

Digital Forensics and Investigations

IT8086 – DICS/PT/Class 1

20th August 2023

Digital Forensic Analysis Report

The Lone Wolf Scenario 2018

Prepared By

Priya d/o Manoharan – P7460509

Table of Contents

1. INTRODUCTION	3
1.1 Background	3
1.2 Summary Of Case and Tasking	4
1.3 Statement of Compliance	4
2. FORENSIC EXAMINATION	4
2.1 Tools	4
2.2 Chain of Custody	5
2.3 Evidence Classes	5
2.3.1 Evidence Class 1 – Partitions and File Types.....	6 & 7
2.3.2 Evidence Class 2 – Planning Documents	8 – 14
2.3.3 Evidence Class 3 – Jim Cloudy's Thought Process and Login Data ..	14 – 23
2.3.4 Evidence Class 4 – Emails Between Cloudy Brothers.....	24 – 26
2.3.5 Evidence Class 5 – Cloudy Cloud Storages	27
2.3.6 Evidence Class 6 – Recently Accessed Data	28
2.3.7 Evidence Class 7 – Webkit Browser History (Carving).....	28 & 29
2.3.8 Evidence Class 8 – Google Map Queries	29
2.3.9 Evidence Class 9 – Google Cached Images	29 – 33
2.3.10 Evidence Class 10 – Timeline.....	34
3. CONCLUSION	34
3.1 Summary of Findings:	34
4. ADDITIONAL INFORMATION	34
4.1 References	35
4.2 Resources	35
4.3 Sources	35
4.4 Tools	35

1. Introduction

This forensic report focuses on a case known as the “**Lone Wolf**”, where forensic analysis was conducted on a seized laptop by the police. The data was identified, preserved, and acquired by the Digital Evidence First Responder (DEFR). Subsequently, the Digital Evidence Specialists (DES) at the computer forensics lab analysed the data, providing corroborative evidence of the motivation and intent behind an alleged mass shooting plan.

This investigation was initiated after a concerning report was filed by Paul Cloudy, who is related to the suspect Jim Cloudy. This report led law enforcement to seize Jim Cloudy's laptop. The laptop drives and all contents were copied onto an SSD using the FTK Imager program, enabling a closer analysis of the digital evidence for suspicious activities.

Our analysis involves examining the hard drive, files, documents, images, and studying the temporary data in the laptop's memory (RAM) to gain insights into the motivations and intentions behind Jim Cloudy's actions. Additionally, this report includes a timeline of events and acknowledges individual contributions.

1.1. Background

Upon the seizure of the suspect's laptop, the acquisition was conducted on the **6th of April 2018**, Friday, using **AccessData® FTK® Imager 3.1.1.8**. The laptop's data was preserved, imaged, and stored as segmented files, labelled as **LoneWolf.E01** through **LoneWolf.E09**. The acquisition process commenced at 08:50:44 and concluded at 09:42:25. And the acquired date and time: **Friday, April 6 2018, 12:50:44**.

The image was verified with **MD5** and **SHA1** checksums, ensuring the integrity of the acquired data. The physical drive, a **Samsung SSD 850 PRO 512GB**, was preserved as a physical evidentiary item for further analysis in the Lone Wolf scenario investigation.

Item 1 – Identification details for Lone Wolf case

Description	Laptop's Data
Acquired Using	AccessData® FTK® Imager 3.1.1.8
Drive Model	Samsung SSD 850 PRO 512GB
Drive Serial Number	S250NSAG505708H
File Name of Image	LoneWolf.E01 to LoneWolf.E09
MD5 (Verified)	7af48fa65519e84246b1729e5b68f140
SHA1 (Verified)	694e26624d1ea029eb50d793b198edf85be4b4fc

1.2. Summary of Case and Tasking

The case codenamed for investigation, “**Lone Wolf**” revolves around the planning undertaken by the suspect, Jim Cloudy, who left digital footprints on his laptop and cloud accounts. The main objective of this forensic report is to systematically extract and compile evidence obtained from the seized laptop. This compilation of pieces of evidence will help us understand Jim Cloudy’s intentions and motivations behind the alleged mass shooting plan.

1.3. Statement of Compliance

In preparing this report, I acted as a Digital Evidence Specialist to present my findings with accuracy and fairness. My aim is to provide a clear and unbiased account of the digital forensics’ findings presented in this report at the time of assessment.

2. Forensic Examination

The forensic examination section outlines digital evidence analysis process, including the tools employed, chain of custody procedures, and the classification of evidence classes.

2.1. Tools

■ Imaging Software Tool:

➤ AccessData FTK Imager 3.1.1.8:

- This tool ensures the original digital evidence remains unaltered during the preservation process. This maintains the chain of custody and the integrity of the evidence. The files are then compressed and encapsulated into what we call an image of the drive, designated with the “.E01” extension.

■ Artefact Extraction and Analysis Tools:

➤ Magnet Axiom Process and Examine Version 5.8.0.27495:

- This tool allowed us to manage large volumes of digital evidence, including operating system data, file and folder system artifacts, as well as deleted file fragments and unallocated space.

➤ Autopsy 4.20.0:

- Additionally, the Autopsy tool enabled the extraction of the entire C drive folder attributed to the user “Jim Cloudy”.

2.2. Chain of Custody

Consultant Name	Priya Manoharan	ID	P7460509
Auditee	Jim Cloudy		
Date Seized	April 6 th 2018	Time Seized	05:35:02 AM
Location of Seizure	5850 Cameron Run Terrace, Alexandria, VA 22303, USA		

Description of Evidence		
Item #	Quantity	Description of Item [Model, OS, Hostname]
1	1	Dell Latitude E6430 Windows 10 Education DESKTOP-PM6C56D

Chain of Custody		
Case Number	Offense	
LoneWolf_001	"Mass Shooting Plot Suspected"	
Digital Evidence First Responder	Tom Moore	
Digital Evidence Specialists	Tom Moore	Priya Manoharan
Submitting Officer	Priya Manoharan	ID P7460509
Suspect	Jim Cloudy	

2.3. Evidence Classes

In line with the investigation requirements and our objective, we centred on obtaining crucial evidence to support our investigation of Jim Cloudy's alleged mass shooting plan.

Evidence Class	Description	Type
1	Partitions, File Types, Data Artifacts	Autopsy Tree folders
2	Planning Documents	docx, pdf, pptx
3	Thought Process and Login Data	Gmail, gdoc → docx, txt Microsoft Notebook onepkg
4	Emails Between Cloudy Brothers	Gmail, Lonewolf.mbox
5	Cloudy Cloud Storages	Amazon S3 Bucket, Box, Dropbox, Google Drive
6	Recently Accessed Data	Memdump.mem
7	Webkit Browser History (Carving)	Memdump.mem
8	Google Maps Queries	Memdump.mem
9	Google Cached Images	Image/jpeg
10	Timeline	Autopsy Timeline Graph

2.3.1. Evidence Class 1 – Partitions and File Types

In the LoneWolf.E01 image file, there are a total of 6 volumes of partitions found. Under ID number “**vol 7 (Basic Data Partition: 1259520-1000214527)**” as shown in the image below, the item that was particularly significant was the folder named “**jcloudy**”.

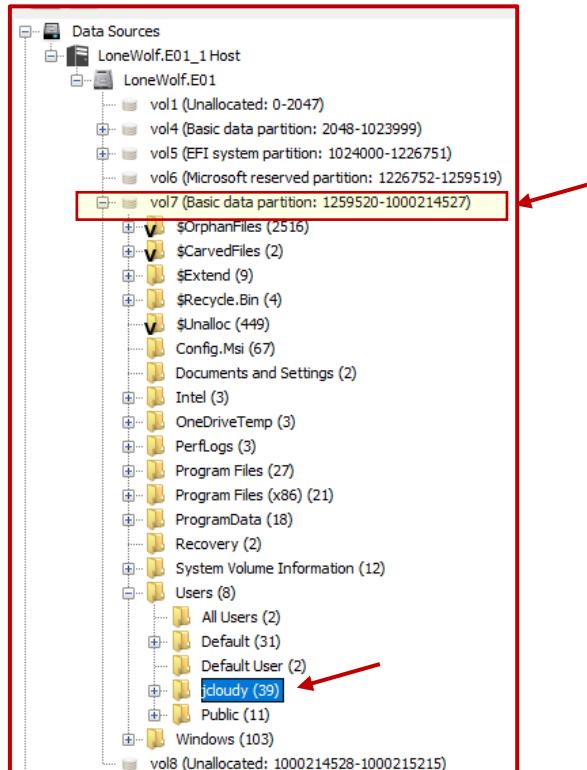


Fig.1

The pie chart below displays the file types and the count of data for “**Vol 7**”. The most notable ones are images, videos, audio, documents, executables, unknown, and other.

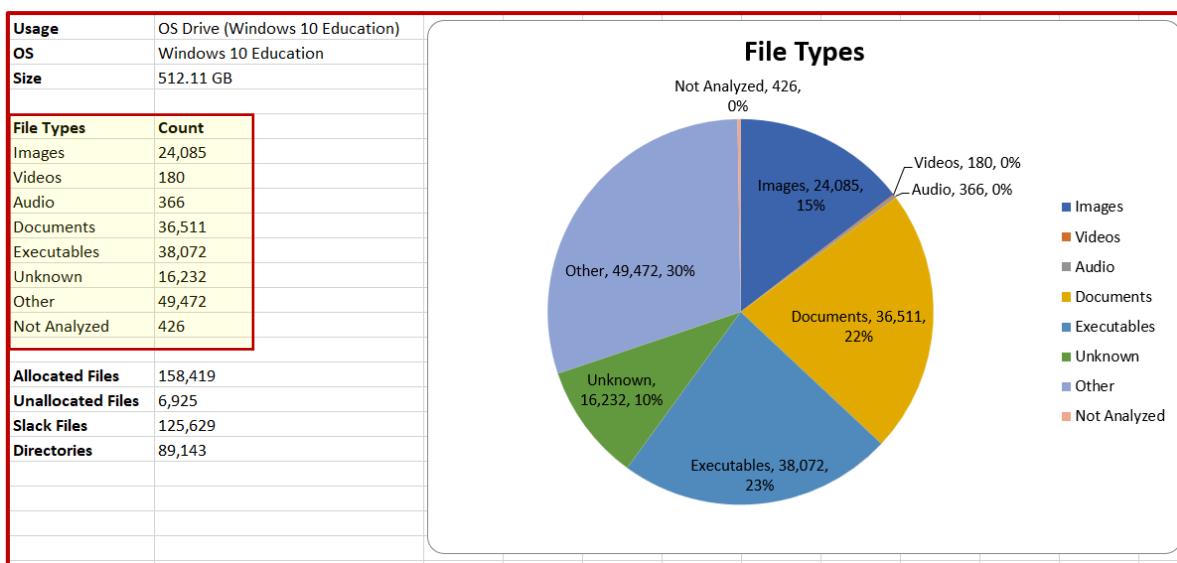
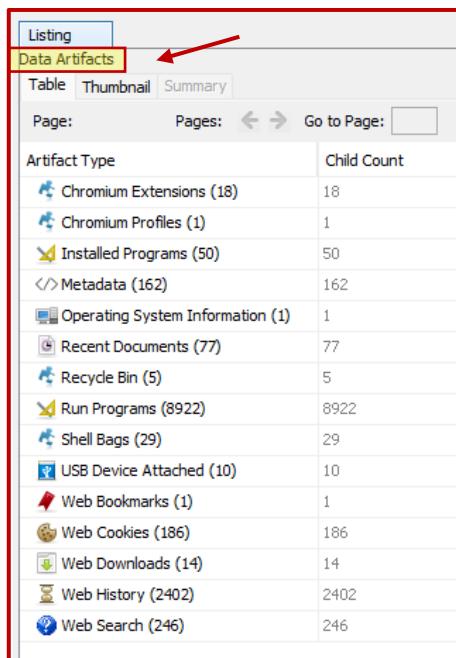


Fig.2

Based off of the pie chart, Autopsy extracted and listed notable data from the suspect's "**jcloudy**" account under the "**Data Artifacts**" folder. It listed what documents, programs, and web searches were made by the suspect.

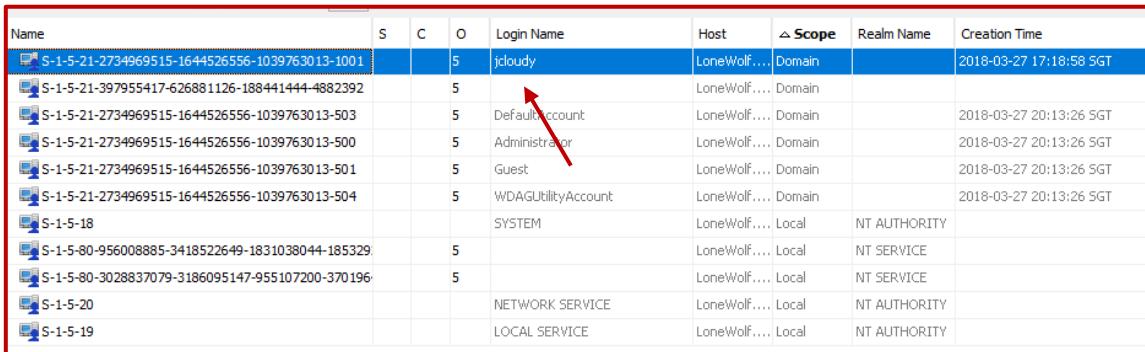


The screenshot shows a table titled "Data Artifacts" with a red arrow pointing to the tab. The table lists various artifact types and their counts:

Artifact Type	Child Count
Chromium Extensions (18)	18
Chromium Profiles (1)	1
Installed Programs (50)	50
Metadata (162)	162
Operating System Information (1)	1
Recent Documents (77)	77
Recycle Bin (5)	5
Run Programs (8922)	8922
Shell Bags (29)	29
USB Device Attached (10)	10
Web Bookmarks (1)	1
Web Cookies (186)	186
Web Downloads (14)	14
Web History (2402)	2402
Web Search (246)	246

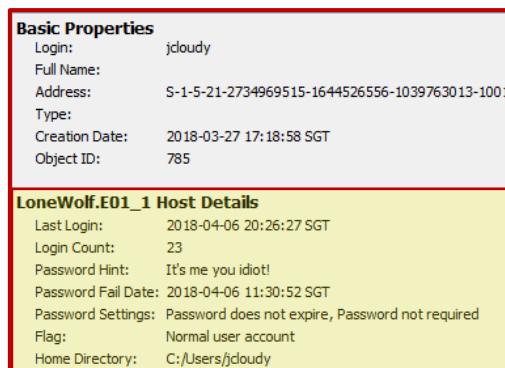
Fig.3

And within the same tree folder's "**OS Accounts**", we can see the login name "**jcloudy**".



The screenshot shows a table of OS accounts with a red arrow pointing to the "Login Name" column for the first row, which is "jcloudy".

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-21-2734969515-1644526556-1039763013-1001			5	jcloudy	LoneWolf....	Domain		2018-03-27 17:18:58 SGT
S-1-5-21-397955417-626881126-188441444-4882392			5		LoneWolf....	Domain		
S-1-5-21-2734969515-1644526556-1039763013-503			5	DefaultAccount	LoneWolf....	Domain		2018-03-27 20:13:26 SGT
S-1-5-21-2734969515-1644526556-1039763013-500			5	Administrator	LoneWolf....	Domain		2018-03-27 20:13:26 SGT
S-1-5-21-2734969515-1644526556-1039763013-501			5	Guest	LoneWolf....	Domain		2018-03-27 20:13:26 SGT
S-1-5-21-2734969515-1644526556-1039763013-504			5	WDAGUtilityAccount	LoneWolf....	Domain		2018-03-27 20:13:26 SGT
S-1-5-18				SYSTEM	LoneWolf....	Local	NT AUTHORITY	
S-1-5-80-956008885-3418522649-1831038044-185329			5		LoneWolf....	Local	NT SERVICE	
S-1-5-80-3028837079-3186095147-955107200-370196			5		LoneWolf....	Local	NT SERVICE	
S-1-5-20				NETWORK SERVICE	LoneWolf....	Local	NT AUTHORITY	
S-1-5-19				LOCAL SERVICE	LoneWolf....	Local	NT AUTHORITY	

Fig.4


Basic Properties

Login:	jcloudy
Full Name:	
Address:	S-1-5-21-2734969515-1644526556-1039763013-1001
Type:	
Creation Date:	2018-03-27 17:18:58 SGT
Object ID:	785

LoneWolf.E01_1 Host Details

Last Login:	2018-04-06 20:26:27 SGT
Login Count:	23
Password Hint:	It's me you idiot!
Password Fail Date:	2018-04-06 11:30:52 SGT
Password Settings:	Password does not expire, Password not required
Flag:	Normal user account
Home Directory:	C:/Users/jcloudy

Fig.5

2.3.2. Evidence Class 2 – Planning Documents

These evidence artefacts were obtained from Jim Cloudy's user account “**jcloudy**”. The evidences unfold his plans to commit a mass shooting in the future. **Each evidence has a hash value** that has been computed to demonstrate the original integrity of the file as imaged from the suspect's laptop retained. No alterations were made on any files.

Item 2 – Exhibit A – Planning.docx

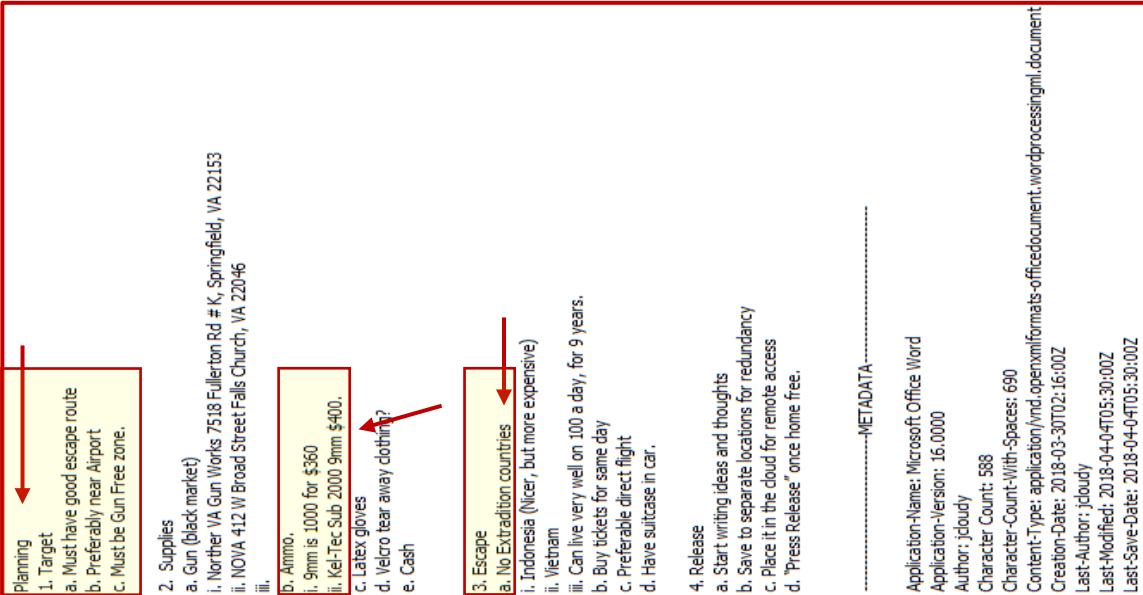
Exhibit A											
File Name	Planning.docx										
File Path	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/Planning.docx										
MD5	4ef414e469b7830faa2db429fe1321ee										
SHA256	0d87fa0cb21fd3cd3e2eab41149e611593f0c6a5224ed264cd5632692c126e12										
Created	Friday, 30 March 2018, 10:16:48 am										
Modified	Wednesday, 4 April 2018, 1:30:41 pm										
Accessed	Thursday, 17 August 2023, 12:14 pm										
Metadata:	Application-Name: Microsoft Office Word Application-Version: 16.0000 Author: jcloudy Character Count: 588 Character-Count-With-Spaces: 690 Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document Creation-Date: 2018-03-30T02:16:00Z Last-Autho r : jcloudy Last-Modified: 2018-04-04T05:30:00Z Last-Save-Date: 2018-04-04T05:30:00Z Line-Count: 4 Page-Count: 1 Paragraph-Count: 1 Revision-Number: 9 Template: Normal Total-Time: 2635 Word-Count: 103 X-Parsed-By: org.apache.tika.parser.DefaultParser cp:revision: 9 creator: jcloudy date: 2018-04-04T05:30:00Z										
 <table border="1"> <tr> <td>Planning</td> <td> 1. Target a. Must have good escape route b. Preferably near Airport c. Must be Gun Free zone. </td> </tr> <tr> <td>2.</td> <td> Supplies a. Gun (black market) i. Northern VA Gun Works 7518 Fullerton Rd # K, Springfield, VA 22153 ii. NOVA 412 W Broad Street Falls Church, VA 22046 iii. </td> </tr> <tr> <td></td> <td> d. Ammo. i. 9mm is 1000 For \$360 ii. Fel-Tec Sub 2000 9mm \$400. c. Latex gloves d. Velcro tear away clothing? e. Cash </td> </tr> <tr> <td></td> <td> 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. </td> </tr> <tr> <td></td> <td> 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. </td> </tr> </table>		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. Northern VA Gun Works 7518 Fullerton Rd # K, Springfield, VA 22153 ii. NOVA 412 W Broad Street Falls Church, VA 22046 iii.		d. Ammo. i. 9mm is 1000 For \$360 ii. Fel-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.
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. Northern VA Gun Works 7518 Fullerton Rd # K, Springfield, VA 22153 ii. NOVA 412 W Broad Street Falls Church, VA 22046 iii.										
	d. Ammo. i. 9mm is 1000 For \$360 ii. Fel-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.										

