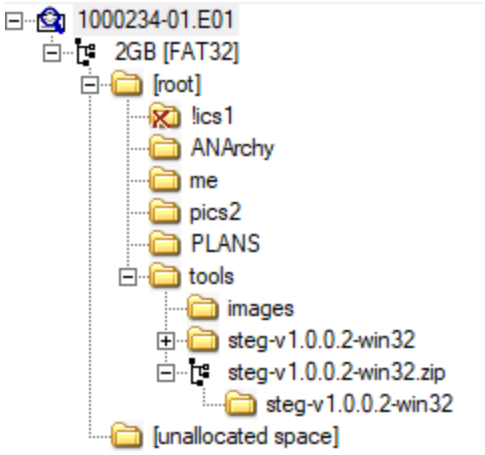
St. John's University

Final Project

Introduction to Digital Forensics/DFR 1001
John Benavides & Phillip Herman
Dr. Schmeelk
10 December 2019

The following is the documentation of the forensic report of a USB Drive that was given to us from the intake officer from the lab. Our objective is it find enough evidence to link the individual who was caught trying to sneak into St. John's University which eventually lead to a shootout with police. Tools used were FTK imager and Steg. When we looked deeper into the USB, we found a few different files in root. We found a few different files named !pics1, ANArchy, me, pics2 and PLANS. We also found the USB was 2GB[FAT32]. We can also see that the individual has stenography tools such as Steg which can indicate him using stenography or attempting to learn it. The following is the evidence that linked the individual to the crimes.



Evidence #1- 1ics1 Folder

In this folder we found multiple images of cats which is a known way for individuals to hide pornographic images of children. We then took the image and saved it from FTK Imager and imported into Steg to do a deeper analysis. After going each image, we didn't find any links to child pornographic to this individual. Image 1.1 and Image 1.2 are presented below.

Image 1.1- Files shown in Folder

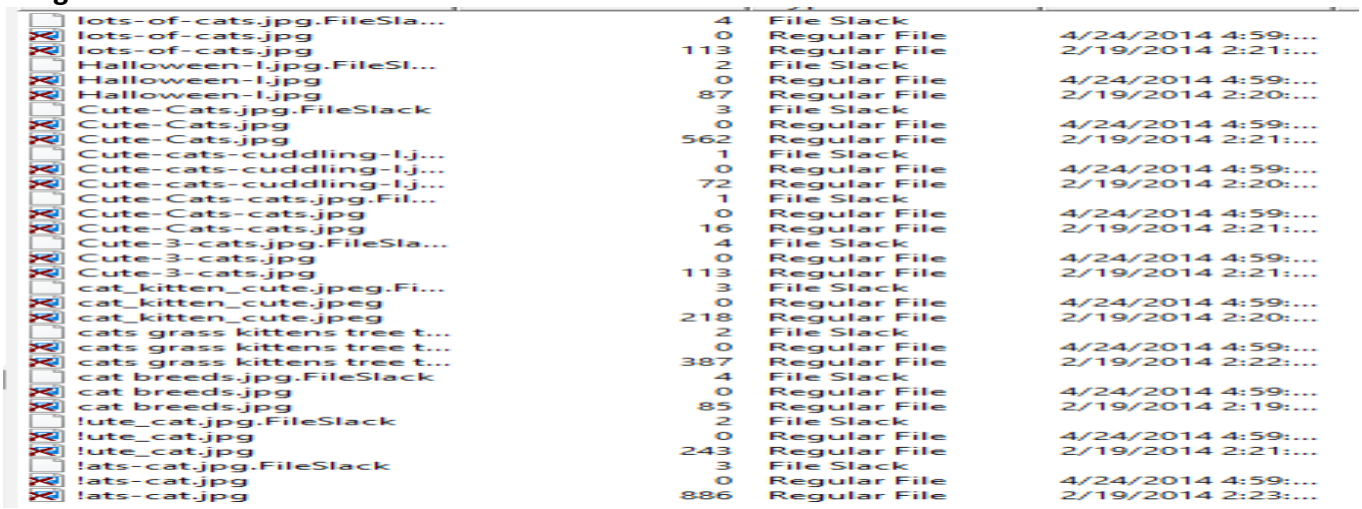
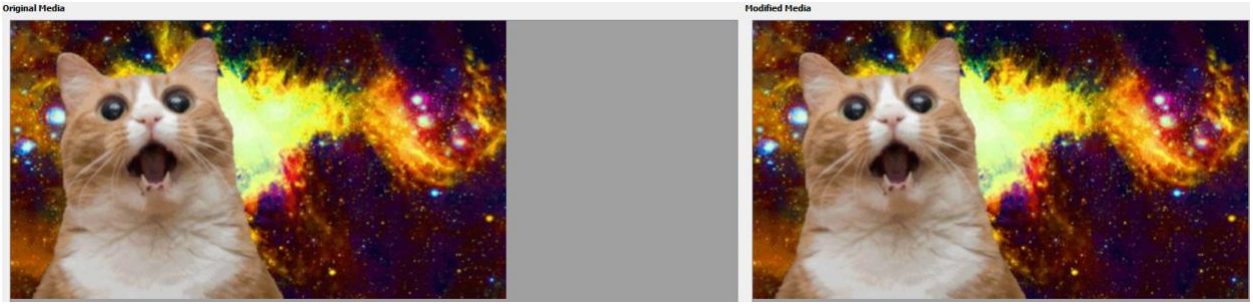


