

Northeastern University

College of Computer and Information Science

Case Project

CY5210 Information System Forensics

Instructor: Elton Booker

Samyukta Kurikala

EXECUTIVE SUMMARY

On April 7th, 2018, the Alexandria Police Department was alerted to the behavior of Jim Cloudy by his brother, Paul Cloudy. A search warrant was executed, and Jim Cloudy's laptop was seized. The device was imaged using FTK Imager. Analysis of the laptop revealed evidence of planning for a mass shooting at a town hall meeting in Sterling, VA, on April 7th, 2018. Jim Cloudy's intent was to attack the meeting and then flee to Bali, Indonesia.

Examination of the laptop identified documents, applications, and cloud syncing capabilities that detailed the planning, timing, and potential details of the attack. Jim Cloudy used various cloud storage services, including AWS S3, Dropbox, Box, and Google Drive, to store and share his plans. The "Operation 2nd Hand Smoke.pptx" file and "AIRPORT INFORMATION.docx" file contained explicit details of the planned attack, including target location, date, time, and escape plan. The "rootkey.xlsx" file potentially contained credentials for cloud access.

The analysis also revealed evidence of financial planning, including a substantial savings account and potential marijuana growing activities. Jim Cloudy's browser history documented research on the target location, travel to Bali, and related topics. The FTK Imager log provided a clear chain of custody.

Recommendations include further investigation of cloud storage accounts, financial records, and potential accomplices. Jim Cloudy should face legal charges for his planned attack. The cloud storage accounts should be deleted to prevent misuse.

INTRODUCTION

On 8th March 2025, I was notified of a potential threat by the Alexandria Police Department. The department requested a full analysis of a seized laptop to determine the scope of a planned attack. The incident was initially reported by Paul Cloudy, who alerted the police regarding his brother, Jim Cloudy's, concerning behavior. Paul provided access to Jim's cloud storage accounts, revealing documents detailing a planned mass shooting. This activity raised concerns regarding potential acts of violence and the need to understand the full extent of the planned attack.

I downloaded the forensic image of the seized laptop, **DESKTOP-PM6C56D**, provided by the Alexandria Police Department on April 7th, 2018, and commenced my analysis. My primary goal is to assess any evidence related to the planning, timing, and potential details of the mass shooting. I examined the system for documents, applications, and cloud syncing capabilities that could provide details about the planned attack. At the time of acquisition, the following windows were open: the Downloads folder, OneNote displaying "Jim's Notebook," and Chrome displaying the "Brother Chat" Google Doc.

The chain of custody document was completed on March 8th, 2025.

```
Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 62,260
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 1,000,215,216
[Physical Drive Information]
Drive Model: Samsung SSD 850 PRO 512GB
Drive Serial Number: S250NSAG505708H
Drive Interface Type: SCSI
Removable drive: False
Source data size: 488386 MB
Sector count: 1000215216
[Computed Hashes]
MD5 checksum: 7af48fa65519e84246b1729e5b68f140
SHA1 checksum: 694e26624d1ea029eb50d793b198edf85be4b4fc

Image Information:
Acquisition started: Fri Apr 06 08:50:44 2018
Acquisition finished: Fri Apr 06 09:42:25 2018
Segment list:
F:\CFRS 780 Lone Wolf Scenario\Evidence Files\LoneWolf.E01
F:\CFRS 780 Lone Wolf Scenario\Evidence Files\LoneWolf.E02
F:\CFRS 780 Lone Wolf Scenario\Evidence Files\LoneWolf.E03
F:\CFRS 780 Lone Wolf Scenario\Evidence Files\LoneWolf.E04
F:\CFRS 780 Lone Wolf Scenario\Evidence Files\LoneWolf.E05
F:\CFRS 780 Lone Wolf Scenario\Evidence Files\LoneWolf.E06
F:\CFRS 780 Lone Wolf Scenario\Evidence Files\LoneWolf.E07
F:\CFRS 780 Lone Wolf Scenario\Evidence Files\LoneWolf.E08
F:\CFRS 780 Lone Wolf Scenario\Evidence Files\LoneWolf.E09

Image Verification Results:
Verification started: Fri Apr 06 09:42:26 2018
Verification finished: Fri Apr 06 10:24:18 2018
MD5 checksum: 7af48fa65519e84246b1729e5b68f140 : verified
SHA1 checksum: 694e26624d1ea029eb50d793b198edf85be4b4fc : verified
```

The hash verification of the acquired image was successful, ensuring the integrity of the forensic image.

ANALYSIS

I focused my analysis on the key registry hives (SAM, SECURITY, SOFTWARE, SYSTEM) and user hives (NTUSER.DAT and USERCLASS.DAT). These hives played a critical role in identifying user-specific activities, system configurations and security settings that provided insight into unauthorized or malicious activities.

During my analysis, I identified USB devices that were plugged into the system. A detailed examination of the devices determined a potential involvement in the incident.

Further, an application analysis was carried out using artifacts like Prefetch files, LNK files, Jump Lists and Shellbags. These were essential in identifying recently executed applications and potentially malicious programs running on the system.

The subsections below explain the findings in detail, providing a comprehensive view of the analysis process and the obtained evidence.

REGISTRY ANALYSIS

The Windows registry for **DESKTOP-PM6C56D** was analyzed for specific system configurations and settings, user specific settings, and user activity using Windows Registry Ripper v2.8. The SAM, SYSTEM, SOFTWARE and user hives (NTUSER.DAT and USERCLASS.DAT) were reviewed for relevant information pertinent to this investigation. The Windows registry identifies current system configuration and settings that may be useful to show the current state of the system and the actions performed by all users on a system.

USER/GROUP INFORMATION

- **Users:**

Table 1 – User Information

| Username | SID | Last Login |
|--------------------|--|-------------------------|
| Administrator | S-1-5-21-2734969515-1644526556-1039763013-500 | Never |
| Guest | S-1-5-21-2734969515-1644526556-1039763013-501 | Never |
| DefaultAccount | S-1-5-21-2734969515-1644526556-1039763013-503 | Never |
| WDAGUtilityAccount | S-1-5-21-2734969515-1644526556-1039763013-504 | Never |
| jcloudy | S-1-5-21-2734969515-1644526556-1039763013-1001 | 2018-04-06 12:26:27Z |

- **Groups:**

- **Administrators**

- S-1-5-21-2734969515-1644526556-1039763013-1001 - jcloudy

- S-1-5-21-2734969515-1644526556-1039763013-500 – Administrator

jcloudy has logged into the system 23 times.

Password Policies:

- > Password does not expire
- > Password not required
- > Normal user account

Password Hint : "It's me you idiot!"

- The Administrator group has 2 users Administrator and jcloudy-
- There do not seem to be any other groups of interest.-
- No user is given access to login remotely.

