# Lab 04 – Tool Validation

Our task in this lab is to determine if our tool results for a particular operation are valid. To assist with this validation task and the particulars of how Autopsy uses PhotoRec to carve for files in unallocated space, there's a spreadsheet labeled FATCalculator.xlsx attached to the Dropbox. It is **not** a perfect calculator for all situations (only works for contiguously allocated clusters), but it will work for this lab. The target of the spreadsheet is to make the calculations easier to follow and include notes on their purpose.

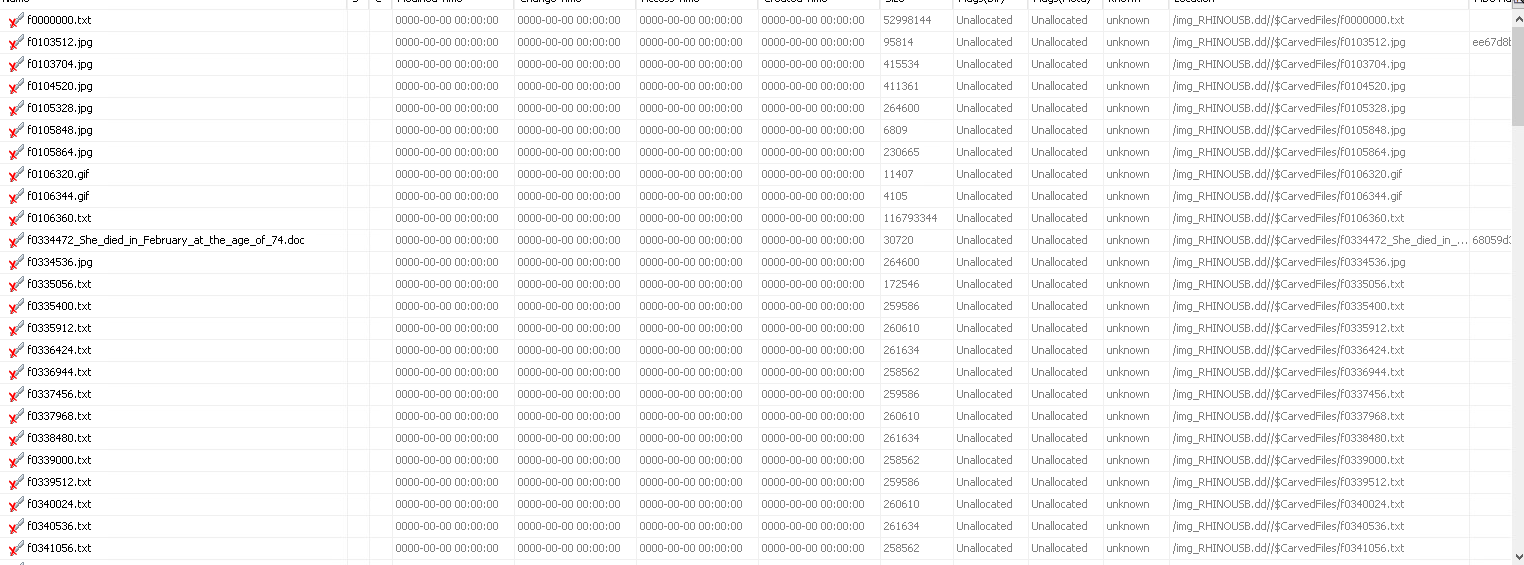
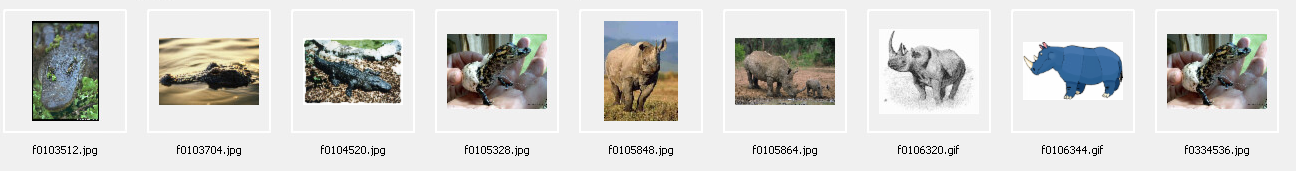
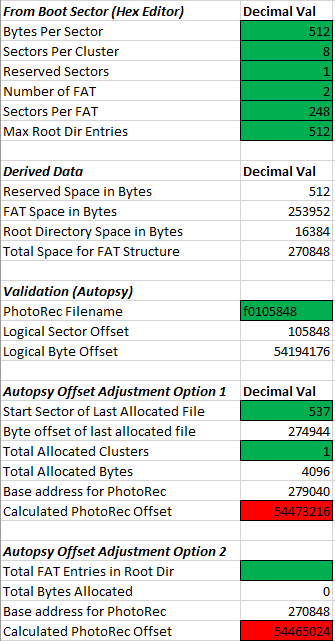
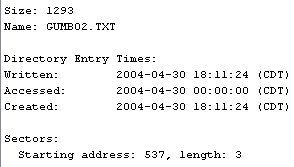
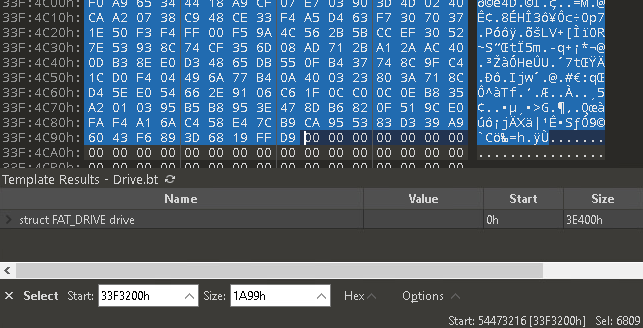
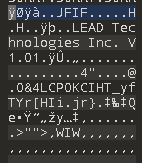
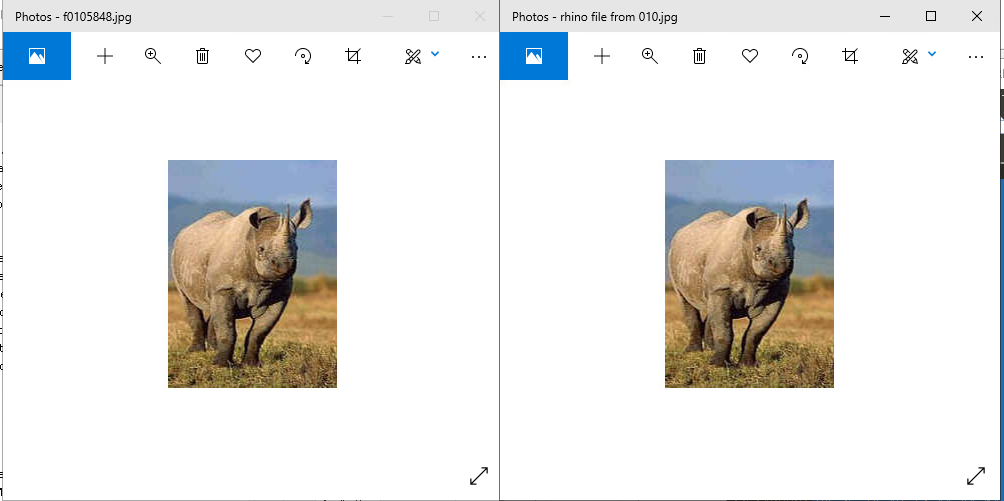
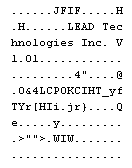
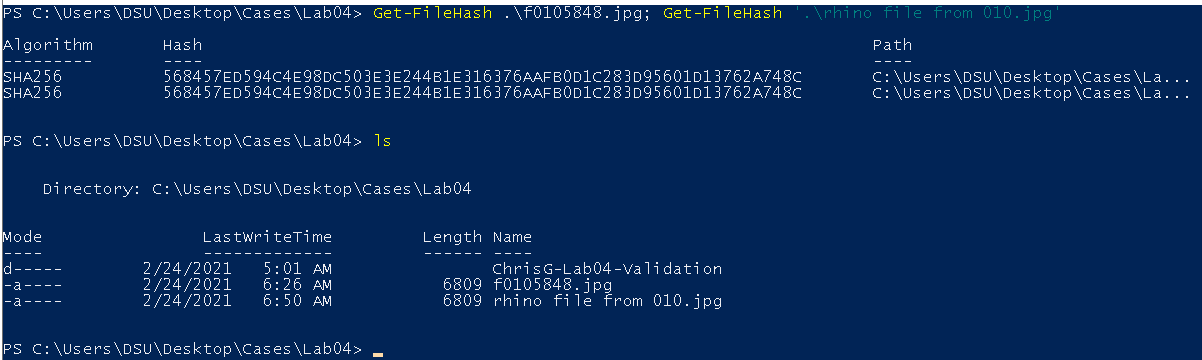
We will be using the vApp in the IA Lab labeled <username>\_CSC388\_Zwach\_Validate. There is a single VM called *Win10* that contains all tools necessary to complete the lab.