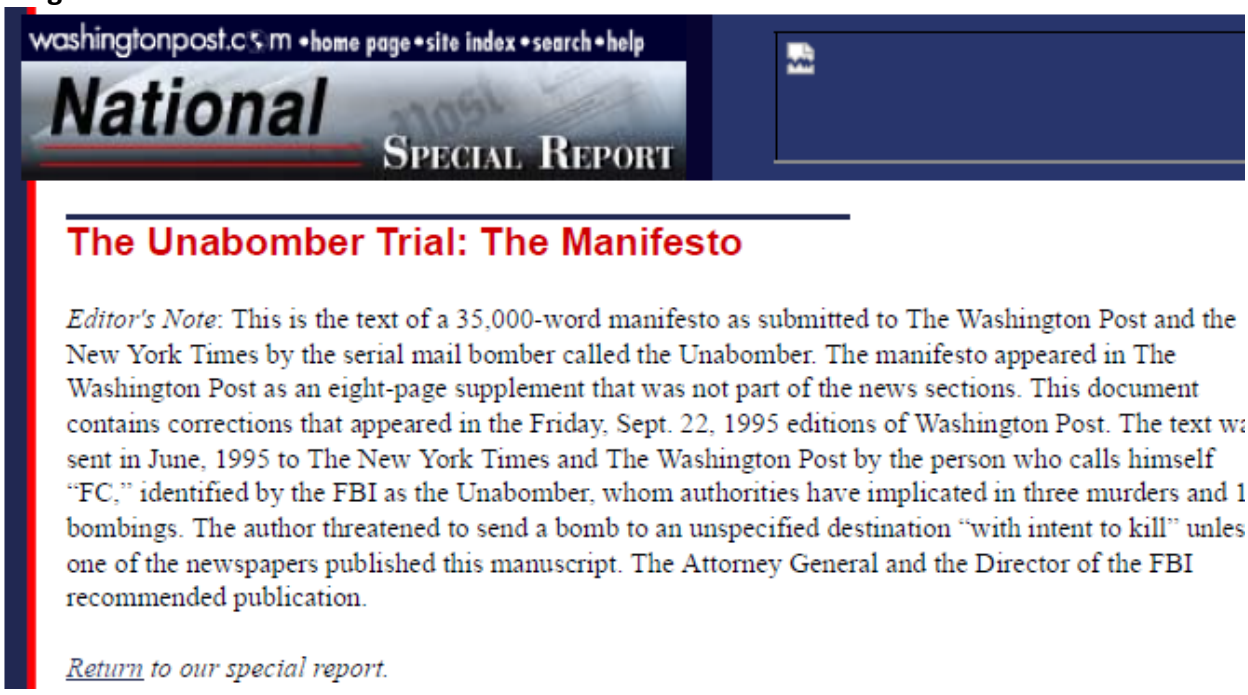
Image 1.2- Steg analysis



Evidence #2- ANArchy

In this folder we found documentation on acts that could be linked towards potential terrorist crime. Articles of trials of famous bombing attacks, Sarin gas attacks and how to make a bomb were some of the things found inside this folder. When I clicked on HOW TO MAKE A BOMB a video of a person explaining how to make a bomb started playing. We also found a word document titled Last Resort which was a letter from Christopher Jordan Dorner written to America. The document contained Christopher's thoughts on police and the hatred he had towards the American government. A book called AnarchistCookBook was also found in this folder which teaches an individual many different types of crimes including credit card fraud, generic bomb making and phone tapes. The amount of evidence found can link this individual towards potential terrorist attacks in the future. Image 2.1, 2.2, 2.3 are presented below.