Fig.6

The above exhibit A table's *figure.6* screenshot contains the included metadata of the suspect's plot to commit a mass shooting at a specific location with a quick escape route that is near to an airport. He had plans to flee to countries with no extradition treaty with the U.S., and Indonesia, a country with no extradition laws, was mentioned. For weapons to be used for the planned mass shooting, suspect had chosen two types of ammunition.

Item 3 – Exhibit B – AIRPORT INFORMATION.docx

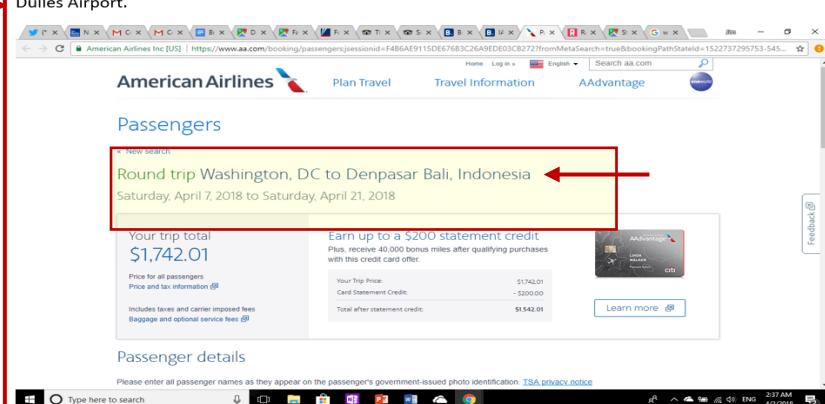
Exhibit B	
File Name	AIRPORT INFORMATION.docx
File Path	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/AIRPORT INFORMATION.docx
MD5	297eec248647f33f887d72328ab56f3c
SHA256	1fb5577d8559562d97ac3023e0ca91cc6b8b55d2e5fabaa81160c109f0abf9b6
Created	Friday, 30 March 2018, 10:29:57 am
Modified	Wednesday, 4 April 2018, 12:59:32 pm
Accessed	Thursday, 17 August 2023, 09:42 am
Metadata:	Application-Name: Microsoft Office Word Application-Version: 16.0000 Author: jcloudy Character Count: 215 Character-Count-With-Spaces: 251 Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document Creation-Date: 2018-03-30T02:29:00Z Last-Author: jcloudy Last-Modified: 2018-04-04T04:59:00Z Last-Save-Date: 2018-04-04T04:59:00Z Line-Count: 1 Page-Count: 1 Paragraph-Count: 1 Revision-Number: 9 Template: Normal Total-Time: 4701 Word-Count: 37 X-Parsed-By: org.apache.tika.parser.DefaultParser cp:revision: 9 creator: jcloudy date: 2018-04-04T04:59:00Z
AIRPORT INFORMATION Ronald Reagan has best record of on-time departures. Dulles has flights to Indonesia. With Layover in Qatar. 22 min from Fairfax County Democratic Committee, 8500 Executive Park Ave, Fairfax, VA 22031 to Dulles Airport.	
 A screenshot of a web browser displaying flight search results from American Airlines. The search is for a round trip from Washington, DC to Denpasar, Bali, Indonesia, departing on April 7, 2018, and returning on April 21, 2018. The total trip cost is \$1,742.01. The browser interface includes the American Airlines logo, travel information links, and a passengers section. A red arrow points to the search results box, and another red arrow points to the trip summary at the bottom of the page.	

Fig.7

Item 4 – Exhibit C – The Cloudy Manifesto.docx

Exhibit C

File Name	The Cloudy Manifesto.docx
File Path	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/The Cloudy Manifesto.docx
MD5	14c07920ddc81fdbd489e61d60e5c9f28
SHA256	fee91c8bafb9fb51574b11bfeed5a08b89e7bb90e874c07d95562c76380f2c65
Created	Monday, 2 April 2018, 9:35:27 am
Modified	Monday, 2 April 2018, 9:35:27 am
Accessed	Thursday, 17 August 2023, 02:23 pm
Metadata:	<p>Application-Name: Microsoft Office Word Application-Version: 16.0000 Author: jcloudy Character Count: 4087 Character-Count-With-Spaces: 4795 Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document Creation-Date: 2018-04-02T01:00:00Z Last-Author: jcloudy Last-Modified: 2018-04-02T01:35:00Z Last-Save-Date: 2018-04-02T01:35:00Z Line-Count: 34 Page-Count: 7 Paragraph-Count: 9 Revision-Number: 1 Template: Normal Total-Time: 35 Word-Count: 717 X-Parsed-By: org.apache.tika.parser.DefaultParser cp:revision: 1 creator: jcloudy date: 2018-04-02T01:35:00Z</p>

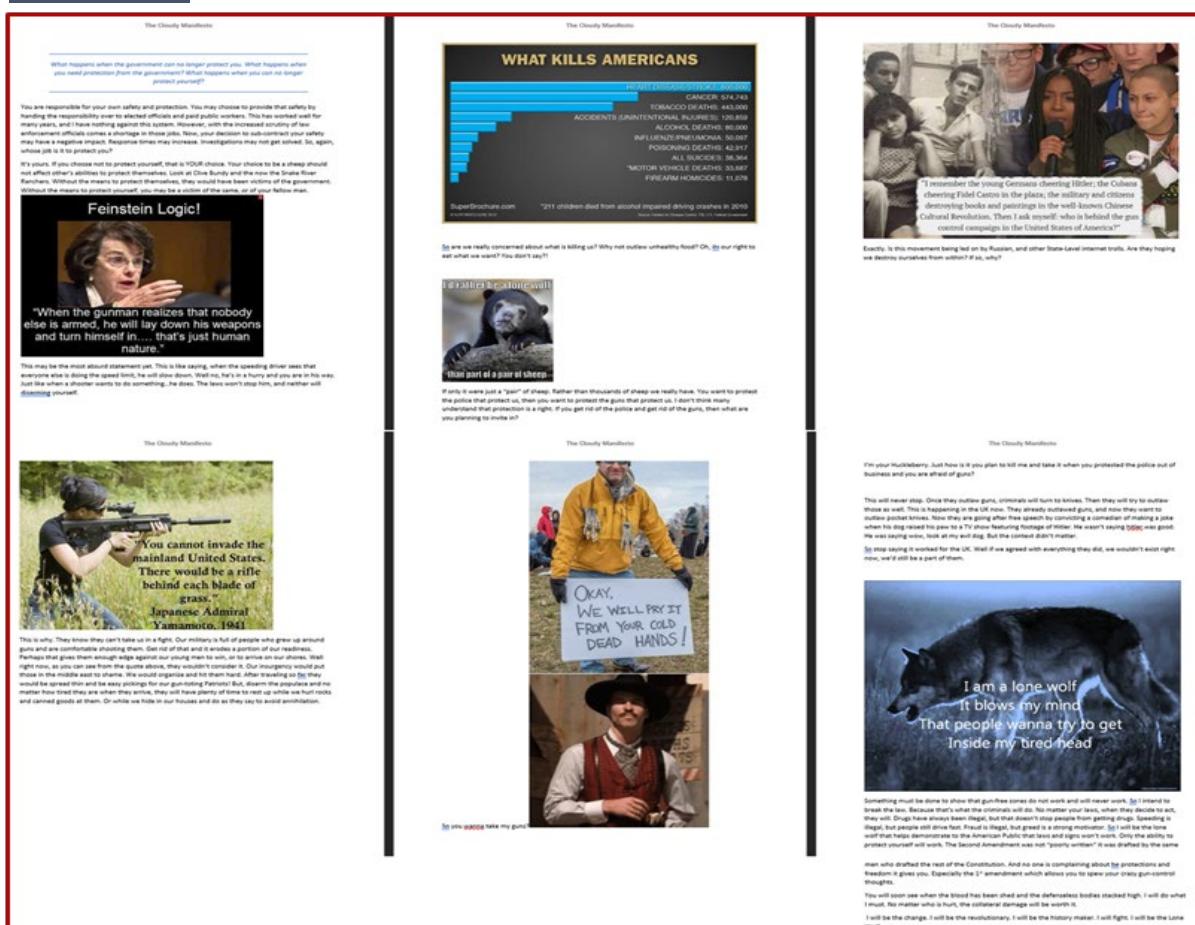


Fig 8

Item 5 – Exhibit D.00A – Operation 2nd Hand Smoke.pptx

Exhibit D.00A

File Name	Operation 2nd Hand Smoke.pptx
File Path	/img_LoneWolf.E01/vol_vo17/Users/jcloudy/Desktop/Operation 2nd Hand Smoke.pptx
MD5	b301fbf4104fb64b566b076c12a5d113
SHA256	7b08d680f342f3d28a79c2a324bfd0576586958992cd738319aec3ccd5d1e129
Created	Wednesday, 4 April 2018, 12:56:19 pm
Modified	Wednesday, 4 April 2018, 1:11:27 pm
Accessed	Thursday, 17 August 2023, 02:43 pm
Metadata:	<p>Application-Name: Microsoft Office PowerPoint Application-Version: 16.0000 Author: jcloudy Content-Type: application/vnd.openxmlformats-officedocument.presentationml.presentation Creation-Date: 2018-04-04T04:32:32Z Last-Author: jcloudy Last-Modified: 2018-04-04T05:11:27Z Last-Save-Date: 2018-04-04T05:11:27Z Paragraph-Count: 4 Presentation-Format: Widescreen Revision-Number: 7 Slide-Count: 7 Total-Time: 33 Word-Count: 12 X-Parsed-By: org.apache.tika.parser.DefaultParser cp:revision: 7 creator: jcloudy date: 2018-04-04T05:11:27Z </p>

While compiling the PowerPoint presentation, he captured a series of screenshots along with the corresponding website URLs and taskbar date and time, storing them on his Microsoft OneDrive account.

Screenshot Metadata												
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flag(Dir)	Flag(Meta)	Known	Location
[parent folder]				2018-04-03 14:37:38 SGT	2018-04-03 14:37:38 SGT	2018-04-03 14:37:38 SGT	2018-03-27 17:50:13 SGT	256	Allocated	Allocated	Unknown	(img_LoneWolf.E01/vol_vo17/Users/jcloudy/Desktop/Operation 2nd Hand Smoke.pptx)
[current folder]				2018-04-04 13:00:44 SGT	2018-04-04 13:00:44 SGT	2018-04-04 13:00:44 SGT	2018-04-03 14:37:38 SGT	56	Allocated	Allocated	Unknown	(img_LoneWolf.E01/vol_vo17/Users/jcloudy/Desktop/Operation 2nd Hand Smoke.pptx)
2018-04-04(1).png	1	5		2018-04-04 13:25:29 SGT	2018-04-04 13:25:29 SGT	2018-04-04 13:25:29 SGT	2018-04-03 14:37:38 SGT	1789665	Allocated	Allocated	Unknown	(img_LoneWolf.E01/vol_vo17/Users/jcloudy/Desktop/Operation 2nd Hand Smoke.pptx)
2018-04-04(2).png	1	5		2018-04-04 13:00:44 SGT	2018-04-04 13:00:44 SGT	2018-04-04 13:00:44 SGT	2018-04-03 14:37:38 SGT	57023	Allocated	Allocated	Unknown	(img_LoneWolf.E01/vol_vo17/Users/jcloudy/Desktop/Operation 2nd Hand Smoke.pptx)
2018-04-04(3).png	1	5		2018-04-04 13:00:33 SGT	2018-04-04 13:00:33 SGT	2018-04-04 13:00:33 SGT	2018-04-04 13:05:33 SGT	96463	Allocated	Allocated	Unknown	(img_LoneWolf.E01/vol_vo17/Users/jcloudy/Desktop/Operation 2nd Hand Smoke.pptx)
2018-04-04(2).png	1	5		2018-04-04 13:00:08 SGT	2018-04-04 13:00:08 SGT	2018-04-04 13:00:08 SGT	2018-04-04 13:05:08 SGT	96915	Allocated	Allocated	Unknown	(img_LoneWolf.E01/vol_vo17/Users/jcloudy/Desktop/Operation 2nd Hand Smoke.pptx)
2018-04-04(3).png	1	5		2018-04-04 13:00:33 SGT	2018-04-04 13:00:33 SGT	2018-04-04 13:00:33 SGT	2018-04-04 13:05:33 SGT	96463	Allocated	Allocated	Unknown	(img_LoneWolf.E01/vol_vo17/Users/jcloudy/Desktop/Operation 2nd Hand Smoke.pptx)
2018-04-03(1).png	1	5		2018-04-03 14:39:37 SGT	2018-04-03 14:39:37 SGT	2018-04-03 14:39:37 SGT	2018-04-03 14:39:37 SGT	47019	Allocated	Allocated	Unknown	(img_LoneWolf.E01/vol_vo17/Users/jcloudy/Desktop/Operation 2nd Hand Smoke.pptx)

Fig.9

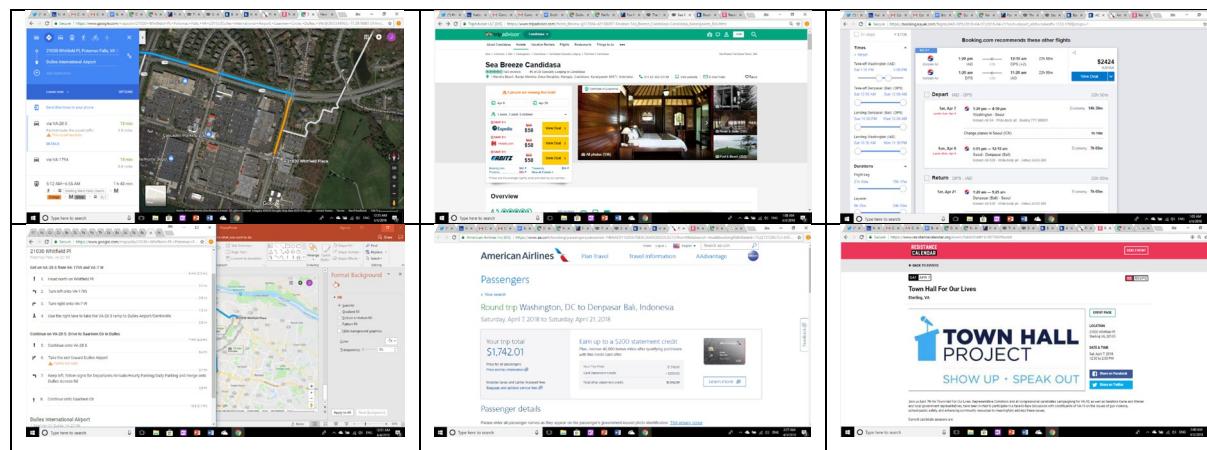


Table.1

Item 5 – Exhibit D.01A – Contents within Operation 2nd Hand Smoke.pptx

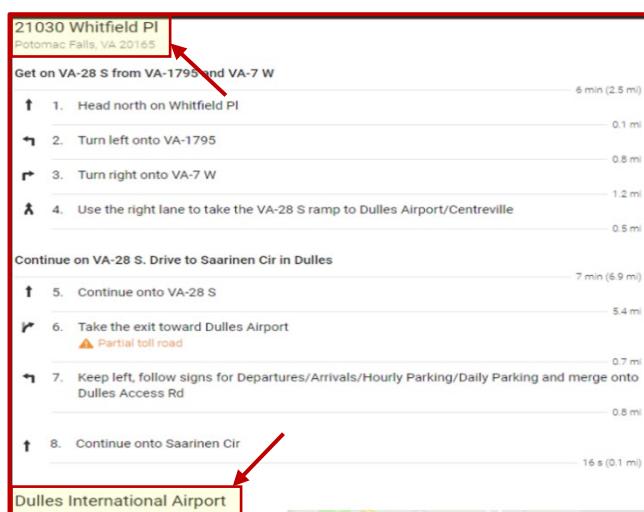
Exhibit D.01A

**Fig.10**

The *figure.10* screenshot on the left is the suspect's PowerPoint presentation "**Operation 2nd Hand Smoke**" that establishes where he intends to execute his plan.

Slide 2: shows the Town Hall Project (gun safety) event date, **Saturday April 7th 2018** and time **1230hrs** to **1400hrs**. **Location: Cascades Library, 21030 Whitfield place sterling, VA 20165.**

Slide 4 and 5 (figure.11 and 12): The suspect has colour coded the routes he intended to take to the Cascades Library and exit out towards the Dulles International airport.

