

**Case Project 03**

**CY5210 Information System Forensics**

**Instructor: Elton Booker**

**Jonathan Metzger**

**November 20th, 2022**

## Table of Contents

<b>TABLE OF CONTENTS .....</b>	<b>2</b>
<b>EXECUTIVE SUMMARY .....</b>	<b>3</b>
<b>INTRODUCTION .....</b>	<b>4</b>
<b>ANALYSIS.....</b>	<b>5</b>
REGISTRY ANALYSIS.....	5
USER INFORMATION .....	6
GROUP INFORMATION.....	7
SYSTEM INFORMATION.....	8
USER ACTIVITY .....	10
USB DEVICE ACTIVITY .....	12
APPLICATIONS AND MALWARE.....	12
PREFETCH.....	14
SHELL ITEMS.....	15
<b>CONCLUSION .....</b>	<b>18</b>
<b>APPENDIX.....</b>	<b>19</b>
APPENDIX I: FORENSIC TOOLS .....	19
APPENDIX II: REGISTRY PAT .....	19
APPENDIX III: ARTIFACTS LIST .....	20
APPENDIX IV: PREFETCH ANALYSIS .....	22
APPENDIX V: SHELLBAG ANALYSIS .....	27
APPENDIX VI: LINK ANALYSIS .....	30
APPENDIX VII: JUMP LIST ANALYSIS.....	33
APPENDIX VIII: USB ANALYSIS .....	34
APPENDIX IX: CHAIN OF CUSTODY REPORT .....	35
APPENDIX X: OPERATION 2 <sup>ND</sup> HAND SMOKE.....	36

## **EXECUTIVE SUMMARY**

In this case study, I will include findings that pertain to a recent case of a planned but never carried out violent mass shooting attack on a town hall meeting scheduled from 12:30 until 14:00 on April 7th, 2018, at the Cascades Library in Sterling, VA. The purpose of the meeting was to discuss solutions to gun violence which United States Senators attended.

Jim Cloudy is a resident from Alexandria, VA, who is unhappy with the media coverage of gun violence and is a pro 2nd amendment activist. J. Cloudy is unemployed, stays up late, and has trouble sleeping. He wrote multiple pieces on his dissatisfaction of “gun-control” and is known to follow extremist websites that pertain to gun freedom.

Before the town hall event, Jim’s brother Paul became suspicious of Jim’s behavior and notified police. Of the evidence collected by the Cyber Forensics on J. Cloudy’s laptop, it had multiple “Lone Wolf” diagrams and references to anti-government views and how he would have to take matters into his own hands to protect his freedom. It was also found that Jim created “The Cloudy Manifesto” that described these views and how the government has failed him. He created a plan of attack on the town hall event and an escape plan to Bali where he claimed to be suddenly going on a vacation trip.

The analysis section of this report will outline the evidence found on J. Cloudy’s laptop to back up the suspicion by his brother Paul of Jim’s planned attack on the town hall event.

## INTRODUCTION

Paul Cloudy notified police of suspicion that his brother Jim Cloudy was planning an attack on the town hall event on April 7<sup>th</sup>, 2018, at the Cascades Library in Sterling, Virginia. The Cyber Forensics team collected data from Jim's laptop on April 6<sup>th</sup>, 2018, at 09:42:25 where they found compelling evidence to support Paul's claim. The forensics team has the authority to inspect Jim's laptop and any external media that may have been connected to it before Jim's apprehension. It is collected in the chain of custody document found in APPENDIX IX of this document the system that was analyzed, any relevant external media, and who worked on the case study report. Below is the hash verification of the image obtained by police of Jim's laptop, which was believed to hold evidence of Jim's incrimination. Any tools or paths used for the analysis portion of the case study can be found in APPENDIX I and APPENDIX II.

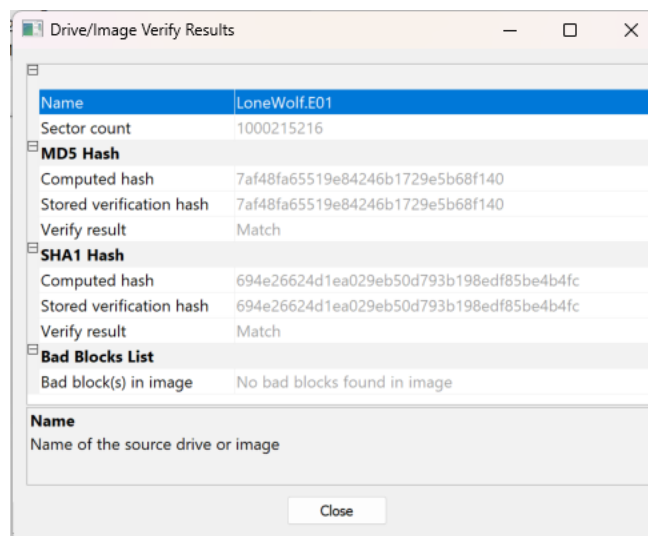


Figure 1 Hash Verification of LoneWolf.E01

## **ANALYSIS**

The analysis will cover Windows Registry, System Information, User activity, USB Device activity, Application and Malware use, Prefetch, Shellbags, Linkfiles, and JumpLists. By the forensics team obtaining this information from the incident response team, we will be able to piece together Jim Cloudy's intentions to carry out with a mass shooting attack on the town hall event.

### **REGISTRY ANALYSIS**

The Windows Registry identifies current system configurations and settings used during the investigation. They can show the current state of the system and actions performed by all users on the system. The following Hives were analyzed for the analysis using the tool Access Data FTK Imager, which can be found in APPENDIX III:

- **NONAME [NTFS]/[root]/Windows/System32/config/SAM**
- **NONAME [NTFS]/[root]/Windows/System32/config/SYSTEM**
- **NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE**
- **NONAME [NTFS]/[root]/Users/jcloudy/NTUSER.DAT**

The SAM Registry Hive focused on profiling users and groups. The SYSTEM Registry Hive identified system information and configuration settings. The SOFTWARE Registry Hive revealed applications downloaded, installed, executed, and uninstalled onto the system. The NTUSER.DAT Registry Hive focused on specific user activity.

## USER INFORMATION

Within the SAM report, forensic investigator can see user and group information. Users for this system have the Domain UID of **S-1-5-21-2734969515-1644526556-1039763013**. With “S” indicating the type is a SID, “1” as the revision level, “5” as the authority value, “21” meaning that it is a domain ID, and 2734969515-1644526556-1039763013 as the “unique identifier.” Next are each username “RID” of the system specified in the below table. Together make the “Security IDentified” or SID. Using the template:

**“<id\_type>-<rev\_level>-<auth\_value>-<spec\_id>-<unique\_identifier>-<RID>”**

**The jcloudy SID is S-1-5-21-2734969515-1644526556-1039763013-1001**

The user information of the system of interest is in the below table with the username, RID, Status with the number of logins, last login, group associated with, and password information. User account jcloudy is the focus of this analysis since it was used on the system of interest with 23 logins up until the reported attack time. Jim Cloudy had administrator access to the system and could have done a better job covering the tracks of his attack. He attempted to use his admin privileges to remove applications from the system but was later found in the forensic investigations. The latest password reset on 2018-03-27 correlated to around when he was provided the new system by Paul when he provided the new system after Jim destroyed his older laptop.

Username	RID	Status	Last Login	Password Reset	Group	Password
jcloudy	1001	Enabled, 23 logins	2018-04-06 12:26:27Z	2018-03-27 09:18:58Z	Administrators	Not Required/Not Expired
Administrator	500	Disabled	Never	Never	Administrators	Not Expire
Guest	501	Disabled	Never	Never	Guests	Not Required/Not Expired
DefaultAccount	503	Disabled	Never	Never	System Managed Accounts Group	Not Required/Not Expired

Table 1 User Information

## **GROUP INFORMATION**

As shown in the table in the previous section, no user was under the group Remote Desktop Users, so that no user could SSH into the system. However, the Administrator, jcloudy, is under the privileged group of Administrators. Any user in this group can cause potential harm to the system and the organization the system is associated with. The jcloudy user account was the only one enabled on the system, which shows that J. Cloudy executed actions on the system. Cloudy did activities on the system with the RID 1001. That information can be important when tracking his efforts on the system and how his actions can prove that he planned to carry on the attack at the town hall meeting on April 7<sup>th</sup>, 2018. The only way anyone else had access or suspicion of J. Cloudy's actions was when he provided his cloud storage access to Paul.

**SYSTEM INFORMATION****KEY**

`${ControlSet}` = HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001

`${CurrentVersion}` = HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

Key	Location	Value
<b>Microsoft OS Version</b>	<code>\${CurrentVersion}\ProductName</code>	Windows 10 Education
<b>Build Version</b>	<code>\${CurrentVersion}\CurrentBuild</code>	16299
<b>Current Control Set</b>	<code>\${ControlSet}</code>	001
<b>Computer Name</b>	<code>\${ControlSet}\Control\ComputerName\ComputerName</code>	DESKTOP-PM6C56D
<b>Time Zone</b>	<code>\${ControlSet}\Control\TimeZoneInformation</code>	Eastern Standard Time
<b>OS Install Date</b>	<code>\${CurrentVersion}\InstallDate</code>	2018-03-27 at 12:13:27Z
<b>Network Interfaces</b>	<code>\${ControlSet}\Services\NetBT\Parameters\Interfaces\Tcpip_{49e11da8-a9a9-4046-a9e2-67d832c476b5}</code>	192.168.0.7
<b>AutoStart Programs</b>	<code>\${CurrentVersion}\Run</code>	<p>LastWrite Time 2018-03-28 00:43:22Z            OneDrive - "C:\Users\jcloudy\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background            GoogleDriveSync - "C:\Program Files\Google\Drive\googledrivesync.exe" /autostart</p> <p>LastWrite Time 2018-04-04 05:59:41Z            Uninstall 18.025.0204.0009 - C:\Windows\system32\cmd.exe /q /c rmdir /s /q "C:\Users\jcloudy\AppData\Local\Microsoft\OneDrive\18.025.0204.0009"</p>
<b>Last Shutdown Time</b>	<code>\${ControlSet}\Control\Windows\ShutdownTime</code> <code>\$. /convert_binary_time.py &lt;REG_BINARY&gt;</code>	Tue Mar 27, 2018, 21:45:28Z

Table 2 System Information

Our goal was to collect the system's configurations, settings, user data, and activity by scoping a complete picture of the action that went on around the time of the alert. The hostname "DESKTOP-PM6C56D" was analyzed by the Forensics team to inspect the malicious activity that was reported. On the Windows 10 Education system, we found that the operating installation time was 2018-03-27 at 12:13:27 and set in Eastern Standard time. This proved that



the new system was used right before the planned attack. We used Registry Ripper to analyze the hives of SAM, SYSTEM, SOFTWARE, and User (NTUSER.DAT and USRCLASS.DAT). The system's network configurations are set to IP Address 192.168.0.7. The system's last shutdown time was the same day as the installation date, meaning the system was never shut down while J. Cloudy was planning his attack. This made it easier for investigators to access the jcloudy user account and retrieve any impersonating evidence.

There were three Autostart actions on the system. Two were removing the cloud storage accounts, GoogleDrive and OneDrive. The jcloudy user also attempted to manually remove the OneDrive directory within his account on the command line to cover his tracks. Even though these areas were removed from the system, data was still saved on the physical hard drive to be collected as evidence.

