CIS/ECE 387 Fall 2018 Lab6

Due: **11/19/2018**

ACTIVITY: KEYWORD SEARCH WITH AUTOPSY

REGULAR EXPRESSION

A regular expression, regex or regexp, is a sequence of characters that define a search pattern. Usually this pattern is used by string searching algorithms for "find" or "find and replace" operations on strings, or for input validation.

To explore the regular expression and keyword search features available in Autopsy, we will create a new case and add a logical evidence file named “GREP-Examples.txt”.

Your job is to perform keyword search from a given keyword list and highlight all the matches on the evidence file.

SOFTWARE AND DOWNLOADS

In this activity, we will mainly use the Keyword Search module in Autopsy.

- Autopsy Keyword Search User Guide

Download the logical evidence file, GREP-Examples.txt, the keyword list file, GREP-Keyword-List.txt, and the regular expression instruction file, GREP_Operator.pdf, on canvas under the Files->Labs->Lab6 folder.

INSTRUCTIONS

1. Launch Autopsy and create a case, Create New Case and name it as “Regular Expression Keyword Search”.
2. Add data source type: choose *Logical Files*; browse and select the path to "GREP-Examples.txt".
3. In the *Ingest (processing) modules* window, uncheck all modules except the “Keyword Search”;
4. Click “Keyword Search” and then click *Global Setting*.
5. At the Global Keyword Search Setting window, click “new list” and input the “GREP” as the list name.

6. Click “New Keywords” and then copy and paste the keyword list from the “GREP-keyword-list.txt” file, and check “regular expression” button.
7. Click “OK” twice; click *Next* and then click *Finish*.
8. Review the search results under Results > Keyword Hits > GREP, and find all the matches.

Report

Your report should include the activity log (the steps you take or the commands you run) with some screenshots and/or outputs, **highlight all the matches in the logical evidence file (GREP-examples.txt) and embedded it in the report**, and a brief reflection on what you learned (one or two paragraphs).

Please submit your lab report to Canvas under the “lab6” assignment folder. Each group just submits one report.