SYSTEM INFORMATION

- **Microsoft OS Version:** Windows 10 Education
- **Build Version:** 16299.rs3_release.170928-1534
- **Current Control Set:** ControlSet001
- **OS Install Date:** 2018-03-27 12:13:27Z
- **Computer Name:** DESKTOP-PM6C56D
- **Time Zone:** Eastern Standard Time
- **Network Interfaces with Last Connection Time:** Ethernet - Intel(R) 82579LM Gigabit Network Connection - 2018-04-06 07:26:19Z
- **Autostart Programs:** Dropbox, AKMonitor
- **Last Shutdown Time:** 2018-03-27 21:45:28Z

USER ACTIVITY

- **Windows Search History:** J. Cloudy does not seem to have any windows search history according to the lack of evidence identified under the registry key according to the lack of evidence identified under the registry key NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery.
- **Typed Paths:** J. Cloudy has not appeared to have searched for specific paths on the system according to the lack of evidence identified under the registry key NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths.
- **RecentDocs:** There are 38 recent docs opened by the user and will be listed in a separate section.
- **Last Executed Commands:** No commands were run from the START -> RUN box.

RECENT DOCS

This is a list of all the recent docs opened by J. Cloudy:

| | |
|--|---|
| 11 = Downloads 37 = rootkey.csv 36 = Hardware and Sound 35 = ::{025A5937-A6BE-4686-A844-36FE4BEC8B6D} 10 = DemGun.jpg 34 = LeftUsesBoycotts.pdf 33 = AMEN.pdf 12 = Planning.docx 32 = UKknifeBan.pdf 31 = SelfDefenseisMurder.pdf 30 = Cloudy thoughts (4apr).docx 29 = Desktop 7 = OneDrive 28 = Operation 2nd Hand Smoke.pptx 13 = AIRPORT INFORMATION.docx 27 = The Cloudy Manifesto.docx 16 = Sheep.jpg 26 = HoldMyTidePod.jpg 22 = DeathToll.jpg 25 = Huckleberry.png 24 = DemLogic.jpg | 23 = RedGuns.jpg 21 = BladeofGrass.jpg 20 = CubaDearmed.jpg_large 19 = Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'.html 18 = Larry King_ Time to Repeal the 'Poorly Written' Second Amendment.html 17 = DarkWolf.png 15 = MyTiredHead.jpg 14 = HoldMyTidePod.jpg_large 3 = The Internet 9 = defaultapps 8 = pdp?ProductId=9WZDNCRFJ1P3&ocid=QF 6 = Getting started with OneDrive.pdf 5 = System and Security 4 = ::{BB06C0E4-D293-4F75-8A90-CB05B6477EEE} 2 = windowsupdate 1 = CloudLog (D:) 0 = ::{025A5937-A6BE-4686-A844-36FE4BEC8B6D} |
|--|---|

J Cloudy opened various documents, pictures and applications. The rootkey.csv gave away his AWS credentials. The pictures and documents he opened have words like “knife”, “gun”, a presentation named “Operation 2nd Hand Smoke” and a document named ‘Planning’. All these recent documents seem suspicious and need to be investigated further.

APPLICATION ANALYSIS

An application analysis was conducted to identify the frequently used applications. The prefetch files were exported using FTK Imager. I used PECmd.exe v1.5.1 for prefetch analysis. Out of all the applications. The table below shows the applications of interest.

PREFETCH ANALYSIS

The prefetch analysis suggests that the user installed and used various cloud services like BoxSync, S3 Browser, One Drive, Dropbox and Google Drive. The user also installed a program call “installbackupandsync” on 3/27/2018 at 11:40. Apart from cloud services the user appears to have visited browsers like Chrome multiple times. There are many pictures relevant to the user’s planning that were screenshots of Chrome pages. All these applications must be thoroughly investigated.

Table 2 – Prefetch Analysis for DESKTOP-PM6C56D

| Application Name | Times Ran | First Time | Last Time |
|---------------------|-----------|-----------------|----------------|
| BOXSYNC.EXE | 4 | 3/28/2018 0:44 | 4/5/2018 2:05 |
| S3BROWSER-WIN32.EXE | 5 | 3/27/2018 23:57 | 4/5/2018 6:06 |
| ONEDRIVE.EXE | 5 | 3/27/2018 9:21 | 4/4/2018 5:59 |
| DROPBOX.EXE | 10 | 3/28/2018 0:03 | 4/6/2018 12:35 |
| GOOGLEDRIVESYNC.EXE | 10 | 3/27/2018 11:40 | 4/5/2018 1:53 |
| CHROME.EXE | 90 | 3/27/2018 9:32 | 4/6/2018 12:34 |

SHELL ITEM ANALYSIS

Shell item analysis was done. I analyzed Shellbags, Jump Lists and LNK Files. Shellbags provide evidence of accessed or deleted directories, even if the files themselves no longer exist. Jumplists identify frequently used programs and LNK files contain metadata about files and applications that were opened.

Table 3 – Shellbag Analysis for DESKTOP-PM6C56D

| Filename | Location | User Account | Created Time | Modified Time |
|---|---|--------------|----------------|----------------|
| Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun' _files | Desktop\My Computer\Desktop\Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun' _files | jcloudy | 3/30/2018 4:32 | 3/30/2018 4:32 |
| OneDrive | Desktop\My Computer\C:\Users\jcloudy\OneDrive | jcloudy | 3/27/2018 9:21 | 4/4/2018 5:59 |
| Dropbox | Desktop\My Computer\C:\Users\jcloudy\Dropbox | jcloudy | 3/28/2018 0:06 | 4/4/2018 5:32 |
| Box Sync | Desktop\My Computer\C:\Users\jcloudy\Box Sync | jcloudy | 3/28/2018 0:53 | 4/5/2018 2:11 |
| Google Drive | Desktop\Shared Documents Folder (Users Files)\Google Drive | jcloudy | 3/28/2018 0:43 | 3/28/2018 0:43 |

After a shellbag analysis using SBECmd v2.1.0 was done, I found out that the user had various cloud services installed on the system in the Desktop folder. Apart from OneDrive, all the other services were installed at almost the same time on 28th March 2018 between 00:00 and 01:00. There was also a suspicious looking file called “Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun ‘ _files” and its contents must be investigated.

