**Project Release Week 4 Due week 7.**

**Background**

You have been called to consult on a potential intrusion analysis case. The company is concerned the system was used for some illegal activity were the user accessed confidential files that the user was not supposed to access The system has two user accounts which are the main suspects involved in this case ("joker" and "IEUser"). Remember: SCREENSHOT OR IT DID NOT HAPPEN ;)

Using the sample report in this module as a guide, write a report of an intrusion analysis for. Your report does not need to be lengthy; however, your report should be thorough. Intrusion analysts will typically document positive and negative findings. Negative findings are frequently presented to rule certain activities out during an investigation. While we have covered many topics in this course, you are encouraged to perform additional research to augment your intrusion analysis just as you would in real-world situations.

The project is to be submitted in a Microsoft Word document. Please include your name in your project.

**Sample Report Format:**

* Attached is a sample report format. This report has been given to Stevenson University by the Defense Computer Forensics Laboratory (DCFL). The format has been modified for our use. The same report format will be used in Mock Trial (FSCOR 702) and Mock Intrusion (CYBF 710). For this project, you are not required to write a report that includes the Methodology section. (You must write a complete report in FSCOR 702 and CYBF 710.)

1. What is the hash value for the given forensic image?
2. Which user account was used to access some confidential documents?
3. Explain in detail what proof do you have to support your answer?
4. Did the user access the confidential files from a local drive or network location?
5. What proof do you have to support your answer?
6. List all the files that were accessed with full paths.
7. Provide two different evidence to prove that those files were truly accessed.
8. Which application was used to open any of the confidential document(s)?
9. The next three questions are related to the image with the text "AnotherPassword4U" found inside the user's home directory.
10. What is the full path to the files of interest?
11. What is the Volume Serial Number where the file exists?
12. What are the Modified, Accessed, and Creation (MAC) timestamps in UTC for the file?
13. The DCode.exe application was used by one of the users. Provide evidence to the next four questions below, but, be careful, this is a tricky question!!!
14. Which user do you think ran the application and what evidence do you have to support your hypothesis?
15. How many times was it used?
16. When was it last used?
17. Where was the application located (full path)?This is done so your results can be used in legal proceedings.