**CIS-387: Digital Forensics (4 credits)**

**With Dr. Jinhua Guo**

**Lab 7 - National Software Reference Library (NSRL) Hash Analysis**

**Demetrius Johnson**

**November 16, 2022**

# INSTRUCTIONS

## Downloading NSRL index file from <http://sourceforge.net/projects/autopsy/files/NSRL/>:

Graphical user interface, text, application, chat or text message

Description automatically generated

# 1. Launch Autopsy and create a case, Create New Case and name it as “Hash Analysis”.

Graphical user interface, text, application

Description automatically generated

# 2. Add data source type: choose Disk Image; browse and select the path to "CBARROW.E01".

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

# 3. In the Ingest (processing) modules window, uncheck all modules except the “Hash Database Lookup Module” and “PhotoRec Carver Module”;

Graphical user interface, application

Description automatically generated

# 4. Click “Hash Database Lookup Module” and the click Global Setting.

Graphical user interface, application, Word

Description automatically generated

# 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.

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

# 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”.

Graphical user interface, text, application

Description automatically generated

# 7. Click “OK”; and click “Add Hashes to Hash Set” and then copy and paste the following MD5 hashes:

1. 7d97aa329fe261c90bf68ee4104d4b85
2. 74a61bd54942d7e68fa0748e29dae219
3. 324c5372431efb4e01aa4849f3f0cb18
4. 2f649e8bb4ac958fd9ae8295da15200a
5. a58012d0bc57365fd58e975761fca8b9

Graphical user interface, application, Word

Description automatically generated

Graphical user interface, text, application

Description automatically generated

# 8. Click “OK” twice; click Next and then click Finish.

Graphical user interface, text, application

Description automatically generated

# 9. Review the search results under Results > Hashset Hits > BadPictures, and find all the hits.

Graphical user interface, application, Word

Description automatically generated

## It appears that 5 out of 6 hashes from BadFile Hash set has made a hit:

Text

Description automatically generated

Graphical user interface

Description automatically generated

Graphical user interface, application

Description automatically generated

A picture containing text, tree, screenshot

Description automatically generated

Graphical user interface

Description automatically generated with medium confidence

A picture containing text

Description automatically generated

Notice this last file is the same file as the first file; they are exact matches, they just have different meta data (such as filename for example).

# 10. Click and Open “Timeline” window, select “List” view mode, and review some known files.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

## So I have noticed if I filter the timeline by \*must include hash hit\*, it only shows 1 file (and different times the file meta data was updated). It is the raisedenoten.jpg file. The other files that had hash hits as seen in Analysis results did not show up in the timeline.

Graphical user interface, text, application

Description automatically generated

## So I checked the meta data for the other files I was expecting to show up, since they are indeed hash hits. Turns out, it cannot appear on timeline because the meta data shows that for the other 5 hash hits they do not have any data modified/accessed/created times. The files may have been corrupted or purposely the metadata was deleted/nulled.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text

Description automatically generated

# Summary/Reflection

Overall, I have gained a very valuable skill using the Autopsy digital forensic tool. Now, if I have a machine that has poor performance and I suspect that there may be a virus on the machine, I can capture an image of my entire disk drive and hash all files. Then, I can use the NSRL hash database set to compare to all of my files. The analysis done by the tool will automatically give me hash hits so that I can know if and which kind of known bad file is on my machine! Then I can proceed to the path of that hash hit on my actual machine that I made the disk image copy of and delete/remove the file/program! In essence, this lab helped me to be able to conduct digital forensic audits using the Autopsy tool more effectively and added to my knowledge of the use of the tool, and it has enabled me to do an autopsy of any of my everyday personal devices or for the devices of someone else to scan for viruses in a very effective, safe way (especially because the image file is read only as per the digital forensic software design).