## USER ACTIVITY

The forensics team went through the user activity of J. Cloudy on both of his accounts. They reviewed the user's Windows Search History, Typed Paths, RecentDocs, Last Executed Commands, and UserAssist findings. Additionally, collected from the Google Drive's **[https\\_drive.google.com\\_0.indexeddb.blob](https://drive.google.com_0.indexeddb.blob)** document was the Brother Chat that had conversations between Paul and Jim. Within the OneNote application on Microsoft's OneDrive, the Jim's Notebook was found and can be traced to evidence of Jim's thoughts and notes that he took prior to his plan to attack the town hall. These registry locations can be found in APPENDIX II.

- **Windows Search History**

There were no windows search history done on the system. There were two HTML searches by using the S3 or Chrome web browsers. This case study is not related to company exposure or malware applications. This case study's scope is on J. Cloudy planning an attack on a town hall meeting and had documents provided in the analysis to back up that claim.

- **Typed Paths**

NTUSER.DAT hive reports no typed paths for either user due to the lack of evidence identified under the registry key.

- **RecentDocs**

There are 38 items in RecentDocs within the NTUSER Hive. The most recent item of interest is the "rootkey.csv" downloaded from the external media. This file contains the AWS private key, another cloud storage to be used. This may have been from the older system that

was destroyed, which could have provided more information on J. Cloudy's actions. Other RecentDocs included plans of the attack like The Cloud Manifesto.docx, Extremist-related documents, Planning.docx, and AIRPORT INFORMATION. Those documents can be connected to his plan for the town hall attack and should be looked at closely.

- **LastExecutedCommands**

J. Cloudy's last executed commands included the "mshta.exe" application at 2018-03-27 13:10:38Z, which relates to viewing html files. These files included "Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'.html" and "Larry King\_Time to Repeal the 'Poorly Written' Second Amendment.html". These web pages can be linked to Jim's dissatisfaction of the government's policy on gun control. It aligns with other documents found on the system that relate to extremist views that can lead to Jim wanted to commit a mass shooting at the town hall event.

Another command that J. Cloudy ran relates to uninstalling the OneDrive application at 2018-04-04 05:59:41Z. This can be an attempt for Jim to try to cover his tracks of the cloud documents that he created to plan the attack on the town hall event.

- **UserAssist**

A list of the UserAssist executables of interest can be found in the below table.

Executables	LastWriteTime
Microsoft.Office.POWERPNT.EXE.15 (2)	2018-04-04 05:00:26Z
Google\Drive\googledrivesync.exe (3)	2018-04-05 01:54:25Z
Box\Box Sync\BoxSync.exe (2)	2018-04-05 02:05:01Z
Microsoft Office\Root\Office16\WINWORD.EXE (1)	2018-04-05 07:02:25Z
Microsoft.Office.OneNote_8wekyb3d8bbwe!microsoft.onenoteim (3)	2018-04-06 08:26:06Z
Microsoft Office\Root\Office16\EXCEL.EXE (1)	2018-04-06 12:27:04Z
Dropbox.Desktop.Client (2)	2018-04-02 01:43:38Z

Table 3 UserAssist

The applications used Excel, Word and PowerPoint can be linked to rootkey.csv, Planning.docx and Operation 2<sup>nd</sup> Hand Smoke.pptx which specify details of the attack and used prior. GoogleDrive, Dropbox and BoxSync are cloud storages that J. Cloudy could use these applications to back up his data or transfer it from his old destroyed system to his new one. OneNote was also used which links to “Jim’s Notebook” that was saved under his OneDrive cloud account.

### USB DEVICE ACTIVITY

The forensics team identified an external media device that was connected to the system. It was used when the new system was installed which shows that data was copied from the media to the system. From the evidence collected, there were various documents that showed extremist views and plans for the attack at the town hall meeting on April 7<sup>th</sup>. The media was not used again which means that data wasn’t copied to the media. The table below shows the external media, serial number, account used on the system, and first and last time the external media was used. It can be concluded that the external media was used initially to transfer documents onto Paul’s old laptop that Jim used after he destroyed his old laptop.

Device Name	Serial Number	User Account	First Time	Last Time
SanDisk Extreme USB Drive	AA010215170355310594	jcloudy	2018-03-27 09:22:21Z	2018-03-27 21:45:54Z

Table 4 USB Device Connected to “desktop-pm6c56d”

### APPLICATIONS AND MALWARE

The scope of this case study is focused on applications that support the claim that J. Cloudy used the cloud to store his documents pertaining to his planned attack on the town hall.

There was no malware found on the system and is not related to this case study. From the table below, it shows applications of interest that were downloaded, installed executed on the system by the jcloudy account with its timestamp of last used. J. Cloud downloaded, installed, and then uninstalled Box Sync, Google Drive and Dropbox. He uninstalled Microsoft OneDrive from the system. These cloud storages help documents of Jim's extremist views, his manifesto, plans to attack the town hall and airport information to escape to Bali. Additionally, he used Microsoft Office Word and PowerPoint to document his thoughts, and Chrome and S3 Browser to search for pro-gun and anti-government webpages. With J. Cloudy's attempt to uninstall these application, and their related application data, he tried to hide his tracks of his actions on the system that was being investigated.

Filename	LastUsed	Download	Installed	Executed	Uninstalled
<b>Microsoft OneDrive v.18.044.0301.0006</b>	2018-04-04 05:59:40Z				X
<b>Microsoft Office 365 ProPlus - en-us v.16.0.8431.2236</b>	2018-03-27 09:45:17Z				X
<b>Google Chrome v.65.0.3325.181</b>	2018-03-27 09:32:50Z	X	X	X	X
<b>Box Sync v.4.0.7900.0</b>	2018-03-29 20:23:17Z	X	X	X	X
<b>Backup and Sync from Google v.3.40.8921.5350</b>	2018-03-27 23:46:40Z	X	X	X	X
<b>Dropbox v.46.4.65</b>	2018-03-29 21:10:16Z	X	X	X	X
<b>S3 Browser version 7.6.9 v.7.6.9.0</b>	2018-03-27 23:57:19Z	X	X	X	X

Table 5 Applications by LastUsed

## PREFETCH

Since the scope of this case study focuses on documents stored in the cloud, it was interesting to see the RunCount of the cloud storage applications BoxSync, Dropbox, GoogleDrive and OneDrive. As shown in the prefetch table below, it shows that cloud storages were ran multiple times by the jcloudy user.

Executable Name	Source Created	Source Modified	Source Accessed	Size	RunCount	Last Run	First Run	Volume0Serial
BOXSYNC.EXE	2022-11-19 19:55:47	2018-04-05 02:05:05	2022-11-19 19:56:45	353998	4	2018-04-05 02:05:01	2018-03-28 00:44:34	AA920881
BOXSYNCSETUP.EXE	2022-11-19 19:55:48	2018-03-28 00:44:16	2022-11-19 19:56:45	82368	1	2018-03-28 00:44:06	n/a	AA920881
CMD.EXE	2022-11-19 19:55:47	2018-04-05 02:05:02	2022-11-19 19:56:45	9136	6	2018-04-05 02:05:02	2018-03-28 00:44:35	AA920881
DROPBOX.EXE	2022-11-19 19:55:47	2018-04-06 12:35:19	2022-11-19 19:56:46	205978	10	2018-04-06 12:35:09	2018-04-02 01:43:26	4C36F4AC
EXCEL.EXE	2022-11-19 19:55:47	2018-04-06 12:27:14	2022-11-19 19:56:46	208902	1	2018-04-06 12:27:04	n/a	4C36F4AC
GOOGLEDRIVESYNC.EXE	2022-11-19 19:55:48	2018-04-05 01:53:45	2022-11-19 19:56:46	1216002	10	2018-04-05 01:53:42	2018-03-30 02:25:52	AA920881
MICROSOFT.ONEDRI VE.APP.EXE	2022-11-19 19:55:48	2018-03-27 09:54:31	2022-11-19 19:56:48	222934	1	2018-03-27 09:54:21	n/a	AA920881
MICROSOFT.PHOTO S.EXE	2022-11-19 19:55:48	2018-04-06 12:46:50	2022-11-19 19:56:48	260032	2	2018-04-06 12:46:49	2018-04-05 02:45:27	AA920881
MICROSOFTEDGE.EX E	2022-11-19 19:55:48	2018-03-27 09:29:01	2022-11-19 19:56:48	218182	1	2018-03-27 09:28:51	n/a	AA920881
NOTEPAD.EXE	2022-11-19 19:55:48	2018-03-27 09:23:24	2022-11-19 19:56:49	40322	1	2018-03-27 09:23:14	n/a	4C36F4AC
ONEDRIVE.EXE	2022-11-19 19:55:47	2018-04-04 05:59:51	2022-11-19 19:56:49	230652	5	2018-04-04 05:59:40	2018-03-27 09:21:46	4C36F4AC
POWERPNT.EXE	2022-11-19 19:55:47	2018-04-04 05:00:36	2022-11-19 19:56:50	239512	2	2018-04-04 05:00:26	2018-04-04 04:31:45	4C36F4AC

Table 6 Prefetch Analysis for "desktop-pm6c56d"

A conclusion can be drawn that J. Cloudy uploaded his documents to the cloud to be accessed at any time on any device. His purpose was to back up his manifesto and plans to attack the town hall to be accessed afterwards. What he didn't expect was the search warrant was placed for his arrest, investigators were able to collect those documents as evidence to incriminate him for his planned attack. Other applications that were ran were the cmd executable to remove OneDrive and view html web pages, excel to view his AWS secret key to access virtual machines, and Notepad and PowerPoint to document his views and plans. By piecing these applications together with documents opened by the jcloudy user, investigators can gather a scenario of J. Cloudy's plans for a mass shooting at the town hall event. The full list of Prefetch applications can be found in APPENDIX IV.

## SHELL ITEMS

The below table identifies the areas of interest in the shell bag analysis located in APPENDIX V. The user J. Cloudy accesses the System and Security section in control panel. This area is a privileged area and can be used to open firewall protections or permissions for malicious activity. Activity can include allowing the use of cloud-based software like Dropbox or external media. The user also accessed the F drive which can be linked to the SanDisk Extreme USB Drive removable media USB. The analysis shows that the user connected the external media to the system, downloaded multiple documents that relate to extremist views and plans to attack the town hall meeting, and cloud storages where these documents can be stored. Luckily for investigators, these files were able to be collected and viewed.

Absolute Path	Shell Type	Value	First Interacted	Last Interacted
Desktop\F:\	Users property view: Drive letter	F:\		
Desktop\F:\CFRS 780 Lone Wolf Scenario	Directory	CFRS 780 Lone Wolf Scenario		
Desktop\My Computer\Desktop\Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun' _files	Directory	Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun' _files	2018-04-05 02:13:26	2018-04-05 02:13:26
Desktop\My Computer\C:\Users\jcloudy\Desktop	Directory	Desktop	2018-03-30 02:29:55	2018-04-05 02:39:06
Desktop\My Computer\C:\Users\jcloudy\OneDrive	Directory	OneDrive	2018-04-05 02:11:56	
Desktop\Control Panel\System and Security\System	GUID: Control panel	System	2018-03-27 09:33:44	2018-03-27 09:33:44
Desktop\Control Panel\Hardware and Sound\Power Options\System Settings	Variable: Users property view	System Settings	2018-04-06 08:32:19	2018-04-06 08:32:19
Desktop\Shared Documents Folder (Users Files)\Dropbox	Users Files Folder	Dropbox	2018-03-28 00:06:27	
Desktop\Shared Documents Folder (Users Files)\Google Drive	Users Files Folder	Google Drive	2018-03-28 00:43:25	
Desktop\Shared Documents Folder (Users Files)\Box Sync	Users Files Folder	Box Sync	2018-04-04 05:32:00	2018-04-05 02:05:13

Table 7 Shellbag Items

From the table below of the Ink list, the documents of interest include The Cloudy Manifesto, Operation 2<sup>nd</sup> Hand Smoke.pptx (found in APPENDIX X), Planning.docx and AIRPORT INFORMATION.docx. They are displayed below and shows the views of J. Cloudy, his plans for the attack and escape. The other files listed are websites, images and pdfs of extreme memes or articles that can show what type of person Jim is. The full list can be found in APPENDIX VI.

