CMSI 387-01

Operating Systems

Spring 2014

Assignment 0501

The final task for the semester is a classic digital forensics exercise: reading a disk at the hex level. The work has been virtually spelled out for you step by step. Just follow along, then read the bytes.

Outcomes

This assignment will affect your proficiency measures for outcomes *1a*, *1b*, *2e*, and *4d–4f*.

Not for Submission

File system interface and implementation are covered in SGG Chapters 10 and 11.

For Submission

"CSI: FS"—The Short Version

Make an *ext2/ext3* disk image, mount it, put some files on it, print the user view of the file system (i.e., a series of *ls* invocations), dump the disk image to hex, and identify, at the hex level, the various sections listed in Step 6 of The Long Version.

"CSI: FS"—The Long Version

1. To create the disk image, you'll need to learn how to use the *dd* ("disk dump") command. The following example creates a new file called *image* consisting of 1024 default-size blocks, and initializes its contents with zeroes:

   dd if=/dev/zero of=image count=1024

2. You should now have a file that is equivalent to a brand-new, unformatted disk. "Format" it by installing an empty *ext2/ext3* file system on it:

   mke2fs image

3. Mount the disk image—this is what requires *sudo* access:

   mount -o loop -o nosuid -o nodev image mountpoint

   …where *mountpoint* is the directory under which you'd like to mount *image*. You can use *df* to verify that your command worked. To unmount the disk image, do:

   umount mountpoint

   Again, *df* will tell you if all went well.

4. Create the following items within that mounted file system:
   a. A non-empty text file at the top-level directory of the file system
   b. A directory at the top-level directory of the file system
   c. A second non-empty text file inside that subdirectory (give it different content so you can differentiate the two files)
   d. A symbolic link inside that subdirectory to the text file in the top-level directory
   e. A hard link from the top-level directory to the text file in the subdirectory

5. Run a series of *ls* commands on the now-populated file system, and note the output. Feel free to use various *ls* switches (e.g., *–F*, *–l*, *–a*, *–i*, etc.) to see as much interesting information as possible.

6. Dump the disk image file to hex using *hexdump –C*, then identify these items:
   a. The disk image's superblock
   b. The directory entries for the files, links, and directories that you created
   c. Where applicable, the inodes for the items that you created
   d. Where applicable, the data blocks occupied by these items

Get a feel for that and enjoy the hacker buzz **:)** For your souvenirs, commit and push the following artifacts to */homework/csi-fs*:

- The disk image file itself (it shouldn't be very large anyway)
- A text file showing your shell activity while performing this task up to step 5
- A file in any widely readable format showing the relevant *hexdump* segments for the items requested in step 6