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

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 6th 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	LoneWolf_001	**Offense**	"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**".

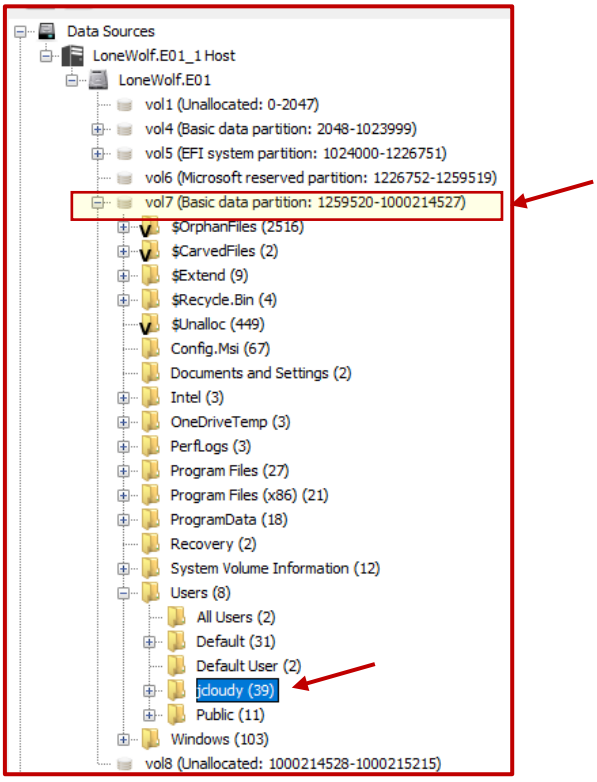


Fig.1

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

Usage	OS Drive (Windows 10 Education)
OS	Windows 10 Education
Size	512.11 GB

File Types	**Count**
Images	24,085
Videos	180
Audio	366
Documents	36,511
Executables	38,072
Unknown	16,232
Other	49,472
Not Analyzed	426

Allocated Files	158,419
Unallocated Files	6,925
Slack Files	125,629
Directories	89,143

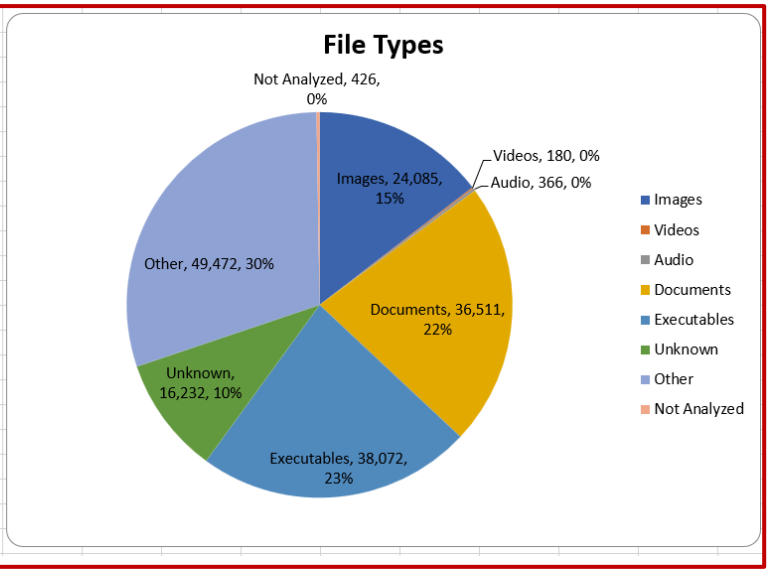


Fig.2

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.

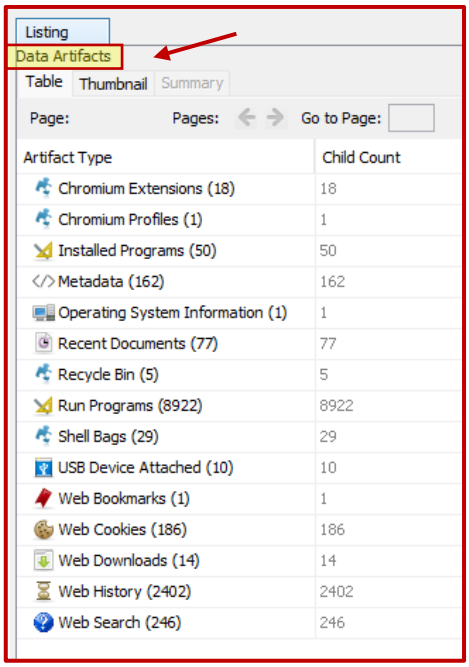
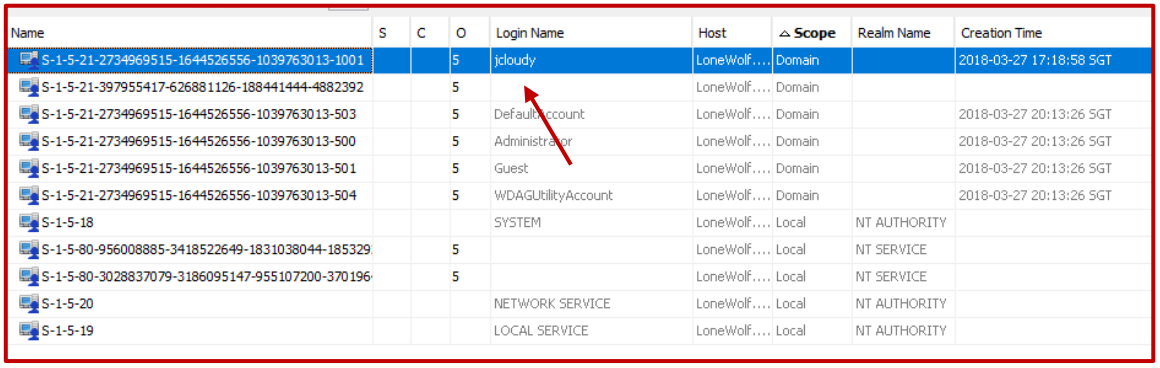


Fig.3

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

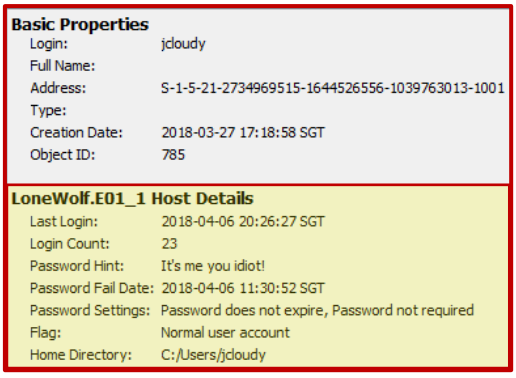


Fig.5

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-Author: 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

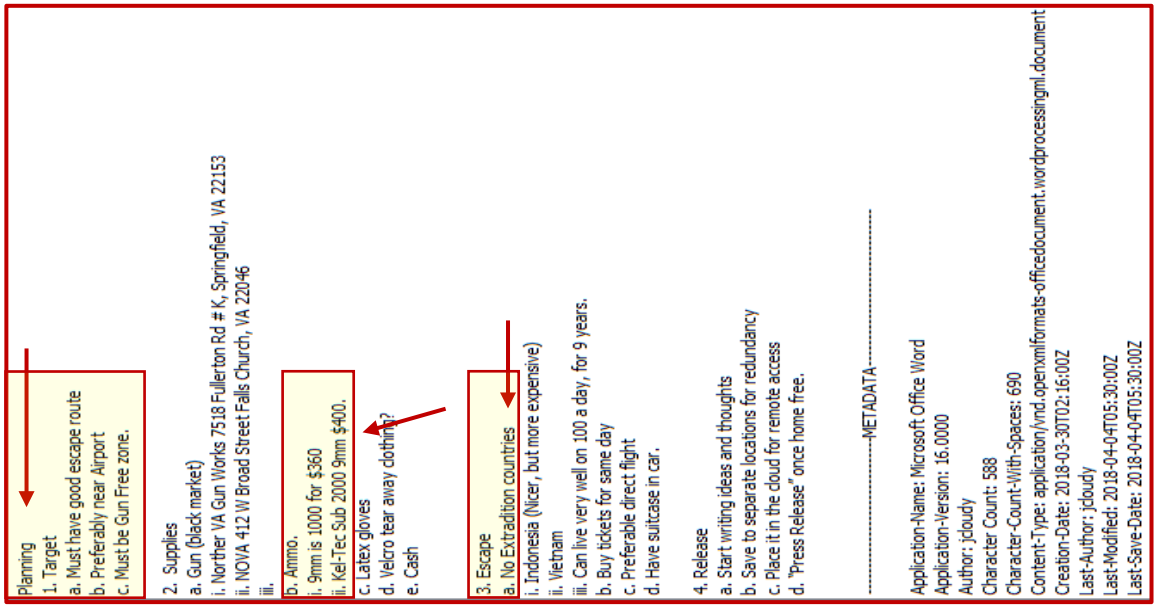


Fig.6

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

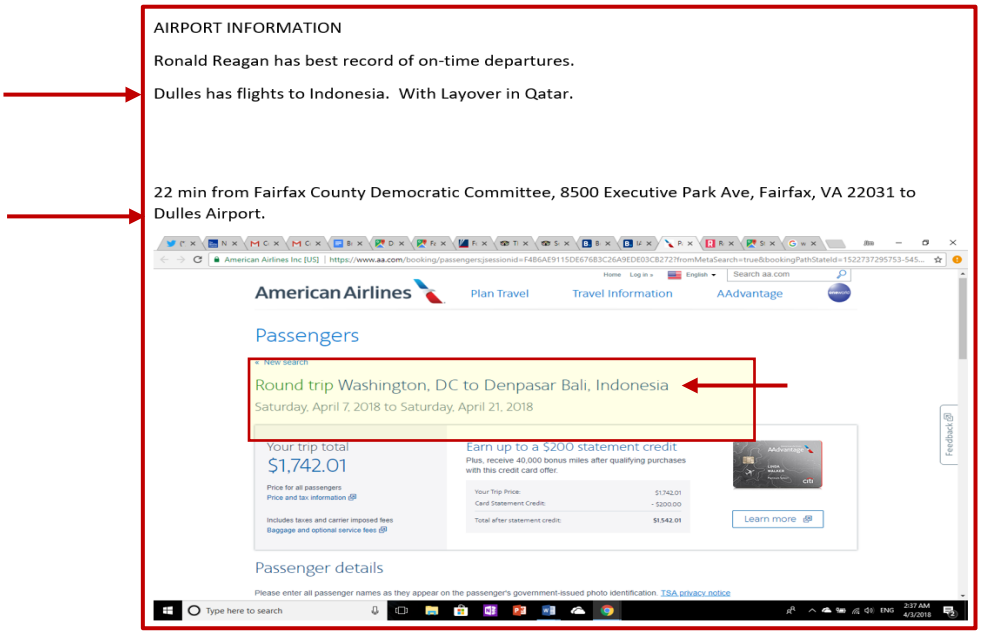


Fig.7

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	14c07920ddc81fbd489e61d60e5c9f28
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:	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

