

Security Analysis, Techniques and procedures

Lab 4a

Wales Institute of Science and Art
Applied Computing
I.Q Building, Room 205
Swansea
SA1 8EW

Introduction

The Computer Forensics investigation is a methodological approach of preparing for an investigation, collecting and analyzing digital evidence. It is also managing the case from the reporting of the crime till the case's conclusion. The process takes place in a computer forensic lab.

Computer forensics plays a vital role in the investigation and prosecution of cyber criminals. The process includes acquisition, inspection, and reporting of information stored across computers and networks related to a civil or criminal incident. Forensic investigators are trained professionals who can extract, analyze, report, and investigate cases that involve technology as the source or the victim of a crime.

As a computer forensics investigator, it is important to have knowledge of the process involved during a forensics investigation, such as collecting digital evidence, building a computer forensics lab, recovering the deleted data, etc.

Task 1: Enable Write Blocking in a Windows computer

Use of write blockers is extremely important while attempting to create forensic images of the seized evidence devices.

Although this can be done in the software itself, it is highly advisable to use hardware write blockers that ensure maximum protection of the original evidence device from being manipulated.

The use of hardware write blockers is also a recommended and accepted part of the forensic imaging practice in the court of law.

In this lab exercise, we would be walking through the procedure for enabling write protection for any external storage media connected to a Windows computer through the USB port.

Step 1: Use Windows key + R keyboard shortcut to open the RUN command.

Step 2: Type **regedit** and click OK.

Step 3: Go to the following path

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

Step 4: Right-click the Control (folder) key, select New, and click Key.

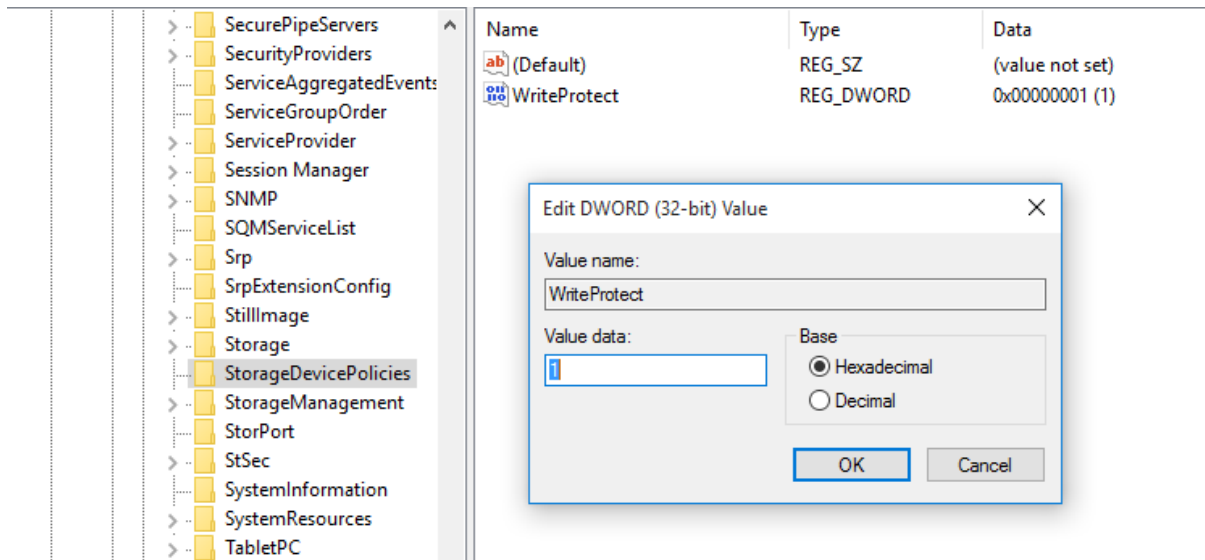
Step 5: Name the new key **StorageDevicePolicies** and press Enter.

Step 6: Select this new key, right-click on the right side, select New and click DWORD (32-bit) value.

Step 7: Name the new word as **WriteProtect** and press Enter.

Step 8: Double click the newly created DWORD and change its value from 0 to 1.

Step 9: Click OK and close the registry.



