# CIT 430/530 – Forensics Lab #1

## The Digital Forensics Process and Working with SIFT

In this lab you will work with the SIFT forensic workstation to familiarize yourself with the tool and gain experience with the ‘Collection’, ‘Examination’ and ‘Analysis’ phases of DFRWS framework, which is used to structure and organize the Digital Forensic process.

### DFRWS Framework: Collecting Data

Collecting evidence includes maintaining a chain of custody and creating a forensic copy of evidence to work with during the investigation. For the purposes of this lab, forensic copies of the files to be analyzed have already been made. Follow the steps below to begin the examination.

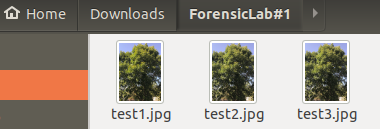
1. Power on your SIFT appliance and use the credentials below to login.

* Username: sansforensic
* Password: forensics

1. In the left menu bar, select the ‘Files’ button, open the ‘Downloads’ folder, then open the ‘ForensicLab#1’ folder.

Image of file folder location in left menu bar on SIFT workstation

1. Double-click the three test JPEG files to open them in ImageViewer.



* Are there any differences in the photos you can detect visually?
  + **From what I can tell, no there is no visual differences I can detect right off the bat.**

Image of button to select to view an images properties. 

1. Inside ImageViewer, select the button with three bars and scroll to ‘Properties’ at the bottom of the dropdown menu.

* Are there any differences in the data reported on the ‘General’ tab?
  + **In the general tab there was no differences located between the three pictures besides their names.**

### Analyzing Data

For each test JPEG file view the content under the ‘General’, ‘Metadata’ and ‘Details’ tabs to complete the table below. Be sure to expand any arrows to see all pieces of information.

|  |  |  |  |
| --- | --- | --- | --- |
| **File Name** | **Size (Width, Height, Bytes)** | **File Type** | **Time Stamp Information (original and digitized)** |
| **test1.jpg** | Width: 3024 pixels  Height: 4032 pixels  Bytes: 6.9 MB | JPEG | Original: **2019:08:03 17:45:29** |
| Digitized: **2019:08:03 17:45:29** |
| **test2.jpg** | Width: 3024 pixels  Height: 4032 pixels  Bytes: 6.9 MB | JPEG | Original: **2019:08:03 17:45:29** |
| Digitized: **2019:08:03 17:45:29** |
| **test3.jpg** | Width: 3024 pixels  Height: 4032 pixels  Bytes: 6.9 MB | JPEG | Original: **2019:08:03 17:45:29** |
| Digitized: **2019:08:09 19:15:29** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **File Name** | **Camera Make** | **Camera Model** | **Flash (on/off)** | **Image Creator** |
| **test1.jpg** | Apple | Iphone7 | on | N/A |
| **test2.jpg** | Apple | Canon | off | Phillip J. Fry |
| **test3.jpg** | BigSky | Iphone7 | on | Unknown |

#### Analyzing data with ExifTool

The ExifTool is a program commonly used in a computer forensic investigation to examine metadata from the command-line. The tool also allows metadata to be modified.

**Resources for ExifTool**

* <https://exiftool.org/sample_images.html> - image repository
* <https://exiftool.org/examples.html> ExifTool command line examples
* <https://metacpan.org/pod/exiftool> & <https://metacpan.org/pod/exiftool#WRITING-EXAMPLES> Reading and Writing metadata from ExifTool

Image if the terminal icon

1. Open a new terminal window by clicking the ‘Terminal’ button on the left menu.
2. Change to the ForensicLab#1 directory with the command below

**cd Downloads/’ForensicLab#1’/**

1. Use the following command to view metadata for Working.jpg

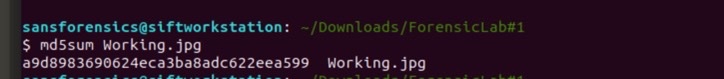
**exif Working.jpg**

1. Make note of the following values reported in the output

* Manufacturer
  + **Apple**
* Model
  + **Iphone 7**
* Flash
  + **Yes**
* XP author
  + **N/A**
* Copyright
  + **N/A**
* Date and Time stamps
  + Original: **2019:08:03 17:45:29**
  + Digitized: **2019:08:03 17:45:29**

1. Calculate a md5 hash for Working.jpg and make a note of its value

**Md5sum Working.jpg**

****

1. Modify Working.jpg using exif with the following commands:

* Change the camera manufacturer

**exiftool -m -make=Nikon Working.jpg**

* Change the camera model

**exiftool -m -model=D3500 Working.jpg**

* Turn Flash off

**exiftool -m -flash=off Working.jpg**

* Add an author

**exiftool -m -xpauthor=’your NKU ID’ Working.jpg**

* Edit the original date/time

**exiftool '-datetimeoriginal=yesterdaysDateTime' Working.jpg**

Ex: exiftool '-createdate=2020:02:13 14:30:26' test1.jpg

* Edit the digitized date/time

**exiftool '-createdate=todaysDateTime' Working.jpg**

Ex: exiftool '-createdate=2020:02:14 14:30:26' test1.jpg

1. Verify your changes using the exif command below, then calculate the md5 hash again. Provide a screenshot from both outputs.

**exif Working.jpg**

**Text

Description automatically generated**

**md5sum Working.jpg**

**Text

Description automatically generated**

### DFRWS Framework: Analyzing Data

At this point we have examined various files, used two different tools to verify metadata and experimented with one of the tools to further our understanding. For the purposes of this lab, imagine that the three test JPEG files were collected as evidence in a copyright infringement lawsuit and metadata from these files all report something different. We’ll need to examine the original file to obtain a better picture of events.

1. Use ImageViewer to open the Victim.jpg file and test JPEG files for a visual comparison. Next, use exiftool to view the metadata for the four files.

*Note: you may want to use a new terminal window to the view exif output for each image file.*

1. Calculate a md5 hash for Victim.jpg
   1. Text

      Description automatically generated with low confidence
2. Be sure to note any significant differences found between the files as you will need this information in the next section.
   1. **Time stamps**
   2. **Authors**
   3. **File modification**
   4. **File access date/time**

### DFRWS Framework: Presentation

This phase requires an investigator to report their findings and give an impression of the events that occurred. In other words, this is the part of the investigation where we explain what happened, how it happened and the proof we have verifying our interpretation of events.

1. Write 1 to 2 paragraphs addressing the following points:
   * If Victim.jpg is the original file, how was it determined that the test JPEG files were copies?
   * Describe the process someone could use to modify the test JPEG files.
   * As the forensic investigator for this case, do you think the actions performed on the test JPEG files are malicious? Why or why not?

I do think that the Victim.jpg is the original file, I figured out that the test JPEG files were copies due to looking at the difference between the file modification date/time, file access date/time, and file inode change in date/time. You can see the differences in times, and you can go back through all the files to fine the original dates and times of the original file which is the Victim.jpg. The process we can use to modify the test JPEG files is the exiftool -m followed by what you want to change in the file rather that be the model or camera type, etc. Followed by the file you would like to change. In my opinion as a forensic investigator, I do not think the actions done here were meant to be a malicious act. I feel as if this was a simple data editing for pictures and modifying simple subjects such as camera type. I was unable to find malicious content in which I think the images would cause harm to others, I do not see a problem with the content switch on the test files.