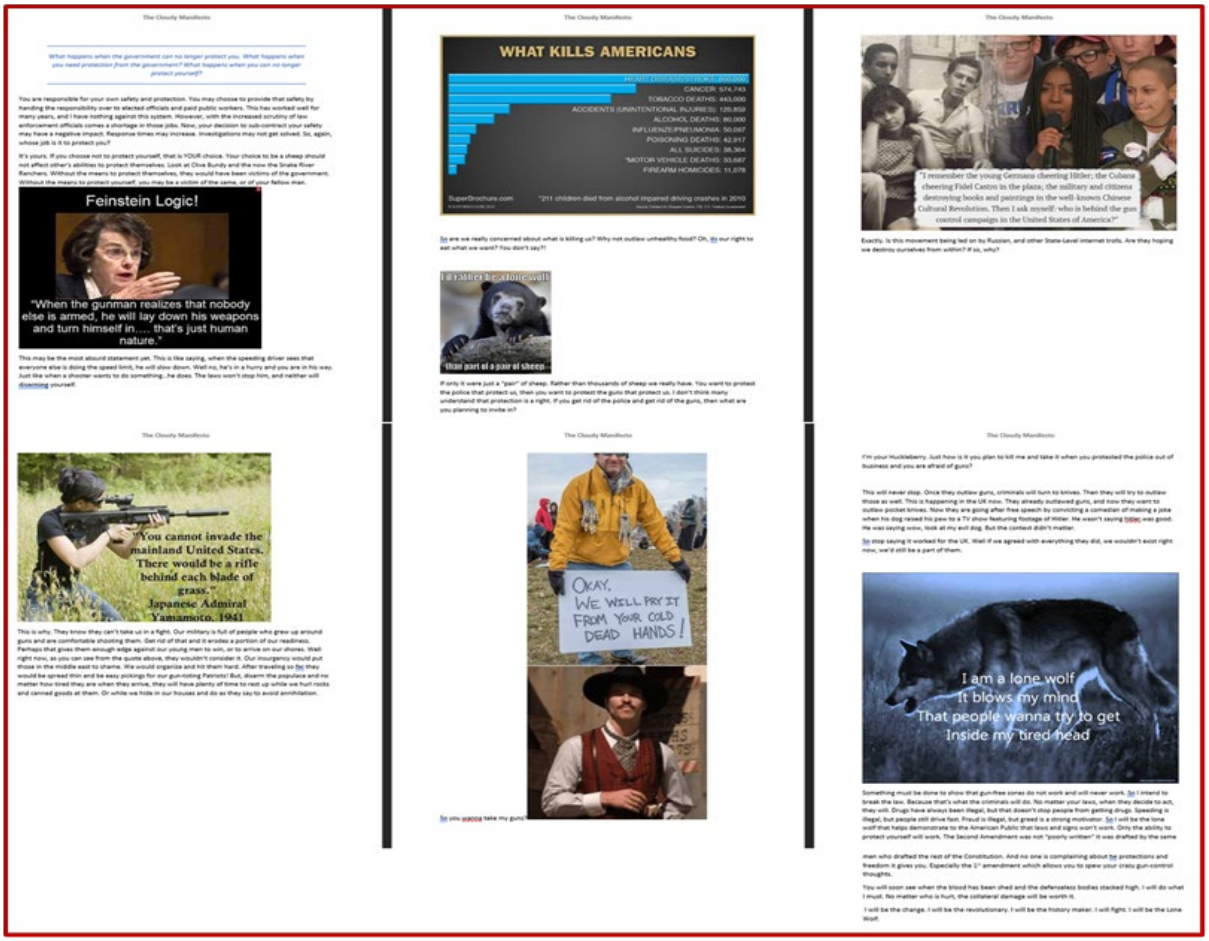


Fig.8

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_vol7/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:	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

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.

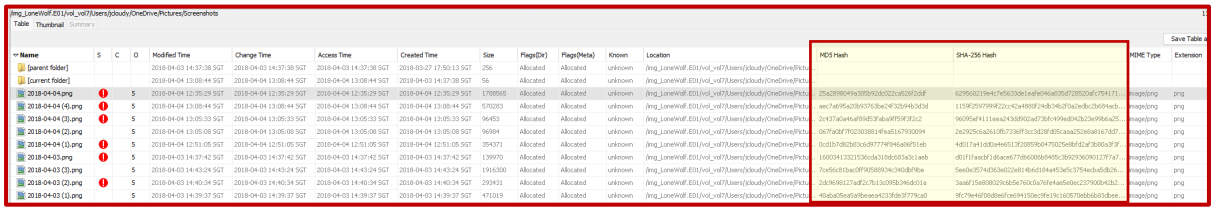


Fig.9

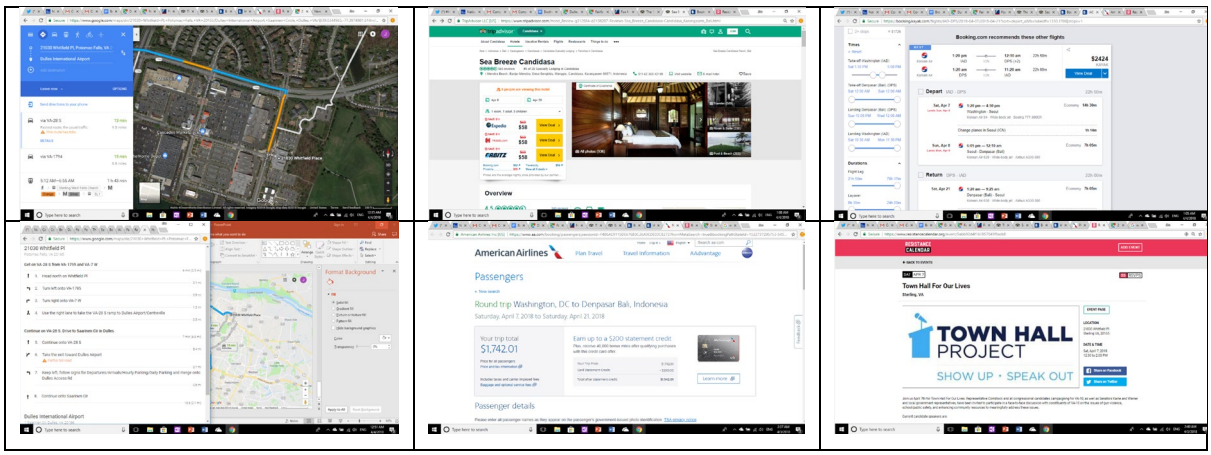


Table.1

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

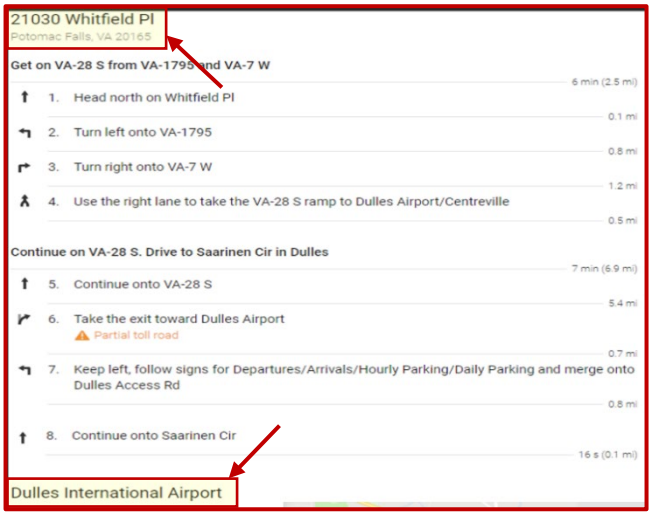


Fig.12

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*)