LocalPath	Source Created	Source Modified	Source Accessed	File Size	Drive Type	Volume Serial	Machine ID
C:\Users\jcloudy\Desktop\Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'.html	2018-03-30 04:32:25	2018-03-30 04:32:26	2022-11-17 00:26:43	0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\Larry King_ Time to Repeal the 'Poorly Written' Second Amendment.html	2018-03-30 04:29:48	2018-03-30 04:29:48	2018-03-30 04:29:48	0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\LeftUsesBoycotts.pdf	2018-04-06 03:56:32	2018-04-06 03:56:32	2018-04-06 03:56:32	0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\AIRPORT INFORMATION.docx	2018-03-30 02:29:57	2018-04-04 05:11:46	2018-04-04 05:11:46	172684	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Downloads\rootkey.csv	2018-04-06 12:27:08	2018-04-06 12:27:08	2018-04-06 12:27:08	90	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\HoldMyTidePod.jpg_large	2018-03-30 03:29:20	2018-03-30 03:29:20	2018-03-30 03:29:20	0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\Planning.docx	2018-03-30 02:16:48	2018-04-05 08:32:48	2018-04-05 08:32:48	14060	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Downloads\DemGun.jpg	2018-03-29 23:17:51	2018-04-06 08:29:08	2018-04-06 08:29:08	124847	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\DeathToll.jpg	2018-03-31 04:16:22	2018-04-02 01:10:19	2018-04-02 01:10:19	61596	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\HoldMyTidePod.jpg	2018-04-02 01:12:41	2018-04-02 01:12:41	2018-04-02 01:12:41	43525	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\UKknifeBan.pdf	2018-04-05 05:51:41	2018-04-05 05:51:41	2018-04-05 05:51:41	0	Fixed storage media (Hard drive)	AA920881	
D:\key.txt	2018-03-27 09:23:14	2018-03-27 09:23:14	2018-03-27 09:23:14	183	Removable storage media (Floppy, USB)	4C36F4AC/CloudLog	
C:\Users\jcloudy\Desktop\SelfDefenseisMurder.pdf	2018-04-05 05:48:40	2018-04-05 05:48:40	2018-04-05 05:48:40	0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\OneDrive	2018-03-27 09:51:12	2018-04-05 02:01:58	2018-04-05 02:01:58	4096	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\DemLogic.jpg	2018-03-31 04:19:35	2018-03-31 04:19:35	2018-03-31 04:19:35	0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\The Cloudy Manifesto.docx	2018-04-02 01:35:27	2018-04-03 06:11:21	2018-04-03 06:11:21	816313	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\Operation 2nd Hand Smoke.pptx	2018-04-04 04:56:19	2018-04-04 05:31:23	2018-04-04 05:31:23	4408968	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\Cloudy thoughts (4apr).docx	2018-04-05 02:39:29	2018-04-05 02:41:01	2018-04-05 02:41:01	12547	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d

Table 8 LNK Files

Also attached is the rootkey that was downloaded onto the system with an Access Key. This can be used for AWS instances that can be spun up, used, and then destroyed. These documents are highlighted in red in the table below.



Figure 2 Planning and Escape Documents



The table below covers the JumpList files that relate to the case study. A lot of the information overlaps with the LNK files but focuses more on what was found within the jcloudy user directories.

Local Path	Target Created	Target Modified	Target Accessed	File Size	Drive Type	Volume	Machine ID
C:\Users\jcloudy\Desktop\AIRPORT INFORMATION.docx	2018-03-30 02:29:57	2018-03-30 02:29:57	2018-03-30 02:29:57	11802	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\Cloudy thoughts (4apr).docx	2018-04-05 02:39:29	2018-04-05 02:39:30	2018-04-05 02:39:30	12547	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\CubaDearmed.jpg	2018-03-30 21:22:55	2018-03-30 21:22:56	2018-03-30 21:22:40	83378	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\DeathToll.jpg	2018-03-31 04:16:22	2018-03-31 04:16:22	2018-03-31 04:16:11	61596	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\Operation 2nd Hand Smoke.pptx	2018-04-04 04:56:19	2018-04-04 04:56:19	2018-04-04 04:56:19	3853056	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\Planning.docx	2018-03-30 02:16:48	2018-04-04 05:30:41	2018-04-04 05:30:41	14060	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\The Cloudy Manifesto.docx	2018-04-02 01:35:27	2018-04-02 01:35:27	2018-04-02 01:35:27	816313	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Downloads\rootkey.csv	2018-03-27 23:59:20	2018-03-27 23:59:20	2018-03-27 23:59:20	90	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
D:\key.txt	2018-03-22 03:05:22	2018-03-22 03:05:24	2018-03-22 03:05:24	183	Removable storage media (Floppy, USB)	4C36F4AC/CloudLog	n/a

Table 9 Jump Lists

What was found was the Cloud Thoughts.docx that are documented thoughts of J. Cloudy and his dissatisfaction of the government's handling of gun control. It can be observed that the 'key.txt' file from the D drive CloudLog external media was copied onto the system as 'rootkey.csv' to be used on the system.

From this analysis, documents were found on the system that relate to J. Cloudy planning the attack on the town hall meeting. Applications that were used, internet documents that were accessed, and documents written by J. Cloudy point to the conclusion that he was planning a mass shooting event and fleeing to Bali never to return to the United States.

## CONCLUSION

To conclude, the evidence provided in LoneWolf.E01 proved that Jim Cloudy planned to attack the town hall meeting on April 7<sup>th</sup>, 2018. There is enough evidence found on his computer to back up the suspicion from him friend Paul with documents of Jim's plans and extremist views. When Jim destroyed his laptop, he kept his documents on external media that he plugged into Paul's laptop to download. From that information, on Jim's OneDrive was a Planning document, Operation 2<sup>nd</sup> Hand Smoke PowerPoint, The Cloudy Manifesto and Airport information. He did reconnaissance work of the town hall event with pictures found on the OneDrive of the location of the event, his route to the town hall and then to the airport, and the flight information to Bali.

Recommendations include to charge Jim with a planned attack on the town hall event. There is enough evidence to show Jim's displeasure of how gun control was being handled. Instead of voicing his opinion constructively, he planned to act violently and flee the country with no plans to return. Thanks to Paul's tip on Jim's suspicious behaviors, police were able to stop the incident from occurring. Because forensics investigators could access Jim's unencrypted laptop, they could paint a picture of Jim's intentions and plans of attack.

## APPENDIX

### APPENDIX I: Forensic Tools

Tool	Version	Command
Access Data Forensic Toolkit (FTK)	v6.4	GUI
Access Data FTK Imager	v3.4.2.6	GUI
Registry Ripper	v3.0	GUI
Autopsy	v4.6.0	GUI
USBDeviceForensics	v1.5.2	GUI
AccessData Registry Viewer	v2.0	GUI
ShellBags Explorer*	V1.0	GUI
DCode Date	V4.02	GUI
Prefetch*	v1.5	PECmd -d "Directory for Prefetch Files" --csv "Directory Output\pf.csv"
Link File*	v1.5	LECmd -d "Directory for Link Files" --csv "Directory Output\lnk.csv"
Jump List*	v1.5	JLECmd -d "Directory for Jump Files" --csv "Directory Output\jmp.csv"
Shellbags Cmd	v2.0	SBECmd -d "Directory for ShellBag Items" --csv "Directory Output\sb.csv"

\*Eric Zimmerman's Tools (Source: <https://ericzimmerman.github.io/#!index.md>)

### APPENDIX II: Registry Pat

Hive	Directory	Name	Description
NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer	TypedPaths	Paths Typed by User
NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer	WordWheelQuery	Windows Search History
NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer	RecentDocs	Recent Documents
NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer	UserAssist	User Program execution
NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer\	<Policies>\RunMRU	User Command execution
NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion	Run	Applications Ran
NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion	RunOnce	Applications Ran Once
NTUSER.DAT	Software\Microsoft\Windows\Shell	Bags (Desktop)	ShellBags
NTUSER.DAT	Software\Microsoft\Windows\Shell	BagMRU (Desktop)	ShellBags List
NTUSER.DAT	System\CurrentControlSet\Services\Tcpip\Parameters	Interfaces	Network Interfaces
USRCLASS.DAT	Local Settings\Software\Microsoft\Windows\Shell	Bags (Explorer)	ShellBags
USRCLASS.DAT	Local Settings\Software\Microsoft\Windows\Shell	BagMRU (Explorer)	ShellBags List

### APPENDIX III: Artifacts List

#### I. NTFS Files

- NONAME [NTFS]/[root]/\$MFT
- NONAME [NTFS]/[root]/\$LogFile

#### II. Registry Hives

- NONAME [NTFS]/[root]/Windows/System32/config/SYSTEM
- NONAME [NTFS]/[root]/Windows/System32/config/SECURITY
- NONAME [NTFS]/[root]/Windows/System32/config/SAM
- NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
- NONAME [NTFS]/[root]/Users/jcloudy/NTUSER.DAT
- NONAME  
[NTFS]/[root]/Users/jcloudy/AppData/Local/Microsoft/Windows/UsrClass.dat

#### III. Logs

- NONAME [NTFS]/[root]/Windows/System32/winevt/Logs

#### IV. Additional Shellbag Folders

- NONAME [NTFS]/[root]/Windows/Prefetch
- NONAME [NTFS]/[root]/Users/jcloudy/AppData
- NONAME  
[NTFS]/[root]/Users/jcloudy/AppData/Roaming/Microsoft/Windows/Recent

#### V. User's Profile Folders

- NONAME [NTFS]/[root]/Users/jcloudy/Desktop
- NONAME [NTFS]/[root]/Users/jcloudy/Documents
- NONAME [NTFS]/[root]/Users/jcloudy/Downloads
- NONAME [NTFS]/[root]/Users/jcloudy/Dropbox

#### VI. Additional Artifacts

- NONAME [NTFS]/[root]/\$Recycle.Bin (folder)
- NONAME [NTFS]/[root]/Windows/INF/setupapi.dev.log

- NONAME [NTFS]/[root]/Users/jcloudy/AppData/Local/Google/Chrome/User  
Data/Default/IndexedDB/https\_drive.google.com\_0