**Fig.11****Fig.12**

Furthermore, the suspect had planned his flight, which departs from Washington at 1:20 pm (just before the Town Hall project event ending at 2 pm), and lands in Seoul at 4:50 pm. From Seoul, he travels to Denpasar (Bali, Indonesia), arriving at 12:10 am. Notably, Indonesia does not have extradition treaty laws with the US, which Jim Cloudy seemingly considered, as evidenced by his searches for lodging at the Sea Breeze Candidasa hotel. In figure.13 he made the destination searches at https://booking.kayak.com/flights/IAD-DPS/2018-04-07/2018-04-21?sort=depart_a&fs=takeoff=1330,1700|;stops=1 on 04/04/2018 at 05:04:23

AM. We were able to verify this search in memory dump file (see figure.14)

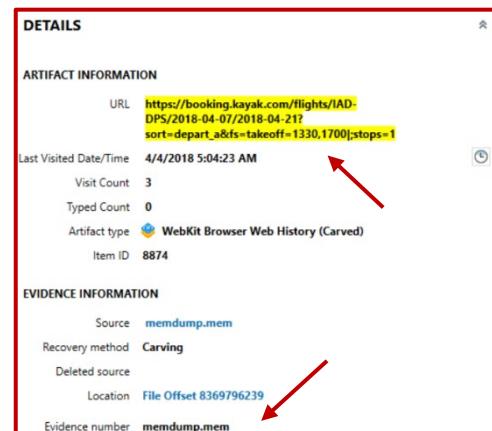
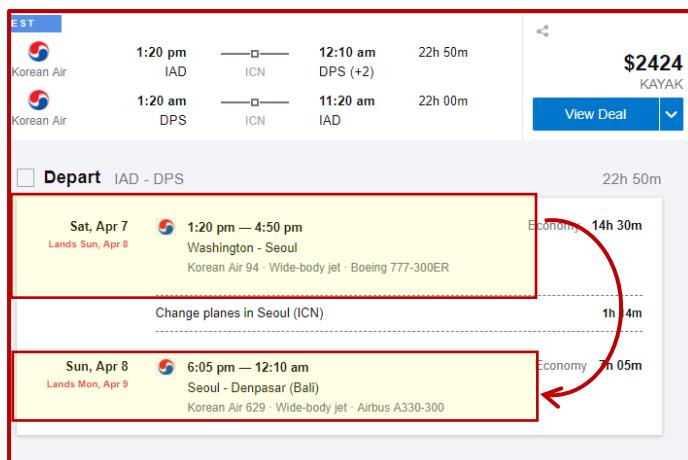


Fig.13

Fig.14

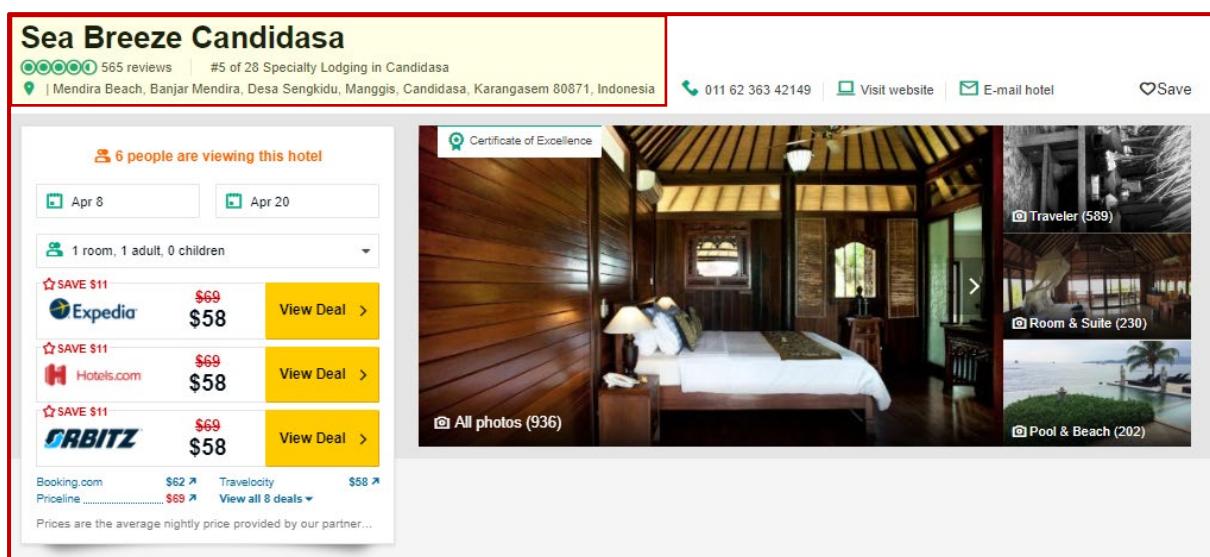


Fig.15

The series of information put together from the “**planning.docx**” document to “**The Cloudy Manifesto.docx**” document has yielded substantial insights into Jim Cloudy’s intentions. These documents reveal his intention to acquire ammunition, execute his “mass shooting plan” on the 7th of April 2018, and then meticulously chart a direct escape route from Cascades Library to Dulles International Airport, followed by his plan to flee to Indonesia.

Furthermore, documents curated by Jim Cloudy shed light on his perspectives on left-wing and right-wing politics, gun-control policies, the preservation of 2nd Amendment rights, and his stance on gun-free zones.

2.3.3. Evidence Class 3 – Thought process and Login Data

Item 6 – Exhibit E – Cloudy thoughts (4apr).docx

Exhibit E	
File Name	Cloudy thoughts (4apr).docx
File Path	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/Cloudy thoughts (4apr).docx
MD5	f8c2bc733c109a88405dfd13b47d0690
SHA256	37cd60bccb8cf01fd36be13d89e5df64749bcc072133d3bad1ed0c430e436dfd
Created	Thursday, 5 April 2018, 10:39:29 am
Modified	Thursday, 5 April 2018, 10:39:30 am
Accessed	Friday, 18 August 2023, 06:59 am
Metadata:	Application-Name: Microsoft Office Word Application-Version: 16.0000 Author: jcloudy Character Count: 986 Character-Count-With-Spaces: 1156 Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document Creation-Date: 2018-04-05T02:32:00Z Last-Author: jcloudy Last-Modified: 2018-04-05T02:39:00Z Last-Save-Date: 2018-04-05T02:39:00Z Line-Count: 8 Page-Count: 1 Paragraph-Count: 2 Revision-Number: 1 Template: Normal Total-Time: 7 Word-Count: 172 X-Parsed-By: org.apache.tika.parser.DefaultParser cp:revision: 1 creator: jcloudy date: 2018-04-05T02:39:00Z

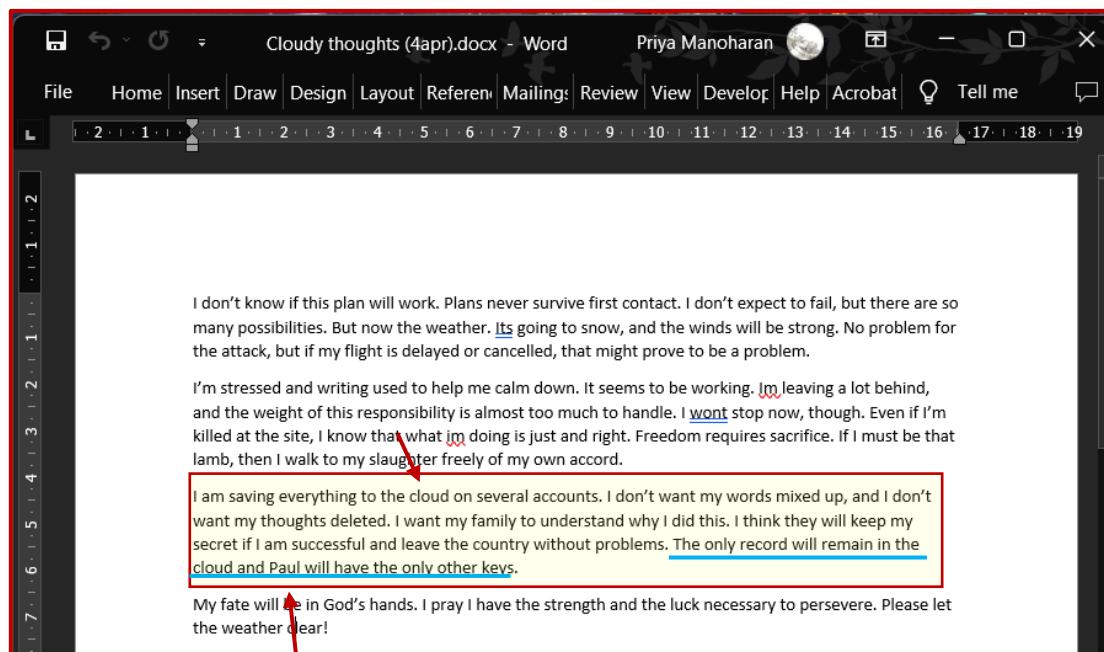


Fig.16

Item 7 – Exhibit F.00A – Gmail Webmail (memdump.mem)

Exhibit F.00A

DETAILS		DETAILS	
ARTIFACT INFORMATION		ARTIFACT INFORMATION	
Email(s)	me <jimcloudy1@gmail.com>, Paul <paulcloudy2@gmail.com> (6)	Email(s)	me <jimcloudy1@gmail.com>, Paul <paulcloudy2@gmail.com> (9)
Subject	Computer	Subject	Computer
Sent Date/Time - Local Time	Fri, Mar 30, 2018 at 8:58 PM	Sent Date/Time - Local Time	Sat, Mar 31, 2018 at 2:03 PM
Last Activity Date/Time	31/3/2018 12:58:09 AM	Last Activity Date/Time	31/3/2018 7:44:39 PM
Snippet	And how would YOU implement the solution? Unless you get elected its going to be hard to implement your own solutions... On Thu, Mar 29, 2018 at 10:14 PM, Jim Cloudy <jimcloudy1@gmail.com>	Snippet	I'm sure you are right, but its the ones with airtime that influence the policy. Without airtime, you cant get your message across. So you usually have to say or do something drastic to be heard.
Status	Read / Unread	Status	Read / Read
Artifact type	Gmail Webmail	Artifact type	Gmail Webmail
Item ID	8681	Item ID	11295
EVIDENCE INFORMATION		EVIDENCE INFORMATION	
Source	memdump.mem	Source	memdump.mem
Recovery method	Carving	Recovery method	Carving
Deleted source		Deleted source	
Location	File Offset 8250066462	Location	File Offset 10603766772
Evidence number	memdump.mem	Evidence number	memdump.mem
1		2	
DETAILS		DETAILS	
ARTIFACT INFORMATION		ARTIFACT INFORMATION	
Email(s)	Paul <paulcloudy2@gmail.com>	Email(s)	me <jimcloudy1@gmail.com>, Paul <paulcloudy2@gmail.com> (11)
Subject	Computer	Subject	Computer
Sent Date/Time - Local Time	Sat, Mar 31, 2018 at 2:03 PM	Sent Date/Time - Local Time	Sat, Mar 31, 2018 at 2:03 PM
Last Activity Date/Time	6/4/2018 6:57:20 AM	Last Activity Date/Time	4/4/2018 5:15:06 AM
Snippet	If you're up, jump on the chat doc real quick. On Wed, Apr 4, 2018 at 1:15 AM, Jim Cloudy <jimcloudy1@gmail.com> wrote: Hey man, meet me on the chat page. On Sat, Mar 31, 2018 at 4:08 PM, Jim	Snippet	Hey man, meet me on the chat page. On Sat, Mar 31, 2018 at 4:08 PM, Jim Cloudy <jimcloudy1@gmail.com> wrote: Just doing research on this stuff makes me think the government is watching me. Spooky
Status	Read	Status	Read / Read
Artifact type	Gmail Webmail	Artifact type	Gmail Webmail
Item ID	2562	Item ID	15507
EVIDENCE INFORMATION		EVIDENCE INFORMATION	
Source	memdump.mem	Source	memdump.mem
Recovery method	Carving	Recovery method	Carving
Deleted source		Deleted source	
Location	File Offset 2058754769	Location	File Offset 15734340058
Evidence number	memdump.mem	Evidence number	memdump.mem
4		3	

Fig.17

Gmail Webmail	Sent Date/Time - Local...	Last Activity...	Artifact...	Source	Recovery method	Location	Item ID
	Fri, Mar 30, 2018 at 8:58 PM	31/3/2018 12:58:09 AM	Gmail Webmail	memdump.mem	Carving	File Offset 8250066462	8681
	Fri, Mar 30, 2018 at 8:58 PM	31/3/2018 12:58:09 AM	Gmail Webmail	memdump.mem	Carving	File Offset 8250066678	8683
	Sat, Mar 31, 2018 at 2:03 PM	31/3/2018 7:44:39 PM	Gmail Webmail	memdump.mem	Carving	File Offset 10603766772	11295
	Sat, Mar 31, 2018 at 2:03 PM	31/3/2018 7:44:39 PM	Gmail Webmail	memdump.mem	Carving	File Offset 10603766988	11297
	Sat, Mar 31, 2018 at 2:03 PM	4/4/2018 5:15:06 AM	Gmail Webmail	memdump.mem	Carving	File Offset 15734340058	15507
	Sat, Mar 31, 2018 at 2:03 PM	4/4/2018 5:15:06 AM	Gmail Webmail	memdump.mem	Carving	File Offset 15734340274	15508
	Sat, Mar 31, 2018 at 2:03 PM	6/4/2018 6:57:20 AM	Gmail Webmail	memdump.mem	Carving	File Offset 2058754661	2561
	Sat, Mar 31, 2018 at 2:03 PM	6/4/2018 6:57:20 AM	Gmail Webmail	memdump.mem	Carving	File Offset 2058754769	2562

The email conversation between Jim Cloudy and Paul Cloudy revealed their exchanges often occurred through an alternative channel. They referred to it as “**chat page**” on their email. Through our analysis we were able to identify the “**chat page**” to be a Google document file titled as “**brother chat.gdoc**”.

Unfortunately, our attempts to fully explore the contents of this “**brother chat.gdoc**” document was stored in a cloud-based platform. As of 2023, Google and Outlook email accounts, along with their data, were erased. Thus, creating an obstacle in our examination. As a result, we were unable to access further insights from these cloud-based platforms.

However, during the initial course of digital forensics analysis in 2018, Tom Moore, our Digital Evidence First Responder (DEFR) and Digital Evidence Specialist (DES) was able to extract cloud-related data before it was permanently erased. This reclamation of information offers the potential to provide meaningful context to our ongoing investigation. To verify the Google document’s integrity, I used PowerShell to check its integrity and Autopsy.

```
PS C:\Users\Preeya\Desktop> Get-FileHash "Brother Chat.gdoc" -Algorithm SHA256
Algorithm      Hash                                     Path
----          ----
SHA256        09B278B3C798BDCC3E77EC5A10A3096B9B6C766E14E84655D54511AE5912DA19
C:\Users\Preeya\Desktop\Brother Chat.gdoc
```

Fig.18

The recovered Google document has been **converted** to one **word document** and one **text document** for us to access and analyse the contents within.

```
PS C:\Users\Preeya\Desktop> Get-FileHash "Brother Chat.docx" -Algorithm SHA256
Algorithm      Hash                                     Path
----          ----
SHA256        4C0F94A69BEF1CB327F6EC13C5D48026D43AD0AE07CC72A450338451BF6E2359
C:\Users\Preeya\Desktop\Brother Chat.docx
```

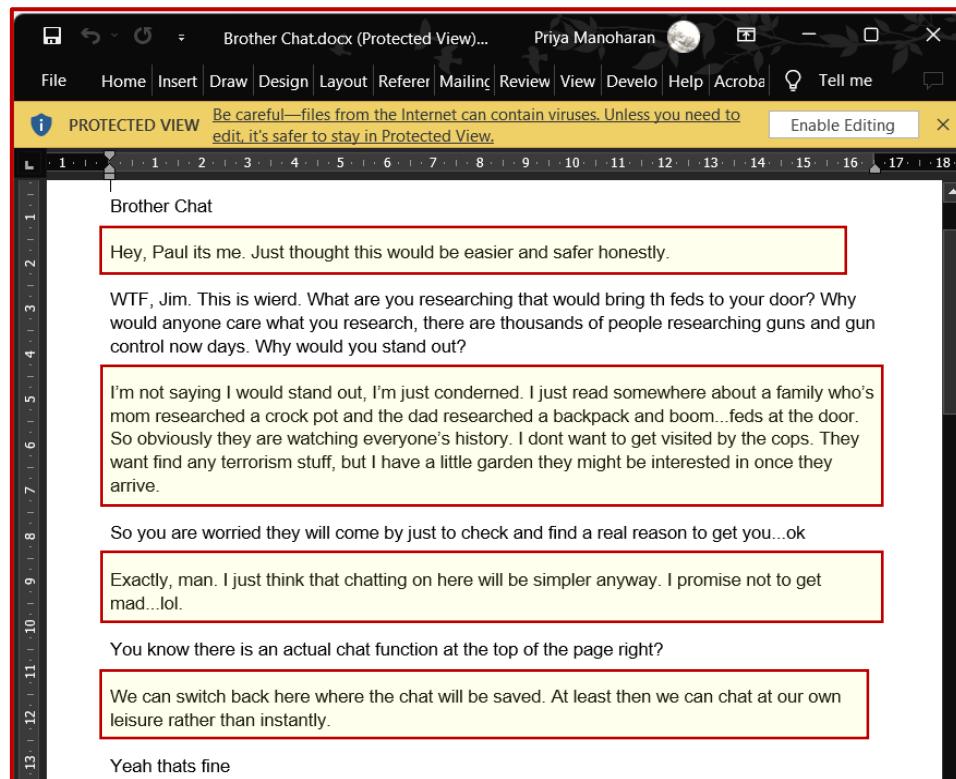
Fig.19

[SPACE INTENTIONALLY LEFT BLANK]

Item 7 – Exhibit F.01A – Brother Chat.gdoc (word version)**Exhibit F.01A**

File Name	Brother Chat.gdoc
File Path	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Google Drive/Brother Chat.gdoc
MD5	9eb42bf9159828639cc2f30214050e0f
SHA256	09b278b3c798bdcc3e77ec5a10a3096b9b6c766e14e84655d54511ae5912da19
Created	Sunday, 1 April 2018, 04:09:54 am
Modified	Friday, 6 April 2018, 15:20:00 pm
Accessed	Friday, 18 August 2023, 01:39 pm
DEFR & DES	Tom Moore

Chat 1: The red highlighted box is Jim.

**Fig.20**

[SPACE INTENTIONALLY LEFT BLANK]

Item 7 – Exhibit F.01B – Brother Chat.gdoc (word version)**Exhibit F.01B**

Chat 2: The red highlighted box is Jim.

Brother Chat.docx (Protected View)... Priya Manoharan

Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Edit

Hey, where you been man?

Just been busy the last couple of days

Oh ok

I'm just trying to get my head right. I've decided to go on vacation this weekend. Odd hours doing odd jobs, plus all the gun control nonsense has me pretty stressed.

THat might do you some good. Where to?/

Bali!

No way?! That would be tons of fun

How long?

Yeah it looked nice and I have the money, so why not.

Not sure how long. Who know, I might like it so much I dont come back...lol!

Gotta come back sometime...

You think I'm joking, man. But I'm not. Its super cheap over there. Ive got enough money to last the next 10 years...if im frivilous. And forever if I'm cheap and get a job.

Whoa whoa whoa.

You seriously are going to move to Indonesia....this weekend. No goodbye, no nothing, just gone? Have you lost your mind? Its not a question of money. What about your family?

You'd be able to visit, and I could come back maybe. I dunno. Not sure what will happen. I've heard its kinda dangerous though, so if anything happens to me I've got some papers and stuff I'd like you to have. I've got em stored on the cloud and I'll give you all the passwords and stuff before I leave.

What the hell do you mean, dangerous? Its a tourist spot. How dangerous can it be, unless you plan on making it dangerous! Whats going on man? Why dont you come over for a couple of days, and we can talk...you wont miss your flight..just give you some time with family and to talk things over.

Stop trying to talk me out of it. I've made up my mind. I'm going to Bali. I'll stay there a few days and then travel around Indonesia for a little while to see how things go. Clear my head, and if I decide that I want to come back I will.

Its spontaneous adventure...you know me.

Yeah, I do know you, the last time you had a spontaneous adventure you were gone for two years. You nearly killed a guy in a bar over a girl, then you just disappeared. So why are you disappearing now?

