**CY5210 Case Study 3 Scenario**

**Overview**

The 2018 Lone Wolf scenario is a set of materials from a fictional seizure of a laptop of a fictional individual who was planning a mass shooting. In the scenario, the individual’s brother alerted the police regarding the increasingly concerning behavior of his brother. As a result of the alert, the police seized the brother’s laptop. The laptop was then imaged with the FTK Imager program.

**Background**

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.

Jim is currently unemployed and has trouble sleeping, so he sometimes spends odd hours on the computer. While officially unemployed, the scenario briefly alludes to his marihuana growing activities, and an amassed savings of $325,000. Jim becomes increasingly irate concerning the growing support for “gun-control”. Jim starts writing about his personal views and begins planning a “Lone Wolf” style attack. Jim wants to ensure his views are saved for posterity and his documents and plans can be accessed from anywhere; therefore, he uploads documents to a variety of cloud storage services. Prior to the planned date of the attack Jim gives Paul access to his cloud storage accounts. Paul is suspicious based on Jim’s sudden decision to go on vacation and not come back. When Paul reads some of the documents he notifies police and a Search Warrant of Jim’s apartment is executed and he is apprehended while talking to Paul online.

Jim’s plan was attack a town hall meeting scheduled from 12:30PM until 2:00PM on April 7th, 2018, at the Cascades Library, 21030 Whitfield Pl, Sterling, VA, 20165. The meeting was held to discuss solutions for gun violence and was attended by two U.S. Senators. Meeting Room B has a seating capacity of 130 people. After the attack, Jim planned to fly from Dulles International Airport to Bali Indonesia, where there is no current extradition treaty. Sometime after his arrival, he planned to release a “press statement” explaining his actions. Jim had no intention of ever returning to the U.S. and calculated he could live comfortably in Bali for nine years on savings alone.

**Considerations and Caveats**

It is difficult to control every aspect of a given scenario; however, creating an outline of the scenario’s desired progression was helpful. A detailed script was avoided which allowed for deviation based on real world events and real time search results. As an example, the location to be targeted was not known at the start of the scenario. Rather, it was developed during the scenario to replicate the research progression, scheduling, and decision making that would be necessary during a real event. Other considerations may include the use of paid services. For this scenario, the Amazon Web Services account was created on a separate computer to prevent credit card data from being leaked. However, the username and password for the account are stored within the image. Recovery of this information would allow a malicious actor to create virtual machine instances or use other AWS services at the expense of the cardholder. The public and private keys for the S3 bucket were also downloaded to the target machine during the scenario. With these keys, it would be possible to store large quantities of data, or host malicious files, again at the cardholder’s expense. Because of these facts, the AWS account was deleted after it was no longer needed to prevent misuse by third parties.

During creation of the scenario several instances of unintended data were produced. Some of these were not discovered until after the examination of the forensic image. For instance, soon after the scenario started, the screen began displaying typed text in Cyrillic for a short period of time. This was resolved by the “user” and is evident in the search history. As another example, the Jim Cloudy google account was created on a separate computer. This account was mistakenly left logged-in on that computer. During that time, several files were downloaded to the computer from another Google Drive. These file names appeared on the target image within “Users/jcloudy/AppData/ Local/Google/Chrome/User Data/Default/IndexedDB/https\_drive.google.com\_0. indexeddb.blob”, even though the target computer never directly interacted with those files. Finally, the license for Microsoft Office was associated with a real university email address.

Future work should consider the use of virtual machines (VM) for scenario creation. While the use of standard hardware eliminated artifacts associated with VMs, the 512GB SSD, and 16GB of RAM introduced the need to process null data. While this would be realistic considering the scenario user’s newly acquired computer and short run-time, it may be unnecessarily burdensome for some examination and testing situations.

**Scope**

A live acquisition of the laptop’s SSD and memory was conducted using FTK Imager Lite. There were three open windows at the time of acquisition.

* The Downloads folder, which displayed installation files for Box Sync, Dropbox, Backup and Sync, and S3 Browser. This folder also contained a Microsoft Excel spreadsheet name “rootkey”.
* The OneNote application, which displayed the contents of “Jim’s Notebook”.
* The Chrome Browser, which displayed the contents of the Google Doc, “Brother Chat”, which was being utilized as chat forum between Jim Cloudy and Paul Cloudy. In addition, the document’s built-in chat feature also displayed content between Jim Cloudy and Paul Cloudy.

Using the forensic techniques covered in this course, identify any documents, applications, and cloud syncing capabilities that provide details about the planning, timing and potential details of the mass shooting. Be sure to include the analysis of applications, the registry, browsing activity and associated metadata. Provide a chain of custody based on the FTK Imager log data and document your findings in a forensic case report template.