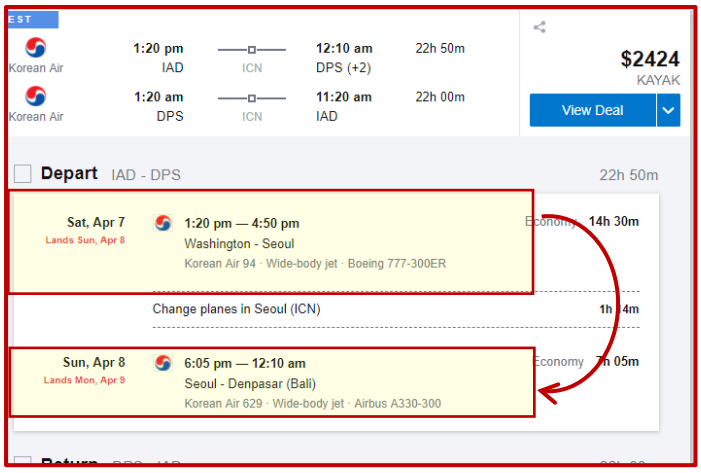


Fig.13

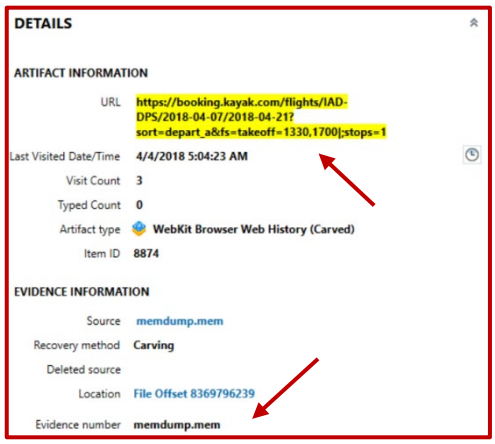


Fig.14

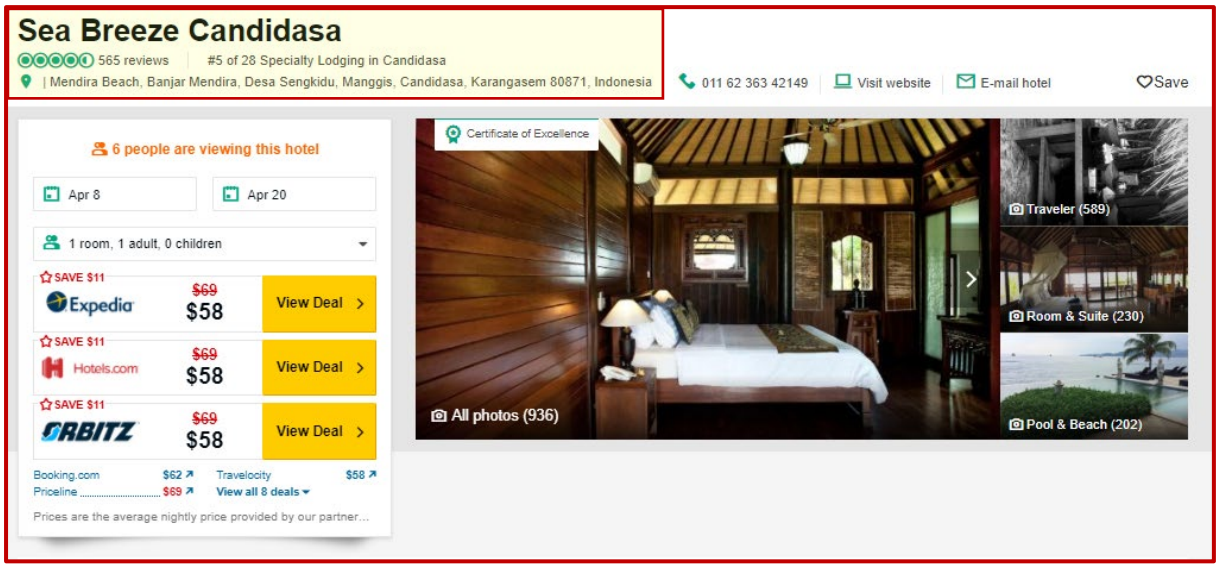


Fig.15

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

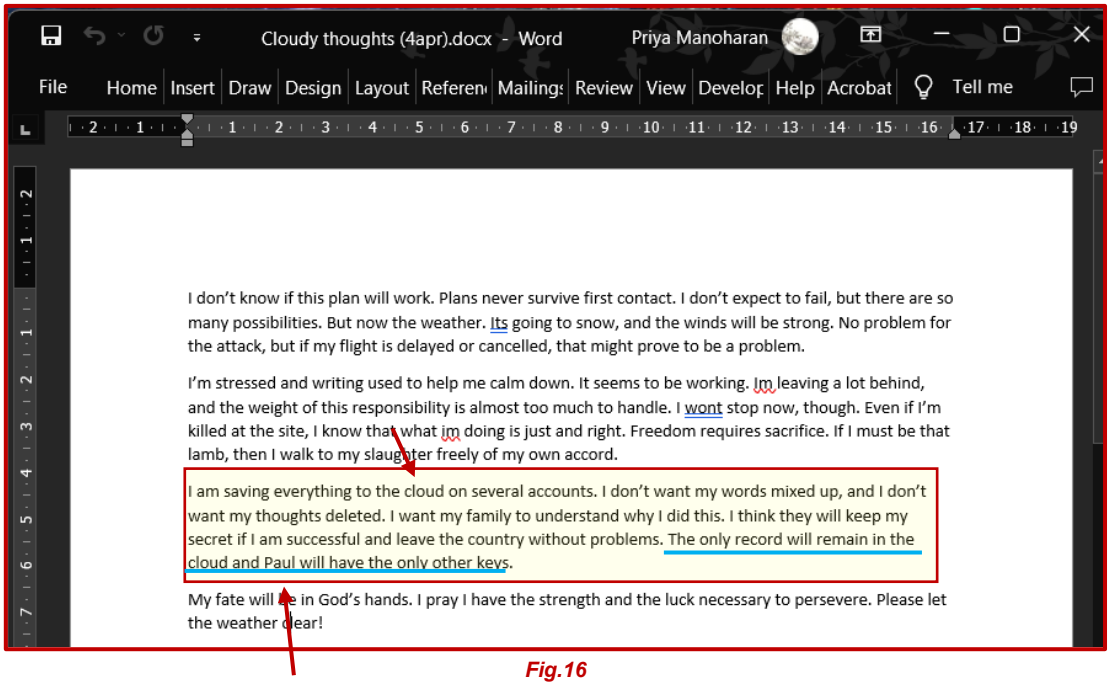


Fig.16

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

Exhibit F.00A

DETAILS

ARTIFACT INFORMATION

Email(s)	me <jimcloudy1@gmail.com>, Paul <paulcloudy2@gmail.com> (6)
Subject	Computer
Sent Date/Time - Local Time	Fri, Mar 30, 2018 at 8:58 PM
Last Activity Date/Time	31/3/2018 12:58:09 AM
Snippet	And how would YOU implement the solution? Unless you get elected it's going to be hard to implement your own solutions... On Thu, Mar 29, 2018 at 10:14 PM, Jim Cloudy <jimcloudy1@gmail.com>
Status	Read / Unread
Artifact type	Gmail Webmail
Item ID	8681

EVIDENCE INFORMATION

Source	memdump.mem
Recovery method	Carving
Deleted source	
Location	File Offset 8250066462
Evidence number	memdump.mem

1

DETAILS

ARTIFACT INFORMATION

Email(s)	me <jimcloudy1@gmail.com>, Paul <paulcloudy2@gmail.com> (9)
Subject	Computer
Sent Date/Time - Local Time	Sat, Mar 31, 2018 at 2:03 PM
Last Activity Date/Time	31/3/2018 7:44:39 PM
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 / Read
Artifact type	Gmail Webmail
Item ID	11295

EVIDENCE INFORMATION

Source	memdump.mem
Recovery method	Carving
Deleted source	
Location	File Offset 10603766772
Evidence number	memdump.mem

2

DETAILS

ARTIFACT INFORMATION

Email(s)	Paul <paulcloudy2@gmail.com>
Subject	Computer
Sent Date/Time - Local Time	Sat, Mar 31, 2018 at 2:03 PM
Last Activity Date/Time	6/4/2018 6:57:20 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
Status	Read
Artifact type	Gmail Webmail
Item ID	2562

EVIDENCE INFORMATION

Source	memdump.mem
Recovery method	Carving
Deleted source	
Location	File Offset 2058754769
Evidence number	memdump.mem

4

DETAILS

ARTIFACT INFORMATION

Email(s)	me <jimcloudy1@gmail.com>, Paul <paulcloudy2@gmail.com> (11)
Subject	Computer
Sent Date/Time - Local Time	Sat, Mar 31, 2018 at 2:03 PM
Last Activity Date/Time	4/4/2018 5:15:06 AM
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 / Read
Artifact type	Gmail Webmail
Item ID	15507

EVIDENCE INFORMATION

Source	memdump.mem
Recovery method	Carving
Deleted source	
Location	File Offset 15734340058
Evidence number	memdump.mem

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.

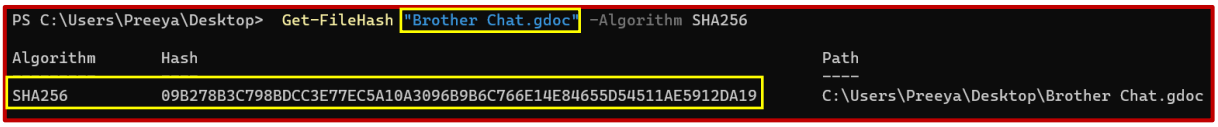


Fig.18

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

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.

