# Digital Forensics – Lab 04

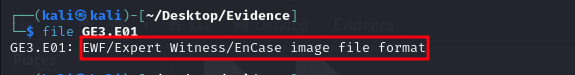
### Ahmad Abdullah i22-1609

## Introduction

In this Lab task, we used SleuthKit, a CLI version of the Autopsy program, to analyse Forensic images. This tool is faster for small images where we know exactly what we are looking for.

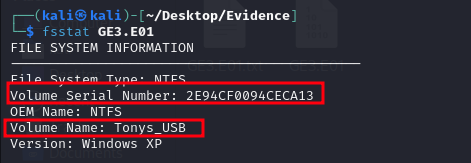
**Task#1: What is the Image File Format?**

Using *file* utility we find out that the file is of EWF format file. File utility tells s about the extension of a the given file.



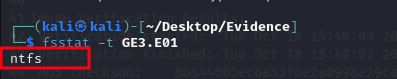
**Task#2: What is the Volume Serial Number and Volume Name**?

A good utility of sleuthkit is fsstat which tells us a good amount of information about the volume of the image file. Simply entering *fsstat image\_file* gives us the information we were looking for.



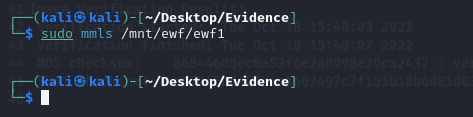
**Task#3: What is the File System Type? (e.g., FAT, EXT, etc.)**

Using same utility with flag -t which is used to get the image type specifically.



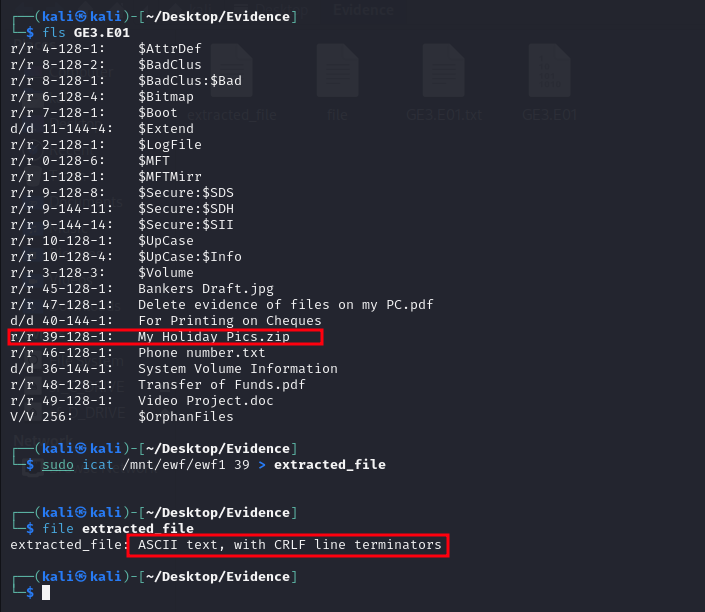
**Task#4: How many partitions are there?**

Since it shows us no output we assume that there are no partitions.



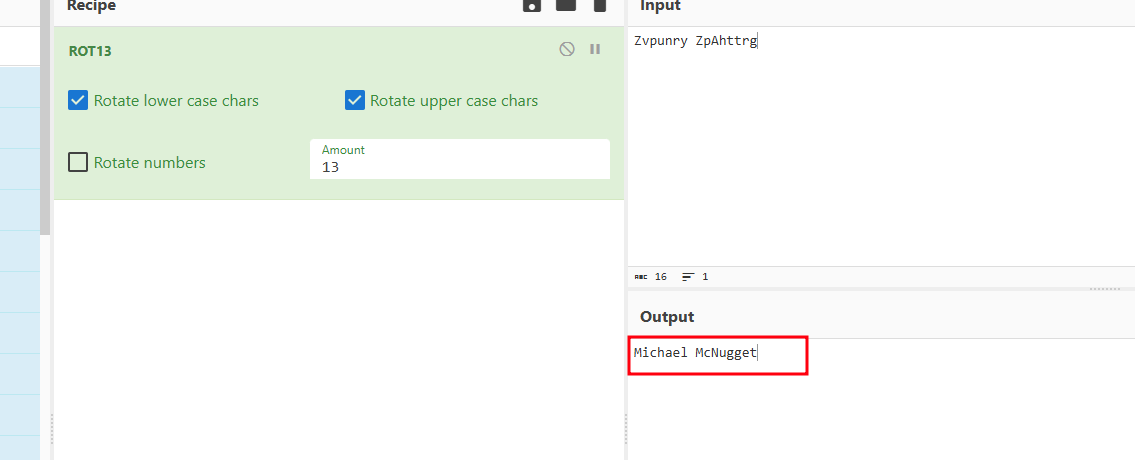
**Task#5: Name the file with a mismatched extension. Hint: Hexed.it and Gary are close friends who share a lot with me.**

The only file that had mismatched extension was My Holiday pics.zip which was actually a text file. We extracted it using icat util and used file utility to find its extension.



**Task#6: Use Cipher Identifier if you encounter any encoded text, such as &quot;kHrkn Bqqzon.&quot;**

The cipher text we found was in Phone Number.txt file and using ROT13 it gave us the actual person who it belonged to.



**Task#7: What is the password for the Password-Protected PDF? Hint: Hexed.it and the devil is in the details.**

Password of the protected pdf is: Catch me  
Using this we found the contents of the file