He wasnt nearly killed. And I'm not disappearing. I'm telling you where I'm going.

Worst case I'm gone until the political climate settles down a little. Then I come back and enjoy ole USA. i'll call you when I get there.

Youve lost your mind, but okay man.

We will miss you.

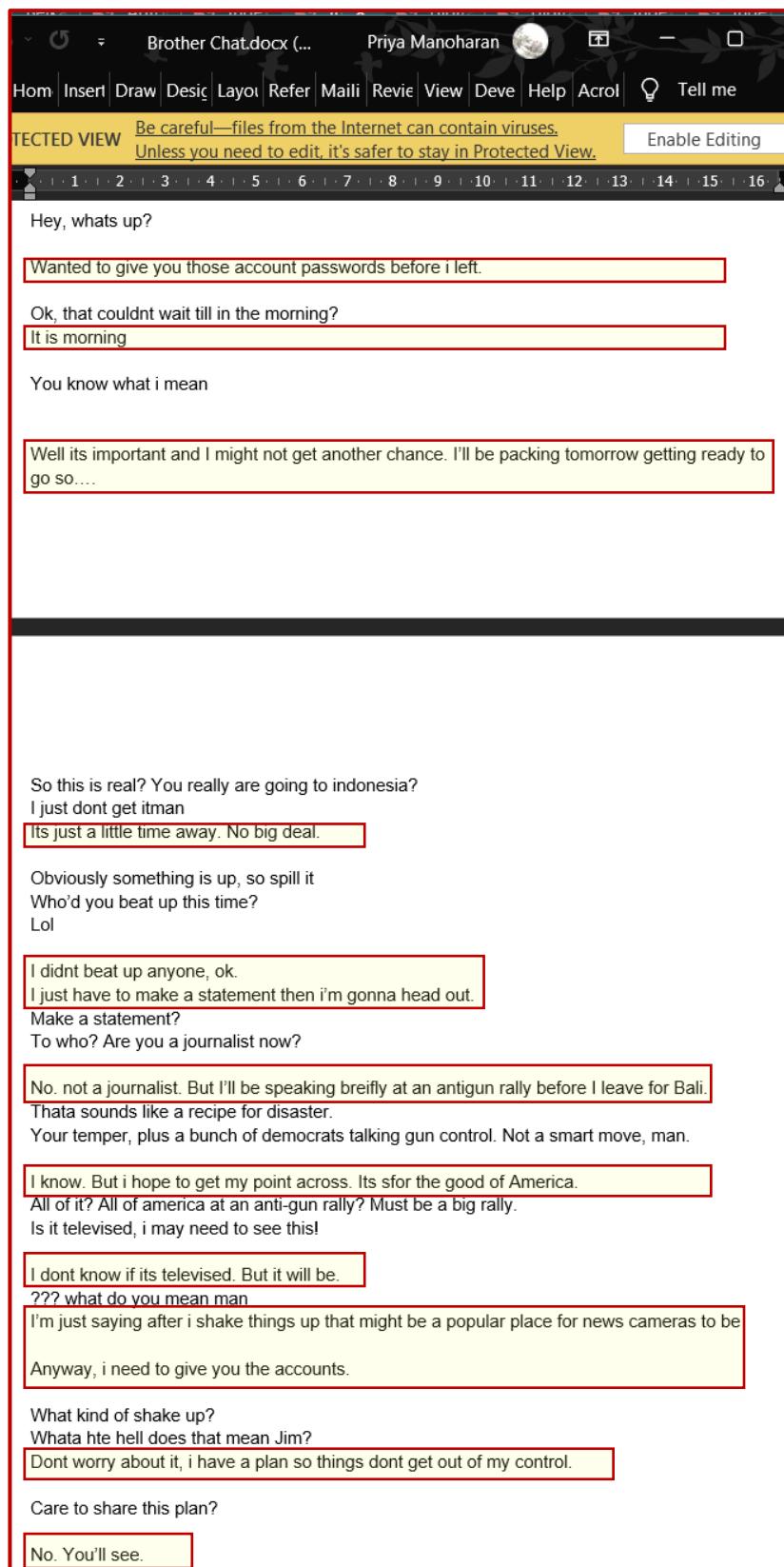
Yeah, dont tell the parents I'm gone until I'm gone. I dont want them driving up here.

Ok.

Fig.21

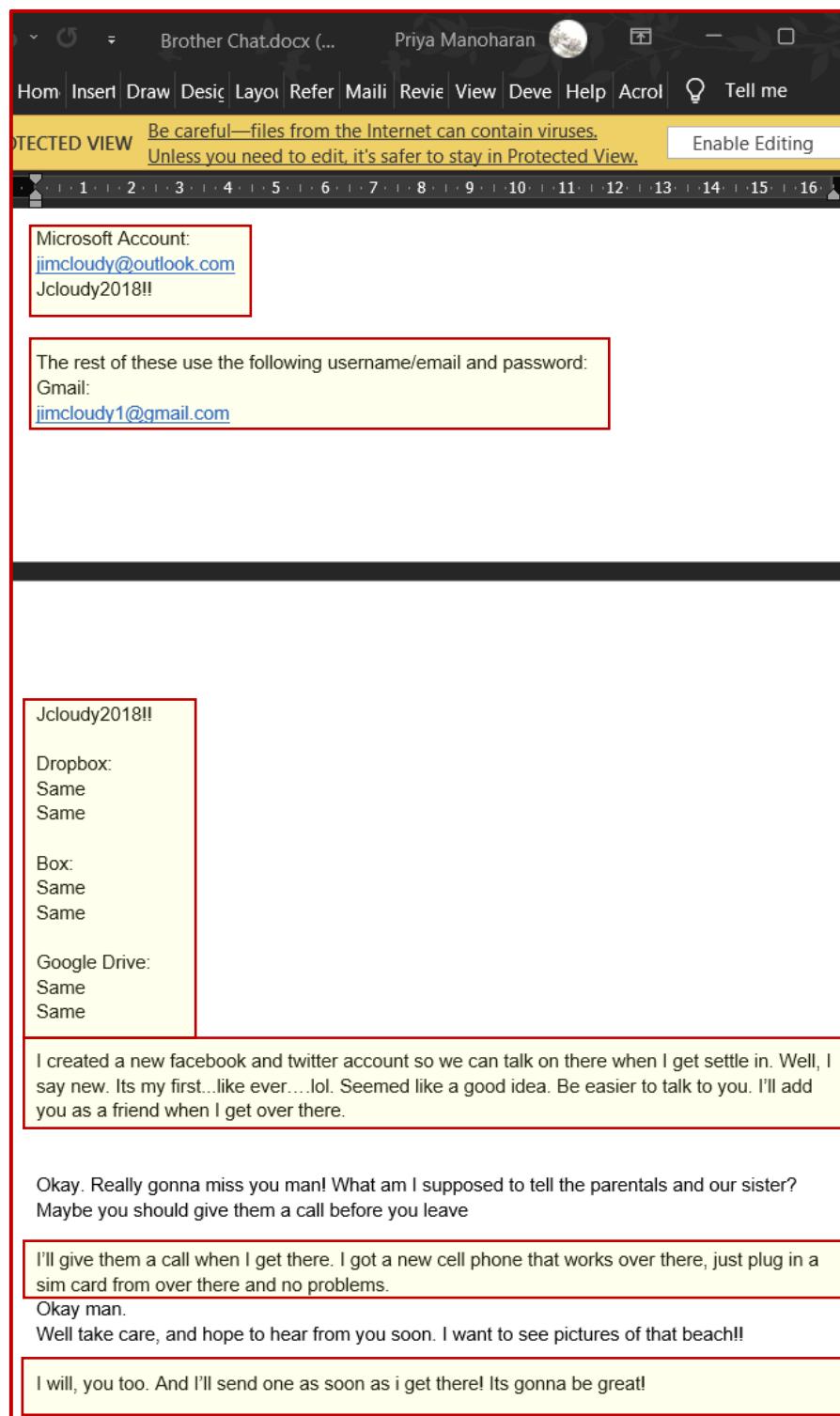
Item 7 – Exhibit F.01C – Brother Chat.gdoc (word version)**Exhibit F.01C**

Chat 3 Part I: The red highlighted box is Jim.

**Fig.22**

Item 7 – Exhibit F.01D – Brother Chat.gdoc (word version)**Exhibit F.01D**

Chat 3 Part II: The red highlighted box is Jim.

**Fig.23**

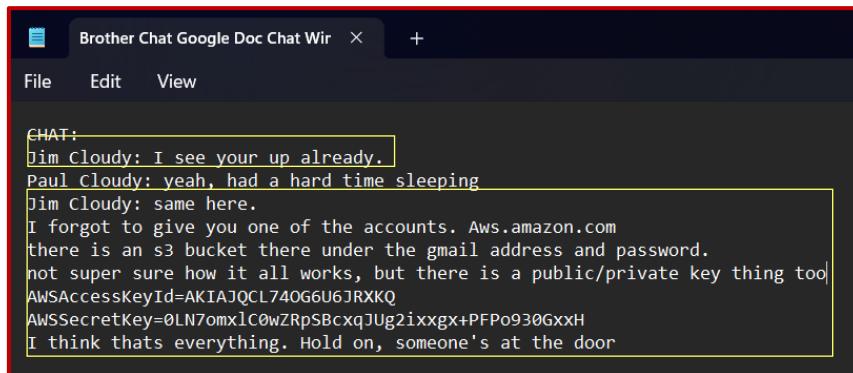
Item 7 – Exhibit F.02 – Brother Chat.gdoc (text version)

Exhibit F.02

PS C:\Users\Preeya\Desktop> Get-FileHash "Brother Chat Google Doc Chat Window.txt"	-Algorithm SHA256
Algorithm	Hash
SHA256	BA05EC7140440AD463B6FA4E7685CABE368CB96890132DD7D2828AC3BECA5534

Fig.24

Chat 4: The yellow highlighted box is Jim.

**Fig.25**

Item 7 – Exhibit F.03 – Login Data

Exhibit F.03

origin_url	action_url	username_element	username_value	password_element	password_value	signon_realm	prefer	form_data	possible_username_pairs
https://login.microsoftonline.com/common/oauth2/authorize	https://login.microsoftonline.com/common/login	loginfmt		passwd	07778772107???	https://login.microsoftonline.com/	0	SI	
https://www.dropbox.com/egister	https://www.dropbox.com/egister	email	jimcloudy1@gmail.com	password	07778772107???	https://www.dropbox.com/	1	Tl; http	<Cloudy
https://twitter.com/login	https://twitter.com/sessions	session(username_or_email)	jimcloudy1@gmail.com	session(passwor	d	https://twitter.com/	1	? lhttp	
https://login.live.com/login.srf	https://login.live.com/pssecure/post.srf	loginfmt	jimcloudy1@outlook.com	passwd	07778772107???	https://login.live.com/	1	? f1	
https://account.box.com/signup/n/personal	https://account.box.com/login/credentials	login	jimcloudy1@gmail.com	password	07778772107???	https://account.box.com/	1	<1	
https://signin.aws.amazon.com/signin	https://signin.aws.amazon.com/signin	resolving_input	jimcloudy1@gmail.com	password	07778772107???	https://signin.aws.amazon.com/	1	?Shttp	

Fig.26

I export this login data from Autopsy. These online accounts matches with the ones Jim Cloudy shared with his brother Paul Cloudy during their chat in the “**brother chat.gdoc**”. Together with this information, we noted Jim Cloudy has 2 email addresses. **Gmail: jimcloudy1@gmail.com** and **Microsoft Outlook: jimcloudy@outlook.com** that he used for his accounts.

[SPACE INTENTIONALLY LEFT BLANK]

Item 8 – Exhibit G – Jim's Notebook.url (onepkg)**Exhibit G**

File Name	Jim's Notebook.url
File Path	/img_LoneWolf.E01/vol_vo17/Users/jcloudy/OneDrive/Documents/Jim's Notebook.url
MD5	840fb715c63dc194fea68033a1c77844
SHA256	34130062b0dc3268b775fecc08d5316b3fc037c68df201049f4507c05785cf1f
Created	Tuesday, 27 March 2018, 17:50:14 pm
Modified	Friday, 6 April 2018, 12:03:46 pm
Accessed	Saturday, 19 August 2023, 01:34 pm
URL	[InternetShortcut] URL=https://onedrive.live.com/redir.aspx?cid=b5e4e06f22924dca&resid=B5E4E06F22924DCA!110&type=3

MATCHING RESULTS (23 of 556,806)

Item ID	Item	Artifact type	Artifact c...	Date and ti...	
426249	Jim's Notebook	Internet Explorer Favorites	Web Related		
426251	OneDrive	Cloud Services URLs	Refined Results		
517167	https://d.docs.live.net/b5e4e06f22924dca/Documents/Jim's Notebook	Potential Browser Activity	Web Related		
549092	https://d.docs.live.net/b5e4e06f22924dca/Documents/Jim's Notebook/	Potential Browser Activity	Web Related		
549095	https://d.docs.live.net/b5e4e06f22924dca/Documents/Jim's Notebook/	Potential Browser Activity	Web Related		
523529	https://onedrive.live.com/edit.aspx?cid=b5e4e06f22924dca&page=view...	Chrome Current Tabs	Web Related	2/4/2018 1:46:05 AM	
524247	https://onedrive.live.com/edit.aspx?cid=b5e4e06f22924dca&page=view...	Chrome Current Tabs	Web Related	5/4/2018 4:03:46 AM	
532535	Jim's Notebook.url	OneDrive	Cloud Storage	6/4/2018 4:03:46 AM	
524362	https://onedrive.live.com/edit.aspx?cid=b5e4e06f22924dca&page=view...	Chrome Current Tabs	Web Related	6/4/2018 4:07:45 AM	
529891	https://onedrive.live.com/edit.aspx?cid=b5e4e06f22924dca&page=view...	WebKit Browser Web History (Carved)	Web Related	6/4/2018 4:07:45 AM	
530833	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=15229876...	WebKit Browser Web History (Carved)	Web Related	6/4/2018 4:07:45 AM	
531739	https://onedrive.live.com/edit.aspx?cid=b5e4e06f22924dca&page=view...	Chrome Web History	Web Related	6/4/2018 4:07:45 AM	
532695	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=15229876...	Chrome Web History	Web Related	6/4/2018 4:07:45 AM	
335031	Jim's Notebook.url	UsnJrl	Operating System	6/4/2018 6:14:39 AM	
335032	Jim's Notebook.url	UsnJrl	Operating System	6/4/2018 6:14:39 AM	
335033	Jim's Notebook.url	UsnJrl	Operating System	6/4/2018 6:14:39 AM	
335034	Jim's Notebook.url	UsnJrl	Operating System	6/4/2018 6:14:39 AM	
335036	Jim's Notebook.url	UsnJrl	Operating System	6/4/2018 6:14:39 AM	
335037	Jim's Notebook.url	UsnJrl	Operating System	6/4/2018 6:14:39 AM	
335038	Jim's Notebook.url	UsnJrl	Operating System	6/4/2018 6:14:39 AM	
335039	Jim's Notebook.url	UsnJrl	Operating System	6/4/2018 6:14:39 AM	
335040	Jim's Notebook.url	UsnJrl	Operating System	6/4/2018 6:14:39 AM	

Fig.27

Tom Moore, (DEFR) and (DES) was able to extract the OneNote cloud-related data in 2018 before it was permanently erased.

[SPACE INTENTIONALLY LEFT BLANK]

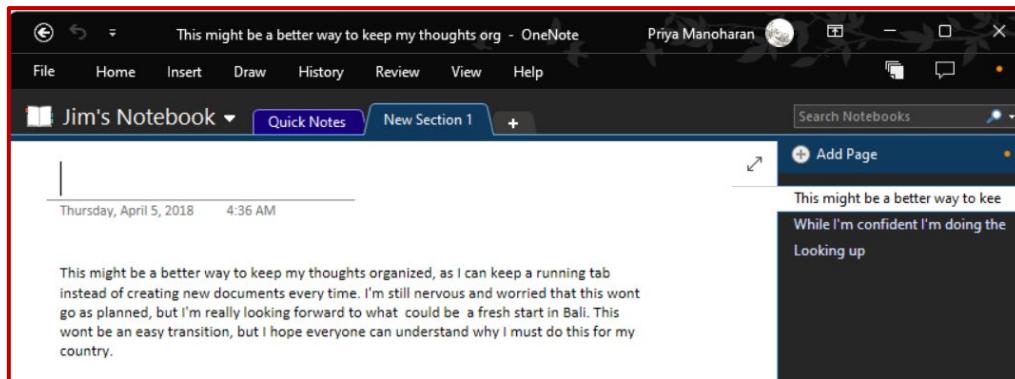


Fig.28

While I'm confident I'm doing the right thing, I can't be sure that it will work. Nor can I be sure that everyone will interpret my actions the way I mean them to be. That's why I left the manifesto and that's why I will continue to type here. I've been increasingly caught off guard by the level of deception being implemented by gun control Nazis. The use of crisis actors is certainly shocking. The use of child protestors/crisis actors is shockingly brilliant. They can say whatever they want, but if we rebut their lies, it's equated to child abuse. How dare you attack this teenager who is sharing our propaganda!

Reading an article now about a bomb that blew up at Sam's club.
<https://www.theblaze.com/news/2018/04/05/explosive-device-detonated-in-a-sams-club-second-device-found-in-suspects-car>

Bombs are illegal. You can't buy them at the store. Killers are going to kill regardless of the law. Cain killed Abel with a rock. Regardless of our laws criminals will break them to achieve their goals.

Taking away guns limits our ability to protect ourselves from criminals. But it also (surprise) limits our ability to protect ourselves from an abusive government. Sure, at this moment there isn't a big problem with the government oppressing us (just little ones), but that doesn't mean there won't be a problem in 100 years. Laws last until they are no longer needed. If it ever passed, a gun ban would never be repealed, for the same reason it passed. Guns are easy to point to, and any politician who tried to rally support to repeal would be looked at as though he didn't care about our safety. The gun Nazis will only get stronger, so it may be that the 2nd amendment will die regardless.

But if I can help delay that atrocity, then I'm willing to commit another atrocity. Operation 2nd Hand Smoke is a go on Saturday. A hundred targets. 2000 bullets. Endless freedom.

This guy gets it!
<https://www.theblaze.com/video/preach-gun-owner-slams-leftists-over-gun-violence-in-impassioned-speech-at-city-council> Wow! That's exactly it. If we give up our guns, the gangsters won't. It's illegal for the gangs to have guns now. But the cops don't have the ability to take them. But they can take the law-abiding citizens' guns, because they will abide by the law. They will do what the law says. And then the gangs will take over. Who's going to protect us then? Can't protect ourselves, the police are already overworked, and oh yeah, they are bad guys too apparently. They can't even protect themselves without being sued or retaliated against. So how are they going to protect us? They won't. They can't.

Fig.29

Looking up

Things are looking up. I've got my bags mostly packed already. Gave the account information to my brother, who at some point will probably read this. Hello. And it looks like the weather is clearing up for Saturday, so no snow delays! Maybe this is a sign from God. I am doing what I need to do for this country. With God on my side, I can't fail.

Fig.30

2.3.4. Evidence Class 4 – Emails Between Cloudy Brothers

During the analysis of the memory dump file, we uncovered Gmail fragments of emails between Jim Cloudy and Paul Cloudy from March 29th 2018 to March 31st 2018.