Image 2.1- Article titled The UnaBomber Trial: The Manifesto


washingtonpost.com • home page • site index • search • help

National

Special Report

The Unabomber Trial: The Manifesto

Editor's Note: This is the text of a 35,000-word manifesto as submitted to The Washington Post and the New York Times by the serial mail bomber called the Unabomber. The manifesto appeared in The Washington Post as an eight-page supplement that was not part of the news sections. This document contains corrections that appeared in the Friday, Sept. 22, 1995 editions of Washington Post. The text wa sent in June, 1995 to The New York Times and The Washington Post by the person who calls himself "FC," identified by the FBI as the Unabomber, whom authorities have implicated in three murders and 1 bombings. The author threatened to send a bomb to an unspecified destination "with intent to kill" unles one of the newspapers published this manuscript. The Attorney General and the Director of the FBI recommended publication.

Return to our special report.

Image 2.2- Article on Sarin gas attacks in Japan

THE SARIN GAS ATTACK
IN JAPAN AND THE RELATED
FORENSIC INVESTIGATION

Image 2.3- Article on a man who attacked a Batman screening

Gunman turns 'Batman' screening into real-life 'horror film'

By **Michael Pearson**, CNN
updated 9:59 PM EDT, Fri July 20, 2012

Evidence #3- ME

In this folder we found images of a man who we believe to be Christopher Jordan Donnor. The images are a man holding a gun which appears to be an Uzi which carries 9mm ammunition which was the type of ammo found on the crime scene when he had a shootout with police. Image 3.1 and 3.2 are presented below.

Image 3.1- Gun selfie #1

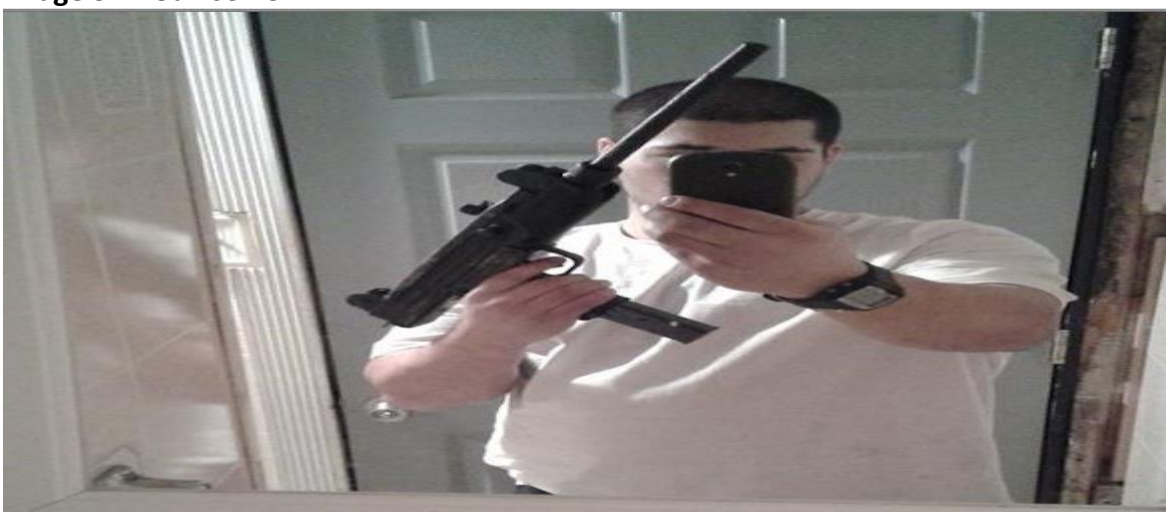
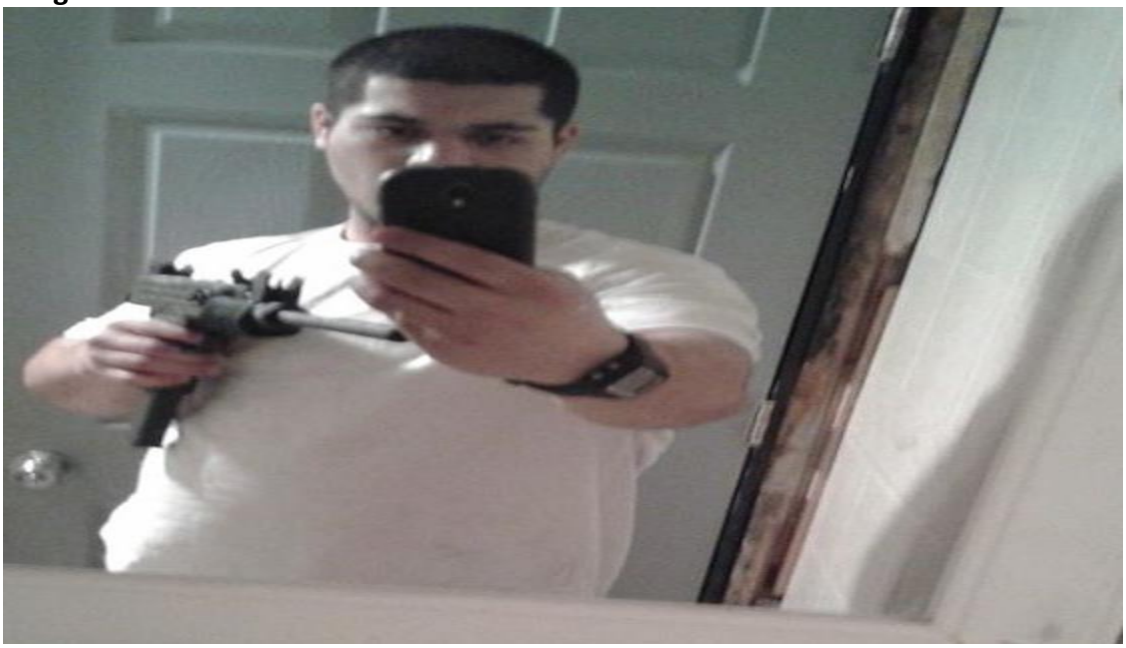


