EXIF Analyzer: Synopsis

PROJECT NAME
EXIF Analyzer

DELIVERABLES
- exifAnalyzer.py

OVERVIEW
Digital images contain various pieces of metadata encoded in EXIF (Exchangeable Image File Format) headers that can be used to gain useful insight into the camera that is responsible for taking the picture. Additionally, with the proliferation of smartphones with GPS technology in today's society, images are typically geotagged when they are taken. Utilizing basic analysis and grouping techniques, it is possible to categorize images as belonging to a specific make and model of camera (or phone).

In the case of a forensic investigation, this information can be used to corroborate or disprove the whereabouts of an individual. Furthermore, it can be used to create a digital timeline for further analysis with the remainder of evidence.

OBJECTIVES
- Carve a disk image (dd) and place all files in an extraction directory to be further analyzed
- Ingest an entire directory and determine which images contain EXIF data
- Of the images that contain EXIF data, determine which images have been geotagged and group them by location
- Perform analysis of the images and group them into clusters based on location, manufacturer, model, software and time.
- Create CSV (Comma Separated Value), Database (SQLite), KML (Keyhole Markup Language), and KMZ (Keyhole Markup Compressed) files to allow the data to be further analyzed in other applications.

COMPILING
exifAnalyzer.py can either be executed directly from the command line using arguments, or imported via another Python script and instantiated.

DEPENDENCIES
- The Sleuth Kit (TSK) 4.0.2 is required if file carving is to be performed. If the script is only processing directories of pictures, TSK does not need to be installed.
- exifAnalyzer requires several non-standard Python libraries. They can be installed them with the following command:

```
$ pip install simplekml PIL pygeocoder sqlalchemy
```