CFRS 772: Forensic Artifact Extraction
Homework 10

1. **Write a module as follows...**
    i. Call the module hw10.py
    ii. The module should have four functions:
        1. isBmp
            a. takes a filename as input
            b. returns TRUE if file is BMP, FALSE otherwise
        2. isTxt
            a. takes a filename as input
            b. returns TRUE if file is plaintext, FALSE otherwise
        3. isKeylog
            a. takes a filename as input
            b. returns TRUE if data might be keylogger data, FALSE otherwise
        4. isProcessMonitor
            a. takes a filename as input
            b. returns TRUE if data might be process monitor data, FALSE otherwise
        5. isScreenshot
            a. takes a filename as input
            b. returns TRUE if data might be screenshot data, FALSE otherwise

2. **Notes:**
    - you can assume that the keylogger, process monitor, and screenshot tools used are those from class (where the output is written to a file)
    - only call the #3 - #5 isX functions if the filetype is a match for that type of monitor
        - e.g., if isBmp is true, then call is Screenshot
        - e.g., if isTxt is true, then call isKeylog and isProcessMonitor
    - checking that a file is plaintext is tricky; I'm just looking for "good enough" here
        - maybe count ASCII characters as percent of total chars? (feel free to google for code snippets to do this – it's not as trivial as it sounds; be sure to attribute any code that is not yours – in a comment is adequate).
    - you can write a wrapper to run through the 20 files automatically (see below re: the 20 test files)
    - think generally but creatively
    - file (header byte) signatures at: https://www.garykessler.net/library/file_sigs.html

3. **Check your code using HxD**
    - view the files as hex, check headers, check content, and check in default viewer for that type

On BlackBoard, submit your Python code as a zip file containing your program named hw10.py. In the comments

section on BlackBoard, summarize the results for the three file types, e.g., which files (by number 1-20) are:

keylogger data: file numbers...
proces monitor data: file numbers...
screenshot data: file numbers...
none of the above: file numbers