# Forensics Final System Analysis – Lone Wolf

Your task for the final system analysis for this term is the Lone Wolf Scenario[[1]](#footnote-1). The image provided does not contain material that would be considered obscene or illegal but does contain some elements that may be alarming (gun violence). **The scenario is a work of fiction; the characters described within are fictional.**

## Scenario

Jim Cloudy is a resident of Alexandria, VA. He is unhappy with the media’s coverage of gun violence and what he perceived as an attack on the 2nd Amendment. Prior to the start of the scenario, Jim gets into a heated online argument with his brother, Paul Cloudy. During this argument Jim destroys his laptop by throwing it on the floor. Jim disposes of this laptop using his Apartment’s trash chute, which is collected daily. Paul gives Jim one of his old laptops with the promise that he wouldn’t break it. Paul wiped the laptop’s drive prior to giving it to Jim. Jim does not encrypt any data and takes no overt steps to obfuscate data.

The laptop has been seized by law enforcement after Paul Cloudy reported the odd behavior of Jim Cloudy and an image was captured with FTK Imager. You are receiving that image as evidence today.

## Analysis

Review the image either in the FTK platform provided by DSU (<https://vm.dsu.edu>), the vApp labeled *Artifacts*, on your local machine, or any combination of those. The disk images referenced as well as some tool reports are available from the originator of the scenario: <https://digitalcorpora.org/corpora/scenarios/2018-lone-wolf-scenario>.

**If you use the FTK analysis VM, please log out when you have completed your analysis to release the resources to the pool; we have 35 FTK licenses we all must share.** Your VM will reset 12 hours after you discontinue using it regardless of if you log out or not, so beware that progress will be lost if you leave the VM for too long.

Path to disk images in FTK VM: C:\LoneWolf\_Image\_Files (also a desktop shortcut)  
Path to disk images in vApp: E:\DiskImages

## Reporting

Your only deliverable for this task is a final report. Your format should be formal and consistent, but you need not focus on generating an imaginary company/law enforcement agency, titles, etc. A simple report, with the details of Jim Cloudy’s plan or other useful info from the machine is fine. You can include tool reports if you like as appendices. To get FTK reports from the VM via Horizon, you can navigate to D2L and use the locker function or consider using OneDrive, Google Drive, or so on. You will not be able to export artifacts from the vApp.

1. © 2018 Thomas Moore - <https://digitalcorpora.s3.amazonaws.com/corpora/scenarios/2018-lonewolf/Lone%20Wolf%20Scenario%20Copyright.pdf> [↑](#footnote-ref-1)