CFRS 772: Forensic Artifact Extraction
Homework 11

1. **Complete the Autopsy Data Ingest Module writing tutorial:**

   - Link to the tutorial:

     http://www.basistech.com/python-autopsy-module-tutorial-2-the-data-source-ingest-module/

   - Notes:
     - We did tutorial 1 (File Ingest modules) as a lab in class; this homework is to do the 2nd tutorial on DataSource Ingest modules
     - The first part of the tutorial talks about "the database". There are two databases related to the tutorial: the Autopsy central database (the Autopsy "BlackBoard") and the SQLite database you are extracting from the data source (the tutorial isn't always clear about which one it is referencing, but you can probably tell from context).
     - Note the links to source code in the tutorial - you do not need to do significant manual code entry.
     - The GitHub link in the tutorial to the sample database is broken; the correct link is below (the sample Python scripts and EXE file are here too):

       https://github.com/sleuthkit/autopsy/tree/develop/pythonExamples/Aug2015DataSourceTutorial
       https://github.com/sleuthkit/autopsy/tree/develop/pythonExamples

     - If you're not familiar with Autopsy, there is a decent quick start guide at the link below.

       http://sleuthkit.org/autopsy/docs/user-docs/4.10.0/quick_start_guide.html

2. **Complete the Volatility plugin tutorial:**

   - Link to the tutorial:

     https://gist.github.com/bridgeythegeek/bf7284d4469b60b8b9b3c4bfd03d051e

   - Notes:
     - Use vm.mem from class for your test data

3. **Submit your two final Autopsy Data Ingest modules and your final Volatility plugin to BlackBoard as a single zip file called hw11.zip (name the modules per the tutorials) <u>and</u> (also in BlackBoard)**

   a. A screenshot of Autopsy showing your two modules in the checkbox list of modules to run when you process a data source.
   b. Two screenshots showing the output (in Autopsy) after running your modules (one screenshot for each module from Tutorial 2 - one for the database module and one for the executable module).
   c. A screenshot or copy/paste of the output when you run your Volatility plugin.