## APPENDIX IV: Prefetch Analysis

Executable Name	Source Created	Source Modified	Source Accessed	Size	Run Count	Last Run	First Run	Volume Serial
AKMONITOR.EXE	2022-11-19 19:55:47	2018-03-27 09:33:30	2022-11-19 19:56:45	51476	3	2018-03-27 09:33:20	2018-03-27 09:23:02	4C36F4AC
AM_BASE_PATCH1.EXE	2022-11-19 19:55:48	2018-04-04 05:57:30	2022-11-19 19:56:45	13206	1	2018-04-04 05:57:29		AA920881
AM_DELTA.EXE	2022-11-19 19:55:48	2018-04-04 05:57:40	2022-11-19 19:56:45	12884	2	2018-04-04 05:57:30	2018-04-03 06:01:26	AA920881
AM_DELTA_PATCH_1.26 3.1737.0.E	2022-11-19 19:55:47	2018-03-31 04:14:48	2022-11-19 19:56:45	12186	1	2018-03-31 04:14:38		AA920881
AM_DELTA_PATCH_1.26 5.5.0.EXE	2022-11-19 19:55:47	2018-04-05 04:17:22	2022-11-19 19:56:45	12688	1	2018-04-05 04:17:15		AA920881
AM_DELTA_PATCH_1.26 5.91.0.EXE	2022-11-19 19:55:47	2018-04-06 03:48:06	2022-11-19 19:56:45	12706	1	2018-04-06 03:47:57		AA920881
AM_ENGINE_PATCH_1.1.14600.4.E	2022-11-19 19:55:48	2018-04-04 05:57:28	2022-11-19 19:56:45	13392	1	2018-04-04 05:57:27		AA920881
APPLICATIONFRAMEHOST.EXE	2022-11-19 19:55:47	2018-03-27 23:39:00	2022-11-19 19:56:45	66058	3	2018-03-27 23:38:50	2018-03-27 09:27:12	AA920881
AUDIODG.EXE	2022-11-19 19:55:47	2018-04-06 12:35:18	2022-11-19 19:56:45	23332	47	2018-04-06 12:35:08	2018-04-05 05:40:49	AA920881
BACKGROUNDTASKHOST.EXE	2022-11-19 19:55:48	2018-04-06 12:46:49	2022-11-19 19:56:45	103750	22	2018-04-06 12:46:39	2018-03-28 01:30:19	AA920881
BACKGROUNDTASKHOST.EXE	2022-11-19 19:55:48	2018-04-06 12:27:08	2022-11-19 19:56:45	53368	15	2018-04-06 12:27:08	2018-03-28 00:47:14	AA920881
BOXSYNCE.XE	2022-11-19 19:55:47	2018-04-05 02:05:05	2022-11-19 19:56:45	353998	4	2018-04-05 02:05:01	2018-03-28 00:44:34	AA920881
BOXSYNCE_TUP.EXE	2022-11-19 19:55:48	2018-03-28 00:44:16	2022-11-19 19:56:45	82368	1	2018-03-28 00:44:06		AA920881
BOXSYNCE_TUP.EXE	2022-11-19 19:55:47	2018-03-28 00:44:06	2022-11-19 19:56:45	52206	1	2018-03-28 00:44:00		4C36F4AC
BYTECODEGENERATOR.EXE	2022-11-19 19:55:48	2018-04-05 01:51:51	2022-11-19 19:56:45	30682	7	2018-04-05 01:51:51	2018-03-27 09:36:21	AA920881
CALCULATOR.EXE	2022-11-19 19:55:48	2018-03-31 19:50:15	2022-11-19 19:56:45	105320	1	2018-03-31 19:50:05		AA920881
CHROME.EXE	2022-11-19 19:55:47	2018-03-31 20:09:32	2022-11-19 19:56:45	61412	7	2018-03-31 20:09:32	2018-03-27 09:32:51	AA920881
CHROME.EXE	2022-11-19 19:55:48	2018-04-06 03:55:53	2022-11-19 19:56:45	36270	4	2018-04-06 03:55:43	2018-04-05 05:47:47	AA920881
CHROME.EXE	2022-11-19 19:55:48	2018-04-05 05:45:34	2022-11-19 19:56:45	36080	1	2018-04-05 05:45:24		AA920881
CMD.EXE	2022-11-19 19:55:47	2018-04-05 02:05:02	2022-11-19 19:56:45	9136	6	2018-04-05 02:05:02	2018-03-28 00:44:35	AA920881
COMPATTEL_RUNNER.EXE	2022-11-19 19:55:48	2018-04-05 08:42:32	2022-11-19 19:56:45	14124	9	2018-04-05 08:42:25	2018-03-27 09:35:10	AA920881
CONHOST.EXE	2022-11-19 19:55:48	2018-04-06 12:29:29	2022-11-19 19:56:45	24780	47	2018-04-06 12:29:29	2018-04-04 04:31:45	AA920881
CONSENT.EXE	2022-11-19 19:55:48	2018-04-06 12:40:38	2022-11-19 19:56:45	181732	14	2018-04-06 12:40:36	2018-03-27 09:36:32	407F6516
COREDPUSSVR.EXE	2022-11-19 19:55:48	2018-03-27 09:52:54	2022-11-19 19:56:45	27986	2	2018-03-27 09:52:44	2018-03-27 09:52:02	AA920881

COREDPUSS VR.EXE	2022-11-19 19:55:47	2018-04-06 04:13:27	2022-11-19 19:56:45	28204	1	2018-04-06 04:13:17		AA920881
COREDPUSS VR.EXE	2022-11-19 19:55:48	2018-04-05 02:18:48	2022-11-19 19:56:46	29388	2	2018-04-05 02:18:38	2018-03-28 00:15:50	AA920881
DLLHOST.EX E	2022-11-19 19:55:48	2018-04-06 12:27:30	2022-11-19 19:56:46	24086	21	2018-04-06 12:27:25	2018-04-05 01:51:33	AA920881
DLLHOST.EX E	2022-11-19 19:55:47	2018-04-06 12:39:50	2022-11-19 19:56:46	27556	89	2018-04-06 12:39:45	2018-04-06 03:44:15	AA920881
DLLHOST.EX E	2022-11-19 19:55:47	2018-04-06 12:40:43	2022-11-19 19:56:46	15522	49	2018-04-06 12:40:38	2018-04-05 04:16:53	AA920881
DLLHOST.EX E	2022-11-19 19:55:47	2018-04-05 02:39:09	2022-11-19 19:56:46	29750	3	2018-04-05 02:39:04	2018-03-30 02:16:22	4C36F4AC
DLLHOST.EX E	2022-11-19 19:55:47	2018-04-06 03:40:22	2022-11-19 19:56:46	30838	1	2018-04-06 03:40:11		AA920881
DLLHOST.EX E	2022-11-19 19:55:47	2018-04-06 08:31:55	2022-11-19 19:56:46	45154	1	2018-04-06 08:31:49		AA920881
DLLHOST.EX E	2022-11-19 19:55:47	2018-04-04 04:30:48	2022-11-19 19:56:46	22876	4	2018-04-04 04:30:38	2018-03-27 12:13:30	AA920881
DLLHOST.EX E	2022-11-19 19:55:47	2018-04-06 08:32:01	2022-11-19 19:56:46	31310	2	2018-04-06 08:31:55	2018-04-06 08:31:49	4C36F4AC
DLLHOST.EX E	2022-11-19 19:55:48	2018-03-27 23:39:19	2022-11-19 19:56:46	35928	2	2018-03-27 23:39:14	2018-03-27 09:32:59	AA920881
DROPBOX.E XE	2022-11-19 19:55:47	2018-04-06 12:35:19	2022-11-19 19:56:46	205978	10	2018-04-06 12:35:09	2018-04-02 01:43:26	4C36F4AC
DROPBOXU PDATE.EXE	2022-11-19 19:55:47	2018-03-28 00:03:32	2022-11-19 19:56:46	97672	2	2018-03-28 00:03:21	2018-03-28 00:03:20	4C36F4AC
DROPBOXU PDATE.EXE	2022-11-19 19:55:47	2018-04-06 08:28:03	2022-11-19 19:56:46	52760	200	2018-04-06 08:28:03	2018-04-05 07:25:06	AA920881
DRVINST.EX E	2022-11-19 19:55:48	2018-04-06 12:35:09	2022-11-19 19:56:46	263978	12	2018-04-06 12:35:08	2018-03-27 09:17:24	AA920881
EXCEL.EXE	2022-11-19 19:55:47	2018-04-06 12:27:14	2022-11-19 19:56:46	208902	1	2018-04-06 12:27:04		4C36F4AC
EXPLORER.E XE	2022-11-19 19:55:47	2018-03-28 00:44:33	2022-11-19 19:56:46	269976	2	2018-03-28 00:44:22	2018-03-28 00:43:24	AA920881
FILECOAUT H.EXE	2022-11-19 19:55:47	2018-04-04 05:40:15	2022-11-19 19:56:46	39522	2	2018-04-04 05:40:08	2018-03-27 21:28:35	4C36F4AC
FILESYNCCO NFIG.EXE	2022-11-19 19:55:48	2018-04-04 05:59:40	2022-11-19 19:56:46	33456	1	2018-04-04 05:59:40		4C36F4AC
FIRSTLOGO NANIM.EXE	2022-11-19 19:55:48	2018-03-27 09:20:08	2022-11-19 19:56:46	52726	1	2018-03-27 09:19:58		AA920881
FTK IMAGER.EX E	2022-11-19 19:55:48	2018-04-06 12:41:30	2022-11-19 19:56:46	114946	1	2018-04-06 12:41:20		407F6516
FTK IMAGER.EX E	2022-11-19 19:55:48	2018-04-06 12:40:48	2022-11-19 19:56:46	25372	1	2018-04-06 12:40:38		407F6516
GOOGLEDRIV ESYNC.EXE	2022-11-19 19:55:48	2018-04-05 01:53:45	2022-11-19 19:56:46	1216002	10	2018-04-05 01:53:42	2018-03-30 02:25:52	AA920881
GOOGLEUP DATE.EXE	2022-11-19 19:55:47	2018-03-27 09:29:45	2022-11-19 19:56:47	122732	1	2018-03-27 09:29:35		AA920881
GOOGLEUP DATE.EXE	2022-11-19 19:55:47	2018-03-27 23:40:44	2022-11-19 19:56:48	54282	1	2018-03-27 23:40:34		4C36F4AC
GOOGLEUP DATE.EXE	2022-11-19 19:55:47	2018-04-06 08:34:27	2022-11-19 19:56:48	49694	42	2018-04-06 08:34:27	2018-04-04 04:31:02	AA920881
GOOGLEUP DATE.EXE	2022-11-19 19:55:47	2018-03-27 09:29:39	2022-11-19 19:56:48	51354	1	2018-03-27 09:29:29		AA920881
HXTSR.EXE	2022-11-19 19:55:48	2018-04-06 03:30:45	2022-11-19 19:56:48	76770	1	2018-04-06 03:30:44		AA920881
LOCKAPP.E XE	2022-11-19 19:55:48	2018-03-30 03:27:49	2022-11-19 19:56:48	102428	1	2018-03-30 03:03:20		AA920881

