ECE4095 Trustable Computing Systems Lab
March 27, 2013

Disk Analysis

The goal of this lab is to recover data from a disk image using a forensic analysis tool. The primary goal is to see if you an unencrypt the "Great Pickup Lines.doc" file in the Frodo Baggins Documents directory

1. Create a AccessData Forensic Toolkit Demo case

Open up the Forensic Toolkit Demo program.

Create a new case by choosing File->New Case

Fill in the Case Number and Case Name and then click Next on the next few dialog screens.

When you get to the add evidence screen, Click "Add Evidence", choose "Acquired Image of Drive", and add the precious.img disk image that was provided. It will take a few minutes for FTL to process the image.

2. Analyze the case

There are several tools to help you analyze the image. If you use the explore tab, you can look at various files in the file system. The DriveFreeSpace file is where deleted files may reside.

The search tab will allow you to search for certain keywords in text. Type in a search term, click Add, and then click "View Cumulative Results" to get a list of all the files with that term.

Once you find the password, you can choose Tools->Enter EFS Password to encrypt the files. If it worked, the decrypted files will be placed in the efs/decrypt folder in the case directory.

3. Lab Assignment

What to hand in:

1. Turn in the unencrypted "Great Pickup Lines.doc" file
2. Turn in a report on how you found the password and what are the potential vulnerabilities in disk storage systems.