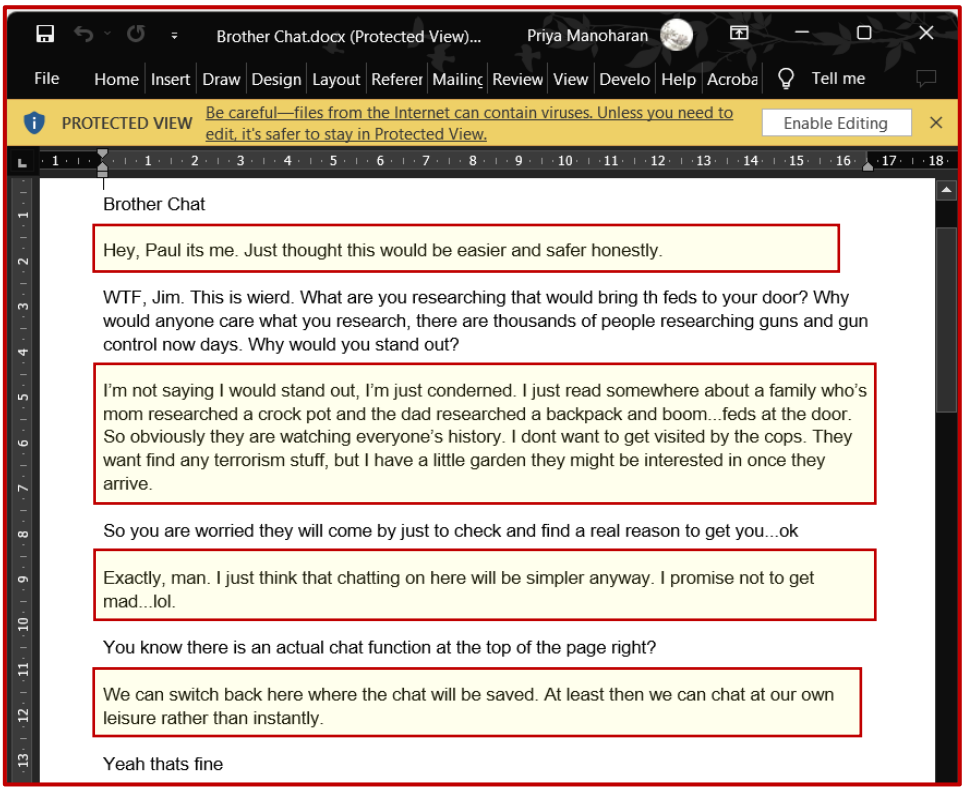


Fig.20

[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.

