on ‘Next’



1. Repeat steps 5-9. When you get to the part of entering a password for the hidden volume, use a password different from the outer volume. This is very important.

**Note:** You would probably want to use a stronger password for the hidden volume, and a slightly weaker password for the outer volume.

Questions

1. In step 5 of the lab, you could choose a different hashing algorithm for the encryption. We will talk about hashing later on, but if we’re doing symmetric encryption why does Veracrypt need a hashing algorithm?

Curiosity is your friend.

1. In step 8, the program asked for you to move the mouse around. What is the point of randomness generated from this? How is it used in the encryption?
2. Certain countries have a [Key disclosure laws](http://en.wikipedia.org/wiki/Key_disclosure_law). How do you think Veracrypt can help circumvent the law that is in place? Do you agree with these laws? Explain.
3. In the previous question, we talked about Key disclosure laws. How does the US handle the disclosure of passwords? If you were crossing airports and security officials demanded your password, do you have to?
4. In order to submit this lab, you will need to place the answers to this lab into a Veracrypt volume that is not more then 250KB. You may use any password(s) that you like.

How do you plan to get the password to the volume to the grader securely?

If you plan to place the password in the email what’s the point of encryption if anyone can read it. Think about the best way possible without leaking the password to anyone (even the email servers). Only you and the grader should know the key.

1. Read the some of the following articles:

<https://isc.sans.edu/forums/diary/True+Crypt+Compromised+Removed/18177/>

<http://www.tomsguide.com/us/Truecrypt-may-be-compromised,news-18861.html>

[http://krebsonsecurity.com/2014/05/true-goodbye-using-Veracrypt-is-not-secure/](http://krebsonsecurity.com/2014/05/true-goodbye-using-truecrypt-is-not-secure/)

Based on your readings, do you still think Truecyrpt is still safe to use? Explain. Can you think of any alternatives to Veracrypt that you would trust using?

Submission

Answer the questions above and place them in a Veracrypt container with a hidden volume. On the outer container place an image of any animal. In the inner container, place the answers to the questions as lab06.docx. Upload the file to your **itp125 folder** on the web hosting.

Set the password to the outer container to be: **mypersonalstuff**

Set the password to the hidden container to be: **snowdendocuments**

Make sure you can see the file by publicly accessing the URL using any web browser of your choosing.