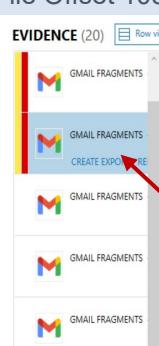
Item 9 – Exhibit H.00A – Gmail Fragments (4apr).docx

Exhibit H.00A

Artifact Type	Gmail Fragments
Item ID	5167
Source	Memdump.mem
Recovery Method	Carving
Location	File Offset 5585487736
Screenshot	 <p>The screenshot shows a list of Gmail fragments extracted from a memory dump. At the top, there is a 'CREATE EXPORT /' button. Below it, several entries are listed, each with a small Gmail icon and the word 'GMAIL FRAGMENTS'. The list continues down the page.</p>

Item 9 – Exhibit H.01A – Gmail Fragments (4apr).docx

Exhibit H.01A

Artifact Type	Gmail Fragments
Item ID	11568
Source	Memdump.mem
Recovery Method	Carving
Location	File Offset 10896461626
Screenshot	 <p>The screenshot shows a list of Gmail fragments extracted from a memory dump. At the top, there is a 'CREATE EXPORT /' button. Below it, several entries are listed, each with a small Gmail icon and the word 'GMAIL FRAGMENTS'. The list continues down the page.</p>

Based on the extraction done in 2018 by Tom Moore (DEFR and DES), we were able to analyse and reconstruct a clear picture of the entire conversation between the Cloudy brothers. It is in this email Sat, Mar 31st 2018, Jim Cloudy mentions of being watched by the government. This suggest that the “**AKMonitor.exe**” we found during our analysis indicts the law enforcement may have been logging his every move or it could be his psychology.

Item 9 – Exhibit H.02A – Google Takeout

Exhibit H.02A

Artifact Type	Gmail
Item ID	1_H.02A
Source	Tom Moore Analysis
Location	Google
<pre>--94eb2c0592f2013b3d0568baed5d--</pre> <p>From 1596791357101027798@xxx Wed Apr 04 05:15:05 +0000 2018 X-GM-THRID: 1596244801769939120 X-Gmail-Labels: LoneWolf,Sent MIME-Version: 1.0 Received: by 179.93.147.200 with HTTP; Tue, 3 Apr 2018 22:15:05 -0700 (PDT) In-Reply-To: <CAG5i1tn7xs3jyBHTf71tc17Tvu7wgTVVYBQHJGfvXJ4n_R+Njg@mail.gmail.com> References: <CAG5i1tPhrrLFxs+BmZT14H=iHjB028PoV2duQ0tmfjkplYaw@mail.gmail.com> <CAJ5GETiuWrjEGf0+xx+eNMwFHud3wRcb63E8z6HtwzjQuR6rRQ@mail.gmail.com> <CAG5i1tnJdv_qx15iGjcG9f5i+j=+OYhv7xhG0ZKgBbxH+6d0UQ@mail.gmail.com> <CAJ5GETgZjlBLckjZpVRToM=jX2rw8qQ1HBn6Sb1Aqd85AhGy1w@mail.gmail.com> <CAG5i1tn8gQ1_F7fqYfm2en70K2fftjb8sv2mjOHxaaA_FroMc@mail.gmail.com> <CAJ5GEThsV4C4VDCtNeugQa=5gJL2mQnR0c1+JHw_w4BsYwRg@mail.gmail.com> <CAG5i1tmfG06jq5=FwZ8pHuOUoK7mXRpEmb..rpza8H9aAC9=Ag@mail.gmail.com> <CAJ5GEThavB0t+kHXabNCMy8AS=pw1z6BKTsBaapYXvWbdzGFQg@mail.gmail.com> <CAG5i1tnsessP18dheof405PEs10jPqt3-R3-q2cbmqJH5EWMu@mail.gmail.com> <CAG5i1tn7xs1yBHTf71tc17Tvu7wgTVVYBQHJGfvXJ4n_R+Njg@mail.gmail.com></p> <p>Date: Wed, 4 April 2018 01:15:05 -0400 Delivered-To: jimcloudy@gmail.com Message-ID: <CAG5i1tmzXBgqyHiXREii+yRsqmzoYEj2NTR3PpmLxi+H=JcMQ@mail.gmail.com> Subject: Re: Computer From: Jim Cloudy <jimcloudy1@gmail.com> To: Paul Cloudy <paulcloudy2@gmail.com> Content-Type: multipart/alternative; boundary="089e08290fd4ed75000568fee7f9"</p> <p>--089e08290fd4ed75000568fee7f9 Content-Type: text/plain; charset="UTF-8" Hey man, meet me on the chat page.</p> <p>On Sat, Mar 31, 2018 at 4:08 PM, Jim Cloudy <jimcloudy1@gmail.com> wrote:</p> <p>> Just doing research on this stuff makes me think the government is > watching me. Spooky feeling. I'm sure they have no reason to, but I think > we should start talking over something that isn't email. I'll send you a > link to a google document, just open and type and I can see what you type > instantly. Its like an ad hoc chat program. ></p> <p>> On Sat, Mar 31, 2018 at 3:34 PM, Jim Cloudy <jimcloudy1@gmail.com> wrote: > >> I'm sure you are right, but its the ones with airtime that influence the >> policy. Without airtime, you cant get your message across. So you usually >> have to say or do something drastic to be heard. >> No idea when I'll be able to some by next. I know its not that far away, >> but its a pain to get loose from work and drive over there. Been thinking >> of taking a trip outside the country for awhile. I've got some vacation >> time saved up. >> >> On Sat, Mar 31, 2018 at 2:03 PM, Paul Cloudy <paulcloudy2@gmail.com> >> wrote: >> >>> That's probably not a fair representation of all Democrats. Those are >>> just the ones that get airtime because of their sensationalism. It's good >>> TV. But for those people, I don't think that any type of tragedy would ever >>> convince them that they were wrong. Even if they disarmed the entire >>> population, if a single gun got through and was used to kill someone, then >>> that would be enough to push for stricter controls. I'm not a fan of more >>> Government, but I do think that SOMETHING should be done. Stricter >>> background checks, longer waiting times, mandatory training, I don't know. >>> So when will you be home next?</p>	

Last email sent on the 4th of April 2018, 01:15:05 AM

Screenshot
(fig.31 – p1)

Item 9 – Exhibit H.02AA – Google Takeout**Exhibit H.02AA**

Artifact Type	Gmail
Item ID	1_H.02AA
Source	Tom Moore Analysis
Location	Google
Screenshot (fig.31 – p2)	<p>...</p> <p>>>> On Sat, Mar 31, 2018 at 12:28 AM, Jim Cloudy <jimcloudy1@gmail.com> >>> wrote: >>></p> <p>>>> Im not looking to get elected, but that doesnt mean I cant make a >>> difference. The insane logic behind some of what these gun control nuts are >>> saying...If I lay down my guns, the bad guys will lay down theres? And who >>> is causing all these riots and violent protests? Its not law abiding gun >>> owners! I dont want to live in a world where I have to rely on someone else >>> for my safety. I can take care of myself, at least until the cops arrive. >>> Its just dumb to think that we suddenly shoulndt need guns. Our huge gun >>> ownership is one reason why we've never been invaded! Who would dare? You >>> think the insurgency in Iraq was bad? But if Obama would have gotten his >>> way, NATO would have come here an taken them. Then what? We'd be under >>> occupation, AND unarmed. Who would come over next...it would be a turkey >>> shoot! Its gonna take something drastic for everyone to wake up, and thats >>> a shame.</p> <p>>>></p> <p>>>> On Fri, Mar 30, 2018 at 8:58 PM, Paul Cloudy <paulcloudy2@gmail.com> >>> wrote: >>></p> <p>>>>> And how would YOU implement the solution? Unless you get elected it's >>>> going to be hard to implement your own solutions... >>></p> <p>>>> On Thu, Mar 29, 2018 at 10:14 PM, Jim Cloudy <jimcloudy1@gmail.com> >>> wrote: >>></p> <p>>>>>> I told you on the phone I was sorry. Its just all the damn news >>>> stories are really getting to me. And yes I am thinking of solutions, I >>>> just dont know how to implement them yet. I'll let you know more after I've >>>> done some research.</p> <p>>>>></p> <p>>>>> On Thu, Mar 29, 2018 at 7:25 PM, Paul Cloudy <paulcloudy2@gmail.com> >>>> wrote: >>>></p> <p>>>>>> yes, I avoided the question, because your computer didn't die. You >>>> killed it because you didn't agree with me. I was trying to avoid you >>>> killing the one I just gave you. I understand what you are saying, but >>>> don't you believe that SOMETHING should be done to prevent gun deaths? >>>> Sure, maybe things have gotten better, but that doesn't mean we should stop >>>> improving. That's like saying, oh you're in 7th grade, you know so much >>>> more now than ever before, guess we should just stop here. Good luck. If >>>> you have some ideas for fixing things instead of complaining about everyone >>>> who does have ideas, then let me hear them.</p> <p>>>>></p> <p>>>>> On Thu, Mar 29, 2018 at 7:12 PM, Jim Cloudy <jimcloudy1@gmail.com> >>>> wrote: >>>></p> <p>>>>>> I see you avoided the 2nd amendment question... >>>> what i was trying to say the other day, before my computer died, >>>> was that i think its insane that we see fewer gun deaths than ever, and >>>> because of that we should now ban guns. No sense. No sense at all. It wont >>>> work for america, just like its not working for anywhere else. It makes >>>> even less sense that they want to ban guns at the same time they want to >>>> demonize the police. So who the hell is gonna help us now. We cant have >>>> guns, and the police all quit or are fired. So whats the plan? Are we gonna >>>> throw rocks at them they have in the schools now? Its just dumb. I >>>> dont get it.</p> <p>>>>></p> <p>>>>> On Thu, Mar 29, 2018 at 12:34 AM, Paul Cloudy < >>>> paulcloudy2@gmail.com> wrote: >>>></p> <p>>>>>> No problem, man! Let me know if you need anything else! I'm over >>>> at the parentals still...everyone says hello back! >>>> Take care and stay out of trouble! lol >>>> Paul >>>></p> <p>>>>></p> <p>>>>> On Thu, Mar 29, 2018 at 12:27 AM, Jim Cloudy <jimcloudy1@gmail.com> >>>> > wrote: >>>></p> <p>>>>>> Hey Paul!</p> <p>>>>>></p> <p>>>>>> I got the computer a couple of days ago. Its setup and running >>>>> now. Thanks again! What do you make of all this crap on the news? Guess I >>>>> should be more specific. The old retired Justice saying the 2nd amendment >>>>> should be repealed. Crazy, man. They really think that signs telling people >>>>> not to bring guns to a place will protect them. Bullshit.</p> <p>>>>>></p> <p>>>>>> Anyway, tell our lousy sister I said hello! Talk to you soon. >>>>> -Jim</p>

1st email sent on
the 29th of March
2018, 12:27 AM

2.3.5. Evidence Class 5 – Cloudy Cloud Storages

Item 10 – Exhibit I – Types of storages Jim Cloudy used

Exhibit I

Item ID	Item	Artifact type	Artifact c...	Date and time
3899	http://s3browser.com/	WebKit Browser Web History (Carved)	Web Related	27/3/2018 11:50:22 PM
3901	https://tntdrive.com/	WebKit Browser Web History (Carved)	Web Related	27/3/2018 11:48:21 PM
2735	https://s3.console.aws.amazon.com/s3/buckets/cloudy-thoughts/...	Potential Browser Activity	Web Related	
6002	https://s3.console.aws.amazon.com/s3/buckets/cloudy-thoughts/...	Potential Browser Activity	Web Related	
6087	https://s3.console.aws.amazon.com/s3/buckets/cloudy-thoughts/...	Potential Browser Activity	Web Related	
17146	https://s3.console.aws.amazon.com/s3/buckets/cloudy-thoughts/...	Potential Browser Activity	Web Related	
9919	https://s3.console.aws.amazon.com/s3/buckets/cloudy-thoughts/...	Potential Browser Activity	Web Related	

Fig.32

s3 Bucket uses AWS keys which were uncovered in the downloads folder together with the executable applications that showed what items he had installed.

Users > jcloudy > Downloads			
Name	Date modified	Type	Size
BoxSyncSetup.exe	28/3/2018 8:18 am	Application	35,372 KB
DropboxInstaller.exe	28/3/2018 8:03 am	Application	674 KB
installbackupandsync.exe	28/3/2018 7:40 am	Application	1,104 KB
s3browser-7-6-9.exe	28/3/2018 7:50 am	Application	2,426 KB
\$130	6/4/2018 4:30 pm	File	64 KB
rootkey.csv	28/3/2018 7:59 am	Microsoft Excel Co...	1 KB

Fig.33

The exact same keys, Jim Cloudy messaged Paul Cloudy in
“Item 7 – Exhibit F.02 – Brother Chat.gdoc (text version)”.

AWSAccessKeyId=AKIAJQCL74OG6U6JRXKQ

AWSSecretKey=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

Users > jcloudy > Box Sync > Desktop			
Name	Date	Type	Size
HoldMyTidePod.jpg	30/3/2018 11:29 am	JPG File	43 KB
MyTiredHead.jpg	30/3/2018 11:31 am	JPG File	106 KB
Sheep.jpg	30/3/2018 11:32 am	JPG File	11 KB
DarkWolf.png	30/3/2018 11:33 am	PNG File	590 KB
CubaDearmed.jpg	31/3/2018 5:22 am	JPG File	82 KB
BladeofGrass.jpg	31/3/2018 12:15 pm	JPG File	198 KB
DeathToll.jpg	31/3/2018 12:16 pm	JPG File	61 KB
RedGuns.jpg	31/3/2018 12:16 pm	JPG File	121 KB
DemLogic.jpg	31/3/2018 12:19 pm	JPG File	24 KB
Huckleberry.png	31/3/2018 12:23 pm	PNG File	300 KB
The Cloudy Manifes...	2/4/2018 9:35 am	Microsoft Word D...	798 KB
AIRPORT INFORMA...	4/4/2018 12:59 pm	Microsoft Word D...	169 KB
Operation 2nd Han...	4/4/2018 1:11 pm	Microsoft PowerPo...	4,306 KB
Planning.docx	4/4/2018 1:30 pm	Microsoft Word D...	14 KB

Fig.34 - BoxSync

Users > jcloudy > Dropbox			
Name	Date modified	Type	Size
Cubs' Anthony Rizzo Praises Parklan...	15/8/2023 9:23 pm	File folder	
Larry King_Time to Repeat the 'Poo...	15/8/2023 9:23 pm	File folder	
LARRYK-1.copy0	15/8/2023 9:23 pm	COPYD File	0 KB
\$130	6/4/2018 8:35 pm	File	8 KB
Cubs' Anthony Rizzo Praises Parklan...	5/4/2018 10:13 am	HTML File	280 KB
Larry King_Time to Repeat the 'Poo...	5/4/2018 10:13 am	HTML File	283 KB
BladeofGrass.jpg	5/4/2018 10:13 am	JPG File	198 KB
CubaDearmed.jpg	5/4/2018 10:13 am	JPG File	82 KB
DeathToll.jpg	5/4/2018 10:13 am	JPG File	61 KB
DemLogic.jpg	5/4/2018 10:13 am	JPG File	24 KB
HoldMyTidePod.jpg	5/4/2018 10:13 am	JPG File	43 KB
MyTiredHead.jpg	5/4/2018 10:13 am	JPG File	106 KB
RedGuns.jpg	5/4/2018 10:14 am	JPG File	121 KB
Sheep.jpg	5/4/2018 10:14 am	JPG File	11 KB
Operation 2nd Hand Smoke.pptx	4/4/2018 1:11 pm	Microsoft PowerPoint	4,306 KB
AIRPORT INFORMATION.docx	5/4/2018 10:13 am	Microsoft Word Doc...	169 KB
Planning.docx	5/4/2018 10:14 am	Microsoft Word Doc...	14 KB
The Cloudy Manifesto.docx	2/4/2018 9:35 am	Microsoft Word Doc...	798 KB
DarkWolf.png	5/4/2018 10:13 am	PNG File	590 KB
Huckleberry.png	5/4/2018 10:13 am	PNG File	300 KB
Box Sync	5/4/2018 10:13 am	Shortcut	2 KB
Dropbox	5/4/2018 10:13 am	Shortcut	2 KB
Google Drive	5/4/2018 10:13 am	Shortcut	2 KB

Fig.36 - Dropbox

Users > jcloudy > Google Drive			
Name	Date modified	Type	Size
\$130	4/4/2018 1:31 pm	File	4 KB
Brother Chat.gdoc	6/4/2018 3:20 pm	Google Docs	1 KB
Operation 2nd Hand Smoke.pptx	4/4/2018 1:11 pm	Microsoft PowerPo...	4,306 KB
The Cloudy Manifesto.docx	2/4/2018 9:35 am	Microsoft Word D...	798 KB

Fig.35 – Google Drive

2.3.6. Evidence Class 6 – Recently Accessed Data

During the analysis of the memory dump file, we searched for the programs he often ran, websites he accessed and what documents were recently opened.