You may now try to plug in any external USB storage media and try to perform write operations (rename a file, paste a copied file, etc.), which would be denied and the USB device would be write-protected.

Task 2: Forensic Imaging

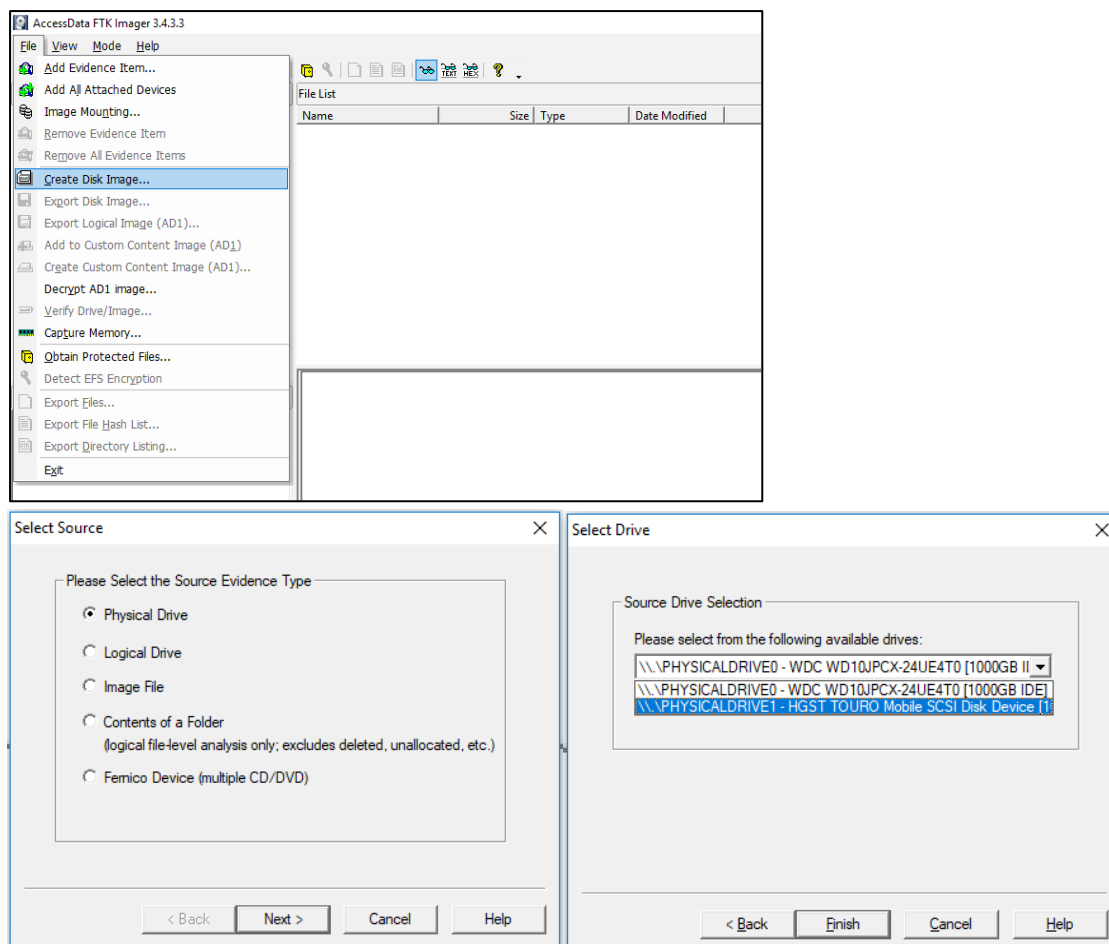
Forensic imaging involves creating a bit-stream image of the evidence device.

In this lab exercise, we would be using AccessData's FTK Imager software for creating a bit stream image of our external storage drive.