## Deliverables

A single new Word or PDF document containing:

* Screenshots of steps 3 - 7
* Responses to the prompts

## Lab Steps

1. Create a new case in Autopsy
   1. Case Name: YourName-Lab04-Validation
   2. Base Directory: C:\Users\DSU\Desktop\Cases\Lab04
      1. You'll have to create this directory
   3. Examiner Name: Your Name
2. Add the RHINOUSB.dd image as a data source
   1. Path: C:\Users\DSU\Desktop\Evidence\RHINOUSB.dd
   2. Time Zone: America/Chicago
   3. Processing Options: Default (Should be all ingest modules except Plaso)
3. After processing, review the deleted files shown in the tree view at left. Document your findings with a scree
4. Isolate one of the jpgs of rhinos - determine its location in the file allocation table
   1. The filename generated by PhotoRec should contain a logical sector number
   2. You can use the FATCalculator.xlsx workbook
   3. Provide a screenshot of your math (or the data in the worksheet)
5. Open the disk image in 010 hex editor and attempt to parse the FAT; provide a screenshot
6. Is the jpg present at the offset? Document the finding with a screenshot.
7. 
8. Extract the jpg from the RHINOUSB.dd image using 010. Hash the file with the PowerShell cmdlet *Get-FileHash*. Provide a screenshot of both that hash, and the file hash in Autopsy here.

## Writing Prompts

1. In your own words, describe how the process above validates the results from Autopsy.

by demonstrating the capacity to identify the exact location on disk of the files recognized by the tool we can prove the authenticity of the results it reports, eliminating the possibility of false positives (and any eliminate any claims against the evidences authenticity on account of hand-wavy technology magic).

1. Based on the tasks covered in this lab, how practical do you think it is to validate each artifact type with a hex editor? Would you generally validate this way or by comparing outputs of similar tools?

It is not very efficient to validate artifacts in this way, and unless the case required absolute confidence, or if any relevant files looked irregular – basically, if it’s not necessary, I would choose not validate them in this way.

## Notes

* Processing with autopsy should take a relatively small amount of time but consider starting processing and returning a few minutes later after a snack or a nap. The state of the vApp will be preserved if it is suspended.
* The log files for Autopsy modules can be useful (Help->Open Log Folder)
* The logical sector number and img\_offset returned by Autopsy **will** differ from the actual offset into the disk image since Autopsy only sends unallocated space to the PhotoRec module
* The *-Algorithm* argument to *Get-FileHash* in PowerShell can be used to select MD5 instead of SHA256
* The file *charlie-2009-12-07.E01* is included for analysis as well in the Evidence directory if you'd like to complete the Chapter 6 Hands-On Projects, but is not required for this assignment