Table 4 – Jump List Analysis for DESKTOP-PM6C56D

The Jump List file analysis was done using JLECmd v1.5.1.

| Filename | MRU | AppId | User Account | Source Created (First) | Source Modified (Last) |
|--|-----|------------------|--------------|------------------------|------------------------|
| C:\Users\jcloudy\Desktop\Planning.docx | 3 | 5f7b5f1e01b83767 | jcloudy | 3/27/2018 9:21 | 4/6/2018 12:27 |
| C:\Users\jcloudy\Desktop\Cloudy thoughts (4apr).docx | 6 | 5f7b5f1e01b83767 | jcloudy | 3/27/2018 9:21 | 4/6/2018 12:27 |
| C:\Users\jcloudy\Desktop\AIRPORT INFORMATION.docx | 8 | 5f7b5f1e01b83767 | jcloudy | 3/27/2018 9:21 | 4/6/2018 12:27 |
| C:\Users\jcloudy\Desktop\The Cloudy Manifesto.docx | 9 | 5f7b5f1e01b83767 | jcloudy | 3/27/2018 9:21 | 4/6/2018 12:27 |
| C:\Users\jcloudy\Desktop\Operation 2nd Hand Smoke.pptx | 7 | 5f7b5f1e01b83767 | jcloudy | 3/27/2018 9:21 | 4/6/2018 12:27 |

These documents are critical to the investigation due to their direct relevance to Jim Cloudy's planned mass shooting. "Planning.docx" likely details the attack, "AIRPORT INFORMATION.docx" confirms his escape plan, "The Cloudy Manifesto.docx" and "Cloudy thoughts (4apr).docx" appear to be of interest. "Operation 2nd Hand Smoke.pptx" potentially contains coded details of the attack. Collectively, these files provide a comprehensive view of Cloudy's intentions, planning, and the timeline leading up to the thwarted event, making them essential components of the forensic analysis.

Apart from these, there are a lot of images which were accessed too that were used in these documents that were downloaded from the internet. The list is added to the appendix.

Table 5 – LNK File Analysis for DESKTOP-PM6C56D

| Filename | Location | User Account | Source Created (First) | Source Modified (Last) |
|-------------------------------|--|--------------|------------------------|------------------------|
| rootkey.csv | C:\Users\jcloudy\Downloads\rootkey.csv | jcloudy | 4/6/2018 12:37 | 4/6/2018 12:37 |
| Operation 2nd Hand Smoke.pptx | C:\Users\jcloudy\Desktop\Operation 2nd Hand Smoke.pptx | jcloudy | 4/4/2018 4:56 | 4/4/2018 5:31 |
| Planning.docx | C:\Users\jcloudy\Desktop\Planning.docx | jcloudy | 3/30/2018 2:16 | 4/5/2018 8:32 |
| Cloudy Manifesto.docx | C:\Users\jcloudy\Desktop\The Cloudy Manifesto.docx | jcloudy | 4/2/2018 1:35 | 4/3/2018 6:11 |
| AIRPORT INFORMATION.docx | C:\Users\jcloudy\Desktop\AIRPORT INFORMATION.docx | jcloudy | 3/30/2018 2:29 | 4/4/2018 5:11 |

The LNK file analysis done using LECmd v1.5.1 reveals a series of files accessed and user activity on DESKTOP-PM6C56D. This list represents a collection of file paths extracted from a user's computer and provides a snapshot of their recent activity and stored data. Notably, several files directly relate to the investigation's focus, such as "AIRPORT INFORMATION.docx," "Planning.docx," "Cloudy thoughts (4apr).docx," "Operation 2nd Hand Smoke.pptx," and "The Cloudy Manifesto.docx," suggesting deliberate planning. Other files, with names like "DemGun.jpg," "RedGuns.jpg," and "UKknifeBan.pdf," are controversial. This list provides a crucial starting point for investigators to reconstruct Jim Cloudy's actions, motivations, and the timeline leading up to the planned attack. A complete list is added to the appendix.

ACTIVITY TIMELINE

- 03/27/2018 12:13: Jim Cloudy got his new laptop.
- 03/27/2018 : Downloaded various .pdf, .ppt, .jpg and .png files to use for his planning.
- 03/27/2018 9:21 : He installed One Drive.
- 03/27/2018 9:32: He installed Chrome.
- 03/27/2018 11:40 : He installed Google Drive.
- 03/27/2018 23:57 : He installed S3 Browser.
- 03/28/2018 0:44 : He installed BoxSync.
- 03/30/2018 : Created Planning.docx, Cloudy thoughts (4apr).docx, AIRPORT INFORMATION.docx, The Cloudy Manifesto.docx.
- 04/04/2018 4:56 :Created Operation 2nd Hand Smoke.pptx.
- 04/06/2018 : Accessed all the documents he created.
- 04/07/2018 : Day the attack was planned.

CLOUD FORENSIC ANALYSIS

Table 6 – Installed software on DESKTOP-PM6C56D

| Installed Software | Version |
|--------------------------------|------------------------|
| Microsoft Office 365 ProPlus | 1708 (Build 8431.2236) |
| Microsoft Edge Browser | 41.16299.248.0 |
| Microsoft OneDrive Application | 18.044.0301.0006 |
| Google Chrome Browser | 65.0.3325.181, 64-bit |
| Google Backup and Sync | 3.40.8921.5350 |
| Box Sync Application | 4.0.7900.0 |
| Dropbox Application | 47.4.74 |
| NetSDK S3 Browser Application | 7.6.9 |

These are the case related software installed on the system. There are a total of 5 cloud services.

Cloud Services:

