**ZIP file of the image along with MD5 checksum:**

[https://umd.box.com/s/h4eheva4pxd2uunaujsddf2mo8i8ffcg (Links to an external site.)](https://umd.box.com/s/h4eheva4pxd2uunaujsddf2mo8i8ffcg)

**Investigation Background**

You are the Imperial Forces best forensic analyst. At a great cost the Imperial Army has come into possession of an image of a hard drive for a rebel scum malware writer. Their codes have plagued our computers for the last time, infecting them but also using it to send messages across the galaxy.

Your mission is to analyze the image of the Rebel malware writer hard drive. Find out what their newest “malware” does, any messages it may send out, and review the image for other useful intelligence.

**Your deliverable is a report of your findings covering:**

1 - Find the final version of the malware writer’s malware

2 - Determine what the message contained inside of the final malware is

3 - Find some other interesting items/artifacts/clues that are definitely **'relevant**' to the investigation that will aide the Imperial Forces. Include these in your report in order to get full credit.

4. - Describe two challenges or difficulties you had to overcome to complete the final project.

You can make this as short or as long as you feel is needed.  In the end I want to see what the message inside the final version of the malware is and anything else of interest you find along the way that is relevant the with the final version of the malware.  "For grading purposes I am a fan of short, sweet, and to the point".

\*\*\*Remember you are a Forensic Investigator that will deliver your findings so proceed from that mindset of clues and **include** relevant reasons why, behind your thoughts. Include **the individual steps** you took for each artifact. These are required to get full points.

**NOTE: THE MALWARE IS NOT ACTUAL MALWARE. I PROMISE.** It just sends some network traffic (for you to analyze) But if you want to be paranoid it’s always safe to run it inside a VM.

\*All screenshots should have your name visible in the screen content in original context such as a folder name or a case name

\*\*Include brief explanations of your thought process... why you chose a certain artifact to investigate, what stood out to you, etc...

\*\*\*An example Forensic report outline/format (4 main sections) can be found here: http://www.legalexecutiveinstitute.com/understanding-digital-forensics-report/

\*\*\*\*There is an opportunity for a few points extra credit from the final based on conciseness, originality, creativity and delivery.

\*\*\*\*\*Name the Autopsy case name for this project as your first & last name. Failure to due so will result in project failure. The case name should be visible in screenshots.

**Hints**

Get stuck?

Message me, I offer **TWO** free hints.

Additional hints are available but each one will cost you 5% from your final project grade.  I will verify with you that you are 100% sure you want an extra hint before I give one. But it is better to use an extra hint than not to finish.