Name: Perceptual Hash Calculator

Version: 1.0

Author: Yuming Chen [ychen54@gmu.edu]

File list: PHash.py, phash.jar

**Introduction**

This jython autopsy module can calculate perceptual hash value of jpg files in the data source with pHash algorithm. If there is an import of perceptual hash value, it also can calculate the difference between the import and other pictures' value, and look for similar pictures.

**1. Making Your Module Folder**

Every Python module in Autopsy gets its own folder. To find out where you should put your Python module, launch Autopsy and choose the Tools -> Python Plugins menu item. That will open a folder in your AppData folder, such as “C:\Users\username\AppData\Roaming\autopsy\python\_modules”.

Make a folder inside of there to store your module. Call it “PHashModule”. Copy the PHash.py and phash.jar into this new folder.

**2. Editing the Path of jar**

Open PHash.py with notepad.

Line 86: sys.path.append(r"D:\Files\Course\772\Final\phash.jar")

Please replace the file path in the parentheses with your real file path.

**3. Run the Module**

**a. Execute Autopsy**

**b. Load a case**

Since it's a data source ingest module, you can input any kind of case source, e.g. drive, image, folder.

**c. Run Ingest Module**

Tools -> Run Ingest Modules -> Check Phash Module -> Finish

**Tip:** You can choose if you want to look for similar pictures with a hash value or not. If you check to activate pHashToCheck, please enter a perceptual hash value in hex format into the input box.

**4. Get Output**

Help -> Open Log Folder

Open the latest autopsy.log file and you will see the output.

**Test Data**

Case Source: Folder TestData (Any image or folder contains pictures)

Check to activate pHashToCheck: Yes

Input Box: 90c8d0d24a2c166c

**Output Example**

INFO: Processing file: ETO3.JPG

INFO: ETO3.JPG:Path ==> D:\Files\Course\772\case\testfolder\Temp\Pictures\ETO3.JPG

INFO: ETO3.JPG:pHash ==> 90c8d0d24a2c166c

INFO: pHashToCheck ==> 90c8d0d24a2d160e

INFO: ETO3.JPG:Difference ==> 4

INFO: ETO3.JPG:Similar? ==> True