- Dropbox
- OneDrive
- Amazon S3

- Google Drive
- Box Sync

/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Dropbox 62 Results

Table Thumbnail Summary

Save Table as CSV

| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Known | Location |
|---|---|---|---|-------------------------|-------------------------|-------------------------|-------------------------|--------|------------|-------------|---------|------------|
| .dropbox | | | 1 | 2018-03-27 20:06:29 EDT | 2018-03-27 20:06:29 EDT | 2018-03-27 20:06:29 EDT | 2018-03-27 20:06:29 EDT | 36 | Allocated | Allocated | unknown | /img_LoneW |
| .dropbox.cache | | | | 2018-04-06 08:35:52 EDT | 2018-04-06 08:35:52 EDT | 2018-04-06 08:35:52 EDT | 2018-03-27 20:06:29 EDT | 56 | Allocated | Allocated | unknown | /img_LoneW |
| AIRPORT INFORMATION.docx | | | 1 | 2018-04-04 22:13:38 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:25 EDT | 172684 | Allocated | Allocated | unknown | /img_LoneW |
| AIRPORT INFORMATION.docx:com.dropbox.attributes | | | 1 | 2018-04-04 22:13:38 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:25 EDT | 83 | Allocated | Allocated | unknown | /img_LoneW |
| AIRPORT INFORMATION.docx:com.dropbox.attrs | | | 1 | 2018-04-04 22:13:38 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:25 EDT | 27 | Allocated | Allocated | unknown | /img_LoneW |
| BladeofGrass.jpg | | | 1 | 2018-04-04 22:13:40 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:25 EDT | 201810 | Allocated | Allocated | unknown | /img_LoneW |
| BladeofGrass.jpg:com.dropbox.attributes | | | 1 | 2018-04-04 22:13:40 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:25 EDT | 83 | Allocated | Allocated | unknown | /img_LoneW |
| BladeofGrass.jpg:com.dropbox.attrs | | | 1 | 2018-04-04 22:13:40 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:25 EDT | 27 | Allocated | Allocated | unknown | /img_LoneW |
| Box Sync.lnk | | | 1 | 2018-04-04 22:13:42 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:25 EDT | 1606 | Allocated | Allocated | unknown | /img_LoneW |
| Box Sync.lnk:com.dropbox.attributes | | | 1 | 2018-04-04 22:13:42 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:25 EDT | 83 | Allocated | Allocated | unknown | /img_LoneW |
| Box Sync.lnk:com.dropbox.attrs | | | 1 | 2018-04-04 22:13:42 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:25 EDT | 27 | Allocated | Allocated | unknown | /img_LoneW |
| CubaDearmed.jpg | | | 1 | 2018-04-04 22:13:43 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:25 EDT | 83378 | Allocated | Allocated | unknown | /img_LoneW |
| CubaDearmed.jpg:com.dropbox.attributes | | | 1 | 2018-04-04 22:13:43 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:25 EDT | 83 | Allocated | Allocated | unknown | /img_LoneW |
| CubaDearmed.jpg:com.dropbox.attrs | | | 1 | 2018-04-04 22:13:43 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:25 EDT | 27 | Allocated | Allocated | unknown | /img_LoneW |
| Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too | | | 1 | 2018-04-04 22:13:45 EDT | 2018-04-06 08:35:29 EDT | 2018-04-06 08:35:29 EDT | 2018-04-06 08:35:26 EDT | 286463 | Allocated | Allocated | unknown | /img_LoneW |
| Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too | | | 1 | 2018-04-04 22:13:45 EDT | 2018-04-06 08:35:29 EDT | 2018-04-06 08:35:29 EDT | 2018-04-06 08:35:26 EDT | 83 | Allocated | Allocated | unknown | /img_LoneW |
| Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too | | | 1 | 2018-04-04 22:13:45 EDT | 2018-04-06 08:35:29 EDT | 2018-04-06 08:35:29 EDT | 2018-04-06 08:35:26 EDT | 28 | Allocated | Allocated | unknown | /img_LoneW |
| Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too | | | | 2018-04-06 08:35:51 EDT | 2018-04-06 08:35:51 EDT | 2018-04-06 08:35:51 EDT | 2018-04-06 08:35:22 EDT | 56 | Allocated | Allocated | unknown | /img_LoneW |
| DarkWolf.png | | | 1 | 2018-04-04 22:13:46 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:25 EDT | 603749 | Allocated | Allocated | unknown | /img_LoneW |
| DarkWolf.png:com.dropbox.attributes | | | 1 | 2018-04-04 22:13:46 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:25 EDT | 83 | Allocated | Allocated | unknown | /img_LoneW |
| DarkWolf.png:com.dropbox.attrs | | | 1 | 2018-04-04 22:13:46 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:28 EDT | 2018-04-06 08:35:25 EDT | 28 | Allocated | Allocated | unknown | /img_LoneW |

The Dropbox folder and it's file contents. The user uploaded all the crucial documents discussed earlier to Dropbox.

/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Google Drive 7 Results

Table Thumbnail Summary

Save Table as CSV

| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Known | Location |
|-------------------------------|---|---|---|-------------------------|-------------------------|-------------------------|-------------------------|---------|------------|-------------|---------|-----------------------------------|
| .tmp.drivedownload | | | | 2018-04-04 01:32:04 EDT | 2018-04-04 01:32:04 EDT | 2018-04-04 01:32:04 EDT | 2018-03-31 16:09:54 EDT | 48 | Allocated | Allocated | unknown | /img_LoneWolf.E01/vol_vol7/Users/ |
| Brother Chat.gdoc | | | 1 | 2018-04-06 03:20:00 EDT | 2018-04-06 03:21:28 EDT | 2018-04-06 03:20:00 EDT | 2018-03-31 16:09:54 EDT | 178 | Allocated | Allocated | unknown | /img_LoneWolf.E01/vol_vol7/Users/ |
| Operation 2nd Hand Smoke.pptx | | | 1 | 2018-04-04 01:11:27 EDT | 2018-04-04 01:32:04 EDT | 2018-04-04 01:31:54 EDT | 2018-04-04 01:31:54 EDT | 4408968 | Allocated | Allocated | unknown | /img_LoneWolf.E01/vol_vol7/Users/ |
| The Cloudy Manifesto.docx | | | 1 | 2018-04-01 21:35:27 EDT | 2018-04-01 21:36:35 EDT | 2018-04-01 21:36:28 EDT | 2018-04-01 21:36:28 EDT | 816313 | Allocated | Allocated | unknown | /img_LoneWolf.E01/vol_vol7/Users/ |
| [current folder] | | | | 2018-04-04 01:31:54 EDT | 2018-04-04 01:31:54 EDT | 2018-04-04 01:31:54 EDT | 2018-03-27 20:43:22 EDT | 56 | Allocated | Allocated | unknown | /img_LoneWolf.E01/vol_vol7/Users/ |
| [parent folder] | | | | 2018-03-27 20:53:56 EDT | 2018-03-27 20:53:56 EDT | 2018-03-27 20:53:56 EDT | 2018-03-27 05:18:58 EDT | 256 | Allocated | Allocated | unknown | /img_LoneWolf.E01/vol_vol7/Users/ |
| desktop.ini | | | 1 | 2018-03-27 20:43:36 EDT | 2018-03-27 20:43:36 EDT | 2018-03-27 20:43:36 EDT | 2018-03-27 20:43:22 EDT | 174 | Allocated | Allocated | unknown | /img_LoneWolf.E01/vol_vol7/Users/ |

Google Drive folder and it's file contents. This folder contains the Brother Chat that was open during acquisition.

/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Box Sync 5 Results

Table Thumbnail Summary

Save Table as CSV

| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Known | Location |
|---------------------------|---|---|---|-------------------------|-------------------------|-------------------------|-------------------------|------|-------------|-------------|---------|---|
| Desktop | | | | 2018-04-04 22:21:13 EDT | 2018-04-04 22:21:13 EDT | 2018-04-04 22:21:13 EDT | 2018-04-04 22:11:14 EDT | 56 | Allocated | Allocated | unknown | /img_LoneWolf.E01/vol_vol7/Users/jcloudy/ |
| The Cloudy Manifesto.docx | | | 0 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0 | Unallocated | Allocated | unknown | /img_LoneWolf.E01/vol_vol7/Users/jcloudy/ |
| [current folder] | | | | 2018-04-04 22:11:14 EDT | 2018-04-04 22:11:14 EDT | 2018-04-04 22:11:14 EDT | 2018-03-27 20:53:56 EDT | 56 | Allocated | Allocated | unknown | /img_LoneWolf.E01/vol_vol7/Users/jcloudy/ |
| [parent folder] | | | | 2018-03-27 20:53:56 EDT | 2018-03-27 20:53:56 EDT | 2018-03-27 20:53:56 EDT | 2018-03-27 05:18:58 EDT | 256 | Allocated | Allocated | unknown | /img_LoneWolf.E01/vol_vol7/Users/jcloudy/ |
| desktop.ini | | | 1 | 2018-03-27 20:53:57 EDT | 2018-03-27 20:53:57 EDT | 2018-03-27 20:53:57 EDT | 2018-03-27 20:53:57 EDT | 88 | Allocated | Allocated | unknown | /img_LoneWolf.E01/vol_vol7/Users/jcloudy/ |

















