Deleted File Persistence Process Notes

Setup:

1. Install FTK Imager:
    - a. http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.4.2
2. Configure a Ubuntu VM or similar for processing:
    - a. Install DFXML, fiwalk, and idifference2.py (see GitHub/simsong/dfxml)
    - b. Install adiff.py and trace_file.py (see GitHub/jjonesu/DeletedFilePersistence)
    - c. Create a local folder under Windows and share the folder with the VM

Create Images:

1. Insert/attach device to be tested
2. Put files on device or create content or use device, as needed
3. Take image 0:
    - a. Launch FTK Imager
    - b. Answer “yes” to UAC if prompted
    - c. File > Create Disk Image > Physical Drive > Next
    - d. Select USB device from dropdown list (probably the last one in the list)
        - i. Click Finish
    - e. Uncheck all boxes except Precalculate Progress Statistics
    - f. Click Add
        - i. Raw(dd) > Next
        - ii. Don’t enter anything for Evidence Item Information; just click Next
        - iii. Browse to a local destination folder
            1. Create a new folder for each set of images
            2. The folder should be on the part of the local drive that is shared with the VM
        - iv. Name the file “0” (that’s zero, no quotes)
        - v. Set Image Fragment Size to 0
        - vi. Click Finish
        - vii. Click Start
        - viii. Let it run until complete; will take about 1 minute per GB
4. Delete one or more files
5. Take image 1
    - a. Same as image 0 except for filename is 1, not 0
6. Conduct more activitiy
7. Take image 2
    - a. Same as image 0 and 1 except for filename is 2
8. Repeat steps 6 and 7 as necessary, incrementing the filename each time
9. When done, proceed to Image Analysis

Image Analysis:

1. Check adiff.py user settings:
    a. ../python/adiff.py
2. Run adiff.py
    a. From folder with images…
    b. $ python3 ../python/adiff.py
    c. Will take about 1 minute to process 3 1 GB images
3. Check deleted.db file
    a. $ sqlite3 deleted.db
    b. > SELECT count(DISTINCT filename) from deleleted_files;
        i. Should return the number of deleted files you tracked
4. Check trace_file.py settings
    a. ../python/trace_file.py
5. Run trace_file.py
    a. From folder with images…
    b. $ python3 ../python/trace_file.py
        i. Just hit Enter the first time to list files tracked; should match deleted.db
        ii. Run a second time and type “*” (asterisk, no quotes) then Enter to process all files
6. Examine the output on screen, PDF graphs, and other output data files