Item 11 – Exhibit J – Recently Accessed data (memdump.mem)

Exhibit J																																													
Recent Program run times	<table border="1"> <thead> <tr> <th>Program</th><th>Folder</th><th>Run Times</th><th>Last Run</th></tr> </thead> <tbody> <tr><td>DROPBOXUPDATE.EXE</td><td>DROPBOX</td><td>200</td><td>2018/04/06 16:28:03</td></tr> <tr><td>CHROME.EXE</td><td>GOOGLE</td><td>90</td><td>2018/04/06 20:34:21</td></tr> <tr><td>NVTRAY.EXE</td><td>NVIDIA CORPORATION</td><td>54</td><td>2018/04/06 20:40:37</td></tr> <tr><td>GOOGLEUPDATE.EXE</td><td>GOOGLE</td><td>42</td><td>2018/04/06 16:34:27</td></tr> <tr><td>MPCMDRUN.EXE</td><td></td><td>19</td><td>2018/04/06 11:40:11</td></tr> <tr><td>DROPBOX.EXE</td><td>DROPBOX</td><td>10</td><td>2018/04/06 20:35:09</td></tr> <tr><td>OFFICECLICKTORUN.EXE</td><td>COMMON FILES</td><td>10</td><td>2018/04/06 20:29:30</td></tr> <tr><td>GOOGLEDRIVESYNC.EXE</td><td>GOOGLE</td><td>10</td><td>2018/04/05 09:53:42</td></tr> <tr><td>S3BROWSER-WIN32.EXE</td><td>S3 BROWSER</td><td>5</td><td>2018/04/05 14:06:42</td></tr> <tr><td>ONEDRIVE.EXE</td><td>AppData</td><td>5</td><td>2018/04/04 13:59:40</td></tr> </tbody> </table> <p>Types Recent Programs Recent Domains Recent Web Searches</p>	Program	Folder	Run Times	Last Run	DROPBOXUPDATE.EXE	DROPBOX	200	2018/04/06 16:28:03	CHROME.EXE	GOOGLE	90	2018/04/06 20:34:21	NVTRAY.EXE	NVIDIA CORPORATION	54	2018/04/06 20:40:37	GOOGLEUPDATE.EXE	GOOGLE	42	2018/04/06 16:34:27	MPCMDRUN.EXE		19	2018/04/06 11:40:11	DROPBOX.EXE	DROPBOX	10	2018/04/06 20:35:09	OFFICECLICKTORUN.EXE	COMMON FILES	10	2018/04/06 20:29:30	GOOGLEDRIVESYNC.EXE	GOOGLE	10	2018/04/05 09:53:42	S3BROWSER-WIN32.EXE	S3 BROWSER	5	2018/04/05 14:06:42	ONEDRIVE.EXE	AppData	5	2018/04/04 13:59:40
Program	Folder	Run Times	Last Run																																										
DROPBOXUPDATE.EXE	DROPBOX	200	2018/04/06 16:28:03																																										
CHROME.EXE	GOOGLE	90	2018/04/06 20:34:21																																										
NVTRAY.EXE	NVIDIA CORPORATION	54	2018/04/06 20:40:37																																										
GOOGLEUPDATE.EXE	GOOGLE	42	2018/04/06 16:34:27																																										
MPCMDRUN.EXE		19	2018/04/06 11:40:11																																										
DROPBOX.EXE	DROPBOX	10	2018/04/06 20:35:09																																										
OFFICECLICKTORUN.EXE	COMMON FILES	10	2018/04/06 20:29:30																																										
GOOGLEDRIVESYNC.EXE	GOOGLE	10	2018/04/05 09:53:42																																										
S3BROWSER-WIN32.EXE	S3 BROWSER	5	2018/04/05 14:06:42																																										
ONEDRIVE.EXE	AppData	5	2018/04/04 13:59:40																																										
Recent Domains Accessed	<table border="1"> <thead> <tr> <th>Domain</th><th>Visits</th><th>Last Accessed</th></tr> </thead> <tbody> <tr><td>google.com</td><td>1367</td><td>2018/04/06 20:26:22</td></tr> <tr><td>kayak.com</td><td>223</td><td>2018/04/04 13:04:23</td></tr> <tr><td>yahoo.com</td><td>103</td><td>2018/04/06 12:07:24</td></tr> <tr><td>amazon.com</td><td>102</td><td>2018/04/05 14:06:28</td></tr> <tr><td>box.com</td><td>72</td><td>2018/04/05 10:10:50</td></tr> <tr><td>gunbroker.com</td><td>65</td><td>2018/03/31 12:46:19</td></tr> <tr><td>live.com</td><td>56</td><td>2018/04/06 12:07:45</td></tr> <tr><td>weather.com</td><td>53</td><td>2018/04/06 16:25:53</td></tr> <tr><td>dropbox.com</td><td>44</td><td>2018/04/05 10:13:07</td></tr> <tr><td>youtube.com</td><td>34</td><td>2018/04/05 16:25:45</td></tr> </tbody> </table> <p>Recent Domains</p>	Domain	Visits	Last Accessed	google.com	1367	2018/04/06 20:26:22	kayak.com	223	2018/04/04 13:04:23	yahoo.com	103	2018/04/06 12:07:24	amazon.com	102	2018/04/05 14:06:28	box.com	72	2018/04/05 10:10:50	gunbroker.com	65	2018/03/31 12:46:19	live.com	56	2018/04/06 12:07:45	weather.com	53	2018/04/06 16:25:53	dropbox.com	44	2018/04/05 10:13:07	youtube.com	34	2018/04/05 16:25:45											
Domain	Visits	Last Accessed																																											
google.com	1367	2018/04/06 20:26:22																																											
kayak.com	223	2018/04/04 13:04:23																																											
yahoo.com	103	2018/04/06 12:07:24																																											
amazon.com	102	2018/04/05 14:06:28																																											
box.com	72	2018/04/05 10:10:50																																											
gunbroker.com	65	2018/03/31 12:46:19																																											
live.com	56	2018/04/06 12:07:45																																											
weather.com	53	2018/04/06 16:25:53																																											
dropbox.com	44	2018/04/05 10:13:07																																											
youtube.com	34	2018/04/05 16:25:45																																											
Recently Opened Documents	<table border="1"> <thead> <tr> <th>Path</th><th>Date</th></tr> </thead> <tbody> <tr><td>C:\Users\jcloudy\Downloads\rootkey.csv</td><td>2018/04/06 20:27:08</td></tr> <tr><td>No preferred path found</td><td>2018/04/06 16:31:50</td></tr> <tr><td>C:\Users\jcloudy\Desktop\LeftUsesBoycotts.pdf</td><td>2018/04/06 11:56:32</td></tr> <tr><td>C:\Users\jcloudy\Desktop\AMEN.pdf</td><td>2018/04/06 11:55:00</td></tr> <tr><td>C:\Users\jcloudy\Desktop\UKnifeBan.pdf</td><td>2018/04/05 13:51:41</td></tr> <tr><td>C:\Users\jcloudy\Desktop\SelfDefenseisMurder.pdf</td><td>2018/04/05 13:48:40</td></tr> <tr><td>C:\Users\jcloudy\Desktop\Cloudy thoughts (4apr).docx</td><td>2018/04/05 10:39:30</td></tr> <tr><td>C:\Users\jcloudy\Desktop</td><td>2018/04/05 10:24:19</td></tr> <tr><td>C:\Users\jcloudy\Desktop\Operation 2nd Hand Smoke.pptx</td><td>2018/04/04 12:56:20</td></tr> <tr><td>C:\Users\jcloudy\Desktop\The Cloudy Manifesto.docx</td><td>2018/04/02 09:35:27</td></tr> </tbody> </table> <p>Recently Opened Documents</p>	Path	Date	C:\Users\jcloudy\Downloads\rootkey.csv	2018/04/06 20:27:08	No preferred path found	2018/04/06 16:31:50	C:\Users\jcloudy\Desktop\LeftUsesBoycotts.pdf	2018/04/06 11:56:32	C:\Users\jcloudy\Desktop\AMEN.pdf	2018/04/06 11:55:00	C:\Users\jcloudy\Desktop\UKnifeBan.pdf	2018/04/05 13:51:41	C:\Users\jcloudy\Desktop\SelfDefenseisMurder.pdf	2018/04/05 13:48:40	C:\Users\jcloudy\Desktop\Cloudy thoughts (4apr).docx	2018/04/05 10:39:30	C:\Users\jcloudy\Desktop	2018/04/05 10:24:19	C:\Users\jcloudy\Desktop\Operation 2nd Hand Smoke.pptx	2018/04/04 12:56:20	C:\Users\jcloudy\Desktop\The Cloudy Manifesto.docx	2018/04/02 09:35:27																						
Path	Date																																												
C:\Users\jcloudy\Downloads\rootkey.csv	2018/04/06 20:27:08																																												
No preferred path found	2018/04/06 16:31:50																																												
C:\Users\jcloudy\Desktop\LeftUsesBoycotts.pdf	2018/04/06 11:56:32																																												
C:\Users\jcloudy\Desktop\AMEN.pdf	2018/04/06 11:55:00																																												
C:\Users\jcloudy\Desktop\UKnifeBan.pdf	2018/04/05 13:51:41																																												
C:\Users\jcloudy\Desktop\SelfDefenseisMurder.pdf	2018/04/05 13:48:40																																												
C:\Users\jcloudy\Desktop\Cloudy thoughts (4apr).docx	2018/04/05 10:39:30																																												
C:\Users\jcloudy\Desktop	2018/04/05 10:24:19																																												
C:\Users\jcloudy\Desktop\Operation 2nd Hand Smoke.pptx	2018/04/04 12:56:20																																												
C:\Users\jcloudy\Desktop\The Cloudy Manifesto.docx	2018/04/02 09:35:27																																												

2.3.7. Evidence Class 7 – Webkit Browser History (Carving)

Item 12 – Exhibit K – Webkit Browser History (Carving) (memdump.mem)

Exhibit K																																																																																																																																															
“Guns”	<table border="1"> <thead> <tr> <th>URL</th><th>Last Visited Date</th><th>Title</th><th>Visit Count</th><th>Source</th><th>Location</th><th>Evidence number</th><th>Recovery</th><th>Item ID</th></tr> </thead> <tbody> <tr><td>https://tntdrive.com/</td><td>27/3/2018 3:48</td><td>This New Race Gun Will Change EVERYTHING!!! - YouTube</td><td>1</td><td>memdump.mem</td><td>File Offset 4564410230</td><td>memdump.mem</td><td>Carving</td><td>3901</td></tr> <tr><td>https://console.aws.amazon.com/iam/home?region=</td><td>27/3/2018 3:58</td><td>TOP 5 FIGHTING GUNS - YouTube</td><td>1</td><td>memdump.mem</td><td>File Offset 5290203916</td><td>memdump.mem</td><td>Carving</td><td>4788</td></tr> <tr><td>https://www.youtube.com/watch?v=tr3e3Ynck</td><td>28/3/2018 0:07</td><td>How easy is it to get a gun in the United States? - Quora</td><td>1</td><td>memdump.mem</td><td>File Offset 5290201636</td><td>memdump.mem</td><td>Carving</td><td>4768</td></tr> <tr><td>https://www.youtube.com/watch?v=umIPCVpaU4</td><td>28/3/2018 0:07</td><td>just how easy is it to buy an illegal gun - Google Search</td><td>1</td><td>memdump.mem</td><td>File Offset 5290201527</td><td>memdump.mem</td><td>Carving</td><td>4766</td></tr> <tr><td>https://www.box.com/home</td><td>28/3/2018 0:11</td><td>The NRA Is Wrong: The Myth of Illegal Guns</td><td>1</td><td>memdump.mem</td><td>File Offset 5290201432</td><td>memdump.mem</td><td>Carving</td><td>4763</td></tr> <tr><td>https://www.google.com/search?q=mega+cloud+stor</td><td>28/3/2018 0:55</td><td>submachine guns - Google Search</td><td>1</td><td>memdump.mem</td><td>File Offset 6772844911</td><td>memdump.mem</td><td>Carving</td><td>6772</td></tr> <tr><td>https://www.google.com/search?q=gun+ruger+10+22&rlz</td><td>28/3/2018 0:56</td><td>Northern Virginia Gun Works - Google Search</td><td>1</td><td>memdump.mem</td><td>File Offset 6772844725</td><td>memdump.mem</td><td>Carving</td><td>6770</td></tr> <tr><td>https://www.google.com/search?q=1CL1CHB&rlz</td><td>29/3/2018 23:06</td><td>anti gun rally near me - Google Search</td><td>1</td><td>memdump.mem</td><td>File Offset 1983949987</td><td>memdump.mem</td><td>Carving</td><td>2473</td></tr> <tr><td>https://www.nokia.com/en_intphones/nokiaphones/216-29/3/2018 8:31</td><td>upcoming anti gun rally near me - Google Search</td><td>1</td><td>memdump.mem</td><td>File Offset 1983949879</td><td>memdump.mem</td><td>Carving</td><td>2471</td></tr> <tr><td>https://www.google.com/search?q=gun+control+great+britain</td><td>30/3/2018 8:31</td><td>- Google Search</td><td>1</td><td>memdump.mem</td><td>File Offset 9601815696</td><td>memdump.mem</td><td>Carving</td><td>10292</td></tr> <tr><td>https://www.google.com/maps/place/indonesia/@-2/2/2018 0:53</td><td>f n 5 7 amm For Sale - Buy f n 5 7 ammo Online at GunBroker.com</td><td>1</td><td>memdump.mem</td><td>File Offset 1865476163</td><td>memdump.mem</td><td>Carving</td><td>2331</td></tr> <tr><td>https://www.google.com/search?q=scaleslibrary</td><td>3/4/2018 6:47</td><td>gun store near me - Google Search</td><td>1</td><td>memdump.mem</td><td>File Offset 2677224208</td><td>memdump.mem</td><td>Carving</td><td>3119</td></tr> <tr><td>https://www.google.com/search?q=cscadeslibrary</td><td>3/4/2018 6:47</td><td>gunstore near me - Google Search</td><td>1</td><td>memdump.mem</td><td>File Offset 2677223965</td><td>memdump.mem</td><td>Carving</td><td>3117</td></tr> <tr><td>https://www.google.com/search?q=cscadeslibrary</td><td>3/4/2018 6:47</td><td>kelce 2000 site:gunbroker.com - Google Search</td><td>1</td><td>memdump.mem</td><td>File Offset 2677223722</td><td>memdump.mem</td><td>Carving</td><td>3115</td></tr> <tr><td>https://www.google.com/search?q=cscadeslibrary</td><td>3/4/2018 6:47</td><td>gunbroker - Google Search</td><td>1</td><td>memdump.mem</td><td>File Offset 2677223479</td><td>memdump.mem</td><td>Carving</td><td>3113</td></tr> </tbody> </table> <p>WebKit Browser Web History (Car)</p>	URL	Last Visited Date	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID	https://tntdrive.com/	27/3/2018 3:48	This New Race Gun Will Change EVERYTHING!!! - YouTube	1	memdump.mem	File Offset 4564410230	memdump.mem	Carving	3901	https://console.aws.amazon.com/iam/home?region=	27/3/2018 3:58	TOP 5 FIGHTING GUNS - YouTube	1	memdump.mem	File Offset 5290203916	memdump.mem	Carving	4788	https://www.youtube.com/watch?v=tr3e3Ynck	28/3/2018 0:07	How easy is it to get a gun in the United States? - Quora	1	memdump.mem	File Offset 5290201636	memdump.mem	Carving	4768	https://www.youtube.com/watch?v=umIPCVpaU4	28/3/2018 0:07	just how easy is it to buy an illegal gun - Google Search	1	memdump.mem	File Offset 5290201527	memdump.mem	Carving	4766	https://www.box.com/home	28/3/2018 0:11	The NRA Is Wrong: The Myth of Illegal Guns	1	memdump.mem	File Offset 5290201432	memdump.mem	Carving	4763	https://www.google.com/search?q=mega+cloud+stor	28/3/2018 0:55	submachine guns - Google Search	1	memdump.mem	File Offset 6772844911	memdump.mem	Carving	6772	https://www.google.com/search?q=gun+ruger+10+22&rlz	28/3/2018 0:56	Northern Virginia Gun Works - Google Search	1	memdump.mem	File Offset 6772844725	memdump.mem	Carving	6770	https://www.google.com/search?q=1CL1CHB&rlz	29/3/2018 23:06	anti gun rally near me - Google Search	1	memdump.mem	File Offset 1983949987	memdump.mem	Carving	2473	https://www.nokia.com/en_intphones/nokiaphones/216-29/3/2018 8:31	upcoming anti gun rally near me - Google Search	1	memdump.mem	File Offset 1983949879	memdump.mem	Carving	2471	https://www.google.com/search?q=gun+control+great+britain	30/3/2018 8:31	- Google Search	1	memdump.mem	File Offset 9601815696	memdump.mem	Carving	10292	https://www.google.com/maps/place/indonesia/@-2/2/2018 0:53	f n 5 7 amm For Sale - Buy f n 5 7 ammo Online at GunBroker.com	1	memdump.mem	File Offset 1865476163	memdump.mem	Carving	2331	https://www.google.com/search?q=scaleslibrary	3/4/2018 6:47	gun store near me - Google Search	1	memdump.mem	File Offset 2677224208	memdump.mem	Carving	3119	https://www.google.com/search?q=cscadeslibrary	3/4/2018 6:47	gunstore near me - Google Search	1	memdump.mem	File Offset 2677223965	memdump.mem	Carving	3117	https://www.google.com/search?q=cscadeslibrary	3/4/2018 6:47	kelce 2000 site:gunbroker.com - Google Search	1	memdump.mem	File Offset 2677223722	memdump.mem	Carving	3115	https://www.google.com/search?q=cscadeslibrary	3/4/2018 6:47	gunbroker - Google Search	1	memdump.mem	File Offset 2677223479	memdump.mem	Carving	3113
URL	Last Visited Date	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID																																																																																																																																							
https://tntdrive.com/	27/3/2018 3:48	This New Race Gun Will Change EVERYTHING!!! - YouTube	1	memdump.mem	File Offset 4564410230	memdump.mem	Carving	3901																																																																																																																																							
https://console.aws.amazon.com/iam/home?region=	27/3/2018 3:58	TOP 5 FIGHTING GUNS - YouTube	1	memdump.mem	File Offset 5290203916	memdump.mem	Carving	4788																																																																																																																																							
https://www.youtube.com/watch?v=tr3e3Ynck	28/3/2018 0:07	How easy is it to get a gun in the United States? - Quora	1	memdump.mem	File Offset 5290201636	memdump.mem	Carving	4768																																																																																																																																							
https://www.youtube.com/watch?v=umIPCVpaU4	28/3/2018 0:07	just how easy is it to buy an illegal gun - Google Search	1	memdump.mem	File Offset 5290201527	memdump.mem	Carving	4766																																																																																																																																							
https://www.box.com/home	28/3/2018 0:11	The NRA Is Wrong: The Myth of Illegal Guns	1	memdump.mem	File Offset 5290201432	memdump.mem	Carving	4763																																																																																																																																							
https://www.google.com/search?q=mega+cloud+stor	28/3/2018 0:55	submachine guns - Google Search	1	memdump.mem	File Offset 6772844911	memdump.mem	Carving	6772																																																																																																																																							
https://www.google.com/search?q=gun+ruger+10+22&rlz	28/3/2018 0:56	Northern Virginia Gun Works - Google Search	1	memdump.mem	File Offset 6772844725	memdump.mem	Carving	6770																																																																																																																																							
https://www.google.com/search?q=1CL1CHB&rlz	29/3/2018 23:06	anti gun rally near me - Google Search	1	memdump.mem	File Offset 1983949987	memdump.mem	Carving	2473																																																																																																																																							
https://www.nokia.com/en_intphones/nokiaphones/216-29/3/2018 8:31	upcoming anti gun rally near me - Google Search	1	memdump.mem	File Offset 1983949879	memdump.mem	Carving	2471																																																																																																																																								
https://www.google.com/search?q=gun+control+great+britain	30/3/2018 8:31	- Google Search	1	memdump.mem	File Offset 9601815696	memdump.mem	Carving	10292																																																																																																																																							
https://www.google.com/maps/place/indonesia/@-2/2/2018 0:53	f n 5 7 amm For Sale - Buy f n 5 7 ammo Online at GunBroker.com	1	memdump.mem	File Offset 1865476163	memdump.mem	Carving	2331																																																																																																																																								
https://www.google.com/search?q=scaleslibrary	3/4/2018 6:47	gun store near me - Google Search	1	memdump.mem	File Offset 2677224208	memdump.mem	Carving	3119																																																																																																																																							
https://www.google.com/search?q=cscadeslibrary	3/4/2018 6:47	gunstore near me - Google Search	1	memdump.mem	File Offset 2677223965	memdump.mem	Carving	3117																																																																																																																																							
https://www.google.com/search?q=cscadeslibrary	3/4/2018 6:47	kelce 2000 site:gunbroker.com - Google Search	1	memdump.mem	File Offset 2677223722	memdump.mem	Carving	3115																																																																																																																																							
https://www.google.com/search?q=cscadeslibrary	3/4/2018 6:47	gunbroker - Google Search	1	memdump.mem	File Offset 2677223479	memdump.mem	Carving	3113																																																																																																																																							
“Arms”	<table border="1"> <thead> <tr> <th>URL</th><th>Last Visited Date</th><th>Title</th><th>Visit Count</th><th>Source</th><th>Location</th><th>Evidence number</th><th>Recovery</th><th>Item ID</th></tr> </thead> <tbody> <tr><td>https://www.google.com/search?q=tntdrive+vs+r11C1CHB</td><td>27/3/2018 23:49</td><td>Dual Wielding Challenge vs Army Sniper - YouTube</td><td>1</td><td>memdump.mem</td><td>File Offset 2393070091</td><td>memdump.mem</td><td>Carving</td><td>2837</td></tr> <tr><td>https://megabackup.com/buynow/buynow-eol</td><td>28/3/2018 0:55</td><td>Services 4€ NOVA FIREARMS</td><td>1</td><td>memdump.mem</td><td>File Offset 9530391711</td><td>memdump.mem</td><td>Carving</td><td>10103</td></tr> <tr><td>https://megabackup.com/buynow/four-plans-im-cle?</td><td>28/3/2018 0:55</td><td>FFL & Transfers 4€ NOVA FIREARMS</td><td>1</td><td>memdump.mem</td><td>File Offset 9530391819</td><td>memdump.mem</td><td>Carving</td><td>10104</td></tr> <tr><td>https://www.google.com/search?q=cassadeslibrary+meeting</td><td>3/4/2018 6:47</td><td>Home Protect & Defend Firearms Training</td><td>1</td><td>memdump.mem</td><td>File Offset 2677224451</td><td>memdump.mem</td><td>Carving</td><td>3121</td></tr> <tr><td>https://www.google.com/search?q=cassadeslibrary</td><td>3/4/2018 6:48</td><td>KELCE 2000 site:gunbroker.com - Google Search</td><td>2</td><td>memdump.mem</td><td>File Offset 2677224707</td><td>memdump.mem</td><td>Carving</td><td>3123</td></tr> </tbody> </table> <p>WebKit Browser Web History (Car)</p>	URL	Last Visited Date	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID	https://www.google.com/search?q=tntdrive+vs+r11C1CHB	27/3/2018 23:49	Dual Wielding Challenge vs Army Sniper - YouTube	1	memdump.mem	File Offset 2393070091	memdump.mem	Carving	2837	https://megabackup.com/buynow/buynow-eol	28/3/2018 0:55	Services 4€ NOVA FIREARMS	1	memdump.mem	File Offset 9530391711	memdump.mem	Carving	10103	https://megabackup.com/buynow/four-plans-im-cle?	28/3/2018 0:55	FFL & Transfers 4€ NOVA FIREARMS	1	memdump.mem	File Offset 9530391819	memdump.mem	Carving	10104	https://www.google.com/search?q=cassadeslibrary+meeting	3/4/2018 6:47	Home Protect & Defend Firearms Training	1	memdump.mem	File Offset 2677224451	memdump.mem	Carving	3121	https://www.google.com/search?q=cassadeslibrary	3/4/2018 6:48	KELCE 2000 site:gunbroker.com - Google Search	2	memdump.mem	File Offset 2677224707	memdump.mem	Carving	3123																																																																																								
URL	Last Visited Date	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID																																																																																																																																							
https://www.google.com/search?q=tntdrive+vs+r11C1CHB	27/3/2018 23:49	Dual Wielding Challenge vs Army Sniper - YouTube	1	memdump.mem	File Offset 2393070091	memdump.mem	Carving	2837																																																																																																																																							
https://megabackup.com/buynow/buynow-eol	28/3/2018 0:55	Services 4€ NOVA FIREARMS	1	memdump.mem	File Offset 9530391711	memdump.mem	Carving	10103																																																																																																																																							
https://megabackup.com/buynow/four-plans-im-cle?	28/3/2018 0:55	FFL & Transfers 4€ NOVA FIREARMS	1	memdump.mem	File Offset 9530391819	memdump.mem	Carving	10104																																																																																																																																							
https://www.google.com/search?q=cassadeslibrary+meeting	3/4/2018 6:47	Home Protect & Defend Firearms Training	1	memdump.mem	File Offset 2677224451	memdump.mem	Carving	3121																																																																																																																																							
https://www.google.com/search?q=cassadeslibrary	3/4/2018 6:48	KELCE 2000 site:gunbroker.com - Google Search	2	memdump.mem	File Offset 2677224707	memdump.mem	Carving	3123																																																																																																																																							
“Ranch”	<table border="1"> <thead> <tr> <th>URL</th><th>Last Visited Date</th><th>Title</th><th>Visit Count</th><th>Source</th><th>Location</th><th>Evidence number</th><th>Recovery</th><th>Item ID</th></tr> </thead> <tbody> <tr><td>https://twitter.com/search?q=k23Molonlabe&src=</td><td>28/3/2018 1:11</td><td>federal government vs ranchers - Google Search</td><td>1</td><td>memdump.mem</td><td>File Offset 6772843776</td><td>memdump.mem</td><td>Carving</td><td>6758</td></tr> <tr><td>https://twitter.com/</td><td>29/3/2018 4:22</td><td>OFFICIAL STATEMENT: Snake River Ranchers vs Federal Government The Th</td><td>1</td><td>memdump.mem</td><td>File Offset 9350390133</td><td>memdump.mem</td><td>Carving</td><td>10093</td></tr> </tbody> </table> <p>WebKit Browser Web History (Car)</p>	URL	Last Visited Date	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID	https://twitter.com/search?q=k23Molonlabe&src=	28/3/2018 1:11	federal government vs ranchers - Google Search	1	memdump.mem	File Offset 6772843776	memdump.mem	Carving	6758	https://twitter.com/	29/3/2018 4:22	OFFICIAL STATEMENT: Snake River Ranchers vs Federal Government The Th	1	memdump.mem	File Offset 9350390133	memdump.mem	Carving	10093																																																																																																																			
URL	Last Visited Date	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID																																																																																																																																							
https://twitter.com/search?q=k23Molonlabe&src=	28/3/2018 1:11	federal government vs ranchers - Google Search	1	memdump.mem	File Offset 6772843776	memdump.mem	Carving	6758																																																																																																																																							
https://twitter.com/	29/3/2018 4:22	OFFICIAL STATEMENT: Snake River Ranchers vs Federal Government The Th	1	memdump.mem	File Offset 9350390133	memdump.mem	Carving	10093																																																																																																																																							