Listing

/img_LoneWolf_E01/vol_v07/Users/cloudy/Box Sync/Desktop

16 Results

TableThumbnailSummary

Save Table as CSV

| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Known | Location |
|---|---|---|---|-------------------------|-------------------------|-------------------------|-------------------------|---------|------------|-------------|---------|----------------------------------|
|  AIRPORT INFORMATION.docx | 1 | | | 2018-04-04 00:59:32 EDT | 2018-04-04 22:21:10 EDT | 2018-04-04 22:21:10 EDT | 2018-04-04 00:59:32 EDT | 172684 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |
|  BladeOfGrass.jpg | 1 | | | 2018-03-31 00:15:53 EDT | 2018-04-04 22:21:13 EDT | 2018-04-04 22:21:12 EDT | 2018-03-31 00:15:53 EDT | 201810 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |
|  CubaDeamed.jpg | 1 | | | 2018-03-30 17:22:56 EDT | 2018-04-04 22:21:10 EDT | 2018-04-04 22:21:10 EDT | 2018-03-30 17:22:56 EDT | 83378 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |
|  DarkWolf.png | 1 | | | 2018-03-29 23:33:51 EDT | 2018-04-04 22:21:12 EDT | 2018-04-04 22:21:12 EDT | 2018-03-29 23:33:51 EDT | 603749 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |
|  DeathToll.jpg | 1 | | | 2018-03-31 00:16:22 EDT | 2018-04-04 22:21:01 EDT | 2018-04-04 22:21:01 EDT | 2018-03-31 00:16:22 EDT | 61596 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |
|  Demologic.jpg | 1 | | | 2018-03-31 00:19:35 EDT | 2018-04-04 22:21:02 EDT | 2018-04-04 22:21:02 EDT | 2018-03-31 00:19:35 EDT | 24465 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |
|  HoldMyTidePod.jpg | 1 | | | 2018-03-29 23:29:20 EDT | 2018-04-04 22:21:03 EDT | 2018-04-04 22:21:03 EDT | 2018-03-29 23:29:20 EDT | 43525 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |
|  Huckberry.jpg | 1 | | | 2018-03-31 00:23:25 EDT | 2018-04-04 22:21:05 EDT | 2018-04-04 22:21:05 EDT | 2018-03-31 00:23:25 EDT | 306471 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |
|  MyTiredhead.png | 1 | | | 2018-03-29 23:31:11 EDT | 2018-04-04 22:21:06 EDT | 2018-04-04 22:21:06 EDT | 2018-03-29 23:31:11 EDT | 107630 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |
|  Operation 2nd Hand Smoke.pptx | 1 | | | 2018-04-04 01:11:27 EDT | 2018-04-04 22:11:18 EDT | 2018-04-04 22:11:16 EDT | 2018-04-04 01:12:03 EDT | 4408968 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |
|  Planning.docx | 1 | | | 2018-04-04 01:30:41 EDT | 2018-04-04 22:21:04 EDT | 2018-04-04 22:21:04 EDT | 2018-04-04 01:30:41 EDT | 14060 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |
|  RedGuns.jpg | 1 | | | 2018-03-31 00:16:59 EDT | 2018-04-04 22:21:09 EDT | 2018-04-04 22:21:09 EDT | 2018-03-31 00:16:59 EDT | 122915 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |
|  Sheep.jpg | 1 | | | 2018-03-29 23:32:40 EDT | 2018-04-04 22:21:07 EDT | 2018-04-04 22:21:07 EDT | 2018-03-29 23:32:40 EDT | 11073 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |
|  The Cloudy Manifesto.docx | 1 | | | 2018-04-01 21:35:27 EDT | 2018-04-04 22:11:16 EDT | 2018-04-04 22:11:15 EDT | 2018-04-01 21:36:38 EDT | 816313 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |
|  [current folder] | | | | 2018-04-04 22:21:13 EDT | 2018-04-04 22:21:13 EDT | 2018-04-04 22:21:13 EDT | 2018-04-04 22:11:14 EDT | 56 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |
|  [parent folder] | | | | 2018-04-04 22:11:14 EDT | 2018-04-04 22:11:14 EDT | 2018-04-04 22:11:14 EDT | 2018-03-27 20:53:56 EDT | 56 | Allocated | Allocated | unknown | /img_LoneWolf_E01/vol_v07/Users/ |

The Box Sync folder and the file contents in its subfolder “Desktop”. This folder contained the pictures the user used in his documents.