# 2022\_CaseStudy\_03

LOGONUI.E XE	2022-11-19 19:55:47	2018-04-06 12:26:20	2022-11-19 19:56:48	127858	21	2018-04-06 08:34:55	2018-04-04 21:29:06	AA920881
MAKECAB.E XE	2022-11-19 19:55:47	2018-04-04 05:45:59	2022-11-19 19:56:48	23500	1	2018-04-04 05:46:00		AA920881
MICROSOFT .MSN.WEAT HER.EXE	2022-11-19 19:55:47	2018-04-04 05:40:36	2022-11-19 19:56:48	142704	1	2018-04-04 05:40:26		AA920881
MICROSOFT .ONEDRIVE. APP.EXE	2022-11-19 19:55:48	2018-03-27 09:54:31	2022-11-19 19:56:48	222934	1	2018-03-27 09:54:21		AA920881
MICROSOFT .PHOTOS.EX E	2022-11-19 19:55:48	2018-04-06 12:46:50	2022-11-19 19:56:48	260032	2	2018-04-06 12:46:49	2018-04-05 02:45:27	AA920881
MICROSOFT .PHOTOS.EX E	2022-11-19 19:55:47	2018-04-04 05:40:08	2022-11-19 19:56:48	267494	4	2018-04-04 05:40:07	2018-04-02 01:10:21	AA920881
MICROSOFT EDGE.EXE	2022-11-19 19:55:48	2018-03-27 23:39:00	2022-11-19 19:56:48	147090	1	2018-03-27 23:38:50		AA920881
MICROSOFT EDGE.EXE	2022-11-19 19:55:48	2018-03-27 09:29:01	2022-11-19 19:56:48	218182	1	2018-03-27 09:28:51		AA920881
MICROSOFT EDGECP.EXE	2022-11-19 19:55:47	2018-03-27 09:35:34	2022-11-19 19:56:48	175792	10	2018-03-27 09:35:24	2018-03-27 09:29:01	AA920881
MPCMDRU N.EXE	2022-11-19 19:55:47	2018-04-06 03:40:11	2022-11-19 19:56:48	33500	19	2018-04-06 03:40:11	2018-03-30 21:18:59	AA920881
MPSIGSTUB .EXE	2022-11-19 19:55:48	2018-04-05 04:17:16	2022-11-19 19:56:48	519390	8	2018-04-05 04:17:15	2018-03-27 09:39:24	AA920881
MSCORSVW .EXE	2022-11-19 19:55:47	2018-04-05 08:42:29	2022-11-19 19:56:49	105942	16	2018-04-05 08:42:29	2018-03-27 10:51:28	AA920881
MSCORSVW .EXE	2022-11-19 19:55:47	2018-04-04 05:45:59	2022-11-19 19:56:49	109048	20	2018-04-04 05:45:59	2018-03-28 00:44:10	AA920881
MSIEXEC.EX E	2022-11-19 19:55:48	2018-03-29 20:23:24	2022-11-19 19:56:49	418134	10	2018-03-29 20:23:13	2018-03-27 09:45:18	AA920881
MSIEXEC.EX E	2022-11-19 19:55:47	2018-03-29 20:23:25	2022-11-19 19:56:49	55102	9	2018-03-29 20:23:14	2018-03-27 09:47:16	AA920881
NGEN.EXE	2022-11-19 19:55:48	2018-04-04 05:45:59	2022-11-19 19:56:49	25690	18	2018-04-04 05:45:58	2018-03-27 10:51:03	AA920881
NGENTASK. EXE	2022-11-19 19:55:47	2018-04-04 05:46:03	2022-11-19 19:56:49	77626	6	2018-04-04 05:46:03	2018-03-27 10:49:33	AA920881
NGENTASK. EXE	2022-11-19 19:55:47	2018-04-05 08:42:29	2022-11-19 19:56:49	78954	9	2018-04-05 08:42:26	2018-03-27 10:58:31	AA920881
NOTEPAD.E XE	2022-11-19 19:55:48	2018-03-27 09:23:24	2022-11-19 19:56:49	40322	1	2018-03-27 09:23:14		4C36F4AC
NVTRAY.EX E	2022-11-19 19:55:47	2018-04-06 12:40:37	2022-11-19 19:56:49	27872	54	2018-04-06 12:40:37	2018-04-06 04:39:04	AA920881
OFFICEC2RC LIENT.EXE	2022-11-19 19:55:47	2018-04-06 12:29:42	2022-11-19 19:56:49	102606	3	2018-04-06 12:29:32	2018-03-27 09:36:00	AA920881
OFFICECLIC KTORUN.EX E	2022-11-19 19:55:47	2018-04-06 12:29:35	2022-11-19 19:56:49	265014	10	2018-04-06 12:29:29	2018-03-30 21:12:16	AA920881
ONEDRIVE.E XE	2022-11-19 19:55:47	2018-04-04 05:59:51	2022-11-19 19:56:49	230652	5	2018-04-04 05:59:40	2018-03-27 09:21:46	4C36F4AC
ONEDRIVES ETUP.EXE	2022-11-19 19:55:47	2018-04-04 05:58:14	2022-11-19 19:56:49	216184	4	2018-04-04 05:58:13	2018-03-27 09:21:57	4C36F4AC
ONENOTEI M.EXE	2022-11-19 19:55:48	2018-04-06 07:24:39	2022-11-19 19:56:49	254822	1	2018-04-06 07:24:28		AA920881
ONENOTEI M.EXE	2022-11-19 19:55:48	2018-03-27 09:49:32	2022-11-19 19:56:49	166292	1	2018-03-27 09:49:22		AA920881
OOBENETW ORKCONNE CTIONFLOW .EXE	2022-11-19 19:55:48	2018-03-27 12:15:14	2022-11-19 19:56:50	176472	1	2018-03-27 12:15:03		AA920881



OPENWITH.EXE	2022-11-19 19:55:47	2018-04-02 01:10:22	2022-11-19 19:56:50	122742	2	2018-04-02 01:10:18	2018-03-27 09:51:12	AA920881
PICKERHOS T.EXE	2022-11-19 19:55:48	2018-03-27 09:54:33	2022-11-19 19:56:50	53942	1	2018-03-27 09:54:28		AA920881
POWERPNT.EXE	2022-11-19 19:55:47	2018-04-04 05:00:36	2022-11-19 19:56:50	239512	2	2018-04-04 05:00:26	2018-04-04 04:31:45	4C36F4AC
PRINTFILTE RPIPELINES VC.EXE	2022-11-19 19:55:47	2018-04-06 03:56:42	2022-11-19 19:56:50	76990	4	2018-04-06 03:56:32	2018-04-05 05:48:40	AA920881
REGSVR32.EXE	2022-11-19 19:55:48	2018-03-29 21:10:15	2022-11-19 19:56:50	34670	9	2018-03-29 21:10:15	2018-03-27 09:21:30	AA920881
RUNDLL32.EXE	2022-11-19 19:55:47	2018-04-06 12:26:31	2022-11-19 19:56:50	48704	1	2018-04-06 12:26:30		AA920881
RUNDLL32.EXE	2022-11-19 19:55:48	2018-04-06 12:26:24	2022-11-19 19:56:50	27672	1	2018-04-06 12:26:23		AA920881
RUNDLL32.EXE	2022-11-19 19:55:48	2018-04-06 12:26:27	2022-11-19 19:56:50	48680	1	2018-04-06 12:26:27		AA920881
RUNDLL32.EXE	2022-11-19 19:55:47	2018-04-06 12:39:44	2022-11-19 19:56:50	18524	1	2018-04-06 12:39:44		AA920881
RUNDLL32.EXE	2022-11-19 19:55:48	2018-04-06 12:26:31	2022-11-19 19:56:50	27672	1	2018-04-06 12:26:30		AA920881
RUNDLL32.EXE	2022-11-19 19:55:47	2018-04-06 06:24:46	2022-11-19 19:56:50	15654	5	2018-04-06 06:24:45	2018-03-29 13:45:48	AA920881
RUNDLL32.EXE	2022-11-19 19:55:48	2018-04-06 12:26:27	2022-11-19 19:56:50	27680	1	2018-04-06 12:26:26		AA920881
RUNTIMEBR OKER.EXE	2022-11-19 19:55:47	2018-04-06 04:13:26	2022-11-19 19:56:50	26414	1	2018-04-06 04:13:16		AA920881
RUNTIMEBR OKER.EXE	2022-11-19 19:55:47	2018-03-31 19:50:21	2022-11-19 19:56:50	18700	1	2018-03-31 19:50:11		AA920881
RUNTIMEBR OKER.EXE	2022-11-19 19:55:47	2018-04-05 02:18:48	2022-11-19 19:56:50	44610	3	2018-04-05 02:18:38	2018-03-28 00:15:50	AA920881
RUNTIMEBR OKER.EXE	2022-11-19 19:55:48	2018-04-05 02:45:31	2022-11-19 19:56:50	932	1	2018-04-05 02:45:21		AA920881
RUNTIMEBR OKER.EXE	2022-11-19 19:55:47	2018-04-06 12:27:18	2022-11-19 19:56:50	21828	13	2018-04-06 12:27:08	2018-03-28 00:43:54	AA920881
RUNTIMEBR OKER.EXE	2022-11-19 19:55:47	2018-04-06 12:45:33	2022-11-19 19:56:50	14648	3	2018-04-06 12:45:23	2018-04-05 02:44:23	AA920881
RUNTIMEBR OKER.EXE	2022-11-19 19:55:47	2018-04-04 05:40:36	2022-11-19 19:56:50	14972	1	2018-04-04 05:40:26		AA920881
RUNTIMEBR OKER.EXE	2022-11-19 19:55:48	2018-04-05 08:33:15	2022-11-19 19:56:50	51174	1	2018-04-05 08:33:05		AA920881
RUNTIMEBR OKER.EXE	2022-11-19 19:55:48	2018-04-06 07:24:39	2022-11-19 19:56:50	44944	1	2018-04-06 07:24:29		AA920881
S3BROWSE R-7-6-9.TMP	2022-11-19 19:55:47	2018-03-27 23:51:20	2022-11-19 19:56:50	48026	1	2018-03-27 23:51:10		4C36F4AC
S3BROWSE R-7-6-9.TMP	2022-11-19 19:55:47	2018-03-27 23:51:22	2022-11-19 19:56:50	55124	1	2018-03-27 23:51:12		AA920881
S3BROWSE R-WIN32.EXE	2022-11-19 19:55:47	2018-04-05 06:06:52	2022-11-19 19:56:50	232058	5	2018-04-05 06:06:42	2018-03-27 23:57:21	AA920881
SCHTASKS.EXE	2022-11-19 19:55:47	2018-04-06 12:29:29	2022-11-19 19:56:51	18226	14	2018-04-06 12:29:29	2018-03-27 09:45:17	AA920881
SEARCHFILTE RHOST.EXE	2022-11-19 19:55:47	2018-04-06 12:35:29	2022-11-19 19:56:51	16116	313	2018-04-06 12:35:19	2018-04-06 07:12:06	AA920881
SEARCHPRO TOCOLHOST .EXE	2022-11-19 19:55:47	2018-04-06 12:35:28	2022-11-19 19:56:51	17592	301	2018-04-06 12:35:18	2018-04-06 07:12:06	AA920881
SEARCHUI.EXE	2022-11-19 19:55:48	2018-03-28 00:44:34	2022-11-19 19:56:51	205518	2	2018-03-28 00:44:24	2018-03-27 09:56:49	AA920881