	WebKit Browser Web History (Car)																																																						
"Rifles"	<table border="1"> <thead> <tr> <th>URL</th><th>Last Visited Date</th><th>Title</th><th>Visit Count</th><th>Source</th><th>Location</th><th>Evidence number</th><th>Recovery</th><th>Item ID</th></tr> </thead> <tbody> <tr> <td>https://us-east-1.signin.aws.amazon.com/oauth/signin?igr=27/3/2018 23:54</td><td></td><td>best tactical rifle - YouTube</td><td>1</td><td>memdump.mem</td><td>file Offset 292363095</td><td>memdump.mem</td><td>Carving</td><td>3256</td></tr> <tr> <td>https://app.box.com/login/assertion?la=Live!V1z9</td><td>28/3/2018 01:18</td><td>There would be a rifle behind every blade of grass - Google Search</td><td>1</td><td>memdump.mem</td><td>file Offset 7944046224</td><td>memdump.mem</td><td>Carving</td><td>8232</td></tr> <tr> <td>https://www.youtube.com/results?search_query=best</td><td>28/3/2018 05:53</td><td>concealable tactical rifles - Google Search</td><td>1</td><td>memdump.mem</td><td>file Offset 6772845112</td><td>memdump.mem</td><td>Carving</td><td>6774</td></tr> <tr> <td>https://www.youtube.com/watch?v=msnQf5V9Y</td><td>28/3/2018 05:53</td><td>9mm rifles - Google Search</td><td>1</td><td>memdump.mem</td><td>file Offset 794404973</td><td>memdump.mem</td><td>Carving</td><td>8226</td></tr> <tr> <td>https://hangouts.google.com/webchat/u/0/loadProfile</td><td>1/4/2018 22:43</td><td>National Rifle Association of America - Google Maps</td><td>1</td><td>memdump.mem</td><td>file Offset 1865476336</td><td>memdump.mem</td><td>Carving</td><td>2333</td></tr> </tbody> </table>	URL	Last Visited Date	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID	https://us-east-1.signin.aws.amazon.com/oauth/signin?igr=27/3/2018 23:54		best tactical rifle - YouTube	1	memdump.mem	file Offset 292363095	memdump.mem	Carving	3256	https://app.box.com/login/assertion?la=Live!V1z9	28/3/2018 01:18	There would be a rifle behind every blade of grass - Google Search	1	memdump.mem	file Offset 7944046224	memdump.mem	Carving	8232	https://www.youtube.com/results?search_query=best	28/3/2018 05:53	concealable tactical rifles - Google Search	1	memdump.mem	file Offset 6772845112	memdump.mem	Carving	6774	https://www.youtube.com/watch?v=msnQf5V9Y	28/3/2018 05:53	9mm rifles - Google Search	1	memdump.mem	file Offset 794404973	memdump.mem	Carving	8226	https://hangouts.google.com/webchat/u/0/loadProfile	1/4/2018 22:43	National Rifle Association of America - Google Maps	1	memdump.mem	file Offset 1865476336	memdump.mem	Carving	2333
URL	Last Visited Date	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID																																															
https://us-east-1.signin.aws.amazon.com/oauth/signin?igr=27/3/2018 23:54		best tactical rifle - YouTube	1	memdump.mem	file Offset 292363095	memdump.mem	Carving	3256																																															
https://app.box.com/login/assertion?la=Live!V1z9	28/3/2018 01:18	There would be a rifle behind every blade of grass - Google Search	1	memdump.mem	file Offset 7944046224	memdump.mem	Carving	8232																																															
https://www.youtube.com/results?search_query=best	28/3/2018 05:53	concealable tactical rifles - Google Search	1	memdump.mem	file Offset 6772845112	memdump.mem	Carving	6774																																															
https://www.youtube.com/watch?v=msnQf5V9Y	28/3/2018 05:53	9mm rifles - Google Search	1	memdump.mem	file Offset 794404973	memdump.mem	Carving	8226																																															
https://hangouts.google.com/webchat/u/0/loadProfile	1/4/2018 22:43	National Rifle Association of America - Google Maps	1	memdump.mem	file Offset 1865476336	memdump.mem	Carving	2333																																															
"Police"	<table border="1"> <thead> <tr> <th>URL</th><th>Last Visited Date</th><th>Title</th><th>Visit Count</th><th>Source</th><th>Location</th><th>Evidence number</th><th>Recovery</th><th>Item ID</th></tr> </thead> <tbody> <tr> <td>https://www.dropbox.com/l/AAB3lMeYQbNs2ck2u9</td><td>28/3/2018 0:14</td><td>police response times by zip code - Google Search</td><td>1</td><td>memdump.mem</td><td>file Offset 7929916618</td><td>memdump.mem</td><td>Carving</td><td>8260</td></tr> <tr> <td>https://www.google.com/url?sa=t&source=web&rct=j&q=&t</td><td>28/3/2018 0:14</td><td>which state has the worst police response times - Google Search</td><td>1</td><td>memdump.mem</td><td>file Offset 7929916706</td><td>memdump.mem</td><td>Carving</td><td>8263</td></tr> </tbody> </table>	URL	Last Visited Date	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID	https://www.dropbox.com/l/AAB3lMeYQbNs2ck2u9	28/3/2018 0:14	police response times by zip code - Google Search	1	memdump.mem	file Offset 7929916618	memdump.mem	Carving	8260	https://www.google.com/url?sa=t&source=web&rct=j&q=&t	28/3/2018 0:14	which state has the worst police response times - Google Search	1	memdump.mem	file Offset 7929916706	memdump.mem	Carving	8263																											
URL	Last Visited Date	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID																																															
https://www.dropbox.com/l/AAB3lMeYQbNs2ck2u9	28/3/2018 0:14	police response times by zip code - Google Search	1	memdump.mem	file Offset 7929916618	memdump.mem	Carving	8260																																															
https://www.google.com/url?sa=t&source=web&rct=j&q=&t	28/3/2018 0:14	which state has the worst police response times - Google Search	1	memdump.mem	file Offset 7929916706	memdump.mem	Carving	8263																																															
"Demo"	<table border="1"> <thead> <tr> <th>URL</th><th>Last Visited Date</th><th>Title</th><th>Visit Count</th><th>Source</th><th>Location</th><th>Evidence number</th><th>Recovery</th><th>Item ID</th></tr> </thead> <tbody> <tr> <td>https://mail.google.com/mail/u/0/#inbox/16299397516d902</td><td>28/3/2018 0:14</td><td>Democratic national headquarters - Google Search</td><td>1</td><td>memdump.mem</td><td>file Offset 7929916902</td><td>memdump.mem</td><td>Carving</td><td>8264</td></tr> <tr> <td>https://mail.google.com/mail/u/0/#inbox/compose/28/700207</td><td>29/3/2018 4:27</td><td>democrat building reston va - Google Search</td><td>2</td><td>memdump.mem</td><td>file Offset 7567794359</td><td>memdump.mem</td><td>Carving</td><td>7767</td></tr> <tr> <td>https://www.quora.com/How-easy-is-it-to-get-a-gun-in-the-US</td><td>29/3/2018 4:29</td><td>reston virginia democratic party building - Google Search</td><td>1</td><td>memdump.mem</td><td>file Offset 7567794763</td><td>memdump.mem</td><td>Carving</td><td>7768</td></tr> <tr> <td>https://www.google.com/search?q=democratic+party+building</td><td>29/3/2018 23:03</td><td>fairfax democratic building - Google Search</td><td>1</td><td>memdump.mem</td><td>file Offset 1983950652</td><td>memdump.mem</td><td>Carving</td><td>2475</td></tr> <tr> <td>https://hangouts.google.com/webchat/u/0/loadClientsAndProd</td><td>30/3/2018 21:09</td><td>Democratic offices in DC - Google Search</td><td>2</td><td>memdump.mem</td><td>file Offset 1983947366</td><td>memdump.mem</td><td>Carving</td><td>2458</td></tr> </tbody> </table>	URL	Last Visited Date	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID	https://mail.google.com/mail/u/0/#inbox/16299397516d902	28/3/2018 0:14	Democratic national headquarters - Google Search	1	memdump.mem	file Offset 7929916902	memdump.mem	Carving	8264	https://mail.google.com/mail/u/0/#inbox/compose/28/700207	29/3/2018 4:27	democrat building reston va - Google Search	2	memdump.mem	file Offset 7567794359	memdump.mem	Carving	7767	https://www.quora.com/How-easy-is-it-to-get-a-gun-in-the-US	29/3/2018 4:29	reston virginia democratic party building - Google Search	1	memdump.mem	file Offset 7567794763	memdump.mem	Carving	7768	https://www.google.com/search?q=democratic+party+building	29/3/2018 23:03	fairfax democratic building - Google Search	1	memdump.mem	file Offset 1983950652	memdump.mem	Carving	2475	https://hangouts.google.com/webchat/u/0/loadClientsAndProd	30/3/2018 21:09	Democratic offices in DC - Google Search	2	memdump.mem	file Offset 1983947366	memdump.mem	Carving	2458
URL	Last Visited Date	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID																																															
https://mail.google.com/mail/u/0/#inbox/16299397516d902	28/3/2018 0:14	Democratic national headquarters - Google Search	1	memdump.mem	file Offset 7929916902	memdump.mem	Carving	8264																																															
https://mail.google.com/mail/u/0/#inbox/compose/28/700207	29/3/2018 4:27	democrat building reston va - Google Search	2	memdump.mem	file Offset 7567794359	memdump.mem	Carving	7767																																															
https://www.quora.com/How-easy-is-it-to-get-a-gun-in-the-US	29/3/2018 4:29	reston virginia democratic party building - Google Search	1	memdump.mem	file Offset 7567794763	memdump.mem	Carving	7768																																															
https://www.google.com/search?q=democratic+party+building	29/3/2018 23:03	fairfax democratic building - Google Search	1	memdump.mem	file Offset 1983950652	memdump.mem	Carving	2475																																															
https://hangouts.google.com/webchat/u/0/loadClientsAndProd	30/3/2018 21:09	Democratic offices in DC - Google Search	2	memdump.mem	file Offset 1983947366	memdump.mem	Carving	2458																																															
"Tac"	<table border="1"> <thead> <tr> <th>URL</th><th>Last Visited Date</th><th>Title</th><th>Visit Count</th><th>Source</th><th>Location</th><th>Evidence number</th><th>Recovery</th><th>Item ID</th></tr> </thead> <tbody> <tr> <td>https://us-east-1.signin.aws.amazon.com/oauth/signin?igr=27/3/2018 23:54</td><td></td><td>best tactical rifle - YouTube</td><td>1</td><td>memdump.mem</td><td>file Offset 292363095</td><td>memdump.mem</td><td>Carving</td><td>3256</td></tr> <tr> <td>https://app.box.com/login/profile/setup</td><td>28/3/2018 0:17</td><td>Japanese quote about attacking america - Google Search</td><td>1</td><td>memdump.mem</td><td>file Offset 7944046060</td><td>memdump.mem</td><td>Carving</td><td>8228</td></tr> <tr> <td>https://www.youtube.com/results?search_query=best+tactical</td><td>28/3/2018 05:53</td><td>concealable tactical rifles - Google Search</td><td>1</td><td>memdump.mem</td><td>file Offset 6772845112</td><td>memdump.mem</td><td>Carving</td><td>6774</td></tr> </tbody> </table>	URL	Last Visited Date	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID	https://us-east-1.signin.aws.amazon.com/oauth/signin?igr=27/3/2018 23:54		best tactical rifle - YouTube	1	memdump.mem	file Offset 292363095	memdump.mem	Carving	3256	https://app.box.com/login/profile/setup	28/3/2018 0:17	Japanese quote about attacking america - Google Search	1	memdump.mem	file Offset 7944046060	memdump.mem	Carving	8228	https://www.youtube.com/results?search_query=best+tactical	28/3/2018 05:53	concealable tactical rifles - Google Search	1	memdump.mem	file Offset 6772845112	memdump.mem	Carving	6774																		
URL	Last Visited Date	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID																																															
https://us-east-1.signin.aws.amazon.com/oauth/signin?igr=27/3/2018 23:54		best tactical rifle - YouTube	1	memdump.mem	file Offset 292363095	memdump.mem	Carving	3256																																															
https://app.box.com/login/profile/setup	28/3/2018 0:17	Japanese quote about attacking america - Google Search	1	memdump.mem	file Offset 7944046060	memdump.mem	Carving	8228																																															
https://www.youtube.com/results?search_query=best+tactical	28/3/2018 05:53	concealable tactical rifles - Google Search	1	memdump.mem	file Offset 6772845112	memdump.mem	Carving	6774																																															

The above “***Item 12 – Exhibit K – Webkit Browser History (Carving) (memdump.mem)***” are some crucial searches that were made by the suspect that were carved during the memory dump analysis.

2.3.8. Evidence Class 8 – Google Map Queries

Item 13 – Exhibit L – Google Map Queries (memdump.mem)

Exhibit L

EVIDENCE (17)											Column View				
Search Query	Date/Time	Center of Map	Source Address	Destination Address	Artifact	Artifact ID	Artifact type	Source	Location	Evidence ID	Item ID				
Dulles International Airport	28/07/2018 17:56:09	38.951763,-77.561597			Potential Browser Activity	2122	Google Maps Queries	memdump:map	File Offset:1772203277	memdump:map	9				
Indonesia	2/4/2018 15:58:38 AM	-1.875015,106.76055648			Whitelisted IP, Potomac Falls, VA	2331	Google Maps Queries	memdump:map	File Offset:1854701963	memdump:map	2332				
National Rifle Association of America	29/7/2018 11:16:24 PM	38.844015,-77.007707			Whitelisted IP, Potomac Falls, VA	2461	Google Maps Queries	memdump:map	File Offset:1893477576	memdump:map	2463				
	38.867711,-77.307099				Fairfax County Democratic Committee, 8500 Ox Run Rd	2462	Potential Browser Activity	6132	Google Maps Queries	memdump:map	File Offset:1812477209	memdump:map	8533		
	4/6/2018 4:59:16 AM	38.960145,-77.447236	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535475	memdump:map	8671		
	4/6/2018 4:49:46 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8673		
	4/6/2018 4:49:38 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8674		
	4/6/2018 4:50:24 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8675		
	4/6/2018 4:47:43 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8676		
	4/6/2018 4:47:42 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8677		
	4/6/2018 4:46:34 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8678		
	4/6/2018 4:46:33 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8679		
	4/6/2018 4:46:31 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8680		
	4/6/2018 4:46:31 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8681		
	4/6/2018 4:46:31 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8682		
	4/6/2018 4:46:31 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8683		
	4/6/2018 4:46:31 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8684		
	4/6/2018 4:46:31 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8685		
	4/6/2018 4:46:31 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8686		
	4/6/2018 4:46:31 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8687		
	4/6/2018 4:46:31 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8688		
	4/6/2018 4:46:31 AM	38.970399,-77.395179	2100 Whitelisted IP, Potomac Falls, VA	20165	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1897535864	memdump:map	8689		
Dulles International Airport	38.953116,-77.517019				Whitelisted IP, Potomac Falls, VA	2670	Dulles International Airport, Saarinen Circle, Dulles, VA	2670	Whitelisted IP, Potomac Falls, VA	2670	Google Maps Queries	memdump:map	File Offset:1555386833	memdump:map	15299

There are repeated searches made from **Cascades Library** to **Dulles International Airport**, and two other destinations address to 1) **National Rifle Association of America**, and 2) **Fairfax County Democratic Committee**.