Listing

Keyword search 1 - 53

Keyword search 3 - backup











img_LoneWolf.E01\vol_v07\Program Files\S3 Browser

Table

Thumbnail

Summary

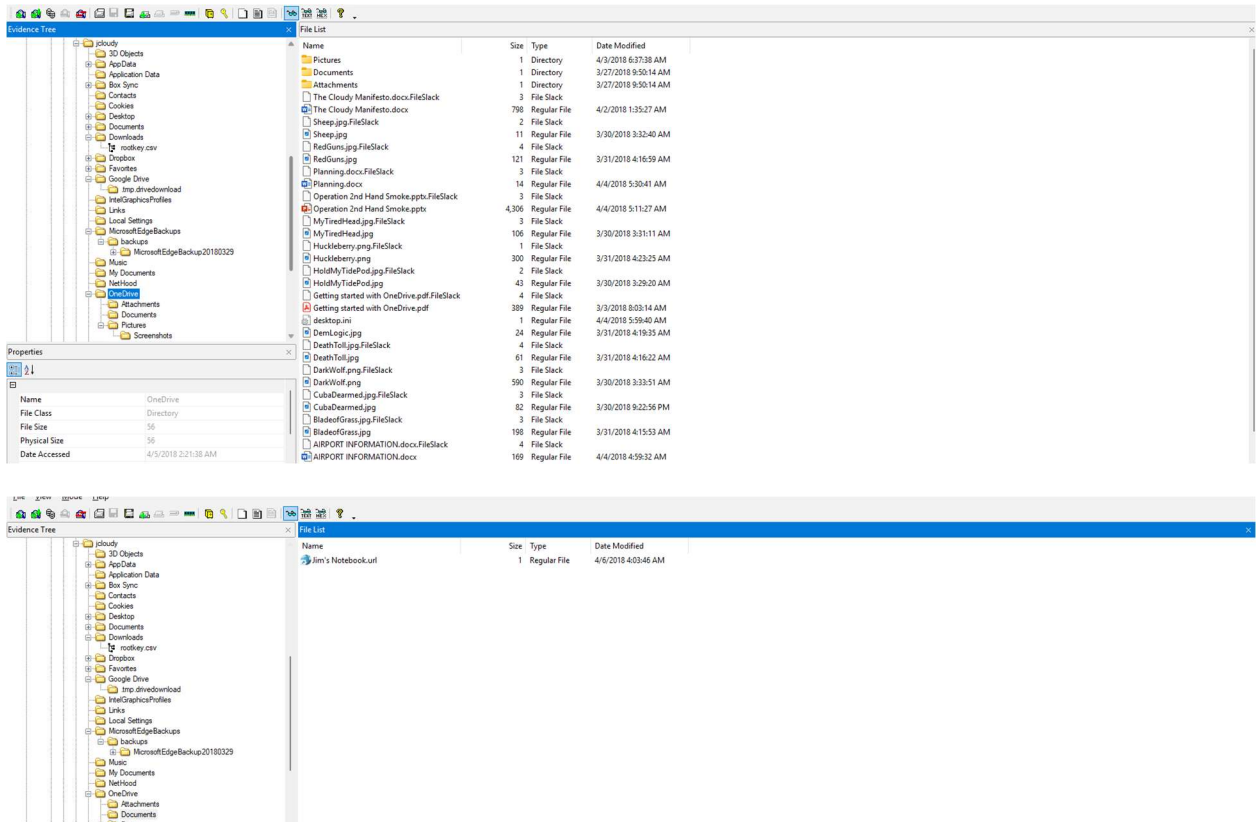
Save Table as CSV

| △ Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Known | Location |
|---|---|---|---|-------------------------|-------------------------|-------------------------|-------------------------|---------|------------|-------------|---------|---|
|  Buy Pro Version.url | | | 1 | 2017-05-22 13:34:24 EDT | 2018-03-27 19:57:19 EDT | 2018-03-27 19:57:19 EDT | 2018-03-27 19:57:19 EDT | 189 | Allocated | Allocated | unknown | img_LoneWolf.E01\vol_v07\Program Files\S3 |
|  Home Page.url | | | 1 | 2017-05-22 13:34:24 EDT | 2018-03-27 19:57:19 EDT | 2018-03-27 19:57:19 EDT | 2018-03-27 19:57:19 EDT | 174 | Allocated | Allocated | unknown | img_LoneWolf.E01\vol_v07\Program Files\S3 |
|  Ionic.Zip.dll | | ▼ | 1 | 2017-05-22 13:34:24 EDT | 2018-03-27 19:57:19 EDT | 2018-03-27 19:57:19 EDT | 2018-03-27 19:57:19 EDT | 462336 | Allocated | Allocated | unknown | img_LoneWolf.E01\vol_v07\Program Files\S3 |
|  [current folder] | | | | 2018-03-27 19:57:19 EDT | 2018-03-27 19:57:19 EDT | 2018-03-27 19:57:19 EDT | 2018-03-27 19:57:18 EDT | 56 | Allocated | Allocated | unknown | img_LoneWolf.E01\vol_v07\Program Files\S3 |
|  [parent folder] | | | | 2018-03-27 20:44:07 EDT | 2018-03-27 20:44:07 EDT | 2018-03-27 20:44:07 EDT | 2017-09-29 09:46:33 EDT | 168 | Allocated | Allocated | unknown | img_LoneWolf.E01\vol_v07\Program Files\S3 |
|  license.txt | | ▼ | 1 | 2017-05-22 13:34:24 EDT | 2018-03-27 19:57:19 EDT | 2018-03-27 19:57:19 EDT | 2018-03-27 19:57:19 EDT | 5731 | Allocated | Allocated | unknown | img_LoneWolf.E01\vol_v07\Program Files\S3 |
|  s3browser-con.exe | | ▼ | 1 | 2018-03-27 16:09:44 EDT | 2018-03-27 19:57:19 EDT | 2018-03-27 19:57:18 EDT | 2018-03-27 19:57:18 EDT | 618112 | Allocated | Allocated | unknown | img_LoneWolf.E01\vol_v07\Program Files\S3 |
|  s3browser-win32.exe | | ▼ | 1 | 2018-03-27 16:09:42 EDT | 2018-03-27 19:57:19 EDT | 2018-03-27 19:57:18 EDT | 2018-03-27 19:57:18 EDT | 3042432 | Allocated | Allocated | unknown | img_LoneWolf.E01\vol_v07\Program Files\S3 |
|  unino000.dat | | ▼ | 1 | 2018-03-27 19:57:19 EDT | 2018-03-27 19:57:19 EDT | 2018-03-27 19:57:18 EDT | 2018-03-27 19:57:18 EDT | 11189 | Allocated | Allocated | unknown | img_LoneWolf.E01\vol_v07\Program Files\S3 |
|  unino000.exe | | | 1 | 2018-03-27 19:51:12 EDT | 2018-03-27 19:57:18 EDT | 2018-03-27 19:57:18 EDT | 2018-03-27 19:57:18 EDT | 719521 | Allocated | Allocated | unknown | img_LoneWolf.E01\vol_v07\Program Files\S3 |

The S3 Browser folder and its file contents.

The screenshot shows a Windows Explorer window with the 'Downloads' folder selected. The file list contains the following items:

| Name | Size | Type | Date Modified |
|--------------------|-------|------------------|---------------------|
| 2018-04-04.png | 2 | File Slack | 4/4/2018 4:35:20 AM |
| 2018-04-04.png | 1,747 | Regular File | 4/4/2018 4:35:20 AM |
| 2018-04-04 (6).png | 4 | File Slack | 4/4/2018 4:35:20 AM |
| 2018-04-04 (6).png | 557 | Regular File | 4/4/2018 5:08:44 AM |
| 2018-04-04 (3).png | 2 | File Slack | 4/4/2018 5:05:33 AM |
| 2018-04-04 (3).png | 95 | Regular File | 4/4/2018 5:05:33 AM |
| 2018-04-04 (2).png | 2 | File Slack | 4/4/2018 5:05:08 AM |
| 2018-04-04 (2).png | 95 | Regular File | 4/4/2018 5:05:08 AM |
| 2018-04-04 (1).png | 2 | File Slack | 4/4/2018 4:51:05 AM |
| 2018-04-04 (1).png | 347 | Regular File | 4/4/2018 4:51:05 AM |
| 2018-04-03.png | 4 | File Slack | 4/3/2018 6:37:42 AM |
| 2018-04-03.png | 137 | Regular File | 4/3/2018 6:37:42 AM |
| 2018-04-03 (3).png | 1 | File Slack | 4/3/2018 6:43:24 AM |
| 2018-04-03 (3).png | 1,874 | Regular File | 4/3/2018 6:43:24 AM |
| 2018-04-03 (2).png | 2 | File Slack | 4/3/2018 6:40:34 AM |
| 2018-04-03 (2).png | 287 | Regular File | 4/3/2018 6:40:34 AM |
| 2018-04-03 (1).png | 480 | Regular File | 4/3/2018 6:39:37 AM |
| 930 | 4 | NTFS Index Al... | 4/4/2018 5:08:44 AM |



These are the screenshots of the One Drive folder and its subfolders “Pictures” and “Documents”