## 2022\_CaseStudy\_03

SETUP.EXE	2022-11-19 19:55:48	2018-04-06 12:26:30	2022-11-19 19:56:51	110144	3	2018-04-06 12:26:29	2018-04-06 12:26:22	AA920881
SETUP.X86. EN- US_O365PR OPLUSRE	2022-11-19 19:55:47	2018-03-27 09:35:42	2022-11-19 19:56:51	72270	2	2018-03-27 09:35:32	2018-03-27 09:35:29	AA920881
SHELLEXPER IENCEHOST. EXE	2022-11-19 19:55:47	2018-03-28 00:44:34	2022-11-19 19:56:51	146052	3	2018-03-28 00:44:24	2018-03-27 09:56:49	AA920881
SMARTSCRE EN.EXE	2022-11-19 19:55:48	2018-04-06 12:40:46	2022-11-19 19:56:51	44138	26	2018-04-06 12:40:36	2018-04-05 02:23:51	AA920881
SOFTWARE _REPORTER _TOOL.EXE	2022-11-19 19:55:47	2018-04-05 01:49:09	2022-11-19 19:56:51	27112	4	2018-04-05 01:48:59	2018-04-05 01:48:59	AA920881
SPEECHRUN TIME.EXE	2022-11-19 19:55:48	2018-04-06 12:46:49	2022-11-19 19:56:51	66402	1	2018-04-06 12:46:39		AA920881
SPPSVC.EXE	2022-11-19 19:55:48	2018-04-06 12:29:39	2022-11-19 19:56:51	32470	36	2018-04-06 12:29:29	2018-04-05 07:54:23	AA920881
SVCHOST.E XE	2022-11-19 19:55:48	2018-04-06 03:47:59	2022-11-19 19:56:51	55456	11	2018-04-06 03:47:49	2018-03-27 09:39:39	AA920881
SVCHOST.E XE	2022-11-19 19:55:48	2018-04-04 05:46:01	2022-11-19 19:56:51	20310	1	2018-04-04 05:45:51		AA920881
SVCHOST.E XE	2022-11-19 19:55:48	2018-04-06 06:17:44	2022-11-19 19:56:51	75738	4	2018-04-06 06:17:33	2018-03-27 23:31:40	AA920881
SVCHOST.E XE	2022-11-19 19:55:48	2018-04-06 08:25:35	2022-11-19 19:56:51	15946	23	2018-04-06 08:25:25	2018-04-05 01:49:00	AA920881
SVCHOST.E XE	2022-11-19 19:55:47	2018-04-06 12:46:42	2022-11-19 19:56:51	45992	167	2018-04-06 12:46:32	2018-04-06 06:14:34	AA920881
SVCHOST.E XE	2022-11-19 19:55:48	2018-04-05 08:42:35	2022-11-19 19:56:51	21814	8	2018-04-05 08:42:25	2018-03-27 09:22:22	AA920881
SVCHOST.E XE	2022-11-19 19:55:48	2018-04-06 03:34:24	2022-11-19 19:56:51	22710	9	2018-04-06 03:34:14	2018-03-27 09:50:07	AA920881
SVCHOST.E XE	2022-11-19 19:55:47	2018-04-03 06:01:14	2022-11-19 19:56:51	69118	4	2018-04-03 06:01:04	2018-04-01 05:42:13	AA920881
SVCHOST.E XE	2022-11-19 19:55:48	2018-04-06 12:35:18	2022-11-19 19:56:51	19628	1	2018-04-06 12:35:08		AA920881
SVCHOST.E XE	2022-11-19 19:55:48	2018-04-06 12:35:18	2022-11-19 19:56:51	12040	1	2018-04-06 12:35:08		AA920881
SVCHOST.E XE	2022-11-19 19:55:48	2018-04-06 12:46:49	2022-11-19 19:56:51	49854	1	2018-04-06 12:46:39		AA920881
SVCHOST.E XE	2022-11-19 19:55:47	2018-04-06 12:26:24	2022-11-19 19:56:51	19200	36	2018-04-06 12:26:14	2018-04-05 08:16:52	AA920881
SVCHOST.E XE	2022-11-19 19:55:48	2018-04-06 08:27:46	2022-11-19 19:56:51	33292	22	2018-04-06 08:27:36	2018-04-03 06:50:44	AA920881
SVCHOST.E XE	2022-11-19 19:55:47	2018-04-06 12:46:42	2022-11-19 19:56:51	18458	55	2018-04-06 12:46:32	2018-04-06 04:12:55	AA920881
SVCHOST.E XE	2022-11-19 19:55:48	2018-04-06 08:25:01	2022-11-19 19:56:51	21700	23	2018-04-06 08:24:51	2018-04-05 01:51:25	AA920881
SVCHOST.E XE	2022-11-19 19:55:47	2018-04-05 01:51:31	2022-11-19 19:56:51	39324	29	2018-04-05 01:51:21	2018-04-01 22:45:59	AA920881
SVCHOST.E XE	2022-11-19 19:55:48	2018-04-06 08:25:00	2022-11-19 19:56:51	15508	1	2018-04-06 08:24:50		AA920881
SVCHOST.E XE	2022-11-19 19:55:48	2018-04-06 12:35:18	2022-11-19 19:56:51	47672	5	2018-04-06 12:35:08	2018-03-27 09:45:41	AA920881
SVCHOST.E XE	2022-11-19 19:55:47	2018-04-06 08:29:18	2022-11-19 19:56:51	20522	29	2018-04-06 08:29:08	2018-04-04 04:33:45	AA920881
SVCHOST.E XE	2022-11-19 19:55:48	2018-04-06 12:46:42	2022-11-19 19:56:51	19584	73	2018-04-06 12:46:32	2018-04-06 04:12:55	AA920881
SVCHOST.E XE	2022-11-19 19:55:47	2018-04-06 08:24:48	2022-11-19 19:56:51	29622	34	2018-04-06 08:24:38	2018-04-05 07:06:11	AA920881

SVCHOST.EXE	2022-11-19 19:55:48	2018-04-06 12:40:48	2022-11-19 19:56:51	21340	43	2018-04-06 12:40:38	2018-04-05 01:51:22	AA920881
SYSTEMSET TINGS.EXE	2022-11-19 19:55:48	2018-04-06 12:46:48	2022-11-19 19:56:51	242974	9	2018-04-06 12:46:38	2018-03-27 09:30:01	AA920881
TASKHOST W.EXE	2022-11-19 19:55:48	2018-04-06 12:47:02	2022-11-19 19:56:52	65484	129	2018-04-06 12:47:01	2018-04-06 06:45:00	AA920881
TASKMGR.EXE	2022-11-19 19:55:48	2018-03-28 00:48:47	2022-11-19 19:56:52	135540	1	2018-03-28 00:48:37		4C36F4AC
TIWORKER. EXE	2022-11-19 19:55:47	2018-04-06 12:26:43	2022-11-19 19:56:52	75456	20	2018-04-06 12:26:33	2018-04-01 05:41:58	AA920881
TRUSTEDIN STALLER.EX E	2022-11-19 19:55:48	2018-04-06 12:26:43	2022-11-19 19:56:52	19298	32	2018-04-06 12:26:33	2018-04-04 05:40:01	AA920881
VSSVC.EXE	2022-11-19 19:55:47	2018-04-05 08:42:35	2022-11-19 19:56:52	31412	9	2018-04-05 08:42:25	2018-03-27 09:33:22	AA920881
WERFAULT. EXE	2022-11-19 19:55:47	2018-04-02 01:44:17	2022-11-19 19:56:52	262250	6	2018-04-02 01:44:13	2018-03-28 00:05:37	4C36F4AC
WERMGR.EXE	2022-11-19 19:55:47	2018-04-06 03:34:18	2022-11-19 19:56:52	34630	4	2018-04-06 03:34:18	2018-03-27 09:52:03	AA920881
WIFITASK.E XE	2022-11-19 19:55:48	2018-04-06 06:14:36	2022-11-19 19:56:52	31932	36	2018-04-06 06:14:34	2018-04-01 22:43:05	AA920881
WINSAT.EX E	2022-11-19 19:55:48	2018-04-04 06:29:37	2022-11-19 19:56:52	61866	2	2018-04-04 06:29:27	2018-03-28 13:56:01	AA920881
WINSTORE. APP.EXE	2022-11-19 19:55:48	2018-04-05 02:18:48	2022-11-19 19:56:52	254010	3	2018-04-05 02:18:38	2018-03-28 00:15:49	AA920881
WINSTORE. APP.EXE	2022-11-19 19:55:47	2018-03-27 09:52:54	2022-11-19 19:56:52	268032	2	2018-03-27 09:52:44	2018-03-27 09:52:01	AA920881
WINSTORE. APP.EXE	2022-11-19 19:55:47	2018-04-06 04:13:26	2022-11-19 19:56:52	159332	1	2018-04-06 04:13:16		AA920881
WINWORD. EXE	2022-11-19 19:55:47	2018-04-05 07:02:36	2022-11-19 19:56:52	292164	3	2018-04-05 07:02:25	2018-03-30 02:15:47	4C36F4AC
WMIPRVSE. EXE	2022-11-19 19:55:48	2018-04-06 12:35:24	2022-11-19 19:56:52	22826	1	2018-04-06 12:35:14		AA920881
WMIPRVSE. EXE	2022-11-19 19:55:47	2018-04-06 12:47:58	2022-11-19 19:56:53	35424	128	2018-04-06 12:47:48	2018-04-06 06:56:21	AA920881
WUAUCLT.E XE	2022-11-19 19:55:47	2018-04-06 03:48:06	2022-11-19 19:56:53	28114	20	2018-04-06 03:47:57	2018-03-29 23:39:29	AA920881
WWAHOST. EXE	2022-11-19 19:55:48	2018-03-27 12:14:02	2022-11-19 19:56:53	237870	1	2018-03-27 12:13:30		AA920881

## APPENDIX V: Shellbag Analysis

AbsolutePath	ShellType	Value	FirstInteracted	LastInteracted
Desktop\Home Folder	Root folder: GUID	Home Folder	2018-03-27 09:22:42	
Desktop\D:\	Users property view: Drive letter	D:\		
Desktop\Search Folder	Users property view	Search Folder	2018-03-27 09:26:24	
Desktop\Search Folder	Users property view	Search Folder	2018-03-27 09:26:25	
Desktop\My Computer	Root folder: GUID	My Computer		2018-04-06 12:42:02
Desktop\Control Panel	Root folder: GUID	Control Panel		

Desktop\OneDrive	Root folder: GUID	OneDrive	2018-03-27 09:51:01	
Desktop\Shared Documents Folder (Users Files)	Root folder: GUID	Shared Documents Folder (Users Files)		
Desktop\Box Sync	Root folder: GUID	Box Sync	2018-04-02 01:36:35	
Desktop\Dropbox	Root folder: GUID	Dropbox	2018-04-02 01:36:42	
Desktop\F:\	Users property view: Drive letter	F:\		
Desktop\D:\AKMonitor	Directory	AKMonitor		2018-03-27 09:22:46
Desktop\D:\AKMonitor\logs	Directory	logs		2018-03-27 09:22:48
Desktop\D:\AKMonitor\logs\pic	Directory	pic	2018-03-31 20:29:38	2018-03-31 20:29:38
Desktop\F:\Programs	Directory	Programs		2018-04-06 12:41:06
Desktop\F:\CFRS 780 Lone Wolf Scenario	Directory	CFRS 780 Lone Wolf Scenario		
Desktop\F:\Programs\Imager_Lite_3.1.1	Directory	Imager_Lite_3.1.1	2018-04-06 12:41:08	2018-04-06 12:41:08
Desktop\F:\CFRS 780 Lone Wolf Scenario\FTK_Imager_4_2_0	Directory	FTK_Imager_4_2_0		2018-04-06 12:40:28
Desktop\F:\CFRS 780 Lone Wolf Scenario\FTK_Imager_4_2_0\FTK Imager	Directory	FTK Imager	2018-04-06 12:40:29	2018-04-06 12:40:29
Desktop\My Computer\Desktop	Root folder: GUID	Desktop		
Desktop\My Computer\Downloads	Root folder: GUID	Downloads	2018-03-28 00:42:22	2018-04-06 12:42:02
Desktop\My Computer\Documents	Root folder: GUID	Documents	2018-03-28 00:42:24	
Desktop\My Computer\C:	Drive letter	C:		
Desktop\My Computer\Desktop\Cubs' Anthony Rizzo Praises Parkland Kids, Says	Directory	Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun' _files	2018-04-05 02:13:26	2018-04-05 02:13:26

