Lab Exercise – Digital Acquisition
Principal Instructor: Cal Lee

You are working with, Dr. Matilda Bigschat, a prominent senior employee, who is now retiring and has various materials to transfer before she departs.

When you met with Dr. Bigschat, she provided you with a box full of physical media (CDs, floppies, flash drives, and an external hard drive). In some cases, she could tell you specifically what was on them and why it was important to retain. In other cases, she could only recall that the contents of the media were important to her research, based on where she had filed them in her office.

You examined one of the CDs. There are no labels on it. You used FTK Imager to create a disk image of the drive. You then used FTK Imager to create a disk and to export the files, which you can now find in files.iso and files.zip, respectively.

Task Set 0 – Preparation

- Download and save to your desktop:
  - http://www.ils.unc.edu/callee/files.zip
  - http://www.ils.unc.edu/callee/files.iso
- Tools (already installed on your lab computer)
  - To generate and verify hashes of files: file-verifier++
  - Hex viewer and editor: HxD

Task Set 1 – Seeing what you have – looking in bigschat-files

Inspection at the file level

- Based simply on the properties and names of the files and directories (don't open any files yet), try to make some inferences about what these files are and how they might be related.

Looking at names of specific files

- Find a file called Circular.596
- Do you see any other files that have similar names? If so, make note of which ones they are.

Inspection at the bitstream level

- Generate a hex view of the file called Circular.596 – using HxD
- What can you infer about this file from looking at the hex representation?
- If you identified other files in task 2, also view those in hex view. Do you notice anything similar?

Investigating the .ISO (disk image) file

- Open FTK Imager
- Go to File | Add Evidence Item…
- Select "Image File"
- Browse to files.iso and then select "Finish"
- Navigate the file tree and discuss what you observe

Task Set 2 – Investigation based on hash values

Generate hashes

- Open FileVerifier++
- Click on the "Options" button
- If the "Default Algorithm" is not set to MD5, then change it to MD5 and select "Apply"
- Click "Ok"
- Close the program and then launch it again (ensures that the settings have been changed)
- Click on the "Dirs" button

- Navigate to the bigschat-files folder on your desktop
- Click “Ok”
- You should now see a list of 59 file paths and associated hashes
- Leave this application running

Finding duplicate files

- Look at the MD5 value of Circular.596
- If you identified other files in task 2, are the values the same or different?
- If you notice something interesting about the MD5 values, what can you infer about what happened to the files?

Verify hash values

- Go back to FileVerifier++
- Click on the “Verify All” button
- Don’t enter or change anything, then click on “OK”
- Note whether all rows are green and indicate “Valid” in the Verification column (meaning that the MD5 values have been verified)

Opening files with hex editor

- Pick one or more items from the “files” folder and open them in HxD. You can drag the file onto the HxD icon on your desktop.
- Look at the hex view of each file and see what it reveals about the bitstream content of the file

Changing content with hex editor

- For one or more of the files, change a byte within the file in HxD and then save the changed file.
- Note which files you’ve changed and the **specific place** in the files where you changed them.

Re-Verify hash values

- Be sure to exit out of HxD (if files are open in it, the hash calculation might not work correctly)
- Go back to FileVerifier++
- Click again on the “Verify All” button
- See whether you now have a red row and “Invalid” in the Verification column for the file(s) that you changed.

Change content back to earlier state in hex editor

- Open one or more of the files that you changed earlier, and change the bits back to their previous state, and then save the changed file(s).

Re-Verify hash values

- Go back to FileVerifier++
- Again click on “Verify All” and “OK”
- See whether you again have a green row and “Valid” in the Verification column for the file(s) that you changed.