USER ACTIVITY

Planning

1. Target
 - a. Must have good escape route
 - b. Preferably near Airport
 - c. Must be Gun Free zone.
2. Supplies
 - a. Gun (black market)
 - i. Norther VA Gun Works 7518 Fullerton Rd # K, Springfield, VA 22153
 - ii. NOVA 412 W Broad Street Falls Church, VA 22046
 - iii.
 - b. Ammo.
 - i. 9mm is 1000 for \$360
 - ii. Kel-Tec Sub 2000 9mm \$400.
 - c. Latex gloves
 - d. Velcro tear away clothing?
 - e. Cash
3. Escape
 - a. No Extradition countries
 - i. Indonesia (Nicer, but more expensive)
 - ii. Vietnam
 - iii. Can live very well on 100 a day, for 9 years.
 - b. Buy tickets for same day
 - c. Preferable direct flight
 - d. Have suitcase in car.
4. Release
 - a. Start writing ideas and thoughts
 - b. Save to separate locations for redundancy
 - c. Place it in the cloud for remote access
 - d. "Press Release" once home free.

This is the "Planning" document which the user initially created to brainstorm his plan. It clearly indicates that he was planning an attack and an escape route to a country without extradition. He has perfectly laid out his plan.


Event: 1230 – 1400
Flight:

**RESISTANCE
CALENDAR**[ADD EVENT](#)

[← BACK TO EVENTS](#)

SAT APR 7**RSVPS**

Town Hall For Our Lives
Sterling, VA





**TOWN HALL
PROJECT**
SHOW UP • SPEAK OUT

EVENT PAGE
LOCATION
21030 Whitfield Pl
Sterling VA, 20165
DATE & TIME
Sat, April 7, 2018
12:30 to 2:00 PM
[Share on Facebook](#)
[Share on Twitter](#)

Join us April 7th for Town Hall For Our Lives. Representative Comstock and all congressional candidates campaigning for VA-10, as well as Senators Kaine and Warner and local government representatives, have been invited to participate in a face-to-face discussion with constituents of VA-10 on the issues of gun violence, school/public safety, and enhancing community resources to meaningfully address these issues.

Current candidate speakers are:


This page is part of the Operation 2nd Hand Smoke.pptx. The user has decided his target to be the Town Hall and has mentioned the time of the attack. He also included a map to the location and the picture of the building itself in the document.

EST
 **1:20 pm**  **12:10 am** **22h 50m**
Korean Air IAD ICN DPS (+2)
 **1:20 am**  **11:20 am** **22h 00m**
Korean Air DPS ICN IAD

\$2424
KAYAK
[View Deal](#)

☐ **Depart** IAD - DPS **22h 50m**

Sat, Apr 7
Lands Sun, Apr 8


 **1:20 pm — 4:50 pm**
Washington - Seoul
Korean Air 94 · Wide-body jet · Boeing 777-300ER

Economy 14h 30m

Change planes in Seoul (ICN)

1h 14m

Sun, Apr 8
Lands Mon, Apr 9

 **6:05 pm — 12:10 am**
Seoul - Denpasar (Bali)
Korean Air 629 · Wide-body jet · Airbus A330-300

Economy 7h 05m

☐ **Return** DPS - IAD **22h 00m**

Sea Breeze Candidasa

565 reviews | #5 of 28 Specialty Lodging in Candidasa

Mendira Beach, Banjar Mendira, Desa Sengkidu, Manggis, Candidasa, Karangasem 80871, Indonesia

011 62 363 42149

Visit website

E-mail hotel

Save

6 people are viewing this hotel

Apr 8

Apr 20

1 room, 1 adult, 0 children

SAVE \$11



\$69

\$58

View Deal

SAVE \$11



\$69

\$58

View Deal

SAVE \$11



\$69

\$58

View Deal

Booking.com

\$62

Travelocity

\$58

Priceline

\$69

View all 8 deals

Prices are the average nightly price provided by our partner...

Certificate of Excellence



All photos (936)

Traveler (569)

Room & Suite (230)

Pool & Beach (202)

These were also part of the same document. He planned to go to Bali and booked a flight for April 7th and a room in a hotel from April 8th and April 20th.

The Cloudy Manifesto

What happens when the government can no longer protect you. What happens when you need protection from the government? What happens when you can no longer protect yourself?

You are responsible for your own safety and protection. You may choose to provide that safety by handing the responsibility over to elected officials and paid public workers. This has worked well for many years, and I have nothing against this system. However, with the increased scrutiny of law enforcement officials comes a shortage in those jobs. Now, your decision to sub-contract your safety may have a negative impact. Response times may increase. Investigations may not get solved. So, again, whose job is it to protect you?

It's yours. If you choose not to protect yourself, that is YOUR choice. Your choice to be a sheep should not affect other's abilities to protect themselves. Look at Clive Bundy and the now the Snake River Ranchers. Without the means to protect themselves, they would have been victims of the government. Without the means to protect yourself, you may be a victim of the same, or of your fellow man.

Feinstein Logic!

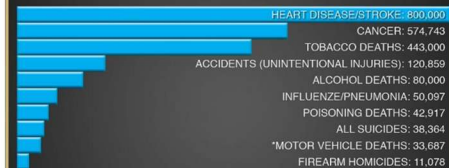


"When the gunman realizes that nobody else is armed, he will lay down his weapons and turn himself in.... that's just human nature."

This may be the most absurd statement yet. This is like saying, when the speeding driver sees that everyone else is doing the speed limit, he will slow down. Well no, he's in a hurry and you are in his way. Just like when a shooter wants to do something...he does. The laws won't stop him, and neither will disarming yourself.

The Cloudy Manifesto

WHAT KILLS AMERICANS



SuperBrochure.com

*211 children died from alcohol impaired driving crashes in 2010

Source: Centers for Disease Control, FBI, U.S. Federal Government

So are we really concerned about what is killing us? Why not outlaw unhealthy food? Oh, it's our right to eat what we want? You don't say?!



This was the Cloudy Manifesto document that highlights the reason for his actions.

CONCLUSION

The forensic analysis of Jim Cloudy's laptop revealed substantial evidence indicating his meticulous planning for a mass shooting event. The examination confirmed the existence of numerous files and digital activities directly related to the planned attack, including detailed planning documents, research on the target location and escape route, and ideological manifestos.

The analysis identified several key files of interest:

- **Planning.docx:** This document likely contained specific details of the planned attack.
- **AIRPORT INFORMATION.docx:** This document confirms Jim Cloudy's escape plans, highlighting his intention to flee to Bali.
- **The Cloudy Manifesto.docx:** This file and the "Cloudy thoughts (4apr).docx" reveal Jim Cloudy's motivations and justifications for the planned attack.
- **Operation 2nd Hand Smoke.pptx:** This file potentially contains coded details of the attack.
- **Image files:** The numerous image files accessed by the user, hint at radicalization, and should be analyzed for further evidence.

