15-498 Information Forensics
Lab #1: Storage

Teams: 5 people per team
Due: 15 February 2011

Introduction

The primary job of an information forensics professional involves understanding the information landscape, bringing together the right information sources, analyzing and interpreting them, and presenting the resulting understanding to the other professionals involved in the matter. Because of the complexity of the environments in which they work, forensics professionals have to be able to resolve many common hurdles faced along the way. And, when appropriate they need to be able to identify the correct professionals to address matters beyond their competency.

Generally speaking, data recovery is a different profession that forensics. Data recovery professionals are not trained and experienced in asking the right questions, pulling together the right pieces, finding the needles in the haystack, analyzing the information, and reaching conclusions about the fact basis of matters in question. They are however very skilled and experience in getting past damage and defects in order to get the haystacks, including the needles, out of devices that are not functioning properly.

This lab isn't designed to help you to become a data recovery professional, although it could be a first step, should you pursue that interest. Instead, it is designed to help you to understand storage systems, in order to help be a better forensics professional. Along with the in class discussion it is designed to help you to understand the capabilities and complexities of data recovery in order that you will have a better understanding of its role in supporting forensics, reasonable expectations, the skills and tools needed by professional data recovery services, and that you'll have a better ability to communicate with your clients and data recovery professionals.

In order to do this, and gain a better understanding of how hard drives work, you'll disassemble two and swap the head assemblies. The goal is to have two retain two working drives. If successful, the goal is to attempt a much more complex and precise platter swap. You'll also recover information from two damaged CDs.

Guesspectations

My guess is that you'll be able to get data off one of the two drives and both of the CDs. But, we'll see.

Hard Drive -- Step-by-Step Guide

1. Take two hard drives for your team. Use the sharpie to label them. You can store them on a shelf in the lab. But, since they all look alike, I'd suggest taking them with you.

2. Test the drives using the enclosures. Make sure they work. Write data on them. Read data from them. They are fresh from the vendor and are reconditioned. It is essential that you test first, and that you place data on both of them for later reading. The more data you place, the more shots you'll have of getting data later.

3. Remove the label form the top of your drive.

4. Remove the shielding plate from the bottom, circuit-board side of the drives. It should be two screws.

5. Carefully examine the "junk drive" in the lab space. Try assembling and disassembling it for practice. You'll also want to try your techniques on it. If other teams are working, try to work together. Bounce ideas off each other. Watch what works and what doesn't

6. You don't have to use one of the aquariums. But, they might help you to exclude dust. Notice that they are on their sides to give you access to the front, while preventing dust from falling in from the top. If you do choose to use them, *be careful – they are fragile glass*.

7. Thoroughly clean your aquarium or other work area.

   The shop vac is designed to be used as a blower. It is set up to blow out mostly filtered air. Do not use it for cleaning. Try to avoid using it, at all. But, if necessary, it can be used to plow off dust. The fear is that the air movement will shake loose other dust, causing it to move around.

   Clean your workspace using regular paper towels until it is truly clean. Then, wipe it down with the micro-fiber cloths until you see no signs of dust, even upon careful inspection.

8. Clean your drives, wipe them down, and place them into your work area.

9. Put on gloves, if you'd like.

10. Remove the head assembly from the first drive:
    a. Remove the screw on the bottom of the of the circuit board that retains the head board connector
    b. Remove the 5 screws from the top and remove the top. You might need to pry it *gently* the first time
    c. Remove the screw that retains the head connector from the top.
    d. Remove the metal plate on top of the assembly. Be careful, it is held in tightly by magnetism. Be steady with it and the rest of the drive.
    e. Using the pick to engage a screw in the center of the spindle, rotate the drive to help the heads slide outward. You'll probably find a clockwise rotation works. Rotate slowly and smoothly while slowly guiding the head assembly to the outside of the platters. You can guide the assembly with a pick, or from the black plastic at the rear
    f. Shim the heads. My suggestion is to use folded plastic pieces. It can hold the arms apart, or it can slide over and under the platter. But, be sure it interacts only with the arms (and, if necessary, the platter surfaces) and not the heads themselves. If the plastic touches the heads, they will be easily damaged.
    g. Slide the heads off of the platters
    h. Unscrew the screw that holds the head assembly down from the top.
    i. Carefully remove the head assembly and set it aside, without disturbing the shims. But, if necessary, do adjust them.
11. Repeat this procedure for the second drive. Have different members of your team perform different roles.
12. Swap the head assemblies. Reassemble one drive completely, then the next
13. Give it a try. Did it work? Copy the data off.
14. If you've gotten to this point, and the drive is working well, please see Greg. He'll help you learn the process of doing a platter swap, which is dramatically more ticklish and requires the construction of a jig. Then, if you'd like, you can give it a try.

CD -- Step-by-Step Guide

0. CD's are much easier than hard drives, at least in so far as we can play with them.
1. Select one cut CD and one severely scratched CD
2. As discussed in class, only use an SCS-owned CD drive, not one of your own. Use either one in the lab space, or in a GHC cluster (or WeH laptop)
3. If the cracking gets any worse during your repair, you may take another CD. We want to avoid the disk shattering within the drive
4. For the cracked disk, your goal is to stabilize the crack, brining the edges together, while trying to cause it to lay flat. Some polishing near the crack might minimize the distraction to the laser
5. For the scratched CD, polish it with sandpaper, then polish. Once it looks new, try to get the data
6. You might find CDCheck, a tool which can do a raw read, of help. You might also try *dd*, with the option set to ignore errors.

Deliverables

1. Your two hard drives (I want to disassemble to inspect, in particular the platters and head arms
2. Your two CDs (I want to see what you did)
3. A report documenting (a) Your process for the first removal/install, (b) what you did differently for the second attempt, (c) your results, and (d) what you got from the experience, if anything (be honest, this is the pilot version of the class), (e) if the lab should be repeated in the future

Important Notes

This lab is really an afternoon or two of work, maybe three with the report. It has been given two week for two reasons. The first is to give everyone time to use the space. The second is to make sure that we have enough of everything for everyone to play. If anything is missing or broken, or if you need more of anything please ask as soon as possible. If I have it, I'll give it to you immediately. If not, I'll order it and get it in a day or two.

You'll need to work as a team. For example, you'll probably want one person holding the drive in place, with one person using the screwdriver, and maybe another person retaining, moving, or removing the head assembly.

Be creative. Improvise.