CFRS 772: Forensic Artifact Extraction
Homework 8

1. **Write a module as follows...**
   - i. Call the module hw8.py
   - ii. The module should have two functions:
     1. retrieveJPG
        - a. takes a url (string) as input
        - b. retrieves the data (file) indicated by the url
        - c. returns the retrieved data as bytes
     2. checkAppended
        - a. takes a block of data (bytes) as input
        - b. checks the data for anything after a terminating 0xFFD9
          - i. check the data <u>header</u> for JPG; if not, then exit with error message
          - ii. if JPG header is ok, then go to end of data and read backwards:
            1. if last two bytes are 0xFFD9, then return b'' (two single quotes, i.e., no bytes)
            2. if last two bytes are not 0xFFD9, then return all data (as bytes) after the last 0xFFD9 (so read backwards until you do find 0xFFD9)

2. **In your main code:**
   - prompt the user for a url
     - o files are located at http://www.xbit.cc/images/fileN.jpg (where N is 1, 2, or 3)
   - call function retrieveJPG
   - use the returned data to call function checkAppended
     - o if no bytes are returned (no appended data), then print a message to that effect: "no bytes after JPG trailer".
     - o if any bytes are returned, then print a message to that effect ("bytes found after trailer") and write the bytes to the local file fileN.jpg.appended (where N is 1, 2, or 3). Use the input URL to extract the filename being checked, and use that filename to construct the local file to which you are writing any found bytes.

3. **Check your code using HxD**
   - files are located at http://www.xbit.cc/images/fileN.jpg (where N is 1, 2, or 3).
   - view the image files as hex and check headers and go to the end of the files to look for appended data.

On BlackBoard, submit your Python code as a zipped version of hw8.py. In the comments section on BlackBoard, summarize the results for the three files, e.g.,

file1: (not jpg, found trailer data, or no trailer data): data (if any was found)

file2: (not jpg, found trailer data, or no trailer data): data (if any was found)
file3: (not jpg, found trailer data, or no trailer data): data (if any was found)

If trailer data is found, include the found data in your comments summary.