The analysis of Prefetch, Shellbags, Jump Lists, and LNK files, along with the examination of cloud storage activities, provided a comprehensive timeline of Jim Cloudy's actions. The significant activity related to cloud services (Dropbox, Box Sync, Google Drive, OneDrive, AWS S3) indicates a deliberate attempt to store and potentially share information related to the planned attack.

Based on the evidence gathered, Jim Cloudy has violated criminal law by actively planning a mass shooting. He should be charged criminally.

Recommendations:

- Jim Cloudy should be immediately charged with conspiracy to commit mass murder and related offenses.
- Law enforcement should conduct a thorough interview with Jim Cloudy to ascertain any potential accomplices or further details of the planned attack.
- A forensic examination of Jim Cloudy's cloud storage accounts (Box, Dropbox, Google Drive, AWS S3) should be conducted to recover any additional data related to the planned attack.
- Financial records should be examined to trace the source of Jim Cloudy's \$325,000 savings and to identify any suspicious transactions.
- Any other electronic devices associated with Jim Cloudy (mobile phones, tablets, etc.) should be seized and forensically examined.
- Any individuals with whom Jim Cloudy communicated online should be identified and interviewed.

TOOLS

- Access Data FTK Imager v4.7.1
- Arsenal Image Mounter v3.4.141
- Registry Ripper v3.0
- Access Data Registry Viewer v2.0.0
- Autopsy v4.6.0

- Eric Zimmerman's tools and version numbers
 - LECmd v1.5.1
 - JLECmd v1.5.1
 - SBECmd v2.1.0
 - PECmd v1.5.1
- USB Detective v1.3.6

APPENDIX

Table 7 - Additional LNK Analysis for DESKTOP-PM6C56D

| SourceCreated | SourceModified | Location |
|-----------------|-----------------|--|
| 4/6/2018 3:55 | 4/6/2018 3:55 | C:\Users\jcloudy\Desktop\AMEN.pdf |
| 3/31/2018 4:15 | 3/31/2018 4:15 | C:\Users\jcloudy\Desktop\BladeofGrass.jpg |
| 3/30/2018 21:22 | 3/30/2018 21:22 | C:\Users\jcloudy\Desktop\CubaDearmed.jpg_large |
| 3/30/2018 4:32 | 3/30/2018 4:32 | C:\Users\jcloudy\Desktop\Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'.html |
| 3/30/2018 3:33 | 3/30/2018 3:33 | C:\Users\jcloudy\Desktop\DarkWolf.png |
| 3/31/2018 4:16 | 4/2/2018 1:10 | C:\Users\jcloudy\Desktop\DeathToll.jpg |
| 3/29/2018 23:17 | 4/6/2018 8:29 | C:\Users\jcloudy\Downloads\DemGun.jpg |
| 3/31/2018 4:19 | 3/31/2018 4:19 | C:\Users\jcloudy\Desktop\DemLogic.jpg |
| 3/30/2018 3:29 | 3/30/2018 3:29 | C:\Users\jcloudy\Desktop\HoldMyTidePod.jpg_large |
| 4/2/2018 1:12 | 4/2/2018 1:12 | C:\Users\jcloudy\Desktop\HoldMyTidePod.jpg |
| 3/31/2018 4:23 | 3/31/2018 4:23 | C:\Users\jcloudy\Desktop\Huckleberry.png |
| 3/30/2018 4:29 | 3/30/2018 4:29 | C:\Users\jcloudy\Desktop\Larry King_ Time to Repeal the 'Poorly Written' Second Amendment.html |
| 4/6/2018 3:56 | 4/6/2018 3:56 | C:\Users\jcloudy\Desktop\LeftUsesBoycotts.pdf |
| 3/30/2018 3:31 | 3/30/2018 3:31 | C:\Users\jcloudy\Desktop\MyTiredHead.jpg |
| 3/31/2018 4:16 | 3/31/2018 4:16 | C:\Users\jcloudy\Desktop\RedGuns.jpg |
| 4/5/2018 5:48 | 4/5/2018 5:48 | C:\Users\jcloudy\Desktop\SelfDefenseisMurder.pdf |
| 3/30/2018 3:32 | 4/2/2018 1:12 | C:\Users\jcloudy\Desktop\Sheep.jpg |
| 4/5/2018 5:51 | 4/5/2018 5:51 | C:\Users\jcloudy\Desktop\UKknifeBan.pdf |

These were the additional files that the user downloaded from the internet as reference and pictures to use in his documents.

Table 8 – Additional Jump List Analysis for DESKTOP-PM6C56D

| SourceCreated | SourceModified | Location |
|----------------|----------------|--|
| 3/27/2018 9:51 | 4/6/2018 3:56 | C:\Users\jcloudy\Desktop\LeftUsesBoycotts.pdf |
| 3/27/2018 9:51 | 4/6/2018 3:56 | C:\Users\jcloudy\Desktop\AMEN.pdf |
| 3/27/2018 9:51 | 4/6/2018 3:56 | C:\Users\jcloudy\Desktop\UKknifeBan.pdf |
| 3/27/2018 9:51 | 4/6/2018 3:56 | C:\Users\jcloudy\Desktop\SelfDefenseisMurder.pdf |
| 3/27/2018 9:51 | 4/6/2018 3:56 | C:\Users\jcloudy\Desktop\Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'.html |
| 3/27/2018 9:51 | 4/6/2018 3:56 | C:\Users\jcloudy\Desktop\Larry King_ Time to Repeal the 'Poorly Written' Second Amendment.html |
| 3/27/2018 9:21 | 4/6/2018 12:27 | C:\Users\jcloudy\Desktop\Sheep.jpg |

| | | |
|----------------|----------------|--|
| 3/27/2018 9:21 | 4/6/2018 12:27 | C:\Users\jcloudy\Desktop\HoldMyTidePod.jpg |
| 3/27/2018 9:21 | 4/6/2018 12:27 | C:\Users\jcloudy\Desktop\DeathToll.jpg |
| 3/27/2018 9:21 | 4/6/2018 12:27 | C:\Users\jcloudy\Desktop\Huckleberry.png |
| 3/27/2018 9:21 | 4/6/2018 12:27 | C:\Users\jcloudy\Desktop\DemLogic.jpg |
| 3/27/2018 9:21 | 4/6/2018 12:27 | C:\Users\jcloudy\Desktop\RedGuns.jpg |
| 3/27/2018 9:21 | 4/6/2018 12:27 | C:\Users\jcloudy\Desktop\BladeofGrass.jpg |
| 3/27/2018 9:21 | 4/6/2018 12:27 | C:\Users\jcloudy\Desktop\CubaDearmed.jpg |
| 3/27/2018 9:21 | 4/6/2018 12:27 | C:\Users\jcloudy\Desktop\DarkWolf.png |
| 3/27/2018 9:21 | 4/6/2018 12:27 | C:\Users\jcloudy\Desktop\MyTiredHead.jpg |

These were the additional files that the user downloaded from the internet as reference and pictures to use in his documents.