'It's too Easy to Get a Gun' _files				
Desktop\My Computer\C:\Users	Directory	Users		2018-03-30 02:29:55
Desktop\My Computer\C:\Users\jcloudy	Directory	jcloudy		2018-03-30 02:29:55
Desktop\My Computer\C:\Users\jcloudy\Desktop	Directory	Desktop	2018-03-30 02:29:55	2018-04-05 02:39:06
Desktop\My Computer\C:\Users\jcloudy\OneDrive	Directory	OneDrive	2018-04-05 02:11:56	
Desktop\My Computer\C:\Users\jcloudy\Dropbox	Directory	Dropbox	2018-04-05 02:12:00	
Desktop\My Computer\C:\Users\jcloudy\Box Sync	Directory	Box Sync	2018-04-05 02:12:11	
Desktop\Control Panel\System and Security	Control Panel Category	System and Security		
Desktop\Control Panel\Hardware and Sound	Control Panel Category	Hardware and Sound		2018-04-06 08:31:56
Desktop\Control Panel\System and Security\System	GUID: Control panel	System	2018-03-27 09:33:44	2018-03-27 09:33:44
Desktop\Control Panel\Hardware and Sound\Power Options	GUID: Control panel	Power Options		2018-04-06 08:31:56
Desktop\Control Panel\Hardware and Sound\Power Options\System Settings	Variable: Users property view	System Settings	2018-04-06 08:32:19	2018-04-06 08:32:19
Desktop\Shared Documents Folder (Users Files)\Dropbox	Users Files Folder	Dropbox	2018-03-28 00:06:27	
Desktop\Shared Documents Folder (Users Files)\Google Drive	Users Files Folder	Google Drive	2018-03-28 00:43:25	
Desktop\Shared Documents Folder (Users Files)\Box Sync	Users Files Folder	Box Sync	2018-04-04 05:32:00	2018-04-05 02:05:13

## APPENDIX VI: Link Analysis

LocalPath	Source Created	Source Modified	Source Accessed	Target Created	Target Modified	Target Accessed	File Size	Drive Type	VolumeSerialNumber	Machine ID
C:\Users\jclouduy\Desktop\Cloudy thoughts (4apr).docx	2018-04-05 02:39:29	2018-04-05 02:41:01	2018-04-05 02:41:01	2018-04-05 02:39:29	2018-04-05 02:39:30	2018-04-05 02:39:30	12547	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jclouduy\Desktop\Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'.html	2018-03-30 04:32:25	2018-03-30 04:32:26	2022-11-17 00:26:43				0	Fixed storage media (Hard drive)	AA920881	
	2018-03-27 09:27:12	2018-03-27 23:39:13	2018-03-27 23:39:13				0	(None)		
	2018-04-06 08:31:50	2018-04-06 08:31:50	2018-04-06 08:31:50				0	(None)		
C:\Users\jclouduy\Desktop\Larry King_ Time to Repeal the 'Poorly Written' Second Amendment.html	2018-03-30 04:29:48	2018-03-30 04:29:48	2018-03-30 04:29:48				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jclouduy\Desktop\LeftUse sBoycotts.pdf	2018-04-06 03:56:32	2018-04-06 03:56:32	2018-04-06 03:56:32				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jclouduy\Desktop\AIRPORT INFORMATION.docx	2018-03-30 02:29:57	2018-04-04 05:11:46	2018-04-04 05:11:46	2018-03-30 02:29:57	2018-04-04 04:59:32	2018-04-04 04:59:32	172684	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jclouduy\Downloads\root key.csv	2018-04-06 12:27:08	2018-04-06 12:27:08	2018-04-06 12:27:08	2018-03-27 23:59:20	2018-03-27 23:59:20	2018-03-27 23:59:20	90	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jclouduy\OneDrive\Getting started with OneDrive.pdf	2018-03-27 09:51:12	2018-03-27 09:51:12	2018-03-27 09:51:12	2018-03-27 09:50:14	2018-03-03 08:03:14	2018-03-27 09:50:15	398083	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jclouduy\Desktop\HoldMy TidePod.jpg_large	2018-03-30 03:29:20	2018-03-30 03:29:20	2018-03-30 03:29:20				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jclouduy\Desktop\RedGun s.jpg	2018-03-31 04:16:59	2018-03-31 04:16:59	2018-03-31 04:16:59				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jclouduy\Desktop\Planning.docx	2018-03-30 02:16:48	2018-04-05 08:32:48	2018-04-05 08:32:48	2018-03-30 02:16:48	2018-04-04 05:30:41	2018-04-04 05:30:41	14060	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jclouduy\Downloads\De mGun.jpg	2018-03-29 23:17:51	2018-04-06 08:29:08	2018-04-06 08:29:08	2018-03-29 23:17:51	2018-03-29 23:17:52	2018-03-29 23:17:40	124847	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jclouduy\Desktop	2018-03-31 04:16:22	2018-04-02 01:10:19	2018-04-02 01:10:19	2018-03-31 04:16:22	2018-03-31 04:16:22	2018-03-31 04:16:11	61596	Fixed storage	AA920881	desktop-pm6c56d

## 2022\_CaseStudy\_03

op\DeathToll.jpg								media (Hard drive)		
C:\Users\jclouduy\Desktop\AMEN.pdf	2018-04-06 03:55:00	2018-04-06 03:55:00	2018-04-06 03:55:00				0	Fixed storage media (Hard drive)	AA920881	
	2018-03-27 09:52:02	2018-03-27 09:52:02	2018-03-27 09:52:02				0	(None)		
C:\Users\jclouduy\Desktop\CubaDearmed.jpg_large	2018-03-30 21:22:55	2018-03-30 21:22:55	2018-03-30 21:22:55				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jclouduy\Desktop\HoldMyTidePod.jpg	2018-04-02 01:12:41	2018-04-02 01:12:41	2018-04-02 01:12:41	2018-03-30 03:29:20	2018-03-30 03:29:20	2018-03-30 03:29:02	43525	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jclouduy\Desktop	2018-04-05 02:24:19	2018-04-05 02:24:19	2018-04-05 02:24:19	2018-03-27 09:18:58	2018-04-05 02:20:17	2018-04-05 02:20:17	8192	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
	2018-03-27 09:27:12	2018-03-27 09:27:12	2018-03-27 09:27:12				0	(None)		
C:\Users\jclouduy\Desktop\BladeofGrass.jpg	2018-03-31 04:15:53	2018-03-31 04:15:53	2018-03-31 04:15:53				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jclouduy\Desktop\UKknifeBan.pdf	2018-04-05 05:51:41	2018-04-05 05:51:41	2018-04-05 05:51:41				0	Fixed storage media (Hard drive)	AA920881	
D:\key.txt	2018-03-27 09:23:14	2018-03-27 09:23:14	2018-03-27 09:23:14	2018-03-22 03:05:22	2018-03-22 03:05:24	2018-03-22 03:05:24	183	Removable storage media (Floppy, USB)	4C36F4AC/CloudLog	
C:\Users\jclouduy\Desktop\SelfDefenseisMurder.pdf	2018-04-05 05:48:40	2018-04-05 05:48:40	2018-04-05 05:48:40				0	Fixed storage media (Hard drive)	AA920881	
	2018-03-27 23:39:13	2018-03-27 23:39:13	2018-03-27 23:39:13				0	(None)		
C:\Users\jclouduy\OneDrive	2018-03-27 09:51:12	2018-04-05 02:01:58	2018-04-05 02:01:58	2018-03-27 09:21:44	2018-04-04 05:59:44	2018-04-04 05:59:44	4096	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jclouduy\Desktop\DemLogic.jpg	2018-03-31 04:19:35	2018-03-31 04:19:35	2018-03-31 04:19:35				0	Fixed storage media (Hard drive)	AA920881	
D:\	2018-03-27 09:23:14	2018-03-27 09:23:15	2022-11-17 00:26:43	1980-01-01 04:00:00	1980-01-01 04:00:00	1980-01-01 04:00:00	0	Removable storage media (Floppy, USB)	4C36F4AC/CloudLog	
C:\Users\jclouduy\Desktop\The Cloudy Manifesto.docx	2018-04-02 01:35:27	2018-04-03 06:11:21	2018-04-03 06:11:21	2018-04-02 01:35:27	2018-04-02 01:35:27	2018-04-02 01:35:27	816313	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
	2018-03-27 09:32:20	2018-03-27 09:32:20	2018-03-27 09:32:20				0	(None)		
C:\Users\jclouduy\Desktop\MyTireHead.jpg	2018-03-30 03:31:10	2018-03-30 03:31:10	2018-03-30 03:31:10				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jclouduy\Desktop\Operation 2nd Hand Smoke.pptx	2018-04-04 04:56:19	2018-04-04 05:31:23	2018-04-04 05:31:23	2018-04-04 04:56:19	2018-04-04 05:11:27	2018-04-04 05:11:27	4408968	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jclouduy\Desktop	2018-03-30 03:33:50	2018-03-30 03:33:50	2018-03-30 03:33:50				0	Fixed storage	AA920881	

## 2022\_CaseStudy\_03

op\DarkWo lf.png								media (Hard drive)		
	2018-03-27 09:32:20	2018-03-27 09:32:20	2018-03-27 09:32:20				0	(None)		
	2018-04-06 08:31:50	2018-04-06 08:31:50	2018-04-06 08:31:50				0	(None)		
C:\Users\jcl oudy\Desktop\Huckleb erry.png	2018-03-31 04:23:25	2018-03-31 04:23:25	2018-03-31 04:23:25				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcl oudy\Desktop\Sheep.j pg	2018-03-30 03:32:40	2018-04-02 01:12:52	2018-04-02 01:12:52	2018-03-30 03:32:40	2018-03-30 03:32:40	2018-03-30 03:32:34	11073	Fixed storage media (Hard drive)	AA920881	desktop- pm6c56d
C:\Users\jcl oudy\Down loads	2018-03-29 23:17:51	2018-04-06 12:27:08	2018-04-06 12:27:08	2018-03-27 09:18:58	2018-04-06 08:30:22	2018-04-06 08:30:22	65536	Fixed storage media (Hard drive)	AA920881	desktop- pm6c56d