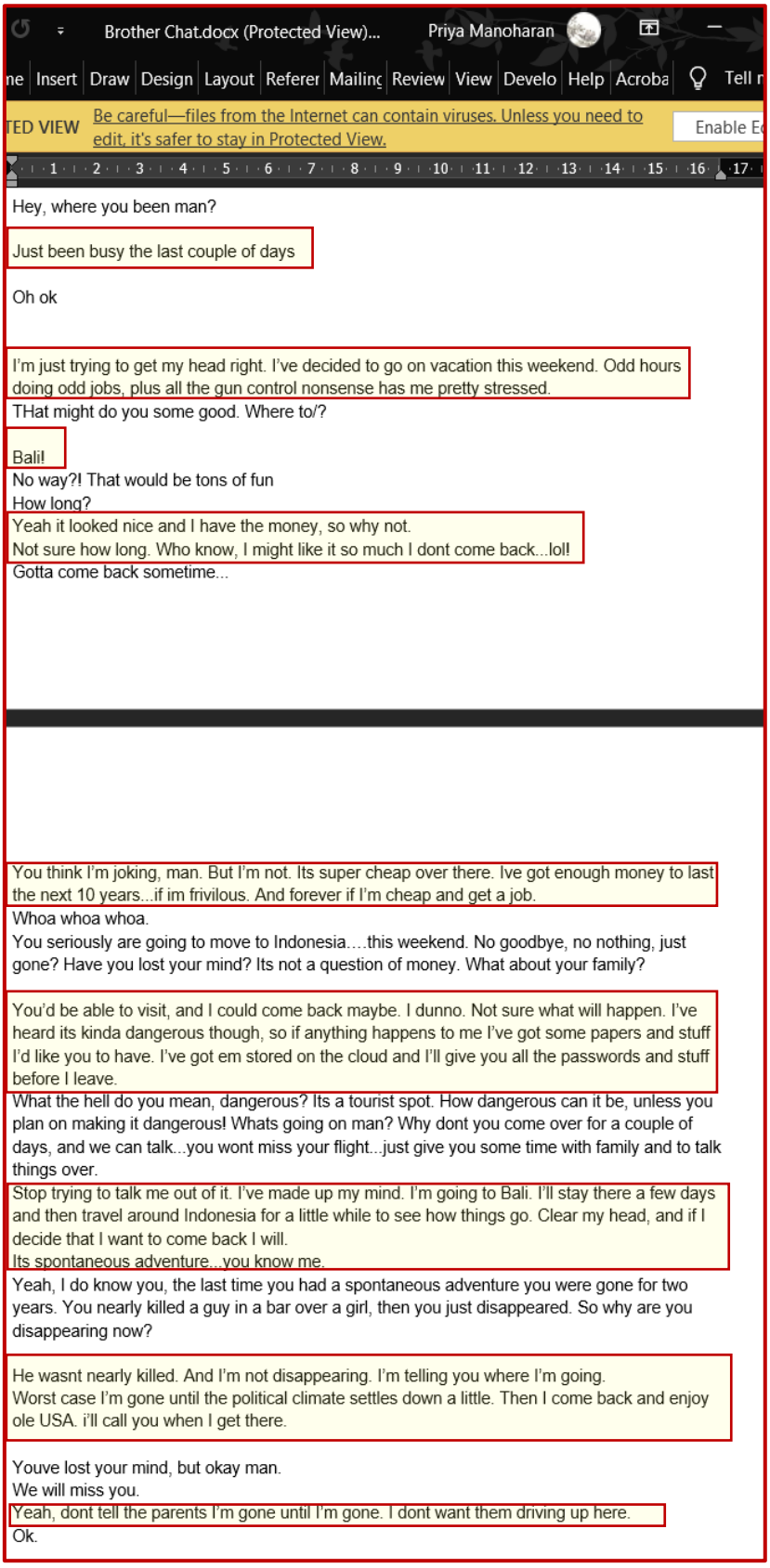


Fig.21

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

Exhibit F.01C

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

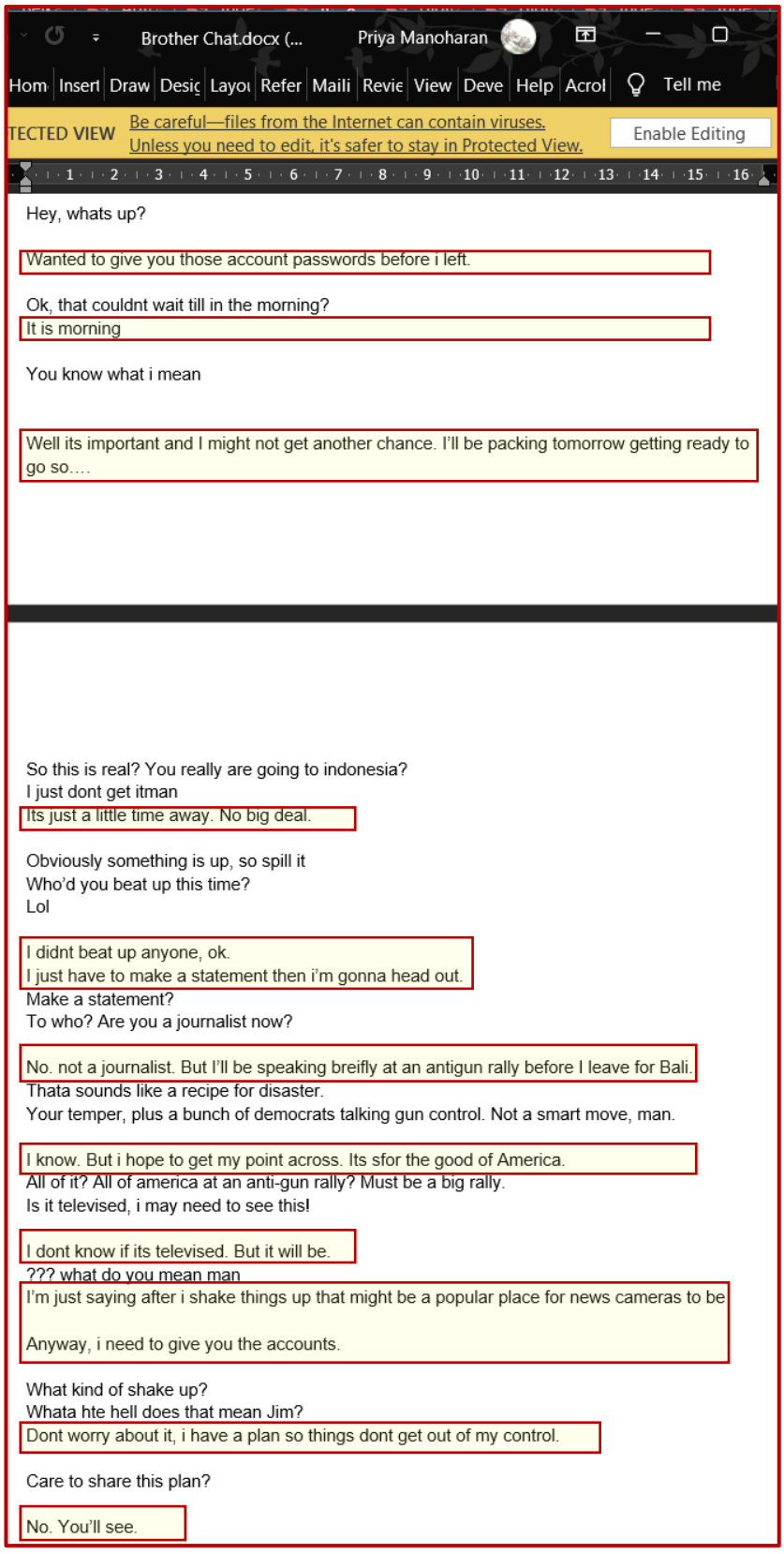


Fig.22

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

Exhibit F.01D

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

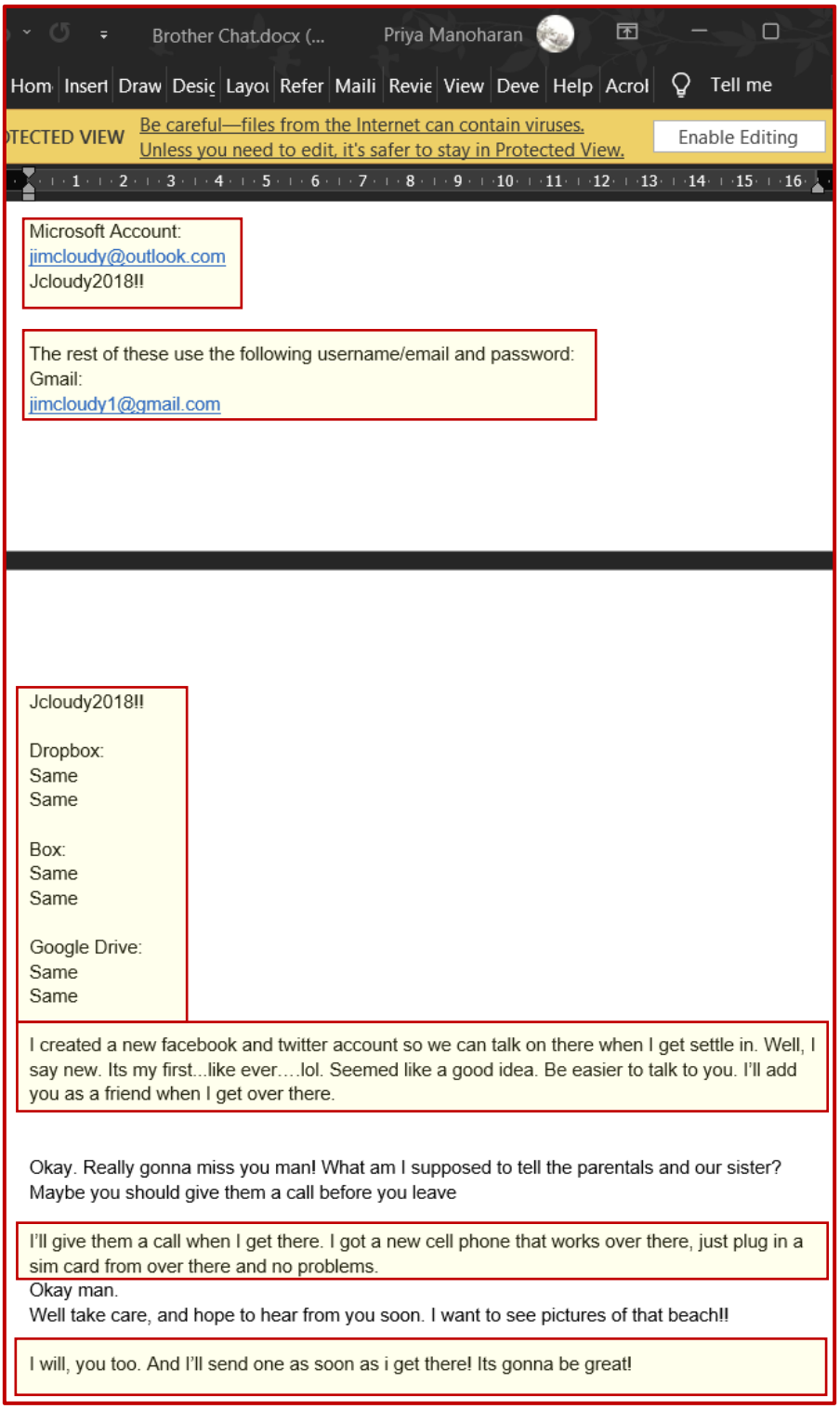


Fig.23

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                                                                   Path
---------       ----                                                                   ----
SHA256          BA05EC7140440AD463B6FA4E7685CABE368CB96890132DD7D2828AC3BECA5534      C:\Users\Preeya\Desktop\Brother Chat Google Doc Chat Window.txt
```

Fig.24

Chat 4: The yellow highlighted box is Jim.

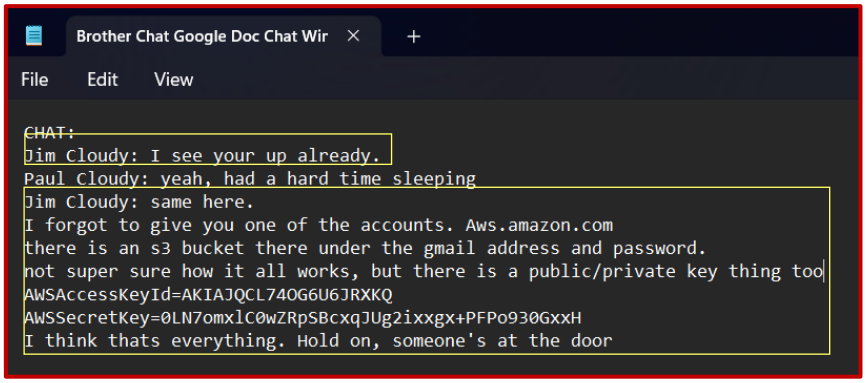


Fig.25

Item 7 – Exhibit F.03 – Login Data

Exhibit F.03

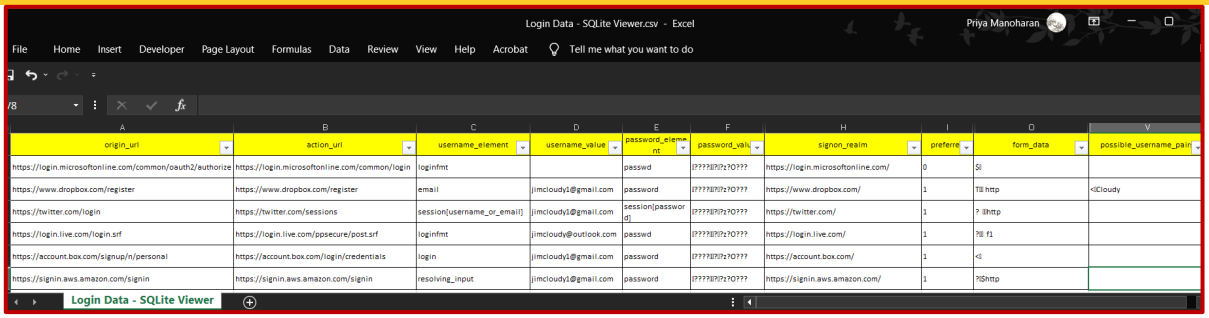


Fig.26

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_vol7/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) — Column view

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 8:38:09 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	UsnJrnl	Operating System	6/4/2018 6:14:39 AM
335032	Jim's Notebook.url	UsnJrnl	Operating System	6/4/2018 6:14:39 AM