Image 3.2- Gun selfie #2



Evidence #4- PLANS

In this folder we found different images of a man with white painted skin, black outlines around his eyes and mouth, long black hair and he's in a black shirt. We also found some pictures of horses and a picture of a spider. I ran these images in Steg just to make sure there wasn't anything hidden and the results came back negative. Image 4.1, 4.2 and 4.3 are presented below.

Image 4.1- Image of a man

Image 4.2- Image of a horse

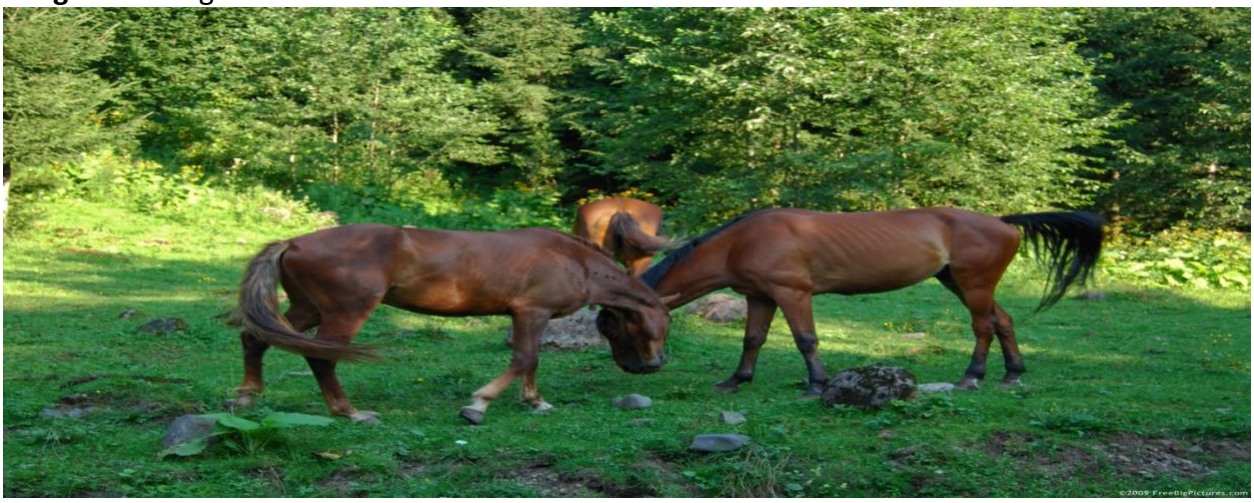


Image 4.3- Image of Spider

Evidence #5- pics2

In this folder we found pictures of car characters from the children movie Lightening McQueen. This can be results of Christopher's interest in cars as we also found a picture of a Camaro with a California license plate TXG 822 and we found an image of a DeLorean. I ran these images through Steg, and everything came back negative. Image 5.1, 5.2 and 5.3 are presented below.

Image 5.1- image of Lightening McQueen

Image 5.2- Image of DeLorean

Image 5.3- Image of Camaro