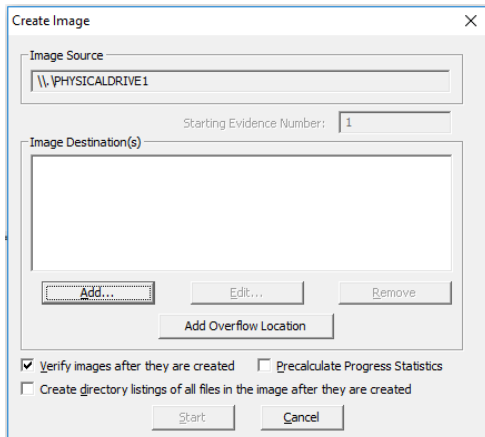
Step 1: Run FTK Imager.exe to start the tool.

Step 2: From the File menu, select "Create a Disk Image" and choose the source of your image.

NOTE: FTK Imager does not guarantee data is not written to the drive, so it is important to use a write blocker.

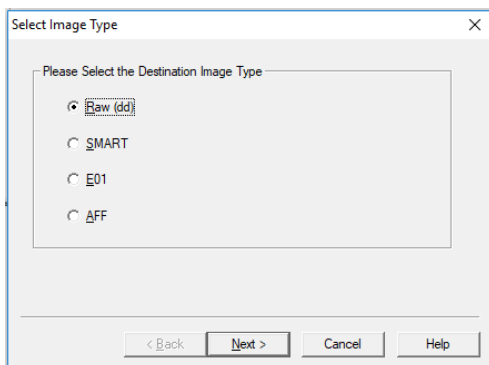


Step 3: Check “Verify images after they are created” so FTK Imager will calculate MD5 and SHA1 hashes of the acquired image.

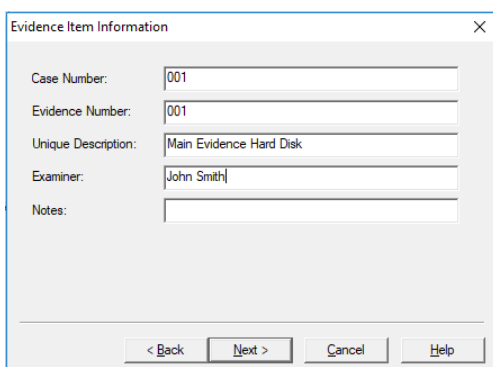


Step 4: Click “Add...” to add the image destination.

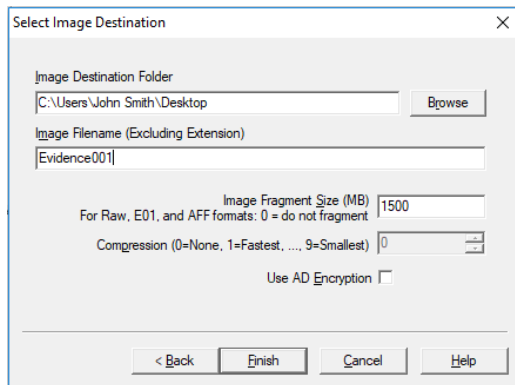
Step 5: Next, select the image type. The type you choose will usually depend on what tools you plan to use on the image. The dd format will work with more open source tools, but you might want SMART or E01 if you will primarily be working with ASR Expert Witness or EnCase, respectively.



Step 6: Next, you may choose to provide evidence information. If you select raw (dd) format, the image meta data will not be stored in the image file itself.

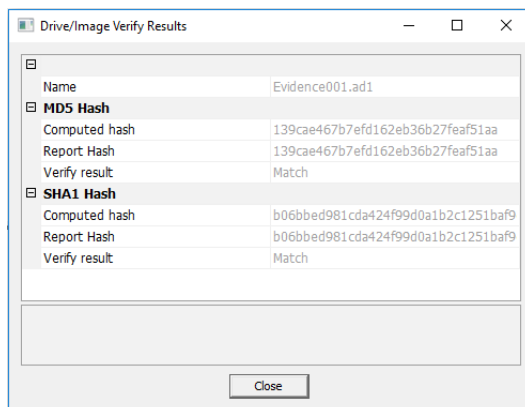


Step 7: Select the Image Destination folder and file name. You can also set the maximum fragment size of image split files. Click Finish to complete the wizard.



Step 8: Click Start to begin the acquisition.

Step 9: A progress window will appear. Once the acquisition is complete, you can view an image summary and the drive will appear in the evidence list in the left hand side of the main FTK Imager window. You can right-click on the drive name to Verify the Image.



