# ENPM687 – Digital Forensics and Incidence Responses

# Final Assignment

*Author – Syed Mohammad Ibrahim*

*UMD ID:* *iamibi*

*UID: 118428369*

*Email:* [*iamibi@umd.edu*](mailto:iamibi@umd.edu)

## Brief Summary of Information

The goal of this document is to go over the Rebel malware hard drive recovered by the Imperial Army. This report will outline the findings and the steps involved in achieving them. The malware has reportedly been connecting with its command-and-control center to transmit information that might cause problems to the Imperial Army. The investigation performed as part of forensics found the plans for the Death Star which can help the Rebel army to initiate a counterattack on Imperial Army.

## Tools Used in the investigation

* Autopsy
* WireShark
* VeraCrypt

## Repository

The following steps were involved in the forensics investigation which yielded the plans for the Death Star that were sent by the malware to C2:

1. The hard drive image provided was of windows XP. The image was loaded in the Autopsy, and it generated the file system hierarchy.
2. While traversing the directories in the “vol2”, I found that under “Documents and Settings/Administrator/Recent” there were a few interesting entries like “obiwan.lnk”, “obiwan2.lnk”. Also, there were a few files that said “plans” in their names like “the-official-rogue-one-death-star-plans-are-revealed.lnk”, etc.
3. Then I proceeded to traverse other folders and found the binaries named “obiwan.exe” and “obiwan2.exe” at the location “Documents and Settings/Administrator/My Documents/code/dist/”. These binaries were generated by the python package called pyinstaller as there were “spec” files present.
4. Along with the binaries, in a folder up, there was a source file called “obiwan.py” which contained the source code of the assumed obiwan.exe binary. However, there were two different binaries found, which questioned the piece of code legitimacy. The only way to confirm is to run them in an isolated environment and track their network calls.
5. The binary “obiwan.exe” was run in an isolated environment with WireShark monitoring the network traffic.

## Recommendations

## Challenges during investigation