335033	Jim's Notebook.url	UsnJrnl	Operating System	6/4/2018 6:14:39 AM
335034	Jim's Notebook.url	UsnJrnl	Operating System	6/4/2018 6:14:39 AM
335036	Jim's Notebook.url	UsnJrnl	Operating System	6/4/2018 6:14:39 AM
335037	Jim's Notebook.url	UsnJrnl	Operating System	6/4/2018 6:14:39 AM
335038	Jim's Notebook.url	UsnJrnl	Operating System	6/4/2018 6:14:39 AM
335039	Jim's Notebook.url	UsnJrnl	Operating System	6/4/2018 6:14:39 AM
335040	Jim's Notebook.url	UsnJrnl	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]

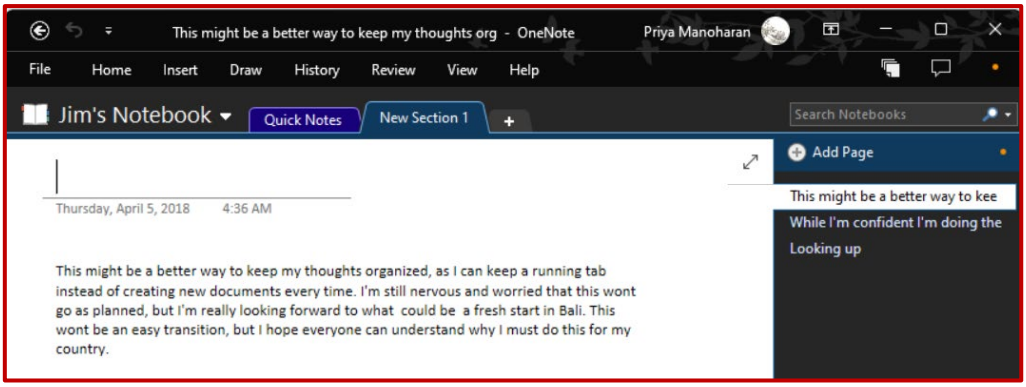


Fig.28

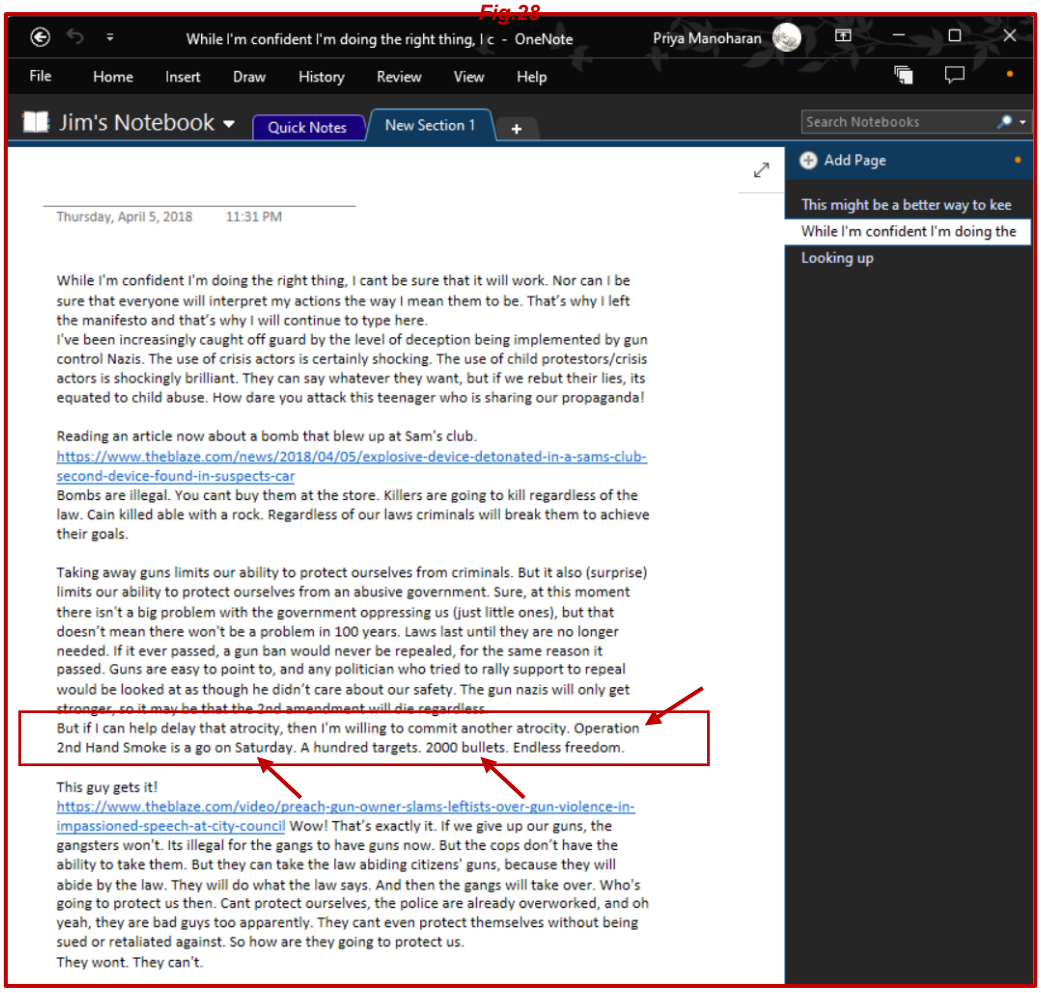


Fig.29

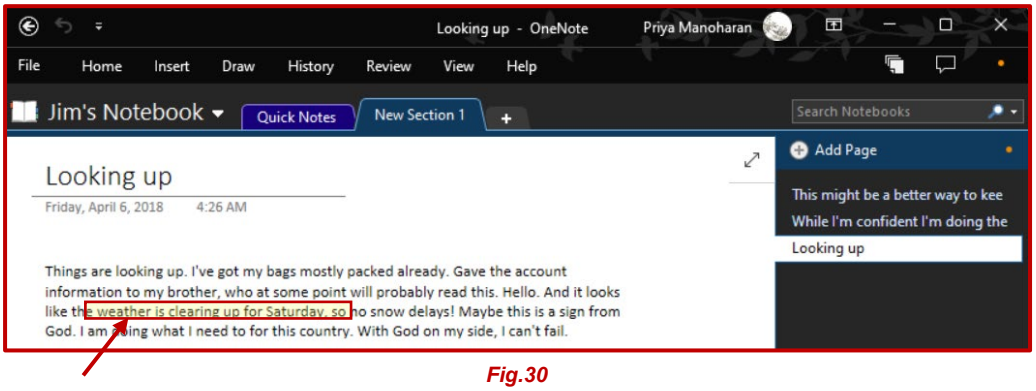
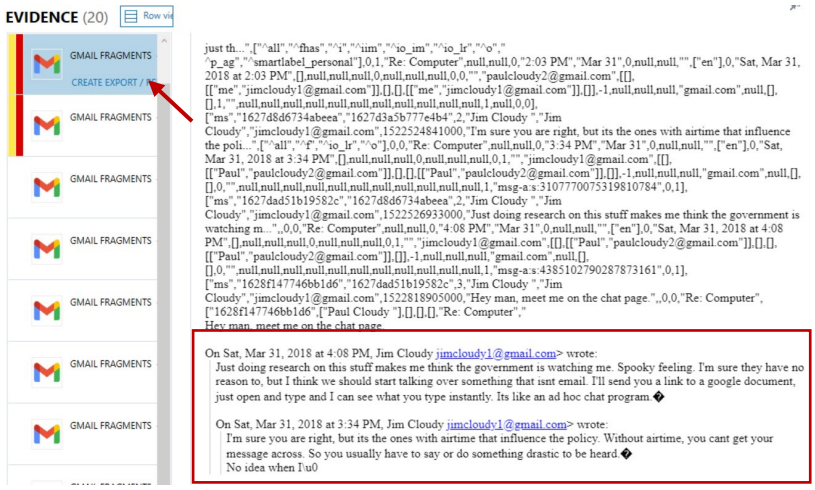


Fig.30

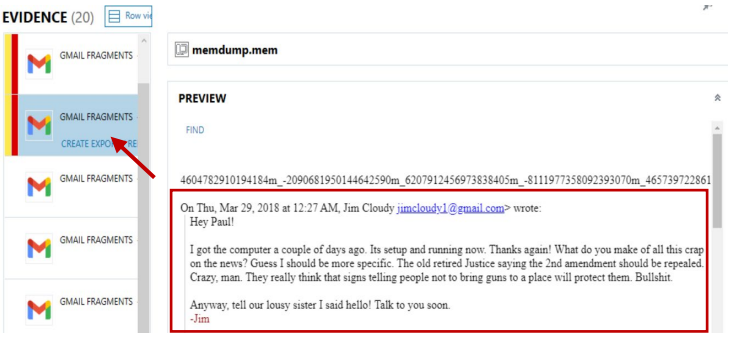
2.3.4. Evidence Class 4 – Emails Between Cloudy Brothers

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	

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	

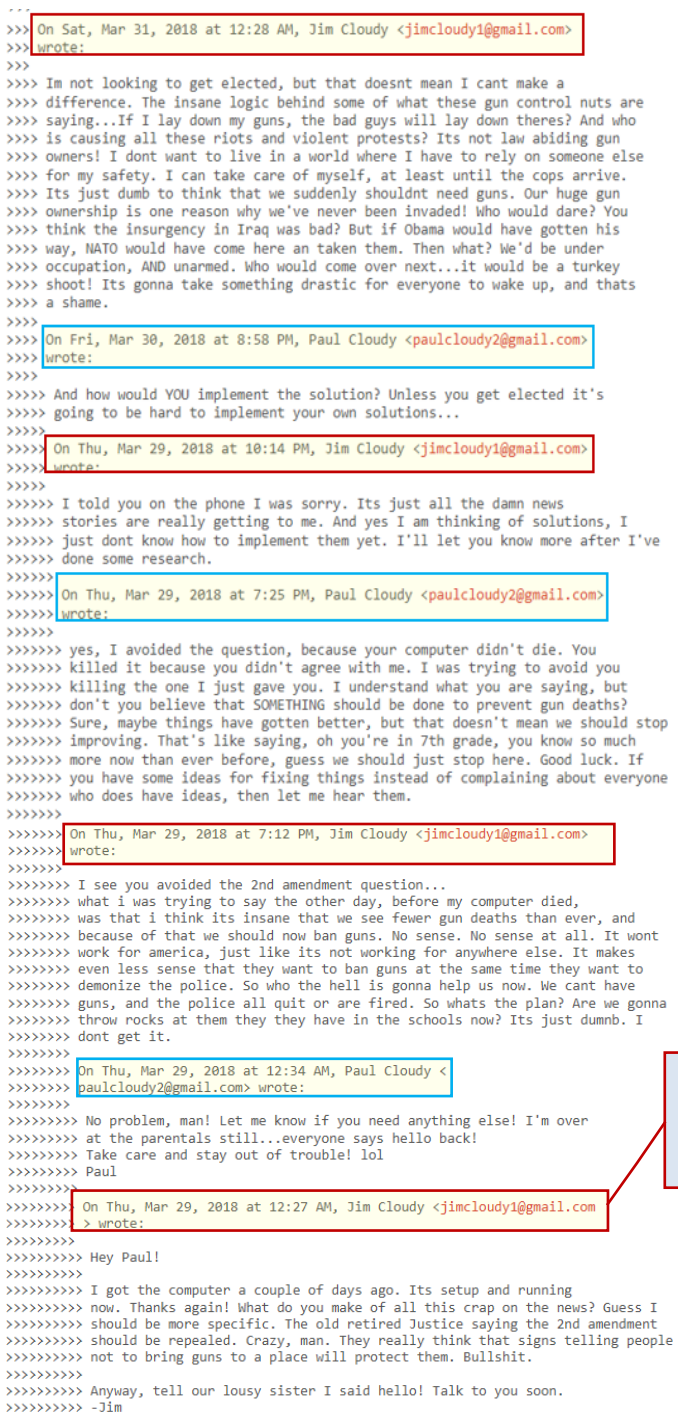
Based on the extraction done in 2018 by Tom Moore (DEFR and DES), we were able to analyse and reconstruct a clear picture of the entire conversation between the Cloudy brothers. It is in this email Sat, Mar 31st 2018, Jim Cloudy mentions of being watched by the government. This suggest that the "**AKMonitor.exe**" 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
Screenshot (fig.31 – p1)	