Step 10: FTK Imager also creates a log of the acquisition process and places it in the same directory as the image, image-name.txt. This file lists the evidence information, details of the drive, check sums, and times the image acquisition started and finished.

Task 3: Verifying Image Integrity

Hash values are important indicators of genuineness and integrity of forensic images and other evidence data.

Although most imaging tools perform integrity checking by validating hashes of forensic images with the original evidence, it is necessary to check integrity of the evidence image with standalone hash calculation tools in cases where the image is moved to another computer or a copy of the image is made prior to analysis.

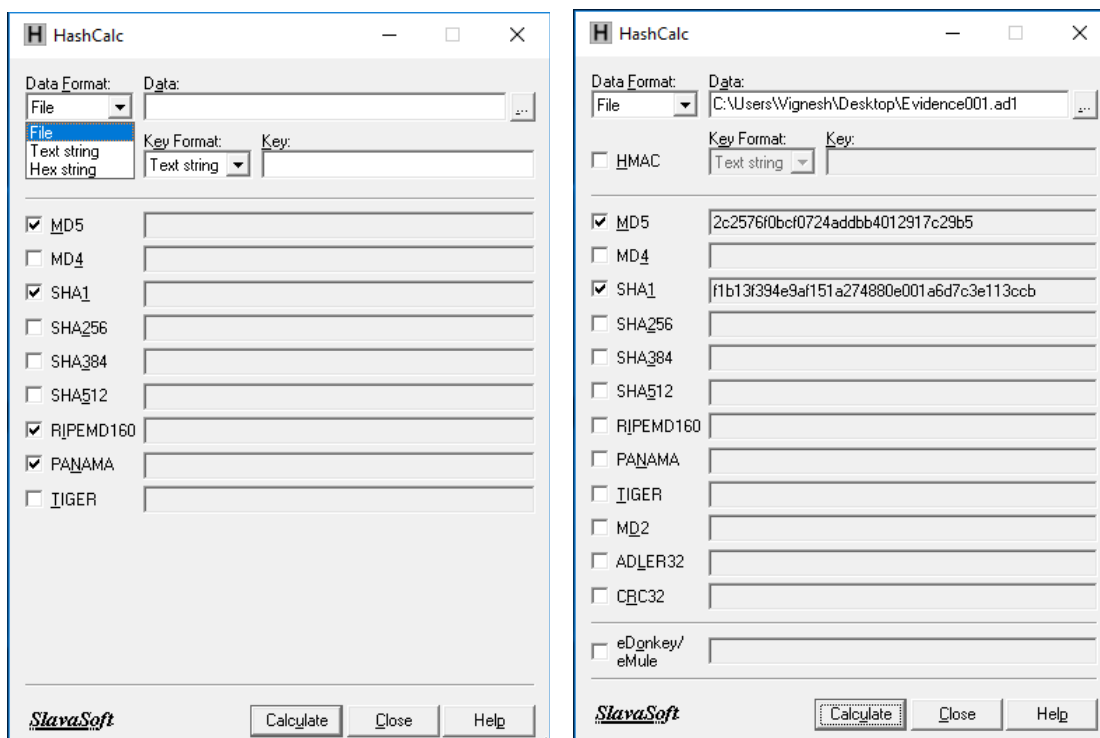
In this lab exercise, we would be using SlavaSoft's HashCalc software for verifying the hash value of a file located on your computer.

Step 1: Run HashCalc.exe to start the tool.

Step 2: Select the Data Format as "File..." from the drop down at the top-left corner of the application.

Step 3: Click the button labelled "... " next to the Data field and browse to the directory where your file is located. Select the file and click Open.

Step 4: Select the hashes which you wish to compute for the input file. In this exercise, we would be calculating the MD5 and SHA1 hashes for the image file. Press the Calculate button.



Step 5: Note the hash value and make some modifications to the file and save it. Now re-compute the hash value for the modified file and note this value. Note that hashes are one-way functions and their value changes even with the slightest modification in the file.

Step 6: Finally, revert back to the original file and undo all your changes to the file. Re-compute the hash value for the file and observe whether it is the same as the original hash value you observed.