## APPENDIX VII: Jump List Analysis

Local Path	Source Created	Source Modified	Source Accessed	Target Created	Target Modified	Target Accessed	File Size	Drive Type	Volume	Machine ID
C:\Users\jcloudy\Downloads\DemGun.jpg	2018-04-02 01:10:19	2018-04-06 08:29:08	2022-11-17 00:26:45	2018-03-29 23:17:51	2018-03-29 23:17:52	2018-03-29 23:17:40	124847	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\Sheep.jpg	2018-04-02 01:10:19	2018-04-06 08:29:08	2022-11-17 00:26:45	2018-03-30 03:32:40	2018-03-30 03:32:40	2018-03-30 03:32:34	11073	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\HoldMyTidePod.jpg	2018-04-02 01:10:19	2018-04-06 08:29:08	2022-11-17 00:26:45	2018-03-30 03:29:20	2018-03-30 03:29:20	2018-03-30 03:29:02	43525	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\DeathToll.jpg	2018-04-02 01:10:19	2018-04-06 08:29:08	2022-11-17 00:26:45	2018-03-31 04:16:22	2018-03-31 04:16:22	2018-03-31 04:16:11	61596	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\OneDrive\Getting started with OneDrive.pdf	2018-03-27 09:51:12	2018-03-27 23:38:50	2022-11-17 00:26:45	2018-03-27 09:50:14	2018-03-03 08:03:14	2018-03-27 09:50:15	398083	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\Planning.docx	2018-03-30 02:16:48	2018-04-05 08:32:48	2022-11-17 00:26:45	2018-03-30 02:16:48	2018-03-30 02:16:49	2018-03-30 02:16:49	11682	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\Cloudy thoughts (4apr).docx	2018-03-30 02:16:48	2018-04-05 08:32:48	2022-11-17 00:26:45	2018-04-05 02:39:29	2018-04-05 02:39:30	2018-04-05 02:39:30	12547	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\AIRPORT INFORMATION.docx	2018-03-30 02:16:48	2018-04-05 08:32:48	2022-11-17 00:26:45	2018-03-30 02:29:57	2018-03-30 02:29:57	2018-03-30 02:29:57	11802	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\The Cloudy Manifesto.docx	2018-03-30 02:16:48	2018-04-05 08:32:48	2022-11-17 00:26:45	2018-04-02 01:35:27	2018-04-02 01:35:27	2018-04-02 01:35:27	816313	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
D:\key.txt	2018-03-27 09:23:14	2018-03-27 09:23:14	2018-03-27 09:23:14	2018-03-22 03:05:22	2018-03-22 03:05:24	2018-03-22 03:05:24	183	Removable storage media (Floppy, USB)	4C36F4AC/CloudLog	
C:\Users\jcloudy\Desktop\Operation 2nd Hand Smoke.pptx	2018-04-04 04:56:19	2018-04-04 05:00:30	2022-11-17 00:26:45	2018-04-04 04:56:19	2018-04-04 04:56:19	2018-04-04 04:56:19	3853056	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\LeftUsesBoycotts.pdf	2018-03-27 09:51:18	2018-04-06 03:56:32	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\AMEN.pdf	2018-03-27 09:51:18	2018-04-06 03:56:32	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\UKknifeBan.pdf	2018-03-27 09:51:18	2018-04-06 03:56:32	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\SelfDefenseisMurder.pdf	2018-03-27 09:51:18	2018-04-06 03:56:32	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'.html	2018-03-27 09:51:18	2018-04-06 03:56:32	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\Larry King_ Time to Repeat the 'Poorly Written' Second Amendment.html	2018-03-27 09:51:18	2018-04-06 03:56:32	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\OneDrive\Getting started with OneDrive.pdf	2018-03-27 09:51:18	2018-04-06 03:56:32	2022-11-17 00:26:45	2018-03-27 09:50:14	2018-03-03 08:03:14	2018-03-27 09:50:15	398083	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Downloads	2018-03-27 09:21:10	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-27 09:18:58	2018-04-06 08:30:22	2018-04-06 08:30:22	65536	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop	2018-03-27 09:21:10	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-27 09:18:58	2018-04-06 08:29:54	2018-04-06 08:29:54	8192	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Dropbox	2018-03-27 09:21:10	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-28 00:06:27	2018-04-04 05:32:30	2018-04-04 05:32:30	4096	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Box Sync	2018-03-27 09:21:10	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-28 00:53:56	2018-04-04 05:32:03	2018-04-04 05:32:03	4096	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Google Drive	2018-03-27 09:21:10	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-28 00:43:22	2018-04-04 05:31:54	2018-04-04 05:31:54	4096	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Pictures	2018-03-27 09:21:10	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-27 09:18:58	2018-03-27 09:20:00	2018-03-27 09:20:00	0	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Documents	2018-03-27 09:21:10	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-27 09:18:58	2018-03-27 09:20:00	2018-03-27 09:20:00	4096	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Downloads\rootkey.csv	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-27 23:59:20	2018-03-27 23:59:20	2018-03-27 23:59:20	90	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\LeftUsesBoycotts.pdf	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\AMEN.pdf	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\Planning.docx	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-30 02:16:48	2018-04-04 05:30:41	2018-04-04 05:30:41	14060	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\UKknifeBan.pdf	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\SelfDefenseisMurder.pdf	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\Cloudy thoughts (4apr).docx	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-04-05 02:39:29	2018-04-05 02:39:30	2018-04-05 02:39:30	12547	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\Operation 2nd Hand Smoke.pptx	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-04-04 04:56:19	2018-04-04 05:11:27	2018-04-04 05:11:27	4408968	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\AIRPORT INFORMATION.docx	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-30 02:29:57	2018-04-04 04:59:32	2018-04-04 04:59:32	172684	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d

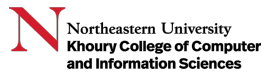
## 2022\_CaseStudy\_03

C:\Users\jcloudy\Desktop\The Cloudy Manifesto.docx	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-04-02 01:35:27	2018-04-02 01:35:27	2018-04-02 01:35:27	816313	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\Sheep.jpg	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-30 03:32:40	2018-03-30 03:32:40	2018-03-30 03:32:34	11073	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\HoldMyTidePod.jpg	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-30 03:29:20	2018-03-30 03:29:20	2018-03-30 03:29:02	43525	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\DeathToll.jpg	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-31 04:16:22	2018-03-31 04:16:22	2018-03-31 04:16:11	61596	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\Huckleberry.png	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\DemLogic.jpg	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\RedGuns.jpg	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\BladeofGrass.jpg	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\CubaDearmed.jpg	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-30 21:22:55	2018-03-30 21:22:56	2018-03-30 21:22:40	83378	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
C:\Users\jcloudy\Desktop\DarkWolf.png	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\Desktop\MyTiredHead.jpg	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45				0	Fixed storage media (Hard drive)	AA920881	
C:\Users\jcloudy\OneDrive\Getting started with OneDrive.pdf	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-27 09:50:14	2018-03-03 08:03:14	2018-03-27 09:50:15	398083	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d
D:\key.txt	2018-03-27 09:21:12	2018-04-06 12:27:08	2022-11-17 00:26:45	2018-03-22 03:05:22	2018-03-22 03:05:24	2018-03-22 03:05:24	183	Removable storage media (Floppy, USB)	4C36F4AC/CloudLog	
C:\Users\jcloudy\Downloads\rootkey.csv	2018-04-06 12:27:07	2018-04-06 12:27:07	2018-04-06 12:27:07	2018-03-27 23:59:20	2018-03-27 23:59:20	2018-03-27 23:59:20	90	Fixed storage media (Hard drive)	AA920881	desktop-pm6c56d

## APPENDIX VIII: USB Analysis

Serial/UID	Description	First Connected (UTC)	Last Connected (UTC)	Last Disconnected (UTC)	Volume Name/Label	Drive Letter(s)	VSN	Last User
AA010215170355310594	SanDisk Extreme USB Device	3/27/2018 12:11:31 PM	3/27/2018 12:13:21 PM	3/27/2018 9:22:13 AM	ESD-USB			
AA010603160707470215	SanDisk Extreme USB Device	3/27/2018 9:22:21 AM	3/27/2018 9:45:54 PM		CloudLog	D:		

## APPENDIX IX: Chain of Custody Report



**Forensic Lab**  
Northeastern University  
Chain of Custody Form

<b>Date:</b> 11/20/2022	<b>Case Number (FAC):</b> 2022_CaseStudy_03	<b>Case Type:</b> Probable Mass Shooting		
<b>Description of Item(s):</b>				
<b>Property Number</b>	<b>Device Type</b>	<b>Make</b>	<b>Model</b>	<b>Serial Number</b>
2022_CaseStudy_03	Laptop	Windows	10 Education	AA920881
<b>Power Cable/Brick</b>	<b>CD/DVD (-R +R - RW)</b>	<b>Case/Peripherals</b>	<b>Dongles</b>	<b>Other</b>
N/A	N/A	N/A	N/A	N/A
<b>(Ext/Int)ernal Drives (Type)</b>	<b>Make</b>	<b>Model</b>	<b>Size</b>	<b>Serial Number</b>
External Media "D:"	SanDisk	Extreme USB Drive	64 GB	AA010215170355310594
<b>Notes for Item(s):</b> (e.g. condition, scratches, blemishes.)				
All items were in fairly good condition and no marks scratches or modifications to the hardware collected.				
<b>Obtained from:</b> (owner of item(s), location, phone number)				
Digital Evidence Specialist, Jon Metzger – 322 Hayden Hall, 613-373-2200				
<b>Released by:</b> (printed name)		<b>Released by:</b> (Signature)		<b>Date/Time Released:</b>
Jon Metzger		<i>Jon Metzger</i>		04/06/2018 09:42:25 EST
<b>Released to:</b> (printed name)		<b>Released to:</b> (Signature)		<b>Date/Time Stored:</b>
Dir. of Homeland Security, James Smith		<i>James Smith</i>		04/06/2018 09:42:25 EST
<b>Temporary disposition of item (s): (where stored)</b>				
In an access-restricted, GSA-approved secure container: GSA001 (Asset Tag or Storage Locker number)				

## APPENDIX X: Operation 2<sup>nd</sup> Hand Smoke

# OPERATION 2ND HAND SMOKE


Event: 1230 – 1400  
Flight:

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

[← BACK TO EVENTS](#)

**SAT** **APR 7**55 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:





## 2022\_CaseStudy\_03

21030 Whitfield Pl

Potomac Falls, VA 20165

Get on VA-28 S from VA-1795 and VA-7 W

1. Head north on Whitfield Pl 6 min (2.5 mi)
2. Turn left onto VA-1795 0.1 mi
3. Turn right onto VA-7 W 0.8 mi
4. Use the right lane to take the VA-28 S ramp to Dulles Airport/Centreville 1.2 mi

Continue on VA-28 S. Drive to Saarinen Cir in Dulles

5. Continue onto VA-28 S 7 min (6.9 mi)
6. Take the exit toward Dulles Airport 5.4 mi  
▲ Partial toll road
7. Keep left, follow signs for Departures/Arrivals/Hourly Parking/Daily Parking and merge onto Dulles Access Rd 0.7 mi
8. Continue onto Saarinen Cir 0.8 mi

Dulles International Airport



EST

Korean Air

1:20 pm IAD

12:10 am DPS (+2)

22h 50m

Korean Air

1:20 am DPS

11:20 am IAD

22h 00m

\$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

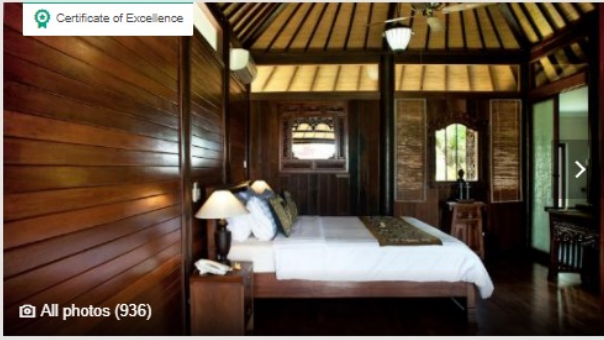
Apr 8 Apr 20

1 room, 1 adult, 0 children

SAVE \$11			
Expedia	\$69	View Deal >	
	\$58		
SAVE \$11			
Hotels.com	\$69	View Deal >	
	\$58		
SAVE \$11			
ORBITZ	\$69	View Deal >	
	\$58		
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 (589)

Room & Suite (230)

Pool & Beach (202)