2.3.9. Evidence Class 9 – Google Cached Images

During the analysis in Autopsy and Magnet Axiom, we discovered some images of concern that merits as potential evidence to this case. The images under **filename: f_0018cd** and **filename: f_0018cb** express animosity towards Parkland shooting survivor David Hogg. Additionally, a collage featuring David Hogg and family **filename: f_001a37** raises suspicions of surveillance. The shooting that occurred on 14 February 2018 which prompted David Hogg to post a tweet encouraging people to call the **Town Hall for Our Lives** events with their congressional representative. One of the locations is Sterling, Virginia, Saturday's town hall that was set for 12:30 p.m. at the Cascades Library on Whitfield Place on the 7th of April 2018.¹

¹ <https://wila.com/news/local/120-town-hall-for-our-lives-events-scheduled-for-saturday-nationwide>

Item 14 – Exhibit M – Google Cached Images (memdump.mem)**Exhibit M**

	<p>Name: /img_LoneWolf.E01/vol_vo17/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_001114</p> <p>Type: File System</p> <p>MIME Type: image/jpeg</p> <p>Size: 31777</p> <p>File Name Allocation: Unallocated</p> <p>Metadata Allocation: Unallocated</p> <p>Modified: 2018-03-30 11:28:43 SGT</p> <p>Accessed: 2018-03-30 11:28:43 SGT</p> <p>Created: 2018-03-30 11:28:43 SGT</p> <p>Changed: 2018-03-30 11:28:43 SGT</p> <p>MD5: 0d2021e326615f5b81eda27630e7b30f</p> <p>SHA-256: ec361e397979bbf13b98fd4914e2c5d1d22ce5abcf77f72993db371636c002fc</p> <p>Hash Lookup: UNKNOWN</p> <p>Results:</p> <p>Internal ID: 18395</p>
	<p>Name: //img_LoneWolf.E01/vol_vo17/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_001784</p> <p>Type: File System</p> <p>MIME Type: image/jpeg</p> <p>Size: 42301</p> <p>File Name Allocation: Unallocated</p> <p>Metadata Allocation: Unallocated</p> <p>Modified: 2018-03-31 12:42:26 SGT</p> <p>Accessed: 2018-03-31 12:42:26 SGT</p> <p>Created: 2018-03-31 12:42:26 SGT</p> <p>Changed: 2018-03-31 12:42:26 SGT</p> <p>MD5: 1e164af729d96e0acecea7326fa2324d</p> <p>SHA-256: 293deec2f50db4672ead37808ee7eee44f522d4ea89dfe4174c37e4868e7a234</p> <p>Hash Lookup: UNKNOWN</p> <p>Results:</p> <p>Internal ID: 15772</p>
	<p>Name: /img_LoneWolf.E01/vol_vo17/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_001786</p> <p>Type: File System</p> <p>MIME Type: image/jpeg</p> <p>Size: 25681</p> <p>File Name Allocation: Unallocated</p> <p>Metadata Allocation: Unallocated</p> <p>Modified: 2018-03-31 12:42:26 SGT</p> <p>Accessed: 2018-03-31 12:42:26 SGT</p> <p>Created: 2018-03-31 12:42:26 SGT</p> <p>Changed: 2018-03-31 12:42:26 SGT</p> <p>MD5: df1624bf6b3f6b66b4061725d44327b8</p> <p>SHA-256: 3b763c9849e3224e95b1b09caf5b63b491372946ccfac64296e52f87f14ce451</p> <p>Hash Lookup: UNKNOWN</p> <p>Results:</p> <p>Internal ID: 15776</p>

	<p>Name: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_0017c1</p> <p>Type: File System MIME Type: image/jpeg Size: 17073 File Name Allocation: Unallocated Metadata Allocation: Unallocated Modified: 2018-03-31 12:44:27 SGT Accessed: 2018-03-31 12:44:27 SGT Created: 2018-03-31 12:44:27 SGT Changed: 2018-03-31 12:44:27 SGT MD5: c70a5efd5f023576dfbb8797d8ba06b1 SHA-256: 31e1c3d2d915b7bce4d048f3c987b16896b7e1e4bccdecf525f175a80e9d00df Hash Lookup Results: UNKNOWN Internal ID: 15848</p>
	<p>Name: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_0017c2</p> <p>Type: File System MIME Type: image/jpeg Size: 19226 File Name Allocation: Unallocated Metadata Allocation: Unallocated Modified: 2018-03-31 12:44:27 SGT Accessed: 2018-03-31 12:44:27 SGT Created: 2018-03-31 12:44:27 SGT Changed: 2018-03-31 12:44:27 SGT MD5: 8bd95702f8e6f758e44c34bb42834299 SHA-256: e6cffa5ddc8fac93f5b1eb2b50d7523a0c360c8c61c558e654224a11fc5f5917 Hash Lookup Results: UNKNOWN Internal ID: 15850</p>
 <p>NRA CONVENTION IN NASHVILLE 78,865 "GUN NUTS" GATHERED FOR 3 DAYS, CARRYING ALL KINDS OF GUNS. ZERO SHOOTING INCIDENTS.</p> <p>THIS WEEKEND IN NYC HOME OF SOME OF THE MOST RESTRICTIVE GUN CONTROL LAWS IN THE NATION. 15 SHOOTINGS. 20 WOUNDED. 1 DEAD.</p> <p>BEHIND ENEMY LINES THIS IS WHAT HAPPENS WHEN ONLY THE BAD GUYS HAVE GUNS. WWW.BEHINDENEMYLINES.RADIO.US</p>	<p>Filename: f_0018cd</p> <p>Source: LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0018cd</p> <p>Recovery Method: Carving Location: File Offset 0 Last Created: 2018-03-31 7:13:35 PM Last Accessed: 2018-03-31 7:13:35 PM Last Modified: 2018-03-31 7:13:35 PM MD5: 815f0b5bc98b9ab619719c0fc54b6295 SHA1: 1f0bbc2e379e38c2940c9028ac9162cead22d5c Item ID: 540104</p>

Derek Weida
Yesterday at 10:19am · 46 comments

RANT: Accurate portrayal of me listening to David Hogg speak. Look, I'm sorry dude, sincerely. It is horrible... School shootings. That said, you have to watch what you say. I'm Derek, I got shot on a house raid in Iraq. My getting shot didn't make me a professional on war, international relations, house raids (obviously 😂), or guns. This horrible thing happened to me but I didn't come home and protest the war... Even though I do kinda have these feelings that Iraq was errr... Questionable. 😂 But it ain't my place. I did my part. So, I empathize with you and your peers because whereas I signed up to be shot at, none of you did. (Not exactly sure you actually got shot AT but that's not the point here). Now... Guns. Here's my two cents: It's not a gun problem, not a people problem, it's a culture thing. Thing... Not problem. America loves guns. Accept that just like I had to accept that America loves God. Don't ever be so quick to tell a whoooooo lot of people how to live. Fucking NOBODY wants school shootings, mass shootings, shootings of any kind where somebody ends up injured or dead. Nobody. But people want their guns. I'm actually kinda with the anti-gun folk. There's no need BUTT! I've learned that the way I live and the things I believe have nothing to do with how others want to live or what they want to believe. I'm a well regulated idealist. 😂 The people you're arguing against... It's not even about the gun. It's about the freedom and the right... And you can't win an argument against that, nor should you (in most cases). The reality is humans gonna human and when humans human bad things happen sometimes but on the grand scale of things... Like 99.999% of people are good. Yes, let's find ways to deter those .001% of people as best we can but they're gonna accomplish their task regardless... Most likely I guess I just want to say don't be so quick to talk. Don't be so quick to think YOU are somehow the ONE person who has things figured out. You want to make a change? Cool!! But... Try to be less of a cunt about it.

Love and respect,
Derek

Filename:	f_001a27
Source	LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\jelcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0018cd
Recovery Method:	Carving
Location	File Offset 0
Last Created:	1/4/2018 1:15:46 AM
Last Accessed:	1/4/2018 1:15:46 AM
Last Modified:	1/4/2018 1:15:46 AM
MD5:	91cf1f068be571d1a6896120df01d989
SHA1:	9fb341ce4422472d6c9e9aff963c40e8b444c31
Item ID:	540247

Sen Dianne Feinstein @SenFeinstein

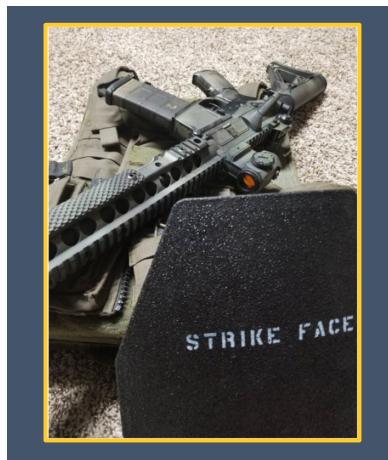
Today we have 15 million assault weapons in the U.S. These are guns modeled after military weapons and then sold to civilians. For what? You can't use it for hunting. You don't need it for defense. What do you really need it for?

7:19 PM · 28 Mar 18

James Woods @RealJamesWoods

Luckily the Founding Fathers, in their extraordinary wisdom, made it none of your business, Senator.

Filename:	f_001a3a
Source	LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\jelcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache\f_001a3a
Recovery Method:	Carving
Location	File Offset 0
Last Created:	1/4/2018 5:32:46 AM
Last Accessed:	1/4/2018 5:32:46 AM
Last Modified:	1/4/2018 5:32:46 AM
MD5:	2ef3beba414c8653ff602bc8992b4b8e
SHA1:	697834904bf70d937fce891f76d67914e9eb288d
Item ID:	540292



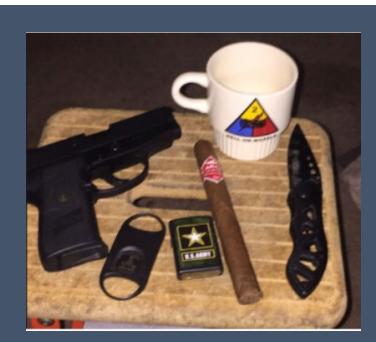
Filename:	f_001a20
Source	LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\jelcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache\f_001a20
Recovery Method:	Carving
Location	File Offset 0
Last Created:	31/3/2018 11:54:46 PM
Last Accessed:	31/3/2018 11:54:46 PM
Last Modified:	31/3/2018 11:54:46 PM
MD5:	bb72c7f33e1c0c60177a2ea297536234
SHA1:	bb92af48236b8a668d855d91450f345926b5bbe7
Item ID:	540272



Filename:	f_001a37
Source	LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache\f_001a37
Recovery Method:	Carving
Location	File Offset 0
Last Created:	1/4/2018 4:03:46 AM
Last Accessed:	1/4/2018 4:03:46 AM
Last Modified:	1/4/2018 4:03:46 AM
MD5:	6912fc48de15d46bfca2e64a9b7b6b2e
SHA1:	3ce0ffd705e619ad62a4edc38ddb42fff79a347e
Item ID:	540269



Filename:	f_0018cb
Source	LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0018cb
Recovery Method:	Carving
Location	File Offset 0
Last Created:	31/3/2018 6:49:35 PM
Last Accessed:	31/3/2018 6:49:35 PM
Last Modified:	31/3/2018 6:49:35 PM
MD5:	0026cf6228748dab6053eff772a9fa18
SHA1:	6c0d2e1736abfe634fc3b9c11861bf827d7261c
Item ID:	540109



Filename:	f_0018cc
Source	LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0018cc
Recovery Method:	Carving
Location	File Offset 0
Last Created:	31/3/2018 7:05:35 PM
Last Accessed:	31/3/2018 7:05:35 PM
Last Modified:	31/3/2018 7:05:35 PM
MD5:	9ddb1d74f40d4cff959a4b6042bad4f
SHA1:	6fe25edb0d7d6a7638090627203bca2b508c33ce
Item ID:	540102



Filename:	f_001a09
Source	LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache\f_001a09
Recovery Method:	Carving
Location	File Offset 0
Last Created:	31/3/2018 8:38:46 PM
Last Accessed:	31/3/2018 8:38:46 PM
Last Modified:	31/3/2018 8:38:46 PM
MD5:	976b2714dc49e06f96c773ce0ca65b9c
SHA1:	c6fe58d8521a3395e99b514c0efee39c2e96a3d3
Item ID:	540227

Based on all the findings we found and gathered thus far, we are able to identify the type of motive that triggered the genesis of his potential criminal psychology, specifically in relation to the elaboration of his potential mass shooting plan.

2.3.10. Evidence Class 10 – Timeline

In order for us to gain an understanding of the events surrounding the case “**Lone Wolf**” case, a timeline analysis was generated using Autopsy tool. This timeline graph provides a visual representation of Jim Cloudy’s digital activities.

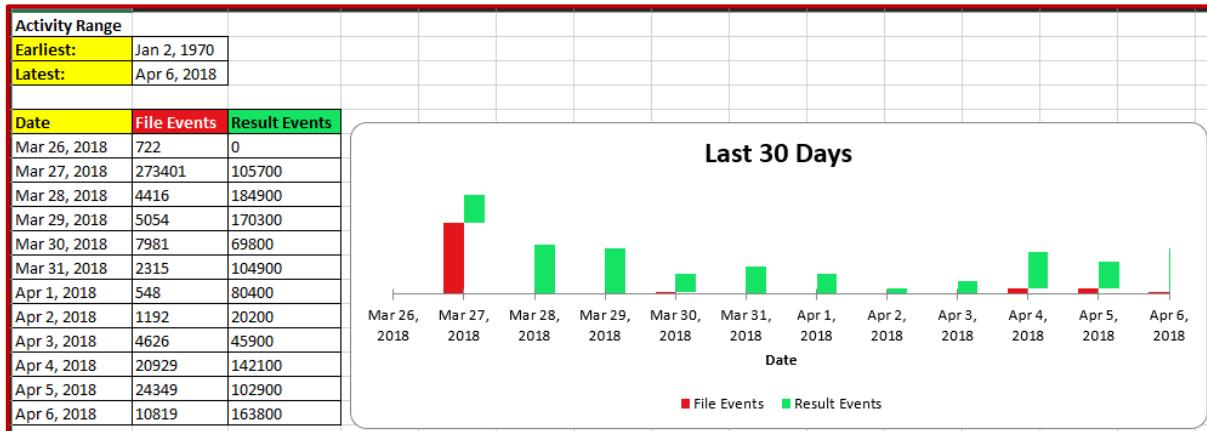


Fig.37 - Timeline

As shown in *figure.37* above, the timeline spans from March 26th 2018 to April 6th 2018, it illustrates the sequence of **file events** and **result events** on each day. This information sheds light on the series of events that took place until the point of investigation.

3. Conclusion

3.1. Summary of Findings

In summary, the digital forensics investigation carried out for the “**Lone Wolf**” case unveiled a series of detailed sequence of events, motivations, and digital activities. This was accomplished through the use of digital forensics tools. Tools I used included Magnet Axiom, Autopsy, and AccessData FTK Imager for the extraction of the “**jcloudy**” folder. To extract emails from the “**mbox**” file extension, Mozilla Thunderbird was used.

It is important to note that Thomas Moore (*Tom Moore*), the creator of this “**2018 Lone Wolf Scenario**” has extracted cloud-related data for students who did not have access to commercial forensics tools. His analysis done in 2018 help me understand the case and its nature. His cloud-data extraction can be found at <http://digitalcorpora.vse.gmu.edu/>

The combination of these techniques, both from my current investigation and Moore's past work, provided valuable insights into the case which helps to understand the subject's intentions, motivations, and actions.

4. Additional Information

4.1. References

- <https://wjla.com/news/local/120-town-hall-for-our-lives-events-scheduled-for-saturday-nationwide>
- <https://www.npr.org/2018/02/28/589502906/a-clearer-picture-of-parkland-shooting-suspect-comes-into-focus>
- <https://www.brightest.io/cause/town-hall-project/activity/town-hall-for-barbara-comstock-republican-va-10/>
- <https://www.joesandbox.com/analysis/74213/0/pdf> [AKMonitor.exe for Keylogger found]
- <https://belkasoft.com/shafik-punja-reviews-belkax> [AKMonitor.exe for Keylogger found]
- https://juliakeffer.files.wordpress.com/2013/06/autopsy_user_guide.pdf

4.2. Resources

- <https://online.fliphhtml5.com/rllbc/zdmn/#p=1>
- <https://mohammedalhumaidcom.files.wordpress.com/2022/01/windows-forensics-analysis-v-1.0-4.pdf>
- [https://adflegal.blob.core.windows.net/mainsite-new/docs/default-source/documents/resources/campaign-resources/life/defund-planned-parenthood/coalfire-systems-digital-forensics-analysis-report-for-cmp-planned-parenthood-videos-\(2015-09-28\).pdf](https://adflegal.blob.core.windows.net/mainsite-new/docs/default-source/documents/resources/campaign-resources/life/defund-planned-parenthood/coalfire-systems-digital-forensics-analysis-report-for-cmp-planned-parenthood-videos-(2015-09-28).pdf)
- <https://www.bod.org.uk/wp-content/uploads/2021/12/Project-Lights-Forensic-Acquisition-and-Analysis-Report-2712211916.pdf>
- <https://www.linkedin.com/pulse/how-open-mbox-file-corbett-software/>

4.3. Sources

- 2018 Lone Wolf Scenario - <https://digitalcorpora.org/corpora/scenarios/2018-lone-wolf-scenario/>
- "brother chat.gdoc" – Google document file: [<http://digitalcorpora.vse.gmu.edu/corpora/scenarios/2018-lonewolf/files/Potentially%20Recoverable/>]
- "mbox" Email file – Google Gmail: [<http://digitalcorpora.vse.gmu.edu/corpora/scenarios/2018-lonewolf/files/Potentially%20Recoverable/>] ← I extracted the content using Thunderbird
- "Jim's notebook" Microsoft OneNote: [<http://digitalcorpora.vse.gmu.edu/corpora/scenarios/2018-lonewolf/files/Potentially%20Recoverable/>]

4.4. Tools

- Magnet Axiom - Used for comprehensive digital evidence analysis.
- Autopsy - Utilized for file and folder analysis, timeline generation, and reporting.
- AccessData FTK Imager - Employed for disk imaging and data extraction.
- Mozilla Thunderbird - Used to extract email data from "mbox" file extension.

[END]