```
--94eb2c0592f2013b3d0568baed5d--

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 10.179.93.147 with HTTP; Tue, 3 Apr 2018 22:15:05 -0700 (PDT)
In-Reply-To: <CAG5i1tn7xsJyBHtf71tc17Tvu7WgTVYYBQHWJGfvXJ4n_R+Njg@mail.gmail.com>
References: <CAG5i1t=PhrrLFxs+BmZT14H=1HiJBOZ8PoVZduQOtmfjkpLYaw@mail.gmail.com>
    <CAJ5GETiuWrjEGf0=x++eNWWfHUd3wRcb63E8z6HtwZjQuR6rRQ@mail.gmail.com>
    <CAG5i1tnJdv_qx1SiGjcG9f5i+ja+OYhv7xhGQZKgBbxM+6dOUQ@mail.gmail.com>
    <CAJ5GETgZjLDLckjZpVRToM=JX2rw8qQ1HBn6Sb1Aqd85AhGy1w@mail.gmail.com>
    <CAG5i1tn8gQi_F7FqYfm2En70K2ffTjB8sv2mjOHxaaA_FroMcQ@mail.gmail.com>
    <CAJ5GEThSv4C4VDcTNeugQaO=5gJLZmQnR0ci+JHw_=w4BsyWRg@mail.gmail.com>
    <CAG5i1tmfG06jqS=FWz8pHuOUoK7mXRpEmbm_rpza8H9aAC9=Ag@mail.gmail.com>
    <CAJ5GEThavBOt+kHXabNcNy8AS=pw1z6BKTsBaaPYxVWbdzGFQg@mail.gmail.com>
    <CAG5i1tnsessPJBdheof405PES10jPqUt3-R3-q2CbmqJH5EWMw@mail.gmail.com>
    <CAG5i1tn7xsJyBHtf71tc17Tvu7WgTVYYBQHWJGfvXJ4n_R+Njg@mail.gmail.com>
Date: Wed, 4 Apr 2018 01:15:05 -0400
Delivered-To: jimcloudy1@gmail.com
Message-ID: <CAG5i1tmzXBgqyHiXREii+yRSqmzoYEj2NTR3PpmLzxi+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"

--089e08290fd4ed75000568fee7f9
Content-Type: text/plain; charset="UTF-8"

