***Guidelines/Tips for Creating Computer Forensics Project***

* Develop a plan/back up plan for each hidden item. For example: If your initial plan for an item is to create a Word document and then manually change the file header, make a backup plan that doesn’t include Microsoft Office (i.e: wordpad). This will prevent you from having to come up with replacement items on the spot.
* If using steganography on an item:
1. Do not use 3rd party downloaded tools (Students should not have to download software to decrypt file).
2. A website may be used. (Example: <https://www.mobilefish.com/services/steganography/steganography.php> )
3. If a password is used to encrypt the hidden message, ensure the password is able to be found (could be its own clue).
* Document & screenshot each hidden item you successfully create, so you will already have the hidings report material for your presentation.
* Using forensic tools to create hidden items is a good idea. (ie: using hex editor to shift bits in a file, instead of using a 3rd party tool, this ensures the file is made how you intended)
* Before submitting the project, open a copy of it with forensic tools to ensure that all material that is meant to be hidden is actually hidden, and no unwanted clues are present (ie: Files you meant to be genuinely deleted are not still there)