CIS/ECE 387 Fall 2018 Lab7

Due: **11/26/2018**

ACTIVITY: Hash Analysis and PhotoRec Carver with Autopsy

HASH DATABASE LOOKUP AND NIST NSRL

The Hash Database Lookup Module calculates MD5 hash values for files and looks up hash values in a database to determine if the file is known bad, known (in general), or unknown.

Autopsy can use the NIST NSRL to detect 'known files'. The NSRL contains hashes of 'known files' that may be good or bad depending on your perspective and investigation type. For example, the existence of a piece of financial software may be interesting to your investigation and that software could be in the NSRL. Therefore, Autopsy treats files that are found in the NSRL as simply 'known' and does not specify good or bad. Ingest modules have the option of ignoring files that were found in the NSRL.

To use the NSRL, you may download a pre-made index from http://sourceforge.net/projects/autopsy/files/NSRL. Download the **NSRL-XYZm-autopsy.zip** (where 'XYZ' is the version number. As of this writing, it is 262) and unzip the file.

SOFTWARE AND DOWNLOADS

In this activity, we will mainly use the Hash Database Lookup Module and PhotoRec Carver Module in Autopsy.

- Autopsy Hash Database Lookup Module User's Guide
- Autopsy PhotoRec Carver Module User's Guide

Download the images files, CBARROW.E01 and CBARROW.E02, on canvas under the Files->Labs->Lab7 folder.

INSTRUCTIONS

1. Launch Autopsy and create a case, Create New Case and name it as “Hash Analysis”.
2. Add data source type: choose *Disk Image*; browse and select the path to "CBARROW.E01".
3. In the *Ingest (processing) modules* window, uncheck all modules except the “Hash Database Lookup Module” and “PhotoRec Carver Module”;
4. Click “Hash Database Lookup Module” and the click *Global Setting*.
5. At the “Global Hash Lookup Setting” window, click “Import Hash Set”, open your downloaded NRSL hash set index file (.idx), and check the “Known” option under the Type of Hash Set.
6. Click “New Hash Set” and then input “BadPictures” in the name field and choose a “Hash Set Path”, and, and check “Notable” type, and check “send ingest inbox messages for each hit”.
7. Click “OK”; and click “Add Hashes to Hast Set” and then copy and paste the following MD5 hashes

   ```
   7d97aa329fe261c90bf68ee4104d4b85
   74a61bd54942d7e68fa0748e29dae219
   324c5372431efb4e01aa4849f3f0cb18
   2f649e8bb4ac958fd9ae8295da15200a
   a58012d0bc57365fd58e975761fca8b9
   ```

8. Click “OK” twice; click *Next* and then click *Finish*.
9. Review the search results under Results > Hashset Hits > BadPictures, and find all the hits.
10. Click and Open “Timeline” window, select “List” view mode, and review some known files.

Report

Your report should include the activity log (the steps you take or the commands you run) with some screenshots and/or outputs, and a brief reflection on what you learned (one or two paragraphs).

Please submit your lab report to Canvas under the “lab7” assignment folder. Each group just submits one report.