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 feeling. I'm sure they have no reason to, but I think
> we should start talking over something that isnt 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.
>
> 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?
```

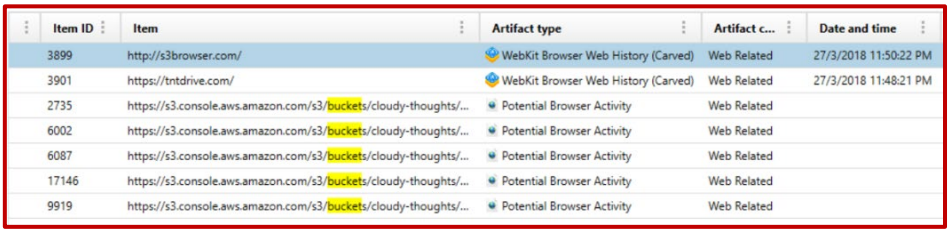
Item 9 – Exhibit H.02AA – Google Takeout

Exhibit H.02AA	
Artifact Type	**Gmail**
Item ID	1_ H.02AA
Source	**Tom Moore Analysis**
Location	Google
Screenshot (fig.31 – p2)	

2.3.5. Evidence Class 5 – Cloudy Cloud Storages

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

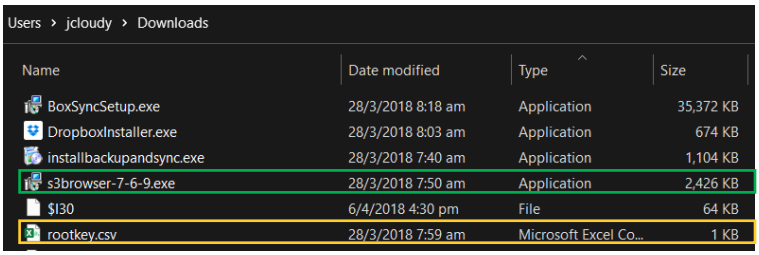
Exhibit I



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

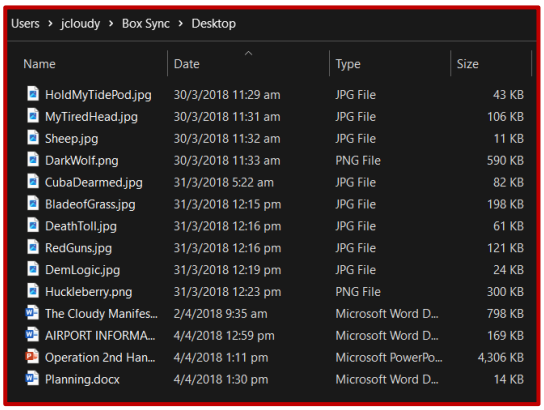
Name	Date modified	Type	Size
BoxSyncSetup.exe	28/3/2018 8:18 am	Application	35,372 KB
DropboxInstaller.exe	28/3/2018 8:03 am	Application	674 KB
installbackupandsync.exe	28/3/2018 7:40 am	Application	1,104 KB
s3browser-7-6-9.exe	28/3/2018 7:50 am	Application	2,426 KB
$I30	6/4/2018 4:30 pm	File	64 KB
rootkey.csv	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)".

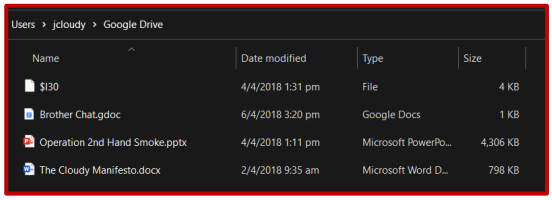
AWSAccessKeyId=AKIAJQCL74OG6U6JRXKQ
AWSSecretKey=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



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

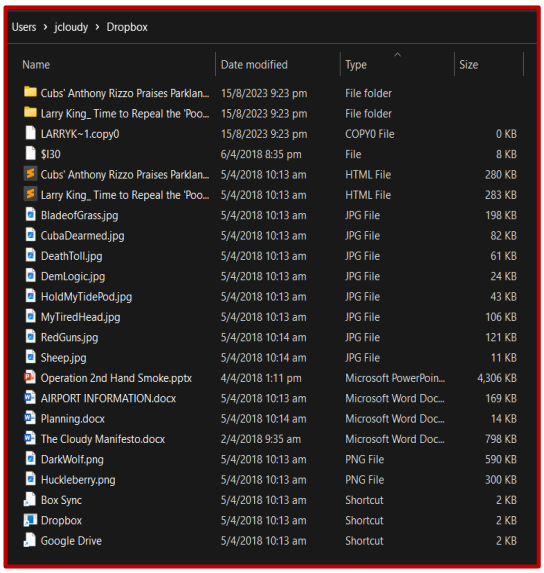
Fig.34 - BoxSync



Users › jcloudy › Google Drive

Name	Date modified	Type	Size
$I30	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



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 Repeal the 'Poo...	15/8/2023 9:23 pm	File folder	
LARRYK~1.copy0	15/8/2023 9:23 pm	COPY0 File	0 KB
$I30	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 Repeal 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 PowerPoin...	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

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

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

Types | Recent Programs | Recent Domains | Recent Web Searches

Recent Domains Accessed

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

Recent Domains

Recently Opened Documents

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\UKknifeBan.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

Recently Opened Documents | Timeline

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

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

Exhibit K

"Guns"

URL	Last Visited Dati	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID
https://tntdrive.com/	27/3/2018 23:48	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 23:58	TOP 5 FIGHTING GUNS - YouTube	1	memdump.mem	File Offset 5290203616	memdump.mem	Carving	4788
https://www.youtube.com/watch?v=rle3EcYnick	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=umIPCvkpaU4	28/3/2018 0:08	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=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?rlz=1C1CHBF_enUS7	29/3/2018 23:04	anti-gun rally near me - Google Search	1	memdump.mem	File Offset 1983949987	memdump.mem	Carving	2473
https://www.nokia.com/en_int/phones/nokia-216-du	29/3/2018 23:04	upcoming anti-gun rally near me - Google Search	1	memdump.mem	File Offset 1983949879	memdump.mem	Carving	2471
https://www.google.com/search?q=lone+wolf&tbm=i	30/3/2018 3:31	gun control great britain - Google Search	1	memdump.mem	File Offset 9601815699	memdump.mem	Carving	10292
https://www.google.com/maps/place/Indonesia/@-2	2/4/2018 0:53	fn 5 7 ammo For Sale - Buy fn 5 7 ammo Online at GunBroker.com	1	memdump.mem	File Offset 1865476163	memdump.mem	Carving	2331
https://www.google.com/search?q=cascades+library	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=cascades+library	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=cascades+library	3/4/2018 6:47	keltec 2000 site:gunbroker.com - Google Search	1	memdump.mem	File Offset 2677223722	memdump.mem	Carving	3115
https://www.google.com/search?q=cascades+library	3/4/2018 6:47	gunbroker - Google Search	1	memdump.mem	File Offset 2677223479	memdump.mem	Carving	3113

WebKit Browser Web History (Car

"Arms"

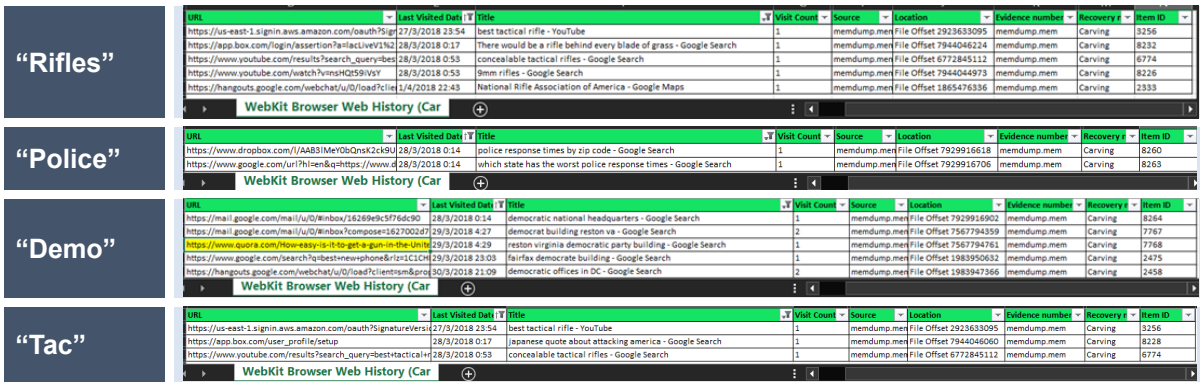
URL	Last Visited Dati	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID
https://www.google.com/search?q=tntdrive+vs&rlz=1C1CHBF_en	27/3/2018 23:49	Dual Wielding Challenge vs Army Sniper - YouTube	1	memdump.mem	File Offset 2393070091	memdump.mem	Carving	2837
https://megabackup.com/buynow/buynow-eol	28/3/2018 0:55	Services â€" NOVA FIREARMS	1	memdump.mem	File Offset 9350391711	memdump.mem	Carving	10103
https://megabackup.com/buynow/four-plans-1m-cle?	28/3/2018 0:55	FFL & Transfers â€" NOVA FIREARMS	1	memdump.mem	File Offset 9350391819	memdump.mem	Carving	10104
https://www.google.com/search?q=cascades+library+meeting+r	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=cascades+library+meeting+r	3/4/2018 6:48	NOVA FIREARMS	2	memdump.mem	File Offset 2677224707	memdump.mem	Carving	3123

WebKit Browser Web History (Car

"Ranch"

URL	Last Visited Dati	Title	Visit Count	Source	Location	Evidence number	Recovery	Item ID
https://twitter.com/search?q=%23MolonLabe&src=ty	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	7	memdump.mem	File Offset 9350390133	memdump.mem	Carving	10093

WebKit Browser Web History (Car

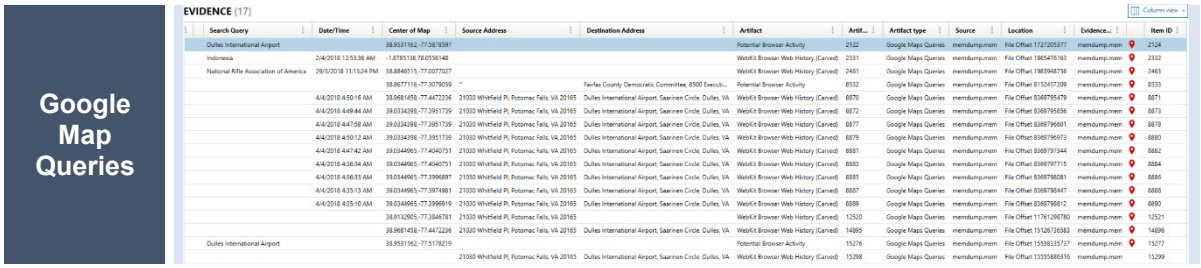


The above "***Item 12 – Exhibit K – Webkit Browser History (Carving) (memdump.mem)***" are some crucial searches that were made by the suspect that were carved during the memory dump analysis.

2.3.8. Evidence Class 8 – Google Map Queries

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

Exhibit L



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://wjla.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

Name:	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_001114
Type:	File System
MIME Type:	image/jpeg
Size:	31777
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2018-03-30 11:28:43 SGT
Accessed:	2018-03-30 11:28:43 SGT
Created:	2018-03-30 11:28:43 SGT
Changed:	2018-03-30 11:28:43 SGT
MD5:	0d2021e326615f5b81eda27630e7b30f
SHA-256:	ec361e397979bbf13b98fd4914e2c5d1d22ce5abcf77f72993db371636c002fc
Hash Lookup Results:	UNKNOWN
Internal ID:	18395

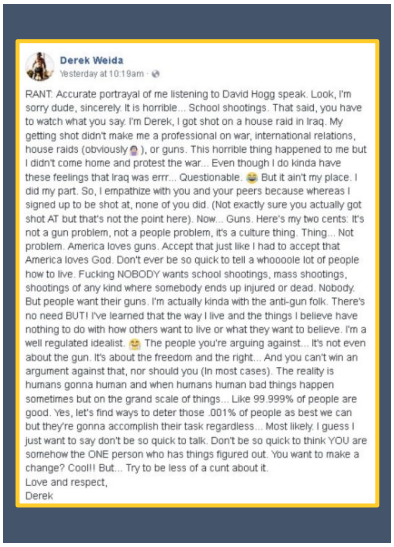
Name:	//img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_001784
Type:	File System
MIME Type:	image/jpeg
Size:	42301
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2018-03-31 12:42:26 SGT
Accessed:	2018-03-31 12:42:26 SGT
Created:	2018-03-31 12:42:26 SGT
Changed:	2018-03-31 12:42:26 SGT
MD5:	1e164af729d96e0acecea7326fa2324d
SHA-256:	293deec2f50db4672ead37808ee7eee44f522d4ea89dfe4174c37e4868e7a234
Hash Lookup Results:	UNKNOWN
Internal ID:	15772

Name:	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_001786
Type:	File System
MIME Type:	image/jpeg
Size:	25681
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2018-03-31 12:42:26 SGT
Accessed:	2018-03-31 12:42:26 SGT
Created:	2018-03-31 12:42:26 SGT
Changed:	2018-03-31 12:42:26 SGT
MD5:	df1624bf6b3f66b6b4061725d44327b8
SHA-256:	3b763c9849e3224e95b1b09caf5b63b491372946ccfac64296e52f87f14ce451
Hash Lookup Results:	UNKNOWN
Internal ID:	15776

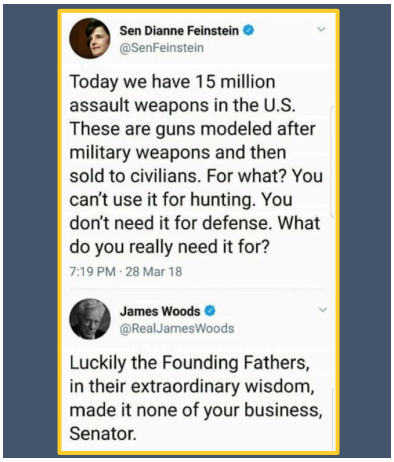
Name:	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_0017c1
Type:	File System
MIME Type:	image/jpeg
Size:	17073
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2018-03-31 12:44:27 SGT
Accessed:	2018-03-31 12:44:27 SGT
Created:	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

Name:	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_0017c2
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

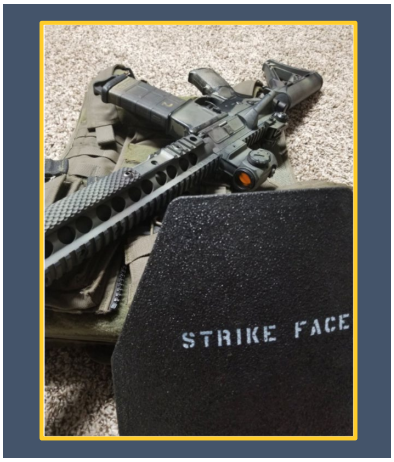
Filename:	f_0018cd
Source	LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\ jcloudy\\AppData\Local\Google\Chrome\User Data\Default\Cache\ f_0018cd
Recovery Method:	Carving
Location	File Offset 0
Last Created:	2018-03-31 7:13:35 PM
Last Accessed:	2018-03-31 7:13:35 PM
Last Modified:	2018-03-31 7:13:35 PM
MD5:	815f0b5bc98b9ab619719c0fc54b6295
SHA1:	1f0bbc2e379e38c2940c9028ac9162cead22d5c
Item ID:	540104



Filename:	f_001a27
Source	LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\ jcloudy\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:	9fb341ce44422472d6c9e9aff963c40e8b444c31
Item ID:	540247



Filename:	f_001a3a
Source	LoneWolf.E01 - Partition 4 (Microsoft NTFS, 476.34 GB)\Users\ jcloudy\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\ jcloudy\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:	6c0d2e1736abfe634fcd3b9c11861bf827d7261c
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:	9ddb1d74f40d4cffe959a4b6042bad4f
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.

Activity Range	
Earliest:	Jan 2, 1970
Latest:	Apr 6, 2018

Date	File Events	Result Events
Mar 26, 2018	722	0
Mar 27, 2018	273401	105700
Mar 28, 2018	4416	184900
Mar 29, 2018	5054	170300
Mar 30, 2018	7981	69800
Mar 31, 2018	2315	104900
Apr 1, 2018	548	80400
Apr 2, 2018	1192	20200
Apr 3, 2018	4626	45900
Apr 4, 2018	20929	142100
Apr 5, 2018	24349	102900
Apr 6, 2018	10819	163800

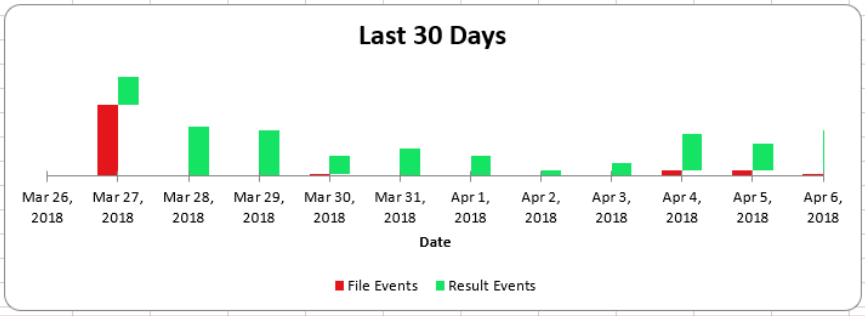


Fig.37 - Timeline

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.fliphtml5.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://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]