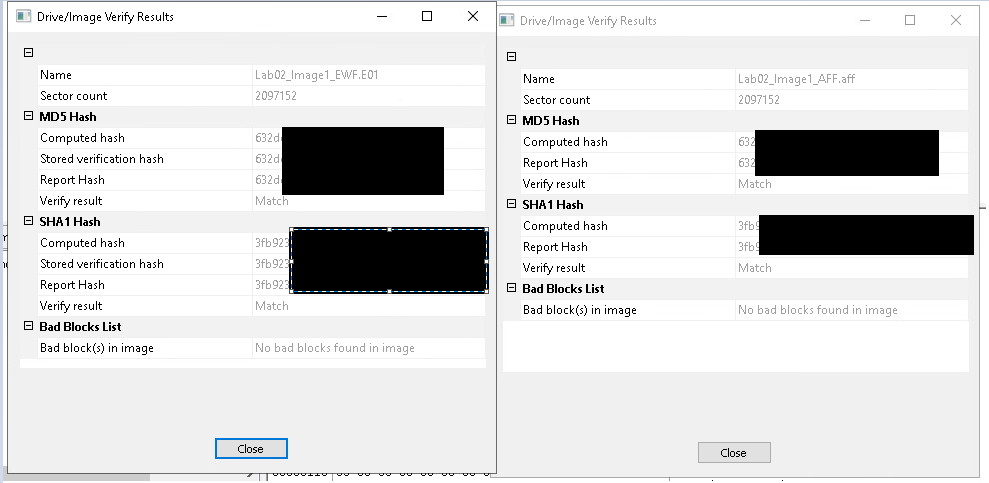
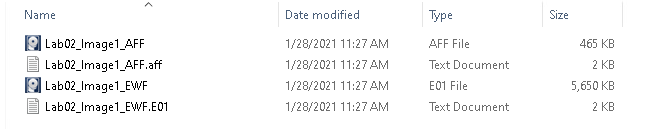
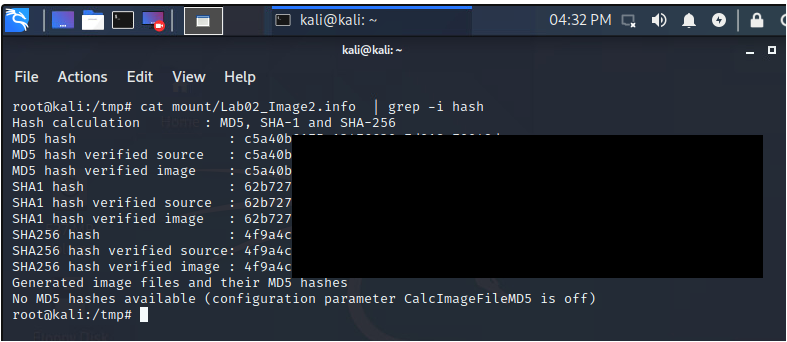
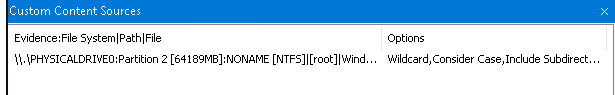
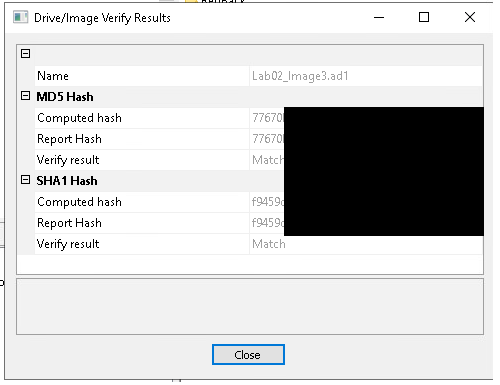
# Lab 02 – Acquisition

Our task in this lab is to demonstrate proficiency in capturing images using a few different techniques.

We will be using the vApp in the IA Lab labeled <username>\_CSC388\_Zwach\_Acquisition. You will find several VM’s there to simulate an environment where we can both capture on an analysis workstation and a subject device using a live disk.

## Lab Steps

1. Using FTK Imager on the Windows-Collection Workstation VM, capture a full physical image of the attached 1GB disk using both AFF and EWF formats.
   1. Provide one screenshot of the resulting hash verification (do not block out your hashes as I have; they’re hidden here to prevent screenshot reuse)  
      Ex: 
   2. Provide one screenshot of the images and their size  
      Ex: 
2. Start the Live Disk Target VM and start Kali Linux in forensic mode by inserting an ISO via Media/Insert Media. Then, capture a full physical EWF image of the ~512MB disk attached. (**Note:** you do not need to format the destination disk like we did in class; you do need to mount it)
   1. Provide one screenshot of the resulting hash verification  
      Ex: 
3. Collect a custom content image of the Windows-Subject Workstation VM targeting only the C:\Windows\System32\config directory
   1. Provide one screenshot of the CCI configuration  
      Ex: 
   2. Provide one screenshot of the resulting hash verification  
      Ex: 

## Writing Prompt

1. Do the hashes for the images from parts 1 and 2 match? Explain why or why not.

## Notes

Mounting a volume in linux is done with the **mount** command. You may have to create a directory to mount the volume to with **mkdir**. To run guymager or mount a volume you will likely need to be root; to switch to root from the terminal you can use **sudo -i**

The SIFT VM is included in the vApp but not required for the lab at all. Feel free to explore as you wish, but know it is not required to interact with it.