CFRS 772: Forensic Artifact Extraction
Final Project

1. **Write a Python module or modules to meet the following requirements:**
   i. You may provide a new forensic capability, extend an existing capability, or replicate (in function only) an existing capability.
   ii. Your solution must integrate with Volatility or Autopsy; integration with other open source tools, or a non-integrated solution, must be pre-approved by the instructor.
   iii. Your solution must include:
      1. appropriately commented source code
      2. solution documentation (e.g., a README.txt file)
         a. how it works
         b. instructions for loading and running under Volatility or Autopsy
         c. how to use it (parameters, etc.)
         d. how to test it
      3. sample data with which to test your solution
2. **Sources for ideas:**
   i. Past Autopsy plugin contest submissions and winners:
      http://www.osdfcon.org/2015-event/2015-module-development-contest/
      https://www.osdfcon.org/2016-event/2016-module-development-contest/
      https://www.osdfcon.org/2017-event/2017-module-development-contest/
      https://www.osdfcon.org/2018-event/2018-module-development-contest/
   ii. Autopsy feature requests:
      https://github.com/sleuthkit/autopsy/labels/Feature%20Request
   iii. Past Volatility plugin contest submissions and winners
      http://www.volatilityfoundation.org/#!2013/c19yz
      http://www.volatilityfoundation.org/#!2014/cjpn
      http://www.volatilityfoundation.org/#!2015/c1qp0
      https://volatility-labs.blogspot.ca/2016/12/results-from-2016-volatility-plugin.html
      https://volatility-labs.blogspot.ca/2017/11/results-from-5th-annual-2017-volatility.html
      https://volatility-labs.blogspot.com/2018/11/results-from-annual-2018-volatility-contests.html
   iv. Volatility plugins
      https://github.com/volatilityfoundation/community
   v. TSK module ideas (would implement as plugins for Autopsy; dated, but maybe useful)
      http://sourceforge.net/p/sleuthkit/mailman/message/29501339/
      http://sourceforge.net/p/sleuthkit/mailman/message/32037509/
   vi. Open lists of forensics ideas:
      http://www.forensicfocus.com/project-ideas
      http://www.forensicswiki.org/wiki/Research_Topics
   vii. Class lectures, labs, and homework.
3. **Rubric (35 points total):**

(0-5 points)	Milestones
(0-10 points)	Installs and runs cleanly
(0-10 points)	Quality of documentation
(0-5 points)	Works on test data, works on other inputs, robustness
(0-5 points)	Presentation