Lab 06: Introduction to Single Purpose Forensic Tools

Lab 06 report Name: Kevin Ubilla

This Lab is extra credit for Unit 8. It is worth 15 points. The Challenge Flags are worth 2.5 Extra Credit points.

1. **Using Hashing Tools to Verify Integrity, Step 17.** You have obtained two MD5 hash numbers, one by doing a grep for MD5 of the **cat image.dd.001.txt** file, and the other by directly calculating it from **image.dd** via the md5sum command. Please capture both commands and both responses and past the capture(s) below.

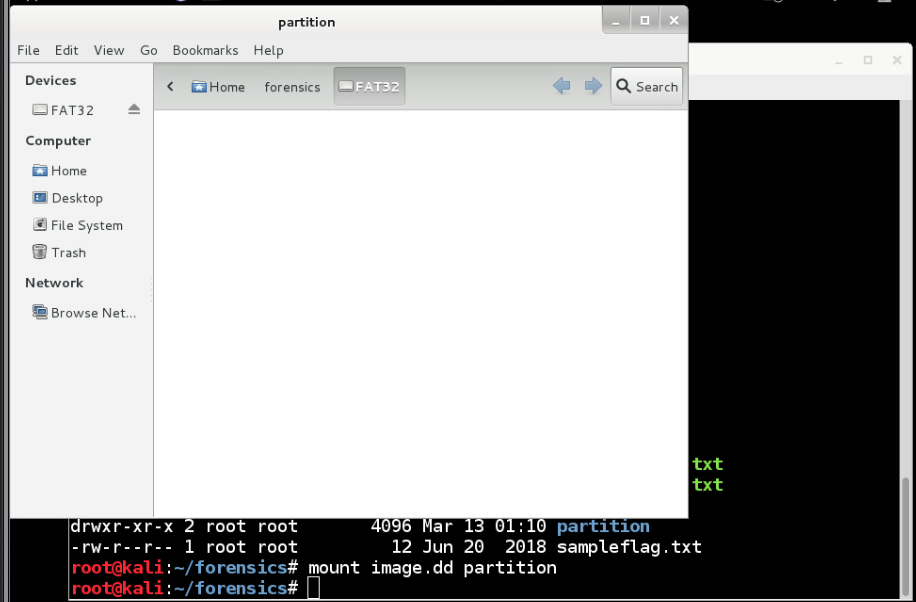
**→**Text

Description automatically generated **←**

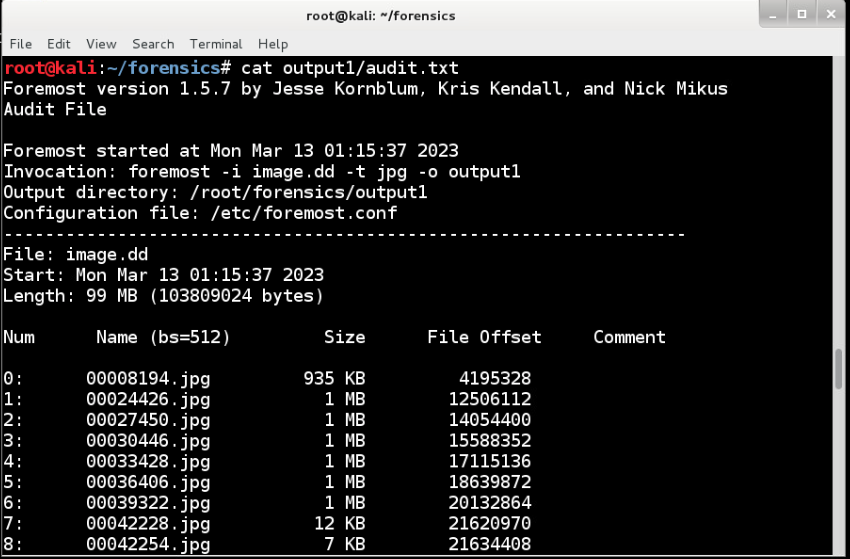
1. **Using Hashing Tools to Verify Integrity, General.** Which hashing algorithm is more accurate, MD5 or SHA1? (As usual, no more than 3 sentences, please.)

**→Sha1 is more complex because it uses 160-bit hashes, whereas MD5 uses only 128-bits. Thus, Sha1 has a higher degree of security. ←**

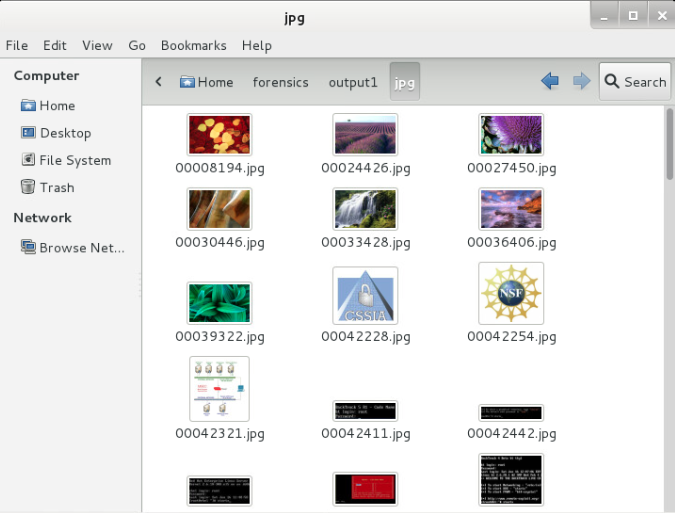
1. **Mounting a Partition with Deleted Files and Folders, Step 4.** You have mounted the image to the Partition Directory by typing **mount image.dd partition**. Please capture the window that summarizes the results below.

**→ ←**

1. **Using Foremost to Carve Files, Step 7:** You just succeeded in carving a number of JPEG files (83) from image.dd. Please list the files whose names you have displayed via the audit log, including the command and the first dozen files (give or take a few), below.

**→ ←**

1. **Using Foremost to Carve Files, Step 12:** Please capture the thumbnail versions of the first dozen or so JPEG files shown in the output1 folder and paste it below.

**→  ←**

1. **Using a Hex Editor, Step 6.** You have discovered that the JPEG files are marked internally with a JFIF file signature header. Why might this be an important feature for a forensic investigator to remember when searching for pictures on a drive? (As usual, please keep your answer to 3 sentences or less.)

**→ Detecting the JFIF header is important because it can be used to speed up search time by only focusing on and thus identifying those files that may be fragmented or needed as part of the investigation. ←**

**If you encountered any issues, either positive or negative, with this Lab, please let me know by commenting here. (This IS an experiment, after all.) I am tuning this according to what you say.**

**→ ←**