Noah Baker

ITP 125 – Lab 6

1. Veracrypt needs a hashing algorithm in order to generate a key to encrypt the plaintext and later open the ciphertext.
2. The key is generated by assigning letters and numbers to the cursor’s different locations across the dialog window. Because the algorithm to generate the key is based on random cursor movements it is very challenging to copy the algorithm in order to crack the key. They key is used to encrypt plaintext and decrypt cryptotext.
3. Veracrypt can circumnavigate Key disclosure laws because they have no idea how the user moved his cursor to generate the key. It is different every time. Encrypting data should be a right because it falls under methods for upholding personal privacy, also a right.
4. TSA does not and will not confiscate laptops or other electronic devices at our checkpoints.  Should anyone at a TSA checkpoint attempt to confiscate your laptop or gain your passwords or other information, please ask to see a supervisor or screening manager immediately.
5. The claims battering TrueCrypt’s security are not confirmed, making any argument against the service’s integrity hearsay. However, TrueCrypt itself has alerted its users with reason to be alarmed. Although it is not clear whether TrueCrypt is compromised, why take the risk by continuing to use TrueCrypt when there are equivalent alternatives?